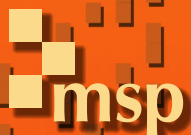


Algebra & Number Theory

Volume 17

2023

No. 2



Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR
Antoine Chambert-Loir
Université Paris-Diderot
France

EDITORIAL BOARD CHAIR
David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Jason P. Bell	University of Waterloo, Canada	Philippe Michel	École Polytechnique Fédérale de Lausanne
Bhargav Bhatt	University of Michigan, USA	Martin Olsson	University of California, Berkeley, USA
Frank Calegari	University of Chicago, USA	Irena Peeva	Cornell University, USA
J.-L. Colliot-Thélène	CNRS, Université Paris-Saclay, France	Jonathan Pila	University of Oxford, UK
Brian D. Conrad	Stanford University, USA	Anand Pillay	University of Notre Dame, USA
Samit Dasgupta	Duke University, USA	Bjorn Poonen	Massachusetts Institute of Technology, USA
Hélène Esnault	Freie Universität Berlin, Germany	Victor Reiner	University of Minnesota, USA
Gavril Farkas	Humboldt Universität zu Berlin, Germany	Peter Sarnak	Princeton University, USA
Sergey Fomin	University of Michigan, USA	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Wee Teck Gan	National University of Singapore	Shunsuke Takagi	University of Tokyo, Japan
Andrew Granville	Université de Montréal, Canada	Pham Huu Tiep	Rutgers University, USA
Ben J. Green	University of Oxford, UK	Ravi Vakil	Stanford University, USA
Christopher Hacon	University of Utah, USA	Akshay Venkatesh	Institute for Advanced Study, USA
Roger Heath-Brown	Oxford University, UK	Melanie Matchett Wood	Harvard University, USA
János Kollár	Princeton University, USA	Shou-Wu Zhang	Princeton University, USA
Michael J. Larsen	Indiana University Bloomington, USA		

PRODUCTION

production@msp.org
Silvio Levy, Scientific Editor


See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2023 is US \$485/year for the electronic version, and \$705/year (+\$65, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW[®] from MSP.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2023 Mathematical Sciences Publishers

Torsion points on elliptic curves over number fields of small degree

Maarten Derickx, Sheldon Kamienny, William Stein and Michael Stoll

Dedicated to the memory of Bas Edixhoven

We determine the set $S(d)$ of possible prime orders of K -rational points on elliptic curves over number fields K of degree d for $d = 4, 5, 6$, and 7 .

1. Introduction

Let K be an algebraic number field and let E be an elliptic curve over K . Then the group $E(K)$ of K -rational points on E is a finitely generated abelian group; in particular, its torsion subgroup $E(K)_{\text{tors}}$ is a finite abelian group, and one can ask which finite abelian groups can occur as the torsion subgroup of $E(K)$ for some elliptic curve over some number field K of degree d .

For $K = \mathbb{Q}$ (equivalently, $d = 1$), Mazur [1977; 1978] famously proved that the known finite list of possibilities for the torsion subgroup is complete. This was later extended by Merel [1996], who showed that for any given degree d , there are only finitely many possibilities for $E(K)_{\text{tors}}$ when $[K : \mathbb{Q}] = d$.

One key step in these finiteness results is to show that there are only finitely many prime numbers p that can divide the order of $E(K)_{\text{tors}}$, i.e., can occur as the order of an element of $E(K)$ for K of degree d . We therefore make the following definition (following [Kamienny and Mazur 1995]).

Definition 1.1. Let $d \geq 1$ be an integer. Then we define $S(d)$ to be the set of all prime numbers p such that there exists a number field K of degree d , an elliptic curve E over K and a point $P \in E(K)$ such that P has order p .

We write $\text{Primes}(x)$ for the set of all prime numbers p such that $p \leq x$.

Mazur showed that

$$S(1) = \text{Primes}(7).$$

Kamienny [1992a] determined

$$S(2) = \text{Primes}(13).$$

Merel [1996, Propositions 2 and 3] showed that

$$S(d) \subseteq \text{Primes}(2^{d+1}d!^{5d/2})$$

MSC2010: primary 11G05; secondary 14G05, 14G25, 14H52.

Keywords: elliptic curve, torsion point, torsion subgroup, number fields of small degree.

for $d \geq 4$. Parent [1999] gave the better bound (for all d)

$$S(d) \subseteq \text{Primes}(65(3^d - 1)(2d)^6).$$

However, Oesterlé had improved this already (as mentioned in Parent's paper) to

$$S(d) \subseteq \text{Primes}((3^{d/2} + 1)^2) \tag{1-1}$$

(except for not ruling out that $43 \in S(3)$) in his unpublished notes [Oesterlé 1994]. It should be noted that Parent actually shows that his bound is valid for prime *power* order p^n of a torsion point when $p \geq 5$ (and he has similar bounds for powers of 2 and 3); this is the main point of his work. Parent [2000; 2003], extending the techniques used by Mazur and Kamienny and relying on Oesterlé's work, proved that

$$S(3) = \text{Primes}(13).$$

The main result of this paper is the following theorem, which extends these results to $d = 4, 5, 6$, and 7.

Theorem 1.2.

$$S(4) = \text{Primes}(17), \quad S(5) = \text{Primes}(19), \quad S(6) = \text{Primes}(19) \cup \{37\}, \quad S(7) = \text{Primes}(23).$$

We also give a simplified proof of Parent's result on $S(3)$. Since we rely on Oesterlé's bound (1-1), a proof of which has not been published so far, we include a proof here that is based on Oesterlé's notes, which he kindly made available to us.

It is much easier to determine the set $S'(d)$ of primes p such that there are *infinitely many* elliptic curves E over number fields K of degree d with distinct j -invariants that have a K -point of order p . This is mostly a question about the gonality of the modular curve $X_1(p)$. The following is known.

Proposition 1.3.

$$\begin{aligned} S'(1) &= \text{Primes}(7), & S'(2) &= \text{Primes}(13), & S'(3) &= \text{Primes}(13), & S'(4) &= \text{Primes}(17), \\ S'(5) &= \text{Primes}(19), & S'(6) &= \text{Primes}(19), & S'(7) &= \text{Primes}(23), & S'(8) &= \text{Primes}(23). \end{aligned}$$

For $d = 1, 2, 3, 4$, this is shown in [Mazur 1977; Kamienny 1992a; Jeon et al. 2011a; 2011b] respectively; for $5 \leq d \leq 8$, this follows from [Derickx and van Hoeij 2014, Theorem 3]. Since clearly $S'(d) \subseteq S(d)$, these results, together with the fact that a quadratic twist $E_{6,37}$ over the sextic number field $K = \mathbb{Q}(\sqrt{5}, \cos(\frac{2\pi}{7}))$ of the elliptic curve

$$1225.b2: y^2 + xy + y = x^3 + x^2 - 8x + 6$$

has a point of order 37 over K [Elkies 1998, Equation 108], reduce the proof of Theorem 1.2 to showing the inclusions " \subseteq ".

We give the following more precise result in the case $d = 6$.

Proposition 1.4. *Let K be a number field of degree 6 and let E/K be an elliptic curve such that there is a point $P \in E(K)$ of exact order 37. Then $j(E) = j(E_{6,37}) = -9317$.*

We prove Proposition 1.4 at the end of Section 8.

The gonality of $X_1(p)$ grows like p^2 [Abramovich 1996]; this implies that $S'(d) \subset \text{Primes}(O(\sqrt{d}))$. On the other hand, denoting by $S_{\text{CM}}(d)$ the set of primes that can occur as orders of points on elliptic curves over a number field of degree d that have complex multiplication, the results of [Clark et al. 2013] show that $S_{\text{CM}}(s) \subset \text{Primes}(O(d))$ and that $3d+1 \in S_{\text{CM}}(d)$ when $3d+1$ is prime. (Let $p = 3d+1$. There is a pair of quadratic points defined over $\mathbb{Q}(\sqrt{-3})$ with j -invariant zero on $X_0(p)$. The set-theoretic preimage gives a Galois orbit of points of degree $2 \cdot \frac{1}{2}(p-1) \cdot \frac{1}{3} = d$ on $X_1(p)$, since the covering $X_1(p) \rightarrow X_0(p)$ ramifies with index 3 above the points with j -invariant zero.) So we will certainly have $S'(d) \subsetneq S(d)$ for infinitely many d . It is perhaps tempting to assume that for large enough d , the only sporadic points of degree d on $X_1(p)$ are CM points, as this seems to be the expectation for rational points on modular curves. This would imply that $S(d) \subseteq \text{Primes}(3d+1)$ for large d . However, consulting the table in [van Hoeij 2012], it appears that there are many sporadic non-CM points (like the degree 6 points on $X_1(37)$ we have mentioned above). Still, the bound $p \leq 3d+1$ is consistent with this information for $d \geq 13$.

The strategy. To show the inclusions “ \subseteq ” in Theorem 1.2, we have to verify that $p \notin S(d)$ for every prime number p that is not in the set on the right-hand side. This is equivalent to the statement that all points of degree dividing d on the modular curve $X_1(p)$ over \mathbb{Q} are cusps. Recall that noncuspidal points on $X_1(N)$, for $N \in \mathbb{Z}_{\geq 2}$, correspond to pairs (E, P) , where E is an elliptic curve and $P \in E$ is a point of exact order N . See Section 2 for some background on modular curves.

Now if $x \in X_1(p)(K)$ is a point defined over a number field K of degree d , but not over a smaller field, then the sum of its Galois conjugates gives a \mathbb{Q} -rational effective divisor of degree d on $X_1(p)$. If x is defined over a smaller field K' , then the degree d' of K' divides d , and we can take d/d' times the sum of the conjugates of x to obtain a \mathbb{Q} -rational effective divisor of degree d again. Effective divisors of degree d on a curve X correspond to points on its d -th symmetric power $X^{(d)}$ (which is the quotient of X^d by the natural action of the symmetric group on d letters). This leads to the following criterion. We write $C_1(p)$ for the set of cusps on $X_1(p)$.

Lemma 1.5. *Let $d \in \mathbb{Z}_{\geq 1}$ and let p be a prime number. If the composition*

$$\alpha : C_1(p)(\mathbb{Q})^d \rightarrow X_1(p)(\mathbb{Q})^d \rightarrow X_1(p)^{(d)}(\mathbb{Q})$$

of natural maps is surjective, then $p \notin S(d)$.

If $p > 2d+1$ and $p \notin S(d')$ for all $d' \leq d$, then the map above is surjective.

Proof. The assumption is equivalent to the statement that every \mathbb{Q} -rational effective divisor of degree d on $X_1(p)$ is a sum of rational cusps. However, if there were a number field K of degree d , an elliptic curve E over K and a point $P \in E(K)$ of order p , then (E, P) would give a K -rational noncuspidal point on $X_1(p)$ and hence, by the discussion above, a \mathbb{Q} -rational effective divisor of degree d that is not supported on (rational) cusps, contradicting the assumption.

For the converse, assume that the map is not surjective. Then there is a \mathbb{Q} -rational effective divisor D of degree d that is not supported on rational cusps. Since the irrational cusps on $X_1(p)$ form one Galois

orbit of size $(p-1)/2 > d$, D is not supported on cusps. This implies that there is a noncuspidal point on $X_1(p)$ of degree $d' \leq d$, and hence $p \in S(d')$. \square

We will follow the strategy that has been established in earlier work by Mazur [1978], Kamienny [1992b; 1992a], Merel [1996], Oesterlé [1994] and Parent [1999; 2000; 2003]. We give an overview of the main steps below; for a nice and more detailed account of Merel's proof of the boundedness of $S(d)$ for all d , see [Rebolledo 2009].

In our exposition, we refer to the existing literature for proofs of many results we are using. Fairly detailed proofs of these statements can be found in an earlier version of this paper [Derickx et al. 2017] or in the doctoral thesis [Derickx 2016].

The task is to show that $p \notin S(d)$ for $3 \leq d \leq 7$ and all primes p not contained in the set on the right-hand side of the equality in Theorem 1.2. We use the criterion of Lemma 1.5, in the equivalent form given below. Before we formulate it, we make some definitions.

Definition 1.6. Let ℓ be a prime. We write $\mathbb{Z}_{(\ell)}$ for the localization of \mathbb{Z} at the prime ideal $(\ell) = \ell\mathbb{Z}$.

Let X be a scheme over $\mathbb{Z}_{(\ell)}$. We denote the natural map $X(\mathbb{Z}_{(\ell)}) \rightarrow X(\mathbb{F}_\ell)$ by red_ℓ . Let $\bar{x} \in X(\mathbb{F}_\ell)$. Then $\text{red}_\ell^{-1}(\bar{x})$ is the *residue class* of \bar{x} . When X is a model over $\mathbb{Z}_{(\ell)}$ of a projective variety over \mathbb{Q} , then $X(\mathbb{Z}_{(\ell)}) = X(\mathbb{Q})$, so that we can think of the residue class of \bar{x} as the set of rational points on X reducing mod ℓ to \bar{x} .

Recall that $X_1(p)$ has a smooth model over $\mathbb{Z}[1/p]$; this implies the corresponding statement for the d -th symmetric power $X_1(p)^{(d)}$.

Lemma 1.7. *Let $\ell \neq p$ be a prime. Assume that:*

- (a) *The residue class of each point $\bar{x} \in X_1(p)^{(d)}(\mathbb{F}_\ell)$ that is a sum of images under red_ℓ of rational cusps contains at most one rational point.*
- (b) *The residue class of each point $\bar{x} \in X_1(p)^{(d)}(\mathbb{F}_\ell)$ that is not a sum of images under red_ℓ of rational cusps contains no rational point.*

Then $p \notin S(d)$.

Proof. Let $x \in X_1(p)^{(d)}(\mathbb{Q})$ and write $\bar{x} = \text{red}_\ell(x) \in X_1(p)^{(d)}(\mathbb{F}_\ell)$. By assumption (b), $\bar{x} = \bar{x}_1 + \cdots + \bar{x}_d$ is a sum of images of rational cusps. Let $x_1, \dots, x_d \in X_1(p)(\mathbb{Q})$ be rational cusps such that $\text{red}_\ell(x_j) = \bar{x}_j$ for $1 \leq j \leq d$. Then $x' = x_1 + \cdots + x_d \in X_1(p)^{(d)}(\mathbb{Q})$ is such that $\text{red}_\ell(x') = \bar{x}$. By assumption (a), x is the only rational point in the residue class of \bar{x} , so it follows that $x' = x \in \text{im}(\alpha)$ with α as in Lemma 1.5. So α is surjective, and Lemma 1.5 shows that $p \notin S(d)$. \square

Fix a rational cusp $c \in X_1(p)(\mathbb{Q})$. We can then define a morphism $\iota : X_1(p)^{(d)} \rightarrow J_1(p)$ by sending $x_1 + \cdots + x_d$ to the class of the divisor $x_1 + \cdots + x_d - d \cdot c$; here $J_1(p)$ denotes the Jacobian variety of $X_1(p)$; see Section 2 below. This map is actually defined over $\mathbb{Z}[1/p]$.

The standard way of verifying assumption (a) is to show that there is a morphism $t : J_1(p) \rightarrow A$

of abelian varieties such that

- (i) $t \circ \iota$ is injective on each residue class of a point \bar{x} as in assumption (a), and
- (ii) $\text{red}_\ell : t(J_1(p)(\mathbb{Q})) \rightarrow A(\mathbb{F}_\ell)$ is injective.

By standard properties of red_ℓ on the rational torsion subgroup, the second condition is satisfied when $t(J_1(p)(\mathbb{Q}))$ is finite and either ℓ is odd or $\ell = 2$ and $t(J_1(p)(\mathbb{Q}))$ has odd order. We can achieve this by choosing A as a factor of $J_1(p)$ that has Mordell–Weil rank zero and t to be the projection to A (plus some technicalities when $\ell = 2$). By work of Kolyvagin and Logachëv [1989] and Kato [2004], it is known that the “winding quotient” $J_1^e(p)$ of $J_1(p)$ has Mordell–Weil rank zero. Assuming the Birch and Swinnerton-Dyer conjecture for abelian varieties, $J_1^e(p)$ is in fact the largest such quotient. See Section 2 for the definition of the winding quotient.

The first condition follows if it can be shown that $t \circ \iota$ is a “formal immersion” at the relevant points \bar{x} ; see Section 4.

We can work with $J_0(p)$ in place of $J_1(p)$. Then there is only one point \bar{x} to consider, which is d times the image of the rational cusp ∞ on $X_0(p)$. This is what Mazur and Kamienny used to determine $S(1)$ and $S(2)$ and is also used in Merel’s proof of an explicit bound on $S(d)$ for all d and Oesterlé’s improvement of the bound. In all this work, odd primes ℓ are used. To deal with $S(3)$, Parent had to work with $J_1(p)$ (which was made possible by Kato’s work showing that the winding quotient has rank zero) and also had to use $\ell = 2$ to exclude some of the primes.

One minor innovation we introduce here is that we work with some intermediate curve X_H between $X_1(p)$ and $X_0(p)$; see again Section 2. This can reduce the necessary work in cases when using $J_0(p)$ is not successful, but the dimension of $J_1(p)$ is too large to make computations feasible.

Assuming Oesterlé’s bound (1-1), verification of assumption (a) amounts to exhibiting a suitable t for each prime $p \leq (3^{d/2} + 1)^2$ such that $p \notin S(d)$ and checking that it satisfies the conditions. This can be done by an explicit computation using modular symbols, which is based on a criterion established by Kamienny for $J_0(p)$ and extended to $J_1(p)$ by Parent. In view of assumption (b) (see below), we work with $\ell = 2$, which necessitates using “Parent’s trick” to deal with the technicalities that arise when ℓ is not odd.

For certain small primes, this is not sufficient. For $d \leq 7$, these primes p have the property that $J_1(p)(\mathbb{Q})$ is finite, which allows us to work with the full Jacobian and perform some more direct computations. This is another new ingredient compared to earlier work. In the course of our work, we establish an open case of a conjecture of Conrad, Edixhoven and Stein: we show that the group $J_1(29)(\mathbb{Q})$ (which is finite) is generated by differences of rational cusps on $X_1(29)$; see Theorem 3.2.

Combining both approaches, we obtain the following result.

Proposition 1.8. *Let $p \leq 2281 = \lfloor (3^{7/2} + 1)^2 \rfloor$ be a prime. If*

$$\begin{aligned} d = 3 \quad \text{and} \quad p \geq 17 \quad \text{or} \quad d = 4 \quad \text{and} \quad p \geq 19 \quad \text{or} \quad d = 5 \quad \text{and} \quad p \geq 23 \\ \text{or} \quad d = 6 \quad \text{and} \quad p \geq 23 \quad \text{or} \quad d = 7 \quad \text{and} \quad p \geq 29, \end{aligned}$$

then assumption (a) of Lemma 1.7 is satisfied.

Proposition 1.8 is proved in Section 5.

We now consider assumption (b) of Lemma 1.7. The simplest way for the assumption to be satisfied is when there are no points \bar{x} that are not sums of images of rational cusps. Equivalently,

- (i) there is no elliptic curve E over $\mathbb{F}_{\ell^{d'}}$ with $d' \leq d$ such that $p \mid \#E(\mathbb{F}_{\ell^{d'}})$, and
- (ii) $p \nmid \ell^{d'} \pm 1$ for all $d' \leq d$.

The first condition excludes the existence of noncuspidal points, whereas the second excludes the possibility that $X_1(p)(\mathbb{F}_{\ell^{d'}})$ contains cusps that are not images of rational cusps. Recall that the irrational cusps are defined over the maximal real subfield of $\mathbb{Q}(\mu_p)$, which has a place of degree dividing d above ℓ if and only if $\ell^d \equiv \pm 1 \pmod{p}$.

We note the following simple consequence.

Lemma 1.9. *If $p > (\ell^{d/2} + 1)^2$, then assumption (b) of Lemma 1.7 is satisfied.*

Proof. If there is an elliptic curve E over $\mathbb{F}_{\ell^{d'}}$ with $d' \leq d$ such that $p \mid \#E(\mathbb{F}_{\ell^{d'}})$, then by the Hasse bound,

$$p \leq \#E(\mathbb{F}_{\ell^{d'}}) \leq (\ell^{d'/2} + 1)^2 \leq (\ell^{d/2} + 1)^2,$$

which is not the case, so condition (i) above is satisfied. Since $p > (\ell^{d/2} + 1)^2 > \ell^d + 1$, condition (ii) is also satisfied. \square

This explains the form of Oesterlé's bound (1-1), which is related to the fact that he is working with $\ell = 3$.

We also see that it is advantageous to use the smallest possible ℓ , because then the condition of Lemma 1.9 covers more primes p . But even using $\ell = 2$, we need to verify assumption (b) for some primes $p < (2^{d/2} + 1)^2$. In some cases, we can still show for such primes that there are no points \bar{x} that are not sums of images of rational cusps, but this is not enough: when

$$(d, p) \in \{(5, 31), (5, 41), (6, 29), (6, 31), (6, 41), (6, 73), (7, 29), (7, 31), (7, 37), (7, 41), (7, 43), \\ (7, 59), (7, 61), (7, 67), (7, 71), (7, 73), (7, 113), (7, 127)\},$$

there actually are such points, and we have to work quite a bit harder to show that they are not images of rational points on $X_1(p)^{(d)}$. This is another novel aspect of our work. We use a number of different approaches (for $p = 37$, see further below).

- (1) For $p \in \{29, 31, 41\}$, we can again use direct computations based on the fact that $J_1(p)(\mathbb{Q})$ is finite and known; see Lemma 3.7.
- (2) For $p \in \{71, 113, 127\}$ and $d = 7$, we use a new criterion based on gonality estimates and working with Hecke operators as correspondences, which shows directly that $p \notin S(d)$; see Corollary 7.2.
- (3) For $(d, p) \in \{(6, 73), (7, 43)\}$, we use an intermediate curve X_H such that $X_H^{(d)}$ possesses a rational point x_H in the image of the relevant residue class and use a formal immersion argument to show that it is the only rational point in this residue class. This implies that every rational point on $X_1(p)^{(d)}$

in the residue class of \bar{x} must map to x_H , but x_H does not lift to a rational point on $X_1(p)^{(d)}$; see Lemmas 8.4 and 8.5.

- (4) For $p \in \{59, 61, 67, 73\}$ and $d = 7$, we use another new criterion that shows that a noncuspidal point $\bar{x} \in X_1(p)^{(d)}(\mathbb{F}_2)$ is not the reduction mod 2 of a rational point by showing that its image in $J_1(p)(\mathbb{F}_2)$ is not in the reduction of the Mordell–Weil group; see Lemma 8.7.

We then obtain the following result.

Proposition 1.10. *For the following pairs of an integer $3 \leq d \leq 7$ and a prime p , assumption (b) of Lemma 1.7 is satisfied:*

$$\begin{aligned} d = 3 & \quad \text{and} \quad p = 11 \quad \text{or} \quad p \geq 17; \\ d = 4 & \quad \text{and} \quad p \geq 19; \\ d = 5 & \quad \text{and} \quad p \geq 23; \\ d = 6 & \quad \text{and} \quad p \geq 23 \quad \text{and} \quad p \neq 37; \\ d = 7 & \quad \text{and} \quad p \geq 29 \quad \text{and} \quad p \neq 37. \end{aligned}$$

Proposition 1.10 is proved in Section 8.

We still have to show Proposition 1.4 and that $37 \notin S(7)$. We combine the approaches in (3) and (4) to do this. We first show using (4) that no noncuspidal point in $X_1(37)^{(7)}(\mathbb{F}_2)$ is the reduction mod 2 of a rational point and there is essentially only one such point in $X_1(37)^{(6)}(\mathbb{F}_2)$. We then use the formal immersion argument as in (3) to show that the remaining points in $X_1(37)^{(d)}(\mathbb{F}_2)$ for $d = 6, 7$ lift uniquely to rational points; see Lemmas 8.8 and 8.9.

Theorem 1.2 then follows from this and Propositions 1.8 and 1.10, using Lemma 1.7 and Oesterlé’s bound (1-1).

A large part of the work done in this paper relies heavily on computations. We provide Magma [Bosma et al. 1997] code (with explanatory comments) for all these computations in an online supplement. The timings we give in some places in this paper were obtained on the last author’s current laptop (as of 2020). All computations together took about one day on this machine. We also provide [SageMath] code at the first author’s GitHub site [Derickx 2020] that independently verifies the claims made in Section 5. Some of these computations rely on modular symbols. See for example [Stein 2007] for the necessary background.

The structure of the paper. We begin by recalling some background on modular curves in Section 2. In Section 3, we quote the list of primes p such that $J_1(p)(\mathbb{Q})$ is finite from [Conrad et al. 2003] and prove that for such primes, $J_1(p)(\mathbb{Q})$ is generated by differences of rational cusps (the new case being $p = 29$) and that the reduction map $J_1(p)(\mathbb{Q}) \rightarrow J_1(p)(\mathbb{F}_2)$ is injective. We use this to prove assumption (b) for $p = 29, 31$, and 41. In Section 4, we introduce formal immersions and state the computational criterion we use to verify assumption (a). Section 5 reports on these computations, and Section 6 contains the proof of Oesterlé’s bound (1-1). In Section 7 we state and prove the criterion used to show that $71, 113, 127 \notin S(7)$. Finally, we complete the verification of assumption (b) in Section 8, which also contains the proof of Proposition 1.4.

What is new in this paper? The main new *result* is Theorem 1.2, which extends the list of known sets $S(d)$ from $d \leq 3$ to $d \leq 7$. Completing the determination of $S(6)$, Proposition 1.4 gives a classification of the sporadic points in $X_1(37)^{(6)}(\mathbb{Q})$. Another new result is Theorem 3.2, which confirms a conjecture made in [Conrad et al. 2003] in a case that was left open in that paper.

We also develop some new *techniques* for proving that $p \notin S(d)$ for suitable $d \geq 1$ and primes p . One point is the use of intermediate curves in various computations instead of just either $X_0(p)$ or $X_1(p)$. Another is the use of explicit computations in the Picard group of $X_1(p)_{\mathbb{F}_2}$ when p is such that $J_1(p)(\mathbb{Q})$ is finite. In addition, we derive two new criteria, one that uses the gonality of $X_1(p)$ and can show directly that $p \notin S(d)$ using global arguments (Proposition 7.1), and a related one that works over \mathbb{F}_2 using Hecke correspondences (Lemma 8.6). Finally, we extend the formal immersion approach that is traditionally used to show what we call assumption (a) to also apply to assumption (b). All this is necessary to be able to determine $S(7)$.

Why stop at $d = 7$? Obviously, determining $S(d)$ gets harder and harder as d grows. When $d = 1$, the formal immersion condition for $X_0(p)$ is essentially trivially satisfied, and assumption (b) for $\ell = 3$ is automatically satisfied for $p > \lfloor (\sqrt{3} + 1)^2 \rfloor = 7$. Once the theoretical framework is in place (which, of course, was the key contribution of Mazur [1977; 1978]), no computation is necessary to obtain the desired result.

For $d = 2$, Kamienny had to come up with a criterion that allows one to verify the formal immersion condition (still for $X_0(p)$). In this case, it can still be shown to hold by a theoretical argument. The trivial bound for assumption (b) when $\ell = 3$ is $p > 16$, which is again sufficient.

For $d = 3$ and larger, one needs to work to verify the formal immersion condition. Merel and Oesterlé managed to find a theoretical argument that does this (for $X_0(p)$ and $\ell = 3$) for p larger than some explicit polynomial in d . Oesterlé then came up with another ingenious way to reduce the remaining cases to a finite and manageable amount of computation, thus proving the bound (1-1). To determine $S(3)$, Parent had to rely on this and to come up with a way of using $X_1(p)$ and $\ell = 2$ to cover the primes between $\lceil (2^{3/2} + 1)^2 \rceil = 15$ and $\lfloor (3^{3/2} + 1)^2 \rfloor = 38$ (and $p = 43$, which had escaped Oesterlé's approach).

For $d \geq 4$, there are two main difficulties, which each get worse as d increases.

- (1) The gap between the best general bound (1-1) and the smallest prime not in $S(d)$ increases exponentially with d . While we can, for each d and each p in this range, verify the formal immersion condition for $X_0(p)$ or some intermediate curve X_H computationally, the computational effort increases considerably with p . For $d = 7$, this part of the computation took about two hours. For $d = 8$, the upper end of this range is about three times as large as for $d = 7$, which lets us expect that doing this in reasonable time would require a massively parallel computation. For $d \geq 9$, this appears to be infeasible in the absence of a major theoretical advance that leads to a significantly reduced general bound.
- (2) The gap between the primes in $S(d)$ and the “easy” range for assumption (b) also increases. Most likely, this increase is also exponential, because we expect that $\max S(d)$ should grow only

polynomially (possibly even linearly). This means that there will be more and more primes p for which we have to show assumption (b) when there are indeed points in $X_1(p)^{(d)}(\mathbb{F}_2)$ that are not sums of images of rational cusps. While we could deal with the “rank-zero primes” $p = 29, 31, 41$ by explicit computations and with the one further such prime $p = 73$ for $d = 6$ by a variant of the formal immersion criterion, this is the point where it gets hard when $d = 7$. To rule out the primes 37, 43, 59, 61, 67, 71, 73, 113, and 127, we needed to develop some new criteria, and some of the computations that are then still necessary run for several hours.

However, it appears that our new criteria can be used to go a bit further. This will be explored in a follow-up paper.

2. Preliminaries on modular curves

A good reference for most of the following is [Diamond and Im 1995].

As usual, we define, for $N \in \mathbb{Z}_{\geq 1}$,

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : N \mid c \right\} \quad \text{and} \quad \Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : (c, d) \equiv (0, 1) \pmod{N} \right\}.$$

$\mathrm{SL}_2(\mathbb{Z})$ and therefore also Γ_0 and Γ_1 act on the complex upper half-plane \mathfrak{H} and on $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$ by Möbius transformations. Then the quotient $Y_j(N)(\mathbb{C}) = \Gamma_j(N) \backslash \mathfrak{H}$ (for $j = 0, 1$) is a Riemann surface that can be compactified to $X_j(N)(\mathbb{C}) = \Gamma_j(N) \backslash \mathfrak{H}^*$ by adding the finitely many cusps $C_j(N) = \Gamma_j(N) \backslash \mathbb{P}^1(\mathbb{Q})$. The points in $Y_1(N)(\mathbb{C})$ classify pairs (E, P) consisting of an elliptic curve E over \mathbb{C} and a point $P \in E(\mathbb{C})$ of exact order N ; in terms of a representative point $\tau \in \mathfrak{H}$, this is given by $E = \mathbb{C}/\Lambda_\tau$ with $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$ and $P = 1/N + \Lambda$. Similarly, $Y_0(N)(\mathbb{C})$ classifies pairs (E, C) where again E is an elliptic curve over \mathbb{C} and $C \subseteq E(\mathbb{C})$ is a cyclic subgroup of order N . The compact Riemann surfaces $X_j(N)(\mathbb{C})$ can be identified with the set of complex points on projective algebraic curves $X_j(N)$ defined over \mathbb{Q} (or even over $\mathbb{Z}[1/N]$). The rational structure is defined in terms of the q -expansions of functions on $X_j(N)(\mathbb{C})$: such a function f lifts to a modular function with respect to $\Gamma_j(N)$ on \mathfrak{H} and therefore has a Laurent series expansion in terms of $q = e^{2\pi i\tau}$. The function field $\mathbb{Q}(X_j(N))$ is then defined to consist of those f whose q -expansion has coefficients in \mathbb{Q} . Since the rational structure is defined in terms of q , the natural moduli interpretation of a point on $X_1(N)$ over \mathbb{Q} (or any field extension K) is as representing a pair (E, φ) , where E is an elliptic curve over \mathbb{Q} (or K) and $\varphi : \mu_N \rightarrow E$ is an embedding of the group μ_N of N -th roots of unity into E as group schemes. This is because the image of $1/N$ under $\tau \mapsto e^{2\pi i\tau}$ is not rational, but a generator of μ_N . Since (over any field K of characteristic not dividing N) there is a natural bijection between pairs (E, P) and pairs (E', φ) as above, the points on $X_1(N)$ can still be understood as classifying elliptic curves over K together with a point of order N , but we have to keep in mind that this is not the same as the moduli interpretation over \mathbb{C} given above. (The bijection is obtained as follows. Given a pair (E, P) and $\zeta \in \mu_N$, the set of $Q \in E[N]$ such that $e_N(Q, P) = \zeta$ forms a coset C_ζ of the subgroup $\mathbb{Z}P$ generated by P . We then set $E' = E/\mathbb{Z}P$ and $\varphi : \zeta \mapsto C_\zeta/\mathbb{Z}P$.)

The space of cusp forms for $\Gamma_j(N)$ is canonically isomorphic to the space of regular differentials

on $X_j(N)(\mathbb{C})$. Under this isomorphism, regular differentials on $X_j(N)$ over \mathbb{Q} correspond to cusp forms whose q -expansion has rational coefficients.

There is a natural map $X_1(N) \rightarrow X_0(N)$ (induced over \mathbb{C} by the identity on \mathfrak{H}^*). This makes $X_1(N)$ into a (possibly ramified) Galois covering of $X_0(N)$, whose Galois group consists of the diamond operators $\langle a \rangle$ for $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, where $\langle -1 \rangle$ is the identity, so the Galois group is naturally isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times / \{\pm 1\}$. In terms of the interpretation of points on $Y_1(N)$ as pairs $(E, \varphi : \mu_N \rightarrow E)$, the action of $\langle a \rangle$ corresponds to precomposing φ with the a -th power map. If $H \subseteq (\mathbb{Z}/N\mathbb{Z})^\times / \{\pm 1\}$ is a subgroup, then we have an intermediate curve $X_H = H \backslash X_1(N)$ between $X_1(N)$ and $X_0(N)$.

We write $\infty \in X_j(N)$ for the cusp that over \mathbb{C} is the image of $\infty \in \mathbb{P}^1(\mathbb{Q})$. Note that $\infty \in X_j(N)(\mathbb{Q})$, since it corresponds to $q = 0$. When $N = p$ is prime, $X_0(p)$ has the two cusps ∞ and the cusp represented by $0 \in \mathbb{P}^1(\mathbb{Q})$, which are both rational, whereas $X_1(p)$ has $p - 1$ cusps, which split into two orbits under the diamond operators, each consisting of $(p - 1)/2$ cusps. One of the orbits contains ∞ and consists of rational cusps, the other orbit consists of cusps defined over the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\mu_p)$; these cusps are all conjugate under the Galois action, and the Galois action is given by diamond operators (since it commutes with them). An analogous statement is true for the cusps of X_H . See [Stevens 1982, Theorem 1.3.1] for a description of the Galois action on the cusps.

We denote the Jacobian varieties of $X_0(N)$, $X_1(N)$ and X_H by $J_0(N)$, $J_1(N)$ and J_H , respectively. They are defined over \mathbb{Q} and extend to abelian schemes over $\mathbb{Z}[1/N]$.

We denote the Hecke algebra, in its various incarnations, by \mathbb{T} . It is generated by the Hecke operators T_n for all $n \geq 1$ or, alternatively, by all T_p for p prime together with diamond operators $\langle a \rangle$ for a generating $(\mathbb{Z}/N\mathbb{Z})^\times / \{\pm 1\}$. The Hecke algebra acts on the integral homology $H_1(X_H(\mathbb{C}), \mathbb{Z})$, on the relative homology $H_1(X_H(\mathbb{C}), \text{cusps}, \mathbb{Z})$, on the associated spaces of modular forms or cusp forms, and as endomorphisms of J_H . The Hecke operators T_n and the diamond operators $\langle a \rangle$ can also be viewed as correspondences on X_H . It will always be clear from the context or explicitly stated which interpretation is considered.

The integral relative homology with respect to the cusps is generated as a \mathbb{Z} -module by modular symbols $\{\gamma_1, \gamma_2\}$ with $\gamma_1, \gamma_2 \in \mathbb{P}^1(\mathbb{Q})$. There is an integration pairing

$$H_1(X_H(\mathbb{C}), \text{cusps}, \mathbb{Z}) \times H^0(X_{H,\mathbb{C}}, \Omega^1) \rightarrow \mathbb{C}, \quad (\xi, \omega) \mapsto \int_{\xi} \omega$$

(if $\xi = \{\gamma_1, \gamma_2\}$, then the integral is along any path in \mathfrak{H}^* joining γ_1 to γ_2); it induces a perfect pairing of real vector spaces between $H_1(X_H(\mathbb{C}), \mathbb{R})$ and $H^0(X_{H,\mathbb{C}}, \Omega^1)$, and the image of the composition

$$\pi : H_1(X_H(\mathbb{C}), \text{cusps}, \mathbb{Z}) \rightarrow H^0(X_{H,\mathbb{C}}, \Omega^1)^* \rightarrow H_1(X_H(\mathbb{C}), \mathbb{R})$$

is in the rational homology $H_1(X_H(\mathbb{C}), \mathbb{Q})$ by the Manin–Drinfeld theorem [Manin 1972; Drinfeld 1973].

Definition 2.1. We set

$$e = \pi(-\{0, \infty\}) \in H_1(X_H(\mathbb{C}), \mathbb{Q});$$

this is called the *winding element*. Its annihilator $\text{Ann}(e)$ in \mathbb{T} is the *winding ideal*. It acts via endomorphisms on J_H ; the quotient $J_H^e := J_H / \text{Ann}(e)J_H$ is the *winding quotient*.

The definition of the winding element goes back to Mazur [1977, Lemma II.18.6 and the definition preceding it] in the case of $J_0(N)$. We note that there is some ambiguity regarding the sign of the winding element in the literature. We follow [Merel 1996, Section 1] here (but, for example, [Parent 1999] uses the opposite sign.) The winding quotient has the following essential property.

Theorem 2.2. *For each subgroup $H \subseteq (\mathbb{Z}/N\mathbb{Z})^\times / \{\pm 1\}$, the Mordell–Weil group $J_H^e(\mathbb{Q})$ is finite.*

Merel [1996, § 1] was the first one to introduce the winding quotient for $J_0(p)$ with p prime, where he also proves that its Mordell–Weil group is finite using a result from [Kolyvagin and Logachëv 1989], which states that an abelian variety A over \mathbb{Q} that is a quotient of $J_0(N)$ has Mordell–Weil rank 0 when $L(A, 1) \neq 0$. Parent [1999, § 3.8] generalized Merel’s statement to composite numbers N . The result of Kolyvagin and Logachëv was generalized by Kato [2004, Corollary 14.3] to quotients of $J_1(N)$. In both [Parent 2000] and [Parent 2003], it is mentioned that the theorem follows from Kato’s generalization. This can be seen by adapting the arguments of [Parent 1999, § 3.8] accordingly. The key point in the proof is that J_H^e is isogenous to a product of simple abelian varieties A over \mathbb{Q} such that $L(A, 1) \neq 0$. Kato’s result then shows that $A(\mathbb{Q})$ is finite.

The following is a variant of [Parent 2000, Proposition 1.8]. We remark that, according to [Diamond and Im 1995, p. 87], the Eichler–Shimura relation on $X_1(N)$ with the modular interpretation used here (and in [Parent 2000]) is different from that valid with the more usual interpretation as parametrizing pairs (E, P) of elliptic curves with a point of order N . We therefore believe that our version is correct, and that (the first part of) Parent’s statement needs to be modified accordingly.

Proposition 2.3. *Let $q \nmid N$ be a prime and $P \in J_H(\mathbb{Q})_{\text{tors}}$ such that q is odd or P has odd order. Then $(T_q - \langle q \rangle - q)(P) = 0$.*

Proof. Let n be the order of P . Then $(T_q - \langle q \rangle - q)(P) \in J_H(\mathbb{Q})$ is a point of order dividing n . We write \bar{P} for the reduction mod q of P , Frob_q for the Frobenius on J_{H, \mathbb{F}_q} and Ver_q for its dual (Verschiebung). Then we have the Eichler–Shimura relation

$$T_{q, \mathbb{F}_q} = \langle q \rangle \text{Frob}_q + \text{Ver}_q \quad \text{and} \quad \text{Ver}_q \circ \text{Frob}_q = q$$

in $\text{End}_{\mathbb{F}_q}(J_{H, \mathbb{F}_q})$; see [Diamond and Im 1995, p. 87]. So, using that $\text{Frob}_q(\bar{P}) = \bar{P}$,

$$T_{q, \mathbb{F}_q}(\bar{P}) = \langle q \rangle \text{Frob}_q(\bar{P}) + \text{Ver}_q(\bar{P}) = \langle q \rangle \bar{P} + q \bar{P},$$

which implies that $(T_{q, \mathbb{F}_q} - \langle q \rangle - q)(\bar{P}) = 0$. Since the reduction map is injective on $J_H(\mathbb{Q})_{\text{tors}}$ when q is odd, and it is injective on odd-order torsion when $q = 2$, the claim follows. \square

Remark. For the proof of Theorem 3.2, it actually does not matter whether one uses $T_q - \langle q \rangle - q$ as in Proposition 2.3 or $T_q - \langle q \rangle q - 1$ as in [Parent 2000]. Up to composition with $\langle q \rangle$ or its inverse, the two operators are conjugate to each other under the Atkin–Lehner involution w_p ; see [Diamond and Im 1995,

p. 56 and Remark 10.2.2]. If we use the “wrong” operators in the proof of Theorem 3.2, then instead of $J_1(29)(\mathbb{Q})_{\text{tors}} \subseteq C$, we find that $w_{29}(J_1(29)(\mathbb{Q})_{\text{tors}}) \subseteq C$, which also implies $J_1(29)(\mathbb{Q})_{\text{tors}} \subseteq w_{29}(C) = C$ (the cusps are permuted by w_p).

Our second application in Corollary 5.2 uses the operators with q odd to kill torsion. By the remark after Corollary 4.3, it is enough to kill 2-torsion. For q an odd prime, the two operators $T_q - \langle q \rangle - q$ and $T_q - \langle q \rangle q - 1$ differ by a multiple of 2 in the Hecke algebra, so they have the same effect on 2-torsion points. This implies that the conclusion of Corollary 4.3 also holds if we use the “wrong” operator and show that $t \circ \iota$ is a formal immersion. In particular, the conclusions of [Parent 2000] are valid.

We will also need the following statement.

Proposition 2.4 (Derickx). *Let $q \nmid N$ be a prime. We consider $t = T_q - \langle q \rangle - q \in \mathbb{T}$ as a correspondence on $X_1(N)$, inducing an endomorphism of the divisor group of $X_1(N)$ over \mathbb{C} . Then the kernel of t is contained in the subgroup of divisors supported in cusps.*

Proof. Let D be a divisor in the kernel of t , so that

$$T_q(D) = \langle q \rangle(D) + qD. \quad (2-1)$$

A noncuspidal point $x \in X_1(N)(\mathbb{C})$ corresponds to an elliptic curve E over \mathbb{C} with additional structure. The point $\langle q \rangle(x)$ corresponds to the same curve E (with modified extra structure), and $T_q(x)$ is a sum of points corresponding to all the elliptic curves that are q -isogenous to E . We define the q -isogeny graph G to have as vertices the isomorphism classes of all elliptic curves over \mathbb{C} ; two vertices are connected by an edge when there is a q -isogeny between the corresponding curves. There is a natural map γ from $Y_1(N)(\mathbb{C})$ to the vertex set of G . Let x be a noncuspidal point in the support of D and let G_x be the connected component of G containing $\gamma(x)$. Let E be the elliptic curve given by x . We distinguish two cases.

First, assume that E does not have CM. Then G_x is an infinite $(q+1)$ -regular tree. Consider a vertex v of G_x that has maximal possible distance from $\gamma(x)$ among all vertices of the form $\gamma(y)$ for a point y in the support of D . Let y_1, \dots, y_n be the points in the support of D such that $\gamma(y_j) = v$, and let w be a neighbor of v whose distance from $\gamma(x)$ is larger than that of v . Each $T_q(y_j)$ contains precisely one point y'_j such that $\gamma(y'_j) = w$, and these points are distinct for distinct points y_j . Since w is not of the form $\gamma(z)$ for a point z in the support of D , this shows that $T_q(D)$ has points in its support that do not occur in the support of $\langle q \rangle(D) + qD$ (recall that $\gamma(\langle q \rangle(y)) = \gamma(y)$). This contradicts the relation (2-1), and we conclude that there can be no non-CM point x in the support of D .

Now consider the case that E has CM. Then G_x is no longer a tree in general, but has the structure of a “volcano”; see [Sutherland 2013]. For a CM elliptic curve over \mathbb{C} , this volcano has infinite depth. Concretely, this means that it consists of a number of rooted $(q+1)$ -regular trees whose roots form a cycle (which may have length 1 or 2). We can now argue as in the first case by choosing v to be a vertex of maximal level (i.e., distance from the root cycle) and w to be a neighbor of v whose level is larger by one. This shows that there can be no CM points in the support of D either.

The only points that we have not excluded from the support of D are the cusps; this proves the claim. \square

Remark. In the case that $N = p$ is a prime, we can describe the kernel exactly. The rational cusps are killed by t , whereas the irrational cusps are killed by $t^* = T_q - q\langle q \rangle - 1$; compare [Parent 2000, Section 2.4] (the rational cusps are those mapping to the cusp ∞ on $X_0(p)$ under the modular interpretation we use). Since $t - t^* = (q - 1)(\langle q \rangle - 1)$ and the divisor group is torsion-free, t kills a divisor supported on irrational cusps if and only if it is invariant under $\langle q \rangle$.

3. Rank-zero primes

We say that a prime p is a *rank-zero prime* when $J_1(p)(\mathbb{Q})$ is finite.

The following result gives us the list of rank-zero primes. This is [Conrad et al. 2003, Proposition 6.2.1]; we include some more information from Section 6.2 of loc. cit.

Proposition 3.1. *The rank-zero primes p are the primes $p \leq 31$ and 41, 47, 59, and 71.*

For all of these, except possibly $p = 29$, the group $J_1(p)(\mathbb{Q})$ is generated by differences of rational cusps, and for all except $p = 17, 29, 31$ and 41, the order of $J_1(p)(\mathbb{Q})$ is odd.

We can add to this the following new result, which confirms Conjecture 6.2.2 in [Conrad et al. 2003] for the smallest open case, $p = 29$.

Theorem 3.2. *The group $J_1(29)(\mathbb{Q})$ is generated by differences of rational cusps.*

Proof. We prove this by a computation using modular symbols, as follows. The group $J_1(29)(\mathbb{C})_{\text{tors}}$ is canonically isomorphic to $M := H_1(X_1(29)(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$. By Proposition 2.3, the image of the rational torsion subgroup is annihilated by $T_q - \langle q \rangle - q$ for all odd primes $q \neq 29$, and it is also annihilated by $\tau - 1$, where τ is induced by complex conjugation. We let M' be the subgroup of M annihilated by $\tau - 1$ and $T_q - \langle q \rangle - q$ for $q = 3, 5, 7$. We find that

$$J_1(29)(\mathbb{Q})_{\text{tors}} \subseteq M' \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^2 \cdot 3 \cdot 7 \cdot 43 \cdot 17837\mathbb{Z}}.$$

We can also compute the cuspidal subgroup C as the image in M of the relative homology $H_1(X_1(29)(\mathbb{C}), \text{cusps}, \mathbb{Z})$ via its embedding into $H_1(X_1(29)(\mathbb{C}), \mathbb{Q})$. We obtain that

$$M' \subseteq C \cong \frac{\mathbb{Z}}{2^2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^2 \cdot 3 \cdot 43 \cdot 17837\mathbb{Z}} \times \frac{\mathbb{Z}}{2^2 \cdot 3 \cdot 7^2 \cdot 43 \cdot 17837\mathbb{Z}}.$$

Finally, we have an explicit homomorphism $\mathbb{Z}[\text{cusps}]^0 \rightarrow C$, where $\mathbb{Z}[\text{cusps}]^0$ denotes the degree-zero part of the free abelian group with basis the cusps of $X_1(29)$. We know that the absolute Galois group of \mathbb{Q} fixes the 14 cusps mapping to the cusp ∞ of $X_0(29)$, whereas the remaining 14 cusps are permuted cyclically via the action of the diamond operators. This allows us to determine

$$J_1(29)(\mathbb{Q}) = J_1(29)(\mathbb{Q})_{\text{tors}} = C^{\text{Gal}_{\mathbb{Q}}} \cong \frac{\mathbb{Z}}{2^2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^2 \cdot 3 \cdot 7 \cdot 43 \cdot 17837\mathbb{Z}},$$

and we can verify that this equals the subgroup generated by differences of rational cusps. \square

Remark. In our Magma code for the computations in the proof above, we rely only on linear algebra functionality (over \mathbb{Q} and \mathbb{Z}): we construct the relevant spaces “by hand” instead of using the built-in modular symbols functionality.

Together with Proposition 3.1, this immediately implies the following.

Corollary 3.3. *If p is a prime such that $J_1(p)(\mathbb{Q})$ is finite, then the latter group is generated by differences of rational cusps on $X_1(p)$.*

We will need the following result on the reduction mod 2.

Proposition 3.4. *If $p > 2$ is a prime such that $J_1(p)(\mathbb{Q})$ is finite, then the reduction map*

$$\text{red}_2 : J_1(p)(\mathbb{Q}) = J_1(p)(\mathbb{Q})_{\text{tors}} \rightarrow J_1(p)(\mathbb{F}_2)$$

is injective.

Proof. Let X be a curve over \mathbb{Q} with good reduction at 2, and let J be its Jacobian variety. Then the kernel of the reduction map $J(\mathbb{Q})_{\text{tors}} \rightarrow J(\mathbb{F}_2)$ is contained in the 2-torsion subgroup [Parent 2000, Lemma 1.7]. So the claim follows for all p such that $J_1(p)(\mathbb{Q})$ is finite of odd order. For the remaining primes on our list, namely $p \in \{17, 29, 31, 41\}$, we check by an explicit computation that $J_1(p)(\mathbb{Q})[2] \rightarrow J_1(p)(\mathbb{F}_2)$ is injective. This then implies the claim for these primes as well.

We now describe this computation. By Corollary 3.3, we know $J_1(p)(\mathbb{Q})$ is generated by differences of rational cusps. The order of this group is known; see [Conrad et al. 2003, § 6.2.3 and Table 1] and note that the order for $p = 29$ given there has to be divided by 2^6 to get the order of the group generated by differences of rational cusps; compare Theorem 3.2. Sutherland (https://math.mit.edu/~drew/X1_altcurves.html) provides equations for planar models of $X_1(p)$ over \mathbb{Q} for the relevant values of p . We use the reduction modulo 2 of this model to check that the subgroup of its Picard group generated by differences of its degree-1 places over \mathbb{F}_2 (which correspond to the rational cusps under reduction mod 2) has the correct order. In fact, it suffices to check that the 2-primary part of the group has the correct order. For $p = 17, 29$, and 31, this only takes a few minutes; for $p = 41$ the computation of the Picard group of $X_1(p)$ over \mathbb{F}_2 takes about eight hours (and 2.5 gigabytes of memory). \square

Remark. If one does not want to wait for several hours for the computation for $p = 41$ to finish, one can alternatively use the intermediate curve X_H corresponding to $d = 4$ in the notation of [Conrad et al. 2003] (then H has index 4). The predicted order of the 2-primary part of $J_H(\mathbb{Q})$ equals that of $J_1(p)(\mathbb{Q})$. We check that the 2-primary part of the subgroup of $J_H(\mathbb{F}_2)$ generated by differences of the images of rational cusps has the correct size.

Remark. For $p = 17$, Proposition 3.4 together with the fact that the \mathbb{Q} -gonality of $X_1(17)$ is 4 gives a simple alternative proof of the main result of [Parent 2003] that $17 \notin S(3)$; see Corollary 3.6 below. (Note that $17 > (2^{3/2} + 1)^2$.)

Remark. The statement of Proposition 3.4 is false for $J_0(p)$. For example, $J_0(17)$ is the elliptic curve with Cremona label $17a1$. It has $J_0(17)(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$, generated by the difference of the two cusps, but the reduction modulo 2 of a generator has only order 2.

We now show that assumption (a) in Lemma 1.7 is satisfied when $\ell = 2$ and p is a rank-zero prime such that the \mathbb{Q} -gonality of $X_1(p)$ is strictly larger than d . The \mathbb{Q} -gonality of a curve X over \mathbb{Q} is the smallest degree of a nonconstant rational function on X defined over \mathbb{Q} .

Recall the embedding $\iota : X_1(p)^{(d)} \rightarrow J_1(p)$ given by fixing a basepoint $c \in C_1(p)(\mathbb{Q})$.

Corollary 3.5. *Let $d \geq 1$ be an integer. If $p > 2$ is a rank-zero prime and the \mathbb{Q} -gonality of $X_1(p)$ is strictly larger than d , then assumption (a) in Lemma 1.7 is satisfied for $\ell = 2$.*

Proof. The map $\iota : X_1(p)^{(d)}(\mathbb{Q}) \rightarrow J_1(p)(\mathbb{Q})$ is injective when the \mathbb{Q} -gonality of $X_1(p)$ exceeds d , since otherwise there are two distinct \mathbb{Q} -rational effective divisors D_1 and D_2 of degree d that are linearly equivalent, which means that there is a rational function f on $X_1(p)$ defined over \mathbb{Q} whose divisor is $D_1 - D_2$, and hence f has degree $\leq d$. This contradicts the condition on the \mathbb{Q} -gonality. By Proposition 3.4, the reduction map $\text{red}_2 : J_1(p)(\mathbb{Q}) \rightarrow J_1(p)(\mathbb{F}_2)$ is injective as well, and therefore $\text{red}_2 \circ \iota = \iota \circ \text{red}_2$ is injective, which implies that red_2 is injective on $X_1(p)^{(d)}(\mathbb{Q})$:

$$\begin{array}{ccc} X_1(p)^{(d)}(\mathbb{Q}) & \xrightarrow{\iota} & J_1(p)(\mathbb{Q}) \\ \downarrow \text{red}_2 & & \downarrow \text{red}_2 \\ X_1(p)^{(d)}(\mathbb{F}_2) & \xrightarrow{\iota} & J_1(p)(\mathbb{F}_2) \end{array} \quad \square$$

The following is an excerpt of [Derickx and van Hoeij 2014, Table 1]. We write $\text{gon}_{\mathbb{Q}}(X)$ for the \mathbb{Q} -gonality of a curve X :

p	11	13	17	19	23	29	31
$\text{gon}_{\mathbb{Q}}(X_1(p))$	2	2	4	5	7	11	12

Also, it follows from [Derickx and van Hoeij 2014, Theorem 3] that $\text{gon}_{\mathbb{Q}}(X_1(p)) > 8$ for $p \in \{41, 47, 59, 71\}$. We deduce the following.

Corollary 3.6. *For the following values of d and p , assumption (a) in Lemma 1.7 is satisfied for $\ell = 2$:*

- $d = 3$ and $p \in \{17, 19, 23, 29, 31, 41, 47, 59, 71\}$,
- $d = 4$ and $p \in \{19, 23, 29, 31, 41, 47, 59, 71\}$,
- $d = 5$ and $p \in \{23, 29, 31, 41, 47, 59, 71\}$,
- $d = 6$ and $p \in \{23, 29, 31, 41, 47, 59, 71\}$,
- $d = 7$ and $p \in \{29, 31, 41, 47, 59, 71\}$.

We now consider assumption (b) of Lemma 1.7 for $p = 29, 31, 41$. We do this here rather than in Section 8, since the computations we do to show that the assumption is satisfied are closely related to those we do to establish Proposition 3.4.

Lemma 3.7. *For $p \in \{29, 31, 41\}$, $d \leq 7$ and $\ell = 2$, assumption (b) of Lemma 1.7 is satisfied.*

Proof. For $d \leq 4$, we have that $p > (2^{d/2} + 1)^2$, and the claim follows from Lemma 1.9. For $(d, p) = (5, 29)$, we observe that there is no elliptic curve over \mathbb{F}_{2^5} with 29 points and that the cusps that are not images of rational cusps are not defined over \mathbb{F}_{2^5} , so there are no points \bar{x} as in assumption (b).

In the other cases, Corollary 3.3 tells us that $J_1(p)(\mathbb{Q})$ is generated by the differences of the rational cusps. This implies that the reduction mod 2 of any \mathbb{Q} -rational point of $X_1(p)^{(d)}$ must map into the subgroup of $J_1(p)(\mathbb{F}_2)$ that is generated by the differences of the images of the rational cusps. We verify that the points \bar{x} as in assumption (b) do not map into that subgroup, which by the above shows that these points are not in the image of the reduction map. This implies the claim. This computation is done together with the computations we do to prove Proposition 3.4. \square

Remark. In a similar way as in Proposition 3.4, we can use the following alternative approach for $p = 41$. There is no elliptic curve E over \mathbb{F}_{2^e} with $41 \mid \#E(\mathbb{F}_{2^e})$ if $e \leq 7$ and $e \neq 5$. There is exactly one elliptic curve E over \mathbb{F}_{2^5} with $\#E(\mathbb{F}_{2^5}) = 41$; this is the curve $y^2 + y = x^3 + x + 1$ already defined over \mathbb{F}_2 . Its automorphism group over \mathbb{F}_{2^5} is cyclic of order 4; we therefore obtain only $10 = (41 - 1)/4$ distinct \mathbb{F}_{2^5} -points on $X_1(41)$ that are not cusps. Let X_H be the intermediate curve between $X_1(41)$ and $X_0(41)$ with H of index 4. Then $X_1(41) \rightarrow X_H$ is an étale cover of degree 5, and the ten \mathbb{F}_{2^5} -points on $X_1(41)$ map to two \mathbb{F}_2 -points on X_H . In fact, $X_H(\mathbb{F}_2)$ consists of six points; four of them are cusps, and the other two are the ones just mentioned. It can be checked that these two points do not map into the subgroup generated by the differences of the four cusps, so that we can conclude in the same way as above.

4. Formal immersions

When p is not a rank-zero prime, so that $J_1(p)(\mathbb{Q})$ has positive rank, then the reduction map $J_1(p)(\mathbb{Q}) \rightarrow J_1(p)(\mathbb{F}_\ell)$ is no longer injective. This means that we need to find a more sophisticated argument to verify assumption (a) of Lemma 1.7.

As mentioned in the introduction, one key idea here is to use a morphism $t : J_1(p) \rightarrow A$ of abelian varieties over \mathbb{Z}_ℓ . We obtain the following commutative diagram:

$$\begin{array}{ccccc}
 X_1(p)^{(d)}(\mathbb{Q}) & \xrightarrow{t} & J_1(p)(\mathbb{Q}) & \xrightarrow{t} & A(\mathbb{Q}) \\
 \downarrow \text{red}_\ell & & \downarrow \text{red}_\ell & & \downarrow \text{red}_\ell \\
 X_1(p)^{(d)}(\mathbb{F}_\ell) & \xrightarrow{t_\ell} & J_1(p)(\mathbb{F}_\ell) & \xrightarrow{t_\ell} & A(\mathbb{F}_\ell)
 \end{array} \tag{4-1}$$

Let $\bar{x} \in X_1(p)^{(d)}(\mathbb{F}_\ell)$ be some point. Assuming that red_ℓ is injective on $t(J_1(p)(\mathbb{Q}))$, it will follow that the residue class of \bar{x} contains at most one rational point, if we can show that the diagonal composition $\text{red}_\ell \circ t \circ \iota = t_\ell \circ \iota_\ell \circ \text{red}_\ell$ is injective on the residue class of \bar{x} .

The strategy for doing that is to take A such that $A(\mathbb{Q})$, or at least $t(J_1(p)(\mathbb{Q}))$, is finite; then the reduction map on $A(\mathbb{Q})$ (or the image of t) will be injective when ℓ is odd; when $\ell = 2$, we can ensure that the reduction map is injective on $t(J_1(p)(\mathbb{Q}))$ by making sure that this image has odd order. It then remains to show that $t \circ \iota$ is injective on the residue class of any point $\bar{x} \in X_1(p)^{(d)}(\mathbb{F}_\ell)$. To do this, we show that $t \circ \iota$ is a formal immersion at each of the points \bar{x} as above. We recall the definition below.

First, some notation. We write \mathcal{O}_X for the structure sheaf of a scheme X , $\mathcal{O}_{X,x}$ for its local ring at a point x of X , and $\widehat{\mathcal{O}}_{X,x}$ for the completion of the local ring with respect to its maximal ideal $\mathfrak{m}_{X,x}$.

Definition 4.1. Let $\phi : X \rightarrow Y$ be a morphism of noetherian schemes and let $x \in X$ be a point. Then ϕ is a *formal immersion at x* if the induced local homomorphism on complete local rings

$$\hat{\phi}^* : \widehat{\mathcal{O}}_{Y,\phi(x)} \rightarrow \widehat{\mathcal{O}}_{X,x}$$

is surjective.

The relevant property of formal immersions for our purposes is the following; this is (a consequence of) [Parent 1999, Lemma 4.13].

Lemma 4.2. *Let $\phi : X \rightarrow Y$ be a morphism of noetherian schemes over $\mathbb{Z}_{(\ell)}$ that is a formal immersion at $x \in X(\mathbb{F}_\ell)$. Then ϕ induces an injective map on residue classes*

$$\phi : \text{red}_\ell^{-1}(x) \rightarrow \text{red}_\ell^{-1}(\phi(x)).$$

Corollary 4.3. *Let $d \in \mathbb{Z}_{\geq 1}$ and let $\ell \neq p$ be primes. Let $t : J_1(p) \rightarrow A$ be a morphism of abelian schemes over $\mathbb{Z}_{(\ell)}$ such that*

- (i) $t(J_1(p)(\mathbb{Q}))$ is finite,
- (ii) $\ell > 2$ or $\#t(J_1(p)(\mathbb{Q}))$ is odd,
- (iii) $t \circ \iota$ is a formal immersion at all $\bar{x} \in X_1(p)^{(d)}(\mathbb{F}_\ell)$ that are sums of images of rational cusps on $X_1(p)$.

Then assumption (a) of Lemma 1.7 is satisfied.

Proof. Note that $X_1(p)$ and $J_1(p)$ have good reduction at ℓ , and hence $J_1(p)$ can be considered as an abelian scheme over $\mathbb{Z}_{(\ell)}$.

Let $x, x' \in X_1(p)^{(d)}(\mathbb{Q})$ be in the residue class of a point \bar{x} that is a sum of images of rational cusps and write $y = t(\iota(x))$, $y' = t(\iota(x'))$. Because x and x' are in the same residue class, the same is true of y and y' . It follows from conditions (i) and (ii) that $\text{red}_\ell : t(J_1(p)(\mathbb{Q})) \rightarrow A(\mathbb{F}_\ell)$ is injective, which implies that $y = y'$. By condition (iii) and Lemma 4.2, $t \circ \iota$ is injective on the residue class of \bar{x} , which finally shows that $x = x'$. \square

Remark. If $\ell = 2$ and we take commuting $t_1, t_2 \in \text{End}_{\mathbb{Q}}(J_1(p))$ such that $t_1(J_1(p)(\mathbb{Q}))$ is finite and t_2 kills the 2-torsion subgroup of $J_1(p)(\mathbb{Q})$, then the conclusion of Corollary 4.3 holds for $t = t_1 t_2$ also when $\#t(J_1(p)(\mathbb{Q}))$ is even (assuming condition (iii) is satisfied); see [Parent 2000, Theorem 1.10].

Writing $A_1 = \text{im}(t_1)$ and taking $A = \text{im}(t)$ without loss of generality, we have the following commutative diagram:

$$\begin{array}{ccccccc}
 X_1(p)^{(d)}(\mathbb{Q}) & \xrightarrow{\iota} & J_1(p)(\mathbb{Q}) & \xrightarrow{t_1} & A_1(\mathbb{Q}) & \xrightarrow{t_2} & A(\mathbb{Q}) \\
 \downarrow \text{red}_2 & & \downarrow \text{red}_2 & & \downarrow \text{red}_2 & & \downarrow \text{red}_2 \\
 X_1(p)^{(d)}(\mathbb{F}_2) & \xrightarrow{\iota} & J_1(p)(\mathbb{F}_2) & \xrightarrow{t_1} & A_1(\mathbb{F}_2) & \xrightarrow{t_2} & A(\mathbb{F}_2)
 \end{array}$$

Take $x, x' \in X_1(p)^{(d)}(\mathbb{Q})$ with the same reduction $\bar{x} \pmod 2$, such that \bar{x} is a sum of images of rational cusps. Then $t_1(\iota(x') - \iota(x))$ is in the kernel of reduction mod 2 of $A_1(\mathbb{Q})$, which (since $A_1(\mathbb{Q})$ is finite) consists of 2-torsion points, so $t(\iota(x')) = t(\iota(x))$ by the assumption on t_2 . We can then conclude as in the proof above.

In our intended application, the set $X_1(p)^{(d)}(\mathbb{F}_\ell)$ can be quite large: the curve $X_1(p)$ has $(p - 1)/2$ \mathbb{Q} -rational cusps; assuming that they account for all of $X_1(p)^{(d)}(\mathbb{F}_\ell)$, the latter set has $\binom{(p-1)/2+d-1}{d}$ elements. Corollary 4.3 requires us to check that $t \circ \iota$ is a formal immersion at each of these points. To reduce the necessary computational effort, we now show how we can use curves intermediate between $X_1(p)$ and $X_0(p)$ that have fewer cusps.

Corollary 4.4. *Let $d \in \mathbb{Z}_{\geq 1}$ and let $\ell \neq p$ be primes. Let X_H be an intermediate curve between $X_1(p)$ and $X_0(p)$. Fix $x_0 \in X_H^{(d)}(\mathbb{Q})$ and define $\iota_H : X_H^{(d)} \rightarrow J_H$ using x_0 as basepoint. Let $t : J_H \rightarrow A$ be a morphism of abelian schemes over $\mathbb{Z}(\ell)$ such that*

- (i) $t(J_H(\mathbb{Q}))$ is finite,
- (ii) $\ell > 2$ or $\#t(J_H(\mathbb{Q}))$ is odd,
- (iii) $t \circ \iota_H$ is a formal immersion at all $\bar{x}_H \in X_H^{(d)}(\mathbb{F}_\ell)$ that are sums of images of rational cusps on $X_1(p)$.

Then assumption (a) of Lemma 1.7 is satisfied.

Proof. Let $\bar{x} \in X_1(p)^{(d)}(\mathbb{F}_\ell)$ be a sum of images of rational cusps and take two points $x, x' \in X_1(p)^{(d)}(\mathbb{Q})$ in the residue class of \bar{x} , where we take x to be the unique sum of rational cusps in this residue class. Write x_H, x'_H for their images in $X_H^{(d)}(\mathbb{Q})$. Then $\bar{x}_H := \text{red}_\ell(x_H) = \text{red}_\ell(x'_H)$ is a sum of images of rational cusps on $X_1(p)$. Arguing as in the proof of Corollary 4.3, we see that $x'_H = x_H$; in particular, x'_H is a sum of images of rational cusps on $X_1(p)$, since this is true for x_H . The set of rational cusps on $X_1(p)$ is the full preimage of the cusp $\infty \in X_0(p)(\mathbb{Q})$. This implies that all points in $X_1(p)^{(d)}(\mathbb{Q})$ that are preimages of x_H under the obvious map are sums of rational cusps. So x' is a sum of rational cusps as well. But red_ℓ is injective on sums of rational cusps (since reduction mod ℓ is injective on cusps; see [Deligne and Rapoport 1973, Theorem IV.3.4]), and hence $x' = x$. □

5. Computational verification of assumption (a)

We use Corollary 4.4 to show that assumption (a) of Lemma 1.7 holds for the relevant pairs (d, p) . To verify the assumptions of Corollary 4.4, we need to do essentially two things: we have to find a suitable

morphism t of abelian schemes that satisfies conditions (i) and (ii), and we have to check that $t \circ \iota$ is a formal immersion at all points in $\bar{x}_H \in X_H^{(d)}(\mathbb{F}_\ell)$ that are sums of images of rational cusps on $X_1(p)$.

To satisfy condition (i), we take a morphism t that factors through the winding quotient J_H^e ; then $t(J_H(\mathbb{Q}))$ is contained in the image of $J_H^e(\mathbb{Q})$ under a morphism of abelian varieties. Since, by Theorem 2.2, $J_H^e(\mathbb{Q})$ is finite, $t(J_H(\mathbb{Q}))$ is finite as well. One possibility is to take the projection $J_H \rightarrow J_H^e$. If we choose $\ell \geq 3$, then condition (ii) is also satisfied. This was used for $J_0(p)$ with p prime and an ℓ that depends on p in the argument of [Merel 1996], and is used for $J_0(p^n)$ with $\ell = 3$ or 5 in the argument of [Parent 1999]. The proof of Oesterlé's bound uses $\ell = 3$; see Section 6.

If we take for t an element of the Hecke algebra $\mathbb{T} \subseteq \text{End}_{\mathbb{Q}}(J_H)$, then the condition for t to factor via the winding quotient is that $t \cdot \text{Ann}(\mathbf{e}) = 0$ in \mathbb{T} . We obtain such t as follows. This is essentially [Parent 2000, Lemma 1.9]; we extend the statement slightly by removing the condition that the characteristic polynomial of t_0 (acting on the space of cusp forms) is squarefree.

Proposition 5.1. *Let $t_0 \in \mathbb{T}$ with factored characteristic polynomial $P(X) = \prod_{i=1}^n P_i(X)^{e_i}$ with respect to its action on $H^0(X_H, \Omega^1)$. Set*

$$I := \{i \in \{1, \dots, n\} \mid (P/P_i)(t_0) \cdot \mathbf{e} = 0 \text{ or } e_i \geq 2\};$$

then $t_1(t_0) := \prod_{i \in I} P_i^{e_i}(t_0)$ is such that $t_1(t_0) \cdot \text{Ann}(\mathbf{e}) = 0$.

Proof. The proof is basically the same as that in [Parent 2000, § 2.5], noting that the factors $P_i^{e_i}(t_0)$ with $e_i \geq 2$ in the product defining $t_1(t_0)$ are used to kill any factor of the Hecke algebra for which we cannot simply decide whether it is contained in $\text{Ann}(\mathbf{e})$. \square

We note that we can compute $P(X)$ and test the condition $(P/P_i)(t_0) \cdot \mathbf{e} = 0$ explicitly using modular symbols, so we can determine $t_1(t_0)$ explicitly for any given t_0 . We see that $t_1(t_0)$ satisfies condition (i) for every $t_0 \in \mathbb{T}$.

To satisfy condition (ii) when $\ell = 2$, we use Proposition 2.3, which implies that for q an odd prime not dividing N , $T_q - \langle q \rangle - q$ kills the rational torsion subgroup of J_H . Combining this with Proposition 5.1 gives the following version of “Parent’s trick”.

Corollary 5.2. *Let X_H be an intermediate curve between $X_1(p)$ and $X_0(p)$. Let $t_0 \in \mathbb{T}$ and let $q \neq p$ be an odd prime. Then*

$$t := t_1(t_0) \cdot (T_q - \langle q \rangle - q) \in \mathbb{T},$$

considered as an element of $\text{End}_{\mathbb{Q}}(J_H)$, satisfies conditions (i) and (ii) of Corollary 4.4 for $\ell = 2$. If $X_H = X_0(p)$ and $p \not\equiv 1 \pmod{8}$, then $t := t_1(t_0)$ satisfies both conditions.

Proof. By Proposition 5.1 and the discussion preceding it, $t_1(t_0)$ satisfies condition (i). Obviously this condition still holds after composing $t_1(t_0)$ with some further morphism. By Proposition 2.3, the factor $T_q - \langle q \rangle - q$ kills the torsion in $t_1(t_0)(J_H(\mathbb{Q})) \subseteq J_H(\mathbb{Q})_{\text{tors}}$, which implies that $t(J_H(\mathbb{Q})) = 0$, so that condition (ii) also holds.

It is known that $J_0(p)(\mathbb{Q})_{\text{tors}}$ is cyclic of order $(p - 1)/\gcd(p - 1, 12)$, generated by the difference of the two (rational) cusps; see [Mazur 1977, Theorem 1]. This implies that the rational torsion group of $J_0(p)$ has odd order when $p \not\equiv 1 \pmod 8$, and so condition (ii) is automatically satisfied. \square

We still need a way of verifying condition (iii) of Corollary 4.4. This is provided by the following version of “Kamienny’s criterion” as given in [Parent 2000, Theorem 1.10, Proposition 2.7]. Parent states this criterion for $X_1(p)$ in place of X_H , but the generalization is immediate.

Proposition 5.3. *Let $H \subseteq (\mathbb{Z}/p\mathbb{Z})^\times / \{\pm 1\}$ be a subgroup. Let $\ell \neq p$ be a prime and consider $t = t_1(t_0)$ as in Proposition 5.1 when ℓ is odd, or t as in Corollary 5.2 when $\ell = 2$. Then $t \circ \iota$ is a formal immersion at all $\bar{x}_H \in X_H^{(d)}(\mathbb{F}_\ell)$ that are sums of images of rational cusps on $X_1(p)$ if for all partitions $d = n_1 + \dots + n_m$ with $n_1 \geq \dots \geq n_m$ and all m -tuples $(d_1 = 1, d_2, \dots, d_m)$ of integers representing pairwise distinct elements of H , the d Hecke operators*

$$(T_i \langle d_j \rangle t)_{\substack{j=1, \dots, m, \\ i=1, \dots, n_j}} \tag{5-1}$$

are \mathbb{F}_ℓ -linearly independent in $\mathbb{T} \otimes \mathbb{F}_\ell$, where \mathbb{T} is considered as a subalgebra of $\text{End}_{\mathbb{Q}}(J_H)$.

We note that we can check the criterion for any given t by a computation with modular symbols.

This criterion was first established by Kamienny [1992b] for $X_0(p)$. In this case, the condition simplifies to:

The d Hecke operators $T_1 t, T_2 t, \dots, T_d t$ are \mathbb{F}_ℓ -linearly independent in $\mathbb{T} \otimes \mathbb{F}_\ell$.

Implementing the criterion implied by Corollary 5.2 and Proposition 5.3 for $X_0(p)$ and running the resulting code gives the following. We take as basepoint for ι the point given by d times the cusp ∞ on $X_0(p)$. Note that $2281 = \lfloor (1 + 3^{7/2})^2 \rfloor$; larger primes will be dealt with using Oesterlé’s bound.

Lemma 5.4. *For each of the following choices of $3 \leq d \leq 7$ and a prime p , there is $t \in \text{End}_{\mathbb{Q}}(J_0(p))$ as in Corollary 5.2 for $\ell = 2$ such that $t \circ \iota : X_0(p)_{\mathbb{Z}(2)}^{(d)} \rightarrow J_0(p)_{\mathbb{Z}(2)}$ is a formal immersion at the point of $X_0(p)^{(d)}(\mathbb{F}_2)$ corresponding to d times the cusp ∞ :*

- $d = 3$ and $47 \leq p \leq 2281, p \neq 73, 79$;
- $d = 4$ and $p \in \{47, 59, 71, 83, 89\}$ or $103 \leq p \leq 2281$;
- $d = 5$ and $p \in \{59, 71, 83\}$ or $103 \leq p \leq 2281$;
- $d = 6$ and $p \in \{71, 107\}$ or $127 \leq p \leq 2281, p \neq 193$;
- $d = 7$ and $p = 131$ or $139 \leq p \leq 2281, p \neq 157, 193$.

Proof. We try $t_0 = T_n$ for $2 \leq n \leq 60$, and when $p \equiv 1 \pmod 8$, we try for each t_0 the additional factor $T_q - (q + 1)$ for primes $3 \leq q \leq 20$ until either the criterion is satisfied or else all combinations are exhausted. (Actually, $n \leq 14$ and $q \in \{3, 5\}$ would be enough, as the computation reveals.) The computation took about 1.5 hours. We note that to exclude $p = 163$ for $d = 7$, we actually needed the statement of Corollary 5.2 that $t = t_1(t_0)$ is sufficient when $p \not\equiv 1 \pmod 8$ (which also helps to speed up the computation, since it eliminates the inner loop over q). For $p = 431$ and $d = 7$, taking $t_0 = T_n$ does not

seem to work. We tried random linear combinations of the first few Hecke operators and were successful with $t_0 = T_2 + T_3 - T_7$. \square

For the remaining primes p of interest for any given degree d , we use the criterion on an intermediate curve X_H ; we try the various groups H ordered by increasing index in $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$, since smaller index means that we have to deal with smaller objects, leading to a faster computation.

If we were to use the criterion of Proposition 5.3 literally, then we would have to run through a potentially very large number of partitions of d combined with choices of d_j . We use the following trick to speed up the computation.

Lemma 5.5. *Let $H \subseteq (\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$ be a subgroup. Let $\ell \neq p$ be a prime, d an integer and $t \in \mathbb{T}$, viewed as an endomorphism of J_H . Let $D \subseteq \mathbb{Z}$ be a set of representatives of the cosets of H with $1 \in D$. Define the set*

$$I := \{(1, i) \mid 1 \leq i \leq d\} \cup \{(k, i) \mid 1 \leq i \leq \lfloor \frac{1}{2}d \rfloor, 1 \neq k \in D\}.$$

Suppose that there is no \mathbb{F}_ℓ -linear dependence among at most d of the images in $\mathbb{T} \otimes \mathbb{F}_\ell$ of the elements $t_{(k,i)} := T_i \langle k \rangle t$ for $(k, i) \in I$, where we consider \mathbb{T} as a subalgebra of $\text{End}_{\mathbb{Q}}(J_H)$. Then the criterion of Proposition 5.3 is satisfied.

Proof. Assume the criterion fails. Then there is a partition $d = n_1 + \dots + n_m$ with $n_1 \geq \dots \geq n_m$ and there are $d_1 = 1, d_2, \dots, d_m \in D$ pairwise distinct such that the d operators $T_i \langle d_j \rangle t$ for $1 \leq j \leq m$ and $1 \leq i \leq n_j$ are linearly dependent in $\mathbb{T} \otimes \mathbb{F}_\ell$. But these operators are all of the form $t_{(k,i)}$ (note $n_j \leq \lfloor \frac{1}{2}d \rfloor$ for $j \geq 2$), so this would produce a linear dependence mod ℓ among d of the $t_{(k,i)}$; this is a contradiction. \square

When implementing this, we can in addition look at each linear relation of weight at most d between the elements in the lemma and check if it is indeed of the “forbidden” form as given in Proposition 5.3. In the cases of interest, the relation space has low enough dimension to allow for the enumeration of all relations and performing this check. We use algorithms for binary linear codes that are included in Magma to do this efficiently.

We obtain the following result.

Lemma 5.6. *For each of the following choices of $3 \leq d \leq 7$ and a prime p , there is a subgroup H of $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$ and $t \in \text{End}_{\mathbb{Q}}(J_H)$ as in Corollary 5.2 for $\ell = 2$ such that $t \circ \iota : X_{H, \mathbb{Z}(2)}^{(d)} \rightarrow J_{H, \mathbb{Z}(2)}$ is a formal immersion at all points of $X_H^{(d)}(\mathbb{F}_2)$ that are sums of images of rational cusps on $X_1(p)$:*

$$\begin{aligned} d = 3 & \quad \text{and} \quad 19 \leq p \leq 2281; \\ d = 4 & \quad \text{and} \quad 19 \leq p \leq 2281, \quad p \neq 29; \\ d = 5 & \quad \text{and} \quad 23 \leq p \leq 2281, \quad p \neq 29; \\ d = 6 & \quad \text{and} \quad 23 \leq p \leq 2281, \quad p \neq 29; \\ d = 7 & \quad \text{and} \quad 37 \leq p \leq 2281. \end{aligned}$$

Proof. For each pair (d, p) that is not covered by Lemma 5.4, we check the criterion of Lemma 5.5 for subgroups H by increasing index. For each H , we again try $t_0 = T_n$ for $2 \leq n \leq 60$ and the second factor given by primes $3 \leq q \leq 20$. The most involved computation is for $d = 7$ and $p = 107$, where we have to take the trivial subgroup H corresponding to $J_1(107)$; this computation took about 35 minutes. Most of the other cases just take a few seconds, a small number of them a few minutes. \square

Proposition 1.8 now follows from Lemma 5.6 and Corollary 3.6.

6. A proof of Oesterlé's bound

The purpose of this section is to provide a proof of Oesterlé's bound (1-1) and thus close a gap in the literature. Oesterlé gives a proof in his notes [1994], which have been available to the people working in the field, but a proof has never appeared in print. The proof below is based on these notes, which Oesterlé kindly provided to us; in particular, we do not claim originality for anything in this section: the ideas are all Oesterlé's. We will use results that are available in the literature by now to simplify the exposition in some places. We state the result of this section as a theorem.

Theorem 6.1 (Oesterlé). *Let $d \geq 3$. If $p > (3^{d/2} + 1)^2$ is a prime, then $p \notin S(d)$.*

We can restrict to $d \geq 3$ here, since the cases $d = 1$ and $d = 2$ have been dealt with by Mazur and Kamienny, respectively.

We will work with $\ell = 3$. By Lemma 1.9, assumption (b) of Lemma 1.7 is always satisfied when $p > (3^{d/2} + 1)^2$. So it is sufficient to show that assumption (a) of Lemma 1.7 holds. This in turn is done by using the formal immersion criterion via the winding quotient of $J_0(p)$. For sufficiently large d , this follows from the following result.

Proposition 6.2. *If $d \geq 3$ and $p \geq 65(2d)^6$ is a prime, then the map*

$$f_{d,p} : X_0(p)^{(d)} \xrightarrow{\iota} J_0(p) \rightarrow J_0^e(p)$$

is a formal immersion at the point $\bar{x} \in X_0(p)^{(d)}(\mathbb{F}_3)$ that is the reduction mod 3 of d times the cusp ∞ on $X_0(p)$.

In particular, Theorem 6.1 holds for $d \geq 26$.

Proof. The first statement is a consequence of [Parent 1999, Theorem 1.8 and Proposition 1.9]. Since $65(2d)^6 < (3^{d/2} + 1)^2$ when $d \geq 26$, the statement of Theorem 6.1 follows for such d by the discussion above. \square

Oesterlé proves a similar statement with a slightly worse bound on p ; Parent uses the same underlying approach.

In principle, Proposition 6.2 reduces the proof of Theorem 6.1 to a finite problem: for each $3 \leq d \leq 25$ and each prime p such that $(3^{d/2} + 1)^2 < p < 65(2d)^6$, we have to check that the map in Proposition 6.2 is a formal immersion at the relevant point, which can be done via Kamienny's criterion given in Proposition 5.3. However, the primes we would have to deal with in this way get much too large and there are way too

many of them to make this practical. So instead, we need a criterion that allows us to deal with all (or many) of these primes at the same time.

One idea that Oesterlé uses here (and also to prove a statement similar to Proposition 6.2 above) is to make use of the intersection pairing on $H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$, which is an alternating perfect pairing into \mathbb{Z} . We will denote this pairing by \bullet .

We will use the following version of Kamienny's criterion. Recall from Definition 2.1 the winding element $e \in H_1(X_0(p)(\mathbb{C}), \mathbb{Q})$.

Proposition 6.3. *The map $f_{d,p}$ as in Proposition 6.2 is a formal immersion at \bar{x} if (and only if) the images of T_1e, \dots, T_de in $\mathbb{T}e/3\mathbb{T}e$ are linearly independent over \mathbb{F}_3 .*

Proof. This is [Parent 1999, Theorem 4.18] for $l = 3$. □

To make use of the intersection pairing, we have to move the elements $T_n e \in H_1(X_0(p)(\mathbb{C}), \mathbb{Q})$ into $H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$. The Hecke operator $T_2 - 3$ sends e into $H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$, since the action of T_2 , viewed as a correspondence on $X_0(p)$, multiplies the cusps 0 and ∞ by 3, so that the boundary of $-(T_2 - 3) \cdot \{0, \infty\}$ is zero. In the same way, we see that $(T_n - \sigma_1(n))e \in H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$ when $n < p$; here $\sigma_1(n)$ denotes the sum of (positive) divisors of n . (This is true in general when $p \nmid n$; when $p \mid n$, one has to replace $\sigma_1(n)$ with the sum of divisors not divisible by p .)

Corollary 6.4. *If $p > (3^{d/2} + 1)^2$ and the images of*

$$(T_2 - 3)T_1e, \dots, (T_2 - 3)T_de$$

in $H_1(X_0(p)(\mathbb{C}), \mathbb{F}_3)$ are linearly independent over \mathbb{F}_3 , then $p \notin S(d)$.

Proof. We show that $f_{d,p}$ is a formal immersion at \bar{x} , which implies the claim. Assume that this is not the case. By Proposition 6.3, there are integers $\lambda_1, \dots, \lambda_d$, not all divisible by 3, such that $\lambda_1 T_1 e + \dots + \lambda_d T_d e \in 3\mathbb{T}e$. Multiplying by $T_2 - 3$, this gives

$$\lambda_1 (T_2 - 3)T_1 e + \dots + \lambda_d (T_2 - 3)T_d e \in 3(T_2 - 3)\mathbb{T}e \subset 3H_1(X_0(p)(\mathbb{C}), \mathbb{Z}),$$

with all terms on the left contained in $H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$. Reducing this relation mod 3 shows that the images of $(T_2 - 3)T_1 e, \dots, (T_2 - 3)T_d e$ in $H_1(X_0(p)(\mathbb{C}), \mathbb{F}_3)$ are linearly dependent. □

We now define the following Hecke operators.

Definition 6.5. Let $n \geq 1$. We set

$$T'_n = \sum_{m|n} \mu\left(\frac{n}{m}\right) T_m,$$

where μ is the Möbius function, and

$$L_n = T'_{2n} - 2T'_n.$$

Then $T_n - \sigma_1(n) = \sum_{m|n} (T'_m - m)$. Using the relations

$$T_2 T_m = \begin{cases} T_{2m} & \text{if } m \text{ is odd,} \\ T_{2m} + 2T_{m/2} & \text{if } m \text{ is even,} \end{cases}$$

we find that

$$(T_2 - 3)T'_n = \begin{cases} L_n & \text{if } n \text{ is odd,} \\ L_n - L_{n/2} & \text{if } n \text{ is even.} \end{cases}$$

Corollary 6.6. *If $p > (3^{d/2} + 1)^2$ and the images of*

$$L_1\mathbf{e}, \dots, L_d\mathbf{e}$$

in $H_1(X_0(p)(\mathbb{C}), \mathbb{F}_3)$ are linearly independent over \mathbb{F}_3 , then $p \notin S(d)$.

Proof. The relations deduced above show that the \mathbb{Z} -submodule of \mathbb{T} generated by L_1, \dots, L_d is the same as the \mathbb{Z} -submodule generated by $(T_2 - 3)T_1, \dots, (T_2 - 3)T_d$. Now use Corollary 6.4. \square

We now introduce notation for certain modular symbols, following [Merel 1996, Section 2]. If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, then the modular symbol $\{\gamma 0, \gamma \infty\}$ depends only on the coset $\Gamma_0(p)\gamma$, which in turn depends only on the image of c/d in $\mathbb{P}^1(\mathbb{F}_p)$. We denote this modular symbol by $\xi(c/d)$. If k is an integer coprime with p , then $\xi(k) = \{0, 1/k\} \in H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$, since the cusp $1/k$ is $\Gamma_0(p)$ -equivalent to 0.

The following result is crucial; we defer its proof until later and first show how Theorem 6.1 can be deduced from it with some computation. For $M \geq 3$ an odd integer, we define

$$\varepsilon_M : (\mathbb{Z}/M\mathbb{Z})^\times \rightarrow \{0, 1\}$$

so that $\varepsilon_M(a + M\mathbb{Z}) = 0$ if $1 \leq a < \frac{1}{2}M$ and $\varepsilon_M(a + M\mathbb{Z}) = 1$ if $\frac{1}{2}M < a < M$. We extend ε_M to a map on all rational numbers a/b with numerator and denominator coprime to M by applying it to the image of a/b in $(\mathbb{Z}/M\mathbb{Z})^\times$.

Lemma 6.7. *Let $d \geq 1$ be an integer, let $M \geq 3$ be an odd integer and let $p > 2dM$ be a prime. Let $u \in \mathbb{Z}$ be such that $pu \equiv 1 \pmod{M}$. Then for a coprime to M and $1 \leq n \leq d$, we have*

$$L_n\mathbf{e} \bullet \left\{ 0, \frac{a}{M} \right\} = \varepsilon_M(na) - \varepsilon_M(nu/a).$$

Corollary 6.8 [Oesterlé 1994, Proposition 8]. *Let d and M be as in Lemma 6.7 and fix $u \in \mathbb{Z}$ coprime with M . If the matrix*

$$\left(\varepsilon_M(na) - \varepsilon_M(nu/a) \right)_{1 \leq n \leq d, a \in (\mathbb{Z}/M\mathbb{Z})^\times},$$

with entries taken in \mathbb{F}_3 , has rank d , then $p \notin S(d)$ for all primes

$$p > \max\{2dM, (3^{d/2} + 1)^2\} \quad \text{such that } pu \equiv 1 \pmod{M}.$$

Proof. By Lemma 6.7, the matrix entries are the intersection numbers, taken mod 3, between $L_n\mathbf{e}$ and $\{0, a/M\}$ in $H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$, when p is a prime as in the statement. So when the matrix has rank d , this implies that $L_1\mathbf{e}, \dots, L_d\mathbf{e}$ are linearly independent mod 3, and the claim follows from Corollary 6.6. \square

Proof of Theorem 6.1. The following table gives, for each $3 \leq d \leq 25$, a value of M as in Corollary 6.8 such that the matrix above has rank d for all $u \in (\mathbb{Z}/M\mathbb{Z})^\times$. By Corollary 6.8, this proves Theorem 6.1 for all $p > \max\{2dM, (3^{d/2} + 1)^2\}$.

d	3	4	5	6	7	8	9	10	11	12	13	14
M	29	37	41	43	47	47	53	53	53	61	73	73
d	15	16	17	18	19	20	21	22	23	24	25	
M	79	79	89	89	89	101	101	109	109	109	127	

Note that $2dM < (3^{d/2} + 1)^2$ for $d \geq 6$. We have already verified the formal immersion criterion (with $\ell = 2$) for the primes between $(3^{d/2} + 1)^2$ and $2dM$ for $3 \leq d \leq 5$ in Lemma 5.6, which implies $p \notin S(d)$ for these primes as well. \square

Remark. Oesterlé deals with the remaining primes p for $3 \leq d \leq 5$ by computing the intersection products $I_n \mathbf{e} \bullet \xi(k)$ for $1 \leq k \leq p-1$ and $1 \leq n \leq d$, where $I_1 = (p-1)/\gcd(p-1, 12)$ is the order of $J_0(p)(\mathbb{Q})_{\text{tors}}$ and $I_n = T'_n - n$ for $n \geq 2$, and verifying that the resulting matrix has rank d (even when reduced modulo any prime $\ell \geq 3$). This works for all cases except $p = 43$ and $p = 73$ for $d = 3$. For $p = 73$, he has a separate argument, whereas he does not mention $p = 43$ further, even though the maximal d for which the rank condition is satisfied is $d = 2$ according to the table at the end of [Oesterlé 1994, Section 7].

From now on until the end of this section, the degree d of the field of definition of the elliptic curves will be irrelevant. We will therefore feel free to use “ d ” as a local variable as in the definition of M_n below, and hope that this will not lead to confusion.

It remains to prove Lemma 6.7. We follow Oesterlé’s notes quite closely here (modulo some changes of notation). We remark that Corollaries 6.12 and 6.13 are in a separate file that Oesterlé made available to Bas Edixhoven and the first author of this paper.

We begin with a result that expresses $(T_n - \sigma_1(n))\mathbf{e}$ for $n < p$ in terms of modular symbols.

Lemma 6.9 [Oesterlé 1994, Corollary 2 of Proposition 10]. *For $n < p$, we have in $H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$ that*

$$(T_n - \sigma_1(n))\mathbf{e} = - \sum_{(a,b,c,d) \in M_n} \xi\left(\frac{c}{d}\right),$$

where

$$M_n = \{(a, b, c, d) \in \mathbb{Z}^4 : a > b \geq 0, d > c > 0, ad - bc = n\}.$$

Proof. This is [Merel 1996, Lemma 2], using that both sides are contained in $H_1(X_0(p)(\mathbb{C}), \mathbb{Z})$. \square

We need a formula for the intersection product. We define the following function on \mathbb{R} :

$$H(x) = \begin{cases} 0 & \text{if } x < 0, \\ \frac{1}{2} & \text{if } x = 0, \\ 1 & \text{if } x > 0. \end{cases}$$

Lemma 6.10 [Oesterlé 1994, Equation (37)]. *Let p be a prime and $k, k' \in \{1, \dots, p-1\}$. We write k_* for the unique element of $\{1, \dots, p-1\}$ such that $kk_* \equiv -1 \pmod{p}$. Then*

$$\xi(k) \bullet \xi(k') = -H(k' - k) + H(k' - k_*) + H(k'_* - k) - H(k'_* - k_*).$$

Proof. By [Merel 1996, Lemma 4], for $k' \notin \{k, k_*\}$, $\xi(k) \bullet \xi(k')$ is the intersection number $(-1, 0, \text{ or } 1)$ of the oriented line segment joining $e^{2\pi i k'_*/p}$ to $e^{2\pi i k'/p}$ and that joining $e^{2\pi i k_*/p}$ to $e^{2\pi i k/p}$. Otherwise the intersection number is zero, since the pairing is alternating and $\xi(k_*) = -\xi(k)$. The formula we have given follows by considering the various possible cyclic orderings of the four points on the unit circle connected by the two line segments. \square

We enlarge M_n slightly and set

$$B_n = \{(a, b, c, d) \in \mathbb{Z}^4 : a > b \geq 0, d > c \geq 0, ad - bc = n\}$$

(so we allow $c = 0$ here) and write $B_n^{b=0}$, $B_n^{b>0}$, $B_n^{c=0}$ and $B_n^{c>0} = M_n$ for the subsets satisfying the indicated extra condition.

We define, for $n \geq 1$, a prime $p > n$ and $k \in \{1, \dots, p-1\}$, the following two quantities:

$$v_{p,n}(k) = \#\{(a, b, c, d) \in \mathbb{Z}_{>0} : ad + bc = n, c \equiv dk \pmod{p}\},$$

$$v'_{p,n}(k) = \#\{(a, b, c, d) \in \mathbb{Z}_{>0} : ad + bc = n, \gcd(c, d) = 1, c \equiv dk \pmod{p}\}.$$

We now give an explicit formula for the intersection number $(T_n - \sigma_1(n))\mathbf{e} \bullet \xi(k)$. Its proof by Oesterlé is quite ingenious.

Proposition 6.11 [Oesterlé 1994, Proposition 12]. *Let p be a prime and $k, n \in \{1, \dots, p-1\}$. Then:*

$$(i) \quad (T_n - \sigma_1(n))\mathbf{e} \bullet \xi(k) = \sum_{m|n} \left(\left\lfloor \frac{mk}{p} \right\rfloor - \left\lfloor \frac{mk_*}{p} \right\rfloor \right) + v_{p,n}(k) - v_{p,n}(k_*).$$

$$(ii) \quad (T'_n - n)\mathbf{e} \bullet \xi(k) = \left\lfloor \frac{nk}{p} \right\rfloor - \left\lfloor \frac{nk_*}{p} \right\rfloor + v'_{p,n}(k) - v'_{p,n}(k_*).$$

Proof. Claim (ii) follows from claim (i) by Möbius inversion. So it suffices to show (i).

We write $k_{c/d}$ for the integer $k \in \{1, \dots, p-1\}$ such that $c \equiv dk \pmod{p}$, where c and d are integers coprime to p . We extend this to all remaining elements $x \in \mathbb{P}^1(\mathbb{Q})$ by setting $k_x = p$. Then Lemmas 6.9 and 6.10 imply that

$$\begin{aligned} (T_n - \sigma_1(n))\mathbf{e} \bullet \xi(k) &= - \sum_{(a,b,c,d) \in M_n} \xi\left(\frac{c}{d}\right) \bullet \xi(k) \\ &= \sum_{(a,b,c,d) \in M_n} (H(k - k_{c/d}) - H(k - k_{-d/c}) - H(k_* - k_{c/d}) + H(k_* - k_{-d/c})). \end{aligned}$$

We note that when $c = 0$, all terms under the summation sign are zero (since $k_0 = k_\infty = p$ and $H(k - p) = H(k_* - p) = 0$), so that we can replace the summation over $M_n = B_n^{c>0}$ by a summation over B_n without changing the value of the sum.

We now observe that there is a bijection

$$\phi_n : B_n^{b>0} \rightarrow B_n^{c>0}, \quad (a, b, c, d) \mapsto (b, -a + mb, d, -c + mb),$$

where $m = \lceil a/b \rceil \geq 2$ is the unique integer such that $0 \leq -a + mb < b$; its inverse is given by

$$(a, b, c, d) \mapsto (-b + m'a, a, -d + m'c, c) \quad \text{with } m' = \lceil d/c \rceil.$$

We split the sum as follows:

$$\begin{aligned} & \sum_{(a,b,c,d) \in B_n} (H(k - k_{c/d}) - H(k - k_{-d/c})) - H(k_* - k_{c/d}) + H(k_* - k_{-d/c}) \\ &= \sum_{(a,b,c,d) \in B_n^{b>0}} (H(k - k_{c/d}) - H(k_* - k_{c/d})) + \sum_{(a,b,c,d) \in B_n^{b>0}} (H(k - k_{c/d}) - H(k_* - k_{c/d})) \\ & \quad - \sum_{(a,b,c,d) \in B_n^{c=0}} (H(k - k_{-d/c}) - H(k_* - k_{-d/c})) - \sum_{(a,b,c,d) \in B_n^{c>0}} (H(k - k_{-d/c}) - H(k_* - k_{-d/c})). \end{aligned} \quad (6-1)$$

Writing the quadruple in the last sum in (6-1) as $\phi_n(a, b, c, d)$, this then gives

$$\sum_{(a,b,c,d) \in B_n^{b>0}} (H(k - k_{c/d}) - H(k_* - k_{c/d})) \quad (6-2)$$

$$- \sum_{(a,b,c,d) \in B_n^{c=0}} (H(k - k_{-d/c}) - H(k_* - k_{-d/c})) \quad (6-3)$$

$$+ \sum_{(a,b,c,d) \in B_n^{b>0}} (H(k - k_{c/d}) - H(k - k_{c/d - \lceil a/b \rceil}) - H(k_* - k_{c/d}) + H(k_* - k_{c/d - \lceil a/b \rceil})). \quad (6-4)$$

We evaluate the three sums in the last expression separately. First note that the second sum (6-3) is zero, since $k_{-d/c} = p$ for $c = 0$ and $H(k - p) = H(k_* - p) = 0$ for all relevant k . We now look at the first sum (6-2), which is the following expression minus the same expression with k replaced by k_* :

$$\sum_{(a,b,c,d) \in B_n^{b>0}} H(k - k_{c/d}) = \sum_{d|n} \sum_{c=0}^{d-1} H(k - k_{c/d}) = \sum_{d|n} \sum_{c=1}^{d-1} H(k - k_{c/d}).$$

We set

$$s(k) = \#\{(c, d) \in \mathbb{Z}^2 : d | n, 0 < c < d, c \equiv dk \pmod{p}\}; \quad (6-5)$$

then the sum above is

$$\sum_{d|n} \#\{c \in \mathbb{Z} : 0 < c < d, k_{c/d} \leq k\} - \frac{1}{2}s(k).$$

Now $dk_{c/d} = up + c$, where $1 \leq u < d$ satisfies $up \equiv -c \pmod{d}$, and so $k_{c/d} = \lceil up/d \rceil$. The map that sends u to c is a permutation of $\{1, \dots, d-1\}$, which implies that

$$\#\{c \in \mathbb{Z} : 0 < c < d, k_{c/d} \leq k\} = \#\{u \in \mathbb{Z} : 0 < u < d, up \leq dk\} = \left\lfloor \frac{dk}{p} \right\rfloor.$$

This gives the expression

$$\sum_{m|n} \left(\left\lfloor \frac{mk}{p} \right\rfloor - \left\lfloor \frac{mk_*}{p} \right\rfloor \right) - \frac{1}{2}(s(k) - s(k_*)) \quad (6-6)$$

for the sum in (6-2).

Now we look at the third sum (6-4). Let $x = c/d$ for some $(a, b, c, d) \in B_n^{b>0}$; then $p > n \geq d > 0$, so $p \nmid d$. If \mathcal{A} is a statement, we set $[\mathcal{A}] = 0$ if \mathcal{A} is false and $[\mathcal{A}] = 1$ if \mathcal{A} is true. Then, by checking the various cases and using that $k_{x-1} = k_x - 1$ when $k_x \neq 1$, we find that

$$H(k - k_x) - H(k - k_{x-1}) = [k_x = 1] - \frac{1}{2}[k = k_x] - \frac{1}{2}[k = k_{x-1}].$$

This implies that

$$H(k - k_x) - H(k - k_{x-1}) - H(k_* - k_x) + H(k_* - k_{x-1}) = \frac{1}{2}[k_* \in \{k_x, k_{x-1}\}] - \frac{1}{2}[k \in \{k_x, k_{x-1}\}].$$

We obtain the following expression for (6-4):

$$\begin{aligned} & \frac{1}{2} \sum_{(a,b,c,d) \in B_n^{b>0}} \sum_{j=0}^{\lceil a/b \rceil - 1} ([k_* \in \{k_{c/d-j}, k_{c/d-j-1}\}] - [k \in \{k_{c/d-j}, k_{c/d-j-1}\}]) \\ &= \frac{1}{2} (\#\{(a, b, c, d) \in B_n^{b>0} : k_{c/d} = k_*\} - \#\{(a, b, c, d) \in B_n^{b>0} : k_{c/d} = k\}) \end{aligned} \quad (6-7)$$

$$+ \frac{1}{2} (\#\{(a, b, c, d) \in B_n^{b>0} : k_{c/d - \lceil a/b \rceil} = k_*\} - \#\{(a, b, c, d) \in B_n^{b>0} : k_{c/d - \lceil a/b \rceil} = k\}) \quad (6-8)$$

$$+ \#\{(a, b, c, d, j) \in U_n : k_* = k_{c/d-j}\} - \#\{(a, b, c, d, j) \in U_n : k = k_{c/d-j}\}, \quad (6-9)$$

where we have set

$$U_n = \left\{ (a, b, c, d, j) : (a, b, c, d) \in B_n^{b>0}, 1 \leq j < \left\lceil \frac{a}{b} \right\rceil \right\}.$$

Now we observe that there is a bijection

$$\psi_n : U_n \rightarrow \{(a, b, c, d) \in \mathbb{Z}_{>0}^4 : ad + bc = n\}, \quad (a, b, c, d, j) \mapsto (b, a - jb, d, -c + jd)$$

(its inverse maps (a, b, c, d) to $(b + ja, a, -d + jc, c, j)$ with $j = \lceil d/c \rceil$). Writing $\psi_n(a, b, c, d, j) = (a', b', c', d')$, we see that $k = k_{c/d-j}$ is equivalent to $k = k_{-d'/c'}$, which is the same as saying that $k_* = k_{c'/d'}$, or that $c' \equiv k_* d' \pmod{p}$. This shows that the terms in line (6-9) above are equal to

$$v_{p,n}(k) - v_{p,n}(k_*).$$

Using the bijection ϕ_n between $B_n^{b>0}$ and $B_n^{c>0}$, we see that the terms in line (6-8) can be written as

$$\begin{aligned} & \frac{1}{2} (\#\{(a, b, c, d) \in B_n^{c>0} : k_{-d/c} = k_*\} - \#\{(a, b, c, d) \in B_n^{c>0} : k_{-d/c} = k\}) \\ &= \frac{1}{2} (\#\{(a, b, c, d) \in B_n^{c>0} : k_{c/d} = k\} - \#\{(a, b, c, d) \in B_n^{c>0} : k_{c/d} = k_*\}). \end{aligned} \quad (6-10)$$

This cancels the part of the terms in line (6-7) in which c is strictly positive, and the terms with $c = 0$ do not contribute anything. What remains is the part with $b = 0$ in (6-10), which is

$$\begin{aligned} \frac{1}{2}(\#\{(c, d) \in \mathbb{Z}_{>0}^2 : d > c > 0, d \mid n, c \equiv dk \pmod{p}\} - \#\{(c, d) \in \mathbb{Z}_{>0}^2 : d > c > 0, d \mid n, c \equiv dk_* \pmod{p}\}) \\ = \frac{1}{2}(s(k) - s(k_*)) \end{aligned}$$

with $s(k)$ as in (6-5). This cancels the contribution coming from $s(k)$ and $s(k_*)$ in (6-6), and we obtain the desired result. \square

Corollary 6.12. *Let $n \geq 1$ be an integer, let c and d be coprime integers such that $c > d > 0$, and let $p > nc$ be a prime. Let a and b be the integers satisfying $0 \leq a < c$, $0 \leq b < d$, and $ad - bc = 1$. Let $k, k_* \in \{1, \dots, p-1\}$ be such that $c \equiv dk \pmod{p}$ and $-d \equiv ck_* \pmod{p}$. Further, let the integers u and u_* satisfy $dk = up + c$ and $ck_* = u_*p - d$.*

Then $0 \leq u < d$, $0 \leq u_ < c$, and*

$$(T'_n - n)\mathbf{e} \bullet \xi(k) = \left\lfloor \frac{nu}{d} \right\rfloor - \left\lfloor \frac{nb}{d} \right\rfloor + \left\lfloor \frac{na}{c} \right\rfloor - \left\lfloor \frac{nu_*}{c} \right\rfloor.$$

Proof. Since $dk - c > -p$ and $dk - c < dp$, we see that $0 \leq u < d$. Since $ck_* + d > 0$ and $ck_* + d < c(k_* + 1) \leq cp$, we also see that $0 \leq u_* < c$.

By Proposition 6.11,

$$(T'_n - n)\mathbf{e} \bullet \xi(k) = \left\lfloor \frac{nk}{p} \right\rfloor - \left\lfloor \frac{nk_*}{p} \right\rfloor + v'_{p,n}(k) - v'_{p,n}(k_*).$$

We evaluate each of the terms.

We have that $nk/p = nu/d + nc/(pd)$ and $p > nc$, so $0 < nc/(pd) < 1/d$, which implies that $\lfloor nk/p \rfloor = \lfloor nu/d \rfloor$.

Similarly, we have that $nk_*/p = nu_*/c - nd/(cp)$ and $p > nd$, so $0 < nd/(pc) < 1/c$, which implies that $\lfloor nk_*/p \rfloor = \lfloor (nu_* - 1)/c \rfloor$.

The third term counts the quadruples (a', b', c', d') of positive integers such that c' and d' are coprime, $a'd' + b'c' = n$, and $c' \equiv d'k \pmod{p}$. The latter implies that $c'd' \equiv cd' \pmod{p}$. Since $0 < c'd' < nd < p$ and $0 < cd' < cn < p$, we must have equality; then the coprimality of c' and d' and of c and d forces $(c', d') = (c, d)$. We have that $nad - nbc = n = a'd' + b'c' = a'd + b'c$, which implies that there is some $t \in \mathbb{Z}$ such that $na - a' = tc$ and $nb + b' = td$. The conditions $a', b' > 0$ then translate into $t < na/c$ and $t > nb/d$. Since $a/c > b/d$, this gives

$$v'_{p,n}(k) = \#\left\{t \in \mathbb{Z} : \frac{nb}{d} < t < \frac{na}{c}\right\} = \left\lfloor \frac{na-1}{c} \right\rfloor - \left\lfloor \frac{nb}{d} \right\rfloor.$$

The fourth term similarly counts quadruples (a', b', c', d') of positive integers such that c' and d' are coprime, $a'd' + b'c' = n$, and $p \mid c'k + d'$. The latter implies that $p \mid cc' + dd'$. But $0 < cc' + dd' < c(c' + d') \leq cn < p$, so there are no such quadruples, and the fourth term is zero.

Finally, note that

$$\left\lfloor \frac{na-1}{c} \right\rfloor - \left\lfloor \frac{nu_*-1}{c} \right\rfloor = \left\lfloor \frac{na}{c} \right\rfloor - \left\lfloor \frac{nu_*}{c} \right\rfloor,$$

as can be seen by considering the cases $c|n$ and $c \nmid n$ separately, taking into account that c is coprime with a and u_* . □

Corollary 6.13. *Let $M \geq 2$ be an integer, let $1 \leq a < M$ be coprime with M , let $n \geq 1$ be an integer, and let $p > nM$ be a prime. We let w denote the integer such that $1 \leq w < M$ and $apw \equiv 1 \pmod{M}$. Then*

$$(T'_n - n)\mathbf{e} \bullet \left\{0, \frac{a}{M}\right\} = \left\lfloor \frac{na}{M} \right\rfloor - \left\lfloor \frac{nw}{M} \right\rfloor.$$

Proof. We prove this by induction on M . If $M = 2$, then $a = 1$. We show the claim more generally for $a = 1$ and $M \geq 2$ arbitrary. We then have $\{0, a/M\} = \xi(M)$. The claim follows by taking $(c, d) = (M, 1)$ (then $(a, b) = (1, 0)$ and $(u, u_*) = (0, w)$) in Corollary 6.12.

Now assume that $M > 2$ and that the claim holds for smaller M . We can then find integers b and d such that $ad - bM = 1$ and $1 \leq d < M$. Then $0 \leq b < d$. If $d = 1$, then $b = 0$ and therefore $a = 1$; this case was already dealt with above. So we can assume that $d \geq 2$.

Let $1 \leq k < p$ be such that $M \equiv dk \pmod{p}$. Then

$$\begin{pmatrix} a-bk & b \\ M-dk & d \end{pmatrix} \cdot \left\{0, \frac{1}{k}\right\} = \left\{\frac{b}{d}, \frac{a}{M}\right\}.$$

The matrix is in $\Gamma_0(p)$, so $\{b/d, a/M\} = \xi(k)$, and hence

$$(T'_n - n)\mathbf{e} \bullet \left\{0, \frac{a}{M}\right\} = (T'_n - n)\mathbf{e} \bullet \left\{0, \frac{b}{d}\right\} + (T'_n - n)\mathbf{e} \bullet \xi(k).$$

We use the induction hypothesis for the first term in the sum and Corollary 6.12 for the second term, where we take $(a, b, c, d) \leftarrow (a, b, M, d)$. Then

$$bpu = bdk - bc \equiv 1 \pmod{d},$$

so u corresponds to w in the induction hypothesis, and $u_* = w$. This gives

$$\begin{aligned} (T'_n - n)\mathbf{e} \bullet \left\{0, \frac{a}{M}\right\} &= \left(\left\lfloor \frac{nb}{d} \right\rfloor - \left\lfloor \frac{nu}{d} \right\rfloor\right) + \left(\left\lfloor \frac{nu}{d} \right\rfloor - \left\lfloor \frac{nb}{d} \right\rfloor + \left\lfloor \frac{na}{M} \right\rfloor - \left\lfloor \frac{nw}{M} \right\rfloor\right) \\ &= \left\lfloor \frac{na}{M} \right\rfloor - \left\lfloor \frac{nw}{M} \right\rfloor. \end{aligned} \quad \square$$

Proof of Lemma 6.7. Using that $L_n = T'_{2n} - 2T'_n = (T'_{2n} - 2n) - 2(T'_n - n)$, Corollary 6.13 gives (note that w does not depend on n)

$$L_n \mathbf{e} \bullet \left\{0, \frac{a}{M}\right\} = \left\lfloor \frac{2na}{M} \right\rfloor - \left\lfloor \frac{2nw}{M} \right\rfloor - 2\left\lfloor \frac{na}{M} \right\rfloor + 2\left\lfloor \frac{nw}{M} \right\rfloor = \varepsilon_M(na) - \varepsilon_M(nw),$$

and we can replace w with u/a , where u is as in Lemma 6.7. □

7. A criterion for ruling out moderately large primes

To exclude some of the larger primes for $d = 7$, we make use of the following criterion, which is due to the first author of this paper.

Proposition 7.1 (Derickx). *Let $d \geq 1$ and let p be a prime. We assume that either*

- (i) $J_1(p)(\mathbb{Q})$ is finite, or
- (ii) there is $a \in (\mathbb{Z}/p\mathbb{Z})^\times / \{\pm 1\}$ such that $\text{ord}(a) > 3d$ and $A = (\langle a \rangle - 1)(J_1(p)(\mathbb{Q}))$ is finite.

In case (ii), we say that “(*) holds” when $\#A$ is odd or, more generally, the 2-primary part of A is contained in the subgroup of $J_1(p)(\mathbb{Q})$ generated by differences of rational cusps. We then set $n = 3$ in case (i) and

$$n = \begin{cases} 5 & \text{if (*) holds and } a \in \{2, 2^{-1}\}, \\ 6 & \text{if (*) holds and } a \notin \{2, 2^{-1}\}, \\ 7 & \text{if (*) does not hold and } a \in \{3, 3^{-1}\}, \\ 8 & \text{if (*) does not hold and } a \notin \{3, 3^{-1}\} \end{cases}$$

in case (ii). Then $nd < \text{gon}_{\mathbb{Q}}(X_1(p))$ implies that $p \notin S(d)$. This holds in particular when

$$d < \frac{325}{2^{16}} \frac{p^2 - 1}{n}.$$

Proof. If $c \in X_1(p)$ is a rational cusp, which we consider as an effective divisor of degree 1, and q is any prime, then $(T_q - \langle q \rangle - q)(c) = 0$. This can be deduced from the modular interpretation of the cusps. (See also [Parent 2000, end of Section 2.4] and note that the rational cusps are those mapping to the cusp ∞ on $X_0(p)$.)

We first consider case (i). Then, by Corollary 3.3, $J_1(p)(\mathbb{Q})$ is generated by differences of rational cusps. By the preceding paragraph, $T_q - \langle q \rangle - q$ kills $J_1(p)(\mathbb{Q})$ for all primes q (including $q = 2$; this improves Proposition 2.3 in this case). In case (ii), $T_q - \langle q \rangle - q$ kills the 2-primary part of A when this is contained in the subgroup generated by differences of rational cusps and kills the odd part of A by Proposition 2.3. So when (*) holds, $T_q - \langle q \rangle - q$ kills A for arbitrary primes q . When (*) does not hold, the statement is true for $q \geq 3$.

We let $x \in X_1(p)^{(d)}(\mathbb{Q})$, considered as an effective divisor of degree d on $X_1(p)$, and fix a rational cusp $c \in X_1(p)$. Then the linear equivalence class $[x - d \cdot c]$ of the divisor $x - d \cdot c$ is a rational point on $J_1(p)$.

Going back to the case (i), set $t = T_2 - \langle 2 \rangle - 2$. Then

$$t(x - d \cdot c) = t(x) - dt(c) = t(x)$$

is a principal divisor, since $t([x - d \cdot c]) = 0$. This implies that the divisors $T_2(x)$ and $\langle 2 \rangle(x) + 2x$ of degree $3d = nd$ are linearly equivalent. But $\text{gon}_{\mathbb{Q}}(X_1(p)) > nd$ by assumption, so the divisors must in fact be equal, and $t(x) = 0$. Now Proposition 2.4 shows that x is a sum of cusps. This implies $p \notin S(d)$.

In case (ii), we set $q = 2$ when (*) holds and otherwise $q = 3$, so that $T_q - \langle q \rangle - q$ kills A . Then $t(J_1(p)(\mathbb{Q})) = \{0\}$, where

$$t = (\langle a \rangle - 1)(T_q - \langle q \rangle - q) = (\langle a \rangle T_q + \langle q \rangle + q) - (T_q + \langle qa \rangle + q \langle a \rangle). \tag{7-1}$$

If $qa = 1$, this simplifies to

$$t = (\langle a \rangle T_q + \langle q \rangle + (q - 1)) - (T_q + q \langle a \rangle), \quad (7-2)$$

and if $a = q$, we obtain

$$t = (\langle a \rangle T_q + q) - (T_q + \langle qa \rangle + (q - 1) \langle a \rangle). \quad (7-3)$$

We write t_1 for the first term and t_2 for the second in the difference (7-1), (7-2) or (7-3). Since the diamond operators are automorphisms of $X_1(p)$ and T_q multiplies degrees by $q + 1$, we see that applying t_1 or t_2 , considered as a correspondence on $X_1(p)$, to an effective divisor of degree d results in an effective divisor of degree nd .

As before, $t(x - d \cdot c) = t(x) - dt(c) = t(x)$ is a principal divisor, and from $\text{gon}_{\mathbb{Q}}(X_1(p)) > nd$, we conclude that

$$t(x) = (T_q - \langle q \rangle - q)(\langle a \rangle - 1)(x) = 0.$$

By Proposition 2.4 again, this implies that $\langle a \rangle(x) - x$ is supported on cusps. Since the diamond operators permute the cusps among themselves, this then implies that $x = x_0 + x_1$, where x_0 is supported in cusps and x_1 does not have cusps in its support and satisfies $\langle a \rangle(x_1) = x_1$. Now the diamond operators act freely on the noncuspidal points of $X_1(p)$ with the exception of points corresponding to elliptic curves with j -invariant 0 or 1728, which can have stabilizers of orders 3 and 2, respectively. The condition $\langle a \rangle(x_1) = x_1$ implies that x_1 is a sum of (sums over) orbits of $\langle a \rangle$, which have length at least $\text{ord}(a)/3$. Since $\text{ord}(a) > 3d$ by assumption, this forces $x_1 = 0$, and we conclude that x is supported in cusps. This again implies that $p \notin S(d)$.

For the last statement, note that

$$\text{gon}_{\mathbb{Q}}(X_1(p)) \geq \text{gon}_{\mathbb{C}}(X_1(p)) \geq \frac{1}{48} \lambda_1(p^2 - 1)$$

by [Abramovich 1996] (using that $\Gamma_1(p)$ has index $(p^2 - 1)/2$ in $\text{PSL}(2, \mathbb{Z})$), where λ_1 is the smallest positive eigenvalue of the Laplace operator on $X_1(p)(\mathbb{C})$, which satisfies $\lambda_1 \geq \frac{975}{4096}$ by [Kim 2003]. \square

Remark. Without the condition $\text{ord}(a) > 3d$ in the case that $J_1(p)(\mathbb{Q})$ has positive rank, the proof shows that any rational point on $X_1(p)^{(d)}$ whose support consists of noncuspidal points must be a sum of orbits of $\langle a \rangle$. This is impossible when d cannot be written as a sum of the possible orbit lengths ($\text{ord}(a)$, together with $\text{ord}(a)/2$ when $\text{ord}(a)$ is even and $\text{ord}(a)/3$ when $\text{ord}(a)$ is divisible by 3). But even when d can be written in this way, this gives strong restrictions. For example, when $\text{ord}(a) = d$ and d is coprime to 6, then such a point must be obtained by pulling back a rational point on X_H , where H is generated by a .

We plan to explore this further in a follow-up paper.

Corollary 7.2.

$$p \notin S(7) \quad \text{for } p \in \{71, 113, 127\}.$$

Proof. We check that for the two primes $p \in \{113, 127\}$, the positive-rank simple factors of $J_1(p)$ already occur in $J_0(p)$. We can thus take any $a \in (\mathbb{Z}/p\mathbb{Z})^{\times}/\{\pm 1\}$; we use $a = 3$, which generates $(\mathbb{Z}/p\mathbb{Z})^{\times}/\{\pm 1\}$

in both cases. In particular, $\text{ord}(a) = (p - 1)/2 > 3 \cdot 7$. We then have $n = 7$ in Proposition 7.1. Since

$$\frac{325}{2^{16}} \frac{p^2 - 1}{7} > 9,$$

all assumptions in Proposition 7.1 are satisfied.

To deal with $p = 71$, we recall that by Proposition 3.1, 71 is a rank-zero prime, so we can apply Proposition 7.1 with $n = 3$. Since

$$\frac{325}{2^{16}} \frac{71^2 - 1}{3} > 8,$$

the claim follows also in this case. \square

Remark. For $p = 73$, the best we can do is use $a = 2$ and $n = 5$ in Proposition 7.1 (by [Conrad et al. 2003, Section 6.2], the torsion subgroup of $J_1(73)(\mathbb{Q})$ is generated by differences of rational cusps). However, the gonality lower bound works only for $d \leq 5$. We would need $\text{gon}_{\mathbb{Q}}(X_1(73)) > 35$. From Table 1 in [Derickx and van Hoeij 2014], it appears that this is very likely the case, but it is also very likely hard to prove. (Note that $\text{ord}(a) = 9 \leq 3d$, but the argument would still work; see the remark following Proposition 7.1.)

8. Verification of assumption (b) of Lemma 1.7

We now discuss assumption (b) of Lemma 1.7 for the remaining pairs of degrees d and primes p . Recall that the assumption is always satisfied (with $\ell = 2$) when $p > (2^{d/2} + 1)^2$; see Lemma 1.9. The following table tells us which primes we still have to consider for each d .

d	3	4	5	6	7
$\lfloor (2^{d/2} + 1)^2 \rfloor$	14	25	44	81	151

In some cases, we can show that all points in $X_1(p)^{(d)}(\mathbb{F}_2)$ are sums of images of rational cusps, even when p is below this bound. The result of [Waterhouse 1969, Theorem 4.1] tells us precisely what the possible orders of $E(\mathbb{F}_{2^d})$ are for elliptic curves E defined over \mathbb{F}_{2^d} . Using this (or a brute-force enumeration of all such curves up to isomorphism), we obtain the following extension of Lemma 1.9.

Lemma 8.1. *The set $X_1(p)^{(d)}(\mathbb{F}_2)$ consists of sums of images of rational cusps for the following pairs of an integer $3 \leq d \leq 7$ and a prime p :*

$$\begin{aligned} d = 3 & \quad \text{and} \quad p = 11 \quad \text{or} \quad p \geq 17, \\ d = 4 & \quad \text{and} \quad p \geq 19, \\ d = 5 & \quad \text{and} \quad p \geq 23 \quad \text{and} \quad p \notin \{31, 41\}, \\ d = 6 & \quad \text{and} \quad p = 23 \quad \text{or} \quad (p \geq 43 \quad \text{and} \quad p \neq 73), \\ d = 7 & \quad \text{and} \quad p \in \{47, 53\} \quad \text{or} \quad (p \geq 79 \quad \text{and} \quad p \notin \{113, 127\}). \end{aligned}$$

Proof. According to [Waterhouse 1969, Theorem 4.1], $\#E(\mathbb{F}_{2^d})$ can take all even values in the Hasse interval $[\lceil(2^{d/2} - 1)^2\rceil, \lfloor(2^{d/2} + 1)^2\rfloor]$ and, in addition, the values

$$\begin{aligned} 2^d + m2^{d/2} + 1 & \text{ for } m \in \{-2, -1, 0, 1, 2\} & \text{if } d \text{ is even;} \\ 2^d + m2^{(d+1)/2} + 1 & \text{ for } m \in \{-1, 0, 1\} & \text{if } d \text{ is odd.} \end{aligned}$$

This allows us to determine the set of primes p such that there are no noncuspidal points of degree $\leq d$ on $X_1(p)_{\mathbb{F}_2}$. The condition that there are no cusps of degree $\leq d$ that are not images of rational cusps excludes in addition $p = 31$ for $d \geq 5$ and $p = 127$ for $d \geq 7$. \square

We note that for the primes not in the list above for a given d , there are indeed points \bar{x} as in assumption (b). If we want to show that $p \notin S(d)$ for one of these primes, we have to do some work to show that there are no rational points in the corresponding residue classes. For $p \in \{29, 31, 41\}$ and $d \geq 5$, we already did this in Lemma 3.7. Taking into account Corollary 7.2, this leaves the primes $p \in \{37, 43, 59, 61, 67\}$ for $d = 7$ and $p = 73$ for $d = 6, 7$.

We can deal with $(d, p) \in \{(6, 73), (7, 43)\}$ in the following way.

Lemma 8.2. *Let $d \geq 1$ be an integer and let p be a prime. Let $\bar{x} \in X_1(p)^{(d)}(\mathbb{F}_2)$ be a point that is not a sum of images of rational cusps. Let $H \subseteq (\mathbb{Z}/p\mathbb{Z})^\times / \{\pm 1\}$ be a subgroup and denote the image of \bar{x} in $X_H^{(d)}(\mathbb{F}_2)$ by \bar{x}_H . Assume that the following conditions are satisfied:*

- (1) *There is $t : J_{H, \mathbb{Z}_{(2)}} \rightarrow A_{\mathbb{Z}_{(2)}}$ such that $t(J_H(\mathbb{Q}))$ is finite of odd order and $t \circ \iota$ (with $\iota : X_H^{(d)} \rightarrow J_H$) is a formal immersion at \bar{x}_H .*
- (2) *There is a rational point $x_H \in X_H^{(d)}(\mathbb{Q})$ such that $\text{red}_2(x_H) = \bar{x}_H$.*

Let $x \in X_1(p)^{(d)}(\mathbb{Q})$ be such that $\text{red}_2(x) = \bar{x}$. Then x maps to x_H under the canonical map $X_1(p)^{(d)} \rightarrow X_H^{(d)}$.

Proof. Let x'_H be the image of x in $X_H^{(d)}(\mathbb{Q})$; then $\text{red}_2(x'_H) = \bar{x}_H = \text{red}_2(x_H)$. Since $t(J_H(\mathbb{Q}))$ is finite of odd order, this implies that $t(\iota(x'_H) - \iota(x_H)) = 0$. Since $t \circ \iota$ is a formal immersion at \bar{x}_H , it follows that $x'_H = x_H$. \square

If, in the situation of Lemma 8.2, x_H does not lift to a rational point on $X_1(p)^{(d)}$, then it follows that no rational point on $X_1(p)^{(d)}$ can reduce mod 2 to \bar{x} . We have to carry this out for all \bar{x} as in assumption (b). To do this, we formulate a criterion that allows us to verify the formal immersion condition in Lemma 8.2 also for points whose support does not consist of cusps.

Lemma 8.3. *Fix a prime ℓ and an integer $d \geq 1$. Let X be a curve over \mathbb{Q} with good reduction at ℓ , with Jacobian variety J . Fix $b \in X(\mathbb{Q})$ and use it to define embeddings $\iota : X \rightarrow J$ and $\iota_d : X^{(d)} \rightarrow J$. Let A be another abelian variety (with good reduction at ℓ) such that there is a homomorphism $t : J \rightarrow A$. Let $L \subseteq H^0(X_{\mathbb{F}_\ell}, \Omega^1)$ be the pullback of $H^0(A_{\mathbb{F}_\ell}, \Omega^1)$ under $t \circ \iota$, and let $\varphi : X_{\mathbb{F}_\ell} \rightarrow \mathbb{P} \text{Tan}_0(A_{\mathbb{F}_\ell}) \cong \mathbb{P}_{\mathbb{F}_\ell}^{\dim A - 1}$ be the morphism determined by the linear system corresponding to L . Let $\bar{x} \in X^{(d)}(\mathbb{F}_\ell)$ be a point that is the sum of d distinct geometric points $\bar{x}_1, \dots, \bar{x}_d \in X(\mathbb{F}_\ell)$. Assume that*

- (i) the differentials in L do not vanish simultaneously at any point \bar{x}_j , and that
- (ii) the points $\varphi(\bar{x}_1), \dots, \varphi(\bar{x}_d) \in \mathbb{P}^{\dim A - 1}(\bar{\mathbb{F}}_\ell)$ span a linear subspace of dimension $d - 1$.

Then $t \circ \iota_d$ is a formal immersion at \bar{x} .

Proof. To show that $t \circ \iota_d$ is a formal immersion, it is sufficient to show that the induced map on tangent spaces $\text{Tan}_{\bar{x}}(X_{\bar{\mathbb{F}}_\ell}^{(d)}) \rightarrow \text{Tan}_{t(\iota(\bar{x}))}(A_{\bar{\mathbb{F}}_\ell})$ is injective; see [Parent 1999, Theorem 4.18]. We can equivalently consider this condition over $\bar{\mathbb{F}}_\ell$.

Since the regular 1-forms on A are invariant under translation, we have a canonical identification of all tangent spaces $\text{Tan}_{\bar{a}}(A_{\bar{\mathbb{F}}_\ell})$ with the tangent space at the origin, whose projectivization is the codomain of φ . Since the differentials in L do not vanish simultaneously at \bar{x}_j , the map φ sends a point $\bar{x}_j \in X(\bar{\mathbb{F}}_\ell)$ to the image in $\mathbb{P} \text{Tan}_0(A_{\bar{\mathbb{F}}_\ell})$ of the tangent space $\text{Tan}_{\bar{x}_j}(X_{\bar{\mathbb{F}}_\ell})$ under $(t \circ \iota)_*$ followed by a suitable translation.

Since the geometric points making up \bar{x} are distinct, we have a canonical isomorphism

$$\text{Tan}_{\bar{x}}(X_{\bar{\mathbb{F}}_\ell}^{(d)}) \cong \bigoplus_{j=1}^d \text{Tan}_{\bar{x}_j}(X_{\bar{\mathbb{F}}_\ell}).$$

The image of $\text{Tan}_{\bar{x}}(X_{\bar{\mathbb{F}}_\ell}^{(d)})$ in $\mathbb{P} \text{Tan}_0(A_{\bar{\mathbb{F}}_\ell})$ under $(t \circ \iota_d)$ followed by a suitable translation is then the linear span of the various images $\varphi(\bar{x}_j)$; the map on tangent spaces is injective if and only if this span has the maximal possible dimension $d - 1$. \square

We will apply this as follows. We use the q -expansions mod 2 of the cusp forms associated to X_H to determine equations for the canonical model of X_{H, \mathbb{F}_2} . We then project away from the subspace where the forms in L vanish (in practice, we compute the image of φ in a similar way and then set up the projection) and check that none of the points \bar{x}_j lie in this subspace. This verifies the nonvanishing condition (i). We then check condition (ii).

Lemma 8.4. *Let $x \in X_1(73)^{(6)}(\mathbb{Q})$. Then $\text{red}_2(x) \in X_1(73)^{(6)}(\mathbb{F}_2)$ is a sum of images of rational cusps.*

Proof. There are, up to isomorphism, exactly two elliptic curves over \mathbb{F}_{2^6} with a point of order 73. They have zero j -invariant (they must be supersingular according to [Waterhouse 1969]) and automorphism group $\mathbb{Z}/6\mathbb{Z}$, so each of them gives rise to $(73 - 1)/6 = 12$ \mathbb{F}_{2^6} -points on $X_1(73)_{\mathbb{F}_2}$. These 24 points split into four orbits of size six under the action of Frobenius (each orbit contains three points coming from each of the two curves), so we obtain exactly four noncuspidal points in $X_1(73)^{(6)}(\mathbb{F}_2)$. There are no cuspidal points that are not sums of images of rational cusps, since the other cusps on $X_1(73)_{\mathbb{F}_2}$ are minimally defined over \mathbb{F}_{2^9} . So we just have to exclude these four noncuspidal points.

Let H be the subgroup of $(\mathbb{Z}/73\mathbb{Z})^\times / \{\pm 1\}$ of index 9. The canonical map $X_1(73) \rightarrow X_H$ is of degree 4 and unramified at all 24 points mentioned above. This implies that they have six distinct images on X_H ; one can check that these points form one Frobenius orbit, so we get one point $\bar{x}_H \in X_H^{(6)}(\mathbb{F}_2)$ that we have to deal with. The Jacobian J_H splits into a copy of $J_{H'}$, where $H \subseteq H'$ has index 3, and a simple 30-dimensional abelian variety A . One can check that A is a factor of the winding quotient and that all isogenous (over \mathbb{Q}) abelian varieties have torsion subgroup of odd order (by computing orders of $A(\mathbb{F}_q)$ for suitable primes q via the Hecke eigenvalues). We take $t = \langle 7 \rangle - 1$; this kills $J_{H'}$ and projects J_H

into A . Since the nonzero eigenvalues of t are invertible mod 2 (they are of the form $\omega - 1$ with $\omega \in \mu_3$), we can work with the q -expansions mod 2 of a basis of the space of cusp forms associated to A . We check, as described above, that $t \circ \iota_6$ is a formal immersion at \bar{x}_H . (In practice, we check this for all Frobenius orbits of length 6 in $X_H(\bar{\mathbb{F}}_2)$, since it is not so easy to determine which point is in the support of \bar{x}_H .)

Note that $X_H \rightarrow X_{H'} \rightarrow X_0(73)$ is the composition of two maps of degree 3, the second of which is étale (by Riemann–Hurwitz: $X_{H'}$ is of genus 13 and $X_0(73)$ has genus 5). Let E_0 be an elliptic curve over \mathbb{Q} with complex multiplication by cube roots of unity. Then E_0 has two Galois-conjugate cyclic subgroups of order 73, with each subgroup defined over $K = \mathbb{Q}(\sqrt{-3})$ (note that 73 splits in K), so E_0 gives rise to a pair of Galois-conjugate points $y_1, y_2 \in X_0(73)(K)$. The preimages of these two points on $X_{H'}$ give six geometric points that are Galois conjugate; the map $X_H \rightarrow X_{H'}$ is totally ramified at each of them, so we find a Galois orbit of size 6 of points in $X_H(\bar{\mathbb{Q}})$, giving rise to a rational point $x_H \in X_H^{(6)}(\mathbb{Q})$. This point reduces mod 2 to \bar{x}_H (as one can show by writing down an explicit twist of $E_{0,K}$ for a certain number field of degree 24 that has a K -rational point of order 73 and checking that the 24 geometric points corresponding to its Galois conjugates reduce to the 24 noncuspidal points in $X_1(73)(\mathbb{F}_{2^6})$ mentioned above), but does not lift to a rational point on $X_1(73)^{(6)}$, since there are no CM elliptic curves with a 73-torsion point over number fields of degree < 24 ; see [Clark et al. 2013, Table 1]. By Lemma 8.2 and the discussion following it, this finishes the proof. \square

Lemma 8.5. *Let $x \in X_1(43)^{(7)}(\mathbb{Q})$. Then $\text{red}_2(x) \in X_1(43)^{(7)}(\mathbb{F}_2)$ is a sum of images of rational cusps.*

Proof. There is, up to isomorphism, exactly one elliptic curve over \mathbb{F}_{2^7} with a point of order 43. It is supersingular; its automorphism group over \mathbb{F}_{2^7} has order 2, since \mathbb{F}_{2^7} does not contain primitive cube roots of unity. It therefore gives rise to 21 noncuspidal points in $X_1(43)(\mathbb{F}_{2^7})$, making up three Galois orbits. The nonrational cusps are also defined over \mathbb{F}_{2^7} . We obtain six points in total in $X_1(43)^{(7)}(\mathbb{F}_2)$ that are not supported in rational cusps. Take H to be the subgroup of index 7. Then the six points above map to two points in $X_H^{(7)}(\mathbb{F}_2)$. For A , we use the winding quotient of J_H ; one can show that each \mathbb{Q} -isogenous abelian variety has odd torsion order. We show as before that $t \circ \iota$ is a formal immersion at the two points in question.

On the other hand, there is a point in $X_H^{(7)}(\mathbb{Q})$ that corresponds to the pullback of the cusp 0 on $X_0(43)$ (note that $X_H \rightarrow X_0(43)$ has degree 7). It does not lift to a rational point on $X_1(43)^{(7)}$, since the nonrational cusps on $X_1(43)$ are points of degree 21. This shows that there are no rational points on $X_1(43)^{(7)}$ whose reduction is cuspidal, but that are not supported in rational cusps.

Consider now the rational point on $X_0(43)$ that corresponds to elliptic curves over \mathbb{Q} with CM by the order of discriminant -43 . Its pullback to X_H again provides us with a rational point on $X_H^{(7)}$, whose reduction must be the other point we have to consider, since such curves have (potentially) good reduction at 2. Again, this point does not lift to a rational point on $X_1(43)^{(7)}$, as can be verified by consulting [Clark et al. 2013, Table 1]. This shows that there are no rational points on $X_1(43)^{(7)}$ whose reduction is noncuspidal. \square

We still have to show that $p \notin S(7)$ for

$$p = 37, 59, 61, 67, 73.$$

We use the following simple observation by the first author of this paper, together with the fact that it is actually possible to check this criterion by a computation.

Lemma 8.6 (Derickx). *Let $d \geq 1$ be an integer and let $p > 2$ be a prime. Assume that $t \in \mathbb{T}$ has the property that $t(J_1(p)(\mathbb{Q})) = \{0\}$, where we consider t as an endomorphism of $J_1(p)$. Let $\bar{x}_0, \bar{x} \in X_1(p)^{(d)}(\mathbb{F}_2)$ be such that \bar{x}_0 is a sum of images of rational cusps. If the divisor $t(\bar{x} - \bar{x}_0)$ on $X_1(p)_{\mathbb{F}_2}$ is not principal (where we now consider t as a correspondence on $X_1(p)_{\mathbb{F}_2}$), then there is no rational point on $X_1(p)^{(d)}$ whose reduction mod 2 is \bar{x} .*

Remark. This result remains valid with an odd positive integer N in place of p . (We need N to be odd so that $X_1(N)$ has good reduction mod 2.)

Proof. Let $x_0 \in X_1(p)^{(d)}(\mathbb{Q})$ be the sum of rational cusps such that $\text{red}_2(x_0) = \bar{x}_0$ and assume that there is some $x \in X_1(p)^{(d)}(\mathbb{Q})$ such that $\text{red}_2(x) = \bar{x}$. Then the divisor $x - x_0$ represents a point in $J_1(p)(\mathbb{Q})$; it follows that $t(x - x_0)$ represents zero and is therefore principal. Applying reduction mod 2 shows that $t(\bar{x} - \bar{x}_0)$ must be principal as well. \square

We can find a suitable Hecke operator t by multiplying an operator that projects $J_1(p)$ into an abelian subvariety of Mordell–Weil rank zero (this is equivalent to this operator factoring through the winding quotient) with an operator that kills rational torsion. For the computations, we will use a model of $X_1(p)$ that is derived directly from the usual modular interpretation, i.e., noncuspidal points on $X_1(p)$ correspond to pairs (E, P) , where E is an elliptic curve and $P \in E$ is a point of exact order p . The effect of a Hecke operator T_n with $p \nmid 2n$ as a correspondence on $X_1(p)_{\mathbb{F}_2}$ in this interpretation is then given by mapping (E, P) to the sum of the pairs $(E', \phi(P))$, where $\phi : E \rightarrow E'$ runs through the cyclic isogenies of degree n . This switch from the “natural” modular interpretation given in Section 2 has the effect that we have to conjugate everything by the Atkin–Lehner involution. Concretely, this means that instead of $T_q - \langle q \rangle - q$ as stated in Proposition 2.3, we have to use $T_q - q \langle q \rangle - 1$ with any odd prime q to kill the rational torsion. We will work with $q = 3$.

For the projection part of t , we will use an operator of the form $\langle a \rangle - 1$, so we take

$$t = (\langle a \rangle - 1)(T_3 - 3\langle 3 \rangle - 1).$$

(This is similar to the idea used in Proposition 7.1.) We use the modular interpretation of the points on $X_1(p)$ to find the image of the divisor $\bar{x} - \bar{x}_0$ under t . Sutherland has computed planar equations for $X_1(N)$ for all $N = p$ in the relevant range, together with explicit expressions relating the coordinates in these equations to the parameters b and c in the Tate form

$$E_{b,c}: y^2 + (1 - c)xy - by = x^3 - bx^2$$

of the associated elliptic curve with point $(0, 0)$ of order N . See [Sutherland 2012]; the equations are available https://math.mit.edu/~drew/X1_altcurves.html.

We find the action of a diamond operator $\langle a \rangle$ on a point on $X_1(p)$ by multiplying the point $P = (0, 0)$ on the associated curve $E_{b,c}$ by a and then bringing the pair $(E_{b,c}, aP)$ into Tate form $(E_{b',c'}, (0, 0))$. To

get the effect of the Hecke operator T_3 , we use the description of T_n given above, i.e., we find the four elliptic curves that are 3-isogenous to $E_{b,c}$ (they may be defined over an extension of the base field we are considering) and find the points corresponding to the isogenous curves together with the image of P . The sum of these four points is then the image of the original point (considered as a divisor of degree 1) under T_3 .

Lemma 8.7. *Let $p \in \{59, 61, 67, 73\}$ and $x \in X_1(p)^{(7)}(\mathbb{Q})$. Then $\text{red}_2(x) \in X_1(p)^{(7)}(\mathbb{F}_2)$ is a sum of images of rational cusps.*

Proof. We determine a suitable a for each of the primes p such that $\langle a \rangle - 1$ projects $J_1(p)$ into an abelian subvariety of rank zero. For $p \in \{59, 67, 73\}$, the only simple components of $J_1(p)$ that have positive rank are also components of $J_0(p)$, so we can take a to be any element of $(\mathbb{Z}/p\mathbb{Z})^\times / \{\pm 1\}$. For $p = 61$, there is a component of positive rank in J_H for the subgroup H of index 6 that does not occur in $J_0(p)$, and all components of positive rank occur in J_H , so we take $a = 3 \equiv 2^6 \pmod{61}$, where 2 is a primitive root mod 61. We note that $\langle a \rangle - 1$ maps x_0 to a degree-zero divisor representing a torsion point in $J_1(p)(\mathbb{Q})$, so we just have to compute $t(\bar{x})$ and check whether this divisor is principal, where \bar{x} and x_0 are as in Lemma 8.6.

We then find all the noncuspidal places of degree at most 7 on $X_1(p)_{\mathbb{F}_2}$. For the computation, it is sufficient to consider one representative in each orbit under the diamond operators. For $p < 73$, we find no such places of degree ≤ 6 and either one (for $p = 61, 67$) or two (for $p = 59$) orbits of places of degree 7. For $p = 73$, there are two orbits of places of degree 6 and one orbit of places of degree 7.

For the representatives \bar{x} of orbits of places of degree 7 (which we identify with effective divisors of degree 7), we compute the divisor $t(\bar{x})$ and verify that it is not principal. This can be done by computing the Riemann–Roch space associated to the divisor; a divisor of degree zero is principal if and only if its Riemann–Roch space is nontrivial. (Magma has a built-in function for testing whether a divisor is principal.)

The places of degree 6 on $X_1(73)_{\mathbb{F}_2}$ give rise to effective divisors of degree 7 by adding one of the images of the rational cusps (which are exactly the \mathbb{F}_2 -points on $X_1(73)$). Applying t to such a sum differs from the result of applying t to the degree 6 divisor coming from the place by a principal divisor, since the rational cusps map to principal divisors. So we only have to check that $t(\bar{x})$ is nonprincipal for the two representatives of orbits of places of degree 6. (We note that this also gives an alternative proof of Lemma 8.4.)

Finally, we note that all other points in $X_1(p)^{(7)}(\mathbb{F}_2)$ are supported in images of rational cusps, since the other cusps give rise to points of degree at least 9 over \mathbb{F}_2 .

The computations took less than one hour each for $p = 59$ and 61, about three hours for $p = 67$ and about seven hours for $p = 73$. □

Remark. We can use this approach also to show that there are no noncuspidal points in $X_1(43)^{(7)}(\mathbb{F}_2)$ that arise as the reduction modulo 2 of a rational point. We would still have to deal with the points arising from Frobenius orbits of cusps that are not images of rational cusps, however; see the proof of Lemma 8.5.

Now Proposition 1.10 follows from Lemmas 3.7, 8.1, 8.4, 8.5, and 8.7 and Corollary 7.2.

Finally, we deal with $p = 37$.

Lemma 8.8. *Modulo the action of Frobenius and the diamond operators, there is exactly one point of degree 6 on $X_1(37)_{\mathbb{F}_2}$ such that the corresponding point $\bar{x} \in X_1(37)^{(6)}(\mathbb{F}_2)$ is the reduction mod 2 of a rational point $x \in X_1(37)^{(6)}(\mathbb{Q})$, and this point x is uniquely determined by \bar{x} .*

Proof. We proceed as in the proof of Lemma 8.7. The only positive-rank factor of $J_1(37)$ occurs in $J_0(37)$ (it is the “first” elliptic curve of rank 1), so we can take any a for the criterion of Lemma 8.6. The computation shows that of the two diamond orbits of places of degree 6, only one satisfies the criterion in Lemma 8.6. (It should be noted that this can be used to verify that we are correct in working with the Hecke operator $T_3 - 3\langle 3 \rangle - 1$: none of the two places satisfies the criterion when using $T_3 - \langle 3 \rangle - 3$ instead, but one of them has to, since there are noncuspidal rational points on $X_1(37)^{(6)}$.)

We know that there is a diamond orbit of rational points that has to reduce to our unique diamond orbit that lifts. To show that the lift is unique, we use Lemma 8.3. The Hecke operator T_{17} projects $J_1(37)$ into an abelian subvariety of rank zero. Its eigenvalues are invertible mod 2 on newforms corresponding to a subvariety of dimension 36, which has odd-order rational torsion subgroup. We then verify the formal immersion criterion (for all points of degree 6, since we work with a different model here and did not try to find an explicit birational map between the two models). \square

Proof of Proposition 1.4. Let $x \in X_1(37)^{(6)}(\mathbb{Q})$ be a point whose support contains no cusps. Since (a) holds for $(d, p) = (6, 37)$ by Proposition 1.8 and there are no noncuspidal points on $X_1(37)_{\mathbb{F}_2}$ of degree ≤ 5 , it follows that $\bar{x} = \text{red}_2(x) \in X_1(37)^{(6)}(\mathbb{F}_2)$ is also a point whose support contains no cusps. By Lemma 8.8, \bar{x} is uniquely determined up to the action of the diamond operators, and there is no other point than x that reduces mod 2 to \bar{x} . On the other hand, we know a point x' with this property; this is a point coming from the curve $E_{6,37}$ with some choice of point of order 37 (they are all in the same diamond orbit). It follows that $x = x'$, which implies the claim. \square

We finish off the determination of $S(7)$ by excluding $p = 37$.

Lemma 8.9. $37 \notin S(7)$.

Proof. As in the proof of Lemma 8.8, we show that there is no point of degree 7 on $X_1(37)_{\mathbb{F}_2}$ such that the corresponding point in $X_1(37)^{(7)}(\mathbb{F}_2)$ is the reduction of a rational point. Now assume that $x \in X_1(37)^{(7)}(\mathbb{Q})$ and consider $\bar{x} = \text{red}_2(x)$. By the preceding statement, the support of \bar{x} must contain a cusp, and the noncuspidal part of \bar{x} must satisfy the criterion of Lemma 8.6. By Lemma 8.8 and its proof, the noncuspidal part is then either empty or in the unique diamond orbit coming from noncuspidal rational points on $X_1(37)^{(6)}$. In the first case, x must be a sum of rational cusps, since assumption (a) holds. To deal with the second case, we verify the formal immersion criterion as in the proof of Lemma 8.8, but now for all sums of an \mathbb{F}_2 -rational cusp and a prime divisor of degree 6. This shows that the criterion is satisfied; therefore the point x is unique in its residue class mod 2. On the other hand, there is a known point in this residue class, which comes from adding the rational cusp that lifts the unique cusp in the support of \bar{x} to the degree 6 divisor lifting the remaining part (this is one of the

sporadic points in $X_1(37)^{(6)}(\mathbb{Q})$. It follows that x is this point; in particular, x has a cusp in its support. So we conclude that every rational point on $X_1(37)^{(7)}$ has a cusp in its support; this is equivalent to the statement that $37 \notin S(7)$. \square

Acknowledgments

We would like to thank Bas Edixhoven, Barry Mazur, and Loïc Merel for their many valuable comments and suggestions, Pierre Parent for his idea to look at CM elliptic curves for the proof of $73 \notin S(6)$ (Lemma 8.4), Filip Najman for some helpful information on sporadic torsion points, and Tessa Schild for her proofreading of an earlier version of this paper. We thank Joseph Oesterlé for kindly allowing us to use his notes [1994] and helping the first author understand the proof of the bound (1-1). We also thank the referee of an earlier version of this paper for some valuable feedback.

References

- [Abramovich 1996] D. Abramovich, “A linear lower bound on the gonality of modular curves”, *Int. Math. Res. Not.* **1996**:20 (1996), 1005–1011. MR Zbl
- [Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, “The Magma algebra system, I: The user language”, *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl
- [Clark et al. 2013] P. L. Clark, B. Cook, and J. Stankewicz, “Torsion points on elliptic curves with complex multiplication”, *Int. J. Number Theory* **9**:2 (2013), 447–479. MR Zbl
- [Conrad et al. 2003] B. Conrad, B. Edixhoven, and W. Stein, “ $J_1(p)$ has connected fibers”, *Doc. Math.* **8** (2003), 331–408. MR Zbl
- [Deligne and Rapoport 1973] P. Deligne and M. Rapoport, “Les schémas de modules de courbes elliptiques”, pp. 143–316 in *Modular functions of one variable, II* (Antwerp, Belgium, 1972), edited by P. Deligne and W. Kuyk, Lecture Notes in Math. **349**, Springer, 1973. MR Zbl
- [Derickx 2016] M. Derickx, *Torsion points on elliptic curves over number fields of small degree*, Ph.D. thesis, Universiteit Leiden, 2016, available at <http://hdl.handle.net/1887/43186>.
- [Derickx 2020] M. Derickx, SageMath code for the verification of assumption (a), 2020, available at https://github.com/koffie/mdsage/blob/master/mdsage/kamiennys_criterion.py.
- [Derickx and van Hoeij 2014] M. Derickx and M. van Hoeij, “Gonality of the modular curve $X_1(N)$ ”, *J. Algebra* **417** (2014), 52–71. MR Zbl
- [Derickx et al. 2017] M. Derickx, S. Kamienny, W. Stein, and M. Stoll, “Torsion points on elliptic curves over number fields of small degree”, preprint, 2017. arXiv 1707.00364
- [Diamond and Im 1995] F. Diamond and J. Im, “Modular forms and modular curves”, pp. 39–133 in *Seminar on Fermat’s last theorem* (Toronto, 1993–1994), edited by V. K. Murty, CMS Conf. Proc. **17**, Amer. Math. Soc., Providence, RI, 1995. MR Zbl
- [Drinfeld 1973] V. G. Drinfeld, “Two theorems on modular curves”, *Funktsional. Anal. i Prilozhen.* **7**:2 (1973), 83–84. In Russian; translated in *Funct. Anal. Appl.* **7** (1973), 155–156. MR Zbl
- [Elkies 1998] N. D. Elkies, “Elliptic and modular curves over finite fields and related computational issues”, pp. 21–76 in *Computational perspectives on number theory* (Chicago, 1995), edited by D. A. Buell and J. T. Teitelbaum, AMS/IP Stud. Adv. Math. **7**, Amer. Math. Soc., Providence, RI, 1998. MR Zbl
- [van Hoeij 2012] M. van Hoeij, “Low degree places on the modular curve $X_1(N)$ ”, preprint, 2012. arXiv 1202.4355
- [Jeon et al. 2011a] D. Jeon, C. H. Kim, and Y. Lee, “Families of elliptic curves over cubic number fields with prescribed torsion subgroups”, *Math. Comp.* **80**:273 (2011), 579–591. MR Zbl

- [Jeon et al. 2011b] D. Jeon, C. H. Kim, and Y. Lee, “Families of elliptic curves over quartic number fields with prescribed torsion subgroups”, *Math. Comp.* **80**:276 (2011), 2395–2410. MR Zbl
- [Kamienny 1992a] S. Kamienny, “Torsion points on elliptic curves and q -coefficients of modular forms”, *Invent. Math.* **109**:2 (1992), 221–229. MR Zbl
- [Kamienny 1992b] S. Kamienny, “Torsion points on elliptic curves over fields of higher degree”, *Int. Math. Res. Not.* **1992**:6 (1992), 129–133. MR Zbl
- [Kamienny and Mazur 1995] S. Kamienny and B. Mazur, “Rational torsion of prime order in elliptic curves over number fields”, pp. 81–100 in *Columbia University Number Theory Seminar* (New York, 1992), Astérisque **228**, Soc. Math. France, Paris, 1995. MR Zbl
- [Kato 2004] K. Kato, “ p -adic Hodge theory and values of zeta functions of modular forms”, pp. 117–290 in *Cohomologies p -adiques et applications arithmétiques, III*, edited by P. Berthelot et al., Astérisque **295**, Soc. Math. France, Paris, 2004. MR Zbl
- [Kim 2003] H. H. Kim, “Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2 ”, *J. Amer. Math. Soc.* **16**:1 (2003), 139–183. MR Zbl
- [Kolyvagin and Logachëv 1989] V. A. Kolyvagin and D. Y. Logachëv, “Finiteness of the Shafarevich–Tate group and the group of rational points for some modular abelian varieties”, *Algebra i Analiz* **1**:5 (1989), 171–196. In Russian; translated in *Leningrad Math. J.* **1**:5 (1990), 1229–1253. MR Zbl
- [Manin 1972] J. I. Manin, “Parabolic points and zeta functions of modular curves”, *Izv. Akad. Nauk SSSR Ser. Mat.* **36** (1972), 19–66. In Russian; translated in *Math. USSR-Izv.* **6** (1972), 19–64. MR Zbl
- [Mazur 1977] B. Mazur, “Modular curves and the Eisenstein ideal”, *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33–186. MR Zbl
- [Mazur 1978] B. Mazur, “Rational isogenies of prime degree”, *Invent. Math.* **44**:2 (1978), 129–162. MR Zbl
- [Merel 1996] L. Merel, “Bornes pour la torsion des courbes elliptiques sur les corps de nombres”, *Invent. Math.* **124**:1-3 (1996), 437–449. MR Zbl
- [Oesterlé 1994] J. Oesterlé, “Torsion des courbes elliptiques sur les corps de nombres”, unpublished notes, 1994.
- [Parent 1999] P. Parent, “Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres”, *J. Reine Angew. Math.* **506** (1999), 85–116. MR Zbl
- [Parent 2000] P. Parent, “Torsion des courbes elliptiques sur les corps cubiques”, *Ann. Inst. Fourier (Grenoble)* **50**:3 (2000), 723–749. MR Zbl
- [Parent 2003] P. Parent, “No 17-torsion on elliptic curves over cubic number fields”, *J. Théor. Nombres Bordeaux* **15**:3 (2003), 831–838. MR Zbl
- [Rebolledo 2009] M. Rebolledo, “Merel’s theorem on the boundedness of the torsion of elliptic curves”, pp. 71–82 in *Arithmetic geometry*, edited by H. Darmon et al., Clay Math. Proc. **8**, Amer. Math. Soc., Providence, RI, 2009. MR Zbl
- [SageMath] W. A. Stein et al., “Sage mathematics software”, Version 9.2, available at <http://www.sagemath.org>.
- [Stein 2007] W. Stein, *Modular forms, a computational approach*, Grad. Stud. in Math. **79**, Amer. Math. Soc., Providence, RI, 2007. MR Zbl
- [Stevens 1982] G. Stevens, *Arithmetic on modular curves*, Progr. Math. **20**, Birkhäuser, Boston, 1982. MR Zbl
- [Sutherland 2012] A. V. Sutherland, “Constructing elliptic curves over finite fields with prescribed torsion”, *Math. Comp.* **81**:278 (2012), 1131–1147. MR Zbl
- [Sutherland 2013] A. V. Sutherland, “Isogeny volcanoes”, pp. 507–530 in *ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium* (San Diego, CA, 2012), edited by E. W. Howe and K. S. Kedlaya, Open Book Ser. **1**, Math. Sci. Publ., Berkeley, CA, 2013. MR Zbl
- [Waterhouse 1969] W. C. Waterhouse, “Abelian varieties over finite fields”, *Ann. Sci. École Norm. Sup. (4)* **2** (1969), 521–560. MR Zbl

Communicated by Bjorn Poonen

Received 2017-07-18

Revised 2021-02-05

Accepted 2022-02-01

maarten@mderickx.nl

Mathematisch Instituut, Universiteit Leiden, Leiden, Netherlands

kamienny@usc.edu

Department of Mathematics, USC Dornsife, Los Angeles, CA, United States

wstein@gmail.com

SageMath, Inc., Renton, WA, United States

michael.stoll@uni-bayreuth.de

Mathematisches Institut, Universität Bayreuth, Bayreuth, Germany

Tame fundamental groups of pure pairs and Abhyankar's lemma

Javier Carvajal-Rojas and Axel Stäbler

Let (R, \mathfrak{m}, k) be a strictly local normal k -domain of positive characteristic and P a prime divisor on $X = \text{Spec } R$. We study the Galois category of finite covers over X that are at worst tamely ramified over P in the sense of Grothendieck–Murre. Assuming that (X, P) is a purely F -regular pair, our main result is that every Galois cover $f : Y \rightarrow X$ in that Galois category satisfies that $(f^{-1}(P))_{\text{red}}$ is a prime divisor. We shall explain why this should be thought as a (partial) generalization of a classical theorem due to S.S. Abhyankar regarding the étale-local structure of tamely ramified covers between normal schemes with respect to a divisor with normal crossings. Additionally, we investigate the formal consequences this result has on the structure of the fundamental group representing the Galois category. We also obtain a characteristic zero analog by reduction to positive characteristics following Bhatt–Gabber–Olsson's methods.

1. Introduction	309
2. Preliminaries on pure log pairs	312
3. Digression on local tame fundamental groups	322
4. Tame fundamental groups: Positive characteristic	343
5. Tame fundamental groups: Characteristic zero	349
Appendix: Splitting primes under strict henselizations	353
Acknowledgements	355
References	355

1. Introduction

Carvajal-Rojas and Stäbler [2023] studied the behavior of *pure F -regularity* under finite covers; see [Carvajal-Rojas and Stäbler 2023, Sections 4 and 5]. In the present work, we shall deepen into the consequences of [loc. cit., Theorems 4.8 and 5.12], which explain the behavior of splitting primes, splitting ratios, and test ideals along closed subvarieties under finite covers. In the spirit of [Carvajal-Rojas et al. 2018; Carvajal-Rojas 2022; Jeffries and Smirnov 2022], we shall do so by studying the conditions

Carvajal-Rojas was supported in part by the NSF CAREER Grant DMS #1252860/1501102, by the ERC-STG #804334 and by FWO Grant #G079218N. Stäbler was supported in part by SFB-Transregio 45 Bonn-Essen-Mainz financed by Deutsche Forschungsgemeinschaft.

MSC2020: 13A35, 14B05, 14H30.

Keywords: pure F -regularity, PLT singularities, fundamental groups, splitting primes, Abhyankar's lemma.

they impose on the structure of covers over purely F -regular singularities that are at worst tamely ramified over the minimal center of F -purity divisor. To this end, consider the following setup.

Setup 1.1. Let $(R, \mathfrak{m}, \ell, K)$ be a strictly local normal ℓ -domain of (equi-)characteristic $p \geq 0$ and dimension ≥ 2 .¹ Set $X := \text{Spec } R$, let $Z \subset X$ be a closed subscheme of codimension ≥ 2 , and set $X^\circ = X \setminus Z$. Let P be a prime divisor on X , whose restriction to X° we denote by P as well. Consider the Galois category $\text{Rev}^P(X^\circ)$ of finite covers over X° that are at worst tamely ramified over P and denote by $\pi_1^{t,P}(X^\circ)$ the corresponding fundamental group; see Section 3.

Terminology 1.2 (local pure log pairs). With notation as in Setup 1.1, we say that (X, P) is a *pure pair* if either $p > 0$ and (X, P) is purely F -regular, or $p = 0$ and $(X, P + \Delta)$ is a purely log terminal pair for some (auxiliary) effective divisor Δ on X with coefficients strictly less than 1; see Section 2 for more details on these definitions.

In positive characteristic, our main result is the following.

Theorem A (Theorem 4.7, Proposition 5.2). *Work in Setup 1.1. If (X, P) is a pure pair, then every connected cover $f: Y^\circ \rightarrow X^\circ$ in $\text{Rev}^P(X^\circ)$ satisfies that $Q := (f^{-1}(P))_{\text{red}}$ is a prime divisor on Y° and (Y, Q) is a pure pair.*

The proof of this result in positive characteristic is inspired by our previous work [Carvajal-Rojas and Stabler 2023]. The analog in characteristic zero is well-known to experts; see Section 5. In a nutshell, we use [loc. cit., Theorem 4.8] and the symmetry induced by the Galois action to prove that there is only one point of Y lying over the generic point of P . Indeed, any such a point must correspond to the splitting prime of the pair (Y, Q) . Then, one may use [loc. cit., Theorem 5.12] to prove that (Y, Q) is a pure pair. In fact, one may do this quantitatively by means of the transformation rule for splitting ratios in [loc. cit., Theorem 4.8]. Theorem A, in combination with finiteness of local fundamental groups [Carvajal-Rojas et al. 2018; Xu 2014], has very strong consequences on the structure of $\pi_1^{t,P}(X^\circ)$. Concretely:

Theorem B (Theorem 4.12). *Work in Setup 1.1. Suppose that (X, P) is a pure pair of characteristic $p > 0$. Then, there exists an exact sequence of topological groups*

$$\hat{\mathbb{Z}}^{(p)} \rightarrow \pi_1^{t,P}(X^\circ) \rightarrow \pi_{1,\text{ét}}^P(X^\circ) \rightarrow 1,$$

where $\pi_{1,\text{ét}}^P(X^\circ)$ is the fundamental group corresponding to the Galois subcategory of covers that are étale over P . The group $\pi_{1,\text{ét}}^P(X^\circ)$ is finite with order prime-to- p and no more than $\min\{1/r(R, P), 1/s(R)\}$, where $r(R, P)$ is the splitting ratio of (R, P) and $s(R)$ is the F -signature of R . Furthermore:

- (1) *The homomorphism $\hat{\mathbb{Z}}^{(p)} \rightarrow \pi_1^{t,P}(X^\circ)$ is injective if the divisor class of P is a prime-to- p torsion element of $\text{Cl } R$. In this case, the short exact sequence*

$$1 \rightarrow \hat{\mathbb{Z}}^{(p)} \rightarrow \pi_1^{t,P}(X^\circ) \rightarrow \pi_{1,\text{ét}}^P(X^\circ) \rightarrow 1$$

splits (as topological groups) if and only if the divisor class of P is trivial.

¹Let us recall that a strictly local ring is a henselian local ring with separably closed residue field.

(2) If P is a nontorsion element of $\text{Cl } X$, we have a short exact sequence

$$0 \rightarrow \varprojlim_{n \in N^P(X^\circ)} \mathbb{Z}/n\mathbb{Z} \rightarrow \pi_1^{t,P}(X^\circ) \rightarrow \pi_{1,\text{ét}}^P(X^\circ) \rightarrow 1,$$

where $N^P(X^\circ) \subset \mathbb{N}$ is the set of prime-to- p positive integers $n \in \mathbb{N}$ for which there is a divisor D on X such that $P - n \cdot D \in \text{Cl } X$ has prime-to- p torsion and $D|_U$ is Cartier, where $U := X^\circ \setminus Z$. The sequence is split if and only if for every $n \in N^P(X^\circ)$ there are divisors D_n with $D_n|_U$ Cartier such that $P = nD_n \in \text{Cl } X$ which are compatible in the sense that $mD_{nm} = D_n$ in $\text{Cl } X$ for all $n, m \in N^P(X^\circ)$.

Remark 1.3. By [Taylor 2019, Corollary 1.2], we expect that $\min\{1/r(R, P), 1/s(R)\} = 1/s(R)$ in Theorem B. Indeed, Taylor's result establishes that this is the case when P has a prime-to- p torsion divisor class.

Over the complex numbers, we obtain the following analog.

Theorem C (Theorem 5.1). *Work in Setup 1.1. Suppose that (X, P) is a pure pair over \mathbb{C} . Then, there is an exact sequence of topological groups*

$$\hat{\mathbb{Z}} \rightarrow \pi_1^{t,P}(X^\circ) \rightarrow \pi_{1,\text{ét}}^P(X^\circ) \rightarrow 1,$$

where $\pi_{1,\text{ét}}^P(X^\circ)$ is finite; it is the fundamental group corresponding to the Galois subcategory of covers which are étale over P . Additionally:

(1) The homomorphism $\hat{\mathbb{Z}} \rightarrow \pi_1^{t,P}(X^\circ)$ is injective if the divisor class of P is a torsion element of $\text{Cl } R$. In this case, the short exact sequence

$$1 \rightarrow \hat{\mathbb{Z}} \rightarrow \pi_1^{t,P}(X^\circ) \rightarrow \pi_{1,\text{ét}}^P(X^\circ) \rightarrow 1,$$

splits (as topological groups) if and only if the divisor class of P is trivial.

(2) If P is a nontorsion element of $\text{Cl } X$, then we have a short exact sequence

$$0 \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow \pi_1^{t,P}(X^\circ) \rightarrow \pi_{1,\text{ét}}^P(X^\circ) \rightarrow 1.$$

The sequence is split if and only if there is a divisor D with $D|_U$ Cartier such that $P = nD \in \text{Cl } X$.

We shall prove Theorems B and C as formal consequences of the following two statements; see Section 3D and especially Theorem 3.29 for further details:

- Every connected cover $f : Y^\circ \rightarrow X^\circ$ in $\text{Rev}^P(X^\circ)$ satisfies that $(f^{-1}(P))_{\text{red}}$ is a prime divisor on Y° .
- There exists a universal étale-over- P cover $\tilde{X}^\circ \rightarrow X^\circ$.

In positive characteristic, we give direct proofs of these statements in Section 4B.

1A. Abhyankar’s lemma. We briefly mention here why the results in this work should be thought of as partial generalizations to Abhyankar’s lemma; see Section 3 for further details.

Abhyankar’s lemma [SGA 1 1971, Expose XIII, 5] is a theorem on the local structure, from the point of view of the tale topology, of finite covers between normal integral schemes that are tamely ramified with respect to a divisor with normal crossings (on the base). It establishes that, locally in the tale topology, any such cover is a quotient of a (generalized) Kummer cover; see [Grothendieck and Murre 1971; Stacks 2005–, Tag 0EYG]. In a sense, Abhyankar’s lemma is a *purity* theorem for Kummer covers. Indeed, by definition and Theorem 3.5, a tamely ramified cover with respect to a divisor is a cover that is Kummer at the codimension 1 tale-germs. Assuming the divisor has normal crossings; which is a regularity condition, Abhyankar’s lemma establishes that such a cover is Kummer at all tale germs.

Let us understand Abhyankar’s lemma with a simple but already fundamental example. With notation as in Setup 1.1, assume that R is regular (or just pure in the sense of [Cutkosky 1995]) and $P = \operatorname{div} f$. A finite cover $R \subset S$ with S a normal local domain is tamely ramified with respect to P if $R_f \subset S_f$ is tale and the generic field extension $K(S)/K(R)$ is tamely ramified with respect to the DVR $R_{(f)}$. An example of such an extension is a Kummer cover: $S = R[T]/(T^n - f)$ with n prime to the characteristic. However, there may exist several non-Kummer tamely ramified covers; see Example 3.14. In general, the connected components of the pullback of a tamely ramified cover $R \subset S$ to $R_{(f)}^{\text{sh}}$ must be Kummer covers and the converse holds provided that $R_f \subset S_f$ is tale; see Theorem 3.5 and Lemma 3.3.

In the above setup, Abhyankar’s lemma establishes that if R/f is regular, then any Galois tamely ramified cover of R with respect to the prime divisor $\operatorname{div} f$ is necessarily Kummer. One may then wonder for what singularities of R/f Abhyankar’s lemma hold. We shall see that in the situation of Theorems B and C, if R/f is either KLT in characteristic zero or strongly F -regular in positive characteristic, then the statement of Abhyankar’s lemma hold. A simpler version of our partial generalization of Abhyankar’s lemma is the following. For the more general statement see Lemma 3.34 (keeping in mind Examples 2.10 and 2.24).

Theorem D (Lemma 3.34, Corollaries 4.17 and 5.4). *With notation as in Setup 1.1, suppose that X is regular and $P = \operatorname{div} f$. If (X, P) is a pure pair, then every Galois tamely ramified cover over X with respect to P is of the form $\operatorname{Spec} R[T]/(T^n - f) \rightarrow X$ for n prime to the characteristic.*

Convention 1.4. If a scheme X or ring R is defined over \mathbb{F}_p , then we denote the e -th iterate of the Frobenius endomorphism by $F^e: X \rightarrow X$, or by $R \rightarrow F_*^e R$. We use the shorthand notation $q := p^e$ to denote the e -th power of the prime p , for instance $F^e: r \mapsto r^q$. We assume all our schemes and rings to be locally noetherian. In positive characteristic we also assume that they are F -finite and hence excellent.

2. Preliminaries on pure log pairs

In this preliminary section, we review the definitions and main aspects of *pure log pairs*. By this, we mean log pairs (X, Δ) that are purely F -regular if defined over a positive characteristic field, or purely log terminal if defined over a characteristic zero field.

2A. Pure F -regularity. Consider $X = \text{Spec } R$ where R is an F -finite normal κ -domain of positive characteristic p and let \mathcal{C} be a Cartier algebra acting on R ; see [Carvajal-Rojas and Stabler 2023, Section 2] for the relevant notions of Cartier algebras and modules in the way we employ them here. Following Schwede [2010], a *center of F -purity (or F -pure center) for (R, \mathcal{C})* is an integral closed subscheme $P = V(\mathfrak{p}) \subset X$ such that \mathfrak{p} is a \mathcal{C} -submodule of R . We say that P is a *minimal center of F -purity for (R, \mathcal{C})* if \mathfrak{p} is a maximal proper \mathcal{C} -submodule. Given a closed point $x \in \text{Spec } R$, we call P a *minimal center of F -purity through x* if $x \in P$.

Following Smolkin [2019, Section 3.1; 2020, Section 4], one defines $\tau_{\mathfrak{p}}(R, \mathcal{C})$ to be the smallest Cartier \mathcal{C} -submodule of R not contained in \mathfrak{p} , which exists provided that $\mathcal{C}_e(R) \not\subset \mathfrak{p}$ for some $e > 0$ (this condition is referred to as *nondegeneracy*); see [Takagi 2008; 2010], compare to [Carvajal-Rojas and Stabler 2023, Section 5.2]. By [Smolkin 2019, Proposition 3.1.14], we see that P is a minimal center of F -purity for (R, \mathcal{C}) if and only if $\tau_{\mathfrak{p}}(R, \mathcal{C}) + \mathfrak{p} = R$. When $\tau_{\mathfrak{p}}(R, \mathcal{C}) = R$, one says that (R, \mathcal{C}) is *purely F -regular along P* . For the generalization to the case \mathfrak{p} is radical, see [Carvajal-Rojas and Stabler 2023, Lemma 5.11].

In the local case, minimal centers of F -purity exist, are unique, and admit a simpler description. Indeed, if (R, \mathfrak{m}) is local then *the* minimal F -pure center of (R, \mathcal{C}) is given by the closed subscheme cut out by the splitting prime $p(R, \mathcal{C})$; see [Schwede 2010, Remark 4.4]. Further, we see that $\tau_{\mathfrak{p}}(R, \mathcal{C}) = R$ if $\mathfrak{p} = p(R, \mathcal{C})$. In other words, in the local case, (R, \mathcal{C}) is always purely F -regular along its (unique) minimal F -pure center. We are implicitly assuming that $p(R, \mathcal{C})$ is a proper ideal of R (i.e., (R, \mathcal{C}) is F -pure).

Still assuming R is local, let $P = V(\mathfrak{p}) \subset X$ be the closed subscheme cut out by a prime ideal $\mathfrak{p} \subset R$. Let $\mathcal{C}_R^{[P]} \subset \mathcal{C}_R$ be the Cartier subalgebra consisting of P -compatible p^{-e} -linear maps. In other words, $\varphi \in \mathcal{C}_{e,R}$ belongs to $\mathcal{C}_{e,R}^{[P]}$ if and only if $\varphi(F_*^e \mathfrak{p}) \subset \mathfrak{p}$. Since the splitting prime $p(R, \mathcal{C}_R^{[P]})$ is the unique largest prime ideal compatible with all the p^{-e} -linear maps in $\mathcal{C}_R^{[P]}$, we have an inclusion

$$\mathfrak{p} \subset p(R, \mathcal{C}_R^{[P]}).$$

This inclusion is an equality exactly when P is the minimal F -pure center of $\mathcal{C}_R^{[P]}$. In particular, we may say that P is a *minimal F -pure center of X* (with no explicit reference to a Cartier algebra) to say that it corresponds to the splitting prime of some Cartier algebra — necessarily $\mathcal{C}_R^{[P]}$. In that case, $(R, \mathcal{C}_R^{[P]})$ is purely F -regular along P .

In this paper, we are interested in minimal F -pure center divisors. In this case, we have:

Proposition 2.1. *Let R be a local normal κ -domain with $P = V(\mathfrak{p})$ a prime divisor on $\text{Spec } R$. Then, we have $\mathcal{C}_R^{[P]} = \mathcal{C}_R^P$, where \mathcal{C}_R^P is the Cartier algebra corresponding to the divisor $\Delta = P$; see [Schwede 2009].²*

Proof. Observe that membership in these Cartier algebras can be checked (by localizing) at \mathfrak{p} , where these Cartier algebras are obviously the same. \square

²It also coincides with $\mathcal{C}_R^{\mathfrak{p}}$ as in [Blickle 2013, Section 3.3].

Notation 2.2. With notation as in Proposition 2.1, we write $p(X, P)$ and $r(X, P)$ (or with X replaced by R) to denote the splitting prime and splitting ratio of the pair $(R, \mathcal{C}_R^{[P]})$. Moreover, we shall write \mathcal{C}_R^P instead of $\mathcal{C}_R^{[P]}$.

Definition 2.3 (purely F -regular local pair). With notation as in Proposition 2.1, we say that the pair (X, P) (or with R in place of X) is *purely F -regular* if P is a minimal F -pure center prime divisor on X .³

Remark 2.4. With notation as in Proposition 2.1, notice that (X, P) is a purely F -regular pair if and only $\tau_p(R, P) = R$, i.e., if (X, P) is purely F -regular along P .

We observe that X must have “mild” singularities to admit a purely F -regular divisor.

Proposition 2.5. *Let (X, P) be a purely F -regular local pair, then R (or X) is strongly F -regular (with respect to its full Cartier algebra \mathcal{C}_R). More generally, if A is a local domain with an action by some Cartier algebra $\mathcal{A} \subset \mathcal{C}_A$, and $C = V(\mathfrak{c})$ a minimal F -pure center prime divisor for $\mathcal{A}^C := \mathcal{A} \cap \mathcal{C}_A^C$ and (A, \mathcal{A}) is F -regular at the generic point of C , then (A, \mathcal{A}) is F -regular.*

Proof. Since $\mathcal{A}^C \subset \mathcal{A}$, we have that $p(A, \mathcal{A}) \subset p(A, \mathcal{A}^C) = \mathfrak{c}$, where the equality follows from \mathfrak{c} being a prime maximal center of F -purity. Since \mathfrak{c} has height 1, $p(\mathcal{A})$ is either 0 or \mathfrak{c} . If $p(\mathcal{A}) = 0$, we are done. If $p(\mathcal{A}) = \mathfrak{c}$, then (A, \mathcal{A}) is not F -regular at the generic point of C , contradicting our hypothesis. To see the first statement follows from the last one, notice that, since R is normal, (R, \mathcal{C}_R) is F -regular at the generic point of P . \square

Remark 2.6. In Proposition 2.5, the normality hypothesis on R is necessary. Indeed, we may consider the Whitney’s umbrella singularity as a counterexample; see [Blickle et al. 2012, Section 4.3.2].

Finally, we recall the global-to-local passage for F -pure centers.

Proposition 2.7. *Let X be the spectrum of a normal \mathcal{k} -domain and let \mathcal{C} be a Cartier algebra on X . Let $P = V(\mathfrak{p})$ be a minimal center of F -purity passing through a geometric point $\bar{x} \rightarrow X$, then $\mathfrak{p} \cdot \mathcal{O}_{X, \bar{x}}^{\text{sh}}$ is the splitting prime of the Cartier $\mathcal{O}_{X, \bar{x}}^{\text{sh}}$ -algebra $\mathcal{O}_{X, \bar{x}}^{\text{sh}} \otimes \mathcal{C}$.*

Proof. See Proposition A.3 in the Appendix. \square

2A1. *Some examples of purely F -regular pairs.* We provide next some examples of purely F -regular pairs. Our method to prove that a given pair is purely F -regular is the following.

Lemma 2.8. *Let R be a normal local domain, $\mathfrak{p} \subset R$ be a prime ideal (not necessarily of height 1), and set $P = V(\mathfrak{p})$. Then, \mathfrak{p} is the splitting prime of $\mathcal{C}_R^{[P]}$ if and only if R/\mathfrak{p} is F -regular with respect to the induced action of $\mathcal{C}_R^{[P]}$. In that case, the splitting ratio of (R, P) is the F -signature of R/\mathfrak{p} with respect to $\mathcal{C}_R^{[P]}$.*

³Note that this is called *divisorially F -regular* in [Hara and Watanabe 2002]. However, we use the *purely F -regular* terminology to emphasize the connections with purely log terminal (PLT) singularities and avoid confusions with *divisorially log terminal* singularities (DLT).

Proof. Note that \mathfrak{p} is the splitting prime of $\mathcal{C}_R^{[P]}$ if and only if R/\mathfrak{p} viewed as an $\mathcal{C}_R^{[P]}$ -module is simple. However, we may equivalently view R/\mathfrak{p} as an $\overline{\mathcal{C}_R^{[P]}}$ -module; compare to [Blickle 2013, discussion before Lemma 2.20]. See [Blickle et al. 2012, Lemma 2.13]. \square

We shall also need the following observation.

Remark 2.9. Consider the category of finite type κ -algebras for some F -finite field κ . Fix an isomorphism $\lambda: \kappa \rightarrow F^1\kappa$ with adjoint $\kappa: F_*\kappa \rightarrow \kappa$. If we have two Cartier linear maps $\Phi, \Psi: F_*^e R \rightarrow R$ for some finite type κ -algebra R , then, by choosing a presentation $S = \kappa[x_1, \dots, x_n] \rightarrow R$ and via [Fedder 1983], we reduce the problem of whether $\Phi = \Psi$ to a computation in the polynomial ring S . Indeed, note that λ induces an isomorphism $f^1\kappa = \omega_S \rightarrow F^1\omega_S$, where $f: \text{Spec } S \rightarrow \text{Spec } \kappa$ is the structural map. Identifying ω_S with S , we obtain an isomorphism $\Sigma: S \rightarrow F^1S$. By [Stäbler 2017, Lemma 4.1], the adjoint of Σ is given by

$$\xi x_1^{i_1} \cdots x_n^{i_n} \mapsto \kappa(\xi) x_1^{(i_1+1)/q} \cdots x_n^{(i_n+1)/q},$$

with the usual convention that $x_i^{a/b}$ is zero whenever the exponent is not an integer. Now, by adjunction $\text{Hom}_R(F_*^e R, R) = \text{Hom}_R(R, F^{e^1} R)$ and by our choice of isomorphism Σ , we have that $\text{Hom}_R(R, F^{e^1} R) \cong \text{Hom}_R(R, R)$, and, by making this identification, Σ induces the identity so that the adjoint of Σ is a generator of $\text{Hom}_R(F_*^e R, R)$.

In this way, if we want to check that two Cartier linear maps of a finite type κ -algebra R coincide, we may reduce, via a choice of presentation and Fedder's criterion to a comparison of two Cartier linear maps in a polynomial ring. For those to coincide in turn, we choose any basis B of $F_*\kappa$ as a κ -module and then just need to check that they agree on $b \cdot x_1^{i_1} \cdots x_n^{i_n}$, where $b \in B$ and $0 \leq i_j \leq q - 1$.

This line of reasoning is also preserved if we pass to completions. Indeed, by [Stacks 2005–, Lemma 0394], we may identify $(F_*R)^\wedge$ with F_*R^\wedge . Since both are finite free modules, the claim is clear.

Example 2.10 (purely F -regular pairs on a regular ambient). Let R be a *regular* local ring. Recall that regular local rings are UFD; see [Stacks 2005–, Lemma 0AG0]. In particular, any prime divisor on $\text{Spec } R$ is principal [Matsumura 1980, Section 19, Theorem 47]. Let $\mathfrak{p} = (f)$ be a height 1 prime ideal of R with corresponding prime divisor P . As an immediate application of Lemma 2.8 and Fedder's criterion [1983], we see that (R, P) is purely F -regular if and only if R/f is a strongly F -regular ring. Moreover, in this case, one has $r(R, P) = s(R/f)$.

Example 2.11 (graded hypersurfaces). Let $R = \kappa[[z, x_0, x_1, \dots, x_d]]/(z^n - x_0h)$ be a normal hypersurface over a perfect field κ , where h is an irreducible weighted polynomial in the variables x_1, \dots, x_d ; see [Singh and Spiroff 2007]. Then, $\text{Cl } R \cong \mathbb{Z}/n\mathbb{Z}$ and the divisor class of (z, h) is a generator for $\text{Cl } R$; see [loc. cit., Corollary 3.4]. Letting P be the prime divisor corresponding to (z, h) , we claim the following.

Claim 2.12. *The pair (R, P) is purely F -regular if $A := \kappa[[x_1, \dots, x_d]]/h$ is strongly F -regular. In that case, $r(R, P) \geq s(A)/n$, and $r(R, P) = 1/n$ if A is regular.*

Proof of claim. Let $S := \kappa[[z, x_0, x_1, \dots, x_d]]$ and $f := z^n - x_0h$. By Fedder's criterion [1983], we have that $\mathcal{C}_{e,R}$ is generated by the reduction of $\Phi^e \cdot f^{q-1} \in \mathcal{C}_{e,S}$ to R , where Φ denotes the Frobenius trace on S . In other words, $\mathcal{C}_R = \overline{\mathcal{C}_R^\phi}$ where $\phi := \overline{\Phi \cdot f^{p-1}}$. Having Proposition 2.1 in mind, we recall that \mathcal{C}_R^P is given, in degree e , by all maps $\phi^e \cdot g$ such that $\text{val}_{\mathfrak{p}} g \geq q - 1$. Note that z is a uniformizer for $R_{\mathfrak{p}}$ and $\text{val}_{\mathfrak{p}} h = n$. In particular, \mathcal{C}_R^P contains the maps $\phi^e \cdot z^i h^j$ where $i + nj = q - 1$. Therefore, the reduction of \mathcal{C}_R^P to $R/\mathfrak{p} \cong \kappa[[x_0, x_1, \dots, x_d]]/h$ contains the maps $\overline{\phi^e \cdot z^i h^j}$ with $i + nj = q - 1$. However, these maps are the reductions of $\Phi^e \cdot z^i h^j f^{q-1}$ to $R/\mathfrak{p} = S/(z, h)$, and we have that

$$z^i h^j f^{q-1} \equiv (-1)^{q-1-j} \binom{q-1}{j} z^{q-1} x_0^{q-1-j} h^{q-1} \pmod{(z^q, h^q)}$$

for all $i + nj = q - 1$. In other words, the reduction of \mathcal{C}_R^P to $R/\mathfrak{p} \cong \kappa[[x_0, x_1, \dots, x_d]]/h \cong S/(z, h)$ contains, in degree e , the reductions of $\Phi^e \cdot z^{q-1} x_0^{q-1-j} h^{q-1}$ for all $j \leq (q-1)/n$. Alternatively, if Ψ is the Frobenius trace for $\kappa[[x_0, x_1, \dots, x_d]]$, we have that the reduction of \mathcal{C}_R^P to $\kappa[[x_0, x_1, \dots, x_d]]/h$ contains the reductions of $\Psi^e \cdot x_0^{q-1-j} h^{q-1}$. Therefore, we have

$$s(R/\mathfrak{p}, \overline{\mathcal{C}_R^P}) \geq \frac{1}{n} \cdot s(A).^4$$

Consequently, by applying Lemma 2.8, we conclude that $\mathfrak{p} = p(R, \mathcal{C}_R^P)$, and furthermore

$$r(R, P) = s(R/\mathfrak{p}, \overline{\mathcal{C}_R^P}) \geq \frac{1}{n} \cdot s(A).$$

To see this is an equality if A is regular, we may use the transformation rule for splitting ratios [Carvajal-Rojas and Stabler 2023, Theorem 4.8]. Indeed, suppose for sake of contradiction that the inequality is strict, and let \tilde{R} be the Veronese-type cyclic cover given by P . That is, $\tilde{R} = \bigoplus_{i=0}^{n-1} \mathfrak{p}^{(i)}$. It is not difficult to see that $\tilde{R} = R[x_0^{1/n}, h^{1/n}]$ and the only prime in \tilde{R} lying over \mathfrak{p} is $\tilde{\mathfrak{p}} = (h^{1/n})$; whose corresponding prime divisor we denote by \tilde{P} . Therefore, $\tilde{\mathfrak{p}}$ must be the splitting prime of the pullback of \mathcal{C}_R^P along the cover $R \subset \tilde{R}$. Hence, the transformation rule for splitting ratios yields $r(\tilde{R}, \tilde{P}) = n \cdot r(R, P) > s(A) = 1$, which is a contradiction. \square

Example 2.13. Let $R = \kappa[[x, y, z, w]]/(xy - zw)$. Recall that the divisor class group of R is free of rank 1; see [Hartshorne 1977, II, Exercise 6.5]. Moreover, the divisor class of the height-1 prime ideal $\mathfrak{p} = (x, z)$ is a generator of $\text{Cl } R$. We claim that $P = V(\mathfrak{p})$ is a minimal F -pure center.

Claim 2.14. *The pair (R, P) is purely F -regular and $r(R, P) \geq \frac{1}{2}$.*

Proof of claim. Let $S = \kappa[[x, y, z, w]]$ and $f = xy - zw$. We use Fedder's criterion [1983] to conclude that $\mathcal{C}_{e,R}$ is generated by the reduction of $\Phi^e \cdot f^{q-1} \in \mathcal{C}_{e,S}$ to R ; where Φ denotes the Frobenius trace on S . That is, $\mathcal{C}_R = \overline{\mathcal{C}_R^\phi}$ where $\phi := \overline{\Phi \cdot f^{p-1}}$. With Proposition 2.1 in mind, recall that \mathcal{C}_R^P is given, in degree e , by all maps $\phi^e \cdot g$ such that $\text{val}_{\mathfrak{p}} g \geq q - 1$. In particular, we have that $\mathcal{C}_{e,R}^P$ contains all the maps $\phi^e \cdot x^i z^j$ such that $i + j = q - 1$. Thus, the reduction of \mathcal{C}_R^P to $R/\mathfrak{p} = \kappa[[y, w]]$ contains, in degree e , the

⁴To see this, note that we may work in the polynomial case as completions have no bearing on the value of F -signatures; see [Yao 2006] or [Carvajal-Rojas et al. 2021, Section 3]. Then, the result follows from the behavior of F -signatures with respect to tensor products; see [Carvajal-Rojas and Smolkin 2020, Proposition 5.5] for instance.

maps $\bar{\phi}^e \cdot x^i y^j$ such that $i + j = q - 1$. Notice that these maps are, respectively, the reductions of the map $\Phi \cdot x^i y^j f^{q-1}$. Nonetheless, one readily sees that

$$x^i y^j f^{p-1} \equiv (-1)^i \binom{p-1}{j} (xz)^{q-1} y^j w^i \pmod{(x^p, z^p)}.$$

Therefore, $\bar{\phi}^e \cdot x^i y^j$, $i + j = q - 1$, is, up to premultiplication by units in κ , the dual map of $F_*^e y^i w^j$ with respect to the free basis of $F_*^e R/\mathfrak{p}$ over R/\mathfrak{p} given by $\{F_*^e y^k w^l \mid 0 \leq k, l \leq q - 1\}$. That is, $\bar{\phi}^e \cdot x^i z^j = \Psi^e \cdot y^j w^i$ where Ψ denotes the Frobenius trace of $R/\mathfrak{p} = \kappa[[y, w]]$. Hence,

$$s(\kappa[[y, w]], \overline{\mathcal{C}_R^P}) \geq \text{area}([0, 1]^{\times 2} \cap \{(y, w) \in \mathbb{R}^2 \mid y + w \geq 1\}) = \frac{1}{2}.$$

This proves the claim by Lemma 2.8. \square

Example 2.15. Let $A := \kappa[[u, v, w, x, y, z]]$ and $I := (\Delta_1, \Delta_2, \Delta_3)$ where $\Delta_1 := vz - wy$, $\Delta_2 := wx - uz$, and $\Delta_3 := uy - vx$. Let $R = A/I$. We claim that the prime divisor P defined by the height-1 prime ideal $\mathfrak{p} := (u, v, w)$ is a minimal F -pure center, and moreover $r(R, P) \geq \frac{1}{6}$. We use Lemma 2.8. To this end, we recall that $\mathcal{C}_{e,R}$ was explicitly computed in [Katzman et al. 2014, Proposition 5.1]. Indeed, for nonnegative integers s, t such that $s + t \leq q - 1$, one writes

$$y^s z^t (\Delta_2 \Delta_3)^{q-1} \equiv x^{s+t} f_{s,t} \pmod{I^{[q]}},$$

for some $f_{s,t}$, which is well-defined mod $I^{[q]}$. Then,

$$I^{[q]} : I = I^{[q]} + (f_{s,t} \mid s, t \geq 0, s + t \leq q - 1).$$

Thus, by Fedder's criterion [1983], $\mathcal{C}_{e,R}$ is generated by $\Phi^e \cdot f_{s,t}$, where Φ is a Frobenius trace associated to A . We choose $f_{0,0}$ to be $(\Delta_2 \Delta_3)^{q-1}$. In fact, we have that $I^{2(q-1)} \subset I^{[q]} : I$. In particular, we have the following relations:

$$y^s z^t f_{0,0} \equiv x^{s+t} f_{s,t} \pmod{I^{[q]}}. \quad (2.15.1)$$

Let $\phi_{s,t}^e$ be the map in $\mathcal{C}_{e,R}$ induced by $\Phi^e \cdot f_{s,t}$ for $s + t \leq q - 1$.

Claim 2.16. \mathcal{C}_R^P contains the maps $\{\phi_{s,t}^e \cdot u^l v^m w^n \mid l + m + n = q - 1, s + t \leq q - 1\}$.

Proof of claim. Observe that, up to premultiplications by units, all the maps $\phi_{s,t}^e$ induce the same map after we localize at $\mathfrak{p} = (u, v, w)$ by (2.15.1). Note that $R_{\mathfrak{p}}$ is a DVR so that $\mathcal{C}_{e,R_{\mathfrak{p}}}$ is principally generated. As the $\phi_{s,t}^e$ generate $\mathcal{C}_{e,R}$, any $\phi_{s,t}^e$ is a generator of $\mathcal{C}_{e,R_{\mathfrak{p}}}$. Now, any element u, v, w is a uniformizer in $R_{\mathfrak{p}}$. To verify the claim, we may localize at \mathfrak{p} , but then $\phi_{s,t}^e u^l v^m w^n$ is of the form $\kappa \cdot t^{l+m+n}$ where κ is a generator of $\text{Hom}(F_*^e R_{\mathfrak{p}}, R_{\mathfrak{p}})$ and t is a uniformizer. This map is \mathfrak{p} -compatible if and only if $m + l + n \geq q - 1$. \square

Next, observe that $R/\mathfrak{p} \cong \kappa[[x, y, z]]$, with Frobenius trace denoted by Ψ . By Remark 2.9, we may choose Ψ in such a way that $\phi_{s,t}^e$ and Ψ^e are induced by the same map $\kappa : F_* \kappa \rightarrow \kappa$. Thus, for all $s + t \leq q - 1$ and all $l + n + m = q - 1$, we have that $\phi_{s,t}^e \cdot u^l v^m w^n$ restricts to a map in $\mathcal{C}_{e,R/\mathfrak{p}}$; say

$\varphi_{s,t}^e \cdot u^l v^m w^n$. Hence, we have an equality $\varphi_{s,t}^e \cdot u^l v^m w^n = \Psi^e \cdot a_{s,t;l,m,n}$ for a uniquely determined $a_{s,t;l,m,n} \in \mathcal{K}[[x, y, z]]$, which are explicitly described as follows:

Claim 2.17. *Let $l, m, n; s, t$ be nonnegative integers such that $l + m + n = q - 1$, $s + t \leq q - 1$. Let us set $q - 1 - s - t =: r \geq 0$, so that $r + s + t = q - 1$. Then, we have that $a_{s,t;l,m,n} = 0$ unless one of the following four triples $(l + r, m + s, n + t)$, $(l + r - q, m + s, n + t)$, $(l + r, m + s - q, n + t)$, $(l + r, m + s, n + t - q)$ belongs to $\{0, \dots, q - 1\}^{\times 3}$, in which case*

$$a_{s,t;l,m,n} = \xi \cdot x^{l+r} y^{m+s} z^{n+t}$$

for some unit $\xi \in \mathbb{F}_p^\times \subset \mathcal{K}^\times$.

Proof of claim. First of all, note that

$$\begin{aligned} f_{0,0} &= \Delta_2^{q-1} \Delta_3^{q-1} = \left(\sum_{a+b=q-1} (-1)^b \binom{q-1}{a} (wx)^a (uz)^b \right) \left(\sum_{c+d=q-1} (-1)^d \binom{q-1}{c} (uy)^c (vx)^d \right) \\ &= \sum_{\substack{a+b=q-1 \\ c+d=q-1}} (-1)^{b+d} \binom{q-1}{a} \binom{q-1}{c} u^{b+c} v^d w^a x^{a+d} y^c z^b. \end{aligned}$$

Therefore,

$$u^l v^m w^n f_{0,0} \equiv - \binom{q-1}{m} \binom{q-1}{n} u^{q-1} v^{q-1} w^{q-1} x^{l+q-1} y^m z^n \pmod{\mathfrak{p}^{[q]}}. \quad (2.17.1)$$

Indeed, after multiplying by $u^l v^m w^n$, every summand vanishes modulo $\mathfrak{p}^{[q]}$ except for the summands where simultaneously $l + b + c \leq q - 1$, $m + d \leq q - 1$, and $n + a \leq q - 1$. However, given the constraints $a + b = q - 1$ and $c + d = q - 1$, we have that

$$(l + b + c) + (m + d) + (n + a) = 3(q - 1).$$

Hence, $l + b + c, m + d, n + a = q - 1$, and also $a + d = l + q - 1$. In particular, $m = c$ and $n = b$. Set $\xi := - \binom{q-1}{m} \binom{q-1}{n} \in \mathcal{K}^\times$.

On the other hand, for $0 \leq i, j, l \leq q - 1$ we have that

$$\begin{aligned} u^l v^m w^n x^i y^j z^k f_{s,t} &= \frac{1}{x^q} u^l v^m w^n x^{i+q-s-t} y^j z^k x^{s+t} f_{s,t} \\ &= \frac{1}{x^q} u^l v^m w^n x^{i+r+1} y^{j+s} z^{k+t} f_{0,0} \\ &\equiv \frac{\xi}{x^q} u^{q-1} v^{q-1} w^{q-1} x^{q+i+r+l} y^{j+s+m} z^{k+t+n} \pmod{\mathfrak{p}^{[q]}} \\ &\equiv \xi u^{q-1} v^{q-1} w^{q-1} x^{i+r+l} y^{j+s+m} z^{k+t+n} \pmod{\mathfrak{p}^{[q]}}. \end{aligned}$$

Therefore,

$$\Phi^e(u^l v^m w^n x^i y^j z^k f_{s,t}) \equiv \xi \Phi^e(u^{q-1} v^{q-1} w^{q-1} x^{i+r+l} y^{j+s+m} z^{k+t+n}) \pmod{\mathfrak{p}}$$

Next, we observe that this element is $0 \pmod{\mathfrak{p}}$ unless

$$i + r + l, j + s + m, k + t + n \equiv q - 1 \pmod{q}.$$

Since all these three sums are at most $3(q-1)$, we then have

$$\begin{cases} i+r+l = q-1 + \alpha q, \\ j+s+m = q-1 + \beta q, \\ k+t+n = q-1 + \gamma q, \end{cases}$$

for some $\alpha, \beta, \gamma \in \{0, 1\}$. However, if we add these equations together, we obtain

$$i+j+k+2(q-1) = 3(q-1) + (\alpha + \beta + \gamma)q.$$

Equivalently,

$$i+j+k = q-1 + (\alpha + \beta + \gamma)q.$$

Being $i+j+k$ at most $3(q-1)$, this forces $\alpha + \beta + \gamma \in \{0, 1\}$. Hence, α, β, γ are either all 0 or one of them is 1 while the other two are 0. In the first case, we then have

$$i+r+l, j+s+m, k+t+n = q-1.$$

Therefore, in this case, we have that $\Phi^e(u^l v^m w^n x^i y^j z^k f_{s,t}) \equiv 0 \pmod{\mathfrak{p}}$ unless

$$i = q-1 - (r+l), j = q-1 - (s+m), k = q-1 - (t+n) \geq 0.$$

In that case, $\Phi^e(u^l v^m w^n x^i y^j z^k f_{s,t}) \equiv \xi \pmod{\mathfrak{p}}$, and so $a_{s,t;l,m,n} = \xi x^{r+l} y^{s+m} z^{t+n}$ (whenever $r+l, s+m, t+n \geq q-1$).

Let us consider now the remaining three cases, i.e., $(\alpha, \beta, \gamma) \in \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$. By symmetry, it suffices to consider $(\alpha, \beta, \gamma) = (1, 0, 0)$. In this case, we have that the element $\Phi^e(u^l v^m w^n x^i y^j z^k f_{s,t})$ vanishes modulo \mathfrak{p} unless

$$q-1 \geq i = q-1 + q - (r+l) \geq 0 \quad \text{and} \quad j = q-1 - (s+m), k = q-1 - (t+n) \geq 0,$$

equivalently

$$0 \leq (r+l) - q \leq q-1 \quad \text{and} \quad j = q-1 - (s+m), k = q-1 - (t+n) \geq 0,$$

which implies $\Phi^e(u^l v^m w^n x^i y^j z^k f_{s,t}) \equiv \xi x \pmod{\mathfrak{p}}$. In this case, $a_{s,t;l,m,n} = \xi x^{r+l} y^{s+m} z^{t+n}$. \square

Let us analyze which maps the first case $(l+r, m+s, n+t) \in \{0, \dots, q-1\}^3$ of Claim 2.17 yields. Note that the map from the set

$$\{(l, m, n; r, s, t) \in \{0, \dots, q-1\}^6 \mid l+m+n, r+s+t = q-1 \text{ and } l+r, m+s, n+t \leq q-1\}$$

to the set

$$\{(i, j, k) \in \{0, \dots, q-1\}^3 \mid i+j+k = 2(q-1)\}$$

defined by

$$(l, m, n; r, s, t) \mapsto (l+r, m+s, n+t)$$

is surjective. Indeed, taking $l = s = 0$ and given $0 \leq r, m \leq q - 1$, we obtain $2(q - 1) = r + t + m + n$ or, put differently, $2(q - 1) - r - m = t + n$. Thus, we see that this case yields the maps $\Psi^e \cdot x^i y^j z^k$ with $i + j + k = 2(q - 1)$. In other words, we obtain the Cartier algebra given by the pair $(\kappa[[x, y, z]], (x, y, z)^2)$.

For the remaining three cases of Claim 2.17, we obtain the maps

$$x \cdot \Psi^e \cdot x^{r+l-q} y^{s+m} z^{t+n}, \quad y \cdot \Psi^e \cdot x^{r+l} y^{s+m-q} z^{t+n}, \quad z \cdot \Psi^e \cdot x^{r+l} y^{s+m} z^{t+n-q}$$

where, respectively, $(r + l - q, s + m, t + n) \in \{0, \dots, q - 1\}$, $(r + l, s + m - q, t + n) \in \{0, \dots, q - 1\}$, $(r + l, s + m, t + n - q) \in \{0, \dots, q - 1\}$. However, these are all nonsurjective maps.

In conclusion, we obtain

$$s(R/\mathfrak{p}, \overline{\mathcal{C}}_R^P) \geq \text{volume}([0, 1]^{\times 3} \cap \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z \geq 2\}) = \frac{1}{6} > 0,$$

where we use [Blickle et al. 2012, Theorem 4.20] for the inequality. Hence, $r(R, P) \geq \frac{1}{6}$ and (R, P) is purely F -regular.

Remark 2.18. In Example 2.15, it would be interesting to fully compute \mathcal{C}_R^P to check whether or not $r(R, P) = 1/6$. The issue is that we cannot apply Fedder’s criterion for R since R is not regular. One may apply Fedder’s criterion to $I + \mathfrak{p}$ in A to work around this.

Question 2.19. Let $C_{r,s}$ be the cone singularity given by the Segre embedding of $\mathbb{P}_{\kappa}^r \times \mathbb{P}_{\kappa}^s$. The F -signatures of these toric rings were computed in [Singh 2005] and it is well-known that $\text{Cl } C_{r,s} \cong \mathbb{Z}$. In fact, $C_{r,s}$ is a determinantal ring. Let $S = \kappa[[x_{i,j} \mid 1 \leq i \leq m, 1 \leq j \leq n]]$ be the power series ring in the $m \times n$ matrix of variables $(x_{i,j})$, and let I_t be the ideal generated by the $t \times t$ minors of $(x_{i,j})$ ($2 \leq t \leq \min\{m, n\}$). The quotient ring $R = R(m, n, t) = S/I_t$ is called a determinantal ring. We observe that $C_{r,s}$ is none other than $R(r + 1, s + 1, 2)$. Moreover, if P is the prime divisor on $\text{Spec } C_{r,s}$ given by $\mathfrak{p} = (x_{1,1}, \dots, x_{1,s+1})$,⁵ then the divisor class of P is a free generator of $\text{Cl } C_{r,s}$. Based on the previous examples, it is natural to ask whether the pair $(C_{r,s}, P)$ is purely F -regular and if so what its splitting ratio is. More generally, if R is an arbitrary determinantal ring, we have that $\text{Cl } R$ is freely generated by P the divisor class of the height-1 prime ideal \mathfrak{p} generated by the $t - 1$ size minors of any set of $t - 1$ rows (or columns); see [Bruns and Vetter 1988, Corollary 8.4]. We ask the same question as before for the pair (R, P) . Note that in order to answer to these questions along the same ideas we had for $C_{1,1}$ and $C_{1,2}$, a good understanding of the colon ideal $I_t^{[q]} : I_t$ is needed. Nonetheless, to the best of the authors’ knowledge, very little is known about this. The authors believe a different approach is required.

2B. Purely log terminal pairs. We refer the reader to [Kollár and Mori 1998] for a detailed exposition on log canonical singularities and to [Ambro 1999] for the notion of (minimal) log canonical centers. We will, however, briefly review these notions here. Let (X, Δ) be a log pair defined over an algebraically closed field of characteristic zero. Fix a log resolution $\pi : Y \rightarrow (X, \Delta)$ and write $\Delta_Y = \pi^*(K_X + \Delta) - K_Y$. The pair (X, Δ) is *log canonical* (LC) if the coefficients of Δ_Y are ≤ 1 . The pair (X, Δ) is called *purely*

⁵In fact, any ideal generated by either a fixed column or row of variables.

log terminal (PLT) if it is LC and the exceptional components of Δ_Y have coefficients < 1 . We say that (X, Δ) is *Kawamata log terminal* (KLT) if all coefficients of Δ_Y are < 1 . A prime divisor P on X is called an *LC center* if the coefficient a_P of the strict transform of P in Δ_Y is ≥ 1 . Since the multiplier ideal $\mathcal{J}(X, \Delta)$ is given by $\pi_* \mathcal{O}_Y(K_Y - \lfloor \pi^*(K_X + \Delta) \rfloor)$, this is equivalent to $\mathcal{O}_X(-P) \supset \mathcal{J}(X, \Delta)$.

In analogy to Proposition 2.7, we recall the global-to-local passage is for LC centers. Let (X, Δ) be a log canonical pair, $\dim X \geq 2$. Let P be an LC center going through a closed point $x \in X$. In studying $\mathcal{O}_{X,x}^{\text{sh}}$, we are free to replace X by any open neighborhood U of x and Δ by Δ_U . In particular, we may assume that (X, Δ) is purely log terminal. Indeed, we may write $\Delta_Y = E_1 + \cdots + E_n + \sum_E a_E E$, for some n and such that $a_E < 1$. Note that one of the E_i , say E_1 is P . By the assumption that P is a divisor and the minimal LC center through x , the other divisors E_i do not contain x . Hence, replacing X by a suitable neighborhood U of x , we may assume that (X, Δ) is PLT and moreover $\lfloor \Delta \rfloor = P$ is a prime divisor going through x .⁶ Thus, we may work in the following setup.

Setup 2.20. Let (X, Δ) be a PLT log pair of dimension at least 2, such that $\lfloor \Delta \rfloor = P$ is a prime divisor going through a closed point $x \in X$. We set $X_x^\circ = \text{Spec } \mathcal{O}_{X,x}^{\text{sh}} \setminus Z$, where Z is some closed subset of codimension ≥ 2 . We denote by P the pullback of P to U .

The following is analogous to Proposition 2.5 and well-known to experts; see [Kollár and Mori 1998, Proposition 2.43].

Proposition 2.21. *Let $(X, \Delta = \sum a_i \Delta_i)$ be a PLT pair with X quasiprojective and $0 \leq a_i \leq 1$. Then there is a \mathbb{Q} -Cartier \mathbb{Q} -divisor Δ' such that the pair $(X, \Delta + \varepsilon \Delta')$ is KLT for all rational $0 < \varepsilon \ll 1$*

Proof. Let $m > 0$ be so that $m\Delta$ is integral. Since X is quasiprojective, there is an ample divisor H . Choose $n \gg 0$ so that $\mathcal{O}_X(nH + m\Delta)$ is globally generated. As the base locus of the linear system $|nH + m\Delta|$ is empty, we find an element D of this linear system having no component in common with Δ . Set $\Delta' = \frac{1}{m}D - \Delta$. Then, $K_X + \Delta + \varepsilon \Delta'$ is \mathbb{Q} -Cartier since Δ' is so: $m \cdot \Delta' = D - m\Delta \sim nH$. Note that $\Delta + \varepsilon \Delta' \geq 0$ for all rational $0 \leq \varepsilon \ll 1$. Since D and Δ share no components, $\lfloor \Delta + \varepsilon \Delta' \rfloor = 0$. As $a(E, X, \Delta + \varepsilon \Delta') \rightarrow a(E, X, \Delta)$ for $\varepsilon \rightarrow 0$, there is ε so that $(X, \Delta + \varepsilon \Delta')$ is KLT. \square

We make precise the connection between purely F -regular pairs and PLT pairs.

Theorem 2.22 [Takagi 2008, Corollary 5.4]. *Let (X, Δ) be a log pair. Spread (X, Δ) out over some finitely generated \mathbb{Z} -algebra A . Then, (X, Δ) is PLT if and only if there is a dense open $U \subset \text{Spec } A$ such that the reduction (X_a, Δ_a) is purely F -regular for all $a \in U$.*

Theorem 2.23. *Let (X, Δ) be an affine PLT pair. Assume that $\lfloor \Delta \rfloor = P$ is an minimal LC center for some closed point $x \in P$. Spread (X, Δ) , P , and x out over some finitely generated \mathbb{Z} -algebra A . Then, for all $a \in U$, where U is a dense open subset of $\text{Spec } A$, the divisor P_a is the minimal F -pure center through x_a . In this situation, a minimal LC center is normal. Conversely, if P is not the minimal LC center through x , then P_a is not the minimal F -pure center for x_a for all closed points in a dense open set.*

⁶That is, the generic point of P is the only codimension 1 point in the non-KLT locus of (X, Δ) .

Proof. See [Schwede 2010, Theorem 6.8]. Schwede’s argument immediately also gives the converse statement: If there is some smaller LC center Q passing through x , after reduction, we obtain an F -compatible ideal q_a strictly containing p_a . Thus, P_a cannot be the minimal F -pure center through x_a . For normality of the minimal LC center see [Fujino and Gongyo 2012, Theorem 7.2]. \square

By Theorems 2.22 and 2.23, examples in Section 2A1 are examples of PLT pairs when we let κ have characteristic zero. However, we need to sharpen our hypothesis for the analog of Example 2.10.

Example 2.24. Let R be regular, local and essentially of finite type over an algebraically closed field of characteristic zero, and let $(f) \subset R$ be a prime ideal. Then, the pair $(R, \operatorname{div} f)$ is a PLT pair if and only if R/f is a (Gorenstein) KLT singularity.

3. Digression on local tame fundamental groups

The objective in this section is twofold. First, we overview all the necessary material regarding tame fundamental groups that we need to establish our results. Second, we prove the theorem establishing that Theorems B and C are formal consequences of structural properties of the Galois category being studied. We start off with our first goal.

3A. Tame ramification, cohomological tameness, and Abhyankar’s lemma. We commence by recalling some standard definitions in [Grothendieck and Murre 1971].

Definition 3.1 (tamely ramified field extensions with respect to a DVR). Let K be a field with a discrete valuation ring (DVR) $(A, (u), \kappa)$. One says that a finite separable field extension L/K is *tamely ramified with respect to A* if for all (the finitely many) discrete valuation rings $(B, (v), \ell)$ of L lying over A , we have that $\kappa \subset \ell$ is separable and $\operatorname{Char} \kappa = p$ does not divide the ramification index of the extension $A \subset B$.⁷ If the extensions $A \subset B$ are étale, we say L/K is *étale with respect to A* .

Definition 3.2 (tamely ramified covers with respect to a divisor). Let X be a connected normal scheme and let $D = \sum_i P_i$ be a reduced effective divisor on X with prime components P_i . One says that a finite cover $Y \rightarrow X$ is *tamely ramified with respect to D* (or *simply over D*) if Y is normal and every connected component $Y' \rightarrow Y \rightarrow X$ of Y is a finite cover X that is étale away from D , and $K(Y')/K(X)$ is tamely ramified with respect to the DVRs \mathcal{O}_{X, η_i} , where η_i is the generic point of P_i .

The following lemma will be important in our forthcoming discussions.

Lemma 3.3 [Grothendieck and Murre 1971, Section 2, Lemma 2.2.8]. *Let $f: Y \rightarrow X$ be a finite cover between connected normal schemes and let $D = \sum_i P_i$ be a reduced divisor on X with prime components P_i . Suppose that $f: Y \rightarrow X$ is étale over the complement of D . The following statements are equivalent:*

⁷The ramification index e is characterized by the equality $u = b \cdot v^e$ with b a unit in B .

- (1) f is a tamely ramified cover with respect to D ,
- (2) For all $x \in D$, the pullback of f along $g: \text{Spec } \mathcal{O}_{X,x} \rightarrow X$ is a tamely ramified cover with respect to g^*D .
- (3) For all $x \in D$, the pullback of f along $g: \text{Spec } \mathcal{O}_{X,x}^{\text{sh}} \rightarrow X$ is a tamely ramified cover with respect to g^*D .
- (4) For all $x \in D$ of codimension 1 (in X), the pullback of f along $g: \text{Spec } \mathcal{O}_{X,x} \rightarrow X$ is a tamely ramified cover with respect to g^*D .
- (5) For all $x \in D$ of codimension 1 (in X), the pullback of f along $g: \text{Spec } \mathcal{O}_{X,x}^{\text{sh}} \rightarrow X$ is a tamely ramified cover with respect to g^*D .

Definition-Proposition 3.4 (Kummer-type cyclic covers, see [Grothendieck and Murre 1971, Example 2.2.4]). *Let (X, D) be as in Definition 3.2 and defined over $\mathbb{Z}[1/n][\zeta]$ where ζ is a primitive n -th root of unity, which means that $n \in \Gamma(X, \mathcal{O}_X)$ is invertible and $\Gamma(X, \mathcal{O}_X)$ contains a primitive n -th root of unity (e.g., X may be defined over a separably closed field of characteristic prime to n). Suppose that $D = n \cdot E$ in $\text{Cl } X$ and E is Cartier away from D . Write $\text{div}_X \kappa + n \cdot E = D$ for some $\kappa \in K(X)^\times$. Then, the finite cover $f: Y \rightarrow X$ determined by the \mathcal{O}_X -algebra*

$$\mathcal{O}_X \xrightarrow{\subset} \bigoplus_{i=0}^{n-1} \mathcal{O}_X(-i \cdot E), \quad \cdot \kappa: \mathcal{O}_X(-n \cdot E) \rightarrow \mathcal{O}_X(-D)$$

is a connected tamely ramified cover over D that is generically cyclic of degree n . We refer to these covers as **Kummer-type cyclic covers** or simply as **Kummer covers** when E and so D are principal divisors. We allow $n = 0$ to include the trivial cover.

Proof. Note that, over $U := X \setminus D$, the cover $Y \rightarrow X$ is the element of $H^1(U, \mu_n)$ corresponding to $\text{div}_U \kappa + n \cdot E|_U = 0$ as $E|_U \in \text{Pic } U$. In particular, $Y|_U \rightarrow U$ is a $\mathbb{Z}/n\mathbb{Z}$ -torsor (as $\zeta \in \Gamma(X, \mathcal{O}_X)$) and in particular étale; see [Milne 1980, III, Section 4, pages 125–126]. Next, we explain why Y is normal. Note that, since f is affine, \mathcal{O}_Y satisfies the (\mathbf{S}_2) condition as so does the \mathcal{O}_X -module $f_*\mathcal{O}_Y = \bigoplus_{i=0}^{n-1} \mathcal{O}_X(-i \cdot E)$. To see why Y satisfies (\mathbf{R}_1) , it suffices to look at those codimension 1 points not lying over (the generic point of) the P_i 's as f is étale away from D . That is, it suffices to check that the \mathcal{O}_{X,P_i} -algebras $\mathcal{O}_{X,P_i} \otimes_{\mathcal{O}_X} f_*\mathcal{O}_Y$ are regular for all i . Observe that $\mathcal{O}_{X,P_i} \otimes_{\mathcal{O}_X} f_*\mathcal{O}_Y \cong \mathcal{O}_{X,P_i}[T]/(T^n - t)$ where t is a uniformizer of \mathcal{O}_{X,P_i} , and further $\mathcal{O}_{X,P_i}[T]/(T^n - t)$ is local with maximal ideal $(t) \oplus \bigoplus_{i=1}^{n-1} \mathcal{O}_{X,P_i} \cdot T = (T)$ and so regular. This computation further shows that $\mathcal{O}_{X,P_i} \otimes_{\mathcal{O}_X} f_*\mathcal{O}_Y$ is an extension of DVRs with ramification index n , which is prime to all residual characteristics of X as $1/n \in \Gamma(X, \mathcal{O}_X)$. This proves that Y is normal.

It remains to prove that Y is connected/integral, for which it suffices to show that $K(X) \otimes_{\mathcal{O}_X} f_*\mathcal{O}_Y$ is a field. Notice that, $K(X) \otimes_{\mathcal{O}_X} f_*\mathcal{O}_Y \cong K(X)[T]/(T^n - \kappa)$. Suppose, for the sake of contradiction, that $K(X)[T]/(T^n - \kappa)$ is not a field. Then, there is $\kappa' \in K(X)^\times$ such that $\text{div } \kappa = \text{div } \kappa'^m$ for some $1 < m \mid n$ (using [Lang 2002, VI, Section 6, Theorem 9.1]); see [Tomari and Watanabe 1992, Corollary 1.9]. Then, $m \cdot (\text{div}_X \kappa' + (n/m)D) = P$, which violates the reducedness of P . \square

Given the equivalence between (a) and (e) in Lemma 3.3, it is of fundamental importance to understand the tamely ramified covers over a strictly local DVR with respect to its uniformizer. In this regard, the following result together with Lemma 3.3 imply that tamely ramified covers are Kummer over the étale-germs at the generic points of the divisor D .

Theorem 3.5 [Serre 1979]. *Let K be a field with a **strictly local** DVR $(A, (u), \mathfrak{k})$ with $\text{Char } \mathfrak{k} = p \geq 0$. Then, every Galois field extension L/K that is tamely ramified with respect to A is Kummer, i.e., $L = K(u^{1/n})$ for some n prime to p , and in particular cyclic. In other words, every Galois tamely ramified cover over $X = \text{Spec } A$ with respect to $\text{div } u$ is Kummer.*

Proof. See [Serre 1979, Chapter IV, Section 2, Proposition 8] for the case $p = 0$. For characteristic $p > 0$, note that, by tameness and \mathfrak{k} being separably closed, we have $p \nmid [L : K]$. One simply replaces the use of Corollary 2 in [loc. cit.] with Corollary IV, Sections 2 and 3. \square

Remark 3.6. The intuition behind Theorem 3.5 is the following; see [Milne 1980, I, Example 5.2(e)]. We think of $\text{Spec } K \cong \text{Spec } A \setminus \{(u)\}$ as an algebraic analog of the punctured disc in the plane, then this result says that $\pi_1^{\text{ét}}(\text{Spec } K)$ is isomorphic to $\hat{\mathbb{Z}}$ — the profinite completion of \mathbb{Z} — at least if the residual characteristic is 0 else what we can say is $\pi_1^{\text{ét}}(\text{Spec } K) \cong \hat{\mathbb{Z}}^{(p)}$.

As mentioned before, Theorem 3.5 tells us that tamely ramified covers over a reduced effective divisor are of a very special type étale-locally around the generic points of the divisor. In case the divisor D in Definition 3.2 has *normal crossings* [Grothendieck and Murre 1971, Section 1.8], *Abhyankar’s lemma* establishes that the same hold at all *special* points in the support of the divisor; see [Grothendieck and Murre 1971, Section 2.3; SGA 1 1971, Exposé XIII, Section 5]. More precisely:

Theorem 3.7 (Abhyankar’s lemma). *With notation as in Definition 3.2, suppose additionally that (X, D) has normal crossings in the sense of [Grothendieck and Murre 1971, Section 1.8]. Then, the connected components of the pullback of $Y \rightarrow X$ along $\text{Spec } \mathcal{O}_{X, \bar{x}}^{\text{sh}} \rightarrow X$ are (quotients) of Kummer covers for all geometric points $\bar{x} \rightarrow X$.*

We are interested in studying tame cover with respect to divisors that may not have normal crossings. Fortunately, our efforts will lead to a generalization of this result when the divisor D is irreducible yet singular; see Lemma 3.34. Following [Kerz and Schmidt 2010; Chinburg et al. 1996], we have a stronger notion of tameness.

Definition 3.8 (cohomological tameness). Let U be a normal connected scheme equipped with a dense open embedding $U \rightarrow X$ with X normal and connected.⁸ We say that a finite Galois cover $V \rightarrow U$ is *cohomologically tamely ramified with respect to X* if its integral closure $f : Y \rightarrow X$ is so that the trace map $\text{Tr}_{Y/X} : f_* \mathcal{O}_Y \rightarrow \mathcal{O}_X$ is surjective. A finite étale cover $V \rightarrow U$ is cohomologically tamely ramified if it can be dominated by a Galois one.

⁸Unlike [Kerz and Schmidt 2010], we do not require X to be proper over some field.

3B. Tame Galois categories and their fundamental groups. Consider the setup:

Setup 3.9. Let $(R, \mathfrak{m}, \kappa, K)$ be a strictly local normal domain of dimension at least 2. Let Z be a closed subscheme of $X := \text{Spec } R$ of codimension at least 2. We consider a prime Weil divisor P on $X^\circ := X \setminus Z$, which extends to a unique prime divisor on X that we also denote by P , then P corresponds to a unique height-1 prime ideal $\mathfrak{p} \subset R$. We set $U := X^\circ \setminus P$. We further set $p := \text{Char } \kappa \geq 0$ and assume that $p \in \mathfrak{p} \subset \mathfrak{m}$, so that $\text{Char } K(P) = p = \text{Char } \kappa$ (here, $K(P)$ is the function field of P , i.e., the residue field of $R_{\mathfrak{p}}$). In particular, after choosing an embedding $\overline{\mathbb{F}}_p \subset \kappa$, we have that $(R, \mathfrak{m}, \kappa, K)$ is a local algebra over \mathbb{Z}_p^{sh} — the maximal unramified extension of \mathbb{Z}_p , which is given by adjoining all prime-to- p roots of unity to \mathbb{Z}_p . Of course, this is just a fancy way to say that R contains all the n -th roots of unity if $p \nmid n$. In particular, we allow $\mathbb{Z}_p^{\text{sh}} \rightarrow R$ to be injective, i.e., R may be of mixed characteristic in this section. However, we are assuming that $R_{\mathfrak{p}}$ has the same (mixed or not) characteristic as R .

We study two types of tame Galois categories in this paper which we introduce next. We invite the reader to consult [Murre 1967; Cadoret 2013] for a thorough exposition on Galois categories and fundamental groups, or the classic, original reference [SGA 1 1971, Exposé V].

3B1. The cohomologically tame Galois category. Working in Setup 3.9, the first tame fundamental group of interest is the fundamental group $\pi_1^{\text{t},X}(X^\circ)$ classifying the Galois category $\text{F}\acute{\text{E}}\text{t}^{\text{t},X}(X^\circ)$ of covers over X° that are cohomologically tamely ramified with respect to X . The minimal (or connected) objects of this Galois category are the local finite extensions $(R, \mathfrak{m}, \kappa, K) \subset (S, \mathfrak{n}, \ell, L)$ such that S is a normal domain, $\text{Tr}_{S/R}: S \rightarrow R$ is surjective, and $R \subset S$ is étale over X° . Thus, $\pi_1^{\text{t},X}(X^\circ) = \varprojlim \text{Gal}(L/K)$ where the limit runs over all Galois extensions L/K inside a fixed separable closure of K such that the integral closure of R in L ; say R^L/R , is étale over X° and $\text{Tr}: R^L \rightarrow R$ is surjective; see [Carvajal-Rojas et al. 2018, Section 2.4].

3B2. The tame Galois category of a prime divisor. In this section, the perspective is quite different from the one above. Working in Setup 3.9, consider the Galois category $\text{Rev}^P(X^\circ)$ of finite covers over X° that are tamely ramified with respect to P . The corresponding fundamental group is denoted by $\pi_1^{\text{t},P}(X^\circ)$ (we choose a geometric generic point as our base point, which is suppressed from the notation). As before, we may restrict ourselves to a local algebra setup as the following remark explains.

Remark 3.10 (reduction to local algebra). Since R is a strictly local normal domain, the Galois objects of the category $\text{Rev}^P(X^\circ)$ are the (generically) Galois local finite extensions of normal domains $(R, \mathfrak{m}, \kappa, K) \subset (S, \mathfrak{n}, \ell, L)$ that are étale over U but tamely ramified over P (i.e., L/K is tamely ramified with respect to $R_{\mathfrak{p}}$). In this way,

$$\pi_1^{\text{t},P}(X^\circ) = \varprojlim \text{Gal}(L/K)$$

where the limit runs over all finite Galois extensions L/K inside some fixed separable closure of K such that the integral closure of R in L is tamely ramified over X° with respect to P . When we refer to a cover $Y^\circ \rightarrow X^\circ$ in $\text{Rev}^P(X^\circ)$, we mean that $Y = \text{Spec } S$ with S as above, and $Y^\circ = Y \setminus f^{-1}(Z)$, where $f: \text{Spec } S \rightarrow \text{Spec } R$ is the corresponding morphism.

Example 3.11 (Kummer-type cyclic covers). Suppose that there is a divisor D on X such that $P = n \cdot D$ in $\text{Cl } X$ and so that $D|_U$ is Cartier. Writing, $\text{div } \kappa + nD = P$, let $S = \Gamma(Y, \mathcal{O}_Y) = \bigoplus_{i=0}^{n-1} R(-iD)$ with $f : Y \rightarrow X$ as in Definition-Proposition 3.4. Let $\mathfrak{n} := \mathfrak{m} \oplus \bigoplus_{i=1}^{n-1} R(-iD)$ and $\mathfrak{q} := \mathfrak{p} \oplus \bigoplus_{i=1}^{n-1} R(-iD)$. One readily sees that these two are ideals of S . In fact, $S/\mathfrak{n} = R/\mathfrak{m} = \kappa$ and $S/\mathfrak{q} = R/\mathfrak{p}$, thereby \mathfrak{n} is maximal and \mathfrak{q} is prime. Moreover, $\mathfrak{n} \cap R = \mathfrak{m}$, $\mathfrak{q} \cap R = \mathfrak{p}$, and $\mathfrak{n}, \mathfrak{q}$ are, respectively, the only primes of S with such property. Further, we have that $\text{ht } \mathfrak{q} = 1$. Indeed, $\text{ht } \mathfrak{q} \leq \text{ht}(\mathfrak{q} \cap R) = \text{ht } \mathfrak{p} = 1$ from integrality of S/R (going-up theorem) and S being a domain rules out the possibility $\text{ht } \mathfrak{q} = 0$ (as clearly $\mathfrak{q} \neq 0$). Thus, $Q = V(\mathfrak{q})$ is a prime divisor on Y . Putting everything together, $(R, \mathfrak{m}, \kappa, K, \mathfrak{p}) \subset (S, \mathfrak{n}, \kappa, K(\kappa^{1/n}), \mathfrak{q})$ defines a cyclic cover in $\text{Rev}^P(X^\circ)$ whose pullback to $R_{\mathfrak{p}}$ is Kummer; see the proof of Definition-Proposition 3.4.

If $\mathfrak{p} = (r)$ is principal, then $\text{div } \kappa + nD = \text{div } r$ and so D is torsion, say of index $m \mid n$. In particular, we may use this to define a connected quasiétale cover $g : W \rightarrow X$ of degree m trivializing D . Then, it follows that the base change $f_W : Y_W \rightarrow W$ is a Kummer cover of the form $\text{Spec } \mathcal{O}_W[T]/(T^n - r) \rightarrow W$. Indeed, after trivializing D , say $D = \text{div } s$, the equality $\text{div } \kappa + n \text{div } s = \text{div } r$ says that $r = us^n \kappa$ for some unit $u \in \Gamma(W, \mathcal{O}_W)$. Then, since $\Gamma(W, \mathcal{O}_W)$ is also strictly henselian, we may say that $u = 1$ by replacing s by $u^{-1/n}s$. Thus, $L(r^{1/n}) = L(\kappa^{1/n})$, where L is the function field of W .

3C. Some examples of tamely ramified covers. In this section, we provide some examples illustrating what may go wrong in Abhyankar’s lemma if the divisor in question is too singular. Additionally, we consider instructive to have some examples at hand that we may use across the forthcoming sections to highlight particular features of our results. We will employ the following useful fact throughout.

Proposition 3.12 [Stacks 2005–, Lemma 09EB]. *Let R be a normal domain with fraction field K . Let L/K be a finite Galois extension of degree d , and let S be the integral closure of R in L . Fix a height 1 prime ideal $\mathfrak{p} \subset R$, and let $\mathfrak{q}_1, \dots, \mathfrak{q}_n \subset S$ be the list of distinct prime ideals of S lying over \mathfrak{p} . Then, all the DVR extensions $R_{\mathfrak{p}} \rightarrow S_{\mathfrak{q}_i}$ share the same ramification index e and residual degree i . Moreover, the formula $d = n \cdot e \cdot i$ holds.*

Terminology 3.13. We shall often refer to i in Proposition 3.12 as the *inertial degree*.

Example 3.14 (the cusp). Let $(R, \mathfrak{m}, \kappa, K)$ be a regular local ring with regular system of parameters $\mathfrak{m} = (x, y)$. We assume $\text{Char } \kappa \neq 2, 3$. Let L be the splitting field of $T^3 + xT + y \in K[T]$. This polynomial is irreducible.⁹ Let $t_1, t_2, t_3 \in L$ be the distinct roots of $T^3 + xT + y$. Setting,

$$\delta := (t_1 - t_2)(t_2 - t_3)(t_1 - t_3)$$

we have that $\delta^2 = -4x^3 - 27y^2 =: \Delta$. In particular, $\delta \notin K$ for Δ is irreducible in R . Therefore, L/K is a Galois extension of degree 6 with $\text{Gal}(L/K) \cong S_3$ — the symmetric group; see [Roman 2006, Section 7.5] or [Lang 2002, VI, Section 2]. In fact, $K(\delta)$ is the fixed field of the (cyclic) alternating group $A_3 \subset S_3$.

⁹Indeed, if it were reducible, it would admit a root in K and further in R by normality of R . In that case, $y = t(t^2 + x)$ for some $t \in R$. Since R is a UFD and y is an irreducible element, this implies that either t or $t^2 + x$ is a unit, and *a fortiori* both are units implying further that y is a unit, which is a contradiction.

Thus, $L = K(\delta, t_1)$ and

$$L = K(\delta)[T]/(T^3 + xT + y).$$

In fact, a direct computation shows that if t is one of the roots then the remaining roots are:

$$\frac{-t}{2} \pm \frac{\delta}{2(3t^2 + x)},$$

where $3t^2 + x \neq 0$ as the minimal polynomial of t over K has degree 3.¹⁰

We set $t = t_1$, and set t_2 to be the root with the positive sign in the above expression. Let S be the integral closure of R in L . Of course, $S \ni \delta, t_1, t_2, t_3$. Then, we have:

Claim 3.15. *$R \subset S$ is a tamely ramified extension with respect to the prime divisor $D = \text{div } \Delta$. Moreover, there are exactly three prime divisors of S lying over (Δ) , with ramification index $e = 2$ and inertial degree $i = 1$.*

Proof of claim. By Definition-Proposition 3.4, the integral closure of R in $K(\delta)$ is $R[\delta]$, so that S is the integral closure of $R[\delta]$ in L . On the other hand, we may consider the flat extension of degree 3

$$R[\delta] \subset R[\delta, t] \cong R[\delta][T]/(T^3 + xT + y).$$

Notice that the discriminant ideal of this extension is (Δ) whereas the different ideal is $(3t^2 + x)$. Therefore, $R \subset R[\delta, t]$ is étale away from D and so $R[\delta, t]_{\delta} = R[\delta, \delta^{-1}, t]$ is normal. In particular, the extension $R[\delta, t] \subset S$ is an equality after localizing at δ (or well at $3t^2 + x$). Thus, the extension $R_{\Delta} \subset S_{\Delta}$ is étale. By Lemma 3.3, we are left with showing $R_{(\Delta)} \rightarrow S_{(\Delta)}$ is a tamely ramified extension. To this end, observe that

$$\Delta = \delta^2 = (t_1 - t_2)^2(t_2 - t_3)^2(t_1 - t_3)^2.$$

Now, let $\mathfrak{q} \subset S$ be a prime ideal lying over (Δ) . It must then contain at least one of the elements $t_1 - t_2, t_2 - t_3, t_1 - t_3$. We argue next it can contain only one of them. Indeed, if it contains two of them it must contain the third one and thus all of them.¹¹ In particular, the ramification index of $R_{(\Delta)} \rightarrow S_{\mathfrak{q}}$ is at least 6 and by applying Proposition 3.12 we conclude that $n = 1, e = 6$, and $i = 1$ (with notation as in Proposition 3.12). In particular, \mathfrak{q} is generated by either of these elements. On the other hand, we have that

$$t_1 - t_2 = \frac{3t(3t^2 + x) - \delta}{2(3t^2 + x)}, \quad t_1 - t_3 = \frac{3t(3t^2 + x) + \delta}{2(3t^2 + x)}, \quad t_2 - t_3 = \frac{2\delta}{2(3t^2 + x)}. \quad (3.15.1)$$

From this, we conclude that all the displayed numerators belong to \mathfrak{q} and so does $6t(3t^2 + x)$. Nonetheless, $\mathfrak{q} \not\ni t$ as otherwise $y = -t(t^2 + x) \in \mathfrak{q} \cap R = (\Delta)$, which is not the case. In this way, our conclusion must

¹⁰In case the reader wants to corroborate this assertion by hand, notice that $T^3 + xT + y = (T - t)(T^2 + tT + t^2 + x)$. Hence, it suffices to verify that these are roots of $T^2 + tT + t^2 + x = (T + t/2)^2 + (3t^2 + 4x)/4$, which in turn boils down to checking $\delta^2 + (3t^2 + 4x)(3t^2 + x)^2 = 0$, which is a straightforward computation.

¹¹For instance, $t_1 - t_3 = (t_1 - t_2) + (t_2 - t_3)$.

be that $3t^2 + x \in \mathfrak{q} \cap R[\delta, t] = \sqrt{(\delta)}$.¹² This, however, is a contradiction. Indeed, we have that $R[\delta, t]$ is a rank-6 free R module and moreover

$$R[\delta, t] = R \cdot 1 \oplus R \cdot t \oplus R \cdot t^2 \oplus R \cdot \delta \oplus R \cdot \delta t \oplus R \cdot \delta t^2 = \langle 1, t, t^2 \rangle_R \oplus \langle \delta, \delta t, \delta t^2 \rangle_R,$$

whence one sees that any power of $3t^2 + x$ is going to belong to the direct summand $\langle 1, t, t^2 \rangle_R$ whereas

$$(\delta) \subset ((\Delta) \cdot \langle 1, t, t^2 \rangle_R) \oplus \langle \delta, \delta t, \delta t^2 \rangle_R.$$

Additionally, an inductive argument readily shows that the constant coefficient of $(3t^2 + x)^n$ is x^n for every exponent n . Putting everything together, we see that $3t^2 + x \in \sqrt{(\delta)}$ yields that $x^n \in (\Delta)$ for some n and so $x \in (\Delta)$, which is the sought contradiction.

In conclusion, the principal ideals $(t_1 - t_2)$, $(t_2 - t_3)$, $(t_1 - t_3) \subset S$ share no minimal prime. By using Proposition 3.12, we conclude that these are (the) prime ideals of S lying over $(\Delta) \subset R$, with ramification index $e = 2$ and inertial degree $i = 1$. This proves the claim. \square

Example 3.16 (Whitney’s umbrella). Let $(R, \mathfrak{m}, \kappa, K)$ be a regular local ring with κ of *odd characteristic*, and let $f := x^2 - y^2z$ where $\mathfrak{m} = (x, y, z)$ is a regular system of parameters. The polynomial expression $x^2 - y^2z$ plays a fundamental role in the description of degree 4 Galois extensions; see [Lang 2002, VI, Example 4]. Thus, we start off by considering the degree 2 Galois extension $E = K(\sqrt{f})$. Next, we consider the tower of degree 2 Galois extensions

$$E \subset E(\sqrt{z}) \subset E(\sqrt{z})(\sqrt{x + y\sqrt{z}}).$$

Set $\alpha = x + y\sqrt{z}$, $\alpha' = x - y\sqrt{z}$, and $\beta = \sqrt{\alpha}$. The above tower is $E \subset E(\alpha) \subset E(\beta)$. By [loc. cit.], $E(\beta)/E$ is a noncyclic degree 4 Galois extension as $\alpha\alpha' = f$ is a square in E . In fact, $E(\beta)/E$ is the splitting field of $T^4 - 2xT^2 + f \in E[T]$:

$$T^4 - 2xT^2 + f = (T^2 - \alpha)(T^2 - \alpha') = (T - \beta)(T + \beta)(T - \sqrt{f}/\beta)(T + \sqrt{f}/\beta).$$

Moreover, $E(\beta)/K$ is a degree 8 noncyclic Galois extension, for it is the splitting field of $T^4 - 2xT^2 + f \in K[T]$. In fact, setting $\beta' := \sqrt{f}/\beta$, we see that $\text{Gal}(E(\beta)/E)$ is generated by the transpositions $\tau: \beta \mapsto -\beta$ and $\sigma: \beta \mapsto \beta'$. Moreover, in $\text{Gal}(E(\beta)/K)$ we have $\rho: \beta \mapsto \beta$, $\sqrt{f} \mapsto -\sqrt{f}$. In this way, $\pi := \sigma\rho: \beta \mapsto \beta'$, $\sqrt{f} \mapsto -\sqrt{f}$ is an element of order 4 whose square and cube are; respectively, τ and $\rho\sigma$. That is, $\text{Gal}(E(\beta)/K)$ is generated by two elements σ and π satisfying relations $\sigma^2 = 1$, $\pi^4 = 1$, and $\sigma\pi = \pi^3\sigma$. In other words, $\text{Gal}(E(\beta)/K)$ is isomorphic the dihedral group — the symmetries of the square. Thus,

$$\text{Gal}(E(\beta)/K) = \{1, \sigma, \rho, \tau, \pi, \sigma\rho, \pi\sigma, \sigma\tau\}.$$

Let S be the integral closure of R in $E(\beta)$. Next, we claim the following.

Claim 3.17. $S = R[\sqrt{z}, \beta, \beta']$

¹²To see the equality, consider $\mathfrak{t} \subset R[\delta, t]$ to be a minimal prime of (δ) . Since $R[t, \delta] \subset S$ is integral, there is at least one prime ideal of S lying over \mathfrak{t} . However, any such a prime must lie over $(\Delta) \subset R$ and so must do \mathfrak{q} .

Proof of claim. By Definition-Proposition 3.4, $R[\sqrt{f}, \sqrt{z}]$ is normal and so it is the integral closure of R in $E(\alpha)$ — the fixed field of $\langle \tau \rangle$. Thus, we just need to prove that S is the integral closure of $R[\sqrt{f}, \sqrt{z}]$ in $E(\beta)$. To this end, we prove that any element $\gamma \in S$ is an $R[\sqrt{f}, \sqrt{z}]$ -linear combination of $1, \beta$, and β' . We know that $\gamma = a + b\beta \in E(\beta)$ for some (uniquely determined) $a, b \in E(\alpha)$. Since $E(\beta)/E(\alpha)$ is a quadratic extension, the minimal polynomial of γ is described in terms of its trace and norm as follows:

$$T^2 + \operatorname{Tr}_{E(\beta)/E(\alpha)}(\gamma)T + \operatorname{N}_{E(\beta)/E(\alpha)}(\gamma).$$

Observe that $\operatorname{Tr}_{E(\beta)/E(\alpha)}(\gamma) = 2a$ and $\operatorname{N}_{E(\beta)/E(\alpha)}(\gamma) = a^2 - b^2\alpha$. Therefore, $\gamma \in S$ if and only if both $2a$ and $a^2 - b^2\alpha$ belong to $R[\sqrt{f}, \sqrt{z}]$, which is equivalent to $a, b^2\alpha \in R[\sqrt{f}, \sqrt{z}]$.

Now, since $b^2\alpha$ belongs to $R[\sqrt{f}, \sqrt{z}]$ so does $b^2f = b^2\alpha\alpha'$. That is, since $b^2\alpha \in R[\sqrt{f}, \sqrt{z}]$, then b^2f belongs to the ideal $(\alpha') \subset R[\sqrt{f}, \sqrt{z}]$. Since $b^2f = (b\sqrt{f})^2$, this is to say that $b\sqrt{f} \in E(\alpha)$ is integral over $(\alpha') \subset R[\sqrt{f}, \sqrt{z}]$. Given that $R[\sqrt{f}, \sqrt{z}]$ is integrally closed in $E(\alpha)$, we conclude that $b\sqrt{f} \in \sqrt{(\alpha')} \subset R[\sqrt{f}, \sqrt{z}]$; see [Kunz 2013, Chapter 2, Corollary 2.6]. The result then follows once we have shown that

$$\sqrt{(\alpha')} = (\alpha', \sqrt{f}), \quad \text{in } R[\sqrt{f}, \sqrt{z}]. \quad (3.17.1)$$

Indeed, granted (3.17.1), we would have that

$$\gamma = a + b\beta = a + (b\sqrt{f})\frac{\beta}{\sqrt{f}} = a + (c\alpha' + d\sqrt{f})\frac{\beta}{\sqrt{f}} = a + d\beta + c\frac{\alpha'}{\beta'} = a + d\beta + c\beta',$$

for some $d, c \in R[\sqrt{f}, \sqrt{z}]$ — we saw before that $a \in R[\sqrt{f}, \sqrt{z}]$.

To prove (3.17.1), observe that the containment from right to left is clear, for $\sqrt{f}^2 = \alpha\alpha'$. For the converse containment, observe that $R[\sqrt{f}, \sqrt{z}]$ is free over R with basis $1, \sqrt{z}, \sqrt{f}, \sqrt{z}\sqrt{f}$. In particular, if an element in $R[\sqrt{f}, \sqrt{z}]$ belongs to $\sqrt{(\alpha')}$ then so does the summand in the R -span of 1 and \sqrt{z} . Thus, it is enough to prove that $r + s\sqrt{z} \in \sqrt{(\alpha')}$; with $r, s \in R$, belongs to (α') . That is, it suffices to explain why the contraction of $\sqrt{(\alpha')} \subset R[\sqrt{f}, \sqrt{z}]$ to $R[\sqrt{z}]$ is the ideal (α') . This, however, follows from observing that $(\alpha') \subset R[\sqrt{z}]$ is a prime ideal. Indeed, observe that $R[\sqrt{z}]$ is a regular local ring (and so an UFD) as its maximal ideal is given by $\mathfrak{m} \oplus R \cdot \sqrt{z} = (x, y, z, \sqrt{z}) = (x, y, \sqrt{z})$. On the other hand, the extension of the prime ideal $(f) \subset R$ to $R[\sqrt{z}]$ splits as $(f) = (\alpha)(\alpha')$. Since there cannot be more than two prime ideals of $R[\sqrt{z}]$ lying over $(f) \subset R$, we conclude that these are (α) and (α') . \square

Claim 3.18. *The extension $R \subset S$ is tamely ramified with respect to the reduced divisor $D = \operatorname{div} z + \operatorname{div} f$. Moreover, for both prime divisors $(z), (f) \subset R$, there are exactly two prime ideals of S lying over with ramification index 2 and inertial degree 2.*

Proof of claim. We begin by proving that $R_{zf} \subset S_{zf}$ is étale. Indeed, we have a tower $R \subset R[\sqrt{f}, \sqrt{z}] \subset S$ where the bottom extension is flat of degree 4. One readily verifies that the discriminant ideal of the bottom extension is (zf) , so it is étale over R_{zf} . It suffices to check that $R[\sqrt{f}, \sqrt{z}]_{zf} \subset S_{zf}$ is étale. To this end, notice that by inverting f we invert α and α' in $R[\sqrt{f}, \sqrt{z}]$ and β and β' in S , for we have the relation

$\alpha\alpha' = f = \beta^2\beta'^2$. In particular, $1/\alpha \in R[\sqrt{f}, \sqrt{z}]_{zf}$ and $1/\beta \in S_{zf}$. Therefore, $R[\sqrt{f}, \sqrt{z}]_{zf} \subset S_{zf}$ is free with basis $1, \beta$ (as $\beta' = \sqrt{f}/\beta = \sqrt{f}/\alpha\beta$) and its discriminant ideal is generated by

$$\begin{vmatrix} 1 & 1 \\ \beta & -\beta \end{vmatrix}^2 = (-2\beta)^2 = 4\alpha,$$

which is a unit and consequently the extension is étale; as needed.

It remains to prove that $E(\beta)/K$ is tamely ramified with respect to both DVRs $R_{(z)}$ and $R_{(f)}$. Nevertheless, this follows from simple characteristic considerations. Indeed, since the extensions are Galois, we know in each case that $8 = n \cdot e \cdot i$ with n being the number of primes lying over, e the ramification indexes, and i the residual degrees; as in Proposition 3.12. Then, e and i are necessarily prime to characteristic, which was assumed odd from the beginning. Recall that $f = \beta^2\beta'^2$. Using Proposition 3.12, this implies that $(\beta), (\beta') \subset S$ are (the) prime ideals of S lying over $(f) \subset R$, and the ramification index is 2 as well as the residual degree.¹³ Similarly, we have that $2y\sqrt{z} = (\beta - \beta')(\beta + \beta')$, so that $4y^2z = (\beta - \beta')^2(\beta + \beta')^2$. Therefore, $(\beta - \beta'), (\beta + \beta') \subset S$ are (the) two prime ideals of S lying over $(z) \subset R$, with ramification index and inertial degree equal to 2.¹⁴ □

Example 3.19. We may specialize Example 3.16 by setting $y = 1$. More precisely, we may consider $(R, \mathfrak{m}, \zeta, K)$ to be a regular local ring of odd residual characteristic with regular system of parameters $\mathfrak{m} = (x, z)$ and set $f := x^2 - z$. Letting L/K be the splitting prime of $T^4 - 2xT^2 + f \in K[T]$, the same arguments *mutatis mutandis* as in Example 3.16 show that $S := R^L = R[\sqrt{z}, \sqrt{x \pm \sqrt{z}}]$ and moreover that $R \subset S$ is a degree 8 Galois tamely ramified extension over $D = \text{div } z + \text{div } f$. Further, for both (regular) prime divisors $(z), (f) \subset R$ there are exactly two prime of S lying over with ramification and inertial indexes equal to 2.

Remark 3.20 (failure of Abhyankar’s lemma for divisors without normal crossings). Observe that Examples 3.14, 3.16 and 3.19 are counterexamples for Abhyankar’s lemma if no regularity condition is imposed on the divisor. Indeed, in each case, we may consider R to be additionally strictly local, then it admits a tamely ramified cover (e.g., S) that is not Kummer (for it is not cyclic). In the cusp case, the divisor D has not normal crossings for it is cut out by a singular (irreducible) equation. In the Whitney’s umbrella case, the divisor has not normal crossings because f is not a regular element in the ring $R_{(x,y)}^{\text{sh}}$ as $f = x^2 - y^2z = (x - y\sqrt{z})(x + y\sqrt{z})$ in this ring. In the case of Example 3.19, we have that z and f are both regular elements yet $R/(z, f)$ is not regular as $(z, f) = (z, x^2)$.

3D. Main formal theorems. Next, we explain why our main results on $\pi_1^{t,P}(X^\circ)$ can be seen as formal consequences of some interesting properties of the Galois category $\text{Rev}^P(X^\circ)$. With notation as in Setup 3.9, to a Galois object $f: Y^\circ \rightarrow X^\circ$ in $\text{Rev}^P(X^\circ)$ of degree d_f we may associate three positive integers n_f, e_f , and i_f which are subject to the relation $d_f = n_f \cdot e_f \cdot i_f$; see Proposition 3.12. With this in mind:

¹³To see that these two ideals are different, note that otherwise would imply that $(\alpha) = (\alpha')$ in $R[\sqrt{z}]$, which is tantamount to say that $(f) \in \text{Spec } R$ is a branch point of $R \subset R[\sqrt{z}]$. This, however, is not the case.

¹⁴Notice that $(\beta - \beta') \neq (\beta + \beta')$ in S as otherwise this would yield that the common ideal contains both (β) and (β') , which is absurd as then they are all the same ideal.

Terminology 3.21. Working in Setup 3.9, we consider the following properties on $\text{Rev}^P(X^\circ)$:

- (1) *P-irreducibility*: Every connected cover $f : Y^\circ \rightarrow X^\circ$ in $\text{Rev}^P(X^\circ)$ satisfies that $Q := (f^{-1}(P))_{\text{red}}$ is a prime divisor on Y° . In other words, with notation as in Remark 3.10, there is exactly one prime, say \mathfrak{q} , lying over \mathfrak{p} in the extension $R \subset S$. If f is Galois, this means $n_f = 1$.
- (2) *inertial boundedness*: There exists $N \in \mathbb{N}$ such that $i_f \leq N$ for all Galois objects $f : Y^\circ \rightarrow X^\circ$ in $\text{Rev}^P(X^\circ)$.
- (3) *inertial tameness*: The inertial degree i_f is prime-to- p for all Galois objects $f : Y^\circ \rightarrow X^\circ$ in $\text{Rev}^P(X^\circ)$.
- (4) *inertial decantation*: Assuming the P -irreducibility of $\text{Rev}^P(X^\circ)$, inertial decantation means that every Galois cover $f : Y^\circ \rightarrow X^\circ$ in $\text{Rev}^P(X^\circ)$ dominates a quasiétale Galois cover $Y'^\circ \rightarrow X^\circ$ in $\text{Rev}^P(X^\circ)$ whose generic degree is the generic degree of $Q := (f^{-1}(P))_{\text{red}} \rightarrow P$. Equivalently, with notation as in Remark 3.10, if $\mathfrak{q} \subset S$ is the only prime lying over \mathfrak{p} , there is a factorization $(R, \mathfrak{m}, \kappa, K; \mathfrak{p}) \subset (S', \mathfrak{n}', \ell', L'; \mathfrak{q}') \subset (S, \mathfrak{n}, \ell, L; \mathfrak{q})$ such that the bottom extension induces an étale-over- P (i.e., quasiétale) cover in $\text{Rev}^P(X^\circ)$ and $[\kappa(\mathfrak{q}') : \kappa(\mathfrak{p})] = [L' : K] = [\kappa(\mathfrak{q}) : \kappa(\mathfrak{p})]$. When the latter degree is 1, we say that f is *totally ramified*.

Remark 3.22. If $\text{Rev}^P(X^\circ)$ is P -irreducible, we may think of the covers in $\text{Rev}^P(X^\circ)$ as local extensions $(R, \mathfrak{m}, \kappa, K; \mathfrak{p}) \subset (S, \mathfrak{n}, \ell, L; \mathfrak{q})$; as in Remark 3.10, where \mathfrak{q} is the only (height 1) prime ideal of S lying over \mathfrak{p} . We follow the convention to denote the prime divisor corresponding to \mathfrak{q} by Q and so on. Note that, if $f : Y^\circ \rightarrow X^\circ$ is a connected cover in $\text{Rev}^P(X^\circ)$, then the category $\text{Rev}^Q(Y^\circ)$ is Q -irreducible and $\text{Rev}^Q(Y^\circ)$ is the Galois category given by the objects of $\text{Rev}^P(X^\circ)$ that lie over (or dominate) the object (Y°, Q) . If f is further Galois, then $\text{Rev}^Q(Y^\circ)$ is inertially bounded (resp. tame) if so is $\text{Rev}^P(X^\circ)$.

Lemma 3.23. *P-irreducibility implies inertial decantation.*

Proof. With notation as in Remark 3.10, since \mathfrak{q} is the only prime lying over \mathfrak{p} , its decomposition group $D := \{\sigma \in \text{Gal}(L/K) \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$ is the whole Galois group $\text{Gal}(L/K)$. Therefore, its inertia group I sits as the kernel in the following short exact sequence of groups

$$1 \rightarrow I \rightarrow \text{Gal}(L/K) \rightarrow \text{Aut}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) \rightarrow 1.$$

By the tameness of the ramification, $\kappa(\mathfrak{q})/\kappa(\mathfrak{p})$ is a finite separable extension and so Galois by [Stacks 2005–, Lemma 09ED]. Thus, we have

$$1 \rightarrow I \rightarrow \text{Gal}(L/K) \rightarrow \text{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p})) \rightarrow 1.$$

We may use the Galois correspondence to obtain a factorization

$$(R, \mathfrak{m}, \kappa, K, P) \subset (S^I, \mathfrak{n}^I, \ell^I, L^I, Q^I) \subset (S, \mathfrak{n}, \ell, L, Q)$$

where both covers are Galois and the upper script I denotes the invariant or fixed elements under the action of I . Moreover, $\text{Gal}(L^I/K) = \text{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$ and the bottom extension is étale at \mathfrak{q}^I ; see [Stacks

2005–, Lemma 09EH], and so quasiétale. Furthermore, $[\kappa(q^I) : \kappa(\mathfrak{p})] = [L^I : K] = [\kappa(q) : \kappa(\mathfrak{p})]$. This proves the lemma. \square

Definition-Proposition 3.24. *In the situation of Setup 3.9, the full subcategory $\text{Rev}_{1,\text{ét}}^P(X^\circ)$ of $\text{Rev}^P(X^\circ)$ consisting of those $Z^\circ \rightarrow X^\circ$ that are étale-over- P is a Galois subcategory. We denote the corresponding fundamental group by $\pi_{1,\text{ét}}^P(X^\circ)$.*

Proof. We follow the proof of [Grothendieck and Murre 1971, Theorem 2.4.2] and only need to verify the conditions G1, G2 and G3 of [SGA 1 1971, Exposé V, 4]. Clearly, X° itself is a final object. For the existence of fiber products, take $Y^\circ \rightarrow Z^\circ, W^\circ \rightarrow Z^\circ$ in $\text{Rev}(X^\circ)$ and consider the following diagram:

$$\begin{array}{ccccc} (Y^\circ \times_{Z^\circ} W^\circ)_{\text{nor}} & \longrightarrow & Y^\circ \times_{Z^\circ} W^\circ & \longrightarrow & Y^\circ \\ & & \downarrow & & \downarrow \\ & & W^\circ & \longrightarrow & Z^\circ \end{array}$$

where the normalization is taken with respect to the total ring of fractions of $Y^\circ \times_{Z^\circ} W^\circ$. By [loc. cit.], this is the fiber product in $\text{Rev}^P(X^\circ)$. Note that $Y^\circ \times_{Z^\circ} W^\circ$ is étale over P since étale morphisms are stable under base change. Moreover, as étale morphisms preserve normality (and X° is normal), we conclude that $Y^\circ \times_{Z^\circ} W^\circ \rightarrow X^\circ$ is normal at P and thus the normalization is an isomorphism at P . The existence of direct sums is clear. Consider now $Y^\circ \rightarrow X^\circ$ a morphism in $\text{Rev}^P(X^\circ)$, G a finite subgroup of $\text{Aut}(Y^\circ)$. Then,

$$\begin{array}{ccc} Y^\circ & \longrightarrow & Y^\circ/G \\ f \downarrow & \swarrow u & \\ X^\circ & & \end{array}$$

is a commutative diagram in $\text{Rev}^P(X^\circ)$. Assume that f is étale over P . If Q is a point in Y° lying over P with image Q' in Y°/G , we have inclusions of DVRs $\mathcal{O}_{X^\circ,P} \subset \mathcal{O}_{Y^\circ/G,Q'} \subset \mathcal{O}_{Y^\circ,Q}$. Since the inclusion $\mathcal{O}_{X^\circ,P} \subset \mathcal{O}_{Y^\circ,Q}$ is unramified, the first extension is also unramified. Hence, u is étale at P . Condition G3 follows just as in [loc. cit.] \square

Lemma 3.25. *Work in Setup 3.9. Suppose that $\text{Rev}^P(X^\circ)$ is P -irreducible. Then, $\text{Rev}^P(X^\circ)$ inertially bounded if and only if $\text{Rev}_{1,\text{ét}}^P(X^\circ)$ has a universal cover, i.e., $\pi_{1,\text{ét}}^P(X^\circ)$ is finite. If $\tilde{f}: \tilde{X}^\circ \rightarrow X^\circ$ is such universal cover, then $\text{Rev}^{\tilde{P}}(\tilde{X}^\circ)$ is so that its Galois objects have inertial degree equal to 1. If $\text{Rev}^P(X^\circ)$ is further inertially tame, then the order of $\pi_{1,\text{ét}}^P(X^\circ)$ is prime-to- p .*

Proof. Since $\text{Rev}^P(X^\circ)$ is P -irreducible, the degree of a Galois object in $\text{Rev}_{1,\text{ét}}^P(X^\circ)$ coincides with its inertial degree. The first and third statements then follow. The second statement follows from the inertial decantation on $\text{Rev}^{\tilde{P}}(\tilde{X}^\circ)$; see Lemma 3.23 and Remark 3.22. \square

By purity of the branch locus, we only need to check inertial boundedness and/or tameness on the regular locus of X , i.e., $X^\circ = X_{\text{reg}}$. This will play a crucial role in Section 5. We make this precise next but it can be skipped for now.

Proposition 3.26. *Work in Setup 3.9. There is a fully faithful functor between Galois categories $\text{Rev}_{1,\acute{\text{e}}\text{t}}^P(X^\circ) \rightarrow \text{F}\acute{\text{E}}\text{t}(X_{\text{reg}})$, which induces a surjective homomorphism between the corresponding fundamental groups. Moreover, this functor induces an isomorphism between fundamental groups if Z cuts out the singular locus of X .*

Proof. Recall that $\text{F}\acute{\text{E}}\text{t}(X_{\text{reg}})$ is equivalent to the Galois subcategory of the absolute Galois category of K given by finite separable extensions $K \subset L \subset K^{\text{sep}}$ such that the integral closure of $R \subset R^L$ in L is étale over X_{reg} ; see [Carvajal-Rojas et al. 2018, Section 2.4]. On the other hand, as mentioned before in Remark 3.10, $\text{Rev}^P(X^\circ)$ corresponds the Galois subcategory given by field extensions where $R \subset R^L$ is étale over U and L/K is tamely ramified with respect to $R_{\mathfrak{p}}$, whereas $\text{Rev}_{1,\acute{\text{e}}\text{t}}^P(X^\circ)$ is the one in which $R \subset R^L$ is étale over U and L/K is étale with respect to $R_{\mathfrak{p}}$; see Definition 3.1. In particular, $\text{Rev}_{1,\acute{\text{e}}\text{t}}^P(X^\circ)$ is (or can be identified with) a full Galois subcategory of $\text{F}\acute{\text{E}}\text{t}(X_{\text{reg}})$. Indeed, if L/K is in $\text{Rev}_{1,\acute{\text{e}}\text{t}}^P(X^\circ)$ then $R \subset R^L$ is quasi-étale, and so induces an étale cover over X_{reg} by Zariski–Nagata–Auslander purity of the branch locus for regular schemes [Stacks 2005–, Lemma 0BMB]; see [Zariski 1958; Nagata 1958; 1959; Auslander 1962]. Moreover, if $X^\circ = X_{\text{reg}}$ (i.e., Z cuts out the singular locus), we have the same categories as in that case $U \subset X_{\text{reg}}$ and X_{reg} contains the regular point of P . It is worth noticing that the normality of X is essential through the previous arguments. Finally, observe that the remaining statements are formal consequences of the just proven; see [Murre 1967, Chapter 5]. \square

Corollary 3.27. *Work in Setup 3.9. Suppose that $\text{Rev}_{1,\acute{\text{e}}\text{t}}^P(X_{\text{reg}})$ has a universal cover (of prime-to- p degree). Then, $\text{Rev}_{1,\acute{\text{e}}\text{t}}^P(X^\circ)$ has a universal cover (of prime-to- p degree).*

Proof. Proposition 3.26 can be summarized as follows: $\pi_{1,1,\acute{\text{e}}\text{t}}^P(X_{\text{reg}}) \cong \pi_1^{1,\acute{\text{e}}\text{t}}(X_{\text{reg}}) \twoheadrightarrow \pi_{1,\acute{\text{e}}\text{t}}^P(X^\circ)$. Thus, finiteness/tameness on the left-hand side group implies finiteness/tameness on the right-hand one. \square

Definition 3.28. Work in Setup 3.9. Define $N^P(X^\circ) \subset \mathbb{N}$ as the set of prime-to- p positive integers $n \in \mathbb{N}$ for which there is a divisor D on X such that $P - n \cdot D \in \text{Cl } X$ has prime-to- p torsion and $D|_U$ is Cartier. Likewise, define $M^P(X^\circ) \subset \mathbb{N}$ as the set of prime-to- p positive integers $n \in \mathbb{N}$ for which there is a divisor D on X such that $P = n \cdot D \in \text{Cl } X$ and $D|_U$ is Cartier. Note that $1 \in M^P(X^\circ) \subset N^P(X^\circ)$.

With the above in place, we have the following theorem.

Theorem 3.29. *Work in Setup 3.9. Suppose that $\text{Rev}^P(X^\circ)$ is P -irreducible and has bounded inertia. Then, there exists a short exact sequence of topological groups*

$$\hat{\mathbb{Z}}^{(p)} \rightarrow \pi_1^{t,P}(X^\circ) \rightarrow \pi_{1,\acute{\text{e}}\text{t}}^P(X^\circ) \rightarrow 1 \quad (3.29.1)$$

where $\pi_{1,\acute{\text{e}}\text{t}}^P(X^\circ)$ is finite and $\hat{\mathbb{Z}}^{(p)}$ is the prime-to- p part of the profinite completion of \mathbb{Z} (if $p = 0$ we shall agree upon $\hat{\mathbb{Z}}^{(p)} := \hat{\mathbb{Z}}$). If $\text{Rev}^P(X^\circ)$ also has tame inertia, then the order of $\pi_{1,\acute{\text{e}}\text{t}}^P(X^\circ)$ is prime-to- p and the following two statements hold:

- If $P \in \text{Cl } X$ has prime-to- p torsion, (3.29.1) yields a short exact sequence

$$0 \rightarrow \hat{\mathbb{Z}}^{(p)} \rightarrow \pi_1^{\text{t},P}(X^\circ) \rightarrow \pi_{1,\text{ét}}^P(X^\circ) \rightarrow 1 \quad (3.29.2)$$

which splits (in the category of topological groups) if and only if $M^P(X^\circ)$ equals the set of prime-to- p positive integers. Further, the sequence is split if and only if $P = 0 \in \text{Cl } X$.

- If $P \in \text{Cl } X$ is nontorsion, (3.29.1) yields a short exact sequence

$$0 \rightarrow \varprojlim_{n \in N^P(X^\circ)} \mathbb{Z}/n\mathbb{Z} \rightarrow \pi_1^{\text{t},P}(X^\circ) \rightarrow \pi_{1,\text{ét}}^P(X^\circ) \rightarrow 1 \quad (3.29.3)$$

which is split (in the category of topological groups) if and only if $N^P(X^\circ) \supset M^P(X^\circ)$ is an equality and there is a compatible system $\{\frac{1}{n}P \in \text{Cl } X\}_{n \in M^P(X^\circ)}$ of factors of P meaning that $m \cdot (\frac{1}{mn}P) = \frac{1}{n}P$ in $\text{Cl } X$ and $\frac{1}{1}P = P$ (e.g., if $\text{Cl } X$ has no prime-to- p torsion). In particular, if $N^P(X^\circ)$ is finite (e.g., $\text{Cl } X$ modulo prime-to- p torsion is finitely generated), there is a short exact sequence

$$0 \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow \pi_1^{\text{t},P}(X^\circ) \rightarrow \pi_{1,\text{ét}}^P(X^\circ) \rightarrow 1 \quad (3.29.4)$$

and so $\pi_1^{\text{t},P}(X^\circ)$ is finite of order prime-to- p . Likewise, (3.29.4) is split if and only if $P \in \text{Cl } X$ is n -divisible with $\frac{1}{n}P \in \text{Pic } U$.

Remark 3.30. The limit in the kernel of (3.29.3) makes sense because, if $m \cdot M = P = n \cdot N$ in $\text{Cl } X$ modulo prime-to- p torsion (with $p \nmid m, n$ and $M|_U, N|_U \in \text{Pic } U$), then $P = l \cdot (a \cdot N + b \cdot M)$ in $\text{Cl } X$ modulo prime-to- p torsion, where: $(m) \cap (n) = (l)$, $am + bn = k$ and $(m, n) = (k)$. In other words, if m, n belong to $N^P(X^\circ)$ then so does their least common multiple l .

The following two lemmas are well-known to experts but are included for lack of a reference.

Lemma 3.31. Let $\phi: (R, \mathfrak{m}) \rightarrow S$ be a finite extension of normal domains. Denote by S^{sh} the strict henselization of S with respect to a prime \mathfrak{n} lying over \mathfrak{m} . Then, the canonical morphism $\text{Spec } S^{\text{sh}} \rightarrow \text{Spec } S \otimes_R R^{\text{sh}}$ is a connected component, in particular a clopen (i.e., closed and open) immersion. Furthermore, assume that:

- (1) (R, \mathfrak{m}) is a DVR,
- (2) ϕ is a generically étale extension, and
- (3) $\phi_{\mathfrak{n}}: R \rightarrow S_{\mathfrak{n}}$ has trivial residue field extension for all maximal ideals \mathfrak{n} lying over \mathfrak{m} .

Then, all the connected components of $\text{Spec } S \otimes_R R^{\text{sh}}$ arise in this way and then are in bijective correspondence with the prime ideals of S lying over \mathfrak{m} .

Proof. By [Stacks 2005–, Lemma 05WR], S^{sh} is obtained as the localization of a prime ideal of $S \otimes_R R^{\text{sh}}$ lying above \mathfrak{n} and \mathfrak{m}^{sh} . Since S is normal and $\text{Spec } S \otimes_R R^{\text{sh}} \rightarrow \text{Spec } S$ is a colimit of étale morphisms, $S \otimes_R R^{\text{sh}}$ is normal by [Stacks 2005–, Lemmas 033C and 037D]. Hence, it is a product of normal domains.

Moreover, $S \otimes_R R^{\text{sh}}$ is a finite algebra over the henselian local ring R^{sh} and thus by [Stacks 2005–, Lemma 04GG (10)] we have

$$S \otimes_R R^{\text{sh}} = \prod_{i=1}^m (S \otimes_R R^{\text{sh}})_{\mathfrak{m}_i}$$

where $\mathfrak{m}_1, \dots, \mathfrak{m}_m$ are the maximal ideals of $S \otimes_R R^{\text{sh}}$ lying over \mathfrak{m}^{sh} . We conclude that $S \otimes_R R^{\text{sh}}$ is a finite product of normal local domains. Since any prime of $S \otimes_R R^{\text{sh}}$ lying above \mathfrak{n} and \mathfrak{m}^{sh} is necessarily maximal, $\text{Spec } S^{\text{sh}} \rightarrow \text{Spec } S \otimes_R R^{\text{sh}}$ is a clopen immersion.

Finally, we discuss the statement regarding the case (R, \mathfrak{m}) is a DVR. Set $(u) = \mathfrak{m}$. In this case, S is a semilocal Dedekind domain and in particular a PID; let $\mathfrak{n}_1, \dots, \mathfrak{n}_n$ be the maximal ideals of S lying over \mathfrak{m} . Let K be the function field of R , so that $\text{Spec } K \rightarrow \text{Spec } R$ defines the open immersion given by the principal open $D(u) = \text{Spec } R_u$. Observe that $(R^{\text{sh}}, \theta(u))$ is a (strictly henselian) DVR as well, where θ is the canonical homomorphism $R \rightarrow R^{\text{sh}}$. With this being said, we see that pullback of the cartesian square

$$\begin{array}{ccc} \text{Spec } S & \longleftarrow & \text{Spec } S \otimes_R R^{\text{sh}} \\ \downarrow & & \downarrow \\ \text{Spec } R & \longleftarrow & \text{Spec } R^{\text{sh}} \end{array}$$

to the Zariski open $\text{Spec } K \rightarrow \text{Spec } R$ is given by the cartesian square

$$\begin{array}{ccc} \text{Spec } L & \longleftarrow & \text{Spec } L \otimes_K K(R^{\text{sh}}) \\ \downarrow & & \downarrow \\ \text{Spec } K & \longleftarrow & \text{Spec } K(R^{\text{sh}}) \end{array}$$

where L denotes the fraction field of S . In particular, the generic rank of the finite R^{sh} -algebra $S \otimes_R R^{\text{sh}}$ is equal to $[L : K]$ —the generic rank of S over R . In particular, we have that

$$[L : K] = \sum_{i=1}^m [K((S \otimes_R R^{\text{sh}})_{\mathfrak{m}_i}) : K(R^{\text{sh}})] = \sum_{i=1}^n [K(S_{\mathfrak{n}_i}^{\text{sh}}) : K(R^{\text{sh}})] + \Sigma,$$

where Σ is the remaining summands, i.e., the sum corresponding to the (*a priori* possible) connected components that are not isomorphic to strict henselizations of S at some of its maximal ideals. Our goal is to prove that $\Sigma = 0$ (i.e., it is an empty summation). To this end, observe that, by combining assumptions (a) and (c) with [Stacks 2005–, Remark 09E8], we have $[L : K] = \sum_{i=1}^n e_i$ where e_i is the ramification index of the extension of DVRs $\phi_{\mathfrak{n}_i} : R \rightarrow S_{\mathfrak{n}_i}$. Hence, it suffices to prove $[K(S_{\mathfrak{n}_i}^{\text{sh}}) : K(R^{\text{sh}})] = e_i$. Observe that the ramification index of $R^{\text{sh}} \rightarrow S_{\mathfrak{n}_i}^{\text{sh}}$ is exactly e_i and its residue field extension is trivial (it is tacitly assumed here that the residue field of both is the same separable closure of $R/\mathfrak{m} = S_{\mathfrak{n}_i}/\mathfrak{n}_i S_{\mathfrak{n}_i}$). The result then follows from [Stacks 2005–, Remark 09E8]. □

Example 3.32. We may use Lemma 3.31 to argue the part in the proof of Claim 3.15 where we explain why there cannot be only one prime of S lying over (Δ) . Indeed, if there were only one such a prime $\mathfrak{q} \subset S$, we saw that the degree 6 extension of DVRs $R_{(\Delta)} \rightarrow S_{\mathfrak{q}}$ has ramification index 6 and Galois group isomorphic to S_3 . However, when we apply Lemma 3.31 and its proof we obtain that $R_{(\Delta)}^{\text{sh}} \rightarrow S_{\mathfrak{q}}^{\text{sh}}$ is a degree 6 extension with Galois group S_3 . Nevertheless, this contradicts Theorem 3.5 as it states that the Galois group must be cyclic.

Either directly or indirectly, we know that there must be three primes $\mathfrak{q}_1 = (t_2 - t_3)$, $\mathfrak{q}_2 = (t_1 - t_3)$, and $\mathfrak{q}_3 = (t_1 - t_2)$ of S lying over $(\Delta) \subset R$, all of them with ramification index 2 and inertial degree 1. As predicted by Lemma 3.31, we can see directly that

$$S \otimes_R R_{(\Delta)}^{\text{sh}} \cong S_{\mathfrak{q}_1}^{\text{sh}} \times S_{\mathfrak{q}_2}^{\text{sh}} \times S_{\mathfrak{q}_3}^{\text{sh}},$$

where each extension $R_{(\Delta)}^{\text{sh}} \subset S_{\mathfrak{q}_i}^{\text{sh}}$ is a degree 2 Kummer extension of strictly local DVRs. Indeed, denoting $\varpi_i := 3t_i^2 + x$, we have from Example 3.14 that $R[\delta, t_i]_{\varpi_i} = S_{\varpi_i}$, and moreover $\text{Spec } S = \bigcup_{i=1}^3 \text{Spec } S_{\varpi_i}$ where $\mathfrak{q}_i \in \text{Spec } S_{\varpi_j}$ if and only if $i = j$ (this follows from (3.15.1) and the argument in the succeeding paragraph). This is nothing but an open covering of $\text{Spec } S$ by standard étale morphisms over $\text{Spec } R[\delta]$ see [Milne 1980, I, Theorem 3.14]. In fact, the morphisms $\text{Spec } S_{\varpi_i} \rightarrow \text{Spec } R[\delta]$ are étale neighborhoods of $(\delta) \subset \text{Spec } R[\delta]$. In particular, the canonical homomorphism $S_{\varpi_i} \rightarrow S_{\mathfrak{q}_i}$ is an isomorphism when twisted by $R[\delta]_{(\delta)}^{\text{sh}}$ — the strict henselization of $R[\delta]$ at (δ) — which is then canonically isomorphic to each of $S_{\mathfrak{q}_i}^{\text{sh}}$. Finally, one verifies directly that the canonical homomorphism $R[\delta] \otimes_R R_{(\Delta)}^{\text{sh}} \rightarrow R[\delta]_{(\delta)}^{\text{sh}}$ is an isomorphism.

Finally, we point out that hypothesis (c) in Lemma 3.31 is (trivially) crucial for the proposition to hold. Indeed, suppose that $R \rightarrow S$ is a finite étale extension of DVRs (i.e., $n, e = 1$ in Proposition 3.12). Then, the generic and inertial degrees coincide; denote them by d . However, $S \otimes_R R^{\text{sh}}$ is product of d copies of R^{sh} . Roughly speaking, we get d connected components of $\text{Spec } S \otimes_R R^{\text{sh}}$ out of just one prime lying over the maximal ideal of R (both are a degree 2 Kummer cover $R_{(\delta)}^{\text{sh}}$ with respect to $\text{div } \Delta$). This concludes the example.

Lemma 3.33. *Let $f: Y \rightarrow X$ be a degree d finite cover of normal integral schemes. Suppose that $f_*\mathcal{O}_Y$ is locally free on some big open $U \subset X$ (i.e., $X \setminus U$ has codimension ≥ 2). Then, the kernel of $f^*: \text{Pic } X \rightarrow \text{Pic } Y$ is d -torsion. In particular, f^* maps nontorsion elements into nontorsion elements.*

Proof. Let \mathcal{L} be an invertible sheaf on X such that $f^*\mathcal{L} \cong \mathcal{O}_Y$. Then, $f_*f^*\mathcal{L} \cong f_*\mathcal{O}_Y$. Nonetheless, $f_*f^*\mathcal{L} \cong f_*(\mathcal{O}_Y \otimes f^*\mathcal{L}) \cong \mathcal{L} \otimes f_*\mathcal{O}_Y$ by the projection formula. Hence, we have an isomorphism $\mathcal{L} \otimes f_*\mathcal{O}_Y \cong f_*\mathcal{O}_Y$. Note that the rank of $f_*\mathcal{O}_Y$ is d . By letting $V = f^{-1}(U)$ and taking determinants we have $\det f_*\mathcal{O}_V \cong \det(\mathcal{L}_V \otimes f_*\mathcal{O}_V) = \mathcal{L}_V^d \otimes \det f_*\mathcal{O}_V$. Therefore, $\mathcal{L}_V^d \cong \mathcal{O}_V$. Since X is normal and $\text{codim } X \setminus U \geq 2$, we conclude that $\mathcal{L}^d \cong \mathcal{O}_X$. □

The following observation plays a crucial role in our main theorem. It can be thought of as a singular Abhyankar’s lemma for prime divisors.

Lemma 3.34. *Work in Setup 3.9 and suppose $\text{Rev}^P(X^\circ)$ to be P -irreducible. Then, every totally ramified cyclic Galois object in $\text{Rev}^P(X^\circ)$ of prime-to- p degree n is (up to isomorphism) a Kummer-type cyclic cover (as in Example 3.11) of degree $n \in M^P(X^\circ)$. In particular, if $P = 0 \in \text{Cl } X$; say $\mathfrak{p} = (f)$, and $\text{Cl } X$ has no prime-to- p torsion, then every totally ramified Galois cover in $\text{Rev}^P(X^\circ)$ is isomorphic to a Kummer cover of the form $\text{Spec } \mathcal{O}_{X^\circ}[T]/(T^n - f) \rightarrow X^\circ$ (with n prime to the characteristic).*

Proof. Let $(R, \mathfrak{m}, \mathcal{K}, K, P) \subset (S, \mathfrak{n}, \mathcal{L}, L, Q)$ in $\text{Rev}^P(X^\circ)$ be a totally ramified cyclic Galois cover of degree n with $p \nmid n$. Its pullback to U induces a connected $\mathbb{Z}/n\mathbb{Z}$ -torsor $V \rightarrow U$ (where $V = Y^\circ \setminus Q$ and $U = X^\circ \setminus P$). Therefore, by Kummer theory [Milne 1980, III, Section 4] and using that R contains a primitive n -th root of unity, there exists an n -torsion Cartier divisor D on U such that $f_U: V \rightarrow U$ is the cyclic cover defined by the spectrum of the finite \mathcal{O}_U -algebra $\mathcal{A} := \bigoplus_{i=0}^{n-1} \mathcal{O}_U(-iD)$ defined via a global section $\mathcal{O}_U \xrightarrow{\cong} \mathcal{O}_U(nD)$, say $\kappa \in K^\times$ such that $\text{div}_U \kappa + nD = 0$ (and so $\cdot \kappa: \mathcal{O}_U(-nD) \rightarrow \mathcal{O}_U$). We write $L = \mathcal{A}_K = K \otimes \mathcal{A} = K(\kappa^{1/n})$. Let \bar{D} be the closure of D in X . Thus, \bar{D} is a Weil divisor on X such that $\bar{D}|_U = D$ and $\text{div}_X \kappa + n\bar{D} = e \cdot P$ where $e = \text{val}_P \kappa$. We may assume that $e \geq 0$ (by replacing both κ and D by their respective inverses if necessary). That is, we may assume $\kappa \in R_{\mathfrak{p}}$. Note that $\text{div}_V \kappa^{1/n} + f_U^* D = 0$ on V , which is obtained by dividing by n the pullback of $\text{div}_U \kappa + nD = 0$. Further, $n \cdot \text{val}_Q \kappa^{1/n} = \text{val}_Q \kappa = n \cdot \text{val}_P \kappa$ (using the hypothesis that the extension is totally ramified) and so $\text{val}_Q \kappa^{1/n} = e \geq 0$. This lets us conclude the following.

Claim 3.35. $(n, e) = 1$.

Proof of claim. Consider the subextension $R_{\mathfrak{p}} \subset R_{\mathfrak{p}}[\kappa^{1/n}] \subset S_{\mathfrak{p}} = S_{\mathfrak{q}}$. Note that $R_{\mathfrak{p}} \subset R_{\mathfrak{p}}[\kappa^{1/n}]$ is a free local extension of rank n , where the maximal ideal of $R_{\mathfrak{p}}[\kappa^{1/n}]$ is $(t, \kappa^{1/n})$ with t a uniformizer of $R_{\mathfrak{p}}$. Also, note that $R_{\mathfrak{p}}[\kappa^{1/n}] \subset S_{\mathfrak{q}}$ is birational. In particular, $S_{\mathfrak{q}}$ is the normalization of $R_{\mathfrak{p}}[\kappa^{1/n}]$. However, this can only happen if $(n, e) = 1$. Indeed, we may base change $R_{\mathfrak{p}} \subset R_{\mathfrak{p}}[\kappa^{1/n}] \subset S_{\mathfrak{q}}$ by $R_{\mathfrak{p}}^{\text{sh}}$ to obtain $R_{\mathfrak{p}}^{\text{sh}} \subset R_{\mathfrak{p}}^{\text{sh}}[\kappa^{1/n}] \subset S_{\mathfrak{q}}^{\text{sh}}$ using Lemma 3.31(c). Nonetheless,

$$R_{\mathfrak{p}}^{\text{sh}}[\kappa^{1/n}] \rightarrow (R[\kappa^{1/n}])_{(t, \kappa^{1/n})}^{\text{sh}}$$

is an isomorphism as $R_{\mathfrak{p}}^{\text{sh}}[\kappa^{1/n}]$ is a strictly local algebra over $R[\kappa^{1/n}]$ (use [Milne 1980, I, Corollary 4.3]) with the same residue field as $R_{\mathfrak{p}}^{\text{sh}}$. Therefore, $R_{\mathfrak{p}}^{\text{sh}}[\kappa^{1/n}] \subset S_{\mathfrak{q}}^{\text{sh}}$ is a normalization by [Stacks 2005–, Tag 0CBM]. However, $R_{\mathfrak{p}}^{\text{sh}}[\kappa^{1/n}] \cong R_{\mathfrak{p}}^{\text{sh}}[T]/(T^n - \kappa) \cong R_{\mathfrak{p}}^{\text{sh}}[T]/(T^n - t^e)$ using that $\kappa = u \cdot t^e$ for some unit $u \in R_{\mathfrak{p}}$ (the latter isomorphism is of course $T \leftrightarrow T/u^{1/n}$). Hence, $(n, e) = 1$ for $R_{\mathfrak{p}}^{\text{sh}}[\kappa^{1/n}]$ is a domain. \square

Thus, there are $a, b \in \mathbb{Z}$ such that $1 = an + be$ and so

$$P = (an + be) \cdot P = n(a \cdot P + b \cdot \bar{D}) + \text{div}_X \kappa^b.$$

Further, $(a \cdot P + b \cdot \bar{D})|_U = b \cdot D \in \text{Pic } U$ and so $n \in M^P(X^\circ)$. Now, the above establishes that $K(\kappa^{b/n})/K$ defines (after taking integral closure) an object in $\text{Rev}^P(X^\circ)$ that is a cyclic cover of Kummer-type. However, $L = K(\kappa^{1/n}) = K(\kappa^{b/n})$ as $(b, n) = 1$ (for $1 = an + be$). Then, S/R in $\text{Rev}^P(X^\circ)$ is a cyclic cover of Kummer-type and $n \in M^P(X^\circ)$, as required.

For the last statement when $\mathfrak{p} = (f)$, see Example 3.11. □

Proof of Theorem 3.29. We will subdivide the proof in two parts. First, we prove the statements of Theorem 3.29 except for those establishing when the short exact sequences split. Once this is done, we proceed to show the statements of Theorem 3.29 characterizing when the given short exact sequences split.

We start with the first part now. By formal properties of Galois categories, we obtain from Lemma 3.25 a short exact sequence of topological groups

$$1 \rightarrow \pi_1^{t, \tilde{P}}(\tilde{X}^\circ) \rightarrow \pi_1^{t, P}(X^\circ) \rightarrow \text{Gal}(\tilde{X}^\circ/X^\circ) \rightarrow 1$$

where $G := \pi_{1, \text{ét}}^P(X^\circ) = \text{Gal}(\tilde{X}^\circ/X^\circ)$. Let d be its order.

Claim 3.36. *By replacing X by \tilde{X} , we may assume that: G is trivial, Galois objects have inertial degree equal to 1, if P is prime-to- p torsion then it is trivial, and further $N^P(X^\circ) = M^P(X^\circ)$.*

Proof of claim. Consider the induced homomorphism $\tilde{f}^*: \text{Cl } X \rightarrow \text{Cl } \tilde{X}$. Then, $\tilde{f}^*: P \mapsto \tilde{P}$. Since \tilde{f} is quasiétale, its restriction to X_{reg}° is a Galois étale cover by the purity of the branch locus. By Lemma 3.33, $\ker \tilde{f}^*$ is d -torsion and \tilde{P} is nontorsion if so is P (as $\text{Cl } X$ is the same as $\text{Pic } U$ for any regular big open $U \subset X$).

Let $\phi: \text{Cl } \tilde{X} \rightarrow \text{Cl } \tilde{U}$ be the restriction homomorphism and set $\Lambda := \phi^{-1}(\text{Pic } \tilde{U})$ (where $\tilde{U} = \tilde{X}^\circ \setminus \tilde{P}$ and so on). We observe that Λ has no prime-to- p torsion. Indeed, let D be a divisor on \tilde{X} such that $D \in \Lambda$ and $D \in \text{Cl } \tilde{X}$ has prime-to- p torsion, say of index $p \nmid n > 1$. Then, the corresponding Veronese-type cyclic cover $\tilde{R} \rightarrow \bigoplus_{i=0}^{n-1} \tilde{R}(-iD)$ induces a quasiétale degree n Galois object in $\text{Rev}^{\tilde{P}}(\tilde{X}^\circ)$, which violates the universality of \tilde{f} .

Now, if $P \in \text{Cl } X$ is torsion, then so is $\tilde{P} \in \text{Cl } \tilde{X}$ and its order divides the one of P . Thus, if $P \in \text{Cl } X$ is prime-to- p torsion then $\tilde{P} \in \text{Cl } \tilde{X}$ is trivial as $\tilde{P} \in \Lambda$.

Finally, we must explain why

$$N^P(X^\circ) = \{n \mid p \nmid n, \tilde{P} = n \cdot N \text{ with } N \in \Lambda\} = N^{\tilde{P}}(\tilde{X}^\circ)$$

The second equality follows from Λ having no prime-to- p torsion as $\tilde{P} - n \cdot N \in \Lambda$ if $N \in \Lambda$. The first equality is obtained as follows. The inclusion “ \subset ” is clear. Indeed, if $P = n \cdot M + T$ in $\text{Cl } X$ where $T \in \text{Cl } X$ has prime-to- p torsion and $M|_U \in \text{Pic } U$. Then, $\tilde{P} = n \cdot \tilde{f}^*M + \tilde{f}^*T$ where $\tilde{f}^*M \in \Lambda$ and $\tilde{f}^*T = 0$ as it is a prime-to- p torsion element of Λ . Conversely, suppose that $\tilde{P} = n \cdot N$ in $\text{Cl } \tilde{X}$ for some $N \in \Lambda$. Let us pullback everything to $W := X_{\text{reg}}^\circ$ whose inverse image under \tilde{f} we denote by \tilde{W} , which is a regular big open of \tilde{X} . Then, by using the Hochschild–Serre spectral sequence [Milne 1980, III, Theorem 2.20], the image of $\tilde{f}^*: \text{Pic } \tilde{W} \rightarrow \text{Pic } W$ lies inside $(\text{Pic } \tilde{W})^G$. As in Lemma 3.33, we may consider the norm homomorphism $N_{\tilde{f}}: \text{Pic } \tilde{W} \rightarrow \text{Pic } W$, which is obtained by applying H^1 to the norm morphism of multiplicative groups $f_*\mathcal{O}_{\tilde{W}}^\times \rightarrow \mathcal{O}_W^\times$ (as subsheaves of $\tilde{K} \supset K$ respectively); see [Stacks 2005–, Tag 0BCX] for details. The key property is that the composition

$$\text{Pic } W \xrightarrow{\tilde{f}^*} \text{Pic } \tilde{W} \xrightarrow{N_{\tilde{f}}} \text{Pic } W$$

is multiplication-by- d . However, since \tilde{f} is Galois, $N_{\tilde{f}}((\text{Pic } \tilde{W})^G) \subset d \cdot \text{Pic } W$ by the same principle and the same for any open of X in place of W . Treating the equality $\tilde{P} = n \cdot N$ in $\text{Pic } \tilde{W}$, on the left hand side we have an element of $(\text{Pic } \tilde{W})^G$ as $\tilde{P} = \tilde{f}^* P$. Since, Λ has no prime-to- p torsion and n is prime-to- p , this implies that $N \in (\text{Pic } \tilde{W})^G$. Therefore, by taking norms, we get $d \cdot P = d \cdot n \cdot M$ in $\text{Pic } W$ where $d \cdot M = N_{\tilde{f}}(N)$, which implies that $M|_U \in \text{Pic } U$ as $N|_{\tilde{U}} \in \text{Pic } \tilde{U}$. Thus, $P = n \cdot M + T$ where T is d -torsion and $M|_U \in \text{Pic } U$. \square

With the above reductions in place, we let $X' := \text{Spec } \mathcal{O}_{X,P}^{\text{sh}}$ be the étale germ of X at (the generic point of) P . Note that $\mathcal{O}_{X,P}^{\text{sh}}$ is none other than the strict henselization of $\mathcal{O}_{X,P} = R_{\mathfrak{p}}$ at its maximal ideal. We argue next that the canonical morphism $X' \rightarrow X$ induces a surjection of fundamental groups

$$\eta: \pi_1^{t,P'}(X'^{\circ}) \rightarrow \pi_1^{t,P}(X^{\circ})$$

where P' is the divisor on X' corresponding to its codimension 1 closed point and X'° is the inverse image of X° along $X' \rightarrow X$.

Claim 3.37. *The pullback functor $\text{Rev}^P(X^{\circ}) \rightarrow \text{Rev}^{P'}(X'^{\circ})$ induces a surjective homomorphism of topological groups $\eta: \pi_1^{t,P'}(X'^{\circ}) \rightarrow \pi_1^{t,P}(X^{\circ})$.*

Proof of claim. Note that the pullback functor is well-defined by Lemma 3.3. By the abstract nonsense regarding Galois categories, the first statement amounts to proving the compatibility between the fiber or fundamental functors; see [Murre 1967, Chapter 5]. Recall that, implicitly, we always take our base point to be some fixed separable closure K^{sep} of K . We are going to choose the base point of $\text{Rev}^{P'}(X'^{\circ})$ compatibly, i.e., so that we have a commutative diagram:

$$\begin{array}{ccccc} R_{\mathfrak{p}}^{\text{sh}} & \longrightarrow & K(R_{\mathfrak{p}}^{\text{sh}}) & \longrightarrow & K(R_{\mathfrak{p}}^{\text{sh}})^{\text{sep}} \\ \theta \uparrow & & \uparrow \theta_K & & \uparrow \theta_K^{\text{sep}} \\ R & \longrightarrow & K & \longrightarrow & K^{\text{sep}} \end{array}$$

Equivalently, we choose K^{sep} to be the subfield of $K(R_{\mathfrak{p}}^{\text{sh}})^{\text{sep}}$ of elements that are algebraic separable over K . To simplify notation, we denote the rings on the top of the diagram from left to right; respectively, by R' , K' , and K'^{sep} . Recall that the fiber functor $\mathcal{F}: \text{Rev}^P(X^{\circ}) \rightarrow \text{FSet}$ is given by

$$\mathcal{F}(S/R) = \text{Hom}_{R\text{-alg}}(S, K) = \text{Hom}_{K\text{-alg}}(L, K^{\text{sep}})$$

for all S/R connected in $\text{Rev}^P(X^{\circ})$. Of course, the same definition applies to the fiber functor $\mathcal{F}': \text{Rev}^{P'}(X'^{\circ}) \rightarrow \text{FSet}$ with K'^{sep} in place of K^{sep} and so on. We need to verify the commutativity of the following diagram of functors:

$$\begin{array}{ccc} \text{Rev}^P(X^{\circ}) & \longrightarrow & \text{Rev}^{P'}(X'^{\circ}) \\ & \searrow \mathcal{F} & \swarrow \mathcal{F}' \\ & \text{Set} & \end{array}$$

where the horizontal arrow is the pullback functor; see [Murre 1967, Section 5.1, Example]. To this end, we perform the following computation with S/R a connected object of $\text{Rev}^P(X^\circ)$:

$$\begin{aligned} \mathcal{F}'(S \otimes_R R') &= \text{Hom}_{R'\text{-alg}}(S \otimes_R R', K'^{\text{sep}}) = \text{Hom}_{R\text{-alg}}(S, K'^{\text{sep}}) = \text{Hom}_{K\text{-alg}}(L, K'^{\text{sep}}) \\ &= \text{Hom}_{K\text{-alg}}(L, K^{\text{sep}}) \\ &= \mathcal{F}(S). \end{aligned}$$

where the penultimate equality follows from the compatibility in our choices of base points. Indeed, since L/K is a finite separable extension, any K -embedding of L into K'^{sep} is going to be contained in K^{sep} — the subfield of K'^{sep} of separable elements over K .

Finally, we explain why η is surjective. According to the abstract nonsense [Murre 1967, Section 5.2.1], η is surjective if and only if the pullback of connected objects is connected. Hence, the surjectivity of η is a simple consequence of the equality $S \otimes_R R' = S_q^{\text{sh}}$ provided by Lemma 3.31 — once we know there is only one prime lying over with trivial inertial degree. \square

As a direct application of Theorem 3.5; see [Milne 1980, I, Section 5, Remark 5.1(e)], we have that

$$\pi_1^{t,P'}(X'^\circ) = \varprojlim_{p \nmid n} \mu_n(K') \xrightarrow{\cong} \varprojlim_{p \nmid n} \mathbb{Z}/n\mathbb{Z} =: \hat{\mathbb{Z}}^{(p)},$$

where it is worth noting that the isomorphism is not canonical as it depends on choices of compatible primitive roots of unity of K' in K'^{sep} . We have constructed a (noncanonical) surjective homomorphism of topological groups

$$\eta': \hat{\mathbb{Z}}^{(p)} \xrightarrow{\cong} \pi_1^{t,P'}(X'^\circ) \twoheadrightarrow \pi_1^{t,P}(X^\circ).$$

which explains (3.29.1). To describe $\ker \eta'$ (resp. $\text{Image } \eta'$), consider the following assertion.

Claim 3.38. *There is a factorization of continuous homomorphisms*

$$\begin{array}{ccc} \hat{\mathbb{Z}}^{(p)} & \xrightarrow{\eta'} & \pi_1^{t,P}(X^\circ) \\ \text{can} \downarrow & \nearrow \eta'' & \\ \varprojlim_{n \in N^P(X^\circ)} \mathbb{Z}/n\mathbb{Z} & & \end{array}$$

where $N^P(X^\circ) = \{n \in \mathbb{N} \mid p \nmid n, P = n \cdot D \text{ with } D|_U \in \text{Pic } U\}$.

Proof of claim. We may assume that $P \in \text{Cl } X$ is nontrivial and so nontorsion. Since η' is surjective, a Galois object $(R, \mathfrak{m}, \zeta, K, P) \subset (S, \mathfrak{n}, \zeta, L, Q)$ in $\text{Rev}^P(X^\circ)$ is cyclic, i.e., $\text{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$. Then, Claim 3.38 amounts to $n \in N^P(X^\circ)$ whenever such cover exists and so the claim follows from Lemma 3.34. \square

Claim 3.39. *The homomorphism η'' in Claim 3.38 is injective.*

Proof of claim. By [Murre 1967, Section 5.2.4], η'' is injective if and only if for all $n \in N^P(X^\circ)$ there exists a cover in $\text{Rev}^P(X^\circ)$ whose pullback to X' (has a connected component that) is a Kummer cover $\mathcal{O}_{X,P}^{\text{sh}} \subset \mathcal{O}_{X,P}^{\text{sh}}[t^{1/n}]$. To this end, for $n \in N^P(X^\circ)$, let us set $\text{div}_X \kappa + n \cdot D = P$ so that $D|_U \in \text{Pic } U$. We

then invoke Example 3.11, Definition-Proposition 3.4. That is, we embed $K(\kappa^{1/n})$ in K^{sep} and note that $K(\kappa^{1/n})/K \in \text{Rev}^P(X^\circ)$ has the required property. \square

With the above in place, we explain next why the short exact sequence of topological groups

$$0 \rightarrow \varinjlim_{n \in N^P(X^\circ)} \mathbb{Z}/n\mathbb{Z} \rightarrow \pi_1^{t,P}(X^\circ) \rightarrow G \rightarrow 1$$

splits if and only if the containment $N^P(X^\circ) \supset M^P(X^\circ)$ is an equality and there are divisors $\frac{1}{n}P$ on X for all $n \in M^P(X^\circ)$ such that: $\frac{1}{1}P = P$ and $m(\frac{1}{mn}P) = \frac{1}{n}P$ in $\text{Cl } X$ for all $m, n \in \mathbb{N}$ so that $mn \in M^P(X^\circ)$. Note that $M^P(X^\circ)$ is an (inversely) directed subset $N^P(X^\circ)$ (with respect to divisibility); see Remark 3.30.

Suppose that $N^P(X^\circ) = M^P(X^\circ)$ and the existence of a compatible system $\{\frac{1}{n}P\}_{n \in M^P(X^\circ)}$ of quotients of P . Recall that $\tilde{f}: \tilde{X} \rightarrow X$ denotes the universal cover of $\text{Rev}_{1,\text{ét}}^P(X^\circ)$. The equality $N^P(X^\circ) = M^P(X^\circ)$ means that for every $n \in N^P(X^\circ)$ there exists $\kappa_n \in K^\times$ such that $\text{div}_{\tilde{X}} \kappa_n + n \cdot \tilde{f}^* D_n = \tilde{P}$ where D_n is a divisor on X such that $D_n|_U$ is Cartier. Although the choice of κ_n is not unique, the cyclic field extension $\tilde{K} \subset \tilde{K}(\kappa_n^{1/n}) \subset K^{\text{sep}}$ is. That is, $\tilde{K}_n := \tilde{K}(\kappa_n^{1/n})$ is independent of the choice of κ_n (which is not necessarily true for $K(\kappa_n^{1/n})$). In fact, these are precisely the Galois objects of $\text{Rev}^{\tilde{P}}(\tilde{X}^\circ)$ with field of fractions inside K^{sep} . Consider the field $\tilde{K}_\infty := \bigcup_{n \in N^P(X^\circ)} \tilde{K}_n \subset K^{\text{sep}}$ (so $\pi_1^{t,P}(X^\circ) = \text{Gal}(\tilde{K}_\infty/K)$). It is worth observing that $K(\kappa_n^{1/n}) \cdot \tilde{K} = \tilde{K}_n$ and $K(\kappa_n^{1/n}) \cap \tilde{K} = K$ (as the normalization of R in $K(\kappa_n^{1/n})$ is totally ramified whereas in \tilde{K} it is quasiétale). By Galois theory [Lang 2002, VI, Section 1, Theorem 1.12], this implies that $\tilde{K}_n/K(\kappa_n^{1/n})$ is Galois and the homomorphism

$$\text{Gal}(\tilde{K}_n/K(\kappa_n^{1/n})) \rightarrow \text{Gal}(\tilde{K}/K) = G, \quad \sigma \mapsto \sigma|_{\tilde{K}}$$

is an isomorphism. In other words, there is an action of G on \tilde{K}_n by K -automorphisms so that $\tilde{K}_n^G = K(\kappa_n^{1/n})$. By the same token, since $K(\kappa_n^{1/n}/K)$ is Galois, the exact sequence

$$1 \rightarrow \text{Gal}(\tilde{K}_n/\tilde{K}) \rightarrow \text{Gal}(\tilde{K}_n/K) \rightarrow G \rightarrow 1$$

then splits (as a direct product) for every n ; see [Lang 2002, VI, Section 1, Theorem 1.14]. Roughly speaking, with the equality $N^P(X^\circ) = M^P(X^\circ)$, we can split the quotient $\text{Gal}(\tilde{K}_\infty/K) \twoheadrightarrow G$ at each finite level quotient $\text{Gal}(\tilde{K}_n/K) \twoheadrightarrow G$. To do this globally, we need these splittings to be compatible under divisibility in $M^P(X^\circ)$. This is precisely what the additional hypothesis regarding the existence of $\{\frac{1}{n}P\}_{n \in M^P(X^\circ)}$ accomplishes. Indeed, by setting $D_n = \frac{1}{n}P$ and $K_n := K(\kappa_n^{1/n})$, the field extensions $\{K_n/K\}_{n \in N^P(X^\circ)}$ yield a projective system in $\text{Rev}^P(X^\circ)$ and we may then set the field $K_\infty := \bigcup_{n \in N^P(X^\circ)} K_n \subset K^{\text{sep}}$. Then, K_∞/K is Galois, $K_\infty \cdot \tilde{K} = \tilde{K}_\infty$, and $K_\infty \cap \tilde{K} = K$ (as $K(\kappa_n^{1/n}) \cap \tilde{K} = K$). As before, this implies that $\tilde{K}_\infty/K_\infty$ is Galois and the homomorphism

$$\text{Gal}(\tilde{K}_\infty/K_\infty) \rightarrow \text{Gal}(\tilde{K}/K) = G, \quad \sigma \mapsto \sigma|_{\tilde{K}}$$

is an isomorphism and the exact sequence

$$1 \rightarrow \text{Gal}(\tilde{K}_\infty/\tilde{K}) \rightarrow \text{Gal}(\tilde{K}_\infty/K) \rightarrow G \rightarrow 1$$

splits, as required. This shows the direction “ \longleftarrow ”.

Conversely, suppose that there is a projection $\pi_1^{t,P}(X^\circ) \rightarrow \varprojlim_{n \in N^P(X^\circ)} \mathbb{Z}/n\mathbb{Z}$ splitting the inclusion $\varprojlim_{n \in N^P(X^\circ)} \mathbb{Z}/n\mathbb{Z} \hookrightarrow \pi_1^{t,P}(X^\circ)$. In particular, for each $n \in N^P(X^\circ)$, there is a cyclic Galois cover $f_n: Y_n^\circ \rightarrow X_n^\circ$ whose ‘‘Galois-theoretic’’ pullback to $\text{Rev}^{\tilde{P}}(\tilde{X}^\circ)$ is a cyclic Galois cover. Thus, f_n must be totally ramified (as can be seen by using the inertial decantation property). Therefore, each f_n is a cyclic cover of Kummer-type by Lemma 3.34. In particular, $N^P(X^\circ) \subset M^P(X^\circ)$. It remains to explain why we have a compatible system of elements $\{\frac{1}{n}P\}$ in $\text{Cl } X$. To this end, assume that f_n is given by $\text{div } \kappa_n + nD_n = P$ (this for each n). We have an inclusion $K(\kappa_n^{1/n}) \subset K(\kappa_{nm}^{1/nm})$. Since the latter extension is cyclic, $K(\kappa_{nm}^{1/n}) = K(\kappa_n^{1/n})$. Hence, by Kummer theory [Milne 1980, see page 126], $\kappa_n/\kappa_{nm} \in (K^\times)^n$; say $\kappa_n/\kappa_{nm} = x^n$. From this we deduce that $n \text{div } x + n(D_n - mD_{nm}) = 0$ and so $\text{div } x + (D_n - mD_{nm}) = 0$, as equalities in $\text{Div } X$. Hence, $D_n = mD_{nm}$ in $\text{Cl } X$. In particular, we may take $\frac{1}{n}P := D_n$ for all n .

Finally, assuming $P \in \text{Cl } X$ is prime-to- p torsion, we still need to show that $M^P(X^\circ) = \mathbb{Z}_{>0}^{(p)}$ if and only if $P = 0$ in $\text{Cl } X$. The ‘‘if’’ direction is clear. Conversely, assume to the contrary that P is nontrivial but $M^P(X^\circ) = \mathbb{Z}_{>0}^{(p)}$. Let ℓ be the order/index of P in $\text{Cl } X$. Since $\ell^a \in M^P(X^\circ)$ for any positive integer a , we find a divisor D_a which is Cartier on U such that $P = \ell^a D_a \in \text{Cl } X$. Let o_a be the order of D_a . In particular, $o_a \mid \ell^{a+1}$ but $o_a \nmid \ell^a$. Let $\ell = \ell_1^{s_1} \cdots \ell_r^{s_r}$ be the prime factorization of ℓ ($\ell_i \neq p$). Then, there is some index i (depending on a) such that $\ell_i^{s_i(a+1)} \mid o_a$. Since a is arbitrary, $\ell_i \geq 2$, and $s_i \geq 1$, we conclude that o_a is arbitrarily large. On the other hand, we may consider the quasiétale Veronese-type cyclic cover defined via $\text{div}_X \kappa + o_a \cdot D_a = 0$. These then yield objects of $\text{Rev}_{1,\acute{e}t}^P(X^\circ)$ of arbitrarily large degree, which contradicts the already proven finiteness of $\pi_{1,\acute{e}t}^P(X^\circ)$.

This demonstrates Theorem 3.29. □

Remark 3.40. The homomorphism η in Claim 3.37 can be defined more succinctly as follows. Recall that $\pi_1^{t,P}(X^\circ)$ is the limit $\varprojlim \text{Gal}(L/K)$ traversing all the finite Galois extensions $K \subset L \subset K^{\text{sep}}$ so that the integral closure S/R of R in L is tamely ramified with respect to P , and *verbatim* for $\pi_1^{t,P'}(X'^\circ)$, where we have fixed $K^{\text{sep}} \subset K'^{\text{sep}}$. For any such a L/K , we must define compatible homomorphisms $\pi_1^{t,P'}(X'^\circ) \rightarrow \text{Gal}(L/K)$. Since L/K is Galois, $\text{Gal}(L/K)$ acts transitively and faithfully on $\mathcal{F}(S) = \text{Hom}_{K\text{-alg}}(L, K^{\text{sep}})$. Nonetheless, as noticed in Claim 3.37, this set is the same set as

$$\mathcal{F}'(S \otimes_R R') = \text{Hom}_{R'\text{-alg}}(S \otimes_R R', K'^{\text{sep}}) = \coprod_i \text{Hom}_{R'\text{-alg}}(S_i, K'^{\text{sep}}) = \coprod_i \text{Hom}_{K'\text{-alg}}(K(S_i), K'^{\text{sep}})$$

where $S \otimes_R R' = \prod_i S_i$ is the decomposition of $S \otimes_R R'$ as a finite product of normal, local, and finite R' -algebras; see the proof of Lemma 3.31. Of course, the given inclusion $K \subset L \subset K^{\text{sep}}$ is an element of this set, say ξ . Therefore, ξ is contained in one and only one of the displayed disjoint sets; let i_0 denote the corresponding index. Letting L_{i_0} be the Galois closure of $K(S_{i_0})$ in K'^{sep} , we have that $\text{Gal}(L_{i_0}/K')$ surjects onto $\text{Aut}_{K'}(K(S_{i_0}))$. On the other hand, we define the homomorphism of groups $\varphi: \text{Aut}_{K'}(K(S_{i_0})) \rightarrow \text{Gal}(L/K)$ by declaring $\varphi(h)$ to be the only element of $\text{Gal}(L/K)$ that when acts on ξ yields $\xi \circ h$. In this way, we have

$$\pi_1^{t,P'}(X'^\circ) \xrightarrow{\text{can}} \text{Gal}(L_{i_0}/K') \twoheadrightarrow \text{Aut}_{K'}(K(S_{i_0})) \xrightarrow{\varphi} \text{Gal}(L/K).$$

The limit over these defines η . Observe that η is surjective if and only if these homomorphisms are all surjective, which is equivalent to the surjectivity of φ for all L/K . However, it is not difficult to see that φ is surjective if and only if $S \otimes_R R'$ is connected.

We illustrate with an example the failure of η being surjective if there were more than one prime lying over. In Example 3.32, we had a canonical isomorphism of R' -algebras

$$S \otimes_R R' = S \otimes_R R_{(\Delta)}^{\text{sh}} \xrightarrow{\cong} S_{q_1}^{\text{sh}} \times S_{q_2}^{\text{sh}} \times S_{q_3}^{\text{sh}}.$$

Note that a K -embedding of L into K'^{sep} is the same as a choice of a square root of Δ ; which in our case it was δ , and the choice of a t_i . For instance, when we chose t_1 to be our “ t ” in Example 3.14, we were choosing the R' -embedding

$$S \otimes_R R' \rightarrow S_{q_1}^{\text{sh}} \times S_{q_2}^{\text{sh}} \times S_{q_3}^{\text{sh}} \rightarrow S_{q_1}^{\text{sh}} \rightarrow K'^{\text{sep}},$$

for this is the one in which L is realized as the field of fractions of $R[\delta, t_1]_{\mathfrak{w}_1} \rightarrow S_{\mathfrak{w}_1}$. This specific embedding was our ξ all along. Now, $S_{q_1}^{\text{sh}}$ is a degree 2 Kummer cover over R' , so its Galois group is cyclic of order 2 with generator $\tau: \delta \mapsto -\delta$. On the other hand, under the canonical bijection $\mathcal{F}(S) = \mathcal{F}'(S \otimes_R R')$, we see that $\xi \circ \tau$ correspond to the K -embedding $L \xrightarrow{(23)} L \rightarrow K^{\text{sep}}$ where $(23) \in \text{Gal}(L/K) \cong S_3$ is the transposition switching t_2 and t_3 (leaving t_1 intact). In other words, we have the following commutative diagram of groups:

$$\begin{array}{ccccc} \pi_1^{t,P}(X^\circ) & \longrightarrow & \text{Gal}(L/K) & \xrightarrow{\cong} & S_3 \\ \downarrow \eta & & \uparrow \varphi & & \uparrow 1 \mapsto (23) \\ \pi_1^{t,P'}(X'^\circ) & \longrightarrow & \text{Gal}(K(S_{q_1}^{\text{sh}})/K') & \xrightarrow{\cong} & \mathbb{Z}/2\mathbb{Z} \end{array}$$

so that η cannot be surjective. This finishes our remarks.

4. Tame fundamental groups: Positive characteristic

We proceed to our study of tame Galois categories in positive characteristic.

4A. Cohomologically tame Galois category of an F -pure singularity. We start by making a simple observation about the cohomologically tame Galois category of an F -pure singularity. This is an application of [Carvajal-Rojas and Stabler 2023, Theorem 4.8] following [Carvajal-Rojas et al. 2018].

Theorem 4.1. *Working in Setup 3.9, suppose that X is F -pure. There exists a cover $\tilde{X}^\circ \rightarrow X^\circ$ in $\text{F}\acute{\text{E}}\text{t}^{t,X}(X^\circ)$ such that, for any cover $V \rightarrow \tilde{X}^\circ$ in $\text{F}\acute{\text{E}}\text{t}^{t,\tilde{X}}(\tilde{X}^\circ)$, its integral closure $\text{Spec } S \rightarrow \text{Spec } \tilde{R}$ satisfies that its restriction $V(p(S)) \rightarrow V(p(\tilde{R}))$ is trivial.*

Proof. Note that [Carvajal-Rojas and Stabler 2023, Theorem 4.8] implies that for all connected cover $Y^\circ \rightarrow X^\circ$ in $\text{F}\acute{\text{E}}\text{t}^{t,X}(X^\circ)$ with integral closure $R \subset S$ we must have $1 \geq r(S) = [\kappa(p(S)) : \kappa(p(R))] \cdot r(R)$. In particular, we have that the generic degree of $V(p(S)) \rightarrow V(p(R))$ is no more than $1/r(R)$. Here,

we use that R is F -pure to say $1/r(R) < \infty$. By formal properties of Galois categories (just as in [Carvajal-Rojas et al. 2018]), there exists a universal cover with the required property after we notice that if the generic degree of $V(p(S)) \rightarrow V(p(R))$ is trivial then the map itself is trivial for both $R/p(R)$ and $S/p(S)$ are strongly F -regular and so normal. \square

Remark 4.2. In Theorem 4.1, notice that if $p(R) \neq 0$ then $p(R) \supset \tau(R)$. Hence, $p(R)$ corresponds to a singular point of X , for $\tau(R)$ cuts out the not strongly- F -regular locus of X . In particular, since X is normal, $\text{ht } p(R) \geq 2$. In other words, either $V(p(R))$ has codimension at least 2 or X is strongly F -regular. Hence, if X is not strongly F -regular, $V(p(R)) \subset X$ has codimension ≥ 2 . Thus, Theorem 4.1 is only interesting in higher dimensions if X is a non- F -regular F -pure singularity. In a sense, this justifies next section.

4B. Tame fundamental group of a purely F -regular local pair. In this section, we provide a study of the Galois category $\text{Rev}^P(X^\circ)$ for a purely F -regular pair (X, P) that will lead to a verification of the hypothesis in Theorem 3.29. To this end, the following three fundamental observations Proposition 4.4, Proposition 4.6, and Theorem 4.7 about covers $(R, \mathfrak{m}, \kappa, K) \subset (S, \mathfrak{n}, \ell, L)$ in $\text{Rev}^P(X^\circ)$; as in Remark 3.10, are in order.

4B1. Three fundamental properties. Consider the following setup.

Setup 4.3. Let $(R, \mathfrak{m}, \kappa, K) \subset (S, \mathfrak{n}, \ell, L)$ be a local finite extension of normal local domains with corresponding morphism of schemes $f: Y \rightarrow X$. Let $X^\circ \subset X$ be a big open (i.e., X° contains every codimension 1 point of X). Assume $f: f^{-1}(X^\circ) \rightarrow X^\circ$ to be tamely ramified with respect to a reduced divisor $D = P_1 + \cdots + P_k$ with prime components $P_i = V(\mathfrak{p}_i)$.¹⁵

We invite the reader to look at [Carvajal-Rojas and Stabler 2023, Section 3] for further details regarding transposability.

Proposition 4.4 (transposability). *Work in Setup 4.3. Then, R is a $\text{Tr}_{S/R}$ -transposable Cartier \mathcal{C}_R^D -module, where $\text{Tr}_{S/R}: S \rightarrow R$ is the (generically induced) nonzero trace map. Moreover, $f^*\mathcal{C}_R^D \subset \mathcal{C}_S^E$ where E is the reduced and effective divisor on Y supported on the prime divisors whose generic point lies over the generic point of some of the P_i .*

Proof. Since X and Y are normal, we must prove that $f^*D - \text{Ram}$ is effective; see [Carvajal-Rojas and Stabler 2023, Section 3] and [Schwede and Tucker 2014, Theorem 5.7]. Let $\mathfrak{q}_{i,1}, \dots, \mathfrak{q}_{i,n_i}$ be the prime ideals of S lying over \mathfrak{p}_i . Then,

$$f^*P_i = e_{i,1} \cdot Q_{i,1} + \cdots + e_{i,n_i} \cdot Q_{i,n_i}$$

where $Q_{i,j}$ is the divisor on Y corresponding to $\mathfrak{q}_{i,j}$, and $e_{i,j}$ is the ramification index of f along $\mathfrak{q}_{i,j}$.¹⁶ Since $\mathfrak{p}_1, \dots, \mathfrak{p}_k \in X$ are the only codimension 1 branch points, the ramification divisor Ram is supported

¹⁵It does not matter whether we think of the divisors involved as divisors on X° or on X .

¹⁶That is, $e_{i,j}$ is the order of the uniformizer of $R_{\mathfrak{p}_i}$ in the DVR $S_{\mathfrak{q}_{i,j}}$; see [Schwede and Tucker 2014, Section 2.2].

on the primes divisor $Q_{i,j}$. Moreover, since the extension is tamely ramified (over X°) with respect to D , we have that

$$\text{Ram} = \sum_{i=1}^k \sum_{j=1}^{n_i} (e_{i,j} - 1) \cdot Q_{i,j},$$

using the same computation as in [Hartshorne 1977, IV, Proposition 2.2]; see [Carvajal-Rojas 2018, Remark 2.9], compare to [Schwede and Tucker 2014, Remark 4.6]. In this way, it clearly follows that

$$D^* := f^*D - \text{Ram} = \sum_{i=1}^k f^*P_i - \text{Ram} = \sum_{i=1}^k \sum_{j=1}^{n_i} Q_{i,j} =: E \geq 0, \quad (4.4.1)$$

as required. The last statement follows by recalling $f^*\mathcal{C}_R^D \subset \mathcal{C}_S^{D^*}$ and $D^* = E$. \square

Remark 4.5. The importance of Proposition 4.4 is that we may apply [Carvajal-Rojas and Stabler 2023, Theorem 5.12 and Remark 5.13] to the pair (R, D) along the map f . In particular, we have the equality

$$\text{Tr}_{S/R}(f_*\tau_{S(-E)}(S, f^*\mathcal{C}_R^D)) = \tau_{R(-D)}(R, D)$$

Recall that $R(-D) = \bigcap_i R(-P_i) = \bigcap_i \mathfrak{p}_i$ and similarly for $S(-E)$. Using this together with Remark 2.4, we may obtain direct proofs of Proposition 4.6 and Theorem 4.7 below. Indeed, if (R, D) is purely F -regular along $R(-D)$, then $\tau_{R(-D)}(R, D) = R$ and so $\text{Tr}_{S/R}$ is surjective. Since $\text{Tr}_{S/R}(\mathfrak{n}) \subset \mathfrak{m}$, see [Carvajal-Rojas et al. 2018, Lemma 2.10; Speyer 2020, Lemma 9], we have that in that case $S = \tau_{S(-E)}(S, f^*\mathcal{C}_R^D) \subset \tau_{S(-E)}(S, E)$. In other words, the pair (S, E) is purely F -regular along E . In particular, the reduced scheme supporting E must have strongly F -regular singularities and so must be normal. Therefore, the irreducible components Q_1, \dots, Q_k cannot intersect pairwise. Nevertheless, S being local, these components intersect at the closed point. Consequently, E must have exactly one irreducible component $E = Q$. Nonetheless, we will provide below proofs for these statement using splitting primes. These proofs are more elementary than [Carvajal-Rojas and Stabler 2023, Theorem 5.12] and the authors believe this approach is valuable in its own right.

Proposition 4.6 (cohomological tameness, see [Kerz and Schmidt 2010]). *Work in Setup 4.3. Suppose that $k = 1$ and $(X, D = P)$ is purely F -regular. Then, the extension $R \subset S$ is cohomologically tame, i.e., $\text{Tr}_{S/R}: S \rightarrow R$ is surjective. Thus, ℓ/κ is separable and $[\ell : \kappa]$ divides $[L : K]$. Furthermore, if ℓ/κ is trivial, then p does not divide $[L : K]$.*

Proof. Let $E = Q_1 + \dots + Q_n$ as in Proposition 4.4 and recall that $E = f^*D - \text{Ram} \geq 0$. Notice that S is $f^*\mathcal{C}_R^P$ -compatible, so $\text{Tr}_{S/R}(S)$ is a nonzero \mathcal{C}_R^P -compatible ideal as $\varphi \circ F_* \text{Tr}_{S/R} = \text{Tr}_{S/R} \circ \varphi^\top$ for all $\varphi \in \mathcal{C}_{e,R}^P$. If $\text{Tr}_{S/R}(S) \subsetneq R$, then $\text{Tr}_{S/R}(S)$ must be contained in the ideal $R(-P)$ — the splitting prime of \mathcal{C}_R^P by hypothesis. In other words,

$$\text{Tr}_{S/R} \in \text{Hom}_R(S, R(-P)) = \text{Hom}_R(S \otimes_R R(P), R) = \text{Hom}_R(S(f^*P), R),$$

which implies $S(f^*P) \subset S(\text{Ram})$ and so $\text{Ram} - f^*P \geq 0$. Thus, $E = 0$, which is absurd.

For the statements regarding $\mathcal{K} \subset \mathcal{L}$, use [Carvajal-Rojas 2018, Proposition 3.17], see [Carvajal-Rojas et al. 2018, Lemma 2.15], with $\Delta = \Delta_\varphi$ and where φ is taken to be any surjective map in $\mathcal{C}_{e,R}^P = (\mathcal{C}_{e,R}^P)^\top$ for $e \gg 0$. Note such a map φ exists because $\mathfrak{p} \neq R$, i.e., (R, P) is F -pure. Notice $\mathcal{C}_{e,R}^P = (\mathcal{C}_{e,R}^P)^\top$ was demonstrated in Proposition 4.4.

For the final statement, since $\text{Tr}_{S/R}(\mathfrak{n}) \subset \mathfrak{m}$, there is an induced \mathcal{K} -linear map $\overline{\text{Tr}}: \mathcal{L} \rightarrow \mathcal{K}$, which is nonzero if $\text{Tr}: S \rightarrow R$ is surjective. However, if \mathcal{L}/\mathcal{K} is trivial then $\overline{\text{Tr}}$ corresponds to the \mathcal{K} -linear map $\mathcal{K} \rightarrow \mathcal{K}$ given by multiplication-by- $[L : K]$. In other words, $[L : K]$ is not zero as an element of \mathcal{K} and so it is prime to p as a natural number. □

Theorem 4.7 (only one prime lying over). *Work in Setup 4.3. Suppose that $k = 1$ and $(X, D = P)$ is purely F -regular. The splitting prime $\mathfrak{q} := \mathfrak{p}(S, f^*\mathcal{C}_R^P)$ is the one and only one prime of S lying over $\mathfrak{p} := R(-P)$. Moreover, (Y, Q) is purely F -regular where $Q = V(\mathfrak{p})$.*

Proof. First, \mathfrak{q} is well-defined by [Carvajal-Rojas and Stäbler 2023, Theorem 4.8] and Propositions 4.4 and 4.6.¹⁷ Next, we prove \mathfrak{q} is unique in lying over \mathfrak{p} . We may pass to a cover of S in proving this and may therefore assume that f is generically Galois by [Grothendieck and Murre 1971, Lemma 2.2.6]. Let \mathfrak{q}' be a prime of S lying over \mathfrak{p} , i.e., $\mathfrak{q}' \cap R = \mathfrak{p}$. It suffices to prove $\mathfrak{q}' \subset \mathfrak{q}$; see [Atiyah and Macdonald 1969, Corollary 5.9]. For this, we use that \mathfrak{q} is a splitting prime ideal and the corresponding definition; see [Carvajal-Rojas and Stäbler 2023, Section 2.3.2] for the definition. It suffices to show $\varphi^\top(F_*^e \mathfrak{q}') \subset \mathfrak{n}$ for all $\varphi \in \mathcal{C}_{e,R}^D$ and $e > 0$ as the right S -span of $\{\varphi^\top \mid \varphi \in \mathcal{C}_{e,R}^D\}$ is $f^*\mathcal{C}_{e,R}^D$; see [Carvajal-Rojas and Stäbler 2023, Remark 2.15(c)].

Claim 4.8. $\text{Tr}_{S/R}(\mathfrak{q}') \subset \mathfrak{p}$.

Proof of claim. This has been shown for \mathfrak{q} in the proof of [Carvajal-Rojas and Stäbler 2023, Theorem 4.8]; see [Carvajal-Rojas and Stäbler 2023, Equation (4.8.2)]. We use the symmetry imposed by the Galois condition to induce this property to the other (possible) primes lying over \mathfrak{p} . Concretely, we have that $\text{Gal}(L/K)$ acts transitively on the set of primes lying over \mathfrak{p} [Stacks 2005–, Lemma 09EA or 0BRI]—although faithfulness might be lost due to ramification. Hence, if a prime is mapped into \mathfrak{p} by $\text{Tr}_{S/R}$ then so are its Galois conjugates, for $\text{Tr}_{S/R}(x) = \sum_{\sigma \in \text{Gal}(L/K)} \sigma(x)$ for all $x \in S$. □

For all $\varphi \in \mathcal{C}_{e,R}^D$, it follows that

$$\text{Tr}_{S/R}(\varphi^\top(F_*^e \mathfrak{q}')) = \varphi(F_*^e \text{Tr}_{S/R}(\mathfrak{q}')) \subset \varphi(F_*^e \mathfrak{p}) \subset \mathfrak{p},$$

where the last containment follows from \mathfrak{p} being the splitting prime of \mathcal{C}_R^D . In other words, $\varphi^\top(F_*^e \mathfrak{q}') \subset \text{Tr}_{S/R}^{-1}(\mathfrak{p}) \subsetneq S$ (as $\text{Tr}_{S/R}$ is surjective by Proposition 4.6). Since $\varphi^\top(F_*^e \mathfrak{q}')$ is an S -module, it must be contained in \mathfrak{n} , which was to be shown. Finally, the pair (Y, Q) is purely F -regular by [Carvajal-Rojas and Stäbler 2023, Theorem 6.12, Remark 5.15] and Remark 2.4. □

¹⁷The other two conditions are always satisfied. The S -linear map $S \rightarrow \omega_{S/R}; 1 \mapsto \text{Tr}_{S/R}$, is generically an isomorphism as L/K is separable. The condition $\text{Tr}_{S/R}(\mathfrak{n}) \subset \mathfrak{m}$ holds as in [Carvajal-Rojas et al. 2018, Lemma 2.10].

Example 4.9. Let R and f be as in Example 2.10. A direct consequence of Theorem 4.7 establishes that if L is a finite separable extension over K — the fraction field of R — then there is one and only one DVR of L lying over $R_{(f)}$ if: $R \subset R^L$ is tamely ramified with respect to $\operatorname{div} f$ and R/f is strongly F -regular. This does not hold without assuming R/f is strongly F -regular (i.e., $(R, \operatorname{div} f)$ is purely F -regular). Indeed, consider the cusp Example 3.14. In this case, the singularities of R/f are not even F -pure. One may still wonder if F -purity of R/f may suffice. To see this is not the case, we may get back to the Whitney's umbrella Example 3.16. Indeed; with notation as in Example 3.16, we specialize to $R = \kappa[[x, y, z]]$ with κ an algebraically closed field of odd characteristic. In [Blickle et al. 2012, Section 4.3.3], it is shown that R/f is F -pure yet not strongly F -regular. In fact, it is proven that $p(R, \operatorname{div} f) = (x, y) \not\supseteq (f)$.¹⁸ Considering $R' := R_{(x,y)}$, (R', f) is a counterexample where R'/f is a (nonnormal) F -pure ring. The authors are unaware of a counterexample (R, f) where R/f is normal and F -pure.

Example 4.10. There are interesting instances of multiple components pairs $(X, P_1 + \dots + P_k)$ where (X, P_i) are all purely F -regular. For example, we may consider $X = \operatorname{Spec} R$ with R as in either Example 2.13 or 2.15. With R as in Example 2.13, we may let $R(-Q) = \mathfrak{q} = (x, w)$. By symmetry on the variables, (X, Q) is a purely F -regular pair as well and moreover $\operatorname{div} x = P + Q$. We may also consider $\mathfrak{p}' = (y, z)$, $\mathfrak{q}' = (y, w)$, $P' = V(\mathfrak{p}')$, and $Q' = V(\mathfrak{q}')$, which all define purely F -regular pairs on X as well. In fact, $\operatorname{div} xy = P + Q + P' + Q' = \operatorname{div} zw$. Thus, $(X, \operatorname{div} x)$ or $(X, \operatorname{div} xy)$ are example where the aforementioned setup holds. Similarly, we may let $X = \operatorname{Spec} R$ with R as in Example 2.15. Then, if we consider $R(-Q) = \mathfrak{q} := (x, y, z)$, by symmetry, (X, Q) is a purely F -regular pair as well and $P + Q = \operatorname{div} ux = \operatorname{div} vy = \operatorname{div} wz$.¹⁹ Thus, $(X, \operatorname{div} ux)$ is another example. In any of these examples $(X, \operatorname{div} f)$, we wonder what the structure of $\operatorname{Rev}^{\operatorname{div} f}(X)$ is.

4B2. Main theorem. With Section 4B1 in place, we are ready to establish our main result. First, we make the following observation.

Remark 4.11. An interesting, conceptual consequence of Propositions 4.4 and 4.6, and Theorem 4.7 is that we may think of the objects in the Galois category $\operatorname{Rev}^P(X^\circ)$ as quintuples $(S, \mathfrak{n}, \ell, L, Q)$ where Q is a prime divisor minimal center of F -purity, which corresponds to the only height 1 prime divisor lying over \mathfrak{p} ; namely, the splitting prime of both $f^*\mathcal{C}_R^P \subset \mathcal{C}_S^Q$, say \mathfrak{q} . In particular, (S, Q) is a purely F -regular pair. Applying [Carvajal-Rojas and Stäbler 2023, Theorem 4.8] (note that its assumptions are verified by Proposition 4.6), we have

$$1 \geq r(S, Q) = [\kappa(\mathfrak{q}) : \kappa(\mathfrak{p})] \cdot r(R, P) > 0.$$

Hence, $[\kappa(\mathfrak{q}) : \kappa(\mathfrak{p})] \leq 1/r(R, P)$. In retrospective, we also see that Q happens to be the divisor $P^* = f^*P - \operatorname{Ram}$ in (4.4.1).

¹⁸In particular, $(R/f, (x, y)/f)$ is a purely F -regular pair where R/f is not normal — this is the counter Remark 2.6 is referring to.

¹⁹Indeed, one verifies that the ideal of R generated by u is the quotient of the ideal $(u, \Delta_1, \Delta_2, \Delta_1) = (u, vx, wx, \Delta_1) = (u, v, w) \cap (u, x, \Delta_1)$ of A , where the latter is a prime decomposition.

Theorem 4.12. *Work in Setup 3.9 and suppose that (X, P) is a purely F -regular pair. Then, $\text{Rev}^P(X^\circ)$ is P -irreducible and has both inertial boundedness and tameness. In particular, there exists an exact sequence of topological groups*

$$\widehat{\mathbb{Z}}^{(P)} \rightarrow \pi_1^{t,P}(X^\circ) \rightarrow \pi_{1,\text{ét}}^P(X^\circ) \rightarrow 1,$$

where $\pi_{1,\text{ét}}^P(X^\circ)$ is a finite group of order at most $\min\{1/r(R, P), 1/s(R)\}$ and prime-to- p . Furthermore, if P is a prime-to- p torsion element of $\text{Cl } X$, the homomorphism $\widehat{\mathbb{Z}}^{(P)} \rightarrow \pi_1^{t,P}(X^\circ)$ is injective and so we have a short exact sequence

$$0 \rightarrow \widehat{\mathbb{Z}}^{(P)} \rightarrow \pi_1^{t,P}(X^\circ) \rightarrow \pi_{1,\text{ét}}^P(X^\circ) \rightarrow 1,$$

which splits if and only if P is the trivial element of $\text{Cl } X$. If P is nontorsion, we have a short exact sequence

$$0 \rightarrow \varprojlim_{n \in N^P(X^\circ)} \mathbb{Z}/n\mathbb{Z} \rightarrow \pi_1^{t,P}(X^\circ) \rightarrow \pi_{1,\text{ét}}^P(X^\circ) \rightarrow 1$$

which splits if and only if $N^P(X^\circ) = M^P(X^\circ)$ and there is a compatible system $\{\frac{1}{n}P \in \text{Cl } X\}_{n \in M^P(X^\circ)}$ of factors of P .

Proof. This is an application of Theorem 3.29 and Section 4B1; see Remark 4.11. Indeed, P -irreducibility holds by Theorem 4.7. Inertial boundedness was explained in Remark 4.11 whereas inertial tameness follows from Proposition 4.6. For the statements regarding the order of G , recall that it is realized as the Galois group of a universal étale-over- P cover $\tilde{X}^\circ \rightarrow X^\circ$. In particular, its generic degree equals $[\kappa(\tilde{\mathfrak{p}}) : \kappa(\mathfrak{p})]$, which is bounded by both $1/r(R, P)$ and $1/s(R)$; for the latter bound simply use [Carvajal-Rojas et al. 2018, Theorem 3.11]. □

Remark 4.13. It is an important folklore conjecture that the divisor class group of a strongly F -regular singularity is finitely generated. We were taught about this question by Karl Schwede but believe that it was originally raised by Melvin Hochster. For more, see [Polstra 2022]. It is known that the torsion subgroup is finite in this case; see [Polstra 2022; Martin 2022]. Finite generation of the class group is known to be true in dimension ≤ 3 ; see [Carvajal-Rojas et al. 2020]. Whenever finite generation of the class group is known, we may improve upon Theorem 4.12 to say that $\pi_1^{t,P}(X^\circ) \in \text{Ext}(G, \mathbb{Z}/n\mathbb{Z})$ for some $n \gg 0$ (in particular finite) and it is a trivial extension if P is n -divisible in $\text{Cl } X$ with $\frac{1}{n} \cdot P$ Cartier on U .

Remark 4.14. In Theorem 4.12, if $X^\circ = X_{\text{reg}}$, we may replace $\pi_{1,\text{ét}}^P(X^\circ)$ with $G = \pi_1^{\text{ét}}(X_{\text{reg}})$ by Proposition 3.26. By [Taylor 2019, Corollary 1.2], $\min\{1/r(R, P), 1/s(R)\} = 1/s(R)$ if P is prime-to- p torsion in $\text{Cl } X$.

Corollary 4.15. *Let $f: Y \rightarrow X$ be a quasiétale cover. If there is a divisor Δ on X such that (X, Δ) is purely F -regular and $r(\mathcal{O}_{X,x}, \Delta) > \frac{1}{2}$ for all $x \in X$, then f is étale.*

Proof. The proof is *mutatis mutandis* the same as in [Carvajal-Rojas et al. 2018, Corollary 3.3]. □

Remark 4.16. In light of [Taylor 2019, Corollary 1.2], it is unclear to the authors whether there are cases where Corollary 4.15 improves upon [Carvajal-Rojas et al. 2018, Corollary 3.3]. One potential candidate for such examples would be determinantal singularities. In [Carvajal-Rojas 2018, Example 4.12], the first named author proved; based on [Cutkosky 1995], that determinantal singularities satisfy purity of the branch locus. With notation as in Question 2.19, it is known that the F -signature of $C_{1,2}$ is $\frac{11}{24} = \frac{1}{2} - \frac{1}{24}$; see [Singh 2005]. On the other hand, we have estimated that $r(C_{1,2}, P) \geq \frac{1}{6}$ in Example 2.15. Nonetheless, our methods were not sufficient to prove (nor disprove) that $r(C_{1,2}, P) > \frac{1}{2}$.

Corollary 4.17. *In the setup of Theorem 4.12, the conclusion of Lemma 3.34 holds.*

Example 4.18 (determinantal singularities). Let R be a determinantal singularity with P a prime divisor generating $\text{Cl } R$; see Question 2.19. Then, $\pi_1^{\text{ét}}(X^\circ)$ is trivial for all Z by [Carvajal-Rojas 2018, Example 4.12]. Therefore, if (R, P) is a purely F -regular pair; see Question 2.19, then $\pi_1^{t,P}(X^\circ)$ is trivial too as P is not divisible in $\text{Cl } X$.

Question 4.19. Let $(X, \text{div } f)$ be any of the examples in Example 4.10. Does Abhyankar's lemma hold for $(X, \text{div } f)$?

Example 4.20 (graded hypersurfaces). With notation as in Example 2.11, suppose that A is strongly F -regular. If n is prime-to- p , then $\pi_1^{t,P}(X_{\text{reg}})$ is a nontrivial element of $\text{Ext}(\mathbb{Z}/n\mathbb{Z}, \hat{\mathbb{Z}}^{(p)})$. Indeed, the corresponding degree n cyclic cover is its universal étale-over- P cover. If n is a p -power — R might be referred to as a Zariski hypersurface — its étale-over- P universal cover is trivial; see [Murre 1967, Proposition 7.2.2]. Therefore, all we can say is that there is a surjection $\hat{\mathbb{Z}}^{(p)} \rightarrow \pi_1^{t,P}(X^\circ)$. Determining the kernel of this surjection may require obtaining an analog of [loc. cit., Proposition 7.2.2] for the category $\text{Rev}^P(X^\circ)$.

5. Tame fundamental groups: Characteristic zero

The goal of this section is to prove the following by reduction to positive characteristics.

Theorem 5.1. *Let (X, Δ) be a log canonical pair, $\dim X \geq 2$, $x \in X$ be a closed point, and $Z \subset X$ be a closed subscheme of codimension ≥ 2 . Denote by P the minimal LC center through x which we assume to be a divisor. Write $X^\circ = \text{Spec } \mathcal{O}_{X,\bar{x}}^{\text{sh}} \setminus Z$ and denote by Δ and P the pullback of Δ and P to X° . Then, $\text{Rev}^P(X^\circ)$ is P -irreducible and has inertial boundedness. In particular, there exists an exact sequence of topological groups*

$$\hat{\mathbb{Z}} \rightarrow \pi_1^{t,P}(X^\circ) \rightarrow \pi_{1,\text{ét}}^P(X^\circ) \rightarrow 1,$$

where $\pi_{1,\text{ét}}^P(X^\circ)$ is finite. Furthermore, if P is a torsion element of $\text{Cl } X$, the homomorphism $\hat{\mathbb{Z}} \rightarrow \pi_1^{t,P}(X^\circ)$ is injective and so we have a short exact sequence

$$0 \rightarrow \hat{\mathbb{Z}} \rightarrow \pi_1^{t,P}(X^\circ) \rightarrow \pi_{1,\text{ét}}^P(X^\circ) \rightarrow 1,$$

which splits if and only if P is the trivial element of $\text{Cl } X$. If $P \in \text{Cl } X$ is nontorsion, we have a short exact sequence

$$0 \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow \pi_1^{\text{t},P}(X^\circ) \rightarrow \pi_{1,\text{ét}}^P(X^\circ) \rightarrow 1$$

which splits if and only if there is a divisor D such that $P = nD$ in $\text{Cl } X$ and $D|_U$ is Cartier.

Proof. In order to prove Theorem 5.1, recall that we may work in Setup 2.20. We want to use Theorem 3.29, and thus need to verify that P -irreducibility and inertial boundedness 3.21 hold for the PLT pair $(R = \mathcal{O}_{X,\bar{x}}^{\text{sh}}, \Delta)$. This will be proven below in Proposition 5.2 and Proposition 5.3 respectively.

We still need to explain why, if P is nontorsion, the set $N^P(X^\circ)$ is finite so that (3.29.4) holds. This however is a direct consequence of [Bingener and Flenner 1984, Theorem 6.1]. \square

Proposition 5.2. *Work in Setup 2.20. Then $\text{Rev}^P(X^\circ)$ satisfies P -irreducibility.*

Proposition 5.3. *Work in Setup 2.20. Then $\text{Rev}^P(X^\circ)$ satisfies inertial boundedness.*

We shall see that inertial boundedness follows from minor modifications of the arguments in [Bhatt et al. 2017]; see Section 5B below. Thus, we prove inertial boundedness by spreading out. While a prove of P -irreducibility is also possible via spreading out, there is a direct proof in characteristic zero which we give below. We are thankful to Karl Schwede for pointing this out to us.

Corollary 5.4. *In the setup of Theorem 5.1, the conclusion of Lemma 3.34 holds.*

5A. P -irreducibility in characteristic zero. We need some preparatory lemmata. Recall that an *étale neighborhood* of a geometric point $\bar{x} \rightarrow \text{Spec } R$ is a factorization through an étale morphism $\text{Spec } R' \rightarrow \text{Spec } R$.

Lemma 5.5. *Let R be normal domain and R^{sh} be its strict henselization at a closed point $x \in \text{Spec } R$. Let $f : \text{Spec } S \rightarrow \text{Spec } R^{\text{sh}}$ be a finite dominant morphism. Then, there exists a connected étale neighborhood $\text{Spec } R'$ of \bar{x} and a cartesian square*

$$\begin{array}{ccc} \text{Spec } S & \xrightarrow{f} & \text{Spec } R^{\text{sh}} \\ \downarrow g & & \downarrow h \\ \text{Spec } S' & \xrightarrow{f'} & \text{Spec } R' \end{array} \tag{5.5.1}$$

with f' finite. Furthermore, if $\mathfrak{p} \subset R$ is a height 1 prime such that $\mathfrak{p}R^{\text{sh}}$ is prime, then $h(\mathfrak{p}R^{\text{sh}})$ is a height-1 prime of R and $h^{-1}(h(\mathfrak{p}R^{\text{sh}})) = \mathfrak{p}R^{\text{sh}}$. Finally, if R is local then R' is normal and S' is normal if and only if S is normal.

Proof. Fix generators (a_1, \dots, a_m) of \mathfrak{p} and write $S = R^{\text{sh}}[b_1, \dots, b_e]$. As $R^{\text{sh}} \rightarrow S$ is finite, there are monic polynomials $f_i \in R^{\text{sh}}[T]$ with $f_i(b_i) = 0$. We denote the coefficients of these f_i by c_{ij} . Since R^{sh} is obtained as a filtered colimit of connected étale neighborhoods $R \rightarrow R'$ of \bar{x} , there is some $R \rightarrow R'$ in the colimit system such that R' contains all the a_i and c_{ij} . By construction, $R \rightarrow R'$ is étale and setting $S' = R'[b_1, \dots, b_e]$ one readily checks that the above diagram is a pullback square. In particular, f' is

finite by construction. Since the fibers of $R \rightarrow R'$ are of dimension zero, $h(\mathfrak{p}R^{\text{sh}}) = \mathfrak{p}R'$ is of height 1. Clearly, $h^{-1}(h(\mathfrak{p}R^{\text{sh}})) = \mathfrak{p}R^{\text{sh}}$.

For the final assertion, note that the weakly étale homomorphism $R' \rightarrow R^{\text{sh}}$ is faithfully flat since $\mathfrak{m}R^{\text{sh}}$ is the maximal ideal of R^{sh} . Since (5.5.1) is a pullback square, $S' \rightarrow S$ is a weakly étale faithfully flat homomorphism too. Thus S' is normal if and only if S is and similarly for R' and R^{sh} by [Stacks 2005–, Lemma 033G and Tag 0950]. \square

Remark 5.6. If $R \rightarrow R^{\text{sh}}$ is the strict henselization with respect to some maximal ideal \mathfrak{m} then, given any ideal $\mathfrak{a} \subset \mathfrak{m}$ such that R/\mathfrak{a} is normal, the extension $\mathfrak{a}R^{\text{sh}}$ is prime. Indeed, we may localize R at \mathfrak{m} and thus assume that R is a local ring. Then, the assertion follows from $R^{\text{sh}} \otimes R/I = (R/I)^{\text{sh}}$ for any ideal $I \subset R$ [Stacks 2005–, Lemma 05WS] and the fact that S^{sh} is a normal domain if and only if S is a normal domain [Stacks 2005–, Lemma 033G].

Lemma 5.7. *Let $g: \text{Spec } T \rightarrow \text{Spec } R$ be a surjective étale morphism or a surjective pro-étale morphism. Let $f: \text{Spec } S \rightarrow \text{Spec } R$ be a morphism. Consider the base change diagram:*

$$\begin{array}{ccc} \text{Spec } S \otimes_R T & \xrightarrow{f'} & \text{Spec } T \\ \downarrow g' & & \downarrow g \\ \text{Spec } S & \xrightarrow{f} & \text{Spec } R \end{array}$$

The morphism f is tame with respect to D , if and only if f' is tame with respect to $g^{-1}(D)$.

Proof. The “only if” implication follows from [Grothendieck and Murre 1971, Lemma 2.2.7]. For the converse, by [Stacks 2005–, Lemmas 033C and 033G], R is normal if and only if T is normal. Likewise, S is normal if and only if $T \otimes_R S$ is normal. Thus, it makes sense to talk about tame morphisms. The remaining assertion is a consequence of [Grothendieck and Murre 1971, Proposition 2.2.9]. \square

Proposition 5.8. *Let (X, Δ) be an affine PLT pair where $\lfloor \Delta \rfloor = P$ is a prime divisor. If $g: Y \rightarrow X$ is a tamely ramified cover over P , then $(g^{-1}(P))_{\text{red}}$ is a normal divisor*

Proof. Write $\Delta = P + \Delta_1$. By [Kollár 2013, Corollary 2.43, (2.41.4)] the pair (Y, Δ') is PLT, where $\Delta' = (g^{-1}(P))_{\text{red}} + g^*\Delta_1$, and $K_{Y'} + \Delta' \sim_{\mathbb{Q}} g^*(K_X + \Delta)$. Note that $\lfloor g^*\Delta_1 \rfloor = 0$. Indeed, since (X, Δ) is PLT, Δ_1 and P have no components in common. Since g is étale over $X \setminus P$ the assertion follows. In this way, we see that $(g^{-1}(P))_{\text{red}}$ is a minimal LC center for some closed point $y \in Y$. Hence, by [Fujino and Gongyo 2012, Theorem 7.2] $(g^{-1}(P))_{\text{red}}$ is normal. \square

Proof of Proposition 5.2. We use the notation of Setup 2.20 and write R^{sh} for $\mathcal{O}_{X,x}^{\text{sh}}$. Let $V \rightarrow \text{Spec } R^{\text{sh}} \setminus Z$ be a cover in $\text{Rev}^P(\text{Spec } R^{\text{sh}} \setminus Z)$. Denote the integral closure of R^{sh} inside $\mathcal{O}_V(V)$ by S . Using Lemma 5.5,

we obtain a cartesian square:

$$\begin{array}{ccc} \text{Spec } S & \xrightarrow{f} & \text{Spec } R^{\text{sh}} \\ \downarrow g & & \downarrow h \\ \text{Spec } S' & \xrightarrow{f'} & \text{Spec } R' \end{array}$$

with f' finite and R' a connected étale neighborhood of $\bar{x} \rightarrow W \subseteq X$, where W is some Zariski open neighborhood of $x \in X$. As usual, we write \mathfrak{p} for the prime corresponding to our fixed prime divisor P on X . As f is finite, S is also strictly henselian [Stacks 2005–, Tag 04GH] and S is the strict henselization of S' with respect to some ideal \mathfrak{n} lying over x .

Since R/\mathfrak{p} is normal as a minimal LC center Theorem 2.23, we deduce from Remark 5.6 that $\mathfrak{p}R^{\text{sh}}$ is prime. Write $\mathfrak{p}' = h(\mathfrak{p}R^{\text{sh}})$. Using Lemma 5.5 again, we have that $h^{-1}(\mathfrak{p}') = \mathfrak{p}R^{\text{sh}}$. Note that f' is tamely ramified with respect to P' by Lemma 5.7. Since $\text{Spec } R'$ is an étale neighborhood of $\bar{x} \rightarrow X$, say $\varphi: \text{Spec } R' \rightarrow X$, we conclude that $(\text{Spec } R', \varphi^*(\Delta))$ is PLT with $[\Delta] = P'$. Thus we can apply Proposition 5.8 to conclude that $Q' = (f'^{-1}(P'))_{\text{red}}$ is normal. We denote the corresponding ideal by \mathfrak{q}' and note that $\mathfrak{q}' \subseteq \mathfrak{n}$. Using Remark 5.6 we see that $\mathfrak{q} := \mathfrak{q}'S$ is prime. In other words, there is only one prime in S' lying over \mathfrak{p}' and contained in \mathfrak{n} . Assume now that $\mathfrak{a} \in f^{-1}(\mathfrak{p})$. Then $h(f(\mathfrak{a})) = \mathfrak{p}'$ and hence $f'(g(\mathfrak{a})) = \mathfrak{p}'$. In particular, $g(\mathfrak{a}) \in f'^{-1}(\mathfrak{p}')$. But clearly, $g(\mathfrak{a}) \subseteq \mathfrak{n}$. Hence, $\mathfrak{a} = \mathfrak{q}$ as desired. \square

5B. Inertial boundedness via spread-out. In the situation of Setup 2.20, write $Y = \text{Spec } \mathcal{O}_{X,x}^{\text{sh}}$ and Y_{reg} for its regular locus. By Corollary 3.27, it suffices to show that inertial boundedness holds for Y_{reg} . To this end, we use the result of [Bhatt et al. 2017, Theorem 1.1], where finiteness of $\pi_1(Y \setminus \{x\})$ is proved via reduction mod p . The proof of [loc. cit., Theorem 1.1] is a combination of Theorem 4.1 and Propositions 5.1 and 6.4 in [loc. cit.]. We can directly apply the latter two in our situation. The argument of Theorem 4.1 needs to be modified slightly. We record this below for completeness.

We will use the following notation for spreading out: If R is a κ -algebra, $A \subset \kappa$ a finitely generated \mathbb{Z} -algebra, then we will write R_A for any fixed finite type A algebra whose base changed generic fiber $R_A \otimes_A \text{Frac}(A) \otimes_{\text{Frac}(A)} \kappa$ recovers R . If $s \in \text{Spec } A$ is a point, then we will write R_s for the corresponding fiber of R_A . We will use similar notation for schemes.

Theorem 5.9. *Let A be a finitely generated \mathbb{Z} -algebra equipped with an embedding $A \rightarrow \mathbb{C}$. Fix an affine finite type scheme X_A over $\text{Spec } A$, a closed point $x_a \in X_A$, and a closed subset $Z_A \subset X_A$ of codimension ≥ 2 . Let us denote by X, Z , and x the base changes to $\text{Spec } \mathbb{C}$. Let us furthermore assume that X is normal. Then, there is a dense open $V \subset \text{Spec } A$ such that for every morphism $\text{Spec } \kappa \rightarrow V$ with κ an algebraically closed field of characteristic p there is a canonical isomorphism*

$$\pi_1(\text{Spec } \mathcal{O}_{X,x}^{\text{sh}} \setminus Z)^{(p)} \cong \pi_1(\text{Spec } \mathcal{O}_{X_\kappa, x_\kappa}^{\text{sh}} \setminus Z_\kappa)^{(p)},$$

where by abuse of notation we write Z for $\alpha^{-1}(Z)$ where $\alpha: \text{Spec } \mathcal{O}_{X,x}^{\text{sh}} \rightarrow \text{Spec } \mathcal{O}_X$ is the canonical morphism and similarly for Z_κ .

Proof. Using resolution of singularities, we may choose a truncated proper hypercover $f : Y_\bullet \rightarrow X$ indexed by $\bullet \in \Delta_{\leq 2}^{\text{op}}$ with Y_i smooth and $D_\bullet := f^{-1}(Z)_{\text{red}} \subset Y_\bullet$ giving an SNC divisor at each level. Moreover, by first blowing up x and then Z , so that both are Cartier divisors, we have that $E_\bullet := f^{-1}(x)_{\text{red}} \subset Y_\bullet$ also yields an SNC divisor at each level. Denoting by I_\bullet the finite index set of components of D_\bullet , each $D_{\bullet,i}$ is smooth over \mathbb{C} and proper over Z . Denoting by J_\bullet the subset of I_\bullet that yields the components of E_\bullet , we also obtain that the $E_{\bullet,j}$ are smooth and proper varieties over \mathbb{C} . We write $U_\bullet := Y_\bullet \setminus D_\bullet$. Let $\mathcal{Y}_{\bullet,\ell} \rightarrow Y_\bullet$ be the ℓ -th root stack associated to the divisors in D_\bullet and let $\mathcal{E}_{\bullet,\ell} \rightarrow E_\bullet$ be its pullback to E_\bullet . Now, we base change everything along $\alpha : \text{Spec } \mathcal{O}_{X,x}^{\text{sh}} \rightarrow \text{Spec } \mathcal{O}_X$ adding a superscript sh for base changes, e.g., $U_\bullet^{\text{sh}} := U_\bullet \times_X \text{Spec } \mathcal{O}_{X,x}^{\text{sh}}$. The appropriate pullback maps induce equivalences

$$\begin{aligned} \text{F}\acute{\text{E}}\text{t}(\text{Spec } \mathcal{O}_{X,x}^{\text{sh}} \setminus Z) &\rightarrow \lim_{\bullet \in \Delta_{\leq 2}} \text{F}\acute{\text{E}}\text{t}(U_\bullet^{\text{sh}}) \leftarrow \lim_{\ell} \text{colim}_{\ell} \text{F}\acute{\text{E}}\text{t}(\mathcal{Y}_{\bullet,\ell}^{\text{sh}}) \\ &\rightarrow \lim_{\bullet \in \Delta_{\leq 2}} \text{colim}_{\ell} \text{F}\acute{\text{E}}\text{t}(\mathcal{E}_{\bullet,\ell}) \cong \text{colim}_{\ell} \lim_{\bullet \in \Delta_{\leq 2}} \text{F}\acute{\text{E}}\text{t}(\mathcal{E}_{\bullet,\ell}). \end{aligned}$$

From left to right, these equivalences are given by Lemmas 2.1, 2.8(2) and 2.2 in [Bhatt et al. 2017], and the isomorphism is due to the fact that filtered colimits commute with finite limits. Having made these minor changes, the rest of the argument now proceeds exactly as [loc. cit., Theorem 4.1]. \square

Proof of Proposition 5.3. Let us write $Y = \text{Spec } \mathcal{O}_{X,x}^{\text{sh}}$. By Corollary 3.27 (and its proof), it suffices to show that $\pi_1(Y_{\text{reg}})$ is finite. Using Proposition 2.21, we may perturb Δ to Δ' so that (X, Δ') is KLT. The nonregular locus of Y is cut out by a radical ideal I and likewise the closed subset Z is also given by some radical ideal J . Passing to a connected étale neighborhood $f : \text{Spec } R' \rightarrow \text{Spec } R$ of \bar{x} ; where $\text{Spec } R$ is some Zariski neighborhood of x , we may assume that $I, J \subset R'$. Note that $(\text{Spec } R', f^*\Delta')$ is also KLT; see [Kollár 2013, 2.14(2)].

Spreading out over some finitely generated \mathbb{Z} -algebra A and passing to closed fibers, we obtain pairs $(\text{Spec } R'_s, f^*\Delta'_s)$ that are F -regular for all s in a dense open of $\text{Spec } A$ (by [Takagi 2004, Corollary 3.4]). By the Nullstellensatz applied to the Jacobson ring A , $\kappa(s)$ is finite and its algebraic closure $\kappa(\bar{s})$ is a separable. Hence, $(\text{Spec } R'_s, f^*\Delta'_s)$ is also F -regular. Write $Y_{\bar{s}}$ for the spectrum of a strict henselization of R'_s at $x_{\bar{s}}$ and $W_{\bar{s}}$ for the closed subset defined by $I_{\bar{s}}$. Applying [Carvajal-Rojas et al. 2018, Theorem 5.1] we get $\pi_1(Y_{\bar{s}} \setminus W_{\bar{s}}) \leq 1/s(Y_{\bar{s}})$. Apply [Bhatt et al. 2017, Propositions 6.4 and 5.1] and Theorem 5.9 to conclude that $\pi_1(X_{\text{reg}})$ is finite. \square

Appendix: Splitting primes under strict henselizations

The goal of this appendix is to show that taking the splitting prime commutes with strict henselization. That is, if $p(\mathcal{C}) = p(R, \mathcal{C}) \subset R$ is the splitting prime for some Cartier algebra \mathcal{C} acting on $(R, \mathfrak{m}, \kappa)$ and $f : \text{Spec } R^{\text{sh}} \rightarrow \text{Spec } R$ is the strict henselization with respect to \mathfrak{m} , then $p(\mathcal{C})R^{\text{sh}} = p(f^*\mathcal{C})$. To make sense of this we first need to explain the notion $f^*\mathcal{C}$.

Lemma A.1. *Let R be a noetherian ring. Consider a colimit over a directed system of ring homomorphisms $\{f_{ij} : S_i \rightarrow S_j\}$ of R -algebras, a Cartier R -algebra \mathcal{C} and a \mathcal{C} -module M . Assume that all of the*

morphisms f_{ij} and one structural map $R \rightarrow S_i$ are either finite, étale, or smooth. Then, $\mathcal{D} = \operatorname{colim} g_{ij}^* \mathcal{C}$ exists and $\mathcal{M} = \operatorname{colim} g_{ij}^! M$ is naturally a \mathcal{D} -module, where we denote by $g_{ij}: \operatorname{Spec} S_j \rightarrow \operatorname{Spec} S_i$ the map corresponding to f_{ij} .

Proof. If $g: \operatorname{Spec} S \rightarrow \operatorname{Spec} R$ then by definition $g^* \mathcal{C} = \mathcal{C} \otimes_R S$ so that we obtain a corresponding directed system of Cartier algebras; see [Blickle and Stäbler 2019, Proposition 5.3]. We thus need to verify that the directed system of modules from which we construct \mathcal{M} are Cartier modules. This is true by [loc. cit., Theorem 5.5]. □

Lemma A.2. *Let $f: \operatorname{Spec} S \rightarrow \operatorname{Spec} R$ be a surjective (essentially of finite type) étale morphism of F -finite local rings. Then $p(f^* \mathcal{C}) = p(\mathcal{C})S$.*

Proof. By [Blickle and Stäbler 2019, Theorem 6.5],²⁰ R is F -regular if and only if S is so. Similarly, by [loc. cit., Proposition 5.13, Lemma 6.1], R is F -pure if and only if S is so. Therefore, we may assume that both splitting primes are nontrivial. Consider the following diagram:

$$\begin{array}{ccc} \operatorname{Spec} S & \xrightarrow{f} & \operatorname{Spec} R \\ \uparrow & & \uparrow \\ \operatorname{Spec} S/p(\mathcal{C})S & \xrightarrow{f'} & \operatorname{Spec} R/p(\mathcal{C}) \end{array}$$

By Lemma 2.8, $R/p(\mathcal{C})$ is F -regular. Since f' is étale, $S/p(\mathcal{C})S$ is also F -regular (note that since f is surjective the fiber is nonempty). Since the minimal primes of $p(\mathcal{C})$ are $f^* \mathcal{C}$ -submodules (see [Schwede 2010, Corollary 4.8]), any minimal prime of $p(\mathcal{C})S$ is a maximal proper $f^* \mathcal{C}$ -submodule. However, $p(f^* \mathcal{C})$ is unique and (since S is F -pure) the maximal proper $f^* \mathcal{C}$ -submodule. Thus, there is only one prime lying over $p(\mathcal{C})$. Since $R/p(\mathcal{C})$ is reduced and f' is étale, $\sqrt{p(\mathcal{C})S} = p(\mathcal{C})S$ is prime and so coincides with $p(f^* \mathcal{C})$. □

Proposition A.3. *Let $(R, \mathfrak{m}, \kappa, K)$ be a normal local domain and \mathcal{C} be a Cartier R -algebra. Denote by R^{sh} the strict henselization of (R, \mathfrak{m}) and by \mathcal{D} the R^{sh} -Cartier algebra obtained as a colimit over the corresponding system of étale algebras. Then, (R, \mathcal{C}) is F -pure if and only if $(R^{\text{sh}}, \mathcal{D})$ is so. Moreover, if $p(\mathcal{C})$ is the splitting prime of (R, \mathcal{C}) then $p(\mathcal{C})R^{\text{sh}} = p(\mathcal{D})$, where $p(\mathcal{D})$ is the splitting prime of $(R^{\text{sh}}, \mathcal{D})$. Conversely, $p(\mathcal{D}) \cap R = p(\mathcal{C})$.*

Proof. Strict henselizations are obtained by a filtered colimit. By [Stacks 2005–, Lemma 0032], we may even obtain it by a *small* filtered colimit. Moreover, having constructed R^{sh} via the usual direct limit of triples, we may *a posteriori* also obtain it as a filtered colimit of a system of étale maps by viewing everything as embedded in R^{sh} . Using Lemma A.1, we obtain \mathcal{D} .

If (R, \mathcal{C}) is F -pure, then also is $(R^{\text{sh}}, \mathcal{D})$ as well as $(S, \varphi^* \mathcal{C})$ for any (essentially) étale morphism $\varphi: \operatorname{Spec} S \rightarrow \operatorname{Spec} R$. Indeed, this follows from [Blickle and Stäbler 2019, Proposition 5.13] in the latter

²⁰Since we are only dealing with Cartier modules that do not have nonminimal associated primes, we may use test element theory in the sense of [Blickle 2013, Theorem 3.11]—thus we may weaken the assumption that the base is essentially of finite type over an F -finite field to F -finite.

case and the former case follows from the latter. Conversely, if $(R^{\text{sh}}, \mathcal{D})$ is not F -pure, say $x \notin \mathcal{D}_+ R^{\text{sh}}$, then we find a surjective étale morphism $\varphi: \text{Spec } S \rightarrow \text{Spec } R$ for which $x \in S$. Thus S is not F -pure but then by faithful flatness R is also not F -pure (using [loc. cit., Lemma 6.1]). In particular, if (R, \mathcal{C}) or $(R^{\text{sh}}, \mathcal{D})$ is not F -pure, then the statement about splitting primes is trivially true.

Assume that both (R, \mathcal{C}) and $(R^{\text{sh}}, \mathcal{D})$ are F -pure. Let $\varphi: \text{Spec } S \rightarrow \text{Spec } R$ be an étale morphism occurring in the colimit and $\mathfrak{n} \subset S$ a prime above \mathfrak{m} . As in the proof of [Stacks 2005–, Lemma 04GN], we may assume that $\mathfrak{m}S = \mathfrak{n}$. Since R^{sh} is local with maximal ideal $\mathfrak{m}R^{\text{sh}}$, the map $S \rightarrow R^{\text{sh}}$ factors through the localization $S_{\mathfrak{n}}$. Thus, $\varphi': \text{Spec } S_{\mathfrak{n}} \rightarrow \text{Spec } R$ is an essentially étale surjective homomorphism. We apply Lemma A.2 to conclude that the splitting prime $p(\varphi'^{\flat}\mathcal{C})$ of $S_{\mathfrak{n}}$ is $p(\mathcal{C})S_{\mathfrak{n}}$. Next, note that any homogeneous element of $\varphi'^{\flat}\mathcal{C}$ is of the form $\kappa \otimes s^q$ with $\kappa \in \mathcal{C}_e$, which acts on $x = r \otimes t \in R \otimes_R S_{\mathfrak{n}}$ as $\kappa \otimes s^q(r \otimes t) = \kappa(r) \otimes st$; see [Blickle and Stäbler 2019, Theorem 5.5]. Use now the well-known isomorphism $F_*^e R \otimes_R S_{\mathfrak{n}} \rightarrow F_*^e S_{\mathfrak{n}}$, $r \otimes s \mapsto rs^q$.

We now prove $p(\mathcal{C})R^{\text{sh}} \subset p(\mathcal{D})$. If $x \in p(\mathcal{C})R^{\text{sh}}$ and $\kappa \in \mathcal{D}_e$, there is an essentially étale morphism $\varphi': \text{Spec } S_{\mathfrak{n}} \rightarrow \text{Spec } R$ as above so that $x \in p(\mathcal{C})S_{\mathfrak{n}} = p(\varphi'^{\flat}\mathcal{C})$ and $\kappa \in \varphi'^{\flat}\mathcal{C}$. Then, since $x \in p(\varphi'^{\flat}\mathcal{C})$, we have $\kappa(x) \in \mathfrak{n} = \mathfrak{m}S \subset \mathfrak{m}R^{\text{sh}}$ and so $x \in p(\mathcal{D})$. Conversely, let $x \in p(\mathcal{D})$. Then, we find $\varphi': \text{Spec } S \rightarrow \text{Spec } R$ as above such that $x \in S$. Since $\kappa(x) \in \mathfrak{m}R^{\text{sh}}$ for all $\kappa \in \mathcal{D}$, we also have $\kappa(x) \in \mathfrak{m}R^{\text{sh}} \cap S = \mathfrak{n}$ for all $\kappa \in \varphi'^{\flat}\mathcal{C}$. Hence, $x \in p(\varphi'^{\flat}\mathcal{C}) = p(\mathcal{C})S \subset p(\mathcal{C})R^{\text{sh}}$ as desired.

We now show $p(\mathcal{D}) \cap R = p(\mathcal{C})$. If $x \in p(\mathcal{D}) \cap R$, for all $\kappa \in \mathcal{D}$ we have $\kappa(x) \in \mathfrak{m}R^{\text{sh}}$ and so $\kappa(x) \in \mathfrak{m}$ for all $\kappa \in \mathcal{C}$. If $x \in p(\mathcal{C})$ then $x \in p(\mathcal{C})R^{\text{sh}} = p(\mathcal{D})$ by the above. \square

Acknowledgements

We would like to thank Bhargav Bhatt, Manuel Blickle, Alessio Caminata, Eloísa Grifo, Zolt Patakfalvi, Karl Schwede, Anurag Singh, Ilya Smirnov, Roberto Svaldi, and Maciej Zdanowicz for very useful discussions and help throughout the preparation of this preprint. The authors are grateful to Karl Schwede for very valuable comments on a draft of this preprint and for suggesting us the use of adjoint ideals to study the perseverance of pure F -regularity. The first named author commenced working on this project while in his last year of Graduate School at the Department of Mathematics of the University of Utah. He is greatly thankful for their hospitality and support. He is particularly grateful to his advisor Karl Schwede for his guidance and generous support. We are also indebted to a diligent referee who pointed out several mistakes in an earlier version.

References

- [Ambro 1999] F. Ambro, *The adjunction conjecture and its applications*, Ph.D. thesis, Johns Hopkins University, 1999, available at <https://www.proquest.com/docview/304508793>. MR
- [Atiyah and Macdonald 1969] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Reading, MA, 1969. MR Zbl
- [Auslander 1962] M. Auslander, “On the purity of the branch locus”, *Amer. J. Math.* **84** (1962), 116–125. MR
- [Bhatt et al. 2017] B. Bhatt, O. Gabber, and M. Olsson, “Finiteness of étale fundamental groups by reduction modulo p ”, preprint, 2017. arXiv 1705.07303

- [Bingener and Flenner 1984] J. Bingener and H. Flenner, “Variation of the divisor class group”, *J. Reine Angew. Math.* **351** (1984), 20–41. MR Zbl
- [Blickle 2013] M. Blickle, “Test ideals via algebras of p^{-e} -linear maps”, *J. Algebraic Geom.* **22**:1 (2013), 49–83. MR Zbl
- [Blickle and Stäbler 2019] M. Blickle and A. Stäbler, “Functorial test modules”, *J. Pure Appl. Algebra* **223**:4 (2019), 1766–1800. MR Zbl
- [Blickle et al. 2012] M. Blickle, K. Schwede, and K. Tucker, “ F -signature of pairs and the asymptotic behavior of Frobenius splittings”, *Adv. Math.* **231**:6 (2012), 3232–3258. MR Zbl
- [Bruns and Vetter 1988] W. Bruns and U. Vetter, *Determinantal rings*, Lecture Notes in Mathematics **1327**, Springer, 1988. MR Zbl
- [Cadoret 2013] A. Cadoret, “Galois categories”, pp. 171–246 in *Arithmetic and geometry around Galois theory*, edited by P. Dèbes et al., Progr. Math. **304**, Springer, 2013. MR Zbl
- [Carvajal-Rojas 2018] J. A. Carvajal-Rojas, *Arithmetic aspects of strong F -regularity*, Ph.D. thesis, The University of Utah, 2018, available at <https://www.proquest.com/docview/2383059777>.
- [Carvajal-Rojas 2022] J. A. Carvajal-Rojas, “Finite torsors over strongly F -regular singularities”, *Épjournal Géom. Algébrique* **6** (2022), Art. 1, 30. MR Zbl
- [Carvajal-Rojas and Smolkin 2020] J. Carvajal-Rojas and D. Smolkin, “The uniform symbolic topology property for diagonally F -regular algebras”, *J. Algebra* **548** (2020), 25–52. MR Zbl
- [Carvajal-Rojas and Stäbler 2023] J. Carvajal-Rojas and A. Stäbler, “On the behavior of F -signatures, splitting primes, and test modules under finite covers”, *J. Pure Appl. Algebra* **227**:1 (2023), Paper No. 107165, 38. MR Zbl
- [Carvajal-Rojas et al. 2018] J. Carvajal-Rojas, K. Schwede, and K. Tucker, “Fundamental groups of F -regular singularities via F -signature”, *Ann. Sci. Éc. Norm. Supér.* (4) **51**:4 (2018), 993–1016. MR
- [Carvajal-Rojas et al. 2020] J. Carvajal-Rojas, J. Kollár, and A. Stäbler, “On the local étale fundamental group of KLT threefold singularities”, preprint, 2020. arXiv 2004.07628
- [Carvajal-Rojas et al. 2021] J. Carvajal-Rojas, K. Schwede, and K. Tucker, “Bertini theorems for F -signature and Hilbert-Kunz multiplicity”, *Math. Z.* **299**:1-2 (2021), 1131–1153. MR Zbl
- [Chinburg et al. 1996] T. Chinburg, B. Erez, G. Pappas, and M. J. Taylor, “Tame actions of group schemes: integrals and slices”, *Duke Math. J.* **82**:2 (1996), 269–308. MR Zbl
- [Cutkosky 1995] S. D. Cutkosky, “Purity of the branch locus and Lefschetz theorems”, *Compositio Math.* **96**:2 (1995), 173–195. MR Zbl
- [Fedder 1983] R. Fedder, “ F -purity and rational singularity”, *Trans. Amer. Math. Soc.* **278**:2 (1983), 461–480. MR Zbl
- [Fujino and Gongyo 2012] O. Fujino and Y. Gongyo, “On canonical bundle formulas and subadjunctions”, *Michigan Math. J.* **61**:2 (2012), 255–264. MR Zbl
- [Grothendieck and Murre 1971] A. Grothendieck and J. P. Murre, *The tame fundamental group of a formal neighbourhood of a divisor with normal crossings on a scheme*, Lecture Notes in Mathematics, Vol. 208 **208**, Springer, 1971. MR Zbl
- [Hara and Watanabe 2002] N. Hara and K.-I. Watanabe, “ F -regular and F -pure rings vs. log terminal and log canonical singularities”, *J. Algebraic Geom.* **11**:2 (2002), 363–392. MR Zbl
- [Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Grad. Texts in Math. **52**, Springer, 1977. MR Zbl
- [Jeffries and Smirnov 2022] J. Jeffries and I. Smirnov, “A transformation rule for natural multiplicities”, *Int. Math. Res. Not.* **2022**:2 (2022), 999–1015. MR Zbl
- [Katzman et al. 2014] M. Katzman, K. Schwede, A. K. Singh, and W. Zhang, “Rings of Frobenius operators”, *Math. Proc. Cambridge Philos. Soc.* **157**:1 (2014), 151–167. MR Zbl
- [Kerz and Schmidt 2010] M. Kerz and A. Schmidt, “On different notions of tameness in arithmetic geometry”, *Math. Ann.* **346**:3 (2010), 641–668. MR
- [Kollár 2013] J. Kollár, *Singularities of the minimal model program*, Cambridge Tracts in Mathematics **200**, Cambridge University Press, 2013. MR

- [Kollár and Mori 1998] J. Kollár and S. Mori, *Birational geometry of algebraic varieties*, Cambridge Tracts in Mathematics **134**, Cambridge University Press, 1998. MR Zbl
- [Kunz 2013] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Springer, 2013. MR Zbl
- [Lang 2002] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics **211**, Springer, New York, 2002. MR Zbl
- [Martin 2022] I. Martin, “The number of torsion divisors in a strongly F -regular ring is bounded by the reciprocal of F -signature”, *Comm. Algebra* **50**:4 (2022), 1595–1605. MR
- [Matsumura 1980] H. Matsumura, *Commutative algebra*, 2nd ed., Mathematics Lecture Note Series **56**, Benjamin/Cummings Publishing Co., Reading, MA, 1980. MR Zbl
- [Milne 1980] J. S. Milne, *Étale cohomology*, Princeton Math. Ser. **33**, Princeton Univ. Press, 1980. MR Zbl
- [Murre 1967] J. P. Murre, *Lectures on an introduction to Grothendieck's theory of the fundamental group*, Tata Institute of Fundamental Research Lectures on Mathematics **40**, Tata Institute of Fundamental Research, Bombay, 1967. MR Zbl
- [Nagata 1958] M. Nagata, “Remarks on a paper of Zariski on the purity of branch loci”, *Proc. Nat. Acad. Sci. U.S.A.* **44** (1958), 796–799. MR Zbl
- [Nagata 1959] M. Nagata, “On the purity of branch loci in regular local rings”, *Illinois J. Math.* **3** (1959), 328–333. MR Zbl
- [Polstra 2022] T. Polstra, “A theorem about maximal Cohen–Macaulay modules”, *Int. Math. Res. Not.* **2022**:3 (2022), 2086–2094. MR Zbl
- [Roman 2006] S. Roman, *Field theory*, 2nd ed., Graduate Texts in Mathematics **158**, Springer, 2006. MR Zbl
- [Schwede 2009] K. Schwede, “ F -adjunction”, *Algebra Number Theory* **3**:8 (2009), 907–950. MR Zbl
- [Schwede 2010] K. Schwede, “Centers of F -purity”, *Math. Z.* **265**:3 (2010), 687–714. MR Zbl
- [Schwede and Tucker 2014] K. Schwede and K. Tucker, “On the behavior of test ideals under finite morphisms”, *J. Algebraic Geom.* **23**:3 (2014), 399–443. MR Zbl
- [Serre 1979] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics **67**, Springer, 1979. MR Zbl
- [SGA 1 1971] A. Grothendieck, *Revêtements étales et groupe fondamental (Séminaire de Géométrie Algébrique du Bois Marie 1960–1961)*, Lecture Notes in Math. **224**, Springer, 1971. MR Zbl
- [Singh 2005] A. K. Singh, “The F -signature of an affine semigroup ring”, *J. Pure Appl. Algebra* **196**:2-3 (2005), 313–321. MR Zbl
- [Singh and Spiroff 2007] A. K. Singh and S. Spiroff, “Divisor class groups of graded hypersurfaces”, pp. 237–243 in *Algebra, geometry and their interactions*, edited by A. Corso et al., Contemp. Math. **448**, Amer. Math. Soc., Providence, RI, 2007. MR
- [Smolkin 2019] D. Smolkin, *Subadditivity of test ideals and diagonal F -regularity*, Ph.D. thesis, 2019, available at <https://www.proquest.com/docview/2505371578>. MR
- [Smolkin 2020] D. Smolkin, “A new subadditivity formula for test ideals”, *J. Pure Appl. Algebra* **224**:3 (2020), 1132–1172. MR Zbl
- [Speyer 2020] D. E. Speyer, “Frobenius split subvarieties pull back in almost all characteristics”, *J. Commut. Algebra* **12**:4 (2020), 573–579. MR Zbl
- [Stäbler 2017] A. Stäbler, “Test module filtrations for unit F -modules”, *J. Algebra* **477** (2017), 435–471. MR Zbl
- [Stacks 2005–] “The Stacks project”, electronic reference, 2005–, available at <http://stacks.math.columbia.edu>.
- [Takagi 2004] S. Takagi, “An interpretation of multiplier ideals via tight closure”, *J. Algebraic Geom.* **13**:2 (2004), 393–415. MR Zbl
- [Takagi 2008] S. Takagi, “A characteristic p analogue of plt singularities and adjoint ideals”, *Math. Z.* **259**:2 (2008), 321–341. MR Zbl
- [Takagi 2010] S. Takagi, “Adjoint ideals along closed subvarieties of higher codimension”, *J. Reine Angew. Math.* **641** (2010), 145–162. MR Zbl
- [Taylor 2019] G. Taylor, “Inversion of adjunction for F -signature”, preprint, 2019. arXiv 1909.10436
- [Tomari and Watanabe 1992] M. Tomari and K. Watanabe, “Normal Z_r -graded rings and normal cyclic covers”, *Manuscripta Math.* **76**:3-4 (1992), 325–340. MR Zbl

[Xu 2014] C. Xu, “Finiteness of algebraic fundamental groups”, *Compos. Math.* **150**:3 (2014), 409–414. MR Zbl

[Yao 2006] Y. Yao, “Observations on the F -signature of local rings of characteristic p ”, *J. Algebra* **299**:1 (2006), 198–218. MR

[Zariski 1958] O. Zariski, “On the purity of the branch locus of algebraic functions”, *Proc. Nat. Acad. Sci. U.S.A.* **44** (1958), 791–796. MR Zbl

Communicated by Bhargav Bhatt

Received 2020-05-06 Revised 2022-02-25 Accepted 2022-04-04

javier.carvajal-rojas@kuleuven.be

KU Leuven, Heverlee, Belgium

staebler@math.uni-leipzig.de

Mathematisches Institut, Universität Leipzig, Leipzig, Germany

Constructions of difference sets in nonabelian 2-groups

T. Applebaum, J. Clikeman, J. A. Davis, J. F. Dillon,
J. Jedwab, T. Rabbani, K. Smith and W. Yolland

*Dedicated to the memory of Robert A. Liebler, a friend and mentor, and a passionate advocate
for studying the action of finite nonabelian groups on combinatorial designs.*

Difference sets have been studied for more than 80 years. Techniques from algebraic number theory, group theory, finite geometry, and digital communications engineering have been used to establish constructive and nonexistence results. We provide a new theoretical approach which dramatically expands the class of 2-groups known to contain a difference set, by refining the concept of covering extended building sets introduced by Davis and Jedwab in 1997. We then describe how product constructions and other methods can be used to construct difference sets in some of the remaining 2-groups. In particular, we determine that all groups of order 256 not excluded by the two classical nonexistence criteria contain a difference set, in agreement with previous findings for groups of order 4, 16, and 64. We provide suggestions for how the existence question for difference sets in 2-groups of all orders might be resolved.

1. Motivation and overview

Difference sets were introduced by Singer [1938] as regular automorphism groups of projective geometries. These examples are contained in the multiplicative group of a finite field, and hence the difference sets in those geometric settings occur in cyclic groups. In the decades following, difference sets were discovered in other abelian groups and subsequently in nonabelian groups. The central objective is to determine which groups contain at least one difference set. Researchers have developed a range of techniques in pursuit of this objective, taking advantage of connections with design theory, coding theory, cryptography, sequence design, and digital communications.

A k -subset D of a group G of order v is a *difference set* with parameters (v, k, λ) if, for all nonidentity elements g in G , the equation

$$xy^{-1} = g$$

has exactly λ solutions (x, y) with $x, y \in D$; the related parameter n is defined to be $k - \lambda$. The complement of a difference set with parameters (v, k, λ) is itself a difference set, with parameters $(v, v - k, v - 2k + \lambda)$ and the same related parameter n . The difference set is nontrivial if $1 < k < v - 1$. A (v, k, λ) difference set in G is equivalent to a symmetric (v, k, λ) design with a regular automorphism group G [Beth et al. 1999].

Davis was supported by NSA grant H98230-12-1-0243. Jedwab was supported by NSERC.

MSC2020: 05B10, 05E18.

Keywords: difference set, nonabelian, 2-group, construction.

Given an element $A = \sum_{g \in G} a_g g$ in the group ring $\mathbb{Z}G$, where each $a_g \in \mathbb{Z}$, we write $A^{(-1)}$ for the element $\sum_{g \in G} a_g g^{-1}$. It is customary in the study of difference sets to abuse notation by identifying a subset D of a group G with the element of the group ring $\mathbb{Z}G$ which is its $\{0, 1\}$ -valued characteristic function. The subset D of G is then a difference set if and only if the $\{0, 1\}$ -valued characteristic function D satisfies the equation

$$DD^{(-1)} = n + \lambda G \quad \text{in } \mathbb{Z}G,$$

in which n represents $n1_G$. Throughout, we shall instead identify the subset D of G with the element of $\mathbb{Z}G$ which is its $\{\pm 1\}$ -valued characteristic function (taking the value -1 for each element of G in D , and $+1$ for each element of G not in D). Under this convention, the subset D of G is a difference set if and only if the $\{\pm 1\}$ -valued function D satisfies

$$DD^{(-1)} = 4n + (v - 4n)G \quad \text{in } \mathbb{Z}G.$$

When $v = 4n$, this reduces to

$$DD^{(-1)} = |G|, \tag{1}$$

in which case the subset D is called a *Hadamard* difference set because the $\{\pm 1\}$ -valued $v \times v$ incidence matrix, whose rows and columns are indexed by the elements of G and whose (g, h) entry is the coefficient of $g^{-1}h$ in D , is a Hadamard matrix.

Example 1.1 [Bruck 1955]. Let $G = C_2^4 = \langle x_1, x_2, x_3, x_4 \rangle$, where C_2 denotes the multiplicative cyclic group of order 2. The set

$$D = \{1, x_1, x_2, x_3, x_4, x_1x_2x_3x_4\}$$

is a $(16, 6, 2)$ Hadamard difference set in G . We identify this set with the element $D = -1 - x_1 - x_2 - x_3 - x_4 - x_1x_2x_3x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$ of the group ring $\mathbb{Z}G$, and then $DD^{(-1)} = 16$.

We call a group containing a Hadamard difference set a *Hadamard group*, and denote the class of Hadamard groups by \mathcal{H} . It is an outstanding problem in combinatorics to determine which groups belong to the class \mathcal{H} ; see [Davis and Jedwab 1996] for a survey and [Jungnickel and Schmidt 1998] for a summary of subsequent results. This paper focuses on determining which 2-groups (namely groups whose order is a power of 2) belong to \mathcal{H} . The relation $v = 4n$ between the parameters of a difference set forces the parameters to be

$$(v, k, \lambda) = (4N^2, 2N^2 - N, N^2 - N) \tag{2}$$

for some integer N [Kesava Menon 1962]. Here N can be positive or negative, and the two values $\pm N$ give the parameters of complementary difference sets and designs. A nontrivial difference set in a 2-group must also have parameters of the form (2), where $N = 2^d$ for some positive integer d [Mann 1965]. We therefore restrict attention to the parameters

$$(v, k, \lambda) = (2^{2d+2}, 2^{2d+1} - 2^d, 2^{2d} - 2^d),$$

where d is a nonnegative integer. The groups of order 2^{2d+2} form a rich source of potential Hadamard difference sets: there are 2 nonisomorphic groups of order 4 (both of which contain a trivial Hadamard difference set); 14 of order 16; 267 of order 64; 56,092 of order 256; and 49,487,367,289 groups of order 1024 [Besche et al. 2002; Burrell 2022; Sloane 2022].

The following product construction contains, as a special case, the earlier result [Kesava Menon 1962; Turyn 1965] that the class \mathcal{H} is closed under direct products.

Theorem 1.2 (Dillon [1985] product construction). *Suppose that $H_1, H_2 \in \mathcal{H}$, and that G is a group containing subgroups H_1 and H_2 satisfying $G = H_1H_2$ and $H_1 \cap H_2 = 1$. Then $G \in \mathcal{H}$.*

Proof. Let D_1 and D_2 be difference sets in H_1 and H_2 , respectively, and let $D = D_1D_2$. By hypothesis, every element g of G has a unique representation $g = h_1h_2$ for some $h_1 \in H_1$ and $h_2 \in H_2$, and so D is $\{\pm 1\}$ -valued. Then

$$DD^{(-1)} = (D_1D_2)(D_1D_2)^{(-1)} = D_1D_2D_2^{(-1)}D_1^{(-1)} = D_1|H_2|D_1^{(-1)} = |H_1||H_2| = |G|. \quad \square$$

In a seminal paper, Turyn used algebraic number theory to prove a first nonexistence result for Hadamard 2-groups.

Theorem 1.3 [Turyn 1965]. *Let G be a group of order 2^{2d+2} containing a normal subgroup K of order less than 2^d such that G/K is cyclic. Then $G \notin \mathcal{H}$.*

Corollary 1.4 (Turyn exponent bound). *Suppose $G \in \mathcal{H}$ is an abelian group of order 2^{2d+2} . Then G has exponent at most 2^{d+2} .*

Dillon later proved a second nonexistence result for Hadamard 2-groups.

Theorem 1.5 [Dillon 1985]. *Let G be a group of order 2^{2d+2} containing a normal subgroup K of order less than 2^d such that G/K is dihedral. Then $G \notin \mathcal{H}$.*

In the ensuing 35 years since the publication of [Dillon 1985], no further nonexistence results for Hadamard 2-groups have been found. In this paper we shall present constructive results that identify new Hadamard 2-groups. In preparation, we introduce some further conventions that will be used throughout.

Let

$$E_r := C_2^r = \langle x_1, x_2, \dots, x_r \rangle$$

be the elementary abelian group of order 2^r . The group E_r is isomorphic to the additive group of the vector space $U_r := \text{GF}(2)^r$ comprising all binary r -tuples $a = (a_1, a_2, \dots, a_r)$, and an explicit isomorphism is given by

$$a = (a_1, a_2, \dots, a_r) \mapsto x^a = x_1^{a_1} x_2^{a_2} \cdots x_r^{a_r}.$$

The *characters* of E_r are the homomorphisms from E_r into the multiplicative group $\{1, -1\}$ given by

$$\chi_u : x^a \mapsto (-1)^{u \cdot a} \quad \text{for all } a \in U_r$$

as u ranges over U_r .

We consider integer-valued functions on G to be interchangeable with elements of $\mathbb{Z}G$: we identify an integer-valued function F on G with the element $\sum_{g \in G} F(g)g$ of the group ring $\mathbb{Z}G$, and conversely we identify a group ring element $\sum_{g \in G} F_g g$ with the function F on G given by $F(g) = F_g$. The character χ_u of E_r may then be written in the group ring $\mathbb{Z}E_r$ as

$$\chi_u = \sum_{a \in U_r} \chi_u(x^a)x^a = \sum_{a \in U_r} (-1)^{u \cdot a} x^a = \sum_{a \in U_r} \prod_{i=1}^r (-1)^{u_i a_i} x_i^{a_i} = \prod_{i=1}^r \sum_{a_i=0}^1 (-1)^{u_i a_i} x_i^{a_i} = \prod_{i=1}^r (1 + (-1)^{u_i} x_i). \tag{3}$$

This is consistent with the common notation χ_0 for the principal character, which takes the value 1 at every group element; we identify this function in $\mathbb{Z}E_r$ with the group ring element $\sum_{e \in E_r} e$, or simply E_r . For each nonzero $u \in U_r$, the complement of the subset of E_r associated with the $\{\pm 1\}$ -valued function χ_u is a subgroup of E_r of index 2, and as u ranges over the nonzero values of U_r we obtain all $2^r - 1$ subgroups of E_r of index 2 in this way.

Example 1.6. Let $E_2 = C_2^2 = \langle x, y \rangle$. The four characters of E_2 are the functions χ_u as u ranges over $U_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$. Expressed in the group ring $\mathbb{Z}E_2$, these functions are

$$\begin{aligned} \chi_{00} &= 1 + x + y + xy = (1 + x)(1 + y), \\ \chi_{01} &= 1 + x - y - xy = (1 + x)(1 - y), \\ \chi_{10} &= 1 - x + y - xy = (1 - x)(1 + y), \\ \chi_{11} &= 1 - x - y + xy = (1 - x)(1 - y), \end{aligned}$$

(where we abbreviate $\chi_{(0,1)}$, for example, as χ_{01}).

The subgroups of E_2 corresponding to $\chi_{01}, \chi_{10}, \chi_{11}$ are $\{1, x\}, \{1, y\}, \{1, xy\}$, respectively.

The group ring interpretation of the characters of E_2 shown in Example 1.6 illustrates the following fundamental properties, which underlie our new constructions of difference sets. These properties can all be derived directly from (3), noting that $\chi_v^{(-1)} = \chi_v$ for all $v \in U_r$.

Proposition 1.7. *Let $\{\chi_u : u \in U_r\}$ be the set of characters of E_r . Then for all $u, v \in U_r$, in the group ring $\mathbb{Z}E_r$ we have:*

- (i) $\chi_u \chi_v^{(-1)} = \begin{cases} 2^r \chi_u & \text{if } u = v, \\ 0 & \text{if } u \neq v. \end{cases}$
- (ii) $\sum_{u \in U_r} \chi_u = 2^r.$
- (iii) $\sum_{e \in E_r} \chi_u(e) = \begin{cases} 2^r & \text{if } u = 0, \\ 0 & \text{if } u \neq 0. \end{cases}$

Since all characters of E_r are $\{\pm 1\}$ -valued, Proposition 1.7(iii) implies that every nonprincipal character on E_r takes the values 1 and -1 equally often.

McFarland gave the following difference set construction based on hyperplanes of a vector space, which produces examples in 2-groups. We prove the construction by interpreting the hyperplanes in terms of characters.

Theorem 1.8 (McFarland [1973] hyperplane construction). *Let J be a group of order 2^{d+1} . Then $J \times E_{d+1} \in \mathcal{H}$.*

Proof. See [Dillon 2010]. Let $\{\chi_u : u \in U_{d+1}\}$ be the set of characters of E_{d+1} . Label the elements of J arbitrarily as $J = \{g_u : u \in U_{d+1}\}$, and let $G = J \times E_{d+1}$. We see from Proposition 1.7(i) and (ii) that, in the group ring $\mathbb{Z}G$, the $\{\pm 1\}$ -valued function

$$D = \sum_{u \in U_{d+1}} g_u \chi_u \tag{4}$$

on G satisfies

$$\begin{aligned} DD^{(-1)} &= \sum_{u,v \in U_{d+1}} g_u \chi_u \chi_v^{(-1)} g_v^{-1} \\ &= 2^{d+1} \sum_{u \in U_{d+1}} g_u \chi_u g_u^{-1} \end{aligned} \tag{5}$$

$$\begin{aligned} &= 2^{d+1} \sum_{u \in U_{d+1}} \chi_u \tag{6} \\ &= 2^{d+1} \cdot 2^{d+1} = |G|. \end{aligned}$$

Therefore D corresponds to a Hadamard difference set in G . □

We shall show how the proof of Theorem 1.8 can be adapted so that the result still holds when E_{d+1} is a normal subgroup of index 2^{d+1} of a group G , but not necessarily a direct factor. The key consideration is how to obtain (6) from (5). The following combinatorial result allows us to do so, by showing that there is a choice for coset representatives g_u of E_{d+1} in G satisfying $\{g_u \chi_u g_u^{-1} : u \in U_{d+1}\} = \{\chi_u : u \in U_{d+1}\}$. Note that a group H acts as a group of permutations on a set S if there is a homomorphism ϕ (called the action of H on S) from H to the group of permutations of S .

Theorem 1.9 [Drisko 1998, Corollary 5]. *Let p be a prime and let H be a finite p -group. Suppose that H acts as a group of permutations on a set S of size $|H|$ according to the action ϕ , and that S contains an element that is fixed under ϕ . Then there is a bijection θ from S to H satisfying*

$$\{\phi(\theta(s))(s) : s \in S\} = S.$$

The bijection θ in Theorem 1.9 selects an element $\theta(s)$ of the group H for each $s \in S$, so that the resulting set of actions of $\theta(s)$ on s is a permutation of the set S . We now explain how this result can be used to extend Theorem 1.8 as desired, proving a conjecture due to Dillon [1990b].

Corollary 1.10 [Drisko 1998, Corollary 9]. *Let G be a group of order 2^{2d+2} containing a normal subgroup $E \cong C_2^{d+1}$. Then $G \in \mathcal{H}$.*

Proof. Let $\hat{E} = \{\chi_u : u \in U_{d+1}\}$ be the set of characters of $E \cong C_2^{d+1}$. We wish to apply Theorem 1.9 with $S = \hat{E}$ and $H = G/E$. Since E is normal in G , and the complements of the subsets of E associated

with the characters χ_u for nonzero u are exactly the subgroups of E of index 2, we have

$$g\chi_u g^{-1} \in \hat{E} \quad \text{for all } g \in G \text{ and } \chi_u \in \hat{E}.$$

Therefore G/E acts on \hat{E} as a group of permutations under the conjugation action

$$\phi(gE)(\chi_u) = g\chi_u g^{-1} \quad \text{for all } gE \in G/E \text{ and } \chi_u \in \hat{E},$$

and the element $\chi_0 = E$ of \hat{E} is fixed under ϕ . Theorem 1.9 then shows that there is a bijection θ from \hat{E} to G/E satisfying

$$\{\phi(\theta(\chi_u))(\chi_u) : \chi_u \in \hat{E}\} = \hat{E}. \quad (7)$$

Writing $\theta(\chi_u) = g_u E$ for each $u \in U_{d+1}$, this gives a set $\{g_u : u \in U_{d+1}\}$ of coset representatives for E in G satisfying

$$\{g_u \chi_u g_u^{-1} : u \in U_{d+1}\} = \{\chi_u : u \in U_{d+1}\}. \quad (8)$$

Use the coset representatives g_u to define D as in (4). The proof of Theorem 1.8 now carries through unchanged, using (8) to obtain (6) from (5). \square

We next illustrate the construction described in Corollary 1.10, for a specific group of order 16.

Example 1.11. Let G be the order 16 modular group $C_8 \rtimes_5 C_2 = \langle x, y : x^8 = y^2 = 1, yxy^{-1} = x^5 \rangle$, and set $X = x^4$ and $Y = y$. Let $E = \langle X, Y \rangle \cong C_2^2$, which is normal but not central in G , and let $\hat{E} = \{\chi_u : u \in U_2\}$ be the set of characters of E :

$$\chi_{00} = (1 + x^4)(1 + y), \quad \chi_{01} = (1 + x^4)(1 - y), \quad \chi_{10} = (1 - x^4)(1 + y), \quad \chi_{11} = (1 - x^4)(1 - y).$$

The center of G is $\langle x^2 \rangle$.

The group $G/E = \{E, xE, x^2E, x^3E\}$ acts on \hat{E} as a group of permutations under the conjugation action ϕ , under which E and x^2E map to the identity permutation on \hat{E} , and xE and x^3E map to the permutation of \hat{E} that fixes χ_{00} and χ_{01} but swaps χ_{10} and χ_{11} .

A bijection θ from \hat{E} to G/E satisfying (7) is

$$\theta(\chi_{00}) = E, \quad \theta(\chi_{01}) = x^2E, \quad \theta(\chi_{10}) = xE, \quad \theta(\chi_{11}) = x^3E,$$

and therefore

$$D = \chi_{00} + x^2\chi_{01} + x\chi_{10} + x^3\chi_{11}$$

is a difference set in G .

The Turyn exponent bound of Corollary 1.4 gives a necessary condition for an abelian 2-group to belong to \mathcal{H} . A series of papers, including [Davis 1991] and [Dillon 1990a], gave constructions in pursuit of a sufficient condition. Kraemer [1993] eventually showed that the necessary condition is also sufficient. This result was proved again by Jedwab [1992] using the alternative viewpoint of a perfect binary array: a matrix representation of the $\{\pm 1\}$ -valued characteristic function of a Hadamard difference set in an abelian group.

Theorem 1.12 [Kraemer 1993]. *Let G be an abelian group of order 2^{2d+2} . Then $G \in \mathcal{H}$ if and only if G has exponent at most 2^{d+2} .*

We next give an instructive example of a Hadamard difference set in an abelian 2-group, which illustrates a fundamental insight on which this paper is based. The group ring elements A_u in Example 1.13 are presented for now without explanation of their origin, but will be revisited in Example 4.13. Group ring elements A, B are *orthogonal* if $AB^{(-1)} = 0$.

Example 1.13. Let $G = C_8^2 = \langle x, y \rangle$, and set $X = x^2$ and $Y = y^2$. Let $K = \langle X, Y \rangle \cong C_4^2$ and $E_2 = \langle X^2, Y^2 \rangle \cong C_2^2$, and let $\{\chi_u : u \in U_2\}$ be the set of characters of E_2 . Define four group ring elements in $\mathbb{Z}K$ by

$$A_{00} = A_{01} = A_{10} = 1 + X + Y - XY \quad \text{and} \quad A_{11} = 1 + X + Y + XY. \tag{9}$$

Direct calculation shows that the A_u satisfy the condition

$$A_u \chi_u A_u^{(-1)} = 4\chi_u \quad \text{for all } u \in U_2. \tag{10}$$

Now in $\mathbb{Z}K$ let

$$\begin{aligned} B_{00} &= A_{00}\chi_{00} = (1 + X + Y - XY)(1 + X^2)(1 + Y^2), \\ B_{01} &= A_{01}\chi_{01} = (1 + X + Y - XY)(1 + X^2)(1 - Y^2), \\ B_{10} &= A_{10}\chi_{10} = (1 + X + Y - XY)(1 - X^2)(1 + Y^2), \\ B_{11} &= A_{11}\chi_{11} = (1 + X + Y + XY)(1 - X^2)(1 - Y^2). \end{aligned}$$

Then from Proposition 1.7(i) and (10), the $B_u = A_u\chi_u$ have the property, for all $u, v \in U_2$, that

$$B_u B_v^{(-1)} = \begin{cases} 16\chi_u & \text{if } u = v, \\ 0 & \text{if } u \neq v, \end{cases} \tag{11}$$

and in particular the B_u are pairwise orthogonal. It follows that the $\{\pm 1\}$ -valued function on G given by

$$D = B_{00} + yB_{01} + xB_{10} + xyB_{11}$$

satisfies

$$DD^{(-1)} = 16(\chi_{00} + \chi_{01} + \chi_{10} + \chi_{11}) = 64$$

by Proposition 1.7(ii), and so D corresponds to a Hadamard difference set in G .

We now show how the condition (10) satisfied by the group ring elements A_u in Example 1.13 can be used to construct difference sets in groups of order 64 other than C_8^2 .

Proposition 1.14. *Let G be a group of order 64 containing a normal subgroup $K \cong C_4^2$. Then $G \in \mathcal{H}$.*

Proof. Let $K = \langle X, Y \rangle \cong C_4^2$. Let $E_2 = \langle X^2, Y^2 \rangle$ be the unique subgroup of K isomorphic to C_2^2 , and let $\widehat{E}_2 = \{\chi_u : u \in U_2\}$ be the set of characters of E_2 . Define four group ring elements in $\mathbb{Z}K$ as in (9), and for each $u \in U_2$ let B_u be the $\{\pm 1\}$ -valued function $A_u\chi_u$ on K . The A_u satisfy (10), and therefore the B_u have the pairwise orthogonality property (11) for all $u, v \in U_2$.

Now E_2 is the unique subgroup of K isomorphic to C_2^2 , and K is normal in G , so E_2 is normal in G . Therefore G/K acts on \widehat{E}_2 as a group of permutations under the conjugation action

$$\phi(gK)(\chi_u) = g\chi_u g^{-1} \quad \text{for all } gK \in G/K \text{ and } \chi_u \in \widehat{E}_2,$$

and $\chi_0 = E_2$ is fixed under ϕ . We may therefore apply Theorem 1.9 with $S = \widehat{E}_2$ and $H = G/K$ to show that there is a set $\{g_u : u \in U_2\}$ of coset representatives for K in G satisfying

$$\{g_u \chi_u g_u^{-1} : u \in U_2\} = \{\chi_u : u \in U_2\}. \tag{12}$$

Let D be the $\{\pm 1\}$ -valued function on G defined by

$$D = \sum_{u \in U_2} g_u B_u \text{ in } \mathbb{Z}G.$$

We calculate

$$DD^{(-1)} = \sum_{u,v \in U_2} g_u B_u B_v^{(-1)} g_v^{-1} = 16 \sum_{u \in U_2} g_u \chi_u g_u^{-1}$$

by (11), and then from (12) and Proposition 1.7(ii) we have

$$DD^{(-1)} = 16 \sum_{u \in U_2} \chi_u = 64.$$

Therefore D corresponds to a Hadamard difference set in G . □

We use the proof of Proposition 1.14 as a model for establishing our principal result, stated below as Theorem 1.15. The key idea is to determine group ring elements A_u satisfying a condition analogous to (10), which ensures that the associated group ring elements $B_u = A_u \chi_u$ have an orthogonality property analogous to (11). Application of Theorem 1.9 then allows us to construct a group ring element D corresponding to a Hadamard difference set. By taking $r = 2$ in Theorem 1.15 and restricting the group G to be abelian, and combining with the Turyn exponent bound of Corollary 1.4, we recover Kraemer’s Theorem 1.12.

Theorem 1.15 (main result). *Let d and r be integers satisfying $d \geq 1$ and $2 \leq r \leq d + 1$. Let G be a group of order 2^{2d+2} containing a normal abelian subgroup of index 2^r , rank r , and exponent at most 2^{d-r+2} . Then $G \in \mathcal{H}$.*

We remark that this paper develops several concepts previously used to construct difference sets. In particular, the constructed group ring elements B_u can be interpreted as covering extended building sets, as introduced by Davis and Jedwab [1997] (see the discussion at the end of Section 2). The novelty here is that imposing the additional structure $B_u = A_u \chi_u$ allows us to handle dramatically more nonabelian groups than before, as illustrated in the proof of Proposition 1.14. Likewise, Proposition 1.14 itself was previously established by Dillon [1990b; 2010] by decomposing a difference set in C_8^2 into four orthogonal group ring elements B_u as in Example 1.13. However, the generalization of Proposition 1.14

to Theorem 1.15 relies crucially on recognizing the additional structure $B_u = A_u \chi_u$ of these group ring elements, whose importance was not previously apparent.

Each of the two groups of order 4 belongs to \mathcal{H} trivially. The third column of Table 1 below shows the number of groups of order 16, 64, and 256 which are possible members of \mathcal{H} , after taking into account those that are excluded by the necessary conditions of Theorems 1.3 and 1.5. We now summarize the theoretical and computational efforts of many researchers over several decades to determine whether these conditions are also sufficient for groups of these orders, with reference to results to be presented in Section 4.

In the 1970s, Whitehead [1975] and Kibler [1978] independently showed by construction that each of the 12 nonexcluded groups of order 16 belongs to \mathcal{H} . We can recover this result by applying Theorem 1.15 to account for the 10 groups containing a normal subgroup isomorphic to C_2^2 , and then using Proposition 4.1 to handle the remaining 2 groups.

In 1990, a collaborative effort led by Dillon showed by a combination of construction and computer search that each of the 259 nonexcluded groups of order 64 belongs to \mathcal{H} ; Liebler and Smith [1993] resolved the status of the final group at the conclusion of a sabbatical visit to Dillon by Smith. Using the software package GAP [2020], we can streamline this effort by applying in sequence the following construction methods: Theorem 1.15 to account for the 237 groups containing a normal subgroup isomorphic to C_2^3 or C_4^2 ; the product construction of Proposition 4.7 to account for 17 further groups; the transfer methods of Section 4C to account for 4 further groups; and the modified signature set method of Section 4D to account for the final group.

In 2011, Dillon initiated a further collaborative effort to investigate the groups of order 256, whose conclusion was that each of the 56,049 nonexcluded groups of order 256 belongs to \mathcal{H} . Major contributions were made by Applebaum [2013], and the status of the final group was resolved by Yolland [2016]. Using GAP, we can likewise streamline this effort by applying in sequence the following construction methods: Theorem 1.15 to account for the 54,633 groups containing a normal subgroup isomorphic to C_2^4 or $C_4^2 \times C_2$ or C_8^2 ; the product construction of Proposition 4.7 to account for 1,358 further groups; the transfer methods of Section 4C to account for 57 further groups; and the modified signature set method of Section 4D to account for the final group.

These theoretical and computational results are summarized in Theorem 1.16 and in Table 1.

Theorem 1.16. *The necessary conditions of Theorems 1.3 and 1.5 for the existence of a difference set are also sufficient in groups of order 4, 16, 64, and 256.*

Theorem 1.16 naturally prompts the following question (about whose answer the authors of this paper have different opinions).

Question 1.17. Are the necessary conditions of Theorems 1.3 and 1.5 for the existence of a difference set in a 2-group also sufficient? That is, does every group G of order 2^{2d+2} , not containing a normal subgroup K of order less than 2^d such that G/K is cyclic or dihedral, belong to \mathcal{H} ?

Group order	Total # groups	# not excluded by Theorems 1.3, 1.5	# in \mathcal{H} by			
			Theorem 1.15	Sections 4A–4B	Section 4C	Section 4D
16	14	12	10	2		
64	267	259	237	17	4	1
256	56,092	56,049	54,633	1,358	57	1

Table 1. Membership in \mathcal{H} of 2-groups of order 16, 64, and 256. Figures in column 5 onwards are for groups not previously counted in column 4 onwards.

The answer to Question 1.17 is “yes” for $d \leq 3$, by Theorem 1.16. It seems that resolution of this question for $d > 3$ must depend only on theoretical methods: currently there is not even a database of the 49,487,367,289 groups of order 1024 [Besche et al. 2002; Burrell 2022], and the authors do not know how to estimate the proportion of the nonexcluded groups of order 2^{2d+2} that are accounted for by Theorem 1.15 as d grows large.

The rest of this paper is organized in the following way. In Section 2, we identify the “signature set” property underlying the construction of Proposition 1.14. In Section 3, we prove our principal result of Theorem 1.15 by restricting attention to signature sets on abelian 2-groups. In Section 4, we describe the various other construction methods used to complete the determination of the groups of order 64 and 256 belonging to \mathcal{H} , involving signature sets on nonabelian groups, products of perfect ternary arrays, transfer methods, and a modification of signature sets. In Section 5, we provide implementation details of the construction methods for groups of order 256 and describe how to quickly verify on a desktop computer that all 56,049 nonexcluded groups of this order belong to \mathcal{H} . In Section 6, we propose some directions for future research.

2. Signature sets

In this section, we identify the structure underlying Proposition 1.14 and set out a framework for proving our principal result, Theorem 1.15.

Definition 2.1. Let K be a group containing a normal subgroup $E \cong C_2^r$, and let $\{\chi_u : u \in U_r\}$ be the set of characters of E . A *signature block on K with respect to χ_u* is a $\{\pm 1\}$ -valued function A_u on a set of coset representatives for E in K that satisfies

$$A_u \chi_u A_u^{(-1)} = \frac{|K|}{2^r} \chi_u \quad \text{in } \mathbb{Z}K.$$

A *signature set on K with respect to E* is a multiset $\{A_u : u \in U_r\}$, where each A_u is a signature block on K with respect to χ_u .

Note that a trivial signature set on C_2^r with respect to itself is given by

$$A_u = 1 \quad \text{for each } u \in U_r.$$

We state two immediate consequences of Definition 2.1.

Lemma 2.2. *Let K be a group containing a normal subgroup $E \cong C_2^r$, and suppose $\{A_u : u \in U_r\}$ is a signature set on K with respect to E . Let $\hat{E} = \{\chi_u : u \in U_r\}$ be the set of characters of E , and let $B_u = A_u \chi_u$ for each $u \in U_r$. Then:*

- (i) *For each $u \in U_r$, the function B_u is $\{\pm 1\}$ -valued on K .*
- (ii) *For all $u, v \in U_r$, in $\mathbb{Z}K$ we have*

$$B_u B_v^{(-1)} = \begin{cases} |K| \chi_u & \text{if } u = v, \\ 0 & \text{if } u \neq v \end{cases}$$

(and so in particular the B_u are pairwise orthogonal).

Proof. (i) Each A_u is a $\{\pm 1\}$ -valued function on a set of coset representatives for E in K , and each χ_u is a $\{\pm 1\}$ -valued function on E . Therefore each $B_u = A_u \chi_u$ is a $\{\pm 1\}$ -valued function on K .

(ii) For all $u, v \in U_r$, in $\mathbb{Z}K$ we have

$$B_u B_v^{(-1)} = A_u \chi_u \chi_v^{(-1)} A_v^{(-1)} = \begin{cases} 2^r A_u \chi_u A_u^{(-1)} & \text{if } u = v, \\ 0 & \text{if } u \neq v \end{cases}$$

by Proposition 1.7(i). Since the A_u form a signature set on K with respect to E , this gives

$$B_u B_v^{(-1)} = \begin{cases} |K| \chi_u & \text{if } u = v, \\ 0 & \text{if } u \neq v. \end{cases} \quad \square$$

The proof of the following theorem is modeled on that of Proposition 1.14. We remark that K need not be a 2-group and need not be abelian.

Theorem 2.3. *Let G be a group containing a normal subgroup $E \cong C_2^r$, and suppose K is a normal subgroup of G of index 2^r containing E . Suppose there exists a signature set on K with respect to E . Then $G \in \mathcal{H}$.*

Proof. Let $\hat{E} = \{\chi_u : u \in U_r\}$ be the set of characters of E . We shall apply Theorem 1.9 with $S = \hat{E}$ and $H = G/K$. Since E is normal in G , and the complements of the subsets of E associated with the characters χ_u for nonzero u are exactly the subgroups of E of index 2,

$$g \chi_u g^{-1} \in \hat{E} \quad \text{for all } g \in G \text{ and } \chi_u \in \hat{E}.$$

Therefore G/K acts on \hat{E} as a group of permutations under the conjugation action

$$\phi(gK)(\chi_u) = g \chi_u g^{-1} \quad \text{for all } gK \in G/K \text{ and } \chi_u \in \hat{E},$$

and the element $\chi_0 = E$ of \hat{E} is fixed under ϕ . Apply Theorem 1.9 to show that there is a set $\{g_u : u \in U_r\}$ of coset representatives for K in G satisfying

$$\{g_u \chi_u g_u^{-1} : u \in U_r\} = \{\chi_u : u \in U_r\}. \tag{13}$$

By assumption, there is a signature set $\{A_u : u \in U_r\}$ on K with respect to E . Let $B_u = A_u \chi_u$ for each $u \in U_r$, and use the coset representatives g_u to define

$$D = \sum_{u \in U_r} g_u B_u \quad \text{in } \mathbb{Z}G, \quad (14)$$

which is a $\{\pm 1\}$ -valued function on G by Lemma 2.2(i). We calculate in $\mathbb{Z}G$ that

$$DD^{(-1)} = \sum_{u, v \in U_r} g_u B_u B_v^{(-1)} g_v^{-1} = |K| \sum_{u \in U_r} g_u \chi_u g_u^{-1}$$

by Lemma 2.2(ii). Then from (13) and Proposition 1.7(ii) we have

$$DD^{(-1)} = |K| \sum_{u \in U_r} \chi_u = 2^r |K| = |G|.$$

Therefore D corresponds to a Hadamard difference set in G . □

The motivating examples of Section 1 both occur as special cases of Theorem 2.3. Corollary 1.10 arises by taking $|G| = 2^{2d+2}$ and $r = d + 1$, with $E = K \cong C_2^{d+1}$ normal in G , and using a trivial signature set on K with respect to itself. Proposition 1.14 arises by taking $|G| = 64$ and $r = 2$, with $K = \langle X, Y \rangle \cong C_4^2$ normal in G and $E = \langle X^2, Y^2 \rangle$ (the unique subgroup of K isomorphic to C_2^2), and using the nontrivial signature set $\{A_{ij} : (i, j) \in U_2\}$ on K with respect to E specified in (9).

Theorem 2.3 establishes the existence of a difference set in G by reference to Theorem 1.9, whose proof as given in [Drisko 1998] is not constructive. To construct such a difference set explicitly, one must therefore determine suitable coset representatives for the normal subgroup K in G satisfying (13). This determination currently requires a computer search that can be computationally expensive, particularly for groups of order 256; see Section 5.

We point out a connection to the study of bent functions (see [Carlet and Mesnager 2016] for a survey), which are equivalent to Hadamard difference sets in elementary abelian 2-groups. Take $G = E_{d+1}^2$ and $E = K = E_{d+1}$ in Theorem 2.3, and let $\{A_u : u \in U_r\}$ be a trivial signature set on K with respect to E for which each A_u is chosen arbitrarily in $\{\pm 1\}$. In this case, the choice of coset representatives $\{g_u : u \in U_{d+1}\}$ for K in G used to construct the difference set D in the proof of Theorem 2.3 is arbitrary. Let a be the Boolean function on U_{d+1} defined by

$$A_u = (-1)^{a(u)} \quad \text{for each } u \in U_{d+1}.$$

Then the $\{0, 1\}$ -valued characteristic function of D is the Maiorana–McFarland bent function $f(u, v) = \pi(u) \cdot v + a(u)$, where π is an arbitrary permutation of U_{d+1} .

In view of Theorem 2.3, our objective in Section 3 is to construct a signature set on a large class of groups K (which we take to be abelian in Section 3, and nonabelian in Section 4). In the remainder of this section, we introduce some preparatory results about signature sets.

We firstly show that a group automorphism of K fixing E maps a signature block on K to another signature block on K .

Proposition 2.4. *Let K be a group containing a normal subgroup $E \cong C_2^r$, and let σ be a group automorphism of K which fixes E . Suppose that A_u is a signature block on K with respect to the character χ_u of E , for some $u \in U_r$. Then σ induces a map on $\mathbb{Z}K$ under which $\sigma(A_u)$ is a signature block on K with respect to the character $\sigma(\chi_u)$ of E .*

Proof. The signature block A_u is $\{\pm 1\}$ -valued on a set of coset representatives for E in K . Since the automorphism σ fixes E , the images of these coset representatives under σ are also a set of coset representatives for E in K on which $\sigma(A_u)$ is $\{\pm 1\}$ -valued. Furthermore

$$\sigma(A_u)\sigma(\chi_u)\sigma(A_u)^{(-1)} = \sigma(A_u\chi_uA_u^{(-1)}) = \frac{|K|}{2^r}\sigma(\chi_u),$$

so $\sigma(A_u)$ is a signature block on K with respect to the character $\sigma(\chi_u)$ of E . □

We next give a simple product construction for signature sets.

Proposition 2.5. *Suppose there exists a signature set on a group K_r with respect to a normal subgroup $E_r \cong C_2^r$, and there exists a signature set on a group K_s with respect to a normal subgroup $E_s \cong C_2^s$. Then there exists a signature set on $K_r \times K_s$ with respect to $E_r \times E_s$.*

Proof. Let $\{A_u : u \in U_r\}$ be a signature set on K_r with respect to E_r , and let $\{\alpha_v : v \in U_s\}$ be a signature set on K_s with respect to E_s . We claim that $\{A_u\alpha_v : u \in U_r, v \in U_s\}$ is a signature set on $K_r \times K_s$ with respect to its normal subgroup $E_r \times E_s$.

The function $A_u\alpha_v$ is $\{\pm 1\}$ -valued on a set of coset representatives for $E_r \times E_s$ in $K_r \times K_s$, because A_u is $\{\pm 1\}$ -valued on a set of coset representatives for E_r in K_r and α_v is $\{\pm 1\}$ -valued on a set of coset representatives for E_s in K_s .

Let $\{\chi_u : u \in U_r\}$ be the set of characters of E_r , and let $\{\psi_v : v \in U_s\}$ be the set of characters of E_s . The set of characters of $E_r \times E_s$ is $\{\chi_u\psi_v : u \in U_r, v \in U_s\}$, and for each $u \in U_r$ and $v \in U_s$ we have

$$\begin{aligned} (A_u\alpha_v)(\chi_u\psi_v)(A_u\alpha_v)^{(-1)} &= A_u\chi_u(\alpha_v\psi_v\alpha_v^{(-1)})A_u^{(-1)} \\ &= A_u\chi_u\frac{|K_s|}{2^s}\psi_vA_u^{(-1)} \\ &= (A_u\chi_uA_u^{(-1)})\frac{|K_s|}{2^s}\psi_v \\ &= \frac{|K_r|}{2^r}\chi_u\frac{|K_s|}{2^s}\psi_v \\ &= \frac{|K_r \times K_s|}{2^{r+s}}(\chi_u\psi_v). \end{aligned} \quad \square$$

To illustrate the previously unrecognized power of the signature set approach, note that Applebaum [2013] used computer search to show that 643 of the 714 groups of order 256, whose membership in \mathcal{H} was then undetermined, belong to \mathcal{H} . Since all 643 of these groups contain a normal subgroup isomorphic to $C_4^2 \times C_2$, this result follows directly from Theorem 2.3 simply by exhibiting a signature set on $C_4^2 \times C_2$ with respect to its unique subgroup isomorphic to C_2^3 . This can be constructed by using Proposition 2.5

to take the product of a signature set on C_4^2 with respect to its unique subgroup isomorphic to C_2^2 (see Example 1.13) with a trivial signature set on C_2 with respect to itself.

Finally, we derive constraints on a signature set in terms of $|K|$ and $|E|$. We will use these constraints to show how Theorem 2.3 can be viewed as refining a construction method for difference sets introduced by Davis and Jedwab [1997], by interpreting a signature set on an abelian group as a special kind of covering extended building set.

Lemma 2.6. *Let K be a group containing a normal subgroup $E \cong C_2^r$, and suppose that $\{A_u : u \in U_r\}$ is a signature set on K with respect to E . Let $\{\chi_u : u \in U_r\}$ be the set of characters of E , and let $B_u = A_u \chi_u$ for each $u \in U_r$. Then the number of times the $\{\pm 1\}$ -valued function B_u on K takes the value -1 is*

$$\begin{cases} \frac{1}{2}|K| & \text{if } u \neq 0, \\ \frac{1}{2}|K| \pm \sqrt{2^{r-2}|K|} & \text{if } u = 0. \end{cases}$$

Proof. By Lemma 2.2(i), each B_u is $\{\pm 1\}$ -valued on K .

Case 1: $u \neq 0$. By Proposition 1.7(iii), the number of times the $\{\pm 1\}$ -valued function χ_u on E takes the value -1 is $\frac{1}{2}|E|$. Since A_u is a $\{\pm 1\}$ -valued function on a set of coset representatives for E in K , the number of times $B_u = A_u \chi_u$ takes the value -1 is $\frac{1}{2}|E||K : E| = \frac{1}{2}|K|$.

Case 2: $u = 0$. Let $c \in \{0, 1, \dots, |K|\}$ be the number of times that B_0 takes the value -1 , and let J be a group of order 2^r . By Theorem 2.3, the group $G = J \times K$ contains a Hadamard difference set D whose corresponding $\{\pm 1\}$ -valued function is defined in (14) as

$$D = g_0 B_0 + \sum_{u \neq 0} g_u B_u \tag{15}$$

for some choice of coset representatives $\{g_u : u \in U_r\}$ for K in G . By (2), the parameters of the difference set D satisfy

$$|G| = 2^r |K| = 4N^2 \quad \text{and} \quad |D| = 2N^2 - N$$

for some integer N , and eliminating N gives

$$|D| = 2^{r-1}|K| \pm \sqrt{2^{r-2}|K|}.$$

But $|D|$ equals the number of times that the function D takes the value -1 , which from (15) and the result for Case 1 gives

$$|D| = c + (2^r - 1)\frac{1}{2}|K|.$$

Equate the two expressions for $|D|$ to give

$$c = \frac{1}{2}|K| \pm \sqrt{2^{r-2}|K|}. \tag{□}$$

Note from Example 1.13 that the number of times the function A_u takes the value -1 is not determined for $u \neq 0$ solely from the hypotheses of Lemma 2.6. However, for $u = 0$ this number is determined as $\frac{1}{2^r} \left(\frac{|K|}{2} \pm \sqrt{2^{r-2}|K|} \right)$ by Lemma 2.6 and the relation $B_0 = A_0\chi_0$, because the $\{\pm 1\}$ -valued function $\chi_0 = E$ takes the value 1 exactly 2^r times.

We can now interpret Theorem 2.3 in the framework of [Davis and Jedwab 1997] for the case that K is abelian. Suppose $\{A_u : u \in U_r\}$ is a signature set on an abelian group K with respect to $E = (x_1, x_2, \dots, x_r) \cong C_2^r$, and let $B_u = A_u\chi_u$ for each $u \in U_r$. In the language of [Davis and Jedwab 1997], we claim that the subsets $\{\frac{1}{2}(K - B_u) : u \in U_r\}$ of K then form a $(\frac{1}{2}|K|, \sqrt{2^{r-2}|K|}, 2^r, \pm)$ covering extended building set on K (satisfying the key additional constraint that $B_u = A_u\chi_u$ for each u). To prove the claim, we require firstly that

$$\left| \frac{1}{2}(K - B_u) \right| = \begin{cases} \frac{1}{2}|K| \pm \sqrt{2^{r-2}|K|} & \text{for a single value of } u, \\ \frac{1}{2}|K| & \text{for all other values of } u. \end{cases}$$

This is given by Lemma 2.6, because $\left| \frac{1}{2}(K - B_u) \right|$ is the number of times that the $\{\pm 1\}$ -valued function B_u takes the value -1 . To complete the proof of the claim, we also require that, for each nonprincipal character ψ of the abelian group K (namely a nontrivial homomorphism from K to the complex roots of unity),

$$\left| \psi \left(\frac{1}{2}(K - B_u) \right) \right| = \begin{cases} \sqrt{2^{r-2}|K|} & \text{for a single value of } u \text{ that depends on } \psi, \\ 0 & \text{for all other values of } u. \end{cases}$$

This is given by applying ψ to the case $u = v$ of Lemma 2.2(ii) to obtain $|\psi(B_u)|^2 = |K|\psi(\chi_u)$, and noting that ψ maps each x_i to $\{1, -1\}$ so that from (3) we have

$$\psi(\chi_u) = \begin{cases} 2^r & \text{for a single value of } u \text{ that depends on } \psi, \\ 0 & \text{for all other values of } u. \end{cases}$$

3. Proof of main result

In this section we prove our main result, Theorem 1.15, as a corollary of Theorem 3.1 below. For an abelian 2-group K of rank r , we shall abbreviate “a signature set on K with respect to its unique subgroup isomorphic to C_2^r ” as “a signature set on K ”.

Theorem 3.1. *Let d and r be integers satisfying $d \geq 1$ and $2 \leq r \leq d + 1$. Let $\mathcal{K}_{d,r}$ be the set of all abelian groups of order 2^{2d-r+2} , rank r , and exponent at most 2^{d-r+2} . Then there exists a signature set on each $K_{d,r} \in \mathcal{K}_{d,r}$.*

Note in Theorem 3.1 that if E is the unique subgroup of $K_{d,r} \in \mathcal{K}_{d,r}$ isomorphic to C_2^r , then E is normal in G . We may therefore apply Theorem 2.3 to obtain Theorem 1.15 as a corollary of Theorem 3.1.

We shall prove Theorem 3.1 using a recursive construction for signature sets on abelian 2-groups. To illustrate the main ideas, we begin with a proof of the special case $r = 2$.

Theorem 3.2 (rank 2 case of Theorem 3.1). *Let d be a nonnegative integer. Then there exists a signature set on $K_d = C_{2^d}^2$.*

Proof. The proof is by induction on $d \geq 1$. The case $d = 1$ is true because there exists a trivial signature set on C_2^2 .

Assume all cases up to $d - 1 \geq 1$ are true. Let $K_{d-1} = \langle X, Y \rangle$, where $X^{2^{d-1}} = Y^{2^{d-1}} = 1$. By the inductive hypothesis, there exists a signature set $\{A_{ij} : (i, j) \in U_2\}$ on K_{d-1} with respect to $\langle X^{2^{d-2}}, Y^{2^{d-2}} \rangle$. By associating the group ring $\mathbb{Z}K_{d-1}$ with the quotient ring $\mathbb{Z}[X, Y]/\langle 1 - X^{2^{d-1}}, 1 - Y^{2^{d-1}} \rangle$, we may regard each group ring element A_{ij} as a polynomial $A_{ij}(X, Y)$ in X and Y , and regard each character of $\langle X^{2^{d-2}}, Y^{2^{d-2}} \rangle$ as a polynomial

$$\chi_{ij}(X, Y) = (1 + (-1)^i X^{2^{d-2}})(1 + (-1)^j Y^{2^{d-2}}) \quad \text{for } (i, j) \in U_2.$$

By assumption, in the polynomial ring $\mathbb{Z}[X, Y]/\langle 1 - X^{2^{d-1}}, 1 - Y^{2^{d-1}} \rangle$ we have

$$A_{ij}(X, Y)\chi_{ij}(X, Y)A_{ij}(X, Y)^{(-1)} = 2^{2d-4}\chi_{ij}(X, Y) \quad \text{for each } (i, j) \in U_2. \quad (16)$$

Let $K_d = \langle x, y \rangle$, where $x^{2^d} = y^{2^d} = 1$, and let $E = \langle x^{2^{d-1}}, y^{2^{d-1}} \rangle$. We wish to construct a signature set $\{\alpha_{ij} : (i, j) \in U_2\}$ on K_d with respect to E . Define the α_{ij} in $\mathbb{Z}K_d$ in terms of the polynomials A_{ij} via

$$\begin{aligned} \alpha_{00} &= (1 + x^{2^{d-2}})A_{00}(x, y^2) + y(1 - x^{2^{d-2}})A_{10}(x, y^2), \\ \alpha_{01} &= (1 + x^{2^{d-2}})A_{01}(x, y^2) + y(1 - x^{2^{d-2}})A_{11}(x, y^2), \\ \alpha_{10} &= (1 + y^{2^{d-2}})A_{10}(x^2, y) + x(1 - y^{2^{d-2}})A_{11}(x^2, y), \\ \alpha_{11} &= (1 + x^{2^{d-2}}y^{2^{d-2}})A_{10}(x^2, xy) + x(1 - x^{2^{d-2}}y^{2^{d-2}})A_{11}(x^2, xy), \end{aligned} \quad (17)$$

and let the characters of E be

$$\psi_{ij} = (1 + (-1)^i x^{2^{d-1}})(1 + (-1)^j y^{2^{d-1}}) \quad \text{for each } (i, j) \in U_2.$$

We first use Proposition 2.4 to show it is sufficient to prove for each $(i, j) \neq (1, 1)$ that α_{ij} is a signature block with respect to ψ_{ij} . Let σ be the group automorphism of K_d that maps x to itself and maps y to xy . Then $\sigma(\alpha_{10}) = \alpha_{11}$ by definition, and σ fixes E , and

$$\sigma(\psi_{10}) = (1 - x^{2^{d-1}})(1 + x^{2^{d-1}}y^{2^{d-1}}) = (1 - x^{2^{d-1}})(1 - y^{2^{d-1}}) = \psi_{11}.$$

Therefore if α_{10} is a signature block on K_d with respect to ψ_{10} , then α_{11} is a signature block on K_d with respect to ψ_{11} by Proposition 2.4.

We next show that α_{00} is a $\{\pm 1\}$ -valued function on a set of coset representatives for E in K_d , and a similar argument shows that the same holds for α_{01} and α_{10} . By definition, $A_{00}(X, Y)$ is $\{\pm 1\}$ -valued on exactly one of the four values

$$\{X^i Y^j, X^i Y^{j+2^{d-2}}, X^{i+2^{d-2}} Y^j, X^{i+2^{d-2}} Y^{j+2^{d-2}}\}$$

for $0 \leq i < 2^{d-2}$, $0 \leq j < 2^{d-2}$. Therefore $A_{00}(x, y^2)$ is $\{\pm 1\}$ -valued on exactly one of the four values

$$\{x^i y^{2j}, x^i y^{2j+2^{d-1}}, x^{i+2^{d-2}} y^{2j}, x^{i+2^{d-2}} y^{2j+2^{d-1}}\}$$

for $0 \leq i < 2^{d-2}$, $0 \leq j < 2^{d-2}$, and so $(1 + x^{2^{d-2}})A_{00}(x, y^2)$ is $\{\pm 1\}$ -valued on exactly one of the four values

$$\{x^i y^{2j}, x^i y^{2j+2^{d-1}}, x^{i+2^{d-1}} y^{2j}, x^{i+2^{d-1}} y^{2j+2^{d-1}}\}$$

for $0 \leq i < 2^{d-1}, 0 \leq j < 2^{d-2}$. Likewise, $y(1 - x^{2^{d-2}})A_{10}(x, y^2)$ is $\{\pm 1\}$ -valued on exactly one of the four values

$$\{x^i y^{2j+1}, x^i y^{2j+2^{d-1}+1}, x^{i+2^{d-1}} y^{2j+1}, x^{i+2^{d-1}} y^{2j+2^{d-1}+1}\}$$

for $0 \leq i < 2^{d-1}, 0 \leq j < 2^{d-2}$. Combining, α_{00} is $\{\pm 1\}$ -valued on exactly one of the four values

$$\{x^i y^j, x^i y^{j+2^{d-1}}, x^{i+2^{d-1}} y^j, x^{i+2^{d-1}} y^{j+2^{d-1}}\}$$

for $0 \leq i < 2^{d-1}, 0 \leq j < 2^{d-1}$.

It remains to show that in $\mathbb{Z}K_d$ we have

$$\alpha_{ij} \psi_{ij} \alpha_{ij}^{(-1)} = 2^{2d-2} \psi_{ij} \quad \text{for each } (i, j) \neq (1, 1). \tag{18}$$

Using $x^{2^d} = 1$, for $i, k \in \{0, 1\}$ we have the identity

$$(1 + x^{2^{d-1}})(1 + (-1)^i x^{2^{d-2}})(1 + (-1)^k x^{-2^{d-2}}) = \begin{cases} 2(1 + x^{2^{d-1}})(1 + (-1)^i x^{2^{d-2}}) & \text{if } i = k, \\ 0 & \text{if } i \neq k, \end{cases}$$

and multiplication by $1 + (-1)^j y^{2^{d-1}}$ for $j \in \{0, 1\}$ then gives

$$(1 + (-1)^i x^{2^{d-2}}) \psi_{0j} (1 + (-1)^k x^{-2^{d-2}}) = \begin{cases} 2(1 + x^{2^{d-1}}) \chi_{ij}(x, y^2) & \text{if } i = k, \\ 0 & \text{if } i \neq k. \end{cases} \tag{19}$$

We can now establish (18) for $(i, j) = (0, 0)$. Using (17), we calculate

$$\begin{aligned} \alpha_{00} \psi_{00} \alpha_{00}^{(-1)} &= ((1 + x^{2^{d-2}})A_{00}(x, y^2) + y(1 - x^{2^{d-2}})A_{10}(x, y^2)) \times \psi_{00} \\ &\quad \times ((1 + x^{-2^{d-2}})A_{00}(x, y^2)^{(-1)} + y^{-1}(1 - x^{-2^{d-2}})A_{10}(x, y^2)^{(-1)}) \\ &= 2(1 + x^{2^{d-1}})A_{00}(x, y^2) \chi_{00}(x, y^2) A_{00}(x, y^2)^{(-1)} \\ &\quad + 2(1 + x^{2^{d-1}})A_{10}(x, y^2) \chi_{10}(x, y^2) A_{10}(x, y^2)^{(-1)}, \end{aligned} \tag{20}$$

using (19) with $i \neq k$ to remove the terms involving $A_{00}(x, y^2)A_{10}(x, y^2)^{(-1)}$ and $A_{10}(x, y^2)A_{00}(x, y^2)^{(-1)}$, and using (19) with $i = k$ to simplify the surviving terms. Take $X = x$ and $Y = y^2$ in (16) to show that, in the polynomial ring $\mathbb{Z}[x, y]/\langle 1 - x^{2^{d-1}}, 1 - y^{2^d} \rangle$,

$$A_{ij}(x, y^2) \chi_{ij}(x, y^2) A_{ij}(x, y^2)^{(-1)} = 2^{2d-4} \chi_{ij}(x, y^2) \quad \text{for each } (i, j) \in U_2.$$

This implies that, in the polynomial ring $\mathbb{Z}[x, y]/\langle 1 - x^{2^d}, 1 - y^{2^d} \rangle$,

$$(1 + x^{2^{d-1}})A_{ij}(x, y^2) \chi_{ij}(x, y^2) A_{ij}(x, y^2)^{(-1)} = 2^{2d-4}(1 + x^{2^{d-1}}) \chi_{ij}(x, y^2) \quad \text{for each } (i, j) \in U_2.$$

Substitution in (20) then gives

$$\alpha_{00} \psi_{00} \alpha_{00}^{(-1)} = 2^{2d-3}(1 + x^{2^{d-1}})(\chi_{00}(x, y^2) + \chi_{10}(x, y^2)) = 2^{2d-2} \psi_{00},$$

so (18) holds for $(i, j) = (0, 0)$.

A similar derivation gives

$$\alpha_{01} \psi_{01} \alpha_{01}^{(-1)} = 2^{2d-3}(1 + x^{2^{d-1}})(\chi_{01}(x, y^2) + \chi_{11}(x, y^2)) = 2^{2d-2} \psi_{01},$$

$$\alpha_{10} \psi_{10} \alpha_{10}^{(-1)} = 2^{2d-3}(1 + y^{2^{d-1}})(\chi_{10}(x^2, y) + \chi_{11}(x^2, y)) = 2^{2d-2} \psi_{10},$$

so that (18) holds for $(i, j) = (0, 1)$ and $(i, j) = (1, 0)$.

Therefore the α_{ij} form a signature set on K_d with respect to E . This shows that case d is true and completes the induction. \square

We next illustrate the recursive construction method used in the proof of Theorem 3.2.

Example 3.3. A trivial signature set $\{A_{ij}^1 : (i, j) \in U_2\}$ on C_2^2 with respect to itself is given by

$$A_{ij}^1 = 1 \quad \text{for all } (i, j) \in U_2.$$

Apply the recursion (17) with $d = 2$ to obtain the signature set $\{A_{ij}^2 : (i, j) \in U_2\}$ on $C_4^2 = \langle x, y \rangle$ with respect to $\langle x^2, y^2 \rangle \cong C_2^2$ given by

$$\begin{aligned} A_{00}^2 &= A_{01}^2 = (1+x) + y(1-x) = 1+x+y-xy, \\ A_{10}^2 &= (1+y) + x(1-y) = 1+x+y-xy, \\ A_{11}^2 &= (1+xy) + x(1-xy) = 1+x-x^2y+xy. \end{aligned}$$

Apply the recursion (17) again with $d = 3$ to obtain the signature set $\{A_{ij}^3 : (i, j) \in U_2\}$ on $C_8^2 = \langle x, y \rangle$ with respect to $\langle x^4, y^4 \rangle \cong C_2^2$ given by

$$\begin{aligned} A_{00}^3 &= (1+x^2)A_{00}^2(x, y^2) + y(1-x^2)A_{10}^2(x, y^2) \\ &= (1+x^2)(1+x+y^2-xy^2) + y(1-x^2)(1+x+y^2-xy^2), \\ A_{01}^3 &= (1+x^2)A_{01}^2(x, y^2) + y(1-x^2)A_{11}^2(x, y^2) \\ &= (1+x^2)(1+x+y^2-xy^2) + y(1-x^2)(1+x-x^2y^2+xy^2), \\ A_{10}^3 &= (1+y^2)A_{10}^2(x^2, y) + x(1-y^2)A_{11}^2(x^2, y) \\ &= (1+y^2)(1+x^2+y-x^2y) + x(1-y^2)(1+x^2-x^4y+x^2y), \\ A_{11}^3 &= (1+x^2y^2)A_{10}^2(x^2, xy) + x(1-x^2y^2)A_{11}^2(x^2, xy) \\ &= (1+x^2y^2)(1+x^2+xy-x^3y) + x(1-x^2y^2)(1+x^2-x^5y+x^3y). \end{aligned}$$

We note that the recursion (17) in the proof of Theorem 3.2 has a simpler form when expressed in terms of group ring elements $B_{ij} = A_{ij}\chi_{ij}$ and $\beta_{ij} = \alpha_{ij}\psi_{ij}$, namely

$$\begin{aligned} \beta_{00}(x, y) &= (1+x^{2^{d-1}})(B_{00}(x, y^2) + yB_{10}(x, y^2)), \\ \beta_{01}(x, y) &= (1+x^{2^{d-1}})(B_{01}(x, y^2) + yB_{11}(x, y^2)), \\ \beta_{10}(x, y) &= (1+y^{2^{d-1}})(B_{10}(x^2, y) + xB_{11}(x^2, y)), \\ \beta_{11}(x, y) &= (1-y^{2^{d-1}})(B_{10}(x^2, xy) + xB_{11}(x^2, xy)). \end{aligned}$$

We now prove Theorem 3.1 in full generality, using the proof of Theorem 3.2 as a model. We abbreviate some of the proof, focusing attention on the parts for which a new argument or additional care is needed.

Proof of Theorem 3.1. The proof is by induction on $d \geq 1$. In the case $d = 1$, we have $r = 2$ and $\mathcal{K}_{1,2} = \{C_2^2\}$. The case $d = 1$ is therefore true, because there exists a trivial signature set on C_2^2 .

Assume all cases up to $d - 1 \geq 1$ are true. We shall write $u = (i, j, u_3, \dots, u_r) \in U_r$ as (i, j, v) , where $v = (u_3, \dots, u_r)$. Let

$$K_{d,r} = C_{2^{a_1}} \times \cdots \times C_{2^{a_r}} = \langle x, y, x_3, \dots, x_r \rangle \in \mathcal{K}_{d,r},$$

where $x^{2^{a_1}} = y^{2^{a_2}} = x_3^{2^{a_3}} = \cdots = x_r^{2^{a_r}} = 1$ and $d - r + 2 \geq a_1 \geq a_2 \geq \cdots \geq a_r \geq 1$ and $\sum_i a_i = 2d - r + 2$. The unique subgroup of $K_{d,r}$ isomorphic to C_2^r is $E_{d,r} = \langle x^{2^{a_1-1}}, y^{2^{a_2-1}}, x_3^{2^{a_3-1}}, \dots, x_r^{2^{a_r-1}} \rangle$.

If $a_r = 1$, then by the inductive hypothesis there is a signature set on the group $\langle x, y, x_3, \dots, x_{r-1} \rangle \in \mathcal{K}_{d-1,r-1}$. In that case we may use Proposition 2.5 to combine this with a trivial signature set on C_2 in order to obtain the required signature set on $K_{d,r}$ with respect to $E_{d,r}$.

We may therefore take $d - r + 2 \geq a_1 \geq a_2 \geq \cdots \geq a_r \geq 2$. This implies that $r \leq d$, and if $r > 2$ then $a_3 \leq d - r + 1$ (otherwise $2d - r + 2 = \sum_i a_i \geq 3(d - r + 2) + (r - 3)2 = 3d - r$, giving the contradiction $r \leq d \leq 2$). By the inductive hypothesis, the group

$$C_{2^{a_1-1}} \times C_{2^{a_2-1}} \times C_{2^{a_3}} \times \cdots \times C_{2^{a_r}} = \langle X, Y, x_3, \dots, x_r \rangle \in \mathcal{K}_{d-1,r},$$

where $X^{2^{a_1-1}} = Y^{2^{a_2-1}} = x_3^{2^{a_3}} = \cdots = x_r^{2^{a_r}} = 1$, therefore contains a signature set $\{A_{ijv} : (i, j, v) \in U_r\}$ with respect to $E_{d-1,r} = \langle X^{2^{a_1-2}}, Y^{2^{a_2-2}}, x_3^{2^{a_3-1}}, \dots, x_r^{2^{a_r-1}} \rangle$.

Regard each group ring element A_{ijv} as a polynomial in X, Y, x_3, \dots, x_r , but abbreviate this as $A_{ijv}(X, Y)$ because we will make variable substitutions only for X and Y . Similarly, regard each character of $E_{d-1,r}$ as a polynomial

$$\chi_{ijv}(X, Y) = (1 + (-1)^i X^{2^{a_1-2}})(1 + (-1)^j Y^{2^{a_2-2}})\tau_v$$

where

$$\tau_v = (1 + (-1)^{u_3} x_3^{2^{a_3-1}}) \cdots (1 + (-1)^{u_r} x_r^{2^{a_r-1}}).$$

By assumption, in the polynomial ring $\mathbb{Z}[X, Y, x_3, \dots, x_r]/\langle 1 - X^{2^{a_1-1}}, 1 - Y^{2^{a_2-1}}, 1 - x_3^{2^{a_3}}, \dots, 1 - x_r^{2^{a_r}} \rangle$ we have

$$A_{ijv}(X, Y)\chi_{ijv}(X, Y)A_{ijv}(X, Y)^{(-1)} = 2^{2d-2r}\chi_{ijv}(X, Y) \quad \text{for each } (i, j, v) \in U_r. \quad (21)$$

We wish to construct a signature set $\{\alpha_{ijv} : (i, j, v) \in U_r\}$ on $K_{d,r}$ with respect to $E_{d,r}$. Define the α_{ijv} in $\mathbb{Z}K_{d,r}$ in terms of the polynomials A_{ijv} via

$$\begin{aligned} \alpha_{00v} &= (1 + x^{2^{a_1-2}})A_{00v}(x, y^2) + y(1 - x^{2^{a_1-2}})A_{10v}(x, y^2), \\ \alpha_{01v} &= (1 + x^{2^{a_1-2}})A_{01v}(x, y^2) + y(1 - x^{2^{a_1-2}})A_{11v}(x, y^2), \\ \alpha_{10v} &= (1 + y^{2^{a_2-2}})A_{10v}(x^2, y) + x(1 - y^{2^{a_2-2}})A_{11v}(x^2, y), \\ \alpha_{11v} &= (1 + x^{2^{a_1-2}}y^{2^{a_2-2}})A_{10v}(x^2, x^{2^{a_1-a_2}}y) + x(1 - x^{2^{a_1-2}}y^{2^{a_2-2}})A_{11v}(x^2, x^{2^{a_1-a_2}}y), \end{aligned} \quad (22)$$

and let the characters of $E_{d,r}$ be

$$\psi_{ijv} = (1 + (-1)^i x^{2^{a_1-1}})(1 + (-1)^j y^{2^{a_2-1}})\tau_v \quad \text{for each } (i, j, v) \in U_r.$$

We firstly use Proposition 2.4 to show it is sufficient to prove for each $(i, j, v) \neq (1, 1, v)$ that α_{ijv} is a signature block with respect to ψ_{ijv} . Let σ be the group automorphism of $K_{d,r}$ that maps x to itself and maps y to $x^{2^{a_1-a_2}}y$ (which has order 2^{a_2}). Then $\sigma(\alpha_{10v}) = \alpha_{11v}$ by definition, and σ fixes $E_{d,r}$,

and $\sigma(\psi_{10v}) = \psi_{11v}$. Therefore if α_{10v} is a signature block on $K_{d,r}$ with respect to ψ_{10v} , then α_{11v} is a signature block on $K_{d,r}$ with respect to ψ_{11v} by Proposition 2.4.

We next show that each α_{00v} is a $\{\pm 1\}$ -valued function on a set of coset representatives for $E_{d,r}$ in $K_{d,r}$, and a similar argument shows that the same holds for each α_{01v} and α_{10v} . Fix $z = x_3^{i_3} \dots x_r^{i_r}$. By definition, $A_{00v}(X, Y)$ is $\{\pm 1\}$ -valued on exactly one of the four values

$$\{X^i Y^j z, X^i Y^{j+2^{a_2-2}} z, X^{i+2^{a_1-2}} Y^j z, X^{i+2^{a_1-2}} Y^{j+2^{a_2-2}} z\}$$

for $0 \leq i < 2^{a_1-2}, 0 \leq j < 2^{a_2-2}$. It follows that α_{00v} is $\{\pm 1\}$ -valued on exactly one of the four values

$$\{x^i y^j z, x^i y^{j+2^{a_2-1}} z, x^{i+2^{a_1-1}} y^j z, x^{i+2^{a_1-1}} y^{j+2^{a_2-1}} z\}$$

for $0 \leq i < 2^{a_1-1}, 0 \leq j < 2^{a_2-1}$.

It remains to show that in $\mathbb{Z}K_{d,r}$ we have

$$\alpha_{ijv} \psi_{ijv} \alpha_{ijv}^{(-1)} = 2^{2d-2r+2} \psi_{ijv} \quad \text{for each } (i, j, v) \neq (1, 1, v). \tag{23}$$

For $i, j, k \in \{0, 1\}$, we have the identity

$$(1 + (-1)^i x^{2^{a_1-2}}) \psi_{0jv} (1 + (-1)^k x^{-2^{a_1-2}}) = \begin{cases} 2(1 + x^{2^{a_1-1}}) \chi_{ijv}(x, y^2) & \text{if } i = k, \\ 0 & \text{if } i \neq k, \end{cases} \tag{24}$$

from which we now establish (23) for $(i, j, v) = (0, 0, v)$. We calculate

$$\begin{aligned} \alpha_{00v} \psi_{00v} \alpha_{00v}^{(-1)} &= ((1 + x^{2^{a_1-2}}) A_{00v}(x, y^2) + y(1 - x^{2^{a_1-2}}) A_{10v}(x, y^2)) \times \psi_{00v} \\ &\quad \times ((1 + x^{-2^{a_1-2}}) A_{00v}(x, y^2)^{(-1)} + y^{-1}(1 - x^{-2^{a_1-2}}) A_{10v}(x, y^2)^{(-1)}) \\ &= 2(1 + x^{2^{a_1-1}}) A_{00v}(x, y^2) \chi_{00v}(x, y^2) A_{00v}(x, y^2)^{(-1)} \\ &\quad + 2(1 + x^{2^{a_1-1}}) A_{10v}(x, y^2) \chi_{10v}(x, y^2) A_{10v}(x, y^2)^{(-1)}, \end{aligned} \tag{25}$$

using (24). Take $X = x$ and $Y = y^2$ in (21) to show that, in the polynomial ring $\mathbb{Z}[x, y, x_3, \dots, x_r] / \langle 1 - x^{2^{a_1}}, 1 - y^{2^{a_2}}, 1 - x_3^{2^{a_3}}, \dots, 1 - x_r^{2^{a_r}} \rangle$,

$$(1 + x^{2^{a_1-1}}) A_{ijv}(x, y^2) \chi_{ijv}(x, y^2) A_{ijv}(x, y^2)^{(-1)} = 2^{2d-2r} (1 + x^{2^{a_1-1}}) \chi_{ijv}(x, y^2) \quad \text{for each } (i, j, v) \in U_r.$$

Substitution in (25) then gives

$$\alpha_{00v} \psi_{00v} \alpha_{00v}^{(-1)} = 2^{2d-2r+1} (1 + x^{2^{a_1-1}}) (\chi_{00v}(x, y^2) + \chi_{10v}(x, y^2)) = 2^{2d-2r+2} \psi_{00v},$$

so (23) holds for $(i, j, v) = (0, 0, v)$.

A similar derivation gives

$$\begin{aligned} \alpha_{01v} \psi_{01v} \alpha_{01v}^{(-1)} &= 2^{2d-2r+1} (1 + x^{2^{a_1-1}}) (\chi_{01v}(x, y^2) + \chi_{11v}(x, y^2)) = 2^{2d-2r+2} \psi_{01v}, \\ \alpha_{10v} \psi_{10v} \alpha_{10v}^{(-1)} &= 2^{2d-2r+1} (1 + y^{2^{a_2-1}}) (\chi_{10v}(x^2, y) + \chi_{11v}(x^2, y)) = 2^{2d-2r+2} \psi_{10v}, \end{aligned}$$

so that (23) holds for $(i, j, v) = (0, 1, v)$ and $(i, j, v) = (1, 0, v)$.

Therefore the α_{ijv} form a signature set on $K_{d,r}$ with respect to $E_{d,r}$. This shows that case d is true and completes the induction. □

We now illustrate the recursive construction method used in the proof of Theorem 3.1.

Example 3.4. We shall construct a signature set on $C_8 \times C_4^2$. By Example 3.3, there is a signature set $\{A'_{ik} : (i, k) \in U_2\}$ on $C_4^2 = \langle x, z \rangle$ with respect to $\langle x^2, z^2 \rangle$ given by

$$\begin{aligned} A'_{00} = A'_{01} = A'_{10} &= 1 + x + z - xz, \\ A'_{11} &= 1 + x - x^2z + xz. \end{aligned}$$

Use the product construction of Proposition 2.5 to combine this with a trivial signature set on C_2 , producing a signature set $\{A_{ijk} : (i, j, k) \in U_3\}$ on $C_4 \times C_2 \times C_4 = \langle x, y, z \rangle$ with respect to $\langle x^2, y, z^2 \rangle \cong C_2^3$ given by

$$\begin{aligned} A_{000} = A_{010} = A_{001} = A_{011} = A_{100} = A_{110} &= 1 + x + z - xz, \\ A_{101} = A_{111} &= 1 + x - x^2z + xz. \end{aligned}$$

Now apply the recursion (22) to produce a signature set $\{\alpha_{ijk} : (i, j, k) \in U_3\}$ on $C_8 \times C_4^2 = \langle x, y, z \rangle$ with respect to $\langle x^4, y^2, z^2 \rangle \cong C_2^3$ given by

$$\begin{aligned} \alpha_{000} &= (1 + x^2)(1 + x + z - xz) + y(1 - x^2)(1 + x + z - xz), \\ \alpha_{001} &= (1 + x^2)(1 + x + z - xz) + y(1 - x^2)(1 + x - x^2z + xz), \\ \alpha_{010} &= (1 + x^2)(1 + x + z - xz) + y(1 - x^2)(1 + x + z - xz), \\ \alpha_{011} &= (1 + x^2)(1 + x + z - xz) + y(1 - x^2)(1 + x - x^2z + xz), \\ \alpha_{100} &= (1 + y)(1 + x^2 + z - x^2z) + x(1 - y)(1 + x^2 + z - x^2z), \\ \alpha_{101} &= (1 + y)(1 + x^2 - x^4z + x^2z) + x(1 - y)(1 + x^2 - x^4z + x^2z), \\ \alpha_{110} &= (1 + x^2y)(1 + x^2 + z - x^2z) + x(1 - x^2y)(1 + x^2 + z - x^2z), \\ \alpha_{111} &= (1 + x^2y)(1 + x^2 - x^4z + x^2z) + x(1 - x^2y)(1 + x^2 - x^4z + x^2z). \end{aligned}$$

4. Further construction methods

As shown in Table 1, our main result (Theorem 1.15) uses signature sets on abelian groups to provide constructions for difference sets in the great majority of the groups of order 64 and 256 that are not excluded by Theorems 1.3 and 1.5. In this section, we describe the methods that were used to show that the 22 remaining groups of order 64, and the 1,416 remaining groups of order 256, all belong to \mathcal{H} .

In Section 4A, we present a construction method arising under Theorem 2.3 from a signature set on a nonabelian group; recall that Definition 2.1 for a signature set does not require the group K to be abelian. In Section 4B, we present a product construction using perfect ternary arrays, without constraining these arrays in relation to a subgroup. In Section 4C, we describe three nonsystematic methods of transferring a difference set in one group to another. We used the methods of Sections 4A–4C to establish that all but one of the 22 remaining nonexcluded groups of order 64, and all but one of the 1,416 remaining nonexcluded groups of order 256, belong to \mathcal{H} . In Section 4D, we describe the construction of a Hadamard difference set in both of these final groups using group representations. In Section 4E, we show that the signature set construction of Section 4A and the perfect ternary array product construction of Section 4B are closely

related and can sometimes be combined, which could in future assist in determining which 2-groups of order larger than 256 belong to \mathcal{H} .

4A. Signature set on nonabelian group. Our first construction method applies Theorem 2.3 to a signature set on a nonabelian group to produce Hadamard difference sets in a variety of larger groups. We illustrate this method by exhibiting a signature set on the quaternion group of order 8.

Proposition 4.1. *Let $Q = \langle x, y : x^4 = y^4 = 1, yxy^{-1} = x^{-1}, x^2 = y^2 \rangle$ be the quaternion group of order 8, and let G be a group of order 16 containing a subgroup isomorphic to Q . Then $G \in \mathcal{H}$.*

Proof. Let $E_1 = \langle x^2 \rangle \cong C_2$, and let

$$\chi_0 = 1 + x^2, \quad \chi_1 = 1 - x^2$$

be the characters of E_1 . Since E_1 is the unique subgroup of Q isomorphic to C_2 , and Q has index 2 and so is normal in G , we have that E_1 is normal in G . Therefore by Theorem 2.3 with $r = 1$, it is sufficient to exhibit a signature set $\{A_0, A_1\}$ on Q with respect to E_1 (and then according to (14) there is a difference set in G of the form $g_0A_0\chi_0 + g_1A_1\chi_1$).

Let $A = 1 - x - y - xy$, and let $\{A_0, A_1\} = \{A, A\}$. Then A is a $\{\pm 1\}$ -valued function on a set of coset representatives for E_1 in Q , and direct calculation shows that $AA^{(-1)} = 4$ in $\mathbb{Z}Q$. Since E_1 is a central subgroup of Q , we therefore have in $\mathbb{Z}Q$ that

$$A_u\chi_uA_u^{(-1)} = A_uA_u^{(-1)}\chi_u = 4\chi_u = \frac{1}{2}|Q|\chi_u \quad \text{for } u \in \{0, 1\},$$

as required. □

As noted prior to Table 1, we can use Theorem 1.15 and Proposition 4.1 to recover the classification of Hadamard groups of order 16 carried out in the 1970s: Theorem 1.15 accounts for the 10 groups containing a normal subgroup isomorphic to C_2^2 , and Proposition 4.1 accounts for 2 further groups (the generalized quaternion group and the semidihedral group) containing a subgroup isomorphic to Q .

Furthermore, using Proposition 2.5 we may now take the product of a signature set on Q with respect to E_1 given in the proof of Proposition 4.1, and a trivial signature set on C_2 , to give a signature set on $Q \times C_2$ with respect to $E_1 \times C_2 \cong C_2^2$. Then from Theorem 2.3, every group of order 64 containing a normal subgroup isomorphic to $Q \times C_2$ belongs to \mathcal{H} .

We now use a Hadamard difference set to construct a signature set on certain groups of order 2^{2d+1} .

Proposition 4.2. *Suppose D is a Hadamard difference set in a group H , and let $E_1 \cong C_2$. Then $\{D, D\}$ is a signature set on $H \times E_1$ with respect to E_1 .*

Proof. We are given that D is a $\{\pm 1\}$ -valued function on the set H of coset representatives for E_1 in $H \times E_1$. Let $\{A_0, A_1\} = \{D, D\}$, and write $E_1 = \langle x \rangle$ so that the characters of E_1 are $\chi_0 = 1 + x$ and $\chi_1 = 1 - x$. Since x commutes with D , we have in $\mathbb{Z}(H \times E_1)$ that

$$A_u\chi_uA_u^{(-1)} = DD^{(-1)}\chi_u = |H|\chi_u = \frac{1}{2}|H \times E_1|\chi_u \quad \text{for } u \in \{0, 1\},$$

as required. □

Corollary 4.3. *Suppose $H \in \mathcal{H}$. Let G be a group containing a normal subgroup $E_1 \cong C_2$, and containing $H \times E_1$ as a subgroup of index 2. Then $G \in \mathcal{H}$.*

Proof. By Proposition 4.2, there exists a signature set on $H \times E_1$ with respect to E_1 . Since E_1 and $H \times E_1$ are both normal in G , we have $G \in \mathcal{H}$ by Theorem 2.3. \square

The technique of constructing Hadamard difference sets from signature sets on nonabelian groups appears to have significant potential, but we do not currently have a method of producing such signature sets that is as powerful as the recursive construction used to prove Theorem 3.1 for abelian groups.

4B. Product of perfect ternary arrays. Our second construction method relies on a key feature of the proof of Proposition 4.1, namely the existence of a $\{+1, 0, -1\}$ -valued function A on the group Q satisfying $AA^{(-1)} = 4$ in $\mathbb{Z}Q$. This function A is also $\{\pm 1\}$ -valued on a set of coset representatives for a subgroup of Q , but we do not require this additional structure in the following definition.

Definition 4.4. Let G be a group. A *perfect ternary array* in G is a $\{+1, 0, -1\}$ -valued function T on G satisfying $TT^{(-1)} = c$ in $\mathbb{Z}G$ for some integer c .

The set of elements of a group G on which a group ring element $A \in \mathbb{Z}G$ is nonzero is the *support* of A ; the size of this set is the *weight* of A , written $\text{wt}(A)$. We firstly show that the integer c in Definition 4.4 is equal to the weight of the perfect ternary array, and that it is a square.

Lemma 4.5. *Let G be a group, and suppose $T = \sum_{g \in G} t_g g$ is a perfect ternary array where each $t_g \in \{+1, 0, -1\}$. Then $TT^{(-1)} = \text{wt}(T) = \left(\sum_{g \in G} t_g\right)^2$.*

Proof. For some integer c , we have

$$c = TT^{(-1)} = \left(\sum_{h \in G} t_h h\right) \left(\sum_{g \in G} t_g g^{-1}\right) = \sum_{k \in G} \left(\sum_{g \in G} t_{kg} t_g\right) k$$

by writing $k = hg^{-1}$. Comparison of the coefficients of 1_G and $k \neq 1_G$ gives

$$\begin{aligned} c &= \sum_{g \in G} t_g^2, \\ 0 &= \sum_{g \in G} t_{kg} t_g \quad \text{for } k \neq 1_G. \end{aligned} \tag{26}$$

These relations together give

$$c = \sum_{k \in G} \sum_{g \in G} t_{kg} t_g = \sum_{g \in G} \left(\sum_{h \in G} t_h\right) t_g = \left(\sum_{g \in G} t_g\right)^2.$$

The result follows by combining with (26), noting that $\sum_{g \in G} t_g^2 = \text{wt}(T)$ because T is $\{+1, 0, -1\}$ -valued. \square

By Lemma 4.5 and (1), we may regard a Hadamard difference set in a group G as a perfect ternary array T in G for which $TT^{(-1)} = |G|$. A survey of results on the matrix representation of a perfect ternary array in an abelian group is given in [Arasu and Dillon 1999]. We next give two examples of perfect ternary arrays of weight 4, whose properties can be verified by direct calculation. The second example appears in the proof of Proposition 4.1.

Example 4.6 (unpublished work of Dillon [1990]). (i) Suppose G is a group containing a nonidentity element x and an involution (element of order 2) y that commutes with x . Then $T = 1 - x - y - xy$ is a perfect ternary array of weight 4 in G .

(ii) Let $Q = \langle x, y : x^4 = y^4 = 1, yxy^{-1} = x^{-1}, x^2 = y^2 \rangle$ be the quaternion group of order 8. Then $T = 1 - x - y - xy$ is a perfect ternary array of weight 4 in Q .

Every perfect ternary array of weight 4 in a group of even order is equivalent to Example 4.6(i) or (ii) [Bhattacharya and Smith 2008, Lemma 2].

We now construct a Hadamard difference set as a product of perfect ternary arrays.

Proposition 4.7 (unpublished work of Dillon [1990], Bhattacharya and Smith [2008]). *Let T_1, T_2, \dots, T_s be subsets of a group G , and let $D = \prod_{i=1}^s T_i$. Suppose that*

- (i) *each T_i is a perfect ternary array in G ,*
- (ii) $\text{wt}(D) = \prod_{i=1}^s \text{wt}(T_i)$,
- (iii) $\text{wt}(D) = |G|$.

Then D corresponds to a Hadamard difference set in G .

Proof. By condition (ii), D is a $\{+1, 0, -1\}$ -valued function on G . Now $DD^{(-1)} = \prod_{i=1}^s \text{wt}(T_i)$ by Lemma 4.5, and then by conditions (ii) and (iii) we have $DD^{(-1)} = |G|$. \square

Since a Hadamard difference set is a special case of a perfect ternary array, we may regard Theorem 1.2 as constructing a Hadamard difference set in G as the product $D_1 D_2$ of two perfect ternary arrays D_1 and D_2 contained in subgroups H_1 and H_2 of G . In contrast, Proposition 4.7 constructs Hadamard difference sets as the product of s perfect ternary arrays T_i , with the important relaxation that each T_i need not be structurally constrained in relation to a subgroup of G .

This generality gives Proposition 4.7 considerable power. We take each T_i to be either a perfect ternary array of weight 4 (having one of the two forms of Example 4.6), or else a Hadamard difference set in a subgroup of G . This allows us to construct all 27 inequivalent difference sets in the 12 groups of order 16 contained in \mathcal{H} [Bhattacharya and Smith 2008]; a difference set in 17 of the 22 remaining nonexcluded groups of order 64; and a difference set in 1,358 of the 1,416 remaining nonexcluded groups of order 256; see Table 1. However, the same generality means that testing whether a group G lies in \mathcal{H} because of Proposition 4.7 (involving a computer search over all suitable perfect ternary arrays) is significantly slower than testing whether G lies in \mathcal{H} because of Theorem 1.15 (involving simply testing whether G contains a suitable normal abelian subgroup); see Section 5 for further details.

4C. Transfer methods. The construction methods of previous sections are collectively sufficient to demonstrate that the great majority of the groups of order 64 and 256 that are not excluded by Theorems 1.3 and 1.5 belong to \mathcal{H} . The key in almost all of these demonstrations is the existence of a signature set on a normal subgroup, from which a difference set arises using Theorem 2.3. Nonetheless, while the signature set concept is very powerful, it does not appear to be sufficient to determine \mathcal{H} completely. The reason is that some groups (2 of order 64, and 10 of order 256) have the property that each of their normal subgroups also occurs as a normal subgroup of a group that is not in \mathcal{H} . We therefore require construction methods that do not rely on a signature set. We now describe three such methods, each of which uses a difference set in one group to discover a difference set in another (and so “transfers” a difference set between the two groups).

The first transfer method makes use of the equivalence between a difference set in a group G and a symmetric design on whose points G acts as a regular (sharply transitive) automorphism group. If the full automorphism group of the design is sufficiently large, it may well contain other subgroups which also act regularly on the points of the design; in this case, each of these subgroups also contains a difference set. For example, the group C_2^4 contains a difference set giving a $(16, 6, 2)$ symmetric design whose 2-rank is 6, and the automorphism group of this design contains 12 nonisomorphic subgroups of order 16 acting regularly on the points of the design. We thereby transfer a single difference set in C_2^4 to a difference set in all 11 of the other Hadamard groups of order 16. Similarly, the group C_2^6 contains a difference set giving a $(64, 28, 12)$ symmetric design whose 2-rank is 8, and the automorphism group of this design contains 171 nonisomorphic subgroups of order 64 acting regularly on the points of the design. We thereby transfer a single difference set in C_2^6 to 170 of the other 258 Hadamard groups of order 64.

The second transfer method applies when a difference set gives an algebraic structure in the group ring that also exists in other group rings. An example is Dillon’s proof [1985] of Theorem 1.5, which transfers a putative difference set in a group with a large dihedral quotient to a difference set in a group with a large cyclic quotient in order to apply the nonexistence result of Theorem 1.3. A second example is Theorem 2.3, which can be viewed as using Theorem 1.9 to transfer a difference set in an abelian group that contains K to a difference set in a variety of nonabelian groups containing K . A third example is [Dillon 1990a, Theorem 2], which transfers a difference set among groups sharing a subgroup H of index 2 and a central element g not in H . In general, suppose that a group G is known to contain a difference set D , and that G contains a large normal subgroup K . Let $\{g_u\}$ be a set of coset representatives for K in G , and partition the elements of D according to their membership of the cosets of K to write $D = \sum_u g_u D_u$, where each $D_u \in \mathbb{Z}K$. Now let G' be a group having the same order as G and containing a normal subgroup K' isomorphic to K . Let ϕ be an isomorphism from K to K' . To transfer the difference set D from G to G' we seek, by hand or by computer search, a set of coset representatives $\{g'_u\}$ for K' in G' for which $\sum_u g'_u \phi(D_u)$ is a difference set in G' .

The third transfer method takes advantage of the structure created by the GAP method for labeling group elements. A difference set D with parameters (v, k, λ) in a group G of order v can be represented in GAP as a k -subset S of the element labels $\{1, 2, \dots, v\}$. Given such a subset S representing a difference

set in G , we test in GAP whether the same subset S also represents a difference set in another group G' of order v . This method appears to have a greater chance of success when the GAP numbering for G' is close to that of G , which often occurs when G' has similar structure to G .

None of these three transfer methods is systematic, and it is not yet clear when they can be expected to succeed. Nonetheless, we were able to apply them to show that all but one of the remaining 5 nonexcluded groups of order 64, and all but one of the remaining 58 nonexcluded groups of order 256, belong to \mathcal{H} ; see Table 1. We construct a difference set in the final group of order 64 and of order 256 in Section 4D.

4D. The final group of order 64 and of order 256. The final two groups whose membership in \mathcal{H} we wish to demonstrate are the order 64 modular group

$$M_{64} = C_{32} \rtimes_{17} C_2 = \langle x, y : x^{32} = y^2 = 1, yxy^{-1} = x^{17} \rangle,$$

and the order 256 group

$$C_{64} \rtimes_{47} C_4 = \langle x, y : x^{64} = y^4 = 1, yxy^{-1} = x^{47} \rangle$$

that is referenced in [GAP 2020] as SmallGroup(256, 536). These nonabelian groups are each a cyclic extension of a cyclic group, and have small center and high exponent. Historically, they were the last groups of their order whose membership in \mathcal{H} was determined: M_{64} in 1991 [Liebler and Smith 1993], and SmallGroup(256, 536) in 2016 [Yolland 2016].

We firstly describe the original construction method used in [Liebler and Smith 1993] and [Yolland 2016], which strengthens the representation theory approach used in [Davis and Smith 1994, Section 5] to construct a difference set in the order 256 group $C_{64} \rtimes_{33} C_4 = \langle x, y : x^{64} = y^4 = 1, yxy^{-1} = x^{33} \rangle$. We shall then reinterpret these constructions as arising from a modification of a signature set.

Proposition 4.8. *Let G be a 2-group, let g be a central involution in G , and let \natural be the natural map from G onto $G/\langle g \rangle$. Suppose there are $\{+1, 0, -1\}$ -valued functions D_0, D_1 on G for which $D_0(1+g)$ and $D_1(1-g)$ have disjoint supports whose union is G , and for which*

$$\natural(D_0)\natural(D_0)^{(-1)} = \frac{1}{4}|G| \quad \text{in } \mathbb{Z}(G/\langle g \rangle), \quad (27)$$

$$D_1(1-g)D_1^{(-1)} = \frac{1}{4}|G|(1-g) \quad \text{in } \mathbb{Z}G. \quad (28)$$

Then $G \in \mathcal{H}$.

Proof. We note that the existence of a central involution g in the 2-group G follows from the class equation for finite groups. Let

$$D = D_0(1+g) + D_1(1-g) \quad \text{in } \mathbb{Z}G, \quad (29)$$

which is a $\{\pm 1\}$ -valued function on G by the assumption on the supports of $D_0(1+g)$ and $D_1(1-g)$.

We now calculate

$$DD^{(-1)} = 2D_0(1+g)D_0^{(-1)} + 2D_1(1-g)D_1^{(-1)} \quad \text{in } \mathbb{Z}G. \quad (30)$$

By (27), in $\mathbb{Z}(G/\langle g \rangle)$ we have

$$\frac{1}{4}|G|1_{G/\langle g \rangle} = \natural(D_0)\natural(D_0)^{(-1)} = (D_0\langle g \rangle)(D_0^{(-1)}\langle g \rangle) = D_0D_0^{(-1)}\langle g \rangle,$$

so that in $\mathbb{Z}G$ we have

$$\frac{1}{4}|G|(1+g) = D_0D_0^{(-1)}(1+g) = D_0(1+g)D_0^{(-1)}$$

because g is central in G . Substitute this and (28) into (30) to obtain

$$DD^{(-1)} = \frac{1}{2}|G|(1+g) + \frac{1}{2}|G|(1-g) = |G|.$$

Therefore D corresponds to a Hadamard difference set in G . □

When applying Proposition 4.8, we firstly seek a $\{+1, 0, -1\}$ -valued group ring element D_0 satisfying condition (27), namely that $\natural(D_0)$ is a perfect ternary array of weight $\frac{1}{4}|G|$ in the factor group $G/\langle g \rangle$. We then seek a $\{+1, 0, -1\}$ -valued group ring element D_1 satisfying (28) for which $D_0(1+g)$ and $D_1(1-g)$ have disjoint supports whose union is G . It turns out that finding D_0 is relatively easy, whereas finding D_1 is much more difficult.

Example 4.9 (Liebler and Smith [1993] construction for M_{64}). We apply Proposition 4.8 to construct a Hadamard difference set in $M_{64} = C_{32} \rtimes_{17} C_2 = \langle x, y : x^{32} = y^2 = 1, yxy^{-1} = x^{17} \rangle$. The center of M_{64} is $\langle x^2 \rangle$, so x^{16} is a central involution.

A $\{+1, 0, -1\}$ -valued group ring element D_0 satisfying

$$\natural(D_0)\natural(D_0)^{(-1)} = 16 \quad \text{in } \mathbb{Z}(M_{64}/\langle x^{16} \rangle)$$

is given by

$$D_0 = A_{00}(1+y) + A_{01}(1-y),$$

where

$$A_{00} = -x^7(1+x^8) + (1-x^8), \quad \text{and} \quad A_{01} = x(1+x^8) + x^4(1-x^8).$$

This was easily found by hand, because the factor group $M_{64}/\langle x^{16} \rangle$ is isomorphic to the abelian group $C_{16} \times C_2$.

A $\{+1, 0, -1\}$ -valued group ring element D_1 satisfying

$$D_1(1-x^{16})D_1^{(-1)} = 16(1-x^{16}) \quad \text{in } \mathbb{Z}M_{64}$$

is given by

$$D_1 = A_{10}(1+y) + A_{11}(1-y),$$

where

$$A_{10} = (x^6 - x^5)(1 - x^8), \quad \text{and} \quad A_{11} = (x^2 + x^3)(1 + x^8).$$

This was found by hand using the irreducible representations induced by the character (homomorphism) that maps x^{16} to -1 .

Now $D_0(1+x^{16})$ has support $(1+x+x^4+x^7)\langle x^8, y \rangle$, and $D_1(1-x^{16})$ has support $(x^2+x^3+x^5+x^6)\langle x^8, y \rangle$. These supports are disjoint and their union is M_{64} . We conclude from the construction of Proposition 4.8 that $D = D_0(1+x^{16}) + D_1(1-x^{16})$ corresponds to a difference set in M_{64} .

Example 4.10 (Yolland [2016] construction for $\text{SmallGroup}(256, 536)$). We apply Proposition 4.8 to construct a Hadamard difference set in $G = C_{64} \rtimes_{47} C_4 = \langle x, y : x^{64} = y^4 = 1, yxy^{-1} = x^{47} \rangle$. The center of G is $\langle x^{32} \rangle$, so x^{32} is a central involution.

A $\{+1, 0, -1\}$ -valued group ring element D_0 satisfying

$$\natural(D_0)\natural(D_0)^{(-1)} = 64 \quad \text{in } \mathbb{Z}(G/\langle x^{32} \rangle)$$

is given by

$$D_0 = A_{00}(1+y^2) + A_{01}(1-y^2),$$

where

$$\begin{aligned} A_{00} &= ((1-x^8) - x^2(1+x^8))(1+x^{16}) + (x^5+x^6y)(1+x^8)(1-x^{16}), \\ A_{01} &= ((1-x^8) - x^5(1+x^8))y(1+x^{16}) + (-x^3(1-x^8)y + x^3(1+x^8))(1-x^{16}). \end{aligned}$$

This was found by hand by seeking a perfect ternary array of weight 64 in the nonabelian factor group $G/\langle x^{32} \rangle \cong C_{32} \rtimes_{15} C_4$.

A $\{+1, 0, -1\}$ -valued group ring element D_1 satisfying

$$D_1(1-x^{32})D_1^{(-1)} = 64(1-x^{32}) \quad \text{in } \mathbb{Z}G$$

is given by

$$D_1 = A_{10}(1+y^2) + A_{11}(1-y^2),$$

where

$$\begin{aligned} A_{10} &= -((x+x^4+x^9+x^{12}+x^{14})(1+x^{16}) + (x^6+x^7-x^{15})(1-x^{16})), \\ A_{11} &= -((x-x^9+x^{10})(1+x^{16}) + (x^2+x^4-x^7+x^{12}-x^{15})(1-x^{16}))y. \end{aligned}$$

This was found by a difficult computer search. Although a naive search for D_1 involves a search space of size 2^{64} , the search was shortened by using the irreducible representations induced by the character (homomorphism) that maps x^{32} to -1 , and by making some simplifying assumptions about the structure of the target difference set [Yolland 2016].

Now $D_0(1+x^{32})$ has support $(1+x^2+x^3+x^5+(1+x^3+x^5+x^6)y)\langle x^8, y^2 \rangle$, and $D_1(1-x^{32})$ has support $(x+x^4+x^6+x^7+(x+x^2+x^4+x^7)y)\langle x^8, y^2 \rangle$. These supports are disjoint and their union is G . We conclude from the construction of Proposition 4.8 that $D = D_0(1+x^{32}) + D_1(1-x^{32})$ corresponds to a difference set in G .

We now reinterpret Examples 4.9 and 4.10 as arising from a modification of a signature set.

Lemma 4.11. *Let G be a group containing a normal subgroup $E \cong C_2^r$, and let $\{\chi_u : u \in U_r\}$ be the set of characters of E . Let A_u be a $\{+1, 0, -1\}$ -valued function on G for each $u \in U_r$, where the A_u have disjoint supports whose union is a set of coset representatives for E_r in G . Suppose that*

$$\sum_{u \in U_r} A_u \chi_u A_u^{(-1)} = \frac{|G|}{2^r} \quad \text{in } \mathbb{Z}G. \quad (31)$$

Then $G \in \mathcal{H}$.

Proof. Let

$$D = \sum_{u \in U_r} A_u \chi_u \quad \text{in } \mathbb{Z}G,$$

which by the assumption on the supports of the A_u is a $\{\pm 1\}$ -valued function on G . We calculate $DD^{(-1)} = |G|$ using Proposition 1.7(i), and so D corresponds to a Hadamard difference set in G . \square

By Proposition 1.7(ii), one way to achieve (31) in Lemma 4.11 would be for the A_u to satisfy the condition in $\mathbb{Z}G$ that

$$A_u \chi_u A_u^{(-1)} = \frac{|G|}{2^{2r}} \chi_u \quad \text{for each } u \in U_r. \quad (32)$$

Such a set of A_u would be similar, but not identical, to a signature set on G with respect to E : the conditions on the supports in Lemma 4.11 are different from those in Definition 2.1, and the constant in (32) is $|G|/2^{2r}$ rather than $|G|/2^r$.

A crucial observation in reinterpreting Examples 4.9 and 4.10 is that a weaker condition than (32) suffices. In particular, in the case $r = 2$, this condition can be weakened to

$$A_{0j} \chi_{0j} A_{0j}^{(-1)} = \frac{1}{16} |G| \chi_{0j} \quad \text{for each } j \in \{0, 1\}, \quad (33)$$

$$A_{10} \chi_{10} A_{10}^{(-1)} + A_{11} \chi_{11} A_{11}^{(-1)} = \frac{1}{16} |G| (\chi_{10} + \chi_{11}), \quad (34)$$

in which the expressions $A_{10} \chi_{10} A_{10}^{(-1)}$ and $A_{11} \chi_{11} A_{11}^{(-1)}$ behave like a ‘‘complementary pair’’ whose sum is the same as if (32) held.

In Example 4.9, the group M_{64} contains the normal subgroup $E_2 = \langle x^{16}, y \rangle \cong C_2^2$ whose characters are

$$\chi_{ij} = (1 + (-1)^i x^{16})(1 + (-1)^j y) \quad \text{for } (i, j) \in U_2.$$

The difference set D takes the form

$$D = D_0(1 + x^{16}) + D_1(1 - x^{16}) = \sum_{(i,j) \in U_2} A_{ij} \chi_{ij}$$

where the A_{ij} take the values specified in the example. These A_{ij} satisfy the conditions of Lemma 4.11 on their supports. Since conjugation by x fixes χ_{00} and χ_{01} but swaps χ_{10} and χ_{11} , we find by direct calculation that

$$A_{0j} \chi_{0j} A_{0j}^{(-1)} = 4 \chi_{0j} \quad \text{for each } j \in \{0, 1\}$$

388 T. Applebaum, J. Clikeman, J. A. Davis, J. F. Dillon, J. Jedwab, T. Rabbani, K. Smith and W. Yolland
and

$$\begin{aligned} A_{10}\chi_{10}A_{10}^{(-1)} + A_{11}\chi_{11}A_{11}^{(-1)} &= (2(1-x^{-1})\chi_{10} + 2(1-x)\chi_{11}) + (2(1+x^{-1})\chi_{10} + 2(1+x)\chi_{11}) \\ &= 4(\chi_{10} + \chi_{11}), \end{aligned}$$

so that (33) and (34) hold.

The reinterpretation of Example 4.10 is similar. $\text{SmallGroup}(256, 536)$ contains the normal subgroup $E_2 = \langle x^{32}, y^2 \rangle \cong C_2^2$, whose characters are

$$\chi_{ij} = (1 + (-1)^i x^{32})(1 + (-1)^j y^2) \quad \text{for } (i, j) \in U_2.$$

The difference set D takes the form

$$D = D_0(1 + x^{32}) + D_1(1 - x^{32}) = \sum_{(i,j) \in U_2} A_{ij}\chi_{ij},$$

where the A_{ij} take the values specified in the example. These A_{ij} satisfy the conditions of Lemma 4.11 on their supports. Conjugation by x fixes χ_{00} and χ_{01} but swaps χ_{10} and χ_{11} , and we find once again (after a long calculation) that (33) and (34) hold.

4E. Combination of signature sets and perfect ternary arrays. The nonabelian signature set approach of Section 4A and the perfect ternary array product construction of Section 4B are closely related. For example, Proposition 4.2 may be interpreted as constructing a signature set on $H \times E_1$ from a perfect ternary array D in H . We now illustrate how a perfect ternary array in a factor group can be used to create a signature block with respect to a specific character. We believe the illustrated method could be useful in future studies of the existence pattern for Hadamard difference sets in 2-groups of order greater than 256.

Lemma 4.12. *Let K be a group containing a central subgroup $E \cong C_2^r$, and let χ be a character of E . Suppose that $\chi = H\chi'$ in $\mathbb{Z}E$ for some subgroup H of E . Let \natural be the natural map from K onto K/H , and suppose that A is a $\{+1, 0, -1\}$ -valued function on K for which $\natural(A)$ is a perfect ternary array of weight 2^{2j} in K/H . Then*

$$A\chi A^{(-1)} = 2^{2j}\chi \quad \text{in } \mathbb{Z}K.$$

Proof. Since $\natural(A)$ is a perfect ternary array of weight 2^{2j} in K/H , in $\mathbb{Z}(K/H)$ we have by Lemma 4.5 that

$$2^{2j}1_{K/H} = \natural(A)\natural(A)^{(-1)} = (AH)(A^{(-1)}H) = AA^{(-1)}H.$$

For $k \in K$, interpret the element kH in K/H as $|H|$ elements in K , so that in the group ring $\mathbb{Z}K$ the above equation becomes

$$2^{2j}H = AA^{(-1)}H.$$

By assumption we have $\chi = H\chi'$, and H and χ' are central in K because E is. Therefore in $\mathbb{Z}K$ we have

$$A\chi A^{(-1)} = AH\chi' A^{(-1)} = AA^{(-1)}H\chi' = 2^{2j}H\chi' = 2^{2j}\chi. \quad \square$$

In Lemma 4.12, note that the group ring condition $\chi = H\chi'$ is equivalent to $H \in \text{Ker}(\chi)$ when the character χ is considered as a homomorphism of E . Also note that if E has index 2^{2j} in K , and A is $\{\pm 1\}$ -valued on a set of coset representatives for E in K , then the conclusion of Lemma 4.12 is that A is a signature block on K with respect to χ .

We now use Lemma 4.12 to explain the origin of the signature set introduced in Example 1.13.

Example 4.13. Let $K = \langle X, Y \rangle \cong C_4^2$ and $E = \langle X^2, Y^2 \rangle \cong C_2^2$, and let $\{\chi_u : u \in U_2\}$ be the set of characters of E . We use Lemma 4.12 to construct the signature set

$$A_{00} = A_{01} = A_{10} = 1 + X + Y - XY \quad \text{and} \quad A_{11} = 1 + X + Y + XY$$

on K that was presented in Example 1.13 without explanation of its origin.

For $\chi = \chi_{00}$ or χ_{10} , take $H = \langle Y^2 \rangle$ and $A = 1 - X - Y - XY$. Then $\natural(A)$ is a perfect ternary array of weight 4 in K/H by Example 4.6(i), because $\natural(Y)$ is an involution that commutes with the nonidentity element $\natural(X)$. Lemma 4.12 then shows that A is a signature block on K with respect to χ_{00} and χ_{10} . Since $A_{00}\chi_{00} = -XYA\chi_{00}$ and $A_{10}\chi_{10} = XA\chi_{10}$ in $\mathbb{Z}K$, it follows from Definition 2.1 and Proposition 1.7(i) that $A_{00} = A_{10}$ is a signature block on K with respect to both χ_{00} and χ_{10} . By symmetry in X and Y , it follows that A_{01} is also a signature block on K with respect to χ_{01} .

For $\chi = \chi_{11}$, take $H = \langle X^2Y^2 \rangle$ and $A = 1 + X + XY - X^2Y$. Then $\natural(A)$ is a perfect ternary array of weight 4 in K/H by Example 4.6(i), because $\natural(XY)$ is an involution that commutes with the nonidentity element $\natural(X)$. By Lemma 4.12 and the relation $A_{11}\chi_{11} = A\chi_{11}$ in $\mathbb{Z}K$, we conclude that A_{11} is a signature block on K with respect to χ_{11} .

5. Computer implementation for groups of order 256

In this section, we provide further details of the streamlined procedure used to establish that each of the 56,049 groups of order 256 not excluded by Theorems 1.3 and 1.5 belongs to \mathcal{H} . We then describe online databases containing difference sets found by this procedure, and explain how the overall result can be quickly verified on a desktop computer using the accepted GAP package *DifSets* [Peifer 2019; DifSets 2019]. We note that *DifSets* provides (via the LoadDifferenceSets command) a listing of all inequivalent difference sets in groups of order 16 and 64.

5A. Procedure. As previously summarized in Section 1, the streamlined procedure for groups of order 256 comprises three stages:

Stage 1: Use Theorem 1.15 to account for the 54,633 groups containing a normal subgroup isomorphic to C_2^4 or $C_4^2 \times C_2$ or C_8^2 .

Stage 2: Use the product construction of Proposition 4.7 to account for 1,358 further groups.

Stage 3: Apply the transfer methods of Section 4C to account for 57 further groups, and the modified signature set method of Section 4D to account for the final group. We do not describe this stage further.

The relationship between the groups handled by Stages 1 and 2 is shown in Figure 1.

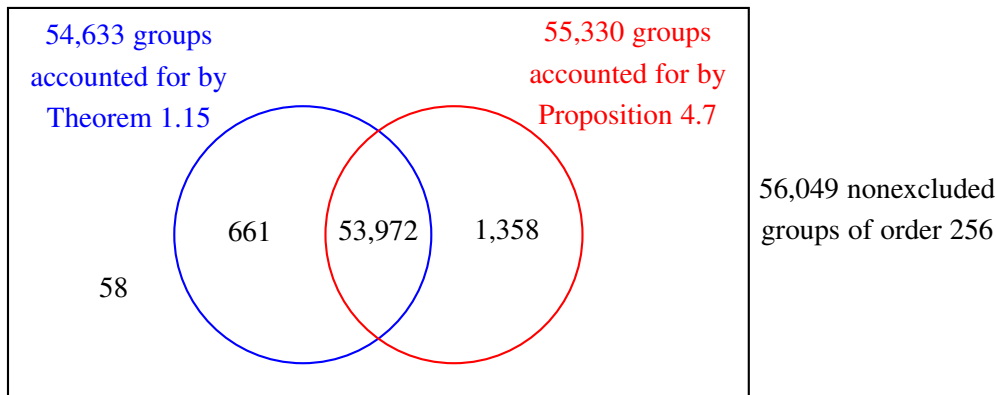


Figure 1. Theorem 1.15 and Proposition 4.7 show that at most 58 of the 56,049 nonexcluded groups of order 256 lie outside \mathcal{H} .

In Stage 1, we wish to construct a difference set in a group G of order 256 containing a normal abelian subgroup K , where K is isomorphic to C_2^4 or $C_4^2 \times C_2$ or C_8^2 . A signature set on K is provided trivially for the case C_2^4 (see the remark following Definition 2.1), by Example 3.4 for the case $C_4^2 \times C_2$, and by Example 3.3 for the case C_8^2 . We then apply the method in the proof of Theorem 2.3 to construct a difference set in G . This requires a set $\{g_u : u \in U_r\}$ of coset representatives for K in G satisfying (13), namely

$$\{g_u \chi_u g_u^{-1} : u \in U_r\} = \{\chi_u : u \in U_r\}.$$

The existence of such a set is guaranteed by Theorem 1.9, but the proof of this result in [Drisko 1998] is non-constructive. We therefore conduct a search for a suitable set of coset representatives $\{g_u\}$. This search is exhaustive for the cases $C_4^2 \times C_2$ and C_8^2 , but random for the case C_2^4 whose search space has size $15! > 10^{12}$.

The results of applying this search procedure to all 56,049 nonexcluded groups, for each of the three choices of K independently, are shown in Figure 2.

In Stage 2, we distinguish six instances of the product construction of Proposition 4.7 according to the form of its input perfect ternary arrays T_1, T_2, \dots, T_s .

- (i) **$\mathbf{H}_{64} \cdot \mathbf{Q}_4$ form.** Take T_1 to be a Hadamard difference set in a subgroup H_1 of G of order 64, and T_2 to be a perfect ternary array of weight 4 in G having the form of Example 4.6(ii) where the quaternion group $Q = \langle x, y \rangle$ of order 8 intersects H_1 in the two-element subgroup $\{1, x^2\}$.
- (ii) **$\mathbf{H}_{64} \cdot \mathbf{H}_4$ form.** Take T_1 to be a Hadamard difference set in a subgroup H_1 of G of order 64, and T_2 to be a Hadamard difference set in a subgroup H_2 of G of order 4, where $G = H_1 H_2$ and $H_1 \cap H_2 = 1$.
- (iii) **$\mathbf{H}_{16} \cdot \mathbf{H}_{16}$ form.** For $i = 1, 2$, take T_i to be a Hadamard difference set in a subgroup H_i of G of order 16, where $G = H_1 H_2$ and $H_1 \cap H_2 = 1$.
- (iv) **$\mathbf{H}_{64} \cdot \mathbf{T}_1$ form.** Take T_1 to be a perfect ternary array of weight 4 in G having the form of Example 4.6(i), and T_2 to be a Hadamard difference set in a subgroup of G of order 64.

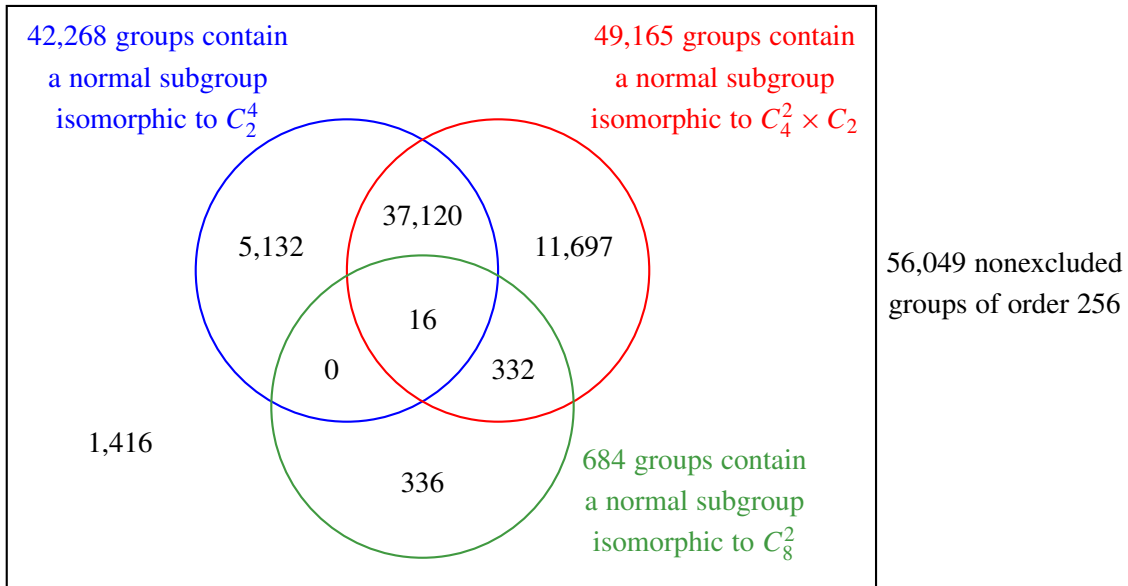


Figure 2. Theorem 1.15 shows that at most 1,416 of the 56,049 nonexcluded groups of order 256 lie outside \mathcal{H} .

- (v) **$H_{16} \cdot T_1 \cdot T_2$ form.** Take each of T_1, T_2 to be a perfect ternary array of weight 4 in G having either of the two forms of Example 4.6, and T_3 to be a Hadamard difference set in a subgroup of G of order 16.
- (vi) **$T_1 \cdot T_2 \cdot T_3 \cdot T_4$ form.** Take each of T_1, T_2, T_3, T_4 to be a perfect ternary array of weight 4 in G having either of the two forms of Example 4.6.

For each of these six forms, we conduct a search for a suitable set of perfect ternary arrays satisfying all the required conditions. The search for the forms (i) to (iii) is relatively fast because the search is restricted to subgroups of the appropriate order. However, the search for the forms (iv) to (vi) is not constrained in this way and can take considerably longer; the search for form (vi) sometimes requires more than a day for a single group.

We therefore begin by searching all 56,049 nonexcluded groups for each of the forms (i) to (iii) independently, with results as shown in Figure 2. We then conduct a search for each of the forms (iv) to (vi) in that order, but only over those groups in which no previous form has been found. The number of groups accounted for and remaining at each step of Stage 2 is shown below:

	$H_{64} \cdot Q_4$ and $H_{64} \cdot H_4$ and $H_{16} \cdot H_{16}$	$H_{64} \cdot T_1$	$H_{16} \cdot T_1 \cdot T_2$	$T_1 \cdot T_2 \cdot T_3 \cdot T_4$
# groups accounted for	51,957	3,119	236	18
# groups remaining	4,092	973	737	719

The Stage 2 searches are exhaustive in that none of the remaining 719 groups contains a difference set having one of the six forms (i) to (vi).

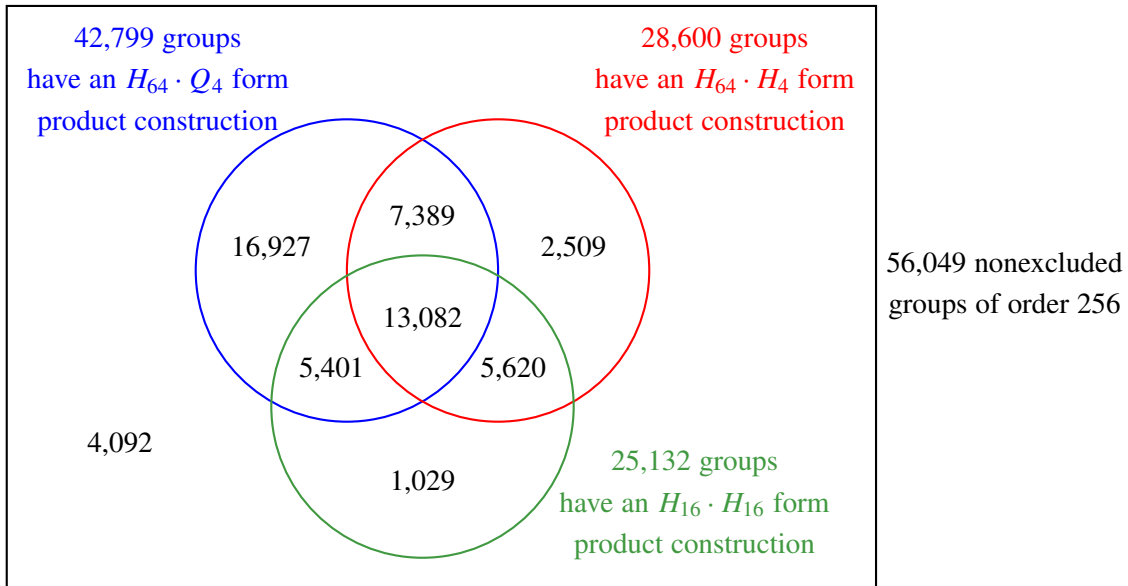


Figure 3. Forms $H_{64} \cdot Q_4$ and $H_{64} \cdot H_4$ and $H_{16} \cdot H_{16}$ of Proposition 4.7 show that at most 4,092 of the 56,049 nonexcluded groups of order 256 lie outside \mathcal{H} .

List	List name	Database name
L_1	HDS256_Normal_02x02x02x02	
L_2	HDS256_Normal_04x04x02	HDS256_NormalSubgroupTransversal.txt
L_3	HDS256_Normal_08x08	
L_4	HDS256_H64byQ4	
L_5	HDS256_H64byH4	HDS256_PTAProduct.txt
L_6	HDS256_H16byH16	
L_7	HDS256_H64byT1	
L_8	HDS256_H16byT1byT2	HDS256_SubgroupProduct.txt
L_9	HDS256_T1byT2byT3byT4	
L_{10}	HDS256	HDS256.txt

Table 2. Organization of difference set databases in [Smith 2022].

5B. Databases and verification. The website [Smith 2022] contains ten lists in GAP format, organized into four databases as shown in Table 2.

Lists L_1 to L_3 correspond to the three circles in Figure 2 (Stage 1). Lists L_4 to L_6 correspond to the three circles in Figure 3 (forms (i) to (iii) of Stage 2). Lists L_7 to L_9 correspond to forms (iv) to (vi) of Stage 2. Each entry of the lists L_1 to L_9 contains at least two fields: a catalog number i that identifies the group $\text{SmallGroup}(256, i)$, and a list of 120 indices taken from $\{1, 2, \dots, 256\}$ in which index j labels group element j according to the GAP ordering given by $\text{Elements}(\text{SmallGroup}(256, i))$.

The list L_{10} contains one entry for each of the 56,092 groups of order 256. If $\text{SmallGroup}(256, i)$ is one of the 43 groups excluded by Theorems 1.3 and 1.5 (see Table 1), then entry i of L_{10} is an empty list of indices. Otherwise, this entry is a list of 120 indices corresponding to a representative difference set in $\text{SmallGroup}(256, i)$. The representative difference set is taken from list L_1 if possible, otherwise from L_2 , and so on to L_9 . This accounts for the origin of all but 58 of the nonempty entries of L_{10} .

After reading the list HDS256 into the current directory, the following GAP code uses Peifer's accepted GAP package *DifSets* [2019] to verify that HDS256 contains an index list corresponding to a difference set for 56,049 groups of the 56,092 groups of order 256, and an empty index list for the remaining 43 groups:

```
LoadPackage("DifSets");
empty := 0;
count := 0;
for i in [1..Length(HDS256)] do;
  if HDS256[i] = [] then
    empty := empty+1;
  else
    if IsDifferenceSet(SmallGroup(256,i), HDS256[i]) then
      count := count+1;
    fi;
  fi;
od;
Print("HDS256 contains ", Length(HDS256), " index lists, of which\n");
Print(count, " correspond to a difference set and ", empty, "
are empty\n");
```

It took less than 20 minutes to run this code on a 2013 iMac desktop computer using a standard implementation of GAP, producing the following output:

```
HDS256 contains 56092 index lists, of which
56049 correspond to a difference set and 43 are empty
```

Although we found it considerably more difficult to construct a difference set in some groups of order 256 than in others, there is no significant variation in verification time among groups of a given order using the `IsDifferenceSet` command of *DifSets*.

6. Future directions

In this section, we propose directions for future research into Hadamard difference sets and their relations to other combinatorial objects.

We have described in this paper a streamlined procedure for demonstrating that all groups of order 64 and 256, apart from those that are excluded by the classical nonexistence results of Theorems 1.3 and 1.5,

belong to the class \mathcal{H} of Hadamard difference sets. While we consider this to be a major achievement in combinatorics, it is unsatisfactory that we do not yet have a completely theoretical demonstration.

We now propose the following directions for future research into Hadamard difference sets, with three overall objectives in mind. The first objective is to simplify and unify the various techniques of Section 4, removing the reliance on extensive computer search and the nonsystematic transfer methods. The second objective is to develop recursive or direct construction techniques for nonabelian groups, that are as powerful as Theorem 3.1 is for constructing signature sets on abelian groups. The third and ultimate objective is to resolve Question 1.17.

- D1. The concept of signature sets on abelian groups (Theorem 3.1) and on nonabelian groups (Section 4A) appears to be very powerful. Develop construction methods to determine all nonabelian groups on which there is a signature set relative to a normal elementary abelian subgroup.
- D2. Apply Lemma 4.12 to create signature sets in nonabelian groups, generalizing the model of Example 4.13.
- D3. Understand when and why the transfer methods of Section 4C succeed.
- D4. Develop a general theory based on the method of Section 4D so that transfer methods are no longer needed for groups of order 64 and 256.
- D5. Representation theory was used to help find the group ring element D_1 in Examples 4.9 and 4.10. Apply representation theory to unify and extend the construction methods of Section 4.
- D6. In the study of bent functions, which are equivalent to Hadamard difference sets in elementary abelian 2-groups, one asks how many inequivalent examples exist in a given group. Determine how many inequivalent Hadamard difference sets in (not necessarily elementary abelian) 2-groups can be constructed using the methods of this paper.
- D7. Formulate a theoretical framework that can be systematically applied to determine all 2-groups belonging to \mathcal{H} .
- D8. Extend the transfer methods of Section 4C to construct Hadamard difference sets in new groups whose order is not a power of 2, for example in groups of order 100 [Golemac and Vučičić 2001], 144 [Vučičić 2019], or 400 [Mandić and Vučičić 2016].

We also propose some further research directions involving the relation of Hadamard difference sets to other combinatorial objects:

- D9. Difference sets in the Hadamard, McFarland, Spence, and Chen–Davis–Jedwab families have parameters (v, k, λ) satisfying $\gcd(v, k - \lambda) > 1$, and are known to share construction methods based on covering extended building sets and semiregular relative difference sets [Davis and Jedwab 1997; Chen 1997]. Adapt the signature set approach for Hadamard difference sets in order to construct difference sets in nonabelian groups for the other three families, and the associated semiregular relative difference sets in nonabelian groups for all four families.

- D10. Determine how many inequivalent designs arise from the Hadamard difference sets constructed in this paper.
- D11. Determine how many inequivalent binary codes arise from the incidence matrices of the Hadamard difference sets constructed in this paper.

References

- [Applebaum 2013] T. Applebaum, *Difference Sets in Non-Abelian 2-Groups*, Honors thesis, University of Richmond, 2013.
- [Arasu and Dillon 1999] K. T. Arasu and J. F. Dillon, “Perfect ternary arrays”, pp. 1–15 in *Difference sets, sequences and their correlation properties* (Bad Windsheim, 1998), edited by A. Pott et al., NATO Adv. Sci. Inst. Ser. C: Math. Phys. Sci. **542**, Kluwer Acad. Publ., Dordrecht, 1999. MR Zbl
- [Besche et al. 2002] H. U. Besche, B. Eick, and E. A. O’Brien, “A millennium project: constructing small groups”, *Internat. J. Algebra Comput.* **12**:5 (2002), 623–644. MR Zbl
- [Beth et al. 1999] T. Beth, D. Jungnickel, and H. Lenz, *Design theory, Vol. I*, 2nd ed., Encyclopedia of Mathematics and its Applications **69**, Cambridge University Press, 1999. MR Zbl
- [Bhattacharya and Smith 2008] C. Bhattacharya and K. W. Smith, “Factoring (16, 6, 2) Hadamard difference sets”, *Electron. J. Combin.* **15**:1 (2008), Research Paper 112, 16. MR Zbl
- [Bruck 1955] R. H. Bruck, “Difference sets in a finite group”, *Trans. Amer. Math. Soc.* **78** (1955), 464–481. MR Zbl
- [Burrell 2022] D. Burrell, “On the number of groups of order 1024”, *Comm. Algebra* **50**:6 (2022), 2408–2410. MR Zbl
- [Carlet and Mesnager 2016] C. Carlet and S. Mesnager, “Four decades of research on bent functions”, *Des. Codes Cryptogr.* **78**:1 (2016), 5–50. MR Zbl
- [Chen 1997] Y. Q. Chen, “On the existence of abelian Hadamard difference sets and a new family of difference sets”, *Finite Fields Appl.* **3**:3 (1997), 234–256. MR Zbl
- [Davis 1991] J. A. Davis, “Difference sets in abelian 2-groups”, *J. Combin. Theory Ser. A* **57**:2 (1991), 262–286. MR Zbl
- [Davis and Jedwab 1996] J. A. Davis and J. Jedwab, “A survey of Hadamard difference sets”, pp. 145–156 in *Groups, difference sets, and the Monster* (Columbus, OH, 1993), edited by K. T. Arasu et al., Ohio State Univ. Math. Res. Inst. Publ. **4**, de Gruyter, Berlin, 1996. MR Zbl
- [Davis and Jedwab 1997] J. A. Davis and J. Jedwab, “A unifying construction for difference sets”, *J. Combin. Theory Ser. A* **80**:1 (1997), 13–78. MR Zbl
- [Davis and Smith 1994] J. A. Davis and K. Smith, “A construction of difference sets in high exponent 2-groups using representation theory”, *J. Algebraic Combin.* **3**:2 (1994), 137–151. MR Zbl
- [DifSets 2019] D. Peifer, “GAP package DifSets: an algorithm for enumerating all difference sets in a group”, 2019, available at <https://www.gap-system.org/Packages/difsets.html>. Version 2.3.1. Zbl
- [Dillon 1985] J. F. Dillon, “Variations on a scheme of McFarland for noncyclic difference sets”, *J. Combin. Theory Ser. A* **40**:1 (1985), 9–21. MR Zbl
- [Dillon 1990a] J. F. Dillon, “Difference sets in 2-groups”, pp. 65–72 in *Finite geometries and combinatorial designs* (Lincoln, NE, 1987), edited by E. S. Kramer and S. S. Magliveras, Contemp. Math. **111**, Amer. Math. Soc., Providence, RI, 1990. MR Zbl
- [Dillon 1990b] J. F. Dillon, “A survey of difference sets in 2-groups: Hadamard groups of order 64”, University of Vermont, 1990. Presented at Marshall Hall conference.
- [Dillon 2010] J. F. Dillon, “Some REALLY beautiful Hadamard matrices”, *Cryptogr. Commun.* **2**:2 (2010), 271–292. MR Zbl
- [Drisko 1998] A. A. Drisko, “Transversals in row-Latin rectangles”, *J. Combin. Theory Ser. A* **84**:2 (1998), 181–195. MR Zbl
- [GAP 2020] The GAP Group, “GAP: groups, algorithms, and programming”, 2020, available at <http://www.gap-system.org>. Version 4.11.0.
- [Golemac and Vučićić 2001] A. Golemac and T. Vučićić, “New difference sets in nonabelian groups of order 100”, *J. Combin. Des.* **9**:6 (2001), 424–434. MR Zbl
- [Jedwab 1992] J. Jedwab, “Generalized perfect arrays and Menon difference sets”, *Des. Codes Cryptogr.* **2**:1 (1992), 19–68. MR Zbl

- [Jungnickel and Schmidt 1998] D. Jungnickel and B. Schmidt, “Difference sets: a second update”, pp. 89–118 in *Combinatorics '98*, Rend. Circ. Mat. Palermo (2) Suppl. **53**, 1998. MR Zbl
- [Kesava Menon 1962] P. Kesava Menon, “On difference sets whose parameters satisfy a certain relation”, *Proc. Amer. Math. Soc.* **13** (1962), 739–745. MR Zbl
- [Kibler 1978] R. E. Kibler, “A summary of noncyclic difference sets, $k < 20$ ”, *J. Combinatorial Theory Ser. A* **25**:1 (1978), 62–67. MR Zbl
- [Kraemer 1993] R. G. Kraemer, “Proof of a conjecture on Hadamard 2-groups”, *J. Combin. Theory Ser. A* **63**:1 (1993), 1–10. MR Zbl
- [Liebler and Smith 1993] R. A. Liebler and K. W. Smith, “On difference sets in certain 2-groups”, pp. 195–211 in *Coding theory, design theory, group theory* (Burlington, VT, 1990), edited by D. Jungnickel et al., Wiley, New York, 1993. MR
- [Mandić and Vučičić 2016] J. Mandić and T. Vučičić, “On the existence of Hadamard difference sets in groups of order 400”, *Adv. Math. Commun.* **10**:3 (2016), 547–554. MR
- [Mann 1965] H. B. Mann, *Addition theorems: The addition theorems of group theory and number theory*, Interscience Publishers John Wiley & Sons, New York, 1965. MR Zbl
- [McFarland 1973] R. L. McFarland, “A family of difference sets in non-cyclic groups”, *J. Combinatorial Theory Ser. A* **15** (1973), 1–10. MR
- [Peifer 2019] D. Peifer, “An algorithm for enumerating difference sets”, *J. Softw. Algebra Geom.* **9**:1 (2019), 35–41. MR Zbl
- [Singer 1938] J. Singer, “A theorem in finite projective geometry and some applications to number theory”, *Trans. Amer. Math. Soc.* **43**:3 (1938), 377–385. MR Zbl
- [Sloane 2022] N. J. A. Sloane, “Number of groups of order 2^n ”, 2022, available at <https://oeis.org/A000679>.
- [Smith 2022] K. Smith, “Difference Set Databases”, 2022, available at <https://tinyurl.com/DifferenceSetDatabase>.
- [Turyn 1965] R. J. Turyn, “Character sums and difference sets”, *Pacific J. Math.* **15** (1965), 319–346. MR Zbl
- [Vučičić 2019] T. Vučičić, “Hadamard difference sets and related combinatorial objects in groups of order 144”, *Rad Hrvat. Akad. Znan. Umjet. Mat. Znan.* **23(538)** (2019), 13–29. MR Zbl
- [Whitehead 1975] E. G. Whitehead, Jr., “Difference sets and sum-free sets in groups of order 16”, *Discrete Math.* **13**:4 (1975), 399–407. MR Zbl
- [Yolland 2016] W. Yolland, “Existence of a difference set in the last group of order 256”, summer research report, Simon Fraser University, 2016.

Communicated by Sergey Fomin

Received 2020-12-02 Revised 2022-02-04 Accepted 2022-04-04

applebaum.taylor@gmail.com	<i>Department of Mathematics and Statistics, University of Richmond, Richmond, VA, United States</i>
<i>Current address:</i>	<i>DeepMind, London, United Kingdom</i>
jclikeman@gmail.com	<i>Department of Mathematics and Statistics, University of Richmond, Richmond, VA, United States</i>
<i>Current address:</i>	<i>Google, Mountain View, CA, United States</i>
jdavis@richmond.edu	<i>Department of Mathematics and Statistics, University of Richmond, Richmond, VA, United States</i>
jfdillon@gmail.com	<i>National Security Agency, Fort George G Meade, MD, United States</i>
jed@sfu.ca	<i>Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada</i>
trabbani@cs.umd.edu	<i>Department of Computer Science, University of Maryland, College Park, MD, United States</i>
kenwsmith54@gmail.com	<i>Department of Mathematics and Statistics, Sam Houston State University, Huntsville, TX, United States</i>
william@metaoptima.com	<i>Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada</i>
<i>Current address:</i>	<i>MetaOptima Technology Inc., Vancouver, BC, Canada</i>

The principal block of a \mathbb{Z}_ℓ -spets and Yokonuma type algebras

Radha Kessar, Gunter Malle and Jason Semeraro

We formulate conjectures concerning the dimension of the principal block of a \mathbb{Z}_ℓ -spets (as defined in our earlier paper), motivated by analogous statements for finite groups. We show that these conjectures hold in certain situations. For this we introduce and study a Yokonuma type algebra for torus normalisers in ℓ -compact groups which may be of independent interest.

1. Introduction

This paper is a contribution to the following broad question: Do there exist structures associated to finite complex reflection groups that play the same role as finite reductive groups play for finite Weyl groups? Broué, Michel and the second author [Malle 1995; Broué et al. 1999; 2014] discovered that to certain complex reflection groups can be associated data sets, called *spetses*, satisfying properties analogous to those of unipotent characters of finite reductive groups. Their construction is based upon generalisations of Hecke algebras which in turn arise from the braid groups associated to the space of regular orbits of complex reflection groups. On the other hand, ℓ -adic reflection groups for a prime number ℓ arise as the “Weyl” groups of certain topological spaces called *ℓ -compact groups* which possess much of the structure of compact groups [Dwyer and Wilkerson 1994; Grodal 2010]. Thus, spetses and ℓ -compact groups widen the context of group theory in two different directions — combinatorics/representation theory and algebraic topology.

We introduced [Kessar et al. 2020] the notion of a \mathbb{Z}_ℓ -spets, a new object to which both the spetsial theory and ℓ -compact group theory can be applied. It can be thought of as a finite reductive group which possesses a representation theory in characteristic zero and at the single prime ℓ . It thus allows one to investigate aspects of the yet not well understood ℓ -modular representation theory of finite reductive groups in a more general setting. We used this to exhibit a surprising consistency of spetses data with the famous Alperin weight conjecture [loc. cit.]. Our results lead us to hope that putting the modular representation theory of finite reductive groups in a broader context will pave the way to a better understanding of some of the deep open problems of representation theory.

Kessar gratefully acknowledges support from EPSRC grant EP/T004592/1. Malle gratefully acknowledges support by the DFG — Project-ID 286237555 — TRR 195.

MSC2020: primary 16G30, 20C08, 20C20, 20F55, 20G40; secondary 20D20, 55R35.

Keywords: ℓ -adic reflection groups, Yokonuma type algebra, principal block, spetses.

In this paper, we develop this theme further. In order to describe our results we recall some features of [Kessar et al. 2020]. Let ℓ be a prime number. Formally, a \mathbb{Z}_ℓ -spets $\mathbb{G} = (W\varphi^{-1}, L)$ is a spetsial ℓ -adic reflection group W on a \mathbb{Z}_ℓ -lattice L together with an element $\varphi \in N_{\text{GL}(L)}(W)$. Via the theory of ℓ -compact groups if q is a power of a prime different from ℓ , then under certain conditions, by [Broto and Møller 2007] one can associate a fusion system \mathcal{F} on a finite ℓ -group S to the pair $\mathbb{G}(q) := (\mathbb{G}, q)$. In this situation, S should be considered as a Sylow ℓ -subgroup of $\mathbb{G}(q)$. It turns out that the ℓ -compact theory provides us, for any $s \in S$, with a centraliser which again is a \mathbb{Z}_ℓ -spets. Using this we attached, in [Kessar et al. 2020], a “principal ℓ -block” B_0 to $\mathbb{G}(q)$, with defect group S . It consists of a collection $\text{Irr}(B_0)$ of sets (“irreducible characters”) in bijection with the unipotent characters attached to the centralisers of elements $s \in S$ (up to \mathcal{F} -conjugation), defined in terms of a collection of Hecke algebras. The construction of B_0 is modelled on and generalises the case of blocks of finite groups of Lie type in nondescribing characteristic. When W is rational and under some natural assumptions on ℓ , we recover the ℓ -fusion system $\mathcal{F}_\ell(\mathbb{G}(q))$ and principal ℓ -block $B_0(\mathbb{G}(q))$ of the associated finite reductive group $\mathbb{G}(q)$. See Section 4 for a description of B_0 and comparison with the rational case.

A primary concern in [Kessar et al. 2020] was the translation of certain local-global statements in modular representation theory to purely local statements using the language of \mathbb{Z}_ℓ -spetses. Here, our considerations are more on the global side, so that actual degrees of characters in $\text{Irr}(B_0)$ (as defined in [loc. cit., Definition 6.7]) play a more significant role. Firstly, we investigate the dimension

$$\dim(B_0) := \sum_{\gamma \in \text{Irr}(B_0)} \gamma(1)^2 \in \mathbb{Z}[x]$$

of B_0 . Motivated by results concerning the divisibility properties of this number for principal blocks of finite groups, we make the following conjecture:

Conjecture 1. *Let $\mathbb{G} = (W\varphi^{-1}, L)$ be a simply connected \mathbb{Z}_ℓ -spets for which ℓ is very good, let q be a power of a prime different from ℓ , and B_0 be the principal ℓ -block of $\mathbb{G}(q)$ with defect group S . Then:*

- (1) $(\dim(B_0)|_{x=q})_\ell = |S|$.
- (2) $(\dim(B_0)|_{x=q})_{\ell'} \equiv |W_{\varphi^{-1}\zeta^{-1}}|_{\ell'} \pmod{\ell}$, where $\zeta \in \mathbb{Z}_\ell^\times$ is the root of unity with $q \equiv \zeta \pmod{\ell}$, and $W_{\varphi^{-1}\zeta^{-1}}$ is the associated relative Weyl group; see [Kessar et al. 2020, Theorems 2.1 and 3.6] for the definition and role of the relative Weyl group.

For a finite group G with principal ℓ -block B_0 the equality $(\dim(B_0))_\ell = |S|$ is closely related to the fact that $|S|$ divides the dimension of each projective indecomposable module Φ_ν associated to $\nu \in \text{IBr}(B_0)$. When B_0 is as in Conjecture 1, and under the additional hypotheses that W is an ℓ' -group, φ is trivial and $q \equiv 1 \pmod{\ell}$, in Section 4B we formulate analogues of $\text{IBr}(B_0)$, decomposition numbers and $\deg \Phi_\nu$ for which we make the following additional conjecture:

Conjecture 2. *In the setting of Conjecture 1 if W is an ℓ' -group, φ is trivial and $q \equiv 1 \pmod{\ell}$ we have:*

- (3) $|S|$ divides $\deg \Phi_\nu|_{x=q}$ for all $\nu \in \text{IBr}(B_0)$.

Conjecture 1 combines the statements of Conjectures 4.2 and 4.3 and Conjecture 2 is restated as Conjecture 4.5 in Section 4. In Proposition 4.6, we prove that Conjectures 1 and 2 hold when W is rational or when $q \equiv 1 \pmod{\ell}$ and W is primitive. The general case for Conjecture 1 appears quite elusive, so we choose to simplify matters by assuming that W is an ℓ' -group, $q \equiv 1 \pmod{\ell}$ and $\varphi = 1$. Under these conditions we are able to show that our conjectures are closely related to certain previously studied properties of Hecke algebras which we discuss next.

Recall that the generic Hecke algebra $\mathcal{H}(W, \mathbf{u})$ of W is a certain quotient of the group algebra of the braid group $B(W)$ of W where \mathbf{u} is a set of parameters indexed by conjugacy classes of distinguished reflections in W . To each irreducible character χ of $\mathcal{H}(W, \mathbf{u})$ over a splitting field one associates a Schur element f_χ which, in turn, is used to define a canonical form

$$t_{W, \mathbf{u}} := \sum_{\chi \in \text{Irr}(\mathcal{H}(W, \mathbf{u}))} \frac{1}{f_\chi} \chi$$

on $\mathcal{H}(W, \mathbf{u})$. This is conjectured to be a symmetrising form [Broué et al. 1999]; see Conjecture 3.3. It is expected that the form $t_{W, \mathbf{u}}$ behaves well under restriction to parabolic subgroups and with respect to the natural map $B(W) \rightarrow W$; if that is the case we say $\mathcal{H}(W, \mathbf{u})$ is *strongly symmetric*; see Definition 3.4. Our main result is the following:

Theorem 1. *Let $\mathbb{G} = (W, L)$ be a simply connected \mathbb{Z}_ℓ -spets. Suppose that $\mathcal{H}(W, \mathbf{u})$ is strongly symmetric, W is an ℓ' -group and $q \equiv 1 \pmod{\ell}$. Then Conjectures 1 and 2 hold.*

Since the strongly symmetric condition is known to hold in many cases (see Proposition 3.5), we obtain:

Corollary 2. *Suppose W is a spetsial irreducible ℓ' -group, $\varphi = 1$ and $q \equiv 1 \pmod{\ell}$. Then Conjecture 1 holds for $\mathbb{G} = (W, L)$, and Conjecture 2 also holds, except possibly when W is primitive of rank at least 3.*

The method behind our proof of Theorem 1 may be even more interesting than the theorem itself. For our approach we introduce and study a Yokonuma type algebra \mathcal{Y} attached to an arbitrary finite ℓ -adic reflection group. We conjecture that \mathcal{Y} is finitely generated and free over its base ring (Conjecture 5.12) and show that this holds in many cases. It seems likely that if ℓ is very good for (W, L) , then \mathcal{Y} is a symmetric algebra with respect to a trace form whose Schur elements are derived from those of various parabolic subalgebras of $\mathcal{H}(W, \mathbf{u})$ (Question 5.18).

When \mathbb{G} is a rational spets which satisfies the hypotheses of Theorem 1, the principal block B_0 of $\mathbb{G}(q)$ is known to be Morita equivalent to SW over a finite extension of \mathbb{Z}_ℓ . The endomorphism algebra of the permutation module which captures this equivalence is a Yokonuma algebra isomorphic to a certain \mathbb{Z}_ℓ -algebra specialisation \mathcal{Y}_ψ of \mathcal{Y} ; see Section 5E. Moreover, the quantities $\dim(B_0)$ and $\deg \Phi_\nu$ ($\nu \in \text{IBr}(B_0)$) can be reexpressed in terms of the corresponding Schur elements of \mathcal{Y}_ψ .

This motivates the study of \mathcal{Y}_ψ and associated numerical properties for arbitrary ℓ -adic reflection groups. In Theorem 5.9 we show that if the parabolic subgroups of the underlying ℓ -adic reflection group are generated by reflections, then \mathcal{Y}_ψ is finitely generated and free over \mathbb{Z}_ℓ ; a result of Külshammer,

Okuyama and Watanabe then allows us to conclude that when the order of W is relatively prime to ℓ , then \mathcal{Y}_ψ is isomorphic to the group algebra of SW ; see Theorem 5.10. We obtain Theorem 1 by applying general results concerning the arithmetic behaviour of Schur elements in symmetric algebras (as discussed in Section 2C) to \mathcal{Y}_ψ , by playing off the form on \mathcal{Y}_ψ inherited from \mathcal{Y} against the standard symmetrising form on the group algebra of SW .

We close the introduction by discussing how the hypotheses on ℓ and W in Theorem 1 might be relaxed. If $\ell \mid |W|$ we have carried out explicit computations in support of Conjecture 1 when $q \equiv 1 \pmod{\ell}$, such as when $W = G(e, 1, 3)$ for $\ell = 3$ and when $W = G_{29}$ for the bad prime $\ell = 5$ assuming $\text{Irr}(B_0)$ is defined appropriately; see [Kessar et al. 2020, Remark 6.16]. In these situations, $\text{Irr}(B_0)$ is only partially describable in terms of the Schur elements of the Yokonuma algebra \mathcal{Y}_ψ . Even for Weyl groups it is a major open problem to find a description involving the Schur elements of a suitable larger algebra.

Structure of the paper. In Section 2 we collect some general material necessary for our proofs. In particular, we discuss certain divisibility properties of Schur elements in symmetric algebras. In Section 3 we recall the construction of Hecke algebras $\mathcal{H}(W, \mathbf{u})$ for complex reflection groups W and the origin of the trace form $t_{W, \mathbf{u}}$, define the property of being strongly symmetric (Definition 3.4) and introduce the relevant specialisations. In Section 4, we recall the description of the principal block of a \mathbb{Z}_ℓ -spets, introduce the notion of dimension and formulate our main conjectures. Our new Yokonuma type algebra \mathcal{Y} attached to an ℓ -adic reflection group (W, L) is defined and studied in Section 5. In Theorem 5.7 we describe the structure of \mathcal{Y} over the field of fractions of the base ring and in Theorem 5.10 we obtain, under additional conditions, a similar structural result for ℓ -adic specialisations of \mathcal{Y} . In Sections 5C and 5D we formulate general freeness and symmetrising form conjectures for \mathcal{Y} and show that the freeness conjecture holds for Coxeter groups (Theorem 5.13) and for most of the imprimitive complex reflection groups (Theorem 5.14). We also discuss the relationship of \mathcal{Y} to the algebra considered by Marin [2018a; 2018b] and in Section 5E we show that when (W, L) arises from a Weyl group the principal block of the classical Yokonuma algebra over \mathbb{Z}_ℓ is a certain specialisation of \mathcal{Y} . Section 5F contains the proof of Theorem 1 (Theorem 5.20) and Corollary 2.

2. Background material

2A. Finite generation of modules. First we record a few general facts on finite generation of modules. The first is a variation on Nakayama's lemma for nilpotent ideals which allows for the dropping of the finite generation hypothesis. Let R be a commutative ring with 1. Recall that the Jacobson radical $J(R)$ of R is the intersection of all maximal left ideals of R .

Lemma 2.1. *Let $I \subseteq J(R)$ be an ideal of R and let M, N be R -modules with $N \subseteq M$ and $M = N + IM$. Suppose that either M/N is finitely generated or that I is nilpotent. Then $N = M$.*

Proof. The case that M/N is finitely generated is the usual case of the Nakayama Lemma. Suppose that $I^r = 0$ for some $r \geq 1$. By hypothesis, $M/N = I(M/N)$. Hence $M/N = I^r(M/N) = 0$, showing that $M = N$. \square

Lemma 2.2. *Let R be a discrete valuation ring with uniformiser π . Suppose that $N \subseteq M$ are R -modules such that $M/\pi M$ is finitely generated, M/N is finitely generated and torsion free, and $\pi^r N = 0$ for some positive integer r . Then M is finitely generated.*

Proof. Since M/N is finitely generated, it suffices to show that N is finitely generated. Now $\pi^r N = 0$. So, in order to show that N is finitely generated it suffices to show that $\pi^i N/\pi^{i+1} N$ is finitely generated for any $i \geq 1$. Multiplication by π^i induces a surjective R -module homomorphism from $N/\pi N$ onto $\pi^i N/\pi^{i+1} N$, hence it suffices to show that $N/\pi N$ is finitely generated. By hypothesis, $M/\pi M$ is finitely generated and $N/(\pi M \cap N)$ is isomorphic to a submodule of $M/\pi M$. Thus, as R is Noetherian, $N/(\pi M \cap N)$ is finitely generated. But since M/N is torsion free, $\pi M \cap N = \pi N$. \square

2B. Clifford theory. The following is standard Clifford theory adapted to quotients of infinite group algebras with respect to finite normal subgroups. For a ring R and ideal I , we will regard without further comment an R/I -module as an R -module via pullback along the canonical homomorphism $R \rightarrow R/I$.

Lemma 2.3. *Let G be a group, T a finite normal subgroup of G and K a field of characteristic 0. For $\theta \in \text{Irr}_K(T)$, denote by e_θ the corresponding primitive central idempotent of KT and by G_θ the stabiliser of θ in G of (finite) index $n_\theta := |G : G_\theta|$. Let I be an ideal of KG and set $I_\theta := e_\theta I e_\theta = I \cap e_\theta K G e_\theta$:*

(a) *There is a K -algebra isomorphism*

$$KG/I \cong \prod_{\theta} \text{Mat}_{n_\theta}(e_\theta K G e_\theta / I_\theta)$$

where θ runs over a set of representatives of G -orbits on $\text{Irr}_K(T)$. Moreover, $e_\theta K G e_\theta / I_\theta = e_\theta K G_\theta e_\theta / I_\theta = K G_\theta e_\theta / I_\theta$ for all $\theta \in \text{Irr}_K(T)$.

(b) *The map $(\theta, U) \mapsto \text{Ind}_{G_\theta}^G U$ induces a bijection between the set of pairs (θ, U) , where θ runs over representatives of G -orbits on $\text{Irr}_K(T)$ and U runs over a set of isomorphism classes of simple $K G_\theta e_\theta / I_\theta$ -modules, and the set of isomorphism classes of simple KG/I -modules.*

Proof. Set $Y = KG/I$ and for $a \in KG$ denote by \bar{a} its image in Y . Let X be the set of orbits of the conjugation action of G on $\text{Irr}_K(T)$ and for each $x \in X$, let $e_x = \sum_{\theta \in x} e_\theta$. So $\{e_x \mid x \in X\}$ is a set of pairwise orthogonal central idempotents of KG with $1_{KG} = \sum_{x \in X} e_x$. Consequently, $\{\bar{e}_x \mid x \in X\}$ is a set of pairwise orthogonal central idempotents of Y with $1_Y = \sum_{x \in X} \bar{e}_x$. Here, we abuse notation to allow for the possibility that some \bar{e}_x are equal to zero. Thus

$$Y = \bigoplus_{x \in X} Y \bar{e}_x$$

and this is also a decomposition of Y into a direct product of K -algebras. Let $x \in X$ and $\theta \in x$. Then,

$$\bar{e}_x = \sum_{g \in G/G_\theta} g \bar{e}_\theta g^{-1}$$

is a decomposition of \bar{e}_x into orthogonal, conjugate idempotents. Hence,

$$Y \bar{e}_x \cong \text{Mat}_{n_\theta}(\bar{e}_\theta Y \bar{e}_\theta)$$

as K -algebras. Now the first assertion of (a) follows since the inclusion of $e_\theta KGe_\theta$ in KG induces an isomorphism $e_\theta KGe_\theta/I_\theta \cong \bar{e}_\theta Y\bar{e}_\theta$.

Since $e_\theta ge_\theta = 0$ for any $g \in G \setminus G_\theta$, and since e_θ is central in KG_θ ,

$$e_\theta KGe_\theta/I_\theta = e_\theta KG_\theta e_\theta/I_\theta = KG_\theta e_\theta/I_\theta,$$

proving the second assertion of (a).

Let V be a simple Y -module. There exists a unique $x \in X$ such that $\bar{e}_x V \neq 0$ (equivalently $e_x V = V$). By the statement and proof of (a), if $\theta \in x$, then

$$V = \bigoplus_{g \in G/G_\theta} g\bar{e}_\theta V, \tag{*}$$

$\bar{e}_\theta V$ is a simple $\bar{e}_\theta Y\bar{e}_\theta$ -module, and the map $V \mapsto (\theta, \bar{e}_\theta V)$ induces a bijection between the set of isomorphism classes of simple Y -modules and the set of pairs (θ, U) , where θ runs over representatives of G -orbits on $\text{Irr}_K(T)$ and U runs over a set of isomorphism classes of simple $\bar{e}_\theta Y\bar{e}_\theta$ -modules. Finally, identifying $\bar{e}_\theta Y\bar{e}_\theta$ -modules with $KG_\theta e_\theta/I_\theta$ -modules via the isomorphism $KG_\theta e_\theta/I_\theta \cong \bar{e}_\theta Y\bar{e}_\theta$ given in the proof of (a), the equation (*) gives that $V = \text{Ind}_{G_\theta}^G(e_\theta V)$. This proves (b). \square

2C. Symmetrising forms and divisibility. Let R be a commutative ring with 1 and let Y be a symmetric R -algebra which is free and finitely generated as R -module. If X is an R -basis of Y , then any symmetrising form $t : Y \rightarrow R$ determines a dual basis $X^\vee = \{x^\vee \mid x \in X\}$ satisfying

$$t(xy^\vee) = \begin{cases} 1 & \text{for } x = y \in X, \\ 0 & \text{for } x, y \in X, x \neq y. \end{cases}$$

The *relative projective element of Y in $Z(Y)$ with respect to t* is defined by $z_t := \sum_{x \in X} xx^\vee$. It depends on t but not on the choice of the basis X ; see [Linckelmann 2018, Sections 2.11 and 2.16] for details.

Now suppose that t is a symmetrising form on Y and let $s : Y \rightarrow R$ be a symmetric form (also known as trace form). Then there exists $u \in Z(Y)$ such that $s = t_u$, where $t_u \in Y^* := \text{Hom}_R(Y, R)$ is defined by $t_u(x) := t(ux)$ for $x \in Y$. The map $u \mapsto t_u$ is an R -module isomorphism between $Z(Y)$ and the R -module of symmetric forms on Y . Moreover, t_u is a symmetrising form if and only if $u \in Z(Y)^\times$. If X is an R -basis of Y and X^\vee is the dual basis with respect to t and if $u \in Z(Y)^\times$, then the dual basis of X with respect to t_u is equal to $X^\vee u^{-1}$, and hence the relative projective element in $Z(Y)$ with respect to t_u is equal to $z_t u^{-1}$.

If Y is a split semisimple algebra over a field K then for any symmetric form $s : Y \rightarrow K$, there exist elements $s_\chi \in K$, $\chi \in \text{Irr}_K(Y)$, such that $s = \sum_{\chi \in \text{Irr}_K(Y)} s_\chi \chi$. Moreover, we claim that s is a symmetrising form if and only if all s_χ are nonzero. For this, note that s is a symmetrising form for Y if and only if its restriction to any block of Y is a symmetrising form for the block. Thus we may assume that Y is split simple, that is, a matrix algebra over K and here the claim is immediate from the fact that the trace map on a matrix algebra is a symmetrising form; see for instance [Linckelmann 2018, Theorem 2.11.3].

Lemma 2.4. *Suppose that K is a field and Y is a split semisimple K -algebra. Let $s : Y \rightarrow K$ be a symmetrising form and let $s_\chi, \chi \in \text{Irr}_K(Y)$, be elements of K such that $s = \sum_\chi s_\chi \chi$. Let $z = z_s \in Z(Y)$:*

- (a) *If V is a Y -module affording the irreducible character χ , then the trace of z^{-1} on V equals s_χ .*
- (b) *The trace of z^{-2} in the left regular representation of Y equals $\sum_{\chi \in \text{Irr}_K(Y)} s_\chi^2$.*

Proof. A straightforward calculation using the standard bases of matrix algebras shows that

$$z = \sum_{\chi \in \text{Irr}_K(Y)} s_\chi^{-1} \chi(1) e_\chi$$

where $e_\chi \in Z(Y)$ is the central idempotent corresponding to χ . In particular, z is invertible in Y with $z^{-1} = \sum_\chi s_\chi \chi(1)^{-1} e_\chi$. The trace formula is an immediate consequence of this.

For (b) we note that the K -linear map

$$s \otimes s : Y \otimes_K Y^{\text{op}} \rightarrow K, \quad (s \otimes s)(y \otimes y') := s(y)s(y'),$$

is a symmetrising form on $Y \otimes_K Y^{\text{op}}$ with corresponding relative projective element $z \otimes z$. Further, $Y \cong \bigoplus_{\chi \in \text{Irr}_K(Y)} V_\chi \otimes V_\chi^*$ as $(Y \otimes_K Y^{\text{op}})$ -modules, where V_χ is an irreducible Y -module with character χ and V_χ^* is an irreducible Y^{op} -module with character χ . So, by part (a) applied with $Y \otimes_K Y^{\text{op}}$ in place of Y , $s \otimes s$ in place of s and $V_\chi \otimes V_\chi^*$ in place of V , $\sum_\chi s_\chi^2$ equals the trace of $z^{-1} \otimes z^{-1}$ on Y . Since z is central in Y , this trace is just the trace of left multiplication by z^{-2} on Y . \square

Lemma 2.5. *Let G be a finite group and K a field such that KG is split semisimple. Let t be the canonical symmetrising form on KG . Let $u \in Z(KG)^\times$, let $\alpha \in K$ be the coefficient of 1 when u^2 is written as a K -linear combination of elements of G and suppose that $t_u = \sum_\chi s_\chi \chi, s_\chi \in K$. Then*

$$\sum_{\chi \in \text{Irr}_K(Y)} s_\chi^2 = \frac{\alpha}{|G|}.$$

Proof. By a straightforward calculation using the set of group elements as basis, the relative projective element of KG with respect to t is $|G|1_{KG}$. Hence the relative projective element of KG with respect to t_u is $|G|u^{-1}$. Now the result follows from Lemma 2.4 since for any $y \in KG$, the trace of the action of y on KG via the left regular representation equals $|G|\beta$, where β is the coefficient of 1 in the standard basis presentation of y . \square

Lemma 2.6. *Let \mathcal{O} be a complete discrete valuation ring with field of fractions K of characteristic zero and residue field $\mathcal{O}/J(\mathcal{O})$ of characteristic ℓ . Let $G = T \rtimes W$ be the semidirect product of a finite abelian ℓ -group T with an ℓ' -group W acting faithfully on T . Let t be the canonical symmetrising form on KG and s a symmetrising form on KG with $s = t_u, u \in Z(KG)^\times$. Let α be the coefficient of 1 when u^2 is expressed as a K -linear combination of elements of G .*

Suppose that the restriction of s to $\mathcal{O}G$ takes values in \mathcal{O} and for any $x \in T, s(x) = \delta_{x,1}$. Then $u \in Z(\mathcal{O}G), \alpha \in \mathcal{O}$ and $\alpha \equiv 1 \pmod{\ell}$.

Proof. The restriction $t' := t|_{\mathcal{O}G}$ is a symmetrising form $\mathcal{O}G \rightarrow \mathcal{O}$ and by hypothesis $s' := s|_{\mathcal{O}G} : \mathcal{O}G \rightarrow \mathcal{O}$ is a symmetric form. Thus there exists $u' \in Z(\mathcal{O}G)$ such that $s' = t'_u$. Extending scalars, by linearity we have that $s = t_u$. Since by hypothesis $s = t_u$, we conclude $u = u' \in Z(\mathcal{O}G)$. This proves the first and second assertions.

For a conjugacy class C of G , denote by \hat{C} the corresponding class sum. Let

$$u = 1 + \sum_C \alpha_C \hat{C}$$

where C runs over the nonidentity conjugacy classes of G . Then for $1 \neq x \in T$ we have $0 = s(x) = t(ux) = \alpha_D$ where D is the conjugacy class of G containing x^{-1} . It follows that

$$u = 1 + \sum_{C \in \mathcal{C}} \alpha_C \hat{C}$$

where \mathcal{C} is the set of conjugacy classes of $G \setminus T$ and

$$\alpha = 1 + \sum_{C \in \mathcal{C}} \alpha_C \alpha_{C^{-1}} |C|,$$

where C^{-1} denotes the class containing the inverses of the elements of C . Since W acts faithfully on T , ℓ divides $|C|$ for all $C \in \mathcal{C}$. Since $u \in Z(\mathcal{O}G)$, all α_C are elements of \mathcal{O} and we obtain the last assertion. \square

The following is a consequence of Tate duality for symmetric algebras over complete discrete valuation rings exhibited in [Eisele et al. 2018]. For an integral domain \mathcal{O} with field of fractions K and Y an \mathcal{O} -algebra which is finitely generated free as \mathcal{O} -module, we set $KY := K \otimes_{\mathcal{O}} Y$.

Proposition 2.7. *Suppose \mathcal{O} is a complete discrete valuation ring with field of fractions K of characteristic zero, Y is a symmetric \mathcal{O} -algebra such that KY is split semisimple. Let $s : KY \rightarrow K$ be a symmetrising form with $s = \sum_{\chi} s_{\chi} \chi$. Suppose that the restriction of s to Y takes values in \mathcal{O} .*

Let U be a projective Y -module and suppose that there is an isomorphism of KY -modules

$$K \otimes_{\mathcal{O}} U \cong \bigoplus_{\chi \in \text{Irr}(KY)} V_{\chi}^{d_{\chi}},$$

where V_{χ} is a simple KY -module with character χ and $d_{\chi} \in \mathbb{N}_0$. Then

$$\sum_{\chi \in \text{Irr}(KY)} s_{\chi} d_{\chi} \in \mathcal{O}.$$

Proof. Let $t : Y \rightarrow \mathcal{O}$ be a symmetrising form and let z be the relative projective element of Y with respect to t . By [Eisele et al. 2018, Proposition 2.2], for any $\gamma \in \text{End}_Y(U)$, the trace of $z^{-1}\gamma$ on $K \otimes_{\mathcal{O}} U$ lies in \mathcal{O} . Here by $z^{-1}\gamma \in \text{End}_{KY}(K \otimes_{\mathcal{O}} U)$ we denote the composition of (the extension to K of) γ with multiplication by z^{-1} .

Denote by $\tilde{t} : KY \rightarrow K$ the K -linear extension of t to KY . Then \tilde{t} is a symmetrising form for KY with relative projective element z . Hence $s = \tilde{t}_u$ for some $u \in Z(KY)$. Since the restriction of s to Y takes values in \mathcal{O} , we have as in the proof of Lemma 2.6 that $u \in Z(Y)$. Let $\gamma : U \rightarrow U$ be multiplication

by u . Since $u \in Z(Y)$, $\gamma \in \text{End}_Y(U)$. Thus the trace of $z^{-1}\gamma$ on $K \otimes_{\mathcal{O}} U$ is an element of \mathcal{O} . Further, zu^{-1} is the relative projective element of KY with respect to s and $z^{-1}\gamma$ is multiplication by $(zu^{-1})^{-1}$. Thus the result follows from Lemma 2.4. \square

The first statement of the next proposition is a theorem of Brauer. The second is also well known to experts; we provide a proof of it for the convenience of the reader.

Proposition 2.8. *Let G be a finite group, S a Sylow ℓ -subgroup of G and H a subgroup of G containing $N_G(S)$. Denote by $B_0(G)$ (respectively $B_0(H)$) the principal ℓ -block of G (respectively H). Then,*

$$(\dim B_0(G))_\ell = (\dim B_0(H))_\ell = |S| \quad \text{and} \quad (\dim B_0(G))_{\ell'} \equiv (\dim B_0(H))_{\ell'} \pmod{\ell}.$$

Proof. Let \mathcal{O} be a complete discrete valuation ring in characteristic zero with algebraically closed residue field of characteristic ℓ . Let $b \in \mathcal{O}G$ be the block idempotent corresponding to $B_0(G)$ and $c \in \mathcal{O}H$ the one corresponding to $B_0(H)$. The group S is a defect group of the principal block $B_0(G)$. Hence as $\mathcal{O}[G \times G]$ -module, $B_0(G)$ has vertex $\Delta S = \{(x, x) \mid x \in S\}$; see [Linckelmann 2018, Remark 6.7.14]. Further, the $\mathcal{O}[H \times H]$ -module $B_0(H)$ is the Green correspondent of $B_0(G)$ in $H \times H$ (see [loc. cit., Theorem 6.7.2], and note that by [loc. cit., Theorem 6.13.14], $B_0(G)$ and $B_0(H)$ are Brauer correspondents). Thus, by properties of the Green correspondence (see [loc. cit., Thm 5.2.1])

$$\text{Ind}_{H \times H}^{G \times G}(\mathcal{O}Hc) = \mathcal{O}Gb \oplus Y$$

where every indecomposable $\mathcal{O}[G \times G]$ -module summand of Y has vertex of order strictly smaller than $|\Delta S| = |S|$. Comparing \mathcal{O} -ranks,

$$\frac{|G|^2}{|H|^2} \text{rk}(\mathcal{O}Hc) = \text{rk}(\mathcal{O}Gb) + \text{rk}(Y).$$

By a standard application of Green's indecomposability theorem and the properties of vertices and sources (see [loc. cit., Section 5.1, Theorem 5.12.3]), the ℓ -part of the rank of any indecomposable $\mathcal{O}X$ -lattice, for X a finite group, is greater than or equal to $|X|_\ell / |Q|$ where Q is a vertex of the lattice. Thus, $(\text{rk}(Y))_\ell$ is strictly greater than $|S|$ and we obtain

$$\frac{|G|^2}{|H|^2} \text{rk}(\mathcal{O}Hc) \equiv \text{rk}(\mathcal{O}Gb) \pmod{\ell|S|}.$$

Now by a theorem of Brauer (see [loc. cit., Theorem 6.7.13]), the ℓ -part of $\dim(B_0(G)) = \text{rk}(\mathcal{O}Gb)$ equals $|S|$ and similarly for $B_0(H)$. The result follows since $|G : H| \equiv 1 \pmod{\ell}$ by Sylow's theorem. \square

2D. Tits deformation theorem. We recall some features of Tits' deformation theorem. Let R and R' be integral domains with field of fractions K and K' respectively and let $\psi : R \rightarrow R'$ be a ring homomorphism. Let Y be an R -algebra which is finitely generated and free as R -module and let Y' denote the R' -algebra $R' \otimes Y$ obtained via extension of scalars through ψ . Let $t : Y \rightarrow R$ be an R -linear map and let $t' : Y' \rightarrow R'$ be its R' -linear extension through ψ .

Theorem 2.9. *Suppose that KY and $K'Y'$ are both split semisimple:*

(a) *The map ψ induces a bijection $\text{Irr}(KY) \rightarrow \text{Irr}(K'Y')$, $\chi \mapsto \chi'$, such that*

$$\chi'(1 \otimes y) = \psi^*(\chi(y)) \quad \text{for all } y \in Y.$$

Here $\psi^ : R^* \rightarrow K^*$ is an extension of ψ to the integral closure R^* of R in K and K^* is some extension field of K' . The bijection preserves dimensions of underlying simple modules.*

(b) *If t is the restriction to Y of a linear combination $\sum_{\chi \in \text{Irr}(KY)} s_\chi \chi$ with $s_\chi \in R_{\mathfrak{p}}$, then the R' -linear map $t' : Y' \rightarrow R'$ is the restriction to Y' of $\sum_{\chi \in \text{Irr}(KY)} \psi(s_\chi) \chi'$. Here \mathfrak{p} is the kernel of ψ , $R_{\mathfrak{p}}$ is the corresponding localisation and $\psi(s_\chi)$ is the image of s_χ under the unique extension of ψ to a ring homomorphism $R_{\mathfrak{p}} \rightarrow K'$.*

Proof. For part (a) see [Curtis and Reiner 1981, Theorem 68.17, Corollary 68.20]. Note that the bijection given in [loc. cit.] is between the sets $\text{Irr}(\bar{K}Y)$ and $\text{Irr}(\bar{K}'Y')$ where \bar{K} and \bar{K}' are algebraic closures of K and K' respectively. Since KY and $K'Y'$ are split, this descends via restriction on both sides to a bijection $\text{Irr}(KY) \rightarrow \text{Irr}(K'Y')$. Now (b) is an immediate consequence of (a). □

3. Hecke algebras and their Schur elements

Let W be a finite complex reflection group, that is, a finite subgroup of $\text{GL}_n(\mathbb{C})$ for some $n \geq 1$ generated by complex reflections. We denote by \mathbb{Q}_W the field generated by the traces of elements of W , a finite extension of \mathbb{Q} . Attached to any reflection $r \in W$ is its reflecting hyperplane $H = \ker(1 - r)$ in \mathbb{C}^n ; its point-wise stabiliser W_H in W is cyclic, generated by reflections. We say that $r \in W_H$ is the *distinguished reflection* associated to H if r generates W_H and has nontrivial eigenvalue $\exp(2\pi i / o(r))$ of smallest possible argument.

3A. From braid groups to trace forms. Let $B(W)$ be the topological braid group of W (see Broué, Malle and Rouquier [Broué et al. 1998]), that is, the fundamental group of the space of regular orbits of W on \mathbb{C}^n . So there is an associated exact sequence

$$1 \rightarrow P(W) \rightarrow B(W) \rightarrow W \rightarrow 1,$$

with kernel the pure braid group $P(W)$. Let $A := \mathbb{Z}_W[\mathbf{u}^{\pm 1}]$, where \mathbb{Z}_W denotes the ring of integers of \mathbb{Q}_W and where $\mathbf{u} = (u_{rj})$ are algebraically independent elements indexed by conjugacy classes of distinguished reflections $r \in W$ and $1 \leq j \leq o(r)$. By [Broué et al. 1998, Definition 4.21] the (*generic*) Hecke algebra $\mathcal{H}(W, \mathbf{u})$ of W is defined to be the quotient of the group algebra $A[B(W)]$ of $B(W)$ over A by the ideal generated by the elements (called *deformed order relations*)

$$\prod_{j=1}^{o(r)} (\mathbf{r} - u_{rj}) \tag{H}$$

for r running over the braid reflections of $B(W)$ (introduced as *generators of the monodromy around a hyperplane* in [loc. cit., 2B]), with r denoting the image of r in W , a distinguished reflection. We will write $A[B(W)] \rightarrow \mathcal{H}(W, \mathbf{u})$, $\mathbf{x} \mapsto h_{\mathbf{x}}$, for the associated quotient map.

We have the following result, first conjectured in [Broué and Malle 1993], with the final cases having been established by Chavli [2018], Marin [2019] and Tsuchioka [2020].

Theorem 3.1 (freeness conjecture). *The algebra $\mathcal{H}(W, \mathbf{u})$ is A -free of rank $|W|$.*

By results of the second author [Malle 1999, Corollary 4.8] there is a positive integer z such that the field of fractions K_W of $\tilde{A} := \mathbb{Z}_W[\tilde{\mathbf{u}}^{\pm 1}] \supseteq A$ is a splitting field of $\mathcal{H}(W, \mathbf{u})$, where $\tilde{\mathbf{u}} = (\tilde{u}_{rj})$ are such that $\tilde{u}_{rj}^z = \exp(-2\pi i j/o(r))u_{rj}$ for all r, j .

Furthermore, by [Malle 2000, Proposition 7.1] to each irreducible character χ of $K_W \otimes_A \mathcal{H}(W, \mathbf{u})$ is associated an element $f_\chi \in \tilde{A}$ called the *Schur element* of χ . The Schur element $p_W := p_W(\mathbf{u}) := f_{1_W}$ of the trivial character 1_W is called the *Poincaré polynomial* of $\mathcal{H}(W, \mathbf{u})$ (a Laurent polynomial in the \tilde{u}_{rj}). For simply laced Coxeter groups, this is in fact the homogenisation of the usual Poincaré polynomial of W .

The collection $\{(\chi, f_\chi) \mid \chi \in \text{Irr}(\mathcal{H}(W, \mathbf{u}))\}$ is Galois-invariant, so in particular

$$t_{W, \mathbf{u}}(h) := \sum_{\chi \in \text{Irr}(\mathcal{H}(W, \mathbf{u}))} \frac{1}{f_\chi} \chi(h)$$

lies in $\text{Frac}(A)$ for all $h \in \mathcal{H}(W, \mathbf{u})$. Thus, this defines a symmetric A -linear map

$$t_{W, \mathbf{u}} : \mathcal{H}(W, \mathbf{u}) \rightarrow \text{Frac}(A), \quad h \mapsto t_{W, \mathbf{u}}(h),$$

called the *canonical trace form on $\mathcal{H}(W, \mathbf{u})$* . We denote also by $t_{W, \mathbf{u}}$ its $\text{Frac}(A)$ -linear extension to $\mathcal{H}_{\text{Frac}(A)}(W, \mathbf{u}) := \text{Frac}(A) \otimes_A \mathcal{H}(W, \mathbf{u})$. This form satisfies the following property:

Proposition 3.2. *There exists a set $\mathcal{B} \subset \mathcal{H}(W, \mathbf{u})$ consisting of monomials in images of braid reflections with $1 \in \mathcal{B}$, such that $t_{W, \mathbf{u}}(b) = \delta_{1, b}$ for $b \in \mathcal{B}$, and the images in W of the $b \in \mathcal{B}$ under the canonical map form a system of representatives of the conjugacy classes of W .*

Proof. First note that the claim easily reduces to the case of irreducible reflection groups. For those, it holds by the construction of the Schur elements f_χ ; see [Malle 1997; 2000] for the exceptional types, and [Geck et al. 2000, Theorem 1.3, Lemma 4.3 and Section 4.5] for the infinite series. \square

Furthermore, $t_{W, \mathbf{u}}$ satisfies a duality with respect to a certain central element, but this will not be of importance here. In analogy with the case of finite Coxeter groups; the theory of spetses predicts the following, see [Broué et al. 1999, Theorem-Assumption 2.1].

Conjecture 3.3. *The form $t_{W, \mathbf{u}}$ takes values in A and is a symmetrising form on $\mathcal{H}(W, \mathbf{u})$.*

The above conjecture has been established for all imprimitive complex reflection groups $G(e, 1, m)$, for example, by Malle and Mathas [1998, Theorem].

Let $W_0 \leq W$ be a reflection subgroup. We denote by $\mathcal{H}(W_0, \mathbf{u}_0)$ the Hecke algebra of W_0 whose parameters \mathbf{u}_0 consist of those parameters for W whose corresponding reflections are, up to conjugacy, contained in W_0 . Since nonconjugate reflections in W_0 might be conjugate in W , $\mathcal{H}(W_0, \mathbf{u}_0)$ is a

specialisation of the generic Hecke algebra of W_0 corresponding to an identification of certain of its parameters. It follows from the freeness conjecture (Theorem 3.1) that $\mathcal{H}(W_0, \mathbf{u}_0)$ is naturally a subalgebra of $\mathcal{H}(W, \mathbf{u})$. Moreover, by the explicit results in [Malle 1999, Theorem 5.2] the field K_W is also a splitting field for $\mathcal{H}(W_0, \mathbf{u}_0)$. By t_{W_0, \mathbf{u}_0} we will mean the corresponding specialisation of the canonical form of the generic Hecke algebra of W_0 . Recall that, by a theorem of Steinberg, all parabolic subgroups of W , that is, stabilisers in $W \leq \mathrm{GL}_n(\mathbb{C})$ of subspaces of \mathbb{C}^n , are reflection subgroups of W .

Definition 3.4. We will say that $\mathcal{H}(W, \mathbf{u})$ is *strongly symmetric* if the following hold:

- (1) $t_{W, \mathbf{u}}$ is a symmetrising form on $\mathcal{H}(W, \mathbf{u})$ and there is a section $W \rightarrow \mathbf{W} \subset B(W)$ of the natural map $B(W) \rightarrow W$ containing 1 whose image in $\mathcal{H}(W, \mathbf{u})$ is an A -basis of $\mathcal{H}(W, \mathbf{u})$ with $t_{W, \mathbf{u}}(h_w) = \delta_{w, 1}$ for all $w \in W$.
- (2) For any parabolic subgroup $W_0 \leq W$, t_{W_0, \mathbf{u}_0} is a symmetrising form on $\mathcal{H}(W_0, \mathbf{u}_0)$ and

$$t_{W, \mathbf{u}}|_{\mathcal{H}(W_0, \mathbf{u}_0)} = t_{W_0, \mathbf{u}_0}.$$

Note that the assertion that (2) holds is referred to as the parabolic trace conjecture in [Chavli and Chlouveraki 2022]. Strong symmetry is known to be satisfied in many cases; here we use the Shephard–Todd notation for irreducible complex reflection groups.

Proposition 3.5. *For the following irreducible groups, $\mathcal{H}(W, \mathbf{u})$ is strongly symmetric:*

- (a) For W a Coxeter group.
- (b) For $W = G(e, p, n)$ with $n \neq 2$ or p odd.
- (c) For $W = G_i$, $i \in \{4, 5, 6, 7, 8\}$.

Proof. First note that property (2) of being strongly symmetric follows for a parabolic subgroup W_0 of W if there exists $\mathbf{W} \subset B(W)$ as in (1) such that

$$\{h_w \mid w \in W_0\} \text{ is an } A\text{-basis of } \mathcal{H}(W_0, \mathbf{u}_0) \quad \text{and} \quad t_{W_0, \mathbf{u}_0}(h_w) = \delta_{w, 1} \text{ for all } w \in W_0. \quad (2')$$

For Coxeter groups, (1) and (2') hold for any section \mathbf{W} consisting of reduced expressions in the standard generators; see [Geck and Pfeiffer 2000, Proposition 8.1.1]. For $W = G(e, p, n)$ the existence of \mathbf{W} satisfying (1) is shown in [Malle and Mathas 1998, Theorem 5.1]. Since any parabolic subgroup of W is a Young subgroup, that is, a product of symmetric groups with a group $G(e, p, n')$ for $n' \leq n$, the Ariki–Koike basis of $\mathcal{H}(W, \mathbf{u})$ considered in [Malle and Mathas 1998] also satisfies (2'); see also [Broué et al. 1999, page 177]. The claim for G_i , $i \in \{4, 5, 6, 7, 8\}$, follows from the explicit results in [Boura et al. 2020]. \square

3B. Specialisations. By a *specialisation* we will mean a ring homomorphism $\psi : A' \rightarrow R$ where A' and R are commutative rings with $A' \supseteq A$. We then set $\mathcal{H}_\psi(W, \mathbf{u}) := R \otimes (A' \otimes_A \mathcal{H}(W, \mathbf{u}))$. If ψ is inclusion we will sometimes write $\mathcal{H}_R(W, \mathbf{u})$ instead of $\mathcal{H}_\psi(W, \mathbf{u})$. The restriction of any specialisation ψ to a subring of A' will again be denoted by ψ as will the composition of ψ with any inclusion $R \hookrightarrow R'$.

We will consider certain types of specialisations. For the remainder of this section, let R be an integral domain containing \mathbb{Z}_W and let K be its field of fractions. Let $\psi_1 : R[\tilde{\mathbf{u}}] \rightarrow R$ be the R -linear homomorphism defined by $\psi_1(\tilde{u}_{rj}) := 1$ for all r and j . So, ψ_1 restricts to the specialisation

$$A \rightarrow \mathbb{Z}_W, \quad u_{rj} \mapsto \exp(2\pi i j/o(r)).$$

By [Bessis 2001, Theorem 0.1], the Hecke algebra maps to the group algebra RW of W under ψ_1 . Combining this with the freeness conjecture, the Tits deformation theorem gives that $\mathcal{H}_{\tilde{K}}(W, \mathbf{u}) := \tilde{K} \otimes_A \mathcal{H}(W, \mathbf{u})$ is isomorphic to the group algebra $\tilde{K}W$, where $\tilde{K} = \text{Frac}(R[\tilde{\mathbf{u}}])$; see Theorem 2.9 and note that $K_W \subseteq \tilde{K}$. Thus, we may and will identify the irreducible characters of $\mathcal{H}_{\tilde{K}}(W, \mathbf{u})$ with $\text{Irr}(W)$ via the bijection $\chi_\phi \leftrightarrow \phi$ induced by ψ_1 . This also induces a labelling of Schur elements of $\mathcal{H}(W, \mathbf{u})$ by $\text{Irr}(W)$ and we will henceforth denote them as f_ϕ , $\phi \in \text{Irr}(W)$. Since K_W is also a splitting field for the Hecke algebra $\mathcal{H}(W_0, \mathbf{u}_0)$ of any reflection subgroup W_0 of W we also have $\mathcal{H}_{\tilde{K}}(W_0, \mathbf{u}) \cong \tilde{K}W_0$. We will similarly identify the irreducible characters of $\mathcal{H}(W_0, \mathbf{u}_0)$ over \tilde{K} with $\text{Irr}(W_0)$.

Now let q be a prime power and suppose that R contains $q^{\pm 1/z}$. We also consider R -linear specialisations of the form

$$\psi_q : R[\tilde{\mathbf{u}}^{\pm 1}] \rightarrow R, \quad \tilde{u}_{rj} \mapsto q^{a_{rj}/z},$$

for integers a_{rj} . Any such ψ_q restricts to a specialisation

$$A \rightarrow \mathbb{Z}_W, \quad u_{rj} \mapsto \zeta_{o(r)}^j q^{a_{rj}},$$

with $\zeta_{o(r)} \in \mathbb{Z}_W$ an $o(r)$ -th primitive root of unity.

Lemma 3.6. *For all $\phi \in \text{Irr}(W)$ we have $\psi_1(f_\phi) = \phi(1)/|W|$ and $\psi_q(f_\phi) \neq 0$.*

Proof. The assertion on ψ_1 follows since by construction the set \mathcal{B} from Proposition 3.2 specialises under ψ_1 to a system of representatives of the conjugacy classes of W . Next, the following can be observed from the explicit form of the Schur elements (and was first stated explicitly in [Chlouveraki 2009, Theorem 4.2.5]): any f_ϕ is a product of a scalar, a monomial in the \tilde{u}_{rj} and a product of cyclotomic polynomials Ψ_i over K_W evaluated at monomials M_i in the $\tilde{u}_{rj}^{\pm 1}$ of total degree 0. Thus we need to see that $\psi_q(\Psi_i(M_i)) \neq 0$. This is clear if $\psi_q(M_i)$ is not a root of unity. Now $\psi_q(M_i)$ can only be a root of unity, if the powers of q cancel completely in $\psi_q(M_i)$, which means that $\psi_q(M_i) = \psi_1(M_i)$ and so $\psi_q(\Psi_i(M_i)) = \psi_1(\Psi_i(M_i))$. But the latter is a factor of $\psi_1(f_\phi) = \phi(1)/|W|$ and hence nonzero. \square

For the next result we note that symmetrising forms remain symmetrising after specialisation, that is if $\theta : \mathcal{O} \rightarrow \mathcal{O}'$ is a ring homomorphism, Y is an \mathcal{O} -algebra which is finitely generated and free as \mathcal{O} -module and $\tau : Y \rightarrow \mathcal{O}$ is a symmetrising form, then the induced \mathcal{O}' -linear form τ' on $Y' := \mathcal{O}' \otimes_{\mathcal{O}} Y$ satisfying $\tau'(1 \otimes y) = \tau(y)$ for $y \in Y$ is a symmetrising form on Y' .

Lemma 3.7. *Assume that $\mathcal{H}(W, \mathbf{u})$ is symmetric over A with respect to the form $t_{W, \mathbf{u}}$ with Schur elements $f_\phi \in \tilde{A}$, $\phi \in \text{Irr}(\mathcal{H}(W, \mathbf{u}))$, and let $K = \text{Frac}(R)$. The algebra $K\mathcal{H}_{\psi_q}(W, \mathbf{u})$ is split semisimple. Let t' be the induced form on $\mathcal{H}_{\psi_q}(W, \mathbf{u})$. For each $\phi \in \text{Irr}(W)$, $\psi_q(f_\phi)$ is the corresponding Schur element of t' .*

Proof. By Lemma 3.6 we have $\psi_q(f_\phi) \neq 0$ for all $\phi \in \text{Irr}(W)$. Now ψ_q is a concatenation of specialisation maps whose kernel is a prime ideal of height 1. So by [Chlouveraki 2009, Theorem 2.4.12], $K\mathcal{H}_{\psi_q}(W, \mathbf{u})$ is also split semisimple. The result thus follows by Tits' deformation theorem (Theorem 2.9). \square

Finally, for an indeterminate x we will also consider the *spetsial specialisation*

$$\psi_s : R[\tilde{\mathbf{u}}^{\pm 1}] \rightarrow R[x^{\pm 1/z}], \quad \tilde{u}_{rj} \mapsto \begin{cases} x^{1/z} & \text{if } j = o(r), \\ 1 & \text{if } 1 \leq j < o(r) \end{cases}$$

(so $\psi_s(u_{r,o(r)}) = x$, $\psi_s(u_{rj}) = \exp(2\pi i j/o(r))$ for $j < o(r)$). Clearly ψ_1 factorises through ψ_s by composition with $x^{1/z} \mapsto 1$ as does any specialisation ψ_q for the case $a_{rj} = 1$ if $j = o(r)$ and $a_{rj} = 0$ if $j < o(r)$ by composition with $x^{1/z} \mapsto q^{1/z}$. We write $\psi_{s,q}$ for this latter specialisation, which will become important in Section 5F. The spetsial specialisation links Schur elements of Hecke algebras to unipotent character degrees of spetses; see Section 4D.

4. Conjectures for the principal block of a \mathbb{Z}_ℓ -spets

In this section we define the dimension of the principal block of a \mathbb{Z}_ℓ -spets, introduced in [Kessar et al. 2020, Section 6.2], and propose some conjectures around this notion.

4A. The principal block of a \mathbb{Z}_ℓ -spets. Let ℓ be a prime and let q be a prime power not divisible by ℓ . Recall that (under some conditions) the set of characters of the principal ℓ -block of a finite reductive group G over \mathbb{F}_q can be described as a union of sets of characters in bijection with the principal e -Harish-Chandra series of unipotent characters of dual-centraliser subgroups $C_{G^*}(s)^*$ where G^* is the ‘‘Langlands dual’’ of G and s runs over conjugacy classes of ℓ -elements of G^* . The principal block of a \mathbb{Z}_ℓ -spets as constructed in [Kessar et al. 2020] is modelled on this description: unipotent characters and the appropriate Harish-Chandra series are provided by the theory of spetses whereas the indexing set of ℓ -elements and corresponding centralisers comes from the theory of ℓ -compact groups and fusion systems. In the next paragraph, we briefly recall this construction. Before doing so, we point out that the description of the principal block of a \mathbb{Z}_ℓ -spets does not involve going over to the dual as one would expect from analogy with the group case. The reason for this is that the fusion system construction that we rely on is for the moment only available for simply connected ℓ -compact groups. However, this departure does not lead to an inconsistency in the group case under the conditions on ℓ with which we are concerned; see [Kessar et al. 2020, Proposition 6.8].

We assume from now till the end of the section that $\ell > 2$. Let $W \leq \text{GL}(L)$ be a finite *spetsial* (see [Malle 1998, Section 3]) ℓ -adic reflection group on a \mathbb{Z}_ℓ -lattice L , and let X be the associated connected ℓ -compact group; see [Broto and Møller 2007, Theorem 1.1]. We assume moreover that X is simply connected and that ℓ is *very good* for (W, L) , in the sense of [Kessar et al. 2020, Definition 2.4]. Let $\varphi \in N_{\text{GL}(L)}(W)$ be of ℓ' -order and $\mathbb{G} = (W\varphi^{-1}, L)$ be the associated simply connected \mathbb{Z}_ℓ -spets. For example any Weyl group W for which ℓ is very good (in the classical sense) determines a \mathbb{Z}_ℓ -spets satisfying the above conditions.

Set $\mathbb{G}(q) := (W\varphi^{-1}, L, q)$. Broto and Møller [2007] showed how to attach to these data a fusion system \mathcal{F} on a finite ℓ -group S , via the associated ℓ -compact group X ; see [Kessar et al. 2020, Theorem 3.2]. Here, S is an extension of a homocyclic ℓ -group T (the *toral part*) by a Sylow ℓ -subgroup of the associated relative Weyl group $W_{\varphi^{-1}\zeta^{-1}}$; see [Kessar et al. 2020, Theorem 3.6]. Note that S and \mathcal{F} only depend on the ℓ -part ℓ^a of $q - \zeta$, where $\zeta \in \mathbb{Z}_\ell^\times$ is the root of unity with $q \equiv \zeta \pmod{\ell}$, not on q itself.

If $\mathbb{G}(q)$ arises from a connected reductive algebraic group \mathbf{G} over $\overline{\mathbb{F}}_q$ with Weyl group W and a Frobenius morphism $F : \mathbf{G} \rightarrow \mathbf{G}$ with respect to an \mathbb{F}_q -structure acting as φ on W , then S is a Sylow ℓ -subgroup of \mathbf{G}^F and \mathcal{F} is the ℓ -fusion system of \mathbf{G}^F on S ; see [Kessar et al. 2020, Remark 3.3 and Section 5.3]. In particular, $T = (\mathbf{T}^F)_\ell$ where \mathbf{T} is a maximal e -split torus of \mathbf{G} .

Under our assumptions, for any $s \in S$ the centraliser $W(s) := C_W(s)$ of s is again an ℓ -adic reflection group, a reflection subgroup of W (see the proof of Theorem 5.2 or Proposition 2.3 of [Kessar et al. 2020]), and by [loc. cit., Proposition 6.2], it is again spetsial. We let $C_{\mathbb{G}}(s) := (W(s)\varphi_s^{-1}, L)$ be the associated \mathbb{Z}_ℓ -spets, where $\varphi_s \in N_{W\varphi}(W(s))$ is defined as in [loc. cit., Section 5.2].

Now recall from [Malle 1995] (for the infinite series of irreducible complex reflection groups) and [Broué et al. 2014] (for the primitive ones) that associated to \mathbb{G} as well as to the various $C_{\mathbb{G}}(s)$ there are sets of unipotent characters $\text{Uch}(\mathbb{G})$ and $\text{Uch}(C_{\mathbb{G}}(s))$, respectively. If W is a Weyl group, these are just the unipotent characters of an associated finite reductive group. For $s \in S$ we let

$$\mathcal{E}(\mathbb{G}, s) = \{\gamma_{s,\lambda} \mid \lambda \in \text{Uch}(C_{\mathbb{G}}(s))\}$$

denote a set in bijection with $\text{Uch}(C_{\mathbb{G}}(s))$ and call it the *characters of \mathbb{G} in the series s* . The sets $\text{Uch}(C_{\mathbb{G}}(s))$ are in canonical bijection for conjugate elements s . Moreover, these sets only depend on ℓ^a , not on q itself. Any unipotent character λ comes with a degree (polynomial) $\lambda(1) \in \mathbb{Z}_\ell[x]$. The *degree of $\gamma_{s,\lambda} \in \mathcal{E}(\mathbb{G}, s)$* is defined as

$$\gamma_{s,\lambda}(1) := |\mathbb{G} : C_{\mathbb{G}}(s)|_{x'} \lambda(1) \in \mathbb{Z}_\ell[x].$$

Here, $|\mathbb{G} : C_{\mathbb{G}}(s)|_{x'}$ means the prime-to- x part of the polynomial $|\mathbb{G}|/|C_{\mathbb{G}}(s)| \in \mathbb{Z}_\ell[x]$, where $|\mathbb{G}|, |C_{\mathbb{G}}(s)|$ are the respective order polynomials; note that the latter divides the former by [Kessar et al. 2020, Lemma 6.6].

Now by [Malle 1995, Folgerung 3.16 and 6.11] and [Broué et al. 2014, 4.31] for any \mathbb{Z}_ℓ -spets \mathbb{H} , for any root of unity η the set of unipotent characters $\text{Uch}(\mathbb{H})$ is naturally partitioned into so-called η -Harish-Chandra series, and one among them, the *principal η -Harish-Chandra series $\mathcal{E}(\mathbb{H}, 1, \eta)$* of $\text{Uch}(\mathbb{H})$ containing $1_{\mathbb{G}}$, is in bijection with the irreducible characters of the corresponding Springer–Lehrer relative Weyl group. In particular, $\mathcal{E}(\mathbb{H}, 1, 1)$ is in bijection with $\text{Irr}(W^\varphi)$.

With this, for ζ as above denote by $\mathcal{E}(\mathbb{G}, s)_\zeta$ the subset of $\mathcal{E}(\mathbb{G}, s)$ in bijection with the principal ζ -Harish-Chandra series of $\text{Uch}(C_{\mathbb{G}}(s))$, and hence also in bijection with the irreducible characters of the relative Weyl group $W(s)_{\varphi_s^{-1}\zeta^{-1}}$.

The following definition from [Kessar et al. 2020, Section 6.2] is inspired by the results of Cabanes–Enguehard on unipotent ℓ -blocks of finite reductive groups; indeed, if \mathbb{G} is a rational spets for which ℓ is

very good, then what we define are exactly the characters in the principal ℓ -block of the corresponding finite group of Lie type $\mathbb{G}(q)$; see [loc. cit., Proposition 6.8].

Definition 4.1. Let $\mathbb{G} = (W\varphi^{-1}, L)$ be a simply connected \mathbb{Z}_ℓ -spets with φ of ℓ' -order such that ℓ is very good for \mathbb{G} (in the sense of [Kessar et al. 2020, Definition 2.4]) and q a prime power with $q \equiv \zeta \pmod{\ell}$. The characters in the principal block B_0 of $\mathbb{G}(q)$ are

$$\text{Irr}(B_0) := \coprod_{s \in S/\mathcal{F}} \mathcal{E}(\mathbb{G}, s)_\zeta,$$

where the union runs over a set S/\mathcal{F} of representatives s of \mathcal{F} -conjugacy classes in S . The dimension of B_0 is defined as

$$\dim(B_0) = \sum_{\gamma \in \text{Irr}(B_0)} \gamma(1)^2 = \sum_{s \in S/\mathcal{F}} \sum_{\lambda \in \mathcal{E}(C_{\mathbb{G}}(s), 1, \zeta)} \gamma_{s, \lambda}(1)^2 \in \mathbb{Z}_\ell[x].$$

Again, these do not depend on q but only on $\ell^a = (q - \zeta)_\ell$.

The dimension of the principal ℓ -block B_0 of a finite group G with Sylow ℓ -subgroup S satisfies $(\dim B_0)_\ell = |S|$ (see Proposition 2.8). We conjecture that our dimension of the principal block $\dim(B_0)$ of $\mathbb{G}(q)$ behaves similarly.

Conjecture 4.2. Let $\mathbb{G} = (W\varphi^{-1}, L)$ be a simply connected \mathbb{Z}_ℓ -spets such that ℓ is very good for \mathbb{G} . Let q be a prime power not divisible by ℓ and S the associated ℓ -group. Then

$$(\dim(B_0)|_{x=q})_\ell = |S|.$$

By further analogy with the group case (see Proposition 2.8) we also conjecture the following global-local statement:

Conjecture 4.3. In the setting of Conjecture 4.2, if $\zeta \in \mathbb{Z}_\ell^\times$ with $q \equiv \zeta \pmod{\ell}$ we have

$$(\dim(B_0)|_{x=q})_{\ell'} \equiv |W_{\varphi^{-1}\zeta^{-1}}|_{\ell'} \pmod{\ell}.$$

Note that Conjectures 4.2 and 4.3 combine to form Conjecture 1.

Example 4.4. We describe S , \mathcal{F} , and $\text{Irr}(B_0)$ in a special case relevant to Theorem 1. Suppose that $q \equiv 1 \pmod{\ell}$ and $\varphi = 1$. Then T may be identified with $L/\ell^a L$ where $\ell^a \parallel (q - 1)$, $W = W_{\varphi^{-1}\zeta^{-1}}$ and the action of W on T in S is the one inherited from the action of W on L . Assume in addition that W is an ℓ' -group. Then the condition that ℓ is very good for (W, L) always holds; see [Kessar et al. 2020, Proposition 2.6]. Further, $S = T$ and \mathcal{F} is the ℓ -fusion system $\mathcal{F}_{SW}(S)$ of the group SW on S ; see [Kessar et al. 2020, Theorem 3.4] and [Broto and Møller 2007, Theorem 9.8]. Moreover, for any $s \in S = T$ the subgroup $W(s)_{\varphi_s^{-1}\zeta^{-1}}$ equals $W(s)$ and hence $\mathcal{E}(\mathbb{G}, s)_1$ is in bijection with $\text{Irr}(W(s))$. So $\text{Irr}(B_0)$ is in bijection with W -classes of pairs (s, ϕ) where $s \in S$ and $\phi \in \text{Irr}(W(s))$.

4B. Decomposition numbers. Suppose in this section that $|W|$ is prime to ℓ , that $\ell \mid (q - 1)$ and that $\varphi = 1$. Recall the description of the principal block B_0 under these assumptions given in Example 4.4.

Since W is an ℓ' -group and S an ℓ -group, we may identify $\text{IBr}(SW)$ with the subset $\text{Irr}(W)$ of $\text{Irr}(SW)$. Similarly, we think of the unipotent characters in B_0 as the irreducible Brauer characters of B_0 and set

$$\text{IBr}(B_0) := \mathcal{E}(\mathbb{G}, 1)_1 \subseteq \text{Irr}(B_0).$$

We associate decomposition numbers, and formal degrees of projective indecomposable characters to B_0 as follows.

The \mathcal{F} -classes of elements of S are the W -conjugacy classes of S . Further, since $(|W|, \ell) = 1$, the Glauberman–Isaacs correspondence gives that the actions of W on S and on $\text{Irr}(S)$ are permutation isomorphic. Thus there is a bijection between the set of W -classes of $\text{Irr}(S)$ and the set of W -classes of S such that if the class of $s \in S$ corresponds to the class of $\hat{s} \in \text{Irr}(S)$, then $W_s = W_{\hat{s}}$ where $W_s, W_{\hat{s}}$ denotes the stabiliser in W of s, \hat{s} respectively. Note that W_s was denoted $W(s)$ in Example 4.4. Such a bijection between the set of W -classes of $\text{Irr}(S)$ and of S will be called W -equivariant if in addition the (class of) $1 \in S$ is sent to the (class of the) trivial character of S . Note that a W -equivariant bijection always exists.

By Clifford theory,

$$\text{Irr}(SW) = \coprod_{\theta \in \text{Irr}(S)/W} \text{Irr}(SW|\theta),$$

where the union runs over a set $\text{Irr}(S)/W$ of representatives θ of W -conjugacy classes of $\text{Irr}(S)$ and where $\text{Irr}(SW|\theta)$ denotes the set of irreducible characters of SW covering θ . Moreover, since $|W|$ is prime to ℓ , $\text{Irr}(SW|\theta)$ is in bijection with $\text{Irr}(W_\theta)$.

By the description of $\text{Irr}(B_0)$ given in Example 4.4, $|\text{Irr}(B_0)| = |\text{Irr}(SW)|$. A bijection $\Theta : \text{Irr}(SW) \rightarrow \text{Irr}(B_0)$, $\gamma \mapsto \hat{\gamma}$, will be said to be W -equivariant if there exists a W -equivariant bijection $\text{Irr}(S) \rightarrow S$ such that for corresponding elements $s \in S$ and $\hat{s} \in \text{Irr}(S)$, Θ restricts to a bijection $\text{Irr}(SW|\hat{s}) \rightarrow \mathcal{E}(\mathbb{G}, s)_1$. Since $\text{IBr}(SW)$ is in bijection with $\text{Irr}(W|1)$, any W -equivariant bijection $\text{Irr}(SW) \rightarrow \text{Irr}(B_0)$ restricts to a bijection $\text{IBr}(SW) \rightarrow \text{IBr}(B_0)$.

Let $\text{Irr}(SW) \rightarrow \text{Irr}(B_0)$, $\gamma \mapsto \hat{\gamma}$, be a W -equivariant bijection. We declare the decomposition matrix of B_0 to be the ℓ -decomposition matrix of SW via this bijection, that is if $d_{\gamma\nu}$ is the decomposition number in SW corresponding to $\gamma \in \text{Irr}(SW)$ and $\nu \in \text{IBr}(SW)$, then we regard $d_{\gamma\nu}$ also as the decomposition number for $\hat{\gamma} \in \text{Irr}(B_0)$ and $\hat{\nu} \in \text{IBr}(B_0)$. Recall that for any $\gamma \in \text{Irr}(SW)$, we have $\gamma(1) = \sum_{\nu \in \text{IBr}(SW)} d_{\gamma\nu} \nu(1)$. In Proposition 4.11 we show that the analogous equations hold in B_0 . We define

$$\text{deg } \Phi_{\hat{\nu}} := \sum_{\gamma \in \text{Irr}(SW)} d_{\gamma\nu} \text{deg}(\hat{\gamma}) \in \mathbb{Z}_\ell[x] \quad \text{for } \hat{\nu} \in \text{IBr}(B_0),$$

to be the formal degrees of projective indecomposable characters of B_0 . The following is a restatement of Conjecture 2.

Conjecture 4.5. *In the setting of Conjecture 4.2, if W has order coprime to ℓ , φ is trivial and $q \equiv 1 \pmod{\ell}$, then for some W -equivariant bijection $\text{Irr}(SW) \xrightarrow{\sim} \text{Irr}(B_0)$ we have that $|S|$ divides $(\text{deg } \Phi_{\hat{\nu}})|_{x=q}$ for all $\hat{\nu} \in \text{IBr}(B_0)$.*

4C. The rational and the primitive cases. We'll prove the above conjectures for most W of order coprime to ℓ in Theorem 5.20. For the moment, let us see why they hold in the rational case:

Proposition 4.6. *Conjectures 4.2, 4.3 and 4.5 hold if \mathbb{G} is a rational spets underlying a finite reductive group.*

Proof. Let \mathbf{G} be a connected reductive group over an algebraically closed field of characteristic p and $F : \mathbf{G} \rightarrow \mathbf{G}$ a Frobenius endomorphism with respect to an \mathbb{F}_q -structure, such that \mathbb{G} is the underlying spets. That is, φ is the automorphism of W induced by F . Recall that S may be identified with a Sylow ℓ -subgroup of \mathbf{G}^F and \mathcal{F} with the fusion system $\mathcal{F}_{\mathbf{G}^F}(S)$; see [Kessar et al. 2020, Remark 3.3(a) and Section 5.3]. Let d be the order of ζ , hence the order of q modulo ℓ . By [loc. cit., Proposition 6.8], there is a degree preserving bijection between $\text{Irr}(B_0)$ and the set of irreducible characters of the principal ℓ -block $B_0(\mathbf{G}^F)$. Note that the bijection given in [loc. cit., Proposition 6.8] is stated to preserve defects but it is easy to check from the setup that for any irreducible character $\gamma_{s,\lambda}$ in B_0 , $\gamma_{s,\lambda}(1)|_{x=q}$ is the degree of the corresponding character of $B_0(\mathbf{G}^F)$. Now the assertion regarding Conjecture 4.2 follows from Proposition 2.8.

As described in Section 4A, $S = T.(W_1)_\ell$ with $W_1 := W_{\varphi^{-1}\zeta^{-1}}$. Under our assumptions on ℓ , $\mathbf{L} := C_{\mathbf{G}}(T)$ is a Levi subgroup, and moreover $N_{\mathbf{G}}(S)^F \leq N_{\mathbf{G}}(T)^F = N_{\mathbf{G}}(\mathbf{L})^F$; see [Malle 2007, Theorems 5.9 and 5.14]. Let $H := N_{\mathbf{G}}(\mathbf{L})^F$. Then Proposition 2.8 shows that in order to prove Conjecture 4.3 for \mathbb{G} it suffices to see that $(\dim B_0(H))_{\ell'} \equiv |W_1|_{\ell'} \pmod{\ell}$. Now $B_0(H)$ is isomorphic to the principal block of $H/O_{\ell'}(\mathbf{L}^F)$. Since S/T acts faithfully on T , T is a Sylow ℓ -subgroup of \mathbf{L}^F , so $H/O_{\ell'}(\mathbf{L}^F) \cong T(N_{\mathbf{G}}(\mathbf{L})^F/\mathbf{L}^F) \cong TW_1$, the latter by the definition of relative Weyl groups. The result follows as TW_1 has a unique ℓ -block.

Finally, we prove Conjecture 4.5 in this situation. So assume $\varphi = 1$ and $q \equiv 1 \pmod{\ell}$. Then $W_1 = W$. As recalled above, there is a degree preserving bijection $\text{Irr}(B_0) \rightarrow \text{Irr}(B_0(\mathbf{G}^F))$. On the other hand, by a result of Puig [1994, Theorem 5.5, Corollary 5.10], as explained in [Cabanes 2018, Proposition 8.11], the principal block of \mathbf{G}^F over a suitably large complete discrete valuation ring \mathcal{O} of characteristic 0, is Morita equivalent to the group algebra $\mathcal{O}[SW]$ (note here $S = T$ as $|W|$ is prime to ℓ and that $W = N_{\mathbf{G}}(\mathbf{T})^F/\mathbf{T}^F$, where \mathbf{T} is a Sylow 1-torus of \mathbf{G} with T the Sylow ℓ -subgroup of \mathbf{T}^F). In particular the decomposition numbers of $\mathcal{O}[SW]$ are decomposition numbers of $B_0(\mathbf{G}^F)$. Thus $(\deg \Phi_{\hat{\nu}})|_{x=q}$ is the dimension of a projective indecomposable module of $B_0(\mathbf{G}^F)$. Now Conjecture 4.5 follows since the dimension of any projective indecomposable module of a finite group algebra $\mathcal{O}G$ is divisible by $|G|_{\ell}$ (for instance, apply Proposition 2.7 with respect to the standard symmetrising form on $\mathcal{O}G$.) \square

To deal with the primitive cases, we use the following:

Lemma 4.7. *Let (W, L) be a finite ℓ -adic reflection group with $|W|$ prime to ℓ and let $W_0 \leq W$ be a parabolic subgroup. For $1 \leq k \leq \text{rk}(W_0)$ there exist $b_k^{W_0} \in \mathbb{Z}$ such that for any prime power $q \equiv 1 \pmod{\ell}$ and \mathcal{F} the fusion system attached to (W, L, q) , on a homocyclic ℓ -group T of exponent a , the number of W -orbits (\mathcal{F} -classes) of elements of T with stabiliser conjugate to W_0 is given by*

$$\frac{1}{|N_W(W_0) : W_0|} \prod_{k=1}^{\text{rk}(W_0)} (\ell^a - b_k^{W_0}).$$

Proof. Let \mathcal{A} denote the set of 1-eigenspaces of reflections in T and denote by $\mathcal{L} = \mathcal{L}(\mathcal{A})$ the lattice of all intersections of elements of \mathcal{A} with minimal element T . By Steinberg’s theorem (see [Kessar et al. 2020, Proposition 2.3]), each $Y \in \mathcal{L}$ is the centraliser in T of some parabolic subgroup. Thus by inclusion/exclusion, the number of W -orbits of elements of T with stabiliser conjugate to W_0 is given by the Euler characteristic of the sublattice $\{Y \in \mathcal{L} \mid C_T(W_0) \leq Y\}$ divided by $|N_W(W_0) : W_0|$. This Euler characteristic has the stated form by [Orlik and Solomon 1982, Theorem 1.2]. \square

The tables in [Orlik and Solomon 1982] explicitly list the integers $b_k^{W_0}$ (and the quantities $|N_W(W_0) : W_0|$) for all parabolic subgroups W_0 of all exceptional complex reflection groups W . An immediate consequence is the following result:

Proposition 4.8. *Conjectures 4.2 and 4.3 hold for all primitive spetsial ℓ -adic reflection groups with $q \equiv 1 \pmod{\ell}$.*

Proof. If W is a Weyl group, the claim follows from Proposition 4.6. For the remaining Coxeter groups, it follows from Theorem 5.20. Otherwise since ℓ is very good, we must have $\ell \nmid |W|$ and

$$W \in \{G_4, G_6, G_8, G_{14}, G_{24}, G_{25}, G_{26}, G_{27}, G_{29}, G_{32}, G_{33}, G_{34}\}.$$

For all of these only $\varphi = 1$ is possible, by [Broué et al. 1999, Proposition 3.13]. We explicitly calculate $\dim(B_0)$ as a polynomial in x using Lemma 4.7 and the tables in [Broué et al. 2014, Appendix]. The required congruences for $\dim(B_0)|_{x=q}$ are readily checked via the substitution $q \mapsto 1 + r\ell^a$ for $r \in \mathbb{Z}$. \square

4D. Character degrees and Schur elements. The proof of Theorem 1 goes through the connection between unipotent character degrees of spetses and Schur elements of corresponding Hecke algebras. We describe this connection in the relevant special case. Let $\mathbb{G} = (W, L)$ be a simply connected \mathbb{Z}_ℓ -spets such that ℓ is very good for \mathbb{G} and q a prime power and let $\psi_s : \mathbb{Z}_\ell[\tilde{\mathbf{u}}^{\pm 1}] \rightarrow \mathbb{Z}_\ell[x^{1/z}]$ be the spetsial specialisation described in Section 3B with $R = \mathbb{Z}_\ell$. The degrees of the unipotent characters $\text{Uch}(\mathbb{G})$ of \mathbb{G} in the principal 1-Harish-Chandra series $\mathcal{E}(\mathbb{G}, 1)_1$ are given by

$$\psi_s(f_{1_W}) / \psi_s(f_\phi) \quad \text{for } \phi \in \text{Irr}(W);$$

see [Malle 1995, Sätze 3.14, 6.10] for the infinite series and [Broué et al. 2014, Axiom 4.16] for the exceptional types. This leads to the following formula for character degrees in the principal block B_0 of $\mathbb{G}(q)$.

Lemma 4.9. *Assume $q \equiv 1 \pmod{\ell}$. Then the degrees of the characters in $\text{Irr}(B_0)$ are given by*

$$\coprod_{s \in S/\mathcal{F}} \left\{ \frac{|C_{\mathbb{G}}(\mathbb{T})|_{x'}}{|C_{C_{\mathbb{G}}(s)}(\mathbb{T}_s)|_{x'}} \frac{\psi_s(p_W)}{\psi_s(f_{s,\phi})} \mid \phi \in \text{Irr}(W(s)) \right\}$$

where \mathbb{T}, \mathbb{T}_s is a Sylow 1-torus of $\mathbb{G}, C_{\mathbb{G}}(s)$, respectively, and the $f_{s,\phi}$ denote the Schur elements of the Hecke algebra $\mathcal{H}(W(s), \mathbf{u}_s)$ of $W(s)$, with the parameters \mathbf{u}_s inherited from $\mathcal{H}(W, \mathbf{u})$.

Proof. As mentioned above for any $s \in S$ the degrees of the unipotent characters in the principal 1-series of $\mathcal{E}(C_{\mathbb{G}}(s), 1)$ are given by

$$\{\psi_s(p_{W(s)})/\psi_s(f_{s,\phi}) \mid \phi \in \text{Irr}(W(s))\} \subset \mathbb{Z}_{\ell}[x].$$

Now by [Malle 2000, Proposition 8.1] we have $\psi_s(p_W) = \psi_s(f_1) = |\mathbb{G} : C_{\mathbb{G}}(\mathbb{T})|_{x'}$ and accordingly $\psi_s(p_{W(s)}) = |C_{\mathbb{G}}(s) : C_{C_{\mathbb{G}}(s)}(\mathbb{T}_s)|_{x'}$. Since by definition the degree of $\gamma_{s,\phi} \in \text{Irr}(B_0)$ is

$$|\mathbb{G} : C_{\mathbb{G}}(s)|_{x'} \psi_s(p_{W(s)})/\psi_s(f_{s,\phi}),$$

our claim follows. □

Lemma 4.10. *In the situation of Lemma 4.9, assume moreover that $|W|$ is coprime to ℓ . Then the degrees of the characters in $\text{Irr}(B_0)$ are given by*

$$\coprod_{s \in S/\mathcal{F}} \{\psi_s(p_W)/\psi_s(f_{s,\phi}) \mid \phi \in \text{Irr}(W(s))\},$$

where $f_{s,\phi}$ denotes the Schur elements of the Hecke algebra $\mathcal{H}(W(s), \mathbf{u}_s)$.

Proof. If ℓ does not divide $|W|$ then we have $S = T$, that is, the centraliser of any ℓ -element $s \in S$ contains the Sylow 1-torus \mathbb{T} , whence $\mathbb{T}_s = \mathbb{T}$ for all s . Now the centraliser of a Sylow 1-torus is a maximal torus since the coset $W\phi$ always contains a 1-regular element by [Malle 2006, Proposition 3.3]; for this note that none of the exceptions in [loc. cit.] is spetsial. So in fact $C_{\mathbb{G}}(\mathbb{T}) = C_{C_{\mathbb{G}}(s)}(\mathbb{T})$ and the stated formula follows from Lemma 4.9. □

By analogy with the group case, we now establish a Brauer reciprocity formula for the Brauer characters and decomposition numbers defined in Section 4B.

Proposition 4.11. *Suppose that W is ℓ -adic spetsial of order coprime to ℓ , $\varphi = 1$ and $q \equiv 1 \pmod{\ell}$. Then for any W -equivariant bijection $\hat{\cdot} : \text{Irr}(SW) \rightarrow \text{Irr}(B_0)$ we have*

$$\deg(\hat{\gamma}) = \sum_{\chi \in \text{IBr}(SW)} d_{\gamma,\chi} \deg(\hat{\chi}).$$

Proof. By Clifford theory the ordinary irreducible characters of $SW = TW$ are obtained as

$$\text{Irr}(TW) = \{\text{Ind}_{TW_{\theta}}^{TW}(\theta \otimes \nu) \mid \theta \in \text{Irr}(T), \nu \in \text{Irr}(W_{\theta})\}.$$

Since $T = O_{\ell}(TW)$ and $|W|$ is prime to ℓ , $\text{IBr}(TW)$ consists of the restrictions to ℓ' -classes of the irreducible characters $1 \otimes \nu$, $\nu \in \text{Irr}(W)$, and we may (and will) thus identify $\text{IBr}(TW)$ with $\text{Irr}(W)$. The ℓ -decomposition numbers of TW are then described as follows: If $\eta \in \text{Irr}(TW)$ then its restriction to ℓ' -classes η^0 can be considered as character of W , and the multiplicity of $\chi \in \text{IBr}(TW) = \text{Irr}(W)$ in η^0 is just $\langle \eta, \chi \rangle$. That is, if $\eta = \text{Ind}_{TW_{\theta}}^{TW}(\theta \otimes \nu)$ as above, then this multiplicity is $\langle \nu, \chi|_{W_{\theta}} \rangle$.

Now assume that $\gamma \in \text{Irr}(B_0)$. Then there is $s \in T$ and $\lambda \in \text{Uch}(C_{\mathbb{G}}(s))_1$ such that $\gamma = \gamma_{s,\lambda}$. Let $\phi \in \text{Irr}(W(s))$ be the irreducible character indexing $\lambda \in \text{Uch}(C_{\mathbb{G}}(s))_1$. Now by Lemma 4.10 we have

$\gamma_{s,\lambda}(1) = \psi_s(p_W)/\psi_s(f_{s,\phi})$. On the other hand, for $\gamma' \in \mathcal{E}(\mathbb{G}, 1)_1$ labelled by $\chi \in \text{Irr}(W)$ we have $\gamma'(1) = \psi_s(p_W)/\psi_s(f_\chi)$. Thus the required equality reads

$$\psi_s(f_{s,\phi})^{-1} = \sum_{\chi \in \text{Irr}(W)} \langle \phi, \chi|_{W_s} \rangle \psi_s(f_\chi)^{-1}.$$

But this holds for spetsial W by the validity of 1-Howlett–Lehrer theory; see [Malle 1995, Sätze 3.14, 6.10] for the infinite series and [Broué et al. 2014, Axiom 4.16] for the exceptional types. \square

5. Yokonuma type algebras for torus normalisers for ℓ -adic reflection groups

When the order of W is prime to ℓ our definition of principal block and Conjectures 4.2, 4.3 and 4.5 are related to a generalisation of Yokonuma algebras to ℓ -adic reflection groups. The classical Yokonuma algebra was defined as the endomorphism algebra of the permutation representation of a finite Chevalley group on a maximal unipotent subgroup [Yokonuma 1967]. It is a deformation of the group algebra of the normaliser of a maximally split torus, to which it becomes isomorphic over a splitting field; see [Lusztig 2005, Section 34]. We propose to extend this construction over the ℓ -adic integers to “torus normalisers” arising from ℓ -compact groups attached to arbitrary ℓ -adic reflection groups. This will allow us in Section 5F to prove Conjectures 4.2, 4.3 and 4.5 in the case $q \equiv 1 \pmod{\ell}$ and $\varphi = 1$.

5A. Definition and first properties. Let ℓ be a prime and W be a finite ℓ -adic reflection group, that is, $W \leq \text{GL}(L)$ with $L = \mathbb{Z}_\ell^n$. Let q be a prime power with $q \equiv 1 \pmod{\ell}$ and a the positive integer such that $\ell^a \parallel (q - 1)$. Let $T = L/\ell^a L$. Then T is homocyclic of exponent ℓ^a and is equipped with a natural action of W . For any reflection $r \in W$ we set $T_r := [T, r] := \langle [t, r] \mid t \in T \rangle \leq T$.

The topological braid group $B := B(W)$ of W (see Section 3A) acts naturally on T through its quotient W . We let \hat{B} be the semidirect product of T with B . Observe that $P(W)$ acts trivially on T , so \hat{B} is a (nonsplit) extension of $T \times P(W)$ by W .

Recall from Section 3A the indeterminates $\mathbf{u} = (u_{rj})$ attached to W . We define a new set $\mathbf{v} = (v_{rj})$ of indeterminates by the linear relations

$$u_{rj} = \zeta_{o(r)}^j (1 + |T_r| v_{rj}) \quad \text{for } r \in W, 1 \leq j \leq o(r),$$

where, for any $k \mid (\ell - 1)$, $\zeta_k \in \mathbb{Z}_\ell$ denotes a primitive k -th root of unity. Let $\hat{A} = \mathbb{Z}_\ell[\mathbf{v}, \mathbf{u}^{-1}]$.

Definition 5.1. Define $\mathcal{Y}(W, a, \mathbf{v})$ to be the quotient of the group algebra $\hat{A}[\hat{B}]$ of $\hat{B} = T \rtimes B$ over \hat{A} by the ideal generated by the deformed order relations

$$\prod_{j=1}^{o(r)} (\mathbf{r} - \zeta_{o(r)}^j (1 + v_{rj} E_r)) \quad \text{with } E_r := \sum_{t \in T_r} t \in \hat{A}[T], \tag{†}$$

where \mathbf{r} runs over the braid reflections of $B \leq \hat{B}$ and r denotes the image of \mathbf{r} in W . We will write $x \mapsto y_x$ for the canonical map $\hat{A}[\hat{B}] \rightarrow \mathcal{Y}(W, a, \mathbf{v})$.

When W is a Weyl group, the deformed order relation (\dagger) generalises the quadratic one from the classical Yokonuma algebra [Juyumaya and Kannan 2001, Theorem 2(2.1)], see also [Marin 2018a, 2.2(3)]. In Section 5E, we show that in this case a suitable specialisation of \mathcal{Y} is isomorphic to a truncation of the classical Yokonuma algebra.

As far as we can tell, there is no direct relation between the algebra $\mathcal{Y}(W, a, \mathbf{v})$ defined above and the ‘‘cyclotomic Yokonuma–Hecke algebra’’ considered by Chlouveraki and d’Andecy [2016, Section 2] for the reflection group $W = G(d, 1, n)$; in their algebra, the underlying reflection group W only acts via its quotient $G(1, 1, n) \cong \mathfrak{S}_n$ on the torus. On the other hand, our construction is related to an algebra defined by Marin [2018a], see Remark 5.16 below.

Henceforth, for simplicity we set $\mathcal{Y} := \mathcal{Y}(W, a, \mathbf{v})$. Note that the specialisation $\psi_1 : \mathbb{Z}_\ell[\mathbf{u}^{\pm 1}] \rightarrow \mathbb{Z}_\ell$, $u_{rj} \mapsto \zeta_{o(r)}^j$, extends to a homomorphism $\hat{A} \rightarrow \mathbb{Z}_\ell$, $v_{rj} \mapsto 0$.

Lemma 5.2. *The following hold:*

- (a) *Under the specialisation $\psi_1 : \hat{A} \rightarrow \mathbb{Z}_\ell$, $v_{rj} \mapsto 0$ (so $u_{rj} \mapsto \zeta_{o(r)}^j$), the algebra \mathcal{Y} specialises to the group algebra of TW .*
- (b) *The quotient of \mathcal{Y} by the ideal I generated by the $\{y_t - 1 \mid t \in T\}$ is isomorphic to the extension $\hat{A} \otimes_A \mathcal{H}(W, \mathbf{u})$ of the generic Hecke algebra of W .*
- (c) *The natural \hat{A} -module homomorphism $\mathcal{Y} \rightarrow \mathcal{H}(W, \mathbf{u})$, $y_r \mapsto h_r$, in (b) has a splitting $\mathcal{H}(W, \mathbf{u}) \rightarrow \hat{A}[\ell^{-1}] \otimes_{\hat{A}} \mathcal{Y}$ given by $h_r \mapsto |T|^{-1} \sum_{t \in T} y_t y_r$.*

Proof. The first parts follows directly from the deformed order relation (\dagger) and the corresponding result of Bessis [2001] for B . For (b), let J_1 be the ideal of $\hat{A}[\hat{B}]$ generated by the elements $\{t - 1 \mid t \in T\}$. Then I is the ideal of $\hat{A}[\hat{B}]$ generated by J_1 and the elements (\dagger) as \mathbf{r} runs over the braid reflections. Let L be the ideal of $\hat{A}[\hat{B}]$ generated by J_1 and the $\prod_{j=1}^{o(r)} (\mathbf{r} - u_{rj})$ as \mathbf{r} runs over braid reflections. Then $\mathcal{H}(W, \mathbf{u}) = \hat{A}[B]/L$. For an element $x = \prod_{j=1}^{o(r)} (\mathbf{r} - \zeta_{o(r)}^j (1 + E_r v_{rj})) \in J_1$ of the form (\dagger) set $x' = \prod_{j=1}^{o(r)} (\mathbf{r} - u_{rj})$. Then $x + J_1 = x' + J_1$, whence $I = L$.

For (c), note that $|T|^{-1} \sum_{t \in T} y_t$ is a central idempotent of $\hat{A}[\ell^{-1}] \otimes_{\hat{A}} \mathcal{Y}$. □

We make some further straightforward observations. First, since for $\ell > 2$ all reflections r in an ℓ -adic reflection group have order prime to ℓ , in that case $T_r \cong \mathbb{Z}/\ell^a \mathbb{Z}$.

For all braid reflections \mathbf{r} , the element E_r commutes with \mathbf{r} and $E_r^2 = |T_r| E_r$. Thus, over $\hat{A}[\ell^{-1}]$, the element $E'_r = |T_r|^{-1} E_r$ is idempotent. Multiplying (\dagger) with E'_r respectively $1 - E'_r$ we obtain the elements

$$(1 - E'_r)(\mathbf{r}^{o(r)} - 1) \quad \text{and} \quad E'_r \prod_{j=1}^{o(r)} (\mathbf{r} - u_{rj}), \tag{\dagger'}$$

which generate the same ideal as (\dagger) over $\hat{A}[\ell^{-1}]$. Thus, (\dagger) ‘‘interpolates’’ between the group relation for r and the deformed Hecke algebra relation (\mathcal{H}) for \mathbf{r} . Let us also note the following:

Lemma 5.3. *The constant coefficient in the deformed order relation (\dagger) is invertible in $\hat{A}[T]$.*

Proof. The constant term in the polynomial relation (\dagger) for a braid reflection r is (up to a root of unity) a product of factors $1 + v_{rj}E_r$, which has inverse

$$1 - \zeta_{o(r)}^j v_{rj}/u_{rj} E_r \in \hat{A}[T]. \quad \square$$

We now give a more tangible description of $\mathcal{Y}(W, a, \mathbf{v})$. Recall that the braid group B has a presentation in terms of certain sets of braid reflections together with so-called braid relations, encoded in *braid diagrams*, such that adding the order relations for the chosen braid reflections, we obtain a presentation of W ; see [Broué et al. 1998, Theorem 2.27] and [Bessis 2001, Theorem 0.1]. Choose reflections r_1, \dots, r_m in W corresponding to a braid diagram for B . It is known that any distinguished reflection of W is then conjugate to one of the r_i , and by their construction all braid reflections projecting onto a fixed reflection of W are conjugate in B . Then using Lemma 5.3 we see that \mathcal{Y} is the associative unital \hat{A} -algebra generated by elements $\{y_t, y_{r_i} \mid t \in T, 1 \leq i \leq m\}$ subject to:

- The y_t satisfy the same relations as the corresponding group elements t (i.e., they generate a subalgebra isomorphic to (possibly a quotient of) the group algebra $\hat{A}[T]$).
- The action relations between the t, r_i , with t replaced by y_t and r_i by y_{r_i} .
- The braid relations between the y_{r_i} .
- The deformed order relations (\dagger) for the y_{r_i} .

5B. On the structure of specialised Yokonuma type algebras. We show that under some additional hypothesis certain specialisations of \mathcal{Y} are isomorphic to the group algebra of TW . The main results are Theorems 5.7 and 5.10.

For a specialisation $\psi : \hat{A} \rightarrow R$ to a commutative ring R , let $\mathcal{Y}_\psi := R \otimes_{\hat{A}} \mathcal{Y}$ denote the extension of scalars by ψ . Then \mathcal{Y}_ψ is the quotient of the group algebra $R\hat{B}$ by the ideal

$$\left\langle \prod_{j=1}^{o(r)} (r - \zeta_{o(r)}^j (1 + \psi(v_{rj})E_r)) \mid r \in B \text{ braid reflection} \right\rangle.$$

Let W_0 be a parabolic subgroup of W and $B_0 = B(W_0)$ be its braid group. In [Broué et al. 1998, Section 2D] is constructed an embedding $B_0 \hookrightarrow B$, well-defined up to P -conjugation, where $B = B(W)$, $P = P(W)$. By [loc. cit., Propositions 2.29 and 2.18] this satisfies:

Lemma 5.4. *Let W_0 be a parabolic subgroup of W . Let \tilde{B}_0 be the inverse image of W_0 in B and let \tilde{P}_0 be the subgroup of P generated by the elements $r^{o(r)}$, as r runs over the distinguished reflections in $W \setminus W_0$. Let B_0 be the braid group of W_0 . The above inclusion $B_0 \hookrightarrow B$ has image contained in \tilde{B}_0 and induces an isomorphism $B_0 \xrightarrow{\sim} \tilde{B}_0/\tilde{P}_0$.*

So we have the following diagram with exact columns:

$$\begin{array}{ccccc}
 1 & & 1 & & 1 \\
 \downarrow & & \downarrow & & \downarrow \\
 P_0 \hookrightarrow P & = & \tilde{P}_0 \rtimes P_0 & = & P \\
 \downarrow & & \downarrow & & \downarrow \\
 B_0 \hookrightarrow \tilde{B}_0 & = & \tilde{P}_0 \rtimes B_0 & \hookrightarrow & B \\
 \downarrow & & \downarrow & & \downarrow \\
 W_0 = W_0 & \hookrightarrow & & & W \\
 \downarrow & & \downarrow & & \downarrow \\
 1 & & 1 & & 1
 \end{array}$$

Remark 5.5. Examples show that the isomorphism $B_0 \xrightarrow{\sim} \tilde{B}_0/\tilde{P}_0$ might more generally hold for all reflection subgroups W_0 of W generated by distinguished reflections (see e.g., [Broué et al. 1998, Proposition 3.24]), so that the assumptions of the subsequent Theorem 5.7 might be relaxed accordingly. We will not need this here.

If W_θ is a parabolic subgroup of W , we will denote by \mathbf{u}_θ the set \mathbf{u}_0 in the notation of Section 3A if W_θ is the reflection subgroup W_0 .

Lemma 5.6. *Let R be an integral domain containing the $|T|$ -th roots of unity with field of fractions K of characteristic 0 and let $\psi : \hat{A} \rightarrow R$ be a specialisation. Let I be the ideal of $R\hat{B}$ generated by*

$$\left\{ \prod_{j=1}^{o(r)} (\mathbf{r} - \zeta_{o(r)}^j (1 + \psi(v_{r_j})E_r)) \mid \mathbf{r} \in B \text{ braid reflection} \right\}.$$

Let $\theta \in \text{Irr}_K(T)$ and $e_\theta \in KT$ the corresponding central idempotent. Suppose that the stabiliser W_θ of θ is a parabolic subgroup of W . Then $e_\theta R\hat{B}e_\theta/e_\theta Ie_\theta \cong \mathcal{H}_\psi(W_\theta, \mathbf{u}_\theta)$ as R -algebras. Here we regard $R\hat{B}$ as a subset of $K\hat{B}$.

Note that the assumption that R contains the $|T|$ -th roots of unity is needed in order to ensure that any ordinary irreducible character of T is R -valued.

Proof. Let \tilde{B}_θ be the full inverse image of W_θ in B . For a braid reflection $\mathbf{r} \in B$ set

$$i_{\mathbf{r}} := \prod_{j=1}^{o(r)} (\mathbf{r} - \zeta_{o(r)}^j (1 + \psi(v_{r_j})E_r)) = (1 - E'_r)(\mathbf{r}^{o(r)} - 1) + E'_r \prod_{j=1}^{o(r)} (\mathbf{r} - \psi(u_{r_j}))$$

where $E'_r = |T_r|^{-1}E_r$. Then

$$\{e_\theta x i_{\mathbf{r}} y e_\theta \mid x, y \in \hat{B}, \mathbf{r} \in B \text{ braid reflection}\}$$

generates $e_\theta Ie_\theta$ as R -module. The set of braid reflections is invariant under conjugation by B , and $v_{r_j} = v_{r'_j}$ whenever r and r' are conjugate. Thus, if $x = tg$, $y = hs$ with $t, s \in T$ and $g, h \in B$ and \mathbf{r} is a

braid reflection, then

$$e_\theta x i_r y e_\theta = \theta(t)\theta(s)e_\theta i_{s_r} g h e_\theta, \quad \text{where } \theta(t), \theta(s) \in R.$$

Thus, $e_\theta I e_\theta$ is the R -span of $\{e_\theta i_r x e_\theta \mid x \in B, r \in B \text{ braid reflection}\}$.

Now $r \in W_\theta$ if and only if $\theta(t^{-1}t^r) = 1$ for all $t \in T$. Thus, $e_\theta E'_r = e_\theta$ if $r \in W_\theta$ and zero otherwise, and so

$$e_\theta i_r = \begin{cases} e_\theta(\mathbf{r}^{o(r)} - 1) & \text{if } \mathbf{r} \notin W_\theta, \\ e_\theta \prod_j (\mathbf{r} - \psi(u_{r_j})) & \text{if } \mathbf{r} \in W_\theta. \end{cases}$$

Further, since $\mathbf{r}^{o(r)} \in P$ commutes with T , we have $e_\theta(\mathbf{r}^{o(r)} - 1)x e_\theta = (\mathbf{r}^{o(r)} - 1)e_\theta x e_\theta$ and if $r \in W_\theta$, then

$$e_\theta \prod_j (\mathbf{r} - \psi(u_{r_j})) x e_\theta = \prod_j (\mathbf{r} - \psi(u_{r_j})) e_\theta x e_\theta.$$

For any $x \in B$, $e_\theta x e_\theta = x e_\theta$ if $x \in \tilde{B}_\theta$ and zero otherwise. Hence $e_\theta I e_\theta$ is the R -span of

$$\{(\mathbf{r}^{o(r)} - 1)x e_\theta \mid x \in \tilde{B}_\theta, r \notin W_\theta\} \cup \left\{ \prod_j (\mathbf{r} - \psi(u_{r_j})) x e_\theta \mid x \in \tilde{B}_\theta, r \in W_\theta \right\}.$$

By the same argument we have that $e_\theta R \hat{B} e_\theta = e_\theta R[T \tilde{B}_\theta] e_\theta$ and since e_θ is $T \tilde{B}_\theta$ -stable and e_θ is idempotent we also have $e_\theta R[T \tilde{B}_\theta] e_\theta = R[T \tilde{B}_\theta] e_\theta$. Since θ is linear and \tilde{B}_θ -stable, there is an R -algebra isomorphism $R \tilde{B}_\theta \cong R[T \tilde{B}_\theta] e_\theta$ given by $x \mapsto x e_\theta$. This induces an isomorphism

$$R \tilde{B}_\theta / J \cong R[T \tilde{B}_\theta] e_\theta / e_\theta I e_\theta$$

where $J \trianglelefteq R \tilde{B}_\theta$ is the ideal generated by $\{\mathbf{r}^{o(r)} - 1 \mid r \notin W_\theta\} \cup \{\prod_j (\mathbf{r} - \psi(u_{r_j})) \mid r \in W_\theta\}$. By Lemmas 5.4 and 5.2(b), $R \tilde{B}_\theta / J \cong \mathcal{H}_\psi(W_\theta, \mathbf{u}_\theta)$. □

Theorem 5.7. *Assume all stabilisers W_θ of elements $\theta \in \text{Irr}(T)$ are parabolic subgroups of W . Let K be a field of characteristic 0 containing the $|T|$ -th roots of unity and let $\psi : \hat{A} \rightarrow K$ be a ring homomorphism. Then:*

(a)
$$\mathcal{Y}_\psi \cong \prod_{\theta} \text{Mat}_{|W:W_\theta|}(K) \otimes_K \mathcal{H}_\psi(W_\theta, \mathbf{u}_\theta)$$

as θ runs over a set of representatives of W -orbits on $\text{Irr}_K(T)$.

(b) $\dim_K \mathcal{Y}_\psi = |TW|$.

(c) *Suppose that $K_W \subseteq K$ and ψ is the inclusion homomorphisms. Then $\mathcal{Y}_\psi \cong K[TW]$.*

Proof. Part (a) is immediate from Lemmas 2.3 and 5.6 applied with $R = K$. Part (b) follows from part (a) by Theorem 3.1 and Lemma 2.3(b) applied with $G = TW$.

Now assume K and ψ are as in (c). As explained in Section 3B, for all $\theta \in \text{Irr}(T)$, $\mathcal{H}_\psi(W_\theta, \mathbf{u}_\theta) = K \otimes_{\hat{A}} \mathcal{H}(W_\theta, \mathbf{u}_\theta) \cong K W_\theta$. Now (c) follows from (a) and Lemma 2.3(a) applied with $G = TW$ and $I = 0$, noting that $K(TW)_\theta e_\theta \cong K W_\theta$. □

We now turn to specialisations of \hat{A} to finite extensions of \mathbb{Z}_ℓ . For the rest of this section, the following notation will be in effect. Let $\mathbb{Z}_\ell \subseteq \mathcal{O}$ be a complete discrete valuation ring with uniformiser π , residue field k and field of fractions K . Let $\psi : \hat{A} \rightarrow \mathcal{O}$ be a \mathbb{Z}_ℓ -algebra homomorphism and denote by $\bar{\psi}$ the composition of ψ with the canonical map $\mathcal{O} \rightarrow k$. Recall that for $x \in \hat{A}[\hat{B}]$ we denote by y_x its image in \mathcal{Y} . For $y \in \mathcal{Y}$ let $\tilde{y} := 1_{\mathcal{O}} \otimes y \in \mathcal{Y}_\psi$, and $\bar{y} := 1_k \otimes y \in \mathcal{Y}_{\bar{\psi}}$.

Lemma 5.8. *Let W be a set of coset representatives of P in B and let J be the ideal of \mathcal{Y}_ψ generated by $\{\tilde{y}_t - 1 \mid t \in T\}$ and π . Then, $kW \cong \mathcal{Y}_\psi/J$ via the map which sends $w \in W$ to $\tilde{y}_w + J$ for $w \in W$ lifting w .*

Proof. For a distinguished reflection $r \in W$, ℓ divides $|T_r|$, hence $u_{rj} \in I$. Now the result follows from Lemma 5.2(b) (suitably adapted to the coefficient ring \mathcal{O}). □

Theorem 5.9. *Let W be a set of coset representatives of P in B . If all stabilisers W_θ of elements $\theta \in \text{Irr}(T)$ are parabolic subgroups of W , then $X := \{\tilde{y}_t \tilde{y}_w \mid t \in T, w \in W\}$ is an \mathcal{O} -basis of \mathcal{Y}_ψ .*

Proof. We first show that $\{\bar{y}_t \bar{y}_w \mid t \in T, w \in W\}$ generates $\mathcal{Y}_{\bar{\psi}}$ as k -vector space. Let $R \subseteq \mathcal{Y}_{\bar{\psi}}$ be the k -span of $\{\bar{y}_t \mid t \in T\}$. Then R is a commutative k -subalgebra of $\mathcal{Y}_{\bar{\psi}}$. Let Q be the ideal of R generated by $\{\bar{y}_t - 1 \mid t \in T\}$. Since T is a finite abelian ℓ -group, Q is a nilpotent ideal of R . We consider $\mathcal{Y}_{\bar{\psi}}$ as a left R -module. Since T is normal in \hat{B} , the R -submodule $Q\mathcal{Y}_{\bar{\psi}}$ of $\mathcal{Y}_{\bar{\psi}}$ is an ideal of $\mathcal{Y}_{\bar{\psi}}$. Further, $Q\mathcal{Y}_{\bar{\psi}}$ is the image of the ideal J of Lemma 5.8 in $\mathcal{Y}_\psi/\pi\mathcal{Y}_\psi \cong \mathcal{Y}_{\bar{\psi}}$ and for any $w \in W$, $\bar{y}_w + Q\mathcal{Y}_{\bar{\psi}} = \tilde{y}_w + J$. So, by Lemma 5.8, $\{\bar{y}_w + Q\mathcal{Y}_{\bar{\psi}} \mid w \in W\}$ generates $\mathcal{Y}_{\bar{\psi}}/Q\mathcal{Y}_{\bar{\psi}}$ as k -vector space and hence as R -module. Applying Lemma 2.1 with $M = \mathcal{Y}_{\bar{\psi}}$ and the nilpotent ideal Q we obtain that $\{\bar{y}_w \mid w \in W\}$ generates $\mathcal{Y}_{\bar{\psi}}$ as R -module. Since R is generated by $\{\bar{y}_t \mid t \in T\}$ as k -vector space we have the required result.

Now we claim that in order to prove the theorem it suffices to prove that \mathcal{Y}_ψ is finitely generated as \mathcal{O} -module. Indeed, suppose that \mathcal{Y}_ψ is finitely generated as \mathcal{O} -module. Then by the previous paragraph and the standard Nakayama lemma (Lemma 2.1) applied to the ring \mathcal{O} and ideal $\pi\mathcal{O}$, the set $X = \{\tilde{y}_t \tilde{y}_w \mid t \in T, w \in W\}$ generates \mathcal{Y}_ψ as \mathcal{O} -module. Then $1 \otimes X$ generates $K \otimes_{\mathcal{O}} \mathcal{Y}_\psi$ as K -vector space and since the latter has dimension $|TW|$ by Theorem 5.7(b), X is an \mathcal{O} basis of \mathcal{Y}_ψ .

It remains only to show that \mathcal{Y}_ψ is finitely generated as \mathcal{O} -module. For this, suppose first that \mathcal{O} -contains the $|T|$ -th roots of unity. Let I be the ideal of $\mathcal{O}\hat{B}$ generated by the (\dagger) -relations, let

$$I' = \bigoplus_{\theta, \mu \in \text{Irr}(T)} e_\theta I e_\mu \subseteq \bigoplus_{\theta, \mu \in \text{Irr}(T)} e_\theta \mathcal{O}\hat{B}e_\mu$$

with $e_\theta \in KT$ as in Lemma 5.6 and let $\tilde{I} = \mathcal{O}\hat{B} \cap I'$. Since I' is an ideal of $\bigoplus e_\theta \mathcal{O}\hat{B}e_\mu$, \tilde{I} is an ideal of $\mathcal{O}\hat{B}$ containing I . On the other hand, $|T|e_\theta \in \mathcal{O}\hat{B}$ for all θ , hence $|T|^2 e_\theta I e_\mu \subseteq I$ and $|T|^2 \tilde{I} \subseteq I$. The kernel of the composition of the inclusion $\mathcal{O}\hat{B} \hookrightarrow \bigoplus e_\theta \mathcal{O}\hat{B}e_\mu$ with the surjection $\bigoplus e_\theta \mathcal{O}\hat{B}e_\mu \rightarrow \bigoplus e_\theta \mathcal{O}\hat{B}e_\mu / I'$ is \tilde{I} . Thus, $\mathcal{O}\hat{B}/\tilde{I}$ is isomorphic to a submodule of $\bigoplus e_\theta \mathcal{O}\hat{B}e_\mu / I'$. On the other hand,

$$\bigoplus_{\theta, \mu \in \text{Irr}(T)} e_\theta \mathcal{O}\hat{B}e_\mu / I' \cong \bigoplus_{\theta, \mu \in \text{Irr}(T)} e_\theta \mathcal{O}\hat{B}e_\mu / e_\theta I e_\mu.$$

If $\mu =^x \theta$ for $x \in B$, then $e_\theta \mathcal{O} \hat{B} e_\mu / e_\theta I e_\mu \cong e_\theta \mathcal{O} \hat{B} e_\theta / e_\theta I e_\theta$ via right multiplication by x and it follows from Lemma 5.6 and Theorem 3.1 that $e_\theta \mathcal{O} \hat{B} e_\theta / e_\theta I e_\theta$ is finitely generated free as \mathcal{O} -module. If θ, μ are in different W -orbits, then $e_\theta \mathcal{O} \hat{B} e_\mu = 0$. By the above displayed equation, $\bigoplus e_\theta \mathcal{O} \hat{B} e_\mu / I'$ is finitely generated free as \mathcal{O} -module. Since \mathcal{O} is a principal ideal domain, and since $\mathcal{O} \hat{B} / \tilde{I}$ is isomorphic to a submodule of $\bigoplus e_\theta \mathcal{O} \hat{B} e_\mu / I'$, it follows that $\mathcal{O} \hat{B} / \tilde{I}$ is finitely generated free as \mathcal{O} -module. Also, $\pi^r(\tilde{I}/I) = 0$ for r equal to twice the π -adic valuation of $|T|$. We saw above that $\mathcal{Y}_\psi / \pi \mathcal{Y}_\psi \cong \mathcal{Y}_{\tilde{\psi}}$ is finitely generated as k -vector space and hence as \mathcal{O} -module. Thus by Lemma 2.2 applied with $M = \mathcal{Y}_\psi = \mathcal{O} \hat{B} / I$ and $N = \tilde{I} / I$ we have \mathcal{Y}_ψ is finitely generated as \mathcal{O} -module.

Now consider the general case. Let \mathcal{O}' be a finite extension of \mathcal{O} containing the $|T|$ -th roots of unity and let ψ' be the composition of ψ with inclusion of \mathcal{O} in \mathcal{O}' . By the previous part, applied with ψ' in place of ψ , $\mathcal{Y}_{\psi'}$ is finitely generated as \mathcal{O}' -module. Since \mathcal{O}' is a finite extension of \mathcal{O} , $\mathcal{Y}_{\psi'}$ is also finitely generated as \mathcal{O} -module. Since \mathcal{O} is a direct summand of \mathcal{O}' as \mathcal{O} -module, the inclusion $\mathcal{O} \hookrightarrow \mathcal{O}'$ is pure. Thus the map $\mathcal{Y}_\psi \rightarrow \mathcal{O}' \otimes_{\mathcal{O}} \mathcal{Y}_\psi \cong \mathcal{Y}_{\psi'}$, $y \mapsto 1 \otimes y$, is injective and consequently \mathcal{Y}_ψ is isomorphic to an \mathcal{O} -submodule of $\mathcal{Y}_{\psi'}$. Since \mathcal{O} is Noetherian and since as shown above $\mathcal{Y}_{\psi'}$ is finitely generated as \mathcal{O} -module, \mathcal{Y}_ψ is finitely generated as \mathcal{O} -module. \square

The following is an application of a theorem of Külshammer, Okuyama and Watanabe; see [Linckelmann 2018, Theorem 4.8.2]. Recall that if R is a commutative ring and C is a subalgebra of an R -algebra B , then B is *relatively C -separable* if B is a direct summand of $B \otimes_C B$ as a (B, B) -bimodule.

Theorem 5.10. *Suppose that W is an ℓ' -group. Then there exists an \mathcal{O} -algebra isomorphism $\mathcal{Y}_\psi \cong \mathcal{O}[TW]$ sending \tilde{y}_t to t for any $t \in T$.*

Proof. Let W be a set of coset representatives of P in B . Since W is an ℓ' -group, W_θ is a parabolic subgroup of W for all $\theta \in \text{Irr}(T)$. Thus, by Theorem 5.9, $\{\tilde{y}_t \tilde{y}_w \mid t \in T, w \in W\}$ is an \mathcal{O} -basis of \mathcal{Y}_ψ . Further, we may regard $\mathcal{O}T$ as an \mathcal{O} -subalgebra of \mathcal{Y}_ψ via the identification of $\mathcal{O}T$ with the subalgebra generated by $\{\tilde{y}_t \mid t \in T\}$. Under this identification, again via Theorem 5.9, there is a homomorphism of $(\mathcal{O}T, \mathcal{O}T)$ -bimodules $\gamma : \mathcal{O}[TW] \rightarrow \mathcal{Y}_\psi$ defined by $\gamma(tw) = \tilde{y}_t \tilde{y}_w$.

Let J be the ideal of \mathcal{Y}_ψ generated by $\{\tilde{y}_t - 1 \mid t \in T\}$ and π . It follows from Lemma 5.8 that the composition of γ with the natural surjection $\mathcal{Y}_\psi \rightarrow \mathcal{Y}_\psi / J$ is an \mathcal{O} -algebra homomorphism. Now we may apply [Linckelmann 2018, Theorem 4.8.2] to obtain an \mathcal{O} -algebra homomorphism $\sigma : \mathcal{O}[TW] \rightarrow \mathcal{Y}_\psi / J$ extending the \mathcal{O} -algebra homomorphism $\mathcal{O}[TW] \rightarrow \mathcal{Y}_\psi / J$ obtained above from γ and satisfying $\sigma(t) = \tilde{y}_t$ for all $t \in T$. For this one needs to have that J is contained in the radical of \mathcal{Y}_ψ and that $\mathcal{O}[TW]$ is relatively $\mathcal{O}T$ -separable. The second condition holds since W is an ℓ' -group (see [loc. cit., Proposition 2.6.9]) whereas the first condition holds since T is a finite normal ℓ -subgroup of \hat{B} and, by Theorem 5.9, \mathcal{Y}_ψ is finitely generated as \mathcal{O} -module.

The surjectivity of σ follows by Nakayama's lemma since the composition of σ with $\mathcal{Y}_\psi \rightarrow \mathcal{Y}_\psi / I$ is surjective and then the injectivity follows since both algebras are free of the same rank. \square

Remark 5.11. The assumption of Theorem 5.7 on stabilisers is satisfied whenever ℓ is very good for W , e.g., when $|W|$ is coprime to ℓ , or if $W = G(e, 1, n)$ with $e \geq 2$; see [Kessar et al. 2020, Proposition 2.3].

5C. Freeness. We propose the following, analogous to the (now proven) freeness conjecture (Theorem 3.1) for cyclotomic Hecke algebras:

Conjecture 5.12. *The algebra \mathcal{Y} is free over \hat{A} of rank $|TW|$. More precisely, there is a section $W \rightarrow \mathbf{W} \subset B$ of the natural map $B \rightarrow W$ containing 1 such that $\{y_t y_{\mathbf{w}} \mid t \in T, \mathbf{w} \in \mathbf{W}\}$ is an \hat{A} -basis of \mathcal{Y} .*

For Weyl groups and parameters occurring in finite reductive groups, the freeness follows from the construction as an endomorphism algebra, and the dimension from the number of double cosets of a maximal unipotent subgroup, that is, the Bruhat decomposition; see [Lusztig 2005, 34.2–34.10] for a detailed investigation. We propose a proof in the case of finite Coxeter groups and for most infinite series of complex reflection groups.

Theorem 5.13. *Conjecture 5.12 holds for any finite Coxeter group.*

Proof. Assume that W is a Coxeter group and choose a presentation of B on braid reflections $r_1, \dots, r_m \in B$ mapping to the Coxeter generators of W . Clearly, the set of all monomials in the y_t, y_{r_i} forms a generating system for \mathcal{Y} as an \hat{A} -module. By the ‘action relations’ any such monomial can be rewritten into an \hat{A} -linear combination of elements $y_t y_{\mathbf{w}}$ with $t \in T$ and \mathbf{w} a monomial in the generators $r_i, 1 \leq i \leq m$. Now by Matsumoto’s lemma, by using the braid relations plus the quadratic relations (\dagger) expressing $y_{r_i}^2$ as a linear combination of smaller powers of y_{r_i}, \mathbf{w} can be rewritten into an $\hat{A}[T]$ -linear combination of elements from a fixed set $\mathbf{W} \subset B$ of reduced expressions of elements of W .

Thus any monomial in the generators is an \hat{A} -linear combination of elements $y_t y_{\mathbf{w}}$ with $t \in T$ and $\mathbf{w} \in \mathbf{W}$. Since the y_t satisfy the same relations as the corresponding $t \in T$, there are at most $|T|$ distinct elements y_t , so we have identified a generating system for \mathcal{Y} of cardinality $|TW|$. By Theorem 5.7 this must be free over K , hence an \hat{A} -basis of \mathcal{Y} . \square

Theorem 5.14. *Conjecture 5.12 holds for $W = G(e, p, n)$ with $e \mid (\ell - 1)$ for any divisor p of e , except possibly when $n = 2, e, p$ are both even and $p \neq e$.*

Proof. The group $W = G(e, p, n)$ is a normal reflection subgroup of $W_1 := G(e, 1, n)$ of index p . First assume that $p < e$. Then the braid group B of W is normal in the braid group B_1 of W_1 of index p by [Broué et al. 1998, Section 3.B1]. Also, the corresponding tori T can be identified, such that $T.B$ is normal in $T.B_1$ of index p . A system of coset representatives is given by $\{r_1^i \mid 0 \leq i \leq p - 1\}$, where $r_1 \in B_1$ lifts a distinguished reflection $r \in W_1$ of order e . Let ζ_e be a primitive e -th root of unity and set $p' := e/p$. Recall the parameters $u_{rj}, 1 \leq j \leq p'$, for \mathcal{Y} at the reflection r . Let K be a sufficiently large extension of $\text{Frac}(\hat{A})$. Consider parameters $u'_{rj} := u_{rj}^{1/p}$ for $1 \leq j \leq p'$, and $u'_{r, j+p'} := \zeta_e^{p'} u'_{rj}$ for $1 \leq j \leq e - p'$. Now over K , the relation (\dagger) for $y_1 := y_{r_1}$ can be rewritten as

$$(1 - E')(y_1^e - 1) + E' \prod_{j=1}^e (y_1 - u'_{rj}) = 0,$$

with $E' := |T_r|^{-1} E_r$; see (\dagger) above. Note that $\prod_{i=0}^{p-1} (y_1 - u'_{r, j+p'i}) = y_1^p - u_{rj}$ for any j . Similarly, over K the relation (\dagger) for the generator y_1^p of \mathcal{Y} can be written as

$$(1 - E')(y_1^{pp'} - 1) + E' \prod_{j=1}^{p'} (y_1^p - u_{rj}) = 0.$$

Thus, we obtain the same relation for y_1^p in \mathcal{Y} as before.

Let \mathcal{Y}_1 be the quotient of $\hat{A}[T.B_1]$ by the deformed order relations, which agree with those for \mathcal{Y} as we just saw and hence can be written over \hat{A} , except in the excluded case $n = 2, e, p$ both even, when $G(e, p, 2)$ contains an additional class of reflections.

We claim that the conjecture holds for W_1 . Our proof for this closely follows some arguments in [Bremke and Malle 1997]. Let $r_1, \dots, r_n \in B$ be braid reflections corresponding to the standard presentation, so that r_2, \dots, r_n generate the braid group on n strands (of type A_{n-1}) and $(r_1 r_2)^2 = (r_2 r_1)^2$. Set $y_2 := y_{r_2}$. Now by Lemma 5.15 below for any $a, b \geq 1$ we have

$$y_2 y_1^a y_2 y_1^b = \alpha y_1^b y_2 y_1^a y_2 + \sum_{i=1}^b (\alpha_i y_1^{a+b-i} y_2 y_1^i + \alpha'_i y_1^i y_2 y_1^{a+b-i})$$

for suitable $\alpha \in \hat{A}[T]^\times$ and $\alpha_i, \alpha'_i \in \hat{A}[T]$. With this, one deduces as in the proof of [loc. cit., Proposition 2.4] that there is a set $\mathcal{B}_1 \subset B_1$ of cardinality $|W_1|$ consisting of monomials in the r_i , as in [loc. cit., Lemma 1.5], such that any monomial in the y_t, y_i can be rewritten in \mathcal{Y}_1 into an \hat{A} -linear combination of the $|TW_1|$ products $\mathcal{B} := \{y_t y_w \mid t \in T, w \in \mathcal{B}_1\}$. Thus, \mathcal{B} is linearly independent over K by Theorem 5.7 and so an \hat{A} -basis of \mathcal{Y}_1 . This proves our claim for W_1 .

Now $\hat{A}[T.B_1] = \bigoplus_{i=0}^{p-1} \hat{A}[T.B]r_1^i$ is $\mathbb{Z}/p\mathbb{Z}$ -graded and multiplication by r_1 defines \hat{A} -module isomorphisms between the summands. Furthermore, the defining ideal I for \mathcal{Y} in $\hat{A}[T.B]$ is contained in the defining ideal I_1 of \mathcal{Y}_1 in $\hat{A}[T.B_1]$, and $I_1 = \bigoplus_{i=0}^{p-1} I r_1^i$ is graded. So $\mathcal{Y}_1 = \hat{A}[T.B_1]/I_1 = \bigoplus_{i=0}^{p-1} \mathcal{Y}_1^i$ and multiplication with y_1 induces \hat{A} -module isomorphisms between the summands on the right. By construction the \hat{A} -basis \mathcal{B} of \mathcal{Y}_1 has the property that $\mathcal{B} = \bigcup_{i=0}^{p-1} (\mathcal{B} \cap \mathcal{Y}_1^i)$, hence $\mathcal{B} \cap \mathcal{Y}$ is an \hat{A} -free generating system of \mathcal{Y} .

Finally assume that $p = e$. Since $G(e, e, 2)$ is a Coxeter group (the dihedral group of order $2e$), by Theorem 5.13 we may assume $n \geq 3$. In this case, the braid group B of $W = G(e, e, n)$ is a normal subgroup of index e of the quotient $\bar{B}_1 = B_1/\langle r_1^e \rangle$ of the braid group of W_1 ; see [Broué et al. 1998, Proposition 3.24]. Thus, \mathcal{Y} is an \hat{A} -subalgebra of $\hat{A}[T.B_1]/I$ where I is generated by $r_1^e - 1$ and the relations (\dagger) for r_2, \dots, r_n . We can now argue precisely as in the previous case. \square

The following was used in the preceding proof:

Lemma 5.15. *Let $\mathcal{Y} = \mathcal{Y}(G(e, 1, n))$ and $y_1, y_2 \in \mathcal{Y}$ images of braid reflections satisfying $y_2 y_1 y_2 y_1 = y_1 y_2 y_1 y_2$ and such that the corresponding reflections $r_1, r_2 \in W$ have order $e, 2$ respectively. Then for all integers $a, b \geq 1$ there exist $\alpha \in \hat{A}[T]^\times$ and $\alpha_i, \alpha'_i \in \hat{A}[T]$ such that*

$$y_2 y_1^a y_2 y_1^b = \alpha y_1^b y_2 y_1^a y_2 + \sum_{i=1}^b (\alpha_i y_1^{a+b-i} y_2 y_1^i + \alpha'_i y_1^i y_2 y_1^{a+b-i}).$$

Proof. Write the relation (†) for y_2 as $y_2^2 = \lambda y_2 + \mu$ with $\mu \in \hat{A}[T]^\times$ and $\lambda \in \hat{A}[T]$, so $y_2^{-1} = \mu^{-1}y_2 - \lambda\mu^{-1}$. The relation between y_1, y_2 implies $y_1^a y_2 y_1 y_2 = y_2 y_1 y_2 y_1^a$ for all $a \geq 1$. Thus we find

$$\begin{aligned} y_2 y_1^a y_2 y_1 &= y_2 y_1^a y_2 y_1 \cdot y_2 y_2^{-1} \\ &= y_2^2 y_1 y_2 y_1^a y_2^{-1} \\ &= (\lambda y_2 + \mu) y_1 y_2 y_1^a (\mu^{-1} y_2 - \lambda \mu^{-1}) \\ &= \mu y_1 y_2 y_1^a y_2 \mu^{-1} + \lambda y_2 y_1 y_2 y_1^a y_2^{-1} - \mu y_1 y_2 y_1^a \lambda \mu^{-1} \\ &= \mu y_1 y_2 y_1^a y_2 \mu^{-1} + \lambda y_1^a y_2 y_1 - \mu y_1 y_2 y_1^a \lambda \mu^{-1} \\ &= \mu' y_1 y_2 y_1^a y_2 + \lambda y_1^a y_2 y_1 - \lambda' y_1 y_2 y_1^a \end{aligned}$$

for suitable $\mu' \in \hat{A}[T]^\times$ and $\lambda' \in \hat{A}[T]$, giving the claim for $b = 1$. For $b = 2$, using the previous result twice we find

$$\begin{aligned} y_2 y_1^a y_2 y_1^2 &= (\mu' y_1 y_2 y_1^a y_2 + \lambda y_1^a y_2 y_1 - \lambda' y_1 y_2 y_1^a) y_1 \\ &= \mu' y_1 y_2 y_1^a y_2 y_1 + \lambda y_1^a y_2 y_1^2 - \lambda' y_1 y_2 y_1^{a+1} \\ &= \mu' y_1 (\mu' y_1 y_2 y_1^a y_2 + \lambda y_1^a y_2 y_1 - \lambda' y_1 y_2 y_1^a) + \lambda y_1^a y_2 y_1^2 - \lambda' y_1 y_2 y_1^{a+1} \\ &= \mu'' y_1^2 y_2 y_1^a y_2 + \sum_{i=1}^2 (\alpha_i y_1^{a+2-i} y_2 y_1^i + \alpha'_i y_1^i y_2 y_1^{a+2-i}) \end{aligned}$$

for suitable $\mu'', \alpha_i, \alpha'_i$. A straightforward induction yields the claim for arbitrary b . □

Remark 5.16. Marin [2018a, Definition 5.4] defines for arbitrary complex reflection groups W an \hat{A} -algebra M attached to W as follows: let \mathcal{L} be the lattice of intersections of the hyperplane arrangement of W . Then M is the quotient of the group algebra over \hat{A} of the semidirect product $\mathcal{L} \rtimes B(W)$ by the deformed order relations (†) for the braid reflections of $B(W)$. This algebra is generated by images of braid reflections r' and idempotents $e_r, r \in W$ a reflection; by [loc. cit., 5.1]. Marin [2018b, Theorem 1.3] shows that M is a free \hat{A} -module of rank $|W||\mathcal{L}|$. If W is ℓ -adic, there is a natural morphism

$$i_W : M \rightarrow \hat{A}[\ell^{-1}] \otimes_{\hat{A}} \mathcal{Y}, \quad r' \mapsto y_r, e_r \mapsto \ell^{-a} E_r,$$

from Marin’s algebra to ours. We expect this to be injective, but in general far from surjective, since his algebra is free of rank independent of ℓ (compare to Theorem 5.7).

5D. A trace form. Assume for the rest of the section that W_θ is a parabolic subgroup of W for all $\theta \in \text{Irr}(T)$; this holds whenever ℓ is very good for (W, L) ; see Remark 5.11. Let K be an extension of \mathbb{Q}_ℓ by the ℓ^a -th roots of unity. Let $\tilde{\mathbf{u}} = (\tilde{u}_{r_j})$ be as in Section 3A and let $\tilde{K} = \text{Frac}(K[\tilde{\mathbf{u}}])$. Recall from Section 3B that for any $\theta \in \text{Irr}(T)$, $\tilde{K} \otimes \mathcal{H}(W_\theta, \mathbf{u}_\theta) \cong \tilde{K} W_\theta$ is split semisimple and the irreducible characters of $\mathcal{H}(W_\theta, \mathbf{u}_\theta)$ over \tilde{K} are identified with $\text{Irr}(W_\theta)$. Here, as before we denote by \mathbf{u}_θ the set \mathbf{u}_0 in the notation of Section 3A if W_θ is the reflection subgroup W_0 . Then, with U a $\tilde{K} \otimes \mathcal{H}(W_\theta, \mathbf{u}_\theta)$ -module affording ϕ and $U_{\theta, \phi} := \text{Ind}_{\hat{B}_\theta}^{\hat{B}}(U)$, Theorem 5.7(a) shows

$$\text{Irr}(\mathcal{Y}_{\tilde{K}}) = \{U_{\theta, \phi} \mid \theta \in \text{Irr}(T)/W, \phi \in \text{Irr}(W_\theta)\}.$$

We let $\chi_{\theta,\phi}$ denote the character of $U_{\theta,\phi}$.

We consider the following nondegenerate trace form $\mathcal{Y} \rightarrow \tilde{K}$:

$$\tau := \tau_{\mathcal{Y}} := \sum_{\theta/W} \sum_{\phi \in \text{Irr}(W_\theta)} \frac{1}{f_{\theta,\phi}} \chi_{\theta,\phi}. \tag{1}$$

Here, for any $\theta \in \text{Irr}(T)$, $f_{\theta,\phi} \in \tilde{A}$ is the Schur element of the Hecke algebra $\mathcal{H}(W_\theta, \mathbf{u}_\theta)$ indexed by ϕ as in Section 3A.

Proposition 5.17. *Assume that W_θ is a parabolic subgroup of W for all $\theta \in \text{Irr}(T)$. Assume also that $\mathcal{H}(W, \mathbf{u})$ is strongly symmetric with respect to $\mathbf{W} \subset B$ as in Definition 3.4. Then we have*

$$\tau(y_t y_{\mathbf{w}}) = \delta_{t,1} \delta_{\mathbf{w},1} |T| \quad \text{for any } t \in T, \mathbf{w} \in \mathbf{W}.$$

Proof. For $\theta \in \text{Irr}(T)$ let C_θ be a system of coset representatives of W_θ in W , and $\mathbf{C}_\theta \subseteq \mathbf{W}$ the corresponding system of coset representatives of $T \cdot \tilde{B}_\theta$ in $T \cdot B$. Let $\theta \in \text{Irr}(T)$ and $\phi \in \text{Irr}(W_\theta)$, and let U be a corresponding representation of $\mathcal{H}(W_\theta, \mathbf{u}_\theta)$ (which we consider as a representation of $\hat{B}_\theta = T \tilde{B}_\theta$ as above). Let us set $U^0(x) := U(x)$ if $x \in T \cdot \tilde{B}_\theta$ and 0 otherwise. Then

$$U_{\theta,\phi}(y_t y_{\mathbf{w}}) = \sum_{\mathbf{x} \in \mathbf{C}_\theta} U^0((y_t y_{\mathbf{w}})^{\mathbf{x}}) = \sum_{\mathbf{x} \in \mathbf{C}_\theta, y_{\mathbf{w}}^{\mathbf{x}} \in \tilde{B}_\theta} \theta(y_t^{\mathbf{x}}) U(y_{\mathbf{w}}^{\mathbf{x}}),$$

so

$$\sum_{\phi \in \text{Irr}(W_\theta)} \frac{1}{f_{\theta,\phi}} \chi_{\theta,\phi}(y_t y_{\mathbf{w}}) = \sum_{\mathbf{x} \in \mathbf{C}_\theta, y_{\mathbf{w}}^{\mathbf{x}} \in \tilde{B}_\theta} \theta(y_t^{\mathbf{x}}) \sum_{\phi \in \text{Irr}(W_\theta)} \frac{1}{f_{\theta,\phi}} \chi_{\theta,\phi}(y_{\mathbf{w}}^{\mathbf{x}}) = \sum_{\mathbf{x} \in \mathbf{C}_\theta, y_{\mathbf{w}}^{\mathbf{x}} \in \tilde{B}_\theta} \theta(y_t^{\mathbf{x}}) t_{W_\theta, \mathbf{u}_\theta}(y_{\mathbf{w}}^{\mathbf{x}})$$

with $t_{W_\theta, \mathbf{u}_\theta}$ as in Definition 3.4. By the choice of \mathbf{W} we have

$$t_{W_\theta, \mathbf{u}_\theta}(y_{\mathbf{w}}^{\mathbf{x}}) = t_{W, \mathbf{u}}(y_{\mathbf{w}}^{\mathbf{x}}) = t_{W, \mathbf{u}}(y_{\mathbf{w}}) = \delta_{\mathbf{w},1}.$$

Thus the form τ evaluates to

$$\tau(y_t y_{\mathbf{w}}) = \sum_{\theta/\mathcal{F}} \sum_{\mathbf{x} \in \mathbf{C}_\theta} \theta(y_t^{\mathbf{x}}) \delta_{\mathbf{w},1} = \sum_{\theta \in \text{Irr}(T)} \theta(y_t) \delta_{\mathbf{w},1} = \delta_{t,1} \delta_{\mathbf{w},1} |T|,$$

as desired. □

It seems natural to ask the following:

Question 5.18. Let (W, L) be a simply connected ℓ -adic reflection group for which ℓ is very good. Does the form $|T|^{-1} \tau$ take values in \hat{A} and is it then a symmetrising form on \mathcal{Y} over \hat{A} ?

Note that an affirmative answer to the first part of Question 5.18 follows under the assumptions of Proposition 5.17.

5E. Relation to classical Yokonuma algebras. Suppose that W is the Weyl group with respect to a maximally split torus T_0 of a connected reductive group G with an \mathbb{F}_q -structure defined by a split Frobenius map $F : G \rightarrow G$. Set $G = G^F$ and set $T_0 = T_0^F$. Let U be the unipotent radical of an F -stable Borel subgroup of G containing T_0 , and let $U = U^F$. Let ℓ be a prime dividing $q - 1$ and set $e_U = |U|^{-1} \sum_{u \in U} u \in \mathbb{Z}_\ell G$. Then

$$\mathcal{Y}' := \text{End}_{\mathbb{Z}_\ell G}(\mathbb{Z}_\ell[G/U]) = e_U \mathbb{Z}_\ell G e_U$$

is the associated classical Yokonuma Hecke algebra [Yokonuma 1967].

Let r_1, \dots, r_m be Coxeter generators of the Weyl group W . For $t \in T_0$, let $t' = e_U t e_U$ and for each i , let $E_i := E_{[T_0, r_i]} e_U$, where for any subgroup $A \leq G$ we denote by E_A the sum of elements of A . By [Juyumaya and Kannan 2001, Theorem 2], \mathcal{Y}' has a generating set $\{t', s_i \mid t \in T_0, 1 \leq i \leq m\}$ such that:

- The t' satisfy the same relations as the corresponding group elements t .
- The action relations between the t, r_i , with t replaced by t' and r_i by s_i hold in \mathcal{Y}' .
- The braid relations between the r_i , with r_i replaced by s_i hold in \mathcal{Y}' .
- $s_i^2 = 1 - q^{-1}(E_i - s_i E_i)$.

Note that Juyumaya–Kannan work over the complex numbers but it can be checked from the explicit description of the s_i s in terms of the standard generators coming from the Bruhat decomposition, that the above holds over any ring in which q is invertible.

Proposition 5.19. *Suppose that there is a W -equivariant isomorphism between T and the Sylow ℓ -subgroup of T_0 . Let H be the ℓ' -Hall subgroup of T_0 , let $e_H = |H|^{-1} E_H$ be the principal block idempotent of $\mathbb{Z}_\ell T_0$ and set $f = e_H e_U$. Let $\psi_q : \hat{A} \rightarrow \mathbb{Z}_\ell$ be the specialisation corresponding to $u_{r_1} \mapsto -1, u_{r_2} \mapsto q$ for all r . Then there is an isomorphism of \mathbb{Z}_ℓ -algebras $\mathcal{Y}_{\psi_q} \cong f \mathcal{Y}' f$.*

Proof. Note that f is an idempotent of $\mathbb{Z}_\ell G$. By considering the generating set of \mathcal{Y}' described above, one sees that f is central in \mathcal{Y}' and for any $x \in H, xf = f$, hence $\{t' f, s_i f \mid t \in T_0, 1 \leq i \leq m\}$ is a generating set for $\mathcal{Y}' f = f \mathcal{Y}' f$.

It follows from the description of \mathcal{Y} via generators and relations given after Lemma 5.3 that there is a surjective \mathbb{Z}_ℓ -algebra homomorphism $\mathcal{Y}_{\psi_q} \rightarrow \mathcal{Y}' f$ which sends the image $\tilde{y}_t \in \mathcal{Y}_{\psi_q}$ of y_t to $(q^{-1} \ell^a / (q - 1)) t' f$ and \tilde{y}_{r_i} to $-s_i f$. By Theorem 5.13, \mathcal{Y}_{ψ_q} is \mathbb{Z}_ℓ -free of rank $|TW|$ and the same is true for $\mathcal{Y}' f$. The last assertion can be seen by considering the standard basis $\{e_U n e_U \mid n \in N_G(T_0)\}$ of \mathcal{Y}' given by the Bruhat decomposition. Thus \mathcal{Y}_{ψ_q} is isomorphic to $f \mathcal{Y}' f$ as claimed. □

5F. Proofs of Theorem 1 and Corollary 2. Throughout this section $\ell > 2$ is a prime, q is a prime power with $q \equiv 1 \pmod{\ell}$ and $a > 0$ such that $\ell^a \parallel (q - 1)$. Let $\mathbb{G} = (W, L)$ be a simply connected \mathbb{Z}_ℓ -spets with W an ℓ' -group. Let \mathcal{F} be the fusion system associated to (W, L) as described in Section 4A, with underlying ℓ -group S . Recall that with the stated assumptions we have $S = T \cong (\mathbb{Z}/\ell^a)^n$ where T is the homocyclic group $L/\ell^a L$ of exponent ℓ^a . We let \mathcal{Y} be the Yokonuma algebra associated to (W, L, q) as in Section 5.

Recall the indeterminates \tilde{u}_{rj} with $\tilde{u}_{rj}^z = \zeta_{o(r)}^{-j} u_{rj}$. By [Malle 1999, Corollary 4.8], z may be chosen to divide the order of the group of roots of unity in \mathbb{Q}_ℓ , that is, $\ell - 1$. As $\ell^a \parallel (q - 1)$, by Hensel's lemma there is a unique root of $X^z - q \in \mathbb{Z}_\ell[X]$ in \mathbb{Z}_ℓ , say $q^{1/z}$, with $\ell^a \parallel (q^{1/z} - 1)$. Let $\mathbb{Z}_\ell \subseteq \mathcal{O}$ be a complete discrete valuation ring containing the $|T|$ -th roots of unity. Let

$$\psi_{s,q} : \mathcal{O}[\tilde{\mathbf{u}}^{\pm 1}] \rightarrow \mathcal{O}, \quad \tilde{u}_{rj} \mapsto \begin{cases} q^{1/z} & \text{if } j = o(r), \\ 1 & \text{if } 1 \leq j < o(r), \end{cases}$$

be the specialisation $\psi_{s,q}$ from Section 3B with $R = \mathcal{O}$. Since $|T_r|$ divides ℓ^a , $\psi_{s,q}$ extends to an \mathcal{O} -linear homomorphism $\mathcal{O}[\tilde{\mathbf{u}}^{\pm 1}, \mathbf{v}] \rightarrow \mathcal{O}$ which we still denote $\psi_{s,q}$. Let $\tilde{K} = \text{Frac}(\mathcal{O}[\tilde{\mathbf{u}}^{\pm 1}])$ and $K = \text{Frac}(\mathcal{O})$.

We restate Theorem 1.

Theorem 5.20. *Let \mathbb{G} be as above. Suppose that $\mathcal{H}(W, \mathbf{u})$ is strongly symmetric as in Definition 3.4. Then Conjectures 4.2, 4.3 and 4.5 hold for \mathbb{G} .*

Proof. Let W_0 be a reflection subgroup of W . By Lemma 3.7, $K \otimes_{\mathcal{O}} \mathcal{H}_{\psi_{s,q}}(W_0, \mathbf{u}_0)$ is split semisimple and $\psi_{s,q}$ induces a bijection $\text{Irr}(\tilde{K} \otimes_A \mathcal{H}(W_0, \mathbf{u}_0)) \rightarrow \text{Irr}(K \otimes_{\mathcal{O}} \mathcal{H}_{\psi_{s,q}}(W_0, \mathbf{u}_0))$. Also recall from Section 3B, $\text{Irr}(\tilde{K} \otimes_A \mathcal{H}(W_0, \mathbf{u}_0))$ is identified with $\text{Irr}(W_0)$ via ψ_1 . Henceforth we identify $\text{Irr}(K \otimes_{\mathcal{O}} \mathcal{H}_{\psi_{s,q}}(W_0, \mathbf{u}_0))$ and $\text{Irr}(W_0)$ via the bijections induced by $\psi_{s,q}$ and ψ_1 .

Denoting the restriction of $\psi_{s,q}$ to \hat{A} again by $\psi_{s,q}$, set $\mathcal{Y}_q := \mathcal{Y}_{\psi_{s,q}}$. Since W is an ℓ' -group, W_θ is a parabolic subgroup of W for all $\theta \in \text{Irr}_K(T)$. Then by Theorem 5.7(a) and the above $K \otimes_{\mathcal{O}} \mathcal{Y}_q$ is split semisimple and $\text{Irr}(K \otimes_{\mathcal{O}} \mathcal{Y}_q)$ is in bijection with pairs (θ, ϕ) as θ runs over representatives of W -orbits of $\text{Irr}(T)$ and $\phi \in \text{Irr}(W_\theta)$. Let $\chi'_{\theta,\phi}$ be the irreducible character corresponding to the pair (θ, ϕ) . Then $\chi'_{\theta,\phi}$ is afforded by the simple module $U'_{\theta,\phi} := \text{Ind}_{\hat{B}_\theta}^{\hat{B}}(U)$ for U a simple $K \otimes_{\mathcal{O}} \mathcal{H}_{\psi_{s,q}}(W_\theta, \mathbf{u}_\theta)$ -module corresponding to ϕ . Here as in Section 5D, $\mathbf{u}_\theta = \mathbf{u}_0$ in the notation of Section 3A if $W_\theta = W_0$.

We consider the following K -linear form on $K \otimes_{\mathcal{O}} \mathcal{Y}_q$:

$$\tau_q := \frac{1}{|T|} \sum_{\theta/W} \sum_{\phi \in \text{Irr}(W_\theta)} \frac{1}{\psi_{s,q}(f_{\theta,\phi})} \chi'_{\theta,\phi}. \tag{2}$$

By Lemma 3.6 this is well defined. Since the coefficient of every irreducible character is nonzero, τ_q is a symmetrising form on $K \otimes_{\mathcal{O}} \mathcal{Y}_q$ with Schur elements $|T| \psi_{s,q}(f_{\theta,\phi})$.

Let $\mathbf{W} \subset B(W)$ be as in Definition 3.4. By Theorem 5.9, $\{\tilde{y}_t \tilde{y}_w \mid t \in T, w \in \mathbf{W}\}$ is an \mathcal{O} -basis of \mathcal{Y}_q . Here, as earlier, for $x \in \mathcal{Y}$, we write $\tilde{x} := 1_{\mathcal{O}} \otimes x \in \mathcal{Y}_q$. As in Proposition 5.17, we have

$$\tau_q(\tilde{y}_t \tilde{y}_w) = \delta_{t,1} \delta_{w,1} \quad \text{for any } t \in T, w \in \mathbf{W},$$

hence the above gives that the restriction of τ_q to \mathcal{Y}_q takes values in \mathcal{O} .

By the strongly symmetric hypothesis, and by Theorem 5.10 there is an \mathcal{O} -algebra isomorphism $\sigma : \mathcal{O}[TW] \rightarrow \mathcal{Y}_q$ whose restriction to T is the identity on T (where we identify T with its image in \mathcal{Y}_q via $t \mapsto \tilde{y}_t, t \in T$). Denote also by σ the extension $K[TW] \rightarrow K \otimes_{\mathcal{O}} \mathcal{Y}_q$. Then $\tau_\sigma := \tau_q \circ \sigma : K[TW] \rightarrow K$ is a symmetrising form on $K[TW]$, with Schur element $|T| \psi_{s,q}(f_{\theta,\phi})$ at the irreducible character of

$K[TW]$ corresponding under σ to the character $\chi'_{\theta, \phi}$ of $K \otimes_{\mathcal{O}} \mathcal{Y}_q$. Further, by the above $\tau_{\sigma}(t) = \delta_{t,1}$ for all $t \in T$ and the restriction of $\tau\sigma$ to $\mathcal{O}[TW]$ takes values in \mathcal{O} . Thus, by Lemmas 2.5 and 2.6,

$$\frac{1}{|T|^2} \sum_{\theta/W} \sum_{\phi \in \text{Irr}(W_{\theta})} \frac{1}{\psi_{s,q}(f_{\theta, \phi}^2)} = \frac{\alpha}{|TW|},$$

where $\alpha \in \mathcal{O}$ is such that $\alpha \equiv 1 \pmod{\ell}$.

Recall that $S = T$ and as explained in Section 4B, there exists a W -equivariant bijection between $\text{Irr}(T)$ and T . Thus the left hand side of the above equals

$$\frac{\psi_{s,q}(d)}{|T|^2 \psi_{s,q}(p_W^2)},$$

where $d := \sum_{s/\mathcal{F}} \sum_{\phi \in \text{Irr}(W(s))} p_W^2 f_{s, \phi}^{-2}$. By Lemma 4.10, $\psi_{s,q}(d) = \dim(B_0)|_{x=q}$. Since $\psi_{s,q}(p_W) \equiv |W| \pmod{\ell}$, we obtain the validity of Conjectures 4.2 and 4.3 from the displayed equation above.

Finally, we prove Conjecture 4.5. First of all note that since σ is the identity on T , for any pair (θ, ϕ) as above the irreducible character of $K[TW]$ corresponding under σ to the character $\chi'_{\theta, \phi}$ of $K \otimes_{\mathcal{O}} \mathcal{Y}_q$ covers θ and therefore is of the form $\gamma_{\theta, \tilde{\phi}} := \text{Ind}_{W_{\theta}}^W(\tilde{\phi})$ for some $\tilde{\phi} \in \text{Irr}(W_{\theta})$. In particular, σ induces a permutation $\phi \mapsto \tilde{\phi}$ of $\text{Irr}(W_{\theta})$. By Proposition 2.7 we have that for any $\nu \in \text{IBr}(TW)$,

$$\sum_{\theta/W} \sum_{\phi \in \text{Irr}(W_{\theta})} \frac{d_{\gamma_{\theta, \tilde{\phi}} \nu}}{\psi_{s,q}(f_{\theta, \phi})}$$

is divisible by $|T|$ in \mathcal{O} . Choose a W -equivariant bijection between $\text{Irr}(T)$ and T and let $\Theta : \text{Irr}(TW) \rightarrow \text{Irr}(B_0)$, $\gamma \mapsto \hat{\gamma}$, be the bijection such that if $\gamma = \text{Ind}_{W_{\theta}}^W(\tilde{\phi})$, then $\hat{\gamma}$ is the element of $\text{Irr}(B_0)$ labelled by (x, ϕ) , where the W -class of $x \in T$ corresponds to the W -class of θ for the chosen W -equivariant bijection between $\text{Irr}(T)$ and T . Then Θ is W -equivariant. Moreover, by Lemma 4.10 the above displayed expression equals $\psi_{s,q}(p_W)^{-1}(\deg \Phi_{\hat{\nu}})|_{x=q}$. The result follows since $\psi_{s,q}(p_W)$ is an invertible element of \mathcal{O} . □

Remark 5.21. The above holds in a more general setting. Drop the assumption that W is spetsial; so W is an ℓ -adic reflection group of order prime to ℓ . Let $\psi_q : \mathcal{O}[\tilde{\mathbf{u}}^{\pm 1}, \mathbf{v}] \rightarrow \mathcal{O}$ be any specialisation as in Section 3B. Suppose that $\tau : \mathcal{H}(W, \mathbf{u}) \rightarrow A$ is a symmetrising form such that the following holds:

- (1) There is a section $W \rightarrow \mathbf{W} \subset B$ of the natural map $B \rightarrow W$ containing 1 whose image in $\mathcal{H}(W, \mathbf{u})$ is an A -basis of $\mathcal{H}(W, \mathbf{u})$ with $\tau(h_{\mathbf{w}}) = \delta_{\mathbf{w},1}$ for all $\mathbf{w} \in \mathbf{W}$.
- (2) For any parabolic subgroup $W_0 \leq W$, $\tau|_{\mathcal{H}(W_0, \mathbf{u}_0)} : \mathcal{H}(W_0, \mathbf{u}_0) \rightarrow A$ is a symmetrising form.

For $s \in S$, $\phi \in \text{Irr}(W(s))$ let $f_{\tau, s, \phi}$ denote the Schur element of $\tau|_{\mathcal{H}(W_0, \mathbf{u}_0)}$ with respect to ϕ where $W_0 = W(s)$. Set

$$d := \sum_{s/\mathcal{F}} \sum_{\phi \in \text{Irr}(W(s))} \frac{p_W^2}{f_{\tau, s, \phi}^2}$$

and for $\nu \in \text{IBr}(SW)$ set

$$\Phi_\nu(1) := \sum_{\gamma \in \text{Irr}(SW)} d_{\gamma\nu} \frac{p_W}{f_{\tau,s,\phi}},$$

where $d_{\gamma\nu}$ is the decomposition number in SW with respect to γ and ν . Then with the same proof as above we get:

- (a) $\psi_{s,q}(d)_\ell = |S|$.
- (b) $\psi_{s,q}(d)/(\psi_{s,q}(p_W)|S|) \equiv 1 \pmod{\ell}$.
- (c) For each $\nu \in \text{IBr}(SW)$, $|S|$ divides $\psi_{s,q}(\Phi_\nu(1))$.

Proof of Corollary 2. By [Malle 1998, Section 3] all imprimitive irreducible spetsial reflection groups are either Coxeter groups, of type $G(e, 1, n)$ or of type $G(e, e, n)$ with $n \geq 3$ and therefore strongly symmetric by Proposition 3.5. Therefore Conjectures 1 and 2 hold for these groups by Theorem 5.20. For the primitive groups, Conjecture 1 holds by Proposition 4.8. Conjecture 2 holds when W is primitive and 2-dimensional by Proposition 3.5(c) and Theorem 5.20; for G_{14} Conjecture 2 holds by direct computation using the description of the decomposition matrix provided in the proof of Proposition 4.11. \square

Acknowledgement

We thank Maria Chlouveraki for providing pointers to results in [Lusztig 2005, Section 34], Markus Linckelmann for useful discussions on several aspects of the paper and in particular on the proof of Theorem 5.10 and Burkhard Külshammer for providing background and references for Proposition 2.8. We are indebted to Ivan Marin and Jean Michel for their pertinent comments on an earlier version. We also thank the referee for numerous constructive comments and recommendations which have helped to improve the readability of the paper.

References

- [Bessis 2001] D. Bessis, “Zariski theorems and diagrams for braid groups”, *Invent. Math.* **145**:3 (2001), 487–507. MR Zbl
- [Boura et al. 2020] C. Boura, E. Chavli, M. Chlouveraki, and K. Karvounis, “The BMM symmetrising trace conjecture for groups G_4, G_5, G_6, G_7, G_8 ”, *J. Symbolic Comput.* **96** (2020), 62–84. MR Zbl
- [Bremke and Malle 1997] K. Bremke and G. Malle, “Reduced words and a length function for $G(e, 1, n)$ ”, *Indag. Math. (N.S.)* **8**:4 (1997), 453–469. MR Zbl
- [Broto and Møller 2007] C. Broto and J. M. Møller, “Chevalley p -local finite groups”, *Algebr. Geom. Topol.* **7** (2007), 1809–1919. MR Zbl
- [Broué and Malle 1993] M. Broué and G. Malle, “Zyklotomische Heckealgebren”, pp. 119–189 in *Représentations unipotentes génériques et blocs des groupes réductifs finis*, Astérisque **212**, Société Mathématique de France, Paris, 1993. MR Zbl
- [Broué et al. 1998] M. Broué, G. Malle, and R. Rouquier, “Complex reflection groups, braid groups, Hecke algebras”, *J. Reine Angew. Math.* **500** (1998), 127–190. MR
- [Broué et al. 1999] M. Broué, G. Malle, and J. Michel, “Towards spetses, I”, *Transform. Groups* **4**:2-3 (1999), 157–218. MR Zbl
- [Broué et al. 2014] M. Broué, G. Malle, and J. Michel, “Split spetses for primitive reflection groups”, pp. vi+146 in *Journées de Géométrie Algébrique d’Orsay*, Astérisque **359**, Société Mathématique de France, Paris, 2014. MR Zbl

- [Cabanes 2018] M. Cabanes, “Local methods for blocks of finite simple groups”, pp. 179–265 in *Local representation theory and simple groups*, edited by R. Kessar et al., Eur. Math. Soc., Zürich, 2018. MR Zbl
- [Chavli 2018] E. Chavli, “The BMR freeness conjecture for the tetrahedral and octahedral families”, *Comm. Algebra* **46**:1 (2018), 386–464. MR Zbl
- [Chavli and Chlouveraki 2022] E. Chavli and M. Chlouveraki, “The freeness and trace conjectures for parabolic Hecke subalgebras”, *J. Pure Appl. Algebra* **226**:10 (2022), Paper No. 107050, 29. MR Zbl
- [Chlouveraki 2009] M. Chlouveraki, *Blocks and families for cyclotomic Hecke algebras*, Lecture Notes in Mathematics **1981**, Springer, 2009. MR Zbl
- [Chlouveraki and d’Andecy 2016] M. Chlouveraki and L. P. d’Andecy, “Markov traces on affine and cyclotomic Yokonuma–Hecke algebras”, *Int. Math. Res. Not.* **2016**:14 (2016), 4167–4228. MR Zbl
- [Curtis and Reiner 1981] C. W. Curtis and I. Reiner, *Methods of representation theory, I: With applications to finite groups and orders*, Wiley, New York, 1981. MR Zbl
- [Dwyer and Wilkerson 1994] W. G. Dwyer and C. W. Wilkerson, “Homotopy fixed-point methods for Lie groups and finite loop spaces”, *Ann. of Math. (2)* **139**:2 (1994), 395–442. MR Zbl
- [Eisele et al. 2018] F. Eisele, M. Geline, R. Kessar, and M. Linckelmann, “On Tate duality and a projective scalar property for symmetric algebras”, *Pacific J. Math.* **293**:2 (2018), 277–300. MR Zbl
- [Geck and Pfeiffer 2000] M. Geck and G. Pfeiffer, *Characters of finite Coxeter groups and Iwahori–Hecke algebras*, London Mathematical Society Monographs. New Series **21**, Oxford University Press, New York, 2000. MR Zbl
- [Geck et al. 2000] M. Geck, L. Iancu, and G. Malle, “Weights of Markov traces and generic degrees”, *Indag. Math. (N.S.)* **11**:3 (2000), 379–397. MR Zbl
- [Grodal 2010] J. Grodal, “The classification of p -compact groups and homotopical group theory”, pp. 973–1001 in *Proceedings of the International Congress of Mathematicians, Volume II*, edited by R. Bhatia et al., Hindustan Book Agency, New Delhi, 2010. MR Zbl
- [Juyumaya and Kannan 2001] J. Juyumaya and S. S. Kannan, “Braid relations in the Yokonuma–Hecke algebra”, *J. Algebra* **239**:1 (2001), 272–297. MR Zbl
- [Kessar et al. 2020] R. Kessar, G. Malle, and J. Semeraro, “Weight conjectures for ℓ -compact groups and spetses”, preprint, 2020. arXiv 2008.07213
- [Linckelmann 2018] M. Linckelmann, *The block theory of finite group algebras, Vol. I*, London Mathematical Society Student Texts **91**, Cambridge University Press, 2018. MR Zbl
- [Lusztig 2005] G. Lusztig, “Character sheaves on disconnected groups, VII”, *Represent. Theory* **9** (2005), 209–266. MR Zbl
- [Malle 1995] G. Malle, “Unipotente Grade imprimitiver komplexer Spiegelungsgruppen”, *J. Algebra* **177**:3 (1995), 768–826. MR Zbl
- [Malle 1997] G. Malle, “Degrés relatifs des algèbres cyclotomiques associées aux groupes de réflexions complexes de dimension deux”, pp. 311–332 in *Finite reductive groups* (Luminy, 1994), edited by M. Cabanes, Progr. Math. **141**, Birkhäuser, Boston, 1997. MR Zbl
- [Malle 1998] G. Malle, “Spetses”, pp. 87–96 in *Proceedings of the International Congress of Mathematicians* (Berlin, 1998), vol. 2, Doc. Math. Extra Vol. **II**, 1998. MR Zbl
- [Malle 1999] G. Malle, “On the rationality and fake degrees of characters of cyclotomic algebras”, *J. Math. Sci. Univ. Tokyo* **6**:4 (1999), 647–677. MR Zbl
- [Malle 2000] G. Malle, “On the generic degrees of cyclotomic algebras”, *Represent. Theory* **4** (2000), 342–369. MR Zbl
- [Malle 2006] G. Malle, “Splitting fields for extended complex reflection groups and Hecke algebras”, *Transform. Groups* **11**:2 (2006), 195–216. MR Zbl
- [Malle 2007] G. Malle, “Height 0 characters of finite groups of Lie type”, *Represent. Theory* **11** (2007), 192–220. MR Zbl
- [Malle and Mathas 1998] G. Malle and A. Mathas, “Symmetric cyclotomic Hecke algebras”, *J. Algebra* **205**:1 (1998), 275–293. MR Zbl
- [Marin 2018a] I. Marin, “Artin groups and Yokonuma–Hecke algebras”, *Int. Math. Res. Not.* **2018**:13 (2018), 4022–4062. MR Zbl

- [Marin 2018b] I. Marin, “Lattice extensions of Hecke algebras”, *J. Algebra* **503** (2018), 104–120. MR Zbl
- [Marin 2019] I. Marin, “Proof of the BMR conjecture for G_{20} and G_{21} ”, *J. Symbolic Comput.* **92** (2019), 1–14. MR Zbl
- [Orlik and Solomon 1982] P. Orlik and L. Solomon, “Arrangements defined by unitary reflection groups”, *Math. Ann.* **261**:3 (1982), 339–357. MR Zbl
- [Puig 1994] L. Puig, “On Joanna Scopes’ criterion of equivalence for blocks of symmetric groups”, *Algebra Colloq.* **1**:1 (1994), 25–55. MR Zbl
- [Tsuchioka 2020] S. Tsuchioka, “BMR freeness for icosahedral family”, *Exp. Math.* **29**:2 (2020), 234–245. MR Zbl
- [Yokonuma 1967] T. Yokonuma, “Sur la structure des anneaux de Hecke d’un groupe de Chevalley fini”, *C. R. Acad. Sci. Paris Sér. A-B* **264** (1967), A344–A347. MR Zbl

Communicated by Pham Huu Tiep

Received 2021-06-30 Revised 2022-03-09 Accepted 2022-04-11

radha.kessar.1@city.ac.uk

*Department of Mathematics, City, University of London, London,
United Kingdom*

malle@mathematik.uni-kl.de

Fachbereich Mathematik, TU Kaiserslautern, Kaiserslautern, Germany

jpgs1@leicester.ac.uk

*Heilbronn Institute for Mathematical Research, Department of Mathematics,
University of Leicester, Leicester, United Kingdom*

Geometric properties of the Kazhdan–Lusztig Schubert basis

Cristian Lenart, Changjian Su, Kirill Zainoulline and Changlong Zhong

We study classes determined by the Kazhdan–Lusztig basis of the Hecke algebra in the K -theory and hyperbolic cohomology theory of flag varieties. We first show that, in K -theory, the two different choices of Kazhdan–Lusztig bases produce dual bases, one of which can be interpreted as characteristic classes of the intersection homology mixed Hodge modules. In equivariant hyperbolic cohomology, we show that if the Schubert variety is smooth, then the class it determines coincides with the class of the Kazhdan–Lusztig basis; this property was known as the smoothness conjecture. For Grassmannians, we prove that the classes of the Kazhdan–Lusztig basis coincide with the classes determined by Zelevinsky’s small resolutions. These properties of the so-called KL Schubert basis show that it is the closest existing analogue to the Schubert basis for hyperbolic cohomology; the latter is a very useful testbed for more general elliptic cohomologies.

1. Introduction	435
2. Formal affine Demazure algebra and its dual	438
3. Hecke algebra, motivic Chern class, and the smoothness criterion	443
4. Dual bases in K -theory and characteristic classes of mixed Hodge modules	446
5. The smoothness conjecture for hyperbolic cohomology	451
6. KL Schubert classes and small resolutions	455
Acknowledgements	462
References	462

1. Introduction

Let G be a split semisimple linear algebraic group with a fixed Borel subgroup B and a maximal torus $T \subset B$. Let P be a parabolic subgroup containing the Borel subgroup B . The varieties G/P and G/B are called flag varieties, and they are among the most concrete objects in algebraic geometry, because of the Bruhat decompositions. For instance, the equivariant cohomology (Chow group) of flag varieties is freely spanned by the classes of Schubert varieties $X(w)$. Similarly, the equivariant K -theory of flag varieties is spanned by the structure sheaves of Schubert varieties. The field of studying intersection theory of these classes is called Schubert calculus, and is related to combinatorics, representation theory, and enumerative geometry.

MSC2020: primary 14M15, 55N20; secondary 05E99, 19L47, 20C08.

Keywords: Schubert calculus, flag variety, K -theory, hyperbolic cohomology, Hecke algebra, Kazhdan–Lusztig Schubert basis.

Due to the failure of Schubert varieties being smooth, the present paper deals with two different directions in generalizing classical Schubert calculus. The first one is concerned with the Chern classes. Although the classical Chern class theory does not work for the singular Schubert varieties, there are generalizations to this case, which are called Chern–Schwartz–MacPherson (CSM) classes [MacPherson 1974; Schwartz 1965a; 1965b] in homology and motivic Chern (MC) classes in K -theory [Brasselet et al. 2010; Aluffi et al. 2019; Fehér et al. 2021]. These generalized Chern classes of Schubert cells are closely related to the corresponding stable bases of the cotangent bundle T^*G/B , defined by Maulik and Okounkov [2019; 2017] in their study of quantum cohomology/ K -theory of Nakajima quiver varieties. These classes are permuted by various Demazure–Lusztig operators [Aluffi and Mihalcea 2016; Aluffi et al. 2017; 2019; Su 2017; Su et al. 2020; Mihalcea et al. 2022], and are related to unramified principal series representations of the Langlands dual group over a nonarchimedean local field [Su et al. 2020; Aluffi et al. 2019].

We focus on the Kazhdan–Lusztig bases of the Hecke algebra, which are related to the intersection cohomology of Schubert varieties. Classically, there are two choices of Kazhdan–Lusztig bases. In this paper, we consider the K -theory classes determined by these two collections of Kazhdan–Lusztig bases. The cohomology case is studied in [Mihalcea and Singh 2020]. We first show that they are dual to each other in Theorems 13 and 22. These dualities are closely related to the characteristic classes of mixed Hodge modules, studied by J. Schürmann and his collaborators [Schürmann 2011; 2017; Brasselet et al. 2010]. Moreover, we interpret one collection of these classes as the motivic Hodge Chern classes of the intersection homology mixed Hodge modules of the Schubert varieties, which immediately implies that they are invariant under the Serre–Grothendieck duality; see Proposition 17 and Corollary 19.

The other direction is to look at more general cohomology theories, namely the equivariant oriented cohomology theories of Levine and Morel. They are those contravariant functors \mathbf{h}_T from the category of smooth (quasi)projective varieties to the category of commutative rings such that for any proper map of varieties, a pushforward of the cohomology groups is defined. One can then define Chern classes, where the first Chern class of the tensor product of line bundles determines a one-dimensional commutative formal group law. The structure of the equivariant oriented cohomology of flag varieties is studied in [Calmès et al. 2016; 2019; 2015; Lenart et al. 2020]. Roughly speaking, there is an algebra generated by push–pull operators between $\mathbf{h}_T(G/B)$ and $\mathbf{h}_T(G/P)$, called the formal affine Demazure algebra \mathbf{D}_F , whose dual \mathbf{D}_F^* is isomorphic to $\mathbf{h}_T(G/B)$.

Since Schubert varieties are not smooth in general, their fundamental classes are not defined beyond the Chow group and K -theory. To resolve the singularities of a Schubert variety $X(w)$, one often uses the Bott–Samelson resolution, which is defined by fixing a reduced decomposition of the Weyl group element w . For an oriented cohomology beyond singular cohomology/ K -theory, the classes determined by such resolutions depend on the choice of the reduced decomposition. This corresponds to the fact that, for general \mathbf{h}_T , the push–pull operators do not satisfy the braid relations [Hoffnung et al. 2014]. Because of this fact, there are no canonically defined Schubert classes.

Aiming for the definition of Schubert classes, in [Lenart and Zainoulline 2017; Lenart et al. 2020], the authors consider the so-called hyperbolic cohomology, denoted by \mathfrak{h} . This corresponds to a 2-parameter

Todd genus, and is the first interesting case after K -theory in terms of complexity. A Riemann–Roch type map is defined from K -theory to the hyperbolic cohomology theory, which induces an action of the Hecke algebra (considered on the K -theory side) on the hyperbolic cohomology of G/B . In this way, the action of the Kazhdan–Lusztig basis defines classes KL_w in $\mathfrak{h}_T(G/B)$, called KL Schubert classes. In [Lenart and Zainoulline 2017; Lenart et al. 2020], there is a conjecture stating that, if the Schubert variety $X(w)$ is smooth, then its fundamental class coincides with the class KL_w . This conjecture is proved in those works in some special cases. Our first main result proves this conjecture in full generality:

Theorem 28. *If the Schubert variety $X(w)$ is smooth, then the class determined by $X(w)$ in $\mathfrak{h}_T(G/B)$ coincides with the KL Schubert class KL_w .*

The idea of the proof is as follows: if $X(w)$ is smooth, then all the Kazhdan–Lusztig polynomials $P_{y,w}$ for any $y \leq w$ are equal to 1, so the Kazhdan–Lusztig basis for w is the sum of the Demazure–Lusztig operators. As mentioned above, the MC classes of Schubert cells in K -theory are permuted by the Demazure–Lusztig operators. So the MC class of $X(w)$ coincides with the KL class in K -theory, and the restriction formula for the former is obtained in [Aluffi et al. 2019] by generalizing a result of Kumar [1996]. By using the Riemann–Roch type map from K -theory to hyperbolic cohomology, we compare the restriction formulas of the class KL_w and of the class of the smooth Schubert variety $X(w)$, and prove the smoothness conjecture (Theorem 28). For partial flag varieties, a similar property is also proved.

As mentioned above, the Kazhdan–Lusztig basis defines classes in the K -theory of flag varieties, but they do not coincide with the fundamental classes of Schubert varieties, whether smooth or not. However, in $\mathfrak{h}_T(G/B)$, our Theorem 28 shows that, for smooth Schubert varieties, their fundamental classes coincide with the classes defined by the Kazhdan–Lusztig basis. It is unclear to us why such phenomena appear, and we hope to explore this in a future project.

Restricting to type A Grassmannians, we prove more geometric and combinatorial properties. For example, Zelevinsky constructed small resolutions of all Schubert varieties [Zelevinskiĭ 1983]. Our second main result is the following:

Theorem 42. *The KL Schubert classes for the Grassmannian coincide with the hyperbolic cohomology classes of the corresponding Zelevinsky resolutions.*

To prove this theorem, note that Zelevinsky’s small resolutions are similar to the Bott–Samelson resolutions, except that, instead of using minimal parabolic subgroups, one considers more general parabolic subgroups. So the small resolution classes can be computed by using relative push–pull operators between hyperbolic cohomology of G/P and G/Q . These operators were studied in [Calmès et al. 2019]. On the other hand, in [Kirillov and Lascoux 2000], a factorization of the Kazhdan–Lusztig basis elements for Grassmannians is exhibited. By carefully transforming this factorization, one can write the Kazhdan–Lusztig basis elements as products of “relative” Kazhdan–Lusztig elements. Finally, by identifying the latter with the relative push–pull operators, one proves Theorem 42. By the uniqueness of the Kazhdan–Lusztig basis, it follows that all small resolution classes are the same.

There have been important developments in Schubert calculus for general cohomology theories. More specifically, for elliptic cohomology, a stable basis in the cotangent bundle T^*G/B was defined (see [Aganagic and Okounkov 2021; Okounkov 2021], which generalizes stable bases for cohomology and K -theory), and canonical classes were associated with Bott–Samelson resolutions of Schubert varieties [Rimányi and Weber 2020; Kumar et al. 2020]. The elliptic cohomology used in the latter papers can be considered as the oriented cohomology theory associated with a certain elliptic formal group law determined by the Jacobi theta functions; meanwhile, the mentioned cohomology classes are elliptic analogues of the CSM classes in ordinary cohomology and the MC classes in K -theory. On the other hand, the hyperbolic formal group law we consider here comes from a singular cubic curve (in Weierstrass form), so it is a singular elliptic formal group law; see [Buchstaber and Bunkova 2010]. The properties of the KL Schubert basis proved in this paper (namely, the smoothness conjecture and the interpretation in terms of the Zelevinsky small resolutions) show that this basis is the closest existing analogue to the Schubert basis for hyperbolic cohomology. Furthermore, the latter is a very useful testbed for more general elliptic cohomologies.

The paper is organized as follows. In Section 2, we recall the algebraic construction of the equivariant oriented cohomology of flag varieties. In Section 3, we recall basic facts about the Hecke algebra, MC classes, and the smoothness criterion. In Section 4, we use Kazhdan–Lusztig bases to define the two collections of KL classes in $K_T(G/B)$ and $K_T(G/P)$, and show that they are dual to each other. We also give a geometric interpretation for one of them using mixed Hodge modules. In Section 5, we recall the definition of KL Schubert classes in hyperbolic cohomology, and prove the smoothness conjecture. In Section 6, we prove Theorem 42, which connects small resolutions for Grassmannians with the corresponding KL Schubert classes.

2. Formal affine Demazure algebra and its dual

We recall the definition of the formal affine Demazure algebra and its relation with equivariant generalized (oriented) cohomology of flag varieties following [Hoffnung et al. 2014; Calmès et al. 2016; 2019] and especially the paper [Calmès et al. 2015].

Notation. Let G be a semisimple simply connected linear algebraic group over \mathbb{C} , and fix B a Borel subgroup with a maximal torus $T \subset B$. Let $X^*(T)$ denote the character lattice of T . Let $W = N_G(T)/T$ be the Weyl group.

Let Σ denote the set of associated roots and let Σ^+ denote the subset of roots in B . For any root α , let $\alpha > 0$ (resp. $\alpha < 0$) denote $\alpha \in \Sigma^+$ (resp. $-\alpha \in \Sigma^+$).

Let $\Pi = \{\alpha_1, \dots, \alpha_n\}$ denote the set of simple roots. Let $\ell: W \rightarrow \mathbb{Z}$ denote the length function. For any $J \subset \Pi$, denote by W_J the parabolic subgroup corresponding to J , by w_J its longest element, and by W^J (resp. ${}^J W$) the set of minimal length representatives of left (resp. right) cosets W/W_J (resp. $W_J \backslash W$). Specifically, $w_0 := w_\Pi \in W$ is the longest element. More generally, if $J' \subset J \subset \Pi$, write $w_{J/J'} := w_J w_{J'} \in W^{J'}$ (resp. $w_{J' \setminus J} := w_{J'} w_J$), that is, $w_{J/J'}$ (resp. $w_{J' \setminus J}$) is the maximal element

(in terms of the Bruhat order) in the set $W_J \cap W^{J'}$ (resp. $W_J \cap J'W$). Write $\Sigma_J := \{\alpha \in \Sigma \mid s_\alpha \in W_J\}$ and $\Sigma_J^\pm := \Sigma_J \cap \Sigma^\pm$. Throughout the paper, we use the notation \setminus for right cosets, not set difference, which is denoted by $-$.

Formal group algebra. Let F be a one-dimensional formal group law over a commutative unital ring R . The formal group algebra $R[[X^*(T)]]_F$ is defined to be the quotient of the completion

$$R[[x_\lambda \mid \lambda \in X^*(T)]]/\mathcal{I}_F,$$

where \mathcal{I}_F is the closure of the ideal generated by $\langle x_0, F(x_\lambda, x_\mu) - x_{\lambda+\mu} \mid \lambda, \mu \in X^*(T) \rangle$. For simplicity it will be denoted by S . It can be shown that if $\{\omega_1, \dots, \omega_n\}$ is a basis of $X^*(T)$, then S is (noncanonically) isomorphic to $R[[\omega_1, \dots, \omega_n]]$.

Localized twisted group ring. Let $Q = S[(1/x_\alpha) \mid \alpha > 0]$, and $Q_W = Q \otimes_R R[W]$. Denote the canonical left Q -basis of Q_W by $\delta_w, w \in W$, and define a product on Q_W by

$$(p\delta_w) \cdot (p'\delta_{w'}) := pw(p')\delta_{ww'} \quad \text{for } p, p' \in Q, w, w' \in W.$$

In particular, we have $\delta_v p = v(p)\delta_v$ for $p \in Q$.

Push-pull elements. For each root α , define the formal push–pull element

$$Y_\alpha := (1 + \delta_{s_\alpha}) \frac{1}{x_{-\alpha}} \in Q_W.$$

For any reduced word $w = s_{i_1} \cdots s_{i_k}$, where s_i is the simple reflection corresponding to the i -th simple root in Π , define $I_w = (i_1, \dots, i_k)$, and $Y_{I_w} = Y_{\alpha_{i_1}} \cdots Y_{\alpha_{i_k}}$. The product Y_{I_w} depends on the choice of the reduced sequence, unless the formal group law F is of the form $x + y + \beta xy$ with $\beta \in R$. For simplicity, write $\delta_i := \delta_{s_i}, Y_i := Y_{\alpha_i}$ and $x_{\pm i} := x_{\pm\alpha_i}$.

Formal affine Demazure algebra. Let \mathbf{D}_F be the subring of Q_W generated by elements of S and push–pull elements Y_i for $i = 1, \dots, n$. This is called the formal affine Demazure algebra. It is proved in [Calmès et al. 2016] that \mathbf{D}_F is a free left S -module with basis $\{Y_{I_w} \mid w \in W\}$.

Example 1. If $R = \mathbb{Z}$ and $F_m(x, y) = x + y - xy$ (multiplicative formal group law), then

$$S \cong \mathbb{Z}[X^*(T)]^\wedge, \quad x_\alpha \mapsto 1 - e^{-\alpha},$$

where the completion is taken with respect to the kernel of the augmentation map $e^\lambda \mapsto 1$. The ring \mathbf{D}_F is then isomorphic to the (completed) affine 0-Hecke algebra.

For $J' \subset J \subseteq \Pi$, write

$$x_{J/J'} := \prod_{\alpha \in \Sigma_J^- - \Sigma_{J'}^-} x_\alpha, \quad x_J := x_{J/\emptyset}.$$

Fixing a set of left coset representatives $W_{J/J'}$ of $W_J/W_{J'}$, we define a push–pull element

$$Y_{J/J'} := \left(\sum_{w \in W_{J/J'}} \delta_w \right) \frac{1}{x_{J/J'}} \in Q_W, \quad Y_J := Y_{J/\emptyset} = \left(\sum_{w \in W_J} \delta_w \right) \frac{1}{x_J}. \tag{1}$$

Note that the definition of $Y_{J/J'}$ depends on the choice of $W_{J/J'}$, and in general $Y_{J/J'}$ might not be in \mathbf{D}_F . Similarly, fixing a set of right coset representatives $W_{J'\setminus J}$ of $W_{J'}\setminus W_J$, one can define $Y_{J'\setminus J}$. If $J = \Pi$, x_Π and Y_Π are correspondingly defined. For instance, if $J = \{i\}$, then $Y_{\{i\}} = Y_{\alpha_i}$. Note that in general $Y_{J/J'} \in Q_W$, but $Y_J \in \mathbf{D}_F$. We have

$$Y_{J/J'}Y_{J'} = Y_J = Y_{J'}Y_{J'\setminus J}. \quad (2)$$

There is an anti-involution ι of \mathbf{D}_F , defined by

$$\iota(p\delta_v) := \delta_{v^{-1}}p \frac{v(x_\Pi)}{x_\Pi} = v^{-1}(p) \frac{x_\Pi}{v^{-1}(x_\Pi)} \delta_v \quad \text{for } p \in Q, v \in W. \quad (3)$$

For example, it is easy to prove that $\iota(Y_J) = Y_J$, and

$$\iota(Y_{I_w}) = Y_{I_w^{-1}}, \quad (4)$$

if I_w^{-1} is the sequence obtained from I_w by reversing the order.

Dual of the Demazure algebra. Let \mathbf{D}_F^* denote the S -linear dual $\text{Hom}_S(\mathbf{D}_F, S)$ with dual basis $Y_{I_w}^*$, $w \in W$. One can also consider the Q -linear dual $Q_W^* = \text{Hom}_Q(Q_W, Q)$, which is isomorphic to the set-theoretic $\text{Hom}(W, Q)$. There is the dual basis f_w , $w \in W$ of Q_W^* such that $f_w(\delta_v) = \delta_{w,v}^{\text{Kr}}$ and $f_w \cdot f_v = \delta_{w,v}^{\text{Kr}} f_w$, where $\delta_{w,v}^{\text{Kr}}$ is the Kronecker symbol. It turns Q_W^* into a commutative ring with identity $\mathbf{1} = \sum_w f_w$. By definition, we have $\mathbf{D}_F^* \subset Q_W^*$ (where the former is a S -module, and the latter is considered as a Q -module), and the product on Q_W^* restricts to the product on \mathbf{D}_F^* .

Two actions on the dual. There are actions denoted by \bullet and \odot of the ring Q_W on its Q -linear dual Q_W^* defined by

$$(p\delta_v)\bullet(qf_w) := qwv^{-1}(p)f_{wv^{-1}} \quad \text{and} \quad (p\delta_v)\odot(qf_w) := pv(q)f_{vw} \quad \text{for } v, w \in W, p, q \in Q. \quad (5)$$

It follows from [Lenart et al. 2020, § 3] that the \bullet -action is Q -linear, while the \odot -action is not, and the two actions commute. We also have $z\bullet pt_e = \iota(z)\odot pt_e$. Moreover, the two actions induce (via the embeddings $\mathbf{D}_F \subset Q_W$ and $\mathbf{D}_F^* \subset Q_W^*$) corresponding actions of \mathbf{D}_F on \mathbf{D}_F^* . For homology and K -theory, the \bullet and \odot actions correspond to the right and left actions considered in [Mihalcea et al. 2022].

The class of a point. For each $w \in W$ define the element

$$pt_w := x_\Pi \bullet f_w = w(x_\Pi)f_w,$$

and call it the class of a point. From the definition, we have $z\bullet pt_e = \iota(z)\odot pt_e$ for $z \in Q_W$, where $e \in W$ denotes the identity element.

Generalized (oriented) cohomology. Given a formal group law F over R , let \mathbf{h} be the corresponding free algebraic generalized (oriented) cohomology theory obtained from the algebraic cobordism Ω of Levine and Morel [2007] by tensoring with F , i.e.,

$$\mathbf{h}(-) := \Omega(-) \otimes_{\Omega(\text{pt})} R.$$

Here $\Omega(\text{pt})$ is the Lazard ring, the coefficient ring of universal formal group law, and $\Omega(\text{pt}) \rightarrow R$ is the evaluation map defining F . Note that such theories are different from the usual generalized cohomology theories from algebraic topology, since the formal group laws do not need to be Landweber exact (since the localization sequences are only right exact; see [Levine and Morel 2007, § 3.2]). We refer to [Levine and Morel 2007] for all the properties of such theories.

In particular, for the additive formal group law $F_a(x, y) = x + y$ one obtains the Chow ring and for the multiplicative group law F_m one gets the usual K -theory.

Equivariant generalized cohomology. Let \mathbf{h}_T be the respective T -equivariant generalized (oriented) cohomology theory of [Calmès et al. 2015, § 2]. Replacing \mathbf{h}_T if necessary by its characteristic completion (see Section 3 there), the main result of [Calmès et al. 2015] says that the formal affine Demazure algebra \mathbf{D}_F and its dual \mathbf{D}_F^* are related to generalized cohomology $\mathbf{h}_T(G/B)$ and $\mathbf{h}_T(G/P_J)$ as follows:

- (1) There is an isomorphism $\mathbf{D}_F^* \cong \mathbf{h}_T(G/B)$, which maps the element $Y_{I_w^{-1}} \bullet \text{pt}_e = Y_{I_w} \odot \text{pt}_e$ to the Bott–Samelson class determined by the sequence I_w .
- (2) Via the above isomorphism, the map $Y_\Pi \bullet _ : \mathbf{D}_F^* \rightarrow (\mathbf{D}_F^*)^W \cong S$ coincides with the map $\mathbf{h}_T(G/B) \rightarrow \mathbf{h}_T(\text{Spec}(k))$.
- (3) The group W acts on \mathbf{D}_F^* by restriction of the \bullet -action via the embedding $W \subset \mathbf{D}_F$. For any subset $J \subset \Pi$, one has an isomorphism $(\mathbf{D}_F^*)^{W_J} \cong \mathbf{h}_T(G/P_J)$, and the map $Y_J : \mathbf{D}_F^* \rightarrow (\mathbf{D}_F^*)^{W_J}$ coincides with the pushforward map $\mathbf{h}_T(G/B) \rightarrow \mathbf{h}_T(G/P_J)$. More generally, the map $Y_{J/J'} \bullet _ : Q_W^* \rightarrow Q_W^*$ restricts to a map $(\mathbf{D}_F^*)^{W_{J'}} \rightarrow (\mathbf{D}_F^*)^{W_J}$, which corresponds to $\mathbf{h}_T(G/P_{J'}) \rightarrow \mathbf{h}_T(G/P_J)$.
- (4) The embedding $\mathbf{D}_F^* \rightarrow Q_W^*$ coincides with the restriction to T -fixed points map $\mathbf{h}_T(G/B) \rightarrow Q \otimes_S \mathbf{h}_T(W)$, and the element pt_w is mapped to the class ϵ_w of T -fixed points of G/B .

Remark 2. Observe that the localization axiom [Calmès et al. 2015, A3] used to prove the above properties can be replaced by a weaker CD-property of [Neshitov et al. 2018, Definition 3.3] which holds for any \mathbf{h}_T defined using the Borel construction (see [Neshitov et al. 2018, Example 3.6]).

Generalized Bott–Samelson varieties. Let P_i, Q_i , for $i = 1, \dots, m$, be a collection of parabolic subgroups such that $Q_i \subset P_i \cap P_{i+1}$ and $Q_m := B$. Define

$$Z = P_1 \times^{Q_1} P_2 \times^{Q_2} \dots \times^{Q_{m-1}} P_m.$$

There is a canonical map

$$\pi : Z/Q_m \rightarrow G/Q_m, \quad (p_1, \dots, p_m) \mapsto p_1 p_2 \cdots p_m.$$

The following lemma will be used in Section 6 in identifying the small resolution of Zelevinsky with the factorization of Grassmannian Kazhdan–Lusztig basis of Kirillov and Lascoux.

Lemma 3. *Under the isomorphism $\mathbf{h}_T(G/B) \cong \mathbf{D}_F^*$ and viewing $\mathbf{h}_T(G/P) \cong (\mathbf{D}_F^*)^{W_P}$, we have*

$$\pi_*(1) = (Y_{P_m/Q_{m-1}} Y_{P_{m-1}/Q_{m-2}} \cdots Y_{P_2/Q_1} Y_{P_1}) \bullet \text{pt}_e.$$

Proof. We use induction on m . If $m = 1$, then the map is $\pi : P_1/Q_1 \rightarrow G/Q_1$. We have the following commutative diagram:

$$\begin{array}{ccc} P_1/Q_1 & \xrightarrow{\pi} & G/Q_1 \\ \downarrow q & & \downarrow p_{P_1/Q_1} \\ \text{pt} & \xrightarrow{i} & G/P_1 \end{array}$$

Here i is the embedding of the identity point. Then

$$\pi_*(1) = \pi_*q_*(1) = (p_{P_1/Q_1})^*i_*(1).$$

According to [Calmès et al. 2015, Lemma 8.8], we see that $i_*(1) = Y_{P_1} \bullet \text{pt}_e$, and $p_{P_1/\emptyset}^*$ is the embedding $(\mathbf{D}_F^*)^{W_{P_1}} \hookrightarrow (\mathbf{D}_F^*)^{W_{Q_1}} \subset \mathbf{D}_F^*$. So it holds when $m = 1$.

Now write $Z' = P_1 \times^{Q_1} P_2 \times^{Q_2} \dots \times^{P_{m-2}} Q_{m-1}$. We then have the commutative diagram

$$\begin{array}{ccc} Z' \times^{Q_{m-1}} P_m/Q_m & \xrightarrow{\pi} & G/Q_m \\ \downarrow q & & \downarrow p_{P_m/Q_m} \\ Z'/Q_{m-1} & \xrightarrow{p_{P_m/Q_{m-1}} \circ \pi'} & G/P_m \end{array}$$

where $\pi' : Z'/Q_{m-1} \rightarrow G/Q_{m-1}$ is the map multiplying all components together. Then

$$\pi_*(1) = \pi_*q_*(1) = (p_{P_m/Q_m})^*(p_{P_m/Q_{m-1}})_*\pi'_*(1).$$

From [Calmès et al. 2015, p. 137], we see that $(p_{P_m/Q_{m-1}})_*$ corresponds to $Y_{P_m/Q_{m-1}} \bullet -$, and $(p_{P_m/Q_m})^*$ is just the embedding $(\mathbf{D}_F)^{W_{P_m}} \hookrightarrow (\mathbf{D}_F)^{W_{Q_m}}$. The conclusion then follows from induction. \square

Corollary 4. *Via the isomorphism $\mathbf{h}_T(G/B) \cong \mathbf{D}_F^*$, we have*

$$\pi_*(1) = (Y_{P_1/Q_1} \cdots Y_{P_{m-1}/Q_{m-1}} Y_{P_m}) \odot \text{pt}_e.$$

Proof. Note $Y_P/QY_Q = Y_P$ for any $P \supset Q$, and $Y_P \bullet \text{pt}_e = Y_P \odot \text{pt}_e$ (see [Lenart et al. 2020, (3.5), (3.8)]). If $m = 2$, we have

$$\begin{aligned} \pi_*(1) &= (Y_{P_2/Q_1} Y_{P_1}) \bullet \text{pt}_e = Y_{P_2/Q_1} \bullet Y_{P_1} \odot \text{pt}_e = Y_{P_2/Q_1} \bullet Y_{P_1/Q_1} \odot Y_{Q_1} \odot \text{pt}_e \\ &= Y_{P_2/Q_1} \bullet Y_{P_1/Q_1} \odot Y_{Q_1} \bullet \text{pt}_e = Y_{P_1/Q_1} \odot (Y_{P_2/Q_1} Y_{Q_1}) \bullet \text{pt}_e = Y_{P_1/Q_1} \odot Y_{P_2} \odot \text{pt}_e. \end{aligned}$$

The general case then follows similarly. \square

We prove a lemma that will be used later in Section 6:

Lemma 5. *We have*

$$Y_{P_1/Q_1} Y_{P_2/Q_2} \cdots Y_{P_{m-1}/Q_{m-1}} Y_{P_m} = Y_{P_1} Y_{Q_1 \setminus P_2} \cdots Y_{Q_{m-1} \setminus P_m}.$$

Proof. This follows from recursive use of the identities (2) and the assumption that $Q_i \subset P_i \cap P_{i+1}$. For example, one has

$$Y_{P_{m-1}/Q_{m-1}} Y_{P_m} = Y_{P_{m-1}/Q_{m-1}} Y_{Q_{m-1}} Y_{Q_{m-1} \setminus P_m} = Y_{P_{m-1}} Y_{Q_{m-1} \setminus P_m}.$$

By induction, the formula holds. \square

3. Hecke algebra, motivic Chern class, and the smoothness criterion

In this section, we recall the definition of the Kazhdan–Lusztig basis and the motivic Chern (MC) classes.

The multiplicative case. Set $R = \mathbb{Z}[t, t^{-1}, (t + t^{-1})^{-1}]$, where t is a parameter. Definitions of Section 2 applied to the multiplicative formal group law F_m over R give the respective formal group algebra and its localization,

$$S_m := R[[X^*(T)]]_{F_m} \quad \text{and} \quad Q_m := S_m \left[\frac{1}{x_\alpha} \mid \alpha > 0 \right],$$

the localized twisted group algebra and the formal affine Demazure algebra,

$$Q_{m,W} := Q_m \otimes_R R[W] \quad \text{and} \quad D_m := \langle S_m, Y_1, \dots, Y_n \rangle \subset Q_{m,W}.$$

The Demazure–Lusztig elements. Define the Demazure–Lusztig elements in $Q_{m,W}$ as

$$\tau_i := Y_i^m (t - t^{-1} e^{\alpha_i}) - t = \frac{t^{-1} - t}{1 - e^{-\alpha_i}} + \frac{t - t^{-1} e^{-\alpha_i}}{1 - e^{-\alpha_i}} \delta_i^m.$$

It can be shown that $\tau_i \in D_m$ for $i = 1, \dots, n$ satisfy the standard quadratic relation $\tau_i^2 = (t^{-1} - t)\tau_i + 1$, and the braid relations. So they generate the Hecke algebra H over R .

Remark 6. Let $y = -t^{-2}$. On $D_m^* \cong R \otimes_{\mathbb{Z}} K_T(G/B)$, as operators, $t^{-1}\tau_i \odot_-$ agrees with \mathcal{T}_i^L , and $t^{-1}\tau_i \bullet_-$ agrees with $\mathcal{T}_i^{R,\vee}$, respectively, where the latter are notions from [Mihalcea et al. 2022, Section 5.3] and [Aluffi et al. 2019].

The Kazhdan–Lusztig basis. Consider the involution of the Hecke algebra $H \rightarrow H$, $z \mapsto \bar{z}$ such that

$$\bar{t} = t^{-1}, \quad \bar{\tau}_i = \tau_i^{-1}. \tag{6}$$

There is a basis of H over R denoted by $\{\gamma_w\}_{w \in W}$ and called the Kazhdan–Lusztig basis. It is invariant under this involution and satisfies

$$\gamma_w \in \tau_w + \sum_{v < w} t \mathbb{Z}[t] \tau_v.$$

We set $t_w = t^{\ell(w)}$ and

$$\gamma_w = \sum_{v \leq w} t_w t_v^{-1} P_{v,w}(t^{-2}) \tau_v,$$

where $P_{v,w}$ are the Kazhdan–Lusztig polynomials. In addition to this, there is another canonical basis defined by (see [Kazhdan and Lusztig 1979]),

$$\tilde{\gamma}_w := \sum_{v \in W} \epsilon_w \epsilon_v t_w^{-1} t_v P_{v,w}(t^2) \tau_v \in \tau_w + \sum_{v < w} t^{-1} \mathbb{Z}[t^{-1}] \tau_v,$$

where ϵ_w is $(-1)^{\ell(w)}$. Since the Schubert variety $X(w_J) \subset G/B$ is smooth, the Kazhdan–Lusztig polynomials satisfy $P_{v,w_J} = 1$ for any $v \leq w_J$. Thus, $\gamma_{w_J} = \sum_{v \leq w_J} t_{w_J} t_v^{-1} \tau_v$.

More generally, for $J' \subset J \subseteq \Pi$, write

$$\gamma_J := \gamma_{w_J}, \quad \gamma_{J/J'} := \sum_{v \in W_J \cap W_{J'}} t_{w_{J/J'}} t_v^{-1} \tau_v, \quad \gamma_{J' \setminus J} := \sum_{v \in W_J \cap J' W} t_{w_{J' \setminus J}} t_v^{-1} \tau_v. \tag{7}$$

It is not difficult to see that

$$\gamma_J = \gamma_{J/J'}\gamma_{J'} = \gamma_{J'}\gamma_{J'\setminus J}. \tag{8}$$

If $Q \subset P$ are the parabolic subgroups corresponding to $J' \subset J$, respectively, write $\gamma_{P/Q} = \gamma_{J/J'}$. For $\gamma_{J/J'}$ and $\gamma_{J'\setminus J}$, the analogue of Lemma 5 holds. It will be used in considering KL Schubert classes in hyperbolic cohomology of partial flag varieties below.

Motivic Chern classes. We recall the definition of the motivic Chern classes, following [Brasselet et al. 2010; Fehér et al. 2021; Aluffi et al. 2019]. Let X be a nonsingular quasiprojective complex algebraic variety with an action of the torus T . Let $G_0^T(\text{var}/X)$ be the (relative) Grothendieck group of varieties over X . By definition, it is the free abelian group generated by isomorphism classes $[f : Z \rightarrow X]$ where Z is a quasiprojective T -variety and f is a T -equivariant morphism modulo the usual additivity relations

$$[f : Z \rightarrow X] = [f : U \rightarrow X] + [f : (Z - U) \rightarrow X],$$

for any T -invariant open subvariety $U \subset Z$.

Theorem 7. *There exists a unique natural transformation $\text{MC}_{-t^{-2}} : G_0^T(\text{var}/X) \rightarrow K_T(X)[t^{-2}]$ satisfying the following properties:*

- (1) *It is functorial with respect to T -equivariant proper morphisms of nonsingular, quasiprojective varieties.*
- (2) *It satisfies the normalization condition*

$$\text{MC}_{-t^{-2}}[\text{id}_X : X \rightarrow X] = \sum (-1)^i t^{-2i} [\wedge^i T_X^*] =: \lambda_{-t^{-2}}(T_X^*) \in K_T(X)[t^{-2}].$$

The nonequivariant case is proved in [Brasselet et al. 2010], and the equivariant case is shown in [Aluffi et al. 2019; Fehér et al. 2021].

Let

$$\mathcal{D}(-) := (-1)^{\dim X} \text{RHom}_{\mathcal{O}_X}(-, \omega_X)$$

be the Serre–Grothendieck duality functor on $K_T(X)$, where $\omega_X := \wedge^{\dim X} T_X^*$ is the canonical bundle of X . Extend it to $K_T(X)[t^{\pm 1}]$ by setting $\mathcal{D}(t^i) = t^{-i}$.

Definition 8. Let $Z \subset X$ be a T -invariant subvariety.

- (1) Define the motivic Chern class of Z to be

$$\text{MC}_{-t^{-2}}(Z) := \text{MC}_{-t^{-2}}([Z \hookrightarrow X]).$$

- (2) Further assume that Z is pure-dimensional. Define the Segre motivic Chern class of Z as follows (see [Mihalcea et al. 2022, Definition 6.2]):

$$\text{SMC}_{-t^{-2}}(Z) := t^{-2 \dim Z} \cdot \frac{\mathcal{D}(\text{MC}_{-t^{-2}}(Z))}{\lambda_{-t^{-2}}(T_X^*)}.$$

Smoothness of Schubert varieties. Consider the variety of complete flags G/B . Let $X(w)^\circ := BwB/B$ and $Y(w)^\circ := B^-wB/B$ be the Schubert cells. The closures $X(w) := \overline{X(w)^\circ}$ and $Y(w) := \overline{Y(w)^\circ}$ are the Schubert varieties. Observe that $u \leq v$ with respect to the Bruhat order if and only if $X(u) \subset X(v)$. Let $\text{pt}_w^m = w(x_\Pi) f_w^m \in Q_{m,W}^*$ denote the class of the T -fixed point ϵ_w corresponding to $w \in W$. Note that here f_w^m is the standard basis in $Q_{m,W}^*$ defined in Section 2, and the superscript m is to indicate the multiplicative formal group law.

The key property of the motivic Chern classes of the Schubert cells that we need are listed below.

Theorem 9. (1) [Mihalcea et al. 2022, Theorem 7.6] *For any $w \in W$, we have*

$$\text{MC}_{-t^{-2}}(X(w)^\circ) = t_w^{-1} \tau_w \odot \text{pt}_e^m.$$

(2) [Aluffi et al. 2019, Theorem 9.1] *For any $u \leq w \in W$, the Schubert variety $X(w)$ is smooth at ϵ_u if and only if*

$$\text{MC}_{-t^{-2}}(X(w))|_u = \prod_{\alpha > 0, u s_\alpha \not\leq w} (1 - e^{u\alpha}) \prod_{\alpha > 0, u s_\alpha \leq w} (1 - t^{-2} e^{u\alpha}),$$

where $\text{MC}_{-t^{-2}}(X(w))|_u$ denotes the pullback of $\text{MC}_{-t^{-2}}(X(w))$ to the fixed point ϵ_u .

Remark 10. (1) This theorem is used to prove the Bump, Nakasuji and Naruse’s conjectures about Casselman bases in unramified principal series representations; see [Bump and Nakasuji 2011; 2019; Naruse 2014; Aluffi et al. 2019; Su 2019].

(2) The “only if” direction of part (2) follows directly from basic properties of motivic Chern classes, and it holds in a much more general setting; see [Aluffi et al. 2019, § 9.1].

Proof. The first part follows from the reference mentioned. The second one follows from the fact $\delta_{w_0} \odot (\text{MC}_{-t^{-2}}(Y(w))) = \text{MC}_{-t^{-2}}(X(w_0 w))$. □

Given $w \in W$, define the coefficients $a_{w,u} \in Q_m$ by the formulas

$$\Gamma_w := \sum_{v \leq w} t_v^{-1} \tau_v = \sum_{u \leq w} a_{w,u} \delta_u^m \in Q_{m,W}. \tag{9}$$

Note that if the Schubert variety $X(w)$ is smooth, then $P_{v,w} = 1$ for all $v \leq w$, so $\Gamma_w = t_w^{-1} \gamma_w$. It is immediate to get the following corollary from Theorem 9.

Corollary 11. *For any $u \leq w \in W$, the Schubert variety $X(w)$ is smooth at the fixed point ϵ_u if and only if*

$$a_{w,u} = \prod_{\alpha > 0, u s_\alpha \leq w} \frac{1 - t^{-2} e^{u\alpha}}{1 - e^{u\alpha}}.$$

Proof. By Theorem 9(1) and Equation (9), we have

$$\begin{aligned} \text{MC}_{-t^{-2}}(X(w)) &= \sum_{v \leq w} \text{MC}_{-t^{-2}}(X(v)^\circ) = \sum_{v \leq w} t_v^{-1} \tau_v \odot \text{pt}_e^m \\ &= \sum_{v \leq w} a_{w,v} \delta_v^m \odot \text{pt}_e^m = \sum_{v \leq w} a_{w,v} \prod_{\alpha > 0} (1 - e^{v\alpha}) f_v. \end{aligned}$$

Thus, we have

$$\text{MC}_{-t^{-2}}(X(w))|_u = a_{w,u} \prod_{\alpha>0} (1 - e^{u\alpha}).$$

The corollary follows from this and Theorem 9(2). □

4. Dual bases in K -theory and characteristic classes of mixed Hodge modules

In this section, we use the two Kazhdan–Lusztig bases of the Hecke algebra to define two collections of classes in K -theory, and show that they are actually dual to each other. We also give a geometric interpretation of one of these collections using the intersection homology mixed Hodge modules. These are also generalized to the partial flag variety case.

K-theory KL classes.

Definition 12. We define two collections of classes (called KL classes) in $K_T(G/B)[t^{\pm 1}]$ as follows:

$$C_w := \gamma_w \odot \text{pt}_e^m \quad \text{and} \quad \tilde{C}_w := \tilde{\gamma}_{w^{-1}w_0} \bullet \text{pt}_{w_0}^m.$$

They form a basis of the localized K -theory $Q_m \otimes_{S_m} K_T(G/B)$.

Let $\langle -, - \rangle$ denote the usual nondegenerate tensor product pairing on $K_T(G/B)[t^{\pm 1}]$, i.e., $\langle f, g \rangle = Y_{\Pi}^m \bullet (f \cdot g)$ for $f, g \in K_T(G/B)[t^{\pm 1}]$. The first result of this section is the following.

Theorem 13. For any $w, v \in W$, we have

$$\langle C_w, \tilde{C}_v \rangle = \delta_{w,v}^{\text{Kr}} \prod_{\alpha>0} (t - t^{-1}e^{-\alpha}).$$

We first recall that the Segre motivic Chern classes of Schubert cells enjoy the following properties.

Lemma 14. (1) For any $v \in W$, we have

$$(\tau_{w_0v})^{-1} \bullet \text{pt}_{w_0}^m = t_{w_0v} \prod_{\alpha>0} (1 - t^{-2}e^{-\alpha}) \text{SMC}_{-t^{-2}}(Y(v)^\circ).$$

(2) For any $u, v \in W$, we have

$$\langle \text{MC}_{-t^{-2}}(X(u)^\circ), \text{SMC}_{-t^{-2}}(Y(v)^\circ) \rangle = \delta_{u,v}^{\text{Kr}}.$$

Proof. The first part follows from Remark 6 and [Mihalcea et al. 2022, Theorem 7.4], while the second one follows from [loc. cit., Theorem 7.1]. □

Remark 15. By definition, $(t^{-1}\tau_i)|_{t=\infty} = Y_i^m - 1$. Thus, from Theorem 9(1), we get

$$\text{MC}_{-t^{-2}}(X(w)^\circ)|_{t=\infty} = t_w^{-a} \tau_w \odot \text{pt}_e^m|_{t=\infty} = [\mathcal{O}_{X(w)}(-\partial X(w))] =: \mathcal{I}_w,$$

where $\partial X(w) = \bigcup_{v<w} X(v)$ is the boundary of the Schubert variety $X(w)$, and \mathcal{I}_w denotes its ideal sheaf. On the other hand, $(t^{-1}\tau_i^{-1})|_{t=\infty} = Y_i^m$. Thus, the first part of the lemma gives

$$\text{SMC}_{-t^{-2}}(Y(v)^\circ)|_{t=\infty} = (t_{w_0v} \tau_{w_0v})^{-1} \bullet \text{pt}_{w_0}^m|_{t=\infty} = [\mathcal{O}_{Y(v)}].$$

Therefore, setting $t = \infty$ in the second part of the lemma, we get the classical fact

$$\langle \mathcal{I}_w, [\mathcal{O}_{Y(v)}] \rangle = \delta_{u,v}^{\text{Kr}}.$$

Proof of Theorem 13. First of all, we have the following inversion formula for the Kazhdan–Lusztig polynomials (see [Kazhdan and Lusztig 1979, Theorem 3.1]):

$$\sum_z \epsilon_y \epsilon_z P_{x,z} P_{w_0 y, w_0 z} = \delta_{x,y}^{\text{Kr}}.$$

Therefore,

$$\sum_z \epsilon_x \epsilon_z P_{w_0 z, w_0 x} P_{z,y} = \delta_{x,y}^{\text{Kr}}. \quad (10)$$

By definition and Theorem 9(1),

$$C_w = \sum_{u \leq w} t_w t_u^{-1} P_{u,w}(t^{-2}) \tau_u \odot \text{pt}_e^m = \sum_{u \leq w} t_w P_{u,w}(t^{-2}) \text{MC}_{-t^{-2}}(X(u)^\circ). \quad (11)$$

On the other hand, since $\tilde{\gamma}_w$ is invariant under the involution, we get

$$\tilde{\gamma}_w = \sum_{v \in W} \epsilon_w \epsilon_v t_w t_v^{-1} P_{v,w}(t^{-2}) \tau_{v^{-1}}^{-1}.$$

Thus,

$$\begin{aligned} \tilde{C}_w &= \tilde{\gamma}_{w^{-1}w_0} \bullet \text{pt}_{w_0}^m \\ &= \sum_{v \geq w} \epsilon_w \epsilon_v t_w t_{v^{-1}w_0} t_{v^{-1}w_0}^{-1} P_{v^{-1}w_0, w^{-1}w_0}(t^{-2}) \tau_{w_0 v}^{-1} \bullet \text{pt}_{w_0}^m \\ &= \prod_{\alpha > 0} (1 - t^{-2} e^{-\alpha}) \sum_{v \geq w} \epsilon_w \epsilon_v t_w t_{v^{-1}w_0} P_{v^{-1}w_0, w^{-1}w_0}(t^{-2}) \text{SMC}_{-t^{-2}}(Y(v)^\circ), \end{aligned} \quad (12)$$

where the last step follows from Lemma 14(1).

Therefore, we have

$$\begin{aligned} \langle C_w, \tilde{C}_y \rangle &= \prod_{\alpha > 0} (1 - t^{-2} e^{-\alpha}) t_w t_{y^{-1}w_0} \sum_u P_{u,w} \sum_v \epsilon_v \epsilon_y P_{v^{-1}w_0, y^{-1}w_0} \delta_{u,v}^{\text{Kr}} \\ &= \prod_{\alpha > 0} (1 - t^{-2} e^{-\alpha}) t_w t_{y^{-1}w_0} \sum_u P_{u,w} \epsilon_u \epsilon_y P_{w_0 u, w_0 y} \\ &= \prod_{\alpha > 0} (t - t^{-1} e^{-\alpha}) \delta_{w,y}^{\text{Kr}}, \end{aligned}$$

where the first equality follows from Lemma 14(2), the second follows from $P_{u,v} = P_{u^{-1}, v^{-1}}$, and the third one follows from (10).

An immediate corollary of the proof is the following.

Corollary 16. *If the Schubert variety $X(w)$ is smooth, then*

$$C_w = \sum_{u \leq w} t_w \text{MC}_{-t^{-2}}(X(u)^\circ) = t_w \text{MC}_{-t^{-2}}(X(w)) \in K_T(G/B)[t^{\pm 1}].$$

Proof. It follows directly from (11) and the fact $P_{u,w} = 1$ for all $u \leq w$. □

Characteristic classes of mixed Hodge modules. For any parabolic subgroup P_J , let $K^0(\text{MHM}(G/P_J, B))$ denote its Grothendieck group of B -equivariant mixed Hodge modules. Recall there is a motivic Hodge Chern transformation (see [Schürmann 2011, Definition 5.3 and Remark 5.5])

$$\text{MHC}_{-t-2} : K^0(\text{MHM}(G/P_J, B)) \rightarrow K_B(G/P_J)[t^{\pm 1}] \simeq K_T(G/P_J)[t^{\pm 1}]$$

such that for any $[f : Z \rightarrow G/P_J] \in G_0^B(\text{var}/(G/P_J))$,

$$\text{MC}_{-t-2}([f : Z \rightarrow G/P_J]) = \text{MHC}_{-t-2}([f! \mathbb{Q}_Z^H]), \tag{13}$$

where $[\mathbb{Q}_Z^H] := [k^* \mathbb{Q}_{\text{pt}}^H] \in K^0(\text{MHM}(Z, B))$ and $k : Z \rightarrow \text{pt}$ is the structure morphism. The construction also works for B^- -equivariant mixed Hodge modules, where B^- is the opposite Borel subgroup. The natural transformation MC_{-t-2} commutes with the Serre–Grothendieck dual as follows [loc. cit., Corollary 5.19]:

$$\text{MHC}_{-t-2} \circ \mathcal{D} = \mathcal{D} \circ \text{MHC}_{-t-2}. \tag{14}$$

Here the first \mathcal{D} is the dual of the mixed Hodge modules, and the second one is the Serre–Grothendieck dual. Both are denoted by \mathcal{D} , if no confusion is possible.

For any $u \in W$, let $i_u : X(u)^\circ \hookrightarrow G/B$ and $j_u : Y(u)^\circ \hookrightarrow G/B$ be the inclusions. Then, by (13),

$$\text{MC}_{-t-2}(X(u)^\circ) = \text{MHC}_{-t-2}([i_u! \mathbb{Q}_{X(u)^\circ}^H]),$$

where $\mathbb{Q}_{X(u)^\circ}^H$ is the constant mixed Hodge module on the Schubert cell $X(u)^\circ$. Since $\mathcal{D} \circ j_{v!} = j_{v*} \circ \mathcal{D}$, and

$$\mathcal{D}(\mathbb{Q}_{Y(v)^\circ}^H) = \mathbb{Q}_{Y(v)^\circ}^H[2 \dim Y(v)^\circ](\dim Y(v)^\circ),$$

where $[2 \dim Y(v)^\circ]$ means shift by $2 \dim Y(v)^\circ$ and $(\dim Y(v)^\circ)$ denotes the twist by the Tate Hodge module $\mathbb{Q}^H(1)^{\otimes \dim Y(v)^\circ}$, Equation (14) gives

$$\text{SMC}_{-t-2}(Y(v)^\circ) = \frac{\text{MHC}_{-t-2}([j_{v*} \mathbb{Q}_{Y(v)^\circ}^H])}{\lambda_{-t-2}(T_{G/B}^*)}.$$

Using these, Lemma 14(2) can also be proved using mixed Hodge modules, by Schürmann. For the analogue in equivariant homology, see [Schürmann 2017, Theorem 1.2].

For any Schubert variety $X(w)$, let $[\text{IC}_{X(w)}^H] \in K^0(\text{MHM}(G/B, B))$ denote the intersection homology Hodge module on $X(w)$. Then it is well known that (see [Kazhdan and Lusztig 1980; Tanisaki 1987; Kashiwara and Tanisaki 2002])

$$[\text{IC}_{X(w)}^H] = \sum_{u \leq w} \epsilon_w P_{u,w}(t^{-2}) [i_u! \mathbb{Q}_{X(u)^\circ}^H].$$

Thus,

$$\text{MHC}_{-t-2}([\text{IC}_{X(w)}^H]) = \sum_{u \leq w} \epsilon_w P_{u,w}(t^{-2}) \text{MC}_{-t-2}(X(u)^\circ).$$

Comparing with (11), we get the following geometric interpretation of the KL classes C_w in Definition 12.

Proposition 17. For any $w \in W$,

$$C_w = t_w \epsilon_w \text{MHC}_{-t^{-2}}([\text{IC}_{X(w)}^H]) \in K_T(G/B)[t^{\pm 1}].$$

Remark 18. If $X(w)$ is smooth or rationally smooth (i.e., $[\text{IC}_{X(w)}^H] = \mathbb{Q}_{X(w)}^H[\dim X(w)]$), then

$$C_w = t_w \epsilon_w \text{MHC}_{-t^{-2}}([\text{IC}_{X(w)}^H]) = t_w \text{MC}_{-t^{-2}}(X(w)).$$

This is compatible with Corollary 16.

An immediate corollary is the following.

Corollary 19. The canonical basis C_w is invariant under the Serre–Grothendieck duality, i.e.,

$$\mathcal{D}(C_w) = C_w \in K_T(G/B)[t^{\pm 1}].$$

Proof. Since

$$\mathcal{D}(\text{IC}_{X(w)}^H) = \text{IC}_{X(w)}^H(\dim X(w)),$$

Equation (14) and Proposition 17 give

$$\mathcal{D}(C_w) = \mathcal{D}(t_w \epsilon_w \text{MHC}_{-t^{-2}}([\text{IC}_{X(w)}^H])) = t_w^{-1} \epsilon_w \text{MHC}_{-t^{-2}}(\mathcal{D}([\text{IC}_{X(w)}^H])) = C_w. \quad \square$$

Parabolic case. In this subsection, we generalize the above results to the parabolic case. Let $J \subset \Pi$ be a subset of simple roots, with corresponding parabolic subgroup P_J . Schubert cells and varieties and opposite Schubert cells and varieties of G/P_J are indicated by subscripts J . Recall there exist parabolic Kazhdan–Lusztig polynomials (see [Deodhar 1987; Kashiwara and Tanisaki 2002]), denoted by $P_{v,w}^J \in \mathbb{Z}[t^{-2}]$, where $v, w \in W^J$. Here our $P_{v,w}^J$ is the $u = -1$ parabolic KL polynomials in [Deodhar 1987], which are also denoted by $P_{v,w}^{J,q}$ in [Kashiwara and Tanisaki 2002, Remark 2.1]. We have the following property, which generalizes [Deodhar 1987, Proposition 3.4].

Lemma 20 [Lenart et al. 2020, Proposition 5.19]. For any $w, v \in W^J$ and $u \in W_J$,

$$P_{vu,ww_J} = P_{v,w}^J.$$

Let $Q_{u,w} := P_{w_0w, w_0u}$ denote the usual inverse KL polynomials, which satisfy

$$\sum_w \epsilon_u \epsilon_w Q_{u,w} P_{w,v} = \delta_{u,v}^{\text{Kr}}.$$

For any $u, w \in W^J$, let $Q_{u,w}^J \in \mathbb{Z}[t^{-2}]$ denote the inverse parabolic KL polynomial (see [Kashiwara and Tanisaki 2002]).¹ Then

$$\sum_{w \in W^J} \epsilon_u \epsilon_w Q_{u,w}^J P_{w,v}^J = \delta_{u,v}^{\text{Kr}}. \tag{15}$$

Moreover, it is related to the usual $Q_{u,w}$ as follows (see [Kashiwara and Tanisaki 2002, Proposition 2.6] or [Soergel 1997]):

$$Q_{u,w}^J = \sum_{v \in W_J} \epsilon_v \epsilon_{w_J} Q_{uw_J, wv}.$$

¹Our $Q_{u,w}^J$ is denoted by $Q_{u,w}^{J,q}$ in [Kashiwara and Tanisaki 2002].

Following (11) and (12), we define the parabolic canonical bases in $K_T(G/P_J)[t^{\pm 1}]$ as follows.

Definition 21. For any $w \in W^J$, let

$$C_w^J := \sum_{u \in W^J, u \leq w} t_w P_{u,w}^J(t^{-2}) \text{MC}_{-t^{-2}}(X(u)_J^\circ),$$

$$\tilde{C}_w^J := \prod_{\alpha \in \Sigma^+ - \Sigma_J^+} (1 - t^{-2}e^{-\alpha}) \sum_{v \in W^J, v \geq w} \epsilon_w \epsilon_v t_{w_J w^{-1} w_0} Q_{w,v}^J(t^{-2}) \text{SMC}_{-t^{-2}}(Y(v)_J^\circ).$$

If $J = \emptyset$, then $C_w^\emptyset = C_w$, and $\tilde{C}_w^\emptyset = \tilde{C}_w$, as defined before.

Let $\langle -, - \rangle_J$ denote the nondegenerate tensor product pairing on $K_T(G/P_J)$. The parabolic analogue of Lemma 14(2) also holds (see [Mihalcea et al. 2022, Theorem 7.2]): for any $u, v \in W^J$,

$$\langle \text{MC}_{-t^{-2}}(X(u)_J^\circ), \text{SMC}_{-t^{-2}}(Y(v)_J^\circ) \rangle_J = \delta_{u,v}^{\text{Kr}}.$$

Combining this with (15), we immediately get the following generalization of Theorem 13.

Theorem 22. For any $u, w \in W^J$,

$$\langle C_w^J, \tilde{C}_u^J \rangle_J = \delta_{u,w}^{\text{Kr}} \prod_{\alpha \in \Sigma^+ - \Sigma_J^+} (t - t^{-1}e^{-\alpha}).$$

We now investigate the relation between KL classes of G/B and G/P_J . For any $w \in W^J$, let us still use i_u to denote the inclusion $X(u)_J^\circ \hookrightarrow G/P_J$. Then the following identity holds in $K^0(\text{MHM}(G/P_J, B))$ (see [Kashiwara and Tanisaki 2002, Corollary 5.1]):

$$[\text{IC}_{X(w)_J}^H] = \sum_{u \in W^J, u \leq w} \epsilon_w P_{u,w}^J [i_{u!} \mathbb{Q}_{X(u)_J}^H].$$

Thus, we get the following parabolic analogue of Proposition 17 and Corollary 19.

Proposition 23. For any $w \in W^J$,

$$C_w^J = t_w \epsilon_w \text{MHC}_{-t^{-2}}([\text{IC}_{X(w)_J}^H]).$$

Moreover, let \mathcal{D}_J denote the Serre–Grothendieck duality functor on G/P_J . Then

$$\mathcal{D}_J(C_w^J) = C_w^J.$$

Recall $\pi_J : G/B \rightarrow G/P_J$ denotes the natural projection. The relation between C_w and C_w^J is given by the following proposition.

Proposition 24. Let $\mathcal{P}_J(t) = \sum_{v \in W_J} t_v$ be the Poincaré polynomial of W_J . Then for any $w \in W^J$,

$$\pi_{J*}(C_{ww_J}) = t_{w_J}^{-1} \mathcal{P}_J(t^2) C_w^J \in K_T(G/P_J)[t^{\pm 1}].$$

Proof. By [Aluffi et al. 2019, Remark 5.5], for any $u \in W^J$ and $v \in W_J$,

$$\pi_{J*}(\text{MC}_{-t^{-2}}(X(uv)^\circ)) = t_v^{-2} \text{MC}_{-t^{-2}}(X(u)_J^\circ),$$

which also follows directly from the following identity about mixed Hodge modules:

$$\pi_{J!}(i_{uv!}\mathbb{Q}_{X(uv)^\circ}^H) = \mathbb{Q}_{X(u)^\circ}^H[-2\ell(v)](-\ell(v)).$$

Thus,

$$\begin{aligned} \pi_{J*}(C_{ww_J}) &= \sum_{u \in W^J, u \leq w} \sum_{v \in W_J} t_w t_{w_J} P_{uv, ww_J} \pi_{J*} \mathbf{MC}_{-t^{-2}}(X(uv)^\circ) \\ &= \sum_{u \in W^J, u \leq w} t_w t_{w_J} P_{u, w}^J \mathbf{MC}_{-t^{-2}}(X(u)^\circ) \sum_{v \in W_J} t_v^{-2} \\ &= C_w^J \sum_{v \in W_J} t_v^{-2} t_{w_J} = C_w^J \sum_{v \in W_J} t_{w_J}^{-1} t_{w_J}^2 t_v^{-2} = C_w^J \sum_{v \in W_J} t_{w_J}^{-1} t_{vw_J}^2 = C_w^J t_{w_J}^{-1} \mathcal{P}_J(t^2), \end{aligned}$$

where the second equality follows from Lemma 20. \square

5. The smoothness conjecture for hyperbolic cohomology

In this section, we use the smoothness criterion to prove the smoothness conjecture. Since we will be working with multiplicative and hyperbolic formal group laws at the same time, we add superscripts or subscripts m (resp. t) in the multiplicative case (resp. hyperbolic case).

The hyperbolic case. Consider the hyperbolic formal group law over $R = \mathbb{Z}[t, t^{-1}, \mu^{-1}]$

$$F_t(x, y) := \frac{x + y - xy}{1 - \mu^{-2}xy},$$

where $\mu = t + t^{-1}$. Note that R depends on only one parameter t . The definitions of Section 2 applied to F_t give the respective rings

$$S_t, \quad Q_t, \quad Q_{t, W}, \quad D_t.$$

Consider a map of formal group laws

$$g: F_t \rightarrow F_m, \quad g(x) = \frac{(1-t^2)x}{x - (t^2 + 1)},$$

so that $F_m(g(x), g(y)) = g(F_t(x, y))$. It induces ring embeddings

$$\psi: S_m \hookrightarrow S_t, \quad \psi(f(x_\lambda)) = f(g(x_\lambda)) \quad \text{for } f(x) \in R[[x]],$$

and

$$\psi: Q_m \hookrightarrow R \left[\frac{1}{1-t^2} \right] \otimes Q_t. \tag{16}$$

Consequently, we have a ring embedding

$$\psi: Q_{m, W} \rightarrow R \left[\frac{1}{1-t^2} \right] \otimes_R Q_{t, W}, \quad \psi(p \delta_w^m) = \psi(p) \delta_w^t \quad \text{for } p \in Q_m, w \in W.$$

It can be shown that

$$\psi(\tau_i) = \mu Y_i^t - t \in D_t \subset Q_{t, W}. \tag{17}$$

Note that in (16), for the target, we have to invert $t^2 - 1$, but for the one in (17), it is not necessary.

One of the most interesting properties of ψ is the following (see [Lenart et al. 2020, Corollary 5.5 (2)]):

$$\mu^{-\ell(w_{J/J'})} \psi(\gamma_{J/J'}) Y_{J'}^t = Y_J^t. \tag{18}$$

In other words, $\psi(\gamma_{J/J'})$ behaves like a replacement of $Y_{J/J'}$; see [Lenart et al. 2020, Remark 5.6]. In particular, letting $J' = \emptyset$, one then has

$$\mu^{-\ell(w_J)} \psi(\gamma_{w_J}) = Y_J^t.$$

Let \mathfrak{h} denote the respective oriented cohomology theory for the hyperbolic formal group law F_t .

Definition 25. Define the KL Schubert class for $w \in W^J$ to be

$$\text{KL}_w^J := \mu^{-\ell(w w_J)} \psi(\gamma_{w w_J}) \odot \text{pt}_e^t \in (\mathbf{D}_t^*)^{W^J} \cong \mathfrak{h}_T(G/P_J).$$

Remark 26. Following [Lenart et al. 2020], one can define a certain involution on some subset $\mathcal{N}_J := \psi(H) \odot \text{pt}_e^t \subset \mathbf{D}_t^*$ so that KL_v^J is invariant under such an involution, similar to the parabolic Kazhdan–Lusztig basis of Deodhar.

Writing the Kazhdan–Lusztig basis as $\gamma_w = \sum_{v \leq w} b_{w,v} \delta_v$, $b_{w,v} \in S_m$, we then have in $K_T(G/B)$

$$C_w = \gamma_w \odot \text{pt}_e^m = \sum_{v \leq w} b_{w,v} \delta_v \odot \left(\prod_{\alpha > 0} (1 - e^\alpha) f_e^m \right) = \sum_{v \leq w} b_{w,v} v \left(\prod_{\alpha > 0} (1 - e^\alpha) \right) f_v^m.$$

On the other hand, inside $\mathfrak{h}_T(G/B)$, we have

$$\text{KL}_w = \mu^{-\ell(w)} \psi(\gamma_w) \odot \text{pt}_e^t = \mu^{-\ell(w)} \sum_{v \leq w} \psi(b_{w,v}) v \left(\prod_{\alpha > 0} x_{-\alpha} \right) f_v^t.$$

Here $x_\alpha \in S_t$. It would be interesting to compare the two classes in different cohomology theories. Here is an example.

Example 27. We consider the SL_3 case, so there are two simple roots α_1, α_2 . Recall that in S_m , we have $x_\lambda = 1 - e^{-\lambda}$. Write $\hat{x}_\lambda = t - t^{-1} e^{-\lambda}$. For simplicity, write $x_{\pm i \pm j} := x_{\pm \alpha_i \pm \alpha_j}$ and $\hat{x}_{\pm i \pm j} = \hat{x}_{\pm \alpha_i \pm \alpha_j}$. Inside $H \subset Q_{m,W}$, we have

$$\begin{aligned} \gamma_{s_i} &= (\delta_{s_i} + 1) \frac{\hat{x}_{-i}}{x_{-i}}, \\ \gamma_{s_1 s_2} &= (\delta_{s_1 s_2} + \delta_{s_2}) \frac{\hat{x}_{-1-2} \hat{x}_{-2}}{x_{-1-2} x_{-2}} + (\delta_{s_1} + 1) \frac{\hat{x}_{-1} \hat{x}_{-2}}{x_{-1} x_{-2}}, \\ \gamma_{s_1 s_2 s_1} &= (\delta_{s_1 s_2 s_1} + \delta_{s_1 s_2} + \delta_{s_2 s_1} + \delta_{s_1} + \delta_{s_2} + 1) \frac{\hat{x}_{-1} \hat{x}_{-2} \hat{x}_{-1-2}}{x_{-1} x_{-2} x_{-1-2}}. \end{aligned}$$

Recall that $\text{pt}_e^m = x_{-1} x_{-2} x_{-1-2} f_e^m \in \mathbf{D}_m^*$. So inside $\mathbf{D}_m^* \cong K_T(G/B) \otimes_{\mathbb{Z}} R$, we have

$$\begin{aligned} C_e &= \text{pt}_e^m, \\ C_{s_1} &= \hat{x}_{-1} x_{-2} x_{-1-2} f_e^m + \hat{x}_1 x_{-2} x_{-1-2} f_{s_1}^m, \\ C_{s_1 s_2} &= \hat{x}_{-1} \hat{x}_{-2} x_{-1-2} f_e^m + \hat{x}_1 \hat{x}_{-1-2} x_{-2} f_{s_1}^m + \hat{x}_{-1} \hat{x}_2 x_{-1-2} f_{s_2}^m + \hat{x}_1 \hat{x}_{1+2} x_{-2} f_{12}^m, \end{aligned}$$

$$C_{s_1s_2s_1} = \hat{x}_{-1}\hat{x}_{-2}\hat{x}_{-1-2}f_e^m + \hat{x}_1\hat{x}_{-2}\hat{x}_{-1-2}f_{s_1}^m + \hat{x}_{-1}\hat{x}_2\hat{x}_{-1-2}f_{s_2}^m + \hat{x}_1\hat{x}_{1+2}\hat{x}_{-1-2}f_{s_1s_2}^m \\ + \hat{x}_2\hat{x}_{1+2}\hat{x}_{-1}f_{s_2s_1}^m + \hat{x}_1\hat{x}_2\hat{x}_{1+2}f_{s_1s_2s_1}^m.$$

Note that so far in this example all notation is in S_m , $Q_{m,w}$ or D_m^* .

On the other hand, one can compute $KL_w \in \mathfrak{h}_T(G/B)$ as follows: Note that $\psi(\hat{x}_i/x_i) = \mu/x_i$ (where the first x_i is in S_m and the second x_i is in S_t). Then

$$KL_e = \text{pt}_e^t, \quad KL_{s_1s_2} = x_{-1-2}f_e^t + x_{-2}f_{s_1}^t + x_{-1-2}f_{s_2}^t + x_{-2}f_{s_1s_2}^t, \\ KL_{s_1} = x_{-1}x_{-1-2}f_e^t + x_{-1-2}x_{-2}f_{s_1}^t, \quad KL_{s_1s_2s_1} = f_e^t + f_{s_1}^t + f_{s_2}^t + f_{s_1s_2}^t + f_{s_2s_1}^t + f_{s_1s_2s_1}^t.$$

In this case, all Schubert varieties are smooth, and it is easy to verify that the classes KL_w coincide with the Schubert classes.

We now prove the smoothness conjecture [Lenart et al. 2020, Conjecture 5.14]. Several special cases were proved in [Lenart and Zainoulline 2017; Lenart et al. 2020], such as the case of $w = w_{J/J'}$ for $J' \subset J \subseteq \Pi$ (i.e., w has “relative” maximal length), and that of Schubert varieties in complex projective spaces.

Theorem 28. *If the Schubert variety $X(w)$ is smooth, then the class determined by $X(w)$ in $\mathfrak{h}_T(G/B)$ coincides with the KL Schubert class KL_w .*

Proof. Since $X(w)$ is smooth, $P_{v,w} = 1$ for any $v \leq w$; see [Billey and Lakshmibai 2000, 6.1.19]. Therefore,

$$\gamma_w = \sum_{v \leq w} t_w t_v^{-1} \tau_v = t_w \sum_{v \leq w} t_v^{-1} \tau_v = t_w \Gamma_w = t_w \sum_{v \leq w} a_{w,v} \delta_v^m.$$

From the definition of ψ , it is easy to verify that

$$\psi\left(\frac{1-t^{-2}e^\alpha}{1-e^\alpha}\right) = \frac{t^{-1}\mu}{x_{-\alpha}}. \tag{19}$$

Then for any $w \in W$, we have

$$KL_w = \mu^{-\ell(w)} \psi(\gamma_w) \odot \text{pt}_e^t \\ = \mu^{-\ell(w)} \psi\left(t_w \sum_{v \leq w} a_{w,v} \delta_v^m\right) \odot \text{pt}_e^t \\ = \mu^{-\ell(w)} t_w \sum_{v \leq w} \psi\left(\prod_{\alpha > 0, v s_\alpha \leq w} \frac{1-t^{-2}e^{u\alpha}}{1-e^{u\alpha}}\right) \delta_v^t \odot \text{pt}_e^t \quad (\text{by Corollary 11}) \\ = \mu^{-\ell(w)} t_w \sum_{v \leq w} \left(\prod_{\alpha > 0, v s_\alpha \leq w} \frac{t^{-1}\mu}{x_{-v\alpha}}\right) \cdot v(x_\Pi^t) f_v^t \quad (\text{by (5) and (19)}) \\ = \sum_{v \leq w} v \left(\frac{\prod_{\alpha < 0} x_\alpha}{\prod_{\alpha < 0, v s_\alpha \leq w} x_\alpha}\right) f_v^t \\ = \sum_{v \leq w} \frac{\prod_{\alpha > 0} x_{-\alpha}}{\prod_{\alpha > 0, s_\alpha v \leq w} x_{-\alpha}} f_v^t.$$

Here the fifth identity follows from the well-known fact that

if $X(w)$ is smooth, then $|\{\alpha > 0 \mid s_\alpha v \leq w\}| = \ell(w)$ for any $v \leq w \in W$,

and the last one is proved as follows: for any $v \leq w \in W$,

$$\begin{aligned} \frac{\prod_{\alpha < 0} x_{v\alpha}}{\prod_{\alpha < 0, v s_\alpha \leq w} x_{v\alpha}} &= \frac{\prod_{\alpha > 0, s_\alpha v < v} x_\alpha \cdot \prod_{\alpha > 0, v < s_\alpha v} x_{-\alpha}}{\prod_{\alpha > 0, s_\alpha v < v} x_\alpha \cdot \prod_{\alpha > 0, v < s_\alpha v \leq w} x_{-\alpha}} \\ &= \frac{\prod_{\alpha > 0, s_\alpha v < v} x_{-\alpha} \cdot \prod_{\alpha > 0, v < s_\alpha v} x_{-\alpha}}{\prod_{\alpha > 0, s_\alpha v < v} x_{-\alpha} \cdot \prod_{\alpha > 0, v < s_\alpha v \leq w} x_{-\alpha}} \\ &= \frac{\prod_{\alpha > 0} x_{-\alpha}}{\prod_{\alpha > 0, s_\alpha v \leq w} x_{-\alpha}}. \end{aligned}$$

Comparing with the restriction formula of $[X(w)]$ in [Lenart et al. 2020, (5.6)], we see that $\text{KL}_w = [X(w)]$. The proof is finished. \square

We now look at the case of partial flag varieties. Let P_J be the parabolic subgroup with the projection map $\pi_J : G/B \rightarrow G/P_J$. Let w_J be the longest element in the subgroup W_J of W determined by J , and $W^J \subset W$ be the set of minimal length representatives of W/W_J . Recall $X(w)_J$ denotes the Schubert variety of G/P_J determined by $w \in W^J$.

For G/P_J , the definition of the KL Schubert class KL_w^J corresponding to $w \in W^J$ is defined by using the so-called parabolic Kazhdan–Lusztig basis. According to the paragraph right after [Lenart et al. 2020, Definition 5.9], via the embedding $\pi_J^* : \mathfrak{h}_T(G/P_J) \rightarrow \mathfrak{h}_T(G/B)$, we have

$$\pi_J^*(\text{KL}_w^J) = \text{KL}_{ww_J}.$$

Corollary 29. *Conjecture 5.14 of [Lenart et al. 2020] holds for any partial flag variety G/P_J ; that is, if the Schubert variety $X(w)_J$ of G/P_J is smooth for $w \in W^J$, then the KL Schubert class KL_w^J of w coincides with the fundamental class $[X(w)_J]$.*

Proof. We have the following commutative diagram:

$$\begin{array}{ccc} \pi_J^{-1}(X(w)_J) & \xrightarrow{i'} & G/B \\ \downarrow \pi_J & & \downarrow \pi_J \\ X(w)_J & \xrightarrow{i} & G/P_J \end{array}$$

Moreover, $\pi_J^{-1}(X(w)_J) = X(ww_J)$. Since $X(w)_J$ is smooth, $X(ww_J)$ is also smooth. Thus, Theorem 28 implies $[X(ww_J)] = \text{KL}_{ww_J}$. On the other hand, by proper base change, we obtain

$$\pi_J^*[X(w)_J] = \pi_J^* i_* [1_{X(w)_J}] = i'_* \pi_J^* [1_{X(w)_J}] = i'_* [1_{X(ww_J)}] = [X(ww_J)],$$

where the third equality follows from the fact that the pullback π_J^* preserves identity. Since $\pi_J^*(\text{KL}_w^J) = \text{KL}_{ww_J}$, and π_J^* is injective, we get $\text{KL}_w^J = [X(ww_J)] \in \mathfrak{h}_T(G/P_J)$. \square

6. KL Schubert classes and small resolutions

In this section, we give a geometric interpretation of the KL Schubert classes (for hyperbolic cohomology) in the case of type A Grassmannians.

For subsets $J' \subset J \subseteq \Pi$, for hyperbolic cohomology, we will use relative push–pull elements $Y_{J'/J}^t$ defined in (1). For simplicity, we will skip the superscript t . Moreover, if $Q \subset P$ are the parabolic subgroups corresponding to $J' \subset J$, respectively, we will write $Y_{P/Q} = Y_{J'/J}$.

Consider the Grassmannian $\text{Gr}_d(\mathbb{C}^{n-d}) = \text{SL}_n/P_J$, where the set of simple roots Π is identified with $\{1, \dots, n-1\}$ and $J := \Pi - \{d\}$. Fix a Schubert variety $X(\lambda)$ of it, which is indexed by a partition $\lambda = (\lambda_1 \geq \dots \geq \lambda_l > 0)$ contained inside the $d \times (n-d)$ rectangle; here we mean that λ is identified with a Young diagram (in English notation), whose top left box is placed on the top left box of the mentioned rectangle.

Alternatively, the Schubert variety $X(\lambda)$ is indexed by a d -subset I_λ of $[n] := \{1, \dots, n\}$, which is constructed as follows. Place the above $d \times (n-d)$ rectangle inside the first quadrant of the xy -plane so that its southwest corner is the origin. Label each horizontal (resp. vertical) unit segment whose left (resp. bottom) endpoint is a lattice point (x, y) by $x + y + 1$. Consider the lattice path from $(0, 0)$ to $(n-d, d)$ defining the southeast boundary of the Young diagram λ when embedded into the $d \times (n-d)$ rectangle as stated above. Then I_λ consists of the labels on the vertical steps of this path.

Yet another indexing of the Schubert variety $X(\lambda)$ is by a *Grassmannian permutation* w_λ in the symmetric group $W = S_n$, which has its unique descent in position d . Written in one-line notation, w_λ consists of the entries in I_λ followed by the entries in $[n] - I_\lambda$, where both sets of entries are ordered increasingly. Here we use $-$ for set difference. Thus, w_λ belongs to the set W^J of lowest coset representatives modulo the parabolic subgroup W_J . Moreover, it has the reduced decomposition

$$w_\lambda = \prod_{(i,j) \in \lambda}^{\rightarrow} s_{d+j-i}, \tag{20}$$

where (i, j) is the box of the Young diagram λ in row i and column j , while in the product we scan the rows of λ from bottom to top, and each row from right to left.

Example 30. We use as a running example the same one as in [Billey and Lakshmibai 2000, Example 9.1.11], namely $n = 10$, $d = 5$, $\lambda = (5, 5, 3, 2, 2)$, $I_\lambda = \{3, 4, 6, 9, 10\}$. In order to illustrate (20), we place the number $d + j - i$ in the box (i, j) of λ , as follows:

5	6	7	8	9
4	5	6	7	8
3	4	5		
2	3			
1	2			

(21)

Thus, we have

$$w_\lambda = [3, 4, 6, 9, 10, 1, 2, 5, 7, 8] = (s_2s_1)(s_3s_2)(s_5s_4s_3)(s_8s_7s_6s_5s_4)(s_9s_8s_7s_6s_5). \tag{22}$$

In [Billey and Lakshmibai 2000, Section 9.1], the permutation w_λ is identified with the d -subset I_λ , and they are encoded into a $2 \times m$ matrix

$$\begin{pmatrix} k_1 \cdots k_m \\ a_1 \cdots a_m \end{pmatrix}, \tag{23}$$

which can be read off from the above lattice path as follows. The entries $0 < k_1 < \cdots < k_m \leq n$ are the labels of the last steps in consecutive sequences of vertical (unit) steps. The entries a_1, \dots, a_m are the lengths of these sequences. The numbers b_0, \dots, b_{m-1} calculated in [Billey and Lakshmibai 2000] are the lengths of the sequences of horizontal steps, where we set $b_0 := 0$ if $l < d$ (i.e., if the lattice path starts with a vertical step). Recall that we also set $a_0 = b_m := \infty$.

Recall that the Schubert variety $X(\lambda)$ has *small resolutions*, which were defined by Zelevinsky [1983]. We briefly recall their construction following [Billey and Lakshmibai 2000, Section 9.1]. This construction starts with the choice of an index i , with $0 \leq i < m$, such that $b_i \leq a_i$ and $a_{i+1} \leq b_{i+1}$ (any such choice can be made). While it is clear that such an index always exists, we avoid the choice of $i = 0$ if $l < d$. Then, a new permutation w^2 is obtained from $w^1 := w_\lambda$ via a certain procedure, which can be rephrased as follows. Consider the i -th outer corner of λ (counting from 0), from southwest to northeast, where the origin is an outer corner if and only if $l < d$. Consider the rectangle R_1 (inside λ) whose southeast vertex is the mentioned outer corner, and which is maximal in that its removal from λ still leaves a Young diagram. It is clear that the size of R_1 is $b_i \times a_{i+1}$. Then w^2 is the Grassmannian permutation corresponding to the Young diagram $\lambda - R_1$.

The above procedure is then iterated. We thus tile the Young diagram λ with rectangles R_1, \dots, R_r . Let us denote by p_i and q_i the height and width of R_i , respectively. We also define the sequence of Grassmannian permutations w^1, \dots, w^r so that the Young diagram of w^i is $\lambda^i := \lambda - \rho^{i-1}$, where $\rho^j := R_1 \cup \dots \cup R_j$. In particular, the Young diagram of w^r is R_r , and the Schubert variety $X(w^r)$ is smooth. Note that $r = m$ if $l = d$, and $r = m - 1$ if $l < d$.

Example 31. We continue Example 30. The encoding of w_λ by the $2 \times m$ matrix (23) and the successive choices of w^1, w^2, w^3 based on it are described in detail in [Billey and Lakshmibai 2000]. In our setup, the tiling of λ with the corresponding rectangles R_1, R_2, R_3 is illustrated below (the number in a box is the index of the rectangle to which that box belongs).

3	3	2	2	2
3	3	2	2	2
3	3	1		
3	3			
3	3			

In order to complete the construction of the Zelevinsky resolution, following [Billey and Lakshmibai 2000, Section 9.1], we need the stabilizer P_{w_λ} of the Schubert variety $X(\lambda) = X(w_\lambda)$. This is the parabolic subgroup corresponding to the subset $\Pi - \{k_1, \dots, k_m\}$; compare (23). More generally, consider the

stabilizers $P_i := P_{w^i}$, for $i = 1, \dots, r$, and $P_{r+1} := P_J$; for simplicity, we use the same notation for the corresponding subsets of Π . Also let $Q_i := P_i \cap P_{i+1}$, for $i = 1, \dots, r$, both as parabolic subgroups and subsets of Π . Then the Zelevinsky resolution of $X(w)$ is expressed as follows:

$$P_1 \times^{Q_1} P_2 \times \cdots \times^{Q_{r-2}} P_{r-1} \times^{Q_{r-1}} X(w^r) =: \tilde{X}(w_\lambda) \rightarrow X(w_\lambda). \tag{24}$$

Therefore, by Corollaries 4 and 29, the pushforward of the fundamental class of $\tilde{X}(w_\lambda)$ inside $\mathfrak{h}_T(G/B)$ is the element

$$Y_{P_1/Q_1} \cdots Y_{P_r/Q_r} Y_J \odot \text{pt}_e^t. \tag{25}$$

Example 32. Continuing Example 31, the operator in (25) is written explicitly as

$$Y_{(\Pi-\{4,6\})/(\Pi-\{4,5,6\})} Y_{(\Pi-\{5\})/(\Pi-\{5,7\})} Y_{(\Pi-\{7\})/(\Pi-\{5,7\})} Y_{\Pi-\{5\}}.$$

Indeed, the parabolic subsets P_i for these examples were exhibited in [Billey and Lakshmibai 2000], while they can also be read off from the Young diagram of $\lambda = (5, 5, 3, 2, 2)$ as indicated above.

We will now state the main technical result of this section, Theorem 34, which is interesting itself, and is needed to make the connection with the KL Schubert classes for the Grassmannian; compare [Lenart et al. 2020]. To this end, we introduce more notation in the above setup. Given the rectangle R_i , with its embedding into the Young diagram of λ and the first quadrant, let C_i and D_i be the sets of labels on its left vertical side and its top horizontal side, respectively. Let

$$c_i := \min C_i, \quad d_i := \max D_i = c_i + p_i + q_i - 1, \quad C'_i := C_i - \{\max C_i\}, \quad D'_i := D_i - \{d_i\}.$$

Finally, let $J_i := C_i \sqcup D'_i$ and $J'_i := C'_i \sqcup D'_i$.

We also need to define the subsets $K'_i \subsetneq K_i$ of Π for $i = 1, \dots, r$. First recall that above we defined the shape ρ^i as the union of the rectangles R_1, \dots, R_i . It is not hard to see that ρ^i is a union of completely disjoint Young diagrams (i.e., they do not share even a single point), aligned from southwest to northeast. Let \mathcal{C}_i be set of indices $j \in \{1, \dots, i\}$ such that the left side of R_j is contained in the left boundary of a component of ρ^i . Similarly, let \mathcal{D}_i be set of indices $k \in \{1, \dots, i\}$ such that the top side of R_k is contained in the top boundary of a component of ρ^i . We now define

$$K'_i := \left(\bigsqcup_{j \in \mathcal{C}_i} C'_j \right) \sqcup \left(\bigsqcup_{k \in \mathcal{D}_i} D'_k \right), \quad K_i := K'_i \sqcup \{\max C_i\}.$$

Note that $J_i \subseteq K_i$ and $J'_i \subseteq K'_i$.

Example 33. Continuing Example 32, we have

$$\begin{aligned} K'_1 = J'_1 = \emptyset \subsetneq K_1 = J_1 = \{5\}, & \quad K'_3 = \{1, 2, 3, 4, 6, 8, 9\} \subsetneq K_3 = \{1, 2, 3, 4, 5, 6, 8, 9\}, \\ K'_2 = J'_2 = \{6, 8, 9\} \subsetneq K_2 = J_2 = \{6, 7, 8, 9\}, & \quad J'_3 = \{1, 2, 3, 4, 6\} \subsetneq J_3 = \{1, 2, 3, 4, 5, 6\}. \end{aligned}$$

As indicated above, all this information is easily read off from the Young diagram of $\lambda = (5, 5, 3, 2, 2)$.

Theorem 34. *In $H \subset Q_{m,W}$, we have*

$$\gamma_{w_\lambda w_J} = \gamma_{J_1/J'_1} \cdots \gamma_{J_r/J'_r} \gamma_J = \gamma_{K_1/K'_1} \cdots \gamma_{K_r/K'_r} \gamma_J. \tag{26}$$

In order to prove Theorem 34, we start by recalling some results from [Kirillov and Lascoux 2000], related to the factorization of Kazhdan–Lusztig elements for the Grassmannian. This paper introduces an element Z_{w_λ} of the Hecke algebra, defined as a product of linear factors in the generators, which are associated with the boxes of the Young diagram λ . Instead of recalling the precise definition, which is not needed here, we will state a weaker form of the factorization, which turns out to be related to factorizations in (26). We will use notation introduced above.

The rectangle R_i corresponds to the Grassmannian permutation

$$v^i := (s_{c_i+q_i-1} \cdots s_{c_i})(s_{c_i+q_i} \cdots s_{c_i+1}) \cdots (s_{c_i+p_i+q_i-2} \cdots s_{c_i+p_i-1});$$

compare (20) and Example 30. It is not hard to see that we have the following factorization of w_λ , which corresponds to a reduced decomposition of w_λ obtained from (20) only by commuting simple reflections:

$$w_\lambda = v^1 \cdots v^r. \tag{27}$$

Example 35. In our running example, the reduced decomposition corresponding to (27) (to be compared with (22) and also (21)) is

$$w_\lambda = [3, 4, 6, 9, 10, 1, 2, 5, 7, 8] = \underbrace{(s_5)}_{v^1} \underbrace{((s_8 s_7 s_6)(s_9 s_8 s_7))}_{v^2} \underbrace{((s_2 s_1)(s_3 s_2)(s_4 s_3)(s_5 s_4)(s_6 s_5))}_{v^3}.$$

The factorization of Z_{w_λ} needed here is the following one, which corresponds to the factorization (27) of w_λ :

$$Z_{w_\lambda} = Z_{v^1} Z_{w^2} = Z_{v^1} \cdots Z_{v^r}. \tag{28}$$

See the proof of [Kirillov and Lascoux 2000, Theorem 3] for details.

The connection between the element Z_{w_λ} and the corresponding parabolic Kazhdan–Lusztig basis element is made in [Kirillov and Lascoux 2000, Theorem 3].

Theorem 36 [Kirillov and Lascoux 2000]. *In $H \subset Q_{m,W}$, we have*

$$Z_{w_\lambda} \gamma_J = \gamma_{w_\lambda w_J}.$$

The proof of Theorem 34 also relies on the following lemmas.

Lemma 37. *Consider $J' \subset J \subseteq \Pi$, and assume that $J \subset [a, b]$ with $a, b \in \Pi$. If $A \subseteq \Pi - [a - 1, b + 1]$, then we have*

$$\gamma_{J/J'} = \gamma_{J \sqcup A / J' \sqcup A} \in Q_{m,W}, \quad Y_{J/J'} = Y_{J \sqcup A / J' \sqcup A} \in Q_{t,W}.$$

Proof. As the sets of simple roots corresponding to J and A are orthogonal to each other, we have $\Sigma_{J \sqcup A}^- = \Sigma_J^- \sqcup \Sigma_A^-$ and $W_{J \sqcup A} = W_J \times W_A$, and similarly for J replaced by J' . Therefore, we have

$$w_{J/J'} := w_J w_{J'} = w_J w_A w_{J'} w_A =: w_{J \sqcup A / J' \sqcup A}, \quad x_{J/J'} = x_{J \sqcup A / J' \sqcup A}, \tag{29}$$

and $W_J/W_{J'}$ is in a natural bijection with $W_{J \sqcup A}/W_{J' \sqcup A}$. The stated equalities follow by plugging these facts into (7) and the definition (1) of the relative push–pull operator. \square

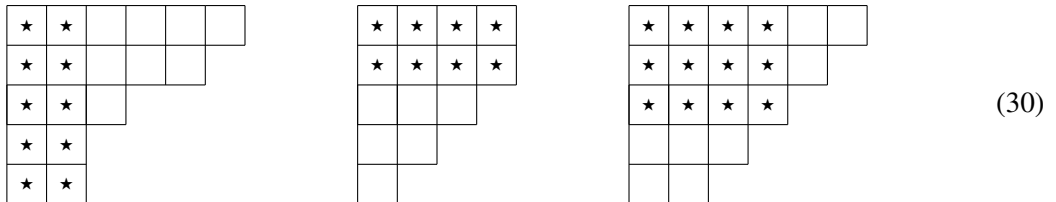
Lemma 38. (1) *We have*

$$K_1 = J_1 \supsetneq K'_1 = J'_1 \subsetneq K_2 \supsetneq K'_2 \subsetneq \cdots \subsetneq K_r \supsetneq K'_r \subseteq J.$$

(2) *For every $i = 1, \dots, r$, we have*

$$\begin{aligned} \gamma_{J_i/J'_i} &= \gamma_{K_i/K'_i} \in \mathcal{Q}_{m,W}, & \gamma_{J'_i \setminus J_i} &= \gamma_{K'_i \setminus K_i} \in \mathcal{Q}_{m,W}, \\ Y_{J_i/J'_i} &= Y_{K_i/K'_i} \in \mathcal{Q}_{t,W}, & Y_{J'_i \setminus J_i} &= Y_{K'_i \setminus K_i} \in \mathcal{Q}_{t,W}. \end{aligned}$$

Proof. It is clear that $K'_r \subseteq J$. Thus, in order to complete the first part, we need to prove $K'_{i-1} \subsetneq K_i$, for $i = 2, \dots, r$. This is obvious if the rectangle R_i is, by itself, a connected component of the shape ρ^i . Other than this, there are three ways in which R_i can be attached to ρ^{i-1} , which are indicated below; the boxes of R_i are marked with \star , and the empty boxes form the relevant component(s) of ρ^{i-1} .



Note that the height (respectively width) of R_i is strictly greater than the number of rows (respectively columns) of the relevant Young diagram to its right (respectively at the bottom). It is also useful to observe that all unit segments with the same label form a northwest to southeast staircase shape, and the labels increase by 1 as we move northeast.

Let B denote the set of labels on the boundary of the rectangle R_i . Using the above notation, in all three cases in (30), we have

$$B = C_i \sqcup D_i = \{c_i, \dots, d_i\}, \quad K_i - B = K'_{i-1} - B, \quad K_i \cap B = C_i \sqcup D'_i = B - \{d_i\} =: J_i.$$

On the other hand, we have $d_i \notin K'_{i-1}$; indeed, in the first and last case in (30), the label d_i is on the left side of a rectangle R_j with $j \in C_{i-1}$, but $d_i \notin C'_j$, because it is the top label on the mentioned side. We conclude that $K'_{i-1} \subseteq K_i$. In fact, the inclusion is strict because we also have $c_i + q_i - 1 \in (K_i \cap B) - K'_{i-1}$.

For the second part, we note that, in addition to the above facts, we have $K'_i \cap B = C'_i \sqcup D'_i =: J'_i$ and $c_i - 1 \notin K_i$. For the latter part, note that, in the last two cases in (30), the label $c_i - 1$ is on the left side of a rectangle R_j with $j \in C_i$ and $j \neq i$, but $c_i - 1 \notin C'_j$, because it is the top label on the mentioned side. The proof is concluded by applying Lemma 37. \square

Proof of Theorem 34. By using the analogue of Lemma 5 for γ , we have

$$\gamma_{K_2/K'_2} \cdots \gamma_{K_r/K'_r} \gamma_J = \gamma_{K_2} \gamma_{K'_2 \setminus K_3} \cdots \gamma_{K'_{r-1} \setminus K_r} \gamma_{K'_r \setminus J} = \gamma_{K'_1} \gamma_{K'_1 \setminus K_2} \gamma_{K'_2 \setminus K_3} \cdots \gamma_{K'_{r-1} \setminus K_r} \gamma_{K'_r \setminus J}. \quad (31)$$

We now prove the theorem using induction on r , with base case $r = 0$, which is trivial. We have

$$\begin{aligned}
 \gamma_{w_\lambda w_J} &\stackrel{\sharp_1}{=} Z_{w_\lambda} \gamma_J \stackrel{\sharp_2}{=} Z_{v^1} Z_{w^2} \gamma_J \stackrel{\sharp_3}{=} Z_{v^1} \gamma_{w^2 w_J} \\
 &\stackrel{\sharp_4}{=} Z_{v^1} \gamma_{J_2/J'_2} \cdots \gamma_{J_r/J'_r} \gamma_J \stackrel{\sharp_5}{=} Z_{v^1} \gamma_{K_2/K'_2} \cdots \gamma_{K_r/K'_r} \gamma_J \\
 &\stackrel{\sharp_6}{=} Z_{v^1} \gamma_{K'_1} \gamma_{K'_1 \setminus K_2} \cdots \gamma_{K'_{r-1}} \gamma_{K_r} \gamma_{K'_r \setminus J} \\
 &\stackrel{\sharp_7}{=} \gamma_{K_1} \gamma_{K'_1 \setminus K_2} \cdots \gamma_{K'_{r-1} \setminus K_r} \gamma_{K'_r \setminus J} \\
 &\stackrel{\sharp_8}{=} \gamma_{K_1/K'_1} \gamma_{K_2/K'_2} \cdots \gamma_{K_r/K'_r} \gamma_J \stackrel{\sharp_9}{=} \gamma_{J_1/J'_1} \gamma_{J_2/J'_2} \cdots \gamma_{J_r/J'_r} \gamma_J.
 \end{aligned}$$

Here \sharp_1 , \sharp_3 , and \sharp_7 are based on Theorem 36, \sharp_2 on (28), \sharp_4 on the induction hypothesis, \sharp_5 and \sharp_9 on Lemma 38(2), \sharp_6 and \sharp_8 on (31), and \sharp_8 on (8); additionally, in \sharp_7 we use the fact that

$$K_1 = J_1 = C_1 \sqcup D'_1 = \{c_1, \dots, d_1 - 1\}, \quad K'_1 = J'_1 = C'_1 \sqcup D'_1 = K_1 - \{\max C_1\},$$

and thus we have $v^1 w_{K'_1} = w_{K_1}$. □

Remark 39. We could not have carried out the above proof using only one of the pairs (J_i, J'_i) and (K_i, K'_i) . Indeed, the first pair does not satisfy the property in Lemma 38(1), which is crucial in the proof. On the other hand, the induction procedure cannot be applied based on the second pair because the respective sets for $\lambda^1 = \lambda$ and λ^2 (corresponding to w^2) are different.

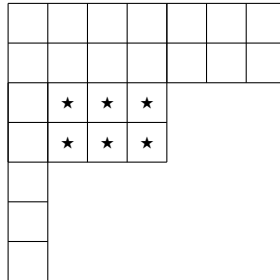
In order to relate Theorem 34 to the Zelevinsky resolution, and more specifically to the operator (25), we need the following result.

Lemma 40. *For every $i = 1, \dots, r$, we have*

$$Y_{J_i/J'_i} = Y_{K_i/K'_i} = Y_{P_i/Q_i}.$$

Proof. By using Lemma 38(2), it suffices to prove $Y_{J_i/J'_i} = Y_{P_i/Q_i}$. Moreover, it suffices to consider $i = 1$, as we can just replace the partition $\lambda^1 = \lambda$ with λ^i . Recall that P_1 is obtained by considering the lattice path from $(0, 0)$ to $(n - d, d)$ defining the southeast boundary of λ^1 , and by excluding from Π the last label in each sequence of vertical steps. Similarly, P_2 corresponds to $\lambda^2 := \lambda - R_1$.

Let B denote the set of labels on the boundary of the rectangle R_1 ; see the diagram below, where the boxes of R_1 are marked with \star .



Using the above notation, we have $B = C_1 \sqcup D_1 = \{c_1, \dots, d_1\}$. Based on the above interpretation of P_1 and P_2 , we deduce

$$\begin{aligned} P_1 \cap B &= C_1 \sqcup D'_1 =: J_1 = B - \{d_1\}, \\ P_2 \cap B &= C'_1 \sqcup D_1, \text{ which implies } Q_1 \cap B = C'_1 \sqcup D'_1 =: J'_1, \\ P_1 - B &\subset P_2 - B, \text{ which implies } P_1 - B = Q_1 - B. \end{aligned}$$

Moreover, we have $c_1 - 1 \notin P_1$ and $d_1 \notin P_1$. Thus, we are under the hypotheses of Lemma 37, so the conclusion follows. \square

We now rephrase Theorem 34 as follows, via the map ψ .

Corollary 41. *We have*

$$\mu^{-\ell(w_\lambda w_J)} \psi(\gamma_{w_\lambda w_J}) = Y_{P_1/Q_1} \cdots Y_{P_r/Q_r} Y_J \in \mathbf{D}_t. \quad (32)$$

Proof. We start by observing that

$$w_{K_i/K'_i} = w_{J_i/J'_i} = v^i \Rightarrow \ell(w_{K_i/K'_i}) = p_i q_i = |R_i|, \quad (33)$$

where $|R_i|$ denotes the number of boxes of the rectangle R_i . Here the first equality is based on (29) and the fact that this result can be applied to the pairs (J_i, J'_i) and (K_i, K'_i) , as discussed in the proof of Lemma 38; the second equality is clear by the definition of v^i .

We now apply $\mu^{-\ell(w_\lambda w_J)} \psi(\cdot)$ to the first and last part of (26). After doing this, the latter can be written as follows:

$$\begin{aligned} &\mu^{-\ell(w_\lambda w_J)} \psi(\gamma_{K_1/K'_1}) \cdots \psi(\gamma_{K_r/K'_r}) \psi(\gamma_J) \\ &\stackrel{\sharp_1}{=} (\mu^{-\ell(w_{K_1/K'_1})} \psi(\gamma_{K_1/K'_1})) \cdots (\mu^{-\ell(w_{K_r/K'_r})} \psi(\gamma_{K_r/K'_r})) (\mu^{-\ell(w_J)} \psi(\gamma_J)) \\ &\stackrel{\sharp_2}{=} (\mu^{-\ell(w_{K_1/K'_1})} \psi(\gamma_{K_1/K'_1})) \cdots (\mu^{-\ell(w_{K_r/K'_r})} \psi(\gamma_{K_r/K'_r})) Y_J \\ &\stackrel{\sharp_3}{=} (\mu^{-\ell(w_{K_1/K'_1})} \psi(\gamma_{K_1/K'_1})) \cdots (\mu^{-\ell(w_{K_r/K'_r})} \psi(\gamma_{K_r/K'_r})) Y_{K'_r} Y_{K'_r \setminus J} \\ &\stackrel{\sharp_4}{=} (\mu^{-\ell(w_{K_1/K'_1})} \psi(\gamma_{K_1/K'_1})) \cdots (\mu^{-\ell(w_{K_{r-1}/K'_{r-1}})} \psi(\gamma_{K_{r-1}/K'_{r-1}})) Y_{K_r} Y_{K'_r \setminus J} \\ &= \cdots \stackrel{\sharp_5}{=} Y_{K_1} Y_{K'_1 \setminus K_2} \cdots Y_{K'_r \setminus J} \\ &\stackrel{\sharp_6}{=} Y_{K_1/K'_1} \cdots Y_{K_r/K'_r} Y_J \stackrel{\sharp_7}{=} Y_{P_1/Q_1} \cdots Y_{P_r/Q_r} Y_J. \end{aligned}$$

Here \sharp_1 is based on (33) and the fact that $\ell(w_\lambda) = \sum_i |R_i|$. Equalities \sharp_2 and \sharp_4 are based on (18), \sharp_3 on (2), \sharp_5 on the repeated use of an argument similar to \sharp_3 followed by \sharp_4 , \sharp_6 on Lemma 5 and \sharp_7 on Lemma 40. \square

We now state the main result of this section.

Theorem 42. *The KL Schubert classes for the Grassmannian coincide with the hyperbolic cohomology classes of the corresponding Zelevinsky resolutions.*

Proof. The result is now immediate by comparing the left- and right-hand sides of (32) with Definition 25 and (25), respectively. \square

Remark 43. Theorem 42 implies that all the Zelevinsky resolutions of a Schubert variety in the Grassmannian have the same class in hyperbolic cohomology (i.e., the corresponding KL Schubert class). This agrees with a result of Totaro [2000], which says that the algebraic theories in a larger class (defined by Krichever [Buchstaber and Bunkova 2010]), which includes hyperbolic cohomology, are invariant under small resolutions.

Acknowledgements

We thank Samuel Evens, Leonardo Mihalcea, and Richard Rimányi for helpful conversations. Lenart acknowledges the partial support from the NSF grants DMS-1362627 and DMS-1855592. Zainoulline acknowledges the partial support from the NSERC Discovery grant RGPIN-2015-04469, Canada. Su thanks J. Schürmann for useful discussions and further thanks P. Aluffi, L. Mihalcea, H. Naruse and G. Zhao for related collaborations. We thank the referees for useful suggestions.

References

- [Aganagic and Okounkov 2021] M. Aganagic and A. Okounkov, “Elliptic stable envelopes”, *J. Amer. Math. Soc.* **34**:1 (2021), 79–133. MR Zbl
- [Aluffi and Mihalcea 2016] P. Aluffi and L. C. Mihalcea, “Chern–Schwartz–MacPherson classes for Schubert cells in flag manifolds”, *Compos. Math.* **152**:12 (2016), 2603–2625. MR Zbl
- [Aluffi et al. 2017] P. Aluffi, L. C. Mihalcea, J. Schürmann, and C. Su, “Shadows of characteristic cycles, Verma modules, and positivity of Chern–Schwartz–MacPherson classes of Schubert cells”, 2017. To appear in *Duke Math. J.* arXiv 1709.08697
- [Aluffi et al. 2019] P. Aluffi, L. C. Mihalcea, J. Schürmann, and C. Su, “Motivic Chern classes of Schubert cells, Hecke algebras, and applications to Casselman’s problem”, preprint, 2019. To appear in *Ann. Sci. Éc. Norm. Supér.* arXiv 1902.10101
- [Billey and Lakshmibai 2000] S. Billey and V. Lakshmibai, *Singular loci of Schubert varieties*, Progress in Mathematics **182**, Birkhäuser, Boston, 2000. MR Zbl
- [Brasselet et al. 2010] J.-P. Brasselet, J. Schürmann, and S. Yokura, “Hirzebruch classes and motivic Chern classes for singular spaces”, *J. Topol. Anal.* **2**:1 (2010), 1–55. MR Zbl
- [Buchstaber and Bunkova 2010] V. M. Buchstaber and E. Y. Bunkova, “Elliptic formal group laws, integral Hirzebruch genera and Krichever genera”, preprint, 2010. arXiv 1010.0944
- [Bump and Nakasuji 2011] D. Bump and M. Nakasuji, “Casselman’s basis of Iwahori vectors and the Bruhat order”, *Canad. J. Math.* **63**:6 (2011), 1238–1253. MR Zbl
- [Bump and Nakasuji 2019] D. Bump and M. Nakasuji, “Casselman’s basis of Iwahori vectors and Kazhdan–Lusztig polynomials”, *Canad. J. Math.* **71**:6 (2019), 1351–1366. MR Zbl
- [Calmès et al. 2015] B. Calmès, K. Zainoulline, and C. Zhong, “Equivariant oriented cohomology of flag varieties”, *Doc. Math.* unnumbered volume (2015), 113–144. MR Zbl
- [Calmès et al. 2016] B. Calmès, K. Zainoulline, and C. Zhong, “A coproduct structure on the formal affine Demazure algebra”, *Math. Z.* **282**:3-4 (2016), 1191–1218. MR Zbl
- [Calmès et al. 2019] B. Calmès, K. Zainoulline, and C. Zhong, “Push-pull operators on the formal affine Demazure algebra and its dual”, *Manuscripta Math.* **160**:1-2 (2019), 9–50. MR Zbl
- [Deodhar 1987] V. V. Deodhar, “On some geometric aspects of Bruhat orderings, II: The parabolic analogue of Kazhdan–Lusztig polynomials”, *J. Algebra* **111**:2 (1987), 483–506. MR Zbl

- [Fehér et al. 2021] L. M. Fehér, R. Rimányi, and A. Weber, “Motivic Chern classes and K-theoretic stable envelopes”, *Proc. Lond. Math. Soc.* (3) **122**:1 (2021), 153–189. MR Zbl
- [Hoffnung et al. 2014] A. Hoffnung, J. Malagón-López, A. Savage, and K. Zainoulline, “Formal Hecke algebras and algebraic oriented cohomology theories”, *Selecta Math. (N.S.)* **20**:4 (2014), 1213–1245. MR Zbl
- [Kashiwara and Tanisaki 2002] M. Kashiwara and T. Tanisaki, “Parabolic Kazhdan–Lusztig polynomials and Schubert varieties”, *J. Algebra* **249**:2 (2002), 306–325. MR Zbl
- [Kazhdan and Lusztig 1979] D. Kazhdan and G. Lusztig, “Representations of Coxeter groups and Hecke algebras”, *Invent. Math.* **53**:2 (1979), 165–184. MR Zbl
- [Kazhdan and Lusztig 1980] D. Kazhdan and G. Lusztig, “Schubert varieties and Poincaré duality”, pp. 185–203 in *Geometry of the Laplace operator* (Honolulu, 1979), edited by R. Osserman and A. Weinstein, Proc. Sympos. Pure Math. **36**, Amer. Math. Soc., Providence, RI, 1980. MR Zbl
- [Kirillov and Lascoux 2000] A. Kirillov, Jr. and A. Lascoux, “Factorization of Kazhdan–Lusztig elements for Grassmanians”, pp. 143–154 in *Combinatorial methods in representation theory* (Kyoto, 1998), edited by K. Koike et al., Adv. Stud. Pure Math. **28**, Kinokuniya, Tokyo, 2000. MR Zbl
- [Kumar 1996] S. Kumar, “The nil Hecke ring and singularity of Schubert varieties”, *Invent. Math.* **123**:3 (1996), 471–506. MR Zbl
- [Kumar et al. 2020] S. Kumar, R. Rimányi, and A. Weber, “Elliptic classes of Schubert varieties”, *Math. Ann.* **378**:1-2 (2020), 703–728. MR Zbl
- [Lenart and Zainoulline 2017] C. Lenart and K. Zainoulline, “A Schubert basis in equivariant elliptic cohomology”, *New York J. Math.* **23** (2017), 711–737. MR Zbl
- [Lenart et al. 2020] C. Lenart, K. Zainoulline, and C. Zhong, “Parabolic Kazhdan–Lusztig basis, Schubert classes, and equivariant oriented cohomology”, *J. Inst. Math. Jussieu* **19**:6 (2020), 1889–1929. MR Zbl
- [Levine and Morel 2007] M. Levine and F. Morel, *Algebraic cobordism*, Springer, 2007. MR Zbl
- [MacPherson 1974] R. D. MacPherson, “Chern classes for singular algebraic varieties”, *Ann. of Math. (2)* **100** (1974), 423–432. MR Zbl
- [Maulik and Okounkov 2019] D. Maulik and A. Okounkov, *Quantum groups and quantum cohomology*, Astérisque **408**, 2019. MR Zbl
- [Mihalcea and Singh 2020] L. C. Mihalcea and R. Singh, “Mather classes and conormal spaces of Schubert varieties in cominuscule spaces”, preprint, 2020. arXiv 2006.04842
- [Mihalcea et al. 2022] L. C. Mihalcea, H. Naruse, and C. Su, “Left Demazure–Lusztig operators on equivariant (quantum) cohomology and K-theory”, *Int. Math. Res. Not.* **2022**:16 (2022), 12096–12147. MR Zbl
- [Naruse 2014] H. Naruse, “Schubert calculus and hook formula”, slides, 73rd Sém. Lothar. Combin., Strobl, Austria, 2014.
- [Neshitov et al. 2018] A. Neshitov, V. Petrov, N. Semenov, and K. Zainoulline, “Motivic decompositions of twisted flag varieties and representations of Hecke-type algebras”, *Adv. Math.* **340** (2018), 791–818. MR Zbl
- [Okounkov 2017] A. Okounkov, “Lectures on K-theoretic computations in enumerative geometry”, pp. 251–380 in *Geometry of moduli spaces and representation theory*, edited by R. Bezrukavnikov et al., IAS/Park City Math. Ser. **24**, Amer. Math. Soc., Providence, RI, 2017. MR Zbl
- [Okounkov 2021] A. Okounkov, “Inductive construction of stable envelopes”, *Lett. Math. Phys.* **111**:6 (2021), art. id. 141, 56 pages. MR Zbl
- [Rimányi and Weber 2020] R. Rimányi and A. Weber, “Elliptic classes of Schubert varieties via Bott–Samelson resolution”, *J. Topol.* **13**:3 (2020), 1139–1182. MR Zbl
- [Schürmann 2011] J. Schürmann, “Characteristic classes of mixed Hodge modules”, pp. 419–470 in *Topology of stratified spaces*, edited by G. Friedman et al., Math. Sci. Res. Inst. Publ. **58**, Cambridge Univ. Press, 2011. MR Zbl
- [Schürmann 2017] J. Schürmann, “Chern classes and transversality for singular spaces”, pp. 207–231 in *Singularities in geometry, topology, foliations and dynamics*, edited by J. L. Cisneros-Molina et al., Springer, 2017. MR Zbl
- [Schwartz 1965a] M.-H. Schwartz, “Classes caractéristiques définies par une stratification d’une variété analytique complexe, I”, *C. R. Acad. Sci. Paris* **260** (1965), 3262–3264. MR Zbl

- [Schwartz 1965b] M.-H. Schwartz, “Classes caractéristiques définies par une stratification d’une variété analytique complexe, II”, *C. R. Acad. Sci. Paris* **260** (1965), 3535–3537. MR Zbl
- [Soergel 1997] W. Soergel, “Kazhdan–Lusztig polynomials and a combinatoric for tilting modules”, *Represent. Theory* **1** (1997), 83–114. MR Zbl
- [Su 2017] C. Su, “Restriction formula for stable basis of the Springer resolution”, *Selecta Math. (N.S.)* **23**:1 (2017), 497–518. MR Zbl
- [Su 2019] C. Su, “Motivic Chern classes and Iwahori invariants of principal series”, 2019. To appear in *Proceedings of International Congress of Chinese Mathematicians*.
- [Su et al. 2020] C. Su, G. Zhao, and C. Zhong, “On the K-theory stable bases of the Springer resolution”, *Ann. Sci. Éc. Norm. Supér. (4)* **53**:3 (2020), 663–711. MR Zbl
- [Tanisaki 1987] T. Tanisaki, “Hodge modules, equivariant K -theory and Hecke algebras”, *Publ. Res. Inst. Math. Sci.* **23**:5 (1987), 841–879. MR Zbl
- [Totaro 2000] B. Totaro, “Chern numbers for singular varieties and elliptic homology”, *Ann. of Math. (2)* **151**:2 (2000), 757–791. MR Zbl
- [Zelevinskiĭ 1983] A. V. Zelevinskiĭ, “Small resolutions of singularities of Schubert varieties”, *Funktsional. Anal. i Prilozhen.* **17**:2 (1983), 75–77. In Russian; translated in *Funct. Anal. Appl.* **17**:2 (1983), 142–144. MR Zbl

Communicated by Sergey Fomin

Received 2021-07-22 Revised 2022-02-09 Accepted 2022-04-04

clenart@albany.edu	<i>Department of Mathematics and Statistics, State University of New York at Albany, Albany, NY, United States</i>
changjiansu@mail.tsinghua.edu.cn	<i>Department of Mathematics, University of Toronto, Toronto, ON, Canada</i>
Current address:	<i>Yau Mathematical Sciences Center, Tsinghua University, Beijing, China</i>
kirill@uottawa.ca	<i>Department of Mathematics and Statistics, University of Ottawa, Ottawa, ON, Canada</i>
czhong@albany.edu	<i>Department of Mathematics and Statistics, State University of New York at Albany, Albany, NY, United States</i>

Some refinements of the Deligne–Illusie theorem

Piotr Achinger and Junecue Suh

We extend the results of Deligne and Illusie on liftings modulo p^2 and decompositions of the de Rham complex in several ways. We show that for a smooth scheme X over a perfect field k of characteristic $p > 0$, the truncations of the de Rham complex in $\max(p-1, 2)$ consecutive degrees can be reconstructed as objects of the derived category in terms of its truncation in degrees at most one (or, equivalently, in terms of the obstruction class to lifting modulo p^2). Consequently, these truncations are decomposable if X admits a lifting to $W_2(k)$, in which case the first nonzero differential in the conjugate spectral sequence appears no earlier than on page $\max(p, 3)$ (these corollaries have been recently strengthened by Drinfeld, by Bhatt and Lurie, and by Li and Mondal). Without assuming the existence of a lifting, we describe the gerbes of splittings of two-term truncations and the differentials on the second page of the conjugate spectral sequence, answering a question of Katz.

The main technical result used in the case $p > 2$ belongs purely to homological algebra. It concerns certain commutative differential graded algebras whose cohomology algebra is the exterior algebra, dubbed by us *abstract Koszul complexes*, of which the de Rham complex in characteristic p is an example.

In the Appendix, we use the aforementioned stronger decomposition result to prove that Kodaira–Akizuki–Nakano vanishing and Hodge–de Rham degeneration both hold for F -split $(p+1)$ -folds.

1. Introduction

1A. Decompositions of the de Rham complex. Deligne and Illusie [1987] showed that for a smooth scheme X over a perfect field k of characteristic $p > 0$, a flat lifting of the Frobenius twist $X' = F_k^* X$ to $W_2(k)$ induces a splitting of the truncation of the de Rham complex in degrees $[0, 1]$, i.e., an isomorphism in the derived category

$$\mathcal{O}_{X'} \oplus \Omega_{X'/k}^1[-1] \xrightarrow{\sim} \tau_{\leq 1}(F_{X/k,*}\Omega_{X/k}^\bullet).$$

Using the algebra structure of the de Rham complex, they further show that it induces an isomorphism

$$\bigoplus_{i < p} \Omega_{X'/k}^i[-i] \xrightarrow{\sim} \tau_{< p}(F_{X/k,*}\Omega_{X/k}^\bullet).$$

With their method, it is unclear if one could extend this further to an isomorphism between $\bigoplus_{i \geq 0} \Omega_{X'/k}^i[-i]$ and $F_{X/k,*}\Omega_{X/k}^\bullet$ if $\dim X \geq p$, i.e., whether the de Rham complex $\Omega_{X/k}^\bullet$ is *decomposable*. As a step further, Deligne and Illusie prove using duality that this is the case if $\dim X = p$.

MSC2020: primary 14F40; secondary 14G17.

Keywords: de Rham cohomology, Koszul complex, Deligne–Illusie, lifting modulo p^2 , conjugate spectral sequence, F -splitting.

© 2023 MSP (Mathematical Sciences Publishers). Distributed under the Creative Commons Attribution License 4.0 (CC BY). Open Access made possible by subscribing institutions via [Subscribe to Open](#).

It is as of today an open problem whether there exists a smooth X over k liftable to $W_2(k)$, necessarily of dimension $\dim X > p$, for which the de Rham complex is not decomposable.¹ In this paper, as a small contribution to this question, we investigate the ways in which the truncation $\tau_{\leq 1}(F_{X/k,*}\Omega_{X/k}^\bullet)$ determines the truncations $\tau_{[a,b]}(F_{X/k,*}\Omega_{X/k}^\bullet)$. Our first result is the following:

Theorem 1.1. *Let X be a smooth scheme over a perfect field k of characteristic $p > 0$ which is liftable to $W_2(k)$. Then the truncations*

$$\tau_{[a,b]}(F_{X/k,*}\Omega_{X/k}^\bullet)$$

are decomposable for $a \leq b < a + p - 1$ when $p > 2$, and for $a \leq b \leq a + 1$ when $p = 2$.

The above result immediately implies that in the conjugate spectral sequence

$$E_2^{ij} = H^i(X', \Omega_{X'/k}^j) \Rightarrow H^{i+j}(X, \Omega_{X/k}^\bullet) \tag{1-1}$$

the differentials d_r^{ij} are zero for $2 \leq r < p$ when $p > 2$, and for $r = 2$ when $p = 2$. As a sample corollary, we obtain the following criterion for degeneration of spectral sequences.

Corollary 1.2. *For X as in Theorem 1.1, suppose that*

$$H^i(X, \Omega_{X/k}^j) = 0 \text{ for } |i - j| \geq p.$$

Then the conjugate spectral sequence (1-1) degenerates. If moreover X is proper over k , then the Hodge to de Rham spectral sequence

$$E_1^{ij} = H^j(X, \Omega_{X/k}^i) \Rightarrow H^{i+j}(X, \Omega_{X/k}^\bullet)$$

degenerates as well.

1B. Truncations of the de Rham complex. Our methods give information about truncations of the de Rham complex without assuming liftability modulo p^2 . Our results in this direction are the strongest and most explicit for truncations in two consecutive degrees. Namely, for a general smooth X over k (not necessarily liftable to $W_2(k)$) and for $q \geq 1$, the truncated complex $\tau_{[q-1,q]}(F_{X/k,*}\Omega_{X/k}^\bullet)$ can be described as the mapping fiber of $\delta^q[-q]$ for a map

$$\delta^q : \Omega_{X'/k}^q \rightarrow \Omega_{X'/k}^{q-1}[2],$$

that is, a class

$$\delta^q \in \text{Ext}^2(\Omega_{X'/k}^q, \Omega_{X'/k}^{q-1}),$$

which is the ‘‘cup product’’ with the negative of the deformation obstruction class

$$\delta^1 = -\text{obs}(X'/k/W_2(k)) \in \text{Ext}^2(\Omega_{X'/k}^1, \mathcal{O}_{X'}) \simeq H^2(X', T_{X'/k}) \tag{1-2}$$

to the existence of a lifting of X' to $W_2(k)$ (see Corollary 4.3). The result in particular implies that the two-term truncation $\tau_{[q-1,q]}(F_{X/k,*}\Omega_{X/k}^\bullet)$ is decomposable if X' lifts to $W_2(k)$, and yields a description

¹*Added in proof:* This problem has been recently resolved by Petrov [2023], who constructed such a variety.

of the differentials on the second page of the conjugate spectral sequence — answering a natural question of Katz.

Theorem 1.3 (see Corollary 4.4). *In the above situation, the differential*

$$d_2^{ij} : H^i(X', \Omega_{X'/k}^j) \rightarrow H^{i+2}(X', \Omega_{X'/k}^{j-1})$$

in the conjugate spectral sequence (1-1) is induced by the cup product with the negative of the obstruction class $\text{obs}(X'/k/W_2(k))$.

Deligne and Illusie [1987, § 3] define the *gerbe of splittings* $\text{sc } K$ of a two-term complex K , and relate the gerbe of splittings of $\tau_{\leq 1}(F_{X/k,*}\Omega_{X/k}^\bullet)$ to the gerbe of liftings of X' to $W_2(k)$. This provides a “categorification” of the equality (1-2). In the same vein, for $p > 2$, our description of the class of $\tau_{[q-1,q]}(F_{X/k,*}\Omega_{X/k}^\bullet)$ can be upgraded to a morphism of gerbes (see Theorem 3.9)

$$\wedge^q : \text{sc}(\tau_{\leq 1}(F_{X/k,*}\Omega_{X/k}^\bullet)) \rightarrow \text{sc}(\tau_{[q-1,q]}(F_{X/k,*}\Omega_{X/k}^\bullet)).$$

Let us now discuss longer truncations of the de Rham complex. The assertion of Theorem 1.1 is subsumed by a recent beautiful observation of Drinfeld [2020, § 5.12.1] (a proof appeared in Bhatt and Lurie [2022]): a lifting of X' to $W_2(k)$ induces a μ_p -action on the de Rham complex $F_{X/k,*}\Omega_{X/k}^\bullet$, which one can use to show that the truncations $\tau_{[q-p+1,q]}(F_{X/k,*}\Omega_{X/k}^\bullet)$ are decomposable for all q (even more recently, Li and Mondal [2021] found an independent proof). However, the method of proof of Theorem 1.1 is completely different and provides interesting information even if X is not liftable to $W_2(k)$. It is deduced from the following result (when $p > 2$) and Corollary 4.3 (when $p = 2$) alluded to above.

Theorem 1.4. *Let X be a smooth scheme over a perfect field k of characteristic $p > 0$, let q be an integer, and let $m < p - 1$. One then has an isomorphism in the derived category of X' ,*

$$\tau_{[q-m,q]}(F_{X/k,*}\Omega_{X/k}^\bullet) \simeq \tau_{\geq q-m}(L\Gamma^q(\tau_{\leq 1}F_{X/k,*}\Omega_{X/k}^\bullet)),$$

where $L\Gamma^q$ is the derived q -th divided power.

1C. Abstract Koszul complexes. The proof of Theorem 1.4 has very little to do with algebraic geometry. To state the main technical result behind it, we need the notion of an *abstract Koszul complex* (Definition 2.1), which is a certain commutative differential graded algebra (cdga) K in a ringed topos for which the multiplication induces isomorphisms

$$\wedge^q \mathcal{H}^1(K) \xrightarrow{\sim} \mathcal{H}^q(K) \quad \text{for all } q \geq 0.$$

Thanks to the Cartier isomorphism, the de Rham complexes $F_{X/k,*}\Omega_{X/k}^\bullet$ in characteristic $p > 0$ are examples of such, and hence the result below immediately implies Theorem 1.4.

Theorem 1.5 (see Theorem 2.8). *Let K be an abstract Koszul complex in a ringed topos (X, \mathcal{O}) satisfying the flatness condition (2-1), and let $q \geq m \geq 1$ be integers such that $m!$ is invertible in \mathcal{O} . Suppose that*

either $q = m$ or that $m + 1$ is a nonzero divisor in \mathcal{O} . Then there exists an isomorphism in the derived category

$$\tau_{\geq q-m}(L\Gamma^q(\tau_{\leq 1}(K))) \xrightarrow{\sim} \tau_{[q-m,q]}(K). \tag{1-3}$$

In (1-3), $L\Gamma^q$ is again the derived q -th divided power, and the source of the map can be more concretely realized as $\tau_{\geq q-m}$ of the Koszul complex

$$\dots \rightarrow \underbrace{\Gamma^{q-i}(K^0) \otimes \wedge^i(\mathcal{Z}^1 K)}_{\text{degree } i} \rightarrow \dots \rightarrow K^0 \otimes \wedge^{q-1}(\mathcal{Z}^1 K) \rightarrow \underbrace{\wedge^q(\mathcal{Z}^1 K)}_{\text{degree } q} \rightarrow 0 \rightarrow \dots$$

For $m = 1$ (and assuming that 2 is a nonzerodivisor), we again obtain more refined information regarding $\tau_{[q-1,q]}K$, including the differentials on the second page of the spectral sequence

$$E_2^{ij} = H^i(X, \mathcal{H}^j(K)) \Rightarrow H^{i+j}(X, K) \quad (\text{see Corollary 4.3}).$$

As observed by Kato [1989], logarithmic de Rham complexes are abstract Koszul complexes, and hence Theorem 1.1 works also in the log case. The inspiration for Theorem 2.8 came from the result of Steenbrink [1995, § 2.8] describing the nearby cycle complex $R\Psi\mathbb{Q}$ for a complex semistable degeneration in terms of the logarithmic structure; see also [Achinger and Ogus 2020, § 4]. It is an interesting question whether Steenbrink’s result can be extended to work with integral coefficients; the nearby cycles $R\Psi\mathbb{Z}$ are coconnective E_∞ -algebra versions of abstract Koszul complexes, but we do not know whether they admit cdga models (see Remark 2.11 and Example 2.3). An affirmative answer would give an application unrelated to the Deligne–Illusie theorem, refining [Achinger and Ogus 2020, Theorem 4.2.2(1)], providing a description of the two-step truncations $\tau_{[q-1,q]}$ of certain logarithmic nearby cycle complexes.

1D. The case $p = 2$ (Theorem 4.1). The description of the truncations $\tau_{[q-1,q]}(F_{X/k,*}\Omega_{X/k}^\bullet)$ and its corollary, Theorem 1.3, can be deduced from the “abstract Koszul complex” machinery and Theorem 1.4, but only for $p > 2$. In contrast, the assertion of Theorem 1.5 is vacuous if $2 \cdot \mathcal{O} = 0$. Accordingly, the computation of the class of $\tau_{[q-1,q]}F_{X/k,*}\Omega_{X/k}^\bullet$, occupying the entire Section 4 is much harder in the case $p = 2$, and uses more information about the de Rham complex than merely its abstract Koszul complex structure. For this technical point, we highlight the passage from (4-3) to (4-4).

It could be worthwhile to extend the methods used in the case of $p = 2$ in order to “compute” the truncations $\tau_{[q-p+1,p]}$ in p consecutive degrees, and it would be interesting to extract the exact abstract properties of the de Rham complex in positive characteristic needed for the proof. Its relationship with the aforementioned result of Drinfeld, Bhatt–Lurie, and Li–Mondal remains elusive.

The results concerning the truncations $\tau_{[q-1,q]}(F_{X/k,*}\Omega_{X/k}^\bullet)$ and Theorem 1.3, including the case $p = 2$, presented here are due to the second author and appeared in his 2007 Ph.D. thesis. After the first author proved Theorem 1.4, the authors decided to publish their results together.

1E. Application to F -split $(p+1)$ -folds. As an illustration of this circle of ideas, using the refinement of the Deligne–Illusie theorem due to Drinfeld, Bhatt–Lurie, and Li–Mondal, we prove in the Appendix that

the Kodaira–Akizuki–Nakano vanishing theorem and the degeneration of the Hodge to de Rham spectral sequence both hold for F -split $(p+1)$ -folds in characteristic p .²

Notation. If K is a cochain complex in an abelian category, we write $\mathcal{Z}^i K = \ker(d : K^i \rightarrow K^{i+1})$, $\mathcal{B}^i K = \operatorname{im}(d : K^{i-1} \rightarrow K^i)$, and $\mathcal{H}^i(K) = \mathcal{Z}^i K / \mathcal{B}^i K$, denote by $\tau_{\leq b}(K)$ the subcomplex

$$\tau_{\leq b}(K) = [\dots \rightarrow K^{b-1} \rightarrow \mathcal{Z}^b K \rightarrow 0 \rightarrow \dots]$$

and by $\tau_{\geq a}(K)$ the quotient $K/\tau_{\leq a}(K)$, and define $\tau_{[a,b]}(K) = \tau_{\geq a}\tau_{\leq b}(K)$. We call K *decomposable* if it is isomorphic in the derived category to the complex with zero differential $\bigoplus \mathcal{H}^i(K)[-i]$.

A *commutative differential graded algebra (cdga)* is an associative graded ring $K = \bigoplus_{n \in \mathbb{Z}} K^n$ which is graded-commutative (i.e., $xy = (-1)^{mn}yx$ for $x \in K^m, y \in K^n$), endowed with a differential $d : K \rightarrow K$ mapping K^n to K^{n+1} and satisfying $d(xy) = dx \cdot y + (-1)^n x \cdot dy$ for $x \in K^n$. We say that K is *coconnective* if $K^n = 0$ for $n < 0$.

2. Abstract Koszul complexes

2A. Definition and examples. We work in a ringed topos (X, \mathcal{O}) .

Definition 2.1 (abstract Koszul complex). A coconnective commutative differential graded \mathcal{O} -algebra K is called an *abstract Koszul complex* if the following conditions are satisfied:

- (i) $\mathcal{O} \rightarrow \mathcal{H}^0(K)$ is an isomorphism.
- (ii) For every $q \geq 1$, the multiplication map $\mathcal{H}^1(K)^{\otimes q} \rightarrow \mathcal{H}^q(K)$ factors through an isomorphism

$$\mu^q : \bigwedge^q \mathcal{H}^1(K) \xrightarrow{\sim} \mathcal{H}^q(K).$$

Example 2.2 (De Rham complex in characteristic $p > 0$). Let X be a smooth scheme over a perfect field k of characteristic $p > 0$, and let $F_{X/k} : X \rightarrow X'$ be its relative Frobenius. Let $K = F_{X/k,*}\Omega_{X/k}^\bullet$ be the de Rham complex, treated as a cdga over $\mathcal{O}_{X'}$. Then the Cartier isomorphisms

$$C : \mathcal{H}^i(F_{X/k,*}\Omega_{X/k}^\bullet) \xrightarrow{\sim} \Omega_{X'/k}^i$$

are multiplicative, and hence K is an abstract Koszul complex over $(X', \mathcal{O}_{X'})$.

More generally, if $f : (X, \mathcal{M}_X) \rightarrow (S, \mathcal{M}_S)$ is a morphism of fine log schemes over \mathbb{F}_p which is smooth and of Cartier type, then the log de Rham complex $F_{X/S,*}\Omega_{(X,\mathcal{M}_X)/(S,\mathcal{M}_S)}^\bullet$ is an abstract Koszul complex [Kato 1989, Theorem 4.12].

Example 2.3 (nearby cycle complexes; see, e.g., [Steenbrink 1995, § 2]). Let X be a complex manifold and let $D = \bigcup D_\alpha$ be a divisor with simple normal crossings on X . Let $j : U = X \setminus D \hookrightarrow X$ be the complementary open immersion, and let $K = Rj_*\mathbb{Q}_U$. Since we are working with rational coefficients,

²Added in proof: These results have recently been improved upon by Petrov (private communication, 2023), who showed that the assumption on dimension is not necessary.

we can find a cdga model for K (e.g., [Kříž and May 1995, Part II, Corollary 1.5]). The purity theorem implies that

$$R^i j_* \mathbb{Q}_U = \wedge^i \left(\bigoplus \mathbb{Q}_{D_\alpha} \right),$$

so any cdga model of K is an abstract Koszul complex over (X, \mathbb{Q}_X) . Moreover, one has an isomorphism in the derived category [Steenbrink 1995, Lemma 2.7] (see also [Achinger and Ogus 2020, § 4])

$$\tau_{\leq 1}(R^1 j_* \mathbb{Z}_U) \simeq [\mathcal{O}_X \xrightarrow{\text{exp}} \mathcal{M}^{\text{gp}}],$$

where \mathcal{M}^{gp} is the sheaf of meromorphic functions without zeros or poles on U . Variants of this construction exist for the nearby cycle complexes $R\Psi\mathbb{Q}$ for a semistable degeneration over a disc, and there exist analogs in ℓ -adic étale cohomology (with \mathbb{Q}_ℓ coefficients).

Recall [SGA 4₂ 1972, exposé V, Definition 1.1] that an \mathcal{O} -module M is *flat* if the functor $(-)\otimes_{\mathcal{O}} M$ is exact on the category of all \mathcal{O} -modules. By the Deligne–Lazard theorem [SGA 4₂ 1972, exposé V, théorème 8.2.12], an \mathcal{O} -module is flat if and only if it is a local inductive limit (see [SGA 4₂ 1972, exposé V, § 8.1]) of free \mathcal{O} -modules of finite rank.

In the following, we will work with abstract Koszul complexes satisfying the additional flatness condition:

$$\text{the } \mathcal{O}\text{-modules } K^0, \mathcal{B}^1 K, \mathcal{Z}^1 K, \text{ and } \mathcal{H}^1(K) \text{ are flat.} \quad (2-1)$$

In particular, this implies that the modules $\mathcal{H}^q(K) \simeq \wedge^q \mathcal{H}^q(K)$ are flat for all $q \geq 0$. The above condition is satisfied in the situation of Examples 2.2 and 2.3.

2B. Koszul complexes. Our goal is to show that to a certain extent, the underlying complex of an abstract Koszul complex satisfying the flatness condition (2-1) is determined by its truncation in degrees ≤ 1 (Theorem 2.8). We achieve this using the notion of the Koszul complex of a map $u : P \rightarrow Q$; see [Illusie 1971, chapitre I, § 4.3] and [Kato and Saito 2004, § 1.1–1.2].

Recall first that if M and N are \mathcal{O} -modules, then for every $q \geq 0$ there is a natural decomposition of the divided (resp. exterior) power

$$\Gamma^q(M \oplus N) = \bigoplus_{a+b=q} \Gamma^a M \otimes \Gamma^b N \quad \left(\text{resp. } \wedge^q(M \oplus N) = \bigoplus_{a+b=q} \wedge^a M \otimes \wedge^b N \right).$$

In what follows, we will use the *comultiplication maps*

$$\eta^q : \Gamma^q M \rightarrow (\Gamma^{q-1} M) \otimes M \quad (\text{resp. } \eta^q : \wedge^q M \rightarrow M \otimes \wedge^{q-1} M)$$

obtained as the composition of Γ^q (resp. \wedge^q) of the diagonal map $M \rightarrow M \oplus M$ and the projection to the $(a, b) = (q-1, 1)$ -part (resp. $(a, b) = (1, q-1)$ -part) in the above decomposition of $\Gamma^q(M \oplus M)$

(resp. of $\wedge^q(M \oplus M)$). Explicitly, we have

$$\eta^q(x_1^{[e_1]} \cdots x_r^{[e_r]}) = \sum_{i=1}^r (x_1^{[e_1]} \cdots x_i^{[e_i-1]} \cdots x_r^{[e_r]}) \otimes x_i \quad (e_1 + \cdots + e_r = q),$$

$$\eta^q(x_1 \wedge \cdots \wedge x_q) = \sum_{i=1}^q (-1)^{i-1} x_i \otimes x_1 \wedge \cdots \wedge \widehat{x}_i \wedge \cdots \wedge x_q.$$

Sometimes we omit the superscript q when it is clear from the context.

Definition 2.4 (Koszul complex $\text{Kos}^q(u)$). Let $u : P \rightarrow Q$ be a map of \mathcal{O} -modules, and let $q \geq 0$ be an integer. Then the q -th Koszul complex $\text{Kos}^q(u)$ is the cochain complex whose i -th term is

$$\text{Kos}^q(u)^i = \Gamma^{q-i}(P) \otimes \wedge^i(Q),$$

with differential $d : \text{Kos}^q(u)^i \rightarrow \text{Kos}^q(u)^{i+1}$ defined as the composition

$$\begin{array}{ccc} \Gamma^{q-i}(P) \otimes \wedge^i(Q) & \xrightarrow{\eta \otimes \text{id}} & \Gamma^{q-i-1}(P) \otimes P \otimes \wedge^i(Q) \\ & & \downarrow \text{id} \otimes u \otimes \text{id} \\ & & \Gamma^{q-i-1}(P) \otimes Q \otimes \wedge^i(Q) \xrightarrow{\text{id} \otimes \wedge} \Gamma^{q-i-1}(P) \otimes \wedge^{i+1}(Q) \end{array}$$

Concretely, with $e_1 + \cdots + e_r = q - i$, $x_1, \dots, x_r \in P$, and $y \in \wedge^i Q$,

$$d(x_1^{[e_1]} \cdots x_r^{[e_r]} \otimes y) = \sum_{j=1}^r (x_1^{[e_1]} \cdots x_j^{[e_j-1]} \cdots x_r^{[e_r]}) \otimes u(x_j) \wedge y.$$

We note here that our convention differs slightly from that in [Kato and Saito 2004] and [Illusie 1971], who use $\wedge^i(Q) \otimes \Gamma^{q-i}(P)$ as the i -th term. The two complexes, ours and theirs, are isomorphic via the map which is $(-1)^i$ times the map switching the two tensor factors in degree i . The reason for this convention is that later in Proposition 3.2 we will obtain the left comultiplication maps on exterior powers, which in applications to the de Rham complex will be compatible with interior multiplication of differential forms.

Proposition 2.5. *Let $u : P \rightarrow Q$ be a map of flat \mathcal{O} -modules, and let $F(u) = [P \xrightarrow{u} Q]$ be the two-term cochain complex with P in degree zero (the mapping fiber). There exist natural isomorphisms in the derived category*

$$\text{Kos}^q(u) \simeq L\Lambda^q(F[1])[-q] \simeq L\Gamma^q(F),$$

where $L\Lambda^q$ (resp. $L\Gamma^q$) is the derived exterior (resp. divided) power.

Proof. Combine [Kato and Saito 2004, Corollary 1.2.7] with [Illusie 1971, chapitre I, 4.3.2.1]. See also [Illusie 1972, chapitre VIII, lemme 2.1.2.1]. □

Corollary 2.6. *For a map $u : P \rightarrow Q$ between flat \mathcal{O} -modules, the complex $\text{Kos}^q(u)$, treated as an object of the derived category, depends only on $F(u) = [P \rightarrow Q]$ up to quasi-isomorphism. In particular, if $F(u)$ is decomposable, then so is $\text{Kos}^q(u)$.*

Proposition 2.7 (compare [Steenbrink 1995, Lemma 1.4]). *Let $u : P \rightarrow Q$ be a map of \mathcal{O} -modules. There exist unique arrows*

$$\Gamma^{q-i}(\ker u) \otimes \wedge^i(Q) \rightarrow \mathcal{Z}^i(\mathrm{Kos}^q(u)) \quad \text{and} \quad \alpha^i : \Gamma^{q-i}(\ker u) \otimes \wedge^i(\mathrm{cok} u) \rightarrow \mathcal{H}^i(\mathrm{Kos}^q(u))$$

making the following diagram commute:

$$\begin{array}{ccc} \Gamma^{q-i}(P) \otimes \wedge^i(Q) & \xlongequal{\quad} & \mathrm{Kos}^q(u)^i \\ \uparrow & & \uparrow \\ \Gamma^{q-i}(\ker u) \otimes \wedge^i(Q) & \longrightarrow & \mathcal{Z}^i(\mathrm{Kos}^q(u)) \\ \downarrow & & \downarrow \\ \Gamma^{q-i}(\ker u) \otimes \wedge^i(\mathrm{cok} u) & \xrightarrow{\alpha^i} & \mathcal{H}^i(\mathrm{Kos}^q(u)) \end{array}$$

Moreover, the map α^i is an isomorphism if P , Q , $\ker u$, $\mathrm{im} u$, and $\mathrm{cok} u$ are all flat.

Proof. The first assertion is straightforward. The second is reduced as in [Illusie 1971, chapitre I, 4.3.1.6] using the Deligne–Lazard theorem to the case where P , Q , $\ker u$, $\mathrm{im} u$, and $\mathrm{cok} u$ are free \mathcal{O} -modules of finite rank. In this case, splitting the surjection $Q \rightarrow \mathrm{cok} u$ one can write $u = u' \oplus u''$, where $u' : P \rightarrow \mathrm{im} u$ and $u'' : 0 \rightarrow \mathrm{cok} u$. The assertion then holds for u' (by [Illusie 1971, chapitre I, 4.3.1.6]) and for u'' (trivially), for all q , and then the assertion for $u = u' \oplus u''$ follows from the isomorphism [Illusie 1971, chapitre I, 4.3.1.5]

$$\mathrm{Kos}^\bullet(u) = \mathrm{Kos}^\bullet(u') \otimes \mathrm{Kos}^\bullet(u''),$$

where $\mathrm{Kos}^\bullet(u) = \bigoplus_{q \geq 0} \mathrm{Kos}^q(u)[q]$. □

2C. Truncations of abstract Koszul complexes. The following theorem is the main result of this section.

Theorem 2.8. *Let $m \geq 0$ be an integer such that $m!$ is invertible in \mathcal{O} , and let $q \geq m$. Suppose that either $q = m$, or that $m + 1$ is not a zero divisor in \mathcal{O} . Let K be an abstract Koszul complex on (X, \mathcal{O}) satisfying the flatness condition (2-1), and write*

$$\tau_{\leq 1} K = [K^0 \xrightarrow{\partial} Z^1 K]$$

for its truncation in degrees ≤ 1 . Then the multiplication maps

$$\mathrm{Kos}^q(\partial)^i = \Gamma^{q-i}(K^0) \otimes \wedge^i(Z^1 K) = \mathrm{Sym}^{q-i}(K^0) \otimes \wedge^i(Z^1 K) \rightarrow K^i$$

for $q - m \leq i \leq q$ (where we can identify Γ^{q-i} with Sym^{q-i} as $q - i \leq m$, so that $(q - i)!$ is invertible in \mathcal{O}) induce a quasi-isomorphism

$$\tau_{\geq q-m}(L\Gamma^q(\tau_{\leq 1}(K))) = \tau_{\geq q-m} \mathrm{Kos}^q(\partial) \xrightarrow{\sim} \tau_{[q-m, q]}(K). \tag{2-2}$$

Proof. The multiplication maps define a morphism of “naive truncations”

$$\begin{array}{ccccccc} \mathrm{Kos}^q(\partial)^{\geq q-m} & = & [\mathrm{Sym}^m(K^0) \otimes \wedge^{q-m}(\mathcal{Z}^1 K) & \longrightarrow & \cdots & \longrightarrow & \wedge^q(\mathcal{Z}^1 K)] \\ \mu \downarrow & & \downarrow & & & & \downarrow \\ \tau_{\leq q}(K)^{\geq q-m} & = & [K^{q-m} & \longrightarrow & \cdots & \longrightarrow & Z^q K] \end{array}$$

To obtain the desired morphism $\mu : \tau_{\geq q-m} \mathrm{Kos}^q(\partial) \rightarrow \tau_{[q-m, q]}(K)$, we need to check that the map

$$\mathrm{Kos}^q(\partial)^{q-m} \rightarrow K^{q-m}$$

takes the image of $\mathrm{Kos}^q(\partial)^{q-m-1} \rightarrow \mathrm{Kos}^q(\partial)^{q-m}$ into $\mathcal{B}^{q-m} K = dK^{q-m-1}$. This is clear if $q = m$, so suppose that $(m + 1)$ is not a zero divisor.

Let $z \in \mathrm{Kos}^q(\partial)^{q-m}$ be the image of $w \in \mathrm{Kos}^q(\partial)^{q-m-1}$, and consider $(m + 1)w$ as an element of the submodule

$$\mathrm{Sym}^{m+1}(K^0) \otimes \wedge^{q-m-1}(\mathcal{Z}^1 K) \subseteq \Gamma^{m+1}(K^0) \otimes \wedge^{q-m-1}(\mathcal{Z}^1 K).$$

Let $u \in K^{q-m-1}$ be the image of $(m + 1)w$ under the multiplication map

$$\mathrm{Sym}^{m+1}(K^0) \otimes \wedge^{q-m-1}(\mathcal{Z}^1 K) \rightarrow K^{q-m-1}.$$

Then $du = (m + 1)\mu(z)$ in K^{q-m} , where $\mu(z)$ is the image of z under the multiplication map, and hence $\mu(z)$ gives an $(m + 1)$ -torsion class in $\mathcal{H}^{q-m}(K)$. Since by assumption $\mathcal{H}^{q-m}(K) \simeq \wedge^{q-m} \mathcal{H}^1(K)$ is flat and $m + 1$ is not a zero divisor, $\mu(z) \in dK^{m-q-1}$ as desired.

Finally, the maps induced by $\mu : \tau_{\geq q-m} \mathrm{Kos}^q(\partial) \rightarrow \tau_{[q-m, q]}(K)$ on cohomology can, thanks to Proposition 2.7, be identified with the maps

$$\mu^i : \wedge^i \mathcal{H}^1(K) \rightarrow \mathcal{H}^i(K) \quad \text{for } q - m \leq i \leq q,$$

which are isomorphisms by assumption. □

Remark 2.9. Implicit in the above proof is the subcomplex $\widetilde{\mathrm{Kos}}^q(u)$ of $\mathrm{Kos}^q(u)$ whose i -th term equals $\mathrm{Sym}^{q-i} K \otimes \wedge^i(\mathcal{Z}^1 K)$. The two complexes agree in degrees $\geq q - m$, and more generally the quotient $\mathrm{Kos}^q(u)^{q-i} / \widetilde{\mathrm{Kos}}^q(u)^{q-i}$ is annihilated by $i!$. This subcomplex probably does not have any “derived meaning”, (for example, it is not clear that it is decomposable if $\tau_{\leq 1}(K)$ is), but its advantage is that there is a multiplication map $\mu : \widetilde{\mathrm{Kos}}^q(u) \rightarrow K$.

Remark 2.10. For an illustration of Theorem 2.8, let us see what happens in the “minimal” situation where it does not apply. To this end, let us consider the de Rham complex $K = [\mathbb{F}_p[x] \rightarrow \mathbb{F}_p[x] dx]$ of the polynomial ring $\mathbb{F}_p[x]$ over \mathbb{F}_p , treated as a complex of modules over $\mathbb{F}_p[x^p]$. Set $m = p - 1$ and $q = p$, and let us check that the intermediate assertion in the proof of Theorem 2.8, that $\mu : \mathrm{Kos}^q(\partial)^{q-m} \rightarrow K^{q-m}$ takes the image of $d_{\mathrm{Kos}} : \mathrm{Kos}^q(\partial)^{q-m-1} \rightarrow \mathrm{Kos}^q(\partial)^{q-m}$ into $\mathcal{B}^{q-m} K = dK^{q-m-1}$, does not hold. Explicitly,

the groups and maps in question form the diagram

$$\begin{array}{ccc}
 \Gamma_{\mathbb{F}_p[x^p]}^p(\mathbb{F}_p[x]) & \xrightarrow{d_{\text{Kos}}} & \Gamma_{\mathbb{F}_p[x^p]}^{p-1}(\mathbb{F}_p[x]) \otimes \mathbb{F}_p[x] dx \quad \simeq \quad \text{Sym}_{\mathbb{F}_p[x^p]}^{p-1}(\mathbb{F}_p[x]) \otimes \mathbb{F}_p[x] dx \\
 \downarrow ? & & \downarrow \mu \\
 d(\mathbb{F}_p[x])^{\subset} & \xrightarrow{\hspace{10em}} & \mathbb{F}_p[x] dx
 \end{array}$$

Let us consider the element $x^{[p]}$ in the top left corner. Its image under the Koszul differential is $x^{[p-1]} \otimes dx = -x^{p-1} \otimes dx$, whose image under μ is $-x^{p-1} dx$, a nonexact form.

This calculation suggests a link with the Cartier operator in the situation where K is the de Rham complex of a smooth scheme in characteristic p . And indeed, we shall see it again in the proof of Theorem 4.1.

Remark 2.11. Our proof of Theorem 2.8 makes use of an explicit model of the cdga K . Thus, for example, if K and K' are equivalent cdgas to which the theorem applies, it is not obvious whether the isomorphisms (2-2) we obtain for K and K' are compatible. More importantly, it does not apply to the more general case of coconnective E_∞ -algebras or cosimplicial commutative rings whose cohomology algebras satisfy axioms (i)–(ii) of Definition 2.1.

Corollary 2.12. *Let K be an abstract Koszul complex, and let n be such that $n!$ is invertible in \mathcal{O} . Suppose that $\tau_{\leq 1}(K)$ is decomposable. Then for $a \leq b < a + n$, the complex $\tau_{[a,b]}(K)$ is decomposable. Moreover, the complex $\tau_{\leq n}(K)$ is decomposable as well.*

2D. Application to de Rham cohomology. We now establish some of the straightforward consequences for de Rham cohomology mentioned in the introduction. The remaining ones shall be established at the end of Section 4.

Proof of Theorem 1.1, case $p > 2$. Let $K = F_{X/k,*} \Omega_{X/k}^\bullet$. By Example 2.2, this is an abstract Koszul complex over the ringed space $(X', \mathcal{O}_{X'})$. By [Deligne and Illusie 1987, théorème 2.1], the liftability assumption implies that the complex $\tau_{\leq 1}(K)$ is decomposable. Corollary 2.12 with $m = p - 1$ implies that $\tau_{[a,b]}(K)$ is decomposable for $a \leq b < a + p - 1$, as desired. □

Proof of Corollary 1.2. The differentials on the E_r -page of (1-1) depend only on the truncations $\tau_{[a,b]}(\Omega_{X/k}^\bullet)$ with $a \leq b < a + r$, and hence all differentials on the pages E_r with $r < p$ vanish. Suppose that $d_r^{ij} \neq 0$. Then in particular $H^i(X, \Omega_{X/k}^j)$ and $H^{i+r}(X, \Omega_{X/k}^{j-r+1})$ are both nonzero, and hence

$$|i - j| < p \quad \text{and} \quad |(i + r) - (j - r + 1)| = |(i - j) + 2r - 1| < p,$$

which implies $r < p$, but that forces $d_r^{ij} = 0$, hence a contradiction. Therefore (1-1) degenerates.

For X proper over k , one can deduce the degeneration of the Hodge to de Rham spectral sequence as in [Deligne and Illusie 1987, corollaire 2.4]. □

Remark 2.13. As in [Deligne and Illusie 1987, § 4] and [Kato 1989, Theorem 4.12(2)], analogous assertions hold for a smooth and separated morphism of \mathbb{F}_p -schemes $X \rightarrow S$, or more generally for a

smooth morphism of Cartier type $f : (X, \mathcal{M}_X) \rightarrow (S, \mathcal{M}_S)$ between fine log schemes over \mathbb{F}_p , assuming that there exists a fine log scheme $(\tilde{S}, \mathcal{M}_{\tilde{S}})$ over $\mathbb{Z}/p^2\mathbb{Z}$ such that \tilde{S} is flat over $\mathbb{Z}/p^2\mathbb{Z}$ and a smooth lifting

$$\tilde{f}' : (\tilde{X}', \mathcal{M}_{\tilde{X}'}) \rightarrow (\tilde{S}, \mathcal{M}_{\tilde{S}})$$

of f' (the base change f under the absolute Frobenius $(S, \mathcal{M}_S) \rightarrow (S, \mathcal{M}_S)$). Here \mathbb{F}_p and $\mathbb{Z}/p^2\mathbb{Z}$ are given the trivial log structure.

3. Truncations in two consecutive degrees and gerbes of splittings

In the following, we make a more detailed analysis of the truncations $\tau_{[q-1, q]}K$ for an abstract Koszul complex K , as well as their associated gerbes of splittings. We keep working in the category of modules in a ringed topos (X, \mathcal{O}) .

3A. First-order attachment maps. For a complex K and an integer q , the truncation

$$\tau_{[q-1, q]}K = [\cdots \rightarrow 0 \rightarrow K^{q-1}/\mathcal{B}^{q-1} \rightarrow \mathcal{Z}^q K \rightarrow 0 \rightarrow \cdots]$$

fits inside the functorial exact triangle

$$\mathcal{H}^{q-1}(K)[1-q] \rightarrow \tau_{[q-1, q]}K \rightarrow \mathcal{H}^q(K)[-q] \xrightarrow{\delta_K^q[-q]} \mathcal{H}^{q-1}(K)[2-q],$$

yielding a morphism

$$\delta_K^q : \mathcal{H}^q(K) \rightarrow \mathcal{H}^{q-1}(K)[2]$$

such that $\delta_K^q[-q]$ is the unique morphism making the above triangle distinguished (see [Achinger and Ogus 2020, Proposition 2.1.1]). Thus the truncation $\tau_{[q-1, q]}K$ is determined by the map δ_K^q , as the mapping fiber of $\delta_K^q[-q]$; it is decomposable if and only if $\delta_K^q = 0$. We note for future reference the effect of the shift functor on the maps δ_K^q :

$$\delta_{K[p]}^q = (-1)^p \delta_K^{p+q}. \tag{3-1}$$

The maps δ_K^q describe the differentials on the second page of the spectral sequence

$$E_2^{pq} = H^p(X, \mathcal{H}^q(K)) \Rightarrow H^{p+q}(X, K).$$

Namely, the differential

$$d_2^{pq} : H^p(X, \mathcal{H}^q(K)) \rightarrow H^{p+2}(X, \mathcal{H}^{q-1}(K)) = H^p(X, \mathcal{H}^{q-1}(K)[2])$$

is the map induced by δ_K^q on $H^p(X, -)$.

3B. Gerbe of splittings. We recall the gerbe of splittings described in [Deligne and Illusie 1987]. Let

$$K = [K^0 \xrightarrow{d} K^1]$$

be a two-term complex (i.e., $K^i = 0$ for $i \neq 0, 1$), and suppose that the two conditions below hold:

- (1) $\mathcal{H}^1(K)$ is locally free of finite rank, and
- (2) the projection of K^0 onto $\mathcal{B}^1 = \text{im}(d)$ locally admits a section.³

One then constructs the gerbe $\text{sc}(K)$ under $\underline{\text{Hom}}(\mathcal{H}^1(K), \mathcal{H}^0(K))$ over X [Deligne and Illusie 1987, § 3.2] as the stackification of the prestack $\text{sc}'(K)$ whose objects are local splittings

$$s : \mathcal{H}^1(K) \rightarrow K^1$$

of the projection $K^1 = \mathcal{Z}^1 K \rightarrow \mathcal{H}^1(K)$, and where morphisms $s \rightarrow s'$ are maps

$$h : \mathcal{H}^1(K) \rightarrow K^0$$

such that $dh = s' - s$. The automorphisms of an object s are then identified with $\underline{\text{Hom}}(\mathcal{H}^1(K), \mathcal{H}^0(K))$, and this makes $\text{sc}(K)$ into a gerbe under $\underline{\text{Hom}}(\mathcal{H}^1(K), \mathcal{H}^0(K))$. We denote by

$$\text{cl sc } K \in H^2(X, \underline{\text{Hom}}(\mathcal{H}^1(K), \mathcal{H}^0(K))) = \text{Ext}^2(\mathcal{H}^1(K), \mathcal{H}^0(K)) = \text{Hom}(\mathcal{H}^1(K), \mathcal{H}^0(K)[2])$$

the class of the gerbe $\text{sc } K$. The following result relates this class to the map δ_K^1 defined previously.

Lemma 3.1 [Deligne and Illusie 1987, proposition 3.3]. *Let $K = [K^0 \rightarrow K^1]$ be a two-term complex satisfying (1) and (2) above. Then, one has the following equality in $\text{Hom}(\mathcal{H}^1(K), \mathcal{H}^0(K)[2])$:*

$$\text{cl sc } K = -\delta_K^1.$$

A bit more generally, suppose that q is an integer and K a complex satisfying the following conditions:

- (1) $K^i = 0$ for $i \neq q - 1, q$,
- (2) $\mathcal{H}^q(K)$ is locally free of finite rank, and
- (3) the projection of K^{q-1} onto $\mathcal{B}^q = \text{im}(d)$ locally admits a section.

Then we denote by $\text{sc}_{[q-1, q]}(K)$ the gerbe of splittings of the complex

$$\dots \rightarrow 0 \rightarrow K^{q-1} \rightarrow K^q \rightarrow 0 \rightarrow \dots$$

concentrated in degrees 0 and 1 and with d being equal to the original differential of K , rather than $(-1)^{q-1}$ times that; this convention has the consequence that

$$\text{cl sc}_{[q-1, q]}(K) = (-1)^{q-1} \text{cl sc}(K[q - 1])$$

in $H^2(X, \underline{\text{Hom}}(\mathcal{H}^q, \mathcal{H}^{q-1}))$. Combined with Lemma 3.1 and (3-1), this implies the following generalization of Lemma 3.1:

$$\text{cl sc}_{[q-1, q]}(K) = -\delta_K^q.$$

When there is no confusion as to what q is, we simply write $\text{sc}(K)$ for $\text{sc}_{[q-1, q]}(K)$.

3C. Truncated Koszul complexes. Let $K = [K^0 \xrightarrow{d} K^1]$ be a two-term complex of modules over $(\mathcal{X}, \mathcal{O})$, and let $q \geq 1$. Using the Koszul complex, one can build another two-term complex, concentrated in

³As pointed out to us by the referee, condition (2) is in fact not needed for the construction. Indeed, if $s' - s : \mathcal{H}^1(K) \rightarrow \mathcal{B}^1$, then locally there exists an $h : \mathcal{H}^1 \rightarrow K^0$ such that $s' - s = dh$.

degrees $[q - 1, q]$:

$$\tau_{\geq q-1}(\mathbf{Kos}^q(d)) = \left[\cdots \rightarrow 0 \rightarrow \frac{K^0 \otimes \wedge^{q-1} K^1}{d(\Gamma^2 K^0 \otimes \wedge^{q-2} K^1)} \rightarrow \wedge^q K^1 \rightarrow 0 \rightarrow \cdots \right].$$

By Proposition 2.7 we have morphisms

$$\alpha^q : \wedge^q \mathcal{H}^1(K) \rightarrow \mathcal{H}^q(\mathbf{Kos}^q(d)) \quad \text{and} \quad \alpha^{q-1} : \mathcal{H}^0(K) \otimes \wedge^{q-1} \mathcal{H}^1(K) \rightarrow \mathcal{H}^{q-1}(\mathbf{Kos}^q(d)), \quad (3-2)$$

which are isomorphisms if K^0 , K^1 , $\mathcal{H}^0(K)$, and $\mathcal{H}^1(K)$ are flat. The following result describes the maps $\delta_{\mathbf{Kos}^q(d)}^q$ and hence the truncation $\tau_{\geq q-1}(\mathbf{Kos}^q(d))$.

Proposition 3.2. *Let $K = [K^0 \xrightarrow{d} K^1]$ be a two-term complex and let $q \geq 1$. Suppose that K^0 , K^1 , $\mathcal{H}^0(K)$, and $\mathcal{H}^1(K)$ are flat. Then the following diagram is commutative:*

$$\begin{array}{ccc} \wedge^q \mathcal{H}^1(K) & \xrightarrow{\eta^q} & \mathcal{H}^1(K) \otimes \wedge^{q-1} \mathcal{H}^1(K) & \xrightarrow{\delta_K^1 \otimes \text{id}} & \mathcal{H}^0(K) \otimes \wedge^{q-1} \mathcal{H}^1(K)[2] \\ \alpha^q \downarrow & & & & \downarrow \alpha^{q-1} \\ \mathcal{H}^q(\mathbf{Kos}^q(d)) & \xrightarrow{\delta_{\mathbf{Kos}^q(d)}^q} & & & \mathcal{H}^{q-1}(\mathbf{Kos}^q(d))[2] \end{array}$$

In other words, using the identifications (3-2), we have the equality

$$\delta_{\mathbf{Kos}^q(d)}^q = (\delta_K^1 \otimes \text{id}) \circ \eta^q$$

of maps $\wedge^q \mathcal{H}^1(K) \rightarrow \mathcal{H}^0(K) \otimes \wedge^{q-1} \mathcal{H}^1(K)[2]$.

Proof. Let us abbreviate $\mathcal{H}^i(K)$ to \mathcal{H}^i . We first check that the two-term complexes $\tau_{\geq q-1} \mathbf{Kos}^q(d)$ and the naive $(q-1)$ -shift of $K \otimes \wedge^{q-1} \mathcal{H}^1$ form the middle square inside a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{H}^0 \otimes \wedge^{q-1} \mathcal{H}^1 & \longrightarrow & \frac{K^0 \otimes \wedge^{q-1} K^1}{d(\Gamma^2(K^0) \otimes \wedge^{q-2} K^1)} & \longrightarrow & \wedge^q K^1 & \longrightarrow & \wedge^q \mathcal{H}^1 & \longrightarrow & 0 \\ & & \text{id} \downarrow & & \downarrow \beta & & \downarrow \alpha & & \downarrow \eta^q & & \\ 0 & \longrightarrow & \mathcal{H}^0 \otimes \wedge^{q-1} \mathcal{H}^1 & \longrightarrow & K^0 \otimes \wedge^{q-1} \mathcal{H}^1 & \xrightarrow{d \otimes \text{id}} & K^1 \otimes \wedge^{q-1} \mathcal{H}^1 & \longrightarrow & \mathcal{H}^1 \otimes \wedge^{q-1} \mathcal{H}^1 & \longrightarrow & 0 \end{array}$$

We define the maps α and β as follows. The map β is uniquely determined by

$$\beta(w \otimes z_1 \wedge \cdots \wedge z_{q-1}) \pmod{d(\Gamma^2(K^0) \otimes \wedge^{q-2} K^1)} = w \otimes [z_1] \wedge \cdots \wedge [z_{q-1}].$$

It is well defined because elements of the form

$$d(w^{[2]} \otimes z_1 \wedge \cdots \wedge z_{q-1}) = w \otimes dw \wedge z_1 \wedge \cdots \wedge z_{q-1}$$

or

$$d(wv \otimes z_1 \wedge \cdots \wedge z_{q-1}) = v \otimes dw \wedge z_1 \wedge \cdots \wedge z_{q-1} + w \otimes dv \wedge z_1 \wedge \cdots \wedge z_{q-1}$$

are sent to zero, since $[dw] = 0 = [dv]$. The map α is the composition

$$\wedge^q K^1 \xrightarrow{\eta^q} K^1 \otimes \wedge^{q-1} K^1 \xrightarrow{\text{id} \otimes \text{proj.}} K^1 \otimes \wedge^{q-1} \mathcal{H}^1.$$

The commutativity of the left- and rightmost squares is trivial to check. To see that the middle square commutes, we take (the class of) $w \otimes z_1 \wedge \cdots \wedge z_{q-1} \in K^0 \otimes \wedge^{q-1} K^1$, and compute

$$\begin{aligned} \alpha(d(w \otimes z_1 \wedge \cdots \wedge z_{q-1})) &= \alpha(dw \wedge z_1 \wedge \cdots \wedge z_{q-1}) \\ &= \sum_{i=1}^q (-1)^i z_i \otimes [dw] \wedge [z_1] \wedge \cdots \wedge \widehat{[z_i]} \wedge \cdots \wedge [z_{q-1}] + dw \otimes [z_1] \wedge \cdots \wedge [z_{q-1}] \\ &= dw \otimes [z_1] \wedge \cdots \wedge [z_{q-1}] = (d \otimes \text{id})(\beta(w \otimes z_1 \wedge \cdots \wedge z_{q-1})). \end{aligned}$$

Now, our commutative diagram of complexes translates into a commutative square in the derived category,

$$\begin{array}{ccc} \wedge^q \mathcal{H}^1 & \xrightarrow{\delta_{\text{Kos}^q(d)}^q} & \mathcal{H}^0 \otimes \wedge^{q-1} \mathcal{H}^1[2] \\ \eta^q \downarrow & & \downarrow \text{id} \\ \mathcal{H}^1 \otimes \wedge^{q-1} \mathcal{H}^1 & \xrightarrow{\delta_K^1 \otimes \text{id}} & \mathcal{H}^0 \otimes \wedge^{q-1} \mathcal{H}^1[2] \end{array}$$

This implies the required assertion. □

3D. Two-term truncations of abstract Koszul complexes. The following result relates the maps δ_K^q and δ_K^1 for a cdga K .

Proposition 3.3. *Suppose 2 is a nonzerodivisor in \mathcal{O} . Let K be a coconnective commutative differential graded algebra such that K^0 , $\mathcal{Z}^1 K$, $\mathcal{H}^0(K)$, and $\mathcal{H}^1(K)$ are flat. Let $q \geq 1$ be an integer such that $\mathcal{H}^{q-1}(K)$ is flat. Then the following diagram commutes:*

$$\begin{array}{ccccc} \wedge^q \mathcal{H}^1(K) & \xrightarrow{\eta^q} & \mathcal{H}^1(K) \otimes \wedge^{q-1} \mathcal{H}^1(K) & \xrightarrow{\delta_K^1 \otimes \text{id}} & \mathcal{H}^0(K) \otimes \wedge^{q-1} \mathcal{H}^1(K)[2] \\ \text{mult.} \downarrow & & & & \downarrow \text{mult.} \\ \mathcal{H}^q(K) & \xrightarrow{\delta_K^q} & & & \mathcal{H}^{q-1}(K)[2] \end{array}$$

Proof. Write $\tau_{\leq 1} K = [K^0 \xrightarrow{\partial} \mathcal{Z}^1 K]$. The proof of Theorem 2.8 (with $m = 1$) provides a morphism of complexes

$$\mu : \tau_{\geq q-1} \text{Kos}^q(\partial) \rightarrow \tau_{[q-1, q]} K.$$

By functoriality of the maps δ^q , we have a commutative square

$$\begin{array}{ccc} \mathcal{H}^q(\tau_{\geq q-1} \text{Kos}^q(\partial)) & \longrightarrow & \mathcal{H}^{q-1}(\tau_{\geq q-1} \text{Kos}^q(\partial))[2] \\ \mu \downarrow & & \downarrow \\ \mathcal{H}^q(\tau_{[q-1, q]} K) & \longrightarrow & \mathcal{H}^{q-1}(\tau_{[q-1, q]} K)[2] \end{array}$$

That is, a commutative square

$$\begin{array}{ccc} \wedge^q \mathcal{H}^1(K) & \longrightarrow & \mathcal{H}^0(K) \otimes \wedge^{q-1} \mathcal{H}^1(K)[2] \\ \downarrow & & \downarrow \\ \mathcal{H}^q(K) & \longrightarrow & \mathcal{H}^{q-1}(K)[2] \end{array}$$

The assertion then follows from Proposition 3.2. □

Remark 3.4. The proof of [Achinger and Ogus 2020, Theorem 4.2.2(1)] implies the assertion of Proposition 3.3 under the stronger assumption that $q!$ is invertible in \mathcal{O} . However, the argument does not use the cdga structure of K , only a weaker structure of a commutative monoid in the derived category $K \otimes^{\mathbb{L}} K \rightarrow K$. In particular, the assertion holds for some E_∞ -algebras which are not a priori equivalent to cdgas.

Remark 3.5. In [Achinger and Ogus 2020, Lemma 2.1.1], it is shown that the maps δ_K^q are compatible with the derived tensor product in the following way. If K and L are complexes and i and j are integers such that $\mathcal{H}^i(K)$ and $\mathcal{H}^j(L)$ are flat \mathcal{O} -modules, then the following square commutes:

$$\begin{array}{ccc} \mathcal{H}^i(K) \otimes \mathcal{H}^j(L) & \xrightarrow{\delta_K^i \otimes 1 + (-1)^i \otimes \delta_L^j} & (\mathcal{H}^{i-1}(K)[2] \otimes \mathcal{H}^j(L)) \oplus (\mathcal{H}^i(K) \otimes \mathcal{H}^{j-1}(L)[2]) \\ \downarrow & & \downarrow \\ \mathcal{H}^{i+j}(K \otimes^{\mathbb{L}} L) & \xrightarrow{\delta_{K \otimes^{\mathbb{L}} L}^{i+j}} & \mathcal{H}^{i+j-1}(K \otimes^{\mathbb{L}} L)[2] \end{array}$$

If $q!$ is invertible in \mathcal{O} , so that $\wedge^q \mathcal{H}^1(K)$ is a direct summand of $\mathcal{H}^1(K)^{\otimes q}$, the assertion of Proposition 3.3 can be deduced from this result.

For illustration, let us see how to do this for $q = 2$. We set $L = K$ and $i = j = 1$ in the above diagram, obtaining the middle square of the diagram below:

$$\begin{array}{ccccc} \wedge^2 \mathcal{H}^1(K) & \xrightarrow{\eta^2} & \mathcal{H}^1(K) \otimes \mathcal{H}^1(K) & \xrightarrow{\text{id} \otimes \delta_K^1} & \mathcal{H}^1(K) \otimes \mathcal{H}^0(K)[2] \\ \downarrow x \wedge y \mapsto \frac{1}{2}(x \otimes y - y \otimes x) & & \downarrow & & \downarrow \frac{1}{2}(\text{shuffle}, \text{id}) \\ \mathcal{H}^1(K) \otimes \mathcal{H}^1(K) & \xrightarrow{\delta_K^1 \otimes 1 - 1 \otimes \delta_K^1} & (\mathcal{H}^0(K)[2] \otimes \mathcal{H}^1(K)) \oplus (\mathcal{H}^1(K) \otimes \mathcal{H}^0(K)[2]) & & \\ \downarrow & & \downarrow & & \\ \mathcal{H}^2(K \otimes^{\mathbb{L}} K) & \xrightarrow{\delta_{K \otimes^{\mathbb{L}} K}^2} & \mathcal{H}^1(K \otimes^{\mathbb{L}} K)[2] & & \\ \downarrow & & \downarrow & & \\ \mathcal{H}^2(K) & \xrightarrow{\delta_K^2} & \mathcal{H}^1(K)[2] & & \end{array}$$

Here, the bottom square certifies the functoriality of δ^2 with respect to the multiplication map $K \otimes^{\mathbb{L}} K \rightarrow K$. Commutativity of the top square is easy to check. Then, commutativity of the exterior square gives the required assertion.

Corollary 3.6. *Suppose 2 is a nonzerodivisor in \mathcal{O} . Let K be an abstract Koszul complex satisfying the flatness condition (2-1) and let $q \geq 1$. We have the following commutative diagram:*

$$\begin{array}{ccccc} \wedge^q \mathcal{H}^1(K) & \xrightarrow{\eta^q} & \mathcal{H}^1(K) \otimes \wedge^{q-1} \mathcal{H}^1(K) & \xrightarrow{\delta_K^1 \otimes \text{id}} & \wedge^{q-1} \mathcal{H}^1(K)[2] \\ \wr \downarrow & & & & \downarrow \wr \\ \mathcal{H}^q(K) & \xrightarrow{\delta_K^q} & & & \mathcal{H}^{q-1}(K)[2] \end{array}$$

In other words, using the vertical identifications, we have the equality

$$\delta_K^q = (\delta_K^1 \otimes \text{id}) \circ \eta^q$$

in $\text{Hom}(\mathcal{H}^q(K), \mathcal{H}^{q-1}(K)[2])$.

Corollary 3.7. *Suppose 2 is a nonzerodivisor in \mathcal{O} . Let K be an abstract Koszul complex satisfying the flatness condition (2-1) and let $q \geq 1$. Then*

$$\text{cl sc}_{[q-1,q]}(K) = \eta^q(\text{cl sc}(\tau_{\leq 1} K)).$$

Corollary 3.8. *Suppose that 2 is a nonzerodivisor in \mathcal{O} . Let K be an abstract Koszul complex satisfying the flatness condition (2-1). Then the differential*

$$d_2^{p,q} : H^p(X, \mathcal{H}^q(K)) \rightarrow H^{p+2}(X, \mathcal{H}^{q-1}(K))$$

equals the cup product with the class

$$\delta_K^1 = -\text{cl sc}(\tau_{\leq 1} K) \in H^2(X, \underline{\text{Hom}}(\mathcal{H}^1(K), \mathcal{H}^0(K))),$$

followed by evaluation.

3E. Morphisms of gerbes of splittings. Let K be an abstract Koszul complex satisfying the flatness condition (2-1). In Corollary 3.7, under the assumption that 2 is a nonzerodivisor in \mathcal{O} , we calculated the gerbe classes $\text{cl sc}_{[q-1,q]} K$ in terms of the class $\text{cl sc}(\tau_{\leq 1} K)$. Below, under the stronger assumption that 2 is invertible, we promote this equality into a morphism of gerbes.

Theorem 3.9. *For each integer $q \geq 1$, there is a morphism*

$$\wedge^q : \text{sc}(\tau_{\leq 1} K) \rightarrow \text{sc}(\tau_{[q-1,q]} K)$$

of gerbes over X , under which the obstruction classes correspond by the relation

$$\text{cl sc}(\tau_{[q-1,q]} K) = \text{ctr}^q(\text{cl sc } \tau_{\leq 1}(K)),$$

where $\text{ctr}^q : \underline{\text{Hom}}(\mathcal{H}^1, \mathcal{H}^0) \rightarrow \underline{\text{Hom}}(\mathcal{H}^q, \mathcal{H}^{q-1})$ denotes the morphism which maps a local section f of the source to the one of the target by the formula

$$\text{ctr}^q(f) : \omega_1 \wedge \cdots \wedge \omega_q \mapsto \sum_{j=1}^q (-1)^{j-1} f(\omega_j) \omega_1 \wedge \cdots \wedge \omega_{j-1} \wedge \omega_{j+1} \wedge \cdots \wedge \omega_q.$$

(Compare the formula for ctr^q with the explicit formula for η^q in Section 2B.)

Notation. Before proceeding to the proof, we gather some notation concerning Čech cohomology. We denote by $\check{C}(U_\bullet, K^\bullet)$ the Čech resolution of a complex K^\bullet with respect to a hypercovering U_\bullet . The differential induced by that of K^\bullet will still be denoted by d , while the Čech differential on the component $\check{C}(U_p, K^q)$,

$$(-1)^q \sum_{i=0}^{p+1} (-1)^i d_i^*,$$

will be denoted by \check{d} . Then the total differential

$$D = d + \check{d}$$

is the differential of the total complex $\check{C}(U_\bullet, K^\bullet)$.

When we compute the obstruction classes, we will use some notation which may not be standard. As usual, for each integer $m \geq -1$, we denote by $[m]$ the set of integers i such that $0 \leq i \leq m$ (empty set for $[-1]$). And we denote by $d_{ij} : [m-2] \rightarrow [m]$ the unique increasing injection omitting i and j , where $0 \leq i < j \leq m$. For example, for $m = 2$, we have

$$d_{02} = d_2 \circ d_0 = d_0 \circ d_1 : [0] \rightarrow [2]$$

(which maps 0 onto 1), where $d_i : [m-1] \rightarrow [m]$ denotes the unique increasing injection omitting i .

On the other hand, we denote by $\text{pr}_i : [0] \rightarrow [m]$ (resp. $\text{pr}_{ij} : [1] \rightarrow [m]$) the unique map sending 0 to i (resp. 0 to i and 1 to j) for $0 \leq i \leq m$ (resp. for $0 \leq i < j \leq m$).

Proof of Theorem 3.9. In order to prove Theorem 3.9, we first describe the morphism, show that it is well defined, and then calculate the obstruction class.

Construction of the functor \wedge^q . We construct $\wedge^q : \text{sc } \tau_{\leq 1} K \rightarrow \text{sc } \tau_{[q-1, q]} K$ by stackifying a morphism between the corresponding prestacks: $\text{sc}' \tau_{\leq 1} K \rightarrow \text{sc}' \tau_{[q-1, q]} K$.

Given an object of $\text{sc}'(\tau_{\leq 1} K)$ over U , that is, a section $s : \mathcal{H}^1 \rightarrow \mathcal{Z}^1$ of the projection $\mathcal{Z}^1 \rightarrow \mathcal{H}^1$ over U , we define $\wedge^q(s)$ as the composite morphism

$$\mathcal{H}^q \simeq \wedge^q(\mathcal{H}^1) \xrightarrow{\wedge^q(s)} \wedge^q(\mathcal{Z}^1) \xrightarrow{\text{prod}} \mathcal{Z}^q,$$

where prod means product; it is clearly a section of $\mathcal{Z}^q \rightarrow \mathcal{H}^q$ over U .

Let s_0 and s_1 be two objects of $sc'(\tau_{\leq 1}K)$ over U and let h be a homotopy from s_0 to s_1 . Then we need to define a corresponding homotopy $\wedge^q(h)$ from $\wedge^q(s_0)$ to $\wedge^q(s_1)$. We first define a map

$$\wedge^q(h) : (\mathcal{H}^1)^{\otimes q} \rightarrow K^{q-1}/\mathcal{B}^{q-1}$$

by letting it send $\omega_1 \otimes \cdots \otimes \omega_q$ (where ω_j are local sections of \mathcal{H}^1) to the class of

$$\sum_{j=1}^q (-1)^{j-1} h(\omega_j) s_0(\omega_1) \wedge \cdots \wedge s_0(\omega_{j-1}) \wedge s_1(\omega_{j+1}) \wedge \cdots \wedge s_1(\omega_q)$$

modulo \mathcal{B}^{q-1} .

It is easy to show that it factors through $\wedge^q \mathcal{H}^1$: if, say, $\omega_1 = \omega_2 = \omega$, then the alternating sum on the right reduces to the difference of the first two terms

$$h(\omega) s_1(\omega) \wedge s_1(\omega_3) \wedge \cdots \wedge s_1(\omega_q) - h(\omega) s_0(\omega) \wedge s_1(\omega_3) \wedge \cdots \wedge s_1(\omega_q),$$

which is equal to

$$h(\omega) dh(\omega) \wedge s_1(\omega_3) \wedge \cdots \wedge s_1(\omega_q),$$

which is a coboundary *since 2 is invertible*. Thus we have defined $\wedge^q(h)$:

$$\begin{array}{ccc} (\mathcal{H}^1)^{\otimes q} & & \\ \downarrow & \searrow \wedge^q(h) & \\ \wedge^q(\mathcal{H}^1) & \xrightarrow[\wedge^q(h)]{} & K^{q-1}/\mathcal{B}^{q-1} \end{array}$$

Then the following calculation shows that $\wedge^q(h)$ is really a homotopy:

$$\begin{aligned} & (\wedge^q(s_1) - \wedge^q(s_0))(\omega_1 \wedge \cdots \wedge \omega_q) \\ &= \sum_{j=1}^q s_0(\omega_1) \wedge \cdots \wedge s_0(\omega_{j-1}) \wedge \{s_1(\omega_j) - s_0(\omega_j)\} \wedge s_1(\omega_{j+1}) \wedge \cdots \wedge s_1(\omega_q) \\ &= \sum_{j=1}^q s_0(\omega_1) \wedge \cdots \wedge s_0(\omega_{j-1}) \wedge \{dh(\omega_j)\} \wedge s_1(\omega_{j+1}) \wedge \cdots \wedge s_1(\omega_q) \\ &= \sum_{j=1}^q (-1)^{j-1} dh(\omega_j) \wedge s_0(\omega_1) \wedge \cdots \wedge s_0(\omega_{j-1}) \wedge s_1(\omega_{j+1}) \wedge \cdots \wedge s_1(\omega_q) \\ &= d[\wedge^q(h)(\omega_1 \wedge \cdots \wedge \omega_q)]. \end{aligned}$$

Functoriality of \wedge^q . Now in order to show that the morphism \wedge^q is a functor, we must show that it is compatible with the composition of homotopies; so let $h : s_0 \Rightarrow s_1$ and $h' : s_1 \Rightarrow s_2$ be two such in the

source. We first define a second homotopy operator

$$H_2^q(h, h') : (\mathcal{H}^1)^{\otimes q} \rightarrow K^{q-2}, \quad \omega_1 \otimes \cdots \otimes \omega_q \mapsto \sum_{1 \leq j < k \leq q} (-1)^{j+k+1} h(\omega_j) h'(\omega_k) s(j, k),$$

where $s(j, k)$ is equal to

$$s_0(\omega_1) \wedge \cdots \wedge s_0(\omega_{j-1}) \wedge s_1(\omega_{j+1}) \wedge \cdots \wedge s_1(\omega_{k-1}) \wedge s_2(\omega_{k+1}) \wedge \cdots \wedge s_2(\omega_q).$$

To show that $\wedge^q(h + h')$ and $\wedge^q(h) + \wedge^q(h')$ are the same homotopies, it suffices to demonstrate the formula

$$[\wedge^q(h + h') - \{\wedge^q(h) + \wedge^q(h')\}](\omega_1 \wedge \cdots \wedge \omega_q) = dH_2^q(\omega_1 \otimes \cdots \otimes \omega_q).$$

One expands the left-hand side and groups the terms involving h and h' separately:

$$\begin{aligned} & \sum_{j=1}^q (-1)^{j-1} \{h(\omega_j) + h'(\omega_j)\} s_0(\omega_1) \wedge \cdots \wedge s_0(\omega_{j-1}) \wedge s_2(\omega_{j+1}) \wedge \cdots \wedge s_2(\omega_q) \\ & \quad - \sum_{j=1}^q (-1)^{j-1} h(\omega_j) s_0(\omega_1) \wedge \cdots \wedge s_0(\omega_{j-1}) \wedge s_1(\omega_{j+1}) \wedge \cdots \wedge s_1(\omega_q) \\ & \quad \quad - \sum_{j=1}^q (-1)^{j-1} h'(\omega_j) s_1(\omega_1) \wedge \cdots \wedge s_1(\omega_{j-1}) \wedge s_2(\omega_{j+1}) \wedge \cdots \wedge s_2(\omega_q) \\ & = \sum_{j=1}^q (-1)^{j-1} h(\omega_j) s_0(\omega_1) \wedge \cdots \wedge s_0(\omega_{j-1}) \wedge \{s_2(\omega_{j+1}) \wedge \cdots \wedge s_2(\omega_q) - s_1(\omega_{j+1}) \wedge \cdots \wedge s_1(\omega_q)\} \\ & \quad + \sum_{k=1}^q (-1)^{k-1} h'(\omega_k) \{s_0(\omega_1) \wedge \cdots \wedge s_0(\omega_{k-1}) - s_1(\omega_1) \wedge \cdots \wedge s_1(\omega_{k-1})\} \wedge s_2(\omega_{k+1}) \wedge \cdots \wedge s_2(\omega_q). \end{aligned}$$

The differences in the curly brackets are themselves alternating sums, so the last expression is equal to

$$\begin{aligned} & \sum_{j=1}^q (-1)^{j-1} h(\omega_j) s_0(\omega_1) \wedge \cdots \wedge s_0(\omega_{j-1}) \\ & \quad \wedge \left\{ \sum_{k>j} (-1)^{k-(j+1)} dh'(\omega_k) \wedge s_1(\omega_{j+1}) \wedge \cdots \wedge s_1(\omega_{k-1}) \wedge s_2(\omega_{k+1}) \wedge \cdots \wedge s_2(\omega_q) \right\} \\ & \quad + \sum_{k=1}^q (-1)^{k-1} h'(\omega_k) \left\{ \sum_{j<k} (-1)^{j-1} (-dh(\omega_j)) \wedge s_0(\omega_1) \wedge \cdots \wedge s_0(\omega_{j-1}) \wedge s_1(\omega_{j+1}) \wedge \cdots \wedge s_1(\omega_{k-1}) \right\} \\ & \quad \quad \quad \wedge s_2(\omega_{k+1}) \wedge \cdots \wedge s_2(\omega_q) \\ & = \sum_{1 \leq j < k \leq q} (-1)^{j+k+1} \{h(\omega_j) dh'(\omega_k) + h'(\omega_k) dh(\omega_j)\} \wedge s(j, k), \end{aligned}$$

and this is now equal to

$$dH_2^q(h, h')(\omega_1 \otimes \cdots \otimes \omega_q). \tag{3-3}$$

This completes the proof of the fact that \wedge^q is a functor.

Calculation of obstruction classes. Finally, we relate the obstruction elements. Let $U_\bullet \rightarrow X$ be an open hypercovering such that one has

- (1) a section $s : \mathcal{H}^1 \rightarrow \mathcal{Z}^1$ of the canonical projection $\mathcal{Z}^1 \rightarrow \mathcal{H}^1$ over U_0 , and
- (2) a homotopy $h : \mathcal{H}^1 \rightarrow K^0$ over U_1 satisfying

$$d_1^* s - d_0^* s = dh. \quad (3-4)$$

Then, by definition, the class of

$$\text{obs} = \text{obs}_1 = d_0^* h - d_1^* h + d_2^* h \in \Gamma(U_2, \underline{\text{Hom}}(\mathcal{H}^1, \mathcal{H}^0))$$

in $H^2(X, \underline{\text{Hom}}(\mathcal{H}^1, \mathcal{H}^0))$ is cl sc $\tau_{\leq 1} K$. On the other hand, by applying \wedge^q to s and h , one sees that the class of

$$\text{obs}_q = d_0^*(\wedge^q h) - d_1^*(\wedge^q h) + d_2^*(\wedge^q h) \in \Gamma(U_2, \underline{\text{Hom}}(\mathcal{H}^q, \mathcal{H}^{q-1}))$$

in $H^2(X, \underline{\text{Hom}}(\mathcal{H}^q, \mathcal{H}^{q-1}))$ is cl sc $\tau_{[q-1, q]} K$.

Now let $\omega_1 \wedge \cdots \wedge \omega_q$ be a local section of $\mathcal{H}^q \simeq \wedge^q \mathcal{H}^1$. Then the evaluation of obs_q at $\omega_1 \wedge \cdots \wedge \omega_q$ is equal to

$$\begin{aligned} & \sum_{j=1}^q (-1)^{j+1} d_0^* h(\omega_j) d_{01}^* s(\omega_1) \wedge \cdots \wedge d_{01}^* s(\omega_{j-1}) \wedge d_{02}^* s(\omega_{j+1}) \wedge \cdots \wedge d_{02}^* s(\omega_q) \\ & - \sum_{j=1}^q (-1)^{j+1} d_1^* h(\omega_j) d_{01}^* s(\omega_1) \wedge \cdots \wedge d_{01}^* s(\omega_{j-1}) \wedge d_{12}^* s(\omega_{j+1}) \wedge \cdots \wedge d_{12}^* s(\omega_q) \\ & + \sum_{j=1}^q (-1)^{j+1} d_2^* h(\omega_j) d_{02}^* s(\omega_1) \wedge \cdots \wedge d_{02}^* s(\omega_{j-1}) \wedge d_{12}^* s(\omega_{j+1}) \wedge \cdots \wedge d_{12}^* s(\omega_q). \end{aligned}$$

One groups the terms around the second sum and gets

$$\begin{aligned} & \sum_{j=1}^q (-1)^{j+1} (d_0^* h - d_1^* h + d_2^* h)(\omega_j) \cdot d_{01}^* s(\omega_1) \wedge \cdots \wedge d_{01}^* s(\omega_{j-1}) \wedge d_{12}^* s(\omega_{j+1}) \wedge \cdots \wedge d_{12}^* s(\omega_q) \\ & + \sum_{j=1}^q (-1)^{j+1} d_0^* h(\omega_j) d_{01}^* s(\omega_1) \wedge \cdots \wedge d_{01}^* s(\omega_{j-1}) \\ & \quad \wedge \{d_{02}^* s(\omega_{j+1}) \wedge \cdots \wedge d_{02}^* s(\omega_q) - d_{12}^* s(\omega_{j+1}) \wedge \cdots \wedge d_{12}^* s(\omega_q)\} \\ & + \sum_{j=1}^q (-1)^{j+1} d_2^* h(\omega_j) \{d_{02}^* s(\omega_1) \wedge \cdots \wedge d_{02}^* s(\omega_{j-1}) - d_{01}^* s(\omega_1) \wedge \cdots \wedge d_{01}^* s(\omega_{j-1})\} \\ & \quad \wedge d_{12}^* s(\omega_{j+1}) \wedge \cdots \wedge d_{12}^* s(\omega_q). \end{aligned}$$

The first alternating sum reduces to the “main” term we want, when taken modulo the coboundaries (\mathcal{B}^{q-1}). In the last two sums, one first notes that, as h is a homotopy from $d_0^* s$ to $d_1^* s$, it follows that $d_0^* h$

is a homotopy from $d_0^* d_0^* s$ to $d_0^* d_1^* s$, that is,

$$d_0^* h : d_{01}^* s \Rightarrow d_{02}^* s.$$

Similarly, $d_2^* h$ is a homotopy from $d_{02}^* s$ to $d_{12}^* s$. Essentially by repeating the last three equalities leading up to (3-3), this time with a minus sign, one sees that the last two sums add up to

$$-dH_2^q(d_0^* h, d_2^* h)(\omega_1 \otimes \cdots \otimes \omega_q),$$

which is a coboundary. Therefore, reducing modulo \mathcal{B}^{q-1} , one gets

$$\text{ev}(\text{obs}_q, \omega_1 \wedge \cdots \wedge \omega_q) = \text{ev}(\text{ctr}^q(\text{obs}_1), \omega_1 \wedge \cdots \wedge \omega_q).$$

This means

$$\text{cl sc } \tau_{[q-1, q]} K = \text{ctr}^q \text{ cl sc } \tau_{\leq 1} K,$$

which completes the proof. □

Remark 3.10. The construction of the map between gerbes can also be carried out using the language of higher topos theory [Lurie 2009]. Let us give a brief outline.

Let $p : Y \rightarrow Z$ be a map of spaces, or more generally in any ∞ -category \mathcal{C} . One can then build the space $\text{sc}(p)$ of splittings of p as the homotopy fiber of

$$p : \text{Hom}_{\mathcal{C}}(Z, Y) \rightarrow \text{Hom}_{\mathcal{C}}(Z, Z)$$

over the identity id_Z . Similarly, if $p : Y \rightarrow Z$ is a map in the derived ∞ -category of a ringed topos (X, \mathcal{O}) , one obtains a sheaf of spaces $\underline{\text{sc}}(p)$ of splittings of p .

In the special case when Y is a two-term complex $K = [K^0 \xrightarrow{d} K^1]$ satisfying the conditions in Section 3B and $Y \rightarrow Z$ is the projection $K \rightarrow \mathcal{H}^1(K)[-1]$, the sheaf $\underline{\text{sc}}(p)$ is a sheaf of groupoids (a stack) and can be identified with the gerbe of splittings $\text{sc } K$.

Applying the functor $\tau_{\geq q-1} L\Gamma^q$ to the map $p : K \rightarrow \mathcal{H}^1(K)[-1]$ one obtains (simply by functoriality) a morphism of sheaves of spaces

$$\underline{\text{sc}}(p) \rightarrow \underline{\text{sc}}(\tau_{\geq q-1} L\Gamma^q(p)).$$

By inspection, the map $\tau_{\geq q-1} L\Gamma^q(p)$ is the projection

$$\tau_{[q-1, q]} \text{Kos}^q(d) \rightarrow \mathcal{H}^q(\text{Kos}^q(d))[-q] = \wedge^q \mathcal{H}^1(K)[-q].$$

This way one obtains by abstract nonsense a morphism of gerbes $\text{sc } K \rightarrow \text{sc}(\tau_{[q-1, q]} \text{Kos}^q(d))$.

In the case when K is an abstract Koszul complex satisfying the flatness condition (2-1), the morphism of gerbes $\text{sc } \tau_{\leq 1} K \rightarrow \text{sc } \tau_{[q-1, q]} K$ obtained this way should agree with the one constructed in Theorem 3.9, though we did not check it.

4. Gerbes of splittings of the de Rham complex

Our method of explicating the truncations $\tau_{[q-1, q]}K$ for an abstract Koszul complex K in terms of the truncation $\tau_{\leq 1}K$ requires that 2 be a nonzerodivisor. In this section, we describe these two-term truncations in the case of the de Rham complex in characteristic $p > 0$ by calculating the class

$$\text{cl sc}(\tau_{[q-1, q]}F_*\Omega_{X/S}^\bullet).$$

The calculation uses more information about the de Rham complex than its being an abstract Koszul complex, namely the nature of the Cartier isomorphism (which we use only for $p = 2$). As a corollary, we deduce that $\tau_{[q-1, q]}(F_*\Omega_{X/S}^\bullet)$ is decomposable if $\tau_{\leq 1}(F_*\Omega_{X/S}^\bullet)$ is, and obtain a description of the d_2 differentials in the conjugate spectral sequence.

Theorem 4.1. *Let S be a scheme of characteristic $p > 0$ and X/S a smooth separated scheme of finite type. Then for each integer q , the class*

$$\text{cl sc}(\tau_{[q-1, q]}F_*\Omega_{X/S}^\bullet)$$

is the image of the class

$$\text{cl sc}(\tau_{\leq 1}F_*\Omega_{X/S}^\bullet)$$

under the contraction map (described in Theorem 3.9).

Proof. We put $K = F_*\Omega_{X/S}^\bullet$, with $F : X \rightarrow X'$ the relative Frobenius of X/S .

To calculate the class, we take an open hypercovering $U_\bullet \rightarrow X'$ such that

(1) over U_0 , one has a section $s : \mathcal{H}^1 \rightarrow \mathcal{Z}^1$ of the projection $\mathcal{Z}^1 \rightarrow \mathcal{H}^1$ and a section

$$\sigma^{(q)} : \mathcal{H}^q \rightarrow (\mathcal{H}^1)^{\otimes q}$$

of the canonical projection $(\mathcal{H}^1)^{\otimes q} \rightarrow \mathcal{H}^q$, and

(2) over U_1 , one has a homotopy $h : \mathcal{H}^1 \rightarrow K^0$ such that

$$dh = d_1^*s - d_0^*s : \mathcal{H}^1 \rightarrow \mathcal{Z}^1.$$

(Let us recall that \mathcal{H}^1 is locally free over $\mathcal{O}_{X'}$, and hence so is $\mathcal{H}^q = \wedge^q \mathcal{H}^1$ for all integers q .) The locally free kernel of the projection $(\mathcal{H}^1)^{\otimes q} \rightarrow \mathcal{H}^q$ being denoted by \mathcal{J}^q , the 1-cocycle

$$d_0^*\sigma^{(q)} - d_1^*\sigma^{(q)} \in \Gamma(U_1, \underline{\text{Hom}}_{\mathcal{O}_{X'}}(\mathcal{H}^q, \mathcal{J}^q))$$

represents the obstruction, in $H^1(X', \underline{\text{Hom}}(\mathcal{H}^q, \mathcal{J}^q)) = \text{Ext}_{\mathcal{O}_{X'}}^1(\mathcal{H}^q, \mathcal{J}^q)$, to the global existence of a section.

Let us calculate the class

$$\text{cl sc } \tau_{[q-1,q]}K \in H^2(X', \underline{\text{Hom}}(\mathcal{H}^q, \mathcal{H}^{q-1}))$$

in characteristic $p \geq 2$. For ease of notation, we denote $\sigma^{(q)}$ simply by σ when no confusion is likely.

To do so, we may choose the composite morphism

$$\mathcal{H}^q \xrightarrow{\sigma^{(q)}} (\mathcal{H}^1)^{\otimes q} \xrightarrow{s^{\otimes q}} (\mathcal{Z}^1)^{\otimes q} \xrightarrow{\wedge} \mathcal{Z}^q,$$

which we denote by $(s^{\wedge q}) \circ \sigma$, as the section of the projection $\mathcal{Z}^q \rightarrow \mathcal{H}^q$ over U_0 .

Then one forms (the negative of) the Čech difference

$$d_1^*(s^{\wedge q}) \circ d_1^* \sigma - d_0^*(s^{\wedge q}) \circ d_0^* \sigma = [(d_1^* s)^{\wedge q} - (d_0^* s)^{\wedge q}] \circ d_0^* \sigma - (d_1^* s)^{\wedge q} \circ (d_0^* \sigma - d_1^* \sigma).$$

One notes that the second term is zero, since the image of $d_0^* \sigma - d_1^* \sigma$ is contained in \mathcal{J}^q , which in turn is annihilated by $(d_1^* s)^{\wedge q}$, for the wedge product is strictly graded commutative.

Then one expresses — over U_1 — the remaining first term as the differential of something:

$$\begin{aligned} & ((d_1^* s)^{\wedge q} - (d_0^* s)^{\wedge q})(\omega_1 \otimes \cdots \otimes \omega_q) \\ &= \sum_{j=1}^q (d_0^* s) \omega_1 \wedge \cdots \wedge (d_0^* s) \omega_{j-1} \wedge (d_1^* s - d_0^* s) \omega_j \wedge (d_1^* s) \omega_{j+1} \wedge \cdots \wedge (d_1^* s) \omega_q \\ &= d \sum_{j=1}^q (-1)^{j+1} h(\omega_j) (d_0^* s) \omega_1 \wedge \cdots \wedge (d_0^* s) \omega_{j-1} \wedge (d_1^* s) \omega_{j+1} \wedge \cdots \wedge (d_1^* s) \omega_q. \end{aligned}$$

One defines $\eta = \eta^{(q)} = \eta(\omega_1 \otimes \cdots \otimes \omega_q)$ to be

$$\sum_{j=1}^q (-1)^{j+1} h(\omega_j) (d_0^* s) \omega_1 \wedge \cdots \wedge (d_0^* s) \omega_{j-1} \wedge (d_1^* s) \omega_{j+1} \wedge \cdots \wedge (d_1^* s) \omega_q$$

in order to have a commutative diagram

$$\begin{array}{ccc} \mathcal{H}^q & \xrightarrow{d_1^*(s^{\wedge q}) \circ d_1^* \sigma - d_0^*(s^{\wedge q}) \circ d_0^* \sigma} & \mathcal{Z}^q \\ & \searrow d_0^* \sigma & \nearrow d \\ & (\mathcal{H}^1)^{\otimes q} \xrightarrow{\bar{\eta}} & K^{q-1}/\mathcal{B}^{q-1} \end{array}$$

in which $\bar{\eta}$ means the composite of η followed by $K^{q-1} \rightarrow K^{q-1}/\mathcal{B}^{q-1}$.

With this, we calculate the class of the gerbe by forming the Čech difference over U_2 :

$$\begin{aligned} (d_0^* - d_1^* + d_2^*)(\bar{\eta} \circ d_0^* \sigma) &= d_0^* \bar{\eta} \circ d_{01}^* \sigma - d_1^* \bar{\eta} \circ d_{01}^* \sigma + d_2^* \bar{\eta} \circ d_{02}^* \sigma \\ &= (d_0^* - d_1^* + d_2^*) \bar{\eta} \circ d_{01}^* \sigma - d_2^* \bar{\eta} \circ (d_{01}^* \sigma - d_{02}^* \sigma). \end{aligned} \tag{4-1}$$

Let us put $\text{obs}_1 = (d_0^* - d_1^* + d_2^*)h$, which represents the class of $\text{sc } \tau_{\leq 1} K$. Then the first summand in the second line of (4-1) can be expressed in terms of obs_1 :

$$\begin{aligned}
& (d_0^* - d_1^* + d_2^*)\bar{\eta}(\omega_1 \otimes \cdots \otimes \omega_q) \\
&= \sum_{j=1}^q (-1)^{j+1} d_0^* h(\omega_j) d_{01}^* s(\omega_1) \wedge \cdots \wedge d_{01}^* s(\omega_{j-1}) \wedge d_{02}^* s(\omega_{j+1}) \wedge \cdots \wedge d_{02}^* s(\omega_q) \\
&\quad - \sum_{j=1}^q (-1)^{j+1} d_1^* h(\omega_j) d_{01}^* s(\omega_1) \wedge \cdots \wedge d_{01}^* s(\omega_{j-1}) \wedge d_{12}^* s(\omega_{j+1}) \wedge \cdots \wedge d_{12}^* s(\omega_q) \\
&\quad + \sum_{j=1}^q (-1)^{j+1} d_2^* h(\omega_j) d_{02}^* s(\omega_1) \wedge \cdots \wedge d_{02}^* s(\omega_{j-1}) \wedge d_{12}^* s(\omega_{j+1}) \wedge \cdots \wedge d_{12}^* s(\omega_q) \\
&= \sum_{j=1}^q (-1)^{j+1} \text{obs}_1(\omega_j) d_{01}^* s(\omega_1) \wedge \cdots \wedge d_{01}^* s(\omega_{j-1}) \wedge d_{12}^* s(\omega_{j+1}) \wedge \cdots \wedge d_{12}^* s(\omega_q) \\
&\quad + \sum_{j=1}^q (-1)^{j+1} d_0^* h(\omega_j) d_{01}^* s(\omega_1) \wedge \cdots \wedge d_{01}^* s(\omega_{j-1}) \wedge \{ (d_{02}^* s^{\wedge(q-j)} - d_{12}^* s^{\wedge(q-j)})(\omega_{j+1} \otimes \cdots \otimes \omega_q) \} \\
&\quad + \sum_{j=1}^q (-1)^{j+1} d_2^* h(\omega_j) \{ (d_{02}^* s^{\wedge(j-1)} - d_{01}^* s^{\wedge(j-1)})(\omega_1 \otimes \cdots \otimes \omega_{j-1}) \} \wedge d_{12}^* s(\omega_{j+1}) \wedge \cdots \wedge s(\omega_q).
\end{aligned}$$

Again, as in the three equalities leading up to (3-3), the differences in the curly brackets are themselves alternating sums, and one sees that the sum of the last two alternating sums is equal to

$$-dH_2^q(d_0^*h, d_2^*h)(\omega_1 \otimes \cdots \otimes \omega_q),$$

hence is zero modulo \mathcal{B}^{q-1} . On the other hand, the first alternating sum is equal to

$$\text{ev}(\text{ctr}(\text{obs}_1), \omega_1 \wedge \cdots \wedge \omega_q).$$

Now we analyze the second summand in the second line of (4-1). It is the cup product of two cohomology classes:

$$\bar{\eta}|_{\mathcal{J}^q} \in \Gamma(U_1, \underline{\text{Hom}}(\mathcal{J}^q, \mathcal{H}^{q-1})) \text{ representing } [\bar{\eta}|_{\mathcal{J}^q}] \in \text{Ext}^1(\mathcal{J}^q, \mathcal{H}^{q-1})$$

and

$$d_0^* \sigma - d_1^* \sigma \in \Gamma(U_1, \underline{\text{Hom}}(\mathcal{H}^q, \mathcal{J}^q)) \text{ representing } [\sigma] \in \text{Ext}^1(\mathcal{H}^q, \mathcal{J}^q).$$

When q is less than $p = \text{char}(S)$, $[\sigma]$ is zero, for in this case one disposes of a canonical section of

$$(\mathcal{H}^1)^{\otimes q} \rightarrow \mathcal{H}^q,$$

namely the antisymmetrization.

On the other hand, if p is odd, then $[\bar{\eta}|_{\mathcal{J}^q}]$ is zero, because (even more strongly) $\bar{\eta}$ itself kills \mathcal{J}^q : for example, it maps a local section

$$\omega \otimes \omega \otimes \omega_3 \otimes \cdots \otimes \omega_q$$

of \mathcal{J}^q to the element

$$[h(\omega) d_1^* s(\omega) - h(\omega) d_0^* s(\omega)] \wedge d_1^* s(\omega_3) \wedge \cdots \wedge d_1^* s(\omega_q) = h(\omega) dh(\omega) \wedge \omega_3 \wedge \cdots \wedge \omega_q \pmod{\mathcal{B}^{q-1}},$$

which is a coboundary when 2 is invertible ($d(h(\omega)^2) = 2h(\omega) dh(\omega)$).

So let us restrict our attention to the case $p = 2$ and show that the class $[\bar{\eta}|_{\mathcal{J}^q}]$ is still zero. First, one can easily check that $\bar{\eta} : (\mathcal{H}^1)^{\otimes q} \rightarrow K^{q-1}/\mathcal{B}^{q-1}$, and a fortiori $\bar{\eta}|_{\mathcal{J}^q} : \mathcal{J}^q \rightarrow \mathcal{Z}^{q-1}/\mathcal{B}^{q-1} = \mathcal{H}^{q-1}$, is *symmetric* in the sense that any element of the form

$$\omega_1 \otimes \cdots \otimes \omega_{j-1} \otimes (\omega_j \otimes \omega_{j+1} + \omega_{j+1} \otimes \omega_j) \otimes \omega_{j+2} \otimes \cdots \otimes \omega_q$$

(when $1 = -1$, adding is subtracting) maps to zero under $\bar{\eta}$. Therefore, one has a commutative diagram

$$\begin{array}{ccccc} \mathcal{J}^q & \longrightarrow & \mathcal{J}^q/\mathcal{J}^q & \xrightarrow{\bar{\eta}} & \mathcal{H}^{q-1} \\ \downarrow & & \downarrow & & \downarrow \\ (\mathcal{H}^1)^{\otimes q} & \longrightarrow & \text{Sym}^q(\mathcal{H}^1) & \longrightarrow & K^{q-1}/\mathcal{B}^{q-1} \end{array}$$

where the composite of the two horizontal arrows in the first row (resp. in the second row) is equal to $\bar{\eta}|_{\mathcal{J}^q}$ (resp. $\bar{\eta}$), and \mathcal{J}^q denotes the (locally free) kernel of the projection $(\mathcal{H}^1)^{\otimes q} \rightarrow \text{Sym}^q(\mathcal{H}^1)$.

We get a notational advantage by taking the quotient by \mathcal{J}^q : now $\mathcal{J}^q/\mathcal{J}^q$ is generated by the images of local sections of the form

$$\omega \otimes \omega \otimes \omega_3 \otimes \cdots \otimes \omega_q. \tag{4-2}$$

Such a local section is mapped under $\bar{\eta}$ onto

$$h(\omega) dh(\omega) \wedge d_0^* s(\omega_3) \wedge \cdots \wedge d_0^* s(\omega_q) \pmod{\mathcal{B}^{q-1}} = [h(\omega) dh(\omega) \pmod{\mathcal{B}^1}] \wedge \omega_3 \wedge \cdots \wedge \omega_q. \tag{4-3}$$

We prove that $[\bar{\eta}|_{\mathcal{J}^q}]$ is zero by finding a 0-cochain z with coefficients in $\text{Hom}(\mathcal{J}^q, \mathcal{H}^{q-1})$, that is, a section of this sheaf over U_0 , such that $\bar{\eta}|_{\mathcal{J}^q} = d_0^* z - d_1^* z$. As we know that $\bar{\eta}|_{\mathcal{J}^q}$ factors through $\bar{\eta} : \mathcal{J}^q/\mathcal{J}^q \rightarrow \mathcal{H}^{q-1}$, it suffices to find $\tilde{z} : \mathcal{J}^q/\mathcal{J}^q \rightarrow \mathcal{H}^{q-1}$ such that

$$\bar{\eta} = d_1^* \tilde{z} - d_0^* \tilde{z}.$$

But from (4-3) and the fact that $C^{-1}W^* dh(\omega) = [h(\omega) dh(\omega)]$, one sees that

$$\bar{\eta}(\omega \otimes \omega \otimes \omega_3 \otimes \cdots \otimes \omega_q) = (C^{-1}W^* dh(\omega)) \wedge \omega_3 \wedge \cdots \wedge \omega_q. \tag{4-4}$$

We denote here by W the base change of the absolute Frobenius endomorphism of S , so that the diagram

$$\begin{array}{ccc} X' & \xrightarrow{W} & X \\ \downarrow & & \downarrow \\ S & \xrightarrow{\text{frob}_S} & S \end{array}$$

is cartesian, by W^* the pullback morphism of differential forms

$$\Omega_{X/S}^1 \rightarrow W_* \Omega_{X'/S}^1$$

and by C^{-1} the (inverse) Cartier operation

$$\Omega_{X'/S}^1 \rightarrow \mathcal{H}^1(F_* \Omega_{X/S}^\bullet)$$

(see [Katz 1970, § 7] and recall $p = 2$). Thus the last expression is the same as

$$C^{-1} W^*(d_1^* s \omega) \wedge \omega_3 \wedge \cdots \wedge \omega_q - C^{-1} W^*(d_0^* s \omega) \wedge \omega_3 \wedge \cdots \wedge \omega_q,$$

and one is led to define over U_0

$$\tilde{z} : \mathcal{J}^q / \mathcal{J}^q \rightarrow \mathcal{H}^{q-1}$$

so that it maps the local section (4-2) modulo \mathcal{J}^q to

$$C^{-1} W^*(s \omega) \wedge \omega_3 \wedge \cdots \wedge \omega_q.$$

As pointed out earlier, local sections of the form (4-2) generate $\mathcal{J}^q / \mathcal{J}^q$, so such \tilde{z} is unique if exists at all. Now its existence can be shown locally: if one has a basis e_1, \dots, e_d of \mathcal{H}^1 over $\mathcal{O}_{X'}$, then the images of the sections

$$\{e_{j_1} \otimes \cdots \otimes e_{j_q} : 1 \leq j_1 \leq \cdots \leq j_q \leq d \text{ with at least one repetition}\}$$

under $\mathcal{J}^q \rightarrow \mathcal{J}^q / \mathcal{J}^q$ form a local basis of $\mathcal{J}^q / \mathcal{J}^q$, and then one can let \tilde{z} map the class of $e_{j_1} \otimes \cdots \otimes e_{j_q}$ to

$$C^{-1} W^*(s(\omega_{j_k})) \wedge (\text{the rest}),$$

where j_k is an index that repeats: if two or more indices repeat, whichever one is chosen, the result is zero, and if an index repeats itself three or more times, it doesn't matter which consecutive terms are chosen, for $1 = -1$ and the sign doesn't matter.

Then one needs to show that any local section of the form (4-2) is mapped as desired under \tilde{z} thus defined. One expresses the sections $\omega, \omega_3, \dots, \omega_q$ as linear combinations of the $\{e_i\}$ and one sees that it boils down to showing the linearity in each variable $\omega_3, \dots, \omega_q$, which is evident, as well as the linearity “in the variable $\omega \otimes \omega$ ”, which is less so.

Let $\omega = \alpha\xi + \beta\theta$, where α, β are sections of $\mathcal{O}_{X'}$ and ξ, θ sections of \mathcal{H}^1 . Then one calculates

$$\begin{aligned} C^{-1}W^*(s(\alpha\xi + \beta\theta)) &= C^{-1}W^*(F^*\alpha \cdot s(\xi) + F^*\beta \cdot s(\theta)) \\ &= C^{-1}(\alpha^2W^*s(\xi) + \beta^2W^*s(\theta)) \\ &= (F^*\alpha)^2C^{-1}W^*s(\xi) + (F^*\beta)^2C^{-1}W^*s(\theta), \end{aligned}$$

where $F^* : \mathcal{O}_{X'} \rightarrow F_*\mathcal{O}_X$ is the canonical pullback morphism; here one uses the fact that $W \circ F$ is equal to the absolute Frobenius of X .

On the other hand, if one expands $\omega \otimes \omega$ as $\alpha^2\xi \otimes \xi + \beta^2\theta \otimes \theta + \alpha\beta(\xi \otimes \theta + \theta \otimes \xi)$, then the last term is symmetric (i.e., lies in \mathcal{J}^2), and hence we get the same result this way.

This can also be explained with the diagram

$$\begin{array}{c} \mathcal{Z}^1 \subseteq F_*\Omega_{X/S}^1 \xrightarrow{F_*(W^*)} F_*W_*\Omega_{X'/S}^1 \xrightarrow{F_*W_*C^{-1}} F_*W_*\mathcal{H}^1(K) = (F_{X'})_*\mathcal{H}^1(K) \\ \uparrow s \\ \mathcal{H}^1(K) \end{array}$$

over U_0 , where $F_{X'}$ denotes the absolute Frobenius of X' ; it shows that the map

$$\omega \mapsto C^{-1}W^*s(\omega)$$

is 2-linear, while “extracting” ω out of $\omega \otimes \omega$ would be 2^{-1} -linear; hence these nonlinearities cancel each other and the map $\omega \otimes \omega \mapsto C^{-1}W^*s(\omega)$ is linear.

This shows that \tilde{z} , hence the 0-cochain z which is obtained by composing \tilde{z} with the projection $\mathcal{J}^q \rightarrow \mathcal{J}^q/\mathcal{J}^q$, is well defined and has the desired property. Therefore the class $[\tilde{\eta}]_{\mathcal{J}^q}$ is zero, and the only thing that contributes to the class (4-1) is the q -th contraction of obs_1 . This ends the proof. \square

By the construction (Theorem 3.9) and the calculation (Theorem 4.1), we immediately get:

Corollary 4.2. *With the notation as in Theorem 4.1, suppose that X'/S is liftable to \tilde{S} . Then for each integer q , the truncation $\tau_{[q-1, q]}F_*\Omega_{X/S}^\bullet$ of length 2 is decomposable in the derived category $D(X', \mathcal{O}_{X'})$.*

Proof. This follows from [Deligne and Illusie 1987, 3.5] (which identifies the obstruction to liftability to the decomposability of $\tau_{\leq 1}F_{X/S,*}\Omega_{X/S}^\bullet$) and Theorems 3.9 and 4.1 (which relate the decomposability of $\tau_{[0, 1]}F_{X/S,*}\Omega_{X/S}^\bullet$ with that of $\tau_{[q-1, q]}F_{X/S,*}\Omega_{X/S}^\bullet$). \square

In particular, we extend the (special) case of Corollary 3.6 applied to the de Rham complex in characteristic $p > 2$, even to the case of $p = 2$.

Corollary 4.3. *Let X be a smooth variety over a perfect field k . Then we have the equality*

$$\delta_{F_{X/k,*}\Omega_{X/k}^\bullet}^q = (\text{id} \otimes \delta_K^1) \circ \eta^q$$

in $\text{Hom}(\Omega_{X'/k}^q, \Omega_{X'/k}^{q-1}[2])$.

Finally, we answer the question of Katz:

Corollary 4.4. *Let S be a scheme of characteristic $p > 0$, $f : X \rightarrow S$ a smooth separated morphism of finite type, and $f' : X' \rightarrow S$ (resp. $F : X \rightarrow X'$) the base change of f by the Frobenius endomorphism of S (resp. the relative Frobenius). Suppose \tilde{S} is a flat \mathbb{Z}/p^2 -scheme whose reduction modulo p yields S . Then the morphism in the conjugate spectral sequence*

$$d_2^{ij} : R^i f'_* \Omega_{X'/S}^j \rightarrow R^{i+2} f'_* \Omega_{X'/S}^{j-1},$$

where one identifies $\mathcal{H}^j(F_* \Omega_{X/S}^\bullet)$ with $\Omega_{X'/S}^j$ via the Cartier isomorphism, can be canonically regarded as the cup product with the additive inverse of the obstruction class (in $H^2(X', T_{X'/S})$) to lifting X'/S over \tilde{S} .

Proof. We first remark that by [Deligne and Illusie 1987, 3.9] it can be directly seen that the obstruction class to lifting does not depend on the choice of a flat \mathbb{Z}/p^2 -lifting \tilde{S} of S . Then the corollary follows from [Deligne and Illusie 1987, 3.5] and Theorems 3.9 and 4.1. □

Appendix: F -split schemes of dimension $p + 1$

Let k be a perfect field of characteristic $p > 0$. As mentioned in the introduction, Drinfeld, Bhatt–Lurie, and Li–Mondal (see [Li and Mondal 2021, Remark 5.7] for context) have obtained the following result.

Theorem A.1 [Drinfeld 2020, § 5.12.1; Bhatt and Lurie 2022, Remark 4.7.18; Li and Mondal 2021, Corollary 5.5]. *Let X be a smooth scheme over a perfect field k of characteristic $p > 0$. Suppose that X is liftable to $W_2(k)$. Then the truncations*

$$\tau_{[q-p+1, q]} F_{X/k, *} \Omega_{X/k}^\bullet$$

are decomposable for all q .

Below, we employ this in order to show Kodaira–Akizuki–Nakano vanishing and Hodge–de Rham degeneration for F -split smooth projective schemes of dimension at most $p + 1$.

Recall [Mehta and Ramanathan 1985] that a k -scheme X is F -split if the morphism $F_X^* : \mathcal{O}_X \rightarrow F_{X, *} \mathcal{O}_X$ is a split injection. Since k is perfect, this is equivalent to the splitting of $F_{X/k}^* : \mathcal{O}_{X'} \rightarrow F_{X/k, *} \mathcal{O}_X$. It is well known that every F -split scheme over k admits a flat lifting to $W_2(k)$ (see [Illusie 1996, § 8.5] for the smooth case or [Langer 2015, § 8, Proposition 4] for the general case).

If X is F -split and if L is a line bundle on X , then tensoring the split injection $\mathcal{O}_X \rightarrow F_{X, *} \mathcal{O}_X$ with L and taking cohomology shows that for all i , $H^i(X, L)$ is a direct summand of $H^i(X, L \otimes F_{X, *} \mathcal{O}_X)$. By the projection formula and the fact that Frobenius is affine this latter summand equals $H^i(X, F_X^* L) = H^i(X, L^p)$, and hence the Frobenius pullback maps

$$F_X^* : H^i(X, L) \rightarrow H^i(X, L^p)$$

are injective. Thus, if $H^i(X, L^m) = 0$ for $m \gg 0$, then already $H^i(X, L) = 0$. Consequently, if X is moreover smooth (or just Gorenstein) and projective, then $H^i(X, L^{-1}) = 0$ for $i < \dim X$ and L ample,

that is, Kodaira vanishing holds on X . Similar reasoning with $L = \mathcal{O}_X$ shows that

$$F_X^* : H^i(X, \mathcal{O}_X) \rightarrow H^i(X, \mathcal{O}_X)$$

is bijective for all $i \geq 0$.

Theorem A.2 (Kodaira–Akizuki–Nakano vanishing). *Let X be a smooth projective scheme over k of dimension $d = p + 1$. If X is F -split, then Kodaira–Akizuki–Nakano vanishing holds for X , i.e., for every ample line bundle L , we have*

$$H^i(X, L^{-1} \otimes \Omega_{X/k}^j) = 0 \quad \text{for } i + j < d = p + 1.$$

Proof. By Serre vanishing, the assertion holds for L^{p^m} for $m \gg 0$. Therefore we may assume that it holds for L^p . Following the proof of [Deligne and Illusie 1987, lemme 2.9], we form the complex $K^\bullet = (L')^{-1} \otimes F_{X/k,*} \Omega_{X/k}^\bullet$, where L' is the pullback of L to X' , and write the two spectral sequences

$${}_I E_1^{ij} = H^j(X', (L')^{-1} \otimes F_{X/k,*} \Omega_{X/k}^i) \Rightarrow H^{i+j}(X', K^\bullet) \tag{A-1}$$

and

$${}_{II} E_2^{ij} = H^i(X', (L')^{-1} \otimes \Omega_{X'/k}^j) \Rightarrow H^{i+j}(X', K^\bullet). \tag{A-2}$$

Now the projection formula gives ${}_I E_1^{ij} = H^j(X, L^{-p} \otimes \Omega_{X/k}^i)$, which vanishes for $i + j \leq p$ by assumption. Consequently the abutment $H^r(X', K^\bullet)$ vanishes for $r \leq p$.

We now investigate the second spectral sequence. Since X is F -split, it lifts to $W_2(k)$. Theorem A.1 implies that the differentials on ${}_{II} E_r^{ij}$ are zero for $r \leq p$. For dimensional reasons, there are no nonzero differentials for $r > p + 1$, and the only two nonzero differentials on ${}_{II} E_{p+1}^{ij}$ are

$$d_{p+1}^{0,p} : H^0(X', (L')^{-1} \otimes \Omega_{X'/k}^p) \rightarrow H^{p+1}(X', (L')^{-1})$$

and

$$d_{p+1}^{0,p+1} : H^0(X', (L')^{-1} \otimes \omega_{X'/k}) \rightarrow H^{p+1}(X', (L')^{-1} \otimes \Omega_{X'/k}^1).$$

We will show that $d_{p+1}^{0,p} = 0$, which will then imply that in (A-2) we have

$${}_{II} E_2^{ij} = {}_{II} E_{p+1}^{ij} = {}_{II} E_\infty^{ij} = 0 \quad \text{for } i + j \leq p.$$

Note that $H^p(X', K^\bullet) = 0$ implies $0 = {}_{II} E_{p+2}^{0,p} = \ker(d_{p+1}^{0,p})$, i.e., $d_{p+1}^{0,p}$ is injective.

By Lemma A.3 below applied to $E = L^{-1}$ and the map $F_{X^-/k} : X^- \rightarrow X$, where $X^- = (F_k)^{-1}(X)$ is the Frobenius *untwist* of X , we have a commutative square:

$$\begin{array}{ccc} H^0(X', (L')^{-1} \otimes \Omega_{X'/k}^p) & \xrightarrow{d_{p+1}^{0,p}(L)} & H^{p+1}(X', (L')^{-1}) \\ \downarrow & & \downarrow F_{X'/k}^* \\ 0 = H^0(X, L^{-p} \otimes \Omega_{X/k}^p) & \xrightarrow{d_{p+1}^{0,p}(F_{X^-/k}^* L^{-1})} & H^{p+1}(X, L^{-p}) \end{array}$$

(In fact the left vertical map is zero.) Here we use the identification $(F_{X^-/k}^*(L^{-1}))' = F_{X/k}^*(L') - 1 = L^{-p}$ and the bottom map is deduced similarly for (the pullback to X^- of) L^p in place of L . The vertical right map is injective because X is F -split and we have a commutative diagram

$$\begin{array}{ccccc}
 & & F_X^* & & \\
 & & \curvearrowright & & \\
 H^{p+1}(X, L^{-1}) & \xrightarrow{\sim} & H^{p+1}(X', (L')^{-1}) & \xrightarrow{F_{X/k}^*} & H^{p+1}(X, L^{-p}) \\
 & W^* & & &
 \end{array}$$

($W : X' \rightarrow X$ being the projection), and the horizontal maps are injective by the previous paragraph. We conclude that $H^0(X', (L')^{-1}) \otimes \Omega_{X'/k}^p = 0$. □

In the proof above, as well as in the proof of Hodge–de Rham degeneration below, we need the following functoriality result.

Lemma A.3. *For a vector bundle E on a smooth k -scheme X , write $K^\bullet(E)$ to denote the complex $E' \otimes F_{X/k,*} \Omega_{X/k}^\bullet$. Let $f : Y \rightarrow X$ be a map of smooth k -schemes. Then f induces a map of complexes $f^* K^\bullet(E) \rightarrow K^\bullet(f^* E)$ and hence a map of spectral sequences*

$$\begin{array}{ccc}
 {}_{II} E_2^{ij}(E) = H^i(X', E' \otimes \Omega_{X'/k}^j) & \Rightarrow & H^{i+j}(X', K^\bullet(E)) \\
 \downarrow & & \downarrow \\
 {}_{II} E_2^{ij}(f^* E) = H^i(Y', (f^* E)' \otimes \Omega_{Y'/k}^j) & \Rightarrow & H^{i+j}(Y', K^\bullet(f^* E))
 \end{array}$$

where the maps $H^i(X', E' \otimes \Omega_{X'/k}^j) \rightarrow H^i(Y', (f^* E)' \otimes \Omega_{Y'/k}^j)$ are induced by the composition

$$H^i(X', E' \otimes \Omega_{X'/k}^j) \rightarrow H^i(Y', (f')^*(E') \otimes (f')^* \Omega_{X'/k}^j) \rightarrow H^i(Y', (f')^*(E') \otimes \Omega_{Y'/k}^j).$$

Proof. This follows from the commutative diagram below:

$$\begin{array}{ccccc}
 Y & \longrightarrow & Y' & \longrightarrow & Y \\
 \downarrow f & & \downarrow f' & & \downarrow f \\
 X & \longrightarrow & X' & \longrightarrow & X \\
 & \searrow & \downarrow & & \downarrow \\
 & & \text{Spec}(k) & \xrightarrow{F_k} & \text{Spec}(k)
 \end{array}$$

Note that $(f')^*(E') \simeq (f^* E)'$. □

Theorem A.4 (Hodge–de Rham degeneration). *Let X be a smooth projective scheme over k of dimension $d = p + 1$. If X is F -split, then the Hodge to de Rham spectral sequence*

$${}_I E_1^{ij} = H^j(X, \Omega_{X/k}^i) \Rightarrow H^{i+j}(X, \Omega_{X/k}^\bullet)$$

degenerates.

Proof. Since X is proper, it is enough to show that the conjugate spectral sequence

$${}_{II}E_2^{ij} = H^i(X', \Omega_{X'/k}^j) \Rightarrow H^{i+j}(X, \Omega_{X/k}^\bullet)$$

degenerates. Since X is F -split, it lifts to $W_2(k)$, and then Theorem A.1 implies that the differentials on the page ${}_{II}E_r^{ij}$ of the conjugate spectral sequence are zero for $r \leq p$.

Since $\dim X = p + 1$, the only possibly nonzero differentials in this spectral sequence are therefore

$$d_{p+1}^{0,p} : H^0(X', \Omega_{X'/k}^p) \rightarrow H^{p+1}(X', \mathcal{O}_{X'})$$

and

$$d_{p+1}^{0,p+1} : H^0(X', \omega_{X'/k}) \rightarrow H^{p+1}(X', \Omega_{X'/k}^1).$$

We will show that $d_{p+1}^{0,p} = 0$. Indeed, functoriality of the above maps with respect to Frobenius (Lemma A.3 with $E = \mathcal{O}_X$ and the relative Frobenius $F_{X^-/k}$) gives a commutative square

$$\begin{array}{ccc} H^0(X', \Omega_{X'/k}^p) & \xrightarrow{d_{p+1}^{0,p}} & H^{p+1}(X', \mathcal{O}_{X'}) \\ F_{X'/k}^* \downarrow & & \downarrow F_{X'/k}^* \\ H^0(X, \Omega_{X/k}^p) & \xrightarrow{d_{p+1}^{0,p} \text{ for } X^-} & H^{p+1}(X, \mathcal{O}_X) \end{array}$$

where $X^- = (F_k^{-1})^* X$ is again the Frobenius untwist of X . Since the Frobenius is zero on Ω^i for $i > 0$, the left vertical map is zero. On the other hand, since X is F -split, the right vertical map is an isomorphism. Therefore the top map $d_{p+1}^{0,p}$ is zero.

Finally, we obtain the vanishing of $d_{p+1}^{0,p+1}$ by comparing dimensions and duality. Indeed, we have

$$\begin{aligned} \dim H^{p+2}(X, \Omega_{X/k}^\bullet) &= \dim H^p(X, \Omega_{X/k}^\bullet) && \text{(Poincaré duality)} \\ &= \sum_{i+j=p} \dim H^i(X', \Omega_{X'/k}^j) && \text{(since } d_{p+1}^{0,p} = 0\text{)} \\ &= \sum_{i+j=p+2} \dim H^i(X', \Omega_{X'/k}^j) && \text{(Serre duality),} \end{aligned}$$

so $d_{p+1}^{0,p+1} = 0$. □

Remark A.5 (see [Li and Mondal 2021, Corollary 5.6] and [Bhatt and Lurie 2022]). In fact, the results of Drinfeld, Bhatt–Lurie, and Li–Mondal yield more than we have stated in Theorem A.1. Namely, for X smooth over k and liftable to $W_2(k)$, there exists a decomposition in the derived category

$$F_{X/k,*} \Omega_{X/k}^\bullet \simeq \bigoplus_{i=0}^{p-1} K_i$$

where $\mathcal{H}^j(K_i) = 0$ unless i and j are congruent modulo p . This implies that in the conjugate spectral sequence, as well as in the second spectral sequence used in the proof of Theorem A.2, nonzero differentials may appear only on pages E_r where r is congruent to one modulo p . We only used this with $r \leq p$, and it would be interesting to obtain new vanishing and degeneration theorems using this stronger fact.

Acknowledgements

Achinger is grateful to Luc Illusie, Shizhang Li, Arthur Ogus, and Vadim Vologodsky for useful comments and stimulating discussions. Suh thanks Nicholas Katz for raising the question that we answer in Theorem 1.3, and Pierre Deligne and Luc Illusie for helpful comments. Both authors thank the referees for helpful comments and suggestions.

Achinger was supported by NCN SONATA grant number UM0-2017/26/D/ST1/00913.

References

- [Achinger and Ogus 2020] P. Achinger and A. Ogus, “Monodromy and log geometry”, *Tunis. J. Math.* **2**:3 (2020), 455–534. MR Zbl
- [Bhatt and Lurie 2022] B. Bhatt and J. Lurie, “Absolute prismatic cohomology”, preprint, 2022. arXiv 2201.06120
- [Deligne and Illusie 1987] P. Deligne and L. Illusie, “Relèvements modulo p^2 et décomposition du complexe de de Rham”, *Invent. Math.* **89**:2 (1987), 247–270. MR Zbl
- [Drinfeld 2020] V. Drinfeld, “Prismatization”, preprint, 2020. arXiv 2005.04746
- [Illusie 1971] L. Illusie, *Complexe cotangent et déformations, I*, Lecture Notes in Mathematics **239**, Springer, 1971. MR Zbl
- [Illusie 1972] L. Illusie, *Complexe cotangent et déformations, II*, Lecture Notes in Mathematics **283**, Springer, 1972. MR Zbl
- [Illusie 1996] L. Illusie, “Frobenius et dégénérescence de Hodge”, pp. 113–168 in *Introduction à la théorie de Hodge*, Panor. Synthèses **3**, Soc. Math. France, Paris, 1996. MR Zbl
- [Kato 1989] K. Kato, “Logarithmic structures of Fontaine–Illusie”, pp. 191–224 in *Algebraic analysis, geometry, and number theory* (Baltimore, MD, 1988), edited by J.-I. Igusa, Johns Hopkins Univ. Press, Baltimore, MD, 1989. MR Zbl
- [Kato and Saito 2004] K. Kato and T. Saito, “On the conductor formula of Bloch”, *Publ. Math. Inst. Hautes Études Sci.* **100** (2004), 5–151. MR Zbl
- [Katz 1970] N. M. Katz, “Nilpotent connections and the monodromy theorem: applications of a result of Turrittin”, *Inst. Hautes Études Sci. Publ. Math.* **39** (1970), 175–232. MR Zbl
- [Kříž and May 1995] I. Kříž and J. P. May, *Operads, algebras, modules and motives*, Astérisque **233**, 1995. MR Zbl
- [Langer 2015] A. Langer, “Bogomolov’s inequality for Higgs sheaves in positive characteristic”, *Invent. Math.* **199**:3 (2015), 889–920. MR Zbl
- [Li and Mondal 2021] S. Li and S. Mondal, “On endomorphisms of the de Rham cohomology functor”, preprint, 2021. To appear in *Geom. Topol.* arXiv 2109.04303
- [Lurie 2009] J. Lurie, *Higher topos theory*, Annals of Mathematics Studies **170**, Princeton Univ. Press, Princeton, NJ, 2009. MR Zbl
- [Mehta and Ramanathan 1985] V. B. Mehta and A. Ramanathan, “Frobenius splitting and cohomology vanishing for Schubert varieties”, *Ann. of Math. (2)* **122**:1 (1985), 27–40. MR Zbl
- [Petrov 2023] A. Petrov, “Non-decomposability of the de Rham complex and non-semisimplicity of the Sen operator”, preprint, 2023. arXiv 2302.11389
- [SGA 4₂ 1972] M. Artin, A. Grothendieck, and J. L. Verdier, *Théorie des topos et cohomologie étale des schémas, Tome 2: Exposés V–VIII* (Séminaire de Géométrie Algébrique du Bois Marie 1963–1964), Lecture Notes in Math. **270**, Springer, 1972. MR Zbl
- [Steenbrink 1995] J. H. M. Steenbrink, “Logarithmic embeddings of varieties with normal crossings and mixed Hodge structures”, *Math. Ann.* **301**:1 (1995), 105–118. MR Zbl

Communicated by Bhargav Bhatt

Received 2021-09-13 Revised 2022-02-10 Accepted 2022-03-25

pachinger@impan.pl

Institute of Mathematics of the Polish Academy of Sciences, Warsaw, Poland

jusuh@ucsc.edu

Mathematics Department, University of California, Santa Cruz, CA, United States

A transference principle for systems of linear equations, and applications to almost twin primes

Pierre-Yves Bienvenu, Xuancheng Shao and Joni Teräväinen

The transference principle of Green and Tao enabled various authors to transfer Szemerédi’s theorem on long arithmetic progressions in dense sets to various sparse sets of integers, mostly sparse sets of primes. In this paper, we provide a transference principle which applies to general affine-linear configurations of finite complexity.

We illustrate the broad applicability of our transference principle with the case of *almost twin primes*, by which we mean either Chen primes or “bounded gap primes”, as well as with the case of primes of the form $x^2 + y^2 + 1$. Thus, we show that in these sets of primes the existence of solutions to finite complexity systems of linear equations is determined by natural local conditions. These applications rely on a recent work of the last two authors on Bombieri–Vinogradov type estimates for nilsequences.

1. Introduction

1A. The problem and its background. Green and Tao [2008] famously proved that the primes contain arbitrarily long arithmetic progressions. Their proof introduced an influential transference principle, stating that if a set of integers is dense inside a *pseudorandom* set, then it contains arbitrarily long arithmetic progressions. This is called a transference principle, since it transfers Szemerédi’s theorem, which states that any dense subset of \mathbb{Z} contains arbitrarily long arithmetic progressions, to a sparse setting. In fact, the proof of Green and Tao relied on Szemerédi’s theorem as a black box.

More generally, given any admissible¹ affine-linear map $\Psi : \mathbb{Z}^d \rightarrow \mathbb{Z}^t$, and a subset \mathcal{P} of the primes, one may ask whether \mathcal{P}^t contains a tuple of the form $\Psi(\mathbf{n})$ with $\mathbf{n} \in \mathbb{Z}^d$. Since the image of an affine-linear map may always be realized as the kernel of another affine-linear map and vice versa, this may be formulated as the problem of determining which linear systems of equations can be solved inside \mathcal{P} .

Since the Green–Tao theorem, a lot of research has been devoted to this question. Note that k -term arithmetic progressions correspond to the map $\Psi(n, d) = (n, n + d, \dots, n + (k - 1)d)$, so this case is handled by the Green–Tao theorem, which actually holds for dense subsets of the primes (or even not too sparse subsets, see [Rimanić and Wolf 2019]). Further, since Szemerédi’s theorem holds for any given translation-invariant linear configuration in place of arithmetic progressions (that is, for homogeneous linear maps Ψ such that $(1, \dots, 1) \in \Psi(\mathbb{Z}^d)$), the Green–Tao theorem also holds for these linear configurations.

MSC2020: 11B30.

Keywords: Szemerédi’s theorem, higher order Fourier analysis.

¹ We say that $\Psi = (\psi_1, \dots, \psi_t)$ is *admissible* if $(\psi_i(\mathbf{n}))_{\mathbf{n} \in \mathbb{Z}^d}$ has no fixed prime divisor for each $i \in [t]$.

Regarding general linear configurations, under the mere assumption that $\Psi = (\psi_1, \dots, \psi_t)$ has finite complexity, (that is, no two of the forms ψ_i are affinely related), Green and Tao [2010b] provided a complete answer in the case where \mathcal{P} is the full set \mathbb{P} of primes, in fact giving an asymptotic formula for the number of $\mathbf{n} \in [N]^d$ for which $\Psi(\mathbf{n}) \in \mathcal{P}^t$ as $N \rightarrow \infty$.

Regarding subsets of the primes, it is known that a number of interesting sparse subsets of the primes contain arbitrarily long arithmetic progressions (or again, any given translation-invariant linear configuration). Indeed, the *Chen primes*

$$\mathcal{P}_{\text{Chen}} := \{p \in \mathbb{P} : p + 2 \in P_2\},$$

where P_2 is the set of integers which have at most two prime factors (counted with multiplicity), have this property by [Zhou 2009], and the *bounded gap primes*

$$\mathcal{P}_{\text{bdd}, H} := \{n \in \mathbb{P} : |[n, n + H] \cap \mathbb{P}| \geq 2\}$$

for large H have this property by [Pintz 2010; 2017]. Primes of the form $x^2 + y^2 + 1$ by [Sun and Pan 2019] have this property as well and for any k , there exists $c_k > 1$ such that for any $c \in [1, c_k)$ the set $\mathbb{P} \cap \{[n^c] : n \in \mathbb{N}\}$ of Piatetski-Shapiro primes contains progressions of length k by [Li and Pan 2019].

However, very little is known when Ψ is not translation-invariant and simultaneously \mathcal{P} is not the full set of the primes. When $\mathcal{P} \subset \mathbb{P}$ is the (dense) set of the shifted squarefree primes (i.e., primes p such that $p - 1$ is squarefree), for any finite complexity Ψ , an asymptotic for the number of $\mathbf{n} \in [N]^d$ for which $\Psi(\mathbf{n}) \in \mathcal{P}$ was proven by the first author [Bienvenu 2017]. When it comes to non-translation-invariant configurations in subsets of the primes, previous research has concentrated on the ternary Goldbach system, that is, the affine-linear map $\Psi_N(n, m) = (n, m, N - n - m)$. The subsets of the primes where it was studied include subsets of relative density above a certain threshold [Li and Pan 2010; Shao 2014], the set of primes of the form $x^2 + y^2 + 1$ [Teräväinen 2018], the set of primes in a given Chebotarev class [Kane 2013], the set of Fouvry–Iwaniec primes $x^2 + p^2$ with p prime [Grimmelt 2022], and the set of primes admitting a given primitive root [Frei et al. 2021]. More relevantly for the present study, Matomäki and the second author [Matomäki and Shao 2017] showed that any sufficiently large odd integer (resp. integer congruent to three modulo six) is a sum of three bounded gap primes (resp. three Chen primes). Both of these types of primes have properties akin to those of twin primes, and are therefore referred to as *almost twin primes*.

We mention that all of the papers [Matomäki and Shao 2017; Teräväinen 2018; Grimmelt 2022; Kane 2013; Frei et al. 2021; Shao 2014] rely on classical Fourier analysis, which is considerably simpler than higher order Fourier analysis, and hence the proofs do not adapt to any systems Ψ of complexity at least 2. The papers [Zhou 2009; Pintz 2010; 2017; Sun and Pan 2019; Li and Pan 2019], in turn, all use the Green–Tao transference principle, and hence the proofs do not adapt to any non-translation-invariant configurations Ψ . Our main result handles the case of arbitrary finite complexity systems Ψ when \mathcal{P} is the set of almost twin primes.

1B. Results on linear equations. Now we state our results on linear equations in almost twin primes precisely. Let $\mathcal{H} = \{h_1, \dots, h_m\}$ be an admissible m -tuple: for every prime p , there exists $n \in \mathbb{N}$ such that $\prod_{i \in [m]} (n + h_i) \not\equiv 0 \pmod{p}$. Let $\mathcal{P}_{\mathcal{H}} := \{n \in \mathbb{N} : |(n + \mathcal{H}) \cap \mathbb{P}| \geq 2\}$. Note that $\mathcal{P}_{\mathcal{H}}$ is actually not a subset of the primes; in fact $\mathcal{P}_{\text{bdd}, H} = \mathbb{P} \cap \bigcup_{\mathcal{H} \subset [0, H]} \mathcal{P}_{\mathcal{H}}$. Define the weighted indicator functions of the Chen primes and $\mathcal{P}_{\mathcal{H}}$ by

$$\theta_1(n) := (\log n)^2 1_{\mathcal{P}_{\text{Chen}}}(n) 1_{p|n(n+2) \Rightarrow p \geq n^{1/10}}, \quad \theta_2(n) := (\log n)^m 1_{\mathcal{P}_{\mathcal{H}}}(n) 1_{p|\prod_{i=1}^m (n+h_i) \Rightarrow p \geq n^\rho},$$

where $m = |\mathcal{H}| \geq 2$ and $\rho \in (0, 1)$.

Then we know by Chen’s theorem [1973] and Maynard’s theorem [2016], upon assuming that m is large enough and ρ is small enough, that $\sum_{n \leq N} \theta_i(n) \gg N$ for $i \in \{1, 2\}$ (and we have upper bounds of the same order of magnitude by Selberg’s sieve). Throughout this paper, we fix such m, ρ , and we also fix an admissible m -tuple \mathcal{H} in the definition of θ_2 .

Theorem 1.1 (arbitrary linear configurations weighted by almost twin primes). *Let $i \in \{1, 2\}$. Let $\eta > 0$, $N, d, t, L \geq 1$, and let $\Psi = (\psi_1, \dots, \psi_t) : \mathbb{Z}^d \rightarrow \mathbb{Z}^t$ be a system of affine-linear forms of finite complexity whose homogeneous parts have coefficients bounded in modulus by L .*

Then there exists a constant $C_i(\Psi) \geq 0$ such that the following holds. Let $K \subset [-N, N]^d$ be a convex body satisfying $\text{Vol}(K) \geq \eta N^d$ and $\Psi(K) \subset [1, N]^t$. Then, for $N \geq N_0(L, \eta, d, t)$, we have

$$\sum_{\mathbf{n} \in K \cap \mathbb{Z}^d} \prod_{j \in [t]} \theta_i(\psi_j(\mathbf{n})) \gg_{L, \eta, d, t} C_i(\Psi) \text{Vol}(K). \tag{1-1}$$

Further $C_i(\Psi) > 0$ unless there is an obstruction modulo some prime p . More precisely, $C_1(\Psi) > 0$ as soon as for every prime p there exists $\mathbf{n} \in \mathbb{Z}^d$ such that $\prod_{i \in [t]} \psi_i(\mathbf{n})(\psi_i(\mathbf{n}) + 2) \not\equiv 0 \pmod{p}$ and $C_2(\Psi) > 0$ as soon as for every prime p there exists $\mathbf{n} \in \mathbb{Z}^d$ such that $\prod_{i \in [t]} \prod_{j \in [m]} (\psi_i(\mathbf{n}) + h_j) \not\equiv 0 \pmod{p}$.

Note that the hypotheses imply that the nonhomogeneous coefficients of Ψ are bounded in modulus by $(dL + 1)N$. It turns out that $C_i(\Psi) \gg_{d, t, L, i} 1$ whenever $C_i(\Psi) > 0$; therefore the right-hand side of the estimate (1-1) is $\gg_{d, t, L, i} \text{Vol}(K)$ whenever it is not 0.

We can also obtain an analogous result for primes of the form $x^2 + y^2 + 1$. Let

$$\theta_3(n) := (\log(2n))^{3/2} 1_{\mathbb{P}}(n) 1_{n=x^2+y^2+1, x, y \in \mathbb{Z}} \tag{1-2}$$

be the weighted indicator function of primes of the form $x^2 + y^2 + 1$. By a result of Iwaniec [1972], we have $\sum_{n \leq N} \theta_3(n) \gg N$ (and we have an upper bound of the same order of magnitude from Selberg’s sieve).

Theorem 1.2 (arbitrary linear configurations weighted by primes of the form $x^2 + y^2 + 1$). *Theorem 1.1 continues to hold with θ_3 in place of θ_i . Moreover, $C_3(\Psi) > 0$ as soon as for every prime p there exists $\mathbf{n} \in \mathbb{Z}^d$ such that $\prod_{i \in [t]} \psi_i(\mathbf{n})(\psi_i(\mathbf{n}) + a(p)) \not\equiv 0 \pmod{p}$, where $a(p) = -1$ if $p \equiv -1 \pmod{4}$ and $a(p) = 0$ otherwise.*

Theorem 1.1 has an immediate corollary to linear systems of equations within the Chen or bounded gap primes.

Corollary 1.3 (linear equations in almost twin primes). *Let $L_1, \dots, L_t : \mathbb{Z}^d \rightarrow \mathbb{Z}$ be linear forms. Consider the linear system of equations*

$$L_i(\mathbf{n}) = 0 \quad \text{for all } i \in 1, \dots, t. \quad (1-3)$$

Suppose that the system has a solution in the positive real numbers. Then

- (i) *The system (1-3) has a solution in $\mathcal{P}_{\text{Chen}}^d$, provided that it has a solution in A_p^d for every prime p , where $A_p = \{x \in \mathbb{Z}/p\mathbb{Z} : x(x+2) \not\equiv 0 \pmod{p}\}$.*
- (ii) *The system (1-3) has a solution in $\mathcal{P}_{\mathcal{H}}^d$, provided that $0 \in \mathcal{H}$ and it has a solution in B_p^d for every prime p , where $B_p = \{x \in \mathbb{Z}/p\mathbb{Z} : \prod_{j \in [m]} (x + h_j) \not\equiv 0 \pmod{p}\}$.*

Proof. We may assume that each L_i is primitive (i.e., its coefficients have no common prime factor) and that the linear forms are linearly independent (so $t \leq d$ and the system has full rank t). Since our system is homogeneous, we may assume that the span of the linear forms L_i does not contain a linear form which has exactly two or one nonzero coefficients; indeed, otherwise there exists $(i, j) \in [d]^2$ and coefficients $(a_i, a_j) \in \mathbb{Z}^2 \setminus \{0, 0\}$ such that $i \neq j$ and for any solution $(n_1, \dots, n_d) \in \mathbb{Z}^d$ of the system we have $a_i n_i - a_j n_j = 0$. If $a_i a_j = 0$ then $n_i n_j = 0$ and so the system has no solution in A_p^d nor in B_p^d (because $0 \in \mathcal{H}$). So we may assume that both a_i and a_j are nonzero and coprime. But then either $a_i = a_j = 1$ and we may eliminate a variable to obtain an equivalent system with fewer variables, or there is a prime p dividing a_i but not a_j (or vice versa). We infer $n_i n_j \equiv 0 \pmod{p}$, so the system has no solution in A_p^d nor in B_p^d .

Therefore, the lattice of integer solutions of the system has a multiplicity-free parametrization of the form $\Psi(\mathbb{Z}^{d-t})$, where $\Psi : \mathbb{Z}^{d-t} \rightarrow \mathbb{Z}^d$ is a system of linear forms. The system Ψ has finite complexity, since no two forms of Ψ are linearly dependent, owing to the assumption about the span of the L_i not containing linear forms with exactly one or two nonzero coefficients.

Further, the local conditions (i) and (ii) imply that $C_1(\Psi) > 0$ and $C_2(\Psi) > 0$, respectively. We can then apply Theorem 1.1 to the convex body $K = \{\mathbf{x} \in \mathbb{R}^{d-t} : \Psi(\mathbf{x}) \in [1, N]^d\}$ with $N \rightarrow \infty$, which satisfies $\text{Vol}(K) \gg N^{d-t}$ since the original system of equations has a solution in the positive real numbers, to conclude the proof. \square

As we will see, our method works more generally for $\mathcal{P}_{\mathcal{H},k} := \{n \in \mathbb{N} : |(n + \mathcal{H}) \cap \mathbb{P}| \geq k\}$ instead of $\mathcal{P}_{\mathcal{H}}$ whenever the admissible tuple \mathcal{H} is sufficiently large in terms of k .

1C. Transference principles. Given a finite complexity affine-linear map $\Psi : \mathbb{Z}^d \rightarrow \mathbb{Z}^t$ (often referred to as a system of finite complexity), a function $f : [N] \rightarrow \mathbb{R}_{\geq 0}$ (typically a weighted indicator function of a set of arithmetic interest) and a convex body $K \subset \mathbb{R}^d$, the Ψ -count of f in K is given by

$$T_{\Psi}(f, K) := \sum_{\mathbf{n} \in K \cap \mathbb{Z}^d} \prod_{i \in [t]} f(\psi_i(\mathbf{n})).$$

Thus Theorem 1.1 is about lower-bounding $T_\Psi(\theta_i, K)$ for $i \in \{1, 2\}$. Assume that

$$\sum_{n \in [N]} f(n) \geq \delta N$$

for some $\delta > 0$ and infinitely many integers N . If f takes its values in $[0, 1]$ and if additionally Ψ is a homogeneous translation-invariant linear system, a functional version of Szemerédi’s theorem (see [Tao and Vu 2010, Theorem 11.1]) allows one to prove that $T_\Psi(f, K) \gg_\delta \text{Vol}(K)$. Now, if f is instead unbounded (for example, the von Mangoldt function), the Green–Tao transference principle consists in approximating f (assuming that $f \leq \nu$ for some “pseudorandom measure” ν), by a bounded function $\tilde{f} : [N] \rightarrow [0, 1]$ (called a dense model of f) in such a way that $T_\Psi(f, K) \approx T_\Psi(\tilde{f}, K)$, and invoking Szemerédi’s theorem.

In our case, however, as we are interested in non-translation-invariant systems, we will need a different dense model and hence a different transference principle. To see the need for a different transference principle, consider the set $A = \{n \in \mathbb{N} : \{\sqrt{2}n^2\} \in [\frac{1}{3}, \frac{1}{3} + \frac{1}{100}]\}$ where $\{\cdot\}$ denotes the fractional part of a real number; any translation-invariant configuration can be found inside this set since it is dense by Weyl’s criterion, but note that the configuration $(x, x + y, x + 2y, y)$ does not occur in A due to the relationship $(x + 2y)^2 - 2(x + y)^2 + x^2 - 2y^2 = 0$.

In the case of the ternary Goldbach system $\Psi = \Psi_N : (n, m) \mapsto (n, m, N - n - m)$, the Matomäki–Shao transference principle [2017] provides, under a Fourier-type condition, an approximating function \tilde{f} to f satisfying again $T_\Psi(f, K) \approx T_\Psi(\tilde{f}, K)$, which is lower bounded pointwise: $\tilde{f}(n) \gg_\delta 1$; however, this does not generalize to the higher complexity case, as the set A above (which is Fourier uniform) demonstrates.

The proof of our main theorem produces more generally a lower bounded dense model for any system of finite complexity. This results in a transference principle (Theorem 3.2) of independent interest, which allows us to lower bound $T_\Psi(f, K)$ as desired for any function f which is bounded by a pseudorandom measure and dense in every “higher order Bohr set” (to be defined precisely later). We then check these two conditions for our weighted indicator functions of almost twin primes, i.e., functions θ_1 and θ_2 . This will follow by working out a reduction to the case of equidistributed higher order Bohr sets (Section 5) and then adapting a Bombieri–Vinogradov theorem for primes twisted by nilsequences [Shao and Teräväinen 2021], proven by the last two authors. We also note that our transference principle is slightly stronger than the Green–Tao transference principle even for translation-invariant systems in the sense that our pseudorandomness requirement is weaker (we do not need the correlation condition from [Green and Tao 2008]); we achieve this relaxation by applying work of Dodos and Kanellopoulos [2022].

2. Notation and preliminary definitions

Throughout the paper, we will use bold face characters to denote vectors or tuples. The set of nonnegative reals is denoted by $\mathbb{R}_{\geq 0}$. The expectation notation $\mathbb{E}_{x \in X}$ shall mean, for a finite set X , the averaging operator $\frac{1}{|X|} \sum_{x \in X}$. Further we will use the Vinogradov notation $f \ll g$ or $g \gg f$ whenever two functions f and g from \mathbb{N} to \mathbb{R} satisfy $|f| \leq Cg$ for some constant $C > 0$; the parameters on which the implied

constant C depends may be indicated as subscripts. The conjunction $f \ll g$ and $g \ll f$ will be denoted by $f \asymp g$. For any assertion A , the number 1_A is 1 if A is true and 0 if it is false. The indicator function of a set X will also be denoted by 1_X , which should generate no ambiguity. As usual, we denote by Λ , φ , d_k the von Mangoldt, Euler, and k -fold divisor functions, respectively. The greatest common divisor of two integers n and m will be denoted by (n, m) . A vector or tuple of numbers will usually be denoted in bold font and its components in regular font. Given an integer N , we denote the interval of integers $\{1, \dots, N\}$ by $[N]$. We will often identify the sets $[N]$ and $\mathbb{Z}/N\mathbb{Z}$, which we always implicitly do in the natural way (reduction modulo N). Thus a function f defined on $[N]$ may naturally be seen as a function on $\mathbb{Z}/N\mathbb{Z}$ and vice versa. When x is a positive real number, we define $[x] = [N]$ where $N = \lfloor x \rfloor$ is the integral part of x .

2A. Systems of linear forms. Let $\Psi = (\psi_1, \dots, \psi_t) : \mathbb{Z}^d \rightarrow \mathbb{Z}^t$ be a system of affine-linear forms. We first define a quantity that captures the local behavior of Ψ modulo a prime p .

Definition 2.1 (local factors). For each prime p , define the p -adic local factor of Ψ as

$$\beta_p(\Psi) := \mathbb{E}_{\mathbf{a} \in (\mathbb{Z}/p\mathbb{Z})^d} \prod_{i \in [t]} \frac{p}{\varphi(p)} 1_{\psi_i(\mathbf{a}) \not\equiv 0 \pmod{p}}.$$

Observe that Ψ is admissible as defined in footnote 1 if and only if $\beta_p(\Psi) \neq 0$ for each p .

We need to control the asymptotic behavior of β_p as p approaches infinity, whence the following easy variant of [Green and Tao 2010b, Lemma 1.3].

Lemma 2.2. *Let $\Psi = (\psi_1, \dots, \psi_t) : \mathbb{Z}^d \rightarrow \mathbb{Z}^t$ be an admissible system of affine-linear forms, and let p be a prime. Suppose that there are t_p linear forms among ψ_1, \dots, ψ_t modulo p such that no two of them are linearly dependent over \mathbb{F}_p , and that t_p is maximal for this property. Then*

$$\beta_p(\Psi) = \left(\frac{p}{\varphi(p)} \right)^{t-t_p} (1 + O_{d,t}(p^{-2})).$$

Proof. Without loss of generality, assume that no two of $\psi_1, \dots, \psi_{t_p}$ are proportional modulo p , and let $\Psi_p = (\psi_1, \dots, \psi_{t_p})$. By maximality of t_p , $\beta_p(\Psi) = (p/\varphi(p))^{t-t_p} \beta_p(\Psi_p)$. Since no two of ψ_i, ψ_j with $1 \leq i < j \leq t_p$ can be linearly dependent modulo p , one can follow the proof of [Green and Tao 2010b, Lemma 1.3] to conclude that $\beta_p(\Psi_p) = 1 + O_{d,t}(p^{-2})$. \square

The next crucial condition on linear systems that we will require is the aforementioned *finite complexity* condition, which we now quantify. For an affine-linear form ψ , let $\dot{\psi}$ be its linear part.

Definition 2.3 (complexity of a system). For $A \subset [t]$, let V_A be the set of linear forms on \mathbb{Z}^d generated by $\{\dot{\psi}_i \mid i \in A\}$. Let $i \in [t]$. A system Ψ of linear forms is said to be of *complexity at most k at i* if there exists a partition of $[t] \setminus \{i\}$ into at most $k+1$ parts such that $\dot{\psi}_i \notin V_A$ for each part A of the partition. It is said to be of *complexity at most k* if it is of complexity at most k at any $i \in [t]$. The complexity is the minimum k such that the complexity is at most k , if there is any such $k \in \mathbb{N}$, in which case $k \leq t-2$. Otherwise, it is said to be infinite.

A convenient parametrization of a system of finite complexity is the normal form (see [Green and Tao 2010b, Definition 4.2]), which we now define; it facilitates multiple applications of the Cauchy–Schwarz inequality, yielding the generalized von Neumann theorem [Green and Tao 2010b, Proposition 7.1] which we will use later. Let $\mathbf{e}_1, \dots, \mathbf{e}_d$ be the canonical basis of \mathbb{Z}^d .

Definition 2.4 (normal form of a system). The system Ψ is in *s-normal form at $i \in [t]$* if there exists a set $J_i \subset [t] \setminus \{i\}$ of cardinality at most $s + 1$ such that $\prod_{j \in J_i} \psi_i(\mathbf{e}_j) \neq 0$ whereas for all $k \in [t] \setminus \{i\}$, we have $\prod_{j \in J_i} \psi_k(\mathbf{e}_j) = 0$. The system Ψ is in *s-normal form* if it is in *s-normal form at each $i \in [t]$* .

One may assume that $s \leq t - 2$. Clearly, a system in *s-normal form* has complexity at most s . Due to a simple linear-algebraic argument from [Green and Tao 2010b, Theorem 4.5], we may assume in Theorems 1.1 and 1.2 that the system Ψ is in *s-normal form* for some $s \leq t - 2$. We summarize this reduction in the following proposition.

Proposition 2.5. *Let $\Psi : \mathbb{Z}^d \rightarrow \mathbb{Z}^t$ be a system of complexity s and $K \subset [-N, N]^d$ be a convex body such that $\Psi(K) \in [1, N]^t$. Suppose that the homogeneous coefficients of Ψ are bounded by L . Then there exist an integer $d' = O_{d,t}(1)$, an integer $N' = O(N)$, a real number $L' = O(L^{O(1)})$, a convex body $K' \subset [-N', N']^{d'}$ and a system $\Psi' : \mathbb{Z}^{d'} \rightarrow \mathbb{Z}^t$ of affine-linear forms in *s-normal form* such that for any t functions $g_1, \dots, g_t : \mathbb{Z} \rightarrow \mathbb{R}$, we have*

$$\frac{1}{\text{Vol}(K)} \sum_{\mathbf{n} \in \mathbb{Z}^d \cap K} \prod_{i \in [t]} g_i(\psi_i(\mathbf{n})) = \frac{1}{\text{Vol}(K')} \sum_{\mathbf{n} \in \mathbb{Z}^{d'} \cap K'} \prod_{i \in [t]} g_i(\psi'_i(\mathbf{n})).$$

Further, we have $\text{Vol}(K')/N'^d \gg \text{Vol}(K)/N^d$.

In this form, this proposition is essentially [Bienvenu 2018, Proposition 2.5].

2B. Gowers norms.

Definition 2.6 (Gowers norms over abelian groups). Let Z be a finite abelian group. Let $g : Z \rightarrow \mathbb{C}$ be a function and $k \geq 1$ an integer. The *Gowers U^k norm* of g is the expression

$$\|g\|_{U^k(Z)} := \left(\mathbb{E}_{x \in Z} \mathbb{E}_{\mathbf{h} \in Z^k} \prod_{\boldsymbol{\omega} \in \{0,1\}^k} \mathcal{C}^{|\boldsymbol{\omega}|} g(x + \boldsymbol{\omega} \cdot \mathbf{h}) \right)^{2^{-k}},$$

where \mathcal{C} is the conjugation operator and $|\boldsymbol{\omega}| := \sum_{i \in [k]} \omega_i$.

For $k \geq 2$, this does define a norm, whereas $\|f\|_{U^1(Z)} = |\mathbb{E}_{x \in Z} f(x)|$. For every $k \geq 1$, we have $\|g\|_{U^k(Z)} \leq \|g\|_{U^{k+1}(Z)}$.

Definition 2.7 (Gowers norms over intervals). Given a function $f : \mathbb{Z} \rightarrow \mathbb{C}$ and an integer N , we define its Gowers norm $\|f\|_{U^k[N]}$ over the interval $[N]$ as

$$\|f\|_{U^k[N]} := \frac{\|f \cdot 1_{[N]}\|_{U^k(\mathbb{Z}/N'\mathbb{Z})}}{\|1_{[N]}\|_{U^k(\mathbb{Z}/N'\mathbb{Z})}},$$

where $N' > 2N$ (say $N' = 2N + 1$ for concreteness) and $f \cdot 1_{[N]}$ and $1_{[N]}$ are extended to $\mathbb{Z}/N'\mathbb{Z}$ in the natural way. By [Frantzikinakis and Host 2017, Lemma A.2], this definition is independent of the choice of N' .

Observe that if N and N' are two integers satisfying $\alpha N' \leq N \leq N'$ for some $\alpha > 0$ and a function $f : [N] \rightarrow \mathbb{C}$ is extended to $\mathbb{Z}/N'\mathbb{Z}$ by setting $f(n) = 0$ for $n \in \mathbb{Z}/N'\mathbb{Z} \setminus [N]$, then $\|f\|_{U^s[N]} \asymp_{\alpha,s} \|f\|_{U^s(\mathbb{Z}/N'\mathbb{Z})}$ (see [Green and Tao 2010b, Lemma B.5]). Another norm that we will need is the L^p norm on $[N]$ equipped with the uniform probability measure, thus

$$\|f\|_{L^p[N]} := (\mathbb{E}_{x \in [N]} |f(x)|^p)^{1/p},$$

for $p \geq 1$ a real number. Finally, we define the dual Gowers norm over an interval by

$$\|f\|_{U^k[N]^*} := \sup_{\|g\|_{U^k[N]}=1} |\mathbb{E}_{x \in [N]} f(x)g(x)|.$$

2C. Nilsequences.

Definition 2.8 (nilsequences). Let G be a connected, simply connected nilpotent Lie group, and let $\Gamma \leq G$ be a lattice. A *filtration* $G_\bullet = (G_i)_{i=0}^\infty$ on G is an infinite sequence of subgroups of G (which are also connected, simply connected nilpotent Lie groups) satisfying

$$G = G_0 = G_1 \supset G_2 \supset \dots,$$

and such that the commutators satisfy $[G_i, G_j] \subset G_{i+j}$, and with the additional conditions that $\Gamma_i := \Gamma \cap G_i$ is a lattice in G_i for $i \geq 0$ and $G_{s+1} = \{\text{id}\}$ for some s .

The least such s is called the *degree* of G_\bullet and the manifold G/Γ is called a *nilmanifold*.

A *polynomial sequence* on G (adapted to the filtration G_\bullet) is a sequence $g : \mathbb{Z} \rightarrow G$ satisfying the derivative condition

$$\partial_{h_1} \cdots \partial_{h_k} g(n) \in G_k$$

for all $k \geq 0$, $n \in \mathbb{Z}$ and $h_1, \dots, h_k \in \mathbb{Z}$, where $\partial_h g(n) := g(n+h)g(n)^{-1}$ denotes the discrete derivative with shift h .

Now fix a nilmanifold G/Γ , a filtration G_\bullet of degree s and a polynomial sequence $g : \mathbb{Z} \rightarrow G$. Further, assume that the nilmanifold is equipped with a Malcev basis \mathcal{X} (see [Green and Tao 2012a, Definition 2.1, Definition 2.4]; note that the Malcev basis depends on the fixed filtration, not only on the manifold). A Malcev basis induces a right-invariant metric on G (see [Green and Tao 2012a, Definition 2.2]), which descends to a right-invariant metric on G/Γ and will usually be denoted by $d_{\mathcal{X}}(\cdot, \cdot)$. If $F : G/\Gamma \rightarrow \mathbb{C}$ is Lipschitz with respect to the metric on G/Γ induced by \mathcal{X} , it is bounded by compactness so we let

$$\|F\|_{\text{Lip}(\mathcal{X})} = \|F\|_\infty + \sup_{\substack{x,y \in G/\Gamma \\ x \neq y}} \frac{|F(x) - F(y)|}{d_{\mathcal{X}}(x,y)},$$

and we call a sequence of the form $n \mapsto F(g(n)\Gamma)$ a *nilsequence*. The degree of the nilsequence is then s , and it is said to be of *complexity* at most M if each of the degree s , the dimension of G/Γ , the rationality of \mathcal{X} and the Lipschitz constant of F is at most M .

We now introduce a class of nilsequences of bounded degree and controlled complexity.

Definition 2.9. Let $s \geq 1$ and $\Delta, K \geq 2$. Define $\Xi_s(\Delta, K)$ to be the collection of all nilsequences $\xi : \mathbb{Z} \rightarrow \mathbb{C}$ of the form $\xi(n) = F(g(n)\Gamma)$, where

- (1) G/Γ is a nilmanifold of dimension at most Δ , equipped with a filtration G_\bullet of degree $\leq s$ and a K -rational Malcev basis \mathcal{X} ;
- (2) $g : \mathbb{Z} \rightarrow G$ is a polynomial sequence adapted to G_\bullet ;
- (3) $F : G/\Gamma \rightarrow \mathbb{C}$ is a Lipschitz function satisfying $\|F\|_{\text{Lip}(\mathcal{X})} \leq 1$.

Definition 2.10 (equidistributed nilsequences). For $\eta \in (0, 1)$ and $x \geq 2$, define $\Xi_s(\Delta, K; \eta, x)$ to be the collection of those nilsequences $\xi \in \Xi_s(\Delta, K)$ of the form $\xi(n) = F(g(n)\Gamma)$ that fulfill the additional condition that the sequence $(g(n)\Gamma)_{1 \leq n \leq 10x}$ is totally η -equidistributed in G/Γ (defined in [Green and Tao 2012a, Definition 1.2]).

We will loosely call such nilsequences η -equidistributed. We caution that this notation is slightly different from [Shao and Teräväinen 2021], in that we do not require $\int_{G/\Gamma} F = 0$ (where the integral is taken with respect to the unique Haar measure on G/Γ). We shall use $\Xi_s^0(\Delta, K; \eta, x)$ to denote the set of η -equidistributed nilsequences in $\Xi_s(\Delta, K; \eta, x)$ satisfying the additional condition that $\int_{G/\Gamma} F = 0$.

3. A transference principle for arbitrary systems of linear equations

A fundamental notion related to transference principles is that of *pseudorandom measures*, the basic philosophy being that if a function is bounded by such a measure, it behaves as if it was bounded by 1.

Definition 3.1. A function $\nu : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{R}_{\geq 0}$ is said to satisfy the $(d_0, t_0, L_0, \varepsilon)$ -linear forms conditions if it satisfies the following. Let $1 \leq d \leq d_0$ and $1 \leq t \leq t_0$. For every finite complexity system of affine-linear forms $\Psi = (\psi_1, \dots, \psi_t) : \mathbb{Z}^d \rightarrow \mathbb{Z}^t$ with linear coefficients bounded by L_0 in modulus, the following estimate holds:

$$\left| \mathbb{E}_{\mathbf{n} \in (\mathbb{Z}/N\mathbb{Z})^d} \prod_{i \in [t]} \nu(\psi_i(\mathbf{n})) - 1 \right| \leq \varepsilon. \tag{3-1}$$

If it satisfies the (M, M, M, ε) -linear forms conditions, it is said to be (M, ε) -pseudorandom.

Observe that $\|\nu - 1\|_{U^k(\mathbb{Z}/N\mathbb{Z})} = O(\varepsilon^{1/2^k})$ as soon as ν satisfies the $(k+1, 2^k, 1, \varepsilon)$ -linear forms conditions, and that the constant coefficients of Ψ are unrestricted. Note that our definition is less restrictive than that of Green and Tao [2010b], since we do not require the so-called correlation condition.

The aim of this section is to prove the following theorem.

Theorem 3.2 (transference principle for linear systems). *Let $t, d, L, s \geq 1$ be integers, and let $\delta, \eta > 0$ be real numbers. Then there exist constants $M \geq 1$ depending on d, t, L and $Y, \varepsilon > 0$ depending on d, t, L, δ such that the following holds. Let $\Psi = (\psi_1, \dots, \psi_t) : \mathbb{Z}^d \rightarrow \mathbb{Z}^t$ be a system of affine-linear forms of complexity s whose homogeneous parts have coefficients bounded by L . Let N be a large enough prime and α be small enough (both in terms of t, d, L, η). Let $K \subset [-N, N]^d$ be a convex body satisfying*

$\text{Vol}(K) \geq \eta N^d$ and $\Psi(K) \subset [1, N]^t$. Lastly, for each $i \in [t]$, let $\lambda_i : [N] \rightarrow \mathbb{R}_{\geq 0}$ be a function. Assume that the following additional hypotheses hold.

(i) There exists an (M, α) -pseudorandom measure $\nu : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{R}_{\geq 0}$ such that

$$\lambda_i(n) \leq \nu(n) \quad \text{for each } i \in [t] \text{ and } n \in [N],$$

where we identify $[N]$ and $\mathbb{Z}/N\mathbb{Z}$ in the natural way.

(ii) Each function λ_i is dense in higher order Bohr sets in the sense that

$$\mathbb{E}_{n \in [N]} \lambda_i(n) \xi(n) \geq \delta \mathbb{E}_{n \in [N]} \xi(n)$$

for every nilsequence $\xi : \mathbb{Z} \rightarrow [0, 1]$ of degree $\leq s$ and of complexity at most Y that satisfies $\mathbb{E}_{n \leq N} \xi(n) \geq \varepsilon$.

Then we have

$$\mathbb{E}_{\mathbf{n} \in K \cap \mathbb{Z}^d} \lambda_1(\psi_1(\mathbf{n})) \lambda_2(\psi_2(\mathbf{n})) \cdots \lambda_t(\psi_t(\mathbf{n})) \geq 0.99\delta^t. \quad (3-2)$$

We now present the tools which will enable us to prove this. We need a notion of higher order Bohr sets, which are roughly speaking sets that are approximated by level sets of nilsequences to any given accuracy. The following definitions of s -measurable sets and s -factors are from [Green and Tao 2020, Section 2].

Definition 3.3 (s -measurable sets). Let $s \geq 1$ and let $\Phi : \mathbb{R} \rightarrow \mathbb{R}$ be a growth function. A subset $E \subset [N]$ is called s -measurable with growth function Φ if, for any $M \geq 1$, there exists a degree $\leq s$ nilsequence $\xi : \mathbb{Z} \rightarrow [0, 1]$ of complexity at most $\Phi(M)$ such that $\|1_E - \xi\|_{L^2[N]} \leq 1/M$.

Definition 3.4. If \mathcal{B} is a partition of $[N]$, we call its parts $E \in \mathcal{B}$ atoms. The conditional expectation of a function $f : [N] \rightarrow \mathbb{R}$ with respect to \mathcal{B} is the function $\mathbb{E}[f|\mathcal{B}]$ which is constant on each atom, equal to the average of f on the atom.

Definition 3.5 (s -factors). Let $s \geq 1$ and let $\Phi : \mathbb{R} \rightarrow \mathbb{R}$ be a function. A partition \mathcal{B} of $[N]$ is called an s -factor of complexity at most M and growth function Φ if \mathcal{B} contains at most M atoms and each atom is s -measurable of growth function Φ .

The following two propositions will be important in our proof of Theorem 3.2. The first one is the weak regularity lemma² proved in [Green and Tao 2010a, Corollary 2.6].

Proposition 3.6 (weak regularity lemma). Let $s \geq 1$ and $\varepsilon > 0$. Let $f : [N] \rightarrow \mathbb{R}$ be a function with $|f(n)| \leq 1$ pointwise. There exists a function $\Phi : \mathbb{R} \rightarrow \mathbb{R}$ depending only on s, ε and an s -factor \mathcal{B} of complexity $O_{s,\varepsilon}(1)$ and growth function Φ such that $\|f - \mathbb{E}(f|\mathcal{B})\|_{U^{s+1}(\mathbb{Z}/N\mathbb{Z})} \leq \varepsilon$.

²It was discovered recently that the reference [Green and Tao 2010a] contains a slight error. See the arXiv version [Green and Tao 2020] for details and a correction. Nevertheless, the regularity lemma part of that reference is unaltered, only the counting lemma (and what depends on it) was not entirely correct.

In the just cited the reference, the Gowers norms are interval Gowers norms, but this makes no difference since the $U^{s+1}(\mathbb{Z}/N\mathbb{Z})$ and $U^{s+1}[N]$ norms are equivalent on bounded functions (see [Frantzikinakis and Host 2017, Lemma A.4] for instance). We also state the dense model theorem from the work of Dodos and Kanellopoulos [2022, Corollary 4.4].

Proposition 3.7 (dense model theorem). *Let $s \geq 1$ and let Z be a finite abelian group. Let $0 < \eta \leq 1$. Suppose that $\nu : Z \rightarrow \mathbb{R}_{\geq 0}$ satisfies $\|\nu - 1\|_{U^{2s}(Z)} \leq \eta$, and that $f : Z \rightarrow \mathbb{R}$ is a function such that $|f(n)| \leq \nu(n)$ pointwise. Then we may decompose $f = f_1 + f_2$, where*

$$\sup_{n \in Z} |f_1(n)| \leq 1 \quad \text{and} \quad \|f_2\|_{U^s(Z)} = o_{\eta \rightarrow 0; s}(1).$$

Further, if f is nonnegative, so is f_1 .

We note that this version of the dense model theorem has weaker hypotheses than the one in [Green and Tao 2010b] (it does not require the so-called correlation condition), a fact that will be important for us. A dense model for arithmetic progressions was also achieved without correlation conditions by Conlon, Fox and Zhao [Conlon et al. 2014; 2015], but their dense model is not as strong as we need since it is not close in the Gowers norms topology to the function to be modeled.

Finally, we state a version of the generalized von Neumann theorem [Green and Tao 2010b, Proposition 7.1' in Appendix C].

Proposition 3.8 (generalized von Neumann theorem). *Let t, d, L, s be positive integer parameters. Let δ, ε be in $(0, 1)$ and $N \geq 1$. Then there is a positive constant D , depending on t, d and L such that the following holds. Let $\nu : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{R}_{\geq 0}$ be a (M, ε) -pseudorandom measure, and suppose that $f_1, \dots, f_t : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{R}$ are functions with $|f_i(x)| \leq \nu(x)$ for all $i \in [t]$ and $x \in \mathbb{Z}/N\mathbb{Z}$. Suppose that $\Psi = (\psi_1, \dots, \psi_t)$ is a system of affine-linear forms in s -normal form whose linear coefficients are bounded by L . Let $K' \subset (\mathbb{Z}/N\mathbb{Z})^d$ be identified with $K \cap \mathbb{Z}^d$ where $K \subset [-N/4, N/4]^d$ is a convex set. Finally, suppose that*

$$\min_{1 \leq j \leq t} \|f_j\|_{U^{s+1}[N]} \leq \delta. \tag{3-3}$$

Then we have

$$\mathbb{E}_{\mathbf{n} \in (\mathbb{Z}/N\mathbb{Z})^d} \mathbf{1}_{K'}(\mathbf{n}) \prod_{i \in [t]} f_i(\psi_i(\mathbf{n})) = o_{\delta \rightarrow 0}(1) + o_{N \rightarrow \infty; \delta}(1) + o_{\varepsilon \rightarrow 0; \delta}(1),$$

where the $o(1)$ terms may also depend on d, t, L .

In the cited reference, the parameter ε is itself $o_{N \rightarrow \infty}(1)$ but we make it independent here, whence the slightly different statement.

We are now ready to state and prove a crucial lemma.

Proposition 3.9 (decomposition into a uniformly lower bounded and Gowers uniform components). *Let $s \geq 1$ and let $N \geq 1$ be an integer. Let $\delta, \varepsilon, \rho$ be real constants in the interval $(0, 1)$. Then there exist quantities $\iota \in (0, 1)$, $Y > 0$, $\eta \in (0, 1)$ depending only on $s, \varepsilon, \rho, \delta$ such that the following holds. Suppose*

that $\nu : [N] \rightarrow \mathbb{R}_{\geq 0}$ satisfies $\|\nu - 1\|_{U^{2s+2}(\mathbb{Z}/N\mathbb{Z})} \leq \eta$, where we naturally identify $[N]$ with $\mathbb{Z}/N\mathbb{Z}$. Let $f : [N] \rightarrow \mathbb{R}_{\geq 0}$ be a function such that $f(n) \leq \nu(n)$ pointwise. Further, suppose that

$$\mathbb{E}_{n \in [N]} f(n)\xi(n) \geq \delta \mathbb{E}_{n \in [N]} \xi(n)$$

for every nilsequence $\xi : \mathbb{Z} \rightarrow [0, 1]$ of degree $\leq s$ and of complexity at most Y that satisfies $\mathbb{E}_{n \leq N} \xi(n) \geq \iota N$. Then there exists a decomposition $f = f_3 + f_4$ where $f_3 \geq (1 - \rho)\delta$ pointwise and $\|f_4\|_{U^{s+1}(\mathbb{Z}/N\mathbb{Z})} \leq \varepsilon$.

Proof. Without loss of generality, we may assume that ε is small enough in terms of δ and ρ . Let $\varepsilon' \leq \varepsilon/3$ be a sufficiently small constant, to be determined later. Applying Proposition 3.7, we may write $f = f_1 + f_2$ where f_1 takes its values in $[0, 1]$ and $\|f_2\|_{U^{s+1}(\mathbb{Z}/N\mathbb{Z})} \leq \varepsilon'$. Then using Proposition 3.6 on f_1 , we decompose $f_1 = h + g$ where $h = \mathbb{E}[f_1|\mathcal{B}]$ and \mathcal{B} is an s -factor of complexity $O_{s,\varepsilon}(1)$ and growth function Φ , and $\|g\|_{U^{s+1}(\mathbb{Z}/N\mathbb{Z})} \leq \varepsilon/3$. The growth function Φ of \mathcal{B} depends only on ε and s .

Note that $h = \sum_{E \in \mathcal{B}} c_E 1_E$, where $c_E = \frac{1}{|E|} \sum_{n \in [N]} f_1(n) 1_E(n)$ for any atom E of \mathcal{B} . Fix $c = (\varepsilon/3)^{2^{s+1}}/|\mathcal{B}|$, so $c^{-1} = O_{s,\varepsilon}(1)$. We effect the splitting

$$h = \sum_{E \in \mathcal{B}} (c_E + \delta 1_{|E| < cN}) 1_E - \sum_{\substack{E \in \mathcal{B} \\ |E| < cN}} \delta 1_E.$$

We denote by h_1 the first sum and h_2 the second one.

Since $\delta \in [0, 1]$, we see that $\|h_2\|_{L^1[N]} \leq c|\mathcal{B}| = (\varepsilon/3)^{2^{s+1}}$. Crudely estimating by the triangle inequality, this implies that $\|h_2\|_{U^{s+1}(\mathbb{Z}/N\mathbb{Z})} \leq \varepsilon/3$. Now write $f_3 = h_1$ and $f_4 = g + f_2 + h_2$. By the triangle inequality for Gowers norms, we have

$$\|f_4\|_{U^{s+1}(\mathbb{Z}/N\mathbb{Z})} \leq 3 \cdot \varepsilon/3 = \varepsilon.$$

Our aim is then to show that

$$c_E \geq (1 - \rho)\delta \quad \text{whenever} \quad |E| \geq cN, \tag{3-4}$$

after which $f_3 = h_1 \geq (1 - \rho)\delta$ pointwise follows.

Fix a large enough constant $M > 0$ in terms of c, δ, ρ (explicitly, we may take $M = 4/(c\delta\rho)$) and an atom $E \in \mathcal{B}$ satisfying $|E| \geq cN$. By definition of an s -factor, we may write $1_E = \xi + g_{\text{sml}}$, where $\|g_{\text{sml}}\|_{L^2[N]} \leq 1/M$ and ξ (depending on E) is a nilsequence of degree at most s whose complexity is bounded by $Y := \Phi(M) = O_{s,\varepsilon,\rho,\delta}(1)$. By the Cauchy–Schwarz inequality, we have

$$\left| \sum_{n \in [N]} f_1(n) g_{\text{sml}}(n) \right| \leq N/M.$$

Therefore,

$$c_E \geq \frac{1}{|E|} \sum_{n \in [N]} f_1(n)\xi(n) - 1/(cM).$$

We now recall that $f = f_1 + f_2$, so that (3-4) follows once we show that

$$\sum_{n \in [N]} f(n)\xi(n) \geq \delta|E|(1 - 1/(cM)) \quad \text{and} \quad \left| \sum_{n \in [N]} f_2(n)\xi(n) \right| \leq \rho\delta|E|/2, \tag{3-5}$$

upon setting $M = 4/(c\delta\rho)$. First we bound the correlation of f_2 and ξ . Since f_2 has small U^{s+1} norm, it would be convenient to replace ξ by a function of bounded dual U^{s+1} norm. To achieve this, we invoke³ [Green and Tao 2010b, Proposition 11.2], which yields for any $\kappa > 0$ a splitting $\xi = \xi_1 + \xi_2$, where $\|\xi_1\|_{U^{s+1}(\mathbb{Z}/N\mathbb{Z})^*} \leq K$ for some $K = O_{\kappa,Y}(1)$, while $\|\xi_2\|_\infty \leq \kappa$. We infer that

$$\left| \sum_{n \in [N]} f_2(n)\xi_1(n) \right| \leq \|f_2\|_{U^{s+1}(\mathbb{Z}/N\mathbb{Z})} \|\xi_1\|_{U^{s+1}(\mathbb{Z}/N\mathbb{Z})^*} N \leq \varepsilon' KN. \tag{3-6}$$

Further, since $|f_2| \leq \nu + 1$ pointwise,

$$\left| \sum_{n \in [N]} f_2(n)\xi_2(n) \right| \leq \|\xi_2\|_\infty \sum_{n \in [N]} (\nu(n) + 1) \leq (2 + |\mathbb{E}_{n \in [N]}(\nu(n) - 1)|) \|\xi_2\|_\infty N. \tag{3-7}$$

Recall that $|\mathbb{E}_{n \in [N]}(\nu(n) - 1)| = \|\nu - 1\|_{U^1(\mathbb{Z}/N\mathbb{Z})} \leq \|\nu - 1\|_{U^{2s+2}(\mathbb{Z}/N\mathbb{Z})} \leq \eta < 1$. We conclude that $|\sum_{n \in [N]} f_2(n)\xi_2(n)| \leq 3\kappa N$.

Now, if we choose $\kappa = c\rho\delta/12$ and $\varepsilon' = \rho\delta c/(4K)$ (thus $(\varepsilon')^{-1} = O_{\rho,s,\delta,\varepsilon}(1)$), we have $\varepsilon'K + 3\kappa < c\rho\delta/2$, so by combining (3-6) and (3-7) with the fact that $N \leq c^{-1}|E|$, we obtain the required bound (3-5) for f_2 .

It remains to be shown that the correlation of f and ξ obeys the lower bound in (3-5). By the definition of ξ , we have

$$\sum_{n \in [N]} \xi(n) = |E| - \sum_n g_{\text{sml}}(n) \geq |E|(1 - 1/(cM)) \geq |E|/2 \geq cN/2,$$

so recalling the “denseness in higher order Bohr sets” hypothesis of Proposition 3.9 (letting $\iota = c/2$ there) and the fact that the complexity of ξ is at most Y , the desired estimate (3-5) follows. This was enough to complete the proof. \square

Proof of Theorem 3.2. In view of Proposition 2.5, we may assume that the system Ψ is in s -normal form. Also, upon replacing N by $4N$ (and therefore η by $4^{-d}\eta$), we may assume that $K \subset [-N/4, N/4]$. Fix $\kappa > 0$ small enough (to be determined later). Let ρ be small enough in terms of t (say $\rho = 1/(10000t)$). By hypothesis (i), if N is large enough, we may apply Proposition 3.9, thus obtaining a decomposition $\lambda_i = \lambda_i^{(1)} + \lambda_i^{(2)}$ for each $i \in [t]$ where $\lambda_i^{(1)} \geq (1 - \rho)\delta$ pointwise and $\|\lambda_i^{(2)}\|_{U^{s+1}(\mathbb{Z}/N\mathbb{Z})} \leq \kappa$. Inserting this decomposition in the left-hand side of (3-2), we obtain a splitting of the average into 2^t terms:

$$\mathbb{E}_{\mathbf{n} \in K \cap \mathbb{Z}^d} \prod_{j=1}^t \lambda_j(\psi_j(\mathbf{n})) = \sum_{a_1, a_2, \dots, a_t \in \{1, 2\}} \mathbb{E}_{\mathbf{n} \in K \cap \mathbb{Z}^d} \prod_{j=1}^t \lambda_j^{(a_j)}(\psi_j(\mathbf{n})).$$

One of the 2^t terms involves only the functions $\lambda_i^{(1)}$; since $\lambda_i^{(1)}$ is pointwise lower bounded by $(1 - \rho)\delta$, this term is at least

$$(1 - \rho)^t \delta^t \geq 0.999\delta^t,$$

³In the cited reference, written at a time where the theory of nilsequences was just emerging, the result is stated for linear nilsequences. However, nowadays we know that any polynomial nilsequence may be realized as a linear one, see [Green et al. 2012, Appendix C]. Also the result is stated in terms of interval Gowers norms, but the proof naturally yields $\|\xi_1\|_{U^{s+1}(\mathbb{Z}/N\mathbb{Z})^*} \leq K$ first as it moves from intervals to cyclic groups.

since $\rho = 1/(10000t)$. Any other term involves at least one copy of a uniform function $\lambda_i^{(2)}$. Let $\mathbf{a} \in \{1, 2\}^t \setminus \{(1, \dots, 1)\}$. Since $K \subset [-N/4, N/4]^d$ and $\Psi(K) \subset [1, N]^t$, one may identify K with a subset of $(\mathbb{Z}/N\mathbb{Z})^d$, which we also denote by K , and write

$$\mathbb{E}_{\mathbf{n} \in K \cap \mathbb{Z}^d} \prod_{j=1}^t \lambda_j^{(a_j)}(\psi_j(\mathbf{n})) = \mathbb{E}_{\mathbf{n} \in (\mathbb{Z}/N\mathbb{Z})^d} \mathbf{1}_K(\mathbf{n}) \prod_{j=1}^t \lambda_j^{(a_j)}(\psi_j(\mathbf{n})). \quad (3-8)$$

According to Proposition 3.8 (for which we need M to be sufficiently large in terms of d, t, L and the fact that Ψ is in s -normal form), the right-hand side of (3-8) is bounded by

$$o_{N \rightarrow \infty; \kappa}(1) + o_{\alpha \rightarrow 0; \kappa}(1) + o_{\kappa \rightarrow 0}(1).$$

Therefore, choosing first κ appropriately, and then N sufficiently large and α sufficiently small, we conclude the proof. \square

The rest of the paper is devoted to establishing the hypotheses (i) and (ii) of Theorem 3.2 for the functions θ_1 and θ_2 (and θ_3 in Section 9); we start with hypothesis (i).

4. W -trick and pseudorandom majorants

4A. W -trick. We wish to apply Theorem 3.2 to prove our main theorem, but an initial problem is that the indicator functions of almost twin primes are not bounded by a pseudorandom majorant, as they are biased modulo small primes. We will first have to remove these biases modulo small primes to obtain a pseudorandomly majorized function.

We introduce the general framework we will work with in this section. Let w be an integer and $W = W(w) = \prod_{p \leq w} p$. Let $\rho \in (0, 1)$, $r \geq 1$, and let $\mathcal{H} = \{h_1, \dots, h_r\} \subset \mathbb{N}$ be a set of r pairwise distinct integers and let $\theta = \theta_{\mathcal{H}} : \mathbb{N} \rightarrow \mathbb{R}_{\geq 0}$ be any function supported on the set

$$\{n \in \mathbb{N} : p | n + h_j \implies p > w \text{ for all } j \in [r]\}$$

and satisfying the upper bound

$$\theta(n) \leq \log^r(n+2)$$

for all $n \geq 0$. Observe that the functions θ_1 and θ_2 our main theorem deals with have these properties (with $r = 2$ in the case of θ_1 and $r = m$ in the case of θ_2). Given integers $q > 0$ and b , let

$$\theta_{q,b}(n) := \left(\frac{\varphi(q)}{q} \right)^r \theta(qn + b). \quad (4-1)$$

Proposition 4.1 (reduction to W -tricked sums). *Let the notation be as above. Also let $\eta > 0$, $\gamma > 0$, $N, L, d, t \geq 1$. Let $\Psi = (\psi_1, \dots, \psi_t) : \mathbb{Z}^d \rightarrow \mathbb{Z}^t$ be a finite complexity system of affine-linear forms. Suppose that $\Psi_{\mathcal{H}} := (\psi_i + h_j)_{i \in [t], j \in [r]}$ is admissible and that the linear coefficients of Ψ as well as the elements of \mathcal{H} are bounded by L . Let $K \subset [-N, N]^d$ be a convex body satisfying $\text{Vol}(K) \geq \eta N^d$ and*

$\Psi(K) \subset [1, N]^t$. Suppose that θ satisfies

$$\sum_{\substack{\mathbf{n} \in \mathbb{Z}^d \\ W\mathbf{n} + \mathbf{a} \in K}} \prod_{i=1}^t \theta_{W, c_i(\mathbf{a})}(\psi'_i(\mathbf{n})) \geq \gamma W^{-d} \text{Vol}(K), \quad (4-2)$$

for each $\mathbf{a} \in A$, where

$$A = A_{\Psi, \mathcal{H}} = \{\mathbf{a} \in [W]^d : \forall (i, j) \in [t] \times [r], (\psi_i(\mathbf{a}) + h_j, W) = 1\}$$

and for each $i \in [t]$, the integer $c_i(\mathbf{a}) \in [W]$ and the form $\psi'_i : \mathbb{Z}^d \rightarrow \mathbb{Z}$ are uniquely defined by the relation $\psi_i(W\mathbf{n} + \mathbf{a}) = W\psi'_i(\mathbf{n}) + c_i(\mathbf{a})$. Then, provided that w is large enough in terms of d, t, L , we have

$$\sum_{\mathbf{n} \in K \cap \mathbb{Z}^d} \prod_{i=1}^t \theta(\psi_i(\mathbf{n})) \geq \frac{\gamma}{2} \cdot \prod_p \beta_p \cdot \text{Vol}(K), \quad (4-3)$$

where the local factors $\beta_p = \beta_p(\Psi_{\mathcal{H}})$ are as defined in Definition 2.1.

Proof. We write

$$\mathbb{Z}^d \cap K = \bigcup_{\mathbf{a} \in [W]^d} (\mathbb{Z}^d \cap (W\mathbf{K}_a + \mathbf{a})),$$

where

$$\mathbf{K}_a := \{\mathbf{x} \in \mathbb{R}^d : W\mathbf{x} + \mathbf{a} \in K\}$$

is again a convex body. Putting

$$F(\mathbf{n}) := \prod_{j=1}^t \theta(\psi_j(\mathbf{n}))$$

we can write the left-hand side of (4-3) as

$$\sum_{\mathbf{n} \in \mathbb{Z}^d \cap K} F(\mathbf{n}) = \sum_{\mathbf{a} \in [W]^d} \sum_{\mathbf{n} \in \mathbb{Z}^d \cap \mathbf{K}_a} F(W\mathbf{n} + \mathbf{a}). \quad (4-4)$$

We note that if $\psi_i(\mathbf{a}) + h_j$ is not coprime to p for some $i \in [t]$, some $j \in [r]$ and some prime $p \leq w$, then for each $\mathbf{n} \in \mathbf{K}_a \cap \mathbb{Z}^d$ we have $F(W\mathbf{n} + \mathbf{a}) = 0$: indeed, in that case, the integer $\psi_i(W\mathbf{n} + \mathbf{a}) + h_j$ has a prime factor $p \leq w$, hence does not belong to the support of θ . Thus, the residues \mathbf{a} which bring a nonzero contribution to the right-hand side of (4-4) are all mapped by Ψ to tuples (b_1, \dots, b_t) for which $b_i + h_j$ is coprime to W for all $i \in [t], j \in [r]$.

Recalling the definitions of $A = A_{\Psi, \mathcal{H}}$, the integers $c_i(\mathbf{a})$, the forms ψ'_i and $\theta_{W, b}$, we can then rewrite (4-4) as

$$\sum_{\mathbf{n} \in \mathbb{Z}^d \cap K} F(\mathbf{n}) = \left(\frac{W}{\varphi(W)}\right)^{rt} \sum_{\mathbf{a} \in A} \sum_{\mathbf{n} \in \mathbb{Z}^d \cap \mathbf{K}_a} \prod_{i=1}^t \theta_{W, c_i(\mathbf{a})}(\psi'_i(\mathbf{n})). \quad (4-5)$$

By our assumption (4-2), we have

$$\sum_{\mathbf{n} \in \mathbb{Z}^d \cap \mathbf{K}_a} \prod_{i=1}^t \theta_{W, c_i(\mathbf{a})}(\psi'_i(\mathbf{n})) \geq \gamma W^{-d} \text{Vol}(K) = \gamma \text{Vol}(\mathbf{K}_a) \quad (4-6)$$

for each $\mathbf{a} \in A$, so to obtain the conclusion (4-3) it suffices to prove that

$$\left(\frac{W}{\varphi(W)}\right)^{rt} |A_{\Psi, \mathcal{H}}| \geq \frac{1}{2} W^d \prod_p \beta_p. \tag{4-7}$$

Note that by the Chinese remainder theorem we have

$$\left(\frac{W}{\varphi(W)}\right)^{rt} |A_{\Psi, \mathcal{H}}| = W^d \prod_{p \leq w} \beta_p.$$

Lemma 2.2 implies that $\beta_p = 1 + O_{d,t,L}(p^{-2})$ whenever $|\mathcal{H} \pmod{p}| = r$ (which is the case whenever $w > H$), and $\beta_p > 0$ for any p since $\Psi_{\mathcal{H}}$ is an admissible system. Therefore $\prod_p \beta_p$ is convergent and if $w > H$ we have $\prod_{p \leq w} \beta_p = (1 + O_{d,t,L}(1/w)) \prod_p \beta_p$. Taking w large enough in terms of d, t, L , this concludes the proof of Proposition 4.1. \square

In fact Lemma 2.2 implies that $\beta_p = 1 + O(p^{-1})$ and $\beta_p = 1 + O(p^{-2})$ except when $p \mid \prod_{i,j} (h_i - h_j)$. Combining this with the fact that, for any integer q having z prime factors, we have

$$\prod_{\substack{w < p \\ p \mid q}} (1 + O(p^{-1})) \leq \prod_{w < p < w+z} (1 + O(p^{-1})) = O(\log \log q / \log w).$$

We infer $\prod_{p > w} \beta_p \ll O(\log \log H / \log w)$ so the weaker hypothesis $H \leq \exp(w^{O(1)})$ could suffice instead of $w > H$ at the cost of replacing $\frac{1}{2}$ by a worse constant.

Also we note that the system Ψ' introduced above differs from Ψ only in the constant term, and so it is of finite complexity whenever Ψ is.

4B. Pseudorandom majorants. In order to prove Theorem 1.1, it remains to establish the lower bound (4-2) when θ is either θ_1 or θ_2 , which we will do by invoking Theorem 3.2. In order to appeal to this theorem, we need to supply a pseudorandom majorant for the function $\theta_{W,b}$ where b is coprime to W . The only properties of θ that we need for this construction are that it is supported on the set

$$\{n \in \mathbb{N} : p \mid n + h_j \implies p > n^\rho \text{ for all } j \in [r]\}$$

and satisfies $0 \leq \theta(n) \leq \log^r(n+2)$ (and these are satisfied for θ_1, θ_2 with $r = 2, m$, respectively). Let

$$B_{\mathcal{H}} := \{b \in \mathbb{N} : \forall j \in [r], (b + h_j, W) = 1\}. \tag{4-8}$$

The next proposition provides us with a pseudorandom majorant.

Proposition 4.2 (pseudorandom majorants). *Let $M \geq 1$ and s be integers. Let $\epsilon > 0$. Assume that N and w are large enough in terms of (M, ϵ) and satisfy $w \leq \log \log N$. Let $\mathbf{b} = (b_1, \dots, b_s)$ in $B_{\mathcal{H}}^s$ satisfy $|b_i - b_j| \leq M$ for any $(i, j) \in [s]^2$. Suppose also that θ is as above. Then there is an (M, ϵ) -pseudorandom measure $\nu_{\mathbf{b}} : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{R}_{\geq 0}$ and a constant $c \in (0, 1)$ depending on M only such that*

$$\theta_{W,b_1}(n) + \dots + \theta_{W,b_s}(n) \ll_M \nu_{\mathbf{b}}(n)$$

for all $n \in [N^c, N] \subset \mathbb{Z}/N\mathbb{Z}$.

The fact that the bound does not necessarily hold on the full interval $[N]$ is not a serious restriction, as we may impose θ to be supported in $[N^c, N]$ without changing the left-hand side of (4-2) and (4-3) by more than $O(N^{cd} \log^{O(1)} N) = o(N^d)$. Zhou [2009] and Pintz [2010] already constructed pseudorandom majorants for Chen and bounded gap primes, respectively. We provide here a similar construction. Let $R = N^\gamma$ for some small $\gamma > 0$ to be chosen appropriately. Relying on Green and Tao’s “smoothed” approach [2010b], we define

$$\Lambda_{\chi,\gamma}(n) := \log R \left(\sum_{\ell|n} \mu(\ell) \chi \left(\frac{\log \ell}{\log R} \right) \right)^2, \tag{4-9}$$

where $\chi : \mathbb{R} \rightarrow [0, 1]$ is a smooth, even function supported on $[-2, 2]$ satisfying $\chi(0) = 1 = \int_0^2 |\chi'|^2$. Finally let $\Lambda_{\chi,\gamma,\mathcal{H}}(n) := \prod_{h \in \mathcal{H}} \Lambda_{\chi,\gamma}(n+h)$. Note that this function is periodic (of period $\prod_{\ell \leq R^2} \ell$ for instance), so we extend it on \mathbb{Z} as a periodic function. Once W -tricked, this will be a pseudorandom measure. Ultimately, this is a consequence of the following proposition.

Proposition 4.3 (correlations of sieve weights). *Let $d, t \geq 1$ be integers. Let $D, \eta > 0$. Let $\Psi = (\psi_1, \dots, \psi_t)$ be a finite complexity system of affine-linear forms in d variables. Suppose that $\gamma > 0$ is sufficiently small in terms of d, t . Suppose that the linear coefficients, as well as the integers h_1, \dots, h_r , are bounded in magnitude by D . Assume that w is sufficiently large in terms of d, t, D . Let $K \subset [-N, N]^d$ satisfy $\text{Vol}(K) \geq \eta N^d$. Suppose b_1, \dots, b_t are in $B_{\mathcal{H}}$ (with $B_{\mathcal{H}}$ as in (4-8)). Then*

$$\sum_{\mathbf{n} \in K \cap \mathbb{Z}^d} \prod_{i \in [t]} \Lambda_{\chi,\gamma,\mathcal{H}}(W\psi_i(\mathbf{n}) + b_i) = \text{Vol}(K) \left(\frac{W}{\varphi(W)} \right)^{rt} (1 + o_{w \rightarrow \infty}(1) + O(e^{\sqrt{w}} / \log^{1/20} N)),$$

where the error terms above may depend on d, t, D, η only.

Proof. The left-hand side equals

$$\sum_{\mathbf{n} \in K \cap \mathbb{Z}^d} \prod_{i \in [t], j \in [r]} \Lambda_{\chi,\gamma}(W\psi_i(\mathbf{n}) + b_i + h_j). \tag{4-10}$$

We then apply [Green and Tao 2010b, Theorem D.3] to the system $\mathcal{L} = (W\psi_i + b_i + h_j)_{i \in [t], j \in [r]}$, whereby we assume that γ is small enough in terms of d, t .

Recalling that $\int_0^2 |\chi'|^2 = 1$, [Green and Tao 2010b, Theorem D.3] gives for (4-10) an estimate

$$\text{Vol}(K) \prod_p \beta_p(\mathcal{L}) + O(N^d e^X / (\log R)^{1/20}), \tag{4-11}$$

where $X = \sum_{p \in \mathcal{P}} p^{-1/2}$, and \mathcal{P} is the set of *exceptional primes* of \mathcal{L} , i.e., those primes p such that modulo p some two of the forms of \mathcal{L} are proportional. In view of the hypotheses of [Green and Tao 2010b, Theorem D.3] (bounded homogeneous coefficients), one may fear that the implied constant in the big oh term depends on the size of the homogeneous coefficients of \mathcal{L} , so ultimately on w , but in fact it does not at all as it quickly appears in the proof, since only the behavior of \mathcal{L} modulo each prime p plays

a role in the proof. This is made clear in [Bienvenu 2018, Proposition 2.13]; in fact already in [Green and Tao 2010b, equation (D.24)] the bound (4-11) was applied to a system \mathcal{L} with unbounded coefficients.

Note that the primes in \mathcal{P} are either $\leq w$, or $O_{d,t}(D)$. Assuming w is large enough in terms of d, t, D , we can assume that they are all $\leq w$, and therefore $X \ll \sqrt{w}/\log w$, so the error term in (4-11) becomes $O_{d,t,D,\eta}(\text{Vol}(K)e^{\sqrt{w}}/\log^{1/20} N)$. Moreover, we have $\beta_p = \beta_p(\mathcal{L}) = (p/(p-1))^{rt}$ for $p \leq w$ and $\beta_p = 1 + O_{d,t,D}(p^{-2})$ as p tends to infinity thanks to Lemma 2.2, whence $\prod_p \beta_p = (W/\varphi(W))^{rt}(1 + o_{w \rightarrow \infty}(1))$. This concludes the proof. \square

Proof of Proposition 4.2. In this proof, for any $n \in \mathbb{Z}_N$ or any $n \in \mathbb{Z}$, we will denote by \tilde{n} the unique element of $[N]$ such that $\tilde{n} \equiv n \pmod{N}$.

For $b \in \mathbb{N}$ we define $v_b : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{R}_{\geq 0}$ to be the function $n \mapsto (\varphi(W)/W)^r \Lambda_{\chi,\gamma,\mathcal{H}}(W\tilde{n} + b)$ where $\gamma \in (0, \rho/2)$. This definition naturally gives rise to a function denoted again by v_b on \mathbb{Z} . Further we set $v_{\mathbf{b}}(n) := \frac{1}{s} \sum_{i=1}^s v_{b_i}(n)$. Note that whenever $N^{2\gamma/\rho} \leq n \leq N$ satisfies $\theta(n) > 0$, we have $\theta(n) \leq \log^r(n+2) \ll \log^r R = \Lambda_{\chi,\gamma,\mathcal{H}}(n)$. Hence, whenever $\mathbf{b} = (b_1, \dots, b_s)$ is in $B_{\mathcal{H}}^s$, we have

$$\theta_{W,b_i}(n) \ll_{\gamma} \Lambda_{\chi,\gamma,\mathcal{H}}(Wn + b_i) \ll v_{\mathbf{b}}(n)$$

for each $i \in [s]$ and $n \in [N^{\gamma/\rho}, N]$.

Let us verify that $v_{\mathbf{b}}$ is a (M, ε) -pseudorandom measure. Hence, let $d \leq M$ and $t \leq M$ and $\Psi : \mathbb{Z}^d \rightarrow \mathbb{Z}^t$ be a finite complexity system of affine-linear forms whose linear coefficients are bounded by M . We work in the regime where w and N tend to infinity while $w \leq \log \log N$. It suffices to verify that in this regime

$$\mathbb{E}_{\mathbf{n} \in (\mathbb{Z}/N\mathbb{Z})^d} \prod_{i \in [t]} v_{c_i}(\psi_i(\mathbf{n})) = 1 + o_M(1) \tag{4-12}$$

for any fixed $\mathbf{c} \in \{b_1, \dots, b_s\}^t$. We cannot apply Proposition 4.3 to prove (4-12) at this stage, since this equation effectively concerns a linear system over $\mathbb{Z}/N\mathbb{Z}$ and not over \mathbb{Z} . In other words, there are wrap-around issues. To be able to apply Proposition 4.3, we first rewrite the left-hand side of (4-12) as

$$\mathbb{E}_{\mathbf{n} \in (\mathbb{Z}/N\mathbb{Z})^d} \prod_{i \in [t]} v_{c_i}(\psi_i(\mathbf{n})) = \mathbb{E}_{\mathbf{n} \in [N]^d} \prod_{i \in [t]} v_{c_i}(\widetilde{\psi_i(\mathbf{n})}). \tag{4-13}$$

Observe that the map $\mathbf{n} \mapsto \widetilde{\psi_i(\mathbf{n})}$ is not an affine-linear map, so that we still cannot invoke Proposition 4.3. However, it is piecewise affine-linear. To exploit this property, we decompose $[N]^d$ in boxes of the form

$$B_{\mathbf{u}} = \left\{ \mathbf{x} \in [N]^d : x_j \in \left(\left\lfloor \frac{(u_j - 1)N}{Q} \right\rfloor, \left\lfloor \frac{u_j N}{Q} \right\rfloor \right), j \in [d] \right\},$$

where \mathbf{u} ranges over $[Q]^d$, and Q is some function of N , to be determined later, that tends slowly to infinity with N . Assuming that N/Q tends to infinity, we have

$$\mathbb{E}_{\mathbf{n} \in [N]^d} \prod_{i \in [t]} v_{c_i}(\widetilde{\psi_i(\mathbf{n})}) = \mathbb{E}_{\mathbf{u} \in [Q]^d} \mathbb{E}_{\mathbf{n} \in B_{\mathbf{u}}} \prod_{i \in [t]} v_{c_i}(\widetilde{\psi_i(\mathbf{n})}) + o(1), \tag{4-14}$$

where the $o(1)$ accounts for the fact that all boxes are not exactly of the same size; they are all of size $(N/Q + O(1))^d = (N/Q)^d(1 + o(1))$ though. Call \mathbf{u} and the corresponding box $B_{\mathbf{u}}$ nice if for every

$i \in [t]$ the number $\lceil \psi_i(\mathbf{n})/N \rceil$ is constant as \mathbf{n} ranges in $B_{\mathbf{u}}$; that is, there exists $k = k_{i,\mathbf{u}} \in \mathbb{Z}$ such that $\psi_i(\mathbf{n}) \in (kN, (k+1)N]$ for every $\mathbf{n} \in B_{\mathbf{u}}$. When \mathbf{u} is nice, $\widetilde{\psi_i(\mathbf{n})} = \psi_i(\mathbf{n}) - k_{i,\mathbf{u}}N \in [N]$ for every $i \in [t]$ and $\mathbf{n} \in B_{\mathbf{u}}$. Therefore,

$$\mathbb{E}_{\mathbf{n} \in B_{\mathbf{u}}} \prod_{i \in [t]} v_{c_i}(\widetilde{\psi_i(\mathbf{n})}) = \mathbb{E}_{\mathbf{n} \in B_{\mathbf{u}}} \prod_{i \in [t]} v_{c_i}(\psi_{i,\mathbf{u}}(\mathbf{n})),$$

where the affine-linear map $\Psi_{\mathbf{u}} : \mathbb{Z}^d \rightarrow \mathbb{Z}^t$ is defined by setting $\psi_{i,\mathbf{u}} : \mathbf{n} \mapsto \psi_i(\mathbf{n}) - k_{i,\mathbf{u}}N$. It is clear that this map, having the same homogeneous part as Ψ , is still of finite complexity and has bounded homogeneous coefficients.

Thus, we may now apply Proposition 4.3 to conclude that

$$\mathbb{E}_{\mathbf{n} \in B_{\mathbf{u}}} \prod_{i \in [t]} v_{c_i}(\psi_{i,\mathbf{u}}(\mathbf{n})) = 1 + o_{w \rightarrow \infty; M}(1) + o_{N \rightarrow \infty; M}(1).$$

It remains to handle the other boxes. Suppose that \mathbf{u} is not nice. Thus, there exists $i \in [t]$ and two vectors \mathbf{x}, \mathbf{y} in $B_{\mathbf{u}}$ such that $k := \lceil \psi_i(\mathbf{x})/N \rceil < \lceil \psi_i(\mathbf{y})/N \rceil$. However, we have $|\psi_i(\mathbf{x}) - \psi_i(\mathbf{y})| \leq 2dM(N/Q + 1) < N$, if $Q > 3dM$. Therefore,

$$\psi_i(\mathbf{x})/N \leq k < \psi_i(\mathbf{y})/N \leq \psi_i(\mathbf{x})/N + O_M(1/Q)$$

and

$$\psi_i(\mathbf{x})/N \geq \psi_i(\mathbf{y})/N - O_M(1/Q) \geq k - O_M(1/Q).$$

The last two displayed lines show that both $\psi_i(\mathbf{x})$ and $\psi_i(\mathbf{y})$ are $kN + O(N/Q)$; thus

$$\psi_i(\mathbf{n}) = O_M(N/Q) \pmod{N} \quad \text{for all } \mathbf{n} \in B_{\mathbf{u}}.$$

Further, there exists an integer $k = k_{i,\mathbf{u}}$ such that for all $\mathbf{n} \in B_{\mathbf{u}}$ and $i \in [t]$ either $\psi_i(\mathbf{n}) - kN \in [N]$ or $\psi_i(\mathbf{n}) - (k+1)N \in [N]$; consequently,

$$\begin{aligned} v_{c_i}(\widetilde{\psi_i(\mathbf{n})}) &= v_{c_i}(\psi_i(\mathbf{n}) - k_{i,\mathbf{u}}N) \mathbf{1}_{\psi_i(\mathbf{n}) - k_{i,\mathbf{u}}N \in [N]} + v_{c_i}(\psi_i(\mathbf{n}) - (k_{i,\mathbf{u}} + 1)N) \mathbf{1}_{\psi_i(\mathbf{n}) - (k_{i,\mathbf{u}} + 1)N \in [N]} \\ &\leq v_{c_i}(\psi_i(\mathbf{n}) - k_{i,\mathbf{u}}N) + v_{c_i}(\psi_i(\mathbf{n}) - (k_{i,\mathbf{u}} + 1)N). \end{aligned}$$

Whence the bound

$$\mathbb{E}_{\mathbf{n} \in B_{\mathbf{u}}} \prod_{i \in [t]} v_{c_i}(\widetilde{\psi_i(\mathbf{n})}) \leq \mathbb{E}_{\mathbf{n} \in B_{\mathbf{u}}} \prod_{i \in [t]} (v_{c_i}(\psi_i(\mathbf{n}) - k_{i,\mathbf{u}}N) + v_{c_i}(\psi_i(\mathbf{n}) - (k_{i,\mathbf{u}} + 1)N)). \quad (4-15)$$

Expanding the product makes the right-hand side of inequality (4-15) the sum of 2^t averages, each of which equals $1 + o(1)$ by Proposition 4.3. So the left-hand side of inequality (4-15) is $O(1)$. It remains to prove that not nice boxes are rare. Suppose that \mathbf{u} is not nice. As pointed out above, if Q is large enough, there exists $i \in [t]$ such that $\psi_i(\mathbf{n}) = O_M(N/Q) \pmod{N}$ for all $\mathbf{n} \in B_{\mathbf{u}}$. On the other hand,

$$\psi_i(\mathbf{n}) = \psi_i(\lfloor N\mathbf{u}/Q \rfloor) + O_M(N/Q) = \psi_i(N\mathbf{u}/Q + O(1)) + O_M(N/Q) = N\dot{\psi}_i(\mathbf{u})/Q + \psi_i(0) + O_M(N/Q).$$

Dividing by N/Q yields

$$\dot{\psi}_i(\mathbf{u}) + Q\psi_i(0)/N = O(1) \pmod{Q}. \quad (4-16)$$

Now $\psi_i \neq 0$ and when Q is large enough $\psi_i \neq 0 \pmod{Q}$ as well, so the number of solutions $\mathbf{u} \in [Q]^d$ to the estimate (4-16) is $O(Q^{d-1})$. Multiplying by t , the proportion of bad boxes among all boxes is therefore $O(Q^{-1}) = o(1)$, the implied constant depending on M only. This concludes the proof of the estimate (4-14). \square

5. Almost twin primes in generalized Bohr sets

Now we want to prove hypothesis (ii) in Theorem 3.2 for the W -tricked functions θ_1 and θ_2 . Thus we need to find almost twin primes in s -measurable sets. We start with bounded gap primes. The next proposition establishes hypothesis (ii) in Theorem 3.2 for a function of the form $\theta_{W,b}$ from Section 4, upon letting $b_i = b + h_i$.

Proposition 5.1 (bounded gap primes with nilsequences). *Fix positive integers m, d, Δ , and some $\varepsilon > 0, K \geq 2$. Also let $w \geq 1$ be sufficiently large in terms of $m, d, \Delta, \varepsilon, K$ and let $W = \prod_{p \leq w} p$. There exist $\rho = \rho(m) > 0$, and a positive integer $k = k(m)$, such that the following statement holds for sufficiently large $x \geq x_0(m, d, \Delta, \varepsilon, K, w)$.*

Let $\xi \in \mathfrak{E}_d(\Delta, K)$ be a nilsequence taking values in $[0, 1]$. Let b_1, \dots, b_k be distinct integers satisfying $(b_i, W) = 1$ and $|b_i| \leq \log x$ for each $i \in [k]$. Then

$$\sum_{\substack{n \leq x \\ |\{Wn+b_1, \dots, Wn+b_k\} \cap \mathbb{P}| \geq m \\ p \mid \prod_{i=1}^k (Wn+b_i) \implies p > x^\rho}} \xi(n) \gg_m \left(\prod_p \beta_p \right) \frac{1}{(\log x)^k} \left(\sum_{n \leq x} \xi(n) - \varepsilon x \right),$$

where $\beta_p = \beta_p(\mathcal{L})$ is the local factor defined as in Definition 2.1 for the system of affine-linear forms $\mathcal{L} = \{L_1, \dots, L_k\}$ with $L_i(n) = Wn + b_i$.

We remark that if $p \leq w$ then $\beta_p = (p/\varphi(p))^k$, and if $p > w$ then, writing a_p for the number of distinct residue classes among $b_1, \dots, b_k \pmod{p}$,

$$\beta_p = \left(\frac{p}{\varphi(p)} \right)^k \left(1 - \frac{a_p}{p} \right) = \left(\frac{p}{\varphi(p)} \right)^{k-a_p} (1 + O_k(p^{-2})). \tag{5-1}$$

In particular, if $w > |b_i - b_j|$ for all i, j , we infer that $\prod_p \beta_p \gg (W/\varphi(W))^k$.

We now turn to the corresponding statement for Chen primes.

Proposition 5.2 (Chen primes with nilsequences). *Fix positive integers d, Δ and some $\varepsilon > 0, K \geq 2$. Also let $w \geq 1$ be sufficiently large in terms of $d, \Delta, \varepsilon, K$ and $W = \prod_{p \leq w} p$. The following statement holds for sufficiently large $x \geq x_0(d, \Delta, \varepsilon, K, w)$.*

Let $\xi \in \mathfrak{E}_d(\Delta, K)$ be a nilsequence taking values in $[0, 1]$. Then for some absolute constant $\delta_0 > 0$ and any $1 \leq b \leq W$ with $(b, W) = (b+2, W) = 1$ we have

$$\sum_{\substack{n \leq x \\ Wn+b \in \mathbb{P} \\ Wn+b+2 \in \mathcal{P}_2 \\ p \mid Wn+b+2 \implies p \geq x^{1/10}}} \xi(n) \geq \left(\frac{W}{\varphi(W)} \right)^2 \frac{\delta_0}{(\log x)^2} \left(\sum_{n \leq x} \xi(n) - \varepsilon x \right).$$

We will prove Propositions 5.1 and 5.2 by reducing to the case when the underlying polynomial sequence is equidistributed, and Propositions 5.3 and 5.4, using a factorization theorem for nilsequences.

Proposition 5.3 (bounded gap primes weighted by equidistributed nilsequences). *Fix positive integers m, d, Δ , and some $\varepsilon > 0$, $A \geq 2$. There exist $\rho = \rho(m) > 0$, a positive integer $k = k(m)$, and $C = C(m, d, \Delta) > 0$, such that the following statement holds for sufficiently large $x \geq x_0(m, d, \Delta, \varepsilon, A)$.*

Let $K \geq 2$ and $\eta \in (0, \frac{1}{2})$ be parameters satisfying the conditions

$$\eta \leq K^{-C}(\log x)^{-CA}, \quad K \leq (\log x)^C.$$

Let $\xi \in \Xi_d(\Delta, K; \eta, x)$ be a nilsequence taking values in $[0, 1]$. Let $\mathcal{L} = \{L_1, \dots, L_k\}$ be an admissible k -tuple of linear functions with $L_i(n) = a_i n + b_i$ and $1 \leq a_i \leq (\log x)^A$, $|b_i| \leq x$. Then

$$\sum_{\substack{n \leq x \\ |\{L_1(n), \dots, L_k(n)\} \cap \mathbb{P}| \geq m \\ p \mid \prod_{i=1}^k L_i(n) \Rightarrow p > x^\rho}} \xi(n) \gg_m \frac{\mathfrak{S}(\mathcal{L})}{(\log x)^k} \left(\sum_{n \leq x} \xi(n) - \varepsilon x \right), \quad (5-2)$$

where the singular series is given by $\mathfrak{S}(\mathcal{L}) := \prod_p \beta_p(\mathcal{L})$, i.e.,

$$\mathfrak{S}(\mathcal{L}) = \prod_p \left(1 - \frac{1}{p} \right)^{-k} \left(1 - \frac{|\{n \in \mathbb{Z}/p\mathbb{Z} : L_1(n) \cdots L_k(n) \equiv 0 \pmod{p}\}|}{p} \right) > 0. \quad (5-3)$$

Proposition 5.4 (Chen primes weighted by equidistributed nilsequences). *Fix positive integers d, Δ and some $\varepsilon > 0$, $A \geq 2$. There exists $C = C(d, \Delta) > 0$, such that the following statement holds for sufficiently large $x \geq x_0(d, \Delta, \varepsilon, A)$.*

Let $K \geq 2$ and $\eta \in (0, \frac{1}{2})$ be parameters satisfying the conditions

$$\eta \leq K^{-C}(\log x)^{-CA}, \quad K \leq (\log x)^C.$$

Let $\xi \in \Xi_d(\Delta, K; \eta, x)$ be a nilsequence taking values in $[0, 1]$. Let $\mathcal{L} = \{L_1, L_2\}$ be an admissible set of two linear functions with $L_1(n) = an + b$ and $L_2(n) = an + b + 2$, where $1 \leq a \leq \log x$, $|b| \leq x$. Then for some absolute constant $\delta_0 > 0$ we have

$$\sum_{\substack{n \leq x \\ L_1(n) \in \mathbb{P}, L_2(n) \in P_2 \\ p \mid L_2(n) \Rightarrow p \geq x^{1/10}}} \xi(n) \geq \delta_0 \frac{\mathfrak{S}(\mathcal{L})}{(\log x)^2} \left(\sum_{n \leq x} \xi(n) - \varepsilon x \right),$$

where the singular series is given by (5-3).

The purpose of this section is to deduce Propositions 5.1 and 5.2 from the equidistributed case, Propositions 5.3 and 5.4. We will collect some sieve lemmas in Section 6 and some analytic inputs of Bombieri–Vinogradov type in Section 7 before proving Propositions 5.3 and 5.4 in Section 8.

5A. Dealing with the periodic case. In the deduction process, we need to deal with a local (modulo q) version of Propositions 5.1 and 5.2, where the requirement that all of the $Wn + b_i$ are almost primes is replaced by the local conditions that $(Wn + b_i, q) = 1$.

Lemma 5.5. Fix positive integers k, d, Δ , and some $\varepsilon > 0, K \geq 2$. Also let $w \geq 1$ be sufficiently large in terms of $k, d, \Delta, \varepsilon, K$ and $W = \prod_{p \leq w} p$. Then the following statement holds for sufficiently large $x \geq x_0(k, d, \Delta, \varepsilon, K, w)$.

Let $\xi \in \Xi_d(\Delta, K)$. Let $\{b_1, \dots, b_k\}$ satisfy $(b_i, W) = 1$ for every $i \in [k]$. Let $q \leq x^{0.9}$ be a positive integer with $(q, W) = 1$. Then

$$\left| \beta^{-1} \left(\frac{q}{\varphi(q)} \right)^k \sum_{\substack{n \leq x \\ (\prod_{i=1}^k (Wn + b_i), q) = 1}} \xi(n) - \sum_{n \leq x} \xi(n) \right| \leq \varepsilon x,$$

where $\beta = \prod_{p|q} \beta_p$, and β_p is defined as in Proposition 5.1.

Proof. Let X be the set of $n \leq x$ such that $(Wn + b_i, q) = 1$ for each $1 \leq i \leq k$. Consider the function

$$f(n) = \beta^{-1} \left(\frac{q}{\varphi(q)} \right)^k 1_X(n) - 1.$$

Let us prove first that

$$\|f\|_{U^{d+1}[x]} = o_{x \rightarrow \infty; k, d}(1) + o_{w \rightarrow \infty; k, d}(1).$$

Expanding out $\|f\|_{U^{d+1}[x]}$ and letting $g : \mathbb{Z}^{d+2} \rightarrow \mathbb{Z}^{\{0,1\}^{d+1}}$ be the Gowers norm system

$$(x, \mathbf{h}) \mapsto (x + \omega \cdot \mathbf{h})_{\omega \in \{0,1\}^{d+1}},$$

we are left with the task of proving that

$$\sum_{\mathbf{n} \in \mathcal{D} \cap \mathbb{Z}^{d+2}} \prod_{\omega \in \{0,1\}^{d+1}} f(g_\omega(\mathbf{n})) = o_{x \rightarrow \infty; k, d}(x^{d+2}) + o_{w \rightarrow \infty; k, d}(x^{d+2}), \tag{5-4}$$

where $\mathcal{D} = \{\mathbf{y} \in \mathbb{R}^{d+2} : g_\omega(\mathbf{y}) \in [1, x], \forall \omega \in \{0,1\}^{d+1}\}$. Expanding further, the left-hand side of (5-4) equals

$$\sum_{\Omega \subset \{0,1\}^{d+1}} (-1)^{|\Omega|} \sum_{\mathbf{n} \in \mathcal{D} \cap \mathbb{Z}^{d+2}} \prod_{\omega \in \Omega} \beta^{-1} \left(\frac{q}{\varphi(q)} \right)^k 1_X(g_\omega(\mathbf{n})) = \sum_{\Omega \subset \{0,1\}^{d+1}} (-1)^{|\Omega|} S_\Omega, \tag{5-5}$$

where, after a change of variables, we have

$$S_\Omega = \sum_{\mathbf{a} \in [q]^{d+2}} \sum_{\substack{\mathbf{n} \in \mathbb{Z}^{d+2} \\ q\mathbf{n} + \mathbf{a} \in \mathcal{D}}} \prod_{\omega \in \Omega} \beta^{-1} \left(\frac{q}{\varphi(q)} \right)^k 1_X(g_\omega(q\mathbf{n} + \mathbf{a})). \tag{5-6}$$

Now the summand of the inner sum actually does not depend on \mathbf{n} since $1_X(g_\omega(q\mathbf{n} + \mathbf{a})) = 1_X(g_\omega(\mathbf{a}))$. Let $\mathcal{D}_\mathbf{a} = \{\mathbf{n} \in \mathbb{R}^{d+2} : q\mathbf{n} + \mathbf{a} \in \mathcal{D}\}$, which is a convex body of volume $q^{-(d+2)} \text{Vol}(\mathcal{D})$. Since $\mathcal{D}_\mathbf{a} \subset [1, x/q]^{d+2}$ and $\text{Vol}(\mathcal{D}) \gg_d x^{d+2}$, the number of integral points $\mathbf{n} \in \mathcal{D}_\mathbf{a} \cap \mathbb{Z}^{d+2}$ is

$$\text{Vol}(\mathcal{D}_\mathbf{a}) + O_d((x/q)^{d+1}) = q^{-(d+2)} \text{Vol}(\mathcal{D})(1 + O_d(q/x)).$$

It follows that

$$S_\Omega = (1 + O_d(q/x)) \text{Vol}(\mathcal{D}) \cdot \beta^{-|\Omega|} \mathbb{E}_{\mathbf{a} \in [q]^{d+2}} \prod_{\omega \in \Omega} \left(\frac{q}{\varphi(q)} \right)^k 1_X(g_\omega(\mathbf{a})).$$

By multiplicativity and the definition of the singular series (Definition 2.1), the average over \mathbf{a} above can be written as

$$\prod_{p|q} \left(\mathbb{E}_{\mathbf{a} \in (\mathbb{Z}/p\mathbb{Z})^{d+2}} \prod_{\omega \in \Omega} \prod_{i=1}^k \frac{p}{\varphi(p)} 1_{(Wg_\omega(\mathbf{a})+b_i, p)=1} \right) = \prod_{p|q} \beta_p(\mathcal{G}_\Omega),$$

where \mathcal{G}_Ω is the system of affine-linear forms \mathcal{G}_Ω consisting of $\mathbf{a} \mapsto Wg_\omega(\mathbf{a}) + b_i$ for $\omega \in \Omega$ and $1 \leq i \leq k$. If there are a_p distinct residue classes among $b_1, \dots, b_k \pmod{p}$, then \mathcal{G}_Ω consists of $a_p | \Omega|$ distinct affine-linear forms modulo p , no two of which are linearly dependent (over \mathbb{F}_p). Hence, Lemma 2.2 implies that

$$\beta_p(\mathcal{G}_\Omega) = \left(\frac{p}{\varphi(p)} \right)^{(k-a_p)|\Omega|} (1 + O_{k,d}(p^{-2})).$$

Since $p|q \Rightarrow p > w$, we have $\prod_{p|q} (1 + O_{k,d}(p^{-2})) = 1 + O_{k,d}(w^{-1})$. Putting things together, we have

$$S_\Omega = (1 + O_d(q/x) + O_{k,d}(w^{-1})) \text{Vol}(\mathcal{D}) \cdot \beta^{-|\Omega|} \prod_{p|q} \left(\frac{p}{\varphi(p)} \right)^{(k-a_p)|\Omega|}.$$

From (5-1) we deduce that

$$S_\Omega = (1 + O_{k,d}(qx^{-1} + w^{-1})) \text{Vol}(\mathcal{D})$$

for each $\Omega \subset \{0, 1\}^{d+1}$, and this establishes (5-4).

By [Green and Tao 2010b, Proposition 11.2] (see also footnote 3), the nilsequence ξ can be decomposed as

$$\xi = \xi_1 + \xi_2,$$

where $\|\xi_1\|_{U^{d+1}[x]^*} = O_{d,\Delta,K,\varepsilon}(1)$ and $\|\xi_2\|_\infty \leq \varepsilon/4$. Hence,

$$\left| \sum_{n \leq x} f(n) \xi_1(n) \right| \leq x \|f\|_{U^{d+1}[x]} \cdot \|\xi_1\|_{U^{d+1}[x]^*} \leq \frac{\varepsilon}{2} x,$$

provided that w and x are large enough in terms of $k, d, \Delta, K, \varepsilon$, and

$$\left| \sum_{n \leq x} f(n) \xi_2(n) \right| \leq \|\xi_2\|_\infty \sum_{n \leq x} |f(n)| \leq \frac{\varepsilon}{2} x.$$

Combining the two inequalities above gives

$$\left| \sum_{n \leq x} f(n) \xi(n) \right| \leq \varepsilon x,$$

as desired. □

5B. Reducing to the equidistributed case. We now complete the proof of Propositions 5.1 and 5.2 assuming Propositions 5.3 and 5.4. Let $f : \mathbb{N} \rightarrow \mathbb{C}$ be any function satisfying $|f(n)| \leq 1$ for any $n \in \mathbb{N}$; we will specialize later to the case where f is the indicator functions of the sets over which the summations in these propositions run. Let $\xi : \mathbb{N} \rightarrow [0, 1]$ be a nilsequence in $\mathfrak{E}_d(\Delta, K)$. We want to estimate $\sum_{n \leq x} f(n)\xi(n)$. By Definition 2.9, there exists a nilmanifold G/Γ of dimension at most Δ , equipped with a filtration G_\bullet of degree $\leq d$ and a K -rational Malcev basis \mathcal{X} , a polynomial sequence $g : \mathbb{Z} \rightarrow G$ adapted to G_\bullet and a Lipschitz function $F : G/\Gamma \rightarrow \mathbb{C}$ satisfying $\|F\|_{\text{Lip}(\mathcal{X})} \leq 1$, such that $\xi(n) = F(g(n)\Gamma)$.

Let

$$\mu := \frac{1}{x} \sum_{n \leq x} \xi(n).$$

We may assume that $\mu \geq \varepsilon$, as otherwise there is nothing to prove.

Let $B = B(m, d, \Delta) > 0$ be sufficiently large. To reduce Propositions 5.1 and 5.2 to the case when g is equidistributed, we apply the factorization theorem [Green and Tao 2012a, Theorem 1.19] to obtain some parameter $M \in [\log x, (\log x)^{O_{B,d,\Delta}(1)}]$ and a decomposition $g = \epsilon g' \gamma$ into polynomial sequences $\epsilon, g', \gamma : \mathbb{Z} \rightarrow G$ with the following properties:

- (1) ϵ is (M, x) -smooth, i.e., $d(\epsilon(n), \text{id}_G) \leq M$ and $d(\epsilon(n), \epsilon(n-1)) \leq M/x$ for all $n \in [x]$, with $d = d_{\mathcal{X}}$ the metric used on G .
- (2) g' takes values in a rational subgroup $G' \subseteq G$, equipped with a Malcev basis \mathcal{X}' in which each element is an M -rational combination of the elements of \mathcal{X} , and moreover $\{g'(n)\}_{n \leq x}$ is totally M^{-B} equidistributed in $G'/\Gamma \cap G'$.
- (3) γ is M -rational (so that $\gamma(n)\Gamma$ is an M -rational point for every $n \in \mathbb{Z}$), and moreover $\{\gamma(n)\Gamma\}_{n \in \mathbb{Z}}$ is periodic with period some $q \leq M$.

In the case of Proposition 5.1, we may make the following additional assumption on q by enlarging q and M if necessary: If $b_i \equiv b_j \pmod{p}$ for some $i \neq j$ and some prime p , then p divides q . By (5-1), this implies that if $p \nmid qW$, then $\beta_p = 1 + O_k(p^{-2})$.

Let \mathcal{Q} be a collection of arithmetic progressions of step q and length $\asymp (x/qM)(\log x)^{-100}$ such that $[x] = \bigcup_{P \in \mathcal{Q}} P$. For each $P \in \mathcal{Q}$, let γ_P be the (constant) value of γ on P and consider

$$\sum_{n \in P} f(n)\xi(n) = \sum_{n \in P} f(n)F(\epsilon(n)g'(n)\gamma_P\Gamma). \tag{5-7}$$

We shall first dispose of the smooth part $\epsilon(n)$. Pick an arbitrary $n_p \in P$, and let $\epsilon_p = \epsilon(n_p)$. If $n \in P$, then $|n - n_p| \ll (x/M)(\log x)^{-100}$. Since the Lipschitz norm of F is bounded by 1, we have

$$\begin{aligned} |F(\epsilon(n)g'(n)\gamma_P\Gamma) - F(\epsilon_p g'(n)\gamma_P\Gamma)| &\leq d_{\mathcal{X}}(\epsilon(n)g'(n)\gamma_P, \epsilon(n_p)g'(n)\gamma_P) \\ &= d_{\mathcal{X}}(\epsilon(n), \epsilon(n_p)) \\ &\leq \frac{M}{x}|n - n_p| \ll (\log x)^{-100}, \end{aligned}$$

where we used the right-invariance of the metric d . Hence (5-7) equals

$$\sum_{n \in P} f(n) F(\epsilon_P g'(n) \gamma_P \Gamma) + O(|P|(\log x)^{-100}).$$

Let H_P be the conjugate $H_P = \gamma_P^{-1} G' \gamma_P$, let $\Gamma_P = H_P \cap \Gamma$, let $F_P : H_P \rightarrow [0, 1]$ be the Γ_P -automorphic function defined by $F_P(x) = F(\epsilon_P \gamma_P x)$, and let $g_P : \mathbb{Z} \rightarrow H_P$ be the polynomial sequence defined by $g_P(n) = \gamma_P^{-1} g'(n) \gamma_P$. Thus

$$F(\epsilon_P g'(n) \gamma_P \Gamma) = F_P(g_P(n) \Gamma_P).$$

Some routine arguments (see the Claim at the end of Section 2 in [Green and Tao 2012b]) produce the following properties:

- (1) The subnilmanifold H_P / Γ_P is equipped with a Malcev basis \mathcal{X}_P in which each element is an $M^{O_{d,\Delta}(1)}$ -rational combination of the elements of \mathcal{X} .
- (2) $\{g_P(n)\}_{n \leq x}$ is totally M^{-cB} -equidistributed for some constant $c = c(d, \Delta) > 0$. By choosing B large enough we may ensure that $cB \geq C$, the constant from Propositions 5.3 or 5.4.
- (3) $\|F_P\|_{\text{Lip}} \leq M^{O_{d,\Delta}(1)}$.

Let $y = |P| \gg (x/qM)(\log x)^{-100} \geq x^{1/2}$, and write $P = \{qn + t : n \leq y\}$ for some $t \in \mathbb{Z}$. Let $g'_P : \mathbb{Z} \rightarrow H_P$ be the polynomial sequence defined by $g'_P(n) = g_P(qn + t)$, so that $\{g'_P(n)\}_{n \leq y}$ is still totally M^{-cB} -equidistributed (after possibly reducing the constant c). Then

$$\sum_{n \in P} f(n) F(\epsilon_P g'(n) \gamma_P \Gamma) = \sum_{n \leq y} f(qn + t) F_P(g'_P(n) \Gamma_P). \tag{5-8}$$

Case of Proposition 5.1. Now we specialize to the function f relevant for Proposition 5.1. Write $L_i(n) = Wn + b_i$, and let $\mathcal{L}' = \mathcal{L}'_P = \{L'_1, \dots, L'_k\}$, where L'_i is the linear function defined by $L'_i(n) = L_i(qn + t)$. Let f be the indicator function of the set of integers n such that $\#\{(L_1(n), \dots, L_k(n)) \cap \mathbb{P}\} \geq m$ and $p | L_1(n) \cdots L_k(n) \implies p \geq x^\rho$. Thus

$$\sum_{n \leq y} f(qn + t) F_P(g'_P(n) \Gamma_P) = \sum_{\substack{n \leq y \\ \#\{(L'_1(n), \dots, L'_k(n)) \cap \mathbb{P}\} \geq m \\ p | L'_1(n) \cdots L'_k(n) \implies p \geq x^\rho}} F_P(g'_P(n) \Gamma_P).$$

If \mathcal{L}' remains admissible, then by Proposition 5.3 the right-hand side above is

$$\begin{aligned} &\gg_k \frac{\mathfrak{S}(\mathcal{L}')}{(\log x)^k} \left(\sum_{n \leq y} F_P(g'_P(n) \Gamma_P) - \varepsilon/4 \cdot y \right) = \frac{\mathfrak{S}(\mathcal{L}')}{(\log x)^k} \left(\sum_{n \in P} F(\epsilon_P g'(n) \gamma_P \Gamma) - \varepsilon/4 \cdot |P| \right) \\ &\geq \frac{\mathfrak{S}(\mathcal{L}')}{(\log x)^k} \left(\sum_{n \in P} F(\epsilon(n) g'(n) \gamma_P \Gamma) - \varepsilon/2 \cdot |P| \right), \end{aligned}$$

where the last inequality follows once again from the smoothness of ϵ . By the definition of $\mathfrak{S}(\mathcal{L}')$, we see that \mathcal{L}' is admissible if and only if $(Wt + b_i, q) = 1$ for each $1 \leq i \leq k$, and in this case we have

$$\mathfrak{S}(\mathcal{L}') = \prod_{p \mid qW} \left(1 - \frac{1}{p}\right)^{-k} \prod_{p \nmid qW} \left(1 - \frac{k}{p}\right) \left(1 - \frac{1}{p}\right)^{-k} \asymp \left(\frac{qW}{\varphi(qW)}\right)^k.$$

Putting everything together, under the assumption that \mathcal{L}' is admissible, we have proven that

$$\sum_{\substack{n \in P \\ \{|Wn+b_1, \dots, Wn+b_k\} \cap \mathbb{P}| \geq m \\ p \mid \prod_{i=1}^k (Wn+b_i) \Rightarrow p > x^\rho}} \xi(n) \gg_m \left(\frac{qW}{\varphi(qW)}\right)^k \frac{1}{(\log x)^k} \sum_{n \in P} \left(\xi(n) - \frac{\epsilon}{2}\right).$$

Summing this estimate over all $P \in \mathcal{Q}$, we get

$$\begin{aligned} \sum_{\substack{n \leq x \\ \{|Wn+b_1, \dots, Wn+b_k\} \cap \mathbb{P}| \geq m \\ p \mid \prod_{i=1}^k (Wn+b_i) \Rightarrow p > x^\rho}} \xi(n) &\gg_m \left(\frac{qW}{\varphi(qW)}\right)^k \frac{1}{(\log x)^k} \sum_{\substack{n \leq x \\ (\prod_{i=1}^k (Wn+b_i), q) = 1}} \left(\xi(n) - \frac{\epsilon}{2}\right) \\ &= \left(\frac{W}{\varphi(W)(\log x)} \cdot \frac{q}{\varphi\left(\frac{q}{(q, W)}\right)}\right)^k \sum_{\substack{n \leq x \\ (\prod_{i=1}^k (Wn+b_i), \frac{q}{(q, W)}) = 1}} \left(\xi(n) - \frac{\epsilon}{2}\right). \end{aligned}$$

Finally, applying Lemma 5.5 to the summation on the right-hand side, with q replaced by $q/(q, W)$ and ξ replaced by $\xi - \epsilon/2$, we get that the right-hand side above is at least

$$\left(\frac{W}{\varphi(W)(\log x)}\right)^k \left(\prod_{p \mid q/(q, W)=1} \beta_p\right) \left(\sum_{n \leq x} \xi(n) - \epsilon x\right) = \left(\prod_{p \mid qW} \beta_p\right) \frac{1}{(\log x)^k} \left(\sum_{n \leq x} \xi(n) - \epsilon x\right).$$

The conclusion of Proposition 5.1 follows, since $\beta_p = 1 + O_k(p^{-2})$ for $p \nmid qW$ by our assumption on q .

Case of Proposition 5.2. Finally, we address Proposition 5.2. Thus we return to (5-8) and now specialize to the case where f is the indicator function of the set of integers n such that $L_1(n) \in \mathbb{P}$ and $L_2(n) \in P_2$ and $p \mid L_2(n) \Rightarrow p \geq x^{1/10}$, where $L_1(n) = Wn + b$ and $L_2(n) = Wn + b + 2$. Let $\mathcal{L}' = \mathcal{L}'_P = \{L'_1, L'_2\}$, where for $i \in \{1, 2\}$, the linear function L'_i is defined by $L'_i(n) = L_i(qn + t)$. Then we have

$$\sum_{n \leq y} f(qn + t) F_P(g'_P(n) \Gamma_P) = \sum_{\substack{n \leq y \\ L'_1(n) \in \mathbb{P}, L'_2(n) \in P_2 \\ p \mid L'_2(n) \Rightarrow p \geq x^{1/10}}} F_P(g'_P(n) \Gamma_P).$$

If \mathcal{L}' remains admissible (which happens precisely when $(Wt + b, q) = (Wt + b + 2, q) = 1$), then Proposition 5.4 and the same argument as above prove that the right-hand side above is at least

$$\delta_0 \left(\frac{qW}{\varphi(qW)}\right)^2 \frac{1}{(\log x)^2} \sum_{n \in P} (\xi(n) - \epsilon/2).$$

This time the summation over all $P \in \mathcal{Q}$ yields, after applying Lemma 5.5,

$$\sum_{\substack{n \leq x \\ L_1(n) \in \mathbb{P}, L_2(n) \in P_2 \\ p \mid L_2(n) \Rightarrow p \geq x^{1/10}}} \xi(n) \geq \delta_0 \left(\prod_{p \mid q/(q,W)} \beta_p \right) \left(\frac{W}{\varphi(W)} \right)^2 \frac{1}{(\log x)^2} \left(\sum_{n \leq x} \xi(n) - \varepsilon x \right).$$

The conclusion of Proposition 5.2 follows, since $\beta_p = 1 + O_k(p^{-2})$ for $p > w$ by (5-1).

6. Three sieve lemmas

In the proof of Theorems 1.1 and 1.2, we will need weighted versions of Maynard’s sieve for bounded gap primes, Chen’s sieve for almost twin primes, and Iwaniec’s sieve for primes of the form $x^2 + y^2 + 1$.

Proposition 6.1 (Maynard’s sieve). *For any $\theta \in (0, 1)$, $k \in \mathbb{N}$, there exist constants $C = C(\theta)$, $\rho = \rho(\theta, k)$ such that the following holds.*

Let $(\omega_n)_{n \leq x}$ be any nonnegative sequence, and let $\mathcal{L} = (L_1, \dots, L_k)$ be an admissible k -tuple of linear functions with $L_i(n) = a_i n + b_i$ and $1 \leq a_i, b_i \leq x$. Suppose that (ω_n) obeys these hypotheses:

(i) (prime number theorem). *For each $1 \leq i \leq k$ and some $\delta > 0$, we have*

$$\frac{\varphi(a_i)}{a_i} \sum_{\substack{n \leq x \\ L_i(n) \in \mathbb{P}}} \omega_n \geq \frac{\delta}{\log x} \sum_{n \leq x} \omega_n.$$

(ii) (good distribution in arithmetic progressions). *For some $C_0 > 0$ we have*

$$\sum_{r \leq x^\theta} \max_{c \pmod{r}} \left| \sum_{\substack{n \leq x \\ n \equiv c \pmod{r}}} \omega_n - \frac{1}{r} \sum_{n \leq x} \omega_n \right| \leq C_0 \frac{\sum_{n \leq x} \omega_n}{(\log x)^{101k^2}}.$$

(iii) (Bombieri–Vinogradov). *For each $1 \leq i \leq k$ we have*

$$\sum_{r \leq x^\theta} \max_{\substack{(L_i(c), r) = 1 \\ n \equiv c \pmod{r} \\ L_i(n) \in \mathbb{P}}} \left| \sum_{\substack{n \leq x \\ n \equiv c \pmod{r} \\ L_i(n) \in \mathbb{P}}} \omega_n - \frac{\varphi(a_i)}{\varphi(a_i r)} \sum_{\substack{n \leq x \\ L_i(n) \in \mathbb{P}}} \omega_n \right| \leq C_0 \frac{\sum_{n \leq x} \omega_n}{(\log x)^{101k^2}}.$$

(iv) (Brun–Titchmarsh). *We have*

$$\max_{c \pmod{r}} \sum_{\substack{n \leq x \\ n \equiv c \pmod{r}}} \omega_n \leq \frac{C_0}{r} \sum_{n \leq x} \omega_n,$$

uniformly for $r \leq x^\theta$.

Then, for $x \geq x_0(\theta, k, C_0)$, we have

$$\sum_{\substack{n \leq x \\ \{|L_1(n), \dots, L_k(n)\} \cap \mathbb{P}| \geq C^{-1} \delta \log k \\ p \mid \prod_{i=1}^k L_i(n) \Rightarrow p > x^\rho}} \omega_n \gg_{k, \theta, \delta} \frac{\mathfrak{S}(\mathcal{L})}{(\log x)^k} \sum_{n \leq x} \omega_n,$$

where the singular series $\mathfrak{S}(\mathcal{L})$ is given by (5-3).

Proof. This is [Matomäki and Shao 2017, Theorem 6.2] (with $\alpha = 1$ there), which adds weights to the corresponding statement in [Maynard 2016]. □

In the next sieve lemma for Chen primes, we need the notion of well factorable weights.

Definition 6.2. We say that a sequence $\lambda : [N] \rightarrow \mathbb{R}$ is *well factorable* of level $D \geq 1$, if for any $R, S \geq 1$ satisfying $D = RS$, we can write $\lambda = \lambda_1 * \lambda_2$ for some sequences $|\lambda_1|, |\lambda_2| \leq 1$ supported on $[1, R]$ and $[1, S]$, respectively, with $*$ denoting Dirichlet convolution.

Proposition 6.3 (Chen’s sieve). *Let $\varepsilon > 0$ be a small enough absolute constant. Let $(\omega_n)_{n \leq x}$ be any nonnegative sequence, let $\mathcal{L} = \{L_1, L_2\}$ with $L_i(n) = a_i n + b_i$, $1 \leq a_i \leq \log x$, $|b_i| \leq x$. Suppose that (ω_n) satisfies the following hypotheses:*

(i) (Bombieri–Vinogradov with well factorable weights). *We have*

$$\left| \sum_{\substack{r \leq x^{1/2-\varepsilon} \\ (r, a_2(a_1 b_2 - a_2 b_1))=1}} \lambda(r) \left(\sum_{\substack{n \leq x \\ L_2(n) \equiv 0 \pmod{r} \\ L_1(n) \in \mathbb{P}}} \omega_n - \frac{a_1}{\varphi(a_1 r)} \sum_{n \leq x} \frac{\omega_n}{\log L_1(n)} \right) \right| \ll \frac{\sum_{n \leq x} \omega_n}{(\log x)^{10}}$$

for any well factorable sequence λ of level $x^{1/2-\varepsilon}$, and also for $\lambda = 1_{p \in [P, P']} * \lambda'$ with λ' any well factorable sequence of level $x^{1/2-\varepsilon}/P$ with $P' \in [P, 2P]$ and $P \in [x^{1/10}, x^{1/3-\varepsilon}]$.

(ii) (Bombieri–Vinogradov for almost primes with well factorable weights). *For $j \in \{1, 2\}$ we have*

$$\left| \sum_{\substack{r \leq x^{1/2-\varepsilon} \\ (r, a_1(a_1 b_2 - a_2 b_1))=1}} \lambda(r) \left(\sum_{\substack{n \leq x \\ L_1(n) \equiv 0 \pmod{r} \\ L_2(n) \in B_j}} \omega_n - \frac{\varphi(a_2)}{\varphi(a_2 r)} \sum_{\substack{n \leq x \\ L_2(n) \in B_j}} \omega_n \right) \right| \ll \frac{\sum_{n \leq x} \omega_n}{(\log x)^{10}},$$

where $\lambda(r)$ is as above and

$$B_1 = \{p_1 p_2 p_3 : x^{1/10} \leq p_1 \leq x^{1/3-\varepsilon}, x^{1/3-\varepsilon} \leq p_2 \leq (2x/p_1)^{1/2}, p_3 \geq x^{1/10}\},$$

$$B_2 = \{p_1 p_2 p_3 : x^{1/3-\varepsilon} \leq p_1 \leq p_2 \leq (2x/p_1)^{1/2}, p_3 \geq x^{1/10}\}.$$

(iii) (upper bound on almost primes). *For $j \in \{1, 2\}$ we have*

$$\sum_{\substack{n \leq x \\ L_2(n) \in B_j}} \omega_n \leq (1 + \varepsilon) \cdot \frac{|B_j \cap [1, L_2(x)]|}{\varphi(a_2)x} \sum_{n \leq x} \omega_n.$$

Then, for $x \geq x_0$, we have

$$\sum_{\substack{n \leq x \\ L_1(n) \in \mathbb{P} \\ L_2(n) \in P_2 \\ p | L_2(n) \Rightarrow p \geq x^{1/10}}} \omega_n \geq \delta_0 \frac{\mathfrak{S}(\mathcal{L})}{(\log x)^2} \sum_{n \leq x} \omega_n - O(x^{0.9} \max_n \omega_n),$$

for some absolute constant $\delta_0 > 0$, where the singular series $\mathfrak{S}(L)$ is given by (5-3).

Proof. This is [Matomäki and Shao 2017, Theorem 6.4] (which adds weights to Chen’s sieve), with the slight modification that $|b_i|$ may be as large as x (as opposed to $x^{o(1)}$). However, this restriction on $|b_i|$ was not used in the proof. Also, in [Matomäki and Shao 2017, Theorem 6.4] $\lambda(r)$ was replaced with $\mu(r)^2\lambda(r)$, but since in the proof the sequence $\lambda(r)$ is always a sieve coefficient supported on squarefree numbers, this makes no difference. \square

For stating the weighted sieve for primes of the form $x^2 + y^2 + 1$, we need a notion slightly different from admissibility, which we call amenability, following [Teräväinen 2018, Definition 3.1].

Definition 6.4. We say that a linear function $L(n) = Kn + b$ with $K \geq 1$ and $b \in \mathbb{Z}$ is *amenable* if

- (i) $6^3 \mid K$;
- (ii) $(b, K) = (b - 1, s(K)) = 1$, where $s(n) := \prod_{p \mid n, p \equiv -1 \pmod{4}, p \neq 3} p$;
- (iii) $b - 1 = 2^j 3^{2t} (4h + 1)$ for some $h \in \mathbb{Z}$ with $3 \nmid 4h + 1$, and $j, t \geq 0$ with $2^{j+2} 3^{2t+1} \mid K$.

Here condition (ii) guarantees that there are no local obstructions to $L(n)$ being a prime of the form $x^2 + y^2 + 1$. Conditions (i) and (iii) are introduced for technical reasons to do with sieves in [Teräväinen 2018], but they are not very restrictive.

Proposition 6.5 (weighted sieve for primes of the form $x^2 + y^2 + 1$). *There exists some small $\varepsilon > 0$ such that the following holds. Let $(\omega_n)_{n \leq x}$ be any nonnegative sequence, and let $L(n) = Kn + b$ be amenable with $1 \leq K \leq \log x$. Suppose that (ω_n) obeys the following hypotheses:*

- (i) *For any sequence $(g(\ell))_\ell$ supported on $[1, x^{0.9}]$ and of the form $g = \alpha * \beta$ with α supported on $[x^{1/(3+\varepsilon)}, x^{1-1/(3+\varepsilon)}]$ and $|\alpha(n)|, |\beta(n)| \leq 1$, we have*

$$\left| \sum_{\substack{r \leq x^{1/2-\varepsilon} \\ (r, K)=1}} \lambda_r^{+, \text{LIN}} \sum_{\substack{\ell \leq x^{0.9} \\ (\ell, K)=\delta \\ (\ell, r)=1}} g(\ell) \left(\sum_{\substack{n \leq x \\ p \leq x \\ L(n)=\ell p+1 \\ L(n) \equiv 0 \pmod{r}}} \omega_n - \frac{1}{\varphi(r)} \frac{K}{\varphi(\frac{K}{\delta})} \sum_{n \leq x} \frac{\omega_n}{\ell \log \frac{Kn}{\ell}} \right) \right| \ll \frac{\sum_{n \leq x} \omega_n}{(\log x)^{100}}, \quad (6-1)$$

where $\delta := (b - 1, K)$ and $\lambda_r^{+, \text{LIN}}$ are the upper bound linear sieve coefficients of level $x^{1/2-\varepsilon}$ and sifting parameter $x^{1/5}$.

- (ii) *We have*

$$\left| \sum_{\substack{r \leq x^{3/7-\varepsilon} \\ (r, K)=1}} \lambda_r^{-, \text{SEM}} \left(\sum_{\substack{n \leq x \\ L(n) \in \mathbb{P} \\ L(n) \equiv 1 \pmod{r}}} \omega_n - \frac{1}{\varphi(r)} \frac{K}{\varphi(K)} \sum_{n \leq x} \frac{\omega_n}{\log(Kn)} \right) \right| \ll \frac{\sum_{n \leq x} \omega_n}{(\log x)^{100}}, \quad (6-2)$$

where $\lambda_r^{-, \text{SEM}}$ are the lower bound semilinear sieve coefficients of level $x^{3/7-\varepsilon}$ and sifting parameter $x^{1/(3+\varepsilon)}$.

Then for some absolute constant $\delta_0 > 0$ we have

$$\sum_{\substack{n \leq x \\ L(n) \in \mathbb{P} \\ p|L(n)-1 \Rightarrow p \not\equiv -1 \pmod{4}}} \omega_n \geq \delta_0 \frac{\mathfrak{S}(L)}{(\log x)^{3/2}} \sum_{n \leq x} \omega_n - O(x^{1/2}), \tag{6-3}$$

where the singular series $\mathfrak{S}(L)$ is given by

$$\begin{aligned} \mathfrak{S}(L) := & \prod_{\substack{p \equiv -1 \pmod{4} \\ p \neq 3}} \left(1 - \frac{|\{n \in \mathbb{Z}/p\mathbb{Z} : L(n) \equiv 0 \text{ or } 1 \pmod{p}\}|}{p} \right) \left(1 - \frac{2}{p} \right)^{-1} \\ & \cdot \prod_{p \not\equiv -1 \pmod{4}} \left(1 - \frac{|\{n \in \mathbb{Z}/p\mathbb{Z} : L(n) \equiv 0 \pmod{p}\}|}{p} \right) \left(1 - \frac{1}{p} \right)^{-1}. \end{aligned} \tag{6-4}$$

Proof. This follows from [Teräväinen 2018, Theorem 6.5], taking $\rho_1 = \frac{1}{2} - \varepsilon$, $\rho_2 = \frac{3}{7} - \varepsilon$ and $\sigma = 3 + \varepsilon$ there and using the fact that hypothesis $H(\rho_1, \rho_2, \sigma)$ there holds with these parameters (the n summation in [Teräväinen 2018, Theorem 6.5] is over a dyadic interval, but this clearly makes no difference). \square

7. Bombieri–Vinogradov and Type I/II estimates for nilsequences

In this section, we collect Bombieri–Vinogradov type estimates for nilsequences from [Shao and Teräväinen 2021] that we shall need. Theorems 7.1 and 7.2 below are slight generalizations of [Shao and Teräväinen 2021, Theorems 4.3 and 4.4], respectively.

Theorem 7.1. *Let an integer $s \geq 1$, a large real number $\Delta \geq 2$, and a small real number $\varepsilon \in (0, \frac{1}{3})$ be given. Let $L(n) = an + b$ for some $1 \leq a \leq x^{\varepsilon/2}$ and $|b| \leq x$ with $(a, b) = 1$. There exists a constant $\kappa = \kappa(s, \Delta, \varepsilon) > 0$, such that for any $x \geq 2$, $\eta > 0$ and any nilsequence $\xi \in \mathfrak{E}_s^0(\Delta, \eta^{-\kappa}; \eta, x)$ we have*

$$\sum_{d \leq x^{1/3-\varepsilon}} \max_{(L(c), d)=1} \left| \sum_{\substack{n \leq x \\ n \equiv c \pmod{d}}} \Lambda(L(n)) \xi(n) \right| \ll \eta^\kappa ax (\log x)^2.$$

Theorem 7.2. *Let integers $s \geq 1$, $c \neq 0$, a large real number $\Delta \geq 2$, and a small real number $\varepsilon \in (0, \frac{1}{2})$ be given. Let $L(n) = an + b$ for some $1 \leq a \leq x^{\varepsilon/2}$ and $|b| \leq x$ with $(a, b) = 1$. There exists a constant $\kappa = \kappa(s, \Delta, \varepsilon) > 0$, such that for any well factorable sequence (λ_d) of level $x^{1/2-\varepsilon}$ with $x \geq 2$ and any nilsequence $\xi \in \mathfrak{E}_s^0(\Delta, \eta^{-\kappa}; \eta, x)$ with $\eta > 0$, we have*

$$\left| \sum_{\substack{d \leq x^{1/2-\varepsilon} \\ (d, c)=1}} \lambda_d \sum_{\substack{n \leq x \\ L(n) \equiv c \pmod{d}}} \Lambda(L(n)) \xi(n) \right| \ll \eta^\kappa ax (\log x)^2.$$

Proofs of Theorem 7.1 and 7.2. We deduce Theorem 7.1 from [Shao and Teräväinen 2021, Theorem 4.3]; the deduction of Theorem 7.2 from [Shao and Teräväinen 2021, Theorem 4.4] is completely similar.

Write $\xi(n) = F(g(n)\Gamma)$. One can find a polynomial sequence g' such that $g'(L(n)) = g(n)$, for example, by examining the Taylor coefficients of g in coordinates (see [Green and Tao 2012a, Lemma 6.7]).

We claim that $\{g'(n)\}_{n \leq ax}$ is totally η^c -equidistributed for some small constant $c = c(s, \Delta) > 0$. Suppose that this is not the case. Then by the quantitative Kronecker theorem for nilsequences (see [Green and Tao 2012a, Theorem 2.9]), there is a nontrivial horizontal character χ with $\|\chi\| \ll \eta^{-O_{s,\Delta}(c)}$ such that

$$\|\chi \circ g'\|_{C^\infty(ax)} \ll \eta^{-O_{s,\Delta}(c)}.$$

Since g' is a polynomial sequence, we can write

$$\chi \circ g'(n) = \alpha_0 + \alpha_1 n + \cdots + \alpha_s n^s.$$

Then there is a positive integer $q \ll_s 1$ such that the coefficients satisfy

$$\|q\alpha_i\| \ll_s (ax)^{-i} \eta^{-O_{s,\Delta}(c)}$$

for each $1 \leq i \leq s$. Now

$$\chi \circ g(n) = \chi \circ g'(an + b) = \sum_{i=0}^s \alpha_i (an + b)^i.$$

If we write β_j for the coefficient of n^j in $\eta \circ g$, then one can establish that

$$\|q\beta_j\| \ll_s x^{-j} \eta^{-O_{s,\Delta}(c)}$$

for each $1 \leq j \leq s$. Hence

$$\|q\chi \circ g\|_{C^\infty(x)} \ll_s \eta^{-O_{s,\Delta}(c)}.$$

It now follows (from [Shao and Teräväinen 2021, Lemma 3.6]) that $\{g(n)\}_{n \leq x}$ is not totally $\eta^{-O_{s,\Delta}(c)}$ -equidistributed, which is a contradiction if c is chosen small enough.

Let $\xi'(n) = F(g'(n)\Gamma)$. Then $\xi' \in \Xi_s^0(\Delta, \eta^{-\kappa}; \eta^c, ax)$. After a change of variables, we can write

$$\sum_{\substack{n \leq x \\ n \equiv c \pmod{d}}} \Lambda(L(n))\xi(n) = \sum_{\substack{L(0) < n \leq L(x) \\ n \equiv L(c) \pmod{ad}}} \Lambda(n)\xi'(n).$$

It follows that

$$\sum_{d \leq x^{1/3-\varepsilon}} \max_{(L(c), d)=1} \left| \sum_{\substack{n \leq x \\ n \equiv c \pmod{d}}} \Lambda(L(n))\xi(n) \right| \leq \sum_{d' \leq ax^{1/3-\varepsilon}} \max_{(c', d')=1} \left| \sum_{\substack{L(0) < n \leq L(x) \\ n \equiv c' \pmod{d'}}} \Lambda(n)\xi'(n) \right|.$$

By [Shao and Teräväinen 2021, Theorem 4.3], the right-hand side above is $\ll \eta^{c\kappa} ax (\log x)^2$ for some constant $\kappa = \kappa(s, \Delta, \varepsilon) > 0$. The conclusion follows. \square

We will also need a few type I and type II estimates appearing in [Shao and Teräväinen 2021].

Lemma 7.3 (type I Bombieri–Vinogradov estimate). *Let $x \geq 2$ and $\varepsilon > 0$. Let $1 \leq M \leq x^{1/2}$ and $1 \leq D \leq x^{1/2-\varepsilon}$. Let $s \geq 1$, $\Delta \geq 2$, and $0 < \delta < \frac{1}{2}$. Let $L(n) = an + b$ for some $1 \leq a \leq x^{\varepsilon/2}$ and $|b| \leq x$*

with $(a, b) = 1$. Let $\xi \in \mathfrak{E}_s^0(\Delta, \delta^{-1}; \delta^C, x)$ for some sufficiently large constant $C = C(s, \Delta, \varepsilon)$. Then

$$\sum_{D \leq d \leq 2D} \max_{c \pmod{d}} \sum_{\substack{M \leq m \leq 2M \\ (m, ad)=1}} \left| \sum_{\substack{mn \leq L(x) \\ mn \equiv c \pmod{d} \\ mn \equiv b \pmod{a}}} \xi(L^{-1}(mn)) \right| \ll \delta x.$$

Proof. The case $L(n) = n$ is [Shao and Teräväinen 2021, Proposition 5.5]. We shall quickly reduce the general case to this case.

By the argument in the proof of Theorems 7.1 and 7.2, there exists a nilsequence $\xi' \in \mathfrak{E}_s^0(\Delta, \delta^{-1}; \delta^{C'}, ax)$ for some large constant $C' = C'(s, \Delta, \varepsilon)$, such that $\xi'(n) = \xi(L^{-1}(n))$ if $n \equiv b \pmod{a}$. Then use the identity

$$1_{mn \equiv b \pmod{a}} = \frac{1}{\varphi(a)} \sum_{\chi \pmod{a}} \chi(m) \chi(n) \overline{\chi(b)}$$

to reduce matters to

$$\sum_{D \leq d \leq 2D} \max_{c \pmod{d}} \sum_{\substack{M \leq m \leq 2M \\ (m, ad)=1}} \left| \sum_{\substack{mn \leq L(x) \\ mn \equiv c \pmod{d}}} \chi(mn) \xi'(mn) \right| \ll \delta x$$

for characters $\chi \pmod{a}$. Splitting mn into residue classes \pmod{a} , it suffices to show for all u coprime to a that

$$\sum_{D \leq d \leq 2D} \max_{c \pmod{d}} \sum_{\substack{M \leq m \leq 2M \\ (m, ad)=1}} \left| \sum_{\substack{mn \leq L(x) \\ mn \equiv c \pmod{d} \\ mn \equiv u \pmod{a}}} \xi'(mn) \right| \ll \delta x.$$

Now, applying the Chinese remainder theorem to combine the congruences on mn , and making the change of variables $d' = [d, a] \leq 2aD$, the conclusion then follows from the case $L(n) = n$ that was already established. □

Lemma 7.4 (well factorable type II Bombieri–Vinogradov estimate). *Let $\varepsilon > 0$ be a small constant. Let $x \geq 2$ and $M \in [x^{1/4}, x^{3/4}]$ be large and let $c \neq 0, k$ be fixed integers. Suppose that either*

- (i) λ is well factorable of level $x^{1/2-\varepsilon}$, or
- (ii) $\lambda = 1_{p \in [P, P']} * \lambda'$, where λ' is well factorable of level $x^{1/2-\varepsilon}/P$ and $2P \geq P' \geq P \in [x^{1/10}, x^{1/3-\varepsilon}]$.

Let $s \geq 1, \Delta \geq 2, 0 < \delta < \frac{1}{2}$. Let $L(n) = an + b$ for some $1 \leq a \leq x^{\varepsilon/2}$ and $|b| \leq x$ with $(a, b) = 1$. Let $\xi \in \mathfrak{E}_s^0(\Delta, \delta^{-1}; \delta^C, x)$ for some sufficiently large constant $C = C(s, \Delta, \varepsilon)$. Then

$$\left| \sum_{\substack{d \leq x^{1/2-\varepsilon} \\ (d, ac)=1}} \lambda_d \sum_{\substack{L(x) \leq mn \leq L(2x) \\ M \leq m \leq 2M \\ mn \equiv c \pmod{d} \\ mn \equiv b \pmod{a}}} \alpha(m) \beta(n) \xi(L^{-1}(mn)) \right| \ll \delta ax (\log x)^{O_k(1)},$$

uniformly for sequences $\{\alpha(n)\}$ and $\{\beta(n)\}$ satisfying $|\alpha(n)|, |\beta(n)| \leq d_k(n)$.

This is a consequence of the following somewhat more general statement.

Lemma 7.5. *Let $\varepsilon > 0$ be a small constant. Let $x \geq 2$ and $M \in [x^{1/4}, x^{3/4}]$ be large and let $c \neq 0, k$ be fixed integers. Let $R_1, R_2 \geq 1$ be such that $R_1 \leq x^{1-\varepsilon}/M$, $R_1 R_2 \leq x^{1/2-\varepsilon}$ and $R_1 R_2^2 \leq Mx^{-\varepsilon}$. Let $s \geq 1$, $\Delta \geq 2$, $0 < \delta < \frac{1}{2}$. Let $L(n) = an + b$ for some $1 \leq a \leq x^{\varepsilon/2}$ and $|b| \leq x$ with $(a, b) = 1$. Let $\xi \in \Xi_s^0(\Delta, \delta^{-1}; \delta^C, x)$ for some sufficiently large constant $C = C(s, \Delta, \varepsilon)$. Then*

$$\sum_{\substack{R_1 \leq r_1 \leq 2R_1 \\ R_2 \leq r_2 \leq 2R_2 \\ (r_1 r_2, ac) = 1}} \left| \sum_{\substack{L(x) \leq mn \leq L(2x) \\ M \leq m \leq 2M \\ mn \equiv c \pmod{r_1 r_2} \\ mn \equiv b \pmod{a}}} \alpha(m)\beta(n)\xi(L^{-1}(mn)) \right| \ll \delta ax (\log x)^{O_k(1)},$$

uniformly for sequences $\{\alpha(n)\}$ and $\{\beta(n)\}$ satisfying $|\alpha(n)|, |\beta(n)| \leq d_k(n)$.

To see that Lemma 7.4 follows from Lemma 7.5, it suffices to show that the well factorable sequence λ can be decomposed into convolutions of the form $\gamma * \theta$, where the sequences γ and θ are 1-bounded sequences supported on $[1, 2R_1]$ and $[1, 2R_2]$, respectively, with $R_1 = x^{1-\varepsilon}/M$ and $R_2 = Mx^{-1/2}$. This is evidently true in case (i) of Lemma 7.4 since λ is well factorable. In case (ii), since $P \leq R_1$, we can write $\lambda' = \lambda_1 * \lambda_2$ for some sequences λ_1, λ_2 supported on $[1, R_1/P]$ and $[1, R_2]$, respectively. Then we can take $\gamma = 1_{p \in [P, P']} * \lambda_1$ and $\theta = \lambda_2$.

Proof of Lemma 7.5. By switching the roles of m and n if necessary, we may assume that $M \in [x^{1/2}, x^{3/4}]$. The case $L(n) = n$ follows from [Shao and Teräväinen 2021, Proposition 6.6]. The reduction of the general case to this case is very similar to the corresponding reduction in the proof of Lemma 7.3. \square

In the special case when $\lambda_d = 1_{d=1}$, Lemma 7.4 implies that

$$\left| \sum_{\substack{mn \leq L(x) \\ M \leq m \leq 2M \\ mn \equiv b \pmod{a}}} \alpha(m)\beta(n)\xi(L^{-1}(mn)) \right| \ll_k \delta ax (\log x)^{O_k(1)}. \tag{7-1}$$

In the case $L(n) = n$, this is also the type II information required in Green and Tao’s proof [2012b, Section 3] that the Möbius function is orthogonal to nilsequences.

8. Dealing with the equidistributed case

The goal of this section is to prove Propositions 5.3 and 5.4. We shall apply the sieve lemmas in Section 6 to reduce matters to certain Bombieri–Vinogradov type equidistribution results about primes weighted by nilsequences in arithmetic progressions, which follow from results in Section 7.

8A. Proof of Proposition 5.3. We may assume that $\varepsilon > 0$ is fixed, since x is large enough in terms of ε . In what follows, let B be a large enough constant depending on m, d, Δ . We may assume that C is large enough in terms of B . Recall Definition 2.10 and the notation from that definition, thus $\xi(n) = F(g(n)\Gamma)$, where G/Γ is a nilmanifold equipped with a filtration of degree at most d , etc. Let $\mu = \int_{G/\Gamma} F$, so that

the η -equidistribution of $\{g(n)\}_{n \leq x}$ implies

$$\left| \sum_{n \leq x} (\xi(n) - \mu) \right| \ll x/(\log x)^B. \tag{8-1}$$

We may assume that $\mu \geq \varepsilon/2$, since otherwise (5-2) is trivial.

We will apply Maynard’s sieve method in the form of Proposition 6.1. We need to verify hypotheses (i)–(iv) there for the sequence $\omega_n = \xi(n)$ (with $\delta = \frac{1}{2}$ and $\theta = \frac{1}{10}$, say) and then the claim follows.

Hypothesis (i) (with $\delta = \frac{1}{2}$ in its statement) asserts that

$$\frac{\varphi(a_i)}{a_i} \sum_{\substack{n \leq x \\ L_i(n) \in \mathbb{P}}} \xi(n) \geq \frac{1}{2(\log x)} \sum_{n \leq x} \xi(n).$$

Note that $\xi' := \xi - \mu$ is an equidistributed nilsequence lying in $\Xi_d^0(\Delta, K; \eta, x)$. By partial summation, we have

$$\left| \sum_{\substack{n \leq x \\ L_i(n) \in \mathbb{P}}} \xi'(n) \right| \ll \sup_{2 \leq y \leq x} \frac{1}{\log L_i(y)} \left| \sum_{n \leq y} \Lambda(L_i(n)) \xi'(n) \right| + O(x^{1/2}). \tag{8-2}$$

we may apply (the $d = 1$ case of) Theorem 7.1 to bound the right-hand side of (8-2) by $\ll \eta^\kappa x (\log x)^{A+10}$ for some constant $\kappa = \kappa(d, \Delta) > 0$, which can be made $\ll x (\log x)^{-B}$ by our assumption on η . Hypothesis (i) now follows from the prime number theorem and (8-1).

We turn to hypothesis (ii), which (taking $\theta = \frac{1}{10}$ there) states that

$$\sum_{r \leq x^{1/10}} \max_{c \pmod{r}} \left| \sum_{\substack{n \leq x \\ n \equiv c \pmod{r}}} \xi(n) - \frac{1}{r} \sum_{n \leq x} \xi(n) \right| \ll x/(\log x)^B. \tag{8-3}$$

We may clearly replace $\xi(n)$ by $\xi'(n) = \xi(n) - \mu$ here; the new nilsequence ξ' lies in $\Xi_d^0(\Delta, K; \eta, x)$. Recalling (8-1), our task is to show that

$$\sum_{r \leq x^{1/10}} \max_{c \pmod{r}} \left| \sum_{\substack{n \leq x \\ n \equiv c \pmod{r}}} \xi'(n) \right| \ll x/(\log x)^B.$$

But this follows from Lemma 7.3 with $M = 1$ and $L(n) = n$.

Next we consider hypothesis (iii), which (with $\theta = \frac{1}{10}$) states that

$$\sum_{r \leq x^{1/10}} \max_{(L_i(c), r) = 1} \left| \sum_{\substack{n \leq x \\ n \equiv c \pmod{r} \\ L_i(n) \in \mathbb{P}}} \xi(n) - \frac{\varphi(a_i)}{\varphi(a_i r)} \sum_{\substack{n \leq x \\ L_i(n) \in \mathbb{P}}} \xi(n) \right| \ll x/(\log x)^B. \tag{8-4}$$

Applying the Bombieri–Vinogradov theorem, we may replace $\xi(n)$ by $\xi'(n) = \xi(n) - \mu$ on the left-hand side of (8-4). By the argument we used to verify hypothesis (i), we have

$$\left| \sum_{\substack{n \leq x \\ L_i(n) \in \mathbb{P}}} \xi'(n) \right| \ll x/(\log x)^{B+1}. \tag{8-5}$$

Hence, by partial summation, (8-4) reduces to

$$\sum_{r \leq x^{1/10}} \max_{(L_i(c), r)=1} \left| \sum_{\substack{n \leq y \\ n \equiv c \pmod{r}}} \Lambda(L_i(n)) \xi'(n) \right| \ll x/(\log x)^B \tag{8-6}$$

for $y \in [x(\log x)^{-10B}, x]$. This last claim follows from Theorem 7.1.

Finally, hypothesis (iv) states that

$$\max_{c \pmod{r}} \sum_{\substack{n \leq x \\ n \equiv c \pmod{r}}} \xi(n) \ll \frac{1}{r} \sum_{n \leq x} \xi(n).$$

However, this is trivial, since the left-hand side is $O(x/r)$ and the right-hand side is $\geq \varepsilon x/r$ by the consideration at the beginning of the proof and the fact that $\varepsilon > 0$ is fixed.

This concludes the proof of Proposition 5.3.

8B. Proof of Proposition 5.4. We now turn to Chen primes. Let $\mu = \int_{G/\Gamma} F$. Similarly as in the proof of Proposition 5.3, we may assume that $\mu \geq \varepsilon/2$, and we have (8-1).

We apply a weighted version of Chen’s sieve from Proposition 6.3. We see from it that the claim follows once we verify hypotheses (i)–(iii) there.

Hypothesis (i) states that

$$\left| \sum_{\substack{r \leq x^{1/2-\varepsilon'} \\ (r, 2a)=1}} \lambda(r) \left(\sum_{\substack{n \leq x \\ L_2(n) \equiv 0 \pmod{r} \\ L_1(n) \in \mathbb{P}}} \xi(n) - \frac{a}{\varphi(ar)} \sum_{n \leq x} \frac{\xi(n)}{\log L_1(n)} \right) \right| \ll x/(\log x)^{10} \tag{8-7}$$

for some small enough constant $\varepsilon' > 0$, with $\lambda(r)$ either well factorable of level $x^{1/2-\varepsilon'}$ or a convolution of the shape $1_{p \in [P, P']} * \lambda'$, with λ' a well factorable function of level $x^{1/2-\varepsilon'}/P$ and $2P \geq P' \geq P \in [x^{1/10}, x^{1/3-\varepsilon'}]$. Note first that by the Bombieri–Vinogradov theorem we may replace ξ with $\xi' = \xi - \mu$ on the left-hand side of (8-7) up to negligible error. Note also that

$$\left| \sum_{n \leq x} \frac{\xi'(n)}{\log L_1(n)} \right| \ll x/(\log x)^B$$

by (8-1) and partial summation. Applying partial summation to replace $1_{\mathbb{P}}(L_1(n))$ with the von Mangoldt function, we are left with showing

$$\left| \sum_{\substack{r \leq x^{1/2-\varepsilon'} \\ (r, 2a)=1}} \lambda(r) \sum_{\substack{n \leq y \\ L_2(n) \equiv 0 \pmod{r}}} \Lambda(L_1(n)) \xi'(n) \right| \ll x/(\log x)^{100}$$

for all $y \in [x/(\log x)^{101}, x]$. Since $L_2(n) = L_1(n) + 2$, the condition $L_2(n) \equiv 0 \pmod{r}$ is equivalent to $L_1(n) \equiv -2 \pmod{r}$. So this follows from Theorem 7.2.

The statement of hypothesis (ii) is that, for $j \in \{1, 2\}$, we have

$$\left| \sum_{\substack{r \leq x^{1/2-\varepsilon'} \\ (r, 2a)=1}} \lambda(r) \left(\sum_{\substack{n \leq x \\ L_1(n) \equiv 0 \pmod{r} \\ L_2(n) \in B_j}} \xi(n) - \frac{\varphi(a)}{\varphi(ar)} \sum_{\substack{n \leq x \\ L_2(n) \in B_j}} \xi(n) \right) \right| \ll x/(\log x)^{10}, \tag{8-8}$$

where $\lambda(r)$ is as in hypothesis (i) and

$$B_1 = \{p_1 p_2 p_3 : x^{1/10} \leq p_1 \leq x^{1/3-\varepsilon'}, x^{1/3-\varepsilon'} \leq p_2 \leq (2x/p_1)^{1/2}, p_3 \geq x^{1/10}\},$$

$$B_2 = \{p_1 p_2 p_3 : x^{1/3-\varepsilon'} \leq p_1 \leq p_2 \leq (2x/p_1)^{1/2}, p_3 \geq x^{1/10}\}.$$

First note that $1_{n \in B_j}$ splits into a sum of $(\log x)^{10}$ type II convolutions $\alpha * \beta(n)$, where $|\alpha(n)|, |\beta(n)| \leq 1$ and α is supported on an interval $[M, 2M] \subset [x^{1/3-\varepsilon'}, x^{1/2}]$. Now, we decompose $\xi(n) = \xi'(n) + \mu$ and note that the contribution of the μ term to (8-8) is $\ll x/(\log x)^B$ by a type II Bombieri–Vinogradov estimate [Iwaniec and Kowalski 2004, Theorem 17.4] and the previous observation about $1_{n \in B_j}$ being a sum of type II convolutions. Now we shall prove that

$$\left| \sum_{\substack{n \leq x \\ L_2(n) \in B_j}} \xi'(n) \right| \ll x/(\log x)^B. \tag{8-9}$$

Again by the fact that $1_{L_2(n) \in B_j}$ is of type II, it suffices to prove after a change of variables that

$$\left| \sum_{\substack{mn \leq L_2(x) \\ mn \equiv L_2(0) \pmod{a}}} \alpha(m) \beta(n) \xi'(L_2^{-1}(mn)) \right| \ll x/(\log x)^{2B}$$

for any $|\alpha(n)|, |\beta(n)| \leq 1$, where $\alpha(n)$ is supported on an interval $[M, 2M] \subset [x^{1/3-\varepsilon'}, x^{1/2}]$. But this estimate follows from (7-1) as a special case of Lemma 7.4. Now we have reduced (8-8) to proving

$$\left| \sum_{\substack{r \leq x^{1/2-\varepsilon'} \\ (r, 2a)=1}} \lambda(r) \sum_{\substack{n \leq x \\ L_1(n) \equiv 0 \pmod{r} \\ L_2(n) \in B_j}} \xi'(n) \right| \ll x/(\log x)^{10}. \tag{8-10}$$

The condition $L_1(n) \equiv 0 \pmod{r}$ above is equivalent to $L_2(n) \equiv 2 \pmod{r}$. Once again recalling the type II nature of $1_{L_2(n) \in B_j}$ and using the well factorable type II estimate of Lemma 7.4, we obtain (8-10).

We are left with hypothesis (iii), which states that

$$\sum_{\substack{n \leq x \\ L_2(n) \in B_j}} \xi(n) \leq (1 + \varepsilon') \frac{|B_j \cap [1, L_2(x)]|}{\varphi(a)x} \sum_{n \leq x} \xi(n) \tag{8-11}$$

for $j \in \{1, 2\}$ and for $\varepsilon' > 0$ a small enough constant. This claim follows simply by decomposing $\xi(n) = \xi'(n) + \mu$ and using (8-1), (8-9), and the prime number theorem in arithmetic progressions.

All the hypotheses have now been verified, so the proposition follows.

9. Proof of the main theorem

We now present the proof of our main theorem by combining the work in the previous sections.

Proof of Theorem 1.1. We seek to apply Proposition 4.1 to the functions $\theta = \theta_1$ (in which case $\mathcal{H} = \mathcal{H}_1 = \{0, 2\}$, $r = 2$) and $\theta = \theta_2$ (in which case $\mathcal{H} = \mathcal{H}_2$ is the tuple fixed when we defined θ_2 and $r = m$). To apply this theorem, we need to establish (4-2).

Thus let $\Psi : \mathbb{Z}^d \rightarrow \mathbb{Z}^t$ be a system of finite complexity whose linear coefficients are bounded in modulus by some constant L . Recall that by an easy linear algebraic argument, we may assume that Ψ is in s -normal form for some s . Also suppose that $\mathcal{H} \subset [0, L]$. Let $x \geq 1$ and $K \subset [-x, x]^d$ be a convex body such that $\Psi(K) \subset [1, x]^t$ and $\text{Vol}(K) \geq \eta x^d$ for some constant $\eta > 0$. Let $w \geq 1$ be chosen later (sufficiently large in terms of d, t, L) and let $W = \prod_{p \leq w} p$. Let $(b_1, \dots, b_t) \in B_{\mathcal{H}}^t$. It suffices to prove that

$$\sum_{n \in \mathbb{Z}^d \cap K} \prod_{i \in [t]} \theta_{j, W, b_i}(\psi_i(\mathbf{n})) \gg_{d, t, L, \eta} \text{Vol}(K) \tag{9-1}$$

for $j \in \{1, 2\}$, where, recalling (4-1), $\theta_{j, W, b}$ is defined as $\theta'_{W, b}$ for $\theta' = \theta_j$. We will prove (9-1) by appealing to Theorem 3.2. Let $M = M(d, t, L)$ be the constant produced by this theorem, and suppose that x is large enough and α small enough as in this theorem. Without loss of generality (upon using Bertrand’s postulate, dilating x by a factor of at most 8 and shrinking η by a factor at most 8^d), we may assume that x is prime and $K \subset [-x/4, x/4]^d$. By Proposition 4.2, there exists $c \in (0, 1)$ and $C > 0$ depending only on d, t, L, M (and therefore ultimately on (d, t, L) only) and an (M, α) -pseudorandom measure $\nu_b : \mathbb{Z}/x\mathbb{Z} \rightarrow \mathbb{R}_{\geq 0}$ such that $\theta_{j, W, b_i}(n) \leq C\nu(n)$ whenever $i \in [t]$ and $n \in [x^c, x]$. Define then $\lambda_i : \mathbb{Z}/x\mathbb{Z} \rightarrow \mathbb{R}_{\geq 0}$ by $\lambda_i = \theta_{j, W, b_i} 1_{[x^c, x]}/C$, where as usual we identify $[x]$ and $\mathbb{Z}/x\mathbb{Z}$ in the natural way. Therefore we have $\lambda_i \leq \nu$ on $\mathbb{Z}/x\mathbb{Z}$ by construction, so hypothesis (i) of Theorem 3.2 is satisfied.

We now turn to hypothesis (ii). Let $\delta_1 = \delta_0/(3C)$, where δ_0 is the absolute constant of Proposition 5.2, and δ_2 be the implied constant of Proposition 5.1, for our choice of m , divided by $3C$. Therefore δ_j depends at most on d, t, L for each $j \in [t]$. Let Y_j, ε_j be the corresponding constants given by Theorem 3.2, which are functions of d, t, L, δ_j for $j \in \{1, 2\}$. Fix $i \in [t]$. For $j \in \{1, 2\}$, denote by f_j the function λ_i constructed above from the function $\theta = \theta_j$. We intend to show that

$$\sum_{n \leq x} f_j(n) \xi(n) \geq \delta_j \sum_{n \leq x} \xi(n) \tag{9-2}$$

whenever $\xi : \mathbb{Z} \rightarrow [0, 1]$ is a nilsequence of complexity at most Y_j satisfying $\sum_{n \leq x} \xi(n) \geq \varepsilon_j x$. Since $\sum_{n \leq x^c} \theta_{W, b}(n) \ll x^{c+o(1)}$, it suffices to show that $\sum_{n \leq x} \theta_{W, b}(n) \xi(n) \geq 2C\delta_j \sum_{n \leq x} \xi(n)$. But this follows from Propositions 5.2 and 5.1 assuming x is large enough, and the diameter of \mathcal{H}_2 is smaller than w .

Therefore, the hypotheses of Theorem 3.2 are met; applying this theorem yields (9-1) and we are done. Thus we obtain Theorem 1.1 with $C_i(\Psi) = \prod_p \beta_p(\Psi_{\mathcal{H}_i})$. □

9A. The case of primes of the form $x^2 + y^2 + 1$. We now turn to the proof of Theorem 1.2. We shall be brief with the arguments in places, since they closely resemble those used to prove Theorem 1.1.

Let $\theta_3(n)$ be the weighted indicator of primes of the form $x^2 + y^2 + 1$ given by (1-2). Also denote the set of sums of two squares by

$$S := \{n \geq 1 : n = x^2 + y^2 \text{ for some } x, y \in \mathbb{Z}\}.$$

We follow the proof strategy of Theorem 1.1. Let $W := 6^3 \prod_{3 \leq p \leq w} p$. Define

$$\theta_{3,W,b}(n) := (W/\varphi(W))^{3/2} \theta(Wn + b).$$

We first claim that Theorem 1.2 follows if

$$\sum_{\substack{n \in \mathbb{Z}^d \\ Wn + \mathbf{a} \in K}} \prod_{i=1}^t \theta_{3,W,\psi_i(\mathbf{a})}(\psi_i(n)) \gg W^{-d} \text{Vol}(K), \tag{9-3}$$

for any convex body K satisfying $\Psi(K) \subset [1, x]^d$, $\text{Vol}(K) \gg x^d$ and for each $\mathbf{a} \in \mathcal{A}$, where

$$\mathcal{A} := \{\mathbf{a} \in (\mathbb{Z}/W\mathbb{Z})^d : \forall i \in [t], Wn + \psi_i(\mathbf{a}) \text{ amenable}\}.$$

The proof of this implication is essentially the same as for Proposition 4.1, i.e., we choose $K = K_{\mathbf{a}}$ as there and sum (9-3) over all $\mathbf{a} \in \mathcal{A}$ and note that $|\mathcal{A}| \gg \prod_p \beta'_p W^d$ by the Chinese remainder theorem, where

$$\beta'_p := \mathbb{E}_{\mathbf{a} \in (\mathbb{Z}/p\mathbb{Z})^d} \prod_{i \in [t]} (1 - |A_p|/p)^{-1} 1_{\psi_i(\mathbf{a}) \notin A_p \pmod{p}}$$

and $A_p = \{0, 1\}$ for $p \equiv -1 \pmod{4}$ and $A_p = \{0\}$ otherwise.

Thus, by applying Theorem 3.2, it suffices to prove that the following hold for all fixed w and $1 \leq b_i \leq W$ such that $Wn + b_i$ is amenable.

(1) For any $M \geq 1$, $\alpha > 0$, $t \geq 1$, there exist $0 < c < 1$ and an (M, α) -pseudorandom measure $\nu_b : \mathbb{Z}/x\mathbb{Z} \rightarrow \mathbb{R}_{\geq 0}$ such that $\theta_{W,b_i}(n) \ll_{M,t} \nu(n)$ whenever $i \in [t]$ and $n \in [x^c, x]$.

(2) There exists an absolute constant $\delta_0 > 0$ such that, for any $Y \geq 1$, $\varepsilon > 0$ and $x \geq x_0(Y, \varepsilon)$ large enough, we have

$$\sum_{n \leq x} \theta_{3,W,b_i}(n) \xi(n) \geq \delta_0 \sum_{n \leq x} \xi(n)$$

whenever $\xi : \mathbb{Z} \rightarrow [0, 1]$ is a nilsequence of complexity at most Y satisfying $\sum_{n \leq x} \xi(n) \geq \varepsilon x$.

Proof of (1). This follows from the work of Sun and Pan [2019, Section 2 and in particular Proposition 2.1 there]. □

Proof of (2). Let Y and ε be fixed in the statement of (2). For the proof of (2), it suffices to prove the following result, which is a direct analogue of Proposition 5.1 in the case of bounded gap integers or of Proposition 5.2 in the case of Chen primes. □

Proposition 9.1 (primes of the form $x^2 + y^2 + 1$ with nilsequences). *Fix positive integers d, Δ and some $\varepsilon > 0, K \geq 2$. Also let $w \geq 1$ be sufficiently large in terms of $d, \Delta, \varepsilon, K$ and $W = 6^3 \prod_{3 \leq p \leq w} p$. The following statement holds for sufficiently large $x \geq x_0(d, \Delta, \varepsilon, K, w)$.*

Let $\xi \in \mathfrak{E}_d(\Delta, K)$ be a nilsequence taking values in $[0, 1]$. Then for some absolute constant $\delta_0 > 0$ and any $1 \leq b \leq W$ such that $Wn + b$ is amenable, we have

$$\sum_{\substack{n \leq x \\ Wn+b \in \mathbb{P} \\ Wn+b-1 \in S}} \xi(n) \geq \left(\frac{W}{\varphi(W)}\right)^{3/2} \frac{\delta_0}{(\log x)^{3/2}} \left(\sum_{n \leq x} \xi(n) - \varepsilon x\right).$$

By arguments similar to those in Section 5 (with Lemma 5.5 slightly adjusted to handle the local problem in our setting), we can reduce this to the equidistributed case.

Proposition 9.2 (primes of the form $x^2 + y^2 + 1$ weighted by equidistributed nilsequences). *Fix positive integers d, Δ and some $\varepsilon > 0, A \geq 2$. There exists $C = C(d, \Delta) > 0$, such that the following statement holds for sufficiently large $x \geq x_0(d, \Delta, \varepsilon, A)$.*

Let $K \geq 2$ and $\eta \in (0, \frac{1}{2})$ be parameters satisfying the conditions

$$\eta \leq K^{-C} (\log x)^{-CA}, \quad K \leq (\log x)^C.$$

Let $\xi \in \mathfrak{E}_d(\Delta, K; \eta, x)$ be a nilsequence taking values in $[0, 1]$. Let $L(n) = an + b$ be an amenable linear function, where $1 \leq a \leq \log x, |b| \leq x$. Then for some absolute constant $\delta_0 > 0$ we have

$$\sum_{\substack{n \leq x \\ L(n) \in \mathbb{P} \\ L(n)-1 \in S}} \xi(n) \geq \delta_0 \frac{\mathfrak{S}(L)}{(\log x)^{3/2}} \left(\sum_{n \leq x} \xi(n) - \varepsilon x\right), \tag{9-4}$$

where the singular series is given by (6-4).

The remaining task is then to prove this proposition.

Proof of Proposition 9.2. We may assume that $\varepsilon > 0$ is fixed, since x is large enough in terms of ε .

We apply Proposition 6.5. Thus, in order to obtain (9-4), it suffices to verify hypotheses (i)–(ii) of Proposition 6.5 for $\omega_n = \xi(n)$ in order to obtain the claim. Since $\sum_{n \leq x} \omega_n \geq \varepsilon x \gg x$, it in fact suffices to verify versions of hypotheses (i)–(ii) where $(\sum_{n \leq x} \omega_n)/(\log x)^{100}$ is replaced with $x/(\log x)^{100}$ on the right-hand side of the inequalities (6-1), (6-2).

Write $\xi(n) = \xi'(n) + \mu$, where $\mu = \int_{G/\Gamma} F$. Observing that hypotheses (i)–(ii) hold for constant sequences (in the case of (i) by a bilinear Bombieri–Vinogradov type estimate [Iwaniec and Kowalski 2004, Theorem 17.4] and in the case of (ii) by the classical Bombieri–Vinogradov theorem), it suffices to verify hypothesis (i)–(ii) (with $x/(\log x)^{100}$ on the right-hand side of (6-1), (6-2)) for $\xi'(n)$, which belongs to $\mathfrak{E}_d^0(\Delta, K; \eta, x)$ with $\eta \leq (\log x)^{-CA}$ for a large constant C .

Verifying hypothesis (i). Let $\omega_n = \xi'(n)$. First note that by partial summation and the fact that $\xi' \in \Xi_d^0(\Delta, K; \eta, x)$, we have

$$\left| \sum_{n \leq x} \frac{\xi'(n)}{\log(yn)} \right| \ll \frac{x}{(\log x)^{300}}, \tag{9-5}$$

say, uniformly for $x^{-0.99} \leq y \leq x$. Hence, recalling the definition of $g(\ell)$ in hypothesis (i), and letting $u = (b - 1, a)$, our task is to show that

$$\left| \sum_{\substack{r \leq x^{1/2-\varepsilon} \\ (r,a)=1}} \lambda_r^{+, \text{LIN}} \sum_{\substack{x^{1/(3+\varepsilon)} \leq \ell_1 \leq x^{1/(3+\varepsilon)} \\ \ell_2 \leq x^{0.9-1/(3+\varepsilon)} \\ (\ell_1 \ell_2, a)=u \\ (\ell_1 \ell_2, r)=1}} \alpha(\ell_1) \beta(\ell_2) \left(\sum_{\substack{n \leq x \\ p \leq x \\ L(n)=\ell_1 \ell_2 p+1 \\ L(n) \equiv 0 \pmod{r}}} \xi'(n) \right) \right| \ll \frac{x}{(\log x)^{100}},$$

uniformly for $|\alpha(n)|, |\beta(n)| \leq 1$. Merging the variables ℓ_2 and p as $m = \ell_2 p$, it suffices to show that

$$\left| \sum_{\substack{r \leq x^{1/2-\varepsilon} \\ (r,a)=1}} \lambda_r^{+, \text{LIN}} \sum_{\ell_1 \in I} \alpha(\ell_1) 1_{(\ell_1, r)=1, (\ell_1, a)=u_1} b(m) 1_{(m, r)=1, (m, a)=u_2} \left(\sum_{\substack{n \leq x \\ L(n)=\ell_1 m+1 \\ L(n) \equiv 0 \pmod{r}}} \xi'(n) \right) \right| \ll \frac{x}{(\log x)^{100}},$$

uniformly for $1 \leq u_1, u_2 \leq u$ and $|\alpha(n)|, |\beta(n)| \leq d_2(n)$, where we have set $I := [x^{1/(3+\varepsilon)}, x^{1-1/(3+\varepsilon)}]$ for brevity. We make a linear change of variables in the inner sum over n to reduce to

$$\sum_{\substack{r \leq x^{1/2-\varepsilon} \\ (r,a)=1}} |\lambda_r^{+, \text{LIN}}| \left| \sum_{\ell_1 \in I} \alpha(\ell_1) 1_{(\ell_1, r)=1, (\ell_1, a)=u_1} b(m) 1_{(m, r)=1, (m, a)=u_2} \left(\sum_{\substack{\ell_1 m \leq L(x) \\ \ell_1 m \equiv 1 \pmod{r} \\ \ell_1 m \equiv b-1 \pmod{a}}} \xi' \left(\frac{\ell_1 m + 1 - b}{a} \right) \right) \right| \ll \frac{x}{(\log x)^{101}}.$$

We can replace the sequence $\lambda_r^{+, \text{LIN}}$ above with a well factorable sequence using [Friedlander and Iwaniec 2010, Corollary 12.17], which splits the linear sieve coefficients into a linear combination of boundedly many well factorable sequences. Now the claimed estimate follows directly from the well factorable type II estimate given by Lemma 7.4.

Verifying hypothesis (ii). Let $\omega_n = \xi'(n)$. Again applying (9-5), we reduce to

$$\left| \sum_{\substack{r \leq x^{3/7-\varepsilon} \\ (r,a)=1}} \lambda_r^{-, \text{SEM}} \left(\sum_{\substack{n \leq x \\ L(n) \in \mathbb{P} \\ L(n) \equiv 1 \pmod{r}}} \xi'(n) \right) \right| \ll \frac{x}{(\log x)^{100}}.$$

Making the change of variables $n' = L(n)$, this is equivalent to

$$\left| \sum_{\substack{r \leq x^{3/7-\varepsilon} \\ (r,a)=1}} \lambda_r^{-, \text{SEM}} \left(\sum_{\substack{n \leq L(x) \\ n \in \mathbb{P} \\ n \equiv 1 \pmod{r} \\ n \equiv b \pmod{a}}} \xi'(L^{-1}(n)) \right) \right| \ll \frac{x}{(\log x)^{100}}.$$

Applying partial summation, it suffices to show

$$\left| \sum_{\substack{r \leq x^{3/7-\varepsilon} \\ (r,a)=1}} \lambda_r^{-,\text{SEM}} \left(\sum_{\substack{n \leq y \\ n \equiv 1 \pmod{r} \\ n \equiv b \pmod{a}}} \Lambda(n) \xi'(L^{-1}(n)) \right) \right| \ll \frac{x}{(\log x)^{100}},$$

uniformly for $1 \leq y \leq L(x)$. By Vaughan’s identity, we can write the von Mangoldt function as a sum of $\ll (\log x)^{10}$ convolutions $a * b(n)$, where $|a(n)|, |b(n)| \leq (\log n)d_2(n)$ and $\text{supp}(a) \subset [M, 2M]$ and one of the following holds:

- (1) $M \ll x^{1/3}$ and $b(n) \equiv 1$ or $b(n) \equiv \log n$ (type I case);
- (2) $x^{1/2} \ll M \ll x^{2/3}$ (type II case).

Thus, we reduce to proving that

$$\left| \sum_{\substack{r \leq x^{3/7-\varepsilon} \\ (r,a)=1}} \lambda_r^{-,\text{SEM}} \left(\sum_{\substack{mn \leq L(x) \\ mn \equiv 1 \pmod{r} \\ mn \equiv b \pmod{a}}} a(m)b(n) \xi'(L^{-1}(mn)) \right) \right| \ll \frac{x}{(\log x)^{110}}.$$

In the type I case, we can in fact assume that $b(n) \equiv 1$ by applying partial summation. Now, to handle the type I sums, we can apply the bound $|\lambda_r^{-,\text{SEM}}| \leq 1$, followed by Cauchy–Schwarz to dispose of the $a(m)$ coefficients (this loses a factor of $(\log x)^{10}$, say, so for the resulting sum we need a bound of $x/(\log x)^{120}$). To the resulting sum we can then apply Lemma 7.3 to obtain the desired conclusion.

We then turn to the type II sums. If $M \leq x^{4/7}$, we can directly apply Lemma 7.5 with $R_1 = x^{3/7-\varepsilon}$, $R_2 = 1$, since then $R_1 \leq x^{1-\varepsilon}/M$, $R_1 R_2^2 \leq Mx^{-\varepsilon}$. Hence, we may assume for now on that $x^{4/7} \leq M \ll x^{2/3}$.

We now apply a partial factorization of the lower bound semilinear sieve weights from [Teräväinen 2018, Lemma 9.2, formulas (10.3), (10.4)] (taking $\theta = \varepsilon/2$ and replacing ε with $\varepsilon/10$ in those formulas). Since $x^{1/3-\varepsilon} \ll x^{1-\varepsilon}/M \ll x^{3/7-\varepsilon}$, we conclude that

$$|\lambda_r^{-,\text{SEM}}| \ll (\log x)^2 \max_{R_1, R_2} \sum_{\substack{r=r_1 r_2 \\ r_1 \in [R_1, 2R_1] \\ r_2 \in [R_2, 2R_2]}} 1, \tag{9-6}$$

where the maximum is over those $(R_1, R_2) \in \mathbb{R}_{\geq 1}^2$ satisfying

$$R_1 \leq x^{1-\varepsilon}/M, \quad R_1 R_2^2 \leq Mx^{-\varepsilon}, \quad R_1 R_2 \leq x^{3/7-\varepsilon/2}. \tag{9-7}$$

Hence, applying (9-6), the remaining task is to show that

$$\sum_{\substack{R_1 \leq r_1 \leq 2R_1 \\ R_2 \leq r_2 \leq 2R_2}} \left| \sum_{\substack{mn \leq L(x) \\ mn \equiv 1 \pmod{r_1 r_2} \\ mn \equiv b \pmod{a}}} a(m)b(n) \xi'(L^{-1}(mn)) \right| \ll \frac{x}{(\log x)^{200}}$$

under the constraints (9-7). Since the constraints on R_1, R_2 are precisely as in Lemma 7.5, we may appeal to that lemma to conclude. This completes the verification of hypothesis (i)–(ii), and hence the proof of Theorem 1.2. □

Acknowledgments

Bienvenu is grateful for the financial support and hospitality of the Max Planck Institute for Mathematics, Bonn. While finishing up he was supported by the joint FWF-ANR project Arithrand: FWF: I 4945-N and ANR-20-CE91-0006. Shao was supported by the NSF grant DMS-1802224. Teräväinen was supported by a Titchmarsh Research Fellowship. We thank the anonymous referee for a thorough reading of the paper and many insightful comments and suggestions.

References

- [Bienvenu 2017] P.-Y. Bienvenu, “A higher-dimensional Siegel–Walfisz theorem”, *Acta Arith.* **179**:1 (2017), 79–100. MR Zbl
- [Bienvenu 2018] P.-Y. Bienvenu, *Linear, bilinear and polynomial structures in function fields and the primes*, Ph.D. thesis, University of Bristol, 2018, available at <https://hdl.handle.net/1983/65dafc60-53df-4151-89b2-5efc0eff2b5c>.
- [Chen 1973] J. R. Chen, “On the representation of a larger even integer as the sum of a prime and the product of at most two primes”, *Sci. Sinica* **16** (1973), 157–176. MR
- [Conlon et al. 2014] D. Conlon, J. Fox, and Y. Zhao, “The Green–Tao theorem: an exposition”, *EMS Surv. Math. Sci.* **1**:2 (2014), 249–282. MR Zbl
- [Conlon et al. 2015] D. Conlon, J. Fox, and Y. Zhao, “A relative Szemerédi theorem”, *Geom. Funct. Anal.* **25**:3 (2015), 733–762. MR Zbl
- [Dodos and Kanellopoulos 2022] P. Dodos and V. Kanellopoulos, “Uniformity norms, their weaker versions, and applications”, *Acta Arith.* **203**:3 (2022), 251–270. MR Zbl
- [Frantzikinakis and Host 2017] N. Frantzikinakis and B. Host, “Higher order Fourier analysis of multiplicative functions and applications”, *J. Amer. Math. Soc.* **30**:1 (2017), 67–157. MR Zbl
- [Frei et al. 2021] C. Frei, P. Koymans, and E. Sofos, “Vinogradov’s three primes theorem with primes having given primitive roots”, *Math. Proc. Cambridge Philos. Soc.* **170**:1 (2021), 75–110. MR Zbl
- [Friedlander and Iwaniec 2010] J. Friedlander and H. Iwaniec, *Opera de cribro*, American Mathematical Society Colloquium Publications **57**, Amer. Math. Soc., 2010. MR Zbl
- [Green and Tao 2008] B. Green and T. Tao, “The primes contain arbitrarily long arithmetic progressions”, *Ann. of Math. (2)* **167**:2 (2008), 481–547. MR Zbl
- [Green and Tao 2010a] B. Green and T. Tao, “An arithmetic regularity lemma, an associated counting lemma, and applications”, pp. 261–334 in *An irregular mind*, edited by I. Bárány and J. Solymosi, Bolyai Soc. Math. Stud. **21**, János Bolyai Math. Soc., Budapest, 2010. MR Zbl
- [Green and Tao 2010b] B. Green and T. Tao, “Linear equations in primes”, *Ann. of Math. (2)* **171**:3 (2010), 1753–1850. MR Zbl
- [Green and Tao 2012a] B. Green and T. Tao, “The quantitative behaviour of polynomial orbits on nilmanifolds”, *Ann. of Math. (2)* **175**:2 (2012), 465–540. MR Zbl
- [Green and Tao 2012b] B. Green and T. Tao, “The Möbius function is strongly orthogonal to nilsequences”, *Ann. of Math. (2)* **175**:2 (2012), 541–566. MR Zbl
- [Green and Tao 2020] B. Green and T. Tao, “An arithmetic regularity lemma, associated counting lemma, and applications”, correction, 2020. arXiv 1002.2028v3
- [Green et al. 2012] B. Green, T. Tao, and T. Ziegler, “An inverse theorem for the Gowers $U^{s+1}[N]$ -norm”, *Ann. of Math. (2)* **176**:2 (2012), 1231–1372. MR Zbl
- [Grimmelt 2022] L. Grimmelt, “Vinogradov’s theorem with Fouvry–Iwaniec primes”, *Algebra Number Theory* **16**:7 (2022), 1705–1776. MR Zbl
- [Iwaniec 1972] H. Iwaniec, “Primes of the type $\phi(x, y) + A$ where ϕ is a quadratic form”, *Acta Arith.* **21** (1972), 203–234. MR Zbl

- [Iwaniec and Kowalski 2004] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications **53**, Amer. Math. Soc., 2004. MR Zbl
- [Kane 2013] D. M. Kane, “An asymptotic for the number of solutions to linear equations in prime numbers from specified Chebotarev classes”, *Int. J. Number Theory* **9**:4 (2013), 1073–1111. MR Zbl
- [Li and Pan 2010] H. Li and H. Pan, “A density version of Vinogradov’s three primes theorem”, *Forum Math.* **22**:4 (2010), 699–714. MR Zbl
- [Li and Pan 2019] H. Li and H. Pan, “The Green–Tao theorem for Piatetski–Shapiro primes”, preprint, 2019. arXiv 1901.09372
- [Matomäki and Shao 2017] K. Matomäki and X. Shao, “Vinogradov’s three primes theorem with almost twin primes”, *Compos. Math.* **153**:6 (2017), 1220–1256. MR Zbl
- [Maynard 2016] J. Maynard, “Dense clusters of primes in subsets”, *Compos. Math.* **152**:7 (2016), 1517–1554. MR Zbl
- [Pintz 2010] J. Pintz, “Are there arbitrarily long arithmetic progressions in the sequence of twin primes?”, pp. 525–559 in *An irregular mind*, edited by I. Bárány and J. Solymosi, Bolyai Soc. Math. Stud. **21**, János Bolyai Math. Soc., Budapest, 2010. MR Zbl
- [Pintz 2017] J. Pintz, “Patterns of primes in arithmetic progressions”, pp. 369–379 in *Number theory—Diophantine problems, uniform distribution and applications*, edited by C. Elsholtz and P. Grabner, Springer, 2017. MR Zbl
- [Rimanić and Wolf 2019] L. Rimanić and J. Wolf, “Szemerédi’s theorem in the primes”, *Proc. Edinb. Math. Soc. (2)* **62**:2 (2019), 443–457. MR Zbl
- [Shao 2014] X. Shao, “A density version of the Vinogradov three primes theorem”, *Duke Math. J.* **163**:3 (2014), 489–512. MR Zbl
- [Shao and Teräväinen 2021] X. Shao and J. Teräväinen, “The Bombieri–Vinogradov theorem for nilsequences”, *Discrete Anal.* (2021), art. id. 21. MR Zbl
- [Sun and Pan 2019] Y.-C. Sun and H. Pan, “The Green–Tao theorem for primes of the form $x^2 + y^2 + 1$ ”, *Monatsh. Math.* **189**:4 (2019), 715–733. MR Zbl
- [Tao and Vu 2010] T. Tao and V. H. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics **105**, Cambridge University Press, 2010. MR Zbl
- [Teräväinen 2018] J. Teräväinen, “The Goldbach problem for primes that are sums of two squares plus one”, *Mathematika* **64**:1 (2018), 20–70. MR Zbl
- [Zhou 2009] B. Zhou, “The Chen primes contain arbitrarily long arithmetic progressions”, *Acta Arith.* **138**:4 (2009), 301–315. MR Zbl

Communicated by Ben Green

Received 2021-10-08 Revised 2022-02-21 Accepted 2022-04-11

bienvp@tcd.ie

Institut für Analysis und Zahlentheorie, TU Graz, Kopernikusgasse 24/II, 8010 Graz, Austria

Current address:

School of Mathematics, Trinity College Dublin, Dublin 2, Ireland

xuancheng.shao@uky.edu

Department of Mathematics, University of Kentucky, Lexington, KY, United States

joni.p.teravainen@gmail.com

Mathematical Institute, University of Oxford, Radcliffe Observatory Quarter, Oxford, United Kingdom

Current address:

Department of Mathematics and Statistics, University of Turku, Finland

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in *ANT* are usually in English, but articles written in other languages are welcome.

Length There is no a priori limit on the length of an *ANT* article, but *ANT* considers long articles only if the significance-to-length ratio is appropriate. Very long manuscripts might be more suitable elsewhere as a memoir instead of a journal article.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use L^AT_EX but submissions in other varieties of T_EX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibT_EX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@msp.org with details about how your graphics were generated.

White space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 17 No. 2 2023

Torsion points on elliptic curves over number fields of small degree MAARTEN DERICKX, SHELDON KAMIENNY, WILLIAM STEIN and MICHAEL STOLL	267
Tame fundamental groups of pure pairs and Abhyankar's lemma JAVIER CARVAJAL-ROJAS and AXEL STÄBLER	309
Constructions of difference sets in nonabelian 2-groups T. APPLEBAUM, J. CLIKEMAN, J. A. DAVIS, J. F. DILLON, J. JEDWAB, T. RABBANI, K. SMITH and W. YOLLAND	359
The principal block of a \mathbb{Z}_ℓ -spets and Yokonuma type algebras RADHA KESSAR, GUNTER MALLE and JASON SEMERARO	397
Geometric properties of the Kazhdan–Lusztig Schubert basis CRISTIAN LENART, CHANGJIAN SU, KIRILL ZAINOULLINE and CHANGLONG ZHONG	435
Some refinements of the Deligne–Illusie theorem PIOTR ACHINGER and JUNECUE SUH	465
A transference principle for systems of linear equations, and applications to almost twin primes PIERRE-YVES BIENVENU, XUANCHENG SHAO and JONI TERÄVÄINEN	497