Algebra & Number Theory

Volume 8
2014
No. 4

msp

Algebra & Number Theory

msp.org/ant

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

The subscription price for 2014 is US $225/year for the electronic version, and $400/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers 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. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

ALGEBRA AND NUMBER THEORY 8:4 (2014)
dx.doi.org/10.2140/ant.2014.8.781

The derived moduli space of stable sheaves

Kai Behrend, Ionut Ciocan-Fontanine, Junho Hwang and Michael Rose

We construct the derived scheme of stable sheaves on a smooth projective variety via derived moduli of finite graded modules over a graded ring. We do this by dividing the derived scheme of actions of Ciocan-Fontanine and Kapranov by a suitable algebraic gauge group. We show that the natural notion of GIT stability for graded modules reproduces stability for sheaves.

Introduction

For some years it has been a tenet of geometry that deformation theory problems are governed by differential graded Lie algebras. This leads to formal moduli being given, dually, by differential graded commutative algebras and gives rise to the derived geometry program. Usually, the expectation is that to solve a given *global* moduli problem with a differential graded Lie algebra, this differential graded Lie

MSC2010: 14D20.
Keywords: differential graded schemes, curved differential graded Lie algebras, stable sheaves .

algebra will have to be infinite-dimensional and therefore will be ill-suited for algebraic geometry.

For example, gauge theory can be used to construct analytic moduli spaces of holomorphic vector bundles on a compact complex manifold Y. In the case when the bundles are topologically trivial, the differential graded Lie algebra is $A^{0,\bullet}(Y, M_n)$, the algebra of C^∞-forms of type $(0, \bullet)$ with values in $n \times n$-matrices (or a suitable completion thereof). The differential is the Dolbeault differential, and the bracket is combined from wedge product of forms and commutator bracket of matrices. Almost complex structures are elements $x \in A^{0,1}(Y, M_n)$, and they are integrable if and only if they satisfy the Maurer–Cartan equation

$$dx + \tfrac{1}{2}[x, x] = 0.$$

Dividing the Maurer–Cartan locus by the gauge group $G = A^{0,0}(Y, \mathrm{GL}_n)$, we obtain the moduli space of topologically trivial holomorphic bundles.

One central observation of this paper is that there exists a finite-dimensional analogue of this construction for moduli of coherent sheaves on a smooth projective variety over $\mathbb{C}$. Derived moduli of sheaves have been constructed before (see [Ciocan-Fontanine and Kapranov 2001] or [Toën and Vaquié 2007]), but we believe it is a new observation that there is a finite-dimensional differential graded Lie algebra with an algebraic gauge group, solving this moduli problem globally. Simply by virtue of being the space of Maurer–Cartan elements in a differential graded Lie algebra up to gauge equivalence, the moduli space automatically comes with a derived, or differential graded, structure.

This construction also leads one immediately to the examination of geometric invariant theory (GIT) stability for this algebraic gauge group action. Thus, another result of this paper it that GIT stability for our algebraic gauge group action reproduces the standard notion of stability for sheaves.

Let Y be a smooth projective variety with homogeneous coordinate ring A and $\alpha(t) \in \mathbb{Q}[t]$ a numerical polynomial.

We present a construction of the derived moduli scheme of stable sheaves on Y as a Geometric Invariant Theory quotient of the derived scheme of actions. The derived scheme of actions, $\mathfrak{R}$Act, was introduced by Ciocan-Fontanine and Kapranov [2001] as an auxiliary tool in their construction of the derived scheme of quotients, $\mathfrak{R}$Quot.

The basic idea is to describe a coherent sheaf $\mathscr{F}$ on Y with Hilbert polynomial $\alpha(t)$ in terms of the associated finite-dimensional graded A-module

$$\Gamma_{[p,q]}\mathscr{F} = \bigoplus_{i=p}^{q} \Gamma\big(Y, \mathscr{F}(i)\big),$$

with dimension vector $\alpha|_{[p,q]} = (\alpha(p), \ldots, \alpha(q))$, for $q \gg p \gg 0$. In fact, for any open bounded family $\mathfrak{U}$ of sheaves with Hilbert polynomial $\alpha(t)$ on Y, there exist

$q \gg p \gg 0$, such that

$$\Gamma_{[p,q]} : \mathfrak{U} \longrightarrow \begin{pmatrix} \text{graded } A\text{-modules in } [p,q] \\ \text{with dimension vector } \alpha|_{[p,q]} \end{pmatrix}$$

is an open embedding of moduli functors (i.e., of stacks).

We construct a finite-dimensional differential graded Lie algebra

$$L = \bigoplus_{n=0}^{q-p} L^n$$

together with an algebraic gauge group G (the Lie algebra of G is L^0), acting linearly on L, such that $MC(L)/G$, the quotient of the solution set of the Maurer–Cartan equation

$$dx + \tfrac{1}{2}[x,x] = 0, \quad x \in L^1, \tag{1}$$

by the gauge group, is equal to the set (or rather stack) of graded A-modules concentrated in degrees between p and q with dimension vector $\alpha|_{[p,q]}$, up to isomorphism.

We do this by fixing a finite-dimensional graded vector space V of dimension $\alpha|_{[p,q]}$. Then the degree 1 part of our differential graded Lie algebra is essentially $L^1 = \mathrm{Hom}_{\mathrm{gr}}(A, \mathrm{End}_{\mathbb{C}} V)$, the space of degree preserving $\mathbb{C}$-linear maps from A to $\mathrm{End}_{\mathbb{C}} V$, and the solutions to the Maurer–Cartan equation (1) turn out to be precisely the algebra maps $A \to \mathrm{End}_{\mathbb{C}} V$, that is, the structures of graded A-modules on V. Taking the quotient by the gauge group $G = \mathrm{GL}_{\mathrm{gr}}(V)$ of graded automorphisms of V can be viewed as removing the choice of basis in V.

Equivalently, a family of A-modules can be viewed as a graded vector bundle of rank $\alpha|_{[p,q]}$, that is, a G-torsor, endowed with an A-action. This approach to constructing (derived) moduli of A-modules in these two steps by first constructing moduli of vector bundles, that is, the stack BG, and then a relative (derived) scheme of actions over BG is standard. For example, Toën and Vaquié [2007] use this method to construct moduli of derived category objects.

Our main interest lies in the derived *scheme*, obtained by restricting to stable objects (which are simple) and then removing the automorphism group (which is $\mathbb{C}^*$) by passing to the space underlying the $\mathbb{C}^*$-gerbe.

The quotient L^1/G is an instance of a moduli space of quiver representations. The relevant quiver is directed, which implies that all points of L^1 are unstable for the action of G. Using standard techniques (as in [King 1994]), we modify the action of G on L^1 by a (canonical choice of) character of G to obtain a well-defined GIT problem. Thus we obtain a quasiprojective moduli space $MC(L)^s /\!/ G$ of stable A-modules with a compactification $MC(L)^{ss} /\!/ G$ consisting of semistable A-modules. The key result is the following:

Theorem. *For every bounded family $\mathfrak{U}$ of sheaves on Y with Hilbert polynomial $\alpha(t)$, there exist $q \gg p \gg 0$ such that if $\mathscr{F}$ is a member of $\mathfrak{U}$, then $\mathscr{F}$ is a stable sheaf if and only if $\Gamma_{[p,q]}\mathscr{F}$ is GIT-stable.*

This shows that usual (semi)stability as defined by Simpson [1994] is the natural notion of (semi)stability for sheaves induced from GIT-stability via our construction. Moreover, using the fact that semistable sheaves are bounded and satisfy the valuative criterion for properness, we see that the moduli space of semistable sheaves with Hilbert polynomial $\alpha(t)$ is a union of connected components of the projective scheme $MC(L)^{ss}/\!/G$ of semistable modules.

This gives a new construction of the moduli space of (semi)stable sheaves on a projective variety. One advantage of our approach over others, such as the classical Quot-scheme approach of [Simpson 1994] and [Huybrechts and Lehn 1997] or the Quiver approach of [Álvarez-Cónsul and King 2007], is that Equation (1) provides us with a rather explicit set of equations cutting out the moduli space.

We can also explicitly describe the image of the moduli space of stable sheaves inside the moduli space of $[p,q]$-graded A-modules. Namely, it is the scheme of stable modules whose truncation into an interval $[p',q]$, for suitable p' between p and q, is also stable.

Since $MC(L)/G$ is the moduli space of a differential graded Lie algebra, it (or rather its stable locus) is automatically a differential graded scheme. It is naturally embedded into the smooth stack L^1/G as the "spectrum" of a sheaf of differential graded algebras $\mathscr{R}$ on L^1/G, obtained from the algebra of functions on the affine supermanifold

$$L[1]^{\geq 0},$$

with its induced derivation by descending to the G-quotient. It is this differential graded scheme structure on $MC(L)/G$ which we refer to as a *derived scheme*.

A derived scheme comes with higher obstruction spaces at every point. In our case, the higher obstruction spaces at the sheaf $\mathscr{F}$, or the corresponding point $M = \Gamma_{[p,q]}\mathscr{F}$ of $MC(L)/G$, are given by

$$\operatorname{Ext}^i_{\mathscr{O}_Y}(\mathscr{F},\mathscr{F}) = \operatorname{Ext}^i_A(M,M).$$

The corresponding virtual fundamental class (see [Behrend and Fantechi 1997] and [Ciocan-Fontanine and Kapranov 2009]) is thus the one giving rise to Donaldson–Thomas invariants [Thomas 2000] if Y is Calabi–Yau.

The differential graded Lie algebra L is essentially the degree preserving part of the Hochschild cochain complex

$$L^n = \operatorname{Hom}_{\mathbb{C}}(A^{\otimes n}, \operatorname{End}_{\mathbb{C}} V)$$

of the graded ring A with values in the graded bimodule $\operatorname{End}_{\mathbb{C}} V$, where V is a finite-dimensional graded A-module in degrees from p to q with dimension vector $\alpha|_{[p,a]}$ together with its natural Lie bracket induced from the commutator bracket in $\operatorname{End} V$.

Outline. In Section 1, we construct the derived scheme of finite-dimensional graded A-modules with fixed dimension vector. This works for any algebra over $\mathbb{C}$; in particular, there is no need for commutativity of A. The main purpose of this section is to carefully describe the various differential graded schemes and stacks we construct, and to do this as explicitly as possible in terms of our finite-dimensional differential graded Lie algebra with its gauge group. We hope the introduction of bundles of curved differential graded Lie algebras will clarify the global geometric objects described infinitesimally by differential graded Lie algebras. We also advocate the use of Maurer–Cartan equations as a convenient way to package higher structures, in particular, A_∞-module structures.

Section 2 is devoted to the study of the GIT problem given by the action of the gauge group G on the space L^1. In particular, we construct quasiprojective derived moduli spaces of equivalence classes of stable finite graded A-modules of given dimension vector. We hope there will be applications in noncommutative geometry.

In Section 3 we introduce our projective scheme Y and consider the case where our graded ring A is the homogeneous coordinate ring of Y. We compare the stability notions for sheaves on Y and for graded A-modules. We prove the above theorem and the amplification mentioned.

Finally, in Section 4, we write down the derived moduli problem for sheaves on Y, which is solved by our differential graded scheme. This is the only place where we need Y to be smooth. The reason we need smoothness is to assure that for a coherent sheaf $\mathcal{F}$ on Y, the spaces $\operatorname{Ext}^i_{\mathcal{O}_Y}(\mathcal{F},\mathcal{F})$ vanish for sufficiently large i.

Derived geometry. For us, derived geometry is the geometry of differential graded schemes. We make a few informal remarks here. For more detailed expositions of derived geometry, see Toën–Vezzosi [2004; 2005; 2008] or Lurie [2009].

A *differential graded scheme* is a pair $(T,\mathcal{R}_T)$, where T is a scheme and $\mathcal{R}_T$ is a sheaf of differential graded $\mathbb{C}$-algebras (without restriction on the grading) on T, endowed with a structure morphism of sheaves of algebras $\mathcal{O}_T \to \mathcal{R}_T^0$.

It is natural to require (and we make it part of the definition) that all differential graded schemes $(T,\mathcal{R}_T)$ satisfy $\mathcal{O}_T = \mathcal{Z}^0(\mathcal{R}_T)$, where $\mathcal{Z}^0(\mathcal{R}_T) = \ker(d:\mathcal{R}_T^0 \to \mathcal{R}_T^1)$ is the sheaf of 0-cycles in $\mathcal{R}_T$. This implies that $\mathcal{R}_T$ is a sheaf of differential graded $\mathcal{O}_T$-algebras. Then a *morphism* of differential graded schemes $(T,\mathcal{R}_T)\to(M,\mathcal{R}_M)$ is a pair (ϕ,μ), where $\phi: T\to M$ is a morphism of schemes, and $\mu:\phi^*\mathcal{R}_M\to\mathcal{R}_T$ is a morphism of sheaves of differential graded $\mathcal{O}_T$-algebras.

The *classical scheme* associated to a differential graded scheme $(T,\mathcal{R}_T)$ is the closed subscheme of T given by $\pi_0(T,\mathcal{R}_T) = \operatorname{Spec}_{\mathcal{O}_T} h^0(\mathcal{R}_T)$.

A differential graded scheme is *affine* if it comes from a differential graded algebra which is free as a graded algebra, on a finite set of generators, all in nonpositive degree.

Differential graded schemes form a category. (One may replace morphisms by germs of morphisms, defined in suitable neighborhoods of the classical loci.) This category is enriched over simplicial sets: the n-simplices in $\mathrm{Hom}(X, Y)$ are the morphisms $X \times \Delta_n \to Y$, where Δ_n is the differential graded scheme (which is not affine) corresponding to the differential graded algebra of algebraic differential forms on the algebraic n-simplex.

The category of differential graded schemes also has a natural topology: the étale topology, in which a family $U_i \to U$ is a covering family if $\pi_0(U_i) \to \pi_0(U)$ is a covering family in the usual étale topology, and every $U_i \to U$ is an étale morphism, which means that $\pi_0(U_i) \to \pi_0(U)$ is étale in the usual sense, and

$$h^r(\mathscr{R}_{U_i}) = h^r(\mathscr{R}_U) \otimes_{h^0(\mathscr{R}_U)} h^0(\mathscr{R}_{U_i}) \quad \text{for all } r.$$

A morphism of differential graded schemes is a *quasiisomorphism* if it is étale, and induces an isomorphism on π_0.

In analogy with the definition of algebraic spaces, one can define a derived scheme (or space) to be a simplicial presheaf X on the category of differential graded schemes satisfying two properties:

(i) (sheaf property) For every hypercover $U_\bullet \to U$, the map

$$X(U) \to \operatorname{hocolim} X(U_\bullet)$$

is a weak equivalence.

(ii) (locally affine property) X is étale locally weakly equivalent to a presheaf represented by an affine differential graded scheme.

The simplicial category of derived schemes localizes the differential graded schemes at the quasiisomorphisms.

A particularly nice class of differential graded schemes comes from bundles of curved differential graded Lie algebras on smooth schemes (see the beginning of Section 1B). Our main object of study, $\mathfrak{R}\widetilde{\mathfrak{M}}\mathrm{od}_\alpha^{\mathrm{sp}}(A) = (\widetilde{\mathfrak{M}}^{\mathrm{sp}}, \mathscr{R})$ is of this form.

We find it plausible (this will be proved elsewhere) that differential graded schemes coming from bundles of curved differential graded Lie algebras represent simplicial presheaves satisfying the above two properties (at least if we restrict the underlying base category to affine objects). Therefore, the moduli functor represented by such a "nice" differential graded scheme, in the derived world, would be given directly by the functor it represents over the category of differential graded schemes as defined here. This is the moduli functor we examine.

Index of notation

A	A graded ring.
$\mathfrak{m}$	The maximal ideal of positive degree elements in A.
α	Depending on the context, either a numerical polynomial $\alpha(t) \in \mathbb{Q}[t]$ or a dimension vector $(\alpha_p, \dots, \alpha_q)$.
V	A graded vector space of dimension $\alpha = (\alpha_p, \dots, \alpha_q)$.
L	$L^n = \mathrm{Hom}_{\mathrm{gr}}(\mathfrak{m}^{\otimes n}, \mathrm{End}\, V)$, the differential graded Lie algebra; see Section 1A.
M	The scheme L^1.
X	The Maurer–Cartan locus in M.
$\mathcal{R}_M$	The sheaf of differential graded algebras on M; see Section 1B.
$\mathrm{Act}_{\mathrm{gr}}(A, V)$	The scheme X, when it is viewed as representing the scheme of graded actions of A on V.
$\mathfrak{R}\mathrm{Act}_{\mathrm{gr}}(A, V)$	The differential graded scheme $(M, \mathcal{R}_M)$, which is the derived scheme of actions.
G	The gauge group $G = \prod_{i=p}^{q} \mathrm{GL}(V_i)$.
Δ	The one-parameter subgroup of scalars in G.
$\widetilde{G}$	The quotient group G/Δ.
$\mathfrak{M}$	The quotient stack $[M/G]$.
$\widetilde{\mathfrak{M}}$	The quotient stack $[M/\widetilde{G}]$.
$\widetilde{\mathfrak{M}}^{\mathrm{sp}}$	The open substack of $\widetilde{\mathfrak{M}}$, which is an algebraic space.
$\mathfrak{X}$	The Maurer–Cartan locus in $\mathfrak{M}$.
$\widetilde{\mathfrak{X}}$	The Maurer–Cartan locus in $\widetilde{\mathfrak{M}}$.
$\mathfrak{Mod}_\alpha(A)$	The algebraic stack $\mathfrak{X}$, when it is viewed as the stack of graded A-modules of dimension α.
$\mathfrak{R}\mathfrak{Mod}_\alpha(A)$	The differential graded stack $(\mathfrak{M}, \mathcal{R}_{\mathfrak{M}})$, which is the derived stack of graded modules.
$\widetilde{\mathfrak{Mod}}{}^{\mathrm{sp}}_\alpha(A)$	The algebraic space $\widetilde{\mathfrak{X}}$, when viewed as the space of equivalence classes of simple graded modules.
$\mathfrak{R}\widetilde{\mathfrak{Mod}}{}^{\mathrm{sp}}_\alpha(A)$	The differential graded algebraic space $(\widetilde{\mathfrak{M}}^{\mathrm{sp}}, \mathcal{R})$, which is the derived space of equivalence classes of simple modules.
$\mathfrak{R}\widetilde{\mathfrak{Mod}}{}^{s}_\alpha(A)$	The stable locus inside $\mathfrak{R}\widetilde{\mathfrak{Mod}}{}^{\mathrm{sp}}_\alpha(A)$.
$\mathfrak{R}\widetilde{\mathfrak{Mod}}{}^{\mathrm{sp}}_\alpha(\mathcal{O}_Y)$	The functor of equivalence classes of simple families of coherent sheaves on Y with Hilbert polynomial $\alpha(t)$ parametrized by differential graded schemes.
$\mathfrak{R}\widetilde{\mathfrak{Mod}}{}^{s}_\alpha(\mathcal{O}_Y)$	The stable locus inside $\mathfrak{R}\widetilde{\mathfrak{Mod}}{}^{\mathrm{sp}}_\alpha(\mathcal{O}_Y)$.

Notation and conventions. We work over a field of characteristic zero, which we shall denote by $\mathbb{C}$. All tensor products are over $\mathbb{C}$, unless indicated otherwise. All our differential graded algebras (and sheaves thereof), are graded commutative with unit.

Cohomology sheaves (of a complex of sheaves $\mathscr{E}^\bullet$) we usually denote by $h^i(\mathscr{E})$.

1. The derived scheme of simple graded modules

Let A be a unital graded $\mathbb{C}$-algebra, *not necessarily commutative*, which is all in nonnegative degrees, and such that each graded piece is finite-dimensional. Moreover, we assume that the degree zero piece is one-dimensional, hence equal to $\mathbb{C}$. We denote by $\mathfrak{m}$ the ideal of elements of positive degree in A. Note that $\mathfrak{m}$ is a positively graded algebra without unit. We refer to the grading on A as the *internal* or *projective* grading if there is a fear of confusion. We indicate this grading with lower indices.

Our main example of interest is that A is the homogeneous coordinate ring of a projective variety over $\mathbb{C}$.

A graded A-module is the same thing as a graded $\mathfrak{m}$-module. The advantage of working with $\mathfrak{m}$ is that there is only one module axiom: associativity.

1A. ***The differential graded Lie algebra L.*** Let V be a graded and finite-dimensional vector space

$$V = \bigoplus_{i=p}^{q} V_i .$$

By $\operatorname{End} V$ we denote the algebra of $\mathbb{C}$-linear endomorphisms of V. It inherits a grading from V. Only $\operatorname{End}_i V$ in the range $i \in [p-q, q-p]$ are nonzero.

We denote the dimension vector of V by

$$\alpha = (\alpha_p, \dots, \alpha_q) = (\dim V_p, \dots, \dim V_q).$$

The graded vector space. We consider

$$L^n = \operatorname{Hom}_{\mathrm{gr}}(\mathfrak{m}^{\otimes n}, \operatorname{End} V),$$

the vector space of degree-preserving $\mathbb{C}$-linear maps $\mu : \mathfrak{m}^{\otimes n} \to \operatorname{End} V$, and

$$L = \bigoplus_{n=0}^{\infty} L^n .$$

Thus, $L^0 = \operatorname{End}_{\mathrm{gr}} V$ and $L^1 = \operatorname{Hom}_{\mathrm{gr}}(\mathfrak{m}, \operatorname{End} V)$. We write elements $\mu \in L^n$ as multilinear maps $\mathfrak{m}^{\times n} \to \operatorname{End} V$. To distinguish the grading on L from the projective grading, we may sometimes refer to it as the *external grading*. It is always indicated by upper indices.

Note that every L^n is finite-dimensional and that $L^n = 0$, unless n is in the range $n \in [0, q-p]$ because $\mathfrak{m}$ is positively graded.

Each L^n is bigraded projectively:

$$L^n = \bigoplus_{\substack{q \geq i \geq j \geq p \\ i-j \geq n}} L^n_{ij},$$

where

$$L^n_{ij} = \operatorname{Hom}\big((\mathfrak{m}^{\otimes n})_{i-j}, \operatorname{Hom}(V_j, V_i)\big).$$

For $n = 0$, this simplifies to

$$L^0 = \bigoplus_{i=p}^{q} L^0_{ii}, \quad L^0_{ii} = \operatorname{Hom}(V_i, V_i),$$

and for $n = 1$, we can write

$$L^1 = \bigoplus_{q \geq i > j \geq p} L^1_{ij}, \quad L^1_{ij} = \operatorname{Hom}\big(\mathfrak{m}_{i-j}, \operatorname{Hom}(V_j, V_i)\big).$$

We say that L^0 is diagonal, and L^1 is strictly lower triangular. The higher L^n are restricted to successively smaller southwest corners.

The gauge group. We let $G = \mathrm{GL}_{\mathrm{gr}}(V)$ be the group of degree-preserving linear automorphisms of V and call it the *gauge group*. Of course, L^0 is the Lie algebra of G. The gauge group is graded:

$$G = \prod_{i=p}^{q} G_i, \quad G_i = \mathrm{GL}(V_i).$$

It acts, from the left, via conjugation on L. More precisely, for $g \in G$ and $\mu \in L^n$, we have

$$(g \cdot \mu)(a_1, \ldots, a_n) = g \circ \mu(a_1, \ldots, a_n) \circ g^{-1}. \tag{2}$$

The action of G on L^n preserves the double grading: if $g = (g_p, \ldots, g_q)$ and $\mu \in L^n$, then

$$(g \cdot \mu)_{ij} = g_i \mu_{ij} g_j^{-1}. \tag{3}$$

We call this action the *gauge action*. The group G contains the scalars, $\Delta : \mathbb{C}^* \to G$, $t \mapsto (t, \ldots, t)$, which act trivially. This leads us to also consider the quotient group $\widetilde{G} = G/\Delta$.

The differential. Define $d : L^n \to L^{n+1}$ by the formula

$$d\mu(a_1, \dots, a_{n+1}) = \sum_{i=1}^{n} (-1)^{n-i} \mu(\dots, a_i a_{i+1}, \dots)$$

For example, $d : L^0 \to L^1$ is equal to zero, and $d : L^1 \to L^2$ is given by $d\mu(a, b) = \mu(ab)$.

Of course, $d^2 = 0$. The gauge action preserves the differential. The differential preserves the projective double grading. Note that the gauge group action on L^1 is not modified by a gauge term because $d : L^0 \to L^1$ vanishes.

The complex (L, d) is the subcomplex of internal degree zero of the Hochschild complex of the $\mathbb{C}$-algebra $\mathfrak{m}$ with values in the bimodule $\operatorname{End} V$, where $\operatorname{End} V$ has the trivial (i.e., zero) module structure.

The bracket. For $\mu \in L^m$ and $\mu' \in L^n$ define $\mu \circ \mu' \in L^{m+n}$ by the formula

$$\mu \circ \mu' \,(a_1, \dots, a_{m+n}) = (-1)^{mn} \mu(a_1, \dots, a_m) \circ \mu'(a_{m+1}, \dots, a_{m+n}).$$

An easy sign calculation shows that this operation is associative.

Then, for $\mu \in L^m$ and $\mu' \in L^n$ define $[\mu, \mu'] \in L^{m+n}$ by

$$[\mu, \mu'] = \mu \circ \mu' - (-1)^{mn} \mu' \circ \mu.$$

This operation automatically satisfies the graded Jacobi identity because it is defined as the graded commutator of an associative product.

We can write out the formula for the bracket:

$$\begin{aligned}[\mu, \mu'](a_1, \dots, a_{m+n}) = (-1)^{mn} \mu(a_1, \dots, a_m) \circ \mu'(a_{m+1}, \dots, a_{m+n}) \\ - \mu'(a_1, \dots, a_n) \circ \mu(a_{n+1}, \dots, a_{m+n}).\end{aligned}$$

For example, if $\mu, \mu' \in L^1$, then

$$[\mu, \mu'](a, b) = -\mu(a) \circ \mu'(b) - \mu'(a) \circ \mu(b).$$

The differential d acts as a derivation with respect to the bracket $[\,\cdot\,, \cdot\,]$, that is, for $\mu \in L^m$ and $\mu' \in L^n$, we have

$$d[\mu, \mu'] = [d\mu, \mu'] + (-1)^m [\mu, d\mu'].$$

Thus $(L, d, [\,\cdot\,, \cdot\,])$ is a differential graded Lie algebra.

The gauge group G acts by automorphisms of the differential graded Lie algebra structure on L. This means that we have

$$d(g \cdot \mu) = g \cdot d\mu \quad \text{and} \quad g \cdot [\mu, \mu'] = [g \cdot \mu, g \cdot \mu'].$$

The derivative of the gauge action of G on L is the adjoint action of L^0 on L.

Remark 1.1. The more basic object than L is the truncation $L^{>0} = \tau_{>0}L$, together with G and its gauge action. The differential graded Lie algebra L can be recovered from $(L^{>0}, G)$.

The Maurer–Cartan equation. The Maurer–Cartan equation is

$$d\mu + \tfrac{1}{2}[\mu, \mu] = 0 \quad \text{for } \mu \in L^1.$$

We call $\mu \in L^1$ a *Maurer–Cartan element* if it satisfies this equation. We denote the set of Maurer–Cartan elements by $MC(L)$.

For $\mu \in L^1$, we have $\frac{1}{2}[\mu, \mu] = \mu \circ \mu$, and so μ is a Maurer–Cartan element if and only if

$$d\mu + \mu \circ \mu = 0,$$

or, equivalently, if for all $a, b \in \mathfrak{m}$,

$$\mu(ab) = \mu(a) \circ \mu(b).$$

If we write out this equation degreewise, we get for all $i > k > j$, $a \in \mathfrak{m}_{i-k}$ and $b \in \mathfrak{m}_{k-j}$, the equation $\mu_{ij}(ab) = \mu_{ik}(a) \circ \mu_{kj}(b)$.

Thus $\mu \in L^1$ is a Maurer–Cartan element if and only if it defines a left action of $\mathfrak{m}$ on V. Dividing by the gauge action removes the choice of basis in V. It follows immediately that Maurer–Cartan elements up to gauge equivalence are graded $\mathfrak{m}$-modules up to isomorphism, whose underlying graded vector space is isomorphic to V. We can make this claim precise:

Remark 1.2. Let $[MC(L)/G]$ be the (set-theoretic) transformation groupoid associated to the gauge group action on the Maurer–Cartan elements. Let $(\mathfrak{m}\text{-modules})_\alpha$ denote the category of graded $\mathfrak{m}$-modules with dimension vector α with only isomorphisms. Then we have an equivalence of groupoids

$$[MC(L)/G] \longrightarrow (\mathfrak{m}\text{-modules})_\alpha,$$

given by mapping μ to the $\mathfrak{m}$-module structure it defines on V and mapping an element of G to the isomorphism of $\mathfrak{m}$-module structures it represents. We will turn this into a geometric statement.

1B. ***The moduli stack of L.*** The following construction of the differential graded moduli stack works for any finite-dimensional differential graded Lie algebra concentrated in nonnegative degrees with algebraic gauge group.

Bundles of curved differential graded Lie algebras.

Definition 1.3. A *bundle of curved differential graded Lie algebras* over a scheme (or a stack) M is a graded vector bundle $\mathscr{L}^*$ over M, endowed with three pieces of data:

(i) a section $f \in \Gamma(M, \mathscr{L}^2)$,

(ii) an $\mathcal{O}_M$-linear map of degree one $\delta : \mathscr{L}^* \to \mathscr{L}^*$,

(iii) a $\mathcal{O}_M$-linear alternating bracket of degree zero $[\,\cdot\,,\cdot\,] : \Lambda^2 \mathscr{L}^* \to \mathscr{L}^*$,

subject to four axioms:

(i) $\delta(f) = 0$, as a section of $\mathscr{L}^3$,

(ii) $\delta \circ \delta = [f, \cdot\,]$,

(iii) δ is a graded derivation with respect to the bracket $[\,\cdot\,,\cdot\,]$,

(iv) the bracket $[\,\cdot\,,\cdot\,]$ satisfies the graded Jacobi identity.

A bundle of curved differential graded Lie algebras is a bundle of differential graded Lie algebras only if $f = 0$. All of our bundles of curved differential graded Lie algebras will be concentrated in degrees ≥ 2. The section f is the curving, and the map δ will be referred to as the *twisted differential*.

It will be useful to relax the conditions somewhat and call a *sheaf* of curved differential graded Lie algebras on M a graded sheaf of $\mathcal{O}_M$-algebras, endowed with the same data (i) to (iii), subject to the same constraints (i) to (iv). Sheaves of curved differential graded Lie algebras will also be allowed to have contributions in degrees less than 2. The sheaf of Maurer–Cartan elements of a sheaf of curved differential graded Lie algebras is the preimage of $-f$ under the curvature map $\mathscr{L}^1 \to \mathscr{L}^2$ given by $x \mapsto \delta x + \frac{1}{2}[x, x]$. If $\mathscr{L}$ is a bundle (so that $\mathscr{L}^1 = 0$), then the Maurer–Cartan locus is the scheme-theoretic vanishing locus of f in M.

If $\mathscr{L}$ is a bundle of curved differential graded Lie algebras on M and $\mathscr{R}_M$ a sheaf of differential graded $\mathcal{O}_M$-algebras, then $\mathscr{L} \otimes_{\mathcal{O}_M} \mathscr{R}_M$ is in a natural way a sheaf of curved differential graded Lie algebras.

We do not define the notion of morphism of bundles or sheaves of curved differential graded Lie algebras. More relevant is the notion of morphism of differential graded scheme, which, as we shall see, applies to bundles of curved differential graded Lie algebras.

Associated differential graded scheme or stack. To a bundle of curved differential graded Lie algebras over M we associate a sheaf of differential graded algebras $\mathscr{R}_M$ by letting the underlying sheaf of graded $\mathcal{O}_M$-algebras be

$$\mathscr{R}_M^* = \operatorname{Sym}_{\mathcal{O}_M} \mathscr{L}[1]^\vee, \tag{4}$$

the sheaf of free graded commutative $\mathcal{O}_M$-algebras with unit on the (homologically) shifted dual of $\mathscr{L}$.

The bracket defines a morphism $q_2 : \mathscr{L}[1]^\vee \to \operatorname{Sym}^2_{\mathcal{O}_M} \mathscr{L}[1]^\vee$, the twisted differential a morphism $q_1 : \mathscr{L}[1]^\vee \to \operatorname{Sym}^1_{\mathcal{O}_M} \mathscr{L}[1]^\vee = \mathscr{L}[1]^\vee$ and the curving a morphism $q_0 : \mathscr{L}[1]^\vee \to \operatorname{Sym}^0_{\mathcal{O}_M} \mathscr{L}[1]^\vee = \mathcal{O}_M$. All three morphisms q_i have homological degree

$+1$, and all three extend uniquely to $\mathcal{O}_M$-linear derivations $q_i : \mathcal{R}_M \to \mathcal{R}_M$. Let $q = q_0 + q_1 + q_2$ be the sum of these three derivations. The four axioms of curved differential graded Lie algebra translate into the one condition

$$q^2 = 0$$

for the derivation q on $\mathcal{R}_M$. This defines the differential graded scheme $(\mathcal{R}_M, q)$. We will usually suppress q from the notation.

Note that $X = Z(f) \subset M$, the scheme theoretic vanishing locus of f (the Maurer–Cartan locus), is equal to the subscheme of M defined by the image of $\mathcal{R}^{-1}$ in $\mathcal{R}^0_M = \mathcal{O}_M$. The structure sheaf of X is $\mathcal{O}_X = h^0(\mathcal{R}_M)$.

Example 1.4. Given a finite-dimensional differential graded Lie algebra L, concentrated in degrees > 0, we let $M = L^1 = \operatorname{Spec}\operatorname{Sym}(L^{1\vee})$. Over M we consider for every $i \geq 2$ the trivial vector bundle $\mathcal{L}^i$ with fiber L^i, that is, $\mathcal{L}^i = L^i \times M$. The curvature map $f : L^1 \to L^2$ given by $f(x) = dx + \frac{1}{2}[x, x]$ gives rise to a section of $\mathcal{L}^2$ over M, the twisted differential $\delta = d^\mu : \mathcal{L}^i \to \mathcal{L}^{i+1}$ is defined by the formula $\delta(y) = d^\mu(y) = dy + [\mu, y]$ in the fiber over $\mu \in M = L^1$, and the bracket on $\mathcal{L}$ is constant, that is, equal to the bracket on L in every fiber of $\mathcal{L}$. In this way the differential graded Lie algebra $L = L^{\geq 1}$ gives rise to a bundle of differential graded Lie algebras $\mathcal{L} = \mathcal{L}^{\geq 2}$ over $M = L^1$.

Note that $X = Z(f) \subset M$ is identified with the scheme theoretic Maurer–Cartan locus of L.

If an algebraic group G acts on L by automorphisms of the differential graded Lie algebra structure, the bundle of curved differential graded Lie algebras $\mathcal{L}$ over M inherits a G-action covering the G-action on M (this is just the diagonal action). Thus, the bundle of curved differential graded Lie algebras $\mathcal{L}$ descends to the quotient stack $[M/G]$.

We apply these considerations to the truncation of our differential graded Lie algebra $L^{>0}$ with the gauge group action by G. We obtain a bundle of curved differential graded Lie algebras $\mathcal{L}_{\mathfrak{M}}$ over $\mathfrak{M} = [M/G]$ and a sheaf of differential graded algebras $\mathcal{R}_{\mathfrak{M}}$ over $\mathfrak{M}$.

If we replace G by $\widetilde{G}$, we obtain a bundle of curved differential graded Lie algebras $\mathcal{L}_{\widetilde{\mathfrak{M}}}$ over $\widetilde{\mathfrak{M}} = [M/\widetilde{G}]$ and a sheaf of differential graded algebras $\mathcal{R}_{\widetilde{\mathfrak{M}}}$ over $\widetilde{\mathfrak{M}}$. The Maurer–Cartan locus $X = Z(f) \subset M$ descends to closed substacks $\mathfrak{X} \subset \mathfrak{M}$ and $\widetilde{\mathfrak{X}} \subset \widetilde{\mathfrak{M}}$ such that $\mathcal{O}_{\mathfrak{X}} = h^0(\mathcal{R}_{\mathfrak{M}})$ and $\mathcal{O}_{\widetilde{\mathfrak{X}}} = h^0(\mathcal{R}_{\widetilde{\mathfrak{M}}})$.

Remark 1.5. There is a natural morphism $\mathfrak{M} \to \widetilde{\mathfrak{M}}$, making $\mathfrak{M}$ a $\mathbb{C}^*$-gerbe over $\widetilde{\mathfrak{M}}$. This gerbe is trivial if there exists a line bundle ξ over M and a lifting of the G-action to a G-action on ξ such that Δ acts by scalar multiplication on the fibers of ξ.

The associated functor on differential graded schemes. Suppose the differential graded scheme $(M, \mathcal{R}_M)$ comes from a bundle of curved differential graded Lie algebras as in Equation (4). Given a morphism of schemes $\phi : T \to M$, the sheaf of Maurer–Cartan elements of $\phi^*\mathcal{L} \otimes_{\mathcal{O}_T} \mathcal{R}_T$ is naturally isomorphic to the sheaf of morphisms of differential graded $\mathcal{O}_T$-algebras $\phi^*\mathcal{R}_M \to \mathcal{R}_T$.

$$MC(\phi^*\mathcal{L} \otimes_{\mathcal{O}_T} \mathcal{R}_T) = \mathrm{Mor}_{\mathcal{O}_T}(\phi^* \operatorname{Sym}_{\mathcal{O}_M} \mathcal{L}[1]^\vee, \mathcal{R}_T).$$

In particular, a morphism of differential graded schemes $(T, \mathcal{R}_T) \to (M, \mathcal{R}_M)$ is essentially the same thing as a pair (ϕ, μ), where $\phi : T \to M$ is a morphism of schemes and μ is a global Maurer–Cartan element of the sheaf of curved differential graded Lie algebras $\phi^*\mathcal{L} \otimes_{\mathcal{O}_T} \mathcal{R}_T$.

Lemma 1.6. *If $(M, \mathcal{R}_M)$ comes as in Example 1.4 from a differential graded Lie algebra $L = L^{\geq 1}$, then a morphism $(T, \mathcal{R}_T) \to (M, \mathcal{R}_M)$ is the same thing as a global Maurer–Cartan element in the sheaf of differential graded Lie algebras $L \otimes_{\mathbb{C}} \mathcal{R}_T$.*

Proof. Start with a morphism of differential graded schemes

$$(\phi, \mu) : (T, \mathcal{R}_T) \to (M, \mathcal{R}_M),$$

where we think of μ as a global Maurer–Cartan element in the sheaf of curved differential graded Lie algebras $\phi^*\mathcal{L} \otimes_{\mathcal{O}_Y} \mathcal{R}_T$. The underlying morphism of schemes $\phi : T \to L^1$ can be considered as a section of $L^1 \otimes \mathcal{Z}^0(\mathcal{R}_T)$ over T and hence as a degree 1 section of $L \otimes \mathcal{R}_T$. The section μ can also be thought of as a degree 1 section $L \otimes \mathcal{R}_T$, and it is not hard to check that $\mu + \phi$ is a Maurer–Cartan section of the sheaf of differential graded Lie algebras $L \otimes \mathcal{R}_T$. Conversely, every Maurer–Cartan section of $L \otimes \mathcal{R}_T$ gives rise to a pair (ϕ, μ) and hence to a morphism of differential graded schemes $(T, \mathcal{R}_T) \to (M, \mathcal{R}_M)$. □

Finally, if G acts on L by automorphisms and $\mathfrak{M} = [M/G]$, then a morphism $(T, \mathcal{R}_T) \to (\mathfrak{M}, \mathcal{R}_{\mathfrak{M}})$ is *essentially* the same thing as a pair (E, μ), where E is a principal G-bundle over T, and μ is a global Maurer–Cartan element of the sheaf of differential graded Lie algebras ${}^{E}L \otimes_{\mathcal{O}_T} \mathcal{R}_T$. Here ${}^{E}L$ denotes the associated vector bundle with its induced structure of sheaf of differential graded Lie algebras over $\mathcal{O}_T$.

The derived scheme of actions. We apply these considerations to the differential graded Lie algebra

$$L^{\geq 1} = \mathrm{Hom}_{\mathrm{gr}}(\mathfrak{m}^{\otimes \geq 1}, \operatorname{End} V).$$

Let $(M, \mathcal{R}_M)$ be the differential graded scheme associated as in Example 1.4 to $L^{\geq 1} = \mathrm{Hom}_{\mathrm{gr}}(\mathfrak{m}^{\otimes \geq 1}, \operatorname{End} V)$. So $M = \mathrm{Hom}_{\mathrm{gr}}(\mathfrak{m}, \operatorname{End} V)$. The following is essentially Proposition (3.5.2) of [Ciocan-Fontanine and Kapranov 2001]. (See the same work for the definition of A_∞-action.)

Proposition 1.7. *Suppose $(T, \mathcal{R}_T)$ is a differential graded scheme. A morphism $(T, \mathcal{R}_T) \to (M, \mathcal{R}_M)$ is the same thing as a Maurer–Cartan element in the differential graded Lie algebra*

$$\Gamma\big(T, \operatorname{Hom}(\mathfrak{m}^{\otimes \geq 1}, \operatorname{End} V) \otimes \mathcal{R}_T\big).$$

This, in turn, is the same thing as a graded $\mathcal{R}_T$-linear A_∞-action of $\mathfrak{m} \otimes \mathcal{R}_T$ on $V \otimes \mathcal{R}_T$ or a graded unital *$\mathcal{R}_T$-linear A_∞-action of $A \otimes \mathcal{R}_T$ on $V \otimes \mathcal{R}_T$.*

This justifies calling $(M, \mathcal{R}_M)$ the *derived scheme of graded actions* of A on V and denoting it by $\mathfrak{R}\mathrm{Act}_{\mathrm{gr}}(A, V)$.

The derived stack of modules. Let $(\mathfrak{M}, \mathcal{R}_{\mathfrak{M}})$ be the differential graded stack obtained from $(M, \mathcal{R}_M)$ by dividing by G, and let $\mathfrak{X} \subset \mathfrak{M}$ be the Maurer–Cartan locus.

Proposition 1.8. *Suppose $(T, \mathcal{R}_T)$ is a differential graded scheme. A morphism $(T, \mathcal{R}_T) \to (\mathfrak{M}, \mathcal{R}_{\mathfrak{M}})$ is the same thing as a pair (E, μ), where $E = \bigoplus_{i=p}^{q} E_i$ is a graded vector bundle of dimension vector α over T, and μ is a Maurer–Cartan element in the differential graded Lie algebra*

$$\Gamma\big(T, \mathcal{H}om_{\mathrm{gr}}(\mathfrak{m}^{\otimes \geq 1}, \mathcal{E}nd_{\mathcal{O}_T} E) \otimes_{\mathcal{O}_T} \mathcal{R}_T\big).$$

Such a Maurer–Cartan element μ is the same thing as a graded $\mathcal{R}_T$-linear A_∞-action of $\mathfrak{m} \otimes \mathcal{R}_T$ on $E \otimes_{\mathcal{O}_T} \mathcal{R}_T$, or a graded unital *$\mathcal{R}_T$-linear A_∞-action of $A \otimes \mathcal{R}_T$ on $E \otimes_{\mathcal{O}_T} \mathcal{R}_T$.*

In particular, if T is a classical scheme, a morphism $T \to (\mathfrak{M}, \mathcal{R}_{\mathfrak{M}})$ is the same thing as a morphism $T \to \mathfrak{X}$, which, in turn, is the same thing as a graded vector bundle over T of dimension α, endowed with the structure of a sheaf of graded $\mathfrak{m} \otimes \mathcal{O}_T$-modules or the structure of a sheaf of graded unital *$A \otimes \mathcal{O}_T$-modules.*

There is a universal family over $(\mathfrak{M}, \mathcal{R}_{\mathfrak{M}})$. It is obtained from $V \otimes \mathcal{O}_M$ with its tautological A_∞-action

$$\boldsymbol{\mu} : \mathfrak{m} \otimes V \otimes \mathcal{R}_M \longrightarrow V \otimes \mathcal{R}_M,$$

by descent: the group G acts naturally on V in a way respecting $\boldsymbol{\mu}$.

We call $(\mathfrak{M}, \mathcal{R}_{\mathfrak{M}})$ the *derived stack of graded A-modules* with dimension vector α, and use the notation $\mathfrak{R}\mathfrak{M}\mathrm{od}_\alpha(A) = (\mathfrak{M}, \mathcal{R}_{\mathfrak{M}})$. For the underlying classical stack $\mathfrak{X}$, we write $\mathfrak{M}\mathrm{od}_\alpha(A) = \mathfrak{X}$.

1C. ***The derived space of equivalence classes of simple modules.*** When dividing by $\widetilde{G}$ instead of G, we have to be more careful because the natural action of G on V does not factor through $\widetilde{G}$ as the scalars in G do not act trivially on V. This implies that the universal family of graded A-modules does not descend from $\mathfrak{M}$ to $\widetilde{\mathfrak{M}}$. The obstruction is the $\mathbb{C}^*$-gerbe of Remark 1.5.

Equivalence of simple modules. A *family of graded A-modules* of dimension α parametrized by the scheme T is a graded vector bundle with rank vector α on T together with a unital graded $\mathcal{O}_T$-linear action of $A \otimes \mathcal{O}_T$.

Definition 1.9. A family E of graded A-modules parametrized by T is *simple* if the sheaf of endomorphisms of E is equal to $\mathcal{O}_T$. Two simple families of graded A-modules E, F, parametrized by T are *equivalent*, if there exists a line bundle $\mathscr{L}$ on T, such that F is isomorphic to $E \otimes_{\mathcal{O}_T} \mathscr{L}$, as a family of graded A-modules.

Equivalence classes of simple families of graded A-modules form a presheaf on the site of $\mathbb{C}$-schemes with the étale topology, whose associated sheaf we denote by $\widetilde{\mathfrak{M}}\mathrm{od}_\alpha^{\mathrm{sp}}(A)$.

Let $M^{\mathrm{sp}} \subset M$ be the open subscheme of points with trivial $\widetilde{G}$-stabilizer, and $X^{\mathrm{sp}} = X \cap M$ the intersection with the Maurer–Cartan locus X. Denote by $\widetilde{\mathfrak{M}}^{\mathrm{sp}} \subset \widetilde{\mathfrak{M}}$ and $\widetilde{\mathfrak{X}}^{\mathrm{sp}} \subset \widetilde{\mathfrak{X}}$ the quotients by $\widetilde{G}$.

Remark 1.10. The sheaf $\widetilde{\mathfrak{M}}\mathrm{od}_\alpha^{\mathrm{sp}}(A)$ is isomorphic to the algebraic space $\widetilde{\mathfrak{X}}^{\mathrm{sp}}$.

$$\widetilde{\mathfrak{M}}\mathrm{od}_\alpha^{\mathrm{sp}}(A) = \widetilde{\mathfrak{X}}^{\mathrm{sp}}$$

This proves that $\widetilde{\mathfrak{M}}\mathrm{od}_\alpha^{\mathrm{sp}}(A)$ is algebraic, and gives a modular interpretation of $\widetilde{\mathfrak{X}}^{\mathrm{sp}}$.

Coprime case.

Proposition 1.11. *Suppose that the components of the dimension vector α are coprime. Then the gerbe of Remark 1.5 is trivial. Moreover, the presheaf of equivalence classes of simple families of graded A-modules is a sheaf. In other words, for any $\mathbb{C}$-scheme T, the T-points of the algebraic space $\widetilde{\mathfrak{M}}\mathrm{od}_\alpha^{\mathrm{sp}}(A)$ correspond one-to-one to equivalence classes of simple families. In particular, $\widetilde{\mathfrak{M}}\mathrm{od}_\alpha^{\mathrm{sp}}(A)$ admits a universal family of simple graded A-modules.*

Proof. There exist integers n_i such that $\sum_{i=p}^q n_i\alpha_i = 1$. The character $\rho : G \to \mathbb{C}^*$ given by $\rho(g) = \prod_{i=p}^q \det(g_i)^{n_i}$ satisfies $\langle \Delta, \rho \rangle = 1$. So twisting the action of G on V by ρ^{-1}, the twisted action factors through $\widetilde{G}$, and so after the twist, V descends to $\widetilde{\mathfrak{M}}$. □

Remark 1.12. If

$$\alpha(t) = a_0\binom{t}{0} + a_1\binom{t}{1} + \cdots + a_k\binom{t}{k}$$

is a numerical polynomial $\alpha(t) \in \mathbb{Q}[t]$ of degree k with $a_0, \dots, a_k \in \mathbb{Z}$, and $q - p \geq k$, then

$$\big(\alpha(p), \dots, \alpha(q)\big) = 1 \iff (a_0, \dots, a_k) = 1.$$

Hence $\big(\alpha(p), \dots, \alpha(q)\big) = 1$ if and only if α is primitive (not an integer multiple of another numerical polynomial).

We will write down the derived moduli problem solved by the differential graded algebraic space $(\widetilde{\mathfrak{M}}^{\mathrm{sp}}, \mathcal{R})$.

The derived space of simple modules. Let $(T, \mathcal{R}_T)$ be a differential graded scheme. If F is a graded vector bundle on T, we can sheafify the construction of our differential graded Lie algebra over T, and tensor with $\mathcal{R}_T$ to obtain a sheaf of differential graded Lie algebras

$$\mathcal{H}om_{\mathrm{gr}}(\mathfrak{m}^{\otimes \geq 1}, \mathcal{E}nd_{\mathcal{O}_T} F) \otimes_{\mathcal{O}_T} \mathcal{R}_T. \tag{5}$$

A global Maurer–Cartan element in (5) is the same thing as a graded $\mathcal{R}_T$-linear A_∞-action of $\mathfrak{m} \otimes \mathcal{R}_T$ on $F \otimes_{\mathcal{O}_T} \mathcal{R}_T$.

A *family of graded A-modules* with dimension vector α parametrized by the differential graded scheme $(T, \mathcal{R}_T)$ is a pair (F, μ), where F is a graded vector bundle of dimension α over T, and μ is a global Maurer–Cartan element in (5). Two such families are *equivalent* if they differ by a line bundle on T. We denote the set of equivalence classes of such families by $\mathfrak{R}\widetilde{\mathfrak{M}}\mathrm{od}_\alpha(A)(T)$. Varying $(T, \mathcal{R}_T)$, we get a presheaf $\mathfrak{R}\widetilde{\mathfrak{M}}\mathrm{od}_\alpha(A)$ on the category of differential graded schemes.

Note that a Maurer–Cartan element μ in (5) can be decomposed

$$\mu = \sum_{i=1}^{q-p} \mu_i, \qquad \mu_i \in \mathcal{H}om_{\mathrm{gr}}(\mathfrak{m}^{\otimes i}, \mathcal{E}nd_{\mathcal{O}_T} F) \otimes_{\mathcal{O}_T} \mathcal{R}_T^{1-i}.$$

So $\mu_1 \in \mathcal{H}om_{\mathrm{gr}}(\mathfrak{m}, \mathcal{E}nd_{\mathcal{O}_T} F) \otimes_{\mathcal{O}_T} \mathcal{R}_T^0$. The Maurer–Cartan equation implies that μ_1 takes values in the subsheaf $\mathcal{H}om_{\mathrm{gr}}(\mathfrak{m}, \mathcal{E}nd_{\mathcal{O}_T} F) \otimes_{\mathcal{O}_T} \mathcal{Z}^0(\mathcal{R}_T)$, which is equal to $\mathcal{H}om_{\mathrm{gr}}(\mathfrak{m}, \mathcal{E}nd_{\mathcal{O}_T} F)$ by our definition of differential graded scheme. Thus, we may also think of μ_1 as an $\mathcal{O}_T$-linear map $\mu_1 : \mathfrak{m} \otimes \mathcal{O}_T \to \mathcal{E}nd_{\mathcal{O}_T} F$. We call (F, μ) *simple* if the subsheaf of $\mathcal{E}nd_{\mathcal{O}_T} F$ commuting with the image of μ_1 is equal to $\mathcal{O}_T$. Simple families define the subpresheaf $\mathfrak{R}\widetilde{\mathfrak{M}}\mathrm{od}_\alpha^{\mathrm{sp}}(A) \subset \mathfrak{R}\widetilde{\mathfrak{M}}\mathrm{od}_\alpha(A)$.

Proposition 1.13. *The differential graded algebraic space $(\widetilde{\mathfrak{M}}^{\mathrm{sp}}, \mathcal{R})$ represents the sheaf associated to $\mathfrak{R}\widetilde{\mathfrak{M}}\mathrm{od}_\alpha^{\mathrm{sp}}(A)$. If α is primitive, then $\mathfrak{R}\widetilde{\mathfrak{M}}\mathrm{od}_\alpha^{\mathrm{sp}}(A)$ is a sheaf, and so $(\widetilde{\mathfrak{M}}^{\mathrm{sp}}, \mathcal{R})$ represents $\mathfrak{R}\widetilde{\mathfrak{M}}\mathrm{od}_\alpha^{\mathrm{sp}}(A)$.*

Proof. Let (F, μ) be a simple graded family parametrized by the differential graded scheme $(T, \mathcal{R}_T)$. Write $\mu = \mu_1 + \mu'$, where $\mu' = \sum_{i \geq 2} \mu_i$. Then the pair (F, μ_1) defines a morphism $\phi : T \to \widetilde{\mathfrak{M}}^{\mathrm{sp}}$, and any equivalent simple graded family gives rise to the same morphism $T \to \widetilde{\mathfrak{M}}^{\mathrm{sp}}$. The pullback to T of $\mathcal{R}_{\widetilde{\mathfrak{M}}}$ via the morphism ϕ is equal to the sheaf of symmetric algebras generated over $\mathcal{O}_T$ by the shifted dual of $\mathcal{H}om_{\mathrm{gr}}(\mathfrak{m}^{\geq 2}, \mathcal{E}nd_{\mathcal{O}_T} F)$. Therefore, a morphism $\phi^*\mathcal{R}_{\widetilde{\mathfrak{M}}} \to \mathcal{R}_T$ is the same thing as a global Maurer–Cartan section of the sheaf of curved differential graded Lie algebras (with twisted differential)

$$\mathcal{H}om_{\mathrm{gr}}(\mathfrak{m}^{\geq 2}, \mathcal{E}nd_{\mathcal{O}_T} F) \otimes_{\mathcal{O}_T} \mathcal{R}_T.$$

This is exactly what μ' provides us with. Hence (F, μ) gives rise to a morphism $(T, \mathcal{R}_T) \to (\widetilde{\mathfrak{M}}, \mathcal{R})$.

We have defined a morphism from the presheaf $\mathfrak{R}\widetilde{\mathfrak{Mod}}^{\mathrm{sp}}_{\alpha}(A)$ to the sheaf represented by $(\widetilde{\mathfrak{M}}^{\mathrm{sp}}, \mathcal{R})$. Conversely, every morphism $\phi : T \to \widetilde{\mathfrak{M}}^{\mathrm{sp}}$ is (locally in T) induced by a pair (F, μ_1), and every morphism $\phi^*\mathcal{R}_{\widetilde{\mathfrak{M}}} \to \mathcal{R}_T$ extends μ_1 to μ. This proves that every section of $(\widetilde{\mathfrak{M}}^{\mathrm{sp}}, \mathcal{R})$ comes locally from a section of $\mathfrak{R}\widetilde{\mathfrak{Mod}}^{\mathrm{sp}}_{\alpha}(A)$. This finishes the proof. $\square$

1D. ***The tangent complex.*** Suppose $\mathcal{L} = \mathcal{L}^{\geq 2}$ is a bundle of curved differential graded Lie algebras on the smooth scheme (or algebraic space) M, and let $X \subset M$ be its Maurer–Cartan locus. As a direct consequence of the second axiom (Definition 1.3), the restriction of $(\mathcal{L}, \delta)$ to X is a complex of sheaves of $\mathcal{O}_X$-modules. The derivative of the curving $f : M \to \mathcal{L}^2$ gives rise to an $\mathcal{O}_X$-linear map $T_M|_X \to \mathcal{L}^2|_X$, and we obtain an augmented complex

$$\Theta^\bullet = \big[T_M|_X \longrightarrow \mathcal{L}^2[1]|_X \longrightarrow \mathcal{L}^3[1]|_X \longrightarrow \cdots \big]$$

by the first axiom. This complex $\Theta^\bullet$ of vector bundles on X is called the *tangent complex* of $(M, \mathcal{L})$. The shifts are applied to $\mathcal{L}|_X$ so that $T_M|_X$ will end up in degree 0.

By construction, the 0-th cohomology sheaf is equal to the Zariski tangent sheaf of X:

$$h^0(\Theta^\bullet) = T_X.$$

Next, we will recall how Θ governs deformation and obstruction theory.

Deformation theory for small extensions. Consider a pointed differential graded algebra $A \to \mathbb{C}$, concentrated in nonpositive degrees. Let $A' \to A$ be a small extension of differential graded algebras: this means that the kernel I defined by the short exact sequence

$$0 \longrightarrow I \longrightarrow A' \longrightarrow A \longrightarrow 0,$$

and the kernel of the augmentation $A' \to \mathbb{C}$ annihilate each other. This implies that the A'-module structure on I is induced from the $\mathbb{C}$-vector space structure on I via the augmentation $A' \to \mathbb{C}$. For simplicity, assume that I is concentrated in a specific degree $-r \le 0$. (The classical case is the case $r = 0$.) Denote by $(T, \mathscr{R}_T)$ and $(T', \mathscr{R}_{T'})$ the affine differential graded schemes associated to A and A'.

We will consider a diagram

$$\begin{tikzcd} \operatorname{Spec}\mathbb{C} \arrow[r] \arrow[dr] \arrow[rr, bend left, "P"] & (T, \mathscr{R}_T) \arrow[r, "(\phi,\mu)"] \arrow[d] & (M, \mathscr{R}_M) \\ & (T', \mathscr{R}_{T'}) \arrow[ur, dotted, "(\phi',\mu')"'] & \end{tikzcd} \tag{6}$$

and ask for an obstruction to the existence of the dotted arrow. If a dotted arrow exists, we will classify all possible dotted arrows up to homotopy equivalence (see, for example, [Ciocan-Fontanine and Kapranov 2001] or [Manetti 1999] for the definition of homotopy equivalence).

Proposition 1.14. *There exists a naturally defined element $h \in H^1(P^*\Theta \otimes I)$, which vanishes if and only if a dotted arrow exists in (6). If $h = 0$, then the set of all dotted arrows in (6), up to homotopy equivalence, is in a natural way a principal homogeneous space for the abelian group $H^0(P^*\Theta \otimes I)$.*

Proof. The morphism $(\phi, \mu) : (T, \mathscr{R}_T) \to (M, \mathscr{R}_M)$ is given by a morphism of schemes $\phi : T \to M$ and a Maurer–Cartan element $\mu \in MC(\phi^*\mathscr{L} \otimes_{A^0} A)$. As M is smooth, there is no obstruction to the existence of ϕ', so let us choose ϕ'. Now consider the square zero extension of curved differential graded Lie algebras

$$0 \longrightarrow P^*\mathscr{L} \otimes I \longrightarrow \phi'^*\mathscr{L} \otimes_{A'^0} A' \longrightarrow \phi^*\mathscr{L} \otimes_{A^0} A \longrightarrow 0. \tag{7}$$

We have a Maurer–Cartan element μ in the curved differential graded Lie algebra on the right, which means that

$$f - \delta\mu + \tfrac{1}{2}[\mu, \mu] = 0.$$

We lift μ at random to an element μ' of the curved differential graded Lie algebra in the middle. The obstruction h is defined as

$$h = f' - \delta\mu' + \tfrac{1}{2}[\mu', \mu'],$$

which is an element of $P^*\mathscr{L} \otimes I$ and moreover a 2-cocycle in $P^*\mathscr{L} \otimes I$, hence a 1-cocycle in $P^*\Theta \otimes I$. The proof that the vanishing of h in cohomology is equivalent to the existence of the dotted arrow distinguishes between the cases that $r = 0$ and $r < 0$. For $r < 0$, we have $H^2(P^*\mathscr{L} \otimes I) = H^1(P^*\Theta \otimes I)$, and changing ϕ' while fixing ϕ is impossible. So the question is if there exists $z \in P^*\mathscr{L} \otimes I$ of degree 1, such that $\mu' + z$ is a Maurer–Cartan element in the middle of (7). Such a z will exhibit h as a coboundary (and conversely). For $r = 0$, the element

$h \in H^1(P^*\Theta \otimes I)$ is the classical obstruction to the existence of the dotted arrow in the diagram of classical schemes

$$\begin{tikzcd} \operatorname{Spec} \mathbb{C} \arrow[r] \arrow[dr] & T \arrow[rr] \arrow[d] & & X \arrow[r, hook] & M. \\ & T' \arrow[urr, dotted] & & & \end{tikzcd}$$

Now assume that the obstruction vanishes. The difference between any two Maurer–Cartan lifts of μ defines an element of $H^0(P^*\Theta \otimes I)$. One checks that this difference is a coboundary if and only if the two lifts define homotopy equivalent dotted arrows. □

Corollary 1.15. *For example, if $I = \mathbb{C}[r]$, then the obstructions are contained in $H^{r+1}(P^*\Theta)$ and the deformations are classified by $H^r(P^*\Theta)$.*

Deformations of modules. Let us examine the meaning of Proposition 1.14 for the differential graded algebraic space $(\widetilde{\mathfrak{M}}^{\mathrm{sp}}, \mathscr{R}) = \mathfrak{R}\widetilde{\mathfrak{M}}\mathrm{od}_\alpha^{\mathrm{sp}}(A)$.

So let the $\mathbb{C}$-valued point $P : \operatorname{Spec} \mathbb{C} \to (\widetilde{\mathfrak{M}}^{\mathrm{sp}}, \mathscr{R})$ be represented by the Maurer–Cartan element $\mu \in L$.

Lemma 1.16. *The complex (L, d^μ) is precisely the graded normalized Hochschild cochain complex with coefficients in $(\operatorname{End} V, \mu)$, that is, $\operatorname{End} V$ endowed with the structure of an A-A-bimodule from μ.*

Proof. This is immediate. The normalized or reduced complex is defined, for example, in [Loday 1992, §1.5.7]. □

Corollary 1.17. *The complex $P^*\Theta$ is quasiisomorphic to the augmented graded Hochschild complex*

$$\mathbb{C} \longrightarrow \operatorname{End}_{\mathrm{gr}} V \longrightarrow \operatorname{Hom}_{\mathrm{gr}}(A, \operatorname{End} V) \longrightarrow \operatorname{Hom}_{\mathrm{gr}}(A^{\otimes 2}, \operatorname{End} V) \longrightarrow \cdots .$$

Proof. This follows immediately from the fact that the normalized Hochschild complex is quasiisomorphic to the Hochschild complex, by [Loday 1992, §1.5.7]. □

Corollary 1.18. *Suppose that P corresponds to the A-module $E = (V, \mu)$. Then we have*

$$H^i(P^*\Theta) = \begin{cases} \operatorname{Ext}^i_A(E, E)_{\mathrm{gr}} & \text{if } i > 0, \\ \operatorname{Hom}_A(E, E)_{\mathrm{gr}}/\mathbb{C} & \text{for } i = 0. \end{cases}$$

The tangent complex Θ itself is quasiisomorphic to the augmented complex

$$\mathbb{C} \longrightarrow R\,\mathscr{H}om_A(\mathscr{E}, \mathscr{E})_{\mathrm{gr}},$$

where $\mathscr{E}$ is the universal family of graded A-modules on $\widetilde{\mathfrak{X}}^{\mathrm{sp}} = \widetilde{\mathfrak{M}}\mathrm{od}_\alpha^{\mathrm{sp}}(A)$.

Proof. This is a consequence of the standard fact that (graded) Hochschild cohomology computes (graded) extension spaces. A proof in the ungraded case can be found in Lemma 1.9.1 of [Weibel 1994]. □

Corollary 1.19. *In a situation given by a diagram such as (6), assume that $I = \mathbb{C}[r]$, as in Corollary 1.15. Then obstructions are contained in* $\operatorname{Ext}^{r+1}_A(E, E)_{\mathrm{gr}}$ *and deformations are classified by* $\operatorname{Ext}^r_A(E, E)_{\mathrm{gr}}$ *(or* $\operatorname{Hom}_A(E, E)_{\mathrm{gr}}/\mathbb{C}$, *for* $r = 0$*).*

2. Stability

We will apply geometric invariant theory to the construction of the quotient of $M = L^1$ by the gauge group G as a quasiprojective scheme.

First, since the scalars in G act trivially, no point of L^1 can be stable for the action of G. This prompts us to replace G by $\widetilde{G} = G/\Delta$. Second, the *canonical* one-parameter subgroup $\lambda_0(t) = (t^p, \dots, t^q)$ is central and acts by (see Equation (3))

$$(\lambda_0(t) \cdot \mu)_{ij} = t^{i-j}\mu_{ij},$$

and hence destabilizes every element of L^1, as $i > j$ if $\mu_{ij} \neq 0$. Thus the affine quotient $\operatorname{Spec} \mathbb{C}[L^1]^G$ is trivial, equal to $\operatorname{Spec} \mathbb{C}$.

In fact, the quotient of L^1 by G classifies quiver representations for a certain quiver, and so we are in the situation worked out by King [1994]. Our quiver has $q - p + 1$ vertices labeled $p, \dots, q$, and for every pair of vertices $i < j$, there are $\dim A_{j-i}$ arrows from i to j. The vector space $L^1 = \operatorname{Hom}_{\mathrm{gr}}(\mathfrak{m}, \operatorname{End} V)$ is denoted $\mathcal{R}(Q, \alpha)$ by King; the group G is denoted by $\mathrm{GL}(\alpha)$.

To linearize the action of $\widetilde{G}$ on L^1, we choose a vector of integers

$$\theta = (\theta_p, \dots, \theta_q) \quad \text{such that} \quad \sum_{i=p}^{q} \theta_i \alpha_i = 0.$$

This defines the character $\chi_\theta : \widetilde{G} \to \mathbb{C}$ by

$$\chi_\theta(g) = \prod_{i=p}^{q} \det(g_i)^{\theta_i},$$

which we use to linearize the action.

For a graded vector subspace $W \subset V$, define

$$\theta(W) = \sum_{i=p}^{q} \theta_i \dim W_i.$$

Note that whether or not $\mu \in L^1$ satisfies the Maurer–Cartan equation, it makes sense to speak of graded submodules $W \subset V$ with respect to μ.

Proposition 2.1 (King). *The point $\mu \in L^1$ is (semi)stable for the action of $\widetilde{G}$ linearized by χ_θ if and only if for every proper graded μ-submodule $0 < W < V$ we have $\theta(W)$ $(\geq)$ 0. (Here we use the usual convention that to characterize stability, the strict inequality applies, and for semistability the weak inequality is used.)*

Denote by L^s and L^{ss} the open subsets of L^1 of stable and semistable points, respectively. Similarly, denote by X^s and X^{ss} the open subsets of stable and semistable points inside the Maurer–Cartan subscheme $X \subset L^1$.

The geometric invariant theory quotient of L^1 by $\widetilde{G}$ is the projective scheme

$$L^1/\!/\widetilde{G} = \mathbb{P}\mathrm{roj} \bigoplus_{n=0}^{\infty} \mathbb{C}[L^1]^{G,\chi^n},$$

where $\mathbb{C}[L^1]^{G,\chi^n} = \{ f : L^1 \to \mathbb{C} \mid f(gx) = \chi^n(g) f(x) \}$ is the space of χ^n-twisted invariants of G in $\mathbb{C}[L^1]$. The quotient $L^1/\!/\widetilde{G}$ is indeed projective since $\mathbb{C}[L^1]^G = \mathbb{C}$.

Corollary 2.2. *The scheme $L^s/\!/\widetilde{G}$ is a quasiprojective smooth scheme contained as an open subscheme in the algebraic space $\widetilde{\mathfrak{M}}^{\mathrm{sp}}$. It is a locally fine moduli space for equivalence classes of stable quiver representations. In the coprime case, it is a fine moduli space.*

The scheme $L^1/\!/\widetilde{G} = L^{ss}/\!/\widetilde{G}$ is a projective scheme containing $L^s/\!/\widetilde{G}$ as an open subscheme. Its points are in one-to-one correspondence with S-equivalence classes of semistable quiver representations.

Corollary 2.3. *The differential graded scheme $(L^s/\!/\widetilde{G}, \mathcal{R})$ is a quasiprojective differential graded scheme, which represents the sheaf associated to $\mathfrak{R}\widetilde{\mathfrak{M}}\mathrm{od}^s_\alpha(A)$, the presheaf of equivalence classes of families of stable graded A-modules.*

In the coprime case, $(L^s/\!/\widetilde{G}, \mathcal{R})$ represents $\mathfrak{R}\widetilde{\mathfrak{M}}\mathrm{od}^s_\alpha(A)$.

Example 2.4. Maybe the most canonical of all characters is the one defined by $\theta_p = -\dim V_q$, $\theta_q = \dim V_p$ and all other $\theta_i = 0$. We call it the *extremal* character. For this character, (semi)stability reads

$$\dim W_p \dim V_q \ (\leq) \dim W_q \dim V_p,$$

or, equivalently,

$$\frac{\dim W_p}{\dim W_q} \ (\leq) \ \frac{\dim V_p}{\dim V_q},$$

or

$$\frac{\dim W_p}{\dim V_p} \ (\leq) \ \frac{\dim W_q}{\dim V_q}.$$

For example, stability implies that V_p generates V as an A-module.

Definition 2.5. We call the $[p, q]$-graded A-module M (semi)stable if the corresponding point μ in $L^1 = \mathrm{Hom}_{\mathrm{gr}}\big(\mathfrak{m}, \mathrm{End}(M)\big)$ is (semi)stable with respect to the linearization of $\widetilde{G}$ given by the extremal character.

Example 2.6. Another canonical character is the determinant of the action of G on L^1. It has

$$\theta_i = \sum_{j<i} \dim A_{i-j} \dim V_j - \sum_{j>i} \dim A_{j-i} \dim V_j,$$

and gives rise to the (semi)stability condition

$$\sum_{i<j} \dim A_{j-i} \dim W_i \dim V_j \ (\leq) \sum_{i<j} \dim A_{j-i} \dim W_j \dim V_i.$$

3. Moduli of sheaves

We will now assume that $A = \bigoplus_{n\geq 0} \Gamma\big(Y, \mathcal{O}(n)\big)$ for a connected projective scheme Y.

3A. ***The adjoint of the truncation functor.*** For a scheme T, we denote the projection $Y \times T \to T$ by π_T.

Let T be a scheme and $\mathcal{F}_T$ a coherent sheaf on $Y \times T$. Then

$$\Gamma_{[p,q]}\mathcal{F}_T = \bigoplus_{i=p}^{q} \pi_{T*}\big(\mathcal{F}(i)\big)$$

is a graded sheaf of coherent $\mathcal{O}_T$-modules with A-module structure.

Proposition 3.1. *The functor*

$$\Gamma_{[p,q]} : (\text{coherent sheaves of } \mathcal{O}_{Y\times T}\text{-modules}) \\ \longrightarrow ([p, q]\text{-graded coherent sheaves of } A \otimes \mathcal{O}_T\text{-modules})$$

has a left adjoint, which we shall denote by $\mathcal{S}$. The functor $\mathcal{S}$ commutes with arbitrary base change.

Proof. First note that graded coherent $A \otimes \mathcal{O}_T$-modules concentrated in the interval $[p, q]$ form an abelian category with kernels, cokernels, images and direct sums constructed degreewise, and that $\Gamma_{[p,q]}$ is an additive functor so that the statement makes sense.

Then, by the claimed compatibility with base change, we may assume that T is affine, $T = \mathrm{Spec}\, B$.

Let M be a graded $A \otimes B$-module concentrated in the interval $[p, q]$, and let

$$\bigoplus_j A(-m_j) \otimes B \longrightarrow \bigoplus_i A(-n_i) \otimes B \longrightarrow M \longrightarrow 0$$

be a presentation of M (by graded homomorphisms) as a graded $A \otimes B$-module. Assume that all n_i are in the interval $[p, q]$.

Define $\mathcal{S}M$ to be the cokernel in the diagram of $\mathcal{O}_{Y\times T}$-modules

$$\bigoplus_{m_j \in [p,q]} \mathcal{O}_{Y\times T}(-m_j) \longrightarrow \bigoplus_i \mathcal{O}_{Y\times T}(-n_i) \longrightarrow \mathcal{S}M \longrightarrow 0, \tag{8}$$

where the first sum extends only over those indices j such that m_j is in the interval $[p, q]$. Let us prove that $\mathcal{S}M$ defined in this way satisfies

$$\mathrm{Hom}_{\mathcal{O}_{Y\times T}}(\mathcal{S}M, \mathcal{F}) = \mathrm{Hom}^{\mathrm{gr}}_{A\otimes B}(M, \Gamma_{[p,q]}\mathcal{F}), \tag{9}$$

for all $\mathcal{O}_{Y\times T}$-modules $\mathcal{F}$. Given such $\mathcal{F}$, consider the commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{O}_{Y\times T}}\Big(\bigoplus_i \mathcal{O}_{Y\times T}(-n_i), \mathcal{F}\Big) \arrow[r] \arrow[d, equal] & \mathrm{Hom}_{\mathcal{O}_{Y\times T}}\Big(\bigoplus_{m_j\in[p,q]} \mathcal{O}_{Y\times T}(-m_j), \mathcal{F}\Big) \arrow[d, equal] \\
\mathrm{Hom}^{\mathrm{gr}}_{A\otimes B}\Big(\bigoplus_i A(-n_i)\otimes B, \Gamma_{[p,q]}\mathcal{F}\Big) \arrow[r] & \mathrm{Hom}^{\mathrm{gr}}_{A\otimes B}\Big(\bigoplus_j A(-m_j)\otimes B, \Gamma_{[p,q]}\mathcal{F}\Big)
\end{tikzcd}$$

This diagram induces an equality of the kernels of the horizontal maps, and these kernels are the two sides of (9), thus proving (9).

To prove that the adjoint functor $\mathcal{S}$ commutes with base change, consider a base change diagram

$$\begin{tikzcd}
Y\times T' \arrow[r] \arrow[d, "v"'] & T' \arrow[d, "u"] \\
Y\times T \arrow[r] & T
\end{tikzcd}$$

and note that $\Gamma_{[p,q]} \circ v_* = u_* \circ \Gamma'_{[p,q]}$ in obvious notation. It follows that for the adjoint functors we have the equality $v^* \circ \mathcal{S} = \mathcal{S}' \circ u^*$, which is the claimed compatibility with base change. □

3B. ***Open immersion.*** Fix a numeric polynomial $\alpha(t) = a_0\binom{t}{0} + \cdots + a_k\binom{t}{k}$.

Let $\mathfrak{U}$ be a finite type open substack of the algebraic stack of coherent sheaves on Y with Hilbert polynomial $\alpha(t)$.

For $q > p > 0$ let $\mathfrak{Mod}^{[p,q]}_\alpha(A)$ be the algebraic stack of $[p, q]$-graded A-modules of dimension $\alpha|_{[p,q]}$. Recall that $\mathfrak{Mod}^{[p,q]}_\alpha(A) = [MC(L)/G]$, in the notation of Section 1.

Proposition 3.2. *Given $\mathfrak{U}$, there exists p such that for all $q > p$ the functor $\Gamma_{[p,q]}$ defines a morphism of algebraic stacks*

$$\Gamma_{[p,q]} : \mathfrak{U} \longrightarrow \mathfrak{Mod}^{[p,q]}_\alpha(A).$$

If q is sufficiently large, then $\Gamma_{[p,q]}$ is a monomorphism of stacks.

Proof. Let p be large enough such that every sheaf in $\mathfrak{U}$ is Castelnuovo–Mumford p-regular. Then, for every $i \geq p$, the sheaf $\pi_{T*}\mathscr{F}(i)$ is locally free of rank $\alpha(i)$ on T. Hence $\Gamma_{[p,q]}\mathscr{F}$ is a $\mathfrak{Mod}_{\alpha}^{[p,q]}(A)$-family over T, and we have the required morphism of stacks.

Now let, in addition, q be large enough for $\mathscr{O}_Y(q-p)$ to be Castelnuovo–Mumford regular. Then $\Gamma_{[p,q]}$ is a monomorphism of stacks because for every family of p-regular sheaves $\mathscr{F}$, the adjunction map $\mathscr{S}(\Gamma_{[p,q]}\mathscr{F}) \to \mathscr{F}$ is an isomorphism. See [Álvarez-Cónsul and King 2007], Theorem 3.4 and Proposition 4.1, for a proof of a similar statement. In our context, we may proceed as follows:

First note that we may assume that the parameter scheme T is affine, $T = \operatorname{Spec} B$, as in the proof of Proposition 3.1.

Let $V = \Gamma(Y, \mathscr{F}(p))$, and $\mathscr{G}$ the kernel in:

$$0 \longrightarrow \mathscr{G} \longrightarrow V \otimes_B \mathscr{O}_Y(-p) \longrightarrow \mathscr{F} \longrightarrow 0.$$

Then the fact that $\mathscr{O}_Y(q-p)$ is regular implies that $\mathscr{G}$ is q-regular. (See Lemma 3.3 in [Álvarez-Cónsul and King 2007].) Let $W = \Gamma\big(Y, \mathscr{G}(q)\big)$, so that we have a surjection $W \otimes_B \mathscr{O}_Y(-q) \twoheadrightarrow \mathscr{G}$ and a presentation of $\mathscr{F}$:

$$W \otimes_B \mathscr{O}_Y(-q) \longrightarrow V \otimes_B \mathscr{O}_Y(-p) \longrightarrow \mathscr{F} \longrightarrow 0$$

We remark that q-regularity of $\mathscr{G}$ implies that this sequence stays exact after twisting by $\mathscr{O}_Y(i)$ and taking global sections for all $i \geq q$. Thus the sequence of graded $A \otimes B$-modules

$$W \otimes A(-q) \longrightarrow V \otimes A(-p) \longrightarrow \Gamma_{\geq p}\mathscr{F} \longrightarrow 0$$

is exact in degrees $\geq q$. We can construct from this a presentation of $\Gamma_{\geq p}\mathscr{F}$ by adding some relations whose degrees are between p and q. Then we can turn this presentation of $\Gamma_{\geq p}\mathscr{F}$ into a presentation of $\Gamma_{[p,q]}\mathscr{F}$ by adding relations in degrees larger than q. These extra relations in degrees larger than q are ignored when constructing $\mathscr{S}(\Gamma_{[p,q]}\mathscr{F})$; see the proof of Proposition 3.1. The extra relations of degree between p and q do not affect the cokernel in Equation (8). We conclude that we have a presentation

$$W \otimes_B \mathscr{O}_Y(-q) \longrightarrow V \otimes_B \mathscr{O}_Y(-p) \longrightarrow \mathscr{S}(\Gamma_{[p,q]}\mathscr{F}) \longrightarrow 0.$$

This proves that $\mathscr{S}(\Gamma_{[p,q]}\mathscr{F}) = \mathscr{F}$. $\square$

Proposition 3.3. *For $q \gg p \gg 0$ the morphism $\Gamma_{[p,q]} : \mathfrak{U} \to \mathfrak{Mod}_{\alpha}^{[p,q]}(A)$ is étale.*

Proof. Let $A' \to A \to \mathbb{C}$ be a small extension of pointed $\mathbb{C}$-algebras (not differential graded). Let $T = \operatorname{Spec} A$ and $T' = \operatorname{Spec} A'$. Consider a 2-commutative diagram

$$\begin{tikzcd} T \arrow[r, "\mathscr{F}"] \arrow[d, hook] & \mathfrak{U} \arrow[d, "\Gamma_{[p,q]}"] \\ T' \arrow[r, "M'"] \arrow[ur, dotted] & \mathfrak{Mod}_{\alpha}^{[p,q]}(A) \end{tikzcd}$$

of solid arrows. We have to prove that the dotted arrow exists, uniquely, up to a unique 2-isomorphism. This follows from standard deformation-obstruction theory. We need that $\Gamma_{[p,q]}$ induces a bijection on deformation spaces and an injection on obstruction spaces (associated to the above diagram). It is well known that deformations of $\mathscr{F}$ are classified by $\operatorname{Ext}^1_{\mathbb{O}_Y}(\mathscr{F}, \mathscr{F})$, and obstructions are contained in $\operatorname{Ext}^2_{\mathbb{O}_Y}(\mathscr{F}, \mathscr{F})$. We saw in Corollary 1.18 that deformations of $M'|_T$ are classified by $\operatorname{Ext}^1_A(M, M)_{\mathrm{gr}}$ and obstructions are contained in $\operatorname{Ext}^2_A(M, M)_{\mathrm{gr}}$, where $M = \Gamma_{[p,q]}(\mathscr{F})$. It is proved in [Ciocan-Fontanine and Kapranov 2001], (4.3.3.a) and (4.3.4) that for fixed i, there exist $q \gg p \gg 0$ such that $\operatorname{Ext}^i_{\mathbb{O}_Y}(\mathscr{F}, \mathscr{F}) = \operatorname{Ext}^i_A(\Gamma_{[p,q]}\mathscr{F}, \Gamma_{[p,q]}\mathscr{F})_{\mathrm{gr}}$. (Note that the assumption in [Ciocan-Fontanine and Kapranov 2001] that Y be smooth is not used for this result. It is only used to exchange quantifiers: namely to get uniform p and q, which work for *all* $i \geq 0$.) $\square$

Corollary 3.4. *For $q \gg p \gg 0$ the morphism $\Gamma_{[p,q]} : \mathfrak{U} \to \mathfrak{Mod}_{\alpha}^{[p,q]}(A)$ is an open immersion.*

3C. ***Stable sheaves.*** Let Y be a connected projective scheme. We denote the Hilbert polynomial of a coherent sheaf $\mathscr{F}$ on Y by $h(\mathscr{F}, t) = h(\mathscr{F})$.

For our purposes, the following characterization of stability of $\mathscr{F}$ is most useful.

Definition 3.5. The sheaf $\mathscr{F}$ is *(semi)stable* if and only if for every proper subsheaf $0 < \mathscr{F}' < \mathscr{F}$ we have

$$\frac{h(\mathscr{F}', p)}{h(\mathscr{F}, p)} \,(\leq)\, \frac{h(\mathscr{F}', q)}{h(\mathscr{F}, q)} \quad \text{for } q \gg p \gg 0.$$

(As usual, this means the strict inequality for "stable" and the weak inequality for "semistable".)

The condition needs only to be checked for *saturated* subsheaves. (A subsheaf is saturated if the corresponding quotient is pure of the same dimension as $\mathscr{F}$.)

Remark 3.6. We can say, informally, that the limiting slope of the quotient of Hilbert polynomials $h(\mathscr{F}')/h(\mathscr{F})$ is $(\geq)\ 0$, for all proper saturated subsheaves.

This stability condition looks very similar to the condition given by the extremal character for A-modules (see Example 2.4), but to relate the two notions is not completely trivial.

Theorem 3.7. *Given $\mathfrak{U}$, it is possible to choose $q \gg p \gg 0$ in such a way that the following holds: if $\mathscr{F}$ is a $\mathfrak{U}$-sheaf, then $\mathscr{F}$ is a (semi)stable sheaf if and only if $M = \Gamma_{[p,q]}\mathscr{F}$ is a (semi)stable graded A-module (Definition 2.5).*

Proof. By Grothendieck's lemma (see [Huybrechts and Lehn 1997], Lemma 1.7.9), the family $\mathfrak{U}'$ of all saturated destabilizing subsheaves of all sheaves in $\mathfrak{U}$ is bounded. We choose p large enough to ensure that all sheaves in $\mathfrak{U}$ and $\mathfrak{U}'$ are p-regular. Note that the sheaves in $\mathfrak{U}'$ have only finitely many Hilbert polynomials. So we can choose $q \gg p \gg 0$ in such a way that the limiting slope of all quotients of all Hilbert polynomials involved is measured correctly by p and q.

Additionally, we choose p and q sufficiently large as explicated in [Álvarez-Cónsul and King 2007]. (This choice is only needed for the "converse", below.)

Let us first suppose that M is (semi)stable and prove that $\mathscr{F}$ is (semi)stable. So let $0 \subsetneq \mathscr{F}' \subsetneq \mathscr{F}$ be a saturated subsheaf. We wish to prove, of course, that $\mathscr{F}'$ does not violate (semi)stability of $\mathscr{F}$. So let us assume it does. Then by our choices, both $\mathscr{F}'$ and $\mathscr{F}$ are p-regular.

Since $\Gamma_{[p,q]}$ is left exact, we get a graded submodule

$$M' = \Gamma_{[p,q]}\mathscr{F}' \hookrightarrow \Gamma_{[p,q]}\mathscr{F}.$$

Moreover, $0 \subsetneq M' \subsetneq M$, as $\mathscr{F}' = \mathscr{S}M'$ because $\mathscr{F}'$ is p-regular. Since $M = \Gamma_{[p,q]}\mathscr{F}$ is (semi)stable, we know that

$$\frac{\dim \Gamma(Y, \mathscr{F}'(p))}{\dim \Gamma(Y, \mathscr{F}(p))} (\leq) \frac{\dim \Gamma(Y, \mathscr{F}'(q))}{\dim \Gamma(Y, \mathscr{F}(q))}.$$

By p-regularity, this implies that

$$\frac{h(\mathscr{F}', p)}{h(\mathscr{F}, p)} (\leq) \frac{h(\mathscr{F}', q)}{h(\mathscr{F}, q)},$$

and so $\mathscr{F}'$ does *not* violate (semi)stability, a contradiction.

Conversely, assume that $\mathscr{F}$ is (semi)stable. If $0 < M' < M$ is a (semi)stability violating submodule, then $(M'_p, M'_q) \subset (M_p, M_q)$ is a Kronecker submodule in the sense of [Álvarez-Cónsul and King 2007]. To prove that $(M'_p, M'_q) \neq (0, 0)$, note that $\Gamma_{[p,q]}\mathscr{F}$ does not have any nontrivial submodules which vanish in the top degree q. (This is an elementary fact about sheaves on projective schemes.) To prove that $(M'_p, M'_q) \neq (M_p, M_q)$, note that $\Gamma_{[p,q]}\mathscr{F}$ is generated in the lowest degree p, by p-regularity of $\mathscr{F}$.

Thus, applying [ibid., Theorem 5.10], we see that M' does *not* violate (semi)stability, a contradiction. □

3D. ***Moduli of sheaves.*** Let $\alpha(t)$ be a Hilbert polynomial. Let $\mathfrak{U}^{ss}$ be the bounded family of all semistable sheaves with Hilbert polynomial $\alpha(t)$. Choose $q \gg p \gg 0$ as prescribed by Theorem 3.7 for $\mathfrak{U}^{ss}$.

Let $U^s \subset U^{ss}$ be the moduli spaces of stable (respectively, semistable) sheaves on Y with Hilbert polynomial $\alpha(t)$.

Corollary 3.8. *We have a commutative diagram of open immersions of schemes.*

$$\begin{tikzcd} U^{ss} \arrow[r, "\Gamma_{[p,q]}"] & X^{ss}/\!/\widetilde{G} \\ U^s \arrow[u] \arrow[r, "\Gamma_{[p,q]}"] & \widetilde{\mathfrak{Mod}}^s_{\alpha|_{[p,q]}}(A) \arrow[u] \end{tikzcd}$$

The two schemes in the top row are projective. Hence, U^{ss} is a union of connected components of $X^{ss}/\!/\widetilde{G}$.

In the case where α is primitive, we have $U^s = U^{ss}$, and so U^s is a union of components of $\widetilde{\mathfrak{Mod}}^s_{\alpha|_{[p,q]}}$ via the functor $\Gamma_{[p,q]}$.

Remark 3.9. Assume we are in the primitive case. Then $U^s \subset L^s/\!/\widetilde{G}$ is a closed subscheme of the smooth scheme $L^s/\!/\widetilde{G}$, cut out by the descended Maurer–Cartan equation $dx + \frac{1}{2}[x, x] = 0$. This gives rather explicit equations for U^s inside a smooth scheme. Note that we do not prove that $L^s/\!/\widetilde{G}$ is projective, in the primitive case.

3E. ***An amplification.*** By using three integers $q \gg p' \gg p \gg 0$, we can describe the image of $\Gamma_{[p,q]} : \mathfrak{U}^s \to \mathfrak{Mod}_{\alpha|_{[p,q]}}(A)$ explicitly.

We denote by $\mathfrak{Mod}_{\alpha|_{[p,q]}}(A)' \subset \mathfrak{Mod}_{\alpha|_{[p,q]}}(A)$ the open substack of graded A-modules which are generated in degree p.

Theorem 3.10. *Let $\mathfrak{U}$ be, as above, a bounded open family of sheaves on Y. Then for $q \gg p' \gg p \gg 0$, the functor $\Gamma_{[p,q]}$ induces an open immersion*

$$\Gamma_{[p,q]} : \mathfrak{U} \longrightarrow \mathfrak{Mod}_{\alpha|_{[p,q]}}(A)',$$

and the image of $\mathfrak{U}^s$ ($\mathfrak{U}^{ss}$) is equal to the locus of modules whose truncation into the interval $[p', q]$ is (semi)stable.

Proof. The first claim is clear: p-regularity of $\mathscr{F}$ implies that $\Gamma_{[p,q]}\mathscr{F}$ is generated in degree p.

The fact that $\mathfrak{U}^s$ ($\mathfrak{U}^{ss}$) is contained in the $[p', q]$-(semi)stable locus follows from Theorem 3.7.

Let M be an A-module concentrated in degrees $[p, q]$, generated in degree p, and of dimension $\alpha|_{[p,q]}$. Then we will use Gotzmann persistence to prove that $\mathscr{F} = \mathscr{S}(M)$ has Hilbert polynomial α, and we will make sure that all $\mathscr{S}(M)$ obtained in this way are p'-regular. This will imply that $M_{[p',q]} = \Gamma_{[p',q]}\mathscr{F}$, and we can again apply Theorem 3.7 to deduce that if $M_{[p',q]}$ is (semi)stable, then $\mathscr{F}$ is (semi)stable.

We briefly recall the persistence theorem (see [Gotzmann 1978] and [Gasharov 1997], especially Theorem 4.2). First, for integers $a \geq 0$ and $t \geq 1$, there exist unique integers $m_t > m_{t-1} > \cdots > m_1 \geq 0$, such that $a = \sum_{i=1}^{t} \binom{m_i}{i}$. Then one defines $a^{\langle t \rangle} = \sum_{i=1}^{t} \binom{m_i+1}{i+1}$. One significance of this definition is the following: if $\mathscr{E}$ is a coherent sheaf of $\mathbb{O}_Y$-modules, such that $\mathscr{E}(p)$ is globally generated, and if $h(t)$ is the Hilbert polynomial of $\mathscr{E}$, then $h(t+1) = h(t)^{\langle t-p \rangle}$, for $t \gg 0$. The persistence theorem says the following:

Suppose A is a graded $\mathbb{C}$-algebra, generated in degree 1, with relations in degree $\leq r$ for an integer $r \geq 1$. Let M be a graded A-module and G a finite-dimensional graded $\mathbb{C}$-vector space such that the following sequence of graded A-modules is exact:

$$0 \longrightarrow K \longrightarrow A \otimes_{\mathbb{C}} G \longrightarrow M \longrightarrow 0.$$

(i) (Macaulay bound) If $\deg G \leq p$, then $\dim M_{d+1} \leq (\dim M_d)^{\langle d-p \rangle}$ for all $d \geq p+1$. Moreover, there exists a d such that $\dim M_{d'+1} = (\dim M_{d'})^{\langle d'-p \rangle}$, for all $d' \geq d$.

(ii) (persistence) If in addition K is generated in degree less than or equal to r', where $r' \geq p+r$, and if $\dim M_{d+1} = (\dim M_d)^{\langle d-p \rangle}$ for some $d \geq r'$, then $\dim M_{d'+1} = (\dim M_{d'})^{\langle d'-p \rangle}$ for all $d' \geq d$.

We may assume that $\alpha(t+1) = \alpha(t)^{\langle t-p \rangle}$, for all $t \geq p$.

Now let M be an A-module in $[p, q]$ of dimension $\alpha|_{[p,q]}$ and generated in degree p. We have the exact sequence

$$0 \longrightarrow K \longrightarrow A_{[0,q-p]} \otimes M_p \longrightarrow M \longrightarrow 0,$$

where the kernel K exists (at most) in degrees $[p+1, q]$. Let $\widetilde{K} \subset A \otimes M_p$ be the submodule generated by K, and let $\widetilde{M}$ be the quotient

$$0 \longrightarrow \widetilde{K} \longrightarrow A \otimes M_p \longrightarrow \widetilde{M} \longrightarrow 0.$$

Thus $\widetilde{K}$ is generated in degree $\leq q$.

Our first claim is that $\widetilde{K}$ is actually generated in degree $p+1$. We will do this by descending induction. So suppose $\widetilde{K}$ is generated in degree $\leq r'$ for $p+1 < r' \leq q$, but not in degree $\leq r'-1$. Then let $\widetilde{K}' < \widetilde{K}$ be the submodule generated by the degree $\leq r'-1$ part of $\widetilde{K}$. Let $\widetilde{M}' = (A \otimes M_p)/\widetilde{K}'$ be the quotient. Then we have

$$(\dim \widetilde{M}'_{r'-1})^{\langle r'-1-p \rangle} \geq \widetilde{M}'_{r'} > \widetilde{M}_{r'} = (\widetilde{M}_{r'-1})^{\langle r'-1-p \rangle},$$

which implies $\dim \widetilde{M}'_{r'-1} > \dim \widetilde{M}_{r'-1}$, which is absurd, as these two spaces are equal. Thus $\widetilde{K}$ is, indeed, generated in degrees $\leq r'-1$, and we conclude that it is, in fact, generated in degree $p+1$.

Now, the persistence theorem implies that $\dim \widetilde{M}_{t+1} = \dim \widetilde{M}_t^{\langle t-p \rangle}$ for $t > p+r$.

As $\mathcal{S}(M)$ is the sheaf associated to $\widetilde{M}$, this implies that the Hilbert polynomial of $\mathcal{S}(M)$ is equal to α, as claimed.

We remark that the family of all A-modules generated in degree p by $\alpha(p)$ elements, whose relations are in degree $p+1$, is bounded. Therefore, we can choose $p' > p$ in such a way that all sheaves associated to such modules are p'-regular. This will imply that all $\mathcal{S}(M)$ obtained from $\mathfrak{Mod}_{\alpha|_{[p,q]}}(A)'$ are p'-regular.

It remains to prove that a suitable choice of p' will assure that the truncation of M into the interval $[p', q]$ is equal to $\Gamma_{[p',q]}\mathcal{F}$, where $\mathcal{F} = \mathcal{S}(M)$.

Now, the canonical map $\widetilde{M} \to \Gamma_{\geq p}\mathcal{F}$ is an isomorphism in sufficiently high degree. But as the family of all $\widetilde{M}$ which occur is bounded, there exists a uniform p' which will assure that $\widetilde{M}|_{\geq p'} \to \Gamma_{\geq p'}\mathcal{F}$ is an isomorphism. This finishes the proof of the last remaining fact that $M|_{[p',q]} = \Gamma_{[p',q]}\mathcal{S}(M)$. $\square$

Corollary 3.11. *We have*

$$U^{ss} = \widetilde{\mathfrak{Mod}}^{[p',q]\text{-}ss}_{\alpha|_{[p,q]}}(A)' \quad \textit{and} \quad U^{s} = \widetilde{\mathfrak{Mod}}^{[p',q]\text{-}s}_{\alpha|_{[p,q]}}(A)',$$

in obvious notation. In the primitive case, all four schemes are equal.

Remark 3.12. If an A-module in $[p, q]$ is stable (not just semistable), then it is generated in degree p. Thus U^s can also be described as the scheme of modules in the interval $[p, q]$ of dimension $\alpha|_{[p,q]}$ which are stable and whose truncation into the interval $[p', q]$ is also stable.

4. Derived moduli of sheaves

Finally, we will construct the differential graded moduli scheme of stable sheaves on the projective variety Y. From now on, we have to assume that Y is smooth. Let $\alpha(t)$ be a numerical polynomial, and $p \gg 0$. For simplicity, let us assume that $\alpha(t)$ is primitive.

Definition 4.1. A *family of coherent sheaves* on Y of Hilbert polynomial $\alpha(t)$, parametrized by the differential graded scheme $(T, \mathcal{R}_T)$, is a pair (E, μ), where E is a graded quasicoherent sheaf

$$E = \bigoplus_{i \geq p} E_i$$

on T and each E_i is a vector bundle of rank $\operatorname{rk} E_i = \alpha(i)$. Moreover, μ is a "unital" Maurer–Cartan element in the differential graded Lie algebra

$$\Gamma\big(T, \mathcal{H}om_{\mathrm{gr}}(A^{\otimes \geq 1}, \mathcal{E}nd_{\mathcal{O}_T} E) \otimes_{\mathcal{O}_T} \mathcal{R}_T\big)\,;$$

in other words a graded unital $\mathcal{R}_T$-linear A_∞-action of $A \otimes \mathcal{R}_T$ on $E \otimes_{\mathcal{O}_T} \mathcal{R}_T$.

We denote the functor of equivalence classes (see Definition 1.9) of simple such families by $\mathfrak{R}\widetilde{\mathfrak{Mod}}^{\mathrm{sp}}_{\alpha}(\mathcal{O}_Y)$.

If for every point $P : \operatorname{Spec}\mathbb{C} \to T$, the associated coherent sheaf on Y is (semi)stable, then the family (E, μ) is a *(semi)stable* family.

Lemma 4.2. *We have*

$$\mathfrak{R}\widetilde{\mathfrak{Mod}}^{\mathrm{sp}}_{\alpha}(\mathbb{O}_Y) = \varprojlim_{q \gg p} \mathfrak{R}\widetilde{\mathfrak{Mod}}^{\mathrm{sp}}_{\alpha|_{[p,q]}}(A),$$

as set-valued presheaves on the category of differential graded schemes.

Proof. Obvious. □

Corollary 4.3. *The functor $\mathfrak{R}\widetilde{\mathfrak{Mod}}^{\mathrm{sp}}_{\alpha}(\mathbb{O}_Y)$ is represented by the projective limit of differential graded algebraic spaces*

$$\mathfrak{R}\widetilde{\mathfrak{Mod}}^{\mathrm{sp}}_{\alpha}(A) = \varprojlim_{q \gg p} \mathfrak{R}\widetilde{\mathfrak{Mod}}^{\mathrm{sp}}_{\alpha|_{[p,q]}}(A).$$

Proposition 4.4. *The projective limit*

$$\varprojlim_{q \gg p} \mathfrak{R}\widetilde{\mathfrak{Mod}}^{\mathrm{sp}}_{\alpha|_{[p,q]}}(A)$$

stabilizes as far as quasiisomorphism is concerned. More precisely, for $q' \gg q \gg p$ the morphism

$$\mathfrak{R}\widetilde{\mathfrak{Mod}}^{\mathrm{sp}}_{\alpha|_{[p,q']}}(A) \longrightarrow \mathfrak{R}\widetilde{\mathfrak{Mod}}^{\mathrm{sp}}_{\alpha|_{[p,q]}}(A)$$

is a quasiisomorphism of differential graded algebraic spaces.

Proof. Here we use that Y is smooth to deduce that

$$\operatorname{Ext}^i_{\mathbb{O}_Y}(E, E) = \operatorname{Ext}^i_A(\Gamma_{[p,q]}E, \Gamma_{[p,q]}E),$$

for $q \gg p$. Then we use the fact that if π_0 agrees and tangent complex cohomologies agree, then a morphism of differential graded schemes is a quasiisomorphism. □

Corollary 4.5. *If $q \gg p$, then $\mathfrak{R}\widetilde{\mathfrak{Mod}}^{\mathrm{sp}}_{\alpha}(\mathbb{O}_Y)$ is quasiisomorphic to $\mathfrak{R}\widetilde{\mathfrak{Mod}}^{\mathrm{sp}}_{\alpha|_{[p,q]}}(A)$. Moreover, $\mathfrak{R}\widetilde{\mathfrak{Mod}}^{s}_{\alpha}(\mathbb{O}_Y)$ is an open and closed differential graded subscheme of $\mathfrak{R}\widetilde{\mathfrak{Mod}}^{\mathrm{sp}}_{\alpha|_{[p,q]}}(A)$.*

References

[Álvarez-Cónsul and King 2007] L. Álvarez-Cónsul and A. King, "A functorial construction of moduli of sheaves", *Invent. Math.* **168**:3 (2007), 613–666. MR 2008d:14015 Zbl 1137.14026

[Behrend and Fantechi 1997] K. Behrend and B. Fantechi, "The intrinsic normal cone", *Invent. Math.* **128**:1 (1997), 45–88. MR 98e:14022 Zbl 0909.14006

[Ciocan-Fontanine and Kapranov 2001] I. Ciocan-Fontanine and M. Kapranov, "Derived Quot schemes", *Ann. Sci. École Norm. Sup.* (4) **34**:3 (2001), 403–440. MR 2002k:14003 Zbl 1050.14042

[Ciocan-Fontanine and Kapranov 2009] I. Ciocan-Fontanine and M. Kapranov, "Virtual fundamental classes via dg-manifolds", *Geom. Topol.* **13**:3 (2009), 1779–1804. MR 2010e:14012 Zbl 1159.14002

[Gasharov 1997] V. Gasharov, "Extremal properties of Hilbert functions", *Illinois J. Math.* **41**:4 (1997), 612–629. MR 98m:13024 Zbl 0908.13009

[Gotzmann 1978] G. Gotzmann, "Eine Bedingung für die Flachheit und das Hilbertpolynom eines graduierten Ringes", *Math. Z.* **158**:1 (1978), 61–70. MR 58 #641 Zbl 0352.13009

[Huybrechts and Lehn 1997] D. Huybrechts and M. Lehn, *The geometry of moduli spaces of sheaves*, Aspects of Mathematics **E31**, Vieweg, Braunschweig, 1997. MR 98g:14012 Zbl 0872.14002

[King 1994] A. D. King, "Moduli of representations of finite-dimensional algebras", *Quart. J. Math. Oxford Ser.* (2) **45**:180 (1994), 515–530. MR 96a:16009 Zbl 0837.16005

[Loday 1992] J.-L. Loday, *Cyclic homology*, Grundlehren der Mathematischen Wissenschaften **301**, Springer, Berlin, 1992. MR 94a:19004 Zbl 0780.18009

[Lurie 2009] J. Lurie, *Higher topos theory*, Annals of Mathematics Studies **170**, Princeton University Press, Princeton, NJ, 2009. MR 2010j:18001 Zbl 1175.18001

[Manetti 1999] M. Manetti, "Deformation theory via differential graded Lie algebras", pp. 21–48 in *Seminari di geometria algebrica* (Pisa, 1998–1999), Scuola Normale Superiore, Pisa, 1999. MR 1754793

[Simpson 1994] C. T. Simpson, "Moduli of representations of the fundamental group of a smooth projective variety, I", *Inst. Hautes Études Sci. Publ. Math.* **79**:79 (1994), 47–129. MR 96e:14012 Zbl 0891.14005

[Thomas 2000] R. P. Thomas, "A holomorphic Casson invariant for Calabi-Yau 3-folds, and bundles on $K3$ fibrations", *J. Differential Geom.* **54**:2 (2000), 367–438. MR 2002b:14049 Zbl 1034.14015

[Toën and Vaquié 2007] B. Toën and M. Vaquié, "Moduli of objects in dg-categories", *Ann. Sci. École Norm. Sup.* (4) **40**:3 (2007), 387–444. MR 2009m:18015 Zbl 1140.18005

[Toën and Vezzosi 2004] B. Toën and G. Vezzosi, "From HAG to DAG: derived moduli stacks", pp. 173–216 in *Axiomatic, enriched and motivic homotopy theory*, NATO Sci. Ser. II Math. Phys. Chem. **131**, Kluwer Acad. Publ., Dordrecht, 2004. MR 2005f:14001 Zbl 1076.14002

[Toën and Vezzosi 2005] B. Toën and G. Vezzosi, "Homotopical algebraic geometry, I: Topos theory", *Adv. Math.* **193**:2 (2005), 257–372. MR 2007b:14038 Zbl 1120.14012

[Toën and Vezzosi 2008] B. Toën and G. Vezzosi, *Homotopical algebraic geometry, II: Geometric stacks and applications*, vol. 193, Mem. Amer. Math. Soc. **902**, Amer. Math. Soc., Providence, RI, 2008. MR 2009h:14004

[Weibel 1994] C. A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics **38**, Cambridge University Press, Cambridge, 1994. MR 95f:18001 Zbl 0797.18001

Communicated by Mikhail Kapranov
Received 2010-04-28 Revised 2012-09-03 Accepted 2012-11-21

behrend@math.ubc.ca — *Department of Mathematics, University of British Columbia, 1984 Mathematics Road, Vancouver BC V6T 1Z2, Canada*

ciocan@math.umn.edu — *School of Mathematics, University of Minnesota, 206 Church Street SE, Minneapolis, MN 55455, United States*

jhhwang@math.ubc.ca — *Department of Mathematics, University of British Columbia, 1984 Mathematics Road, Vancouver BC V6T 1Z2, Canada*

michael.a.j.rose@gmail.com — *Department of Mathematics, University of California, Berkeley, 970 Evans Hall, Berkeley, CA 94720, United States*

ALGEBRA AND NUMBER THEORY 8:4 (2014)
dx.doi.org/10.2140/ant.2014.8.813

Averages of the number of points on elliptic curves

Greg Martin, Paul Pollack and Ethan Smith

If E is an elliptic curve defined over $\mathbb{Q}$ and p is a prime of good reduction for E, let $E(\mathbb{F}_p)$ denote the set of points on the reduced curve modulo p. Define an arithmetic function $M_E(N)$ by setting $M_E(N) := \#\{p : \#E(\mathbb{F}_p) = N\}$. Recently, David and the third author studied the average of $M_E(N)$ over certain "boxes" of elliptic curves E. Assuming a plausible conjecture about primes in short intervals, they showed the following: for each N, the average of $M_E(N)$ over a box with sufficiently large sides is $\sim K^*(N)/\log N$ for an explicitly given function $K^*(N)$.

The function $K^*(N)$ is somewhat peculiar: defined as a product over the primes dividing N, it resembles a multiplicative function at first glance. But further inspection reveals that it is not, and so one cannot directly investigate its properties by the usual tools of multiplicative number theory. In this paper, we overcome these difficulties and prove a number of statistical results about $K^*(N)$. For example, we determine the mean value of $K^*(N)$ over all N, odd N and prime N, and we show that $K^*(N)$ has a distribution function. We also explain how our results relate to existing theorems and conjectures on the multiplicative properties of $\#E(\mathbb{F}_p)$, such as Koblitz's conjecture.

1. Introduction

Let E be an elliptic curve defined over the field $\mathbb{Q}$ of rational numbers. For the sake of concreteness, we assume that the affine points of E are given by a Weierstrass equation of the form

$$E : Y^2 = X^3 + aX + b, \tag{1}$$

where a and b are integers satisfying the condition $-16(4a^3 + 27b^2) \neq 0$. For any prime p where E has good reduction, we let $E(\mathbb{F}_p)$ denote the group of $\mathbb{F}_p$-points on the reduced curve. Kowalski [2006] introduced the arithmetic function $M_E(N)$, defined by

$$M_E(N) = \#\{p \text{ prime} : \#E(\mathbb{F}_p) = N\}.$$

MSC2010: primary 11G05; secondary 11N37, 11N60.
Keywords: elliptic curves, Koblitz conjecture, mean values of arithmetic functions.

The Hasse bound [1936a; 1936b; 1936c] implies that if p is counted by $M_E(N)$, then p lies between $(\sqrt{N}-1)^2$ and $(\sqrt{N}+1)^2$. Thus, $M_E(N)$ is a well-defined (finite) integer.

The problem of obtaining good estimates for $M_E(N)$ appears to be very difficult. The condition imposed by Hasse's bound together with an upper bound sieve gives the weak upper bound $M_E(N) \ll \sqrt{N}/\log(N+1)$ for any $N \geq 1$. Except in the case that E has complex multiplication, nothing stronger is known. As we will explain later, the average value of $M_E(N)$ as N varies over various sets of integers is related to some important theorems and conjectures in number theory. David and the third author established an "average value theorem" for $M_E(N)$ as E varies over a family of elliptic curves [David and Smith 2013]. That work was inspired by pioneering results of Fouvry and Murty [1996], who proved an average value theorem for counts of supersingular primes. Unfortunately, because of the restriction that all primes counted by $M_E(N)$ lie between $(\sqrt{N}-1)^2$ and $(\sqrt{N}+1)^2$, the result of [David and Smith 2013] is necessarily conditional upon a conjecture about the distribution of primes in short intervals (see Conjecture 1.5 below).

The main result of [David and Smith 2013] introduced a strange arithmetic function, which was called $K(N)$ because it is "almost a constant". In order to define $K(N)$, we recall the common notation $\nu_p(n)$ for the exact power of p that divides n, so that $n = \prod_p p^{\nu_p(n)}$. We also recall the Kronecker symbol $\left(\frac{a}{b}\right)$, an extension of the Jacobi symbol that is defined for all integers a and $b \neq 0$ (see, for instance, [Cohen 1993, Definition 1.4.8, p. 28]).

Definition 1.1. For any positive integer N, we define

$$K(N) = \prod_{p \nmid N}\left(1 - \frac{\left(\frac{N-1}{p}\right)^2 p + 1}{(p-1)^2(p+1)}\right)\prod_{p \mid N}\left(1 - \frac{1}{p^{\nu_p(N)}(p-1)}\right).$$

We also define $K^*(N) = K(N)N/\phi(N)$, where $\phi(N)$ is the usual Euler totient function.

As we will see later, it is actually the function $K^*(N)$ that has an interesting connection to the function $M_E(N)$. The purpose of the present work is a statistical study of the function $K^*(N)$. Our computations will illustrate a technique for dealing with arithmetic functions that have a form similar to, but are not exactly, multiplicative functions. Our first main result is the computation of the average value of K^*, first over all N and then over odd values of N.

Theorem 1.2. *For $x \geq 2$, we have*

$$\sum_{N \leq x} K^*(N) = x + O\left(\frac{x}{\log x}\right) \quad \textit{and} \quad \sum_{\substack{N \leq x \\ N \text{odd}}} K^*(N) = \frac{x}{3} + O\left(\frac{x}{\log x}\right).$$

Thus K^* has average value 1 on all N and average value $2/3$ on odd N.

Our second main result is the computation of the average value of K^* on primes. We employ the usual notation $\pi(x) = \#\{p \le x : p \text{ is prime}\}$.

Theorem 1.3. *Fix $A > 1$. For $x \ge 2$,*

$$\sum_{p \le x} K^*(p) = \tfrac{2}{3} C_2 J \pi(x) + O_A\left(\frac{x}{(\log x)^A}\right). \tag{2}$$

Here the constants C_2 and J are defined by

$$C_2 = \prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right), \tag{3}$$

and

$$J = \prod_{p>2}\left(1 + \frac{1}{(p-2)(p-1)(p+1)}\right). \tag{4}$$

Furthermore, the asymptotic formula (2) also holds for $\sum_{p \le x} K(p)$.

Remark. We have written C_2 and J as two separate constants because C_2 arises naturally by itself in the analysis of the function $K(N)$; see (5) below.

The technique we use to establish Theorems 1.2 and 1.3, which is dictated by the unusual Definition 1.1 for $K(N)$, is of interest in its own right: the function K looks much like a multiplicative function but actually is not. One can rewrite Definition 1.1 in the following form:

$$K(N) = C_2 F(N-1) G(N) \tag{5}$$

where C_2 is the twin primes constant defined in (3),

$$F(n) = \prod_{\substack{p \mid n \\ p>2}}\left(1 - \frac{1}{(p-1)^2}\right)^{-1} \prod_{p \mid n}\left(1 - \frac{1}{(p-1)^2(p+1)}\right), \tag{6}$$

and

$$G(n) = \prod_{\substack{p \mid n \\ p>2}}\left(1 - \frac{1}{(p-1)^2}\right)^{-1} \prod_{p^\alpha \| n}\left(1 - \frac{1}{p^\alpha(p-1)}\right). \tag{7}$$

So to understand the average value of $K(N)$, we are forced to deal with the correlation between the multiplicative function F, evaluated at $N-1$, and the multiplicative function G evaluated at the neighboring integer N. It is perhaps somewhat surprising that the average values of $C_2 F(N-1) G(N)$ described in Theorem 1.2 come out to simple rational numbers.

That we can successfully compute average values of the function K^*, even though it is not truly multiplicative, makes it natural to wonder whether we can analyze K^* in other ways; this is indeed the case. Our next result is an analogue for $K^*(N)$ of a classical result of Schoenberg [1928] for the function $n/\phi(n)$. Recall that a *distribution function* $D(u)$ is a nondecreasing, right-continuous function $D : \mathbb{R} \to [0, 1]$ for which $\lim_{u\to-\infty} D(u) = 0$ and $\lim_{u\to\infty} D(u) = 1$.

Theorem 1.4. *The function K^* possesses a distribution function relative to the set of all natural numbers N. In other words, there exists a distribution function $D(u)$ with the property that at each of its points of continuity,*

$$D(u) = \lim_{x\to\infty} \frac{1}{x}\#\{N \le x : K^*(N) \le u\}.$$

As a consequence of Theorems 1.2 and 1.3, we are able to show that the main result of [David and Smith 2013] is consistent with various unconditional results. As mentioned above, the restriction imposed by the Hasse bound creates a short-interval problem in any study of $M_E(N)$ when N is held fixed. Indeed, the interval is so short that not even the Riemann hypothesis is any help. This problem is circumvented in [David and Smith 2013] by assuming a conjecture in the spirit of the classical Barban–Davenport–Halberstam theorem.

Conjecture 1.5. *Recall the notation*

$$\theta(x; q, a) = \sum_{\substack{p\le x\\ p\equiv a \ (\mathrm{mod}\ q)}} \log p.$$

Let $0 < \eta \le 1$ and $\beta > 0$ be real numbers. Suppose that X, Y, and Q are positive real numbers satisfying $X^\eta \le Y \le X$ and $Y/(\log X)^\beta \le Q \le Y$. Then

$$\sum_{q\le Q} \sum_{\substack{1\le a\le q\\ (a,q)=1}} \left| \theta(X+Y; q, a) - \theta(X; q, a) - \frac{Y}{\phi(q)} \right|^2 \ll_{\eta,\beta} Y Q \log X.$$

Remark. Languasco, Perelli, and Zaccagnini [Languasco et al. 2010] have established Conjecture 1.5 in the range $\eta > \frac{7}{12}$; they also showed, assuming the generalized Riemann hypothesis, that any $\eta > \frac{1}{2}$ is admissible.

Given integers a and b satisfying $-16(4a^3 + 27b^2) \ne 0$, let $E_{a,b}$ denote the elliptic curve given by the Weierstrass equation (1). Then, given positive parameters A and B, let $\mathscr{E}(A, B)$ denote the set defined by

$$\mathscr{E}(A, B) = \{E_{a,b} : |a| \le A, |b| \le B, -16(4a^3 + 27b^2) \ne 0\}.$$

David and Smith [2013; 2014] established the following average value theorem (in fact a stronger version of it) for $M_E(N)$ taken over the family $\mathscr{E}(A, B)$.

Proposition 1.6. *Assume the Barban–Davenport–Halberstam estimate* (Conjecture 1.5) *holds for some* $\eta < \frac{1}{2}$. *Let* ϵ *be a positive real number, and let* $A > N^{1/2+\epsilon}$ *and* $B > N^{1/2+\epsilon}$ *be real numbers satisfying* $AB > N^{3/2+\epsilon}$. *Then, for any positive real number* R,

$$\frac{1}{\#\mathscr{E}(A,B)} \sum_{E\in\mathscr{E}(A,B)} M_E(N) = \frac{K^*(N)}{\log N} + O_{\eta,\epsilon,R}\left(\frac{1}{(\log N)^R}\right).$$

Remarks. (1) It is not necessary to assume that Conjecture 1.5 holds for a fixed $\eta < 1/2$. It is enough to assume that it holds for $Y = \sqrt{X}/(\log X)^{\beta+2}$.

(2) The originally published formula in [David and Smith 2013] contained an error in the definition of $K^*(N)$, which was corrected in [David and Smith 2014] to the form given in Definition 1.1. See the end of Section 2 for further discussion of the original version of $K^*(N)$.

(3) The proof of Proposition 1.6 given in [David and Smith 2013] is restricted to odd values of N, but further work by Chandee, Koukoulopoulos, David, and Smith [Chandee et al. 2014] establishes the proposition for even values of N as well.

We note, as in [Kowalski 2006], that computing the average value of $M_E(N)$ over the integers $N \le x$ is easily seen to be equivalent to the prime number theorem. In particular,

$$\sum_{N\le x} M_E(N) = \sum_{p\le(\sqrt{x}+1)^2} \#\{N \le x : \#E(\mathbb{F}_p) = N\} = \pi(x) + O(\sqrt{x}). \tag{8}$$

Similarly, the average value of $M_E(N)$ taken over the integers $N \le x$ that satisfy a congruence condition is equivalent to an appropriate application of the Chebotarev density theorem. For example, if the 2-division field of E is an S_3-extension of $\mathbb{Q}$, then the Chebotarev density theorem implies that

$$\sum_{\substack{N\le x\\ N \text{ odd}}} M_E(N) \sim \frac{1}{3}\frac{x}{\log x}.$$

(The calculation of the constant $\frac{1}{3}$ reduces to the fact that two-thirds of the elements of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, which is the automorphism group of $E[2]$, have even trace.) If E is given by the Weierstrass equation (1), the 2-division field is easily seen to be the splitting field of the polynomial $X^3 + aX + b$. Since almost all cubics (when ordered by height) have S_3 as their Galois groups, it seems reasonable to conjecture that

$$\frac{1}{\#\mathscr{E}(A,B)} \sum_{\substack{N\le x\\ N \text{ odd}}} \sum_{E\in\mathscr{E}(A,B)} M_E(N) = \frac{x}{3\log x} + O\left(\frac{x}{(\log x)^2}\right), \tag{9}$$

provided that A and B are growing fast enough with respect to x. A precise version of this conjecture was established by Banks and Shparlinski [2009, Theorem 19]. (In fact, their theorem shows that an analogous estimate holds with the condition "N odd" replaced by "$m \nmid N$", for any given integer m.) The asymptotic result (9), together with the result of Theorem 1.2 for odd N, shows that if we average the two sides of the equation in Proposition 1.6, we obtain consistent results (unconditionally). Similarly, the result of Theorem 1.2 for all N allows us to infer the asymptotic formula

$$\frac{1}{\#\mathscr{E}(A,B)} \sum_{N \le x} \sum_{E \in \mathscr{E}(A,B)} M_E(N) = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right),$$

which is consistent with (8). We can therefore, if we wish, view Theorem 1.2 as additional evidence for the conclusion of Proposition 1.6.

A similar problem arises if we consider only primes p. Computing the average value of $M_E(p)$ over the primes $p \le x$ is easily seen to be equivalent to the famous Koblitz conjecture [1988]:

Conjecture 1.7 (Koblitz). *Given an elliptic curve E defined over the rational field $\mathbb{Q}$, there exists a constant $C(E)$ with the property that as $x \to \infty$,*

$$\sum_{\substack{p \le x \\ p \text{ prime}}} M_E(p) \sim C(E) \frac{x}{(\log x)^2}.$$

The constant $C(E)$ appearing in Koblitz's conjecture may be zero, in which case the asymptotic is interpreted to mean that there are only finitely many primes p such that $M_E(p) > 0$. An obvious obstruction to there being infinitely many primes with $M_E(p) > 0$ is for E to be isogenous to a curve possessing nontrivial rational torsion. It was once thought that this was the only case when $C(E) = 0$, but this turned out to be false; see [Zywina 2011, Section 1.1] for an explicit counterexample due to Nathan Jones.

The main theorem of [Balog et al. 2011] may be reinterpreted to say that the asymptotic formula

$$\begin{aligned} \frac{1}{\#\mathscr{E}(A,B)} \sum_{\substack{p \le x \\ p \text{ prime}}} \sum_{E \in \mathscr{E}(A,B)} M_E(p) &= \tfrac{2}{3} C_2 J \int_2^x \frac{dt}{(\log t)^2} + O_A\left(\frac{x}{(\log x)^A}\right) \\ &= \tfrac{2}{3} C_2 J \frac{x}{(\log x)^2} + O\left(\frac{x}{(\log x)^3}\right) \qquad (10) \end{aligned}$$

holds unconditionally for A and B growing fast enough with respect to x. Jones [2009] has averaged the explicit formula for $C(E)$ over the family $\mathscr{E}(A, B)$ and shown that the result is consistent with the above formula. We view this as good evidence for the Koblitz conjecture. Equation (10), together with our Theorem 1.3, shows that we obtain consistent results (unconditionally) when we average the two sides of the equation in Proposition 1.6 over the primes $N \le x$. Thus all of the conjectures and conditional theorems mentioned above reinforce one another's validity.

We note that the asymptotic formulas (9) and (10), in which we average over odd integers N or primes p up to x, both hold for a much wider range of A and B than is suggested by Proposition 1.6. In particular, Banks and Shparlinski [2009] developed a character-sum argument based on a large sieve inequality to show that one may take $A, B > x^{\epsilon}$ and $AB > x^{1+\epsilon}$ in elliptic-curve averaging problems of this sort, when the average number of elliptic curve isomorphism classes modulo p satisfying the desired property is somewhat large. Baier [2009] was able to adapt this technique to make similar improvements to the required length of the average in the (fixed trace) Lang–Trotter problem, where the average number of classes modulo p is significantly smaller. Given Baier's result, it seems possible that Proposition 1.6, in which the odd integer N is fixed, could itself be shown to hold provided that $A, B > N^{\epsilon}$ (note that such an improvement would still seem to require that $AB > N^{3/2+\epsilon}$ rather than the weaker condition $AB > N^{1+\epsilon}$). As we are primarily concerned with the multiplicative function K^* herein, however, we have not pursued this line of thinking.

The remainder of the article is organized as follows. We begin by establishing Theorem 1.2 in Section 2. Briefly, we approximate the function $K^*(N)$ by a similar function whose values depend only upon the small primes dividing N and $N-1$; we then calculate the average value of this truncated function by partitioning the numbers being averaged over into "configurations" based on local data about N and $N-1$ at these small primes. We prove the related Theorem 1.3 in Section 3; here the calculation of the main term is simpler since the argument of K^* is always a prime, while the estimation of the error term is more complicated due to the need to invoke results on the distribution of primes in arithmetic progressions. Finally, we establish Theorem 1.4 in Section 4 by studying the moments of K^*.

Notation. As above, we employ the Landau–Bachmann o and O notation, as well as the associated Vinogradov symbols $\ll$, $\gg$ with their usual meanings; any dependence of implied constants on other parameters is denoted with subscripts. We reserve the letters ℓ and p for prime variables. For each natural number n, we let $P(n)$ denote the largest prime factor of n, with the convention that $P(1) = 1$. The natural number n is said to be *y-friable* (sometimes called *y-smooth*) if $P(n) \le y$. We write $\Psi(x, y)$ for the number of y-friable integers not exceeding x. By a *partition* of a set S, we mean any collection of disjoint sets whose union is S; we do *not* require that all of the sets in the collection be nonempty.

2. The average value of K^*

For notational convenience, set $R(N) := N/\phi(N)$, so that $K^*(N) = K(N)R(N)$. By definition, $K(N)$ is a product over primes, while $R(N) = \prod_{\ell \mid N}(1-1/\ell)^{-1}$ can also be viewed as such a product. Moreover, it is the small primes that have the largest influence on the magnitude of these products. This suggests it might be useful to study the truncated functions K_z and R_z defined by

$$K_z(N) := \prod_{\substack{p\nmid N\\ p\le z}}\left(1-\frac{\left(\frac{N-1}{p}\right)^2 p+1}{(p-1)^2(p+1)}\right)\prod_{\substack{p\mid N\\ p\le z}}\left(1-\frac{1}{p^{\nu_p(N)}(p-1)}\right)$$

and

$$R_z(N) := \prod_{\substack{p\mid N\\ p\le z}}(1-1/p)^{-1}.$$

We give the proof of the first half of Theorem 1.2, concerning the average of $K(N)R(N)$ over all N, in complete detail. The proof of the second claim, concerning the average over odd N, can be proved in the same way; the necessary changes to the argument are indicated briefly at the end of this section.

The first half of Theorem 1.2 will be deduced from a corresponding estimate for the mean value of $K_z(N)R_z(N)$:

Proposition 2.1. *Let $x \ge 3$, and set $z := \frac{1}{10}\log x$. We have*

$$\sum_{N\le x} K_z(N)R_z(N) = x + O(x^{3/4}).$$

We will establish this proposition at the end of this section (it follows upon combining Lemmas 2.7 and 2.8). At this point, we show how Theorem 1.2 can be deduced from the proposition.

Proof of Theorem 1.2, assuming Proposition 2.1. It suffices to show that with $z = \frac{1}{10}\log x$,

$$\sum_{N\le x} |K_z(N)R_z(N) - K(N)R(N)| \ll x/z. \tag{11}$$

Now $0 \le K(N) \le K_z(N) \le 1$ and $0 \le R_z(N) \le R(N)$, so that

$$\begin{aligned}|K_z(N)R_z(N)-K(N)R(N)| &\le |K_z(N)||R_z(N)-R(N)|+|K_z(N)-K(N)|R(N)\\ &\le (R(N)-R_z(N))+(K_z(N)-K(N))R(N).\end{aligned}$$

Thus, it is enough to show that the sums of $R(N)-R_z(N)$ and $(K_z(N)-K(N))R(N)$ up to x are also $\ll x/z$.

Write $R(N) = \sum_{d \mid n} g(d)$ for an auxiliary function g. By a straightforward calculation with the Möbius inversion formula, we see that g vanishes except at squarefree integers d, for which $g(d) = 1/\phi(d)$. Hence, for all real $t > 0$,

$$\sum_{N \le t} R(N) = \sum_{N \le t} \sum_{d \mid N} g(d) = \sum_{d \le t} \frac{1}{\phi(d)} \sum_{\substack{N \le t \\ d \mid N}} 1 \le \sum_{d \le t} \frac{t}{d\phi(d)} \le t \sum_{d=1}^{\infty} \frac{1}{d\phi(d)}$$
$$= t \prod_p \left(1 + \frac{1}{p(p-1)} + \frac{1}{p^3(p-1)} + \cdots\right)$$
$$\ll t, \tag{12}$$

so that $R(N)$ is bounded on average. Now writing $R_z(N) = \sum_{d \mid n} g_z(d)$ for an auxiliary function $g_z(d)$, one finds that g_z vanishes except on squarefree z-friable integers d, where again $g_z(d) = 1/\phi(d)$. In particular, $g(d) - g_z(d)$ is nonnegative for all d, and $g(d) - g_z(d) = 0$ when $d \le z$. We deduce that

$$\sum_{N \le x} (R(N) - R_z(N)) = \sum_{N \le x} \sum_{d \mid N} (g(d) - g_z(d)) \le \sum_{N \le x} \sum_{\substack{d \mid N \\ d > z}} \frac{1}{\phi(d)}$$
$$= \sum_{z < d \le x} \sum_{\substack{N \le x \\ d \mid N}} \frac{1}{\phi(d)} \le \sum_{d > z} \frac{x}{d\phi(d)}.$$

Partitioning this last sum into dyadic intervals, we have

$$\sum_{N \le x} (R(N) - R_z(N)) \le \sum_{k=1}^{\infty} \sum_{2^{k-1}z < d \le 2^k z} \frac{x}{d\phi(d)} = x \sum_{k=1}^{\infty} \sum_{2^{k-1}z < d \le 2^k z} \frac{R(d)}{d^2}$$
$$\le x \sum_{k=1}^{\infty} \frac{1}{(2^{k-1}z)^2} \sum_{d \le 2^k z} R(d) \ll x \sum_{k=1}^{\infty} \frac{1}{(2^{k-1}z)^2} 2^k z$$
$$\ll \frac{x}{z} \sum_{k=1}^{\infty} \frac{1}{2^k} \ll \frac{x}{z},$$

where we used the estimate (12) in the second-to-last inequality. This proves the desired upper bound for the partial sums of $R(N) - R_z(N)$.

The partial sums of $(K_z(N) - K(N))R(N)$ are easier. Since each factor appearing in the products defining K_z and K has the form $1 - O(1/\ell^2)$, it follows that $K(N)/K_z(N) \ge 1 - O\big(\sum_{\ell > z} 1/\ell^2\big) \ge 1 - O(1/z)$. Thus, $K_z(N) - K(N) = K_z(N)(1 - K(N)/K_z(N)) \le 1 - K(N)/K_z(N) \ll 1/z$. It follows that

$$\sum_{N \le x} (K_z(N) - K(N))R(N) \ll \frac{1}{z} \sum_{N \le x} R(N) \ll \frac{x}{z},$$

using the estimate (12) once more in the last step. This completes the proof of Theorem 1.2, assuming Proposition 2.1. □

In the remainder of this section, we concentrate on proving Proposition 2.1. Our strategy, already alluded to in the introduction, is to partition the integers $N \le x$ according to local data at small primes. We choose the partition so that the values $K_z(N)$ and $R_z(N)$ are constant along each set belonging to the partition (which we call a *configuration*). For the remainder of this section, we continue to assume that $x \ge 3$ and that $z = \frac{1}{10}\log x$.

Definition 2.2. We define the *configuration space* $\mathscr{S}$ as the set of all 4-tuples of the form

$$(\mathscr{A}, \mathscr{B}, \mathscr{C}, \{e_\ell\}_{\ell\in\mathscr{B}}),$$

where the sets $\mathscr{A}, \mathscr{B}, \mathscr{C}$ partition the set of primes up to z and the e_ℓ are positive integers. (Although $\mathscr{S}$ depends upon z and hence x, we will not include this dependence in the notation.)

To each $N \le x$, we can associate a unique configuration in the following manner.

Definition 2.3. Given $N \le x$, define three subsets of the primes in $[2, z]$ by setting $\mathscr{A} := \{\ell \le z : \ell \nmid N(N-1)\}$, $\mathscr{B} := \{\ell \le z : \ell \mid N\}$, and $\mathscr{C} := \{\ell \le z : \ell \mid N-1\}$. For each $\ell \in \mathscr{B}$, set $e_\ell := \nu_\ell(N)$. Then $\sigma = (\mathscr{A}, \mathscr{B}, \mathscr{C}, \{e_\ell\}_{\ell\in\mathscr{B}}) \in \mathscr{S}$ is called the *configuration* σ corresponding to N and is denoted σ_N.

Remark. One checks easily that the value $K_z(N)R_z(N)$ depends only on $\sigma = \sigma_N$. Thus, we often abuse notation by referring to $K_z(\sigma)$ and $R_z(\sigma)$ instead of $K_z(N)$ and $R_z(N)$.

We can rewrite the sum considered in Proposition 2.1 in the form

$$\sum_{N\le x} K_z(N)R_z(N) = \sum_{\sigma\in\mathscr{S}} K_z(\sigma)R_z(\sigma) \sum_{\substack{N\le x\\ \sigma_N=\sigma}} 1. \tag{13}$$

In the next lemma, we estimate the inner sum on the right side of (13) in two ways.

Lemma 2.4. *For each $\sigma \in \mathscr{S}$, we have*

$$\sum_{\substack{N\le x\\ \sigma_N=\sigma}} 1 = d_\sigma x + O(x^{1/5}), \tag{14}$$

where

$$d_\sigma := \left(\prod_{\ell\in\mathscr{A}}(1-2/\ell)\right)\left(\prod_{\ell\in\mathscr{B}}\frac{1}{\ell^{e_\ell}}(1-1/\ell)\right)\left(\prod_{\ell\in\mathscr{C}}\frac{1}{\ell}\right). \tag{15}$$

We also have the crude upper bound

$$\sum_{\substack{N \le x \\ \sigma_N = \sigma}} 1 \le x \prod_{\ell \in \mathscr{B}} \ell^{-e_\ell} \tag{16}$$

for any $\sigma \in \mathscr{S}$.

Proof. The condition that $\sigma_N = \sigma$ is equivalent to a congruence condition on N modulo

$$m_\sigma := \Bigg(\prod_{\ell \in \mathscr{A} \cup \mathscr{C}} \ell \Bigg) \Bigg(\prod_{\ell \in \mathscr{B}} \ell^{e_\ell + 1} \Bigg). \tag{17}$$

Indeed, $\sigma_N = \sigma$ precisely when N belongs to a union of $\prod_{\ell \in \mathscr{A}} (\ell - 2) \prod_{\ell \in \mathscr{B}} (\ell - 1)$ congruence classes modulo m_σ. This implies that

$$\sum_{\substack{N \le x \\ \sigma_N = \sigma}} 1 = \frac{x}{m_\sigma} \prod_{\ell \in \mathscr{A}} (\ell - 2) \prod_{\ell \in \mathscr{B}} (\ell - 1) + O\Bigg(\prod_{\ell \in \mathscr{A} \cup \mathscr{B}} \ell \Bigg) = d_\sigma x + O\Bigg(\prod_{\ell \le z} \ell \Bigg).$$

By our choice of z and the prime number theorem, $\prod_{\ell \le z} \ell < x^{1/5}$ for large x, and so we have established the formula (14). To justify the inequality (16), it suffices to observe that if $\sigma_N = \sigma$, then $\prod_{\ell \in \mathscr{B}} \ell^{e_\ell}$ divides N. □

The modulus m_σ, defined in (17), will continue to play a key role in subsequent arguments. It will be convenient to know that m_σ nearly determines σ; this is the substance of our next result.

Lemma 2.5. *For each natural number* m, *the number of* $\sigma \in \mathscr{S}$ *with* $m_\sigma = m$ *is* $O(x^{1/4})$.

Proof. Suppose that $m_\sigma = m$, where $\sigma = (\mathscr{A}, \mathscr{B}, \mathscr{C}, \{e_\ell\}_{\ell \in \mathscr{B}})$. Since the sets $\mathscr{A}, \mathscr{B}, \mathscr{C}$ partition the primes up to z, the number of possibilities for these sets is $3^{\pi(z)} = \exp(O(\log x / \log\log x)) = x^{o(1)}$. Having chosen these sets, the exponents e_ℓ, for $\ell \in \mathscr{B}$, are determined by the prime factorization of m. This proves the lemma with $\frac{1}{4}$ replaced by any positive ϵ. □

We next investigate two sums over m_σ for future use in estimating error terms.

Lemma 2.6. *For each* $\sigma \in \mathscr{S}$, *define* m_σ *by* (17). *Then for all* $x \ge 3$,

$$x^{6/5} \log\log x \sum_{\substack{\sigma \in \mathscr{S} \\ m_\sigma > x}} \frac{1}{m_\sigma} + x^{1/5} \log\log x \sum_{\substack{\sigma \in \mathscr{S} \\ m_\sigma \le x}} 1 \ll x^{3/4}. \tag{18}$$

Proof. We proceed by Rankin's method:

$$
\begin{aligned}
x^{6/5} \log\log x \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma > x}} \frac{1}{m_\sigma} &+ x^{1/5}\log\log x \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma \le x}} 1 \\
&\le x^{6/5}\log\log x \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma > x}} \left(\frac{m_\sigma}{x}\right)^{7/8} \frac{1}{m_\sigma} + x^{1/5}\log\log x \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma \le x}} \left(\frac{x}{m_\sigma}\right)^{1/8} \\
&= x^{13/40}\log\log x \sum_{\sigma\in\mathscr{S}} \frac{1}{m_\sigma^{1/8}}.
\end{aligned}
$$

Every value of m_σ is z-friable, and there are at most $x^{1/4}$ configurations $\sigma\in\mathscr{S}$ for every possible value of m_σ by Lemma 2.5. Therefore

$$
\begin{aligned}
x^{13/40}\log\log x \sum_{\sigma\in\mathscr{S}} \frac{1}{m_\sigma^{1/8}} &\ll x^{13/40}\log\log x \cdot x^{1/4} \sum_{m\ z\text{-friable}} \frac{1}{m^{1/8}} \\
&= x^{23/40}\log\log x \prod_{p\le z}\left(1+\frac{1}{p^{1/8}}+\frac{1}{p^{1/4}}+\cdots\right) \\
&= x^{23/40}\log\log x \prod_{p\le z}\left(1-\frac{1}{p^{1/8}}\right)^{-1}.
\end{aligned}
$$

Each factor in the product is at most $(1-2^{-1/8})^{-1} < 13$, and so the product is less than $13^{\pi(z)} = 13^{O(\log x/\log\log x)} = x^{o(1)}$. Thus the left-hand side of (18) is $\ll x^{23/40+o(1)}\log\log x \ll x^{3/4}$ as claimed. □

The next lemma relates the mean value of $K_z(N)R_z(N)$, taken over odd N, to the sum of $K_z(\sigma)R_z(\sigma)d_\sigma$, taken over all configurations σ.

Lemma 2.7. *For all $x\ge 3$,*

$$
\sum_{N\le x} K_z(N)R_z(N) = x\sum_{\sigma\in\mathscr{S}} K_z(\sigma)R_z(\sigma)d_\sigma + O(x^{3/4}).
$$

Proof. We begin by noting that the upper bounds

$$
\begin{aligned}
&0\le K(N)\le K_z(N)\le 1,\\
&0\le R_z(N)\le R(N)\ll \log\log x
\end{aligned}
\tag{19}
$$

are valid for all $N\le x$. We have

$$\begin{aligned}\sum_{N\le x} K_z(N)R_z(N) &= \sum_{\sigma\in\mathscr{S}} K_z(\sigma)R_z(\sigma) \sum_{\substack{N\le x\\ \sigma_N=\sigma}} 1\\ &= \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma\le x}} K_z(\sigma)R_z(\sigma) \sum_{\substack{N\le x\\ \sigma_N=\sigma}} 1 + \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma> x}} K_z(\sigma)R_z(\sigma) \sum_{\substack{N\le x\\ \sigma_N=\sigma}} 1\\ &= \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma\le x}} K_z(\sigma)R_z(\sigma)(d_\sigma x + O(x^{1/5}))\\ &\qquad + O\Bigl(\sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma> x}} K_z(\sigma)R_z(\sigma)x\prod_{\ell\in\mathscr{B}}\ell^{-e_\ell}\Bigr)\end{aligned}$$

by Lemma 2.4. Using the upper bounds (19) for K_z and R_z, we deduce after extending the first sum to infinity that

$$\begin{aligned}\sum_{N\le x} K_z(N)R_z(N) &= x\sum_{\sigma\in\mathscr{S}} K_z(\sigma)R_z(\sigma)d_\sigma + O\Bigl(x\log\log x \sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma> x}} d_\sigma\Bigr)\\ &\qquad + O\Bigl(x^{1/5}\log\log x\sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma\le x}} 1 + x\log\log x\sum_{\substack{\sigma\in\mathscr{S}\\ m_\sigma> x}}\prod_{\ell\in\mathscr{B}}\ell^{-e_\ell}\Bigr);\end{aligned}$$

since the inequality $d_\sigma \le \prod_{\ell\in\mathscr{B}}\ell^{-e_\ell}$ follows from definition (15), the first error term is dominated by the second. Because $\prod_{\ell\in\mathscr{B}}\ell^{-e_\ell} = m_\sigma^{-1}\prod_{\ell\le z}\ell < m_\sigma^{-1}x^{1/5}$ once x is large, this error term is $\ll x^{3/4}$ by Lemma 2.6, and the proof is complete. □

In view of Lemma 2.7, Proposition 2.1 is a consequence of this remarkable identity:

Lemma 2.8.
$$\sum_{\sigma\in\mathscr{S}} K_z(\sigma)R_z(\sigma)d_\sigma = 1.$$

Proof. Referring back to the definitions of K_z and R_z, we see that for $\sigma\in\mathscr{S}$,

$$\begin{aligned}K_z(\sigma)R_z(\sigma) &= \prod_{\ell\in\mathscr{A}}\Bigl(1-\frac{1}{(\ell-1)^2}\Bigr)\times\prod_{\ell\in\mathscr{B}}\Bigl(1-\frac{1}{\ell^{e_\ell}(\ell-1)}\Bigr)\Bigl(1-\frac{1}{\ell}\Bigr)^{-1}\\ &\qquad\times\prod_{\ell\in\mathscr{C}}\Bigl(1-\frac{1}{(\ell-1)^2(\ell+1)}\Bigr).\end{aligned}\tag{20}$$

Multiplying by the expression (15) for d_σ, we find that

$$\begin{aligned}K_z(\sigma)R_z(\sigma)d_\sigma &= \Bigl(\prod_{\ell\in\mathscr{A}}\frac{\ell-2}{\ell-1}\Bigr)^2\times\prod_{\ell\in\mathscr{B}}\frac{1}{\ell^{e_\ell}}\Bigl(1-\frac{1}{\ell^{e_\ell}(\ell-1)}\Bigr)\\ &\qquad\times\prod_{\ell\in\mathscr{C}}\frac{\ell^2-\ell-1}{(\ell-1)^2(\ell+1)}.\end{aligned}\tag{21}$$

Recall that σ is a 4-tuple with entries $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$, and $\{e_\ell\}_{\ell\in\mathscr{B}}$. We sum the expression (21) over the possibilities for $\{e_\ell\}$. We have

$$\sum_{\substack{\{e_\ell\}\\ \text{each } e_\ell\geq 1}} \prod_{\ell\in\mathscr{B}} \frac{1}{\ell^{e_\ell}}\left(1-\frac{1}{\ell^{e_\ell}(\ell-1)}\right) = \prod_{\ell\in\mathscr{B}} \sum_{e_\ell=1}^{\infty} \frac{1}{\ell^{e_\ell}}\left(1-\frac{1}{\ell^{e_\ell}(\ell-1)}\right).$$

By a short computation,

$$\sum_{e_\ell=1}^{\infty} \frac{1}{\ell^{e_\ell}}\left(1-\frac{1}{\ell^{e_\ell}(\ell-1)}\right) = \frac{\ell^2-2}{(\ell+1)(\ell-1)^2}.$$

Thus, if we now fix only $\mathscr{A}$, $\mathscr{B}$, and $\mathscr{C}$ and sum over all corresponding configurations σ, we have

$$\begin{aligned}
\sum_{\substack{\sigma\in\mathscr{S}\\ \mathscr{A},\mathscr{B},\mathscr{C}\text{ fixed}}} K_z(\sigma)R_z(\sigma)d_\sigma
&= \left(\prod_{\ell\in\mathscr{A}} \frac{\ell-2}{\ell-1}\right)^2 \left(\prod_{\ell\in\mathscr{B}} \frac{\ell^2-2}{(\ell+1)(\ell-1)^2}\right)\left(\prod_{\ell\in\mathscr{C}} \frac{\ell^2-\ell-1}{(\ell-1)^2(\ell+1)}\right)\\
&= \left(\prod_{\ell\in\mathscr{A}} P_{\mathscr{A}}(\ell)\right)\left(\prod_{\ell\in\mathscr{B}} P_{\mathscr{B}}(\ell)\right)\left(\prod_{\ell\in\mathscr{C}} P_{\mathscr{C}}(\ell)\right), \qquad (22)
\end{aligned}$$

where for notational convenience we have defined

$$P_{\mathscr{A}}(\ell) = \left(\frac{\ell-2}{\ell-1}\right)^2, \quad P_{\mathscr{B}}(\ell) = \frac{\ell^2-2}{(\ell+1)(\ell-1)^2}, \quad P_{\mathscr{C}}(\ell) = \frac{\ell^2-\ell-1}{(\ell-1)^2(\ell+1)}. \qquad (23)$$

To finish the proof, we sum the right-hand side of (22) over all possibilities for $\mathscr{A}$, $\mathscr{B}$, and $\mathscr{C}$. The only condition on the sets $\mathscr{A}$, $\mathscr{B}$, and $\mathscr{C}$ is that they partition the set of primes not exceeding z. Hence,

$$\begin{aligned}
\sum_{\sigma\in\mathscr{S}} K_z(\sigma)R_z(\sigma)d_\sigma &= \sum_{\substack{\mathscr{A},\mathscr{B},\mathscr{C}\text{ disjoint}\\ \mathscr{A}\cup\mathscr{B}\cup\mathscr{C}=\{\ell\leq z\}}} \left(\prod_{\ell\in\mathscr{A}} P_{\mathscr{A}}(\ell)\right)\left(\prod_{\ell\in\mathscr{B}} P_{\mathscr{B}}(\ell)\right)\left(\prod_{\ell\in\mathscr{C}} P_{\mathscr{C}}(\ell)\right)\\
&= \prod_{\ell\leq z}(P_{\mathscr{A}}(\ell)+P_{\mathscr{B}}(\ell)+P_{\mathscr{C}}(\ell)).
\end{aligned}$$

However, $P_{\mathscr{A}}(\ell)+P_{\mathscr{B}}(\ell)+P_{\mathscr{C}}(\ell)=1$, identically! This completes the proof of the lemma, and so also of Proposition 2.1. □

As already remarked above, the first half of Theorem 1.2 follows immediately upon combining Lemmas 2.7 and 2.8.

Proof of the second half of Theorem 1.2. The condition that N is odd amounts to the requirement that $2\in\mathscr{C}$ in the configuration notation of this section. If we carry this requirement through the proofs of Lemmas 2.7 and 2.8, the bulk of the argument is essentially unchanged, but the new conclusions are that

$$\sum_{\substack{N\le x\\ 2\nmid N}} K_z(N)R_z(N) = x\sum_{\substack{\sigma\in\mathscr{S}\\ 2\in\mathscr{C}}} K_z(\sigma)R_z(\sigma)\,d_\sigma + O(x^{3/4})$$

and

$$\begin{aligned}\sum_{\substack{\sigma\in\mathscr{S}\\ 2\in\mathscr{C}}} K_z(\sigma)R_z(\sigma)\,d_\sigma &= \sum_{\substack{\mathscr{A},\mathscr{B},\mathscr{C}\text{ disjoint}\\ \mathscr{A}\cup\mathscr{B}\cup\mathscr{C}=\{\ell\le z\}\\ 2\in\mathscr{C}}}\Bigl(\prod_{\ell\in\mathscr{A}} P_{\mathscr{A}}(\ell)\Bigr)\Bigl(\prod_{\ell\in\mathscr{B}} P_{\mathscr{B}}(\ell)\Bigr)\Bigl(\prod_{\ell\in\mathscr{C}} P_{\mathscr{C}}(\ell)\Bigr)\\ &= P_C(2)\prod_{2<\ell\le z}(P_{\mathscr{A}}(\ell)+P_{\mathscr{B}}(\ell)+P_{\mathscr{C}}(\ell)) = P_C(2).\end{aligned}$$

(We assume in going from the first line to the second that $z\ge 2$, i.e., that $x\ge e^{20}$.) Since $P_C(2)=\frac{1}{3}$, the second half of Theorem 1.2 follows. □

Most mathematical coincidences have explanations, of course, and the magical-seeming $P_{\mathscr{A}}(\ell)+P_{\mathscr{B}}(\ell)+P_{\mathscr{C}}(\ell)=1$ is no different. One might guess that $P_{\mathscr{A}}(\ell)$, $P_{\mathscr{B}}(\ell)$, and $P_{\mathscr{C}}(\ell)$ are probabilities of certain events occurring, and this is exactly right: as γ ranges over all elements of $\mathrm{GL}_2(\mathbb{F}_\ell)$, the expression $\det(\gamma)+1-\operatorname{tr}(\gamma)$ is congruent to 0 (mod ℓ) with probability $P_{\mathscr{B}}(\ell)$, congruent to 1 (mod ℓ) with probability $P_{\mathscr{C}}(\ell)$, and congruent to each of the $\ell-2$ other residue classes with probability $P_{\mathscr{A}}(\ell)/(\ell-2)$. (See [David and Wu 2012, Equation (2.2)] for this computation, as well as for the precise connection to elliptic curves.)

We conclude this section by saying a few words about the function that was originally published in [David and Smith 2013], which we will here call K° to avoid confusion with the corrected function K^*. For N odd, let

$$\begin{aligned}K^\circ(N) = \frac{N}{\phi(N)}\prod_{p\nmid N}\left(1-\frac{\left(\frac{N-1}{p}\right)^2 p+1}{(p-1)^2(p+1)}\right)\prod_{\substack{p\mid N\\ 2\nmid\nu_p(N)}}\left(1-\frac{1}{p^{\nu_p(N)}(p-1)}\right)\\ \times\prod_{\substack{p\mid N\\ 2\mid\nu_p(N)}}\left(1-\frac{p-\left(\frac{-N_p}{p}\right)}{p^{\nu_p(N)+1}(p-1)}\right),\end{aligned}$$

where $N_p=N/p^{\nu_p(N)}$ is the p-free part of N. This function is even further from being a multiplicative function than K^*, since its value can depend even on the residue class modulo p of the p-free part of N. Nevertheless, our techniques can in fact determine the average value of the function K° as well.

To investigate the average of K°, we would expand the notion of a configuration to a sextuple $(\mathscr{A},\mathscr{B}_1,\mathscr{B}_2,\mathscr{C},\{e_\ell\}_{\ell\in\mathscr{B}_1\cup\mathscr{B}_2},\{a_\ell\}_{\ell\in\mathscr{B}_2})$, where $\mathscr{A},\mathscr{B}_1,\mathscr{B}_2,\mathscr{C}$ partition the set of primes up to z, the e_ℓ are positive integers, and the a_ℓ are integers satisfying $1\le a_\ell\le\ell-1$. We would modify Definition 2.3 by setting $\mathscr{B}_1:=\{\ell\le z: 2\nmid e_\ell\}$

and $\mathcal{B}_2 := \{\ell \le z : 2 \mid e_\ell\}$ and, for $\ell \in \mathcal{B}_2$, choosing $a_\ell \in \{1, \dots, \ell - 1\}$ such that $a_\ell \equiv N/\ell^{e_\ell} \pmod{\ell}$. The analogue of (21) would be

$$K_z^\circ(\sigma)\, d_\sigma = \biggl(\prod_{\ell\in\mathcal{A}} \frac{\ell-2}{\ell-1}\biggr)^2 \biggl(\prod_{\ell\in\mathcal{C}} \frac{\ell^2-\ell-1}{(\ell-1)^2(\ell+1)}\biggr) \biggl(\prod_{\ell\in\mathcal{B}_1} \frac{1}{\ell^{e_\ell}}\Bigl(1 - \frac{1}{\ell^{e_\ell}(\ell-1)}\Bigr)\biggr)$$
$$\times \biggl(\prod_{\ell\in\mathcal{B}_2} \frac{1}{\ell^{e_\ell}(\ell-1)}\Bigl(1 - \frac{\ell - \bigl(\frac{-a_\ell}{\ell}\bigr)}{\ell^{e_\ell+1}(\ell-1)}\Bigr)\biggr).$$

We would then hold $\mathcal{A}$, $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{C}$, and the e_ℓ fixed and sum over all $\prod_{\ell\in\mathcal{B}_2}(\ell-1)$ possibilities for the a_ℓ; this has the effect of replacing the Legendre symbol $\bigl(\frac{-a_\ell}{\ell}\bigr)$ by its average value 0. At this point in the argument, the factors corresponding to primes in $\mathcal{B}_1$ and $\mathcal{B}_2$ would be identical, and the calculation would soon dovetail with (22).

We felt these few details of the determination of the average value of K° were worth mentioning, as an example of the wider applicability of our method and the more complicated configuration spaces that can be used.

3. The average of K^* over primes

In this section we establish Theorem 1.3. The main component of the proof is the following asymptotic formula for the sum of the multiplicative function F evaluated on shifted primes.

Proposition 3.1. *Let F be the multiplicative function defined in (6) and let J be the constant defined in (4). For any $x > 2$ and for any positive real number A,*

$$\sum_{p\le x} F(p-1) = J\pi(x) + O_A(x/(\log x)^A).$$

Proof. Write $F(n) = \sum_{d\mid n} g(d)$ for an auxiliary function g (not the same function as in the proof of Theorem 1.2) which is also multiplicative. By a direct computation with the Möbius inversion formula, g vanishes unless d is squarefree. Moreover, $g(2) = -\frac{1}{3}$, while for odd primes ℓ,

$$g(\ell) = \frac{1}{(\ell-2)(\ell+1)}. \tag{24}$$

Writing $\pi(x; d, 1)$ for the number of primes $p \le x$ with $p \equiv 1 \pmod{d}$, we have

$$\begin{aligned}\sum_{p\le x} F(p-1) &= \sum_{p\le x} \sum_{d\mid p-1} g(d)\\ &= \sum_{d\le(\log x)^A} g(d)\pi(x; d, 1) + \sum_{(\log x)^A<d\le x} g(d)\pi(x; d, 1).\end{aligned} \tag{25}$$

We first consider the second sum on the last line. Trivially, $\pi(x; d, 1) < \dfrac{x}{d}$, and so

$$\biggl|\sum_{(\log x)^A < d \le x} g(d)\pi(x; d, 1)\biggr| \le x \sum_{d > (\log x)^A} \frac{|g(d)|}{d}. \tag{26}$$

When $g(d)$ is nonvanishing, the formula (24) yields

$$d^2 g(d) \ll \prod_{\ell \mid d,\ \ell > 2} \frac{\ell^2}{\ell^2 - \ell - 2} \ll \prod_{\ell \mid d} \Bigl(1 - \frac{1}{\ell}\Bigr)^{-1} = \frac{d}{\phi(d)},$$

and hence $g(d) \ll 1/(d\phi(d))$ for all values of d. In particular, using the crude lower bound $\phi(d) \gg d^{1/2}$ (compare with the precise Theorem 2.9 of [Montgomery and Vaughan 2007, p. 55]), we find that $g(d) \ll d^{-3/2}$. Thus, (26) gives

$$\sum_{(\log x)^A < d \le x} g(d)\pi(x; d, 1) \ll x \sum_{d > (\log x)^A} d^{-5/2} \ll x(\log x)^{-3A/2},$$

and so (25) becomes

$$\sum_{p \le x} F(p-1) = \sum_{d \le (\log x)^A} g(d)\pi(x; d, 1) + O(x(\log x)^{-3A/2}). \tag{27}$$

To deal with the remaining sum, we invoke the Siegel–Walfisz theorem [Montgomery and Vaughan 2007, Corollary 11.21, p. 381]. That theorem implies that for a certain absolute constant $c > 0$,

$$\begin{aligned}\sum_{d \le (\log x)^A} g(d)\pi(x; d, 1) &= \sum_{d \le (\log x)^A} g(d)\biggl(\frac{\pi(x)}{\phi(d)} + O_A(x \exp(-c\sqrt{\log x}))\biggr)\\ &= \pi(x) \sum_{d \le (\log x)^A} \frac{g(d)}{\phi(d)} + O_A\biggl(x \exp(-c\sqrt{\log x}) \sum_{d=1}^{\infty} |g(d)|\biggr)\\ &= \pi(x) \sum_{d=1}^{\infty} \frac{g(d)}{\phi(d)}\\ &\quad + O_A\biggl(\pi(x) \sum_{d > (\log x)^A} \frac{|g(d)|}{\phi(d)} + x \exp(-c\sqrt{\log x}) \sum_{d=1}^{\infty} |g(d)|\biggr).\end{aligned}$$

In the error term, we again use the crude bounds $g(d) \ll d^{-3/2}$ and $\phi(d) \gg d^{1/2}$, obtaining

$$\sum_{d \le (\log x)^A} g(d)\pi(x; d, 1) = \pi(x) \sum_{d=1}^{\infty} \frac{g(d)}{\phi(d)} + O_A\bigl(\pi(x)(\log x)^{-A} + x \exp(-c\sqrt{\log x}) \cdot 1\bigr),$$

whereupon (27) becomes

$$\sum_{p \le x} F(p-1) = \pi(x) \sum_{d=1}^{\infty} \frac{g(d)}{\phi(d)} + O_A(x(\log x)^{-A}).$$

Finally, the constant in this main term is an absolutely convergent sum of a multiplicative function, and hence it can be expressed as the Euler product

$$\begin{aligned} \sum_{d=1}^{\infty} \frac{g(d)}{\phi(d)} &= \prod_{\ell} \left(1 + \frac{g(p)}{\phi(p)} + \frac{g(p^2)}{\phi(p^2)} + \cdots \right) \\ &= \frac{2}{3} \prod_{\ell > 2} \left(1 + \frac{1}{(\ell-1)(\ell-2)(\ell+1)}\right) = \frac{2}{3} J \end{aligned}$$

by (24). This completes the proof of the proposition. □

Proof of Theorem 1.3. We first claim that the asymptotic formula (2) for K^* follows easily from the same asymptotic formula for K. Indeed, for each prime p, we have $K^*(p) = K(p)p/(p-1) = K(p) + O(K(p)/p)$. Because each local factor in Definition 1.1 is of the form $1 + O(p^{-2})$, we see that K is absolutely bounded. Thus

$$\sum_{p \le x} K^*(p) = \sum_{p \le x} K(p) + O\left(\sum_{p \le x} \frac{1}{p}\right) = \sum_{p \le x} K(p) + O(\log\log x),$$

and so it suffices to establish the asymptotic formula (2) for K.

For each prime p, the decomposition (5) gives $K(p) = C_2 F(p-1)G(p)$, where F and G are defined in equations (6) and (7) respectively. Again, all local factors in these definitions are of the form $1 + O(p^{-2})$; hence $G(p) = 1 + O(1/p^2)$ and F is absolutely bounded. Therefore,

$$\begin{aligned} \sum_{p \le x} K(p) = \sum_{p \le x} C_2 F(p-1)G(p) &= C_2 \sum_{p \le x} F(p-1) + O\left(\sum_{p \le x} \frac{F(p-1)}{p^2}\right) \\ &= C_2 \sum_{p \le x} F(p-1) + O(1), \end{aligned}$$

so the desired asymptotic formula (2) is a direct consequence of Proposition 3.1. □

4. The distribution function of K^*

The goal of this section is to establish the existence of the distribution function of $K^*(N)$. We do so by bounding the moments of $K^*(N)$:

$$\mu_k := \lim_{x \to \infty} \frac{1}{x} \sum_{N \le x} K^*(N)^k. \tag{28}$$

We describe below how Theorem 1.4 follows from Proposition 4.3. Before we can bound these moments, however, we must prove that the moments even exist. In Theorem 1.2 we determined that $\mu_1 = 1$, and the same method of determining μ_k applies in general.

Proposition 4.1. *For every natural number k, the limit (28) defining μ_k exists.*

Proof. Following the proof of Proposition 2.1, we obtain (with minimal changes to the argument) that for each fixed k,

$$\sum_{N\le x}(K_z(N)R_z(N))^k = x\sum_{\sigma\in\mathscr{S}} K_z(\sigma)^k R_z(\sigma)^k d_\sigma + O_k(x^{3/4}), \tag{29}$$

where $z=\frac{1}{10}\log x$ and d_σ is defined in (15). Note that for $N\le x$,

$$\begin{aligned}
&(K_z(N)R_z(N))^k - (K(N)R(N))^k\\
&\qquad \ll_k \max\{K(N)R(N),\, K_z(N)R_z(N)\}^{k-1}\cdot|K(N)R(N)-K_z(N)R_z(N)|\\
&\qquad \ll_k (\log\log x)^{k-1}\cdot|K(N)R(N)-K_z(N)R_z(N)|
\end{aligned}$$

by the bounds in (19); therefore

$$\begin{aligned}
\sum_{N\le x}K^*(N)^k &= \sum_{N\le x}(K_z(N)R_z(N))^k + \sum_{N\le x}\big((K(N)R(N))^k-(K_z(N)R_z(N))^k\big)\\
&= \sum_{N\le x}(K_z(N)R_z(N))^k\\
&\qquad\qquad + O_k\bigg((\log\log x)^{k-1}\sum_{N\le x}\big|K(N)R(N)-K_z(N)R_z(N)\big|\bigg).
\end{aligned}$$

Using (29) in the main term and the estimate (11) in the error term, we obtain

$$\begin{aligned}
\sum_{N\le x}K^*(N)^k &= x\sum_{\sigma\in\mathscr{S}}K_z(\sigma)^kR_z(\sigma)^kd_\sigma + O_k\big(x^{3/4}+(\log\log x)^{k-1}x/z\big)\\
&= x\sum_{\sigma\in\mathscr{S}}K_z(\sigma)^kR_z(\sigma)^kd_\sigma + O_k\bigg(\frac{x}{\log x}(\log\log x)^{k-1}\bigg).
\end{aligned}$$

Dividing both sides by x and passing to the limit, we deduce that

$$\mu_k = \lim_{x\to\infty}\sum_{\sigma\in\mathscr{S}}K_z(\sigma)^kR_z(\sigma)^kd_\sigma, \tag{30}$$

provided that this limit exists.

To compute the sum over σ in (30), we follow the proof of Lemma 2.8; however, the details are somewhat messier. With the four components $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$, $\{e_\ell\}_{\ell\in\mathscr{B}}$ of σ as before, we write down the expansion for $K_z(\sigma)^kR_z(\sigma)^kd_\sigma$ analogous to (21). This expansion is made up of three pieces, which are products over primes ℓ in $\mathscr{A}$, $\mathscr{B}$, and $\mathscr{C}$. The $\mathscr{B}$ product depends additionally on the tuple $\{e_\ell\}_{\ell\in\mathscr{B}}$. We sum over all possibilities for $\{e_\ell\}_{\ell\in\mathscr{B}}$ to remove this dependence. After straightforward but uninspiring computations, we find that fixing only $\mathscr{A}$, $\mathscr{B}$, and $\mathscr{C}$,

$$\sum_{\sigma} K_z(\sigma)^k R_z(\sigma)^k d_\sigma = \Big(\prod_{\ell\in\mathscr{A}} P_{\mathscr{A}}(\ell)\Big)\Big(\prod_{\ell\in\mathscr{B}} P_{\mathscr{B}}(\ell)\Big)\Big(\prod_{\ell\in\mathscr{C}} P_{\mathscr{C}}(\ell)\Big),$$

where (we suppress the dependence on k in the notation on the left-hand sides)

$$\begin{aligned} P_{\mathscr{A}}(\ell) &= \left(1-\frac{2}{\ell}\right)^{k+1}\left(1-\frac{1}{\ell}\right)^{-2k}, \\ P_{\mathscr{B}}(\ell) &= \left(1-\frac{1}{\ell}\right)^{1-k}\sum_{d=1}^{\infty}\frac{1}{\ell^d}\left(1-\frac{1}{\ell^d(\ell-1)}\right)^k, \\ P_{\mathscr{C}}(\ell) &= \frac{1}{\ell}\left(1-\frac{1}{(\ell-1)^2(\ell+1)}\right)^k. \end{aligned} \tag{31}$$

(Note that when $k=1$, these expressions reduce to the expressions in (23).) To compute the sum appearing in (30), we sum over $\mathscr{A}$, $\mathscr{B}$, and $\mathscr{C}$, keeping in mind that these sets partition the primes in $[2,z]$. We find that

$$\sum_{\sigma\in\mathscr{S}} K_z(\sigma)^k R_z(\sigma)^k d_\sigma = \prod_{\ell\le z}(P_{\mathscr{A}}(\ell)+P_{\mathscr{B}}(\ell)+P_{\mathscr{C}}(\ell)),$$

and so from (30),

$$\mu_k = \prod_{\ell}(P_{\mathscr{A}}(\ell)+P_{\mathscr{B}}(\ell)+P_{\mathscr{C}}(\ell)). \tag{32}$$

It remains to show that this product converges. From the definitions (31), we find that

$$\begin{aligned} P_{\mathscr{A}}(\ell) &= 1-2/\ell+O_k(1/\ell^2), \\ P_{\mathscr{B}}(\ell) &= 1/\ell+O_k(1/\ell^2), \\ P_{\mathscr{C}}(\ell) &= 1/\ell+O_k(1/\ell^2). \end{aligned}$$

It follows that each term in the product from (32) is $1+O(1/\ell^2)$; consequently, that product converges, which completes the proof of the proposition. □

Remarks. For any given k, we can explicitly compute $P_{\mathscr{A}}$, $P_{\mathscr{B}}$, and $P_{\mathscr{C}}$ and thus write down an exact expression for μ_k as an infinite product over primes. For example, taking $k=2$, we find that

$$\mu_2 = \prod_{\ell}\left(1+\frac{\ell^5-\ell^3-2\ell^2-2\ell-1}{(\ell-1)^4(\ell+1)^2(\ell^2+\ell+1)}\right) \approx 1.261605.$$

Now that we know these moments μ_k exist, we proceed to establish an upper bound for them as a function of k. The following result, well-known in the theory of probability (see, for example, [Durrett 2010, Theorem 3.3.12, p. 123]), allows us to pass from such an upper bound to the existence of a limiting distribution function.

Lemma 4.2. *Let $F_1, F_2, \dots$ be a sequence of distribution functions. Suppose that for each positive integer k, the limit $\lim_{n\to\infty}\int u^k\,dF_n(u)=\mu_k$ exists. If*

$$\limsup_{k\to\infty}\frac{\mu_{2k}^{1/2k}}{2k}<\infty,$$

then there is a unique distribution function F possessing the μ_k as its moments, and F_n converges weakly to F.

We will apply Lemma 4.2 with

$$F_n(u):=\frac{\#\{m\le n:K^*(m)\le u\}}{\#\{m\le n\}},$$

for which

$$\lim_{n\to\infty}\int u^k\,dF_n(u)=\lim_{n\to\infty}\frac{1}{n}\sum_{m\le n}K^*(m)^k=\mu_k$$

(so that the uses of μ_k in (28) and Lemma 4.2 are consistent). In light of Lemma 4.2, Theorem 1.4 is a consequence of the following upper bound.

Proposition 4.3. *The moments μ_k defined in (28) satisfy $\log\mu_k\ll k\log\log k$ for large k. In particular, $(\mu_{2k}^{1/2k})/2k\ll(\log k)^A/k$ for some constant A.*

Proof. Recall that $R(N)$ denotes the function $N/\phi(N)$. The number μ_k is the k-th moment of the function $K(N)R(N)$, and that function is bounded pointwise by $R(N)$. So μ_k is bounded above by μ_k', where

$$\mu_k':=\lim_{x\to\infty}\frac{1}{x}\sum_{N\le x}R(N)^k.$$

Thus, it suffices to establish the estimate $\log\mu_k'\ll k\log\log k$.

By a result known already to Schur (see [Schoenberg 1928, p. 194]; see also [Montgomery and Vaughan 2007, Exercise 14, p. 42]), we have that for each k,

$$\mu_k'=\prod_p\left(1-\frac{1}{p}+\frac{1}{p}\left(1-\frac{1}{p}\right)^{-k}\right)=\prod_p\left(1+\frac{1}{p}\left(\left(\frac{p}{p-1}\right)^k-1^k\right)\right).$$

By the mean value theorem,

$$\begin{aligned}1+\frac{1}{p}\left(\left(\frac{p}{p-1}\right)^k-1^k\right)&=1+O\left(\frac{k}{p(p-1)}\left(\frac{p}{p-1}\right)^{k-1}\right)\\&=1+O\left(\frac{k}{p^2}\left(1+\frac{1}{p-1}\right)^{k-1}\right)<1+O\left(\frac{k}{p^2}\exp\left(\frac{k-1}{p-1}\right)\right),\end{aligned}$$

and so

$$\mu_k' < \prod_{p\le k}\left(1+O\left(\frac{k}{p^2}\exp\left(\frac{k-1}{p-1}\right)\right)\right)\prod_{p>k}\left(1+O\left(\frac{k}{p^2}\exp\left(\frac{k-1}{p-1}\right)\right)\right). \tag{33}$$

In the first product, we use the crude inequality

$$1+O\left(\frac{k}{p^2}\exp\left(\frac{k-1}{p-1}\right)\right) < 1+O\left(k\exp\left(\frac{k}{p-1}\right)\right) \ll k\exp\left(\frac{k}{p-1}\right),$$

so that for some absolute constant C,

$$\begin{aligned}\prod_{p\le k}\left(1+O\left(\frac{k}{p^2}\exp\left(\frac{k-1}{p-1}\right)\right)\right) &\le \prod_{p\le k} Ck\exp\left(\frac{k}{p-1}\right)\\ &\le (Ck)^{\pi(k)}\exp\left(k\sum_{p\le k}\frac{1}{p-1}\right)\\ &= \exp(O(k))\exp(O(k\log\log k)).\end{aligned}$$

In the second product, the exponential factor is uniformly bounded, so

$$\begin{aligned}\prod_{p>k}\left(1+O\left(\frac{k}{p^2}\exp\left(\frac{k-1}{p-1}\right)\right)\right) &= \prod_{p>k}\left(1+O\left(\frac{k}{p^2}\right)\right)\\ &< \prod_{p>k}\left(\exp\left(O\left(\frac{k}{p^2}\right)\right)\right)\\ &\le \exp\left(O\left(\sum_p \frac{k}{p^2}\right)\right) = \exp(O(k)).\end{aligned}$$

In light of these last two estimates, (33) yields $\mu_k' \le \exp(O(k\log\log k))$ as required. □

Remarks. It is worthwhile to make a few remarks about the behavior of $D(u)$. Let $u_0 := \frac{2}{3}C_2$. We can view Equation (20), with $z=\infty$, as providing us with a conveniently factored Euler product expansion of $K^*(N)$. Comparing the terms of this expansion with those in the product expansion for C_2, one sees that $K^*(N) > u_0$ for all N. In fact, one finds that $K^*(N)$ is bounded away from u_0 unless N is odd and all of the small odd primes belong to $\mathscr{A}$, i.e., unless $2\nmid N$ and $N(N-1)$ has no small odd prime factors. Conversely, if $2\nmid N$ and $N(N-1)$ has no small odd prime factors, an averaging argument shows that $K^*(N)$ is usually close to u_0. In this way, one proves that $D(u_0)=0$ while $D(u)>0$ for $u>u_0$.

Since $K(N)$ is absolutely bounded and bounded away from zero, several results on $D(u)$ follow immediately from corresponding results for the distribution function of $N/\phi(N)$, whose behavior has been studied by Erdős [1946] and Weingartner [2007; 2012]. In particular, from [Erdős 1946, Theorem 1], we see that $D(u) > 1 - \exp(-\exp(Cu))$ for a certain constant $C > 0$ and all large u.

Finally, we remark that there is an alternative, more arithmetic approach to the proof of Theorem 1.4, based on ideas and results of Erdős [1935; 1937; 1938] and Shapiro [1973]. This approach allows us to show that the distribution function $D(u)$ of Theorem 1.4 is continuous everywhere and strictly increasing for $u > u_0$. We omit the somewhat lengthy arguments for these claims.

Acknowledgements

We thank Igor Shparlinski for bringing [Banks and Shparlinski 2009] to our attention. We also thank the anonymous referee for a careful reading of the manuscript.

References

[Baier 2009] S. Baier, "A remark on the Lang–Trotter conjecture", pp. 11–18 in *New directions in value-distribution theory of zeta and L-functions*, edited by R. Steuding and J. Steuding, Shaker, Aachen, 2009. MR 2011k:11075 Zbl 1250.11056

[Balog et al. 2011] A. Balog, A.-C. Cojocaru, and C. David, "Average twin prime conjecture for elliptic curves", *Amer. J. Math.* **133**:5 (2011), 1179–1229. MR 2012j:11118 Zbl 1281.11052

[Banks and Shparlinski 2009] W. D. Banks and I. E. Shparlinski, "Sato–Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height", *Israel J. Math.* **173** (2009), 253–277. MR 2011a:11121 Zbl 1250.11064

[Chandee et al. 2014] V. Chandee, C. David, D. Koukoulopoulos, and E. Smith, "The frequency of elliptic curve groups over prime finite fields", preprint, 2014. arXiv 1405.6923

[Cohen 1993] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics **138**, Springer, Berlin, 1993. MR 94i:11105 Zbl 0786.11071

[David and Smith 2013] C. David and E. Smith, "Elliptic curves with a given number of points over finite fields", *Compos. Math.* **149**:2 (2013), 175–203. MR 3020306 Zbl 06144655

[David and Smith 2014] C. David and E. Smith, "Corrigendum: Elliptic curves with a given number of points over finite fields (*Compos. Math.* **149**:2 (2013), 175–203)", *Compos. Math.* (2014).

[David and Wu 2012] C. David and J. Wu, "Pseudoprime reductions of elliptic curves", *Canad. J. Math.* **64**:1 (2012), 81–101. MR 2932170 Zbl 1271.11090

[Durrett 2010] R. Durrett, *Probability: theory and examples*, 4th ed., Cambridge University Press, 2010. MR 2011e:60001 Zbl 1202.60001

[Erdős 1935] P. Erdős, "On the density of some sequences of numbers", *J. London Math. Soc.* **10**:2 (1935), 120–125. MR 1574238 Zbl 0012.01004

[Erdős 1937] P. Erdős, "On the density of some sequences of numbers, II", *J. London Math. Soc.* **12**:1 (1937), 7–11. Zbl 0016.01204

[Erdős 1938] P. Erdős, "On the density of some sequences of numbers, III", *J. London Math. Soc.* **13**:2 (1938), 119–127. MR 1574138 Zbl 0018.29301

[Erdős 1946] P. Erdős, "Some remarks about additive and multiplicative functions", *Bull. Amer. Math. Soc.* **52** (1946), 527–537. MR 7,507g Zbl 0061.07901

[Fouvry and Murty 1996] E. Fouvry and M. R. Murty, "On the distribution of supersingular primes", *Canad. J. Math.* **48**:1 (1996), 81–104. MR 97a:11084 Zbl 0864.11030

[Hasse 1936a] H. Hasse, "Zur Theorie der abstrakten elliptischen Funktionenkörper, I: Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung", *J. Reine Angew. Math.* **175** (1936), 55–62. Zbl 0014.14903

[Hasse 1936b] H. Hasse, "Zur Theorie der abstrakten elliptischen Funktionenkörper, II: Automorphismen und Meromorphismen. Das Additionstheorem", *J. Reine Angew. Math.* **175** (1936), 69–88. Zbl 0014.24901

[Hasse 1936c] H. Hasse, "Zur Theorie der abstrakten elliptischen Funktionenkörper, III: Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung", *J. Reine Angew. Math.* **175** (1936), 193–208. Zbl 0014.24902

[Jones 2009] N. Jones, "Averages of elliptic curve constants", *Math. Ann.* **345**:3 (2009), 685–710. MR 2010j:11090 Zbl 1177.14067

[Koblitz 1988] N. Koblitz, "Primality of the number of points on an elliptic curve over a finite field", *Pacific J. Math.* **131**:1 (1988), 157–165. MR 89h:11023 Zbl 0608.10010

[Kowalski 2006] E. Kowalski, "Analytic problems for elliptic curves", *J. Ramanujan Math. Soc.* **21**:1 (2006), 19–114. MR 2007c:11108 Zbl 1144.11069 arXiv math/0510197

[Languasco et al. 2010] A. Languasco, A. Perelli, and A. Zaccagnini, "On the Montgomery–Hooley theorem in short intervals", *Mathematika* **56**:2 (2010), 231–243. MR 2011g:11179 Zbl 1238.11087

[Montgomery and Vaughan 2007] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory, I: Classical theory*, Cambridge Studies in Advanced Mathematics **97**, Cambridge University Press, 2007. MR 2009b:11001 Zbl 1142.11001

[Schoenberg 1928] I. Schoenberg, "Über die asymptotische Verteilung reeller Zahlen mod 1", *Math. Z.* **28**:1 (1928), 171–199. MR 1544950 JFM 54.0212.02

[Shapiro 1973] H. N. Shapiro, "Addition of functions in probabilistic number theory", *Comm. Pure Appl. Math.* **26** (1973), 55–84. MR 51 #3107 Zbl 0253.10043

[Weingartner 2007] A. Weingartner, "The distribution functions of $\sigma(n)/n$ and $n/\phi(n)$", *Proc. Amer. Math. Soc.* **135**:9 (2007), 2677–2681. MR 2009c:11156 Zbl 1169.11042

[Weingartner 2012] A. Weingartner, "The distribution functions of $\sigma(n)/n$ and $n/\phi(n)$, II", *J. Number Theory* **132**:12 (2012), 2907–2921. MR 2965199 Zbl 06097270

[Zywina 2011] D. Zywina, "A refinement of Koblitz's conjecture", *Int. J. Number Theory* **7**:3 (2011), 739–769. MR 2012e:11107 Zbl 1278.11064

Communicated by Joseph Silverman
Received 2012-08-26 Revised 2013-12-14 Accepted 2014-02-15

gerg@math.ubc.ca *Department of Mathematics, University of British Columbia, Room 121, 1984 Mathematics Road, Vancouver, BC V6T 1Z2, Canada*

pollack@uga.edu *Department of Mathematics, University of Georgia, Boyd Graduate Studies Research Center, Athens, GA 30602, United States*

ecsmith13@liberty.edu *Department of Mathematics, Liberty University, 1971 University Blvd., Lynchburg, VA 24502, United States*

ALGEBRA AND NUMBER THEORY 8:4 (2014)
dx.doi.org/10.2140/ant.2014.8.837

Noncrossed product bounds over Henselian fields

Timo Hanke, Danny Neftin and Jack Sonn

The existence of noncrossed product division algebras (finite-dimensional central division algebras with no maximal subfield that is Galois over the center) was for a time the biggest open problem in the theory of division algebras, until it was settled by Amitsur.

Motivated by Brussel's discovery of noncrossed products over $\mathbb{Q}((t))$, we describe the "location" of noncrossed products in the Brauer group of general Henselian valued fields with arbitrary value group and global residue field. We show that within the fibers defined canonically by Witt's decomposition of the Brauer group of such fields, crossed products and noncrossed products are, roughly speaking, separated by an index bound. This generalizes a result of Hanke and Sonn for rank-1 valued Henselian fields.

Furthermore, we show that the new index bounds are of different nature from the rank-1 case. In particular, all fibers not covered by the rank-1 case contain noncrossed products, unless the residue characteristic interferes.

1. Introduction

A finite-dimensional division algebra over its center F is called a *crossed product* if it has a maximal commutative subfield which is Galois over F, and otherwise a *noncrossed product*.

After Amitsur [1972] settled the fundamental long-standing problem of existence of noncrossed products, they were discovered over more familiar fields. Most notably, Brussel [1995; 2002] showed that noncrossed products exist over complete discrete rank-1 valued fields with a global residue field,[1] for example, over $\mathbb{Q}((x))$. From this basic case, their existence over many other fields was derived, for example, over all finitely generated fields that are neither finite nor global [Brussel 2002], and over all function fields of curves over complete discrete valuation rings [Brussel 2001; Chen 2010].

MSC2010: primary 16S35; secondary 11R32, 12F12.
Keywords: noncrossed product, division algebra, Henselian fields.

[1] By a global field we mean a finite extension of $\mathbb{Q}$ or a finite extension of $\mathbb{F}_q(t)$, where $\mathbb{F}_q$ is a finite field.

The basic setup used for Brussel's discovery is Witt's description [1936] of the Brauer group $\mathrm{Br}(F)$ of a complete discrete rank-1 valued field. More precisely, Witt's theorem describes the inertially split part $\mathrm{SBr}(F)$, which consists of all elements of $\mathrm{Br}(F)$ split by an unramified extension (see [Hanke 2011, §5]). Witt's theorem applies more generally to Henselian fields F with arbitrary value group Γ (see [Scharlau 1969; Jacob and Wadsworth 1990, §5; Aljadeff et al. 2007, Theorem 3.2]; or the section titled "The canonical Brauer group filtration" in [Tignol and Wadsworth $\geq$ 2014]), for example, to the field of iterated Laurent series $\mathbb{Q}((x_1))\ldots((x_r))$, and gives an isomorphism

$$\mathrm{SBr}(F) \cong \mathrm{Br}(K) \oplus \mathrm{Hom}_c(G_K, \Delta/\Gamma), \tag{1-1}$$

where K is the residue field and G_K is its absolute Galois group equipped with the Krull topology, Δ is the divisible hull of Γ, Δ/Γ is equipped with the discrete topology, and Hom_c is the group of continuous homomorphisms.

Assume K is a global field. Hanke and Sonn [2011] took the approach of fixing an element $\chi \in \mathrm{Hom}_c(G_K, \Delta/\Gamma)$ and considering the *fiber* $\mathrm{Br}(K)+\chi$. We call χ *cyclic* if its image $\mathrm{Im}(\chi)$ is cyclic. For cyclic χ, [Hanke and Sonn 2011] shows that for every $N \in \mathbb{N}$ there are only two possible cases:

(I) all division algebras of index N in the fiber over χ are crossed products;

(II) the fiber over χ contains infinitely many noncrossed products of index N.

Furthermore, and most importantly, there are bounds on the exponents in the prime decomposition of N such that case (I) occurs "below the bounds" and case (II) "above". A precise formulation of this result is the special case of Theorem 1.1 below, in which χ is assumed to be cyclic.[2]

Little was known about the appearance of noncrossed products in the more complicated case of noncyclic χ. In fact, there were only two examples [Coyette 2012; Hanke 2004] of noncyclic χ, the fiber of which contains noncrossed products.

In the present paper, we show that the phenomenon discovered in [Hanke and Sonn 2011] for cyclic χ holds more generally for arbitrary χ (Theorem 1.1). Moreover, we show that "away from char K" noncrossed products appear in every noncyclic fiber (Theorem 1.2).

Note that by [Jacob and Wadsworth 1990, Theorem 5.15(a)], the index of an element in the fiber over χ is always a multiple of $|\chi| := |\mathrm{Im}(\chi)|$.

Theorem 1.1. *There exists a collection of bounds $b_p = b_p(\chi) \in \mathbb{N} \cup \{\infty\}$, where p runs through the rational primes, such that, for every natural number $m = \prod p^{n_p}$,*

[2] In order to see that Theorem 1.1 for cyclic χ was proved in [Hanke and Sonn 2011] not only for rank-1 valued fields, one should replace [Hanke and Sonn 2011, Brussel's Lemma, p. 322] by [Hanke 2011, Corollary 5].

(a) *if* $n_p \leq b_p(\chi)$ *for all* p, *then all division algebras of index* $m|\chi|$ *in the fiber over* χ *are crossed products*;

(b) *if* $n_p > b_p(\chi)$ *for some* p, *then the fiber over* χ *contains infinitely many noncrossed products of index* $m|\chi|$.

Our proof of Theorem 1.1 includes the case of cyclic χ and is simpler than [Hanke and Sonn 2011].

Note that $b_p(\chi) = \infty$ is allowed, and hence, as shown in [Hanke and Sonn 2011], it may happen that for some cyclic χ, only (I) occurs. However, in striking contrast to the cyclic case, we show:

Let M be the fixed field of the kernel of χ.

Theorem 1.2. *If* $p \neq \operatorname{char} K$ *and the* p*-Sylow subgroup of* $\operatorname{Im}(\chi)$ *is noncyclic*, *then*:

(i) $b_p(\chi) < \infty$;

(ii) *if* M *does not contain the* p*-th roots of unity*, *then* $b_p(\chi) = 0$.

In particular, *the fiber over* χ *contains noncrossed products whenever the maximal prime-to-*$\operatorname{char} K$ *subgroup of* $\operatorname{Im}(\chi)$ *is noncyclic.*

This is in contrast to the cyclic case because, according to [Hanke and Sonn 2011], $b_p(\chi) = \infty$ can occur for cyclic χ, even if M does not contain the p-th roots of unity. Thus, neither of statements (i) and (ii) of Theorem 1.2 holds for cyclic χ.

Section 4 demonstrates, for noncyclic χ, how a description of the bounds obtained from the proof of Theorem 1.1 can be used to compute the bounds in examples. In particular, we obtain new noncrossed products of low index (Examples 4.1, 4.3) and show that, unlike in the rank-1 case, the value of the bound $b_p(\chi)$ can be zero regardless of the number of roots of unity in M.

2. Existence of bounds

Setup. Let F be a Henselian valued field with value group Γ and residue field a global field K. Let Δ denote the divisible hull of Γ. We fix an isomorphism as in (1-1) and write $\alpha + \chi$ to denote an element of $\operatorname{SBr}(F)$ corresponding to (α, χ).

Throughout the paper, we consider the character $\chi \in \operatorname{Hom}_c(G_K, \Delta/\Gamma)$ as fixed. We let M denote the fixed field of the kernel of χ, which is a finite abelian extension of K with Galois group $\operatorname{Im}(\chi)$.

Let $\mathbb{P}$ be the set of finite rational primes, and for any $p \in \mathbb{P}$, $n \in \mathbb{N}$, denote by $v_p(n)$ the maximal exponent e such that $p^e \mid n$.

Towards the proof of Theorem 1.1. For $\alpha \in \operatorname{Br}(K)$, we denote by α^M the image of α in $\operatorname{Br}(M)$ under the restriction map. The index formula [Jacob and Wadsworth

1990, Theorem 5.15(a)][3] gives

$$\operatorname{ind}(\alpha+\chi)=|\chi|\operatorname{ind}\alpha^M.$$

Therefore, in order to prove Theorem 1.1, we consider the following condition on χ:

For every $\alpha \in \operatorname{Br}(K)$ with $\operatorname{ind}\alpha^M = m$, the division algebra underlying $\alpha+\chi$ is a crossed product. $\quad$ (I_m)

For a global field K, we shall prove the existence of bounds $b_p(\chi)$ such that (I_m) holds if and only if $v_p(m) \le b_p(\chi)$ for all $p \in \mathbb{P}$. The details of our proof will reveal that if (I_m) does not hold, then there are in fact infinitely many $\alpha \in \operatorname{Br}(K)$ with $\operatorname{ind}\alpha^M = m$ such that the division algebra underlying $\alpha+\chi$ is a noncrossed product (Remark 2.9). The proof of Theorem 1.1 will then be completed.

Galois covers. We say that a field $L \supseteq M$ is a *cover* of M/K if L/K is Galois. In this case, we call $m := [L:M]$ the *degree* of the cover and speak of L as an *m-cover*.

The division algebra underlying $\alpha+\chi$ is a crossed product if and only if the division algebra underlying α^M contains a maximal subfield which is Galois over K (see [Hanke 2011, Corollary 5; Brussel 1995, p. 381, Corollary] for complete discrete rank-1 valued F). Such maximal subfields are characterized as the m-covers of M/K that split α, where $m = \operatorname{ind}\alpha^M$ (see, for example, [Pierce 1982, Corollary 13.3]). Condition (I_m) is therefore equivalent to:

Every $\alpha \in \operatorname{Br}(K)$ with $\operatorname{ind}\alpha^M = m$ is split by an m-cover of M/K. $\quad$ (A_m)

Remark 2.1. (i) For the equivalence of (I_m) and (A_m) it is not required that K be a global field.

(ii) Condition (A_m) is a condition on M rather than on χ. (A_m) can be considered more generally for any Galois extension M/K. In fact, from now on M may be replaced by an arbitrary finite Galois extension of the global field K.

Local and global splitting covers. Let L be a cover of the fixed Galois extension M/K. We write $K_{\mathfrak{p}}$ for the completion at $\mathfrak{p}$ and $[L:M]_{\mathfrak{p}} := [L_{\mathfrak{P}} : M_{\mathfrak{P}\cap M}]$ for the *local degree* of L at $\mathfrak{p}$, where $\mathfrak{P}$ is any prime of L dividing $\mathfrak{p}$.

Let $\alpha \in \operatorname{Br}(K)$. For a prime $\mathfrak{p}$ of K, let $\operatorname{ind}_{\mathfrak{p}}\alpha := \operatorname{ind}(\alpha^{K_{\mathfrak{p}}})$ and $\operatorname{inv}_{\mathfrak{p}}\alpha \in \mathbb{Q}/\mathbb{Z}$ be the Hasse invariant at $\mathfrak{p}$. Recall (see, for example, [Pierce 1982, §17.10]) that $\operatorname{inv}_{\mathfrak{p}}\alpha$ is of order $\operatorname{ind}_{\mathfrak{p}}\alpha$ and that $\operatorname{inv}_{\mathfrak{P}}\alpha^L = [L:K]_{\mathfrak{p}}\operatorname{inv}_{\mathfrak{p}}\alpha$ for any Galois extension L/K and $\mathfrak{P} \mid \mathfrak{p}$. Thus, $L_{\mathfrak{P}}$ splits $\alpha^{K_{\mathfrak{p}}}$ if and only if $\operatorname{ind}_{\mathfrak{p}}\alpha \mid [L:K]_{\mathfrak{p}}$, and $L_{\mathfrak{P}}$ embeds into the division algebra underlying $\alpha^{K_{\mathfrak{p}}}$ if and only if $[L:K]_{\mathfrak{p}} \mid \operatorname{ind}_{\mathfrak{p}}\alpha$. We also get

$$v_p(\operatorname{ind}_{\mathfrak{p}}\alpha) \le v_p(\operatorname{ind}_{\mathfrak{p}}\alpha^L) + v_p([L:K]_{\mathfrak{p}}), \tag{2-1}$$

[3] Theorem 5.15(a) of [Jacob and Wadsworth 1990] does not require that K be a global field.

where $\operatorname{ind}_{\mathfrak{p}} \alpha^L := \operatorname{ind} \alpha^{L_{\mathfrak{P}}}$ for any prime $\mathfrak{P}$ of L dividing $\mathfrak{p}$. Furthermore, (2-1) is an equality if $v_p(\operatorname{ind}_{\mathfrak{p}} \alpha^L) > 0$.

By the theorem of Albert, Brauer, Hasse, and Noether (see, for example, [Pierce 1982, §18.4]), a Brauer class over a global field is split by a field L if and only if its completions are split by L. In particular, for any cover L of M/K,

$$L \text{ splits } \alpha \text{ if and only if } \operatorname{ind}_{\mathfrak{p}} \alpha^M \mid [L:M]_{\mathfrak{p}} \text{ for all primes } \mathfrak{p} \text{ of } K. \tag{2-2}$$

Limits on local indices. Our first goal is to translate (A_m) to a condition about the existence of M/K with prescribed local degrees at finitely many primes of K (see Proposition 2.8 below). For this, in view of (2-2), we analyze the possible local indices $\operatorname{ind}_{\mathfrak{p}} \alpha^M$. We describe upper limits for the possible local indices in Lemmas 2.3 and 2.4, using the following terminology:

Definition 2.2. For $p \in \mathbb{P}$, let $u_p^{(1)}, u_p^{(2)}, \ldots$ be the family of numbers $v_p([M:K]_{\mathfrak{p}})$, where $\mathfrak{p}$ runs over the primes of K, ordered so that $u_p^{(1)} \geq u_p^{(2)} \geq \ldots$. If $u_p^{(1)} > u_p^{(2)}$, then the unique prime $\mathfrak{p}$ of K with $v_p([M:K]_{\mathfrak{p}}) = u_p^{(1)}$ is called *p-isolated* in M/K. We denote by g_p the gap $u_p^{(1)} - u_p^{(2)}$, so that $g_p > 0$ if and only if there is a p-isolated prime. We shall call a prime $\mathfrak{p}$ of K *isolated* if it is p-isolated for some $p \in \mathbb{P}$.

Let U_p be the set of primes $\mathfrak{p}$ of K for which $v_p([M:K]_{\mathfrak{p}}) \geq u_p^{(2)}$. Let U consist of the isolated primes in M/K, and if $|U_2|$ is finite and odd, also of the primes in U_2.

The following properties are deduced from Chebotarev's density theorem. For every infinite prime $\mathfrak{q}$ of K, $[M:K]_{\mathfrak{q}}$ is at most 2. If $2 \mid [M:K]$, by Chebotarev's theorem, there is a finite prime $\mathfrak{p}$ such that $[M:K]_{\mathfrak{p}} = 2$. In particular, infinite primes are nonisolated, and for every $i \in \mathbb{N}$ there is a finite prime $\mathfrak{p}_i$ with

$$v_p([M:K]_{\mathfrak{p}_i}) = u_p^{(i)}. \tag{2-3}$$

Moreover, for any prime $\mathfrak{q}$ of K unramified in M, by Chebotarev's theorem, there is a prime $\mathfrak{p}$ with $[M:K]_{\mathfrak{p}} = [M:K]_{\mathfrak{q}}$. Hence, isolated primes must ramify nontrivially in M/K, and the set U is finite. For every $p \in U_p$, the set U_p can be infinite, and in view of (2-3), it contains at least two finite primes.

For $m \in \mathbb{N}$ and a prime $\mathfrak{p}$ of K, define

$$w_p(m, \mathfrak{p}) := \begin{cases} v_p(m) & \text{if } \mathfrak{p} \text{ is non-}p\text{-isolated}, \\ \max\{v_p(m) - g_p, 0\} & \text{if } \mathfrak{p} \text{ is } p\text{-isolated}. \end{cases} \tag{2-4}$$

Note that the dependence on $\mathfrak{p}$ is marginal[4] and that clearly $w_p(m, \mathfrak{p}) \leq v_p(m)$.

[4] A reader who for the time being decides to disregard the possible appearance of isolated primes may substitute $v_p(m)$ for $w_p(m, \mathfrak{p})$.

Lemma 2.3. *For every* $\alpha \in \mathrm{Br}(K)$ *and prime* $\mathfrak{p}$ *of* K,

$$v_p(\mathrm{ind}_{\mathfrak{p}}\, \alpha^M) \le w_p(\mathrm{ind}\, \alpha^M, \mathfrak{p}). \tag{2-5}$$

Proof. Set $k := v_p(\mathrm{ind}_{\mathfrak{p}}\, \alpha^M)$, $n := v_p(\mathrm{ind}\, \alpha^M)$, and let $u_p^{(1)}, u_p^{(2)}$ be as above. For a non-p-isolated prime $\mathfrak{p}$, the assertion holds since $k \le n$. Assume that $\mathfrak{p}$ is p-isolated. The assertion to prove is: $k = 0$ or $n \ge k + g_p$. Assume $k > 0$. By (2-1),

$$v_p(\mathrm{ind}_{\mathfrak{p}}\, \alpha) = v_p(\mathrm{ind}_{\mathfrak{p}}\, \alpha^M) + v_p([M:K]_{\mathfrak{p}}) = k + u_p^{(1)}.$$

Since the sum of Hasse invariants of α is 0, there exists a prime $\mathfrak{p}_1 \ne \mathfrak{p}$ of K with $v_p(\mathrm{ind}_{\mathfrak{p}_1}\, \alpha) \ge k + u_p^{(1)}$. Since $v_p([M:K]_{\mathfrak{p}_1}) \le u_p^{(2)}$, (2-1) gives

$$n \ge v_p(\mathrm{ind}_{\mathfrak{p}_1}\, \alpha^M) \ge v_p(\mathrm{ind}_{\mathfrak{p}_1}\, \alpha) - v_p([M:K]_{\mathfrak{p}_1}) \ge k + u_p^{(1)} - u_p^{(2)} = k + g_p. \quad \square$$

To prove the second restriction, we use the following inequality, which holds[5] for every prime $\mathfrak{p}$ of K, $p \in \mathbb{P}$, and $m \in \mathbb{N}$:

$$w_p(m, \mathfrak{p}) + v_p([M:K]_{\mathfrak{p}}) \le v_p(m) + u_p^{(2)}, \tag{2-6}$$

with equality if and only if $\mathfrak{p} \in U_p$.

Lemma 2.4. *Let* $\alpha \in \mathrm{Br}(K)$ *with* $v_2(\mathrm{ind}\, \alpha^M) > g_2$ *and let* $p = 2$. *Then the number of primes* $\mathfrak{p} \in U_2$ *for which* (2-5) *is an equality is even.*

Proof. Let $m = \mathrm{ind}\, \alpha^M$. Let $U_{2,\alpha}$ be the set of primes $\mathfrak{p} \in U_2$ for which (2-5) is an equality. Then (2-1), (2-5), and (2-6) imply

$$\begin{aligned} v_2(\mathrm{ind}_{\mathfrak{p}}\, \alpha) &\le v_2(\mathrm{ind}_{\mathfrak{p}}\, \alpha^M) + v_2([M:K]_{\mathfrak{p}}) \\ &\le w_2(\mathrm{ind}\, \alpha^M, \mathfrak{p}) + v_2([M:K]_{\mathfrak{p}}) \le v_2(\mathrm{ind}\, \alpha^M) + u_2^{(2)} \end{aligned} \tag{2-7}$$

for every prime $\mathfrak{p}$ of K, with equalities for every $\mathfrak{p} \in U_{2,\alpha}$. Since (2-6) is strict for $\mathfrak{p} \notin U_2$ and (2-5) is strict for $\mathfrak{p} \in U_2 \setminus U_{2,\alpha}$, (2-7) is strict for every prime $\mathfrak{p} \notin U_{2,\alpha}$.

Let $r := v_2(\mathrm{ind}\, \alpha^M) + u_2^{(2)}$. Since (2-7) holds for all $\mathfrak{p}$, we have $v_2(\mathrm{ind}\, \alpha) \le r$ with equality if and only if $U_{2,\alpha}$ is nonempty. If $v_2(\mathrm{ind}\, \alpha) < r$, then $U_{2,\alpha}$ is empty and the assertion holds. Thus, we may assume $v_2(\mathrm{ind}\, \alpha) = r$ and write $\mathrm{ind}\, \alpha = 2^r m'$ for odd m'. Then the class $\alpha' := \alpha^{2^{r-1} m'} \in \mathrm{Br}(K)$ has exponent 2, nontrivial Hasse invariants at primes of $U_{2,\alpha}$, and trivial invariants outside $U_{2,\alpha}$. Since the sum of invariants of α' is 0, $|U_{2,\alpha}|$ is even. $\square$

Lemmas 2.3 and 2.4 lead to upper limits on local indices (see Proposition 2.8). We shall now construct elements which attain these upper bounds. We divide the construction into several cases:

---

[5] This inequality is easily verified separately for p-isolated and non-p-isolated primes.

Definition 2.5. For a finite set S of primes of K and $m \in \mathbb{N}$, (S, m) is *balanced* if $v_2(m) \le g_2$ or $|S \cap U_2|$ is even. We say that (S, m) is *balanceable* if S can be enlarged so that (S, m) is balanced, and otherwise *unbalanceable*.

Remark 2.6. Note that (S, m) is unbalanceable if and only if $|U_2|$ is odd, $S \supseteq U_2$, and $v_2(m) > g_2$. In particular, (S, m) can be unbalanceable only if m is even.

Lemma 2.4 shows that if $(S, 2^n)$ is unbalanceable, then there are no elements $\alpha \in \mathrm{Br}(K)$ with $\operatorname{ind} \alpha^M = 2^n$, and $\operatorname{ind}_{\mathfrak{p}} \alpha^M = 2^{w_2(2^n, \mathfrak{p})}$ for every $\mathfrak{p} \in S$. The following lemma constructs such elements if (S, m) is balanced.

Lemma 2.7. *Let n be a positive integer, $p \in \mathbb{P}$, $m = p^n$, and $\mathfrak{q} \in U_2$. Let S be a finite set of primes of K which contains at least two finite primes of U_p.*

Then there exists $\alpha \in \mathrm{Br}(K)$, with $\operatorname{ind} \alpha^M = m$, $\operatorname{ind}_{\mathfrak{p}} \alpha^M = 1$ for all $\mathfrak{p} \notin S$ and $\operatorname{ind}_{\mathfrak{p}} \alpha^M = \gcd(p, 2)$ for every real $\mathfrak{p} \in S$ which is unramified in M, such that

(i) *if (S, m) is balanced, then $\operatorname{ind}_{\mathfrak{p}} \alpha^M = p^{w_p(m, \mathfrak{p})}$ for all finite $\mathfrak{p} \in S$;*

(ii) *if (S, m) is unbalanceable, then $p = 2$, $\mathfrak{q} \in S$, $w_2(m, \mathfrak{q}) > 0$, $\operatorname{ind}_{\mathfrak{p}} \alpha^M = 2^{w_2(m, \mathfrak{p})}$ for all finite $\mathfrak{p} \in S \setminus \{\mathfrak{q}\}$, and $2^{w_2(m, \mathfrak{q}) - 1} \mid \operatorname{ind}_{\mathfrak{q}} \alpha^M$.*

Proof. Write $S_p := U_p \cap S$. Note that if (S, m) is unbalanceable then $p = 2$, $U_2 \subseteq S$, and $n - g_2 > 0$, and hence $\mathfrak{q} \in U_2 \subseteq S$ and $w_2(m, \mathfrak{q}) \ge n - g_2 > 0$.

If $p = 2$ and (S, m) is balanced, we claim that $|S_2|$ can be assumed to be even. Indeed, if $|S_2|$ is odd, then $n \le g_2$, M/K has a 2-isolated prime $\mathfrak{p}_1$, and $w_2(m, \mathfrak{p}_1) = 0$. Hence by Lemma 2.3, for any $\alpha \in \mathrm{Br}(K)$ with $\operatorname{ind} \alpha^M = m$, one has $\operatorname{ind}_{\mathfrak{p}_1} \alpha^M = 1$. Thus, we may add or remove $\mathfrak{p}_1$ from S without changing the desired assertion. We may therefore assume that $|S_2|$ is even, proving the claim.

We define α by setting its Hasse invariants. Let $\mathfrak{q}_1, \mathfrak{q}_2$ be two distinct finite primes in S_p. If (S, m) is unbalanceable, assume $\mathfrak{q}_1 = \mathfrak{q}$. Set $\operatorname{inv}_{\mathfrak{p}} \alpha$ to be of order $p^{r_{\mathfrak{p}}}$, where $r_{\mathfrak{p}} = n + v_p([M:K]_{\mathfrak{p}})$ for every finite $\mathfrak{p} \in S \setminus S_p$ and $r_{\mathfrak{p}} = n + u_p^{(2)}$ for every finite $\mathfrak{p} \in S_p \setminus \{\mathfrak{q}_1, \mathfrak{q}_2\}$, and of order $\gcd(p, 2)$ for every real $\mathfrak{p} \in S \setminus \{\mathfrak{q}_1, \mathfrak{q}_2\}$.

The order of all invariants we have set so far divides $p^{n+u_p^{(2)}}$. If (S, m) is balanced, we can set $\operatorname{inv}_{\mathfrak{q}_2} \alpha$ to be of order $p^{n+u_p^{(2)}}$ such that $x := \sum_{\mathfrak{p} \in S \setminus \{\mathfrak{q}_1\}} \operatorname{inv}_{\mathfrak{p}} \alpha$ has order $p^{n+u_p^{(2)}}$. Note that this is possible for $p = 2$ since the invariants which were set to be of order $2^{n+u_2^{(2)}}$ are at primes of $S_2 \setminus \{\mathfrak{q}_1, \mathfrak{q}_2\}$, a set of even order. If (S, m) is unbalanceable then $p = 2$, $n + u_2^{(2)} \ge 2$, and we can set $\operatorname{inv}_{\mathfrak{q}_2} \alpha = a/2^{n+u_2^{(2)}}$ for odd a such that $x := \sum_{\mathfrak{p} \in S \setminus \{\mathfrak{q}_1\}} \operatorname{inv}_{\mathfrak{p}} \alpha = b/2^{n+u_2^{(2)}}$ with $b \not\equiv 0 \pmod 4$. Note that this is possible since a can be chosen to be congruent to either 1 or 3 (mod 4).

Setting $\operatorname{inv}_{\mathfrak{q}_1} \alpha := -x$ and $\operatorname{inv}_{\mathfrak{p}} \alpha = 0$ for $\mathfrak{p} \notin S$ completes the definition of α. By (2-1), we have

$$v_p(\operatorname{ind}_{\mathfrak{p}} \alpha^M) = \max\{v_p(\operatorname{ind}_{\mathfrak{p}} \alpha) - v_p([M:K]_{\mathfrak{p}}), 0\}. \tag{2-8}$$

For finite $\mathfrak{p} \in S \setminus S_p$, we have $v_p(\operatorname{ind}_{\mathfrak{p}} \alpha) = n + v_p([M:K]_{\mathfrak{p}})$, and hence $\operatorname{ind}_{\mathfrak{p}} \alpha^M = p^n$ by (2-8). For finite $\mathfrak{p} \in S_p \setminus \{\mathfrak{q}_1\}$, we have $v_p(\operatorname{ind}_{\mathfrak{p}} \alpha) = n + u_p^{(2)}$, and hence (2-8) gives $\operatorname{ind}_{\mathfrak{p}} \alpha^M = p^{w_p(m,\mathfrak{p})}$ for all finite $\mathfrak{p} \in S \setminus \{\mathfrak{q}_1\}$, and $\operatorname{ind}_{\mathfrak{p}} \alpha^M = \gcd(p, 2)$ for all real $\mathfrak{p} \in S \setminus \{\mathfrak{q}_1\}$ unramified in M/K. If (S, p^n) is balanced, $\operatorname{ind}_{\mathfrak{q}_1} \alpha = p^{n+u_p^{(2)}}$, and hence by (2-8) we have $\operatorname{ind}_{\mathfrak{q}_1} \alpha^M = p^{w_p(p^n,\mathfrak{q}_1)}$, as required.

If (S, p^n) is unbalanceable then $p = 2$, $2^{n+u_2^{(2)}-1} \mid \operatorname{ind}_{\mathfrak{q}_1} \alpha$, $n > g_2$, and hence $w_2(2^n, \mathfrak{q}_1) > 0$. Thus, (2-8) and (2-6) give

$$v_2(\operatorname{ind}_{\mathfrak{q}_1} \alpha^M) \geq n + u_2^{(2)} - 1 - v_2([M:K]_{\mathfrak{q}_1}) = w_2(2^n, \mathfrak{q}_1) - 1.$$

Since $\operatorname{ind}_{\mathfrak{p}} \alpha^M \mid p^n$ for all $\mathfrak{p}$, $\operatorname{ind} \alpha^M \mid p^n$. Since S_p contains two finite primes, at least one of these primes $\mathfrak{p}$ satisfies $w_p(m, \mathfrak{p}) = n$, and hence $\operatorname{ind} \alpha^M = \operatorname{ind} \alpha_{\mathfrak{p}}^M = p^n$. $\square$

Covers with prescribed local degrees. We can now translate (A$_m$) to a condition on the local degrees of covers. Let $m \in \mathbb{N}$. For a finite prime $\mathfrak{p}$ of K, define $d_{\mathfrak{p}}(m) \in \mathbb{N}$ by requiring $p \in \mathbb{P}$ for every $v_p(d_{\mathfrak{p}}(m)) = w_p(m, \mathfrak{p})$. For an infinite prime $\mathfrak{p}$ of K, set $d_{\mathfrak{p}}(m) := \gcd(m, 2)$ if $\mathfrak{p}$ is real and unramified in M and $d_{\mathfrak{p}}(m) := 1$ otherwise.

Clearly, $d_{\mathfrak{p}}(m) \mid m$ for any $\mathfrak{p}$, and $d_{\mathfrak{p}}(m) = m$ if $\mathfrak{p}$ is finite and nonisolated.

Proposition 2.8. *Condition* (A$_m$) *is equivalent to*:

For every finite set S and $\mathfrak{q} \in U_2$, M/K has an m-cover L such that $d_{\mathfrak{p}}(m) \mid [L:M]_{\mathfrak{p}}$ for every $\mathfrak{p} \in S$, except for $\mathfrak{p} = \mathfrak{q}$ when (S, m) is unbalanceable, in which case $(d_{\mathfrak{q}}(m)/2) \mid [L:M]_{\mathfrak{q}}$. (B$_m$)

Proof. (B$_m$) $\Longrightarrow$ (A$_m$): Let $\alpha \in \operatorname{Br}(K)$ with $\operatorname{ind} \alpha^M = m$. Let S be the set of primes $\mathfrak{p}$ of K such that $\operatorname{ind}_{\mathfrak{p}} \alpha \neq 1$. For every finite $\mathfrak{p}$ and $p \in \mathbb{P}$, Lemma 2.3 implies

$$v_p(\operatorname{ind}_{\mathfrak{p}} \alpha^M) \leq w_p(m, \mathfrak{p}) = v_p(d_{\mathfrak{p}}(m)).$$

If $\mathfrak{p}$ is real and unramified in M, $\operatorname{ind}_{\mathfrak{p}} \alpha^M \mid \gcd(m, 2) = d_{\mathfrak{p}}(m)$. Thus, $\operatorname{ind}_{\mathfrak{p}} \alpha \mid d_{\mathfrak{p}}(m)$ for all primes $\mathfrak{p}$ of K. If (S, m) is balanceable, (B$_m$) gives an m-cover L for which $\operatorname{ind}_{\mathfrak{p}} \alpha^M \mid [L:M]_{\mathfrak{p}}$ for all $\mathfrak{p} \in S$. Hence, by (2-2), L splits α.

Assume (S, m) is unbalanceable. By Lemma 2.4, there is a prime $\mathfrak{q} \in U_2 \subseteq S$ for which

$$v_2(\operatorname{ind}_{\mathfrak{q}} \alpha^M) \leq w_2(m, \mathfrak{q}) - 1.$$

It follows that $\operatorname{ind}_{\mathfrak{p}} \alpha^M \mid d_{\mathfrak{p}}(m)$ for all $\mathfrak{p} \neq \mathfrak{q}$ and $\operatorname{ind}_{\mathfrak{q}} \alpha^M \mid (d_{\mathfrak{q}}(m)/2)$. Letting L be the m-cover obtained by applying (B$_m$) with S and $\mathfrak{q}$, we have $\operatorname{ind}_{\mathfrak{p}} \alpha^M \mid [L:M]_{\mathfrak{p}}$ for all $\mathfrak{p} \in S$. Hence, by (2-2), L splits α.

(A$_m$) $\Longrightarrow$ (B$_m$): Let S be any finite set of primes of K and $\mathfrak{q} \in U_2$. For every $p \mid m$, if $|S \cap U_p| \geq 2$, let $S_p := S$; otherwise form S_p by adding to S finite primes of U_p, so that $|S_p \cap U_p| = 2$. Note that (S_2, m) is unbalanceable if and only if (S, m) is unbalanceable. If (S_2, m) is balanceable, enlarge S_2 to assume that (S_2, m) is balanced.

For every $p \mid m$, construct α_p by applying Lemma 2.7 with p, $n = v_p(m)$, $\mathfrak{q}$, and S_p. Set $\alpha = \sum_{p|m} \alpha_p$. Since $S_p \supseteq S$, by the definition of $d_\mathfrak{p}(m)$, the properties of α_p, $p \mid m$, give $\operatorname{ind} \alpha^M = m$, $\operatorname{ind}_\mathfrak{p} \alpha^M = \gcd(m, 2)$ for all real $\mathfrak{p} \in S$ which are unramified in M, and $\operatorname{ind}_\mathfrak{p} \alpha^M = d_\mathfrak{p}(m)$ for every finite $\mathfrak{p} \in S$, except for $\mathfrak{p} = \mathfrak{q}$ when (S, m) is unbalanceable, in which case $\operatorname{ind}_\mathfrak{q} \alpha^M = d_\mathfrak{q}(m)/2$. Applying (A_m) to α, we obtain the desired cover L. □

Remark 2.9. The proof of Proposition 2.8 shows that if there are noncrossed products $\alpha + \chi$ with $\operatorname{ind} \alpha^M = m$, then there are infinitely many such noncrossed products. Indeed, if (B_m) fails for a set S_0, it fails for every set S containing S_0, so that (S, m) is balanceable if and only if (S_0, m) is balanceable. The proof reveals that for every such set S, there is an α whose Hasse invariants are nonzero at primes of S and $\alpha + \chi$ is a noncrossed product. In particular, there are infinitely many such classes α.

Definition 2.10. For a prime $\mathfrak{p}$ of K, we say that the cover L has *full local degree* at $\mathfrak{p}$ if $[L : M]_\mathfrak{p} = [L : M]$ for finite $\mathfrak{p}$, or if $[L : M]_\mathfrak{p} = \gcd(2, [L : M])$ for real $\mathfrak{p}$, or if $\mathfrak{p}$ is complex. For a set S of primes of K, we say L has *full local degree in* S if L has full local degree at each $\mathfrak{p} \in S$.

Note that (B_m) requires full local degree at every $\mathfrak{p} \in S \setminus U$.

Lemma 2.11. *Let $m' \mid m$. Suppose there is a finite nonempty set S_0 disjoint from U such that any m-cover of M/K with full local degree in S_0 contains an m'-cover. Then (B_m) implies $(\mathrm{B}_{m'})$.*

Proof. Let $\mathfrak{p}_1$ be a finite prime for which $v_2([M : K]_{\mathfrak{p}_1}) = u_2^{(1)}$. For a given finite set S, let $S' := S \cup S_0$. Note that there are three possible cases: (a) (S', m') and (S', m) are balanceable; (b) (S', m') and (S', m) are unbalanceable; (c) (S', m') is balanceable and (S', m) is not. Also note that (c) occurs only if $w_2(m', \mathfrak{p}_1) = 0$.

If (b) occurs, fix a prime $\mathfrak{q} \in U_2$. Let L be an m-cover obtained by applying (B_m) to S', S' and $\mathfrak{q}$, and S' and $\mathfrak{p}_1$ in cases (a), (b), (c), respectively. Since $S_0 \cap U = \varnothing$, L has full local degree in S_0. By assumption, L contains an m'-cover L' of M/K. Since $d_\mathfrak{p}(m) \mid [L : M]_\mathfrak{p}$ (resp. $(d_\mathfrak{p}(m)/2) \mid [L : M]_\mathfrak{p}$) implies $d_\mathfrak{p}(m') \mid [L' : M]_\mathfrak{p}$ (resp. $(d_\mathfrak{p}(m')/2) \mid [L' : M]_\mathfrak{p}$) for all primes $\mathfrak{p}$ of K, L' satisfies $d_\mathfrak{p}(m') \mid [L' : M]_\mathfrak{p}$ for all $\mathfrak{p} \in S$ except for $\mathfrak{p} = \mathfrak{q}$ when (b) holds, in which case $(d_\mathfrak{q}(m')/2) \mid [L' : M]_\mathfrak{p}$. □

Reduction to prime powers. Having shown the equivalence of (I_m) and (B_m), we now consider (B_m). We provide choices of the set S that enforce tight restrictions on the structure of $\mathrm{Gal}(L/K)$ for covers L of M/K with full local degree in S.

Our first usage of this strategy is in reducing (B_m) from arbitrary $m \in \mathbb{N}$ to prime powers. Except for the part concerning the characteristic of K (Lemma 2.13 below), this reduction is identical to the corresponding one in [Hanke and Sonn 2011].

Let $m = \prod p^{n_p}$ be the prime factorization. By taking field composita of covers, if $(\mathrm{B}_{p^{n_p}})$ holds for all $p \mid m$, then (B_m) holds. We show:

Proposition 2.12. *(B_m) holds if and only if $(\mathrm{B}_{p^{n_p}})$ holds for all $p \mid m$.*

We first treat the wild case separately:

Lemma 2.13. *If $p = \operatorname{char} K$ then (B_{p^n}) holds for all $n \in \mathbb{N}$.*

Proof. Let $n \in \mathbb{N}$ and S be a finite set of primes of K. For every $\mathfrak{p} \in S$ there is a cyclic p^n-extension $L'(\mathfrak{p})/K_{\mathfrak{p}}$ which is disjoint from $M_{\mathfrak{p}}$ (see [Koch 1970, Satz 10.4][6]). By the Grunwald–Wang theorem, there is a cyclic p^n-extension L'/K whose completion at $\mathfrak{p}$ is $L'_{\mathfrak{p}} = L'(\mathfrak{p})$ for all $\mathfrak{p} \in S$. Let $L := L'M$. Since $L'_{\mathfrak{p}} \cap M_{\mathfrak{p}} = K_{\mathfrak{p}}$, one has $[L : M]_{\mathfrak{p}} = p^n$ for all $\mathfrak{p} \in S$. Thus, L is a p^n-cover of M/K with full local degree in S. □

It remains to show that (B_m) implies $(\mathrm{B}_{p^{n_p}})$ for all $p \mid m$ with $p \neq \operatorname{char} K$.

Proof of Proposition 2.12. Let $p \mid m$ with $p \neq \operatorname{char} K$. By [Hanke and Sonn 2011, §7, p. 325, Corollary], there are infinitely many primes $\mathfrak{p}$ of K such that for any m-cover of M/K with full local degree at $\mathfrak{p}$, the p-Sylow subgroup of $\operatorname{Gal}(L/M)$ has a complement $\operatorname{Gal}(L/M_0)$ which is normal in $\operatorname{Gal}(L/K)$, and hence L contains a p^n-cover M_0 of M/K. (Note that the assumption M/K cyclic is never used in the proof of [Hanke and Sonn 2011, §7, p. 325, Corollary].) Since U is finite we can choose such $\mathfrak{p} \notin U$. The proof is completed by setting $S_0 := \{\mathfrak{p}\}$ in Lemma 2.11. □

An invariant subgroup. We are now able to complete the proof of Theorem 1.1. As outlined in Section 2, and using Propositions 2.8 and 2.12, it remains to prove Proposition 2.14 below. Let $p \in \mathbb{P}$ be fixed.

Proposition 2.14. *For any $n \in \mathbb{N}$, (B_{p^n}) implies $(\mathrm{B}_{p^{n-1}})$.*

Indeed, the bound $b_p(\chi)$ of Theorem 1.1 is the maximal n for which (B_{p^n}) holds if such a maximum exists, and $b_p(\chi) = \infty$ otherwise. For more details on the description of $b_p(\chi)$, see Corollary 2.17 below.

For any cover L of M/K, we consider the group extension

$$1 \to \operatorname{Gal}(L/M) \to \operatorname{Gal}(L/K) \to \operatorname{Gal}(M/K) \to 1. \tag{2-9}$$

We will analyze several kinds of constraints that are imposed on (2-9) by the condition that L has full local degree in S_0, for certain chosen sets S_0. More precisely, after showing that the kernel $A := \operatorname{Gal}(L/M)$ can be assumed to be abelian, we focus on constraints regarding the conjugation action of $B := \operatorname{Gal}(M/K)$ on A. The analysis of this action is the main ingredient in the proofs of both Proposition 2.14 and Theorem 1.2 below.

[6] Koch's book has been translated into English. However, Theorem 10.4 in the English version contains a typo: "finitely generated" should be replaced by "on countably many generators".

In view of Lemma 2.13, we assume from now on that $p \neq \operatorname{char} K$. Fix p^n and set $T := M \cap K(\mu_{p^\infty})$. For the proof of Proposition 2.14, it will suffice to analyze the action of $\operatorname{Gal}(M/T)$ on A.

Lemma 2.15. *There exists a finite set S_0 of primes of K disjoint from U such that for any p^n-cover L of M/K with full local degree in S_0, the kernel A is abelian, the group* $\operatorname{Gal}(M/T)$ *acts trivially on A, and A has rank at most* 2.

Proof. At first fix a $\sigma \in \operatorname{Gal}(M/T)$. By the Chebotarev density theorem, the Galois extension $M(\mu_{p^n})/K$ has infinitely many unramified finite primes $\mathfrak{P}$ of $M(\mu_{p^n})$ whose Frobenius element restricts to the identity on $K(\mu_{p^n})$ and to σ on M. Of those infinitely many $\mathfrak{P}$, choose one such that $\mathfrak{p} := \mathfrak{P} \cap K \notin U$ and p does not divide the norm $N(\mathfrak{p})$. (There are only finitely many $\mathfrak{P}$ that do not satisfy this, since $p \neq \operatorname{char} K$.) Since $p \nmid N(\mathfrak{p})$ and $\mu_{p^n} \subset K_{\mathfrak{p}}$, we have $N(\mathfrak{p}) \equiv 1 \pmod{p^n}$.

Assume a p^n-cover L of M/K has full local degree at the chosen $\mathfrak{p}$. Let $\mathfrak{P}$ be a prime of L dividing $\mathfrak{p}$. The decomposition group $\operatorname{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ then equals $\operatorname{Gal}(L/M^\sigma)$, where M^σ is the fixed field of σ. We will show that $\operatorname{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ is abelian, and thus σ acts trivially on $\operatorname{Gal}(L/M)$: since $\operatorname{char} K \nmid N(\mathfrak{p})$, $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is tame. Therefore, $\operatorname{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ is a metacyclic group, generated by the inertia group $I_{\mathfrak{P}}$ and the Frobenius element, with the Frobenius acting on $I_{\mathfrak{P}}$ by raising each element to the power $N(\mathfrak{p})$. Since $\mathfrak{p}$ is unramified in M, $|I_{\mathfrak{P}}|$ divides p^n. Hence $\operatorname{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ is abelian, because $N(\mathfrak{p}) \equiv 1 \pmod{p^n}$.

Now let Σ be a set of generators of $\operatorname{Gal}(M/T)$, or $\Sigma = \{1\}$ if $M = T$. For each $\sigma \in \Sigma$, choose a prime $\mathfrak{p}_\sigma$ as described in the first paragraph of the proof. Then $S_0 := \{\mathfrak{p}_\sigma \mid \mathfrak{p} \in \Sigma\}$ has the desired property. $\square$

By Lemma 2.11, Proposition 2.14 is completed once we show:

Proposition 2.16. *Let S_0 be as in Lemma 2.15. Any p^n-cover of M/K with full local degree in S_0 contains a p^{n-1}-cover of M/K.*

Proof. We have assumed $p \neq \operatorname{char} K$. Let $B = \operatorname{Gal}(M/K)$. Let L be a p^n-cover of M/K with full local degree in S_0. By Lemma 2.15, the kernel A is abelian. The subgroup $A[p]$ of p-torsion elements is a characteristic subgroup and hence invariant under the action of B (we say *B-invariant*). It suffices to find a B-invariant subgroup $A_0 \leq A[p]$ of order p; then the fixed field L^{A_0} is the desired p^{n-1}-cover.

If A is cyclic then $A[p]$ itself is such a subgroup; hence, assume A noncyclic for the rest of the proof.

Recall that $A[p]$ is an $\mathbb{F}_p$-vector space and that any action of some group H on $A[p]$ is a representation of H over $\mathbb{F}_p$. In this sense, the H-invariant subgroups of order p are the H-invariant subspaces of dimension 1.

By Lemma 2.15, B acts on A through $\operatorname{Gal}(T/K)$. Let $\operatorname{Gal}(T/K) = P \oplus C$ with P the p-part and $|C|$ prime to p. Then $|C|$ divides $p-1$. Since $|C|$ is prime to p, any representation of C over $\mathbb{F}_p$ is semisimple and hence decomposes into a product of irreducible representations. Since $\mathbb{F}_p$ contains the $|C|$-th roots of unity, the irreducible representations of C are of dimension 1. Thus, there is a C-invariant subgroup $A_0 \leq A[p]$ of order p.

By Lemma 2.15, A has rank 2, that is, $A[p] \cong C_p \times C_p$. This group has exactly $p+1$ order-p subgroups, say $A_0, \dots, A_p$, which are permuted by the action of B. Thus, we have an induced action of B on the set of indices $\{0, \dots, p\}$.

We know A_0 is C-invariant. If A_0 is P-invariant then A_0 is B-invariant and we are done. Assume A_0 is not P-invariant. Since P is a p-group, there are two P-orbits on $\{0, \dots, p\}$, say $\{0, \dots, p-1\}$ and $\{p\}$. Since P and C commute and A_0 is C-invariant, each of $A_0, \dots, A_{p-1}$ is also C-invariant. Hence the remaining subgroup A_p is C-invariant and P-invariant. We found a B-invariant subgroup A_p of A with $|A_p| = p$. As noted in the beginning of the proof, this gives the assertion. □

This completes the proof of Proposition 2.14, and hence of Theorem 1.1.

Summary. In addition to the existence of bounds (Theorem 1.1) we get:

Corollary 2.17. *The bound $b_p(\chi)$ is the maximal n such that for every finite set S of primes of K and $\mathfrak{q} \in U_2$, there is a p^n-cover L of M/K satisfying*:

(i) $d_{\mathfrak{p}}(p^n) \mid [L:M]_{\mathfrak{p}}$ *for all $\mathfrak{p} \in S$, except for $\mathfrak{p} = \mathfrak{q}$ when $p = 2$ and $(S, 2^n)$ is unbalanceable*, *in which case* $(d_{\mathfrak{q}}(2^n)/2) \mid [L:M]_{\mathfrak{q}}$;

(ii) $A = \mathrm{Gal}(L/M)$ *is abelian of rank at most* 2;

(iii) $\mathrm{Gal}(M/T)$ *acts trivially on A via conjugation in* $\mathrm{Gal}(L/K)$.

If no maximal n exists, *then* $b_p(\chi) = \infty$.

Proof. Let S_0 be a finite set of primes of K that is disjoint from U. Suppose that any p^n-cover of L with full local degree in S_0 has a certain property. Then this property can be added to the condition (B_{p^n}) without changing the truth value of (B_{p^n}), because the set S in (B_{p^n}) can be enlarged by S_0. By Lemma 2.15, this argument applies to the properties (ii) and (iii). Hence, the corollary is a consequence of Proposition 2.14. □

Remark 2.18. Regarding condition (i) in Corollary 2.17, if $\mathfrak{p}$ is not isolated, then $d_{\mathfrak{p}}(p^n) \mid [L:M]_{\mathfrak{p}}$ is equivalent to saying that L has full local degree at $\mathfrak{p}$.

Regarding condition (iii) in Corollary 2.17, if M and $K(\mu_{p^\infty})$ are disjoint over K, then (iii) is equivalent to saying that the group extension (2-9) is central.

3. Finiteness of bounds

The exponents of kernels. Suppose we use the setup described in Section 2, so that M/K is an abelian extension of global fields. Let $p \in \mathbb{P}$ be fixed and different from char K, and as before set $T := K(\mu_{p^\infty}) \cap M$. In Section 2 we showed that suitable choices of the set S put constraints on structure of covers L of M/K with full local degree in S, to the extent that the action of $\mathrm{Gal}(M/T)$ on $A = \mathrm{Gal}(L/M)$ is trivial. This was sufficient to prove the existence of the bounds. Now, in order to prove the finiteness of the bounds, we analyze constraints on the action of the entire group $B = \mathrm{Gal}(M/K)$ on A. The set S for this purpose will be constructed from the families Q_σ, which we define next for each $\sigma \in B$.

Denote by p^s the number of p-power roots of unity in M and by r the maximal number for which $\mu_{2^r} \subseteq M(\sqrt{-1})$. Let U be the finite set defined in Definition 2.2, so that for every finite set S, condition (B_m) requires full local degree at every prime $\mathfrak{p} \in S \setminus U$.

Fix an element $\sigma \in B$ and let f_σ be the order of the restriction $\sigma_{|T}$ of σ to T. We define Q_σ to be the set of all primes $\mathfrak{p} \notin U$ of K, unramified in M, whose Frobenius automorphism in M/K is σ, and such that the norm $N(\mathfrak{p})$ is prime to p and is of order strictly greater than f_σ as an element of $(\mathbb{Z}/p^{s+1}\mathbb{Z})^*$ (resp. mod $(\mathbb{Z}/2^{r+2}\mathbb{Z})^*$ if $p = 2$).

Lemma 3.1. *For every $\sigma \in B$, the set Q_σ is infinite.*

Proof. Assume without loss of generality that $\sqrt{-1} \in M$. Otherwise, repeat the proof for a lift $\tau \in \mathrm{Gal}(M(\sqrt{-1})/K)$ of σ to deduce that Q_τ is infinite. Since $Q_\tau \subseteq Q_\sigma$ and $f_\tau \geq f_\sigma$, the assertion for σ follows. Note that under this assumption we have $r = s$, so we will use only s in the rest of the proof. Set $T' := K(\mu_{p^{s+1}})$ (resp. $T' := K(\mu_{2^{s+2}})$ if $p = 2$) and note that $T' \cap M = T$.

We first claim that $\mathrm{Gal}(T'/K)$ contains an element σ' of order greater than f_σ whose restriction to T is $\sigma_{|T}$. For $s > 0$, $T = K(\mu_{p^s})$, and hence the group $\mathrm{Gal}(T/T^\sigma)$ is naturally identified with a subgroup H of $(\mathbb{Z}/p^s\mathbb{Z})^*$, and $\mathrm{Gal}(T'/T^\sigma)$ is identified with the full preimage of H under the natural projection

$$\pi : (\mathbb{Z}/p^{s+1}\mathbb{Z})^* \to (\mathbb{Z}/p^s\mathbb{Z})^* \quad (\text{resp. } \pi : (\mathbb{Z}/2^{s+2}\mathbb{Z})^* \to (\mathbb{Z}/2^s\mathbb{Z})^* \text{ if } p = 2).$$

The claim follows for $s > 0$ since each element of $(\mathbb{Z}/p^s\mathbb{Z})^*$ has a preimage under π of a greater order. If $s = 0$, then p is odd, and the claim holds, as the restriction map $\mathrm{Gal}(T'/T^\sigma) \to \mathrm{Gal}(T/T^\sigma)$ is an epimorphism of cyclic groups with nontrivial kernel.

Since σ and σ' agree on T, Chebotarev's density theorem implies that there are infinitely many primes $\mathfrak{p}$ of K, with $p \nmid N(\mathfrak{p})$, whose Frobenius automorphism is σ' in T'/K and is σ in M/K. Such primes are in Q_σ since the order of the norm of $\mathfrak{p}$ as an element in $(\mathbb{Z}/p^{s+1}\mathbb{Z})^*$ (resp. in $(\mathbb{Z}/2^{s+2}\mathbb{Z})^*$) is the same as the order of their Frobenius automorphism in $K(\mu_{p^{s+1}})/K$ (resp. in $K(\mu_{2^{s+2}})/K$). □

For a prime $\mathfrak{p}$ of K, denote by $e_\mathfrak{p}(L/K)$ the ramification index of $\mathfrak{p}$ in a Galois extension L/K.

Lemma 3.2. *Let S_0 be as in Lemma 2.15 and let $\sigma \in B$. Suppose that a p^n-cover L of M/K has full local degree in S_0 and at $\mathfrak{p} \in Q_\sigma$. Then $e_\mathfrak{p}(L/K) \mid p^s$ if p is odd and $e_\mathfrak{p}(L/K) \mid 2^{r+1}$ if $p = 2$.*

Proof. By Lemma 2.15, the kernel A is abelian, $\mathrm{Gal}(M/T)$ acts trivially on A, and hence the action of B on A factors through the action of $\mathrm{Gal}(T/K)$. Thus, σ acts on the inertia group $I \subseteq A$ of $\mathfrak{p}$ in L/K as an automorphism of order at most f_σ.

Assume on the contrary that there is an element $a \in I$ of order p^{s+1} (resp. 2^{r+2} if $p = 2$). Since $\mathfrak{p}$ is tamely ramified in L, σ acts on I by raising each element to the power $N(\mathfrak{p})$ and hence defines an automorphism of order greater than f_σ on $\langle a \rangle$, a contradiction. □

We derive Theorem 1.2 from the following proposition, whose proof appears in the end of this subsection.

Proposition 3.3. *Assume the p-Sylow subgroup of B is noncyclic. Then there exists a finite set S_0 of primes of K disjoint from U such that for any p^n-cover L of M/K with full local degree in S_0, $\mathrm{Gal}(L/M)$ is abelian of rank at most 2 and exponent at most p^s (resp. 2^{r+2} if $p = 2$).*

If the p-Sylow subgroup of B is noncyclic, then Proposition 3.3 allows us to improve on Corollary 2.17 by adding the following property to the list:

(iv) $\exp A \mid p^s$ *if p is odd and* $\exp A \mid 2^{r+2}$ *if $p = 2$.*

In particular, since A has rank at most 2, $b_p(\chi) \le 2s$ if p is odd and $b_p(\chi) \le 2(r+2)$ if $p = 2$. This proves Theorem 1.2.

The proof of Proposition 3.3 relies on the following group-theoretic proposition, whose proof is given starting on page 851.

Proposition 3.4. *Let*

$$1 \to A \to G \xrightarrow{\pi} B \to 1 \tag{3-1}$$

be an extension of nontrivial abelian p-groups A, B. If B is noncyclic and $\pi^{-1}\langle x \rangle$ is cyclic for all $x \in B$, then $|A| = 2$.

Proof of Proposition 3.3. Replacing K with the fixed field of the p-Sylow subgroup of B, we can assume without loss of generality that B is a p-group. By the assumptions of the proposition, B is a noncyclic abelian group.

Choose S_0 to be the set from Lemma 2.15 joined with one $\mathfrak{p}_\sigma \in Q_\sigma$ for each $\sigma \in B$. Suppose L is a p^n-cover of M/K with full local degree in S_0.

By Lemma 2.15, A is abelian of rank at most 2. Since the p^s-torsion subgroup $A[p^s]$ is a characteristic subgroup of A, it is a normal subgroup of $\mathrm{Gal}(L/K)$ and hence the fixed field $L_0 := L^{A[p^s]}$ is Galois over K. If $p = 2$, then we consider $L_0 := L^{A[2^{r+1}]}$ instead, which is also Galois over K. To prove our claim it suffices to show that $L_0 = M$ (resp. $[L_0 : M] \le 2$ if $p = 2$).

Fix an element $\sigma \in B$ and let $\mathfrak{P}_\sigma$ be a prime of L which divides $\mathfrak{p}_\sigma$. Let $I_\sigma \subseteq A$ be the inertia group of $\mathfrak{P}_\sigma$ in L/K. By Lemma 3.2, $|I_\sigma| \le p^s$ (resp. $|I_\sigma| \le 2^{r+1}$) and hence $I_\sigma \subseteq A[p^s]$ (resp. $I_\sigma \subseteq A[2^{r+1}]$). Thus, L_0/K is unramified at $\mathfrak{p}_\sigma$ and hence $\mathfrak{P}_\sigma \cap L_0$ has a cyclic decomposition group in L_0/K. Since L_0 has full local degree at $\mathfrak{p}$, the decomposition group of $\mathfrak{P}_\sigma \cap L_0$ in L_0/K is $\mathrm{Gal}(L_0/M^\sigma)$, and hence L_0/M^σ is a cyclic extension.

Since L_0/M^σ is cyclic for all $\sigma \in B$ and since B is noncyclic, Proposition 3.4 applied to the group extension

$$1 \to \mathrm{Gal}(L_0/M) \to \mathrm{Gal}(L_0/K) \to \mathrm{Gal}(M/K) \to 1$$

shows $L_0 = M$ (resp. $[L_0 : M] \le 2$ if $p = 2$), proving the claim. □

Central group extensions. The last ingredient is a proof of Proposition 3.4. We begin with elementary properties of commutators in a central group extension

$$1 \to A \to G \to B \to 1 \tag{3-2}$$

of abelian groups A, B. Let $s : B \to G$ be a section of $G \to B$ (not necessarily a homomorphism).

Lemma 3.5. *Commutators in G are bimultiplicative. That is, the map*

$$\beta : B \times B \to A, \quad (x, y) \mapsto [s(x), s(y)]$$

does not depend on the choice of s and is bimultiplicative.

Proof. Since $[G, G] \subseteq A \subseteq Z(G)$, we have

$$[ab, x] = abxb^{-1}a^{-1}x^{-1} = a(bxb^{-1}x^{-1})xa^{-1}x^{-1} = [a, x][b, x].$$

Similarly one checks $[x, ab] = [x, a][x, b]$, that is, that commutators are bimultiplicative. The statement about β follows from this. □

We next look at the meaning of the condition that $\pi^{-1}\langle x \rangle$ is cyclic for $x \in B$. For $x = 1$ it means A is cyclic, and for $x \ne 1$ one has:

Lemma 3.6. *Assume A is cyclic. For $x \in B$, $x \ne 1$, $\pi^{-1}\langle x \rangle$ is cyclic if and only if A is trivial or generated by $s(x)^{\operatorname{ord} x}$.*

In order to prove Proposition 3.4, we now assume A, B are nontrivial p-groups and A is cyclic. The map

$$\gamma : B[p] \to A/A^p, \quad x \mapsto s(x)^p$$

is obviously independent of the choice of s.

Lemma 3.7. *Assume A, B are nontrivial p-groups and A is cyclic.*

(i) *For $x \in B[p]$, $x \ne 1$, $\pi^{-1}\langle x \rangle$ is cyclic if and only if $\gamma(x) \ne 1$.*

(ii) *If p is odd then γ is a homomorphism.*

(iii) *If $p=2$ then γ is a homomorphism if and only if $\beta(x,y)\in A^2$ for all x,y in $B[2]$.*

Proof. (i) is Lemma 3.6. Since $[G,G]\subseteq A\subseteq Z(G)$, we have $(s(x)s(y))^p = s(x)^p s(y)^p \beta(x,y)^{p(p-1)/2}$ for all $x,y\in B$. In particular, for all $x,y\in B[p]$,

$$\gamma(xy)=s(xy)^pA^p=(s(x)s(y))^pA^p=\gamma(x)\gamma(y)\beta(x,y)^{p(p-1)/2}.$$

Thus γ is a homomorphism if and only if $\beta(x,y)^{p(p-1)/2}\in A^p$. If $p=2$ then $p(p-1)/2=1$, proving (iii). For p odd, we use Lemma 3.5 to see that $\beta(x,y)\in A[p]$ for all $x,y\in B[p]$, so the term $\beta(x,y)^{p(p-1)/2}$ vanishes. □

Proof of Proposition 3.4. Let A,B be nontrivial abelian p-groups, A cyclic and B noncyclic. By hypothesis and Lemma 3.7(i), $\gamma(x)\neq 1$ for all $x\in B[p]$, $x\neq 1$. Therefore, if γ is a homomorphism then it is injective, in contradiction to A being cyclic and B noncyclic. Hence, γ is not a homomorphism. By parts (ii) and (iii) of Lemma 3.7, we have $p=2$ and an element $a:=\beta(x,y)\notin A^2$ for some $x,y\in B[2]$. By Lemma 3.5, $a\in A[2]\setminus A^2$ and hence $|A|=2$. □

4. Examples

Suppose we are in the setup described in Section 2. In particular, $\alpha\in \mathrm{Br}(K)$, $\chi\in \mathrm{Hom}(G_K,\Delta/\Gamma)$, and M is the fixed field of $\ker\chi$, an abelian extension of K. In this section we provide examples of noncrossed products with the smallest possible indices in fibers over noncyclic χ.

For $p\in\mathbb{P}$, let $p^{s_p(M)}$ denote the number of p-power roots of unity in M. If $\alpha+\chi$ has index equal to $|\chi|$, then the division algebra contained in $\alpha+\chi$ is a crossed product, because α is split by M. Therefore, noncrossed products of index p^2 are possible only if $|\chi|=p$, in particular only if χ is cyclic.

Suppose χ is noncyclic with $|\chi|=p^2$. If $b_p(\chi)=0$, then the fiber over χ contains infinitely many noncrossed products of index $p|\chi|$. By Theorem 1.2, this happens, for example, whenever $s_p(M)=0$. We give examples of bicyclic χ with $|\chi|=p^2$ and $b_p(\chi)=0$ but $s_p(M)\geq 1$. Note that such a phenomenon is in contrast to the case of cyclic χ, for which one always has $b_p(\chi)\geq s_p(M)$ (see [Hanke and Sonn 2011]).

For $p=2$, an example as described above was given over $K=\mathbb{Q}$ in [Hanke 2004] and over $K=\mathbb{F}_q(t)$ for all $q\equiv 3 \pmod 8$ in [Coyette 2012, Example 2.8]. These turn out to be special cases of our Examples 4.1 and 4.3 below.

We start with $K=\mathbb{Q}$ and $p=2$:

Example 4.1. Let q,ℓ be odd primes such that $q\equiv 3 \pmod 4$, $q\not\equiv -\ell \pmod 8$, and q is a nonsquare modulo ℓ. Note that for any odd prime ℓ, a suitable q can be chosen using Dirichlet's theorem.[7] Let $M := \mathbb{Q}(\sqrt{q}, \sqrt{-\ell})$. Corollary 2.17 applied with $S = \{\ell\}$ and the following claim show $b_p(\chi) = 0$.

Claim. The extension $M/\mathbb{Q}$ has no isolated primes and there is no 2-cover L of M/K with local degree $[L : M]_\ell = 2$.

Proof. Set $K_1 := \mathbb{Q}(\sqrt{q})$, $K_2 := \mathbb{Q}(\sqrt{-\ell})$ and let χ be a character for which the fixed field of $\ker\chi$ is M.

We first check that $M/\mathbb{Q}$ has no isolated primes. The prime ℓ ramifies in K_2 and is inert in K_1, so $[M : \mathbb{Q}]_\ell = 4$.

Case $\ell \equiv 3 \pmod 4$: By reciprocity, ℓ is a square modulo q, and hence $-\ell$ is a nonsquare modulo q. The prime q thus ramifies in K_1 and is inert in K_2, so $[M : \mathbb{Q}]_q = 4$.

Case $\ell \equiv 1 \pmod 4$: Since $q \not\equiv -\ell \pmod 8$, we have $\mathbb{Q}_2(\sqrt{q}) \neq \mathbb{Q}_2(\sqrt{-\ell})$, so $[M : \mathbb{Q}]_2 = 4$. In any case, $M/\mathbb{Q}$ has no isolated prime.

Now assume L is a 2-cover of $M/\mathbb{Q}$ with full local degree at ℓ. Since K_1 is real and M is not, M/K_1 does not have a cyclic 2-cover. Since $q \equiv 3 \pmod 4$, -1 is not a square in $\mathbb{Q}_q$. This implies that $\mathbb{Q}_q$ does not have any totally ramified degree-4 extension, so that any ramified quadratic extension of $\mathbb{Q}_q$ cannot have a cyclic 2-cover. Thus, globally, $K_1/\mathbb{Q}$ does not have a cyclic 2-cover. The inertia field of ℓ in $L/\mathbb{Q}$ contains K_1 and is cyclic over $\mathbb{Q}$, and thus is equal to K_1. This is a contradiction because L is then a cyclic 2-cover of M/K_1. $\square$

Remark. (i) Suppose $M/\mathbb{Q}$ is as in Example 4.1. Consider $\alpha \in \mathrm{Br}(\mathbb{Q})$ such that $\operatorname{ind}\alpha = 8$ and $\operatorname{ind}\alpha^{\mathbb{Q}(\chi)} = 2$. Since ℓ is not 2-isolated in $M/\mathbb{Q}$, we can find such an α with $\operatorname{ind}_\ell \alpha = 8$. Since $M/\mathbb{Q}$ does not have a 2-cover L with $[L : M]_\ell = 2$, no 2-cover of $M/\mathbb{Q}$ splits α. Hence, the underlying division algebra of $\alpha + \chi$ is a noncrossed product of index 8.

(ii) In Example 4.1 we can choose $(\ell, q) = (3, 11), (5, 7), (7, 3)$, etc. The example in [Hanke 2004] is the case $\ell = 7$ and $q = 3$.

We now turn to arbitrary global fields K and a prime $p \neq \operatorname{char} K$. Example 4.1 does not generalize immediately because its proof uses a real prime. The following argument uses a third finite prime instead of a real prime:

Proposition 4.2. *Let K be a global field and let $p \in \mathbb{P}$ with $p \neq \operatorname{char} K$. Assume $s := s_p(K) > 0$. Let $\mathfrak{p}$ be any prime of K with $p \nmid N(\mathfrak{p})$. There exists a bicyclic extension M/K with group $C_{p^s} \times C_{p^s}$ and without isolated primes such that no p-cover L of M/K has $[L : M]_\mathfrak{p} = p$.*

[7] Using the reciprocity law, it is also possible to choose a suitable ℓ for any prime $q \equiv 3 \pmod 4$.

Proof. By Chebotarev's density theorem, there are primes $\mathfrak{q}_1, \mathfrak{q}_2$ of K such that $N(\mathfrak{q}_i) \equiv 1 \pmod{p^s}$ but $N(\mathfrak{q}_i) \not\equiv 1 \pmod{p^{s+1}}$. By the Grunwald–Wang theorem, there are cyclic extensions K_i/K of degree $[K_i : K] = p^s$ such that in K_1, $\mathfrak{p}$ is inert, $\mathfrak{q}_1$ is totally ramified, and $\mathfrak{q}_2$ splits completely; and in K_2, $\mathfrak{q}_1$ is inert and $\mathfrak{p}$ and $\mathfrak{q}_2$ are totally ramified. Since $\mathfrak{p}$ and $\mathfrak{q}_1$ both have full local degree in M, M/K has no isolated primes.

Since $N(\mathfrak{q}_1) \not\equiv 1 \pmod{p^{s+1}}$ and $\mathfrak{q}_1$ is totally ramified in K_1/K, K_1/K does not have a cyclic p-cover. Similarly, considering $\mathfrak{q}_2$, M/K_1 does not have a cyclic p-cover.

Assume on the contrary there is a p-cover L of M/K with $[L : M]_{\mathfrak{p}} = p$. Since the inertia field of $\mathfrak{p}$ contains K_1 and is cyclic over K, it equals K_1. This shows that L is a cyclic p-cover of M/K_1, a contradiction. □

Example 4.3. Let $p \in \mathbb{P}$ and $K = \mathbb{F}_q(t)$ for $q \equiv 1 \pmod{p}$, so that $s := s_p(K) > 0$. Assume $a \notin (K^\times)^p$. Let $M = K\left(\sqrt[p^s]{t},\ \sqrt[p^s]{(t-1)(t-a)}\right)$. By the following claim, the proof of Proposition 4.2 applies to M and the primes $\mathfrak{p} = (t-a)$, $\mathfrak{q}_1 = (t)$, $\mathfrak{q}_2 = (t-1)$. Therefore, $b_p(\chi) = 0$ for any χ for which M is the fixed field of $\ker \chi$.

For $q \equiv 3 \pmod 4$ and $p = 2$, Example 4.3 is identical to [Coyette 2012, Example 2.8].

Claim. Let $K_1 = K(\sqrt[p^s]{t})$, $K_2 = K\left(\sqrt[p^s]{(t-1)(t-a)}\right)$. Then $(t-a)$ is inert in K_1 and totally ramified in K_2, (t) is totally ramified in K_1 and inert in K_2, and $(t-1)$ splits completely in K_1 and is totally ramified in K_2.

Proof. In K_1 we have: $t \equiv a \pmod{t-a}$ is not a p-th power and $t \equiv 1 \pmod{t-1}$ is a p^s-th power, and hence $(t-a)$ is inert, $(t-1)$ splits completely, and (t) is totally ramified.

In K_2 we have: $(t-1)(t-a) \equiv a \pmod{t}$ is not a p-th power, and hence (t) is inert and $(t-1)$, $(t-a)$ are totally ramified. □

Acknowledgments

The authors would like to thank Eli Aljadeff for the financial support of Hanke's visit to the Technion in 2010 and Julia Hartmann for supporting the visit of Neftin to RWTH Aachen in 2009. We also thank the referee for very helpful remarks which improved this paper. This material is based upon work supported by the National Science Foundation under Award No. DMS-1303990.

References

[Aljadeff et al. 2007] E. Aljadeff, J. Sonn, and A. R. Wadsworth, "Projective Schur groups of Henselian fields", *J. Pure Appl. Algebra* **208**:3 (2007), 833–851. MR 2007k:11196 Zbl 1113.11066

[Amitsur 1972] S. A. Amitsur, "On central division algebras", *Israel J. Math.* **12** (1972), 408–420. MR 47 #6763 Zbl 0248.16006

[Brussel 1995] E. Brussel, "Noncrossed products and nonabelian crossed products over $\mathbb{Q}(t)$ and $\mathbb{Q}((t))$", *Amer. J. Math.* **117**:2 (1995), 377–393. MR 96a:16014 Zbl 0822.16013

[Brussel 2001] E. S. Brussel, "Noncrossed products over $k_{\mathfrak{p}}(t)$", *Trans. Amer. Math. Soc.* **353**:5 (2001), 2115–2129. MR 2001j:16022 Zbl 0971.16009

[Brussel 2002] E. S. Brussel, "Non-crossed products over function fields", *Manuscripta Math.* **107**:3 (2002), 343–353. MR 2003f:16027 Zbl 1009.16019

[Chen 2010] F. Chen, "Indecomposable and noncrossed product division algebras over curves over complete discrete valuation rings", 2010. arXiv 1004.3935

[Coyette 2012] C. Coyette, "Mal'cev–Neumann rings and noncrossed product division algebras", *J. Algebra Appl.* **11**:3 (2012), 1250052, 12. MR 2928120 Zbl 1263.16022

[Hanke 2004] T. Hanke, "An explicit example of a noncrossed product division algebra", *Math. Nachr.* **271** (2004), 51–68. MR 2005e:16044 Zbl 1063.16025

[Hanke 2011] T. Hanke, "Galois subfields of inertially split division algebras", *J. Algebra* **346** (2011), 147–151. MR 2842074 Zbl 1248.16017

[Hanke and Sonn 2011] T. Hanke and J. Sonn, "The location of noncrossed products in Brauer groups of Laurent series fields over global fields", *Math. Ann.* **350**:2 (2011), 313–337. MR 2012i:16037 Zbl 1242.16021

[Jacob and Wadsworth 1990] B. Jacob and A. Wadsworth, "Division algebras over Henselian fields", *J. Algebra* **128**:1 (1990), 126–179. MR 91d:12006 Zbl 0692.16011

[Koch 1970] H. Koch, *Galoissche Theorie der p-Erweiterungen*, Springer, 1970. MR 45 #233 Zbl 0216.04704

[Pierce 1982] R. S. Pierce, *Associative algebras*, Graduate Texts in Mathematics **88**, Springer, New York, 1982. MR 84c:16001 Zbl 0497.16001

[Scharlau 1969] W. Scharlau, "Über die Brauer-Gruppe eines Hensel-Körpers", *Abh. Math. Sem. Univ. Hamburg* **33** (1969), 243–249. MR 41 #185 Zbl 0179.07804

[Tignol and Wadsworth $\geq$ 2014] J.-P. Tignol and A. Wadsworth, "Value functions on simple algebras, and associated graded algebras", In preparation.

[Witt 1936] E. Witt, "Schiefkörper über diskret bewerteten Körpern", *J. Reine Angew. Math.* **176** (1936), 153–156. Zbl 0016.05102

Communicated by Raman Parimala
Received 2012-11-01 Revised 2013-10-28 Accepted 2013-12-05

hanke@math.rwth-aachen.de *Lehrstuhl D für Mathematik, Rheinisch-Wesfälische Technische Hochschule Aachen, Templergraben 64, D-52062 Aachen, Germany*

neftin@umich.edu *Department of Mathematics, University of Michigan, 530 Church St., Ann Arbor, MI 48109-1043, United States*

sonn@math.technion.ac.il *Department of Mathematics, Technion–Israel Institute of Technology, Technion City, 32000 Haifa, Israel*

ALGEBRA AND NUMBER THEORY 8:4 (2014)
dx.doi.org/10.2140/ant.2014.8.857

Yangians and quantizations of slices in the affine Grassmannian

Joel Kamnitzer, Ben Webster, Alex Weekes and Oded Yacobi

We study quantizations of transverse slices to Schubert varieties in the affine Grassmannian. The quantization is constructed using quantum groups called shifted Yangians — these are subalgebras of the Yangian we introduce which generalize the Brundan–Kleshchev shifted Yangian to arbitrary type. Building on ideas of Gerasimov, Kharchev, Lebedev and Oblezin, we prove that a quotient of the shifted Yangian quantizes a scheme supported on the transverse slices, and we formulate a conjectural description of the defining ideal of these slices which implies that the scheme is reduced. This conjecture also implies the conjectural quantization of the Zastava spaces for PGL_n of Finkelberg and Rybnikov.

1. Introduction

We initiate a program which relates the geometry of affine Grassmannians with the representation theory of shifted Yangians. More precisely, we study slices in affine Grassmannians which arise naturally in geometric representation theory; they correspond to weight spaces of irreducible representations under the geometric Satake correspondence. Our main result is that certain subquotients of Yangians quantize these slices.

There is a general program to study symplectic resolutions by means of the representation theory of their quantizations, generalizing the interplay between semisimple Lie algebras and nilpotent cones. We believe that the representation theory of shifted Yangians and its relationship to the geometry of slices in the affine Grassmannian will prove to be a very fruitful area of inquiry.

1A. ***Slices in the affine Grassmannian.*** Let G be a complex semisimple group and consider its *thick affine Grassmannian* $\mathsf{Gr} = G((t^{-1}))/G[t]$. Attached to each pair of dominant coweights $\lambda \geq \mu$, we have Schubert varieties $\mathsf{Gr}^\lambda, \mathsf{Gr}^\mu \subset \mathsf{Gr}$, with $\mathsf{Gr}^\mu \subset \overline{\mathsf{Gr}^\lambda}$. The neighborhood in $\overline{\mathsf{Gr}^\lambda}$ of a point in Gr^μ is encapsulated in a transversal slice to the latter variety in the former, which we denote by $\overline{\mathsf{Gr}^\lambda_\mu}$. This

Webster was supported by NSF grant DMS-1151473 and by NSA grant H98230-10-1-0199.
MSC2010: primary 20G42; secondary 53D55, 14M15, 14D24.
Keywords: quantization, affine Grassmannian, quantum groups, Yangian.

slice is an important object of study in geometric representation theory because under the geometric Satake correspondence it is related to the μ weight space in the irreducible representation of $G^\vee$ of highest weight λ.

The Manin triple $\big(\mathfrak{g}[t], t^{-1}\mathfrak{g}[\![t^{-1}]\!], \mathfrak{g}((t^{-1}))\big)$ provides Gr with the structure of a Poisson variety. The slice $\overline{\mathsf{Gr}^\lambda_\mu}$ is an affine Poisson subvariety, and thus its coordinate ring is naturally a Poisson algebra. The purpose of this paper is to explicitly describe quantizations of this Poisson algebra.

1B. ***Quotients of shifted Yangians.*** The slice $\overline{\mathsf{Gr}^\lambda_\mu}$ is defined as the intersection $\overline{\mathsf{Gr}^\lambda} \cap \mathsf{Gr}_\mu$, where Gr_μ is an orbit of the group $G_1[\![t^{-1}]\!]$, the first congruence subgroup of $G[\![t^{-1}]\!]$. Thus on the level of functions $\mathbb{O}(\overline{\mathsf{Gr}^\lambda_\mu})$ is a quotient of $\mathbb{O}(\mathsf{Gr}_\mu)$, and $\mathbb{O}(\mathsf{Gr}_\mu)$ is a subalgebra of $\mathbb{O}(G_1[\![t^{-1}]\!])$. In order to quantize $\overline{\mathsf{Gr}^\lambda_\mu}$ we follow a three-step procedure which mirrors this construction.

We first construct a version Y of the Yangian, which is a subalgebra of the Drinfeld Yangian. Next, we define natural subalgebras $Y_\mu \subset Y$, called *shifted Yangians*, that quantize Gr_μ. This generalizes the shifted Yangian for $\mathfrak{gl}_n$ introduced by Brundan and Kleshchev [2006]. Finally, we define a quotient Y^λ_μ of Y_μ using some remarkable representations of Y as difference operators, constructed by Gerasimov, Kharchev, Lebedev and Oblezin [Gerasimov et al. 2004].

Theorem A. *The algebras defined above are all quantizations of the analogous geometric objects. That is*:

(1) *The Yangian Y quantizes $G_1[\![t^{-1}]\!]$.*

(2) *The shifted Yangian Y_μ quantizes Gr_μ.*

(3) *The quotient Y^λ_μ quantizes a (possibly nonreduced) scheme supported on $\overline{\mathsf{Gr}^\lambda_\mu}$.*

Item (1) is proven using a duality between quantum groups due to Drinfeld and Gavarini, (2) follows simply from (1), and (3) follows using the Gerasimov–Kharchev–Lebedev–Oblezin (GKLO) representation. In fact, we produce a family $Y^\lambda_\mu(\boldsymbol{c})$ of quantizations which we conjecture to map surjectively to the universal family in the sense of Bezrukavnikov and Kaledin [2004].

Unfortunately, we are not able to prove that the scheme quantized by Y^λ_μ is reduced. However, we do provide a conjectural description of the generators of the ideal of $\overline{\mathsf{Gr}^\lambda_\mu}$ inside Gr_μ and prove that this conjecture implies that Y^λ_μ quantizes the reduced scheme structure on $\overline{\mathsf{Gr}^\lambda_\mu}$. Moreover, we prove that this conjecture gives a simple description for the ideal defining Y^λ_μ.

1C. ***Motivation and relation to other work.*** Brundan and Kleshchev [2006] construct an isomorphism between quotients of shifted Yangians of $\mathfrak{gl}_n$ and W-algebras of $\mathfrak{gl}_m$. On the one hand, it is known that W-algebras are quantizations of Slodowy slices. On the other hand, by the work of Mirković and Vybornov [2007], we have an isomorphism between Slodowy slices for $\mathfrak{sl}_m$ and slices in the affine Grassmannian for GL_n. Thus via these results, we see that quotients of shifted Yangians for $\mathfrak{gl}_n$ quantize slices in the affine Grassmannian for GL_n. This motivated us to look for a direct construction of quantizations of affine Grassmannian slices (for any semisimple G) using quotients of shifted Yangians. (The idea that the Brundan–Kleshchev isomorphism should be thought of as a quantization of the Mirković–Vybornov isomorphism was independently observed by Losev [2012, Remark 5.3.4].)

If we take a limit of $\overline{\mathrm{Gr}^{\lambda}_{\mu}}$ as $\lambda \to \infty$ and $\lambda - \mu$ is fixed, then the slice $\overline{\mathrm{Gr}^{\lambda}_{\mu}}$ becomes the Zastava space $Z_{\lambda-\mu}$. Finkelberg and Rybnikov [2010] have given conjectural quantizations of Zastava spaces (for PGL_n) using quotients of Borel Yangians, which are a limit of shifted Yangians. We prove that our conjecture about the ideal of $\overline{\mathrm{Gr}^{\lambda}_{\mu}}$ implies the conjecture of Finkelberg and Rybnikov.

Earlier work on shifted Yangians by Brundan and Kleshchev [2008] suggests that one natural direction for future work is the study of a version of category $\mathcal{O}$ over the algebra Y^{λ}_{μ}. Because of the geometric Satake correspondence, we think of category $\mathcal{O}$ for Y^{λ}_{μ} as a categorification of a weight space in a representation of the Langlands dual group $G^{\vee}$. Thus we expect that these categories (with λ fixed) carry categorical $\mathfrak{g}^{\vee}$-actions. Moreover, conjectures of Braden, Licata, Proudfoot and Webster [Braden et al. $\geq$ 2014] suggest that category $\mathcal{O}$ for Y^{λ}_{μ} should be Koszul dual to similar categories constructed from quiver varieties (in type A, we expect that this reduces to parabolic-singular duality of Beilinson, Ginzburg and Soergel [Beilinson et al. 1996]).

2. Symplectic structure on slices in the affine Grassmannian

2A. ***Notation.*** For any group H, we will write $H((t^{-1})) = H(\mathbb{C}((t^{-1})))$ for its loop group and write $H[t] = H(\mathbb{C}[t])$ and $H[\![t^{-1}]\!] = H(\mathbb{C}[\![t^{-1}]\!])$ for its usual subgroups. Let $H_1[\![t^{-1}]\!]$ denote the first congruence subgroup of $H[\![t^{-1}]\!]$, i.e., the kernel of the evaluation at $t^{-1} = 0$, $H[\![t^{-1}]\!] \to H$.

Throughout, G will denote a fixed complex semisimple group with opposite Borel subgroups B, B_-, unipotent subgroups N, N_-, maximal torus T, Weyl group W, set of roots Δ, and simple roots $\{\alpha_i\}_{i\in I}$. We will be concerned with both the coweights and the weights of G, which we will be careful to distinguish throughout the paper. Note that the coweights of G are the weights of its Langlands dual group $G^{\vee}$, which we will occasionally consider in this paper.

We write $\{\omega_i\}_{i\in I}$ for the fundamental weights of the simply connected form of G.

Following Drinfeld, we use generators e_i, f_i, h_i for $\mathfrak{g}$, where

$$[h_i, e_j] = (\alpha_i, \alpha_j)e_j, \quad [h_i, f_j] = -(\alpha_i, \alpha_j) f_j, \quad [e_i, f_j] = \delta_{ij} h_i,$$

along with the usual Serre relations. Let $(a_{ij})_{1\le i,j\le n}$ be the Cartan matrix of $\mathfrak{g}$, and let d_i be the unique coprime positive integers such that $b_{ij} = d_i a_{ij}$ is a symmetric matrix. Then the associated invariant form on $\mathfrak{g}$ is defined by $(e_i, f_j) = \delta_{ij}$ and $(\alpha_i, \alpha_j) = (h_i, h_j) = d_i a_{ij}$, and in particular, h_i is the image of α_i under the identification of $\mathfrak{h}$ and $\mathfrak{h}^*$.

This is as opposed to the standard Chevalley generators e_i', f_i', h_i', which we will identify as

$$e_i = -d_i^{1/2} e_i', \quad f_i = -d_i^{1/2} f_i', \quad h_i = d_i h_i'.$$

In this way we have fundamental weights $\omega_i(h_j') = \delta_{ij}$ and a lift of the Weyl group defined via $\overline{s_i} = \exp(f_i')\exp(-e_i')\exp(f_i')$.

If μ is a weight or coweight, we write $\mu^* = -w_0\mu$. Likewise, we write i^* if $\alpha_{i^*} = -w_0\alpha_i$.

Let V be a representation of G, and let $v \in V$, $\beta \in V^*$. The matrix entry $\Delta_{\beta,v}$ is a function on G given by $\Delta_{\beta,v}(g) = \langle \beta, gv\rangle$. If $w_1, w_2 \in W$ and τ is a dominant weight, we define

$$\Delta_{w_1\tau, w_2\tau}(g) = \langle \overline{w_1} v_{-\tau}, \overline{w_2} v_\tau\rangle$$

using the lift described above, where v_τ is the highest-weight vector for the irreducible representation $V(\tau)$ and $v_{-\tau}$ is the dual lowest-weight vector in $V(\tau^*)$.

Using this matrix entry (also known as a generalized minor), we define the function $\Delta_{\beta,v}^{(s)}$ on $G((t^{-1}))$, for $s \in \mathbb{Z}$, whose value at g is the coefficient of t^{-s} in the polynomial $\Delta_{\beta,v}(g)$. So we have the formula

$$\Delta_{\beta,v}(g) = \sum_{s=-\infty}^{\infty} \Delta_{\beta,v}^{(s)}(g) t^{-s}.$$

2B. ***Slices in the affine Grassmannian.*** Let G be a semisimple complex group. In this paper, we will work with the *thick affine Grassmannian* $\mathsf{Gr} = G((t^{-1}))/G[t]$. We have an embedding of the usual thin affine Grassmannian into the thick affine Grassmannian

$$G((t))/G[\![t]\!] \cong G[t, t^{-1}]/G[t] \hookrightarrow G((t^{-1}))/G[t].$$

We work with the thick affine Grassmannian since it is forced upon us by the noncommutative algebras we consider. One manifestation of this is that the thick Grassmannian is an honest scheme, while the thin Grassmannian is only an ind-scheme. However, at a first reading, this difference will be of little importance, and the reader can pretend that we are working with the usual thin affine Grassmannian.

Any coweight λ can be thought of as a $\mathbb{C}[t, t^{-1}]$-point of G, which we can think of as a $\mathbb{C}((t^{-1}))$-point as well. To avoid confusion, we use t^λ to denote this point in $G((t^{-1}))$. We also use t^λ for the image of t^λ in Gr.

Let λ and μ denote dominant coweights. Define

$$\mathsf{Gr}^\lambda = G[t]t^\lambda, \quad \mathsf{Gr}_\mu = G_1[[t^{-1}]]t^{w_0\mu}.$$

Recall that the thin affine Grassmannian is precisely $\bigcup_\lambda \mathsf{Gr}^\lambda$.

Our main object of interest will be

$$\mathsf{Gr}^{\overline{\lambda}}_\mu := \overline{\mathsf{Gr}^\lambda} \cap \mathsf{Gr}_\mu.$$

This variety is a transverse slice to Gr^μ inside of $\overline{\mathsf{Gr}^\lambda}$ since Gr_μ intersects every Gr^ν transversely and the intersection $\mathsf{Gr}^{\overline{\mu}}_\mu$ is just the point $t^{w_0\mu}$. In particular, this variety is nonempty if and only if $\mu \le \lambda$, that is, if $\mathsf{Gr}^\mu \subset \overline{\mathsf{Gr}^\lambda}$. These varieties arise naturally under the geometric Satake correspondence of Lusztig [1983], Ginzburg [1995], and Mirković and Vilonen [2007]: the intersection homology of $\mathsf{Gr}^{\overline{\lambda}}_\mu$ is identified with the μ-weight space of the irreducible $G^\vee$-representation of highest weight λ.

Note that $\mathbb{C}^\times$ acts on Gr by loop rotation. This action preserves the $G[t]$ and $G_1[[t^{-1}]]$ orbits, and so $\mathbb{C}^\times$ acts on $\mathsf{Gr}^{\overline{\lambda}}_\mu$. The following result is standard (it is a special case of general results about flag varieties and their big cells).

Proposition 2.1. (1) *$\mathsf{Gr}^{\overline{\lambda}}_\mu$ is an affine variety of dimension $2\langle\rho, \lambda-\mu\rangle$.*

(2) *The action of $\mathbb{C}^\times$ on $\mathsf{Gr}^{\overline{\lambda}}_\mu$ contracts $\mathsf{Gr}^{\overline{\lambda}}_\mu$ to the unique fixed point $t^{w_0\mu}$.*

Example 2.2. If $\lambda = \mu + \alpha_i^\vee$, then $\mathsf{Gr}^{\overline{\lambda}}_\mu$ is isomorphic to the Kleinian singularity $\mathbb{C}^2/(\mathbb{Z}/n+2)$, where $n = \langle\mu, \alpha_i\rangle$. To see this, first we identify

$$\mathbb{C}^2/(\mathbb{Z}/n+2) = \{(u, v, w) \mid uv + w^{n+2} = 0\},$$

and then we define the isomorphism

$$\begin{aligned} &\mathbb{C}^2/(\mathbb{Z}/n+2) \to \mathsf{Gr}^{\overline{\lambda}}_\mu, \\ &(u, v, w) \mapsto \phi_i\left(\begin{bmatrix} 1-wt^{-1} & vt^{-(n+1)} \\ ut^{-1} & 1+wt^{-1}+\cdots+w^{n+1}t^{-(n+1)} \end{bmatrix}\right)t^{w_0\mu}, \end{aligned}$$

where $\phi_i : \mathrm{SL}_2 \to G$ denotes the SL_2 corresponding to α_i.

Let $G((t^{-1}))_\mu$ denote the stabilizer of $t^{w_0\mu}$ inside of $G((t^{-1}))$. The following easy result describes the stabilizer on the Lie algebra level.

Lemma 2.3. $\mathrm{Lie}\big(G((t^{-1}))_\mu\big) = \mathfrak{t}[t] \oplus \bigoplus_{\alpha\in\Delta} t^{\langle\alpha, w_0\mu\rangle}\mathfrak{g}_\alpha[t]$.

Proof. The result follows immediately after observing that for $g \in G((t^{-1}))$, we have $g \in G((t^{-1}))_\mu$ if and only if $t^{-w_0\mu}gt^{w_0\mu} \in G[t]$. □

In what follows, we will need the following set-theoretic description of $\overline{\mathsf{Gr}^\lambda}$ due to Finkelberg and Mirković [1999, (10.2)]. As we shall see, it is much trickier to find a description of this variety with its natural reduced scheme structure.

Proposition 2.4. *Let $g \in G((t^{-1}))$. We have $[g] \in \overline{\mathsf{Gr}^\lambda}$ if and only if $\Delta^{(s)}_{\beta,v}(g) = 0$ for all dominant weights τ, for all $v \in V(\tau)$, $\beta \in V(\tau)^*$, and for all $s < \langle \lambda, w_0\tau\rangle$.*

Proof. Fix τ and let k be the minimal s such that there exist $\beta \in V(\tau)^*$, $v \in V(\tau)$ with $\Delta^{(s)}_{\beta,v}(g) \neq 0$ (if such a minimum exists). It is easy to see that k only depends on the $G[t]$ double coset containing g. Thus if $[g] \in \mathsf{Gr}^\lambda$, we have that $k = \langle \lambda, w_0\tau\rangle$. The result follows. $\square$

The proof makes it clear that the Proposition holds even if τ only ranges over a set of dominant weights which spans (over $\mathbb{Q}$) the weight lattice.

2C. ***Symplectic structure on the affine Grassmannian.*** There is a nondegenerate pairing on $\mathfrak{g}((t^{-1}))$ coming from residue and the invariant form on $\mathfrak{g}$. Hence the Lie algebras $\mathfrak{g}[t]$, $t^{-1}\mathfrak{g}[[t^{-1}]]$, and $\mathfrak{g}((t^{-1}))$ form a Manin triple (see [Drinfeld 1987, Example 3.3]). This induces a Poisson–Lie structure on $G((t^{-1}))$ with $G[t]$ and $G_1[[t^{-1}]]$ as Poisson subgroups. In particular, it coinduces a Poisson structure on Gr, by standard calculations which date back to work of Drinfeld [1993].

Let us state a couple of results concerning the interaction between this symplectic structure and the geometry considered in the previous section. These results were originally obtained by Mirković (personal communication).

Theorem 2.5. *Subvarieties $\mathsf{Gr}^\lambda_\mu = \mathsf{Gr}^\lambda \cap \mathsf{Gr}_\mu$ are symplectic leaves of Gr.*

Proof. First we note that Gr^λ_μ are connected by [Richardson 1992, 1.4], since $\mathfrak{g}((t^{-1})) = \mathfrak{g}[t] \oplus t^{-1}\mathfrak{g}[[t^{-1}]]$. The argument is stated there for finite-dimensional groups, but carries through to the loop situation without issues. Then the result follows from [Lu and Yakimov 2008, Corollary 2.9]. $\square$

These are not all symplectic leaves of Gr, since not every $G_1[[t^{-1}]]$-orbit contains a point $t^{w_0\mu}$ and not every $G[t]$-orbit contains a point t^λ. A general symplectic leaf which lies in the thin affine Grassmannian is of the form $\mathsf{Gr}^\lambda \cap G_1[[t^{-1}]]gt^{w_0\mu}$, where $g \in G$.

Let $S^\mu = N((t^{-1}))t^{w_0\mu}$. An *MV cycle* is a component of $\overline{\mathsf{Gr}^\lambda} \cap S^\mu$. By Mirković–Vilonen, these MV cycles give a basis for weight spaces of irreducible representations of the Langlands dual group. As we now see, the MV cycles are Lagrangians in $\mathsf{Gr}^{\overline{\lambda}}_\mu$.

Proposition 2.6. *$\overline{\mathsf{Gr}^\lambda} \cap S^\mu$ is a Lagrangian subvariety of $\mathsf{Gr}^{\overline{\lambda}}_\mu$.*

Proof. First we prove that $\overline{\mathsf{Gr}^\lambda} \cap S^\mu \subset \mathsf{Gr}^{\overline{\lambda}}_\mu$. Since N is unipotent, we have that $N((t^{-1})) = N_1[[t^{-1}]]N[t]$. Now by Lemma 2.3, we have that $N[t]t^{w_0\mu} = t^{w_0\mu}$. Hence $N((t^{-1}))t^{w_0\mu} = N_1[[t^{-1}]]t^{w_0\mu}$ and thus $S^\mu \subset \mathsf{Gr}_\mu$.

From [Mirković and Vilonen 2007, Theorem 3.2], $\dim \overline{\mathsf{Gr}^\lambda} \cap S^\mu = \langle \rho, \lambda - \mu\rangle$, and thus the intersection $\overline{\mathsf{Gr}^\lambda} \cap S^\mu$ is half-dimensional in $\mathsf{Gr}^{\overline{\lambda}}_\mu$. Hence it is Lagrangian if and only if it is coisotropic. The variety $\mathsf{Gr}^{\overline{\lambda}}_\mu$ is affine, and so it suffices to check that the Poisson bracket of any two functions that vanish on $\overline{\mathsf{Gr}^\lambda} \cap S^\mu$ vanishes there as well. The functions vanishing on $S^\mu \cap \overline{\mathsf{Gr}^\lambda}$ are generated by all functions of negative weight under the action of the coweight $\rho^\vee : \mathbb{C}^\times \to G$. Since that action preserves the Poisson structure, the Poisson bracket of two negative weight functions is again of negative weight; this completes the proof. $\square$

It is natural to ask whether $\mathsf{Gr}^{\overline{\lambda}}_\mu$ has a symplectic resolution. Let us temporarily assume that G is of adjoint type and let us fix a sequence $\vec{\lambda} = (\lambda_1, \dots, \lambda_n)$ of fundamental coweights such that $\lambda = \lambda_1 + \cdots + \lambda_n$. (If we do not assume that G is of adjoint type, then we may not be able to write λ as a sum of fundamental coweights of G.) Then we have the open and closed convolutions

$$\mathsf{Gr}^{\vec{\lambda}} := \mathsf{Gr}^{\lambda_1} \tilde{\times} \cdots \tilde{\times} \mathsf{Gr}^{\lambda_n}, \quad \overline{\mathsf{Gr}^{\vec{\lambda}}} := \overline{\mathsf{Gr}^{\lambda_1}} \tilde{\times} \cdots \tilde{\times} \overline{\mathsf{Gr}^{\lambda_n}}$$

along with the convolution morphisms $m : \mathsf{Gr}^{\vec{\lambda}} \to \overline{\mathsf{Gr}^\lambda}$ and $\bar{m} : \overline{\mathsf{Gr}^{\vec{\lambda}}} \to \overline{\mathsf{Gr}^\lambda}$. (Here the convolution $A \tilde{\times} B$ of two $G[t]$-invariant subsets A, B in Gr is defined by $p^{-1}(A) \times_{G[t]} B$, where $p : G((t^{-1})) \to \mathsf{Gr}$.)

Let

$$\mathsf{Gr}^{\vec{\lambda}}_\mu := m^{-1}(\mathsf{Gr}_\mu), \quad \mathsf{Gr}^{\overline{\vec{\lambda}}}_\mu := \bar{m}^{-1}(\mathsf{Gr}_\mu).$$

Recall that a normal variety X with a fixed symplectic structure Ω on its smooth locus is said to have *symplectic singularities* if, locally on X, there are resolutions of singularities $p : U \to X$, where $p^*\Omega$ is the restriction of a closed 2-form on U (which is not assumed to be nondegenerate on the exceptional locus).

A variety X is said to have *terminal singularities* if there is a resolution of singularities of X such that each irreducible exceptional fiber has positive discrepancy, that is, X is as close to being smoothly resolved as is crepantly possible. A *terminalization* $X \to Y$ is a map which is birational, proper, and crepant with X having terminal singularities. We say a variety X is $\mathbb{Q}$-*factorial* if every Weil divisor on X has an integer multiple which is Cartier.

Theorem 2.7. *The variety $\mathsf{Gr}^{\overline{\lambda}}_\mu$ has symplectic singularities, and $\mathsf{Gr}^{\overline{\vec{\lambda}}}_\mu$ is a $\mathbb{Q}$-factorial terminalization of $\mathsf{Gr}^{\overline{\lambda}}_\mu$.*

Proof. First, we claim that $\mathsf{Gr}^{\overline{\vec{\lambda}}}_\mu$ has singular locus in codimension at least 4. Since Gr_μ is transverse to every $G[t]$-orbit, the codimension of the singular locus cannot jump when we pass to $\mathsf{Gr}^{\overline{\vec{\lambda}}}_\mu$, so we need only establish the same result for $\mathsf{Gr}^{\overline{\vec{\lambda}}}$, for which it suffices to consider the case of a fundamental coweight. If ω_i is a fundamental coweight and ν is a dominant coweight such that $\mathsf{Gr}^\nu \subset \mathsf{Gr}^{\overline{\omega_i}}$, then we have that $\rho^\vee(\omega_i - \nu) \geq 2$, since $\omega_i - \alpha_j$ is never dominant. Thus, the singular locus Gr^ν has codimension at least 4.

As Beauville [2000, (1.2)] notes, since $\mathsf{Gr}^{\overline{\vec{\lambda}}}_\mu$ is regular in codimension 3 and normal, the existence of a symplectic form on its smooth locus implies that it has symplectic singularities. Since we have a Poisson map $\mathrm{Gr}^{\overline{\vec{\lambda}}}_{\mu} \to \mathrm{Gr}^{\overline{\lambda}}_{\mu}$, this variety also has symplectic singularities. By a result of Namikawa [2001, Corollary 1], this regularity in codimension 3 also implies that $\mathrm{Gr}^{\overline{\vec{\lambda}}}_{\mu}$ is terminal.

Because each local singularity in $\mathrm{Gr}^{\overline{\vec{\lambda}}}_{\mu}$ is a local singularity in $\mathrm{Gr}^{\overline{\vec{\lambda}}}$, and these are the product of local singularities in $\mathrm{Gr}^{\overline{\omega_i}}$, we need only prove $\mathbb{Q}$-factoriality in this case. The group of Weil divisors of $\mathrm{Gr}^{\overline{\omega_i}}$ is the same as that of Gr^{ω_i}, which is an affine bundle over G/P_i, where P_i is the maximal parabolic containing all negative simple root spaces but $\mathfrak{g}_{-\alpha_i}$. Thus, the Weil divisor group of G/P_i is isomorphic to $\mathbb{Z}$.

Since $\mathrm{Gr}^{\overline{\omega_i}}$ is projective, *some* Weil divisor on $\mathrm{Gr}^{\overline{\omega_i}}$ is Cartier. Thus, the group generated by any nontrivial Weil divisor must intersect the image of the Cartier divisors, and so $\mathrm{Gr}^{\overline{\omega_i}}$ is $\mathbb{Q}$-factorial.[1]

By general properties of Schubert varieties and Bott–Samuelson resolutions, the map $\mathrm{Gr}^{\overline{\vec{\lambda}}}_{\mu} \to \mathrm{Gr}^{\overline{\lambda}}_{\mu}$ is proper and birational. The preimage of Gr^{μ} for $\mu \neq \lambda, \lambda - \alpha_i$ has codimension at least 4, so any exceptional divisor must be the closure of a component of the preimage of $\mathrm{Gr}^{\lambda-\alpha_i}$. The coefficients of these divisors in the discrepancy can thus be computed locally in a neighborhood of $x \in \mathrm{Gr}^{\lambda-\alpha_i}$, but the germ of the map is equivalent to the minimal resolution of a Kleinian singularity by Example 2.2. The Kleinian singularities are known to be crepant. $\square$

An obvious question is when $\mathrm{Gr}^{\overline{\lambda}}_{\mu}$ has a symplectic resolution. First, we make the following conjecture.

Conjecture 2.8. *Any symplectic resolution of* $\mathrm{Gr}^{\overline{\lambda}}_{\mu}$ *is of the form* $\mathrm{Gr}^{\overline{\vec{\lambda}}}_{\mu}$.

We can easily see when $\mathrm{Gr}^{\overline{\vec{\lambda}}}_{\mu}$ is actually a resolution.

Theorem 2.9. *The following are equivalent.*

(1) $\mathrm{Gr}^{\overline{\lambda}}_{\mu}$ *possesses a symplectic resolution of singularities.*

(2) $\mathrm{Gr}^{\overline{\vec{\lambda}}}_{\mu}$ *is smooth and thus is a symplectic resolution of singularities of* $\mathrm{Gr}^{\overline{\lambda}}_{\mu}$.

(3) $\mathrm{Gr}^{\vec{\lambda}}_{\mu} = \mathrm{Gr}^{\overline{\vec{\lambda}}}_{\mu}$.

(4) *There do not exist coweights* $\nu_1, \ldots, \nu_n$ *such that* $\nu_1 + \cdots + \nu_n = \mu$; *for all* k, ν_k *is a weight of* $V(\lambda_k)$; *and for some* k, ν_k *is a not an extremal weight of* $V(\lambda_k)$ (*here we regard the* ν_k *as weights of* $G^\vee$).

Proof. (1) $\Longrightarrow$ (2): If $\mathrm{Gr}^{\overline{\lambda}}_{\mu}$ has a symplectic resolution, then by [Namikawa 2011, 5.6], any $\mathbb{Q}$-factorial terminalization of $\mathrm{Gr}^{\overline{\lambda}}_{\mu}$, in particular $\mathrm{Gr}^{\overline{\vec{\lambda}}}_{\mu}$, is smooth.

[1] We thank Alexander Braverman for suggesting this portion of the argument to us.

(2) $\implies$ (1): In this case, $\mathrm{Gr}^{\bar{\vec{\lambda}}}_\mu$ is an example of a symplectic resolution of singularities.

(2) $\Rightarrow$ (3): By [Evens and Mirković 1999, Theorem 0.1(b)], the smooth locus of $\overline{\mathrm{Gr}^\lambda}$ is precisely Gr^λ. Thus the smooth locus of $\mathrm{Gr}^{\bar{\vec{\lambda}}}$ is precisely $\mathrm{Gr}^{\vec{\lambda}}$.

Next we assume that there is a point x in $\mathrm{Gr}^{\bar{\vec{\lambda}}}_\mu$ not in $\mathrm{Gr}^{\vec{\lambda}}_\mu$; we know that $\mathrm{Gr}^{\bar{\vec{\lambda}}}$ is not smooth at x. By the transversality of the $G_1[\![t^{-1}]\!]$ and $G[t]$ orbits, the completion of $\mathrm{Gr}^{\bar{\vec{\lambda}}}$ at x coincides with the completion of $\mathrm{Gr}^{\bar{\vec{\lambda}}}_\mu$ at x times something smooth. Therefore $\mathrm{Gr}^{\bar{\vec{\lambda}}}_\mu$ cannot be smooth at x either.

(3) $\implies$ (2): Clear.

(3) $\implies$ (4): If there exist $\nu_1, \dots, \nu_n$ as in (3), then $(t^{\nu_1}, t^{\nu_1+\nu_2}, \dots, t^\mu) \in \mathrm{Gr}^{\bar{\vec{\lambda}}}_\mu \smallsetminus \mathrm{Gr}^{\vec{\lambda}}_\mu$.

(4) $\implies$ (3): Suppose that there exists

$$(L_1, \dots, L_n) \in \mathrm{Gr}^{\bar{\vec{\lambda}}}_\mu \smallsetminus \mathrm{Gr}^{\vec{\lambda}}_\mu.$$

Recall that we have a $\mathbb{C}^\times \times T$ action on Gr where the first factor acts by loop rotation. Consider a map $\mathbb{C}^\times \to \mathbb{C}^\times \times T$ which is the identity into the first factor and a generic dominant coweight into the second factor. We get a resulting $\mathbb{C}^\times$ action on Gr whose attracting sets are the I_- orbits, where I_- is the preimage of B under $G[\![t^{-1}]\!] \to G$.

Let

$$(t^{\mu_1}, \dots, t^{\mu_n}) = \lim_{s\to 0} s \cdot (L_1, \dots, L_n).$$

From the definition of $\mathrm{Gr}^{\bar{\vec{\lambda}}}_\mu$, we see that $\mu_n = \mu$. Also, for each k, we see that $d(t^{\mu_{k-1}}, t^{\mu_k}) \le \lambda_k$ (where d denotes the dominant coweight valued distance function on Gr), and so $\nu_k := \mu_k - \mu_{k-1}$ is a weight of $V(\lambda_k)$. Thus we obtain $\nu_1, \dots, \nu_n$ with $\nu_1 + \dots + \nu_n = \mu$. Moreover, since $(L_1, \dots, L_n) \notin \mathrm{Gr}^{\vec{\lambda}}_\mu$, we have $d(L_{k-1}, L_k) < \lambda_k$ for some k, and so ν_k is a nonextremal weight of $V(\lambda_k)$. □

If λ is a sum of minuscule coweights, then the above conditions hold. For any simple G not of type A, there are nonminiscule fundamental coweights λ; for such λ, we can choose μ such that the above conditions do not hold. So there exist $\mathrm{Gr}^{\overline{\lambda}}_\mu$ which do not admit symplectic resolutions.

2D. ***Beilinson–Drinfeld Grassmannian.*** Using the Beilinson–Drinfeld Grassmannian, we can define a family of Poisson varieties over $\mathbb{A}^n$ whose special fiber is $\mathrm{Gr}^{\overline{\lambda}}_\mu$. In this work, this family will only be used as motivation for a similar family of quantizations of $\mathrm{Gr}^{\overline{\lambda}}_\mu$; as illustrated in works such as [Bezrukavnikov and Kaledin 2004; Braden et al. 2012; Losev 2012], the universal symplectic deformation of a symplectic singularity as a symplectic variety is intimately tied to understanding its quantizations (see Section 4D). From this perspective, a natural next step (beyond the scope of this paper) would be to study quantizations of the total spaces of these deformations, not just of a single fiber.

Recall that we have the moduli interpretation of the affine Grassmannian (see [Mirković and Vilonen 2007, Section 5])

$$\mathsf{Gr} = \big\{(E,\phi) \mid E \text{ is a principal } G\text{-bundle on } \mathbb{P}^1 \\ \text{and } \phi : E|_{\mathbb{P}^1 \smallsetminus \{0\}} \to E^0|_{\mathbb{P}^1 \smallsetminus \{0\}} \text{ is an isomorphism}\big\},$$

where E^0 denotes the trivial G-bundle. We say that (E,ϕ) has *Hecke type* λ at 0 if (E,ϕ) gives a point in Gr^λ under the above identification.

Note that the action of $G[\![t^{-1}]\!]$ by left multiplication in the homogeneous space definition becomes change of trivialization in the new definition. Thus the $G[\![t^{-1}]\!]$ orbit of (E,ϕ) is determined by isomorphism class of the G-bundle E, which is given by a dominant coweight. Note also that the action of $G_1[\![t^{-1}]\!]$ corresponds to changes of trivialization which do not change anything at ∞.

Let μ be a dominant coweight and let P be the corresponding standard parabolic subgroup (so that W_P is the stabilizer of μ in the Weyl group). Let E be a principal G-bundle of type μ. Then E has a canonical P-structure.

Now let $(E,\phi) \in \mathsf{Gr}$. Let μ be the isomorphism type of E. Then ϕ_∞ carries the parabolic structure at ∞ to a parabolic subgroup of G of type μ. Hence we see that the $G_1[\![t^{-1}]\!]$ orbits on Gr are labeled by a pair consisting of a dominant coweight μ and a parabolic subgroup of G of type μ. In particular, Gr_μ is the locus of those (E,ϕ) where E has isomorphism type μ and the parabolic subgroup produced is the standard one.

We now consider the Beilinson–Drinfeld deformation of the affine Grassmannian. This is a family $\mathsf{Gr}_{\mathbb{A}^n}$ over $\mathbb{A}^n$ whose fiber at $a_1,\dots,a_n \in \mathbb{A}^n$ is given as

$$\mathsf{Gr}_{a_1,\dots,a_n} = \big\{(E,\phi) \mid E \text{ is a principal } G\text{-bundle on } \mathbb{P}^1 \\ \text{and } \phi : E|_{\mathbb{P}^1 \smallsetminus \{a_1,\dots,a_n\}} \to E^0|_{\mathbb{P}^1 \smallsetminus \{a_1,\dots,a_n\}} \text{ is an isomorphism}\big\}.$$

Let $\mathsf{Gr}_{\mu,\mathbb{A}^n}$ be the locus of (E,ϕ), where E has isomorphism type μ and the parabolic subgroup at ∞ is the standard one.

Specializing to one choice of parameters, we can consider changes of trivialization acting on $\mathsf{Gr}_{a_1,\dots,a_n}$. Let $G_1(\mathbb{P}^1 \smallsetminus \{a_1,\dots,a_n\})$ denote the kernel of $G(\mathbb{P}^1 \smallsetminus \{a_1,\dots,a_n\}) \to G$ given by evaluation at ∞. Then $\mathsf{Gr}_{\mu,(a_1,\dots,a_n)}$ is an orbit of $G_1(\mathbb{P}^1 \smallsetminus \{a_1,\dots,a_n\})$.

We may also think of this locus in terms of the $\mathbb{C}^\times$ action. We have an action of $\mathbb{C}^\times$ on $\mathsf{Gr}_{\mathbb{A}^n}$ coming from the action of $\mathbb{C}^\times$ on $\mathbb{P}^1$. Note that this action moves the base $\mathbb{A}^n$. On the central fiber $\mathsf{Gr}_{(0,\dots,0)} = \mathsf{Gr}$, this action of $\mathbb{C}^\times$ restricts to the loop rotation action on Gr. Hence the fixed points of this $\mathbb{C}^\times$ action are the same as the fixed points of the loop rotation action, namely, the sets Gt^μ inside the affine Grassmannian. Moreover, we have that $\mathsf{Gr}_{\mu,\mathbb{A}^n}$ is the attracting set for $t^{w_0\mu}$ under the $\mathbb{C}^\times$ action.

We have a fiberwise Poisson structure on $\mathsf{Gr}_{\mathbb{A}^n}$ using the Manin triples described in [Etingof and Kazhdan 1998, Corollary 2.10 and Proposition 2.12]. As in Section 2C, we get a Poisson structure on $\mathsf{Gr}_{\mu,(a_1,\dots,a_n)}$.

Now let us choose an expression $\lambda = \lambda_1 + \cdots + \lambda_n$, where $\lambda_1, \dots, \lambda_n$ are fundamental coweights. This gives us a colored divisor D on $\mathbb{P}^1$ defined by $D = \sum \lambda_i a_i$. We will think of D as a function on $\mathbb{P}^1$ with values in the dominant coweights. Now we define

$$\mathsf{Gr}^{\lambda_1,\dots,\lambda_n}_{\mu,(a_1,\dots,a_n)} := \{(E,\phi) \in \mathsf{Gr}_{\mu,(a_1,\dots,a_n)} \mid (E,\phi) \text{ has Hecke type } D(x) \text{ for all } x \in \mathbb{P}^1\}.$$

From the above analysis, it is possible to show that these are symplectic leaves in $\mathsf{Gr}_{\mu,(a_1,\dots,a_n)}$.

Fixing $(\lambda_1, \dots, \lambda_n)$ and letting $(a_1, \dots, a_n)$ vary, this forms a family of $\mathbb{A}^n$. The central fiber of this family is $\mathsf{Gr}^{\lambda}_{\mu}$.

Now, define

$$\mathsf{Gr}^{\overline{\lambda_1,\dots,\lambda_n}}_{\mu,(a_1,\dots,a_n)} := \{(E,\phi) \in \mathsf{Gr}_{\mu,(a_1,\dots,a_n)} \mid (E,\phi) \text{ has Hecke type } \le D(x) \text{ for all } x \in \mathbb{P}^1\}.$$

Then we obtain a family of symplectic varieties over $\mathbb{A}^n$ whose central fiber is $\mathsf{Gr}^{\overline{\lambda}}_{\mu}$.

2E. ***Direct system on slices and Zastava spaces.*** We now look at what happens to $\mathsf{Gr}^{\overline{\lambda}}_{\mu}$ when we increase λ, μ, keeping $\lambda - \mu$ fixed.

Let us fix ν in the positive coroot cone. Let μ, μ' be dominant coweights with $\mu' - \mu$ dominant. From Lemma 2.3, we know that the stabilizer of $t^{w_0\mu'}$ in $G_1[[t^{-1}]]$ contains the stabilizer of $t^{w_0\mu}$ in $G_1[[t^{-1}]]$. So we can define a map $\mathsf{Gr}_{\mu} \to \mathsf{Gr}_{\mu'}$ by $gt^{w_0\mu} \mapsto gt^{w_0\mu'}$. From Proposition 2.4, we see that this restricts to a map

$$\mathsf{Gr}^{\overline{\mu+\nu}}_{\mu} \to \mathsf{Gr}^{\overline{\mu'+\nu}}_{\mu'}.$$

By construction, it is a Poisson map.

Clearly these maps are compatible with composition. Thus with ν fixed we get a direct system of slices $\{\mathsf{Gr}^{\overline{\mu+\nu}}_{\mu}\}_{\mu}$. The limit of this system is an ind-scheme, but in general it will not be represented by a scheme.

On the other hand, we can consider the Zastava space Z_ν, an affine variety, as defined in [Finkelberg and Mirković 1999]. It is a partial compactification of the moduli space Z°_ν of based maps from $\mathbb{P}^1$ into G/B of degree ν. The variety Z_ν carries an action of $\mathbb{C}^\times$, extending the action of $\mathbb{C}^\times$ on Z°_ν which rotates the source of the map.

The following result shows that the algebras of functions $\mathbb{O}(\mathsf{Gr}^{\overline{\mu+\nu}}_{\mu})$ stabilize to $\mathbb{O}(Z_\nu)$.

Theorem 2.10 [Braverman and Finkelberg 2011, Theorem 2.8]. *There exists a map $\mathsf{Gr}^{\overline{\mu+\nu}}_{\mu} \to Z_\nu$. These maps are compatible with the above direct system on the slices* *and with the actions of* $\mathbb{C}^\times$. *Moreover, the induced maps* $\mathbb{O}(Z_\nu)_N \to \mathbb{O}(\overline{\mathrm{Gr}^{\mu+\nu}_\mu})_N$ *are isomorphisms if* $N \leq \langle \alpha_i, \mu \rangle$ *for all* i.

Remark 2.11. The theorem provides Z_ν with a Poisson structure. On the other hand, Z_ν° carries a symplectic structure as described in [Finkelberg et al. 1999]. It is expected that these two structures are compatible.

Example 2.12. Let us take $G = \mathrm{PGL}_2$ and $\nu = \alpha^\vee$, the simple coroot. Then (as in Example 2.2), for $n \geq 0$,

$$\overline{\mathrm{Gr}^{n\omega^\vee+\alpha^\vee}_{n\omega^\vee}} \cong \{(u, v, w) \mid uv + w^{n+2} = 0\}.$$

Moreover, for $m \geq n$, the map $\overline{\mathrm{Gr}^{n\omega^\vee+\alpha^\vee}_{n\omega^\vee}} \to \overline{\mathrm{Gr}^{m\omega^\vee+\alpha^\vee}_{m\omega^\vee}}$ is given by $(u, v, w) \mapsto (u, vw^{m-n}, w)$. This is because we have an equality in $\mathrm{Gr}_{\mathrm{PGL}_2}$:

$$\begin{aligned}\begin{bmatrix} 1 - wt^{-1} & vt^{-(n+1)} \\ ut^{-1} & 1 + wt^{-1} + \cdots + w^{n+1}t^{-(n+1)} \end{bmatrix}&\begin{bmatrix} 1 & 0 \\ 0 & t^m \end{bmatrix} \\ &= \begin{bmatrix} 1 - wt^{-1} & vw^{m-n}t^{-(m+1)} \\ ut^{-1} & 1 + wt^{-1} + \cdots + w^{m+1}t^{-(m+1)} \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & t^m \end{bmatrix}.\end{aligned}$$

On the other hand, the Zastava space Z_α is $\mathbb{A}^2$. The map in Theorem 2.10 is given by $(u, v, w) \mapsto (u, w)$.

With respect to the $\mathbb{C}^\times$ action on

$$\overline{\mathrm{Gr}^{n\omega^\vee+\alpha^\vee}_{n\omega^\vee}} = \{(u, v, w) \mid uv + w^{n+2} = 0\},$$

the variables u, w have weight 1 and v has weight $n + 1$. So we can see that

$$\mathbb{O}(Z_\alpha) = \mathbb{C}[u, w] \to \mathbb{O}\big(\overline{\mathrm{Gr}^{n\omega^\vee+\alpha^\vee}_{n\omega^\vee}}\big) = \mathbb{C}[u, v, w]/(uv + w^{n+2})$$

is an isomorphism in degrees $0, \ldots, n$, as predicted by Theorem 2.10.

The Poisson structure on $\overline{\mathrm{Gr}^{n\omega^\vee+\alpha^\vee}_{n\omega^\vee}}$ is given by

$$\{w, u\} = u, \quad \{w, v\} = -v, \quad \{u, v\} = (n + 2)w^{n+1},$$

while the Poisson structure on Z_α is given by

$$\{w, u\} = u.$$

Finally, note that the $\mathbb{C}$-points of the ind-scheme $\lim_n \overline{\mathrm{Gr}^{n\omega^\vee+\alpha^\vee}_{n\omega^\vee}}$ are

$$\{(u, w) \mid u \in \mathbb{C}^\times, w \in \mathbb{C}\} \cup \{(0, 0)\},$$

which is a proper subset of $\mathbb{C}^2$, and hence this ind-scheme is not equal to $\mathbb{A}^2$.

2F. ***Description of the Poisson structure.*** We would like to describe the Poisson structure on $G_1[[t^{-1}]]$ in a little more detail. Let $C \in \mathfrak{g} \otimes \mathfrak{g}$ be the Casimir element for the bilinear form. Picking dual bases, we may represent this element as $C = \sum J_a \otimes J^a$; this Casimir element allows us to describe the Poisson bracket of two minors. This can be written more compactly using the series

$$\Delta_{\beta,v}(u) = \sum_{s \geq 0} \Delta_{\beta,v}^{(s)} u^{-s}.$$

Note that $\Delta_{\beta,v}^{(0)} = \langle \beta, w \rangle$ is a constant function.

Proposition 2.13. *The Poisson bracket* $\{\Delta_{\beta_1,v_1}(u_1), \Delta_{\beta_2,v_2}(u_2)\}$ *is equal to*

$$\frac{1}{u_1 - u_2} \sum_a \Delta_{\beta_1, J_a v_1}(u_1) \Delta_{\beta_2, J^a v_2}(u_2) - \Delta_{J_a \beta_1, v_1}(u_1) \Delta_{J^a \beta_2, v_2}(u_2)$$

in $\mathcal{O}(G_1[[t^{-1}]])[[u_1^{-1}, u_2^{-1}]]$.

Proof. The cobracket $\mathfrak{g}((t^{-1})) \to \mathfrak{g}((u_1)) \otimes \mathfrak{g}((u_2))$ is coboundary. If we let $r(u_1, u_2) = C/(u_1 - u_2)$, it is given by

$$a(t) \mapsto \big[a(u_1) \otimes 1 + 1 \otimes a(u_2), r(u_1, u_2)\big].$$

As described earlier, the Lie algebra $\mathfrak{g}((t^{-1}))$ carries an inner product

$$(f, g)_t = -\operatorname{res}_{t=0}(f, g)$$

for which $t^{-1}\mathfrak{g}[[t^{-1}]]$ is Lagrangian and complementary to $\mathfrak{g}[t]$; this realizes $\mathfrak{g}((t^{-1}))$ as the (topological) Drinfeld double of $t^{-1}\mathfrak{g}[[t^{-1}]]$. In particular,

$$G_1[[t^{-1}]] \subset G((t^{-1}))$$

is a Poisson subgroup, and the Poisson bracket of any two functions on $G_1[[t^{-1}]]$ can be calculated taking the bracket of any two extensions to all of $G((t^{-1}))$ and then restricting to $G_1[[t^{-1}]]$.

Thus, the Poisson structure on $G((t^{-1}))$ is defined by

$$\pi = r^L(u_1, u_2) - r^R(u_1, u_2),$$

the difference of the left translation and right translation of the element $r(u_1, u_2)$ considered as a bivector at the identity. If $X \in t^{-1}\mathfrak{g}[[t^{-1}]]$ and $g \in G_1[[t^{-1}]]$, we identify X with a tangent vector at g by left translation. Then we have

$$(d\Delta_{\beta,v})_g(X) = \langle \beta, gXv \rangle.$$

Hence

$$
\begin{aligned}
\big\{\Delta_{\beta_1,v_1}(u_1),\, \Delta_{\beta_2,v_2}(u_2)\big\}(g) \\
&= \big\langle \pi,\, (d\Delta_{\beta_1,v_1})_g \otimes (d\Delta_{\beta_2,v_2})_g(g)\big\rangle \\
&= \big\langle r^L(u_1,u_2) - r^R(u_1,u_2),\, (d\Delta_{\beta_1,v_1})_g \otimes (d\Delta_{\beta_2,v_2})_g(g)\big\rangle \\
&= \frac{1}{u_1-u_2}\bigg(\sum_a \langle \beta_1,\, g(u_1)J_a v_1\rangle\langle \beta_2,\, g(u_2)J^a v_2\rangle \\
&\qquad - \sum_a \langle \beta_1,\, J_a g(u_1)v_1\rangle\langle \beta_2,\, J^a g(u_2)v_2\rangle\bigg) \\
&= \frac{1}{u_1-u_2}\sum_a \Delta_{\beta_1,J_a v_1}(u_1)\Delta_{\beta_2,J^a v_2}(u_2) - \Delta_{J_a\beta_1,v_1}(u_1)\Delta_{J^a\beta_2,v_2}(u_2),
\end{aligned}
$$

where the last step follows from the invariance of the pairing between dual representations. □

We can unpack Proposition 2.13 into the following equations:

$$\big\{\Delta^{(r+1)}_{\beta_1,v_1},\, \Delta^{(s)}_{\beta_2,v_2}\big\} - \big\{\Delta^{(r)}_{\beta_1,v_1},\, \Delta^{(s+1)}_{\beta_2,v_2}\big\} = \sum \Delta^{(r)}_{J_a\beta_1,v_1}\Delta^{(s)}_{J^a\beta_2,v_2} - \Delta^{(r)}_{\beta_1,J_a v_1}\Delta^{(s)}_{\beta_2,J^a v_2} \tag{1}$$

for $r, s \geq 0$. These equations specify all the desired Poisson brackets.

2G. ***A conjectural description of the ideal of*** $\overline{\mathsf{Gr}^{\lambda}_{\mu}}$**.** In this section, we give a conjectural description of the ideal of $\overline{\mathsf{Gr}^{\lambda}_{\mu}}$ as a subvariety of $\mathsf{Gr}_0 = G_1[\![t^{-1}]\!]$. Let G^{sc} denote the simply connected cover of G. Note that the natural map $G^{\mathrm{sc}}_1[\![t^{-1}]\!] \to G_1[\![t^{-1}]\!]$ is an isomorphism. This allows us to consider $\Delta^{(s)}_{\omega_i,\omega_i}$ as functions on $G_1[\![t^{-1}]\!]$, even if ω_i are not weights of G (for example if G is of adjoint type).

We begin with the case of $\mu = 0$. Let J^λ_0 denote the ideal in $\mathbb{O}(G_1[\![t^{-1}]\!])$ Poisson generated by $\Delta^{(s)}_{\omega_i,\omega_i}$ for $s > \langle \lambda, \omega_{i^*}\rangle$ and for $i \in I$.

Conjecture 2.14. *The ideal of* $\overline{\mathsf{Gr}^{\lambda}_{0}}$ *in* $\mathbb{O}(G_1[\![t^{-1}]\!])$ *is* J^λ_0.

Let us make some comments on this conjecture. First, we have the following result.

Proposition 2.15. J^λ_0 *is generated as an ordinary ideal by* $\Delta^{(s)}_{\beta,v}$ *for* $s > \langle \lambda, \omega_{i^*}\rangle$ *and for* $i \in I$, *where* β, v *range over bases for* $V(\omega_i)^*$ *and* $V(\omega_i)$.

Proof. Let I be the ideal generated as an ordinary ideal by $\Delta^{(s)}_{\beta,v}$ for $s > \langle \lambda, \omega_{i^*}\rangle$. First, we show that this ideal is contained in J^λ_0.

We claim that $\Delta^{(s)}_{\omega_i,v} \in J^\lambda_0$ for all $v \in V(\omega_i)$ and $s > \langle \lambda, \omega_{i^*}\rangle$. We proceed by downward induction on the weight of v. The base case of v is highest weight follows by definition. For the inductive step, suppose that v is not highest weight. In this case, $v = \sum f_j v_j$ for some v_j of higher weight than v.

Fix s with $s > \langle \lambda, \omega_{i^*} \rangle$. Using (1) with $s = 0$ and the expression for the Casimir (for notation see Section 3B)

$$C = C_{\mathfrak{h}} + \sum_{\alpha \in \Phi_+} C_\alpha e_\alpha \otimes f_\alpha + C_\alpha f_\alpha \otimes e_\alpha,$$

where $(e_\alpha, f_\alpha) = C_\alpha^{-1}$, we see that

$$\{\Delta^{(r)}_{\omega_i, v_j}, \Delta^{(1)}_{\omega_j, s_j \omega_j}\} = -\Delta^{(r)}_{\omega_i, f_j v_j}.$$

Thus we see that

$$\Delta^{(s)}_{\omega_i, v} = \sum_j \Delta^{(s)}_{\omega_i, f_j v_j} = -\sum_j \{\Delta^{(s)}_{\omega_i, v_j}, \Delta^{(1)}_{\omega_j, s_j \omega_j}\}.$$

All the terms on the right-hand side lie in J_0^λ by the inductive assumption, and thus $\Delta^{(s)}_{\omega_i, v} \in J_0^\lambda$.

Now we claim that $\Delta^{(s)}_{\beta, v} \in J_0^\lambda$ for all $\beta \in V(\omega_i)^*$, $v \in V(\omega_i)$, and $s > \langle \lambda, \omega_{i^*} \rangle$.

We have already proven this claim when $\beta = v_{-\omega_i}$, so we proceed by induction on the weight of β. Suppose that $\beta \in V(\omega_i)^*$ is not lowest weight and assume that the claim holds for all β of lower weight. In this case, we can write $\beta = \sum e_j \beta_j$ for some β_j of lower weight.

Fix s with $s > \langle \lambda, \omega_{i^*} \rangle$. Again using the above expression for the Casimir, we find that

$$\{\Delta^{(s)}_{\beta_j, v}, \Delta^{(1)}_{s_j \omega_j, \omega_j}\} = \Delta^{(s)}_{\beta_j, e_j v} - \Delta^{(s)}_{e_j \beta_j, v}.$$

Thus we see that

$$\Delta^{(s)}_{\beta, v} = \sum_j \Delta^{(s)}_{e_j \beta_j, v} = \sum_j \{\Delta^{(s)}_{\beta_j, v}, \Delta^{(1)}_{s_j \omega_j, \omega_j}\} - \Delta^{(s)}_{\beta_j, e_j v}.$$

All the terms on the right-hand side lie in J_0^λ by the inductive assumption, and thus $\Delta^{(s)}_{\beta, v} \in J_0^\lambda$. This shows that $I \subset J_\lambda^0$.

It remains to show that I is a Poisson ideal. Since $\Delta^{(s)}_{\beta, v}$, for $\beta \in V(\omega_i)^*$, $v \in V(\omega_i)$, $i \in I$, generates $\mathcal{O}(G_1[\![t^{-1}]\!])$, it suffices to check that I is closed under Poisson bracket with these elements. This follows immediately from (1). $\square$

Combining this proposition with Proposition 2.4, we obtain the following.

Corollary 2.16. *The vanishing set of J_0^λ is $\overline{\mathrm{Gr}_0^\lambda}$.*

Thus in order to establish Conjecture 2.14, it only remains to show that I_0^λ is radical.

Remark 2.17. Let $G = \mathrm{SL}_n$. By an observation which goes back to Lusztig [1981, Section 2], we know that there is an isomorphism $\overline{\mathsf{Gr}_0^{n\omega_1}} \cong \mathcal{N}$, the nilpotent cone of $\mathfrak{sl}_n$. For any dominant coweight λ with $\lambda \leq n\omega_1$, under this isomorphism $\overline{\mathsf{Gr}_0^{\lambda}}$ is taken to a nilpotent orbit closure. Thus, the above conjecture implies generators for the ideal of a nilpotent orbit closure inside the nilpotent cone of $\mathfrak{sl}_n$. From this perspective, one can see that Conjecture 2.14 would imply the main result of [Weyman 1989], which gives generators for the ideals of nilpotent orbit closures. This gives additional evidence toward the conjecture, but also suggests it will be difficult to prove.

Remark 2.18. One could imagine a similar conjecture for the ideal of $\overline{\mathsf{Gr}^{\lambda}}$ inside of the homogeneous coordinate ring of Gr with respect to its natural determinant line bundle. However, this conjecture is false, already for SL_2 and $\lambda = \alpha$.

We will need the following generalization of Conjecture 2.14, which describes the ideal of $\overline{\mathsf{Gr}^{\lambda}_{\mu}}$. Consider the subgroup $G_1[\![t^{-1}]\!]_\mu$ defined as the stabilizer in $G_1[\![t^{-1}]\!]$ of $t^{w_0\mu}$. Note that, by Lemma 2.3, $G_1[\![t^{-1}]\!]_\mu \subset N_1[\![t^{-1}]\!]$.

By the orbit-stabilizer theorem, we see that $\mathsf{Gr}_\mu = G_1[\![t^{-1}]\!]/G_1[\![t^{-1}]\!]_\mu$, and so $\mathbb{O}(\mathsf{Gr}_\mu) = \mathbb{O}(G_1[\![t^{-1}]\!])^{G_1[\![t^{-1}]\!]_\mu}$. Moreover, the map $G_1[\![t^{-1}]\!] \to \mathsf{Gr}_\mu$ is Poisson, and thus $\mathbb{O}(\mathsf{Gr}_\mu)$ is a Poisson subalgebra of $\mathbb{O}(G_1[\![t^{-1}]\!])$.

Lemma 2.19. *The subalgebra* $\mathbb{O}(\mathsf{Gr}_\mu)$ *contains*

$$\begin{aligned} \Delta^{(s)}_{s_i\omega_i,\omega_i} &\quad \textit{for all } i \in I,\ s > 0, \\ \Delta^{(s)}_{\omega_i,\omega_i} &\quad \textit{for all } i \in I,\ s > 0, \\ (\Delta_{\omega_i,s_i\omega_i}/\Delta_{\omega_i,\omega_i})^{(s)} &\quad \textit{for all } i \in I,\ s > \langle \mu^*, \alpha_i \rangle. \end{aligned}$$

Later we will see that these elements generate $\mathbb{O}(\mathsf{Gr}_\mu)$ as a Poisson algebra.

Proof. Note that the action of $G_1[\![t^{-1}]\!]_\mu$ on $\mathbb{O}(G_1[\![t^{-1}]\!])$ is given by $(k \cdot f)(g) = g(fk)$ for $k \in G_1[\![t^{-1}]\!]_\mu$, $f \in \mathbb{O}(G_1[\![t^{-1}]\!])$, and $g \in G_1[\![t^{-1}]\!]$. In particular, we see that $k \cdot \Delta_{\beta,v} = \Delta_{\beta,kv}$.

Since $G_1[\![t^{-1}]\!]_\mu \subset N_1[\![t^{-1}]\!]$, the minors $\Delta_{\omega_i,\omega_i}$ and $\Delta_{s_i\omega_i,\omega_i}$ will be $G_1[\![t^{-1}]\!]_\mu$-invariant. Hence all $\Delta^{(s)}_{s_i\omega_i,\omega_i}$, $\Delta^{(s)}_{\omega_i,\omega_i}$ lie in $\mathbb{O}(\mathsf{Gr}_\mu)$.

On the other hand, let us consider the coefficients of the $\Delta_{\omega_i,s_i\omega_i}$ minor. If $k \in G_1[\![t^{-1}]\!]_\mu$, then we have $k \cdot v_{s_i\omega_i} = v_{s_i\omega_i} + \Delta_{\omega_i,s_i\omega_i}(k) v_{\omega_i}$. Hence if $g \in G_1[\![t^{-1}]\!]$, then

$$\frac{\Delta_{\omega_i,s_i\omega_i}(gk)}{\Delta_{\omega_i,\omega_i}(gk)} = \frac{\Delta_{\omega_i,s_i\omega_i}(g) + \Delta_{\omega_i,\omega_i}(g)\Delta_{\omega_i,s_i\omega_i}(k)}{\Delta_{\omega_i,\omega_i}(g)} = \frac{\Delta_{\omega_i,s_i\omega_i}(g)}{\Delta_{\omega_i,\omega_i}(g)} + \Delta_{\omega_i,s_i\omega_i}(k).$$

By Lemma 2.3, we have $\Delta_{\omega_i,s_i\omega_i}(k) \in t^{-\langle w_0\mu,\alpha_i\rangle}\mathbb{C}[t]$. Hence the coefficient of t^{-s} in $\Delta_{\omega_i,s_i\omega_i}/\Delta_{\omega_i,\omega_i}$ is invariant under the action of $G_1[\![t^{-1}]\!]_\mu$ for $s > \langle \mu^*, \alpha_i \rangle$. Thus $(\Delta_{\omega_i,s_i\omega_i}/\Delta_{\omega_i,\omega_i})^{(s)} \in \mathbb{O}(\mathsf{Gr}_\mu)$ for $s > \langle \mu^*, \alpha_i \rangle$. □

Let J^{λ}_{μ} denote the ideal of $\mathcal{O}(\mathsf{Gr}_{\mu})$ Poisson generated by $\Delta^{(s)}_{\omega_i,\omega_i}$ for $i \in I$ and $s > \langle \lambda - \mu, \omega_{i^*} \rangle = m_i$.

Conjecture 2.20. *The ideal of* $\overline{\mathsf{Gr}^{\lambda}_{\mu}}$ *in* $\mathcal{O}(\mathsf{Gr}_{\mu})$ *is* J^{λ}_{μ}.

This conjecture generalizes Conjecture 2.14. When $\mu \neq 0$, we do not have a set of (ordinary) generators for J^{λ}_{μ} as in Proposition 2.15. However, we will now establish an analogue of Corollary 2.16.

Proposition 2.21. *The vanishing locus of* J^{λ}_{μ} *is* $\overline{\mathsf{Gr}^{\lambda}_{\mu}}$.

Proof. The vanishing locus of J^{λ}_{μ} is the union of the symplectic leaves in the vanishing locus of $\Delta^{(s)}_{\omega_i,\omega_i}$ for $i \in I$ and $s > \langle \lambda - \mu, \omega_{i^*} \rangle = m_i$; after all, the vanishing set is a union of symplectic leaves and if these functions vanish on a symplectic leaf, then so do all Poisson brackets with them.

These generalized minors vanish on $\overline{\mathsf{Gr}^{\lambda}_{\mu}}$ by Proposition 2.4. So it suffices to prove the vanishing locus of our generators does not contain Gr^{ν}_{μ} for some $\nu \not\leq \lambda$.

Fix $\nu \not\leq \lambda$ such that $\mu \leq \nu$. Then $d = \langle \nu - \mu, \omega_{i^*} \rangle > \langle \lambda - \mu, \omega_{i^*} \rangle$ for some i. We will prove that there exists a point in Gr^{ν}_{μ} on which $\Delta^{(d)}_{\omega_i,\omega_i}$ is nonzero.

Let $I^+_+ = I \subset G((t^{-1}))$ denote the standard Iwahori and let $I^+_- = w_0 I^+_+ w_0^{-1}$ be the preimage of B_- in $G[t]$. We claim that it suffices to prove that

$$I^+_- t^{w_0\nu} I^+_+ \cap G_-[\![t^{-1}]\!] t^{w_0\mu} \neq \varnothing \quad \text{in } G((t^{-1})). \tag{2}$$

To see that (2) suffices, let $g \in G_1[\![t^{-1}]\!]$ such that $gt^{w_0\mu}$ lies in the above intersection. As $I^+_-, I^+_+ \subset G[t]$, we see that $gt^{w_0\mu} \in \mathsf{Gr}^{\nu}_{\mu}$. Finally, we can write $g = b_- t^{w_0\nu} b_+ t^{-w_0\mu}$ for $b_- \in I^+_-$, $b_+ \in I^+_+$, and an elementary computation shows that $\Delta^{(d)}_{\omega_i,\omega_i}(b_- t^{w_0\nu} b_+ t^{-w_0\mu}) \neq 0$.

To prove (2), we work in the affine flag variety $G((t^{-1}))/I$ and note that (2) is equivalent to nonemptiness of the intersection $I^+_- t^{w_0\nu} \cap G_-[\![t^{-1}]\!] t^{w_0\mu}$ in $G((t^{-1}))/I$. Let I^-_+ denote the preimage of B in $G[\![t^{-1}]\!]$ under evaluation at $t^{-1} = 0$. Since μ is dominant, B fixes $t^{w_0\mu}$ and thus $G_-[\![t^{-1}]\!] t^{w_0\mu} = I^-_+ t^{w_0\mu}$. Thus we reduce to proving that

$$I^+_- t^{w_0\nu} \cap I^-_+ t^{w_0\mu} \neq \varnothing \quad \text{in } G((t^{-1}))/I.$$

Twisting by w_0, we reduce to proving that

$$I^+_+ w_0 t^{w_0\nu} \cap I^-_- w_0 t^{w_0\mu} \neq \varnothing \quad \text{in } G((t^{-1}))/I,$$

where I^-_- is the preimage of B_- in $G[\![t^{-1}]\!]$. From general theory of flag varieties, this is equivalent to $w_0 t^{w_0\nu} \geq w_0 t^{w_0\mu}$ in the Bruhat order on the (extended) affine Weyl group. This last fact is easily verified under our hypothesis that μ, ν are dominant and $\nu \geq \mu$. □

3. Yangians

3A. ***The Drinfeld Yangian.*** As mentioned in the introduction, we will study subquotients of Yangians in order to quantize our slices. We will actually need a slight variant on the usual Yangian, which will be produced via a theory developed by Gavarini [2007; 2002]. We begin with the usual Yangian, which we call the *Drinfeld Yangian* to avoid confusion with the Yangian we wish to consider.

We define the Drinfeld Yangian $U_h\mathfrak{g}[t]$ as the associative $\mathbb{C}[\![h]\!]$-algebra with generators $e_i^{(s)}$, $h_i^{(s)}$, $f_i^{(s)}$ for $i \in I$ and $r, s \in \mathbb{N}$ and relations

$$\begin{aligned}
\big[h_i^{(s)}, h_j^{(s)}\big] &= 0,\\
\big[e_i^{(r)}, f_i^{(s)}\big] &= \delta_{ij} h_i^{(r+s)},\\
\big[h_i^{(0)}, e_j^{(s)}\big] &= (\alpha_i, \alpha_j) e_j^{(s)},\\
\big[h_i^{(r+1)}, e_j^{(s)}\big] - \big[h_i^{(r)}, e_j^{(s+1)}\big] &= \frac{h(\alpha_i, \alpha_j)}{2}\big(h_i^{(r)} e_j^{(s)} + e_j^{(s)} h_i^{(r)}\big),\\
\big[h_i^{(0)}, f_j^{(s)}\big] &= -(\alpha_i, \alpha_j) f_j^{(s)},\\
\big[h_i^{(r+1)}, f_j^{(s)}\big] - \big[h_i^{(r)}, f_j^{(s+1)}\big] &= -\frac{h(\alpha_i, \alpha_j)}{2}\big(h_i^{(r)} f_j^{(s)} + f_j^{(s)} h_i^{(r)}\big),\\
\big[e_i^{(r+1)}, e_j^{(s)}\big] - \big[e_i^{(r)}, e_j^{(s+1)}\big] &= \frac{h(\alpha_i, \alpha_j)}{2}\big(e_i^{(r)} e_j^{(s)} + e_j^{(s)} e_i^{(r)}\big),\\
\big[f_i^{(r+1)}, f_j^{(s)}\big] - \big[f_i^{(r)}, f_j^{(s+1)}\big] &= -\frac{h(\alpha_i, \alpha_j)}{2}\big(f_i^{(r)} f_j^{(s)} + f_j^{(s)} f_i^{(r)}\big),\\
i \neq j,\ N = 1 - a_{ij} \implies& \operatorname{sym}\big[e_i^{(r_1)}, [e_i^{(r_2)}, \dots [e_i^{(r_N)}, e_j^{(s)}] \dots]\big] = 0,\\
i \neq j,\ N = 1 - a_{ij} \implies& \operatorname{sym}\big[f_i^{(r_1)}, [f_i^{(r_2)}, \dots [f_i^{(r_N)}, f_j^{(s)}] \dots]\big] = 0,
\end{aligned}$$

where sym denotes symmetrization with respect to $r_1, \dots, r_N$.

The following result of Drinfeld [1987, Example 6.3] will be our starting point.

Theorem 3.1. $U_h\mathfrak{g}[t]$ *is a quantization of* $\mathfrak{g}[t]$. *More precisely, there is an isomorphism of co-Poisson Hopf algebras* $U_h\mathfrak{g}[t]/hU_h\mathfrak{g}[t] \cong U\mathfrak{g}[t]$, *where* $U\mathfrak{g}[t]$ *carries the co-Poisson structure coming from the Manin triple* $\big(\mathfrak{g}[t], t^{-1}\mathfrak{g}[\![t^{-1}]\!], \mathfrak{g}((t^{-1}))\big)$.

3B. ***PBW basis for the Drinfeld Yangian.*** Fix any order on the nodes of the Dynkin diagram; for each positive root α, we let $\check{\alpha}$ denote the smallest simple root such that $\hat{\alpha} = \alpha - \check{\alpha}$ is again a positive root.

We define $e_\alpha \in \mathfrak{g}$ for $\alpha \in \Delta_+$ recursively by

$$e_{\alpha_i} = e_i \quad \text{and} \quad e_\alpha = [e_{\hat{\alpha}}, e_{\check{\alpha}}].$$

We extend this definition to $U_h\mathfrak{g}[t]$ by setting

$$e^{(r)}_{\alpha_i} = e^{(r)}_i \quad \text{and} \quad e^{(r)}_\alpha = [e^{(r)}_{\hat{\alpha}}, e^{(0)}_{\check{\alpha}}].$$

Similarly, we define f_α and $f^{(r)}_\alpha$. We have the following PBW theorem for the Drinfeld Yangian due to Levendorskii [1993].

Proposition 3.2. (1) *Under the isomorphism $U_h\mathfrak{g}[t]/hU_h\mathfrak{g}[t] \cong U\mathfrak{g}[t]$, $e^{(r)}_\alpha$ corresponds to $e_\alpha t^r$.*

(2) *Ordered monomials in the $e^{(r)}_\alpha$, $h^{(r)}_i$, $f^{(r)}_\beta$ form a PBW basis for $U_h\mathfrak{g}[t]$.*

3C. ***Drinfeld–Gavarini duality.*** Our goal is to give a quantization of the Poisson–Hopf algebra $\mathcal{O}(G_1[\![t^{-1}]\!])$ using the Drinfeld Yangian $U_h\mathfrak{g}[t]$. For this we will use the quantum groups duality of Drinfeld and Gavarini.

We describe in brief one half of Drinfeld–Gavarini duality [Drinfeld 1987; Gavarini 2007; 2002]. Let (H, Δ, ϵ) be a Hopf algebra over $\mathbb{C}[\![h]\!]$. Consider maps $\Delta^n : H \to H^{\otimes n}$ for $n \geq 0$ defined by $\Delta^0 = \epsilon$, $\Delta^1 = \mathrm{id}_H$, and

$$\Delta^n = (\Delta \otimes \mathrm{id}^{\otimes(n-2)}) \circ \Delta^{n-1}$$

for $n \geq 2$. Let $\delta^n = (\mathrm{id}_H - \epsilon)^{\otimes n} \circ \Delta^n$, and define the Hopf subalgebra

$$H' = \{a \in H \mid \delta^n(a) \in h^n H^{\otimes n}\}.$$

In general, H'/hH' is a commutative Hopf algebra over $\mathbb{C}$ and can be given the Poisson bracket

$$\{a + hH', b + hH'\} = h^{-1}[a, b] + hH'.$$

Suppose that G is a Poisson affine algebraic group, namely the maximal spectrum of a Poisson commutative Hopf algebra $\mathcal{O}(G)$, and let $\mathfrak{g}$, $\mathfrak{g}^*$ be its tangent and cotangent Lie bialgebras. Let $U_h = U_h(\mathfrak{g})$ be a quantization of $U(\mathfrak{g})$.

Theorem 3.3 [Gavarini 2007, Theorem 2.2]. *There is an isomorphism of Poisson–Hopf algebras*

$$U_h{}'/hU_h{}' \cong \mathcal{O}(G^*),$$

where G^* is a connected algebraic group with tangent Lie bialgebra $\mathfrak{g}^*$.

By [Gavarini 2002], for any basis $\{\overline{x}_\alpha\}$ of $\mathfrak{g}$, there exists a lift $\{x_\alpha\}$ in U_h such that

- $\epsilon(x_\alpha) = 0$,
- $U_h{}'$ is generated by $\{hx_\alpha\}$, and
- ordered monomials in these generators span $U_h{}'$ over $\mathbb{C}[\![h]\!]$.

In particular, if $\{\overline{x}_i\}$ generates $\mathfrak{g}$, then $\{hx_i + hU_h{}'\}$ generates $U_h{}'/hU_h{}'$ as a Poisson algebra.

To allow for easier identification of U_h'/hU_h' and $\mathbb{O}(G^*)$, we can reformulate Theorem 3.3 as follows. Consider

$$\mathscr{L} = \mathrm{Der}(U_h'/hU_h') := \{\varphi : U_h'/hU_h' \to \mathbb{C} \mid \varphi(ab) = \varphi(a)\epsilon(b) + \epsilon(a)\varphi(b)\},$$

with Lie bracket

$$[\varphi, \phi](a) = (\varphi \otimes \phi)\big(\Delta(a) - \Delta^{\mathrm{op}}(a)\big)$$

and cobracket

$$\delta(\varphi)(a \otimes b) = \varphi(\{a, b\}).$$

This is the Lie bialgebra of the Poisson algebraic group $\mathrm{Spec}(U_h'/hU_h')$.

The isomorphism described in Theorem 3.3 can be rephrased as follows.

Corollary 3.4. *There is an isomorphism of Lie bialgebras $\mathfrak{g}^* \cong \mathscr{L}$ defined by*

$$\overline{y} \mapsto \big(hx + hU_h' \mapsto \langle \overline{y}, \overline{x} \rangle\big)$$

for x a lift of $\overline{x} \in \mathfrak{g}$, extended by the Leibniz rule. This isomorphism yields a perfect Poisson–Hopf pairing $\langle \cdot , \cdot \rangle : U(\mathfrak{g}^*) \times U_h'/hU_h' \to \mathbb{C}$.

3D. ***Our Yangian.*** We will now apply this theory to the Drinfeld Yangian $U_h\mathfrak{g}[t]$. We let $Y := (U_h\mathfrak{g}[t])'$. We will refer to Y as the Yangian from now on. Note that it is a subalgebra of the usual Yangian.

For $X = E_\alpha, H_i, F_\alpha$ and $r \geq 1$, we define $X^{(r)} = hx^{(r-1)}$. By the general remarks above, these elements generate Y and monomials in these generators give a PBW basis for Y. We define a grading on Y where $X^{(r)}$ has degree r.

Theorem 3.5. *The $X^{(r)}$ generate Y subject to the relations*

$$\begin{aligned}
\big[H_i^{(s)}, H_j^{(s)}\big] &= 0,\\
\big[E_i^{(r)}, F_j^{(s)}\big] &= h\delta_{ij} H_i^{(r+s-1)},\\
\big[H_i^{(1)}, E_j^{(s)}\big] &= h(\alpha_i, \alpha_j) E_j^{(s)},\\
\big[H_i^{(r+1)}, E_j^{(s)}\big] - \big[H_i^{(r)}, E_j^{(s+1)}\big] &= \tfrac{1}{2} h(\alpha_i, \alpha_j)\big(H_i^{(r)} E_j^{(s)} + E_j^{(s)} H_i^{(r)}\big),\\
\big[H_i^{(1)}, F_j^{(s)}\big] &= -h(\alpha_i, \alpha_j) F_j^{(s)},\\
\big[H_i^{(r+1)}, F_j^{(s)}\big] - \big[H_i^{(r)}, F_j^{(s+1)}\big] &= -\tfrac{1}{2} h(\alpha_i, \alpha_j)\big(H_i^{(r)} F_j^{(s)} + F_j^{(s)} H_i^{(r)}\big),\\
\big[E_i^{(r+1)}, E_j^{(s)}\big] - \big[E_i^{(r)}, E_j^{(s+1)}\big] &= \tfrac{1}{2} h(\alpha_i, \alpha_j)\big(E_i^{(r)} E_j^{(s)} + E_j^{(s)} E_i^{(r)}\big),\\
\big[F_i^{(r+1)}, F_j^{(s)}\big] - \big[F_i^{(r)}, F_j^{(s+1)}\big] &= -\tfrac{1}{2} h(\alpha_i, \alpha_j)\big(F_i^{(r)} F_j^{(s)} + F_j^{(s)} F_i^{(r)}\big),
\end{aligned}$$

$$\operatorname{sym}\big[E_i^{(r_1)}, [E_i^{(r_2)}, \dots [E_i^{(r_N)}, E_j^{(s)}] \dots]\big] = 0 \quad \textit{if } i \neq j \textit{ and } N = 1 - a_{ij},$$
$$\operatorname{sym}\big[F_i^{(r_1)}, [F_i^{(r_2)}, \dots [F_i^{(r_N)}, F_j^{(s)}] \dots]\big] = 0 \quad \textit{if } i \neq j \textit{ and } N = 1 - a_{ij},$$
$$E_{\alpha_i} = E_i,$$
$$\big[E_{\hat{\alpha}}^{(r)}, E_{\check{\alpha}}^{(1)}\big] = h E_{\alpha}^{(r)},$$
$$F_{\alpha_i} = F_i,$$
$$\big[F_{\hat{\alpha}}^{(r)}, F_{\check{\alpha}}^{(1)}\big] = h F_{\alpha}^{(r)}.$$

We can repackage these generators and relations using generating series. Let

$$E_i(u) = \sum_{s=1}^{\infty} E_i^{(s)} u^{-s}, \quad H_i(u) = 1 + \sum_{s=1}^{\infty} H_i^{(s)} u^{-s}, \quad F_i(u) = \sum_{s=1}^{\infty} F_i^{(s)} u^{-s}.$$

Then the above relations can be written in series form. For example, the series version of the commutator relation between E_i and F_i is

$$[E_i(u), F_j(v)] = -\delta_{ij} \frac{h}{u - v} \big(H_i(u) - H_i(v)\big). \tag{3}$$

Remark 3.6. Note that the Drinfeld Yangian $U_h\mathfrak{g}[t]$ and our Yangian Y have natural $\mathbb{C}[h]$-forms; moreover, their $h = 1$ specializations $U_1\mathfrak{g}[t]$ and Y_1 coincide as Hopf algebras. The gradings on $U_h\mathfrak{g}[t]$ and on Y give rise to two different filtrations on Y_1. In the work of Brundan and Kleshchev [2006], these filtrations appear as the "loop filtration" and the "Kazhdan filtration", respectively.

3E. *Identification of Yangian with functions of $G_1[\![t^{-1}]\!]$.* From the results above, we can deduce that there is a perfect Hopf pairing between $U(t^{-1}\mathfrak{g}[\![t^{-1}]\!])$ and Y/hY, as per Corollary 3.4. Let us denote by Q the root lattice for $\mathfrak{g}$, let Q_+ denote the positive root cone, and let $Q_> = Q_+ \setminus \{0\}$ and $Q_< = -Q_>$.

Lemma 3.7. *The Drinfeld Yangian $U_h\mathfrak{g}[t]$, Y, and Y/hY are all Q-graded Hopf algebras* (*all tensor products being graded by total degree*). *The pairing between $U(t^{-1}\mathfrak{g}[\![t^{-1}]\!])$ and Y/hY respects this grading.*

Proof. The Hopf grading on these spaces is induced by the action of the elements $h_i^{(0)}$ (resp. $H_i^{(1)}$). In each case, coproducts preserve total degree since the coproduct is a homomorphism and the above elements are Lie algebra-like.

It is clear from Corollary 3.4 that the pairing between $U(t^{-1}\mathfrak{g}[\![t^{-1}]\!])$ and Y/hY respects the grading for pairings $\langle y, x\rangle$ when $y \in t^{-1}\mathfrak{g}[\![t^{-1}]\!]$ and $x \in Y_0$. The result follows for monomials $y_1 \dots y_k \in U(t^{-1}\mathfrak{g}[\![t^{-1}]\!])$ by induction on k. $\square$

For $\alpha \in Q$, let $Y(\alpha)$ be the corresponding component of Y/hY as per Lemma 3.7.

Proposition 3.8. *In Y/hY we have*:

$$\Delta(H_i^{(r)}) = H_i^{(r)} \otimes 1 + 1 \otimes H_i^{(r)} + \sum_{s=1}^{r-1} H_i^{(s)} \otimes H_i^{(r-s)} + \bigoplus_{\substack{\alpha+\beta=0 \\ \alpha\in Q_<, \beta\in Q_>}} Y(\alpha)\otimes Y(\beta),$$

$$\Delta(E_i^{(r)}) = E_i^{(r)} \otimes 1 + 1 \otimes E_i^{(r)} + \sum_{s=1}^{r-1} H_i^{(s)} \otimes E_i^{(r-s)} + \bigoplus_{\substack{\alpha+\beta=\alpha_i \\ \alpha\in Q_<, \beta\in Q_>}} Y(\alpha)\otimes Y(\beta),$$

$$\Delta(F_i^{(r)}) = F_i^{(r)} \otimes 1 + 1 \otimes F_i^{(r)} + \sum_{s=1}^{r-1} F_i^{(s)} \otimes H_i^{(r-s)} + \bigoplus_{\substack{\alpha+\beta=-\alpha_i \\ \alpha\in Q_<, \beta\in Q_>}} Y(\alpha)\otimes Y(\beta).$$

Proof. To begin, we recall that $\Delta(X^{(1)}) = X^{(1)} \otimes 1 + 1 \otimes X^{(1)}$ for all $x \in \mathfrak{g}$. Also, using the presentation of $U_h\mathfrak{g}[t]$ with generators x, $J(x)$ for $x \in \mathfrak{g}$ (for which the coproduct is known), a direct calculation yields

$$\Delta(H_i^{(2)}) = H_i^{(2)} \otimes 1 + 1 \otimes H_i^{(2)} + H_i^{(1)} \otimes H_i^{(1)} - \sum_{\beta\in\Phi_+} C_\beta(\beta,\alpha_i) F_\beta^{(1)} \otimes E_\beta^{(1)},$$

where $(e_\beta, f_\beta) = C_\beta^{-1}$. We prove the coproduct for $E_i^{(r)}$ by induction on r, using the identity

$$E_i^{(r+1)} = \frac{1}{(\alpha_i,\alpha_i)} \{H_i^{(2)}, E_i^{(r)}\} - H_i^{(1)} E_i^{(r)}.$$

The coproduct of the right side is expanded using the Poisson–Hopf algebra relations, the formula for $\Delta(H_i^{(2)})$, and the inductive hypothesis. The above identity is then applied again to reduce the terms in the result, and yields the form as claimed.

An analogous induction proves the case of $\Delta(F_i^{(r)})$. Finally, we take the coproduct of the identity

$$H_i^{(r)} = \{E_i^{(r)}, F_i^{(1)}\}$$

to finish the proof. □

Recall that the pairing between $U(t^{-1}\mathfrak{g}[\![t^{-1}]\!])$ and Y/hY is determined, as per Corollary 3.4, by the pairing between $t^{-1}\mathfrak{g}[\![t^{-1}]\!]$ and $\mathfrak{g}[t]$ given in Section 2F. Take an "FHE" total ordering on the generators $f_\alpha t^r$, $h_i t^r$, $e_\alpha t^r$ for $U(t^{-1}\mathfrak{g}[\![t^{-1}]\!])$. Then it is easy to see that the previous lemma and proposition completely control the pairing between $U(t^{-1}\mathfrak{g}[\![t^{-1}]\!])$ and Y/hY for the corresponding PBW basis. For example, $-F_i^{(r)}$ acts as the dual of the basis element $e_i t^{-r}$, etc.

Theorem 3.9. *There is an isomorphism $\phi : Y/hY \cong \mathcal{O}(G_1[\![t^{-1}]\!])$ of $\mathbb{N}$-graded*

Poisson–Hopf algebras such that

$$\phi(H_i(u)) = \prod_j \Delta_{\omega_j,\omega_j}(u)^{-a_{ji}},$$

$$\phi(F_i(u)) = d_i^{-1/2} \frac{\Delta_{\omega_i, s_i\omega_i}(u)}{\Delta_{\omega_i,\omega_i}(u)},$$

$$\phi(E_i(u)) = d_i^{-1/2} \frac{\Delta_{s_i\omega_i,\omega_i}(u)}{\Delta_{\omega_i,\omega_i}(u)},$$

where $\mathbb{O}(G_1[\![t^{-1}]\!])$ *is graded using the loop rotation* $\mathbb{C}^\times$ *action.*

Proof. We check explicitly that the right-hand sides act as described by the previous proposition. Let $X = (x_1 t^{r_1}) \dots (x_k t^{r_k}) \in U(t^{-1}\mathfrak{g}[\![t^{-1}]\!])$ be a basis monomial with the FHE order as chosen above. Then we have

$$\frac{\Delta_{\omega_i,s_i\omega_i}(u)}{\Delta_{\omega_i,\omega_i}(u)}(X) = -d_i^{-1/2} \frac{\partial^k}{\partial z_1 \dots \partial z_k} \frac{\langle v_{-\omega_i}, (1+z_1u^{r_1}x_1)\dots(1+z_ku^{r_k}x_k) f_i v_{\omega_i}\rangle}{\langle v_{-\omega_i}, (1+z_1u^{r_1}x_1)\dots(1+z_ku^{r_k}x_k) v_{\omega_i}\rangle}\bigg|_{z_1=\dots=z_k=0},$$

noting that $\overline{s_i} v_{\omega_i} = f_i' v_{\omega_i} = -d_i^{-1/2} f_i v_{\omega_i}$ in the generalized minor (see Section 2A). Since we have an FHE order, to get something nonzero in the right-hand numerator, x_k must be a multiple of e_i, since $e_i f_i v_{\omega_i} = h_i v_{\omega_i} = d_i v_{\omega_i}$. In this case, $z_k u^{r_k} e_i$ does not contribute to the denominator, and the remaining factors cancel, leaving

$$\frac{\Delta_{\omega_i,s_i\omega_i}(u)}{\Delta_{\omega_i,\omega_i}(u)}(X) = -d_i^{1/2} \frac{\partial^k}{\partial z_1 \dots \partial z_k} z_k u^{r_k}\bigg|_{z_1=\dots=z_k=0},$$

so X must have been $e_i t^r$ to start with. But this is precisely how $d_i^{1/2} F_i(u)$ acts on X. Similar computations hold in the two remaining cases.

To prove the equality for $H_i(u)$ one can also work in $\mathbb{O}(G_1[\![t^{-1}]\!])$, and build off the known results $E_i(u)$ and $F_i(u)$, since we must have

$$\frac{\phi(H_i(u)) - \phi(H_i(v))}{u - v} = -\{\phi(E_i(u)), \phi(F_i(v))\}.$$

We can then use formula (1) and identities for generalized minors.

The nondegeneracy of both Hopf pairings implies that ϕ is an injection. It follows that ϕ is an isomorphism from a dimension count; both Y/hY and $\mathbb{O}(G_1[\![t^{-1}]\!])$ have Hilbert series for the loop grading given by

$$\prod_{i=1}^{\infty} \frac{1}{(1-q^i)^{\dim \mathfrak{g}}}.$$

Indeed, for Y/hY this follows from the PBW theorem coming from Y, since Y is a free $\mathbb{C}[\![h]\!]$-algebra. On the other hand, the Hilbert series on $\mathbb{O}(G_1[\![t^{-1}]\!])$ is the same as the Hilbert series for $\operatorname{Sym}(t^{-1}\mathfrak{g}[\![t^{-1}]\!])$, since as $G_1[\![t^{-1}]\!]$ is pro-unipotent, we have an isomorphism of vector spaces. $\square$

3F. *Shifted Yangians.* The Yangian has a very interesting class of subalgebras: the shifted Yangians. Let μ be a dominant coweight.

We will now redefine elements

$$F_\alpha^{(s)} = \frac{1}{h}\big[F_{\hat{\alpha}}^{(s-\langle\mu^*,\check{\alpha}\rangle)}, F_{\check{\alpha}}^{(\langle\mu^*,\check{\alpha}\rangle+1)}\big], \tag{4}$$

for α a positive nonsimple root and for $s > \langle\mu^*, \alpha\rangle$. Note that these $F_\alpha^{(s)}$ depend on μ.

Definition 3.10. The *shifted Yangian* Y_μ is the subalgebra of Y generated by $E_\alpha^{(s)}$ for all α, s, $H_i^{(s)}$ for all i, s, and $F_\alpha^{(s)}$ for $s > \langle\mu^*, \alpha\rangle$.

Proposition 3.11. (1) *Monomials in the $E_\alpha^{(s)}$, $H_i^{(s)}$, $F_\alpha^{(s)}$ give a basis for Y_μ.*

(2) *The natural map $Y_\mu/hY_\mu \to Y/hY$ is injective.*

Proof. We first construct a PBW basis for Y slightly different from the one described in Section 3D. The generators $E_\alpha^{(s)}$ are defined as usual (see Section 3D). The generators $F_\alpha^{(s)}$ are given the usual definition when $s \le \langle\mu^*, \alpha\rangle$, but for $s > \langle\mu^*, \alpha\rangle$ we take definition (4). By the general remarks following Theorem 3.3, ordered monomials in generators $F_\alpha^{(s)}$, $H_i^{(s)}$, $E_\alpha^{(s)}$ are a PBW basis of Y.

Any element $x \in Y_\mu$ can be expressed as a linear combination of these PBW monomials. We now show that any monomials appearing in such an expression do not contain factors of the form $F_\alpha^{(s)}$ for $s \le \langle\mu^*, \alpha\rangle$.

By definition, x is a linear combination of (unordered) monomials in $F_\alpha^{(s)}$, $H_i^{(t)}$, $E_\alpha^{(u)}$, where $s > \langle\mu^*, \alpha\rangle$. To put x in PBW form, one has to commute these generators past each other. By definition, when $s > \langle\mu^*, \alpha\rangle$, $F_\alpha^{(s)}$ is a linear combination of monomials built from $F_i^{(t)}$, where $t > \langle\mu^*, \alpha_i\rangle$. Therefore it suffices to show that when commuting such $F_i^{(t)}$ past the other generators of Y_μ one never obtains factors of the form $F_j^{(u)}$ for $u \le \langle\mu^*, \alpha_j\rangle$. This is a direct consequence of the relations appearing in Theorem 3.5.

This proves the first statement of the theorem. The second part is a direct consequence of the first. $\square$

In the limit as $\mu \to \infty$, we then obtain Y_∞, which is the subalgebra generated by all $E_\alpha^{(s)}$, $A_i^{(s)}$. This is called the *Borel Yangian* in [Finkelberg and Rybnikov 2010].

We will now show that this shifted Yangian is a quantization of Gr_μ. Recall that $\mathbb{O}(\mathsf{Gr}_\mu)$ is embedded as a Poisson subalgebra of $\mathbb{O}(G_1[\![t^{-1}]\!])$.

Theorem 3.12. *The isomorphism ϕ restricts to an isomorphism of Poisson algebras from Y_μ/hY_μ to $\mathcal{O}(\mathsf{Gr}_\mu)$.*

Proof. First note that Y_μ/hY_μ is generated as a Poisson algebra by all $E_i^{(s)}$, $A_i^{(s)}$, and those $F_i^{(s)}$ for $i > \langle \mu^*, \alpha_i\rangle$. We note that Lemma 2.19 shows that the image of these generators under ϕ land in the subalgebra $\mathcal{O}(\mathsf{Gr}_\mu)$.

Since $\mathcal{O}(\mathsf{Gr}_\mu)$ is a Poisson subalgebra of $\mathcal{O}(G_1[\![t^{-1}]\!])$, we see that ϕ restricts to a map $Y_\mu/hY_\mu \to \mathcal{O}(G_1[\![t^{-1}]\!])$. This map is injective, since it is the restriction of an injective map. Thus, we only need to show that it is surjective, which we do by a dimension count.

Note that by Lemma 2.3, the isotropy Lie algebra of $t^{w_0\mu}$ in $G_1[\![t^{-1}]\!]$ is the finite-dimensional nilpotent Lie algebra

$$\bigoplus_{\alpha\in\Delta_+}\bigoplus_{i=1}^{-\langle w_0\mu,\alpha\rangle} t^{-i}\mathfrak{g}_\alpha.$$

As a $\mathbb{C}^*$-module, the functions on the group are identical to those on the Lie algebra by the unipotence of the stabilizer. Thus, if we let $d(k)$ be the number of roots such that $\langle w_0\mu, \alpha\rangle < k$, the Hilbert series of the functions on the stabilizer is

$$\prod_{i=1}^{\infty}\frac{1}{(1-q^i)^{d(i)}}.$$

The Hilbert series of $\mathcal{O}(G_1[\![t^{-1}]\!])^{G_1[\![t^{-1}]\!]_\mu}$ is the quotient of that of $\mathcal{O}(G_1[\![t^{-1}]\!])$ by that of functions on the stabilizer. That is, it is

$$\prod_{i=1}^{\infty}\frac{1}{(1-q^i)^{\dim\mathfrak{g}-d(i)}}.$$

On the other hand, the PBW basis for the shifted Yangian gives us the same Hilbert series for Y_μ. □

Thus the shifted Yangian Y_μ gives a quantization of Gr_μ.

Remark 3.13. We should note that it is this theorem that forces us to use the thick Grassmannian; it will fail if we take the analogue of Gr_μ in the thin affine Grassmannian, since this has "too many" functions, and will correspond to a completion of Y_μ.

3G. ***Deformation of the Yangian.*** We consider a deformation of the Yangian, which we think of as related to the Beilinson–Drinfeld Grassmannian deforming the affine Grassmannian. We consider for each node i in the Dynkin diagram an infinite sequence of parameters $r_i^{(1)}, r_i^{(2)}, \ldots \in \mathbb{C}[\![h]\!]$ and their generating series $r_i(u) = 1 + r_i^{(1)}u^{-1} + \cdots$.

Consider the algebra $Y(\boldsymbol{r})$ generated by the coefficients of $E_i(u)$, $F_i(u)$, $A_i(u)$. The relations are as in the previous section, with the relation (3) replaced by

$$(u-v)\big[E_i(u), F_i(v)\big] = -h\big(r_i(u)H_i(u) - r_i(v)H_i(v)\big), \tag{5}$$

and let $Y_\mu(\boldsymbol{r})$ be the shifted analogue of this algebra. $Y(\boldsymbol{r})$ is actually isomorphic to the trivial deformation of the Yangian via the map $H_i(u) \mapsto H_i(u)/r_i(u)$.

4. Quantization of slices

In order to quantize the slices $\mathsf{Gr}^{\overline{\lambda}}_\mu$, we will need to define a quotient of Y_μ (and its deformations $Y_\mu(\boldsymbol{r})$).

4A. ***Change of Cartan generators.*** It will be convenient for us to change the Cartan generators of Y. Following [Gerasimov et al. 2004], we define $A_i^{(s)}$ by the equation

$$H_i(u) = \frac{\displaystyle\prod_{j \neq i} \prod_{p=1}^{-a_{ji}} A_j\Big(u - \frac{h}{2}(\alpha_i + p\alpha_j, \alpha_j)\Big)}{A_i(u) A_i\Big(u - \frac{h}{2}(\alpha_i, \alpha_i)\Big)}, \tag{6}$$

where $A_i(u) = 1 + \sum_{s=1}^{\infty} A_i^{(s)} u^{-s}$.

Example 4.1. In the $G = \mathrm{SL}_2$ case, this gives $H(u) = \dfrac{1}{A(u)A(u-h)}$, and so for example we have

$$H^{(1)} = -2A^{(1)}, \qquad H^{(2)} = 3{A^{(1)}}^2 - hA^{(1)} - 2A^{(2)}.$$

Proposition 4.2 [Gerasimov et al. 2004, Lemma 2.1]. *Equation (6) uniquely determines all the $A_i^{(s)}$.*

One can think of the new generators $A_i^{(s)}$ as being related to the fundamental coweights of G, whereas the $H_i^{(s)}$ match with the simple coroots. In particular, we have the following result which follows by setting $h = 0$ in (6).

Proposition 4.3. *Let*

$$\phi : Y/hY \to \mathcal{O}(G_1[\![t^{-1}]\!])$$

be the isomorphism from Theorem 3.9. Then $\phi(A_i^{(s)}) = \Delta^{(s)}_{\omega_i,\omega_i}$.

4B. ***The GKLO representation.*** In this section, we describe certain representations via difference operators of shifted Yangians, based on [Gerasimov et al. 2004]. Fix an orientation of the Dynkin diagram; we will write $i \leftarrow j$ to denote arrows in this quiver. This will replace the ordering on the simple roots in [loc. cit.].

Fix a dominant coweight λ such that $\mu \leq \lambda$ and let $m_i = \langle \lambda - \mu, \omega_{i^*}\rangle$ and let $\lambda_i = \langle \lambda, \alpha_{i^*}\rangle$.

Define a $\mathbb{C}[\![h]\!]$-algebra D^λ_μ, with generators $z_{i,k}, \beta_{i,k}, \beta_{i,k}^{-1}$, for $i \in I$ and $1 \leq k \leq m_i$, and $(z_{i,k} - z_{i,l})^{-1}$, and relations that all generators commute except that $\beta_{i,k} z_{i,k} = (z_{i,k} + d_i h)\beta_{i,k}$.

This algebra D^λ_μ is an algebra of h-difference operators.

Proposition 4.4. *The algebra D^λ_μ is a free $\mathbb{C}[\![h]\!]$-algebra and we have an isomorphism of Poisson algebras*

$$D^\lambda_\mu / h D^\lambda_\mu \cong \mathbb{C}\big[z_{i,k}, (z_{i,k} - z_{i,l})^{-1}, \beta_{i,k}, \beta_{i,k}^{-1}\big],$$

where the right-hand side is given the Poisson structure defined by $\{\beta_{i,k}, z_{i,k}\} = d_i \beta_{i,k}$ and all other generators Poisson commute.

Proof. Obviously, we have a map

$$\mathbb{C}\big[z_{i,k}, (z_{i,k} - z_{i,l})^{-1}, \beta_{i,k}, \beta_{i,k}^{-1}\big] \to D^\lambda_\mu / h D^\lambda_\mu$$

by observing that $D^\lambda_\mu / h D^\lambda_\mu$ is commutative. From the Bergman diamond lemma, we see that the algebra D^λ_μ has a PBW basis consisting of

$$h^p \cdot \prod \beta_{i,k}^{\pm a_{i,k}} \cdot \prod z_{j,k}^{b_{j,k}} \cdot \prod_{k<\ell} (z_{i,k} - z_{i,\ell})^{e_{i,k,\ell}}$$

subject to the restriction that if $b_{j,k} \neq 0$, then k must be maximal in its equivalence class for the relation given by the transitive closure of the binary relation $k \sim \ell$ if $e_{j,k,\ell} \neq 0$. Freeness over $\mathbb{C}[\![h]\!]$ follows immediately and since the same monomials give a basis of $\mathbb{C}[\![h]\!]\big[z_{i,k}, (z_{i,k} - z_{i,l})^{-1}, \beta_{i,k}, \beta_{i,k}^{-1}\big]$, this confirms that we have the desired isomorphism. The Poisson bracket calculation follows immediately from the relations. $\square$

Fix some complex numbers $c_i^{(r)}$ for $i \in I$, $1 \leq r \leq \lambda_i$. For any variable x, consider the monic degree-λ_i polynomial whose coefficients are the numbers $c_i^{(r)}$,

$$C_i(x) = x^{\lambda_i} + c_i^{(1)} x^{\lambda_i - 1} + \cdots + c_i^{(\lambda_i)}.$$

Note that $x^{-\lambda_i} C_i(x) = 1 + c_i^{(1)} x^{-1} + \cdots + c_i^{(\lambda_i)} x^{-\lambda_i}$. We also introduce polynomials $Z_i(x) = \prod_{k=1}^{m_i} (x - z_{i,k})$ and $Z_{i,k}(x) = \prod_{\ell \neq k} (x - z_{i,\ell})$. Let $\mu_i = \langle \mu, \alpha_{i^*} \rangle$ and set $F_{\mu,i}(u) = \sum_{s=1}^\infty F_i^{(s+\mu_i)} u^{-s}$. Finally, for any $\boldsymbol{c}$ as above, define $\boldsymbol{r}$ by

$$r_i(u) = u^{-\lambda_i} C_i(u) \frac{\prod_{j \neq i} \prod_{p=1}^{-a_{ji}} \Big(1 - u^{-1}\Big(h d_i \frac{a_{ij}}{2} + h d_j p\Big)\Big)^{m_j}}{(1 - h d_i u^{-1})^{m_i}}. \tag{7}$$

We are now ready to define the *GKLO representation*:

Theorem 4.5. *There is a map of* $\mathbb{C}[\![h]\!]$*-algebras*, $\Psi^\lambda_\mu : Y_\mu(\boldsymbol{r}) \to D^\lambda_\mu$, *defined by*:

$$A_i(u) \mapsto u^{-m_i} Z_i(u),$$

$$E_i(u) \mapsto d_i^{-1/2} \sum_{k=1}^{m_i} \frac{\prod_{j \to i} \prod_{p=1}^{-a_{ji}} Z_j\Big(z_{i,k} - hd_i \frac{a_{ij}}{2} - hd_j p\Big)}{(u - z_{i,k}) Z_{i,k}(z_{i,k})} \beta_{i,k}^{-1}.$$

And $F_{\mu,i}(u)$ *maps to*

$$-d_i^{-1/2} \sum_{k=1}^{m_i} C_i(z_{i,k} + hd_i) \frac{\prod_{j \leftarrow i} \prod_{p=1}^{-a_{ji}} Z_j\Big(z_{i,k} - hd_i\Big(\frac{a_{ij}}{2} - 1\Big) - hd_j p\Big)}{(u - z_{i,k} - hd_i) Z_{i,k}(z_{i,k})} \beta_{i,k}.$$

Proof. When $\mu = 0$, this is a reformulation of Theorem 3.1(i) of [Gerasimov et al. 2004]. Suppose then that $\mu \neq 0$. Then the proof of the theorem cited applies to all the relations in Y_μ except for the commutator relation between $E_i(u)$ and $F_{\mu,i}(v)$.

In the shifted Yangian this relation takes the form

$$(u - v)\big[E_i(u), F_{\mu,i}(v)\big] = h\big(J_{\mu,i}(v) - J_{\mu,i}(u)\big), \tag{8}$$

where $J_i(v) = r_i(v) H_i(v) = \sum_{p=0}^{\infty} J_i^{(p)} v^{-p}$ and

$$J_{\mu,i}(v) = \sum_{p=1}^{\infty} J_i^{(p+\mu_i)} v^{-p}.$$

To express the left-hand side of (8), we set

$$L_i(v) = \frac{C_i(z_{i,k} + hd_i) \prod_{j \neq i} \prod_{p=1}^{-a_{ji}} Z_j\Big(z_{i,k} - hd_i\Big(\frac{a_{ij}}{2} - 1\Big) - hd_j p\Big)}{Z_{i,k}(z_{i,k} + hd_i) Z_{i,k}(z_{i,k})(v - z_{i,k} - hd_i)},$$

$$R_i(v) = \frac{C_i(z_{i,k}) \prod_{j \neq i} \prod_{p=1}^{-a_{ji}} Z_j\Big(z_{i,k} - hd_i \frac{a_{ij}}{2} - hd_j p\Big)}{Z_{i,k}(z_{i,k} - hd_i) Z_{i,k}(z_{i,k})(v - z_{i,k})}.$$

Then the left-hand side of (8) is equal to

$$d_i^{-1} \sum_{k=1}^{m_i} \big(L_i(v) - R_i(v)\big) - \big(L_i(u) - R_i(u)\big).$$

Note that we expressed this sum as a "v-part" minus a "u-part".

Now we consider the right-hand side of (8). Note that

$$\lambda_i = \mu_i + 2m_i + \sum_{j \leftrightarrow i} a_{ji} m_j.$$

Therefore,

$$r_i(u) = u^{-\mu_i} \frac{C_i(u) \prod_{j \neq i} \prod_{p=1}^{-a_{ji}} \left(u - hd_i \frac{a_{ij}}{2} - hd_j p\right)^{m_j}}{u^{m_i}(u - hd_i)^{m_i}}.$$

Now

$$H_i(u) \mapsto \frac{u^{m_i}(u - hd_i)^{m_i}}{\prod_{j \neq i} \prod_{p=1}^{-a_{ji}} \left(u - hd_i \frac{a_{ij}}{2} - hd_j p\right)^{m_j}} \frac{\prod_{j \neq i} \prod_{p=1}^{-a_{ji}} Z_j\left(u - hd_i \frac{a_{ij}}{2} - hd_j p\right)}{Z_i(u) Z_i(u - hd_i)},$$

and hence

$$r_i(u) H_i(u) \mapsto u^{-\mu_i} C_i(u) \frac{\prod_{j \neq i} \prod_{p=1}^{-a_{ji}} Z_j\left(u - hd_i \frac{a_{ij}}{2} - hd_j p\right)}{Z_i(u) Z_i(u - hd_i)}.$$

Therefore

$$C_i(u) \frac{\prod_{j \neq i} \prod_{p=1}^{-a_{ji}} Z_j\left(u - hd_i \frac{a_{ij}}{2} - hd_j p\right)}{Z_i(u) Z_i(u - hd_i)} = \sum_{p=0}^{\infty} J_i^{(p)} u^{\mu_i - p}.$$

On the other hand,

$$J_{\mu,i}(u) = \sum_{p=\mu_i+1}^{\infty} J_i^{(p)} u^{\mu_i - p},$$

showing that $J_{\mu,i}(u)$ is a truncation of

$$C_i(u) \frac{\prod_{j \neq i} \prod_{p=1}^{-a_{ji}} Z_j\left(u - hd_i \frac{a_{ij}}{2} - hd_j p\right)}{Z_i(u) Z_i(u - hd_i)}.$$

More precisely, for $r = 1, 2, \ldots,$

$$h J_{\mu,i}(u)\big|_{u^{-r}} = h C_i(u) \frac{\prod_{j \neq i} \prod_{p=1}^{-a_{ji}} Z_j\left(u - hd_i \frac{a_{ij}}{2} - hd_j p\right)}{Z_i(u) Z_i(u - hd_i)}\bigg|_{u^{-r}}.$$

Using partial fractions, we have that $\dfrac{h}{Z_i(u)Z_i(u-hd_i)}$ equals

$$\sum_{k=1}^{m_i} \frac{1}{Z_{ik}(z_{ik})Z_{ik}(z_{ik}+hd_i)(u-z_{ik}-hd_i)} - \frac{1}{Z_{ik}(z_{ik})Z_{ik}(z_{ik}-hd_i)(u-z_{ik})}.$$

Therefore for $r = 1, 2, \dots$, the u^{-r}-coefficient of $hJ_{\mu,i}(u)$ is equal to the u^{-r}-coefficient of

$$\sum_{k=1}^{m_i} \frac{C_i(u) \prod_{j\neq i} \prod_{p=1}^{-a_{ji}} Z_j\Big(u - hd_i\frac{a_{ij}}{2} - hd_j p\Big)}{Z_{ik}(z_{ik})Z_{ik}(z_{ik}+hd_i)(u-z_{ik}-hd_i)} - \frac{C_i(u) \prod_{j\neq i} \prod_{p=1}^{-a_{ji}} Z_j\Big(u - hd_i\frac{a_{ij}}{2} - hd_j p\Big)}{Z_{ik}(z_{ik})Z_{ik}(z_{ik}-hd_i)(u-z_{ik})}.$$

Now observe that for any polynomial $p(u)$ and for $r = 1, 2, \dots$,

$$\frac{p(u)}{u-z}\Big|_{u^{-r}} = \frac{p(z)}{u-z}\Big|_{u^{-r}}.$$

Therefore for $r = 1, 2, \dots$, the u^{-r}-coefficient of $hu^{\mu_i} J_{\mu,i}(u)$ is equal to the u^{-r}-coefficient of $\sum_{k=1}^{m_i} L_i(u) - R_i(u)$, proving (8). □

Example 4.6. If $\mathfrak{g} = \mathfrak{sl}_2$ and $\lambda = \alpha^\vee$, $\mu = 0$, then the formulas above simplify considerably. In this case,

$$A(u) \mapsto 1 - zu^{-1}, \quad E(u) \mapsto \frac{1}{u-z}\beta^{-1},$$

and $F(u) \mapsto -\big((z+h)^2 + c^{(1)}(z+h) + c^{(2)}\big)\dfrac{1}{u-z-h}\beta$. In particular,

$$H^{(1)} \mapsto 2z, \quad E^{(1)} \mapsto \beta^{-1}, \quad F^{(1)} \mapsto -\big((z+h)^2 + c^{(1)}(z+h) + c^{(2)}\big)\beta.$$

Restrict this representation to the copy of $\mathfrak{sl}_2$ generated by $E^{(1)}$, $H^{(1)}+c^{(1)}+h$, $F^{(1)}$, and consider these as difference operators acting on the polynomial ring $\mathbb{C}[z]$. (More precisely, these act on $\mathbb{C}[\![h]\!][z]$, but one can specialize h to 1.) This is a standard Whittaker module for $\mathfrak{sl}_2$ with generic nilpotent character.

Remark 4.7. We can define a $\mathbb{Z}$-grading on D^λ_μ by setting

$$\deg h = 1, \quad \deg z_{i,k} = 1, \quad \deg \beta_{i,k} = m_i + \sum_{i\to j} a_{ij}m_j + \lambda_i - \mu_i.$$

With this definition, the GKLO representation preserves grading.

4C. ***Quantization of the slices*** $\overline{\mathsf{Gr}^{\lambda}_{\mu}}$**.** For any $\boldsymbol{c}$ as above, let $Y^{\lambda}_{\mu}(\boldsymbol{c})$ be the image of $Y_{\mu}(\boldsymbol{r})$ in D^{λ}_{μ} under the GKLO representation Ψ^{λ}_{μ} and let $I^{\lambda}_{\mu}(\boldsymbol{c})$ denote the kernel of Ψ^{λ}_{μ} (here $\boldsymbol{r}$ is determined from $\boldsymbol{c}$ by (7)).

Note that $Y^{\lambda}_{\mu}(\boldsymbol{c})$ is free as a $\mathbb{C}[\![h]\!]$-algebra since it is a subalgebra of D^{λ}_{μ}, a free $\mathbb{C}[\![h]\!]$-algebra.

We have the isomorphism $Y_{\mu}(\boldsymbol{c}) \to Y_{\mu}$ from Section 3G and thus we get an isomorphism of Poisson algebras $Y_{\mu}(\boldsymbol{c})/hY_{\mu}(\boldsymbol{c}) \to \mathbb{O}(\mathsf{Gr}_{\mu})$ from Theorem 3.12. On the other hand, because $Y^{\lambda}_{\mu}(\boldsymbol{c})$ is free as a $\mathbb{C}[\![h]\!]$-algebra, we get a surjection of Poisson algebras $Y_{\mu}(\boldsymbol{c})/hY_{\mu}(\boldsymbol{c}) \to Y^{\lambda}_{\mu}(\boldsymbol{c})/hY^{\lambda}_{\mu}(\boldsymbol{c})$.

We will now establish the following theorem, which shows that Y^{λ}_{μ} is a quantization of scheme supported on $\overline{\mathsf{Gr}^{\lambda}_{\mu}}$.

Theorem 4.8. *There is a surjective map of Poisson algebras $Y^{\lambda}_{\mu}(\boldsymbol{c})/hY^{\lambda}_{\mu}(\boldsymbol{c}) \to \mathbb{O}(\overline{\mathsf{Gr}^{\lambda}_{\mu}})$ which is an isomorphism modulo the nilradical of the left-hand side.*

Remark 4.9. Consider the map

$$Y^{\lambda}_{\mu}(\boldsymbol{c})/hY^{\lambda}_{\mu}(\boldsymbol{c}) \to \mathbb{C}\big[z_{i,k}, (z_{i,k}-z_{i,l})^{-1}, \beta_{i,k}, \beta_{i,k}^{-1}\big]$$

obtained by reducing the GKLO representation mod h. If we knew that this map was injective, then we would know that $Y^{\lambda}_{\mu}(\boldsymbol{c})/hY^{\lambda}_{\mu}(\boldsymbol{c})$ was reduced and that the map from Theorem 4.8 was an isomorphism. We will in fact make a stronger conjecture.

If Conjecture 2.20 holds, then we can strengthen Theorem 4.8 as follows.

Theorem 4.10. *If Conjecture 2.20 holds, then*:

(1) *There is an isomorphism of Poisson algebras $Y^{\lambda}_{\mu}(\boldsymbol{c})/hY^{\lambda}_{\mu}(\boldsymbol{c}) \to \mathbb{O}(\overline{\mathsf{Gr}^{\lambda}_{\mu}})$.*

(2) *$Y^{\lambda}_{\mu}(\boldsymbol{c})$ is the quotient of $Y_{\mu}(\boldsymbol{c})$ by the 2-sided ideal generated by $A_i^{(s)}$ for $s > m_i, i \in I$.*

Proof of Theorem 4.8. Via the isomorphism $Y_{\mu}(\boldsymbol{c})/hY_{\mu}(\boldsymbol{c}) \to \mathbb{O}(\mathsf{Gr}_{\mu})$, we can regard $Y^{\lambda}_{\mu}(\boldsymbol{c})/hY^{\lambda}_{\mu}(\boldsymbol{c})$ as a quotient of $\mathbb{O}(\mathsf{Gr}_{\mu})$ by an ideal, which we denote by I_2.

First, note that $\Psi^{\lambda}_{\mu}(A_i^{(s)}) = 0$ for $i \in I$, $s > m_i$, and thus $\Delta^{(s)}_{\omega_i,\omega_i} \in I_2$ for $i \in I$ and $s > m_i$. Since I_2 is a Poisson ideal, we see that $J^{\lambda}_{\mu} \subset I_2$.

By Proposition 2.21, we see that the vanishing locus of J^{λ}_{μ} is $\overline{\mathsf{Gr}^{\lambda}_{\mu}}$, and thus the vanishing locus of I_2 is contained in $\overline{\mathsf{Gr}^{\lambda}_{\mu}}$. Thus it suffices to show that the vanishing locus of I_2 is not strictly contained in $\overline{\mathsf{Gr}^{\lambda}_{\mu}}$.

Since I_2 is a Poisson ideal, we see that $V(I_2)$ is a Poisson subvariety of $\overline{\mathsf{Gr}^{\lambda}_{\mu}}$ and thus is the union of $\overline{\mathsf{Gr}^{\nu}_{\mu}}$, for $\nu \leq \lambda$. Suppose that we have

$$V(I_2) = \bigcup_j \overline{\mathsf{Gr}^{\nu_j}_{\mu}}$$

for $\nu_j < \lambda$. For each j, there exists i such that $\langle \nu_j - \mu, \omega_{i^*}\rangle < \langle \lambda - \mu, \omega_{i^*}\rangle = m_i$. Thus applying Proposition 2.4, $\prod_i \Delta^{(m_i)}_{\omega_i,\omega_i}$ vanishes on $\bigcup_j \mathsf{Gr}^{\bar{\nu}_j}_\mu$. Hence for some k, we have $\big(\prod_i \Delta^{(m_i)}_{\omega_i,\omega_i}\big)^k \in I_2$.

On the other hand, we see that under the GKLO representation

$$\Psi^\lambda_\mu(A_i^{(m_i)}) = (-1)^{m_i} z_{i,1} \dots z_{i,m_i},$$

and thus under the map

$$\mathbb{O}(\mathsf{Gr}_\mu) \cong Y_\mu(\boldsymbol{c})/hY_\mu(\boldsymbol{c}) \to D^\lambda_\mu / hD^\lambda_\mu \cong \mathbb{C}\big[z_{i,k}, (z_{i,k} - z_{i,l})^{-1}, \beta_{i,k}, \beta_{i,k}^{-1}\big],$$

$\big(\prod_i \Delta^{(m_i)}_{\omega_i,\omega_i}\big)^k$ is mapped to a monomial in the $z_{i,k}$. In particular, this shows that $\big(\prod_i \Delta^{(m_i)}_{\omega_i,\omega_i}\big)^k$ does not lie in I_2, contradicting the previous paragraph.

Thus we conclude that $V(I_2) = \mathsf{Gr}^\lambda_\mu$ as desired. □

Proof of Theorem 4.10. Suppose I_1 is the ideal of $\mathsf{Gr}^{\bar{\lambda}}_\mu$ in $\mathbb{O}(\mathsf{Gr}_\mu)$.

Let K be the ideal in $Y_\mu(\boldsymbol{c})$ generated by $A_i^{(s)}$ for $s > m_i$, $i \in I$. Then we have an inclusion $K \subset I^\lambda_\mu(\boldsymbol{c})$ and a resulting map

$$K/hK \to I^\lambda_\mu(\boldsymbol{c})/hI^\lambda_\mu(\boldsymbol{c}) = I_2$$

which may not be injective. Let I_3 denote the image of this map. From the definitions, we see that $I_3 \subset I_2$. Moreover, we have that $J^\lambda_\mu \subset I_3$, since I_3 is a Poisson ideal and it contains the generators of I_3.

In the previous proof we showed that $I_2 \subset I_1$. Thus we have a chain of inclusions $J^\lambda_\mu \subset I_3 \subset I_2 \subset I_1$. On the other hand, Conjecture 2.20 shows us that $I_1 = J^\lambda_\mu$.

Hence we conclude that $I_1 = I_2 = I_3 = J^\lambda_\mu$. So the first assertion holds.

For the second assertion, note that $I_3 = I_2$ implies that $K/hK \to I^\lambda_\mu(\boldsymbol{c})/hI^\lambda_\mu(\boldsymbol{c})$ is surjective. Let $L = I^\lambda_\mu(\boldsymbol{c})/K$. The long exact sequence for $\otimes_{\mathbb{C}[\![h]\!]}\mathbb{C}$ gives

$$K/hK \to I^\lambda_\mu(\boldsymbol{c})/hI^\lambda_\mu(\boldsymbol{c}) \to L/hL \to 0,$$

and thus $L/hL = 0$. By Nakayama's lemma, we conclude that $L = 0$, and thus $K = I^\lambda_\mu(\boldsymbol{c})$ as desired. □

4D. ***Universality of the quantization.*** There is already a rich literature on the theory of deformation quantizations of symplectic varieties. The most relevant work for us is [Bezrukavnikov and Kaledin 2004], showing the existence and uniqueness of deformation quantizations of symplectic resolutions. This theory can be applied directly to a smooth convolution variety $\mathsf{Gr}^{\overline{\vec{\lambda}}}_\mu$. Moreover, as noted by Braden, Proudfoot and Webster [Braden et al. 2012, 3.4], it can be extended in a very straightforward way to the nonsmooth case $\mathsf{Gr}^{\overline{\vec{\lambda}}}_\mu$, since we know that $\mathsf{Gr}^{\overline{\vec{\lambda}}}_\mu$ is a terminalization (Theorem 2.7).

This shows that the variety $\mathsf{Gr}^{\overline{\lambda}}_{\mu}$ has a canonical family of quantizations which extend to a deformation quantization sheaf on $\mathsf{Gr}^{\overline{\vec{\lambda}}}_{\mu}$. The base of this family is the same as the base for the universal deformation of $\mathsf{Gr}^{\overline{\lambda}}_{\mu}$ as a symplectic singularity (as constructed by Kaledin and Verbitsky [2002] or Namikawa [2011]). By [Namikawa 2010, 1.1], this base $\mathbb{B}$ is an affine space modulo the action of a finite group. This group can be described by looking at the codimension-2 strata of the product of $\mathsf{Gr}^{\overline{\lambda}}_{\mu}$, which are $\mathsf{Gr}^{\lambda-\alpha_i}_{\mu}$, and taking the product of the Weyl groups attached to them by the McKay correspondence, which (using Example 2.2) in our case results in the symmetric groups $S_{\lambda,\mu} = \prod_{i:m_i>0} S_{\lambda_i}$. Here we use the fact that these strata are simply connected.

For the remainder of this section, let us regard the complex numbers $r_i^{(s)}$ and $c_i^{(s)}$ as variables and let $\tilde{Y}_\mu$ be the $\mathbb{C}[r_i^{(s)}]$-algebra which recovers the old $Y_\mu(\boldsymbol{r})$ upon specializing the variables. Let

$$\tilde{Y}^\lambda_\mu = \tilde{Y}_\mu \otimes_{\mathbb{C}[r_i^{(s)}]} \mathbb{C}[c_i^{(s)}] \big/ \big(\big\{A_i^{(s)} \mid s > m_i\big\}\big)$$

(here we use a map $\mathbb{C}[r_i^{(s)}] \to \mathbb{C}[c_i^{(s)}]$ given by (7)). If Conjecture 2.20 (and hence Theorem 4.10) holds, then $\tilde{Y}^\lambda_\mu$ can be specialized (via a map $\mathbb{C}[c_i^{(s)}] \to \mathbb{C}$) to each of the $Y^\lambda_\mu(\boldsymbol{c})$. We conjecture that $\tilde{Y}^\lambda_\mu$ is related to the above universal quantization as follows.

First note that the BD analogue $\mathsf{Gr}^{\overline{\vec{\lambda}}}_{\mu;\mathbb{A}^{\rho(\lambda)}}$ is a symplectic deformation of $\mathsf{Gr}^{\overline{\lambda}}_{\mu}$ over the base $\mathbb{A}^{\rho(\lambda)}$, and thus is the pull-back of the universal deformation by a map $b : \mathbb{A}^{\rho(\lambda)} \to \mathbb{B}$.

Conjecture 4.11. (1) *The map $b : \mathbb{A}^{\rho\lambda} \to \mathbb{B}$ descends to a surjective map $\tilde{b} : \mathbb{A}^{\rho\lambda}/S_{\lambda,\mu} \to \mathbb{B}$.*

(2) *The algebra $\tilde{Y}^\lambda_\mu$ is the base change along $\tilde{b}$ of the universal, Bezrukavnikov–Kaledin-type quantization.*

Example 4.12. We continue Example 4.6, so $G = \mathrm{SL}_2$ and $\lambda = \alpha^\vee$, $\mu = 0$. Note that in Y^λ_μ, we have that $E^{(s)} = (-A^{(1)})^{s-1} E^{(1)}$, and $F^{(s)} = F^{(1)}(-A^{(1)})^{s-1}$, and so Y^λ_μ is generated by $E^{(1)}$ and $F^{(1)}$.

Let $U_h\mathfrak{sl}_2$ denote the h-version of the universal enveloping algebra of $\mathfrak{sl}_2$. Let $C = EF + FE + \frac{1}{2}H^2$ be its Casimir element. For any complex number c, let Z_c denote the ideal in $U_h\mathfrak{sl}_2$ generated by the central element $C - c$. Standard results give that $U_h\mathfrak{sl}_2/Z_c$ is a quantization of the nilpotent cone of $\mathfrak{sl}_2$, which is isomorphic as a Poisson variety to $\mathsf{Gr}^{\overline{\lambda}}_{\mu}$.

The map

$$E^{(1)} \mapsto E, \quad H^{(1)} \mapsto H + c^{(1)} + h, \quad F^{(1)} \mapsto F$$

defines an isomorphism $Y^\lambda_\mu \cong U_h\mathfrak{sl}_2/Z_c$, where $c = 2c^{(2)} - \frac{1}{2}(c^{(1)})^2 + \frac{1}{2}h^2$. If we don't specialize, then the same formulas combined with the assignment

$$c^{(2)} \mapsto -\tfrac{1}{2}C + \tfrac{1}{4}(c^{(1)})^2 - \tfrac{1}{4}h^2$$

give an isomorphism

$$\tilde{Y}^2_0 \cong U_h(\mathfrak{sl}_2)[c^{(1)}].$$

In this example, $U_h(\mathfrak{sl}_2)$ is the universal quantization and $c^{(1)}$ a trivial deformation parameter. The universal family is

$$\mathfrak{sl}_2 \xrightarrow{\operatorname{tr}(a^2)} \mathbb{C}.$$

Since the fiber of the BD analogue over $(x, y) \in \mathbb{A}^2$ can be identified with matrices with eigenvalues x and y, the map b is just $b(x, y) = \frac{1}{4}(x - y)^2$. Thus, choosing $x + y$ and $(x - y)^2$ as generators of symmetric functions, $\tilde{b}$ is just the projection map $\mathbb{A}^2 \to \mathbb{A}^1$.

The sum of the $c_i^{(1)}$ is always a trivial deformation parameter; usually this is the only such parameter, but there are degenerate cases where other parameters can be trivialized as well (for example, if $\lambda = \mu$).

4E. ***Quantization of Zastava spaces.*** Here we assume that Conjecture 2.20 holds, and thus we will assume the conclusions of Theorem 4.10.

Let us fix ν in the positive coroot cone. Choose some μ_0 such that $\mu_0 + \nu$ is dominant. Let $\boldsymbol{c}$ be a collection of complex numbers as above and consider $Y^{\mu_0+\nu}_{\mu_0}(\boldsymbol{c})$.

Now for any dominant μ with $\mu \geq \mu_0$, we extend $\boldsymbol{c}$ by 0 and (slightly abusing notation) consider $Y^{\mu+\nu}_{\mu}(\boldsymbol{c})$. Since the generators of $Y^{\mu+\nu}_{\mu}(\boldsymbol{c})$ are a subset of the generators of $Y^{\mu_0+\nu}_{\mu_0}(\boldsymbol{c})$ and the relations are the same, we obtain a map $Y^{\mu+\nu}_{\mu}(\boldsymbol{c}) \to Y^{\mu_0+\nu}_{\mu_0}(\boldsymbol{c})$. It is easy to see that this map is an isomorphism on the N-th filtered piece if $\langle \mu, \alpha_i \rangle \geq N$ for all i.

Thus this system stabilizes to the algebra $Y^{\infty+\nu}_{\infty}$, which is the quotient of the Borel Yangian Y_∞ by the 2-sided ideal generated by $A_i^{(s)}$ for $s > \langle \nu, \alpha_i \rangle$; perhaps surprisingly, this limit doesn't depend on $\boldsymbol{c}$ or our starting μ_0.

Combining Theorem 4.10 with Theorem 2.10, we obtain the following (dependent on Conjecture 2.20), which was conjectured in [Finkelberg and Rybnikov 2010] for $G = \mathrm{SL}_n$ (and proven for $G = \mathrm{SL}_2$).

Theorem 4.13. *$Y^{\infty+\nu}_{\infty}/hY^{\infty+\nu}_{\infty}$ is isomorphic to the Poisson algebra $\mathbb{O}(Z_\nu)$.*

Remark 4.14. As mentioned above, the GKLO representation gives rise to a map of graded Poisson algebras

$$Y^\lambda_\mu(\boldsymbol{c})/hY^\lambda_\mu(\boldsymbol{c}) \to D^\lambda_\mu(\boldsymbol{c})/hD^\lambda_\mu(\boldsymbol{c})$$

(which we expect is an inclusion) and thus to a $\mathbb{C}^\times$-equivariant map of Poisson varieties

$$\prod_i (\mathbb{C}^{m_i} \smallsetminus \Delta) \times (\mathbb{C}^\times)^{m_i} \to \mathsf{Gr}^\lambda_\mu,$$

which we expect to be étale.

If we then compose with the map $Gr^\lambda_\mu \to Z_{\lambda-\mu}$, we obtain $\prod_i (\mathbb{C}^{m_i} \smallsetminus \Delta) \to Z_{\lambda-\mu}$, which was studied in [Gerasimov et al. 2004].

Acknowledgements

We would like to thank Alexander Braverman, Pavel Etingof, Mikhail Finkelberg, Ivan Mirković, Sergey Oblezin, Travis Schedler and Catharina Stroppel for extremely useful conversations. We also thank the referees for their careful reading of this paper.

References

[Beauville 2000] A. Beauville, "Symplectic singularities", *Invent. Math.* **139**:3 (2000), 541–549. MR 2001f:14008 Zbl 0958.14001

[Beilinson et al. 1996] A. Beilinson, V. Ginzburg, and W. Soergel, "Koszul duality patterns in representation theory", *J. Amer. Math. Soc.* **9**:2 (1996), 473–527. MR 96k:17010 Zbl 0864.17006

[Bezrukavnikov and Kaledin 2004] R. Bezrukavnikov and D. Kaledin, "Fedosov quantization in algebraic context", *Mosc. Math. J.* **4**:3 (2004), 559–592, 782. MR 2006j:53130 Zbl 1074.14014

[Braden et al. 2012] T. Braden, N. Proudfoot, and B. Webster, "Quantizations of conical symplectic resolutions, I: Local and global structure", preprint, 2012. arXiv 1208.3863

[Braden et al. ≥ 2014] T. Braden, A. Licata, N. Proudfoot, and B. Webster, "Quantizations of conical symplectic resolutions, II: Category $\mathcal{O}$", in preparation.

[Braverman and Finkelberg 2011] A. Braverman and M. Finkelberg, "Semi-infinite Schubert varieties and quantum K-theory of flag manifolds", preprint, 2011. arXiv 1111.2266

[Brundan and Kleshchev 2006] J. Brundan and A. Kleshchev, "Shifted Yangians and finite W-algebras", *Adv. Math.* **200**:1 (2006), 136–195. MR 2006m:17010 Zbl 1083.17006

[Brundan and Kleshchev 2008] J. Brundan and A. Kleshchev, "Representations of shifted Yangians and finite W-algebras", *Mem. Amer. Math. Soc.* **196**:918 (2008), viii+107. MR 2009i:17020 Zbl 1169.17009

[Drinfeld 1987] V. G. Drinfeld, "Quantum groups", pp. 798–820 in *Proceedings of the International Congress of Mathematicians* (Berkeley, CA), vol. 1–2, edited by A. M. Gleason, Amer. Math. Soc., Providence, RI, 1987. MR 89f:17017 Zbl 0667.16003

[Drinfeld 1993] V. G. Drinfeld, "On Poisson homogeneous spaces of Poisson–Lie groups", *Teoret. Mat. Fiz.* **95**:2 (1993), 226–227. In Russian; translated in *Theoret. and Math. Phys.* **95**:2 (1993), 524–535. MR 94k:58045 Zbl 0852.22018

[Etingof and Kazhdan 1998] P. Etingof and D. Kazhdan, "Quantization of Lie bialgebras, III", *Selecta Math.* (*N.S.*) **4**:2 (1998), 233–269. MR 2000i:17033 Zbl 0915.17009

[Evens and Mirković 1999] S. Evens and I. Mirković, "Characteristic cycles for the loop Grassmannian and nilpotent orbits", *Duke Math. J.* **97**:1 (1999), 109–126. MR 2000h:22017 Zbl 1160.22306

[Finkelberg and Mirković 1999] M. Finkelberg and I. Mirković, "Semi-infinite flags, I: Case of global curve $\boldsymbol{P}^1$", pp. 81–112 in *Differential topology, infinite-dimensional Lie algebras, and applications*, edited by A. Astashkevich and S. Tabachnikov, Amer. Math. Soc. Transl. Ser. 2 **194**, Amer. Math. Soc., Providence, RI, 1999. MR 2001j:14029 Zbl 1076.14512

[Finkelberg and Rybnikov 2010] M. Finkelberg and L. Rybnikov, "Quantization of Drinfeld Zastava", preprint, 2010. arXiv 1009.0676

[Finkelberg et al. 1999] M. Finkelberg, A. Kuznetsov, N. Markarian, and I. Mirković, "A note on a symplectic structure on the space of G-monopoles", *Comm. Math. Phys.* **201**:2 (1999), 411–421. MR 2000g:53095 Zbl 0981.53083

[Gavarini 2002] F. Gavarini, "The quantum duality principle", *Ann. Inst. Fourier* (*Grenoble*) **52**:3 (2002), 809–834. MR 2003d:17016 Zbl 1054.17011

[Gavarini 2007] F. Gavarini, "The global quantum duality principle", *J. Reine Angew. Math.* **612** (2007), 17–33. MR 2008k:17015 Zbl 1204.17010

[Gerasimov et al. 2004] A. Gerasimov, S. Kharchev, D. Lebedev, and S. Oblezin, "On a class of representations of the Yangian and moduli space of monopoles", preprint, 2004. arXiv math/0409031

[Ginzburg 1995] V. Ginzburg, "Perverse sheaves on a loop group and Langlands duality", preprint, 1995. arXiv alg-geom/9511007

[Kaledin and Verbitsky 2002] D. Kaledin and M. Verbitsky, "Period map for non-compact holomorphically symplectic manifolds", *Geom. Funct. Anal.* **12**:6 (2002), 1265–1295. MR 2004e:32011 Zbl 1032.58009

[Levendorskii 1993] S. Z. Levendorskii, "On PBW bases for Yangians", *Lett. Math. Phys.* **27**:1 (1993), 37–42. MR 94b:17027 Zbl 0781.17004

[Losev 2012] I. Losev, "Isomorphisms of quantizations via quantization of resolutions", *Adv. Math.* **231**:3-4 (2012), 1216–1270. MR 2964603 Zbl 06094077

[Lu and Yakimov 2008] J.-H. Lu and M. Yakimov, "Group orbits and regular partitions of Poisson manifolds", *Comm. Math. Phys.* **283**:3 (2008), 729–748. MR 2009i:53084 Zbl 1153.53059

[Lusztig 1981] G. Lusztig, "Green polynomials and singularities of unipotent classes", *Adv. in Math.* **42**:2 (1981), 169–178. MR 83c:20059 Zbl 0473.20029

[Lusztig 1983] G. Lusztig, "Singularities, character formulas, and a q-analog of weight multiplicities", pp. 208–229 in *Analysis and topology on singular spaces, II, III* (Luminy, 1981), Astérisque **101**, Soc. Math. France, Paris, 1983. MR 85m:17005 Zbl 0561.22013

[Mirković and Vilonen 2007] I. Mirković and K. Vilonen, "Geometric Langlands duality and representations of algebraic groups over commutative rings", *Ann. of Math.* (2) **166**:1 (2007), 95–143. MR 2008m:22027 Zbl 1138.22013

[Mirković and Vybornov 2007] I. Mirković and M. Vybornov, "Quiver varieties and Beilinson–Drinfeld Grassmannians of type A", preprint, 2007. arXiv 0712.4160

[Namikawa 2001] Y. Namikawa, "A note on symplectic singularities", preprint, 2001. arXiv math/0101028

[Namikawa 2010] Y. Namikawa, "Poisson deformations of affine symplectic varieties, II", *Kyoto J. Math.* **50**:4 (2010), 727–752. MR 2012b:14067 Zbl 1211.14040

[Namikawa 2011] Y. Namikawa, "Poisson deformations of affine symplectic varieties", *Duke Math. J.* **156**:1 (2011), 51–85. MR 2012a:14023 Zbl 1208.14028

[Richardson 1992] R. W. Richardson, "Intersections of double cosets in algebraic groups", *Indag. Math.* (*N.S.*) **3**:1 (1992), 69–77. MR 93b:20081 Zbl 0833.22001

[Weyman 1989] J. Weyman, "The equations of conjugacy classes of nilpotent matrices", *Invent. Math.* **98**:2 (1989), 229–245. MR 91g:20070 Zbl 0717.20033

Communicated by Edward Frenkel
Received 2013-01-10 Revised 2013-08-02 Accepted 2013-08-31

jkamnitz@math.toronto.edu *Department of Mathematics, University of Toronto, 40 St. George Street, Toronto, ON M5S 2E4, Canada*

bwebster@virginia.edu *Department of Mathematics, University of Virginia, 141 Cabell Drive, Charlottesville, VA 22904, United States*

alex.weekes@utoronto.ca *Department of Mathematics, University of Toronto, 40 St. George Street, Toronto, ON M5S 2E4, Canada*

oded.yacobi@sydney.edu.au *School of Mathematics and Statistics, University of Sydney, NSW 2006, Australia*

ALGEBRA AND NUMBER THEORY 8:4 (2014)
dx.doi.org/10.2140/ant.2014.8.895

Equidistribution of values of linear forms on quadratic surfaces

Oliver Sargent

In this paper, we investigate the distribution of the set of values of a linear map at integer points on a quadratic surface. In particular, it is shown that, subject to certain algebraic conditions, this set is equidistributed. This can be thought of as a quantitative version of the main result from a previous paper. The methods used are based on those developed by A. Eskin, S. Mozes and G. Margulis. Specifically, they rely on equidistribution properties of unipotent flows.

1. Introduction

Consider the following situation. Let X be a rational surface in $\mathbb{R}^d$, R be a fixed region in $\mathbb{R}^s$ and $F : X \to \mathbb{R}^s$ be a polynomial map. An interesting problem is to investigate the size of the set

$$Z = \{x \in X \cap \mathbb{Z}^d : F(x) \in R\}$$

consisting of integer points in X such that the corresponding values of F are in R. Suppose that the set of values of F at the integer points of X is dense in $\mathbb{R}^s$. In this case, the set Z will be infinite. However, the set

$$Z_T = \{x \in X \cap \mathbb{Z}^d : F(x) \in R,\ \|x\| \leq T\}$$

can be considered. This set will be finite, and its size will depend on T. Typically, the density assumption indicates that the set Z might be equidistributed within the set of all integer points in X. Namely, as T increases, the size of the set Z_T should be proportional to the appropriately defined volume of the set

$$\{x \in X : F(x) \in R,\ \|x\| \leq T\}$$

consisting of real points on X with values in R and bounded norm. Such a result, if it is obtained, can be seen as quantifying the denseness of the values of F at integral points.

MSC2010: primary 11E99; secondary 37A17, 37A45.
Keywords: quadratic forms, linear maps, integral values, unipotent flows.

The situation described above is too general, but it serves as motivation for what is to come. So far, what is proved is limited to special cases. For instance, when $M : \mathbb{R}^d \to \mathbb{R}^s$ is a linear map, classical methods can be used to establish necessary and sufficient conditions that ensure the values of M on $\mathbb{Z}^d$ are dense in $\mathbb{R}^s$. The equidistribution problem described above can also be considered in this case. It is straightforward to obtain an asymptotic estimate for the number of integer points with bounded norm whose values lie in some compact region of $\mathbb{R}^s$ [Cassels 1972].

When $Q : \mathbb{R}^d \to \mathbb{R}$ is a quadratic form, the situation is that of the Oppenheim conjecture. Margulis [1989] obtained necessary and sufficient conditions to ensure that the values of Q on $\mathbb{Z}^d$ are dense in $\mathbb{R}$. Considerable work has gone into the equidistribution problem in this case, first by Dani and Margulis [1993], who obtained an asymptotic lower bound for the number of integers with bounded height such that their images lie in a fixed interval. Later, Eskin, Margulis and Mozes [Eskin et al. 1998] gave the corresponding asymptotic upper bound for the same problem. The major ingredient, used in the proof of Oppenheim conjecture, is to relate the density of the values of a quadratic form at integers to the density of certain orbits inside a homogeneous space. This connection was first noted by M. S. Raghunathan in the late 1970s (appearing in print in [Dani 1981], for instance). It is, in this way, using tools from dynamical systems to study the orbit closures of subgroups corresponding to quadratic forms, that Margulis proved the Oppenheim conjecture. Similarly, the later refinement, due to Dani and Margulis [1990], who considered the values of quadratic forms at primitive integral points, and work on the equidistribution (quantitative) problem by Dani and Margulis and Eskin, Margulis and Mozes, was also obtained by studying the orbit closures of subgroups acting on homogeneous spaces.

Similar techniques were also used by Gorodnik [2004] to study the set of values of a pair, consisting of a quadratic and linear form, at integer points and in [Sargent 2013] to establish conditions sufficient to ensure that the values of a linear map at integers lying on a quadratic surface are dense in the range of the map. The main result of this paper deals with the corresponding equidistribution problem and is stated in the following:

Theorem 1.1. *Suppose Q is a quadratic form on $\mathbb{R}^d$ such that Q is nondegenerate and indefinite with rational coefficients. Let $M = (L_1, \dots, L_s) : \mathbb{R}^d \to \mathbb{R}^s$ be a linear map such that*:

(1) *The following relations hold*: $d > 2s$ *and* $\operatorname{rank}(Q|_{\ker(M)}) = d - s$.

(2) *The quadratic form $Q|_{\ker(M)}$ has signature (r_1, r_2), where $r_1 \geq 3$ and $r_2 \geq 1$.*

(3) *For all $\alpha \in \mathbb{R}^s \setminus \{0\}$, $\alpha_1 L_1 + \dots + \alpha_s L_s$ is nonrational.*

Let $a \in \mathbb{Q}$ be such that the set $\{v \in \mathbb{Z}^d : Q(v) = a\}$ is nonempty. Then there exists $C_0 > 0$ such that, for every $\theta > 0$ and all compact $R \subset \mathbb{R}^s$ with piecewise smooth *boundary, there exists a* $T_0 > 0$ *such that, for all* $T > T_0$,

$$(1-\theta)C_0 \operatorname{Vol}(R)T^{d-s-2} \leq |\{v \in \mathbb{Z}^d : Q(v) = a,\ M(v) \in R,\ \|v\| \leq T\}| \leq (1+\theta)C_0 \operatorname{Vol}(R)T^{d-s-2},$$

where $\operatorname{Vol}(R)$ *is the* s*-dimensional Lebesgue measure of* R.

Remark 1.2. The constant C_0 appearing in Theorem 1.1 is such that

$$C_0 \operatorname{Vol}(R)T^{d-s-2} \sim \operatorname{Vol}(\{v \in \mathbb{R}^d : Q(v) = a,\ M(v) \in R,\ \|v\| \leq T\}),$$

where the volume on the right is the Haar measure on the surface defined by $Q(v) = a$.

Remark 1.3. Theorem 1.1 should hold with the condition that $\operatorname{rank}(Q|_{\ker(M)}) = d - s$ replaced by the condition that $\operatorname{rank}(Q|_{\ker(M)}) > 3$. Dealing with the more general situation requires taking into account the nontrivial unipotent part of $\operatorname{Stab}_{\mathrm{SO}(Q)}(M)$; as such, lower bounds could probably be proved using methods of [Dani and Margulis 1993], but so far, no way has been found to obtain the statement that would be needed in order to obtain an upper bound.

Remark 1.4. As in [Eskin et al. 1998], it would be possible to obtain a version of Theorem 1.1 where the condition that $\|v\| < T$ was replaced by $v \in TK_0$, where K_0 is an arbitrary deformation of the unit ball by a continuous and positive function. It should also be possible to obtain a version of Theorem 1.1 where the parameters T_0 and C_0 remain valid for any pair (Q, M) coming from compact subsets of pairs satisfying the conditions of the theorem.

Remark 1.5. The cases when the quadratic form $Q|_{\ker(M)}$ has signature $(2, 2)$ or $(2, 1)$ can be considered exceptional. There are asymptotically more integers than expected (by a factor of $\log T$) lying on certain surfaces defined by quadratic forms of signature $(2, 2)$ or $(2, 1)$. This leads to counterexamples of Theorem 1.1 in the cases when the quadratic form $Q|_{\ker(M)}$ has signature $(2, 2)$ or $(2, 1)$. Details of these examples are found in Section 6.

Outline of the paper. The proof of Theorem 1.1 rests on statements about the distribution of orbits in certain homogeneous spaces. The philosophy is that equidistribution of the orbits corresponds to equidistribution of the points considered in Theorem 1.1. Consider the following:

Ratner's equidistribution theorem [Ratner 1994]. *Let* G *be a connected Lie group,* Γ *a lattice in* G *and* $U = \{u_t : t \in \mathbb{R}\}$ *a one-parameter unipotent subgroup of* G. *Then for all* $x \in G/\Gamma$, *the closure of the orbit* Ux *has an invariant measure* $\mu_{\overline{Ux}}$ *supported on it, and for all bounded continuous functions* f *on* G/Γ,

$$\lim_{T\to\infty} \frac{1}{T} \int_0^T f(u_t x) = \int_{\overline{Ux}} f \, d\mu_{\overline{Ux}}.$$

Recall that in the proof of the quantitative Oppenheim conjecture [Eskin et al. 1998] one needs to consider an unbounded function on the space of lattices. Similarly, in order to prove Theorem 1.1, one needs to consider an unbounded function F on a certain homogeneous space. The basic idea is to try to apply Ratner's equidistribution theorem to F in order to show that the average of the values of F evaluated along a certain orbit converges to the average of F on the entire space. This is the fact that corresponds to the fact that integral points on the quadratic surface with values in R are equidistributed. The main problem in doing this is that F is unbounded, and so one must obtain an ergodic theorem taking a similar form to Ratner's equidistribution theorem but valid for unbounded functions. In order to do this, one needs precise information about the behavior of the orbits near the cusp. This information is obtained in Section 3 and comes in the form of nondivergence estimates for certain dilated spherical averages. In order to obtain these estimates, we use a certain function defined by Benoist and Quint [2012]. The required ergodic theorem is then proved in Section 4. Finally in Section 5, the proof of Theorem 1.1 is completed using an approximation argument similar to that found in [Eskin et al. 1998]. Specifically, the averages of F over the space are related to the quantity $C_0 \operatorname{Vol}(R) T^{d-s-2}$ and the averages of F along an orbit are related to the number of integer points with bounded height, lying on the surface and with values in R. In Section 2, the basic notation is set up and the main results from Sections 3 and 4 are stated.

2. Set-up

2A. ***Main results.*** For the rest of the paper, the following convention is in place: s, d and p will be fixed natural numbers such that $2s < d$ and $0 < p < d$. Also, r_1 and r_2 will be varying, natural numbers such that $d - s = r_1 + r_2$. Let $\mathscr{L}$ denote the space of linear forms on $\mathbb{R}^d$, and let $\mathscr{C}_{\text{Lin}}$ denote the subset of $\mathscr{L}^s$ such that for all $M \in \mathscr{C}_{\text{Lin}}$ Condition (3) of Theorem 1.1 is satisfied. A quadratic form on $\mathbb{R}^d$ is said to be defined over $\mathbb{Q}$ if it has rational coefficients or is a scalar multiple of a form with rational coefficients. For a a rational number, let $\mathfrak{Q}(p, a)$ denote quadratic forms on $\mathbb{R}^d$ defined over $\mathbb{Q}$ with signature $(p, d-p)$ such that the set $\{v \in \mathbb{Z}^d : Q(v) = a\}$ is nonempty for all $Q \in \mathfrak{Q}(p, a)$. Define

$$\begin{aligned}&\mathscr{C}_{\text{Pairs}}(a, r_1, r_2)\\ &\qquad = \{(Q, M) : Q \in \mathfrak{Q}(p, a),\ M \in \mathscr{C}_{\text{Lin}} \text{ and } Q|_{\ker(M)} \text{ has signature } (r_1, r_2)\}.\end{aligned}$$

Note that for $r_1 \geq 3$ and $r_2 \geq 1$ the set $\mathscr{C}_{\text{Pairs}}(a, r_1, r_2)$ consists of pairs satisfying the conditions of Theorem 1.1. Although the set $\mathscr{C}_{\text{Pairs}}(a, r_1, r_2)$ and hence its subsets and sets derived from them depend on a, this dependence is not a crucial one, so from now on, most of the time, this dependence will be omitted from the notation. For $M \in \mathscr{L}^s$ and $R \subset \mathbb{R}^s$ a connected region with smooth boundary, let

$V_M(R) = \{v \in \mathbb{R}^d : M(v) \in R\}$. For $Q \in \mathfrak{Q}(p, d-p)$, $a \in \mathbb{Q}$ and $\mathbb{K} = \mathbb{R}$ or $\mathbb{Z}$, let $X_Q^a(\mathbb{K}) = \{v \in \mathbb{K}^d : Q(v) = a\}$. Denote the annular region inside $\mathbb{R}^d$ by $A(T_1, T_2) = \{v \in \mathbb{R}^d : T_1 \le \|v\| \le T_2\}$. Using this notation, we state the following (equivalent) version of Theorem 1.1, which will be proved in Section 5:

Theorem 2.1. *Suppose that $r_1 \ge 3$, $r_2 \ge 1$ and $a \in \mathbb{Q}$. Then for all $(Q, M) \in \mathscr{C}_{\text{Pairs}}(a, r_1, r_2)$, there exists $C_0 > 0$ such that, for every $\theta > 0$ and all compact $R \subset \mathbb{R}^s$ with piecewise smooth boundary, there exists a $T_0 > 0$ such that, for all $T > T_0$,*

$$(1-\theta)C_0 \operatorname{Vol}(R)T^{d-s-2} \le |X_Q^a(\mathbb{Z}) \cap V_M(R) \cap A(0, T)| \le (1-\theta)C_0 \operatorname{Vol}(R)T^{d-s-2}.$$

Remark 2.2. As remarked previously, the cases when $r_1 = 2$ and $r_2 = 2$ or $r_1 = 2$ and $r_2 = 1$ are interesting. In dimensions 3 and 4, there can be more integer points than expected lying on some surfaces defined by quadratic forms of signature $(2, 2)$ or $(2, 1)$; this means that the statement of Theorem 2.1 fails for certain pairs. In Section 6, these counterexamples are explicitly constructed. Moreover, it is shown that this set of pairs is big in the sense that it is of second category. We note that as in [Eskin et al. 1998] one could also show that this set has measure 0 and one could prove the expected asymptotic formula as in Theorem 2.1 for almost all pairs.

Even though Theorem 2.1 fails when $r_1 = 2$ and $r_2 = 2$ or $r_1 = 2$ and $r_2 = 1$, we do have the following uniform upper bound, which will be proved in Section 5 and is analogous to Theorem 2.3 from [Eskin et al. 1998]:

Theorem 2.3. *Let $R \subset \mathbb{R}^s$ be a compact region with piecewise smooth boundary and $a \in \mathbb{Q}$.*

(I) *If $r_1 \ge 3$ and $r_2 \ge 1$, then for all $(Q, M) \in \mathscr{C}_{\text{Pairs}}(a, r_1, r_2)$ there exists a constant C depending only on (Q, M) and R such that, for all $T > 1$,*

$$|X_Q^a(\mathbb{Z}) \cap V_M(R) \cap A(0, T)| \le CT^{d-s-2}.$$

(II) *If $r_1 = 2$ and $r_2 = 1$ or $r_1 = r_2 = 2$, then for all $(Q, M) \in \mathscr{C}_{\text{Pairs}}(a, r_1, r_2)$ there exists a constant C depending only on (Q, M) and R such that, for all $T > 2$,*

$$|X_Q^a(\mathbb{Z}) \cap V_M(R) \cap A(0, T)| \le C(\log T)T^{d-s-2}.$$

2B. ***A canonical form.*** For $v_1, v_2 \in \mathbb{R}^d$, we will use the notation $\langle v_1, v_2\rangle$ to denote the standard inner product in $\mathbb{R}^d$. For a set of vectors $v_1, \dots, v_i \in \mathbb{R}^d$, we will also use the notation $\langle v_1, \dots, v_i\rangle$ to denote the span of $v_1, \dots, v_i$ in $\mathbb{R}^d$; although this could lead to some ambiguity, the meaning of the notation should be clear from the context.

For some computations, it will be convenient to know that our system is conjugate to a canonical form. Let $e_1, \dots, e_d$ be the standard basis of $\mathbb{R}^d$. Let (Q_0, M_0) be the pair consisting of a quadratic form and a linear map defined by

$$Q_0(v) = Q_{1,\dots,s}(v) + 2v_{s+1}v_d + \sum_{i=s+2}^{s+r_1} v_i^2 - \sum_{i=s+r_1+1}^{d-1} v_i^2 \quad \text{and} \quad M_0(v) = (v_1, \dots, v_s),$$

where $v_i = \langle v, e_i \rangle$ and $Q_{1,\dots,s}(v)$ is a nondegenerate quadratic form in variables $v_1, \dots, v_s$. By Lemma 2.2 of [Sargent 2013], all pairs (Q, M) such that the signature of $Q|_{\ker(M)}$ is (r_1, r_2) and $\operatorname{rank}(Q|_{\ker(M)}) = d - s$ are equivalent to the pair (Q_0, M_0) in the sense that there exist $g_d \in \mathrm{GL}_d(\mathbb{R})$ and $g_s \in \mathrm{GL}_s(\mathbb{R})$ such that $(Q, M) = (Q_0^{g_d}, g_s M_0^{g_d})$, where for $g \in \mathrm{GL}_d(\mathbb{R})$ we write $Q = Q_0^g$ if and only if $Q_0(gv) = Q(v)$ for all $v \in \mathbb{R}^d$. Moreover, since $R \subset \mathbb{R}^s$ is arbitrary, up to rescaling and possibly replacing R by $g_s R$, we assume that $g_d \in \mathrm{SL}_d(\mathbb{R})$ and that g_s is the identity. Let

$$\mathscr{C}_{\mathrm{SL}}(a, r_1, r_2) = \{g \in \mathrm{SL}_d(\mathbb{R}) : (Q_0^g, M_0^g) \in \mathscr{C}_{\mathrm{Pairs}}(a, r_1, r_2)\}.$$

For $g \in \mathscr{C}_{\mathrm{SL}}(a, r_1, r_2)$, let G_g be the identity component of the group $\{x \in \mathrm{SL}_d(\mathbb{R}) : Q_0^g(xv) = Q_0^g(v)\}$, $\Gamma_g = G_g \cap \mathrm{SL}_d(\mathbb{Z})$, $H_g = \{x \in G_g : M_0^g(xv) = M_0^g(v)\}$ and $K_g = H_g \cap g^{-1} O_d(\mathbb{R}) g$. By examining the description of the subgroup H_g given in Section 2.3 of [Sargent 2013], it is clear that K_g is a maximal compact subgroup of H_g. It is a standard fact that G_g is a connected semisimple Lie group and hence has no nontrivial rational characters. Therefore, because Q_0^g is defined over $\mathbb{Q}$, the Borel–Harish-Chandra theorem [Platonov and Rapinchuk 1991, Theorem 4.13] implies Γ_g is a lattice in G_g. We will consider the dynamical system that arises from H_g acting on G_g/Γ_g. For $\mathbb{K} = \mathbb{R}$ or $\mathbb{Z}$, the shorthand $X^a_{Q_0^g}(\mathbb{K}) = X_g(\mathbb{K})$ will be used.

2C. ***Equidistribution of measures.*** Consider the function α as defined in [Eskin et al. 1998]. It is an unbounded function on the space of unimodular lattices in $\mathbb{R}^d$. It has the properties that it can be used to bound certain functions that we will consider and it is left-K_I-invariant. Similar functions have been considered in [Schnell 1995], where it is related to various quantities involving successive minima of a lattice. Let Δ be a lattice in $\mathbb{R}^d$. For any such Δ, we say that a subspace U of $\mathbb{R}^d$ is Δ-rational if $\mathrm{Vol}(U/U \cap \Delta) < \infty$. Let

$$\Psi_i(\Delta) = \{U : U \text{ is a } \Delta\text{-rational subspace of } \mathbb{R}^d \text{ with } \dim U = i\}.$$

For $U \in \Psi_i(\Delta)$, define $d_\Delta(U) = \mathrm{Vol}(U/U \cap \Delta)$. Note that $d_\Delta(U) = \|u_1 \wedge \cdots \wedge u_i\|$, where $u_1, \dots, u_i$ is a basis for $U \cap \Delta$ over $\mathbb{Z}$ and the norm on $\bigwedge^i(\mathbb{R}^d)$ is induced from the euclidean norm on $\mathbb{R}^d$. Now we recall the definition of the function α:

$$\alpha_i(\Delta) = \sup_{U \in \Psi_i(\Delta)} \frac{1}{d_\Delta(U)} \quad \text{and} \quad \alpha(\Delta) = \max_{0 \le i \le d} \alpha_i(\Delta).$$

Here we use the convention that, if U is the trivial subspace, then $d_\Delta(U) = 1$; hence,

$\alpha_0(\Delta) = 1$. Also note that, if Δ is a unimodular lattice, then $d_\Delta(\mathbb{R}^d) = 1$ and hence $\alpha_d(\Delta) = 1$.

In (2-2) and Theorem 2.5, we consider α as a function on G_g/Γ_g; this is done via the canonical embedding of G_g/Γ_g into the space of unimodular lattices in $\mathbb{R}^d$, given by $x\Gamma_g \to x\mathbb{Z}^d$. Specifically, every $x \in G_g/\Gamma_g$ can be identified with its image under this embedding before applying α to it. For $f \in C_c(\mathbb{R}^d)$ and $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$, we define the function $F_{f,g} : G_g/\Gamma_g \to \mathbb{R}$ by

$$F_{f,g}(x) = \sum_{v \in X_g(\mathbb{Z})} f(xv). \tag{2-1}$$

The function α has the property that there exists a constant $c(f)$ depending only on the support and maximum of f such that, for all x in G_g/Γ_g,

$$F_{f,g}(x) \le c(f)\,\alpha(x). \tag{2-2}$$

The last property is well known and follows from Minkowski's theorem on successive minima; see Lemma 2 of [Schmidt 1968] for example. Alternatively, see [Henk and Wills 2008] for an up-to-date review of many related results.

We will be carrying out integration on various measure spaces defined by the groups introduced at the beginning of the section. With this in mind, let us introduce the following notation for the corresponding measures. If v denotes some variable, the notation dv is used to denote integration with respect to Lebesgue measure and this variable. Let μ_g be the Haar measure on G_g/Γ_g; if $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$, then since Γ_g is a lattice in G_g we can normalize so that $\mu_g(G_g/\Gamma_g) = 1$. In addition, ν_g will denote the measure on K_g normalized so that $\nu_g(K_g) = 1$. Let m_g^a denote the Haar measure on $X_g^a(\mathbb{R})$ defined by

$$\int_{\mathbb{R}^d} f(v)\,dv = \int_{-\infty}^{\infty} \int_{X_g^a(\mathbb{R})} f(v)\,dm_g^a(v)\,da. \tag{2-3}$$

The following provides us with our upper bounds and will be proved in Section 3:

Theorem 2.4. *Let $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$ be arbitrary, and let $\Delta = g\mathbb{Z}^d$. Let $\{a_t : t \in \mathbb{R}\}$ denote a self-adjoint one-parameter subgroup of* SO(2, 1) *embedded into H_I so that it fixes the subspace $\langle e_{s+2}, \dots, e_{d-1}\rangle$ and only has eigenvalues e^{-t}, 1 and e^t.*

(I) *Suppose $r_1 \ge 3$, $r_2 \ge 1$ and $0 < \delta < 2$; then*

$$\sup_{t>0} \int_{K_I} \alpha(a_t k\Delta)^\delta \,d\nu_I(k) < \infty.$$

(II) *Suppose $r_1 = r_2 = 2$ or $r_1 = 2$ and $r_2 = 1$; then*

$$\sup_{t>1} \frac{1}{t} \int_{K_I} \alpha(a_t k\Delta)\,d\nu_I(k) < \infty.$$

In Section 4, we will modify the results from Section 4 of [Eskin et al. 1998] and combine them with Theorem 2.4 to prove the following, which will be a major ingredient of the proof of Theorem 2.1:

Theorem 2.5. *Suppose $r_1 \geq 3$ and $r_2 \geq 1$. Let $A = \{a_t : t \in \mathbb{R}\}$ be a one-parameter subgroup of H_g such that there exists a continuous homomorphism $\rho : \mathrm{SL}_2(\mathbb{R}) \to H_g$ with $\rho(D) = A$ and $\rho(\mathrm{SO}(2)) \subset K_g$, where $D = \left\{\begin{pmatrix} t & 0 \\ 0 & t^{-1}\end{pmatrix} : t > 0\right\}$. Let $\phi \in L^1(G_g/\Gamma_g)$ be a continuous function such that, for some $0 < \delta < 2$ and some $C > 0$,*

$$|\phi(\Delta)| < C\alpha(\Delta)^\delta \quad \text{for all } \Delta \in G_g/\Gamma_g. \tag{2-4}$$

Then for all $\epsilon > 0$ and all $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$, there exists $T_0 > 0$ such that, for all $t > T_0$,

$$\left| \int_{K_g} \phi(a_t k)\, d\nu_g(k) - \int_{G_g/\Gamma_g} \phi \, d\mu_g \right| \leq \epsilon.$$

3. The upper bounds

In this section, we prove Theorem 2.4. By definition, $H_I \cong \mathrm{SO}(r_1, r_2)$ and is embedded in $\mathrm{SL}_d(\mathbb{R})$ so that it fixes $\langle e_1, \ldots, e_s\rangle$. Let $\{a_t : t \in \mathbb{R}\}$ denote a self-adjoint one-parameter subgroup of $\mathrm{SO}(2, 1)$ embedded into H_I so that it fixes the subspace $\langle e_{s+2}, \ldots, e_{d-1}\rangle$. Moreover, suppose that the only eigenvalues of a_t are e^{-t}, 1 and e^t. For $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$, let $\Delta = g\mathbb{Z}^d$.

3A. ***Proof of Part (I) of Theorem 2.4.*** The aim is to construct a function $f : H_I \to \mathbb{R}$ that is contracted by the operator

$$A_t f(h) = \int_{K_I} f(a_t k h)\, d\nu_I(k).$$

We say that f is contracted by the operator A_t if for any $c > 0$ there exists $t_0 > 0$ and $b > 0$ such that, for all $h \in H_I$,

$$A_{t_0} f(h) < c f(h) + b.$$

This fact will be used in conjunction with the following:

Proposition 3.1 [Eskin et al. 1998, Proposition 5.12]. *Let $f : H_I \to \mathbb{R}$ be a strictly positive function such that*:

(1) *For any $\epsilon > 0$, there exists a neighborhood $V(\epsilon)$ of 1 in H_I such that*

$$(1-\epsilon) f(h) \leq f(uh) \leq (1+\epsilon) f(h)$$

for all $h \in H_I$ and $u \in V(\epsilon)$.

(2) *The function f is left-K_I-invariant.*

(3) $f(1) < \infty$.

(4) *The function f is contracted by the operator A_t.*

Then $\sup_{t>0} A_t f(1) < \infty$.

It is clear that, if in addition to satisfying Properties (1)–(4) we have $\alpha(h\Delta)^\delta \leq f(h)$ for all $h \in H_I$, then the conclusion of Part (I) of Theorem 2.4 follows. We define the function in three stages. In the first stage, we define a function on the exterior algebra of $\mathbb{R}^d$; then this function is used to define a function on the space of lattices in $\mathbb{R}^d$. Finally we use that function to define a function with the required properties.

3A.1. *A function on the exterior algebra of* $\mathbb{R}^d$. Let $\bigwedge(\mathbb{R}^d) = \bigoplus_{i=1}^{d-1} \bigwedge^i(\mathbb{R}^d)$. We say that $v \in \bigwedge(\mathbb{R}^d)$ has degree i if $v \in \bigwedge^i(\mathbb{R}^d)$. Let $\Omega_i = \{v_1 \wedge \cdots \wedge v_i : v_1, \ldots, v_i \in \mathbb{R}^d\}$ be the set of monomial elements of $\bigwedge(\mathbb{R}^d)$ with degree i. Define $\Omega = \bigcup_{i=1}^{d-1} \Omega_i$. Consider the representation $\rho : H_I \to \mathrm{GL}(\bigwedge(\mathbb{R}^d))$. Since H_I is semisimple, this representation decomposes as a direct sum of irreducible subrepresentations. Associated to each of these subrepresentations is a unique highest weight. Let $\mathcal{P}$ denote the set of all these highest weights. For $\lambda \in \mathcal{P}$, denote by U^λ the sum of all of the subrepresentations with highest weight λ and let $\tau_\lambda : \bigwedge(\mathbb{R}^d) \to U^\lambda$ be the orthogonal projection.

Let $\epsilon > 0$. For $0 < i < d$ and $v \in \bigwedge^i(\mathbb{R}^d)$, the following function was defined by Benoist and Quint [2012]. Let

$$\varphi_\epsilon(v) = \begin{cases} \min_{\lambda \in \mathcal{P}\setminus\{0\}} \epsilon^{\gamma_i} \|\tau_\lambda(v\|)^{-1} & \text{if } \|\tau_0(v)\| \leq \epsilon^{\gamma_i}, \\ 0 & \text{else,} \end{cases}$$

where for $0 < i < d$ we define $\gamma_i = (d-i)i$. In fact, the definition of φ_ϵ given here is a special case of the definition given in [Benoist and Quint 2012]. In that definition of φ_ϵ, there is an extra set of exponents depending on $\lambda \in \mathcal{P}\setminus\{0\}$ appearing. However, we see that in our case we may choose all of these exponents to be equal to 1.

Let $\mathcal{F} = \{v \in \bigwedge(\mathbb{R}^d) : H_I v = v\}$ be the fixed vectors of H_I. Let $\mathcal{F}^c$ be the orthogonal complement of $\mathcal{F}$.

Remark 3.2. Since $\max_{\lambda \in \mathcal{P}\setminus\{0\}} \|\tau_\lambda(v)\|$ defines a norm on $\mathcal{F}^c$, there exist constants c_1 and c_2 depending on ϵ and the γ_i's such that

$$c_1 \|v\|^{-1} \leq \varphi_\epsilon(v) \leq c_2 \|v\|^{-1}$$

for all $v \in \mathcal{F}^c$.

Remark 3.3. For $0 < i < d$ and $v \in \bigwedge^i(\mathbb{R}^d) \setminus \{0\}$, we have $\varphi_\epsilon(v) = \infty$ if and only if v is H_I-invariant and $\|v\| \leq \epsilon^{\gamma_i}$.

We will need to refer to the constant defined as $b_1 = \sup\{\varphi_\epsilon(v) : v \in \bigwedge(\mathbb{R}^d), \|v\| \geq 1\}$. Benoist and Quint [2012, Lemma 4.2] showed that the function φ_ϵ satisfies the following convexity property:

Lemma 3.4. *There exists a positive constant C such that, for any $0 < \epsilon < C^{-1}$, $u \in \Omega_{i_1}$, $v \in \Omega_{i_2}$ and $w \in \Omega_{i_3}$ with $i_1 \geq 0$, $i_2 > 0$ and $i_3 > 0$ such that $\varphi_\epsilon(u \wedge v) \geq 1$ and $\varphi_\epsilon(u \wedge w) \geq 1$, one has*:

(1) *If $i_1 > 0$ and $i_1 + i_2 + i_3 < d$, then*

$$\min\{\varphi_\epsilon(u \wedge v), \varphi_\epsilon(u \wedge w)\} \leq (C\epsilon)^{1/2} \max\{\varphi_\epsilon(u), \varphi_\epsilon(u \wedge v \wedge w)\}.$$

(2) *If $i_1 = 0$ and $i_1 + i_2 + i_3 < d$, then*

$$\min\{\varphi_\epsilon(v), \varphi_\epsilon(w)\} \leq (C\epsilon)^{1/2}\varphi_\epsilon(v \wedge w).$$

(3) *If $i_1 > 0$, $i_1 + i_2 + i_3 = d$ and $\|u \wedge v \wedge w\| \geq 1$, then*

$$\min\{\varphi_\epsilon(u \wedge v), \varphi_\epsilon(u \wedge w)\} \leq (C\epsilon)^{1/2}\varphi_\epsilon(u).$$

(4) *If $i_1 = 0$, $i_1 + i_2 + i_3 = d$ and $\|v \wedge w\| \geq 1$, then*

$$\min\{\varphi_\epsilon(v), \varphi_\epsilon(w)\} \leq b_1.$$

We also need to obtain uniform bounds for the spherical averages of φ_ϵ. In order to do this, we use the following:

Lemma 3.5 [Eskin et al. 1998, Lemma 5.2]. *Let V be a finite-dimensional real inner-product space, A a self-adjoint linear transformation of V, K a closed connected subgroup of $O(V)$ and S a closed subset of the unit sphere in V. Assume the only eigenvalues of A are -1, 0 and 1, and denote by W^-, W^0 and W^+ the corresponding eigenspaces. Assume that $Kv \not\subset W^0$ for any $v \in S$ and that there exists a self-adjoint subgroup H_1 of* $\mathrm{GL}(V)$ *with the following properties*:

(1) *The Lie algebra of H_1 contains A.*

(2) *H_1 is locally isomorphic to* $\mathrm{SO}(3, 1)$.

(3) *$H_1 \cap K$ is a maximal compact subgroup of H_1.*

Then for any δ, $0 < \delta < 2$,

$$\lim_{t\to\infty} \sup_{v \in S} \int_K \|\exp(tA)kv\|^{-\delta}\, d\nu(k) = 0.$$

Using Lemma 3.5, we can obtain the following bound on the spherical averages:

Lemma 3.6. *Suppose $r_1 \geq 3$ and $r_2 \geq 1$. Then for all $\epsilon > 0$, $0 < \delta < 2$ and $c > 0$, there exists $t_0 > 0$ such that, for all $t > t_0$ and all $v \in \mathcal{F}^c \setminus \{0\}$,*

$$\int_{K_I} \varphi_\epsilon(a_t kv)^\delta\, d\nu_I(k) < c\varphi_\epsilon(v)^\delta.$$

Proof. The subset $S = \{v \in \bigwedge(\mathbb{R}^d) : \|v - \tau_0(v)\| = 1\}$ is a closed subset of the unit sphere in $\bigwedge(\mathbb{R}^d)$. We have $a_t = \exp(tA)$ for an appropriate choice of A satisfying the conditions of Lemma 3.5.

We claim that, for any $v \in S$, $Kv \not\subset W^0$. To see this, let

$$H_v = \{h \in H_I : hkv = kv \text{ for all } k \in K_I\}.$$

Note that K_I normalizes H_v. Let E_v be the subgroup generated by $K_I \cup H_v$. By its definition, E_v also normalizes H_v. Since K_I is a maximal proper subgroup of H_I, in the case that $H_v \not\subset K_I$, we must have $E_v = H_I$. Therefore, H_v is a normal subgroup of H_I. Since $r_1 \geq 3$ and $r_2 \geq 1$, H_I is simple and hence $H_v = H_I$ or H_v is trivial. Since $S \cap \mathscr{F} = 0$, the first case is impossible. Therefore, for all $v \in S$, $H_v \subset K_I$. In particular, this means that $\{a_t : t \in \mathbb{R}\}$ is not contained in H_v. This implies the claim.

Then if $r_1 \geq 3$ and $r_2 \geq 1$, the conditions of Lemma 3.5 are satisfied. Hence, for any δ with $0 < \delta < 2$,

$$\lim_{t\to\infty} \sup_{v\in S} \int_{K_I} \|a_t kv\|^{-\delta}\, d\nu_I(k) = 0.$$

This implies that for all $c > 0$ there exists $t_0 > 0$ such that, for all $t > t_0$ and all $v \in \mathscr{F}^c \setminus \{0\}$,

$$\int_{K_I} \|a_t kv\|^{-\delta}\, d\nu_I(k) < c\|v\|^{-\delta}.$$

Then the claim of the lemma follows from Remark 3.2. □

3A.2. *A function on the space of lattices.* For any lattice Λ, we say that $v \in \Omega$ is Λ-integral if one can write $v = v_1 \wedge \cdots \wedge v_i$ where $v_1, \ldots, v_i \in \Lambda$. Let $\Omega_i(\Lambda)$ and $\Omega(\Lambda)$ be the sets of Λ-integral elements of Ω_i and Ω, respectively. Define $f_\epsilon : \mathrm{SL}_d(\mathbb{R})/\mathrm{SL}_d(\mathbb{Z}) \to \mathbb{R}$ by

$$f_\epsilon(\Lambda) = \max_{v\in\Omega(\Lambda)} \varphi_\epsilon(v).$$

Note that by Remark 3.2 for all $\epsilon > 0$ there exists some constant $c_\epsilon > 0$ such that, for any unimodular lattice Λ, we have

$$\begin{aligned}\max_{v\in\Omega(\Lambda)} \|v\|^{-1} &\leq \max_{0<i<d}\Big(\max_{v\in\Omega_i(\Lambda),\ \|\tau_0(v)\|\leq\epsilon^{\gamma_i}} \|v\|^{-1} + \max_{v\in\Omega_i(\Lambda),\ \|\tau_0(v)\|>\epsilon^{\gamma_i}} \|v\|^{-1}\Big)\\ &\leq c_\epsilon f_\epsilon(\Lambda) + \max_{0<i<d} \epsilon^{-\gamma_i}.\end{aligned} \tag{3-1}$$

Moreover, it follows from the definition of the α function that

$$\alpha(\Lambda) = \max\Big\{\max_{v\in\Omega(\Lambda)} \|v\|^{-1}, 1\Big\}. \tag{3-2}$$

The following is necessary to ensure that the function $f_\epsilon(h\Delta)$ is finite for all $h \in H_I$:

Lemma 3.7. *For all $h \in H_I$, if $u \in \Omega(h\Delta)$, then $u \notin \mathcal{F}$.*

Proof. Suppose for a contradiction that $u \in \Omega(h\Delta) \cap \mathcal{F}$. Suppose that u has degree i for some $0 < i < d$, and let $u = u_1 \wedge \cdots \wedge u_i$ and $U = \langle u_1, \dots, u_i \rangle$. Since $u \in \Omega(h\Delta)$, it follows that $U \cap h\Delta$ is a lattice in U. Moreover, because $u \in \mathcal{F}$, $U \cap \Delta$ is also a lattice in U or equivalently $g^{-1}U \cap \mathbb{Z}^d$ is a lattice in $g^{-1}U$. The subspace $g^{-1}U$ is H_g-invariant.

Conversely, it follows from Lemma 3.4 of [Sargent 2013] that, if V is any H_g-invariant subspace, then either

(1) $V \subseteq g^{-1}\langle e_1, \dots, e_s \rangle$ or

(2) $V = g^{-1}\langle e_{s+1}, \dots, e_d \rangle \oplus V'$ where $V' \subseteq g^{-1}\langle e_1, \dots, e_s \rangle$.

Thus, either V or the orthogonal complement of V is contained in $g^{-1}\langle e_1, \dots, e_s \rangle$. By Corollary 3.2 of [Sargent 2013], $g^{-1}\langle e_1, \dots, e_s \rangle$ contains no subspaces defined over $\mathbb{Q}$. This implies that, if V is any H_g-invariant subspace, then V is not defined over $\mathbb{Q}$. In particular, $V \cap \mathbb{Z}^d$ cannot be a lattice in V. This gives a contradiction. □

3A.3. *A function on H_I.* Define $\tilde{f}_{\Delta,\epsilon} : H_I \to \mathbb{R}$ by

$$\tilde{f}_{\Delta,\epsilon}(h) = f_\epsilon(h\Delta).$$

In view of (3-1) and (3-2), the proof of Part (I) of Theorem 2.4 will be complete provided that Conditions (1)–(4) from Proposition 3.1 are satisfied by the function $\tilde{f}_{\Delta,\epsilon}$ for some $\epsilon > 0$. It is clear that $\tilde{f}_{\Delta,\epsilon}$ is left-K_I-invariant. Also since $\|\tau_\lambda(\rho(h^{-1})\|)^{-1} \le \|\tau_\lambda(hv)\|/\|v\| \le \|\tau_\lambda(\rho(h))\|$ for all $\lambda \in \mathcal{P}$, $v \in \Omega$ and $h \in H_I$, $\tilde{f}_{\Delta,\epsilon}$ also satisfies Condition (1) of Proposition 3.1. From Remark 3.3, we get that $\tilde{f}_{\Delta,\epsilon}(1) = \infty$ only if there exists $v \in \Omega(\Delta) \cap \mathcal{F}$, but by Lemma 3.7, we know that no such v exists and so $\tilde{f}_{\Delta,\epsilon}(1) < \infty$. It remains to show that $\tilde{f}_{\Delta,\epsilon}$ is contracted by the operator A_t. The proof is very similar to that of Proposition 5.3 in [Benoist and Quint 2012].

Lemma 3.8. *Suppose $r_1 \ge 3$ and $r_2 \ge 1$. There exists $\epsilon > 0$ such that, for all $0 < \delta < 2$, the function $\tilde{f}^{\delta}_{\Delta,\epsilon}$ is contracted by the operator A_t.*

Proof. Fix $c > 0$. By Lemma 3.6, there exists $t_0 > 0$ so that, for any $v \in \mathcal{F}^c \setminus \{0\}$,

$$\int_{K_I} \varphi_\epsilon(a_{t_0} k v)^\delta \, d\nu_I(k) < \frac{c}{d} \varphi_\epsilon(v)^\delta. \tag{3-3}$$

Let $m_0 = \|\rho(a_{t_0})\| = \|\rho(a_{t_0}^{-1})\|$. Then for all $v \in \bigwedge(\mathbb{R}^d)$,

$$m_0^{-1} \le \|a_{t_0} v\|/\|v\| \le m_0. \tag{3-4}$$

It follows from the definition of φ_ϵ and (3-4) that

$$m_0^{-1}\varphi_\epsilon(v) \le \varphi_\epsilon(a_{t_0} v) \le m_0 \varphi_\epsilon(v). \tag{3-5}$$

Let

$$\Psi(h\Delta) = \{v \in \Omega(h\Delta) : f_\epsilon(h\Delta) \le m_0^2 \varphi_\epsilon(v)\}.$$

Note that

$$f_\epsilon(h\Delta) = \max_{\psi \in \Psi(h\Delta)} \varphi_\epsilon(\psi). \tag{3-6}$$

Let C be the constant from Lemma 3.4. Assume that ϵ is small enough so that

$$m_0^4 C\epsilon < 1. \tag{3-7}$$

There are now two cases.

Case 1: $f_\epsilon(h\Delta) \le \max\{b_1, m_0^2\}$. In this case, (3-5) and the fact that f_ϵ is left-K_I-invariant imply that $f_\epsilon(a_{t_0} kh\Delta) \le m_0 f_\epsilon(h\Delta)$. Hence,

$$\int_{K_I} f_\epsilon(a_{t_0} kh\Delta)^\delta \, d\nu_I(k) \le (m_0 \max\{b_1, m_0^2\})^\delta. \tag{3-8}$$

Case 2: $f_\epsilon(h\Delta) > \max\{b_1, m_0^2\}$. This implies:

Claim 3.9. *The set $\Psi(h\Delta)$ contains only one element up to sign change in each degree.*

Proof. Assume that, for some $0 < i < d$, $\Psi(h\Delta) \cap \Omega(h\Delta)$ contains two noncolinear elements, v_0 and w_0. Then because $f_\epsilon(h\Delta) > m_0^2$ and v_0 and w_0 are in $\Psi(h\Delta)$, we have $\varphi_\epsilon(v_0) \ge 1$ and $\varphi_\epsilon(w_0) \ge 1$. We can write $v_0 = u \wedge v$ and $w_0 = u \wedge w$, where $u \in \Omega_{i_1}(h\Delta)$, $v \in \Omega_{i_2}(h\Delta)$ and $w \in \Omega_{i_2}(h\Delta)$ with $i_1 \ge 0$ and $i_2 > 0$. There are four cases.

Case 2.1: $i_2 < i$ and $i_2 < d - i$. In this case,

$$f_\epsilon(h\Delta) \le m_0^2 \min\{\varphi_\epsilon(u \wedge v), \varphi_\epsilon(u \wedge w)\} \le (m_0^4 C\epsilon)^{1/2} \max\{\varphi_\epsilon(u), \varphi_\epsilon(u \wedge v \wedge w)\}$$

by Lemma 3.4(1). This implies that

$$f_\epsilon(h\Delta) \le (m_0^4 C\epsilon)^{1/2} f_\epsilon(h\Delta), \tag{3-9}$$

which contradicts (3-7).

Case 2.2: $i_2 = i < d - i$. In this case, $u = 1$. The same computation but using Lemma 3.4(2) still gives (3-9), which is still a contradiction.

Case 2.3: $i_2 = d - i < i$. In this case, $\|u \wedge v \wedge w\|$ is an integer. Therefore, the same computation but using Lemma 3.4(3) still gives (3-9).

Case 2.4: $i_2 = i = d - i$. The same computation, using Lemma 3.4(4), gives

$$f_\epsilon(h\Delta) \le b_1,$$

which is again a contradiction. □

Suppose $v \in \Omega$ is arbitrary. If $v \notin \Psi(h\Delta)$, then $f_\epsilon(h\Delta) > m_0^2 \varphi_\epsilon(v)$, and by left-$K_I$-invariance of φ_ϵ, (3-5) and (3-6), for all $k \in K_I$, we have

$$\begin{aligned}\varphi_\epsilon(a_{t_0}kv) \le m_0\varphi_\epsilon(v) \le m_0^{-1} f_\epsilon(h\Delta)&\\ \le m_0^{-1} \max_{\psi\in\Psi(h\Delta)} \varphi_\epsilon(\psi) \le \max_{\psi\in\Psi(h\Delta)} \varphi_\epsilon(a_{t_0}k\psi).&\end{aligned} \tag{3-10}$$

If $v \in \Psi(h\Delta)$, then (3-10) holds for obvious reasons. Therefore, (3-10) holds for all $v \in \Omega$. Thus, using the definition of f_ϵ and (3-10), we get

$$\begin{aligned}\int_{K_I} f_\epsilon(a_{t_0}kh\Delta)^\delta\, d\nu_I(k) &= \int_{K_I} \max_{v\in\Omega(h\Delta)} \varphi_\epsilon(a_{t_0}kv)^\delta\, d\nu_I(k)\\ &\le \sum_{\psi\in\Psi(h\Delta)} \int_{K_I} \varphi_\epsilon(a_{t_0}k\psi)^\delta\, d\nu_I(k).\end{aligned} \tag{3-11}$$

Using Lemma 3.7, we see that, for all $\psi \in \Psi(h\Delta)$, $\psi \notin \mathscr{F}$ and hence $\psi - \tau_0(\psi) \in \mathscr{F}^c \setminus \{0\}$. Moreover, if $\varphi_\epsilon(a_{t_0}k\psi) \neq 0$, then $\varphi_\epsilon(a_{t_0}k\psi) = \varphi_\epsilon(a_{t_0}k(\psi - \tau_0(\psi)))$ and we can apply (3-3) to get

$$\int_{K_I} \varphi_\epsilon(a_{t_0}k\psi)^\delta\, d\nu_I(k) \le \frac{c}{d}\varphi_\epsilon(\psi)^\delta \tag{3-12}$$

for each $\psi \in \Psi(h\Delta)$. If $\varphi_\epsilon(a_{t_0}k\psi) = 0$, then it is clear that (3-12) also holds. Using Claim 3.9, we obtain

$$\sum_{\psi\in\Psi(h\Delta)} \int_{K_I} \varphi_\epsilon(a_{t_0}k\psi)^\delta\, d\nu_I(k) \le d \max_{\psi\in\Psi(h\Delta)} \int_{K_I} \varphi_\epsilon(a_{t_0}k\psi)^\delta\, d\nu_I(k);$$

the claim of the lemma follows from (3-6), (3-8), (3-11) and (3-12). □

3B. *Proof of Part (II) of Theorem 2.4.* This time, the aim is to construct a function such that it satisfies the conditions of the following:

Lemma 3.10. *Suppose $r_1 = 2$ and $r_2 = 1$ or $r_1 = r_2 = 2$. Let $f : H_I \to \mathbb{R}$ be a strictly positive continuous function such that*:

(1) *For any $\epsilon > 0$, there exists a neighborhood $V(\epsilon)$ of 1 in H_I such that*

$$(1-\epsilon) f(h) \le f(uh) \le (1+\epsilon) f(h)$$

for all $h \in H_I$ and $u \in V(\epsilon)$.

(2) *The function f is left-K_I-invariant.*

(3) $f(1) < \infty$.

(4) *There exist $t_0 > 0$ and $b > 0$ such that, for all $h \in H_I$ and $0 \le t \le t_0$,*

$$A_t f(h) \le f(h) + b.$$

Then $\sup_{t>1}(1/t)A_t f(1) < \infty$.

Proof. Since $\mathrm{SO}(2,1)$ is locally isomorphic to $\mathrm{SL}_2(\mathbb{R})$ and $\mathrm{SO}(2,2)$ is locally isomorphic to $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$, this follows directly from Lemma 5.13 of [Eskin et al. 1998]. □

The general strategy of this subsection is broadly the same as in the last one. First we define a certain function on the exterior algebra of $\mathbb{R}^d$, and then we use this function to define a function that has the properties demanded by Lemma 3.10.

3B.1. *Functions on the exterior algebra of* $\mathbb{R}^d$. As before, we work with a function on the exterior algebra of $\mathbb{R}^d$. This time, the definition is simpler because in this case the vectors fixed by the action of H_I cause no extra problems. For $\epsilon > 0$, $0 < i < d$ and $v \in \bigwedge^i(\mathbb{R}^d)$, we define

$$\widetilde{\varphi}_\epsilon(v) = \epsilon^{\gamma_i} \|v\|^{-1}.$$

If $v \in \bigwedge^0(\mathbb{R}^d)$ or $v \in \bigwedge^d(\mathbb{R}^d)$, then we set $\widetilde{\varphi}_\epsilon(v) = 1$. The following is the analogue of Lemma 3.4:

Lemma 3.11. *Let $i_1 \geq 0$ and $i_2 > 0$ and Λ be a unimodular lattice. Then for all $u \in \Omega_{i_1}(\Lambda)$, $v \in \Omega_{i_2}(\Lambda)$ and $w \in \Omega_{i_2}(\Lambda)$,*

$$\widetilde{\varphi}_\epsilon(u \wedge v)\, \widetilde{\varphi}_\epsilon(u \wedge w) \leq \epsilon^{2i_2} \widetilde{\varphi}_\epsilon(u)\, \widetilde{\varphi}_\epsilon(u \wedge v \wedge w).$$

Proof. This is a direct consequence of Lemma 5.6 from [Eskin et al. 1998] and the fact that $2\gamma_{i_1+i_2} - \gamma_{i_1} - \gamma_{i_1+2i_2} = 2i_2$. □

The following lemma is used to bound the spherical averages. It is analogous to Lemma 3.6 (see also Lemma 5.5 of [Eskin et al. 1998]). It explains why in this case the fixed vectors do not cause problems.

Lemma 3.12. *Suppose $r_1 \geq 2$ and $r_2 \geq 1$. Then for all $t \geq 0$ and $v \in \bigwedge(\mathbb{R}^d) \setminus \{0\}$,*

$$\int_{K_I} \|a_t k v\|^{-1}\, d\nu_I(k) \leq \|v\|^{-1}.$$

Proof. Let $F_v(t) = \int_{K_I} \|a_t k v\|^{-1}\, d\nu_I(k)$. We will show that $\frac{d}{dt} F_v(t) \leq 0$ for all $t \geq 0$ and $v \in \bigwedge(\mathbb{R}^d) \setminus \{0\}$, from which it is clear that the claim of the lemma follows. Let π^- and π^+ be the projections from $\bigwedge(\mathbb{R}^d)$ onto the contracting and expanding eigenspaces of a_t, respectively. Note that

$$\begin{aligned}\frac{d}{dt} F_v(t) &= \int_{K_I} \frac{e^{-2t}\|\pi^-(kv)\|^2 - e^{2t}\|\pi^+(kv)\|^2}{\|a_t k v\|^3}\, d\nu_I(k) \\ &\leq \Big(\frac{\|a_t\|}{\|v\|}\Big)^3 \int_{K_I} (e^{-2t}\|\pi^-(kv)\|^2 - e^{2t}\|\pi^+(kv)\|^2)\, d\nu_I(k). \qquad (3\text{-}13)\end{aligned}$$

Let Q_0 also denote the matrix that defines the quadratic form Q_0. Note that $\|\pi^-(Q_0 v)\| = \|\pi^+(v)\|$ and $\|\pi^+(Q_0 v)\| = \|\pi^-(v)\|$ for all $v \in \bigwedge(\mathbb{R}^d)$. Because

$Q_0^T = Q_0 = Q_0^{-1}$, if $\det(Q_0) = 1$, then $Q_0 \in K_I$, or if $\det(Q_0) = -1$, then $-Q_0 \in K_I$. This means that $Q_0 K_I(v - \tau_0(v)) = K_I \pm (v - \tau_0(v))$ and thus

$$\begin{aligned}\int_{K_I} \|\pi^-(kv)\|^2 \, d\nu_I(k) &= \int_{K_I} \|\pi^+(Q_0(kv))\|^2 \, d\nu_I(k)\\ &= \int_{K_I} \|\pi^+(kv)\|^2 \, d\nu_I(k).\end{aligned} \tag{3-14}$$

Therefore, using (3-13) and (3-14), we have

$$\frac{d}{dt} F_v(t) \le \Big(\frac{\|a_t\|}{\|v\|}\Big)^3 \int_{K_I} \|\pi^+(kv)\|^2 \, d\nu_I(k)(e^{-2t} - e^{2t}) \le 0$$

for all $t \ge 0$ and $v \in \bigwedge(\mathbb{R}^d) \setminus \{0\}$ as required. □

3B.2. *Functions on H_I.* Define $\tilde{f}_{\Delta,\epsilon} : H_I \to \mathbb{R}$ by

$$\tilde{f}_{\Delta,\epsilon}(h) = \sum_{i=1}^{d} \max_{v \in \Omega_i(h\Delta)} \widetilde{\varphi}_\epsilon(v).$$

Note that for all $\epsilon > 0$ there exists some constant $c_\epsilon > 0$ such that, for any unimodular lattice Λ,

$$\max_{v \in \Omega(\Lambda)} \|v\|^{-1} \le c_\epsilon \max_{v \in \Omega(\Lambda)} \widetilde{\varphi}_\epsilon(v) \le c_\epsilon \sum_{i=1}^{d} \max_{v \in \Omega_i(\Lambda)} \widetilde{\varphi}_\epsilon(v).$$

In view of this and (3-2), the proof of Part (II) of Theorem 2.4 will be complete provided that Conditions (1)–(4) from Lemma 3.10 are satisfied by the functions $\tilde{f}_{\Delta,\epsilon}$ for some $\epsilon > 0$. It is clear that $\tilde{f}_{\Delta,\epsilon}$ is left-K_I-invariant. Also since $\|\rho(h^{-1})\|^{-1} \le \|hv\|/\|v\| \le \|\rho(h)\|$ for all $v \in \Omega$ and $h \in H_I$, $\tilde{f}_{\Delta,\epsilon}$ also satisfies Condition (1) of Lemma 3.10. We also have that $\tilde{f}_{\Delta,\epsilon}(1) < \infty$. It remains to show that $\tilde{f}_{\Delta,\epsilon}$ satisfies Condition (4) of Lemma 3.10.

Lemma 3.13. *Suppose $r_1 = 2$ and $r_2 = 1$ or $r_1 = r_2 = 2$. Then there exist $\epsilon > 0$ and $t_0 > 0$ such that, for all $0 \le t < t_0$ and $h \in H_I$,*

$$\int_{K_I} \tilde{f}_{\Delta,\epsilon}(a_t k h) \, d\nu_I(k) \le \tilde{f}_{\Delta,\epsilon}(h).$$

Proof. Let $m_0 = \|\rho(a_{t_0})\|$. Then for all $v \in \bigwedge(\mathbb{R}^d)$ and $0 \le t < t_0$,

$$m_0^{-1} \le \|a_t v\|/\|v\| \le m_0. \tag{3-15}$$

It follows from the definition of $\widetilde{\varphi}_\epsilon$ and (3-15) that, for all $0 \le t < t_0$,

$$m_0^{-1} \widetilde{\varphi}_\epsilon(v) \le \widetilde{\varphi}_\epsilon(a_t v) \le m_0 \widetilde{\varphi}_\epsilon(v). \tag{3-16}$$

Let

$$\Psi(h\Delta) = \bigcup_{i=1}^{d} \bigl\{ v \in \Omega_i(h\Delta) : \max_{v \in \Omega_i(h\Delta)} \widetilde{\varphi}_\epsilon(v) \le m_0^2 \widetilde{\varphi}_\epsilon(v) \bigr\}.$$

Now we show that for ϵ small enough the set $\Psi(h\Delta)$ contains only one element up to sign change in each degree. To see this, assume that, for some $0 < i < d$, $\Psi(h\Delta) \cap \Omega(h\Delta)$ contains two noncolinear elements, v_0 and w_0. We can write $v_0 = u \wedge v$ and $w_0 = u \wedge w$ where $u \in \Omega_{i_1}(h\Delta)$, $v \in \Omega_{i_2}(h\Delta)$ and $w \in \Omega_{i_2}(h\Delta)$ with $i_1 \ge 0$ and $i_2 > 0$. In this case,

$$\tilde{f}_{\Delta,\epsilon}(h)^2 \le d^2 m_0^4 \widetilde{\varphi}_\epsilon(u \wedge v)\, \widetilde{\varphi}_\epsilon(u \wedge w) \le d^2 m_0^4 \epsilon^{2i_2} \tilde{f}_{\Delta,\epsilon}(h)^2$$

by Lemma 3.11. Hence, the claim is true since taking ϵ small enough gives a contradiction.

In view of this discussion, we can suppose that $\Psi(h\Delta) = \{\psi_i\}_{i=1}^d$, where ψ_i has degree i. Let $v \in \Omega_i(h\Delta)$ be arbitrary. If $v \notin \Psi(h\Delta)$, then $\max_{v \in \Omega_i(h\Delta)} \widetilde{\varphi}_\epsilon(v) > m_0^2 \widetilde{\varphi}_\epsilon(v)$, and by left-$K_I$-invariance of $\widetilde{\varphi}_\epsilon$ and (3-16), for all $k \in K_I$, we have

$$\widetilde{\varphi}_\epsilon(a_{t_0} k v) \le m_0 \widetilde{\varphi}_\epsilon(v) \le m_0^{-1} \max_{v \in \Omega_i(h\Delta)} \widetilde{\varphi}_\epsilon(v) = m_0^{-1} \widetilde{\varphi}_\epsilon(\psi_i) \le \widetilde{\varphi}_\epsilon(a_{t_0} k \psi_i). \quad (3\text{-}17)$$

If $v \in \Psi(h\Delta)$, then (3-17) holds for obvious reasons. Therefore, (3-17) holds for all $v \in \Omega$. Thus, using the definition of $\tilde{f}_{\Delta,\epsilon}$ and (3-17), we get

$$\begin{aligned} \int_{K_I} \tilde{f}_{\Delta,\epsilon}(a_{t_0} k h)\, d\nu_I(k) &= \sum_{i=1}^{d} \int_{K_I} \max_{v \in \Omega_i(h\Delta)} \widetilde{\varphi}_\epsilon(a_{t_0} k v)\, d\nu_I(k) \\ &\le \sum_{i=1}^{d} \int_{K_I} \widetilde{\varphi}_\epsilon(a_{t_0} k \psi_i)\, d\nu_I(k). \end{aligned} \quad (3\text{-}18)$$

By Lemma 3.12, there exists $t_0 > 0$ so that, for any $v \in \bigwedge(\mathbb{R}^d)$ and all $0 \le t < t_0$,

$$\int_{K_I} \widetilde{\varphi}_\epsilon(a_{t_0} k \psi_i)\, d\nu_I(k) \le \widetilde{\varphi}_\epsilon(\psi_i) \quad (3\text{-}19)$$

for each $\psi_i \in \Psi(h\Delta)$. The claim of the lemma follows from (3-18) and (3-19). □

4. Ergodic theorems

For subgroups W_1 and W_2 of G_g, let $X(W_1, W_2) = \{g \in G_g : W_2 g \subset g W_1\}$. As in [Eskin et al. 1998], the ergodic theory is based on Theorem 3 from [Dani and Margulis 1993], reproduced below in a form relevant to the current situation:

Theorem 4.1. *Suppose $r_1 \ge 2$ and $r_2 \ge 1$. Let $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$ be arbitrary. Let $U = \{u_t : t \in \mathbb{R}\}$ be a unipotent one-parameter subgroup of G_g and ϕ be a bounded continuous function on G_g/Γ_g. Let $\mathfrak{D}$ be a compact subset of G_g/Γ_g, and let $\epsilon > 0$*

be given. Then there exist finitely many proper closed subgroups $H_1, \dots, H_k$ of G_g such that $H_i \cap \Gamma_g$ is a lattice in H_i for all i and compact subsets $C_1, \dots, C_k$ of $X(H_1, U), \dots, X(H_k, U)$, respectively, such that for all compact subsets F of $\mathscr{D} - \bigcup_{1 \le i \le k} C_i \Gamma_g / \Gamma_g$ there exists a $T_0 > 0$ such that, for all $x \in F$ and $T > T_0$,

$$\left| \frac{1}{T} \int_0^T \phi(u_t x)\, dt - \int_{G_g/\Gamma_g} \phi\, d\mu_g \right| < \epsilon.$$

Remark 4.2. By construction, the subgroups H_i occurring are such that $H_i \cap \Gamma_g$ is Zariski-dense in H_i and hence H_i are defined over $\mathbb{Q}$. For a precise reference, see Theorem 3.6.2 and Remark 3.4.2 of [Kleinbock et al. 2002].

The next result is a reworking of Theorem 4.3 from [Eskin et al. 1998]. The difference is that in Lemma 4.3 the identity is fixed as the base point for the flow and the condition that H_g be maximal is dropped.

Lemma 4.3. *Suppose $r_1 \ge 2$ and $r_2 \ge 1$. Let $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$ be arbitrary. Let $U = \{u_t : t \in \mathbb{R}\}$ be a one-parameter unipotent subgroup of H_g, not contained in any proper normal subgroup of H_g. Let ϕ be a bounded continuous function on G_g/Γ_g. Then for all $\epsilon > 0$ and $\eta > 0$, there exists a $T_0 > 0$ such that, for all $T > T_0$,*

$$\nu_g\left(\left\{k \in K_g : \left| \frac{1}{T} \int_0^T \phi(u_t k)\, dt - \int_{G_g/\Gamma_g} \phi\, d\mu_g \right| > \epsilon \right\}\right) \le \eta. \tag{4-1}$$

Proof. Let $H_1, \dots, H_k$ and $C_1, \dots, C_k$ be as in Theorem 4.1. Let $\gamma \in \Gamma_g$; consider $Y_i(\gamma) = K_g \cap X(H_i, U)\gamma$. Suppose that $Y_i(\gamma) = K_g$; then $Uk\gamma^{-1} \subset k\gamma^{-1} H_i$ for all $k \in K_g$. In other words,

$$k^{-1} U k \subset \gamma^{-1} H_i \gamma \quad \text{for all } k \in K_g. \tag{4-2}$$

The subgroup $\langle k^{-1}Uk : k \in K_g \rangle$ is normalized by $U \cup K_g$ and clearly $\langle k^{-1}Uk : k \in K_g \rangle \subseteq \langle U \cup K_g \rangle \subseteq H_g$. If G is a simple Lie group with finite center, with maximal compact subgroup K, it follows from Exercise A.3, Chapter IV of [Helgason 2001] that K is also a maximal proper subgroup of G. This means that, because H_g is semisimple with finite center, any connected subgroup L of H_g containing K_g can be represented as $L = H' K_g$ where H' is a connected normal subgroup of H_g. Because U is not contained in any proper normal subgroup of H_g, this implies that $\langle U \cup K_g \rangle = H_g$. Therefore, $\langle k^{-1}Uk : k \in K_g \rangle$ is a normal subgroup of H_g, and because U is not contained in any proper normal subgroup of H_g, we have $\langle k^{-1}Uk : k \in K_g \rangle = H_g$. This and (4-2) imply that $H_g \subset \gamma^{-1} H_i \gamma$. Note that $\gamma \in \mathrm{SL}_d(\mathbb{Z})$ and, by Remark 4.2, H_i is defined over $\mathbb{Q}$. Therefore, $\gamma^{-1} H_i \gamma$ is defined over $\mathbb{Q}$; it follows from Theorem 7.7 of [Platonov and Rapinchuk 1991] that $\overline{\gamma^{-1} H_i \gamma \cap \mathrm{SL}_d(\mathbb{Q})} = \gamma^{-1} H_i \gamma$. Therefore, Lemma 3.7 and Proposition 4.1 of [Sargent 2013] imply that $\gamma^{-1} H_i \gamma = G_g$, which is a contradiction, and therefore,

$Y_i(\gamma) \subsetneq K_g$. This means, for all $1 \le i \le k$, $Y_i(\gamma)$ is a submanifold of strictly smaller dimension than K_g and hence

$$\nu_g(Y_i(\gamma)) = 0. \tag{4-3}$$

Note that, because $C_i \subseteq X(H_i, U)$,

$$K_g \cap \bigcup_{1\le i\le k} C_i\Gamma_g \subseteq K_g \cap \bigcup_{1\le i\le k} X(H_i, U)\Gamma_g = \bigcup_{1\le i\le k} \bigcup_{\gamma\in\Gamma_g} Y_i(\gamma),$$

and therefore, (4-3) implies

$$\nu_g\biggl(K_g \cap \bigcup_{1\le i\le k} C_i\Gamma_g\biggr) = 0. \tag{4-4}$$

Let $\mathfrak{D}$ be a compact subset of G_g such that $K_g \subset \mathfrak{D}$. Then from (4-4), it follows that, for all $\eta > 0$, there exists a compact subset F of $\mathfrak{D} - \bigcup_{1\le i\le k} C_i\Gamma_g$ such that

$$\nu_g(F \cap K_g) \ge 1 - \eta. \tag{4-5}$$

From Theorem 4.1, for all $\epsilon > 0$, there exists a $T_0 > 0$ such that, for all $x \in (F \cap K_g)/\Gamma_g$ and $T > T_0$,

$$\left|\frac{1}{T}\int_0^T \phi(u_t x)\,dt - \int_{G_g/\Gamma_g} \phi\,d\mu_g\right| < \epsilon.$$

Therefore, if $k \in K_g$, $T > T_0$ and

$$\left|\frac{1}{T}\int_0^T \phi(u_t k)\,dt - \int_{G_g/\Gamma_g} \phi\,d\mu_g\right| > \epsilon,$$

then $k \in K_g \setminus F$, but $\nu_g(K_g \setminus F) \le \eta$ by (4-5), and this implies (4-1). □

Lemma 4.4. *Suppose $r_1 \ge 2$ and $r_2 \ge 1$. Let $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$ be arbitrary. Let $U = \{u_t : t \in \mathbb{R}\}$ be a one-parameter unipotent subgroup of H_g not contained in any proper normal subgroup of H_g. Let ϕ be a bounded continuous function on G_g/Γ_g. Then for all $\epsilon > 0$ and $\delta > 0$, there exists a $T_0 > 0$ such that, for all $T > T_0$,*

$$\left|\frac{1}{\delta T}\int_T^{(1+\delta)T}\int_{K_g} \phi(u_t k)\,d\nu_g(k)\,dt - \int_{G_g/\Gamma_g} \phi\,d\mu_g\right| < \epsilon.$$

Proof. Let ϕ be a bounded continuous function on G_g/Γ_g. Lemma 4.3 implies for all $\epsilon > 0$, $\eta > 0$ and $d > 0$ there exists a $T_0 > 0$ such that, for all $T > T_0$,

$$\nu_g\left(\left\{k \in K_g : \left|\frac{1}{dT}\int_0^{dT} \phi(u_t k)\,dt - \int_{G_g/\Gamma_g} \phi\,d\mu_g\right| > \epsilon\right\}\right) \le \eta. \tag{4-6}$$

Using (4-6) with $d=1$ and $d=1+\delta$, we get that for all $\epsilon>0$ and $\eta>0$ there exists a subset $\mathscr{C}\subseteq K_g$ with $\nu_g(\mathscr{C})\geq 1-\eta$ such that for all $k\in\mathscr{C}$ the following hold:

$$\left|\int_0^T \phi(u_t k)\,dt - T\int_{G_g/\Gamma_g}\phi\,d\mu_g\right| < \epsilon T,$$

$$\left|\int_0^{(1+\delta)T} \phi(u_t k)\,dt - (1+\delta)T\int_{G_g/\Gamma_g}\phi\,d\mu_g\right| < (1+\delta)T\epsilon.$$

Hence, for all $k\in\mathscr{C}$, we have

$$\begin{aligned}
&\left|\int_T^{(1+\delta)T} \phi(u_t k)\,dt - \delta T\int_{G_g/\Gamma_g}\phi\,d\mu_g\right| \\
&\quad = \left|\int_0^{(1+\delta)T} \phi(u_t k)\,dt - (1+\delta)T\int_{G_g/\Gamma_g}\phi\,d\mu_g - \int_0^T \phi(u_t k)\,dt + T\int_{G_g/\Gamma_g}\phi\,d\mu_g\right| \\
&\quad \leq \left|\int_0^T \phi(u_t k)\,dt - T\int_{G_g/\Gamma_g}\phi\,d\mu_g\right| + \left|\int_0^{(1+\delta)T} \phi(u_t k)\,dt - (1+\delta)T\int_{G_g/\Gamma_g}\phi\,d\mu_g\right| \\
&\quad \leq (2+\delta)T\epsilon.
\end{aligned}$$

This means that, for all $\delta>0$, $\eta>0$ and $\epsilon>0$,

$$\nu_g\left(\left\{k\in K_g : \left|\frac{1}{\delta T}\int_T^{(1+\delta)T}\phi(u_t k)\,dt - \int_{G_g/\Gamma_g}\phi\,d\mu_g\right| < \frac{(2+\delta)\epsilon}{\delta}\right\}\right)\geq 1-\eta.$$

Since we can make ϵ and η as small as we wish, this implies the claim. □

Lemma 4.5. *Suppose $r_1\geq 2$ and $r_2\geq 1$. Let $A=\{a_t : t\in\mathbb{R}\}$ be a one-parameter subgroup of H_g, not contained in any proper normal subgroup of H_g, such that there exists a continuous homomorphism $\rho:\mathrm{SL}_2(\mathbb{R})\to H_g$ with $\rho(D)=A$ and $\rho(\mathrm{SO}(2))\subset K_g$, where $D=\left\{\begin{pmatrix} t & 0\\ 0 & t^{-1}\end{pmatrix} : t>0\right\}$. Let ϕ be a continuous function on G_g/Γ_g vanishing outside of a compact set. Then for all $g\in\mathscr{C}_{\mathrm{SL}}(r_1,r_2)$ and $\epsilon>0$ there exists $T_0>0$ such that, for all $t>T_0$,*

$$\left|\int_{K_g}\phi(a_t k)\,d\nu_g(k) - \int_{G_g/\Gamma_g}\phi\,d\mu_g\right|\leq\epsilon.$$

Proof. This is very similar to the proof of Theorem 4.4 from [Eskin et al. 1998], and some details will be omitted. Fix $\epsilon>0$. Assume that ϕ is uniformly continuous. Let $u_t=\begin{pmatrix} 1 & t\\ 0 & 1\end{pmatrix}$ and $w=\begin{pmatrix} 0 & -1\\ 1 & 0\end{pmatrix}$. Then it is clear that $d_t=\begin{pmatrix} t & 0\\ 0 & t^{-1}\end{pmatrix}=b_t u_t k_t w$, where $b_t=(1+t^{-2})^{-1/2}\begin{pmatrix} 1 & 0\\ -t^{-1} & 1+t^{-2}\end{pmatrix}$ and $k_t=(1+t^{-2})^{-1/2}\begin{pmatrix} 1 & t^{-1}\\ -t^{-1} & 1\end{pmatrix}$. By our assumptions on A, there exists a continuous homomorphism $\rho:\mathrm{SL}_2(\mathbb{R})\to H_g$ such that $\rho(D)=A$ and $\rho(\mathrm{SO}(2))\subset K_g$. Let $\rho(d_t)=d'_t$, $\rho(b_t)=b'_t$, $\rho(k_t)=k'_t$ and $\rho(w)=w'$. Then for all $t>0$ and $g\in\mathscr{C}_{\mathrm{SL}}(r_1,r_2)$,

$$\begin{aligned}\int_{K_g}\phi(d'_t k)\,d\nu_g(k)&=\int_{K_g}\phi(b'_t u'_t k'_t w' k)\,d\nu_g(k)\\&=\int_{K_g}\phi(b'_t u'_t k)\,d\nu_g(k)\end{aligned}\tag{4-7}$$

since $k'_t, w'\in K_g$. It follows from (4-7) that, for $r,t>0$,

$$\begin{aligned}&\left|\int_{K_g}\phi(d'_t k)\,d\nu_g(k)-\int_{K_g}\phi(u'_{rt}k)\,d\nu_g(k)\right|\\&\le\left|\int_{K_g}(\phi(d'_{rt}k)-\phi(d'_t k))\,d\nu_g(k)\right|+\left|\int_{K_g}(\phi(d'_{rt}k)-\phi(u'_{rt}k))d\nu_g(k)\right|\\&=\left|\int_{K_g}(\phi(d'_r d'_t k)-\phi(d'_t k))\,d\nu_g(k)\right|+\left|\int_{K_g}(\phi(b'_{rt}u'_{rt}k)-\phi(u'_{rt}k))\,d\nu_g(k)\right|.\end{aligned}\tag{4-8}$$

By uniform continuity, the fact that $\lim_{t\to\infty}b_t=I$ and (4-8) imply there exist $T_1>0$ and $\delta>0$ such that for $t>T_1$ and $|r-1|<\delta$ we have

$$\left|\int_{K_g}\phi(d'_t k)\,d\nu_g(k)-\int_{K_g}\phi(u'_{rt}k)\,d\nu_g(k)\right|\le\epsilon.$$

Thus, if $T>T_1$, then

$$\left|\int_{K_g}\phi(d'_t k)\,d\nu_g(k)-\frac{1}{\delta T}\int_T^{(1+\delta)T}\int_{K_g}\phi(u'_t k)\,d\nu_g(k)\,dt\right|\le\epsilon.\tag{4-9}$$

Combining (4-9) with Lemma 4.5 via the triangle inequality finishes the proof of the lemma. □

The section is completed by the proof of the main ergodic result, whose proof follows that of Theorem 3.5 in [Eskin et al. 1998].

Proof of Theorem 2.5. Assume that ϕ is nonnegative. Let $A(r)=\{x\in G_g/\Gamma_g:\alpha(x)>r\}$. Choose a continuous nonnegative function g_r on G_g/Γ_g such that $g_r(x)=1$ if $x\in A(r+1)$, $g_r(x)=0$ if $x\notin A(r)$ and $0\le g_r(x)\le 1$ if $x\in A(r)\setminus A(r+1)$. Then

$$\begin{aligned}&\int_{K_g}\phi(a_t k)\,d\nu_g(k)\\&\qquad=\int_{K_g}\phi(a_t k)\,g_r(a_t k)\,d\nu_g(k)+\int_{K_g}(\phi(a_t k)-\phi(a_t k)\,g_r(a_t k))\,d\nu_g(k).\end{aligned}\tag{4-10}$$

Let $\beta = 2-\delta$; then for $x \in G_g/\Gamma_g$,

$$\begin{aligned}\phi(x)\, g_r(x) &\le C\alpha(x)^{2-\beta} g_r(x)\\ &= C\alpha(x)^{2-\beta/2} g_r(x)\,\alpha(x)^{-\beta/2} \le Cr^{-\beta/2}\alpha(x)^{2-\beta/2}.\end{aligned}$$

The last inequality is true because $g_r(x) = 0$ if $\alpha(x) \le r$. Therefore,

$$\int_{K_g} \phi(a_t k)\, g_r(a_t k)\, d\nu_g(k) \le Cr^{-\beta/2} \int_{K_g} \alpha(a_t k)^{2-\beta/2}\, d\nu_g(k). \tag{4-11}$$

Since $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$, $r_1 \ge 3$ and $r_2 \ge 1$, Theorem 2.4(I) implies there exists B such that

$$\begin{aligned}\int_{K_g} \alpha(a_t k)^{2-\beta/2}\, d\nu_g(k) &= \int_{K_I} \alpha \circ g^{-1}(a_t k g)^{2-\beta/2}\, d\nu_I(k)\\ &\le c(g) \int_{K_I} \alpha(a_t k g)^{2-\beta/2}\, d\nu_I(k) < B\end{aligned}$$

for all $t \ge 0$. Then (4-11) implies that

$$\int_{K_g} \phi(a_t k)\, g_r(a_t k)\, d\nu_g(k) \le BCr^{-\beta/2}. \tag{4-12}$$

For all $\epsilon > 0$, there exists a compact subset, $\mathscr{C}$ of G_g/Γ_g, such that $\mu_g(\mathscr{C}) \ge 1-\epsilon$. The function α is bounded on $\mathscr{C}$, and hence, for all $\epsilon > 0$,

$$\begin{aligned}&\lim_{r\to\infty} \mu_g(A(r))\\ &\quad= \lim_{r\to\infty} \bigl(\mu_g(\{x \in \mathscr{C} : \alpha(x) > r\}) + \mu_g(\{x \in (G_g/\Gamma_g) \setminus \mathscr{C} : \alpha(x) > r\})\bigr) \le \epsilon.\end{aligned}$$

This means that

$$\lim_{r\to\infty} \mu_g(A(r)) = 0. \tag{4-13}$$

Note that

$$\int_{G_g/\Gamma_g} \phi(x)\, g_r(x)\, d\mu_g(x) \le \int_{A(r)} \phi(x)\, d\mu_g(x). \tag{4-14}$$

Since $\phi \in L^1(G_g/\Gamma_g)$, (4-13) and (4-14) imply that

$$\lim_{r\to\infty} \int_{G_g/\Gamma_g} \phi(x)\, g_r(x)\, d\mu_g(x) = 0. \tag{4-15}$$

Since the function $\phi(x) - \phi(x)g_r(x)$ is continuous and has compact support, Lemma 4.5 implies for all $\epsilon > 0$ and $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$ there exists $T_0 > 0$ such that, for all $t > T_0$,

$$\left| \int_{K_g} (\phi(a_t k) - \phi(a_t k)\, g_r(a_t k))\, d\nu_g(k) \right.$$
$$\left. - \int_{G_g/\Gamma_g} (\phi(x) - \phi(x)\, g_r(x))\, d\mu_g(x) \right| < \frac{\epsilon}{2}. \quad (4\text{-}16)$$

It is straightforward to check that (4-10), (4-12), (4-15) and (4-16) imply the conclusion of the theorem if r is sufficiently large. □

5. Proof of Theorem 2.1

The proof of Theorem 2.1 follows the same route as that of Sections 3.4–3.5 of [Eskin et al. 1998]. The main modification we make in order to handle the present situation is that we work inside the surface $X_g(\mathbb{R})$ rather than in the whole of $\mathbb{R}^d$. For $t \in \mathbb{R}$ and $v \in \mathbb{R}^d$, define a linear map a_t by

$$a_t v = (v_1, \ldots, v_s, e^{-t} v_{s+1}, v_{s+2}, \ldots, e^t v_d).$$

Note that the one-parameter group $\{\hat{a}_t : t \in \mathbb{R}\} = g^{-1}\{a_t : t \in \mathbb{R}\}g \subset H_g$ and that there exists a continuous homomorphism $\rho : \mathrm{SL}_2(\mathbb{R}) \to H_g$ with $\rho(D) = \{\hat{a}_t : t \in \mathbb{R}\}$ and $\rho(\mathrm{SO}(2)) \subset K_g$ where $D = \left\{ \left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right) : t > 0 \right\}$. Moreover, note that $\{a_t : t \in \mathbb{R}\}$ is self-adjoint and not contained in any normal subgroup of H_g and the only eigenvalues of a_t are e^{-t}, 1 and e^t. In other words, $\{\hat{a}_t : t \in \mathbb{R}\}$ satisfies the conditions of Theorems 2.5 and 2.4. For any natural number n, let S^{n-1} denote the unit sphere in an n-dimensional Euclidean space and let $\gamma_n = \mathrm{Vol}(S^n)$ and $c_{r_1,r_2} = \gamma_{r_1-1}\gamma_{r_2-1}$; then define

$$C_1 = c_{r_1,r_2} 2^{(2-r_1-r_2)/2} = c_{r_1,r_2} 2^{(2-d+s)/2}. \quad (5\text{-}1)$$

5A. ***Proof of Theorem 2.3.*** In Lemma 5.1, it is shown that it is possible to approximate certain integrals over K_g by integrals over $\mathbb{R}^{d-s-2}$. The integral over $\mathbb{R}^{d-s-2}$ can be used like the characteristic function of $R \times A(T/2, T)$; in particular, Theorem 2.3 is proved as an application of Lemma 5.1. It should be noted that Lemma 5.1 is analogous to Lemma 3.6 from [Eskin et al. 1998] and its proof is similar.

Lemma 5.1. *Let f be a continuous function of compact support on $\mathbb{R}^d_+ = \{v \in \mathbb{R}^d : \langle v, e_{s+1}\rangle > 0\}$, and for $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$, let*

$$J_{f,g}(\ell_1, \ldots, \ell_s, r) = \frac{1}{r^{d-s-2}} \int_{\mathbb{R}^{d-s-2}} f(\ell_1, \ldots, \ell_s, r, v_{s+2}, \ldots, v_{d-1}, v_d)\, dv_{s+2} \cdots dv_{d-1},$$

where $v_d = (a - Q_0^g(\ell_1, \ldots, \ell_s, 0, v_{s+2}, \ldots, v_{d-1}, 0))/2r$ so that $Q_0^g(\ell_1, \ldots, \ell_s, r, v_{s+2}, \ldots, v_{d-1}, v_d) = a$. Then for every $\epsilon > 0$, there exists $T_0 > 0$ such that, for *every t with $e^t > T_0$ and every $v \in \mathbb{R}_+^d$ with $\|v\| > T_0$,*

$$\left| C_1 e^{(d-s-2)t} \int_{K_g} f(\hat{a}_t k v)\, d\nu_g(k) - J_{f,g}(M_0^g(v), \|v\| e^{-t}) \right| < \epsilon.$$

Proof. By Lemma 2.2 of [Sargent 2013], for all $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$, there exists a basis of $\mathbb{R}^d$, denoted by $b_1, \dots, b_d$, such that

$$Q_0^g(v) = Q_{1,\dots,s}(v) + 2v_{s+1}v_d + \sum_{i=s+2}^{s+r_1} v_i^2 - \sum_{i=s+r_1+1}^{d-1} v_i^2 \quad \text{and} \quad M_0^g(v) = (v_1, \dots, v_s)$$

and

$$\hat{a}_t(v) = (v_1, \dots v_s, e^{-t} v_{s+1}, v_{s+2}, \dots v_{d-1}, e^t v_d),$$

where $v_i = \langle v, b_i \rangle$ for $1 \le i \le d$ and $Q_{1,\dots,s}(v)$ is a nondegenerate quadratic form in variables $v_1, \dots, v_s$. Let E denote the support of f. Let $c_1 = \inf_{v \in E} \langle v, b_{s+1} \rangle$ and $c_2 = \sup_{v \in E} \langle v, b_{s+1} \rangle$. From the definition of $\hat{a}_t$, it follows that $f(\hat{a}_t w) = 0$ unless

$$|\langle w, b_{s+1} \rangle \langle w, b_d \rangle| \le \beta, \tag{5-2}$$

$$c_1 \le \langle w, b_{s+1} \rangle e^{-t} \le c_2, \tag{5-3}$$

$$\pi'(w) \in \pi'(E), \tag{5-4}$$

where β depends only on E and π' denotes the projection onto the span of $b_1, \dots, b_s$, $b_{s+2}, \dots, b_{d-1}$. For w satisfying (5-2) and (5-3), we have $\langle w, b_d \rangle = O(e^{-t})$. This, together with (5-4) and (5-3), implies that, if $f(\hat{a}_t w) \ne 0$ and t is large, then

$$\|w\| = \langle w, b_{s+1} \rangle + O(e^{-t}). \tag{5-5}$$

Note that by (5-5),

$$\langle \hat{a}_t w, b_{s+1} \rangle = \langle w, b_{s+1} \rangle e^{-t} = e^{-t} \|w\| + O(e^{-2t}) \tag{5-6}$$

and

$$\langle \hat{a}_t w, b_i \rangle = \langle w, b_i \rangle \quad \text{for } 1 \le i \le s \text{ or } s+2 \le i \le d-1. \tag{5-7}$$

Finally,

$$\begin{aligned} \langle \hat{a}_t w, b_d \rangle &= \big(Q_0^g(w) - Q_0^g\big(\langle w, b_1 \rangle, \dots, \langle w, b_s \rangle, 0, \\ &\qquad\qquad \langle w, b_{s+1} \rangle, \dots, \langle w, b_{d-1} \rangle, 0\big)\big) / 2\langle \hat{a}_t w, b_{s+1} \rangle \\ &= \big(Q_0^g(w) - Q_0^g\big(\langle w, b_1 \rangle, \dots, \langle w, b_s \rangle, 0, \\ &\qquad\qquad \langle w, b_{s+1} \rangle, \dots, \langle w, b_{d-1} \rangle, 0\big)\big) / 2e^{-t} \|w\| + O(e^{-t}). \end{aligned} \tag{5-8}$$

Hence, using (5-6), (5-7) and (5-8) together with the uniform continuity of f, applied with $w = kv$ for $v \in \mathbb{R}_+^d$ and $k \in K_g$, we see that for all $\delta > 0$ there exists a

$t_0 > 0$ so that if $t > t_0$ then

$$\left| f(\hat{a}_t kv) - f(v_1, \ldots, v_s, \|v\| e^{-t}, \langle kv, b_{s+1}\rangle, \ldots, \langle kv, b_{d-1}\rangle, v_d) \right| < \delta, \tag{5-9}$$

where v_d is determined by

$$Q_0^g(v_1, \ldots, v_s, \|v\| e^{-t}, \langle kv, b_{s+1}\rangle, \ldots, \langle kv, b_{d-1}\rangle, v_d) = Q_0^g(v) = a.$$

Change basis by letting $f_{s+1} = (b_{s+1} + b_d)/\sqrt{2}$, $f_d = (b_{s+1} - b_d)/\sqrt{2}$ and $f_i = b_i$ for $1 \le i \le s$ or $s+2 \le i \le d-1$. In this basis, $K_g \cong \mathrm{SO}(r_1) \times \mathrm{SO}(r_2)$ consists of orthogonal matrices preserving the subspaces $L_1 = \langle f_1, \ldots, f_s\rangle$, $L_2 = \langle f_{s+1}, \ldots, f_{s+r_1}\rangle$ and $L_3 = \langle f_{s+r_1+1}, \ldots, f_d\rangle$. For $i = 1, 2$ or 3, let π_i denote the orthogonal projection onto L_i. Write $\rho_i = \|\pi_i(v)\|$; then the orbit $K_g v$ is the product of a point and two spheres $\{v_1, \ldots, v_s\} \times \rho_2 S^{r_1-1} \times \rho_3 S^{r_2-1}$, where S^{r_1-1} denotes the unit sphere in L_2 and S^{r_2-1} the unit sphere in L_3.

Suppose $w \in K_g v$ is such that $f(\hat{a}_t w) \ne 0$. Then from (5-2) and (5-3), it follows that $\langle w, b_d\rangle = O(e^{-t})$. Now, set $w_i = \langle w, f_i\rangle$; then $w_{s+1} = 2^{-1/2}\langle w, b_{s+1}\rangle + O(e^{-t})$, $w_d = 2^{-1/2}\langle w, b_{s+1}\rangle + O(e^{-t})$ and, for $1 \le i \le s$ or $s+2 \le i \le d-1$, $w_i = O(1)$. Hence, for $i = 2$ or 3,

$$\rho_i = \|\pi_i(w)\| = 2^{-1/2}\langle w, b_{s+1}\rangle + O(e^{-t}) = 2^{-1/2}\|w\| + O(e^{-t}), \tag{5-10}$$

where the last estimate follows from (5-5).

By integrating (5-9) with respect to K_g, we see that for all $\epsilon > 0$ there exists a $t_0 > 0$ so that if $t > t_0$ then

$$\begin{aligned}\Bigg| \int_{K_g} & f(\hat{a}_t kv)\, d\nu_g(k) \\ & - \int_{K_g} f(v_1, \ldots, v_s, \|v\| e^{-t}, \langle kv, b_{s+1}\rangle, \ldots, \langle kv, b_{d-1}\rangle, v_d)\, d\nu_g(k) \Bigg| < \epsilon. \end{aligned} \tag{5-11}$$

Equation (5-4) implies that, if $f(\hat{a}_t kv) \ne 0$, then kv is within a bounded distance from $\rho_2 f_{s+1} + \rho_3 f_d$. As $\|v\|$ increases, so do the ρ_i and the normalized Haar measure on $\rho_2 S^{r_1-1}$ near $\rho_2 f_{s+1}$ tends to $(1/\operatorname{Vol}(\rho_2 S^{r_1-1}))\, dv_{s+2} \cdots dv_{s+r_1}$ and similarly the Haar measure on $\rho_3 S^{r_2-1}$ near $\rho_3 f_d$ tends to $(1/\operatorname{Vol}(\rho_3 S^{r_2-1}))\, dv_{s+r_1+1} \cdots dv_{d-1}$. This means that as $\|v\|$ tends to infinity the second integral in (5-11) tends to

$$\begin{aligned}\frac{\rho_2^{1-r_1}\rho_3^{1-r_2}}{c_{r_1,r_2}} \int_{\mathbb{R}^{d-s-2}} & f(v_1, \ldots, v_s, \|v\| e^{-t}, v_{s+1}, \ldots, v_d)\, dv_{s+2} \cdots dv_{d-1} \\ &= \frac{(\|v\| e^{-t})^{d-s-2}}{\rho_2^{r_1-1}\rho_3^{r_2-1} c_{r_1,r_2}} J_{f,g}(M_0^g(v), \|v\| e^{-t}). \end{aligned} \tag{5-12}$$

Because (5-10) implies that $\rho_2^{r_1-1}\rho_3^{r_2-1} = 2^{(s+2-d)/2}\|v\|^{d-s-2} + O(e^{-t})$, we can use (5-11) and (5-12) to get that for all $\epsilon > 0$ there exists a $t_0 > 0$ so that if $t > t_0$

and $\|v\| > t_0$ then

$$\left| \int_{K_g} f(\hat{a}_t k v)\, d\nu_g(k) - \frac{e^{t(s+2-d)}}{C_1} J_{f,g}(M_0^g(v), \|v\| e^{-t}) \right| < \epsilon.$$

By dividing through by the factor $\frac{e^{t(s+2-d)}}{C_1}$, we obtain the desired conclusion. □

For f_1 and f_2 continuous functions of compact support on $\mathbb{R}^d_+ = \{v \in \mathbb{R}^d : \langle v, e_{s+1}\rangle > 0\}$, define $J_{f_1,g} + J_{f_2,g} = J_{f_1+f_2,g}$ and $J_{f_1,g} J_{f_2,g} = J_{f_1 f_2,g}$. These operations make the collection of functions of the form $J_{f,g}$ into an algebra of real-valued functions on the set $\mathbb{R}^s \times \{v \in \mathbb{R} : v > 0\}$. Denote this algebra by $\mathscr{A}$. The following will be used in the proofs of Theorems 2.3 and 2.1:

Lemma 5.2. *$\mathscr{A}$ is dense in $C_c(\mathbb{R}^s \times \{v \in \mathbb{R} : v > 0\})$.*

Proof. Let B be a compact subset of $\mathbb{R}^s \times \{v \in \mathbb{R} : v > 0\}$. Let $\mathscr{A}_B$ denote the subalgebra of $\mathscr{A}$ of functions with support B. It is straightforward to check that the algebra $\mathscr{A}_B$ separates points in B and does not vanish at any point in B. Therefore, by the Stone–Weierstrass theorem [Rudin 1976, Theorem 7.32], $\mathscr{A}_B$ is dense in the space of continuous functions on B. Since B is arbitrary, this implies the claim. □

Proof of Theorem 2.3. Let $\epsilon > 0$ be arbitrary and $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$. By Lemma 5.2, there exists a continuous nonnegative function f on $\mathbb{R}^d_+$ of compact support so that $J_{f,g} \geq 1+\epsilon$ on $R \times [1, 2]$. Then if $v \in \mathbb{R}^d$ satisfies $e^t \leq \|v\| \leq 2e^t$, $M_0^g(v) \in R$ and $Q_0^g(v) = a$, then $J_{f,g}(M_0^g(v), \|v\| e^{-t}) \geq 1+\epsilon$. Then by Lemma 5.1, for sufficiently large t,

$$C_1 e^{(d-s-2)t} \int_{K_g} f(\hat{a}_t k v)\, d\nu_g(k) \geq 1$$

if $e^t \leq \|v\| \leq 2e^t$, $M_0^g(v) \in R$ and $Q_0^g(v) = a$. Then summing over $v \in X_g(\mathbb{Z})$, we get

$$\begin{aligned} |X_g(\mathbb{Z}) \cap V_M([a, b]) \cap A(e^t, 2e^t)| &\leq \sum_{v \in X_g(\mathbb{Z})} C_1 e^{(d-s-2)t} \int_{K_g} f(\hat{a}_t k v)\, d\nu_g(k) \\ &= C_1 e^{(d-s-2)t} \int_{K_g} F_{f,g}(\hat{a}_t k)\, d\nu_g(k). \end{aligned} \tag{5-13}$$

Note that

$$\int_{K_g} F_{f,g}(\hat{a}_t k)\, d\nu_g(k) = \int_{K_I} F_{f,g}(g^{-1} a_t k g)\, d\nu_I(k). \tag{5-14}$$

By (2-2), we have the bound $F_{f,g}(x) \leq c(f)\, \alpha(x)$ for all $x \in G_g/\Gamma_g$, where $c(f)$ is a constant depending only on f. Since $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$, Part (I) of Theorem 2.4

implies that if $r_1 \geq 3$ and $r_2 \geq 1$ then

$$\int_{K_I} F_{f,g}(g^{-1}a_t kg)\, d\nu_I(k) < c(f \circ g^{-1}) \int_{K_I} \alpha(a_t kg)\, d\nu_I(k) < \infty. \tag{5-15}$$

In the case when $r_1 = 2$ and $r_2 = 1$ or $r_1 = r_2 = 2$, Part (II) of Theorem 2.4 implies that for all $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$ there exists a constant C so that

$$\int_{K_I} F_{f,g}(g^{-1}a_t kg)\, d\nu_I(k) < c(f \circ g^{-1}) \int_{K_I} \alpha(a_t kg)\, d\nu_I(k) < Ct. \tag{5-16}$$

Hence, (5-13), (5-14) and (5-15) imply that as long as $r_1 \geq 3$ and $r_2 \geq 1$ there exists a constant C_2 such that

$$|X_g(\mathbb{Z}) \cap V_M(R) \cap A(e^t, 2e^t)| \leq C_2 e^{(d-s-2)t}.$$

Similarly, (5-13), (5-14) and (5-16) imply that, if $r_1 = 2$ and $r_2 = 1$ or $r_1 = r_2 = 2$, then

$$|X_g(\mathbb{Z}) \cap V_M(R) \cap A(e^t, 2e^t)| \leq C_2 t e^{(d-s-2)t}.$$

Since we can write $T = e^t$ and

$$A(0, T) = \lim_{n\to\infty} \left(A(0, T/2^n) \bigcup_{i=1}^{n} A(T/2^i, T/2^{i-1}) \right),$$

the theorem follows by summing a geometric series. $\square$

Theorem 2.3 has the following corollary, which is comparable with Proposition 3.7 from [Eskin et al. 1998] and will be used in the proof of Theorem 2.1.

Corollary 5.3. *Let f be a continuous function of compact support on $\mathbb{R}^d_+$. Then for every $\epsilon > 0$ and $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$, there exists $t_0 > 0$ so that, for $t > t_0$,*

$$\left| e^{-(d-s-2)t} \sum_{v \in X_g(\mathbb{Z})} J_{f,g}(M_0^g(v), \|v\| e^{-t}) - C_1 \int_{K_g} F_{f,g}(\hat{a}_t k)\, d\nu_g(k) \right| < \epsilon. \tag{5-17}$$

Proof. Since $J_{f,g}$ has compact support, the number of nonzero terms in the sum on the left-hand side of (5-17) is bounded by $ce^{(d-s-2)t}$ because of Theorem 2.3. Hence, summing the result of Lemma 5.1 over $v \in X_g(\mathbb{Z})$ proves (5-17). $\square$

5B. ***Volume estimates.*** For a compactly supported function h on $\mathbb{R}^s \times \mathbb{R}^d \setminus \{0\}$, we define

$$\Theta(h, T) = \int_{X_g(\mathbb{R})} h(M_0^g(v), v/T)\, dm_g(v).$$

For $\mathscr{X} \subseteq \mathbb{R}^d$, we will use the notation $\mathrm{Vol}_{X_g}(\mathscr{X}) = \int_{X_g(\mathbb{R})} \mathbb{1}_{\mathscr{X} \cap X_g(\mathbb{R})}\, dm_g$ to mean the volume of $\mathscr{X}$ with respect to the volume measure on $X_g(\mathbb{R})$.

The following lemma and its corollary are analogous to Lemma 3.8 from [Eskin et al. 1998], and the proofs share some similarities although it is here that the fact we are integrating over $X_g(\mathbb{R})$ rather than the whole of $\mathbb{R}^d$ becomes an important distinction. In Lemma 5.4, we compute $\lim_{T\to\infty}(1/T^{d-s-2})\Theta(h,T)$. Here it is crucial that h is not defined on $\mathbb{R}^s\times\{0\}$; if it was, using the fact that h can be bounded by an integrable function, one could directly pass the limit inside the integral and the limit would be 0. The basic strategy of Lemma 5.4 is that we evaluate the integral $\int_{X_g(\mathbb{R})} dm_g$ by switching to polar coordinates. This has the effect that the integral changes into an integral over two spheres; then we approximate the spheres by an orbit of K_g and an integral over the coordinates fixed by K_g.

Lemma 5.4. *Suppose that h is a continuous function of compact support in $\mathbb{R}^s\times\mathbb{R}^d\setminus\{0\}$. Then*

$$\lim_{T\to\infty}\frac{1}{T^{d-s-2}}\Theta(h,T)=C_1\int_{K_g}\int_0^\infty\int_{\mathbb{R}^s}h(z,rke_0)r^{d-s-2}\,dz\,\frac{dr}{2r}\,d\nu_g(k),$$

where e_0 is a unit vector in $\mathbb{R}^d$ and C_1 is the constant defined by (5-1).

Proof. By Lemma 2.2 of [Sargent 2013], for all $g\in\mathscr{C}_{\mathrm{SL}}(r_1,r_2)$, there exists a basis of $\mathbb{R}^d$, denoted by $f_1,\dots,f_d$, such that

$$Q_0^g(v)=\sum_{i=1}^{s_1}v_i^2-\sum_{i=s_1+1}^{s}v_i^2+\sum_{i=s+1}^{s+r_1}v_i^2-\sum_{i=s+r_1+1}^{d}v_i^2\quad\text{and}\quad M_0^g(v)=J(v_1,\dots,v_s),$$

where $v_i=\langle v,f_i\rangle$ for $1\le i\le d$, $J\in\mathrm{GL}_s(\mathbb{R})$, s_1 is a nonnegative integer such that $r_1+s_1=p$ and s_2 is a nonnegative integer such that $r_2+s_2=d-p$. Let $L_1=\langle v_1,\dots,v_{s_1},v_{s+1},\dots,v_{s+r_1}\rangle$, $L_2=\langle v_{s_1+1},\dots,v_s,v_{s+r_1+1},\dots,v_d\rangle$, S^{p-1} be the unit sphere inside L_1 and S^{d-p-1} be the unit sphere inside L_2. Let $\alpha\in S^{p-1}$ and $\beta\in S^{d-p-1}$. Using polar coordinates, we can parametrize $v\in X_g(\mathbb{R})$ so that

$$v_i=\begin{cases}\sqrt{a}\alpha_i\cosh t & \text{for } 1\le i\le s_1,\\ \sqrt{a}\beta_{i-s_1}\sinh t & \text{for } s_1+1\le i\le s,\\ \sqrt{a}\alpha_{i-s+s_1}\cosh t & \text{for } s+1\le i\le s+r_1,\\ \sqrt{a}\beta_{i-s_1-r_1}\sinh t & \text{for } s+r_1+1\le i\le d.\end{cases}\tag{5-18}$$

In these coordinates, we may write

$$dm_g(v)=\frac{a^{(d-2)/2}}{2}\cosh^{p-1}t\,\sinh^{q-1}t\,dt\,d\xi(\alpha,\beta)=P(e^t)\,dt\,d\xi(\alpha,\beta),$$

where $P(x)=(a^{(d-2)/2}/2^{d-1})x^{d-2}+O(x^{d-3})$ and ξ is the Haar measure on $S^{p-1}\times S^{q-1}$. Making the change of variables, $r=\sqrt{a}e^t/2T$, gives

$$\sqrt{a}\cosh t=Tr+a/4Tr\quad\text{and}\quad\sqrt{a}\sinh t=Tr-a/4Tr.\tag{5-19}$$

Let $L_1' = \langle v_{s+1}, \dots, v_{s+r_1} \rangle$, $L_2' = \langle v_{s+r_1+1}, \dots, v_d \rangle$, S^{r_1-1} be the unit sphere inside L_1', S^{r_2-1} be the unit sphere inside L_2', $\alpha' \in S^{r_1-1}$ and $\beta' \in S^{r_2-1}$. We may write

$$d\xi(\alpha,\beta) = \delta(\alpha,\beta)\, d\alpha_1 \cdots d\alpha_{s_1}\, d\beta_1 \cdots d\beta_{s_2}\, d\xi'(\alpha',\beta'),$$

where $\delta(\alpha,\beta)$ is the appropriate density function and $d\xi'$ is the Haar measure on $S^{r_1-1} \times S^{r_2-1}$. This gives

$$dm_g(v) = P\Big(\frac{2Tr}{\sqrt{a}}\Big)\, \delta(\alpha,\beta)\, \frac{dr}{r}\, d\alpha_1 \cdots d\alpha_{s_1}\, d\beta_1 \cdots d\beta_{s_2}\, d\xi'(\alpha',\beta'). \tag{5-20}$$

Let $z \in \mathbb{R}^s$. Make the further change of variables

$$(\alpha_1, \dots, \alpha_{s_1}, \beta_1, \dots, \beta_{s-s_1}) = \frac{1}{Tr} J^{-1} z; \tag{5-21}$$

this means that

$$d\alpha_1 \cdots d\alpha_{s_1}\, d\beta_1 \cdots d\beta_{s_2} = \frac{1}{\det(J)(Tr)^s}\, dz. \tag{5-22}$$

Moreover, using (5-18), (5-19) and (5-21) gives

$$M_0^g(v) = z + O(1/T) \quad \text{and} \quad v/T = r(\alpha' + \beta') + O(1/T). \tag{5-23}$$

Since h is continuous and compactly supported, it may bounded by an integrable function and hence

$$\begin{aligned}
&\lim_{T\to\infty} \frac{1}{T^{d-s-2}} \Theta(h,T) \\
&\qquad = \lim_{T\to\infty} \frac{1}{T^{d-s-2}} \int_{X_g(\mathbb{R})} h(M_0^g(v), v/T)\, dm_g(v) \\
&\qquad = \int_{X_g(\mathbb{R})} \lim_{T\to\infty} \frac{1}{T^{d-s-2}} h(M_0^g(v), v/T)\, dm_g(v) \\
&\qquad = \int_{S^{r_1-1}\times S^{r_2-1}} \int_0^\infty \int_{\mathbb{R}^s} h(z, r(\alpha'+\beta')) r^{d-s-2} \delta(\alpha',\beta')\, dz\, \frac{dr}{2r}\, d\xi'(\alpha',\beta'),
\end{aligned}$$

where the last step follows from (5-20), the definition of $P(x)$, (5-22) and (5-23). Note that from the definition of δ it is clear that $\delta(\alpha',\beta') = 1$. Finally, let $e_0 = \frac{1}{\sqrt{2}}(f_1 + f_{p+1})$ and $\frac{1}{\sqrt{2}}(\alpha' + \beta') = ke_0$ and $r' = \sqrt{2} r$ to get that

$$\lim_{T\to\infty} \frac{1}{T^{d-s-2}} \Theta(h,T) = C_1 \int_{K_g} \int_0^\infty \int_{\mathbb{R}^s} h(z, r'ke_0) r'^{d-s-2}\, dz\, \frac{dr'}{2r'}\, d\nu_g(k). \quad \square$$

Corollary 5.5. *For all $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$, there exists a constant $C_3 > 0$ such that for all compact regions $R \subset \mathbb{R}^s$ with piecewise smooth boundary*

$$\lim_{T\to\infty} \frac{1}{T^{d-s-2}} \operatorname{Vol}_{X_g}(V_{M_0^g}(R) \cap A(T/2, T)) = C_3 \operatorname{Vol}(R).$$

Proof. Let $\mathbb{1}$ denote the characteristic function of $R \times A(1/2, 1)$; then it is clear that

$$\lim_{T\to\infty} \frac{1}{T^{d-s-2}} \operatorname{Vol}_{X_g}(V_{M_0^g}(R) \cap A(T/2, T)) = \lim_{T\to\infty} \frac{1}{T^{d-s-2}} \int_{X_g(\mathbb{R})} \mathbb{1}(M_0(gv), v/T)\, dm_g(v) = \lim_{T\to\infty} \frac{1}{T^{d-s-2}} \Theta(\mathbb{1}, T).$$

Since R has piecewise smooth boundary, there exist regions $R_\delta^- \subseteq R \times A(1/2, 1) \subseteq R_\delta^+$ such that $\lim_{\delta\to 0} R_\delta^+ = \lim_{\delta\to 0} R_\delta^- = R$, and for all $\delta > 0$, we can choose continuous compactly supported functions h_δ^- and h_δ^+ on $\mathbb{R}^s \times \mathbb{R}^d \setminus 0$ such that $0 \le h_\delta^- \le \mathbb{1} \le h_\delta^+ \le 1$, $h_\delta^-(v) = \mathbb{1}(v)$ if $v \in R_\delta^-$ and $h_\delta^+(v) = 0$ if $v \notin R_\delta^+$. By Lemma 5.4,

$$\begin{aligned} \lim_{T\to\infty} \frac{1}{T^{d-s-2}} \Theta(h_\delta^-, T) &\le \liminf_{T\to\infty} \frac{1}{T^{d-s-2}} \int_{X_g(\mathbb{R})} \mathbb{1}(M_0(gv), v/T)\, dm_g(v) \\ &\le \limsup_{T\to\infty} \frac{1}{T^{d-s-2}} \int_{X_g(\mathbb{R})} \mathbb{1}(M_0(gv), v/T)\, dm_g(v) \\ &\le \lim_{T\to\infty} \frac{1}{T^{d-s-2}} \Theta(h_\delta^+, T). \end{aligned}$$

It is clear that

$$\begin{aligned} \lim_{\delta\to\infty} \lim_{T\to\infty} \frac{1}{T^{d-s-2}} \Theta(h_\delta^-, T) &= \lim_{\delta\to\infty} \lim_{T\to\infty} \frac{1}{T^{d-s-2}} \Theta(h_\delta^+, T) \\ &= \lim_{T\to\infty} \frac{1}{T^{d-s-2}} \Theta(\mathbb{1}, T); \end{aligned}$$

hence, we can apply Lemma 5.4 to get that

$$\begin{aligned} &\lim_{T\to\infty} \frac{1}{T^{d-s-2}} \Theta(\mathbb{1}, T) \\ &\quad = C_1 \int_{K_g} \int_0^\infty \int_{\mathbb{R}^s} \mathbb{1}(z, rk^{-1}e_0) r^{d-s-2}\, dz\, \frac{dr}{2r}\, d\nu_g(k) \\ &\quad = C_1 \int_{\mathbb{R}^s} \mathbb{1}_R(z)\, dz \int_{K_g} \int_0^\infty \mathbb{1}_{A(1/2,1)}(rk^{-1}e_0) r^{d-s-2}\, \frac{dr}{2r}\, d\nu_g(k) = C_3 \operatorname{Vol}(R). \end{aligned}$$

The last equality holds because

$$\int_{K_g} \int_0^\infty \mathbb{1}_{A(1/2,1)}(rk^{-1}e_0) r^{d-s-2}\, \frac{dr}{2r}\, d\nu_g(k) < \infty$$

as $\mathbb{1}_{A(1/2,1)}$ has compact support and K_g is compact. □

5C. ***Proof of Theorem 2.1.*** By Theorem 4.9 of [Platonov and Rapinchuk 1991], there exist $v_1, \dots, v_j \in X_g(\mathbb{Z})$ such that $X_g(\mathbb{Z}) = \bigsqcup_{i=1}^{j} \Gamma_g v_i$. Let $P_i(g) = \{x \in G_g : xv_i = v_i\}$ and $\Lambda_i(g) = P_i(g) \cap \Gamma_g$. By Proposition 1.13 of [Helgason 2000], there exist Haar measures ϱ_{Λ_i}, p_{Λ_i} and γ_{Λ_i} on $G_g/\Lambda_i(g)$, $P_i(g)/\Lambda_i(g)$ and $\Gamma_g/\Lambda_i(g)$, respectively, such that, for $f \in C_c(G_g/\Lambda_i(g))$ and hence for integrable functions on $G_g/\Lambda_i(g)$,

$$\int_{G_g/\Lambda_i(g)} f d\varrho_{\Lambda_i} = \int_{X_g(\mathbb{R})} \int_{P_i(g)/\Lambda_i(g)} f(xp)\, dp_{\Lambda_i}(p)\, dm_g(x), \tag{5-24}$$

$$\int_{G_g/\Lambda_i(g)} f\, d\varrho_{\Lambda_i} = \int_{G_g/\Gamma_g} \int_{\Gamma_g/\Lambda_i(g)} f(x\gamma)\, d\gamma_{\Lambda_i}(\gamma)\, d\mu_g(x). \tag{5-25}$$

Note that $\Gamma_g/\Lambda_i(g) = \Gamma_g v_i$ is discrete and its Haar measure $d\gamma_{\Lambda_i}$ is just the counting measure and so

$$\int_{\Gamma_g/\Lambda_i(g)} f(x\gamma)\, d\gamma_{\Lambda_i}(\gamma) = \sum_{v \in \Gamma_g v_i} f(xv). \tag{5-26}$$

Therefore, the normalizations already present on m_g and μ_g induce a normalization on p_{Λ_i}. Moreover, it follows from the Borel–Harish-Chandra theorem [Platonov and Rapinchuk 1991, Theorem 4.13] that the measure of $p_{\Lambda_i}(P_i(g)/\Lambda_i(g)) < \infty$ for each $1 \le i \le j$. As in [Eskin et al. 1998; Dani and Margulis 1993], where the proofs rely on Siegel's integral formula, here the proof relies on the following result:

Lemma 5.6. *For all $f \in C_c(X_g(\mathbb{R}))$ and $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$, there exists a constant*

$$C(g) = \sum_{i=1}^{j} p_{\Lambda_i}(P_i(g)/\Lambda_i(g))$$

such that

$$C(g) \int_{X_g(\mathbb{R})} f\, dm_g = \int_{G_g/\Gamma_g} F_{f,g}\, d\mu_g. \tag{5-27}$$

Proof. Note that, for $1 \le i \le j$, $G_g/P_i(g) \cong X_g(\mathbb{R})$. If $f \in C_c(X_g(\mathbb{R}))$, then f is $\Lambda_i(g)$-invariant and therefore can be considered as an integrable function on $G_g/\Lambda_i(g)$ and so

$$\int_{X_g(\mathbb{R})} \int_{P_i(g)/\Lambda_i(g)} f(xp)\, dp_{\Lambda_i}(p)\, dm_g(x) = \int_{P_i(g)/\Lambda_i(g)} dp_{\Lambda_i} \int_{X_g(\mathbb{R})} f\, dm_g. \tag{5-28}$$

Now it follows from the definition of $F_{f,g}$ (i.e., (2-1)), (5-24), (5-25), (5-26) and (5-28) that

$$\int_{G_g/\Gamma_g} F_{f,g}\, d\mu_g = \sum_{i=1}^{j} \int_{G_g/\Gamma_g} \sum_{v\in\Gamma_g v_i} f(xv)\, d\mu_g(x)$$
$$= \sum_{i=1}^{j} \int_{P_i(g)/\Lambda_i(g)} dp_{\Lambda_i} \int_{X_g(\mathbb{R})} f\, dm_g,$$

which is the desired result. □

The final lemma of this section is the counterpart of Lemma 3.9 from [Eskin et al. 1998], and again the proof there is mimicked.

Lemma 5.7. *Let f be a continuous function of compact support on $\mathbb{R}^d_+$. Then for all $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$,*

$$\lim_{T\to\infty} \frac{1}{T^{d-s-2}} \int_{X_g(\mathbb{R})} J_{f,g}(M_0^g(v), \|v\|/T)\, dm_g(v) = C_1 C(g) \int_{G_g/\Gamma_g} F_{f,g}\, d\mu_g,$$

where C_1 is defined by (5-1) and $C(g)$ is defined in Lemma 5.6.

Proof. Let v_i be the components of v when written in the basis $b_1, \dots, b_d$ from Lemma 5.1. Using the change of variables $(v_1, \dots, v_d) \to (z_1, \dots, z_s, r, v_{s+2}, \dots, a)$ where $Q_0^g(v_1, \dots, v_d) = a$, we see that

$$\int_{\mathbb{R}^d} f(v)\, dv = \int_{-\infty}^{\infty} \int_0^{\infty} \int_{\mathbb{R}^s} J_{f,g}(z, r) r^{d-s-2}\, dz\, \frac{dr}{2r}\, da.$$

Hence, it follows from how m_g is defined (i.e., (2-3)) that

$$\int_{X_g(\mathbb{R})} f(v)\, dm_g(v) = \int_0^{\infty} \int_{\mathbb{R}^s} J_{f,g}(z, r) r^{d-s-2}\, dz\, \frac{dr}{2r}. \tag{5-29}$$

Lemma 5.4 and (5-29) imply that

$$\lim_{T\to\infty} \frac{1}{T^{d-s-2}} \int_{X_g(\mathbb{R})} J_{f,g}(M_0^g(v), \|v\|/T)\, dm_g(v)$$
$$= C_1 \int_{K_g} \left(\int_{X_g(\mathbb{R})} f(v)\, dm_g \right) d\nu_g(k).$$

Now the conclusion follows from Lemma 5.6. □

The purpose of Lemma 5.7 is to relate the integral over G_g/Γ_g to an integral over $X_g(\mathbb{R})$ in order that the integral over $X_g(\mathbb{R})$ can be approximated by an integral over K_g via Theorem 2.5. Then the integral over K_g can be approximated by the appropriate counting function via Corollary 5.3. We now proceed to put this into action in the proof of our main theorem, which is just a modification of the proof in [Eskin et al. 1998].

Proof of Theorem 2.1. By Lemma 5.4, the functional Ψ on $C_c(\mathbb{R}^s \times \mathbb{R}^d \setminus \{0\})$ given by

$$\Psi(h) = \lim_{T\to\infty} \frac{1}{T^{d-s-2}} \Theta(h, T)$$

is continuous. For all connected regions $R \subset \mathbb{R}^s$ with smooth boundary, if $\mathbb{1}$ denotes the characteristic function of $R \times A(1/2, 1)$, then for every $\epsilon > 0$ there exist continuous functions h_+ and h_- on $\mathbb{R}^s \times \mathbb{R}^d \setminus \{0\}$ such that, for all $(r, v) \in \mathbb{R}^s \times \mathbb{R}^d \setminus \{0\}$,

$$h_-(r, v) \le \mathbb{1}(r, v) \le h_+(r, v) \tag{5-30}$$

and

$$|\Psi(h_+) - \Psi(h_-)| < \epsilon. \tag{5-31}$$

Let $\mathcal{J}$ denote the space of linear combinations of functions on $\mathbb{R}^s \times \mathbb{R}^d$ of the form $J_{f,g}(r, \|v\|)$, where f is a continuous function of compact support on $\mathbb{R}^d_+$. Let $\mathcal{H}$ denote the collection of functions in $C_c(\mathbb{R}^s \times \mathbb{R}^d \setminus \{0\})$ such that if $h \in \mathcal{H}$ then h takes an argument of the form $(r, \|v\|)$. By Lemma 5.2, $\mathcal{J}$ is dense in $\mathcal{H}$, and since h_+ and h_- belong to $\mathcal{H}$, we may suppose that h_+ and h_- may be written as a finite linear combination of functions from $\mathcal{J}$. The function $F_{f,g}$ defined by (2-1) obeys the bound (2-4) with $\delta = 1$ by (2-2). Moreover, Lemma 3.10 of [Eskin et al. 1998] implies that $F_{f,g} \in L_1(G_g/\Gamma_g)$. Therefore, if $h' \in \{h_+, h_-\}$, then for all $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$, we can apply Theorem 2.5 with the function $F_{f,g}$ followed by Corollary 5.3 and Lemma 5.7 to get that there exists $t_0 > 0$ so that, for all $\epsilon > 0$ and $t > t_0$,

$$\left| \frac{C(g)}{e^{(d-s-2)t}} \sum_{v\in X_g(\mathbb{Z})} h'(M_0^g(v), ve^{-t}) - \Psi(h') \right| < \epsilon. \tag{5-32}$$

From the definition of $\Psi(h)$, we see that for all $h \in C_c(\mathbb{R}^s \times \mathbb{R}^d \setminus \{0\})$ and $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$ there exists $t_0 > 0$ so that, for all $\epsilon > 0$ and $t > t_0$,

$$\left| \frac{1}{e^{(d-s-2)t}} \int_{X_g(\mathbb{R})} h(M_0^g(v), ve^{-t})\, dm_g(v) - \Psi(h) \right| < \epsilon. \tag{5-33}$$

Clearly (5-30) implies

$$\begin{aligned}
&\frac{C(g)}{e^{(d-s-2)t}} \sum_{v\in X_g(\mathbb{Z})} h_-(M_0^g(v), ve^{-t}) - \Psi(h_+) \\
&\qquad \le \frac{C(g)}{e^{(d-s-2)t}} \sum_{v\in X_g(\mathbb{Z})} \mathbb{1}(M_0^g(v), ve^{-t}) - \Psi(h_+) \\
&\qquad \le \frac{C(g)}{e^{(d-s-2)t}} \sum_{v\in X_g(\mathbb{Z})} h_+(M_0^g(v), ve^{-t}) - \Psi(h_+).
\end{aligned} \tag{5-34}$$

Apply (5-31) to the left-hand side of (5-34), and then apply (5-32) with suitable choices of ϵ's to get that for all $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$ there exists $t_0 > 0$ so that, for all $\theta > 0$ and $t > t_0$,

$$\left| \frac{C(g)}{e^{(d-s-2)t}} \sum_{v \in X_g(\mathbb{Z})} \mathbb{1}(M_0^g(v), ve^{-t}) - \Psi(h_+) \right| \leq \frac{\theta}{2}. \tag{5-35}$$

Similarly using (5-30), (5-31) and (5-33), we see that for all $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$ there exists $t_0 > 0$ so that, for all $\theta > 0$ and $t > t_0$,

$$\left| \frac{1}{e^{(d-s-2)t}} \int_{X_g(\mathbb{R})} \mathbb{1}(M_0^g(v), ve^{-t})\, dm_g(v) - \Psi(h_+) \right| \leq \frac{\theta}{2}. \tag{5-36}$$

Hence, using (5-35) and (5-36), we see that for all $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$ there exists $t_0 > 0$ so that, for all $\theta > 0$ and $t > t_0$,

$$\left| C(g) \sum_{v \in X_g(\mathbb{Z})} \mathbb{1}(M_0^g(v), ve^{-t}) - \int_{X_g} \mathbb{1}(M_0^g(v), ve^{-t})\, dm_g(v) \right| \leq \theta. \tag{5-37}$$

This means that for all $g \in \mathscr{C}_{\mathrm{SL}}(r_1, r_2)$ there exists $t_0 > 0$ so that, for all $\theta > 0$ and $t > t_0$,

$$\begin{aligned} (1-\theta) \int_{X_g(\mathbb{R})} \mathbb{1}(M_0^g(v), ve^{-t})\, dm_g(v) &\leq C(g) \sum_{v \in X_g(\mathbb{Z})} \mathbb{1}(M_0^g(v), ve^{-t}) \\ &\leq (1+\theta) \int_{X_g(\mathbb{R})} \mathbb{1}(M_0^g(v), ve^{-t})\, dm_g(v). \end{aligned} \tag{5-38}$$

Hence, for all $(Q, M) \in \mathscr{C}_{\mathrm{Pairs}}(r_1, r_2)$, there exists $t_0 > 0$ so that, for all $\theta > 0$ and $t > t_0$,

$$\begin{aligned} (1-\theta)\, \mathrm{Vol}_{X_Q}(V_M(R) \cap A(T/2, T)) &\leq C(g) |X_Q(\mathbb{Z}) \cap V_M(R) \cap A(T/2, T)| \\ &\leq (1+\theta)\, \mathrm{Vol}_{X_Q}(V_M(R) \cap A(T/2, T)). \end{aligned}$$

The conclusion of the theorem follows by applying Corollary 5.5 and summing a geometric series. □

6. Counterexamples

In small dimensions, there are slightly more integer points than expected on the quadratic surfaces defined by forms with signature $(1, 2)$ and $(2, 2)$. This fact was exploited in [Eskin et al. 1998] to show that the expected asymptotic formula for the situation they consider is not valid for these special cases. In a similar manner, it is possible to construct examples that show that Theorem 1.1 is not valid in the cases that the signature of H_g is $(1, 2)$ or $(2, 2)$. In this section, for the sake of brevity, we restrict our attention to the case when $s = 1$, but we note that similar arguments would hold in the case when $s > 1$. To start with, make the following definitions:

$$\begin{aligned} Q_1(x) &= -x_1x_2 + x_3^2 + x_4^2, \\ Q_2(x) &= x_1x_2 + x_3^2 - x_4^2, \\ Q_3(x) &= -x_1x_2 + x_3^2 + x_4^2 - \alpha x_5^2, \\ L_\alpha(x) &= x_1 - \alpha x_2. \end{aligned}$$

We can now prove:

Lemma 6.1. *Let $\epsilon > 0$; suppose $[a, b] = [1/2 - \epsilon, 1]$ or $[-1, -1/2 + \epsilon]$. Let $a > 0$; then for every $T_0 > 0$, the set of $\beta \in \mathbb{R}$ for which there exists a $T > T_0$ such that*

$$\left|X^a_{Q_1}(\mathbb{Z}) \cap V_{L_\beta}([a, b]) \cap A(0, T)\right| > T(\log T)^{1-\epsilon}$$
$$\text{or} \quad \left|X^a_{Q_2}(\mathbb{Z}) \cap V_{L_\beta}([a, b]) \cap A(0, T)\right| > T(\log T)^{1-\epsilon}$$

is dense. Similarly if $a = 0$, then for every $T_0 > 0$, the set of $\beta \in \mathbb{R}$ for which there exists a $T > T_0$ such that

$$\left|X^a_{Q_3}(\mathbb{Z}) \cap V_{L_\beta}([a, b]) \cap A(0, T)\right| > T^2(\log T)^{1-\epsilon}$$

is dense.

Proof. Let $S_i(\alpha, T, a) = \{x \in \mathbb{Z}^{d_i} : L_\alpha(x) = 0,\ Q_i(x) = a,\ \|x\| \le T\}$, where $d_i = 4$ if $i = 1$ or 2 and $d_i = 5$ if $i = 3$. Lemma 3.14 of [Eskin et al. 1998] implies that

$$|S_i(\alpha, T, a)| \sim c_{i,\alpha} T \log T \qquad \text{for } i = 1, 2 \text{ and } \sqrt{\alpha} \in \mathbb{Q} \text{ and } a > 0, \tag{6-1}$$
$$|S_3(\alpha, T, 0)| \sim c_{3,\alpha} T^2 \log T \qquad \text{for } \sqrt{\alpha} \in \mathbb{Q}, \tag{6-2}$$

where $c_{i,\alpha}$ are constants that depend on α. Note that if $i = 1, 2$ and $x \in S_i(\alpha, T, a) \setminus S_i(\alpha, T/2, a)$, then

$$\frac{T^2}{4} - (\alpha^2 + 1)x_2^2 \le x_3^2 + x_4^2 \le T^2 - (\alpha^2 + 1)x_2^2 \tag{6-3}$$

and

$$x_3^2 + x_4^2 = \alpha x_2^2 + a. \tag{6-4}$$

Similarly if $x \in S_3(\alpha, T, 0) \setminus S_3(\alpha, T/2, 0)$,

$$\frac{T^2}{4} - (\alpha^2 + 1)x_2^2 \le x_3^2 + x_4^2 + x_5^2 \le T^2 - (\alpha^2 + 1)x_2^2 \tag{6-5}$$

and

$$x_3^2 + x_4^2 = \alpha(x_2^2 + x_5^2). \tag{6-6}$$

Combining (6-3) and (6-4) gives

$$\frac{T^2 - 4a}{4(\alpha^2 + \alpha + 1)} \le x_2^2 \le \frac{T^2 - a}{\alpha^2 + \alpha + 1}. \tag{6-7}$$

Respectively, combining (6-5) and (6-6) gives

$$\frac{T^2-(\alpha+1)x_5^2}{4(\alpha^2+\alpha+1)} \le x_2^2 \le \frac{T^2-(\alpha+1)x_5^2}{\alpha^2+\alpha+1}, \tag{6-8}$$

which upon noting that $-T \le x_5 \le T$ offers

$$\frac{T^2-(\alpha+1)T}{4(\alpha^2+\alpha+1)} \le x_2^2 \le \frac{T^2+(\alpha+1)T}{\alpha^2+\alpha+1}. \tag{6-9}$$

Take

$$\beta_\pm = \alpha \pm \sqrt{\frac{\alpha^2+\alpha+1}{T^2}}. \tag{6-10}$$

It is clear that $L_{\beta_\pm}(x) = L_\alpha(x) \pm \sqrt{(\alpha^2+\alpha+1)/T^2}\,x_2$, and hence, if $i=1,2$ and $x \in S_i(\alpha,T,a) \setminus S_i(\alpha,T/2,a)$, then (6-7) implies

$$\begin{aligned} \sqrt{\frac{1}{4}-\frac{a}{T^2}} \le L_{\beta_+}(x) \le \sqrt{1-\frac{a}{T^2}}, \\ -\sqrt{1-\frac{a}{T^2}} \le L_{\beta_-}(x) \le -\sqrt{\frac{1}{4}-\frac{a}{T^2}}. \end{aligned} \tag{6-11}$$

Similarly if $x \in S_3(\alpha,T,0) \setminus S_3(\alpha,T/2,0)$, then (6-9) implies

$$\begin{aligned} \sqrt{\frac{1}{4}-\frac{(\alpha+1)}{T}} \le L_{\beta_+}(x) \le \sqrt{1-\frac{(\alpha+1)}{T}}, \\ -\sqrt{1-\frac{(\alpha+1)}{T}} \le L_{\beta_-}(x) \le -\sqrt{\frac{1}{4}-\frac{(\alpha+1)}{T}}. \end{aligned} \tag{6-12}$$

This means for all $\epsilon > 0$ there exists $T_+ > 0$ such that if $T > T_+$ then $S_i(\alpha,T,a) \subset X^a_{Q_i}(\mathbb{Z}) \cap V_{L_{\beta_+}}([1/2-\epsilon,1]) \cap A(0,T)$; respectively, there also exists $T_- > 0$ such that if $T > T_-$ then $S_i(\alpha,T,a) \subset X^a_{Q_i}(\mathbb{Z}) \cap V_{L_{\beta_-}}([-1,-1/2+\epsilon]) \cap A(0,T)$. By (6-1) and (6-2), for $i=1,2$ and large enough T (depending on α), $|S_i(\alpha,T,a)| > T(\log T)^{1-\epsilon}$ and $|S_i(\alpha,T,a)| > CT^2(\log T)^{1-\epsilon}$. The set of β satisfying (6-10) for rational α and large T is clearly dense, and this proves the lemma. $\square$

Theorem 6.2. *Let $j=1,2$. For every $\epsilon > 0$ and every interval $[a,b]$, there exists a rational quadratic form Q and an irrational linear form L such that* $\mathrm{Stab}_{\mathrm{SO}(Q)}(L) \cong \mathrm{SO}(j,2)$ *such that, for an infinite sequence $T_k \to \infty$,*

$$\left|X_Q^{a_j}(\mathbb{Z}) \cap V_L([a,b]) \cap A(0,T_k)\right| > T_k^j(\log T_k)^{1-\epsilon},$$

where $a_1 > 0$ and $a_2 = 0$.

Proof. Since the interval $[a,b]$ must intersect either the positive or negative reals, there is no loss of generality in assuming, after passing to a subset and rescaling, that $[a, b] = [1/4, 5/4]$ or $[-5/4, -1/4]$. For a given $S > 0$ and $i = 1, 2$, let $\mathcal{U}_S$ be the set of $\gamma \in \mathbb{R}$ for which there exist $\beta \in \mathbb{R}$ and $T > S$ with

$$\left|X^{a_1}_{Q_i}(\mathbb{Z}) \cap V_{L_\beta}([1/2, 1]) \cap A(0, T)\right| > CT \log T \tag{6-13}$$

and

$$|\beta - \gamma| < T^{-2}. \tag{6-14}$$

Then $\mathcal{U}_S$ is open and dense by Lemma 6.1. By the Baire category theorem [Rudin 1987, Theorem 5.6], $\bigcap_{k=1}^{\infty} \mathcal{U}_{2^{k+1}}$ is dense in $\mathbb{R}$ and is in fact of second category and hence uncountable. Let $\gamma \in \bigcap_{k=1}^{\infty} \mathcal{U}_{2^{k+1}} \setminus \mathbb{Q}$; then there exist infinite sequences β_k and T_k such that (6-13) and (6-14) hold with β replaced by β_k and T by T_k. Note that (6-14) implies that, for $\|x\| < T_k$,

$$|L_{\beta_k}(x) - L_\gamma(x)| < \frac{1}{T_k} < \frac{1}{4}$$

so that

$$X^{a_1}_{Q_i}(\mathbb{Z}) \cap V_{L_{\beta_k}}([1/2, 1]) \cap A(0, T_k) \subseteq X^{a_1}_{Q_i}(\mathbb{Z}) \cap V_{L_\gamma}([1/4, 5/4]) \cap A(0, T_k)$$

and hence $|X^{a_1}_{Q_i}(\mathbb{Z}) \cap V_{L_\gamma}([1/4, 5/4]) \cap A(0, T_k)| > CT_k \log T_k$ by (6-13). If $i = 3$, then we can carry out the same process, but we replace $\mathcal{U}_S$ by the set $\mathcal{W}_S$ of $\gamma \in \mathbb{R}$ for which there exist $\beta \in \mathbb{R}$ and $T > S$ with

$$\left|X^{0}_{Q_3}(\mathbb{Z}) \cap V_{L_\beta}([1/2, 1]) \cap A(0, T)\right| > CT^2 \log T$$

and

$$|\beta - \gamma| < T^{-2}. \qquad \square$$

Acknowledgment

The author would like to thank Alex Gorodnik for many helpful discussions and remarks about earlier versions of this paper.

References

[Benoist and Quint 2012] Y. Benoist and J.-F. Quint, "Random walks on finite volume homogeneous spaces", *Invent. Math.* **187**:1 (2012), 37–59. MR 2874934 Zbl 1244.60009

[Cassels 1972] J. W. S. Cassels, *An introduction to Diophantine approximation*, Cambridge Tracts in Mathematics and Mathematical Physics **45**, Hafner, New York, 1972. MR 50 #2084 Zbl 0077.04801

[Dani 1981] S. G. Dani, "Invariant measures and minimal sets of horospherical flows", *Invent. Math.* **64**:2 (1981), 357–385. MR 83c:22009 Zbl 0498.58013

[Dani and Margulis 1990] S. G. Dani and G. A. Margulis, "Orbit closures of generic unipotent flows on homogeneous spaces of SL(3, $\mathbb{R}$)", *Math. Ann.* **286**:1-3 (1990), 101–128. MR 91k:22026 Zbl 0679.22007

[Dani and Margulis 1993] S. G. Dani and G. A. Margulis, "Limit distributions of orbits of unipotent flows and values of quadratic forms", pp. 91–137 in *I. M. Gelfand Seminar* (Moscow, 1993), vol. 1, edited by S. Gelfand and S. Gindikin, Adv. Soviet Math. **16**, American Mathematical Society, Providence, RI, 1993. MR 95b:22024 Zbl 0814.22003

[Eskin et al. 1998] A. Eskin, G. A. Margulis, and S. Mozes, "Upper bounds and asymptotics in a quantitative version of the Oppenheim conjecture", *Ann. of Math.* (2) **147**:1 (1998), 93–141. MR 99a:11043 Zbl 0906.11035

[Gorodnik 2004] A. Gorodnik, "Oppenheim conjecture for pairs consisting of a linear form and a quadratic form", *Trans. Amer. Math. Soc.* **356**:11 (2004), 4447–4463. MR 2005h:11146 Zbl 1051.11034

[Helgason 2000] S. Helgason, *Groups and geometric analysis: integral geometry, invariant differential operators, and spherical functions*, Mathematical Surveys and Monographs **83**, American Mathematical Society, Providence, RI, 2000. MR 2001h:22001 Zbl 0965.43007

[Helgason 2001] S. Helgason, *Differential geometry, Lie groups, and symmetric spaces*, Graduate Studies in Mathematics **34**, American Mathematical Society, Providence, RI, 2001. MR 2002b:53081 Zbl 0993.53002

[Henk and Wills 2008] M. Henk and J. M. Wills, "Minkowski's successive minima", pp. 129–142 in *Number theory and discrete geometry* (Chandigarh, 2005), edited by R. Balasubramanian et al., Ramanujan Math. Soc. Lect. Notes Ser. **6**, Ramanujan Math. Soc., Mysore, 2008. MR 2010f:11114 Zbl 1234.11085

[Kleinbock et al. 2002] D. Kleinbock, N. Shah, and A. Starkov, "Dynamics of subgroup actions on homogeneous spaces of Lie groups and applications to number theory", pp. 813–930 in *Handbook of dynamical systems*, vol. 1A, edited by B. Hasselblatt and A. Katok, North-Holland, Amsterdam, 2002. MR 2004b:22021 Zbl 1050.22026

[Margulis 1989] G. A. Margulis, "Discrete subgroups and ergodic theory", pp. 377–398 in *Number theory, trace formulas and discrete groups* (Oslo, 1987), edited by K. E. Aubert et al., Academic Press, Boston, 1989. MR 90k:22013a Zbl 0675.10010

[Platonov and Rapinchuk 1991] V. P. Platonov and A. S. Rapinchuk, *Алгебраические группы и теория чисел*, Nauka, Moscow, 1991. Translated as *Algebraic groups and number theory*, Pure and Applied Mathematics **139**, Academic Press, Boston, 1994. MR 93j:11023 Zbl 0732.20027

[Ratner 1994] M. Ratner, "Invariant measures and orbit closures for unipotent actions on homogeneous spaces", *Geom. Funct. Anal.* **4**:2 (1994), 236–257. MR 95c:22018 Zbl 0801.22008

[Rudin 1976] W. Rudin, *Principles of mathematical analysis*, 3rd ed., McGraw-Hill, New York, 1976. MR 52 #5893 Zbl 0346.26002

[Rudin 1987] W. Rudin, *Real and complex analysis*, 3rd ed., McGraw-Hill, New York, 1987. MR 88k:00002 Zbl 0925.00005

[Sargent 2013] O. Sargent, "Density of values of linear maps on quadratic surfaces", preprint, 2013. To appear in *J. Number Theor.* arXiv 1111.4428v3

[Schmidt 1968] W. M. Schmidt, "Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height", *Duke Math. J.* **35** (1968), 327–339. MR 37 #161 Zbl 0172.06304

[Schnell 1995] U. Schnell, "Successive minima, intrinsic volumes, and lattice determinants", *Discrete Comput. Geom.* **13**:2 (1995), 233–239. MR 95k:52029 Zbl 0818.52003

Communicated by Peter Sarnak
Received 2013-03-05 Revised 2013-12-10 Accepted 2014-01-22

oliver.sargent@bris.ac.uk Department of Mathematics, University of Bristol, University Walk, Bristol, BS8 1TW, United Kingdom

ALGEBRA AND NUMBER THEORY 8:4 (2014)
dx.doi.org/10.2140/ant.2014.8.933

Posets, tensor products and Schur positivity

Vyjayanthi Chari, Ghislain Fourier and Daisuke Sagaki

Let $\mathfrak{g}$ be a complex finite-dimensional simple Lie algebra. Given a positive integer k and a dominant weight λ, we define a preorder $\preceq$ on the set $P^+(\lambda, k)$ of k-tuples of dominant weights which add up to λ. Let $\sim$ be the equivalence relation defined by the preorder and $P^+(\lambda, k)/\sim$ be the corresponding poset of equivalence classes. We show that if λ is a multiple of a fundamental weight (and k is general) or if $k = 2$ (and λ is general), then $P^+(\lambda, k)/\sim$ coincides with the set of S_k-orbits in $P^+(\lambda, k)$, where S_k acts on $P^+(\lambda, k)$ as the permutations of components. If $\mathfrak{g}$ is of type A_n and $k = 2$, we show that the S_2-orbit of the row shuffle defined by Fomin et al. (2005) is the unique maximal element in the poset.

Given an element of $P^+(\lambda, k)$, consider the tensor product of the corresponding simple finite-dimensional $\mathfrak{g}$-modules. We show that (for general $\mathfrak{g}$, λ, and k) the dimension of this tensor product increases along $\preceq$. We also show that in the case when λ is a multiple of a fundamental minuscule weight ($\mathfrak{g}$ and k are general) or if $\mathfrak{g}$ is of type A_2 and $k = 2$ (λ is general), there exists an inclusion of tensor products along with the partial order $\preceq$ on $P^+(\lambda, k)/\sim$. In particular, if $\mathfrak{g}$ is of type A_n, this means that the difference of the characters is Schur positive.

Introduction

This paper is partially motivated by the following simple observation. The isomorphism classes of simple finite-dimensional representations of the complex simple Lie algebra $\mathfrak{sl}_2$ are indexed by $\mathbb{Z}_+$, the set of nonnegative integers. Given $r \in \mathbb{Z}_+$, let $V(r)$ be a representative of the corresponding isomorphism class. The well-known Clebsch–Gordan formula gives us the following decomposition: for $r, s \in \mathbb{Z}_+$,

$$V(r) \otimes V(s) \cong V(r+s) \oplus V(r+s-2) \oplus \cdots \oplus V(|r-s|).$$

Chari was partially supported by DMS-0901253. Fourier was partially supported by the DFG priority program 1388 “Representation Theory”. Sagaki was partially supported by the Grant-in-Aid for Young Scientists (B) No. 23740003.
MSC2010: 17B67.
Keywords: Schur positivity, tensor products, posets, Lie algebras.

If $r_1, s_1 \in \mathbb{Z}_+$ are such that $r_1 + s_1 = r + s$, it is then immediate that one has an injection of $\mathfrak{sl}_2$-modules

$$V(r) \otimes V(s) \hookrightarrow V(r_1) \otimes V(s_1) \iff |r - s| \geq |r_1 - s_1|. \tag{0-1}$$

In particular, the dimension increases if $\min\{r, s\} \leq \min\{r_1, s_1\}$. Moreover, the pairs (r, r) and $(r, r+1)$ are maximal in the sense that: the corresponding tensor product maps onto to any tensor product corresponding to (r_1, s_1) if $r_1 + s_1 = 2r$ (resp. $r_1 + s_1 = 2r + 1$). Notice that these maximal pairs are actually the simplest examples of the row shuffle of partitions given in [Fomin et al. 2005]. Part of our interest in this problem comes from the fact that the tensor product $V(r) \otimes V(s)$ admits the structure of an indecomposable module for the infinite-dimensional Lie algebra $\mathfrak{sl}_2 \otimes \mathbb{C}[t]$, where $\mathbb{C}[t]$ is the polynomial ring in the indeterminate t. In this case, the map in (0-1) is actually a map of $\mathfrak{sl}_2 \otimes \mathbb{C}[t]$-modules and the module corresponding to the maximal pair is a truncation of a local Weyl module. We shall return to these ideas elsewhere. We mention this only to indicate our original motivation; the results of the current paper are entirely about simple Lie algebras.

Suppose now that $\mathfrak{g}$ is a finite-dimensional simple Lie algebra and P^+ the set of dominant integral weights. We let $P^+(\lambda, 2)$ be the set of "compositions" of λ with at most two parts, that is, pairs of dominant integral weights which add up to λ. If (λ_1, λ_2) and (μ_1, μ_2) are two such compositions, we define a partial order $\preceq$ by requiring that $\min\{\lambda_1(h_\alpha), \lambda_2(h_\alpha)\} \leq \min\{\mu_1(h_\alpha), \mu_2(h_\alpha)\}$ hold for all positive roots α. This order extends in a natural way to $P^+(\lambda, k)$, the set of compositions of λ with k parts for all $k \geq 1$; one just requires the inequality to hold for all partial sums.

For $\mu \in P^+$, let $V(\mu)$ be the corresponding finite-dimensional $\mathfrak{g}$-module. If $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$ are two compositions of λ with k parts and $V(\boldsymbol{\lambda})$, $V(\boldsymbol{\mu})$ are the corresponding tensor products of $\mathfrak{g}$-modules, we prove that

$$\boldsymbol{\lambda} \preceq \boldsymbol{\mu} \implies \dim V(\boldsymbol{\lambda}) \leq \dim V(\boldsymbol{\mu}).$$

If λ is a multiple of a minuscule weight, then we prove that there exists a (noncanonical) inclusion $V(\boldsymbol{\lambda}) \hookrightarrow V(\boldsymbol{\mu})$. In the case when $\mathfrak{g}$ is of type $\mathfrak{sl}_3$ and $k = 2$, we prove that the inclusion holds for all $\lambda \in P^+$. We conjecture that this latter result holds for all simple Lie algebras. Our conjecture may be viewed as a generalization of the row-shuffle conjecture which was made in [Fomin et al. 2005] for representations of $\mathfrak{sl}_{n+1}$. The row-shuffle conjecture was proved in [Lam et al. 2007], showing that our conjecture is true in the case of $\mathfrak{sl}_{n+1}$ for the pair $\boldsymbol{\lambda}$, $\boldsymbol{\mu}$ where $\boldsymbol{\mu}$ is the maximal element in the poset. A completely different approach taken in [Dobrovolska and Pylyavskyy 2007] also gives some evidence for our conjecture in the case of $\mathfrak{sl}_{n+1}$.

The following is an immediate combinatorial consequence of Theorem 1(i) and is perhaps of independent interest. Given two partitions $(0 \leq a_1 \leq a_2 \leq \cdots \leq a_k)$

and $(0 \le b_1 \le b_2 \le \cdots \le b_k)$ of an integer n satisfying

$$\sum_{j=1}^{i} a_j \le \sum_{j=1}^{i} b_j \text{ for all } 1 \le i \le k,$$

we have

$$a_1 \ldots a_k \le b_1 \ldots b_k,$$

with equality if and only if $a_j = b_j$ for all $1 \le j \le k$.

The article is organized as follows. Section 1 has the basic definitions and notation. In Section 2 we introduce the partial order and state the main theorem. In Section 3 we prove that the dimension of the tensor product increases along the partial order. The critical idea in this proof is to show that in the case of $\mathfrak{sl}_2$, the partial order for $k > 2$ is determined by the order at $k = 2$. Once this is done, the proof is a simple application of the Weyl dimension formula. In Section 4 we use the results of Section 2 and the Littelmann path model to prove that for general k and λ a multiple of a minuscule weight, we have an inclusion of tensor products along the partial order. In Section 5 we study the partial order $P^+(\lambda, 2)$ in detail. We identify maximal elements of the poset and prove that the row shuffle is the unique maximal element when $\mathfrak{g}$ is of type $\mathfrak{sl}_{n+1}$. Finally, in Section 6, we use results of Kashiwara and Nakashima on semistandard Young tableaux and crystal bases to prove that in the case that $\mathfrak{g} = \mathfrak{sl}_3$ and $k = 2$, the Schur positivity holds along our order for all $\lambda \in P^+$.

1. Preliminaries

Throughout this paper we denote by $\mathbb{C}$ the field of complex numbers and by $\mathbb{Z}$ (resp. $\mathbb{Z}_+$) the set of integers (resp. nonnegative integers).

1.1. Let $\mathfrak{g}$ denote a finite-dimensional complex simple Lie algebra of rank n and $\mathfrak{h}$ a fixed Cartan subalgebra of $\mathfrak{g}$. Let $I = \{1, \ldots, n\}$ and fix a set $\{\alpha_i : i \in I\}$ of simple roots of $\mathfrak{g}$ with respect to $\mathfrak{h}$ and a set $\{\omega_i : i \in I\}$ of fundamental weights. Let P (resp. P^+) be the $\mathbb{Z}$ (resp. $\mathbb{Z}_+$) span of $\{\omega_i : i \in I\}$. Let R and R^+ be the set of roots and positive roots respectively. For $\alpha \in R^+$, let $\mathfrak{sl}_2(\alpha) = \langle x_\alpha^\pm, h_\alpha \rangle$ be the corresponding subalgebra of $\mathfrak{g}$ isomorphic to $\mathfrak{sl}_2$ and set $h_{-\alpha} = -h_\alpha$ for $\alpha \in R^+$, $h_i = h_{\alpha_i}$. Let W be the Weyl group of $\mathfrak{g}$ and recall that W acts on $\mathfrak{h}$ and $\mathfrak{h}^*$ and that for all $\boldsymbol{w} \in W$, $\lambda \in \mathfrak{h}^*$ and $\alpha \in R^+$, we have

$$(\boldsymbol{w}\lambda)(\boldsymbol{w}h_\alpha) = \lambda(h_\alpha).$$

For $\alpha \in R^+$, let $\boldsymbol{s}_\alpha \in W$ be the corresponding reflection and we set $\boldsymbol{s}_i = \boldsymbol{s}_{\alpha_i}$. Let $\boldsymbol{w}_0 \in W$ be the longest element.

We say that $\lambda \in P^+$ is minuscule if $\lambda(h_\alpha) \in \{0, 1\}$ for all $\alpha \in R^+$. It can be easily seen that if $\lambda \in P^+$ is minuscule, then λ is a fundamental weight. The following is the list of minuscule weights; here we follow the numbering of vertices of the Dynkin diagram for $\mathfrak{g}$ in [Bourbaki 2002].

A_n	$\omega_i,\ 1 \le i \le n$
B_n	ω_n
C_n	ω_1
D_n	$\omega_1, \omega_{n-1}, \omega_n$
E_6	ω_1, ω_6
E_7	ω_7

1.2. For any $\mathfrak{g}$-module M and $\mu \in \mathfrak{h}^*$, set

$$M_\mu = \{m \in M : hm = \mu(h)m,\ h \in \mathfrak{h}\}, \qquad \mathrm{wt}(M) = \{\mu \in \mathfrak{h}^* : M_\mu \neq 0\}.$$

We say M is a *weight module* for $\mathfrak{g}$ if

$$M = \bigoplus_{\mu \in \mathfrak{h}^*} M_\mu.$$

Any finite-dimensional $\mathfrak{g}$-module is a weight module. It is well known that the set of isomorphism classes of irreducible finite-dimensional $\mathfrak{g}$-modules is in bijective correspondence with P^+. For $\lambda \in P^+$ we denote by $V(\lambda)$ a representative of the corresponding isomorphism class.

If $V(\lambda)^*$ is the dual representation of $V(\lambda)$, then

$$V(\lambda)^* \cong V(-\boldsymbol{w}_0\lambda). \tag{1-1}$$

The dimension of $V(\lambda)$ is given by the Weyl dimension formula, namely

$$\dim V(\lambda) = \prod_{\alpha \in R^+} \frac{(\lambda + \rho)(h_\alpha)}{\rho(h_\alpha)}, \tag{1-2}$$

where $\rho = \sum_{i=1}^n \omega_i \in P^+$. Any finite-dimensional $\mathfrak{g}$-module is isomorphic to a direct sum of irreducible modules, and in particular, we have

$$V(\lambda) \otimes V(\mu) \cong \bigoplus_{\nu \in P^+} V(\nu)^{\oplus c_{\lambda,\mu}^\nu}, \qquad c_{\lambda,\mu}^\nu = \dim \mathrm{Hom}_{\mathfrak{g}}\big(V(\nu), V(\lambda) \otimes V(\mu)\big).$$

We shall freely use the fact that

$$V(\lambda) \otimes V(\mu) \cong V(\mu) \otimes V(\lambda)$$

and that

$$\dim \operatorname{Hom}_{\mathfrak{g}}\big(V(\nu), V(\lambda)\otimes V(\mu)\big) = \dim \operatorname{Hom}_{\mathfrak{g}}\big(V(\nu)^*, V(\lambda)^*\otimes V(\mu)^*\big).$$

2. The poset $P^+(\lambda, k)/\sim$ and the main result

2.1. Given an integer $k > 0$ and $\lambda \in P^+$, set

$$P^+(\lambda, k) = \big\{\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_k) \in (P^+)^{\times k} : \lambda_1 + \cdots + \lambda_k = \lambda\big\}.$$

Clearly, $P^+(\lambda, k)$ is a finite set and the symmetric group S_k acts naturally on it. The Weyl group W acts diagonally on $P^+(\lambda, k)$ as follows:

$$\boldsymbol{w}\boldsymbol{\lambda} = \boldsymbol{w}(\lambda_1, \dots, \lambda_k) = (\boldsymbol{w}\lambda_1, \dots, \boldsymbol{w}\lambda_k) \quad \text{for } \boldsymbol{w} \in W.$$

Observe that

$$\boldsymbol{\lambda} \in P^+(\lambda, k) \iff -\boldsymbol{w}_0\boldsymbol{\lambda} \in P^+(-\boldsymbol{w}_0\lambda, k). \tag{2-1}$$

For $\boldsymbol{\lambda} \in P^+(\lambda, k)$, $\alpha \in R^+$, and $1 \le \ell \le k$, set

$$r_{\alpha,\ell}(\boldsymbol{\lambda}) := \min\big\{(\lambda_{i_1} + \cdots + \lambda_{i_\ell})(h_\alpha) : 1 \le i_1 < i_2 < \cdots < i_\ell \le k\big\}.$$

Clearly, $r_{\alpha,k}(\boldsymbol{\lambda}) \ge r_{\alpha,k-1}(\boldsymbol{\lambda}, \alpha) \ge \cdots \ge r_{\alpha,1}(\boldsymbol{\lambda})$. Given $\boldsymbol{\lambda}, \boldsymbol{\mu} \in P^+(\lambda, k)$, we say that $\boldsymbol{\lambda} \preceq \boldsymbol{\mu}$ if

$$r_{\alpha,\ell}(\boldsymbol{\lambda}) \le r_{\alpha,\ell}(\boldsymbol{\mu}) \quad \text{for all } \alpha \in R^+ \text{ and } 1 \le \ell \le k.$$

This defines a preorder on the $P^+(\lambda, k)$. It induces a partial order on the set of equivalence classes with respect to the equivalence relation $\sim$ on $P^+(\lambda, k)$, given by

$$\boldsymbol{\lambda} \sim \boldsymbol{\mu} \iff r_{\alpha,\ell}(\boldsymbol{\lambda}) = r_{\alpha,\ell}(\boldsymbol{\mu}) \quad \text{for all } \alpha \in R^+ \text{ and } 1 \le \ell \le k.$$

The poset has a unique minimal element, which is just the k-tuple $(\lambda, 0, \dots, 0)$.

For ease of notation, we shall not always distinguish between elements of $P^+(\lambda, k)/\sim$ and their representatives in $P^+(\lambda, k)$.

Note that if $\boldsymbol{\lambda}, \boldsymbol{\mu} \in P^+(\lambda, k)$, then

$$\boldsymbol{\lambda} \preceq \boldsymbol{\mu} \iff -\boldsymbol{w}_0\boldsymbol{\lambda} \preceq -\boldsymbol{w}_0\boldsymbol{\mu}. \tag{2-2}$$

We now state the main result of this paper.

Theorem 1. *Let $\mathfrak{g}$ be a finite-dimensional simple Lie algebra and let $k \in \mathbb{Z}_+$ and $\lambda \in P^+$. Assume that $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_k)$ and $\boldsymbol{\mu} = (\mu_1, \dots, \mu_k)$ are elements of $P^+(\lambda, k)$ such that $\boldsymbol{\lambda} \preceq \boldsymbol{\mu}$ in $P^+(\lambda, k)/\sim$.*

(i) *We have*

$$\dim \bigotimes_{s=1}^{k} V(\lambda_s) \le \dim \bigotimes_{s=1}^{k} V(\mu_s),$$

with equality if and only if $\boldsymbol{\lambda} = \boldsymbol{\mu}$ in $P^+(\lambda, k)/\sim$.

(ii) *Let $i \in I$ be such that ω_i is minuscule and let $\lambda = N\omega_i$ for some $N \in \mathbb{Z}_+$. Then*

$$\dim \operatorname{Hom}_{\mathfrak{g}}\left(V(\nu), \bigotimes_{s=1}^{k} V(\lambda_s) \right) \le \dim \operatorname{Hom}_{\mathfrak{g}}\left(V(\nu), \bigotimes_{s=1}^{k} V(\mu_s) \right), \quad \nu \in P^+.$$

(iii) *If $\mathfrak{g}$ is of type A_2, and $k = 2$, then*

$$\boldsymbol{\lambda} \preceq \boldsymbol{\mu} \implies \dim \operatorname{Hom}_{\mathfrak{g}}\big(V(\nu), V(\lambda_1) \otimes V(\lambda_2)\big) \le \dim \operatorname{Hom}_{\mathfrak{g}}\big(V(\nu), V(\mu_1) \otimes V(\mu_2)\big),$$

for all $\nu \in P^+$.

The theorem is proved in the rest of this paper. We conclude this section with some comments on the methods of the proof and give some explanations for the restrictions in the theorem. We also give some context to our result by relating it to others in the literature.

2.2. To prove part (i) of the theorem, we use the Weyl dimension formula to reduce the proof to the case of $\mathfrak{sl}_2$. Recall that the cover relation of $\preceq$ on $P^+(\lambda, k)$ is the pairs $\boldsymbol{\lambda} \prec \boldsymbol{\mu}$, such that there does not exist $\boldsymbol{\nu} \in P^+(\lambda, k)$ with $\boldsymbol{\lambda} \prec \boldsymbol{\nu} \prec \boldsymbol{\mu}$. For $\mathfrak{sl}_2$ we determine this cover relation, which allows us to determine a sufficient condition for the cover relation in $P^+(\lambda, k)$ in general. Part (ii) of the theorem follows from these ideas along with the Littelmann path model. For an arbitrary simple Lie algebra, it seems quite difficult to determine the cover relations even for $k = 2$. For $\mathfrak{sl}_3$ and $k = 2$, we give a sufficient condition for one element to cover another in Section 5. It would appear from our conditions that the cover relation depends heavily on the combinatorics of the Weyl group and the root system. Part (iii) of the theorem is proved by using the information on the cover relation together with results of [Kashiwara and Nakashima 1994; Nakashima 1993] on realization of crystal bases.

2.3. A subject that has been of much interest has been the notion of Schur positivity. Let Λ be the ring of symmetric functions. It is well known [Macdonald 1995] that it has an integral basis given by the Schur functions s_χ, where χ is a partition. A symmetric function is said to be Schur positive if it can be written as a nonnegative integer linear combination of Schur functions.

Suppose now that $\mathfrak{g}$ is of type A_{r-1} and $\lambda \in P^+$, say $\lambda = \sum_{i=1}^{r-1} s_i \omega_i$. Define a partition $\chi(\lambda) = (\chi_1 \ge \cdots \ge \chi_r)$ by $\chi_j = \sum_{p=j}^{r-1} s_p$ if $1 \le j \le r-1$ and set $\chi_r = 0$. On the other hand, given a partition $\chi = \big(\chi_1 \ge \chi_2 \ge \cdots \ge \chi_{r-1} \ge 0\big)$, set $\lambda(\chi) = \sum_{i=1}^{r-1} (\chi_i - \chi_{i+1})\omega_i \in P^+$.

It is known that the character of $V(\lambda)$ is $s_{\chi(\lambda)}$. Parts (ii) and (iii) of Theorem 1 can be reformulated as: let $\boldsymbol{\lambda} = (\lambda_1, \lambda_2)$, $\boldsymbol{\mu} = (\mu_1, \mu_2) \in P^+(\lambda, 2)$; then

$$\boldsymbol{\lambda} \preceq \boldsymbol{\mu} \implies s_{\chi(\mu_1)} s_{\chi(\mu_2)} - s_{\chi(\lambda_1)} s_{\chi(\lambda_2)} = \sum_{\nu \in P^+} c_\nu s_{\chi(\nu)}, \quad c_\nu \ge 0 \text{ for all } \nu \in P^+.$$

We conjecture that this is true more generally:

Conjecture. Let $\mathfrak{g}$ be a simple Lie algebra and let $\lambda \in P^+$ and $\boldsymbol{\lambda} = (\lambda_1, \lambda_2)$, $\boldsymbol{\mu} = (\mu_1, \mu_2) \in P^+(\lambda, 2)$; then

$$\boldsymbol{\lambda} \preceq \boldsymbol{\mu} \implies \dim \operatorname{Hom}_{\mathfrak{g}}\big(V(\nu), V(\lambda_1) \otimes V(\lambda_2)\big) \leq \dim \operatorname{Hom}_{\mathfrak{g}}\big(V(\nu), V(\mu_1) \otimes V(\mu_2)\big), \tag{2-3}$$

for all $\nu \in P^+$.

Part (i) of the theorem could be viewed as giving some additional, but very limited evidence for the conjecture.

2.4. In [Fomin et al. 2005] the authors introduced the notion of a row shuffle. Thus if $\chi = (\chi_1 \geq \chi_2 \geq \cdots \geq \chi_{n-1} \geq 0)$ and $\xi = (\xi_1 \geq \xi_2 \geq \cdots \geq \xi_{n-1} \geq 0)$ are two partitions with at most $n-1$ parts, then the row shuffle is a pair of partitions $(\rho^1(\chi, \xi), \rho^2(\chi, \xi))$ defined as follows. Order the multiset $\{\chi_1, \dots, \chi_{r-1}, \xi_1, \dots, \xi_{n-1}\}$ decreasingly, say $\psi_1 \geq \psi_2 \geq \cdots \geq \psi_{2n-2}$. Set

$$\rho^1(\chi, \xi) = (\psi_1 \geq \psi_3 \geq \cdots \geq \psi_{2n-3} \geq 0),$$
$$\rho^2(\chi, \xi) = (\psi_2 \geq \psi_4 \geq \cdots \geq \psi_{2n-2} \geq 0).$$

In other words, we are shuffling the rows of the joint partition. It was conjectured in [Fomin et al. 2005] and proved in [Lam et al. 2007] that $s_{\rho^1(\chi,\xi)} s_{\rho^2(\chi,\xi)} - s_\chi s_\xi$ is Schur positive. Related conjectures can also be found in [Okounkov 1997; Lascoux et al. 1997]. Partial results on this conjecture were also obtained in [Bergeron et al. 2006; Fran and McNamara 2004; McNamara 2008; McNamara and van Willigenburg 2009; Purbhoo and van Willigenburg 2008].

2.5. The connection of the row shuffle with our partial order is made as follows. Suppose that $\mathfrak{g}$ is of type A_{n-1}, let $\nu, \mu \in P^+$, and set $\lambda = \mu + \nu$. In Section 5.3, we define an element $\boldsymbol{\lambda}_{\max} = (\lambda^1, \lambda^2) \in P^+(\lambda, 2)/\sim$ and prove that it is the unique maximal element in this set. It is a simple calculation to prove that if we take ξ and χ to be the duals of the partitions $\chi(\nu)$ and $\chi(\mu)$, then $\rho^1(\xi, \chi)$ and $\rho^2(\xi, \chi)$ are the duals of the partitions $\chi(\lambda^1)$ and $\chi(\lambda^2)$, respectively. It is well known [Macdonald 1995] that there exists an involution ω of the ring Λ which maps the Schur function associated to a partition ξ to the Schur function associated to its dual. Hence the result of [Lam et al. 2007] proves the following statement: let $\mu, \nu \in P^+$ and let $\lambda = \mu + \nu$. Then

$$\dim \operatorname{Hom}_{\mathfrak{g}}\big(V(\eta), V(\mu) \otimes V(\nu)\big) \leq \dim \operatorname{Hom}_{\mathfrak{g}}\big(V(\eta), V(\lambda^1) \otimes V(\lambda^2)\big) \text{ for all } \eta \in P^+.$$

In other words, their result proves that part (iii) of Theorem 1 is true for A_{n-1} in the case when $\boldsymbol{\mu} = \boldsymbol{\lambda}_{\max}$.
We remark that in [Lam et al. 2007] the authors proved, further, that in the case where $\mathfrak{g}$ is of type A_{n-1}, having Schur positivity for $k = 2$ (and $\boldsymbol{\mu} = \boldsymbol{\lambda}_{\max}$) implies

Schur positivity for arbitrary k; for example, they proved

$$\dim \operatorname{Hom}_{\mathfrak{g}}\big(V(\eta), V(\mu_1)\otimes\cdots\otimes V(\mu_k)\big) \le \dim \operatorname{Hom}_{\mathfrak{g}}\big(V(\eta), V(\lambda^1)\otimes\cdots\otimes V(\lambda^k)\big)$$

for all $k \ge 2$, $(\mu_1, \dots, \mu_k) \in \mathcal{P}(\lambda, k)$ and $\eta \in P^+$, where $(\lambda^1, \dots, \lambda^k)$ is the k-row shuffle of $(\mu_1, \dots, \mu_k)$. One can show (similar to the proposition in 5.3) that $(\lambda^1, \dots, \lambda^k)$ is the unique maximal element in $\mathcal{P}(\lambda, k)$.

2.6. Suppose $\mathfrak{g}$ is of type A_n; then Lam, Postnikov and Pylyavskyy stated the conjecture in 2.3 in an unpublished work (we may refer here to [Dobrovolska and Pylyavskyy 2007]). The following first step in proving this conjecture in the A_n-case has been taken in [Dobrovolska and Pylyavskyy 2007]. It is shown there that for $(\mu_1, \mu_2) \preceq (\lambda_1, \lambda_2) \in P^+(\lambda, 2)$ and $\nu \in P^+$,

$$\dim \operatorname{Hom}_{\mathfrak{g}}\big(V(\nu), V(\mu_1)\otimes V(\mu_2)\big) \neq 0 \implies \dim \operatorname{Hom}_{\mathfrak{g}}\big(V(\nu), V(\lambda_1)\otimes V(\lambda_2)\big) \neq 0.$$

Their approach is completely different from ours, as they use the Horn–Klyachko inequalities. It would be interesting to see if some of the ideas apply also when $\mathfrak{g}$ is not of type A_n.

3. Proof of Theorem 1(i)

The main idea in the proof of part (i) of the theorem is to show that when λ is a multiple of a fundamental weight, the partial order on $P^+(\lambda, k)$ is determined by the partial order on $P^+(\lambda, 2)$. We prove this in the first part of the section and then deduce Theorem 1(i).

3.1. *Assume until further notice that $\mathfrak{g}$ is an arbitrary finite-dimensional simple Lie algebra, and*

$$\lambda \in \mathbb{Z}_+\omega_i \quad \textit{for some } i \in I. \tag{3-1}$$

In particular, we can and will think of λ as a nonnegative integer. It is clear that elements of $P^+(\lambda, k)$ are just k-tuples of nonnegative integers which add up to $\lambda \in \mathbb{Z}_+$. If $\boldsymbol{\lambda} \in P^+(\lambda, k)$, we have

$$r_{\alpha,\ell}(\boldsymbol{\lambda}) = d_i r_{\alpha_i,\ell}(\boldsymbol{\lambda}), \quad h_\alpha = \sum_{i\in I} d_i h_i,$$

and it follows that if $\boldsymbol{\lambda}, \boldsymbol{\mu} \in P^+(\lambda, k)$, then

$$\boldsymbol{\lambda} \preceq \boldsymbol{\mu} \iff r_{\alpha_i,\ell}(\boldsymbol{\lambda}) \le r_{\alpha_i,\ell}(\boldsymbol{\mu}), \quad 1 \le \ell \le k.$$

In other words, the partial order is determined entirely by α_i. So we shall drop the dependence on α and write $r_\ell(\boldsymbol{\lambda})$ for $r_{\alpha_i,\ell}(\boldsymbol{\lambda})$.

3.2.

Lemma. *Let $\boldsymbol{\lambda}, \boldsymbol{\mu} \in P^+(\lambda, k)$. Then $\boldsymbol{\lambda} \sim \boldsymbol{\mu}$ if and only if $\boldsymbol{\mu} = \sigma\boldsymbol{\lambda}$ for some $\sigma \in S_k$, that is, the equivalence class of $\boldsymbol{\lambda}$ is exactly the S_k orbit of $\boldsymbol{\lambda}$.*

Proof. The fact that $\boldsymbol{\lambda} = \sigma\boldsymbol{\mu}$ implies $\boldsymbol{\lambda} \sim \boldsymbol{\mu}$ is clear from the definition of $P^+(\lambda, k)$. For the converse, choose $\sigma, \sigma' \in S_k$ so that $\sigma\boldsymbol{\lambda}$ and $\sigma'\boldsymbol{\mu}$ are partitions of λ, say

$$\sigma\boldsymbol{\lambda} = (\lambda_k \geq \cdots \geq \lambda_1), \qquad \sigma'\boldsymbol{\mu} = (\mu_k \geq \cdots \geq \mu_1).$$

Since $\boldsymbol{\lambda} \sim \sigma\boldsymbol{\lambda}$, it follows that $\sigma\boldsymbol{\lambda} \sim \sigma'\boldsymbol{\mu}$. But this implies that

$$\lambda_1 = \mu_1, \quad \lambda_1 + \lambda_2 = \mu_1 + \mu_2, \quad \ldots, \quad \lambda_1 + \lambda_2 + \cdots + \lambda_k = \mu_1 + \cdots + \mu_k,$$

forcing $\sigma\boldsymbol{\lambda} = \sigma'\boldsymbol{\mu}$, and the Lemma is proved. □

From now on, we will identify the set $P^+(\lambda, k)/\sim$ of equivalence classes with partitions of λ with at most k parts. By abuse of notation, we continue to denote this set by $P^+(\lambda, k)$; note that $\preceq$ is now a partial order on this set. As a consequence, we shall also assume without comment that $r_\ell(\boldsymbol{\lambda}) = \lambda_1 + \cdots + \lambda_\ell$ for $1 \leq \ell \leq k$.

3.3. Let λ be as in (3-1), and let $k \in \mathbb{Z}_+$. Write $\lambda = k\lambda_0 + p_0$, where $0 \leq p_0 < k$ and $\lambda_0 \in \mathbb{Z}_+$. Define $\boldsymbol{\lambda}_{\max} = (\lambda_k \geq \cdots \geq \lambda_1) \in P^+(\lambda, k)$ by

$$\lambda_j = \begin{cases} \lambda_0 & 1 \leq j \leq k - p_0, \\ \lambda_0 + 1 & j > k - p_0. \end{cases}$$

Observe that

$$r_\ell(\boldsymbol{\lambda}_{\max}) = \begin{cases} \ell\lambda_0 & \text{if } 1 \leq \ell \leq k - p_0, \\ (\ell+1)\lambda_0 - k + p_0 & \text{otherwise.} \end{cases}$$

The following result justifies the notation.

Lemma. *Keep the notation above. For all $\boldsymbol{\lambda} \in P^+(\lambda, k)$, we have $\boldsymbol{\lambda} \preceq \boldsymbol{\lambda}_{\max}$. Moreover, $\boldsymbol{\lambda}_{\max}$ is the unique element of $P^+(\lambda, k)$ satisfying*

$$\max_{1 \leq i \leq k} \{\lambda_i\} - \min_{1 \leq i \leq k} \{\lambda_i\} \leq 1. \tag{3-2}$$

Proof. It is clear that $\boldsymbol{\lambda}_{\max}$ satisfies (3-2). If $\boldsymbol{\mu} = (\mu_k \geq \cdots \geq \mu_1) \in P^+(\lambda, k)$ also satisfies (3-2), then $\mu_j - \mu_1 \leq 1$ for all $1 \leq j \leq k$. If $\mu_j = \mu_1$ for all j, then $\lambda = k\mu_1$, and hence we would have $p_0 = 0$ and $\mu_1 = \lambda_0$ as required. Otherwise, fix $j_0 \leq k-1$ such that $\mu_j = \mu_1$ for $1 \leq j \leq k - j_0$ and $\mu_j = \mu_1 + 1$ otherwise. Then

$$\sum_{s=1}^{k} \mu_s = k\mu_1 + j_0 = \lambda = k\lambda_0 + k_0 = \sum_{s=1}^{k} \lambda_s,$$

and hence $\mu_1 = \lambda_0$ and $j_0 = k_0$, which proves that $\boldsymbol{\mu} = \boldsymbol{\lambda}_{\max}$.

Suppose for a contradiction that there exist $\boldsymbol{\lambda} = (\lambda_k \geq \cdots \geq \lambda_1) \in P^+(\lambda, k)$ and $1 \leq j \leq k - p_0$ with $r_j(\boldsymbol{\lambda}) > j\lambda_0$, and assume that j is minimal with this property. Since

$$r_j(\boldsymbol{\lambda}) = \lambda_j + r_{j-1}(\boldsymbol{\lambda}) > j\lambda_0,$$

we get $\lambda_\ell \geq \lambda_j \geq \lambda_0 + 1$ for all $\ell \geq j$. This gives

$$\lambda = \lambda_k + \cdots + \lambda_{j+1} + r_j(\boldsymbol{\lambda}) > (k-j)(\lambda_0 + 1) + j\lambda_0 \geq k\lambda_0 + p_0 = \lambda,$$

which is a contradiction. The case $j > k - p_0$ is similar, and we omit the details. □

3.4. We now prove that the partial order on $P^+(\lambda, k)$ is entirely determined by the partial order $P^+(\lambda, 2)$. The first step is the following result, which determines the cover relation in $P^+(\lambda, 2)$.

Lemma. *Suppose that $\boldsymbol{\lambda} = (\lambda_1 \geq \lambda_2) \in P^+(\lambda, 2)$ and assume that $\boldsymbol{\lambda} \neq \boldsymbol{\lambda}_{\max}$. Then $\boldsymbol{\mu} \in P^+(\lambda, 2)$ covers $\boldsymbol{\lambda}$ if and only if*

$$\boldsymbol{\mu} = (\lambda_2 - 1 \geq \lambda_1 + 1).$$

Proof. Since $\boldsymbol{\lambda} \neq \boldsymbol{\lambda}_{\max}$, we see from the lemma in 3.3 that $\lambda_2 - \lambda_1 > 1$. Hence, $\boldsymbol{\mu} = (\lambda_2 - 1 \geq \lambda_1 + 1) \in P^+(\lambda, k)$ and $\boldsymbol{\lambda} \preceq \boldsymbol{\mu}$. Suppose that there exists $\boldsymbol{\nu} = (\nu_2 \geq \nu_1)$ with $\boldsymbol{\lambda} \prec \boldsymbol{\nu}$. Then $\lambda_1 < \nu_1$, and hence we get $\boldsymbol{\mu} \preceq \boldsymbol{\nu}$, which proves the lemma. □

3.5. Let $\boldsymbol{\lambda} = (\lambda_k \geq \cdots \geq \lambda_1) \in P^+(\lambda, k)$ be such that $\lambda_k - \lambda_1 \geq 2$. Then there exist $1 \leq j_1 < j_2 \leq k$ with

$$\lambda_{j_1} < \lambda_{j_1+1}, \quad \lambda_{j_2-1} < \lambda_{j_2}, \quad \lambda_{j_1} + 2 \leq \lambda_{j_2}.$$

For each such pair (j_2, j_1), we define a partition $\boldsymbol{\lambda}(j_2, j_1) = (\lambda'_k \geq \cdots \geq \lambda'_1)$:

$$\lambda'_i = \begin{cases} \lambda_i & i \neq j_1, j_2, \\ \lambda_{j_2} - 1 & i = j_2, \\ \lambda_{j_1} + 1 & i = j_1. \end{cases} \tag{3-3}$$

Observe that

$$r_\ell(\boldsymbol{\lambda}(j_2, j_1)) = \begin{cases} r_\ell(\boldsymbol{\lambda}) + 1 & j_1 \leq \ell < j_2, \\ r_\ell(\boldsymbol{\lambda}) & \text{otherwise}, \end{cases} \tag{3-4}$$

and so $\boldsymbol{\lambda} \prec \boldsymbol{\lambda}(j_2, j_1)$. The following proposition shows that the partial order on $P^+(\lambda, k)$ is controlled by the partial order on $P^+(\lambda, 2)$.

Proposition. *Let $\boldsymbol{\lambda} = (\lambda_k \geq \cdots \geq \lambda_1) \in P^+(\lambda, k)$ and assume that $\boldsymbol{\mu} \in P^+(\lambda, k)$ covers $\boldsymbol{\lambda}$. Then $\boldsymbol{\mu} = \boldsymbol{\lambda}(j_2, j_1)$ for some $1 \leq j_1 < j_2 \leq k$ with $\lambda_{j_1} < \lambda_{j_1+1}$ and $\lambda_{j_2-1} < \lambda_{j_2}$ and $\lambda_{j_1} + 2 \leq \lambda_{j_2}$.*

Proof. We proceed by induction on k. The lemma in 3.4 shows that induction begins at $k=2$. Assume that $k>2$. Let $\boldsymbol{\lambda} \in P^+(\lambda, k)$, and assume that $\boldsymbol{\mu} \in P^+(\lambda, k)$ covers $\boldsymbol{\lambda}$.

Suppose $r_\ell(\boldsymbol{\lambda}) < r_\ell(\boldsymbol{\mu})$ for all $1 \le \ell < k$. Since $\boldsymbol{\lambda}$ has a cover, it follows that $\boldsymbol{\lambda} \ne \boldsymbol{\lambda}_{\max}$, and so there exist $1 \le j_1 < j_2 \le \ell$ such that $\boldsymbol{\lambda}(j_2, j_1)$ is defined. Now, (3-4) shows that

$$\boldsymbol{\lambda} \prec \boldsymbol{\lambda}(j_2, j_1) \preceq \boldsymbol{\mu},$$

and hence $\boldsymbol{\mu} = \boldsymbol{\lambda}(j_2, j_1)$.

Suppose now that there exists $1 \le \ell < k$ such that $r_\ell(\boldsymbol{\mu}) = r_\ell(\boldsymbol{\lambda})$ and ℓ is minimal with this property. Consider first the case when $\ell = 1$, that is, $\mu_1 = \lambda_1$. Then

$$\boldsymbol{\mu}_0 = (\mu_k \ge \cdots \ge \mu_2), \qquad \boldsymbol{\lambda}_0 = (\lambda_k \ge \cdots \ge \lambda_2)$$

are distinct elements of $P^+(\lambda - \lambda_1, k-1)$ (since $\boldsymbol{\mu} \ne \boldsymbol{\lambda}$). Moreover, we claim that $\boldsymbol{\mu}_0$ covers $\boldsymbol{\lambda}_0$. If there exists $\boldsymbol{\nu}_0 = (\nu_k \ge \cdots \ge \nu_2) \in P^+(\lambda - \lambda_1, k-1)$ such that

$$\boldsymbol{\lambda}_0 \prec \boldsymbol{\nu}_0 \preceq \boldsymbol{\mu}_0,$$

then $\nu_2 \ge \lambda_2 \ge \lambda_1$. Hence, if we set $\boldsymbol{\nu} = (\nu_k \ge \cdots \ge \nu_2 \ge \lambda_1) \in P^+(\lambda,\ k)$, then we get

$$\boldsymbol{\lambda} \prec \boldsymbol{\nu} \preceq \boldsymbol{\mu}.$$

This forces $\boldsymbol{\nu} = \boldsymbol{\mu}$, and hence $\boldsymbol{\nu}_0 = \boldsymbol{\mu}_0$. By induction on k and noting that $k-1 \ge 2$, we see that

$$\boldsymbol{\mu}_0 = \boldsymbol{\lambda}_0(j_2, j_1)$$

for some $2 \le j_1 < j_2 \le k$, and hence $\boldsymbol{\mu} = \boldsymbol{\lambda}(j_2, j_1)$.

It remains to consider the case when $\ell \ge 2$, which in particular would imply that $\mu_1 > \lambda_1$. This time, we take

$$\boldsymbol{\mu}_0 = (\mu_\ell \ge \cdots \ge \mu_1), \qquad \boldsymbol{\lambda}_0 = (\lambda_\ell \ge \cdots \ge \lambda_1)$$

and note that these are elements of $P^+(r_\ell(\boldsymbol{\lambda}), \ell)$ and that $\boldsymbol{\lambda}_0 \prec \boldsymbol{\mu}_0$. We claim again that $\boldsymbol{\mu}_0$ covers $\boldsymbol{\lambda}_0$. Thus, let $\boldsymbol{\nu}_0 = (\nu_\ell \ge \cdots \ge \nu_1) \in P^+(r_\ell(\boldsymbol{\lambda}), \ell)$ be such that

$$\boldsymbol{\lambda}_0 \prec \boldsymbol{\nu}_0 \preceq \boldsymbol{\mu}_0.$$

Then

$$\nu_s + \cdots + \nu_1 \ge \lambda_s + \cdots + \lambda_1, \quad 1 \le s \le \ell, \quad \nu_\ell + \cdots + \nu_1 = \lambda_\ell + \cdots + \lambda_1.$$

Suppose that $\nu_\ell > \lambda_{\ell+1}$. Then we get $\nu_\ell > \lambda_{\ell+1} \ge \lambda_\ell$ and

$$0 < \nu_\ell - \lambda_\ell = (\lambda_{\ell-1} + \cdots + \lambda_1) - (\nu_{\ell-1} + \cdots + \nu_1) \le 0,$$

which is a contradiction. Thus we get $\nu_\ell \le \lambda_{\ell+1}$, and hence

$$\boldsymbol{\nu} = (\lambda_k \ge \cdots \ge \lambda_{\ell+1} \ge \nu_\ell \ge \cdots \ge \nu_1) \in P^+(\lambda, k).$$

Also we see that $\boldsymbol{\lambda} \prec \boldsymbol{\nu} \preceq \boldsymbol{\mu}$. Since $\boldsymbol{\mu}$ is a cover of $\boldsymbol{\lambda}$, this forces $\boldsymbol{\nu} = \boldsymbol{\mu}$, and hence $\boldsymbol{\nu}_0 = \boldsymbol{\mu}_0$. Thus we conclude that $\boldsymbol{\mu}_0$ covers $\boldsymbol{\lambda}_0$. By induction on k, $\boldsymbol{\mu}_0 = \boldsymbol{\lambda}_0(j_2, j_1)$ for some $1 \le j_1 < j_2 \le \ell$. We see that $\boldsymbol{\lambda} \prec \boldsymbol{\lambda}(j_2, j_1) \preceq \boldsymbol{\mu}$, which forces $\boldsymbol{\mu} = \boldsymbol{\lambda}(j_2, j_1)$. Thus we have proved the proposition. $\square$

3.6. *Proof of Theorem 1(i).* Assume first that $\mathfrak{g}$ is $\mathfrak{sl}_2$. Let $\lambda \in P^+ = \mathbb{Z}_+\omega_1$ be an arbitrary dominant integral weight, and let $k \ge 2$. Let $\boldsymbol{\lambda} = (\lambda_k \ge \cdots \ge \lambda_1) \in P^+(\lambda, k)$ and $\boldsymbol{\mu} = (\mu_k \ge \cdots \ge \mu_1) \in P^+(\lambda, k)$ be such that $\boldsymbol{\lambda} \preceq \boldsymbol{\mu}$ (in $P^+(\lambda, k)/\sim$). First we show that if $\boldsymbol{\lambda} \prec \boldsymbol{\mu}$ (in $P^+(\lambda, k)/\sim$), then

$$\dim \bigotimes_{s=1}^{k} V(\lambda_s) < \dim \bigotimes_{s=1}^{k} V(\mu_s), \quad \text{that is,} \quad \prod_{s=1}^{k} (\lambda_s + 1) < \prod_{s=1}^{k} (\mu_s + 1). \tag{3-5}$$

A standard argument shows that there exists a sequence $\boldsymbol{\lambda} = \boldsymbol{\nu}_0, \boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_p = \boldsymbol{\mu}$ of elements of $P^+(\lambda, k)$ such that $\boldsymbol{\nu}_q$ covers $\boldsymbol{\nu}_{q-1}$ for each $1 \le q \le p$. It suffices to show (3-5) in the case when $\boldsymbol{\mu}$ covers $\boldsymbol{\lambda}$. Then, by the proposition in 3.5, there exist $1 \le j_1 < j_2 \le k$ with $\lambda_{j_1} < \lambda_{j_1+1}$ and $\lambda_{j_2-1} < \lambda_{j_2}$ and $\lambda_{j_1} + 2 \le \lambda_{j_2}$ such that $\boldsymbol{\mu} = \boldsymbol{\lambda}(j_2, j_1)$. Thus the inequality (3-5) is equivalent to

$$(\lambda_{j_1} + 1)(\lambda_{j_2} + 1) < (\lambda_{j_1} + 2)\lambda_{j_2}.$$

But this is obvious from the fact that $\lambda_{j_1} + 2 \le \lambda_{j_2}$. Thus we have proved (3-5). Also, we have proved (under the assumption that $\boldsymbol{\lambda} \preceq \boldsymbol{\mu}$) that if

$$\dim \bigotimes_{s=1}^{k} V(\lambda_s) = \dim \bigotimes_{s=1}^{k} V(\mu_s),$$

then $\boldsymbol{\lambda} = \boldsymbol{\mu}$ (in $P^+(\lambda, k)/\sim$). The converse of this statement is obvious by the lemma in 3.2. Thus we have proved Theorem 1(i) in the case of $\mathfrak{sl}_2$.

Assume next that $\mathfrak{g}$ is an arbitrary finite-dimensional simple complex Lie algebra, and that $\lambda \in P^+$ is an arbitrary dominant integral weight. Let $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_k)$, $\boldsymbol{\mu} = (\mu_1, \ldots, \mu_k) \in P^+(\lambda, k)$ be such that $\boldsymbol{\lambda} \preceq \boldsymbol{\mu}$ (in $P^+(\lambda, k)/\sim$). Using the Weyl dimension formula, we see that

$$\dim \bigotimes_{s=1}^{k} V(\lambda_s) = \prod_{s=1}^{k} \prod_{\alpha \in R^+} \frac{(\lambda_s + \rho)(h_\alpha)}{\rho(h_\alpha)},$$
$$\dim \bigotimes_{s=1}^{k} V(\mu_s) = \prod_{s=1}^{k} \prod_{\alpha \in R^+} \frac{(\mu_s + \rho)(h_\alpha)}{\rho(h_\alpha)}.$$

So, in order to prove that $\dim \bigotimes_{s=1}^{k} V(\lambda_s) \le \dim \bigotimes_{s=1}^{k} V(\mu_s)$, it suffices to show that

$$\prod_{s=1}^{k}(\lambda_s+\rho)(h_\alpha) \le \prod_{s=1}^{k}(\mu_s+\rho)(h_\alpha) \quad \text{for each } \alpha \in R^+.$$

For each $\alpha \in R^+$ and $1 \le s \le k$, we set

$$\begin{aligned}
\lambda_s^{(\alpha)} &= (\lambda_s+\rho)(h_\alpha)-1,\\
\mu_s^{(\alpha)} &= (\mu_s+\rho)(h_\alpha)-1,\\
\lambda^{(\alpha)} &= \lambda(h_\alpha)+k(\rho(h_\alpha)-1) = \sum_{s=1}^{k}\lambda_s^{(\alpha)} = \sum_{s=1}^{k}\mu_s^{(\alpha)}.
\end{aligned}$$

Then we see that the elements

$$\boldsymbol{\lambda}^{(\alpha)} = (\lambda_1^{(\alpha)},\dots,\lambda_k^{(\alpha)}), \quad \mu^{(\alpha)} = (\mu_1^{(\alpha)},\dots,\mu_k^{(\alpha)})$$

are elements of $P^+(\lambda^{(\alpha)},k)$ for $\mathfrak{sl}_2$ (or rather $\mathfrak{sl}_2(\alpha)$) satisfying $\boldsymbol{\lambda}^{(\alpha)} \preceq \boldsymbol{\mu}^{(\alpha)}$ (in $P^+(\lambda^{(\alpha)},k)/\sim$). Hence, by the argument for $\mathfrak{sl}_2$ above, we obtain

$$\prod_{s=1}^{k}(\lambda_s+\rho)(h_\alpha) = \prod_{s=1}^{k}(\lambda_s^{(\alpha)}+1) \le \prod_{s=1}^{k}(\mu_s^{(\alpha)}+1) = \prod_{s=1}^{k}(\mu_s+\rho)(h_\alpha),$$

as desired. Also, we deduce that (under the assumption that $\boldsymbol{\lambda} \preceq \boldsymbol{\mu}$)

$$\begin{aligned}
\dim \bigotimes_{s=1}^{k} V(\lambda_s) = \dim \bigotimes_{s=1}^{k} V(\mu_s)&\\
&\iff \prod_{s=1}^{k}(\lambda_s^{(\alpha)}+1) = \prod_{s=1}^{k}(\mu_s^{(\alpha)}+1) \quad \text{for all } \alpha \in R^+\\
&\iff \boldsymbol{\lambda}^{(\alpha)} = \boldsymbol{\mu}^{(\alpha)} \quad \text{for all } \alpha \in R^+ \text{ (by the argument for } \mathfrak{sl}_2 \text{ above)}\\
&\iff \boldsymbol{\lambda} = \boldsymbol{\mu}.
\end{aligned}$$

Thus we have proved Theorem 1(i). □

4. Proof of Theorem 1(ii)

4.1. As in Section 3, we regard elements of $P^+(N\omega_i,k)$ as partitions of N. Also, we deduce from the proposition in 3.5 that Theorem 1(ii) is proved once we establish the following proposition.

Proposition. *Suppose that $r, s \in \mathbb{Z}_+$ and assume that $s \ge r+1$. Let $i \in I$ be such that ω_i is minuscule. Then, for all $\mu \in P^+$, we have*

$$\begin{aligned}
&\dim \operatorname{Hom}_{\mathfrak{g}}\bigl(V(\mu), V(s\omega_i)\otimes V(r\omega_i)\bigr)\\
&\qquad\le \dim \operatorname{Hom}_{\mathfrak{g}}\bigl(V(\mu), V((s-1)\omega_i)\otimes V((r+1)\omega_i)\bigr).
\end{aligned}$$

The proposition is established in the rest of the section using the Littelmann path model.

4.2. We recall the essential definitions and results from [Littelmann 1994; 1995].

Definition. (i) Let $\lambda \in P^+$ and $\mu, \nu \in W\lambda$. We say that $\mu \geq \nu$ if there exists a sequence $\mu = \xi_0, \xi_1, \dots, \xi_m = \nu$ of elements in $W\lambda$ and elements $\beta_1, \dots, \beta_m \in R^+$ of positive roots such that

$$\xi_p = s_{\beta_p}(\xi_{p-1}), \quad \xi_{p-1}(h_{\beta_p}) < 0, \quad 1 \leq p \leq m.$$

Moreover, in this case, we let $\operatorname{dist}(\mu, \nu)$ be the maximal length m of all such possible sequences.

(ii) For $\mu, \nu \in W\lambda$ with $\mu > \nu$ and a rational number $0 < a < 1$, we define an a-chain for (μ, ν) as a sequence $\mu = \xi_0 > \xi_1 > \cdots > \xi_m = \nu$ of elements in $W\lambda$ such that

$$\operatorname{dist}(\xi_{p-1}, \xi_p) = 1, \quad \xi_p = s_{\beta_p}(\xi_{p-1}), \quad a\xi_{p-1}(h_{\beta_p}) \in \mathbb{Z}_{<0}$$

for all $p = 1, 2, \dots, m$.

(iii) An LS path of shape λ is a pair $(\underline{\nu}; \underline{a})$ consisting of a sequence

$$\underline{\nu} = (\nu_1 > \nu_2 > \cdots > \nu_\ell) \quad (\text{for some } \ell \geq 1)$$

of elements in $W\lambda$ and a sequence $\underline{a} = (0 = a_0 < a_1 < \cdots < a_\ell = 1)$ of rational numbers satisfying the condition that there exists an a_p-chain for (ν_p, ν_{p+1}) for $p = 1, 2, \dots, \ell - 1$. We denote by $\mathbb{B}(\lambda)$ the set of all LS paths of shape λ.

4.3. Set $\mathfrak{h}_{\mathbb{R}}^* = \sum_{i=1}^n \mathbb{R}\omega_i$, where $\mathbb{R}$ is the set of real numbers. Given an LS path $\pi = (\underline{\nu}; \underline{a}) = (\nu_1, \nu_2, \dots, \nu_\ell;\ a_0, a_1, \dots, a_\ell)$ of shape λ, define a piecewise linear, continuous map $\pi : [0, 1] \to \mathfrak{h}_{\mathbb{R}}^*$ by

$$\pi(t) = \sum_{p=1}^{q-1} (a_p - a_{p-1})\nu_p + (t - a_{q-1})\nu_q \quad \text{for } a_{q-1} \leq t \leq a_q,\ 1 \leq q \leq \ell. \tag{4-1}$$

Clearly, distinct LS paths give rise to distinct piecewise linear functions with values in $\mathfrak{h}_{\mathbb{R}}^*$, and we shall make this identification freely in what follows.

Given $\xi \in P^+$, we say that an LS path π of shape λ is ξ-dominant if

$$(\xi + \pi(t))(h_i) \geq 0$$

for all $i \in I$ and $t \in [0, 1]$. Note that $\pi = (\nu_1, \nu_2, \dots, \nu_\ell;\ a_0, a_1, \dots, a_\ell)$ is ξ-dominant if and only if $(\xi + \pi(a_p))(h_i) \geq 0$ for all $i \in I$ and $0 \leq p \leq \ell$.

For $\lambda, \xi, \mu \in P^+$, set

$$\mathbb{B}(\lambda)^{\mu}_{\xi\text{-dom}} = \{\pi \in \mathbb{B}(\lambda) : \pi \text{ is } \xi\text{-dominant, and } \xi + \pi(1) = \mu\}. \tag{4-2}$$

Theorem [Littelmann 1994]. *For $\lambda, \xi, \mu \in P^+$, we have*

$$\dim \operatorname{Hom}_{\mathfrak{g}}\big(V(\mu),\ V(\xi) \otimes V(\lambda)\big) = \#\mathbb{B}(\lambda)^{\mu}_{\xi\text{-dom}}. \tag{4-3}$$

4.4. The first step in the proof of the proposition in 4.1 is to describe the set $\mathbb{B}(N\omega_i)$ explicitly when ω_i is minuscule.

Lemma. *Let $i \in I$ be such that ω_i is minuscule. Consider a pair $(\underline{\nu}; \underline{a})$, where $\underline{\nu} = (\nu_1 > \nu_2 > \cdots > \nu_\ell)$ is a sequence of elements in $W(N\omega_i)$ and*

$$\underline{a} = (0 = a_0 < a_1 < \cdots < a_\ell = 1)$$

is a sequence of rational numbers (for some $\ell \geq 1$). Then we have

$$(\underline{\nu}; \underline{a}) \in \mathbb{B}(N\omega_i) \iff Na_p \in \mathbb{Z}_+ \quad \textit{for all } 0 \leq p \leq \ell.$$

Proof. Suppose first that $(\underline{\nu}; \underline{a})$ is such that $Na_p \in \mathbb{Z}_+$ for all $0 \leq p \leq \ell$, in which case we must prove that for $1 \leq p \leq \ell - 1$, there exists an a_p-chain for $(\nu_p,\ \nu_{p+1})$. Since $\nu_p > \nu_{p+1}$, there exists a sequence $\nu_p = \xi_0 > \xi_1 > \cdots > \xi_m = \nu_{p+1}$ of elements in $W(N\omega_i)$ such that

$$\operatorname{dist}(\xi_{q-1}, \xi_q) = 1, \quad \xi_q = s_{\beta_q}(\xi_{q-1}), \quad \xi_{q-1}(h_{\beta_q}) < 0, \quad 1 \leq q \leq m.$$

Writing $\xi_{p-1} = \boldsymbol{w}(N\omega_i)$ with some $\boldsymbol{w} \in W$, we get

$$\xi_{p-1}(h_{\beta_p}) = N \underbrace{(\boldsymbol{w}\omega_i)(h_{\beta_p})}_{\in \mathbb{Z}} \in N\mathbb{Z}_{<0},$$

which gives $a_p \xi_{p-1}(h_{\beta_p}) \in \mathbb{Z}$, as required.

Now suppose that $(\underline{\nu}; \underline{a}) = (\nu_1, \nu_2, \ldots, \nu_\ell;\ a_0, a_1, \ldots, a_\ell) \in \mathbb{B}(N\omega_i)$. If $\nu \in W(N\omega_i)$, then since ω_i is minuscule, we have that $\nu(h_\beta) \in \{0, \pm N\}$ for all $\beta \in R$. We have to prove that $Na_p \in \mathbb{Z}_+$ for $1 \leq p \leq \ell$. The assertion is obvious when $p = 0$ or ℓ. If $1 \leq p \leq \ell - 1$, choose an a_p-chain $\nu_p = \xi_0 > \xi_1 > \cdots > \xi_m = \nu_{p+1}$. Then there exists a positive root β such that

$$\xi_1 = s_\beta(\xi_0), \quad a_p \xi_0(h_\beta) \in \mathbb{Z}_{<0}.$$

In particular, we have $\xi_0(h_\beta) < 0$, which implies that $\xi_0(h_\beta) = -N$. Thus we get $Na_p \in \mathbb{Z}_+$ as required. ☐

4.5. The following observations are trivial but useful:

$$\begin{cases} \nu \in W(r\omega_i) \implies \nu' = \dfrac{r+1}{r}\nu \in W((r+1)\omega_i), \\ \nu, \gamma \in W(r\omega_i),\ \nu > \gamma \implies \nu' > \gamma', \\ 0 \leq a < 1 \implies 0 \leq a' = \dfrac{ra}{r+1} < 1, \quad (r+1)a' \in \mathbb{Z}_+. \end{cases} \tag{4-4}$$

Given $(\underline{\nu};\underline{a}) = (\nu_1,\dots,\nu_\ell;\ a_0,\dots,a_\ell)$, set

$$(\underline{\nu}';\underline{a}') = \begin{cases} \big(\nu_1',\dots,\nu_\ell',(r+1)\omega_i;\ a_0',\dots,a_\ell',1\big) & \text{if } \nu_\ell \neq r\omega_i,\\ \big(\nu_1',\dots,\nu_{\ell-1}',(r+1)\omega_i;\ a_0',\dots,a_{\ell-1}',1\big) & \text{if } \nu_\ell = r\omega_i.\end{cases}$$

We now prove the proposition in 4.1 by showing that for each $\mu \in P^+$, the assignment

$$(\underline{\nu};\underline{a}) \to (\underline{\nu}';\underline{a}')$$

gives an injective map

$$\iota_r : \mathbb{B}(r\omega_i)^{\mu}_{s\omega_i\text{-dom}} \hookrightarrow \mathbb{B}\big((r+1)\omega_i\big)^{\mu}_{(s-1)\omega_i\text{-dom}}.$$

It is immediate from the lemma in 4.4, along with (4-4) and the fact that $(r+1)\omega_i$ is the minimum element in $W((r+1)\omega_i)$ (with respect to the ordering $>$; see also [Littelmann 1995, Remark 4.2]), that

$$(\underline{\nu};\underline{a}) \in \mathbb{B}(r\omega_i) \implies (\underline{\nu}';\underline{a}') \in \mathbb{B}((r+1)\omega_i).$$

Let π and π' be the piecewise linear paths associated to $(\underline{\nu};\underline{a})$ and $(\underline{\nu}';\underline{a}')$, respectively (see (4-1)). We have

$$\pi'(t) = \begin{cases} \pi\Big(\dfrac{r+1}{r}t\Big) & \text{for } 0 \le t \le \dfrac{r}{r+1},\\ \pi(1) + \Big(t - \dfrac{r}{r+1}\Big)(r+1)\omega_i & \text{for } \dfrac{r}{r+1} \le t \le 1.\end{cases} \tag{4-5}$$

This proves immediately that

$$s\omega_i + \pi(1) = \mu \implies (s-1)\omega_i + \pi'(1) = (s-1)\omega_i + \pi(1) + \omega_i = s\omega_i + \pi(1) = \mu.$$

Moreover, since

$$t \in \Big[0,\ \frac{r}{r+1}\Big] \iff \frac{r+1}{r}t \in [0,\ 1],$$

it follows also that if η corresponds to an element of $\mathbb{B}(s\omega_i)$ different from $(\underline{\nu};\underline{a})$, then there exists $t \in [0, r/(r+1)]$ such that

$$\pi'(t) \neq \eta'(t).$$

Thus we have proved that ι_r is injective.

It remains to show that π' is $(s-1)\omega_i$-dominant. Let $j \in I$. If $j \neq i$, we have

$$\big((s-1)\omega_i + \pi'(t)\big)(h_j) = (\pi'(t))(h_j).$$

Since π is $s\omega_i$-dominant, we have

$$0 \le (s\omega_i + \pi(t))(h_j) = (\pi(t))(h_j) \quad \text{for all } 0 \le t \le 1.$$

Thus, by (4-5), we see that $(\pi'(t))(h_j) \geq 0$ for all $0 \leq t \leq r/(r+1)$. Also, for $r/(r+1) \leq t \leq 1$, we have

$$(\pi'(t))(h_j) = (\pi(1))(h_j) + \Big(t - \frac{r}{r+1}\Big)(r+1)\underbrace{\omega_i(h_j)}_{=0} = (\pi(1))(h_j) \geq 0.$$

Thus we have shown that if $j \neq i$, then $\big((s-1)\omega_i + \pi'(t)\big)(h_j) \geq 0$ for all $0 \leq t \leq 1$.

Next, assume that $j = i$. We see from (4-5) that the function

$$\big((s-1)\omega_i + \pi'(t)\big)(h_i)$$

is strictly increasing on $[r/(r+1), 1]$. Thus it suffices to show that

$$\big((s-1)\omega_i + \pi'(t)\big)(h_i) \geq 0 \quad \text{for all } 0 \leq t \leq \frac{r}{r+1}. \tag{4-6}$$

Let $0 \leq q \leq \ell$. We have

$$(\pi'(a'_q))(h_i) = \sum_{p=1}^{q} (a'_p - a'_{p-1})\nu'_p(h_i).$$

Here, we note that $\nu'_p(h_i) \in \{0, \pm(r+1)\}$ since ω_i is assumed to be minuscule. Hence,

$$\begin{aligned}(\pi'(a'_q))(h_i) &= \sum_{p=1}^{q} \underbrace{(a'_p - a'_{p-1})}_{>0}\nu'_p(h_i) \geq -\sum_{p=1}^{q}(a'_p - a'_{p-1})(r+1) \\ &= -(r+1)a'_q = -ra_q \geq -r.\end{aligned}$$

Thus, for every $0 \leq q \leq \ell$,

$$\big((s-1)\omega_i + \pi'(a'_q)\big)(h_i) \geq (s-1) - r = s - (r+1) \geq 0 \quad \text{by assumption,}$$

which implies (4-6). Thus we have proved the proposition. $\square$

5. The poset $P^+(\boldsymbol{\lambda}, 2)/\!\sim$

As we remarked earlier, it is clear that if $\sigma \in S_k$, then $\boldsymbol{\lambda}$ and $\sigma\boldsymbol{\lambda}$ are in the same equivalence class with respect to $\sim$ for all $\boldsymbol{\lambda} \in P^+(\lambda, k)$. However, the following example shows that outside $\mathfrak{sl}_2$, the equivalence class of $\sim$ is in general bigger than the S_k-orbit of an element. Suppose that $\mathfrak{g}$ is of type $\mathfrak{sl}_3$ and that $k = 3$ and $\lambda = 3\omega_1 + 3\omega_2$. Then it is easily seen that

$$\boldsymbol{\lambda} = (\omega_2, \omega_1 + 2\omega_2, 2\omega_1) \sim \boldsymbol{\mu} = (2\omega_1, \omega_1, 2\omega_1 + \omega_2),$$

but clearly $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$ are not in the same S_3-orbit. However, when $k = 2$, we prove below (see the lemma in 5.5) that for all simple Lie algebras, the equivalence class is exactly the S_2-orbit.

5.1. We begin with an equivalent formulation of the preorder in the case $k=2$.

Proposition. *Let $\mathfrak{g}$ be a finite-dimensional simple complex Lie algebra and let $\boldsymbol{\lambda}=(\lambda_1,\lambda_2)$ and $\boldsymbol{\mu}=(\mu_1,\mu_2)$ be elements of $P^+(\lambda,2)/\sim$ for some $\lambda\in P^+$. Then*

$$\begin{aligned}\boldsymbol{\lambda}\preceq\boldsymbol{\mu} &\iff (\lambda_1-\mu_1)(h_\alpha)(\mu_1-\lambda_2)(h_\alpha)\geq 0 \quad \textit{for all } \alpha\in R^+\\ &\iff (\lambda_1-\mu_1)(h_\alpha)(\mu_1-\lambda_2)(h_\alpha)\geq 0 \quad \textit{for all } \alpha\in R.\end{aligned}$$

In particular, if $\boldsymbol{w}\in W$ is such that $\boldsymbol{w}(\lambda_1-\lambda_2)\in P^+$, then

$$\boldsymbol{\lambda}\preceq\boldsymbol{\mu} \iff \boldsymbol{w}(\lambda_1-\mu_1)\in P^+ \ \textit{and}\ \boldsymbol{w}(\mu_1-\lambda_2)\in P^+.$$

Proof. Since $r_{\alpha,2}(\boldsymbol{\mu})=\lambda(h_\alpha)$, we see that

$$r_{\alpha,2}(\boldsymbol{\mu})-2r_{\alpha,1}(\boldsymbol{\mu})=\begin{cases}(\mu_1-\mu_2)(h_\alpha) & \text{if } \mu_2(h_\alpha)\leq\mu_1(h_\alpha),\\ (\mu_2-\mu_1)(h_\alpha) & \text{otherwise,}\end{cases}$$

or in other words that

$$r_{\alpha,2}(\boldsymbol{\mu})-2r_{\alpha,1}(\boldsymbol{\mu})=|(\mu_1-\mu_2)(h_\alpha)|. \tag{5-1}$$

Since $k=2$, we see that

$$\boldsymbol{\lambda}\preceq\boldsymbol{\mu}\iff r_{\alpha,1}(\boldsymbol{\lambda})\leq r_{\alpha,1}(\boldsymbol{\mu}) \quad \text{for all } \alpha\in R^+,$$

and hence we get

$$\begin{aligned}\boldsymbol{\lambda}\preceq\boldsymbol{\mu} &\iff r_{\alpha,2}(\boldsymbol{\mu})-2r_{\alpha,1}(\boldsymbol{\mu})\leq r_{\alpha,2}(\boldsymbol{\lambda})-2r_{\alpha,1}(\boldsymbol{\lambda})\\ &\iff |(\mu_1-\mu_2)(h_\alpha)|\leq|(\lambda_1-\lambda_2)(h_\alpha)|\\ &\iff (\mu_1-\mu_2)(h_\alpha)^2\leq(\lambda_1-\lambda_2)(h_\alpha)^2\\ &\iff (2\mu_1-\lambda_1-\lambda_2)(h_\alpha)^2\leq(\lambda_1-\lambda_2)(h_\alpha)^2\\ &\iff (\lambda_1-\mu_1)(h_\alpha)(\mu_1-\lambda_2)(h_\alpha)\geq 0\end{aligned}$$

for all $\alpha\in R^+$. Since $h_{-\alpha}=-h_\alpha$, we see that

$$\boldsymbol{\lambda}\preceq\boldsymbol{\mu}\iff(\lambda_1-\mu_1)(h_\alpha)(\mu_1-\lambda_2)(h_\alpha)\geq 0 \quad \text{for all } \alpha\in R.$$

Now let $\boldsymbol{w}\in W$ be such that $\boldsymbol{w}(\lambda_1-\lambda_2)\in P^+$. If $\boldsymbol{\lambda}\preceq\boldsymbol{\mu}$, then for all $\alpha\in R^+$,

$$\boldsymbol{w}(\lambda_1-\mu_1)(h_\alpha)\boldsymbol{w}(\mu_1-\lambda_2)(h_\alpha)=(\lambda_1-\mu_1)(h_{\boldsymbol{w}^{-1}\alpha})(\mu_1-\lambda_2)(h_{\boldsymbol{w}^{-1}\alpha})\geq 0$$

by the first statement of the proposition. Also, we have

$$\boldsymbol{w}(\lambda_1-\mu_1)(h_\alpha)+\boldsymbol{w}(\mu_1-\lambda_2)(h_\alpha)=\boldsymbol{w}(\lambda_1-\lambda_2)(h_\alpha)\geq 0 \quad \text{for all } \alpha\in R^+,$$

since $\boldsymbol{w}(\lambda_1-\lambda_2)\in P^+$ by assumption. Thus we conclude that $\boldsymbol{w}(\lambda_1-\mu_1)(h_\alpha)\geq 0$ and $\boldsymbol{w}(\mu_1-\lambda_2)(h_\alpha)\geq 0$ for all $\alpha\in R^+$, which implies that both of $\boldsymbol{w}(\lambda_1-\mu_1)$

and $\boldsymbol{w}(\mu_1 - \lambda_2)$ are dominant. Conversely, assume that both of $\boldsymbol{w}(\lambda_1 - \mu_1)$ and $\boldsymbol{w}(\mu_1 - \lambda_2)$ are dominant. Then, for all $\alpha \in R$,

$$(\lambda_1 - \mu_1)(h_\alpha)(\mu_1 - \lambda_2)(h_\alpha) = \boldsymbol{w}(\lambda_1 - \mu_1)(h_{\boldsymbol{w}^{-1}\alpha})\boldsymbol{w}(\mu_1 - \lambda_2)(h_{\boldsymbol{w}^{-1}\alpha}) \geq 0.$$

Hence, by the first statement of the proposition, we have $\boldsymbol{\lambda} \preceq \boldsymbol{\mu}$. Thus the second statement of the proposition is established. $\square$

5.2. The next result gives information about the maximal elements in $P^+(\lambda, 2)/\sim$.

Lemma. *Let $\lambda \in P^+$ and let $i \in I$, $\boldsymbol{w} \in W$ be such that $\lambda - \boldsymbol{w}^{-1}\omega_i \in P^+$. Then the equivalence classes of (λ, λ) and $(\lambda, \lambda - \boldsymbol{w}^{-1}\omega_i)$ are maximal in the posets $P^+(2\lambda, 2)$ and $P^+(2\lambda - \boldsymbol{w}^{-1}\omega_i, 2)$, respectively.*

Proof. Let $\boldsymbol{\mu} = (\mu_1, \mu_2) \in P^+(2\lambda, 2)$ be such that $(\lambda, \lambda) \preceq \boldsymbol{\mu}$ in $P^+(2\lambda, 2)/\sim$. Using the proposition in 5.1, we get $\lambda - \mu_1 \in P^+$ and $\mu_1 - \lambda \in P^+$, which forces $\mu_1 = \mu_2 = \lambda$ as required.

Similarly, if $\boldsymbol{\mu} \in P^+(2\lambda - \boldsymbol{w}^{-1}\omega_i, 2)/\sim$ with $(\lambda, \lambda - \boldsymbol{w}^{-1}\omega_i) \preceq \boldsymbol{\mu}$, then the proposition in 5.1 gives $\boldsymbol{w}(\lambda - \mu_1) \in P^+$ and $\boldsymbol{w}(\mu_1 - \lambda) + \omega_i \in P^+$. But this is only possible if either $\mu_1 = \lambda_1$ or $\mu_1 - \lambda_1 = -\boldsymbol{w}^{-1}\omega_i$. In either case, this implies that $\boldsymbol{\mu} = (\lambda, \lambda - \boldsymbol{w}^{-1}\omega_i)$ in $P^+(2\lambda - \boldsymbol{w}^{-1}\omega_i, 2)/\sim$. $\square$

5.3. Suppose that $\mathfrak{g}$ is of type A_n. Then we can refine the preceding result as follows. Given $\lambda = \sum_{i=1}^n r_i\omega_i \in P^+$, define elements λ^s, $s = 1, 2$ as follows. If $r_i \in 2\mathbb{Z}_+$ for all $i \in I$, then take $\lambda^1 = \lambda^2 = \lambda$. Otherwise let $1 \leq i_0 < i_1 < \cdots < i_p \leq n$ be the set where r_i is odd and set $I_+ = I \setminus \{i_0, \ldots, i_p\}$. Define

$$\lambda^1 = \sum_{s=0}^{p} \left(\frac{r_{i_s} + (-1)^s}{2}\right)\omega_{i_s} + \sum_{i \in I_+} \left(\frac{r_i}{2}\right)\omega_i, \quad \lambda^2 = \lambda - \lambda^1.$$

In either case, set $\boldsymbol{\lambda}_{\max} = (\lambda^1, \lambda^2)$.

Proposition. *Let $\lambda \in P^+$ and $\mathfrak{g}$ be of type A_n. Then either $\lambda^1 = \lambda^2$ or $\lambda^2 = \lambda^1 - \boldsymbol{w}^{-1}\omega_i$ for some $\boldsymbol{w} \in W$ and $i \in I$. In either case, $\boldsymbol{\lambda}_{\max}$ is the unique maximal element in $P^+(\lambda, 2)/\sim$.*

Proof. If $\lambda^1 \neq \lambda^2$, then by definition, we have

$$\lambda^1 - \lambda^2 = \omega_{i_0} - \omega_{i_1} + \cdots + (-1)^p\omega_{i_p},$$

where $0 \leq i_0 < \cdots < i_p \leq n$. It is elementary to see that $(\lambda^1 - \lambda^2)(h_\alpha) \in \{0, \pm 1\}$, that is, $\lambda^1 - \lambda^2$ is in $W\tau$ for some minuscule $\tau \in P^+$, and hence in $W\omega_i$ for some $i \in I$. It remains to prove that it is the unique maximal element. In other words, we must prove that if $\boldsymbol{\mu} \in P^+(\lambda, 2)$, then $\boldsymbol{\mu} \preceq \boldsymbol{\lambda}_{\max}$. Again, using the proposition in 5.1, it suffices to prove that

$$(\mu_1 - \lambda^1)(h_\alpha)(\mu_1 - \lambda^2)(h_\alpha) = (\mu_1 - \lambda^1)(h_\alpha)(\lambda^1 - \mu_2)(h_\alpha) \geq 0.$$

If $(\mu_1-\lambda^1)(h_\alpha)=0$, there is nothing to prove. If $(\mu_1-\lambda^1)(h_\alpha)>0$, then since $(\lambda^1-\lambda^2)(h_\alpha)\in\{0,\pm1\}$, we get $\mu_1(h_\alpha)\ge\lambda^2(h_\alpha)$ as required. The case when $(\mu_1-\lambda^1)(h_\alpha)<0$ is identical. □

5.4.

Proposition. *Let $\boldsymbol{\lambda},\boldsymbol{\mu}\in P^+(\lambda,2)/\sim$ with $\boldsymbol{\lambda}\prec\boldsymbol{\mu}$ and assume there exist $\boldsymbol{w}\in W$ and $i_0\in I$ such that $\boldsymbol{w}(\lambda_1-\lambda_2)\in P^+$ and*

$$\boldsymbol{w}(\lambda_1-\mu_1)(h_{i_0})\boldsymbol{w}(\mu_1-\lambda_2)(h_{i_0})>0. \tag{5-2}$$

Then $\big(\lambda_1-\boldsymbol{w}^{-1}\omega_{i_0},\lambda_2+\boldsymbol{w}^{-1}\omega_{i_0}\big)\in P^+(\lambda,2)$ and

$$\boldsymbol{\lambda}\prec\big(\lambda_1-\boldsymbol{w}^{-1}\omega_{i_0},\lambda_2+\boldsymbol{w}^{-1}\omega_{i_0}\big)\preceq\boldsymbol{\mu}. \tag{5-3}$$

Proof. First we remark that by (5-2) and the assumption that $\boldsymbol{w}(\lambda_1-\lambda_2)\in P^+$,

$$\boldsymbol{w}(\lambda_1-\lambda_2)(h_{i_0})=\boldsymbol{w}(\lambda_1-\mu_1)(h_{i_0})+\boldsymbol{w}(\mu_1-\lambda_2)(h_{i_0})>0. \tag{5-4}$$

Let us show that $\lambda_1-\boldsymbol{w}^{-1}\omega_{i_0}$ and $\lambda_2+\boldsymbol{w}^{-1}\omega_{i_0}$ are dominant, which implies that $\big(\lambda_1-\boldsymbol{w}^{-1}\omega_{i_0},\lambda_2+\boldsymbol{w}^{-1}\omega_{i_0}\big)\in P^+(\lambda,2)$. For $j\in I$, write

$$\boldsymbol{w}h_j=\sum_{i=1}^n r_ih_i,$$

and note that either $r_i\ge 0$ for all $i\in I$ or $r_i\le 0$ for all $i\in I$. If $r_{i_0}\le 0$, then obviously $(\lambda_1-\boldsymbol{w}^{-1}\omega_{i_0})(h_j)\ge 0$. If $r_i\ge 0$ for all $i\in I$, then we have

$$(\lambda_1-\lambda_2)(h_j)=\boldsymbol{w}(\lambda_1-\lambda_2)(\boldsymbol{w}h_j)\ge r_{i_0}\boldsymbol{w}(\lambda_1-\lambda_2)(h_{i_0})\ge r_{i_0},$$

where the first inequality follows from the assumption that $\boldsymbol{w}(\lambda_1-\lambda_2)\in P^+$, and the second inequality follows from (5-4). Hence $\lambda_1(h_j)\ge\lambda_2(h_j)+r_{i_0}\ge r_{i_0}$, and hence $(\lambda_1-\boldsymbol{w}^{-1}\omega_{i_0})(h_j)\ge 0$, since $\boldsymbol{w}^{-1}\omega_{i_0}(h_j)=r_{i_0}$. Thus we have proved that $\lambda_1-\boldsymbol{w}^{-1}\omega_{i_0}\in P^+$. To prove that $\lambda_2+\boldsymbol{w}^{-1}\omega_{i_0}\in P^+$, we note that if $r_{i_0}\ge 0$, there is nothing to prove. If $r_i\le 0$ for all $i\in I$, then we have

$$(\lambda_1-\lambda_2)(h_j)=\boldsymbol{w}(\lambda_1-\lambda_2)(\boldsymbol{w}h_j)\le r_{i_0}\boldsymbol{w}(\lambda_1-\lambda_2)(h_{i_0})\le r_{i_0},$$

where the first inequality follows from the assumption that $\boldsymbol{w}(\lambda_1-\lambda_2)\in P^+$, and the second inequality follows from (5-4). Hence $\lambda_2(h_j)\ge\lambda_1(h_j)-r_{i_0}\ge -r_{i_0}$, and so $(\lambda_2+\boldsymbol{w}^{-1}\omega_{i_0})(h_j)=\lambda_2(h_j)+r_{i_0}\ge 0$, proving that $\lambda_2+\boldsymbol{w}^{-1}\omega_i\in P^+$.

By the proposition in 5.1, we see that $\boldsymbol{w}(\lambda_1-\mu_1)$ and $\boldsymbol{w}(\mu_1-\lambda_2)$ are in P^+. Hence (5-2) gives

$$\boldsymbol{w}(\lambda_1-\mu_1)(h_{i_0})>0,\quad \boldsymbol{w}(\mu_1-\lambda_2)(h_{i_0})>0,\quad\text{and hence}\quad \boldsymbol{w}(\lambda_1-\lambda_2)(h_{i_0})>0,$$

which in turn gives

$$\boldsymbol{w}(\lambda_1-\mu_1)-\omega_{i_0},\quad \boldsymbol{w}(\mu_1-\lambda_2)-\omega_{i_0},\quad \boldsymbol{w}(\lambda_1-\lambda_2)-\omega_{i_0}\in P^+. \tag{5-5}$$

To prove
$$\boldsymbol{\lambda} \preceq \left(\lambda_1 - \boldsymbol{w}^{-1}\omega_{i_0}, \lambda_2 + \boldsymbol{w}^{-1}\omega_{i_0}\right) \preceq \boldsymbol{\mu},$$
we must show that for all $\alpha \in R^+$,
$$\boldsymbol{w}^{-1}\omega_{i_0}(h_\alpha)\left(\lambda_1 - \boldsymbol{w}^{-1}\omega_{i_0} - \lambda_2\right)(h_\alpha) \geq 0,$$
$$\left(\lambda_1 - \boldsymbol{w}^{-1}\omega_{i_0} - \mu_1\right)(h_\alpha)\left(\mu_1 - \lambda_2 - \boldsymbol{w}^{-1}\omega_{i_0}\right)(h_\alpha) \geq 0,$$
or equivalently that
$$\omega_{i_0}(h_\alpha)\left(\boldsymbol{w}(\lambda_1 - \lambda_2) - \omega_{i_0}\right)(h_\alpha) \geq 0,$$
$$\left(\boldsymbol{w}(\lambda_1 - \mu_1) - \omega_{i_0}\right)(h_\alpha)\left(\boldsymbol{w}(\mu_1 - \lambda_2) - \omega_{i_0}\right)(h_\alpha) \geq 0.$$
But this is now immediate from (5-5).

In order to prove (5-3), it remains to show $\boldsymbol{\lambda} \prec \left(\lambda_1 - \boldsymbol{w}^{-1}\omega_{i_0}, \lambda_2 + \boldsymbol{w}^{-1}\omega_{i_0}\right)$. For that, notice that $\lambda_1 - \boldsymbol{w}^{-1}\omega_{i_0} \notin \{\lambda_1, \lambda_2\}$, since then by the lemma in 5.2, we would have that $\boldsymbol{\lambda}$ is a maximal element of $P^+(\lambda, 2)$, and this would contradict the fact that $\boldsymbol{\lambda} \prec \boldsymbol{\mu}$. □

5.5. In this section, we will show that for $k = 2$, equivalence classes in $P^+(\lambda, 2)$ are the S_2-orbits, generalizing the results of Section 3.2.

Lemma. *Let $\mathfrak{g}$ be arbitrary and let $\boldsymbol{\lambda}, \boldsymbol{\mu} \in P^+(\lambda, 2)$ for some $\lambda \in P^+$. Then $\boldsymbol{\lambda} \sim \boldsymbol{\mu}$ if and only if $\boldsymbol{\mu}$ and $\boldsymbol{\lambda}$ are in the same S_2-orbit.*

Proof. Suppose that $\boldsymbol{\lambda} = (\lambda_1, \lambda_2)$ and $\boldsymbol{\mu} = (\mu_1, \mu_2)$ and set $\nu = \lambda_1 - \lambda_2$ and $\nu' = \mu_1 - \mu_2$. If $\boldsymbol{\lambda} \sim \boldsymbol{\mu}$ then we see from (5-1) that for all $\alpha \in R$, we have $\nu(h_\alpha) = \pm\nu'(h_\alpha)$, where the sign depends on α. It suffices to show that we can choose the sign consistently. Suppose for a contradiction that this is not so; then there exist a connected subset I_0 of I and $i_1, i_2 \in I_0$ such that
$$\begin{aligned} \nu(h_{i_1}) &= \nu'(h_{i_1}) \neq 0, \\ \nu(h_{i_2}) &= -\nu'(h_{i_2}) \neq 0, \\ \nu(h_j) &= \nu'(h_j) = 0, \qquad j \in I_0 \setminus \{i_1, i_2\}. \end{aligned}$$
Set $\beta = \sum_{i \in I_0} \alpha_i$; we can easily check that β is a (positive) root, that is, $\beta \in R^+$. Then
$$\nu(h_\beta) = \nu(h_{i_1}) + \nu(h_{i_2}) = \nu'(h_{i_1}) - \nu'(h_{i_2}) \neq \pm\left(\nu'(h_{i_1}) + \nu'(h_{i_2})\right).$$
Since $\beta \in R^+$, we get the required contradiction. □

6. Proof of Theorem 1(iii)

In this section, we assume that $\mathfrak{g}$ is of type A_2 and prove Theorem 1(iii). We begin by showing that we can restrict our attention to certain elements $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$ of $P^+(\lambda, 2)$.

6.1. Since the poset $P^+(\lambda, 2)$ is finite, it suffices to prove part (iii) of Theorem 1 for $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$, where $\boldsymbol{\mu}$ is a cover of $\boldsymbol{\lambda}$, that is, $\boldsymbol{\lambda} \prec \boldsymbol{\mu}$ and there does not exist $\boldsymbol{\nu} \in P^+(\lambda, 2)$ with $\boldsymbol{\lambda} \prec \boldsymbol{\nu} \prec \boldsymbol{\mu}$. We first show that in fact it suffices to prove Theorem 1(iii) for certain special $\boldsymbol{\lambda}$ and also that for these $\boldsymbol{\lambda}$ we can restrict our attention to certain special covers.

We shall use freely the following two facts. The first is well known.

$$V(\lambda) \otimes V(\mu) \cong_{\mathfrak{g}} V(\mu) \otimes V(\lambda).$$

The second fact is that the partial order on $P^+(\lambda, k)$ is compatible with duals (see (1-1) and (2-2)) and that for all $\lambda, \mu, \nu \in P^+$, we have

$$\dim \operatorname{Hom}_{\mathfrak{g}}\bigl(V(\nu), V(\lambda) \otimes V(\mu)\bigr) = \dim \operatorname{Hom}_{\mathfrak{g}}\bigl(V(-\boldsymbol{w}_0\nu), V(-\boldsymbol{w}_0\lambda) \otimes V(-\boldsymbol{w}_0\mu)\bigr).$$

This allows us to switch freely between proving Theorem 1(iii) either for $\boldsymbol{\lambda} \prec \boldsymbol{\mu}$ or for $-\boldsymbol{w}_0\boldsymbol{\lambda} \prec -\boldsymbol{w}_0\boldsymbol{\mu}$. Recall that $-\boldsymbol{w}_0\omega_1 = \omega_2$.

Proposition. *Let $\lambda \in P^+$ and $\boldsymbol{\lambda} = (\lambda_1, \lambda_2) \in P^+(\lambda, 2)$ and assume that $\boldsymbol{\mu} = (\mu_1, \mu_2)$ covers $\boldsymbol{\lambda}$. It suffices to prove Theorem 1(iii) is true when $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$ satisfy the following conditions for some $\boldsymbol{w} \in \{\mathrm{id}, \boldsymbol{s}_1, \boldsymbol{s}_2\}$:*

$$\boldsymbol{w}(\lambda_1 - \lambda_2) \in P^+, \quad \boldsymbol{w}(\lambda_1 - \lambda_2)(h_1) > 0, \tag{6-1}$$

and either

$$\begin{cases} \boldsymbol{\mu} = (\lambda_1 - \boldsymbol{w}\omega_1,\ \lambda_2 + \boldsymbol{w}\omega_1) \quad \textit{or} \\ \boldsymbol{\mu} = \bigl(\lambda_1 - \boldsymbol{w}(\lambda_1 - \lambda_2)(h_1)\boldsymbol{w}\omega_1,\ \lambda_2 + \boldsymbol{w}(\lambda_1 - \lambda_2)(h_1)\boldsymbol{w}\omega_1\bigr). \end{cases} \tag{6-2}$$

Proof. We first prove that we can assume that $\boldsymbol{\lambda}$ satisfies the conditions in (6-1). Suppose that $\boldsymbol{\lambda} = (\lambda_1, \lambda_2) \in P^+(\lambda, 2)$ is such that $\lambda_1 - \lambda_2 \in P^+$ but $\lambda_1(h_1) = \lambda_2(h_1)$. Since $\boldsymbol{\lambda}$ is not the maximal element in $P^+(\lambda, 2)$, it follows from the lemma in 5.2 that $\lambda_1 \neq \lambda_2$, and hence we must have $\lambda_1(h_2) > \lambda_2(h_2)$. We have $-\boldsymbol{w}_0\boldsymbol{\lambda} \prec -\boldsymbol{w}_0\boldsymbol{\mu}$, and hence $-\boldsymbol{w}_0(\lambda_1 - \lambda_2)(h_1) > 0$. If $\boldsymbol{s}_2(\lambda_1 - \lambda_2) \in P^+$ or $\boldsymbol{s}_1(\lambda_1 - \lambda_2) \in P^+$, a similar argument shows that either $\boldsymbol{\lambda}$ or $-\boldsymbol{w}_0\boldsymbol{\lambda}$ satisfies the conditions in (6-1). Suppose now that $\boldsymbol{w}(\lambda_1 - \lambda_2) \in P^+$ but $\boldsymbol{w} \notin \{\mathrm{id}, \boldsymbol{s}_1, \boldsymbol{s}_2\}$. Then $\boldsymbol{w}\boldsymbol{w}_0 \in \{\mathrm{id}, \boldsymbol{s}_1, \boldsymbol{s}_2\}$, and hence we can work with the pair $(-\boldsymbol{w}_0\lambda_2, -\boldsymbol{w}_0\lambda_1)$.

We now prove that we can also assume that $\boldsymbol{\mu}$ satisfies the conditions in (6-2).

Case 1. Suppose that there exists $i \in I = \{1, 2\}$ such that

$$\boldsymbol{w}(\lambda_1 - \mu_1)(h_i)\boldsymbol{w}(\mu_1 - \lambda_2)(h_i) > 0,$$

where $\boldsymbol{w} \in \{\mathrm{id}, \boldsymbol{s}_1, \boldsymbol{s}_2\}$. We see from the proposition in 5.1 that $\boldsymbol{w}(\lambda_1 - \mu_1)$ and $\boldsymbol{w}(\mu_1 - \lambda_2) \in P^+$. Thus we have $\boldsymbol{w}(\lambda_1 - \mu_1)(h_i) > 0$ and $\boldsymbol{w}(\mu_1 - \lambda_2)(h_i) > 0$. In particular,

$$\boldsymbol{w}(\lambda_1 - \lambda_2)(h_i) = \boldsymbol{w}(\lambda_1 - \mu_1)(h_i) + \boldsymbol{w}(\mu_1 - \lambda_2)(h_i) > 0. \tag{6-3}$$

Subcase 1.1. If $i = 1$, then it follows from the proposition in 5.4 that

$$\boldsymbol{\lambda} \prec \big(\lambda_1 - \boldsymbol{w}^{-1}\omega_1, \lambda_2 + \boldsymbol{w}^{-1}\omega_1\big) = \big(\lambda_1 - \boldsymbol{w}\omega_1, \lambda_2 + \boldsymbol{w}\omega_1\big) \preceq \boldsymbol{\mu}.$$

Since $\boldsymbol{\mu}$ covers $\boldsymbol{\lambda}$, it follows that $\boldsymbol{\mu} = \big(\lambda_1 - \boldsymbol{w}\omega_1, \lambda_2 + \boldsymbol{w}\omega_1\big)$, as required.

Subcase 1.2. If $i = 2$, then it follows from the proposition in 5.4 that

$$\boldsymbol{\lambda} \prec \big(\lambda_1 - \boldsymbol{w}^{-1}\omega_2,\ \lambda_2 + \boldsymbol{w}^{-1}\omega_2\big) = \big(\lambda_1 - \boldsymbol{w}\omega_2,\ \lambda_2 + \boldsymbol{w}\omega_2\big) \preceq \boldsymbol{\mu}.$$

By the "duality", we get

$$-\boldsymbol{w}_0\boldsymbol{\lambda} \prec \big(-\boldsymbol{w}_0\lambda_1 - (-\boldsymbol{w}_0\boldsymbol{w}\omega_2), -\boldsymbol{w}_0\lambda_2 + (-\boldsymbol{w}_0\boldsymbol{w}\omega_2)\big) \preceq -\boldsymbol{w}_0\boldsymbol{\mu}.$$

Since $-\boldsymbol{w}_0\boldsymbol{\mu}$ covers $-\boldsymbol{w}_0\boldsymbol{\lambda}$, we get

$$-\boldsymbol{w}_0\boldsymbol{\mu} = \big(-\boldsymbol{w}_0\lambda_1 - (-\boldsymbol{w}_0\boldsymbol{w}\omega_2), -\boldsymbol{w}_0\lambda_2 + (-\boldsymbol{w}_0\boldsymbol{w}\omega_2)\big).$$

We set $\widetilde{\boldsymbol{w}} = \boldsymbol{w}_0\boldsymbol{w}\boldsymbol{w}_0$ and note that we have

$$\widetilde{\boldsymbol{w}} := \begin{cases} \mathrm{id} & \text{if } \boldsymbol{w} = \mathrm{id}, \\ \boldsymbol{s}_2 & \text{if } \boldsymbol{w} = \boldsymbol{s}_1, \\ \boldsymbol{s}_1 & \text{if } \boldsymbol{w} = \boldsymbol{s}_2. \end{cases}$$

We also have

$$\begin{aligned} \widetilde{\boldsymbol{w}}\big((-\boldsymbol{w}_0\lambda_1) - (-\boldsymbol{w}_0\lambda_2)\big) &= -\boldsymbol{w}_0\boldsymbol{w}(\lambda_1 - \lambda_2) \in P^+, \\ \widetilde{\boldsymbol{w}}\big((-\boldsymbol{w}_0\lambda_1) - (-\boldsymbol{w}_0\lambda_2)\big)(h_1) &= -\boldsymbol{w}_0\boldsymbol{w}(\lambda_1 - \lambda_2)(h_1) \\ &= \boldsymbol{w}(\lambda_1 - \lambda_2)(h_2) > 0 \quad \text{by (6-3)}. \end{aligned}$$

Hence, $-\boldsymbol{w}_0\boldsymbol{\lambda}$ and $-\boldsymbol{w}_0\boldsymbol{\mu}$ satisfy the conditions (with $\boldsymbol{w}$ replaced by $\widetilde{\boldsymbol{w}}$). Hence, if Theorem 1(iii) is established for this pair, then it follows for the pair $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$ as discussed earlier.

Case 2. Suppose that

$$\boldsymbol{w}(\lambda_1 - \mu_1)(h_i)\boldsymbol{w}(\mu_1 - \lambda_2)(h_i) \le 0 \quad \text{for all } i \in I = \{1, 2\},$$

where $\boldsymbol{w} \in \{\mathrm{id}, \boldsymbol{s}_1, \boldsymbol{s}_2\}$. We see from the proposition in 5.1 that $\boldsymbol{w}(\lambda_1 - \mu_1) \in P^+$ and $\boldsymbol{w}(\mu_1 - \lambda_2) \in P^+$. Thus,

$$\boldsymbol{w}(\lambda_1 - \mu_1)(h_i)\boldsymbol{w}(\mu_1 - \lambda_2)(h_i) = 0 \quad \text{for all } i \in I = \{1, 2\},$$

which implies that $\boldsymbol{w}\mu_1(h_i) = \boldsymbol{w}\lambda_1(h_i)$ or $\boldsymbol{w}\mu_1(h_i) = \boldsymbol{w}\lambda_2(h_i)$ for each $i = 1, 2$. Remark that $\boldsymbol{\lambda}$ is not the maximal element, since $\boldsymbol{\lambda} \prec \boldsymbol{\mu}$. Therefore it follows that the only possibilities are

$$\boldsymbol{w}\mu_1 = (\boldsymbol{w}\lambda_2)(h_1)\omega_1 + (\boldsymbol{w}\lambda_1)(h_2)\omega_2 \quad \text{or} \quad \boldsymbol{w}\mu_1 = (\boldsymbol{w}\lambda_1)(h_1)\omega_1 + (\boldsymbol{w}\lambda_2)(h_2)\omega_2.$$

In turn this implies that

$$\begin{aligned}\boldsymbol{\mu} \sim \big((\boldsymbol{w}\lambda_2)(h_1)\boldsymbol{w}^{-1}\omega_1+(\boldsymbol{w}\lambda_1)(h_2)\boldsymbol{w}^{-1}\omega_2,\,(\boldsymbol{w}\lambda_1)(h_1)\boldsymbol{w}^{-1}\omega_1+(\boldsymbol{w}\lambda_2)(h_2)\boldsymbol{w}^{-1}\omega_2\big)\\ = \big(\lambda_1-\boldsymbol{w}(\lambda_1-\lambda_2)(h_1)\boldsymbol{w}^{-1}\omega_1,\,\lambda_2+\boldsymbol{w}(\lambda_1-\lambda_2)(h_1)\boldsymbol{w}^{-1}\omega_1\big)\\ = \big(\lambda_1-\boldsymbol{w}(\lambda_1-\lambda_2)(h_1)\boldsymbol{w}\omega_1,\,\lambda_2+\boldsymbol{w}(\lambda_1-\lambda_2)(h_1)\boldsymbol{w}\omega_1\big),\end{aligned}$$

as required; here we use the fact that

$$\begin{cases}\lambda_1=(\boldsymbol{w}\lambda_1)(h_1)\boldsymbol{w}^{-1}\omega_1+(\boldsymbol{w}\lambda_1)(h_2)\boldsymbol{w}^{-1}\omega_2,\\ \lambda_2=(\boldsymbol{w}\lambda_2)(h_1)\boldsymbol{w}^{-1}\omega_1+(\boldsymbol{w}\lambda_2)(h_2)\boldsymbol{w}^{-1}\omega_2,\end{cases}$$

and then the fact that $\boldsymbol{w}^{-1}=\boldsymbol{w}$. □

6.2. We now recall from [Kashiwara and Nakashima 1994; Nakashima 1993] a tableaux description of tensor product multiplicities. Given $\lambda\in P^+$, let $\mathbb{T}(\lambda)\subset\mathbb{Z}_+^5$ be the subset consisting of tuples $(s_{1,1},s_{1,2},s_{1,3},s_{2,2},s_{2,3})$ satisfying the conditions

$$s_{1,1}+s_{1,2}+s_{1,3}=\lambda(h_1)+\lambda(h_2),\qquad s_{2,2}+s_{2,3}=\lambda(h_2),\tag{6-4}$$

$$s_{1,1}\ge s_{2,2},\qquad s_{1,1}+s_{1,2}\ge s_{2,2}+s_{2,3}.\tag{6-5}$$

Then, it is proved in [Kashiwara and Nakashima 1994] that

$$\dim V(\lambda)=\#\mathbb{T}(\lambda).$$

(This is just the number of semistandard tableaux with entries from $\{1,2,3\}$ of shape λ, where $s_{i,j}$ corresponds to the number of j in the i-th row). Moreover, if $\nu\in P$ and we set

$$\mathbb{T}(\lambda)^\nu=\big\{(s_{i,j})\in\mathbb{T}(\lambda):s_{1,1}-s_{1,2}-s_{2,2}=\nu(h_1),\,s_{1,2}+s_{2,2}-s_{1,3}-s_{2,3}=\nu(h_2)\big\},$$

then

$$\dim V(\lambda)_\nu=\#\mathbb{T}(\lambda)^\nu.$$

In particular, if $(s_{i,j}),(t_{i,j})\in\mathbb{T}(\lambda)^\nu$, then they satisfy

$$s_{1,1}=t_{1,1},\quad s_{1,2}+s_{2,2}=t_{1,2}+t_{2,2},\quad s_{1,3}+s_{2,3}=t_{1,3}+t_{2,3}.\tag{6-6}$$

Suppose now that $\mu,\nu\in P^+$; then [Nakashima 1993]

$$\dim\operatorname{Hom}_{\mathfrak{g}}\big(V(\nu),V(\mu)\otimes V(\lambda)\big)=\#\mathbb{T}(\lambda)^\nu_\mu,\tag{6-7}$$

where $\mathbb{T}(\lambda)^\nu_\mu$ is the subset of $\mathbb{T}(\lambda)^\nu$ consisting of $(s_{1,1},s_{1,2},s_{1,3},s_{2,2},s_{2,3})\in\mathbb{T}(\lambda)$ satisfying the following additional constraints:

$$s_{1,2}\le\mu(h_1),\quad s_{1,3}\le\mu(h_2),\quad s_{2,3}+s_{1,3}\le\mu(h_2)+s_{1,2},\tag{6-8}$$

$$\nu(h_1)+\nu(h_2)=\mu(h_1)+\mu(h_2)+s_{1,1}-s_{1,3}-s_{2,3},\tag{6-9}$$

$$\nu(h_2)=\mu(h_2)+s_{1,2}+s_{2,2}-s_{1,3}-s_{2,3}.\tag{6-10}$$

As a consequence, we see that to prove Theorem 1(iii), we must prove that if $\boldsymbol{\lambda}, \boldsymbol{\mu} \in P^+(\lambda, 2)$, then

$$\boldsymbol{\lambda} \preceq \boldsymbol{\mu} \implies \#\mathbb{T}(\lambda_2)^{\nu}_{\lambda_1} \le \#\mathbb{T}(\mu_2)^{\nu}_{\mu_1} \quad \text{for each } \nu \in P^+. \tag{6-11}$$

This is done in the rest of the section.

6.3. Keep the notation in the proposition in 6.1. In this subsection, we prove that Theorem 1(iii) is true if $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$ satisfy the conditions (6-1) and (6-2) with $\boldsymbol{w} = \mathrm{id}$ or $\boldsymbol{w} = \boldsymbol{s}_2$. By (6-11), it suffices to find an injective map from

$$\mathbb{T}(\lambda_2)^{\nu}_{\lambda_1} \hookrightarrow \mathbb{T}(\lambda_2 + a\boldsymbol{w}\omega_1)^{\nu}_{\lambda_1 - a\boldsymbol{w}\omega_1} = \mathbb{T}(\lambda_2 + a\omega_1)^{\nu}_{\lambda_1 - a\omega_1} \tag{6-12}$$

for each $\nu \in P^+$, where a equals either 1 or $\boldsymbol{w}(\lambda_1 - \lambda_2)(h_1)$; note that

$$\boldsymbol{w}(\lambda_1 - \lambda_2)(h_1) > 0$$

by the second equality of (6-1). This is obtained as a corollary of the following proposition.

Proposition. *Keep the notation above. For each $\nu \in P^+$, there exists $0 \le \ell \le a$ such that for all $(s_{i,j}) \in \mathbb{T}(\lambda_2)^{\nu}_{\lambda_1}$, we have*

$$a - \ell \le s_{1,2} \le \lambda_1(h_1) - \ell, \quad s_{1,3} \le \lambda_1(h_2) - (a - \ell), \quad s_{2,3} \ge a - \ell.$$

Proof. First, let us show that

$$\lambda_1(h_1) + \lambda_1(h_2) - a \ge \lambda_2(h_1) + \lambda_2(h_2), \quad \lambda_1(h_1) - \lambda_2(h_1) \ge a. \tag{6-13}$$

Indeed, since $\boldsymbol{w}(\lambda_1 - \lambda_2)(h_1) \ge a$ by the definition of a, we have

$$\begin{cases} (\lambda_1 - \lambda_2)(h_1) \ge a & \text{if } \boldsymbol{w} = \mathrm{id}, \\ (\lambda_1 - \lambda_2)(h_1 + h_2) \ge a & \text{if } \boldsymbol{w} = \boldsymbol{s}_2, \end{cases}$$

which implies the second (resp. first) inequality of (6-13) if $\boldsymbol{w} = \mathrm{id}$ (resp. $\boldsymbol{w} = \boldsymbol{s}_2$). Also, since $\boldsymbol{w}(\lambda_1 - \lambda_2) \in P^+$, we see that

$$\boldsymbol{w}(\lambda_1 - \lambda_2)(h_1 + h_2) \ge \boldsymbol{w}(\lambda_1 - \lambda_2)(h_1) \ge a.$$

Thus we get

$$\begin{cases} (\lambda_1 - \lambda_2)(h_1 + h_2) \ge a & \text{if } \boldsymbol{w} = \mathrm{id}, \\ (\lambda_1 - \lambda_2)(h_1) \ge a & \text{if } \boldsymbol{w} = \boldsymbol{s}_2, \end{cases}$$

which implies the first (resp. second) inequality of (6-13) if $\boldsymbol{w} = \mathrm{id}$ (resp. $\boldsymbol{w} = \boldsymbol{s}_2$).

By (6-8), we have $t_{1,2} \le \lambda_1(h_1)$ for all $(t_{i,j}) \in \mathbb{T}(\lambda_2)^{\nu}_{\lambda_1}$. Thus we can choose $0 \le \ell \le a$ maximal such that for all $(t_{i,j}) \in \mathbb{T}(\lambda_2)^{\nu}_{\lambda_1}$,

$$t_{1,2} \le \lambda_1(h_1) - \ell.$$

In particular, we can and do fix an element $(s_{i,j}) \in \mathbb{T}(\lambda_2)^{\nu}_{\lambda_1}$ with $s_{1,2} = \lambda_1(h_1) - \ell$.

Suppose that there exists $(t_{i,j}) \in \mathbb{T}(\lambda_2)^{\nu}_{\lambda_1}$, with $t_{1,3} > \lambda_1(h_2) + \ell - a$. Then (6-6) gives

$$t_{2,2} + t_{1,2} = s_{2,2} + s_{1,2} \geq s_{1,2} = \lambda_1(h_1) - \ell.$$

This implies that

$$\begin{aligned}
\lambda_2(h_1) + \lambda_2(h_2) &= t_{1,1} + t_{1,2} + t_{1,3} && \text{by the first equality of (6-4)} \\
&\geq t_{2,2} + t_{1,2} + t_{1,3} && \text{by the first inequality of (6-5)} \\
&\geq \lambda_1(h_1) - \ell + t_{1,3} \\
&> \lambda_1(h_1) - \ell + \lambda_1(h_2) + \ell - a \\
&= \lambda_1(h_1) + \lambda_1(h_2) - a.
\end{aligned}$$

This contradicts the inequality $\lambda_2(h_1) + \lambda_2(h_2) \leq \lambda_1(h_1) + \lambda_1(h_2) - a$ obtained in (6-13).

Suppose now that there exists $(t_{i,j}) \in \mathbb{T}(\lambda_2)^{\nu}_{\lambda_1}$ with $t_{1,2} < a - \ell$. Then we have

$$\begin{aligned}
\lambda_2(h_2) &= t_{2,2} + t_{2,3} && \text{by the second equality of (6-4)} \\
&\leq t_{1,1} + t_{1,2} && \text{by the second inequality of (6-5)} \\
&< t_{1,1} + a - \ell = s_{1,1} + a - \ell && \text{by the first equality of (6-6)} \\
&\leq s_{1,1} + s_{1,3} + a - \ell.
\end{aligned}$$

On the other hand, we have

$$\begin{aligned}
s_{1,1} + s_{1,3} + a - \ell &= \lambda_2(h_1) + \lambda_2(h_2) - s_{1,2} + a - \ell \quad \text{by the first equality of (6-4)} \\
&= \lambda_2(h_1) + \lambda_2(h_2) - (\lambda_1(h_1) - \ell) + a - \ell \\
&= \lambda_2(h_1) + \lambda_2(h_2) - \lambda_1(h_1) + a. \qquad (6\text{-}14)
\end{aligned}$$

Combining the two gives

$$\lambda_2(h_2) < \lambda_2(h_1) + \lambda_2(h_2) - \lambda_1(h_1) + a \quad \text{and so } \lambda_1(h_1) - \lambda_2(h_1) < a,$$

which contradicts the second inequality of (6-13).

Finally suppose that there exists $(t_{i,j}) \in \mathbb{T}(\lambda_2)^{\nu}_{\lambda_1}$ with $t_{2,3} < a - \ell$. Then we have

$$\lambda_2(h_2) = t_{2,2} + t_{2,3} \leq t_{1,1} + t_{2,3} < t_{1,1} + a - \ell = s_{1,1} + a - \ell \leq s_{1,1} + s_{1,3} + a - \ell.$$

Since $s_{1,1} + s_{1,3} + a - \ell = \lambda_2(h_1) + \lambda_2(h_2) - \lambda_1(h_1) + a$ by (6-14), we get

$$\lambda_2(h_2) < \lambda_2(h_1) + \lambda_2(h_2) - \lambda_1(h_1) + a,$$

which again contradicts the second inequality of (6-13). □

The following corollary is now trivially checked using Section 6.2. Thus we have proved that Theorem 1(iii) is true if $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$ satisfy the conditions (6-1) and (6-2) with $\boldsymbol{w} = \mathrm{id}$ or $\boldsymbol{w} = s_2$ (see (6-12)).

Corollary. *Keep the notation and setting in the proposition above. Let $\nu \in P^+$, and let ℓ be as in the proposition above. Then the assignment $(s_{i,j}) \mapsto (s'_{i,j})$,*

$$s'_{1,1} = s_{1,1} + a, \qquad s'_{1,2} = s_{1,2} - (a-\ell), \qquad s'_{1,3} = s_{1,3} + (a-\ell),$$
$$s'_{2,2} = s_{2,2} + (a-\ell), \qquad s'_{2,3} = s_{2,3} - (a-\ell),$$

defines an injective map $\mathbb{T}(\lambda_2)^{\nu}_{\lambda_1} \hookrightarrow \mathbb{T}(\lambda_2 + a\omega_1)^{\nu}_{\lambda_1 - a\omega_1}$.

6.4. Again, keep the notation in the proposition in 6.1. In this subsection, we prove that Theorem 1(iii) is true if $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$ satisfy the conditions (6-1) and (6-2) with $\boldsymbol{w} = \boldsymbol{s}_1$. By (6-11), it suffices to find an injective map from

$$\mathbb{T}(\lambda_2)^{\nu}_{\lambda_1} \hookrightarrow \mathbb{T}(\lambda_2 + a\boldsymbol{s}_1\omega_1)^{\nu}_{\lambda_1 - a\boldsymbol{s}_1\omega_1} = \mathbb{T}\big(\lambda_2 + a(\omega_2 - \omega_1)\big)^{\nu}_{\lambda_1 - a(\omega_2 - \omega_1)} \tag{6-15}$$

for each $\nu \in P^+$, where a equals either 1 or $\boldsymbol{s}_1(\lambda_1 - \lambda_2)(h_1)$; note that

$$\boldsymbol{s}_1(\lambda_1 - \lambda_2)(h_1) > 0$$

by the second equality of (6-1). This is obtained as a corollary of the following proposition.

Proposition. *For each $\nu \in P^+$, there exists $\ell \geq 0$ such that for all $(s_{i,j}) \in \mathbb{T}(\lambda_2)^{\nu}_{\lambda_1}$,*

$$s_{1,1} \geq s_{2,2} + \ell, \qquad s_{1,3} \geq a - \ell.$$

Proof. Suppose that there exists $(t_{i,j}) \in \mathbb{T}(\lambda_2)^{\nu}_{\lambda_1}$ such that either $t_{1,3} = \lambda_1(h_2)$ or $t_{1,3} + t_{2,3} = \lambda_1(h_2) + t_{1,2}$. Then $\ell = 0$ satisfies the condition of the proposition. Indeed, let $(s_{i,j}) \in \mathbb{T}(\lambda_2)^{\nu}_{\lambda_1}$. Then $s_{1,1} \geq s_{2,2} + 0$ is true by the first inequality of (6-5). Also we see by the third equality of (6-6) that

$$s_{1,3} + s_{2,3} = t_{1,3} + t_{2,3} \geq \lambda_1(h_2).$$

Since $s_{2,3} \leq \lambda_2(h_2)$ by (6-5), and $\lambda_1(h_2) - \lambda_2(h_2) + \lambda_1(h_1) - \lambda_2(h_1) \geq 0$ by the fact that $\boldsymbol{s}_1(\lambda_1 - \lambda_2)(h_2) \geq 0$ (recall that $\boldsymbol{s}_1(\lambda_1 - \lambda_2)(h_2) \in P^+$), we get

$$s_{1,3} \geq \lambda_1(h_2) - s_{2,3} \geq \lambda_1(h_2) - \lambda_2(h_2) \geq \lambda_2(h_1) - \lambda_1(h_1) \geq a = a + 0.$$

Consider now the case when for all $(t_{i,j}) \in \mathbb{T}(\lambda_2)^{\nu}_{\lambda_1}$, both of $t_{1,3} < \lambda_1(h_2)$ and $t_{1,3} + t_{2,3} < \lambda_1(h_2) + t_{1,2}$ hold. Since $t_{1,1} \geq t_{2,2}$ by (6-4), we can choose $\ell \geq 0$ minimal with the property that $t_{1,1} \geq t_{2,2} + \ell$ for all $(t_{i,j}) \in \mathbb{T}(\lambda_2)^{\nu}_{\lambda_1}$. If $\ell \geq a$, then the statement of the proposition is trivially true. Assume now that $\ell < a$, and suppose that there exists $(t_{i,j})$ with $t_{1,3} < a - \ell$. Fix $(s_{i,j}) \in \mathbb{T}(\lambda_2)^{\nu}_{\lambda_1}$ such that $s_{1,1} = s_{2,2} + \ell$. Since both of $(s_{i,j})$ and $(t_{i,j})$ are elements of $\mathbb{T}(\lambda_2)^{\nu}$, we have, by (6-4) and (6-6),

$$t_{1,2} + (a-\ell) > t_{1,2} + t_{1,3} = \lambda_2(h_1) + \lambda_2(h_2) - t_{11} = \lambda_2(h_1) + \lambda_2(h_2) - s_{11} = s_{1,2} + s_{1,3}.$$

Hence we get

$$\begin{aligned}\lambda_1(h_1) &\geq t_{1,2} \quad \text{by the first inequality of (6-8)}\\ &> s_{1,2}+s_{1,3}-(a-\ell)\\ &= \big(\lambda_2(h_1)+\lambda_2(h_2)-s_{1,1}\big)+\ell-a \quad \text{by the first equality of (6-4)}\\ &= \lambda_2(h_1)+\lambda_2(h_2)-s_{2,2}-a\\ &\geq \lambda_2(h_1)+\lambda_2(h_2)-\lambda_2(h_2)-a \quad \text{by the second equality of (6-4)}\\ &= \lambda_2(h_1)-a.\end{aligned}$$

So, $\lambda_1(h_1) > \lambda_2(h_1)-a$, which gives $a > \lambda_2(h_1)-\lambda_1(h_1)$, which is a contradiction. Hence $t_{1,3} \geq a-\ell$ for all $(t_{i,j}) \in \mathbb{T}(\lambda_2)^{\nu}_{\lambda_1}$, and the proof is complete. □

The following corollary is now trivially checked using Section 6.2. Thus we have proved that Theorem 1(iii) is true if $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$ satisfy the conditions (6-1) and (6-2) with $\boldsymbol{w} = \boldsymbol{s}_1$ (see (6-15)).

Corollary. *Keep the notation and setting in the proposition above. Let $\nu \in P^+$, and let ℓ be as in the proposition above. Then the assignment $(s_{i,j}) \mapsto (s'_{i,j})$,*

$$s'_{1,1} = s_{1,1}, \qquad s'_{1,2} = s_{1,2}+(a-\ell), \qquad s'_{1,3} = s_{1,3}-(a-\ell),$$
$$s'_{2,2} = s_{2,2}+\ell, \qquad s'_{2,3} = s_{2,3}+(a-\ell),$$

defines an injective map $\mathbb{T}(\lambda_2)^{\nu}_{\lambda_1} \hookrightarrow \mathbb{T}\big(\lambda_2+a(\omega_2-\omega_1)\big)^{\nu}_{\lambda_1-a(\omega_2-\omega_1)}$.

Acknowledgements

The authors thank the Hausdorff Institute for Mathematics for the invitation to participate in the trimester program "On the Interaction of Representation Theory with Geometry and Combinatorics", where this collaboration was initiated. The authors would also thank Anne Schilling for helpful discussions.

References

[Bergeron et al. 2006] F. Bergeron, R. Biagioli, and M. H. Rosas, "Inequalities between Littlewood–Richardson coefficients", *J. Combin. Theory Ser. A* **113**:4 (2006), 567–590. MR 2007f:05175 Zbl 1090.05070

[Bourbaki 2002] N. Bourbaki, *Lie groups and Lie algebras: Chapters 4–6*, Springer, Berlin, 2002. MR 2003a:17001 Zbl 0983.17001

[Dobrovolska and Pylyavskyy 2007] G. Dobrovolska and P. Pylyavskyy, "On products of $\mathfrak{sl}_n$ characters and support containment", *J. Algebra* **316**:2 (2007), 706–714. MR 2008j:17011 Zbl 1130.17004

[Fomin et al. 2005] S. Fomin, W. Fulton, C.-K. Li, and Y.-T. Poon, "Eigenvalues, singular values, and Littlewood–Richardson coefficients", *Amer. J. Math.* **127**:1 (2005), 101–127. MR 2006e:05189 Zbl 1072.15010

[Fran and McNamara 2004] c. B. Fran and P. McNamara, "Some positive differences of products of Schur functions", 2004. arXiv math.CO/0412289

[Kashiwara and Nakashima 1994] M. Kashiwara and T. Nakashima, "Crystal graphs for representations of the q-analogue of classical Lie algebras", *J. Algebra* **165**:2 (1994), 295–345. MR 95c:17025 Zbl 0808.17005

[Lam et al. 2007] T. Lam, A. Postnikov, and P. Pylyavskyy, "Schur positivity and Schur log-concavity", *Amer. J. Math.* **129**:6 (2007), 1611–1622. MR 2009d:05255 Zbl 1131.05096

[Lascoux et al. 1997] A. Lascoux, B. Leclerc, and J.-Y. Thibon, "Ribbon tableaux, Hall–Littlewood functions, quantum affine algebras, and unipotent varieties", *J. Math. Phys.* **38**:2 (1997), 1041–1068. MR 98c:05167 Zbl 0869.05068

[Littelmann 1994] P. Littelmann, "A Littlewood–Richardson rule for symmetrizable Kac–Moody algebras", *Invent. Math.* **116**:1-3 (1994), 329–346. MR 95f:17023 Zbl 0805.17019

[Littelmann 1995] P. Littelmann, "Paths and root operators in representation theory", *Ann. of Math.* (2) **142**:3 (1995), 499–525. MR 96m:17011 Zbl 0858.17023

[Macdonald 1995] I. G. Macdonald, *Symmetric functions and Hall polynomials*, 2nd ed., Oxford University Press, New York, 1995. MR 96h:05207 Zbl 0824.05059

[McNamara 2008] P. R. W. McNamara, "Necessary conditions for Schur-positivity", *J. Algebraic Combin.* **28**:4 (2008), 495–507. MR 2010a:05192 Zbl 1160.05057

[McNamara and van Willigenburg 2009] P. R. W. McNamara and S. van Willigenburg, "Positivity results on ribbon Schur function differences", *European J. Combin.* **30**:5 (2009), 1352–1369. MR 2010i:05352 Zbl 1207.05221

[Nakashima 1993] T. Nakashima, "Crystal base and a generalization of the Littlewood–Richardson rule for the classical Lie algebras", *Comm. Math. Phys.* **154**:2 (1993), 215–243. MR 94f:17015 Zbl 0795.17016

[Okounkov 1997] A. Okounkov, "Log-concavity of multiplicities with application to characters of U(∞)", *Adv. Math.* **127**:2 (1997), 258–282. MR 99a:22028 Zbl 0910.22011

[Purbhoo and van Willigenburg 2008] K. Purbhoo and S. van Willigenburg, "On tensor products of polynomial representations", *Canad. Math. Bull.* **51**:4 (2008), 584–592. MR 2009g:20102 Zbl 1192.05174

Communicated by Georgia Benkart
Received 2013-04-12 Accepted 2013-08-15

vyjayanthi.chari@ucr.edu *Department of Mathematics, University of California, Riverside, CA 92521, United States*

gfourier@math.uni-koeln.de *Mathematisches Institut, Universität zu Köln, Germany*

sagaki@math.tsukuba.ac.jp *Department of Mathematics, University of Tsukuba, Japan*

ALGEBRA AND NUMBER THEORY 8:4 (2014)
dx.doi.org/10.2140/ant.2014.8.963

Parameterizing tropical curves I: Curves of genus zero and one

David E. Speyer

In tropical geometry, given a curve in a toric variety, one defines a corresponding graph embedded in Euclidean space. We study the problem of reversing this process for curves of genus zero and one. Our methods focus on describing curves by parameterizations, not by their defining equations; we give parameterizations by rational functions in the genus-zero case and by nonarchimedean elliptic functions in the genus-one case. For genus-zero curves, those graphs which can be lifted can be characterized in a completely combinatorial manner. For genus-one curves, we show that certain conditions identified by Mikhalkin are sufficient and we also identify a new necessary condition.

In the past ten years, a group of mathematicians, led by Grigory Mikhalkin, have pioneered a new method for studying curves in toric varieties. According to this perspective, one considers curves defined over a field with a nonarchimedean valuation. Using this valuation and an embedding of a curve C into an (algebraic) torus, one constructs a graph embedded in a real vector space. This graph is known as the tropicalization of the curve. From the tropicalization of C, one tries to read off information about the degree and genus of the original curve C, and its intersections

MSC2010: 14T05.
Keywords: tropical geometry, curves, nonarchimedean, Tate curve.

with other subvarieties of the torus. In this introduction, we will write C for a curve embedded in a torus $T \cong (\mathbb{K}^*)^n$ and we will write $\Gamma \subset \mathbb{R}^n$ for the tropicalization of C.

In order to use these tropical methods, we need to know which graphs are tropicalizations of curves. We will refer to a graph which actually is the tropicalization of a curve as a tropical curve. There are certain basic combinatorial conditions which hold for any tropical curve. The first, the *zero-tension condition*, is a description of the possible local structures of a tropical curve around a given vertex (see the beginning of Section 3). We can assign to C a multiset of lattice vectors, which we will call the degree of C, from which we can determine the homology class represented by the closure of C when this closure is taken in a suitable toric compactification of T. The second combinatorial condition is that the directions of the unbounded rays of Γ are given by the degree of C (Section 1). Thirdly, we can show that, modulo some technical conditions, the genus of C is greater than or equal to the first Betti number of Γ (see Theorem 3.1). We will define a *zero-tension curve of genus g and degree δ* to be a graph which has first Betti number g and obeys the obvious conditions to be the tropicalization of a degree-δ curve.

We attack the reverse problem: given a zero-tension curve of genus g and degree δ, when does it come from an actual curve of genus g and degree δ? The main contribution of this paper is to show that methods of nonarchimedean analysis can be used to construct algebraic curves with a given tropicalization. In this paper, we will consider this question for genus-zero and genus-one curves. In the sequel, we will describe the corresponding results for higher-genus curves, where we will need to use Mumford's uniformization results. A second achievement of this paper is to describe a condition — that of being *well spaced* — which permits us to conclude that some "obstructed" curves of genus one can nonetheless be lifted.

I want to state clearly that there is a major difficulty in directly using these results for enumerative purposes involving curves of positive genus. If C is a curve of genus g, than the tropicalization of C is a zero-tension curve with first Betti number less than or equal to g. Therefore, if we want to count genus-g curves obeying some conditions, we should look at all zero-tension curves of genus less than or equal to g, and determine which of them lift to actual genus-g curves obeying the condition (and in how many ways the lifting can be done). However, we have almost no results restricting the capability to lift a tropical curve whose first Betti number is strictly less than g to an actual curve of genus g. When studying curves in toric surfaces, one can use basic dimension-counting arguments to show that there are no such contributions, but this cannot be done for curves in higher-dimensional toric varieties. I expect, therefore, that the primary use of these results will not be to prove exact combinatorial formulas, but rather to provide existence results or lower bounds.

The idea of studying curves via tropical varieties was proposed by Kontsevich and pioneered by Mikhalkin [2005; 2006]. Mikhalkin has proven our main theorems, in any genus, in the case of curves in toric surfaces. A purely algebraic proof was given by Shustin and Tyomkin [2006]. Since Mikhalkin's work, there has been a great deal of research extending his results to more sophisticated enumerative problems concerning curves in toric surfaces. There has been far less work on curves in higher-dimensional toric varieties. The most important result in higher dimensions is that of Nishinou and Siebert [2006], who use log geometry to analyze the case of genus-zero curves and recover essentially all of our results in that case. Finally, we should note that H. Markwig and her collaborators, especially Gathmann, have done major work building the tropical analogue of the moduli spaces of curves and of stable maps and studying it from a combinatorial perspective; see [Gathmann et al. 2009] and the works cited therein. Among their results is reestablishing the validity of the tropical enumeration of curves in $\mathbb{P}^2$ by showing it matches the Caporaso–Harris formula. The moduli space of tropical genus-zero curves was previously described by Mikhalkin [2007].

Newer work. Since this paper was first prepared, several additional relevant papers have appeared. Of particular relevance are the papers of Baker, Payne and Rabinoff [Baker et al. 2012], Helm and Katz [2012], Katz [2012], and Nishinou [2010]. The first is an exhaustive discussion of parametrization of nonarchimedean curves using the language of Berkovich's analytic spaces. In terms of results, this paper goes beyond [Baker et al. 2012] in that we prove that our combinatorially necessary conditions are sufficient to realize tropical curves. In terms of exposition, I hope that the use of the Bruhat–Tits tree rather than Berkovich spaces removes one level of technical requirement.

Helm and Katz relate the lengths of the cycles in the tropical curve to the monodromy action on the cohomology of the general fiber, generalizing the relationship shown in this paper between the length of the cycle in genus one and the valuation of the j-invariant. Katz defines several obstructions to tropical lifting which generalize the well-spacedness condition from this paper.

Nishinou provides an alternate proof that ordinary tropical curves are realizable (in all genuses), using log structures, and provides additional analysis of the superabundant case.

1. Curves in toric varieties

In this section, we will describe how to assign a degree to a curve given with a map to an (algebraic) torus. Throughout this paper, we will write N for the lattice of one-parameter subgroups of the torus and M for the character lattice. We will call the dimension of the torus n. We write $\mathbb{T}$ for the torus, or $\mathbb{T}(\mathbb{K}, N)$ when we want to specify the ground field $\mathbb{K}$ and the lattice N.

Let Σ be a complete rational fan in $\mathbb{Q} \otimes N$ and let $\mathrm{X}(\Sigma)$ be the associated toric variety over an algebraically closed field $\mathbb{K}$. (See [Fulton 1993] for background on toric varieties.) The open torus in $\mathrm{X}(\Sigma)$ is $\mathrm{Hom}(N, \mathbb{K}^*)$. For each ray (one-dimensional cone) of Σ, there is a unique minimal element of N on this ray; if we identify N with $\mathbb{Z}^n$, then the element in question is the unique point of the ray whose coordinates are integers with no common factor. Let $\rho_1, \ldots, \rho_p$ be the set of minimal vectors of the rays of Σ. The following is a special case of Theorem 3.1 of [Fulton and Sturmfels 1997].

Proposition 1.1. *With the notation above, the Chow group A^{n-1} is given by*

$$A^{n-1}(\mathrm{X}(\Sigma)) \cong \left\{ (d_1, d_2, \ldots, d_p) \in \mathbb{Z}^p : \sum_{i=1}^{p} d_i \rho_i = 0 \right\}.$$

This is a subgroup of $H^{2n-2}(\mathrm{X}(\Sigma), \mathbb{Z})$, and equals $H^{2n-2}(\mathrm{X}(\Sigma), \mathbb{Z})$ if $\mathrm{X}(\Sigma)$ is smooth.

Let $\overline{C}$ be a smooth, complete algebraic curve and let $\phi : \overline{C} \to \mathrm{X}(\Sigma)$ be a map from $\overline{C}$ into $\mathrm{X}(\Sigma)$. Let C denote $\phi^{-1}(\mathbb{T}) \subset \overline{C}$, the part of $\overline{C}$ which is mapped to the big torus. Let us say that $(\phi, \overline{C})$ is *torically transverse* if C is nonempty and $\phi(\overline{C})$ is disjoint from the toric strata of codimension two and higher. (This is a specialization of the definition of torically transverse in [Nishinou and Siebert 2006].)

For each ray $\mathbb{Q}_{\geq 0}\rho_i$ of Σ, let Y_i be the codimension-one stratum of $\mathrm{X}(\Sigma)$ associated to ρ_i. Let d_i be the length of $\phi^*(\mathbb{O}_{Y_i})$, in other words, the number of points in $\phi^{-1}(Y_i)$ counted with multiplicity. Then $(d_1, \ldots, d_N)$ satisfies[1] $\sum d_i \rho_i = 0$ and hence corresponds to a class in $A^{n-1}(\mathrm{X}(\Sigma))$. Capping with the fundamental class gives the class in $A_1(\mathrm{X}(\Sigma))$, and hence in $H_2(\mathrm{X}(\Sigma))$, corresponding to C. Thus, if we want to study torically transverse curves representing a particular class in H_2, we may begin by finding the possible preimages of this class in A^{n-1} and studying curves of that degree.

Continue to assume that $(\phi, \overline{C})$ is torically transverse. Let $x \in \overline{C} \setminus C$. We now describe how to determine which ray of Σ corresponds to x, and with what multiplicity, solely by examining the map $C \to \mathbb{T}$. Namely, M is the lattice of characters of the torus, so each element λ of M can be restricted to a function χ^λ on C. Let σ_x be the map which sends λ to the order of vanishing of χ^λ at x; the function σ_x is in N. Write σ_x as $d_x \rho_x$, where d_x is a positive integer and ρ_x is minimal. Then ρ_x is the ray of Σ corresponding to x, and d_x is the multiplicity.

[1] In two paragraphs, we will see an alternate description of the d_i that makes this clear.

We now make a definition: let C be a smooth algebraic curve and let $\phi : C \to \mathbb{T}$ be an algebraic map. Let $\overline{C}$ be the smooth complete curve compactifying C; we impose the condition that ϕ cannot be extended to any point of $\overline{C} \setminus C$. Let x be any point of $\overline{C} \setminus C$. Define σ_x, ρ_x and d_x as before. Let $\rho_1, \ldots, \rho_N$ be the set of distinct values of ρ_x as x ranges over $\overline{C} \setminus C$. For $1 \le i \le N$, let $d_i = \sum_{\rho_x = \rho_i} d_x$ and set $\sigma_i = \sum_{\rho_x=\rho_i} \sigma_x = d_i \rho_i$. We define the set $\{\sigma_1, \ldots, \sigma_N\}$ to be the *degree* of (ϕ, C). Note that this is defined without any choice of toric compactification of $\mathbb{T}$. Note also that we have $\sum \sigma_i = 0$, because any rational function has equally many zeroes and poles on $\overline{C}$.

We then have:

Proposition 1.2. *Let Σ be a complete fan with rays generated by $\rho_1, \ldots, \rho_N$ and let $(d_1, \ldots, d_N)$ be any class in $A^{n-1}(\mathrm{X}(\Sigma))$. There is a bijection between torically transverse curves $(\phi, \overline{C})$ which represent the given class and maps $C \to \mathbb{T}$ which are incapable of being extended to any larger compactification of C and have degree $(d_1\rho_1, \ldots, d_N\rho_N)$; this bijection is given by restriction to the preimage of $\mathbb{T}$ in $\overline{C}$.*

For this reason, we can reformulate questions about constructing torically transverse curves in toric varieties into questions about constructing curves of given degree in tori. Ordinarily, of course, one wishes to consider all curves in some toric variety, not only the torically transverse ones. In many applications, it can be shown by dimensional considerations that all of the curves of interest are torically transverse. Even when this is not true, it is true that, if we specify the cohomology class of a curve in $\mathrm{X}(\Sigma)$, then there are only finitely many possible degrees for curves realizing that cohomology class and not lying in the toric boundary — and those curves which do lie in the toric boundary are in the interiors of smaller toric varieties. For this reason, in this paper we will study problems where we specify the degree of a curve in the torus rather than specifying degrees in a toric compactification.

2. Basic tropical background

In this paper, we will study a great number of polyhedra. All of these will be rational polyhedra, meaning that they are defined by finitely many inequalities of the form $\left\{(x_1, \ldots, x_n) : \sum a_i x_i \le \lambda\right\}$, where $(a_1, \ldots, a_n)$ is an integer vector and λ is a rational number. It will be most convenient to consider these as subsets of $\mathbb{Q}^n$ (for example, in Proposition 2.2). However, we want to be able to use topological language to talk about polyhedral complexes. We therefore adopt the following conventions: a polyhedron is a subset of $\mathbb{Q}^n$, defined by finitely many inequalities as above. When we refer to a point of a polyhedron, we mean a point of $\mathbb{Q}^n$. Nonetheless, when we describe a polyhedral complex using topological terms, such as "connected", "simply connected" and so forth, we will mean the properties of the closure of that complex in $\mathbb{R}^n$. Similar issues will arise concerning metrized graphs. We adopt the conventions that the edges of a metrized graph always have rational lengths and that the points of this graph, considered as a metric space, are the points which have rational distances from all of the vertices. Nevertheless, we will freely speak of graphs as connected, as mapping continuously from one to another, and so forth.

Let $\boldsymbol{O}$ be a complete discrete valuation ring with valuation $v : \boldsymbol{O} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$. We write $\boldsymbol{K}$ for the fraction field of $\boldsymbol{O}$ and κ for the residue field. We always assume that κ is algebraically closed. Let $\mathbb{K}$ be the algebraic closure of $\boldsymbol{K}$, let $v : \mathbb{K} \to \mathbb{Q} \cup \{\infty\}$ be the extension of v to $\mathbb{K}$, let $\mathbb{O}$ be the ring $v^{-1}(\mathbb{Q}_{\geq 0} \cup \{\infty\})$, and let $\mathcal{M}$ and $\boldsymbol{M}$ be the maximal ideals of $\mathbb{O}$ and $\boldsymbol{O}$, respectively. Since κ is algebraically closed, the residue field $\mathbb{O}/\mathcal{M}$ is also equal to κ. For $g \in \mathbb{O}$, write $\mathrm{in}(g)$ for the class of g in κ. We fix a group homomorphism $w \mapsto t^w$ from $\mathbb{Q} \to \mathbb{K}^*$ giving a section of $v : \mathbb{K}^* \to \mathbb{Q}$; this is always possible because v is surjective and $\mathbb{K}^*$ is divisible.[2] We will primarily consider the objects $\mathbb{K}$, $\mathbb{O}$ and $\mathcal{M}$ and only occasionally need to deal with $\boldsymbol{K}$, $\boldsymbol{O}$ and $\boldsymbol{M}$.[3]

We will say that $\mathbb{K}$ is a *power series field* if we are given a section $\iota : \kappa \hookrightarrow \mathbb{O}$ such that $\mathrm{in}(\iota(a)) = a$. If $\mathbb{K}$ is a power series field, we will say that a polynomial $f \in \mathbb{K}[M]$ has *constant coefficients* if its coefficients lie in the image of κ and that a variety $C \subset \mathbb{T}(\mathbb{K}, N)$ has constant coefficients if it is defined by polynomials with constant coefficients. The motivation for this terminology is that we can then think of $\boldsymbol{O}$ as the ring of formal power series in t, writing each element of $\boldsymbol{O}$ canonically as $\sum_i \iota(a_i)t^i$ for some sequence of elements a_i in κ.

Let M be a free abelian group of rank n and let $N = \mathrm{Hom}(M, \mathbb{Z})$. We write $\langle\ ,\ \rangle$ for the pairing $M \times N \to \mathbb{Z}$. For $m \in M$, we will write χ^m for the corresponding element of the group ring $\mathbb{K}[M]$, so that M can be written additively.

Let $f \in \mathbb{K}[M]$ and let $w \in \mathbb{Q} \otimes N$. We can write $f = \sum_{\lambda \in L} f_\lambda \chi^\lambda$, where L is a finite subset of M and each f_λ is a nonzero element of $\mathbb{K}$. Let L_0 be the subset of L on which the function $\lambda \mapsto v(f_\lambda) + \langle \lambda, w \rangle$ achieves its minimum. We define $\mathrm{in}_w(f) = \sum_{\lambda \in L_0} \mathrm{in}(t^{-v(f_\lambda)} f_\lambda) \chi^\lambda$, and we set $\mathrm{in}_w(0) = 0$.

Suppose that $\mathbb{K}$ is a power series field and that $f \in \mathbb{K}[M]$ has constant coefficients, with $f = \sum_{\lambda \in L} \iota(f_\lambda) \chi^\lambda$. Then we can describe $\mathrm{in}_w(f)$ more simply as $\sum_{\lambda \in L_0} f_\lambda \chi^\lambda$; note that we sum over L_0, not over L. This is the definition that is used in Gröbner

[2] It is quite possible to do without this choice, and Sam Payne has advocated doing so. This is doubtless the most morally correct way of proceeding, but it introduces a great deal of notational baggage. In particular, we would be forced to replace tori with principal homogeneous spaces over tori in several places, and would thus no longer have explicit coordinates.

[3] Several earlier tropical works, including some of my own work, attempted to ignore $\boldsymbol{O}$, $\boldsymbol{K}$ and $\boldsymbol{M}$ entirely. The reader should still view these objects as being only technical crutches. However, I have become convinced that it is not worth trying to avoid them completely.

theory, where the field $\mathbb{K}$ is left hidden in the background. Using this alternate definition, we can define $\mathrm{in}_w(f)$ for $f \in \kappa[M]$ and $w \in \mathbb{Q} \otimes N$, even without choosing a field $\mathbb{K}$ to use.

If I is an ideal in $\mathbb{K}[M]$, let $\mathrm{in}_w(I)$ denote the ideal of $\kappa[M]$ generated by $\mathrm{in}_w(f)$ for $f \in I$. If C is the closed subscheme of $\mathbb{T}(\mathbb{K}, N)$ corresponding to I, then we write $\mathrm{in}_w C$ for the closed subscheme of $\mathbb{T}(\kappa, N)$ corresponding to $\mathrm{in}_w I$. The geometric meaning of $\mathrm{in}_w C$ is the following: let t^w denote the element of $\mathbb{T}(\mathbb{K}, N) = \mathrm{Hom}(N, \mathbb{K}^*)$ described by $t^w(\lambda) = t^{\langle \lambda, w \rangle}$ for $\lambda \in N$. Consider the subvariety $t^{-w} \cdot C$ of $\mathbb{T}(\mathbb{K}, N)$, where $\cdot$ denotes the standard action of $\mathbb{T}(\mathbb{K}, N)$ on itself. Let $\overline{t^{-w} \cdot C}$ be the (Zariski) closure of $t^{-w} \cdot C$ in $\mathrm{Spec}\, \mathbb{O}[M]$. Then $\mathrm{in}_w C$ is the fiber of $\overline{t^{-w} C}$ over $\mathrm{Spec}\, \kappa$. Moreover, suppose that $t^w \in \boldsymbol{K}$ and that C is defined over $\boldsymbol{K}$, meaning that there is a subscheme $\boldsymbol{C}$ of $\mathbb{T}(\boldsymbol{K}, N)$ such that $C = \boldsymbol{C} \times_{\boldsymbol{K}} \mathbb{K}$. (Note that we can always achieve these hypotheses by replacing $\boldsymbol{K}$ with a finite extension.) Then we may instead describe $\mathrm{in}_w C$ by taking the Zariski closure of $t^{-w} \boldsymbol{C}$ in $\mathrm{Spec}\, \boldsymbol{O}[M]$.

If I is an ideal of $\kappa[M]$, rather than of $\mathbb{K}[M]$, and w any point of $\mathbb{Q} \otimes N$, then we can define $\mathrm{in}_w I$ to be the ideal in $\kappa[M]$ generated by $\mathrm{in}_w f$ for all $f \in I$, where $\mathrm{in}_w f$ is defined by the alternate definition two paragraphs above. While this is a slight abuse of notation, it should cause no confusion: one meaning of $\mathrm{in}_w I$ is defined for $I \subset \kappa[M]$ and the other for $I \subset \mathbb{K}[M]$ and the meanings are extremely closely related. Specifically, let I be an ideal of $\kappa[\lambda]$, let $w \in \mathbb{Q} \otimes N$ and let $\mathbb{K}'$ be any power series field with associated notation $(\mathbb{K}', v', \mathbb{O}', \mathcal{M}', \kappa')$. Suppose that $w \in \mathbb{Q} \otimes N$ and that $\kappa' = \kappa$. Then $\mathrm{in}_w I = \mathrm{in}_w(\mathbb{K}' \otimes_{\kappa'} I)$.

The following lemma will be of frequent use:

Lemma 2.1. *Let I be an ideal of $\mathbb{K}[M]$. Let w and v be elements of $\mathbb{Q} \otimes N$. Then, for any sufficiently small rational number ϵ, we have $\mathrm{in}_{w+\epsilon v} I = \mathrm{in}_v \mathrm{in}_w I$.*

Proof. This is proved in a less general context as Proposition 1.13 in [Sturmfels 1996]; the proof can be adapted to our setting. □

We now define tropicalization.

Proposition 2.2. *Let C be a closed subscheme of $\mathbb{T}(\mathbb{K}, N)$ and let $I \subset \mathbb{K}[M]$ be the corresponding ideal. Let $w \in \mathbb{Q} \otimes N$. Then the following are equivalent:*

(1) *There is a point $x \in C(\mathbb{K})$ with $v(x) = w$.*

(2) *There is a valuation $\tilde{v} : \mathbb{K}[M]/I \to \mathbb{Q} \cup \{\infty\}$ extending $v : \mathbb{K} \to \mathbb{Q} \cup \{\infty\}$ with the property that $v(\chi^\lambda) = \langle \lambda, w \rangle$ for every λ in N.*

(3) *For every $f \in I$, the polynomial $\mathrm{in}_w f$ is not a monomial.*

(4) *The ideal $\mathrm{in}_w I$ does not contain any monomial.*

(5) *The scheme $\mathrm{in}_w C$ is nonempty.*

Note that in conditions (3) and (4), zero is not considered a monomial.

Proof. The equivalence of (1), (3) and (4) is Theorem 2.1 of [Speyer and Sturmfels 2004]. The proof there that (4) implies (1) is flawed; see [Draisma 2008; Payne 2009b] for corrections and improvements. The equivalence of (4) and (5) is simply the Nullstellensatz — since monomials are units in $\kappa[M]$, the ideal $\operatorname{in}_w I$ contains a monomial if and only if it is all of $\kappa[M]$. The equivalence of (1) and (2) is Theorem 2.2.5 of [Einsiedler et al. 2006]. □

Define the subset of $\mathbb{Q} \otimes N$ where any of the equivalent conditions above holds to be $\operatorname{Trop} C$. Note that condition (3) of the above proposition clearly singles out a closed set. If $\mathbb{K}$ is a power series field and C has constant coefficients, then we can define $\operatorname{Trop} C \subset \mathbb{R}^n$ using the definition of $\operatorname{in}_w f$ which is defined for $f \in \kappa[M]$. There is little risk of confusion in defining $\operatorname{Trop} C$ both for $C \subset \mathbb{T}(\mathbb{K}, N)$ and $C \subset \mathbb{T}(\kappa, N)$. The precise relation is as follows: Let $\mathbb{K}'$ be any power series field, with associated notation $(\mathbb{K}', v', \mathbb{O}', \mathcal{M}', \kappa')$ such that $\kappa' = \kappa$, and let C be a closed subscheme of $\mathbb{T}(\kappa, N)$. Then $\operatorname{Trop} C = \operatorname{Trop}(C \times_{\operatorname{Spec} \kappa'} \operatorname{Spec} \mathbb{K}')$. The next proposition summarizes basic results on the structure of $\operatorname{Trop} C$.

Proposition 2.3. *Let $C \subset \mathbb{T}(\mathbb{K}, N)$. Then* $\operatorname{Trop} C$ *can be given the structure of a polyhedral complex (with finitely many faces). Furthermore, we may do this in such a way that, for σ any face of this polyhedral complex and w and w' two points in the relative interior of σ, we have* $\operatorname{in}_w C = \operatorname{in}_{w'} C$. *If C is d-dimensional then* $\operatorname{Trop} C$ *has dimension d. If C is pure of dimension d then so is* $\operatorname{Trop} C$. *If C is connected then* $\operatorname{Trop} C$ *is connected. If C is connected in codimension one and $\mathbb{K}$ has characteristic zero then* $\operatorname{Trop} C$ *is connected in codimension one.*

If $\mathbb{K}$ is a power series field and C has constant coefficients, then $\operatorname{Trop} C$ *can be given the structure of a polyhedral fan.*

Proof. The existence of the polyhedral structure is proved by Bieri and Groves [1984] using description (2) of $\operatorname{Trop} C$. The claim about initial ideals is proved by Sturmfels [2002] in a slightly more specialized context in the course of proving his Theorem 9.6. The dimensionality claim is also proven in [Bieri and Groves 1984] and is proven by a different method (under more restrictive hypotheses than we adopt here) in [Sturmfels 2002]. Sturmfels proves the pureness claim as well. The connectivity result is proven in [Einsiedler et al. 2006]. The connectivity in codimension one is proven in [Bogart et al. 2007]. That proof is given in a somewhat more restrictive setting than we have adopted here, but there is no difficulty in extending the arguments. □

We will call a polyhedral subdivision of $\operatorname{Trop} C$ a *good* subdivision if, whenever w and w' are two points in the relative interior of the same face σ, we have $\operatorname{in}_w C = \operatorname{in}_{w'} C$. So one of the parts of the above proposition is that $\operatorname{Trop} C$ always has a good subdivision.

Let C be a closed subscheme of $\mathbb{T}(\mathbb{K}, N)$, and suppose that we have equipped $\operatorname{Trop} C$ with a good subdivision, for which σ is a k-dimensional face. Let w lie in the relative interior of σ. Let $H(\sigma) \subset \mathbb{R} \otimes N$ be the vector space spanned by $w_1 - w_2$, for $w_1, w_2 \in \sigma$, and let $\exp(H(\sigma))$ be the corresponding subtorus of $\mathbb{T}(\kappa, N)$.

Proposition 2.4. *With the above notation,* $\operatorname{in}_w(C)$ *is invariant for the action of* $\exp(H(\sigma))$.

Proof. Let $v \in H(\sigma) \cap N$ and let ϵ be a small rational number. Then, from Lemma 2.1, $\operatorname{in}_{w+\epsilon v} C = \operatorname{in}_v \operatorname{in}_w C$ and, by the definition of a good subdivision and $H(\sigma)$, we have $\operatorname{in}_{w+\epsilon v} C = \operatorname{in}_w C$. So $\operatorname{in}_v \operatorname{in}_w C = \operatorname{in}_w C$. The left-hand side is invariant for the one-dimensional subgroup $\exp(\mathbb{R}v)$, so we have shown that $\operatorname{in}_w C$ is invariant under $\exp(\mathbb{R}v)$ for any $v \in H(\sigma) \cap N$. □

In particular, in the above setting, suppose that C is pure of dimension d and $k = d$. Then $\operatorname{in}_w C / \exp(H(\sigma))$ is zero-dimensional. We define $\mu(w) = m(\sigma)$ to be the length of this scheme over κ.

3. Statement of results

We now have enough tropical background to state our main results. We need one combinatorial definition:

Let Γ be a finite graph. We write $\partial\Gamma$ for the set of degree-one vertices of Γ. Let ι be a continuous map $\Gamma \setminus \partial\Gamma \to \mathbb{Q} \otimes N$ such that an edge e of Γ is taken to

(1) either a finite line segment or a point if neither endpoint of e is in $\partial\Gamma$,

(2) an unbounded ray if one endpoint of e is in $\partial\Gamma$, and

(3) a line if both ends of e are in $\partial\Gamma$.

We consider such pairs (ι, Γ) up to reparameterization of the edges of Γ. By our conventions on rationality of polyhedral complexes, $\iota(e)$ has slope in N for every edge e of Γ. If v is a vertex of Γ, and e is an edge of Γ with an endpoint at v, then we write $\rho_v(e)$ for the minimal lattice vector parallel to $\iota(e)$ which points in the direction away from $\iota(v)$. (If v is in $\partial\Gamma$, so that $\iota(e)$ is an unbounded ray or line, then $\iota(v)$ should be thought of as "at infinity", so $\rho_v(e)$ is negative the direction in which $\iota(e)$ goes to infinity.) If e is mapped to a point, define $\rho_v(e)$ to be 0. Suppose that m is a function assigning a positive integer to each edge of Γ. We say that (ι, Γ, m) is a *zero-tension curve* if, for every vertex v in $\Gamma \setminus \partial\Gamma$, we have $\sum_{e \ni v} m(e)\rho_v(e) = 0$. We introduce the notation $\sigma_v(e)$ for $m(e)\rho_v(e)$. If (ι, Γ, m) is any zero-tension curve, we place a metric[4] on $\Gamma \setminus \partial\Gamma$. For any finite edge e, set

[4] This might be only a pseudometric; if ι collapses an edge of Γ, then we have $d(x, y) = 0$ for some x and y which are not equal. This will not be a difficulty.

the length of e to be ℓ, where the endpoints of $\iota(e)$ differ by $\ell\rho_v(e)$. If one or both of the endpoints of e are in $\partial\Gamma$, then we define e to have infinite length.

We define a *partial zero-tension curve* to be a triple (ι, Γ, m) which obeys the above conditions except that if one endpoint of an edge e is in $\partial\Gamma$, we permit that edge to be taken to a finite line segment rather than a ray. Partial zero-tension curves are analogous to analytic maps from a Riemann surface with holes of positive area; zero-tension curves, which will be our main concern, are analogous to algebraic maps from punctured Riemann surfaces.

We define the genus of a zero-tension curve to be the first Betti number of Γ. We define the degree of a zero-tension curve as follows: Let $D \subset N$ be the (finite) set of values assumed by $-\rho_v(e)$ as v ranges through $\partial\Gamma$. For each $\lambda \in D$, let $m_\lambda = \sum m(e)$, where the sum is over e with an endpoint v in $\partial\Gamma$ and $-\rho_v(e) = \lambda$. Then the degree of (ι, Γ, m) is the set $\{m_\lambda \cdot \lambda : \lambda \in D\}$. We now state that, given a curve C, the polyhedral complex $\operatorname{Trop} C$ reflects the degree and genus of the curve.

Theorem 3.1. *Let C be a connected (punctured) curve of genus g over $\mathbb{K}$ equipped with a map $\phi : C \to \mathbb{T}(\mathbb{K}, N)$. Let $\delta \subset N$ be the degree of (C, ϕ). Then there is a connected zero-tension curve (ι, Γ, m) of degree δ and genus at most g with $\iota(\Gamma) =$ $\operatorname{Trop}\phi(C)$. Moreover, choose a good subdivision of* $\operatorname{Trop}\phi(C)$ *and subdivide Γ by the preimage of this subdivision. Then the weights μ on* $\operatorname{Trop} C$ *and m on Γ are related by $\mu(w) = \sum_{\iota(e)\ni w} m(w)$.*

Extend C to a flat family over $\operatorname{Spec}\mathbb{O}$ *whose fiber over* $\operatorname{Spec}\kappa$ *consists of smooth reduced curves glued along nodes.*[5] *If any of the components of the κ-fiber are not rational, then we can take the genus of Γ to be strictly less than g.*

Theorem 3.1 is implicit in the work of many authors, beginning with Grigory Mikhalkin. A complete proof is given in [Nishinou and Siebert 2006]; we explain how to find this theorem in that work: Proposition 6.3 of [Nishinou and Siebert 2006] states that, given C and ϕ, there is degeneration of $\mathbb{T}(\mathbb{K}, N)$ (over Spec $\boldsymbol{O}$) to a union of toric varieties and a degeneration of C (over $\operatorname{Spec}\mathbb{O}$) to a nodal curve so that ϕ extends on the $\operatorname{Spec}\kappa$ fiber to a torically transverse stable map. Write C_0 for the nodal curve and ϕ_0 for the map from C_0. In the course of proving Theorem 8.3, Nishinou and Siebert verify that (C_0, ϕ_0) is an object they call a pre-log curve. In Construction 4.4, they explain how to build a zero-tension curve (ι, Γ, m) from a pre-log curve. The components of C_0 are organized in equivalence classes, where members of the same class are called "indistinguishable". The union of the components in each equivalence class is connected. The vertices of Γ correspond to these classes of C_0, and the edges of Γ to nodes of C_0 connecting components in different classes. Since C_0 is a stable degeneration of a genus-g

[5]For example, extend C to a family of stable curves.

curve, the graph Γ may have first Betti number at most g. This establishes the first paragraph of the theorem.

For the second paragraph, let C'_0 be the κ-fiber of the family described in the second paragraph of the theorem. Let Y be the unique stable limit of $C/\operatorname{Spec}\mathbb{K}$. Then Y is obtained from C'_0 by collapsing some curve of genus zero. So if C'_0 has any nonrational components, so does Y. But Y is also obtained from C_0 by collapsing some genus-zero components, so if C'_0 has nonrational components then so does C_0, and thus Γ must have first Betti number strictly less than g.

We now state the main results of the paper.

Theorem 3.2. *Let (ι, Γ, m) be a zero-tension curve of genus zero and degree δ. Then there is a (punctured) genus-zero curve C over $\mathbb{K}$ and a map $\phi : C \to \mathbb{T}(\mathbb{K}, N)$ such that (C, ϕ) has degree δ and $\iota(\Gamma) = \operatorname{Trop}\phi(C)$. The edge weighting m is related to the multiplicities μ as described in Theorem 3.1.*

Theorem 3.2 was previously proven, by methods of log geometry, in [Nishinou and Siebert 2006].

Theorem 3.3. *Let (ι, Γ, m) be a zero-tension curve of genus one and degree δ. Let $e_1, \dots, e_r$ be the edges of the unique circuit of Γ. Assume that the slopes of $\iota(e_1), \dots, \iota(e_r)$ span $\mathbb{Q} \otimes N$. Then there is a (punctured) genus-one curve C over $\mathbb{K}$ and a map $\phi : C \to \mathbb{T}(\mathbb{K}, N)$ such that (C, ϕ) has degree δ and $\iota(\Gamma) = \operatorname{Trop}\phi(C)$. The edge weighting m is related to the multiplicities μ as described in Theorem 3.1.*

Mikhalkin [2006, Theorem 1] states without proof a result which includes both Theorems 3.2 and 3.3.

The importance of the criterion that the slopes of the edges $\iota(e_1), \dots, \iota(e_r)$ span $\mathbb{Q} \otimes N$ was first pointed out by Mikhalkin. Following Mikhalkin, we say that (ι, Γ, m) is *ordinary* when this condition holds, and *superabundant* when it does not.[6] When dealing with superabundant curves, we need to impose a further criterion, which is original to this paper. Let (ι, Γ, m) be a zero-tension curve of genus one and degree δ. Let $e_1, \dots, u_r$ be the edges of the unique circuit of Γ. Let H be an affine hyperplane in $\mathbb{Q} \otimes N$ containing all of the line segments $\iota(e_i)$, but not containing the entire curve $\iota(\Gamma)$. Let Δ be the connected component of $\Gamma \cap \iota^{-1}(H)$ which contains the circuit of Γ and let $x_1, \dots, x_s$ be the vertices of Δ which are also in the (topological) closure of $\Gamma \setminus \Delta$; we call these the *boundary vertices of* Δ. Let $d_1, \dots, d_s$ be the distances from $x_1, \dots, x_s$ to the nearest point on the circuit of Γ. Then we say that (ι, Γ, m) is *well spaced with respect to H* if the minimum of the numbers $(d_1, \dots, d_s)$ occurs more than once. We say that

[6]The motivation for this terminology is that one can define a space of deformations of (ι, Γ, m). A deformation consists of changing the lengths of the edges of Γ, while keeping the slopes of the images of those edges constant. One can show that ordinary curves have deformation spaces of the "expected dimension", while the deformation space of superabundant curves is larger than expected.

(ι, Γ, m) is *well spaced* if it is well spaced with respect to every H containing the circuit of Γ.

Theorem 3.4. *Assume that κ has characteristic zero. Let (ι, Γ, m) be a zero-tension curve of genus one and degree δ and assume that (ι, Γ, m) is well spaced. Then there is a (punctured) genus-one curve C over $\mathbb{K}$ and a map $\phi : C \to \mathbb{T}(\mathbb{K}, N)$ such that $\iota(\Gamma) = \operatorname{Trop} C$.*

There is a partial converse to this theorem; see Proposition 9.2.

It is possible to prove enumerative versions of all of these results, where we count curves (C, ϕ) with $\operatorname{Trop} \phi(C) = \iota(\Gamma)$ that meet subvarieties of $\mathbb{T}(\mathbb{K}, N)$. We do not do so here. Partially, this is because it would add greatly to the length of the exposition. A more important reason is that, as described in the introduction, we have no results regarding the lifting of zero-tension curves of genus zero to actual curves of genus one and therefore we do not know how to productively apply such enumerative results.

In a sequel to this paper I will establish analogous results for curves of genus greater than one.

4. The Bruhat–Tits tree

We will spend the rest of this paper proving Theorems 3.2, 3.3 and 3.4. One of our main technical tools is the Bruhat–Tits tree. A good reference for our discussion is Chapter 2 of [Morgan and Shalen 1984]. A more sophisticated approach here would be to replace the Bruhat–Tits tree by the analytification of $\mathbb{P}^1(\mathbb{K})$ in the sense of Berkovich. Recently, several authors have begun fully using the Berkovich technology for tropical purposes; the interested reader should begin with [Payne 2009a; Baker et al. 2012]. In this paper, we will restrict ourselves to the more concrete Bruhat–Tits tree.

We denote by $\mathrm{BT}(\mathbb{K})$ the set of $\mathbb{O}$-submodules of $\mathbb{K}^2$ which are isomorphic to $\mathbb{O}^2$, modulo $\mathbb{K}^*$-scaling. We write $\overline{M}$ for the equivalence class of a module M. We equip $\mathrm{BT}(\mathbb{K})$ with the metric where $d(\overline{M}_1, \overline{M}_2)$ is the minimum of the set of ϵ such that there exists an α with $M_1 \supseteq t^{\alpha} M_2 \supseteq t^{\alpha+\epsilon} M_1$; this minimum exists and is independent of the choice of representatives M_1 and M_2. Clearly, $d(\overline{M}_1, \overline{M}_2)$ is always in $\mathbb{Q}$. The metric space $\mathrm{BT}(\mathbb{K})$ is called the Bruhat–Tits tree of $\mathbb{K}$.

If we made the analogous construction working over $\boldsymbol{K}$, we could equip BT with the structure of the vertices of a tree so that distance was the graph-theoretic distance. Instead, $\mathrm{BT}(\mathbb{K})$ is what is called a $\mathbb{Q}$-tree (see [Morgan and Shalen 1984]). We remind our reader of the convention that all metric trees have edges whose lengths are in $\mathbb{Q}$, and the points of such a tree are the points whose distances from the vertices are rational. Being a $\mathbb{Q}$-tree is a more general concept than this; the following proposition lists the "tree-like" properties of $\mathbb{Q}$.

Proposition 4.1. *If $\overline{M}_1$ and $\overline{M}_2 \in \mathrm{BT}(\mathbb{K})$ with $d(\overline{M}_1, \overline{M}_2) = d$, then there is a unique distance-preserving map $\phi : [0, d] \cap \mathbb{Q} \to \mathrm{BT}(\mathbb{K})$ with $\phi(0) = \overline{M}_1$ and $\phi(d) = \overline{M}_2$. Explicitly, if $t^\alpha M_1 \supseteq M_2 \supseteq t^{\alpha+d} M_1$, then $\phi(e) = \overline{t^{\alpha+e} M_1 + M_2}$. We will call the image of ϕ the path from $\overline{M}_1$ to $\overline{M}_2$ and denote it by $[\overline{M}_1, \overline{M}_2]$. If $\overline{M}_1, \dots, \overline{M_n} \subset \mathrm{BT}(\mathbb{K})$, then $\bigcup_{i \neq j} [\overline{M_i}, \overline{M_j}]$ is a metric tree.*

Suppose now that $(x_1 : y_1)$ and $(x_2 : y_2)$ are distinct members of $\mathbb{P}^1(\mathbb{K})$. Then we can similarly define a map $\phi : \mathbb{Q} \to \mathrm{BT}(\mathbb{K})$ by $\phi(e) = \overline{\mathbb{O}(x_1, y_1) + t^e \mathbb{O}(x_2, y_2)}$. We will call the image of this ϕ the *path from* $(x_1 : y_1)$ *to* $(x_2 : y_2)$ and denote it by $[(x_1 : y_1), (x_2 : y_2)]$. (The specific map $\phi : \mathbb{Q} \to \mathrm{BT}(\mathbb{K})$ depends on the choice of representatives (x_1, y_1) and (x_2, y_2), but the image $\phi(\mathbb{Q})$ does not.) Similarly, if $\overline{M} \in \mathrm{BT}(\mathbb{K})$ and $(x : y) \in \mathbb{P}^1(\mathbb{K})$, we can define a semi-infinite path from $(x : y)$ to $\overline{M}$ denoted by $[(x : y), \overline{M}]$. We introduce the notation $\overline{\mathrm{BT}}(\mathbb{K})$ for $\mathrm{BT}(\mathbb{K}) \cup \mathbb{P}^1(\mathbb{K})$.

If Z is a subset of $\overline{\mathrm{BT}}(\mathbb{K})$, we denote by $[Z]$ the subspace $\bigcup_{z,z' \in Z} [z, z']$ of $\overline{\mathrm{BT}}(\mathbb{K})$. For simplicity, assume that $|Z| \geq 3$. If Z is finite, then $[Z]$ is a metric tree with a semi-infinite ray for each member of $Z \cap \mathbb{P}^1(\mathbb{K})$. We will say that this ray has its end at the corresponding member of $Z \cap \mathbb{P}^1(\mathbb{K})$. We will abbreviate $[\{z_1, \dots, z_n\}]$ as $[z_1, \dots, z_n]$.

The case where Z is a four-element subset of $\mathbb{P}^1(\mathbb{K})$ is of particular importance for us. Let $\{w, x, y, z\} \subset \mathbb{P}^1(\mathbb{K}) = \mathbb{K} \cup \{\infty\}$. We define the *cross ratio* $c(w, x : y, z)$ by

$$c(w, x : y, z) = \frac{(w - y)(x - z)}{(w - z)(x - y)}.$$

Note that $c(w, x : y, z) = c(x, w : z, y) = c(y, z : w, x) = c(z, y : x, w)$ and $c(w, x : y, z) = c(w, x : z, y)^{-1}$.

Proposition 4.2. *The metric space $[w, x, y, z]$ is a metric tree with 4 semi-infinite rays and either 1 or 2 internal vertices.*

If $[w, x, y, z]$ has 2 internal vertices, let d be the length of the internal edge and suppose that the rays ending at w and x lie on one side of that edge and the rays through y and z on the other. Then

$$v(c(w, x : y, z)) = 0,$$
$$v(c(w, y : x, z)) = -v(c(w, y : z, x)) = d,$$
$$v(c(w, z : x, y)) = -v(c(w, z : y, x)) = d.$$

The first statement can be strengthened to say that $v(c(w, x : y, z) - 1) = d$. (The valuations of all other permutations of $\{w, x, y, z\}$ can be deduced from these by the symmetries of the cross ratio.)

If $[\{w, x, y, z\}]$ has only 1 internal vertex, then

$$v(c(w, x : y, z) - 1) = v(c(w, x : y, z)) = 0,$$

and the same holds for all permutations of $\{w, x, y, z\}$.

This proposition can be remembered as saying "$v(c(w, x : y, z))$ is the signed length of $[w, x] \cap [y, z]$", where the sign tells us whether the two paths run in the same direction or the opposite direction along their intersection.

Proof. The group $\mathrm{GL}_2(\mathbb{K})$ acts on $\overline{\mathrm{BT}}(\mathbb{K})$ through the action on $\mathbb{K}^2$. It is well known that c is $\mathrm{GL}_2(\mathbb{K})$ invariant, and the definitions of $[x, y]$ and the metric on $\mathrm{BT}(\mathbb{K})$ are clearly $\mathrm{GL}_2(\mathbb{K})$ equivariant. So the whole theorem is invariant under $\mathrm{GL}_2(\mathbb{K})$ and we may use this action to take w, x and y to 0, 1 and ∞.

Our hypothesis in the second paragraph of the proposition is that $[0, 1, \infty, z]$ is a tree with 0 and 1 on one side of a finite edge of length d and z and ∞ on the other. It is easy to check that this is equivalent to requiring that $v(z) = -d < 0$. Then

$$c(0, 1 : \infty, z) = 1 - \frac{1}{z},$$

which does indeed have valuation 0, and $c(0, 1 : \infty, z) - 1 = -1/z$, which does indeed have valuation d. Similarly, $c(0, \infty : 1, z) = 1/z$, which has valuation d, and $c(0, z : 1, \infty) = 1/(1 - z)$, which has valuation d.

In the third paragraph of the proposition, the assumption that the tree has no finite edge implies that $v(z) = v(z - 1) = 0$. The argument then continues as before. □

5. Lemmas on zero-tension curves

We pause to prove two combinatorial lemmas about zero-tension curves.

Lemma 5.1. *Let* (ι, Γ, m) *be a connected partial*[7] *zero-tension curve in* $\mathbb{Q}^n$. *Suppose that* $\iota(\Gamma)$ *is not contained in any hyperplane. Then the set of vectors* $\sigma_v(e)$, *where* v *runs over* $\partial\Gamma$, *spans* $\mathbb{Q}^n$.

Proof. Suppose, for the sake of contradiction, that there is some nonzero $\lambda \in \mathbb{Q}^n$ with $\langle \lambda, \sigma_v(e) \rangle = 0$ for every degree-one vertex v of Γ. Let $h(u)$ be the function $\langle \lambda, \iota(u) \rangle$ on $\Gamma \setminus \partial\Gamma$. As h is constant on every ray of Γ ending at a degree-one vertex, and in particular on all of the unbounded rays of Γ, the function h is bounded on Γ. Let U be the (nonempty) subset of Γ on which h achieves its maximum. Clearly, U is closed.

We now show that U is also open. Clearly, if U contains a point p in the interior of an edge of Γ, then it contains that entire edge and, in particular, U contains an open neighborhood of p. So we just need to show that, if u is a vertex of Γ contained in U, then U contains an open neighborhood of u. If u is a degree-one vertex of Γ, then h is constant in a neighborhood of u by our hypothesis. If u is not a degree-one vertex, then by the zero-tension condition, we have $\sum_{e \ni u} \langle \lambda, \sigma_u(e) \rangle = 0$.

[7] Recall that the adjective partial means we permit edges which end at a vertex of $\partial\Gamma$ to be taken to a finite line segment rather than to an infinite ray.

Since we have assumed that h is maximized at u, we have $\langle \lambda, \sigma_u(e) \rangle \le 0$ for every edge e containing u and we conclude that h is constant in a neighborhood of u, as desired.

So U is open, closed and nonempty. As Γ is connected, $U = \Gamma$ and we have that h is constant on Γ. This contradicts our assumption that $\iota(\Gamma)$ is not contained in any hyperplane. □

Morally, this proof is an instance of the "tropical maximum modulus principle". The linear functional defining H is a harmonic function on Γ in the sense of [Baker and Norine 2007; Gathmann and Kerber 2008] and other papers, and we are showing that if it is bounded, then it is constant.

One difficulty with Theorem 3.1 is that it states that a zero-tension curve with $\iota(\Gamma) = \operatorname{Trop} C$ exists, but it doesn't help us choose from among several possible candidates for (ι, Γ, m). We now introduce a concept that will let us guarantee that essentially only one such (ι, Γ, m) exists. We define (ϕ, C) to be *trivalent* if, for some (equivalently any) good subdivision of $\operatorname{Trop} \phi(C)$, we have $m_e = 1$ for every edge e and the degree of v is at most 3 for every vertex v.

Lemma 5.2. *Let (ϕ, C) be a trivalent curve and (ι, Γ, m) a zero-tension curve with $\iota(\Gamma) = \operatorname{Trop} \phi(C)$, such that if e is any edge of (a good subdivision of) $\operatorname{Trop} \phi(C)$, then we have $m_e = \sum_{\iota(f)=e} m_f$. (The sum is over edges f of Γ mapping to e.)*

Than there is a subgraph Γ' of Γ which maps isomorphically onto $\operatorname{Trop} \phi(C)$. Specifically, we take Γ' to be the union of all edges of Γ which are not contracted to points under ι. In particular, if ι contracts no edge, then $\Gamma \cong \operatorname{Trop} C$.

Proof. First, we note that if e is an edge of $\operatorname{Trop} \phi(C)$, then each point in the interior of e can have only one preimage in Γ, by the equation $1 = m_e = \sum_{\iota(f)=e} m_f$. Next, let x be a vertex of $\operatorname{Trop} \phi(C)$ with edges e_1, e_2 and possibly e_3 coming out of x. Let $y \in \Gamma'$ be a preimage vertex of x. Then there must be edges leaving y which map down to each of the e_i, as otherwise the zero-tension condition would be violated. (If all of the edges leaving y map down to a point, then y is not in Γ'.) Then there can be no other vertex z of Γ' which maps to x, as there are no edges of $\operatorname{Trop} \phi(C)$ left for the edges coming from z to map to.

So every vertex of $\operatorname{Trop} \phi(C)$ and the interior of every edge of $\operatorname{Trop} \phi(C)$ has only one preimage in Γ'; that is, the restriction of ι to Γ' is bijective onto its image. Moreover, Γ' is closed in Γ, so the map $\Gamma' \to \operatorname{Trop} \phi(C)$, like the map $\Gamma \to \operatorname{Trop} \phi(C)$, is a closed map. But we know $\Gamma' \to \operatorname{Trop} \phi(C)$ is bijective, so this is also an open map. A continuous open bijective map is a homeomorphism. □

6. Tropical curves of genus zero

The aim of this section is to prove Theorem 3.2. This result appears in [Nishinou and Siebert 2006] and will also appear in a future publication of Mikhalkin. Our method of proof is not only more explicitly constructive than these, but will also preview many of the methods which we will use to deal with higher-genus curves. Let (ι, Γ, m) be a zero-tension curve with Γ a tree. From now until the end of the paper, fix an identification of N with $\mathbb{Z}^n$.

Proposition 6.1. *Let T be a metric tree with finitely many vertices. Then there is a subset Z of $\overline{\mathrm{BT}}(\mathbb{K})$ such that $[Z]$ is isometric to T. If every leaf of T is at the end of an unbounded edge, then we can take $Z \subset \mathbb{P}^1(\mathbb{K})$.*

Proof. Our proof is by induction on the number of finite-length edges of T. If T has $l \geq 3$ leaves and no finite edges, then T is isometric to $[z_1, \ldots, z_l]$ for $\{z_1, \ldots, z_l\}$ any l elements of $\mathbb{K}^*$ with valuation 0 and distinct images in κ^*. If T is an unbounded edge which is infinite in both directions then $T \cong [0, \infty]$; if T is an unbounded ray which is infinite in one direction then $T = [\mathbb{O}^2, \infty]$; if T is a point then $T \cong [\mathbb{O}^2]$. These are all of the cases with no finite edges, so our base case is complete.

Now let e be a finite edge of T of length d joining vertices v_1 and v_2. Remove e from T, separating T into two trees T_1 and T_2. Define trees T_s', where $s = 1, 2$, by adding an unbounded edge to T_s at v_s. By induction, we can find subsets Z_1 and $Z_2 \subset \overline{\mathrm{BT}}(\mathbb{K})$ with $[Z_s]$ isometric to T_s'. Let $z_s \in Z_s$ be the element of Z_s at the end of the new ray added to T_s.

Without loss of generality, we may assume that $z_1 = 0$ and $z_2 = \infty$. Furthermore, we may translate T_1', preserving 0, so that v_1 lies on $[0, \infty]$, and similarly, we may translate T_2', preserving ∞, so that v_2 lies on $[0, \infty]$. By multiplying Z_1 and Z_2 by elements of $\mathbb{K}^*$, we may assume that these points lie distance d apart with v_2 closer to z_1 than v_1 is. Then T is isometric to $\big[(Z_1 \setminus \{z_1\}) \cup (Z_2 \setminus \{z_2\})\big]$.

If all of the leaves of T were at the end of unbounded edges, then this would also be true of T_1' and T_2', and tracing through the proof, we see that $Z \subset \mathbb{P}^1(\mathbb{K})$. $\square$

Recall that we have been given a zero-tension curve (ι, Γ, m) of genus zero and we want to construct an actual genus-zero curve with $\iota(\Gamma)$ as its tropicalization. Let $Z \subset \mathbb{P}^1(\mathbb{K})$ be such that $[Z]$ is isometric to Γ. We define multisets $Z_1^+, \ldots, Z_n^+, Z_1^-, \ldots, Z_n^-$ as follows: All of the elements of $Z_i^{\pm}$ lie in Z. Let $z \in Z$ correspond to the end of an infinite ray e of Γ. Suppose that $\sigma_z(e) = (s_1, \ldots, s_n)$. Then $z \in Z_i^{\pm}$ if and only if $\pm s_i < 0$. In this case, the number of times that z occurs in $Z_i^{\pm}$ is $|s_i|$. Let ϕ_i be a rational function on $\mathbb{P}^1$ with zeroes at the points of Z_i^+ and poles at the points of Z_i^-. (If ∞ is not in Z_i^+ or Z_i^-, we may take $\phi_i(u) = \prod_{z \in Z_i^+}(u - z) / \prod_{z \in Z_i^-}(u - z)$.) Define a rational map $\phi : \mathbb{P}^1(\mathbb{K}) \to \mathbb{K}^n$ by the formula $\phi(u) = (\phi_1(u), \ldots, \phi_n(u))$. Here u is a coordinate on $\mathbb{P}^1(\mathbb{K})$, thought of as $\mathbb{K} \cup \{\infty\}$.

The following theorem states that C and ϕ satisfy the conditions on the curve and the map in Theorem 3.2; the conclusion of Theorem 3.2 follows.

Theorem 6.2. *The curve $\phi(\mathbb{P}^1(\mathbb{K}))$ is a genus-zero curve of degree the degree of* (ι, Γ, m). Trop $\phi(\mathbb{P}^1(\mathbb{K}))$ *is a translation of* $\iota(\Gamma)$. *Thus, by rescaling the* $\phi_i(u)$ *by elements of* $\mathbb{K}^*$, *we can arrange that* Trop $\phi(\mathbb{P}^1(\mathbb{K}))$ *is* $\iota(\Gamma)$.

From now until the end of the proof, we identify $[Z]$ with Γ so that we can write $\iota : [Z] \to \mathbb{Q}^n$.

Proof. The curve $\phi(\mathbb{P}^1(\mathbb{K}))$ clearly has genus zero. It has the same degree as (ι, Γ, m) because, by Proposition 1.2, the degree can be computed simply by looking at the orders of vanishing of the coordinate functions on $(\mathbb{K}^*)^n$ at the points of $\mathbb{P}^1$ where ϕ is not defined. We built ϕ to have exactly the required zeroes and poles. We now move to the interesting point, the claim that Trop $\phi(\mathbb{P}^1(\mathbb{K}))$ is a translation of $\iota(\Gamma)$.

Let $u \in \mathbb{P}^1(\mathbb{K}) \setminus Z$. Then $[Z]$ is a tree and $[Z \cup \{u\}]$ is a tree with one additional end. Let $b(u)$ be the point of $[Z]$ at which that end is attached. (In Figure 1, $[Z]$ is shown in solid lines, the points of Z are represented by z's, the path from u to $b(u)$ is dashed, and $b(u)$ is the solid dot.) We claim that, up to a translation, $v(\phi(u))$ is $\iota(b(u))$. In other words, if u_1 and u_2 are distinct members of $u \in \mathbb{P}^1(\mathbb{K}) \setminus Z$, we must show that for each i between 1 and n we have

$$v(\phi_i(u_1)) - v(\phi_i(u_2)) = \iota(b(u_1))_i - \iota(b(u_2))_i.$$

It is enough to show this in the case where $b(u_1)$ and $b(u_2)$ lie in the same edge e of $[Z]$. Let $\sigma_{u_2}(e) = (s_1, \dots, s_n)$. We will fix one coordinate i to pay attention to, so i will not appear in our notation. Let $Z_i^+ = \{z_1^+, \dots, z_r^+\}$ and $Z_i^- = \{z_1^-, \dots, z_r^-\}$. We may find constants $1 \le s^+, s^- \le n$ and order the $z_j^\pm$ such that $z_j^\pm$ is on the $b(u_1)$ side of e for $1 \le j \le s^\pm$ and on the $b(u_2)$ side of e for $s^\pm + 1 \le j \le r$. Let d be the distance from $b(u_1)$ to $b(u_2)$.

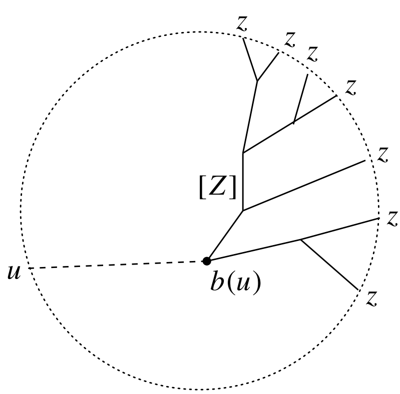


Figure 1. The definition of $b(u)$.

We have

$$
\begin{aligned}
v(\phi_i(u_1)) - v(\phi_i(u_2)) &= v\left(\frac{\phi_i(u_1)}{\phi_i(u_2)}\right) = v\left(\frac{\prod_{j=1}^{r}(u_1 - z_j^+) \,/\, \prod_{j=1}^{r}(u_1 - z_j^-)}{\prod_{j=1}^{r}(u_2 - z_j^+) \,/\, \prod_{j=1}^{r}(u_2 - z_j^-)}\right) \\
&= v\left(\prod_{j=1}^{r} c(u_1, u_2 : z_j^+, z_j^-)\right) \\
&= \sum_{j=1}^{r} v\bigl(c(u_1, u_2 : z_j^+, z_j^-)\bigr) = d(s^+ - s^-).
\end{aligned}
$$

The last equality is by applying Proposition 4.2 to each term.

By the zero-tension condition, $s_i = s^+ - s^-$. So $\iota(b(u_1))_i - \iota(b(u_2))_i$ is also $d(s^+ - s^-)$. □

We pause for two examples.

Example 6.3. Consider the tree in $\mathbb{Q}^3$ with a finite edge running from $(0, 0, 0)$ to $(1, 1, 1)$, infinite edges leaving $(1, 1, 1)$ in directions $(1, 0, 0)$ and $(0, 1, 1)$, and edges departing $(0, 0, 0)$ in directions $(0, -1, 0)$ and $(-1, 0, -1)$. Then $[0, t, 1, t^{-1}]$ is isometric to Γ, with 0, t, 1 and t^{-1} respectively corresponding to the endpoints of the above infinite rays. We have

$$
\begin{aligned}
Z_1^+ &= \{0\}, & Z_2^+ &= \{t\}, & Z_3^+ &= \{t\}, \\
Z_1^- &= \{t^{-1}\}, & Z_2^- &= \{1\}, & Z_3^- &= \{t^{-1}\}.
\end{aligned}
$$

Thus, the map ϕ is given by

$$
u \mapsto \left(\frac{u}{u - t^{-1}}, \frac{u - t}{u - 1}, \frac{u - t}{u - t^{-1}}\right).
$$

The image of this map is a genus-zero curve C with $\operatorname{Trop} C$ equal to the given tree.

Example 6.4. This time we choose a tree with no internal edges but complicated slopes. Consider the tree T in $\mathbb{Q}^3$ with no internal edges and four unbounded rays of slope $(1, 2, 3)$, $(5, -3, 4)$, $(-7, 1, -2)$, $(1, 0, -5)$. Assuming that κ has characteristic 0, the tree $[1, 2, 3, 4] \subset \mathrm{BT}(K)$ is isometric to T. Our multisets $Z_i^{\pm}$ are

$$
\begin{aligned}
Z_1^+ &= \{1, 2, 2, 2, 2, 2, 4\}, & Z_2^+ &= \{1, 1, 3\}, & Z_3^+ &= \{1, 1, 1, 2, 2, 2, 2\}, \\
Z_1^- &= \{3, 3, 3, 3, 3, 3, 3\}, & Z_2^- &= \{2, 2, 2\}, & Z_3^- &= \{3, 3, 4, 4, 4, 4, 4\}.
\end{aligned}
$$

For example, there are 5 occurrences of the number 4 in Z_3^- because ray number 4 of our tree has slope -5 in the x_3 direction.

Our map ϕ is given by

$$u \mapsto \left(\frac{(u-1)(u-2)^5(u-4)}{(u-3)^7}, \frac{(u-1)^2(u-3)}{(u-2)^3}, \frac{(u-1)^3(u-2)^4}{(u-3)^2(u-4)^5}\right).$$

Once again, the image of ϕ is a genus-zero curve whose tropicalization is the given tree.

7. Tropical curves of genus one

Let (Γ, ι, m) be a zero-tension curve where Γ is connected with first Betti number one. This means that Γ has a unique cycle; let $e_1, \dots, e_r$ be the edges of this cycle and let σ_i be the slope $\sigma(e_i)$. Recall that $\sigma(e_i) = m(e_i)\rho(e_i)$, where ρ is the minimal lattice vector along e_i and m is the multiplicity of edge e_i.

Our aim in this section is to prove:

Theorem 3.3. *Let (ι, Γ, m) be a zero-tension curve of genus one and degree δ. Assume that the slopes $\sigma_1, \sigma_2, \dots, \sigma_r$ span $\mathbb{Q} \otimes N$. Then there is a (punctured) genus-one curve C over $\mathbb{K}$ of degree δ and a map $\phi : C \to \mathbb{T}(\mathbb{K}, N)$ such that $\iota(\Gamma) = \operatorname{Trop} \phi(C)$.*

We use Tate's nonarchimedean uniformizations of elliptic curves. A good reference for this subject is Sections 2 and 3 of [Roquette 1970]. Let $q \in \mathbb{K}^*$ with $v(q) > 0$. Tate constructs an elliptic curve E over $\mathbb{K}$ with a bijection $\mathcal{P}$ from $\mathbb{K}^*/q^{\mathbb{Z}}$ to $E(\mathbb{K})$. For u and $z \in \mathbb{K}^*$, define

$$\Theta(u) = \prod_{j=-\infty}^{0} (1 - q^{-j}u) \prod_{j=1}^{\infty} (1 - q^j/u).$$

For any u and q in $\mathbb{K}^*$, there is a finite extension K of $\boldsymbol{K}$ containing u and q and this product is convergent in the nonarchimedean topology on K as long as none of the individual terms are zero. Thus, the product above is well defined for all $u \in \mathbb{K}^* \setminus q^{\mathbb{Z}}$ and it satisfies $\Theta(qu) = (-1/u)\Theta(u)$. (Remember that $\lim_{n\to\infty} q^n = 0$ because $v(q) > 0$.) Thus, if $Z^+ = \{z_1^+, \dots, z_k^+\}$ and $Z^- = \{z_1^-, \dots, z_k^-\}$ are finite multisubsets of K^* with the same cardinality and $\prod_{i=1}^k z_i^+ = \prod_{i=1}^k z_i^-$, then

$$\phi(u; Z_i^+, Z_i^-) := \prod_{i=1}^{k} \frac{\Theta(u/z_i^+)}{\Theta(u/z_i^-)}$$

is a well-defined function on $(\mathbb{K}^*/q^{\mathbb{Z}}) \setminus \left(\bigcup_{j=\infty}^{\infty} q^j \cdot \{z_1^+, \dots, z_k^+, z_1^-, \dots, z_k^-\}\right)$. Consider this product as a function on $E(\mathbb{K})$ with the appropriate points removed. Tate proves that this is a meromorphic function of u with zeroes at the points $\mathcal{P}(z_i^+)$ and poles at $\mathcal{P}(z_i^-)$. Every nonzero meromorphic function on $E(\mathbb{K})$, up to scalar multiples, occurs in this way. (See [Roquette 1970, Section 2, Proposition 1] for the statement that all the nonzero functions in the field which Roquette calls M_K are of this form. See [Roquette 1970, Section 2, Statement IV] for the fact that this field is the meromorphic functions on an elliptic curve over $\mathbb{K}$.)

Remark. By the Jacobi triple product formula, $\Theta(u)$ can be given by the alternate formula $\prod_{i=0}^{\infty}(1-q^i)^{-1} \times \sum_{n=-\infty}^{\infty} q^{\binom{n}{2}}(-u)^n$. But this formula will not be useful to us.

Our goal, given the input data (ι, Γ, m), is to construct a genus-one curve C over $\mathbb{K}$ and a rational map $\phi : C \to (\mathbb{K}^*)^n$ such that $\operatorname{Trop}\phi(C) = \iota(\Gamma)$. The way our construction will proceed is to use (ι, Γ, m) to construct an element $q \in \mathbb{K}^*$, with $v(q) > 0$, and finite multisubsets $Z_1^+, \dots, Z_n^+, Z_1^-, \dots, Z_n^-$, of $\mathbb{P}^1(\mathbb{K})$. We will have $\prod_{z \in Z_i^+} z = \prod_{z \in Z_i^-} z$, which will be the hardest part of the construction to achieve. Thus, we will have a rational map ϕ from the Tate curve $C := \mathbb{K}^*/q^{\mathbb{Z}}$ to $(\mathbb{K}^*)^n$ by $\mathcal{P}(u) \mapsto (\phi(u; Z_1^+, Z_1^-), \dots, \phi(u; Z_n^+, Z_n^-))$. We will have arranged our choices so that $\operatorname{Trop}\phi(C) = \iota(\Gamma)$. We often abbreviate $\phi(u; Z_i^+, Z_i^-)$ to $\phi_i(u)$, when the choice of $Z_i^{\pm}$ is clear.

We begin by discussing the situation for an arbitrary choice of q and $Z_1^{\pm}, \dots, Z_n^{\pm}$. Later, we will specialize our discussion to the particular choices that will derive from the graph Γ. We will use $\gimel(q, Z_\bullet^{\pm})$ to denote the graph we will construct from q and $Z_1^{\pm}, \dots, Z_n^{\pm}$; eventually $\gimel$ will be isomorphic to Γ.[8] We will drop the arguments of $\gimel$ when they should be free from context.

So, let $q \in \mathbb{K}^*$ with $v(q) > 0$ and let $Z_1^+, Z_1^-, \dots, Z_n^+, Z_n^-$ be $2n$ finite nonempty multisubsets of $\mathbb{K}^*$ with $|Z_i^+| = |Z_i^-|$ for $i = 1, 2, \dots, n$. We introduce the notation Z for

$$\bigcup_{i=-\infty}^{\infty} \bigcup_{j=1}^{n} q^i (Z_j^+ \cup Z_j^-).$$

Let[9] $\tilde{\gimel}(q, Z_\bullet^{\pm}) = \bigcup_{z, z' \in Z} [z, z'] \subset \operatorname{BT}(\mathbb{K})$. The metric space $\tilde{\gimel}(q, Z_\bullet^{\pm})$ is invariant under multiplication by $q^{\mathbb{Z}}$; we define $\gimel(q, Z_\bullet^{\pm}) = \tilde{\gimel}(q, Z_\bullet^{\pm})/q^{\mathbb{Z}}$.

Lemma 7.1. *The metric space $\tilde{\gimel}(q, Z_\bullet^{\pm})$ is an infinite tree. The quotient $\tilde{\gimel}(q, Z_\bullet^{\pm})/q^{\mathbb{Z}}$ is a finite graph with first Betti number one, and $\gimel(q, Z_\bullet^{\pm})$ is isometric to a dense subset of U.*

Note that we call a graph "finite" when it has a finite number of vertices and of edges. When the graph is equipped with a metric, as $\tilde{\gimel}$ is, we do *not* take "finite" to imply that all of the edges have finite length.

Proof. First note that for any a and $b \in \mathbb{K}^*$ and any $d \in [0, \infty]$, we either have $d \in [a, q^j b]$ for j sufficiently large or we have $d \in [a, q^{-j} b]$ for j sufficiently large.

[8] The symbol $\gimel$ is the Hebrew letter "gimmel", which makes the same sound as the Greek letter Γ.

[9] We will systematically use the tilde, $\tilde{}$, for objects associated to the universal cover.

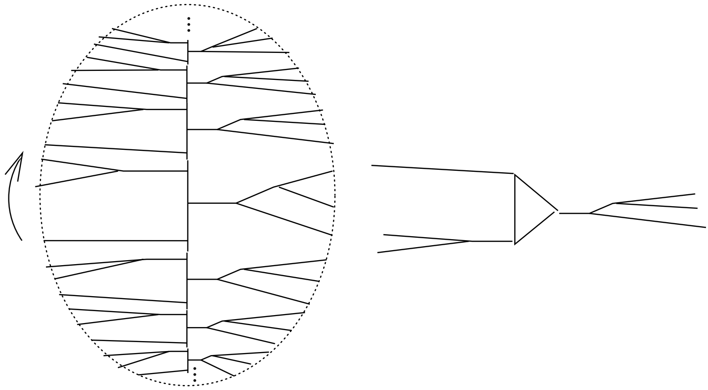


Figure 2. The graphs $\tilde{\gimel}$ and $\gimel$.

The same holds if we take $d \in [a, \infty]$ or $d \in [a, 0]$. So $\tilde{\gimel}$, which by definition is $\bigcup_{z,z' \in Z}[z, z']$, is also $\bigcup_{z,z' \in Z}[0, \infty, z, z']$. Also, note that for any a and $b \in \mathbb{K}^*$, we have $[a, b, 0, \infty] = [a, 0, \infty] \cup [b, 0, \infty]$. (Just check the three possible topologies for the tree $[a, b, 0, \infty]$.) So $\tilde{\gimel} = \bigcup_{z \in Z}[0, z, \infty]$.

For $u \in \mathbb{Q}$, set $T_u = \bigcup_{z \in Z,\ v(z)=u}[0, z, \infty]$, so $\tilde{\gimel} = \bigcup_{u \in \mathbb{Q}} T_u$. If $u \neq u'$ then $T_u \cap T_{u'} = [0, \infty]$. So $\tilde{\gimel}$ is just a central path $[0, \infty]$ with the side stalk $T_u \setminus [0, \infty]$ stuck on for each $u \in v(Z)$. But, for every u, there are only finitely many $u \in Z$ with valuation u, so T_u is just a finite tree. And $v(Z)$ is a union of finitely many copies of $v(q) \cdot \mathbb{Z}$, so in particular $v(Z)$ is a discrete subset of A. So we see that $\tilde{\gimel}$ really is just an infinite tree, consisting of an infinite path with a periodic pattern of finite trees branching off from it.

When we take the quotient of this infinite tree by the periodic shift by $v(q)$ along this path, we get a finite graph. $\square$

In Figure 2, we show $\tilde{\gimel}$ on the left and $\gimel$ on the right for a sample choice of q and Z. The action of q is shown by the boldfaced arrow.

We now define a function s assigning a vector in $\mathbb{Z}^n$ to each edge of $\gimel$; this function will eventually describe the slopes of edges of our tropical curve. Fix an index i between 1 and n and an oriented edge $\tilde{e}$ of $\tilde{\gimel}$. Removing $\tilde{e}$ from $\tilde{\gimel}$ divides $\tilde{\gimel}$ into two components. This gives rise to partitions $Z_i^{\pm} = H_i^{\pm} \sqcup T_i^{\pm}$ of $Z_i^{\pm}$, where $H_i^{\pm}$ consists of those elements of $Z_i^{\pm}$ which are on the "head" side of $\tilde{e}$ and $T_i^{\pm}$ consists of elements of $Z_i^{\pm}$ which are on the "tail" side of $\tilde{e}$. Define

$$\tilde{s}_i(\tilde{e}) = |H_i^+| - |T_i^+| - |H_i^-| + |T_i^-|.$$

Note that each of these multisets is finite, so $\tilde{s}_i(\tilde{e})$ is well defined. Also, note that $\tilde{s}_i(\tilde{e})$ is zero for all but finitely many e. We now define

$$s_i(e) = \sum_{\tilde{e} \text{ lifts } e} \tilde{s}_i(\tilde{e}).$$

Here we are summing over all the edges $\tilde{e}$ of $\tilde{\gimel}$ above the edge e of $\gimel$. Note that all but finitely many terms of this sum are zero. We then define $s(e)$ to be the vector $(s_1(e), \dots, s_n(e))$. Note that $s(e) = s(qe)$, so we may think of s a function on directed edges of $\gimel$, and note that reversing an edge negates s.

Lemma 7.2. *The vectors $s(e)$ obey the zero-tension condition.*

Proof. We will show that the function $\tilde{s}$ on the edges of $\tilde{\gimel}$ obeys the zero-tension condition, so the translates of $\tilde{s}$ will as well, and hence their sum s will. Let v be an internal vertex of $\tilde{\gimel}$ and let $e_1, e_2, \dots, e_p$ be the edges incident to v, which we will direct away from v. Fix an index i between 1 and n; we need to show that $\sum_k \tilde{s}(e_k)_i = 0$. Let T_k be the component of $\tilde{\gimel} \setminus \{v\}$ which contains the interior of e_k. Let D_k be the difference between the cardinalities of $Z_i^+ \cap T_k$ and $Z_i^- \cap T_k$. Since $|Z_i^+| = |Z_i^-|$, we know that $\sum D_k = 0$. We have $\tilde{s}(e_k)_i = D_k - \sum_{m \neq k} D_m$, so $\sum_{k=1}^{p} \tilde{s}(e_k)_i = (p-1)\sum_{k=1}^{p} D_k = 0$. $\square$

We will now consider the effect of adding the following additional condition:

$$\text{for } i = 1, \dots, n, \qquad v\Bigl(\prod_{z \in Z_i^+} z\Bigr) = v\Bigl(\prod_{z \in Z_i^-} z\Bigr). \tag{1}$$

Note that condition (1) is an immediate consequence of the stronger condition

$$\text{for } i = 1, \dots, n, \qquad \prod_{z \in Z_i^+} z = \prod_{z \in Z_i^-} z. \tag{2}$$

Proposition 7.3. *Suppose that condition (1) holds. Let $e_1, e_2, \dots, e_r$ be the edges of the unique cycle of $\gimel$, ordered and oriented cyclically. Let $\ell(e)$ be the length of the edge e of $\tilde{\gimel}$. Then*

$$\sum_{k=1}^{r} \ell(e_k) s(e_k) = 0.$$

Proof. Pick an index i between 1 and n; we will show that $\sum_{k=1}^{r} \ell(e_k) s_i(e_k) = 0$. Recall that we have $|Z_i^+| = |Z_i^-|$. Set $N = |Z_i^+| = |Z_i^-|$ and fix orderings $(z_1^\pm, z_2^\pm, \dots, z_N^\pm)$ of Z_i^+ and Z_i^-. For an oriented edge e of $\tilde{\gimel}$ and an index m between 1 and N, define $\delta_m(e)$ to be 1 if z_m^+ is on the head side of e and z_m^- is on the tail side of e; define $\delta_m(e)$ to be -1 if z_m^+ is on the tail side of e and z_m^- is on the head side of e; define $\delta_m(e)$ to be 0 if z_m^+ and z_m^- are on the same side of e. Then $\tilde{s}_i(e) = \sum_{m=1}^{N} \delta_m(e)$.

Now we have

$$\sum_{k=1}^{r} \ell(e_k) s_i(e_k) = \sum_{k=1}^{r} \ell(e_k) \sum_{j=-\infty}^{\infty} \tilde{s}_i(q^j e_k) = \sum_{e \subset [0,\infty]} \ell(e) \tilde{s}_i(e).$$

Using the expression in the previous paragraph for $\tilde{s}_i(e)$, we see that this equals

$$\sum_{e\subset[0,\infty]} \ell(e) \sum_{m=1}^{N} \delta_m(e) = \sum_{m=1}^{N} \sum_{e\subset[0,\infty]} \ell(e)\delta_m(e),$$

where we may interchange summation because all but finitely many terms are zero. Now the inner sum $\sum_{e\subset[0,\infty]} \ell(e)\delta_m(e)$ is the (signed) sum of the lengths of all edges in $[0,\infty]$ which separate z_m^+ from z_m^-. In other words, the inner sum is the signed length of $[0,\infty] \cap [z_m^+, z_m^-]$. But, by Proposition 4.2, this is simply $v(z_m^+) - v(z_m^-)$. Plugging this into our sum, we see that the quantity we wish to show is zero is $\sum_{m=1}^{N}(v(z_m^+) - v(z_m^-))$. But, by condition (1), we have $v\big(\prod_{z\in Z_i^+} z\big) - v\big(\prod_{z\in Z_i^-} z\big) = 0$, so $\sum_{m=1}^{N}\big(v(z_m^+) - v(z_m^-)\big) = 0$. □

We now build a continuous map $\tilde{f} : \tilde{\daleth} \to \mathbb{Q}^n$. If e is any finite edge of $\tilde{\daleth}$, directed from vertex x to vertex y, then $\tilde{f}(y) = \tilde{f}(x) + \ell(e)s(e)$ and $\tilde{f}(e)$ is the line segment connecting $\tilde{f}(x)$ and $\tilde{f}(y)$. If e is an infinite ray of $\daleth$ then $\tilde{f}(e)$ is an unbounded ray of slope $s(e)$. This map is determined by the $s(e)$ up to translation by an element of $\mathbb{Q}^n$. Using Proposition 7.3, we see that $\tilde{f}$ factors through the quotient graph $\daleth$; we will write the map $\daleth \to \mathbb{Q}^n$ as f. We now come to the fundamental computation that unites our combinatorial constructions with actual geometry:

Proposition 7.4. *Given q and $Z_1^\pm, \dots, Z_n^\pm$ subject to condition (2), define the curve C and the map ϕ as described at the beginning of this section. Define also the graph $\daleth$ and the map f. (Since we have assumed (2), we have (1), so we can define f.) Then* $\operatorname{Trop}\phi(C)$ *is a translation of $f(\daleth)$ and they have the same degree.*

This proof is very similar to the proof of Theorem 6.2. We will make the inconsequential abuse of notation of considering ϕ both as a map from (an open subset of) C and from $\mathbb{K}^* \setminus Z$. Here Z, as above, is $\bigcup_{i=\infty}^{\infty} \bigcup_{j=1}^{n} q^i(Z_j^+ \cup Z_j^-)$.

Proof. Let $u \in \mathbb{K}^* \setminus Z$. Then $[Z \cup \{u\}]$ is a tree, which is the union of $\tilde{\daleth}$ and a path ending at u. Let $b(u) \in \tilde{\daleth}$ be the other end of this path. We claim that, up to a translation, $v(\phi(u))$ is $f(b(u))$. In other words, if u_1 and u_2 are distinct members of $u \in \mathbb{K}^* \setminus Z$, we must show that for each i between 1 and n, we have

$$v(\phi_i(u_1)) - v(\phi_i(u_2)) = f(b(u_1))_i - f(b(u_2))_i.$$

It is enough to show this in the case where $b(u_1)$ and $b(u_2)$ lie in the same edge e of $[Z]$. Let $s(e) = (s_1, \dots, s_n)$. We will fix one coordinate i to pay attention to, so i will not appear in our notation. Let $Z_i^+ = \{z_1^+, \dots, z_N^+\}$ and $Z_i^- = \{z_1^-, \dots, z_N^-\}$. Let d be the distance from $b(u_1)$ to $b(u_2)$.

We have

$$v(\phi_i(u_1)) - v(\phi_i(u_2)) = v\left(\frac{\phi_i(u_1)}{\phi_i(u_2)}\right) = v\left(\frac{\prod_{m=1}^{N} \Theta(u_1/z_m^+)/\Theta(u_1/z_m^-)}{\prod_{m=1}^{N} \Theta(u_2/z_m^+)/\Theta(u_2/z_m^-)}\right)$$
$$= \sum_{m=1}^{N} v\left(\frac{\Theta(u_1/z_m^+)/\Theta(u_1/z_m^-)}{\Theta(u_2/z_m^+)/\Theta(u_2/z_m^-)}\right). \tag{3}$$

Now, by definition,

$$\frac{\Theta(u_1/z_m^+)/\Theta(u_1/z_m^-)}{\Theta(u_2/z_m^+)/\Theta(u_2/z_m^-)} = \prod_{j=-\infty}^{0}\left(\frac{(1-q^{-j}u_1/z_m^+)(1-q^{-j}u_2/z_m^-)}{(1-q^{-j}u_1/z_m^-)(1-q^{-j}u_2/z_m^+)}\right)$$
$$\times \prod_{j=1}^{\infty}\left(\frac{(1-q^{j}z_m^+/u_1)(1-q^{j}z_m^-/u_2)}{(1-q^{j}z_m^-/u_1)(1-q^{j}z_m^+/u_2)}\right)$$
$$= \prod_{j=-\infty}^{\infty} c(q^{-j}u_1, q^{-j}u_2 : z_m^-, z_m^-). \tag{4}$$

Here we may rearrange our product freely because in nonarchimedean analysis all convergent sums and products converge absolutely. So, by Proposition 4.2, we can compute the valuation of (4):

$$v\left(\frac{\Theta(u_1/z_m^+)/\Theta(u_1/z_m^-)}{\Theta(u_2/z_m^+)/\Theta(u_2/z_m^-)}\right) = \sum_{j=-\infty}^{\infty}\bigl(\text{signed length of } [u_1/q^j, u_2/q^j] \cap [z_m^+, z_m^-]\bigr). \tag{5}$$

Now, the sum on m of the signed length of $[u_1/q^j, u_2/q^j] \cap [z_m^+, z_m^-]$ is $d\tilde{s}_i(q^j e)$. So, plugging (5) into (3) and interchanging summation, we obtain

$$v(\phi_i(u_1)) - v(\phi_i(u_2)) = \sum_{j=-\infty}^{\infty} d\tilde{s}_i(q^j e) = ds_i(e) = f(b(u_1))_i - f(b(u_2))_i.$$

This is the desired formula. □

We now know how to build a genus-one curve over $\mathbb{K}$ with a rational map $\phi : C \to (\mathbb{K}^*)^n$ such that $\operatorname{Trop} \phi(C)$ has a given form. In order to prove Theorem 3.3, we need to use (ι, Γ, m) to find q and to find multisubsets $Z_1^{\pm}, \dots, Z_n^{\pm}$ of $\mathbb{K}^*$ such that

(i) for $i = 1, \dots, n$, we have $|Z_i^+| = |Z_i^-|$;

(ii) for $i = 1, \dots, n$, we have $\prod_{z \in Z_i^+} z = \prod_{z \in Z_i^-} z$;

(iii) the graph $\daleth(q, Z_\bullet^{\pm})$ is isometric to Γ; and

(iv) the map f corresponds to ι under the isometry $\daleth(q, Z_\bullet^{\pm}) \cong \Gamma$.

We spend the rest of this section describing the necessary construction. We will first build sets $Y_1^\pm, \dots, Y_n^\pm$ which obey all of these conditions except that, instead of condition (ii), they satisfy the weaker (1) (stated before Proposition 7.3). We will then perturb the $Y_i^\pm$ to give sets $Z_i^\pm$ satisfying this last condition.

Let ℓ be the length of the circuit of Γ. First, we choose[10] q so that $v(q) = \ell$. Let $\tilde{\Gamma}$ be the universal cover of Γ. The graph $\tilde{\Gamma}$ is an infinite tree which has one doubly infinite path with finite trees periodically branching off this path. Choose a point in the interior of an edge e_0 of the circuit of Γ and cut Γ at this point to produce a tree T, so $\tilde{\Gamma}$ is a union of a doubly infinite sequence of copies of T. The tree T has two finite rays and a number of infinite rays. By Proposition 6.1, we can find a subset U of $\overline{\mathrm{BT}}(\mathbb{K})$ such that $T \cong [U]$. There are two elements of $\mathrm{BT}(\mathbb{K})$ in U, which we will call u_0 and u_1; the rest of U is contained in $\mathbb{P}^1(\mathbb{K})$. The distance from u_0 to u_1 is $\ell = v(q)$, so we may (and do) use a transformation in $\mathrm{GL}_2(\mathbb{K})$ to assume that $u_0 = \mathrm{Span}_{\mathbb{O}}((1, 0), (0, 1))$ and $u_1 = \mathrm{Span}_{\mathbb{O}}((q, 0), (0, 1))$. Since u_0 and u_1 are leaves of $[U]$, all the other elements of $U \setminus \{u_0, u_1\}$ must be contained in $v^{-1}((0, \ell)) \subset \mathbb{K}^* \subset \mathbb{P}^1(\mathbb{K})$. We set $Y = \bigcup_{j=-\infty}^{\infty} q^j (U \setminus \{u_0, u_1\})$. Then $[Y] \cong \tilde{\Gamma}$.

We now describe how to choose the multisets $Y_1^\pm, \dots, Y_n^\pm$ as subsets of the set Y. Fix an index i between 1 and n. We first define multisubsets W_i^+ and W_i^- of U. Let v be a leaf of Γ, at the end of the edge e, and let u be the element of U at the end of the corresponding ray of T. Then u will occur $|\sigma_v(e)_i|$ times in $W_i^\pm$, where $\pm$ is the opposite of the sign of $\sigma_v(e)_i$, and will not occur at all in $W_i^\mp$. Note that the assumption that (ι, Γ, m) is zero-tension forces W_i^+ and W_i^- to have the same cardinality. We now modify $W_i^\pm$ slightly to produce $Y_i^\pm$. Let $(s_1, \dots, s_n)$ be the slope of the edge e_0 which we cut to make T. For each i between 1 and n, we take one element of W_i^+ and multiply it by q^{s_i}, leaving the other elements of W_i^+ unchanged. We call the resulting multiset Y_i^+. We take $Y_i^- = W_i^-$. Then $\bigcup_{j=-\infty}^{\infty} q^j \bigcup_{i=1}^{n} (Y_i^+ \cup Y_i^-) = Y$, so we have $\tilde{\daleth}(q, Y_\bullet^\pm) \cong [Y] \cong \tilde{\Gamma}$ and $\daleth(q, Y_\bullet^\pm) \cong \Gamma$.

We need to check that if e is an oriented edge of Γ, then $\sigma(e)$ is equal to $s(e)$. (Note that when writing $s(e)$, we have thought of e as an edge of $\daleth$.) The $s(e)$ obey the zero-tension condition, by Lemma 7.2, so it is enough to check that $s(e) = \sigma(e)$ for (1) e an unbounded ray and (2) $e = e_0$; the zero-tension condition will then determine both $s(e)$ and $\sigma(e)$ for the remaining edges. If e is an unbounded ray, with the leaf v at its end, then we forced there to be $\mp\sigma_v(e)_i$ elements of $Y_i^\pm$ lying at the end of the preimages of e in $\tilde{\daleth}$. For each unbounded ray e' of $\tilde{\daleth}$ (directed towards its leaf), $\tilde{s}(e')_i$ is $\pm$ times the number of elements of $Y_i^\pm$ at the end of e'. So $\sigma(e)_i$ is the sum of $\tilde{s}(e')_i$ over all preimages e' of e. This is precisely the definition of $s(e)_i$.

[10] This construction works for any q of the correct valuation. This is probably unfortunate; it suggests that these methods will need further improvement before they can be used for enumerative problems which are only solvable for certain particular j-invariants.

Now let us consider the case $e = e_0$. If we computed $s(e_0)_i$ using Y_i^+ and Y_i^-, we would get zero, as for every preimage e' of e in $\tilde{\beth}$, all of $U \setminus \{u_0, u_1\}$ lies to one side of e'. When we use Y_i^+ and Y_i^- instead, only one element moves and that element moves past $\sigma(e_0)_i$ preimages of e_0, and we have $\sigma(e_0)_i = s(e_0)_i$.

Lemma 7.5. *For each i between 1 and n, we have $v\big(\prod_{z\in Y_i^+} z\big) = v\big(\prod_{z\in Y_i^-} z\big)$.*

This proof is essentially reversing the proof of Proposition 7.3.

Proof. Fix an index i between 1 and n. We choose an ordering $(y_1^+, y_2^+, \dots, y_m^+)$ of Y_i^+ and an ordering $(y_1^-, y_2^-, \dots, y_m^-)$ of Y_i^-. We want to establish that

$$\sum_{k=1}^{m} v(y_k^+/y_k^-) = 0.$$

Now, y_k^+/y_k^- is the cross ratio $c(y_k^+, y_k^- : 0, \infty)$, so by Proposition 4.2, $v(y_k^+/y_k^-)$ is the signed length of the intersection of $[0, \infty]$ with $[y_k^+, y_k^-]$. We can break up this intersection as a sum over the various edges in the doubly infinite path $[0, \infty]$, so $v(y_k^+/y_k^-) = \pm \sum_{e'\in[0,\infty]\cap[y_k^+, y_k^-]} \ell(e')$, where $\ell(e')$ is the length of e' and the sign describes whether or not the orientation of the path $[y_k^+, y_k^-]$ matches the orientation of e' from 0 to ∞.

We know that for any edge e_j in the circuit of Γ, the signed number of intersections of the paths $[y_1^+, y_1^-], \dots, [y_m^+, y_m^-]$ with the preimages of e_j is $s(e_j)_i$. So $\sum_{k=1}^{m} v(y_k^+/y_k^-) = \sum_{j=1}^{r} \ell(e_j)s(e_j)_i$. But the j-th summand on the right is the displacement in the i-th coordinate between the two endpoints of $\iota(e_j)$. Since the edges $\iota(e_1), \iota(e_2), \dots, \iota(e_r)$ form a closed loop, the sum telescopes to zero. $\square$

Now that we have proven Lemma 7.5, we can speak of the map f.

We have now shown that $\beth \cong \Gamma$, and that, under this identification, $\sigma = s$. It follows that $f(\beth)$ is a translation of $\iota(\Gamma)$, and we will no longer distinguish $\beth$ from Γ. If we had $\prod_{z\in Y_i^+} z = \prod_{z\in Y_i^-} z$, so that the map $\phi : C \to (\mathbb{K}^*)^n$ would exist, then $\operatorname{Trop}\phi(C)$ would be a translation of $f(\Gamma)$. So we will have established Theorem 3.3 if we can simply show that $\prod_{z\in Y_i^+} z = \prod_{z\in Y_i^-} z$. More precisely, what we show is that we can perturb each $Y_i^\pm$ to $Z_i^\pm$, so that this product relation holds, without altering $\tilde{\beth}$ as an abstract tree.

We now describe our perturbative method. We remember that the edges of the circuit of Γ are called $e_1, \dots, e_r$ and we introduce the notation (v_{j-1}, v_j) for the endpoints of e_j, where the indices are cyclic modulo r. Delete the interiors of the edges $e_1, \dots, e_r$ from Γ. Let T_j be the component of the remaining forest containing the vertex v_j of Γ. We will choose constants $u_1, \dots, u_r$ in $\mathbb{K}^*$ with $v(u_1) = \cdots = v(u_r) = 0$, which we think of as associated to the T_j. We modify $Y_i^\pm$ as follows: Let y be an element of $Y_i^\pm$. Consider the component T_j to which

y is attached. Multiply y by u_j to obtain a new element z. The multiset of thus modified elements will form the set $Z_i^{\pm}$.

Now, multiplication by an element u of $\mathbb{K}^*$ with $v(u) = 0$ is an automorphism of $\mathrm{BT}(\mathbb{K})$ which fixes (pointwise) the path $[0, \infty]$. This transformation modifies each component of $\tilde{\mathfrak{I}} \setminus [0, \infty]$ by such an automorphism, so $\tilde{\mathfrak{I}}$ is left unchanged as an abstract tree. So we must understand how multiplication by u_j affects the ratio $\prod_{z \in Z_i^+} z / \prod_{z \in Z_i^-} z$. All of the elements of $Y_i^{\pm}$ which are in T_j are multiplied by u_j. Let $a_{ij} = |Y_i^+ \cap T_j| - |Y_i^- \cap T_j|$. So our modification of the $Y^{\pm}$ multiplies $\prod_{z \in Y_i^+} z / \prod_{z \in Y_i^-} z$ by $\prod_{j=1}^r u_j^{a_{ij}}$.

We want to know that we can choose $u_1, \dots, u_r$ in $v^{-1}(0)$ such that $\prod_{j=1}^r u_j^{a_{ij}} = \prod_{z \in Y_i^+} z / \prod_{z \in Y_i^-} z$ for $i = 1, \dots, n$. We have shown (Lemma 7.5) that the right-hand side of this equation is in $v^{-1}(0)$. So we want to know that the map of abelian groups $v^{-1}(0)^r \mapsto v^{-1}(0)^n$ given by the matrix $A := (a_{ij})$ is surjective. Since $\mathbb{K}$ is algebraically closed, $v^{-1}(0)$ is a divisible group and hence it is enough to know that A has rank n over $\mathbb{Q}$. We now turn to verifying this.

Let Γ' be the graph obtained by taking the circuit of Γ and adding an unbounded ray r_j at each vertex v_j. Let ι' be the map from Γ' into $\mathbb{Q}^n$, where ι' restricted to the circuit of Γ' is ι and the slope of $\iota'(r_j)$ is $(a_{1j}, a_{2j}, \dots, a_{nj})$. Then Γ' and ι' give a zero-tension curve. By our assumption that Γ is ordinary, we know that $\iota'(\Gamma)$ is not contained in any hyperplane. So, by Lemma 5.1, the slopes of the $\iota'(r_j)$ span $\mathbb{Q}^n$. Since the slopes of the $\iota'(r_j)$ are the columns of A, this is the same as saying that A has rank n.

So we deduce that A has full rank over $\mathbb{Q}$ and therefore we can choose $u_1, \dots, u_r$ such that $\prod_{z \in Y_i^+} z / \prod_{z \in Y_i^-} z = \prod_{j=1}^r u_j^{a_{ij}}$ for $i = 1, \dots, n$. This in turn allows us to construct the desired curve C and desired map ϕ.

We conclude with an example of this construction.

Example 7.6. Consider the zero-tension curve of genus one shown in Figure 3, where the map ι is simply an injection. We take all of the edges of the square to have length 1. Then the universal cover, $\tilde{\Gamma}$, is as shown in Figure 4. We need to pick q with $v(q) = 4$; we make the simple choice $q = t^4$. We now cut the circuit of Γ at the edge labeled e to produce the tree T. Set $u_0 = \mathrm{Span}_{\mathbb{O}}((1, 0), (0, 1))$ and $u_1 =$

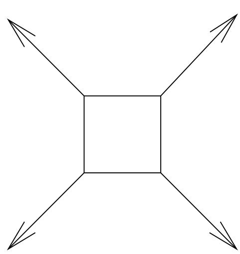


Figure 3. An example of a curve of genus one.

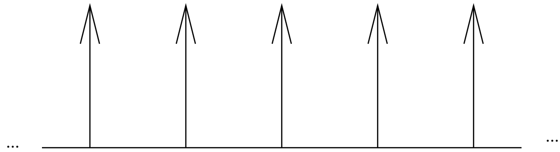


Figure 4. The universal cover of our example.

$\mathrm{Span}_{\mathbb{C}}((1, 0), (0, t^4))$. We take $U = \{u_0, t^0, t^1, t^2, t^3, u_1\}$. The reader is invited to check that, indeed, $[U]$ is isometric to T and $\left[\bigcup_{j=-\infty}^{\infty} q^j (U \setminus \{u_0, u_1\})\right] = [\{t^k\}_{k\in\mathbb{Z}}]$ is isometric to $\tilde{\Gamma}$. The points t^0, t^1, t^2 and t^3 of $\mathbb{P}^1(\mathbb{K})$ correspond to the rays of Γ with slopes $(1, 1)$, $(1, -1)$, $(-1, -1)$ and $(-1, 1)$, respectively.

We now need to choose the multisets Z_1^+, Z_1^-, Z_2^+ and Z_2^-. First we pick subsets $Y_i^\pm$ of U:

$$Y_1^+ = \{t^0, t^1\}, \quad Y_1^- = \{t^2, t^3\},$$
$$Y_2^+ = \{t^0, t^3\}, \quad Y_2^- = \{t^1, t^2\}.$$

We then modify the Y's to produce the Y's. Specifically, we must multiply one of the members of Y_1^+ by q. We obtain

$$Y_1^+ = \{t^4, t^1\}, \quad Y_1^- = \{t^2, t^3\}, \quad Y_2^+ = \{t^0, t^3\}, \quad Y_2^- = \{t^1, t^2\}.$$

This is the stage in the process where we would perturb the Y's to produce the Z's. However, we got lucky this time — we already have $\prod_{z\in Y_i^+} z = \prod_{z\in Y_i^-} z$ for $i = 1, 2$, so no perturbation is necessary and we just take $Z_i^\pm = Y_i^\pm$. So we take the curve C to be $\mathbb{K}^*/t^4$ and we take the map ϕ to be given by $u \mapsto \big(\phi(u; Z_1^+, Z_1^-), \phi(u; Z_2^+, Z_2^-)\big)$. To be completely explicit,

$$u \mapsto \Bigg(\prod_{j=-\infty}^{0} \frac{(1-u/t^{4j+4})(1-u/t^{4j+1})}{(1-u/t^{4j+2})(1-u/t^{4j+3})} \prod_{j=1}^{\infty} \frac{(1-t^{4j+4}/u)(1-t^{4j+1}/u)}{(1-t^{4j+2}/u)(1-t^{4j+3}/u)},$$
$$\prod_{j=-\infty}^{0} \frac{(1-u/t^{4j})(1-u/t^{4j+3})}{(1-u/t^{4j+1})(1-u/t^{4j+2})} \prod_{j=1}^{\infty} \frac{(1-t^{4j}/u)(1-t^{4j+3}/u)}{(1-t^{4j+1}/u)(1-t^{4j+2}/u)} \Bigg).$$

At this point, the reader may reasonably wonder how to extract an actual equation for the curve C. This is basically a problem of *implicitization*, the recovery of the equation of an algebraic variety from a parametric representation, but it is worse than the usual implicitization problem because the parameterization is analytic, not algebraic. This problem deserves study, which has been begun in [Sturmfels and Yu 2008; Sturmfels et al. 2007]. We will describe here a straightforward but unwieldy method. Let Σ denote the complete fan whose rays point in directions $(1, 1)$, $(1, -1)$, $(-1, -1)$ and $(-1, 1)$. Then, by Proposition 1.2, the closure of

$\phi(C)$ in[11] $X(\Sigma)$ is torically transverse and has cohomology class corresponding to the linear relation $(1, 1)+(1, -1)+(-1, -1)+(-1, 1)=0$ between the rays of Σ. Thus, $\phi(C)$ obeys an equation of the form $Px + Qy + R + Sx^{-1} + Ty^{-1} = 0$, for some P, Q, R, S and T in $\mathbb{K}$. Here we have written the coordinates on $(\mathbb{K}^*)^2$ as x and y. In order to find P, Q, R, S and T, expand the infinite products for x and y as Laurent series around $u-1$, and compare the coefficients of $(u-1)^k$ for $k=-1$, 0, 1, 2, 3. Note that this will express P, Q, R, S and T in terms of infinite sums. There is no reason to expect a better result; our algorithm will usually produce curves defined by equations whose coefficients are not algebraic functions of t.

8. Superabundant curves

In this section, we prove Theorem 3.4, which we restate for the reader's convenience.

Theorem 3.4. *Suppose that κ has characteristic zero.*

Let (ι, Γ, m) be a zero-tension curve of genus one and degree δ. Suppose also that (ι, Γ, m) is well spaced. Then there is a (punctured) genus-one curve C over $\mathbb{K}$ and a map $\phi : C \to \mathbb{T}(\mathbb{K}, N)$ of degree δ such that $\iota(\Gamma) = \operatorname{Trop}\phi(C)$.

See the end of Section 3 for the definition of "well spaced". We may as well assume that $\iota(\Gamma)$ is not contained in any hyperplane, as otherwise the problem reduces to constructing a map to a lower-dimensional torus.

For each nonnegative rational number R, let $\Delta(R)$ be the subgraph of Γ consisting of those points with distance less than or equal to R from the circuit of Γ. Let $H(R)$ be the affine linear space spanned by $\Delta(R)$. Then $H(R)$ is an increasing chain of affine spaces which increases at a finite number of discrete indices. Let $n_0, n_1, \dots, n_s = n$ be the dimensions of the various H_R's. (The last term is n, because we are assuming that $\iota(\Gamma)$ is not contained in a hyperplane.) The reader may find this section easier to follow under the simplifying assumption that $n_i = n_0 + i$.

Let $m = n_j$ for some j. Let $R_m = \max\{R : \dim H(R) \le m\}$; let $\Delta_m = \Delta(R_m)$ and $H_m = H(R_m)$. We will also occasionally need to refer to the open subset of Δ_m consisting of those points at distance strictly less than R_m from the circuit of Γ; we denote this by Δ_m^-. We can make a change of basis in N such that H_m is $\operatorname{Span}_{\mathbb{Q}}(e_1, e_2, \dots, e_m)$.

By the arguments in the previous section, we can find $Z_1^{\pm}, \dots, Z_n^{\pm}$, multisubsets of $\mathbb{P}^1(\mathbb{K})$, and $q \in \mathbb{K}^*$, such that $f(\daleth(q, Z_\bullet^{\pm})) = \iota(\Gamma)$. We can use the perturbation arguments of the preceding section to arrange that $\prod_{z\in Z_i^+} z = \prod_{z\in Z_i^-} z$ for $i = 1, \dots, n_0$. However, for $i > n_0$, all we can conclude is that

$$v\Bigl(\prod_{z\in Z_i^+} z\Bigr) = v\Bigl(\prod_{z\in Z_i^-} z\Bigr).$$

[11] Recall that $X(\Sigma)$ is the toric variety associated to the fan Σ.

The strategy of our proof will be to show, by induction on j, that we can arrange for the equality $\prod_{z\in Z_i^+} z = \prod_{z\in Z_i^-} z$ to hold for $i \leq n_j$.

The case where $j = 0$ and $R_0 = 0$ needs to be handled slightly separately; so we will provide the necessary modifications of the argument in that case in square brackets, and address the rest of the proof to the case that $R_j > 0$.

So, suppose that we have $Z_1^\pm, \ldots, Z_n^\pm$ and q such that $f(\beth(q, Z_\bullet^\pm)) = \iota(\Gamma)$ and such that $\prod_{z\in Z_i^+} z = \prod_{z\in Z_i^-} z$ holds for $i \leq n_j$. From now on, we fix j; we set $m = n_j$ and $m' = n_{j+1}$. We introduce the notation U for the group of units u of $\mathbb{O}$ such that $v(u-1) \geq R_m$. [When $j = 0$ and $R_0 = 0$, take U to be the group of all units of $\mathbb{O}$; that is, $v^{-1}(0)$.]

Lemma 8.1. *The abelian group U is divisible.*

Proof. This is where we will use that κ has characteristic zero, and hence that $v(k) = 0$ for every nonzero integer j. Let $u \in U$ and let j be a nonzero integer. Then, since $\mathbb{K}$ is algebraically closed, u has a j-th root in $\mathbb{K}$, and even has a root which lies in $\mathbb{O}$ and reduces to 1 in κ. (Proof — let $u_1, \ldots, u_j$ be the roots of $z^j - u$ in $\mathbb{K}$. Since $jv(u_i) = v(u_i^j) = v(u) = 0$, we know that all of the u_i are in $\mathbb{O}$. Let $\overline{u_i}$ be the reduction of u_i in κ. Then we have $z^j - 1 = \prod(z - \overline{u_i})$ in κ, so by unique factorization in $\kappa[z]$, one of the u_i reduces to 1 in κ.) So let $(1+\pi)^j = u$ with $v(\pi) > 0$. Then $u = 1 + j\pi + \pi^2 c$ where $c \in \mathbb{O}$. As $v(j) = 0$, we have $v(j\pi) < v(\pi^2 c)$, so $v(u-1) = v(j\pi) = v(\pi)$ and we deduce that $v(\pi) \geq R_m$, so $1+\pi$ is in U as desired.

[When $j = 0$ and $R_0 = 0$, we know that any unit of $\mathbb{O}$ has a j-th root in $\mathbb{K}$ since $\mathbb{K}$ is algebraically closed. This j-th root must also have valuation zero.] □

Lemma 8.2. *For each i between 1 and n, the ratio $\prod_{z\in Z_i^+} z / \prod_{z\in Z_i^-} z$ is in U.*

Proof. For $i \leq m$, we have $\prod_{z\in Z_i^+} z / \prod_{z\in Z_i^-} = 1$, which is in U. So fix $i > m$. Let $T_1, \ldots, T_r$ be the components of $\Gamma \setminus \Delta_m^-$. We note that, for each k, we have $|Z_i^+ \cap T_k| = |Z_i^- \cap T_k|$. This is because, by the zero-tension condition, $|Z_i^+ \cap T_k| - |Z_i^- \cap T_k|$ is the i-th component of the edge of Δ_m pointing inward from T_k. Since this is an edge of Δ_m, that component is zero. So we can pair off the elements of $Z_i^+ \cap T_K$ with those of $Z_i^- \cap T_k$. In each pair (z^+, z^-), we have $v(z^+/z^- - 1) = v(c(z^+, \infty; z^-, 0) - 1)$, which is at least R_m by Proposition 4.2. Then $\prod_{z\in Z_i^+} z / \prod_{z\in Z_i^-} z$ is a product of ratios which are in U, and hence is itself in U as we claimed.

[When $j = 0$ and $R_j = 0$, we can't talk about Δ_m^-. Rather, let Δ^- be the interiors of the edges of the loop, so $\Gamma \setminus \Delta^-$ is a forest with one connected component for each vertex of the loop. Define $T_1, T_2, \ldots, T_r$ to be the connected components of this forest. This time, $|Z_i^+ \cap T_k| - |Z_i^- \cap T_k|$ is the sum of the i-th components of the two edges of the loop incident to T_i. As before, these edges are in the loop, so the i-th components are zero. $|Z_i^+ \cap T_k| = |Z_i^- \cap T_k|$ follows as before, and the rest of the proof does as well.] □

We introduce the notation w_i for $\prod_{z \in Z_i^+} z / \prod_{z \in Z_i^-} z$, which we have just shown to be in U. When $1 \leq i \leq m$, then w_i is simply 1.

Let $e_1, \dots, e_p$ be the edges of Γ which are not in Δ_m, but which have endpoints that are in Δ_m. Let $s_1, \dots, s_p$ be the slopes of these edges, directed away from Δ_m. We write the components of s_k as $(s_k^1, \dots, s_k^n)$.

Lemma 8.3. *There exist scalars $a_1, \dots, a_p \in \mathbb{Q}$ such that $\sum a_i s_i = 0$ and such that if e_g and e_h are distinct edges with the same endpoint, then $a_g \neq a_h$.*

Proof. Let t_i be the image of s_i in $\mathbb{Q}^n / H_m$. We first show that we can find $b_1, \dots, b_p$ obeying the required inequalities with $\sum b_i t_i = 0$. Let $L \subset \mathbb{Q}^p$ be the space of p-tuples of rational numbers $(b_1, \dots, b_p)$ such that $\sum b_i t_i = 0$. We want to show that L has a point which is not in the union of the hyperplanes $b_g = b_h$, where (g, h) ranges over pairs of indices such that e_g and e_h share an endpoint. Since L is a linear space, we just need to show that L is not contained in any of these hyperplanes.

Let e_g and e_h share the endpoint x, which is necessarily a boundary vertex of Γ_m. Suppose for the sake of contradiction that L is contained in the hyperplane $a_g = a_h$. Then in particular, L does not contain any point with $b_g = 0$ and $b_h = 1$. This means that t_h is not in the span of $\{t_i\}_{i \neq g,h}$. Equivalently, s_h is not in $V := H_m + \operatorname{Span}(\{s_i\}_{i \neq g,h})$. Let K be a hyperplane in $\mathbb{Q}^n$ which contains V and does not contain s_h. Then x is at distance R_m from the loop of Γ, while every other boundary vertex of $\Gamma \cap \iota^{-1}(K)$ is farther away, contradicting our hypothesis that Γ is well spaced. This contradiction shows that we can find the required b_i.

So, now we have $(b_1, \dots, b_p)$ obeying the required inequalities with $\sum b_i s_i$ in H_m. Let $x_1, \dots, x_r$ be the boundary vertices of Δ_m and let u_k be the slope of the edge of Δ_m pointing inward from x_k. Then, by Lemma 5.1, the u_k span H_m. Let $\sum b_i s_i = \sum c_k u_k$. Now, by the zero-tension condition, $u_k = -\sum_{e_i \ni x_k} s_i$. So we have $\sum_{i=1}^p b_i s_i + \sum_{k=1}^r c_k \sum_{x_k \ni e_i} s_i = 0$. We regroup this expression and take the coefficient of s_i to be our a_i. If e_g and e_h share the endpoint x_k, then the coefficients of s_g and s_h in this expression are $b_g + c_k$ and $b_h + c_k$. Since $b_g \neq b_h$, we also have $b_g + c_k \neq b_h + c_k$ and we have achieved the goal. □

Our strategy will be to choose $u_1, \dots, u_p \in U$ and, for each $Z_i^{\pm}$, multiply those elements of $Z_i^{\pm}$ which lie in the component of $\Gamma \setminus \Delta_m$ containing e_k by u_k. This will have the effect of multiplying w_i by

$$v_i := \prod_{k=1}^{p} u_k^{s_k^i}.$$

We need to achieve two things: make the new values of w_i be 1 for $i \le m'$, and preserve the condition $f(\daleth) = \iota(\Gamma)$.

Now, by Lemma 5.1 applied to $\Delta(R_m + \epsilon)$ for some small ϵ, we know that the s_j span $H(R_{m'})$. Since U is a divisible group, this means that we can arrange to make v_i (above) assume any value that we want for $1 \le i \le m'$. In particular, we can make $w_1 = w_2 = \cdots = w_{m'} = 1$. The trouble is that we might no longer have $\daleth \cong \Gamma$. Now, multiplication by an element of U will fix all of the points of Δ_m and will move each component of $\Gamma \setminus \Delta_m$ by an isomorphism. Our only fear is that two of these components which are connected to Δ_m at the same vertex, say x, will swing so that the edges at which they attach to x, say e_c and e_d, overlap for some length.

Let $(a_1, \dots, a_q) \in \mathbb{Q}^q$ be the vector found in Lemma 8.3. Assume that we have arranged for w_i to be 1 for $i = 1, 2, \dots, n_{j+1}$. Now choose some $u \in U$. For each $Z_i^{\pm}$, take those elements of Z which lie in the component of $\Gamma \setminus \Delta_m$ containing e_k and multiply them by u^{a_k}. This will multiply w_i by u^E where $E = \sum a_k s_k^i = 0$; in other words, it will not change w_i. So this will not break our achievement of making the $w_i = 1$ (for $i = 1, \dots, m'$.) Also, if e_c and e_d share an end point x, then the components of $\Gamma \setminus \Delta_m$ containing e_c and e_d will be multiplied by u^{a_c} and u^{a_d} respectively, two different scalars, and so, for generic $u \in U$, they will not overlap.

We have now completed the inductive step, showing how to make w_i equal to 1 for $i \le n_{j+1}$. Continuing in this manner, we will eventually have all the w_i equal to 1, and thus the map ϕ will be well defined. At that point, we will have a curve C and a map ϕ with $\operatorname{Trop}\phi(C) = \iota(\Gamma)$ as desired.

9. The necessity of well-spacedness and the j-invariant

We have been studying genus-one curves over C by identifying them with Tate curves. It is therefore natural to ask to what extent we may assume that a genus-one curve over $\mathbb{K}$ is a Tate curve.

Theorem 9.1. *Let C be a genus-one curve over $\mathbb{K}$ and $\overline{C}$ its projective completion. Let j be the j-invariant of C. Let $\mathscr{C}$ be the extension of $(\overline{C}, \overline{C} \setminus C)$ to a flat family of stable curves with marked points over $\mathbb{O}$. Then the following are equivalent*:

(1) *C can be expressed as a Tate curve for some $q \in \mathbb{K}^*$ with $v(q) > 0$.*

(2) $v(j) < 0$.

(3) *The fiber of $\mathscr{C}$ over* Spec κ *is a union of genus-zero curves.*

Moreover, if these equivalent conditions hold, we have $v(q) = -v(j)$.

Proof. The equivalence of (1) and (2) is [Roquette 1970, Section 3, Statement VIIIa]. (Observe that Roquette's conditions (i) and (iii) are automatic when $\mathbb{K}$ is algebraically closed, the latter because the Hasse invariant lives in the group

$\mathbb{K}^*/(\mathbb{K}^*)^2$, which is trivial for $\mathbb{K}$ algebraically closed.) If N is the number of points in $\bar{C} \setminus C$, then $\mathscr{C}$ gives a map from $\operatorname{Spec}(\mathbb{O})$ to the moduli space of stable genus-one curves with N marked points. Forgetting all but one of the points, we get a map to the moduli space of stable genus-one curves with one marked point. This moduli space is a copy of the projective line, commonly known as the j-line. Condition (3) is equivalent to saying that this map sends $\operatorname{Spec}\kappa$ to the point at infinity on the j-line, which is exactly what condition (2) says. We have $v(j) = -v(q)$ because $j = q^{-1} + \sum_{i=0}^{\infty} c_i q^i$, where each c_i is an integer and hence has nonnegative valuation. □

Combining the above with the second paragraph of Theorem 3.1, we see that if (ϕ, C) is trivalent and $\operatorname{Trop}\phi(C)$ has first Betti number one, then C is a Tate curve. In this case, we can show that the condition that $\operatorname{Trop}\phi(C)$ be well spaced is necessary, and that the length of the loop of $\operatorname{Trop}\phi(C)$ is necessarily $-v(j)$. Recall that *every* nonzero meromorphic function ϕ on a Tate curve is of the form $a\prod_{i=1}^{m}\big(\Theta(u/z_i^+)/\Theta(u/z_i^-)\big)$ for some $Z^+ = \{z_1^+, \dots, z_m^+\}$ and $Z^- = \{z_1^-, \dots, z_m^-\} \subset \mathbb{K}^*$ with $\prod z_i^+ = \prod z_i^-$.

Proposition 9.2. *Let (ϕ, C) be a trivalent tropical curve of genus one and (ι, Γ, m) a zero-tension curve parameterizing* $\operatorname{Trop}\phi(C)$, *with $b_1(\Gamma) = 1$ and ι injective on Γ. Then the length of the loop of Γ is $-v(j(C))$, where $j(C)$ is the j-invariant of C. Now suppose that κ has characteristic zero. Then (ι, Γ, m) is well spaced.*

The idea that the length of the circuit of Γ is the tropical analogue of the j-invariant was suggested in [Mikhalkin 2006] and pursued in [Kerber and Markwig 2009]. E. Katz and H. and T. Markwig have proven that the length of the circuit of Γ is the j-invariant of a trivalent curve for tropicalizations of cubic curves in $\mathbb{P}^2$.

Proof. Our hypotheses are enough to ensure that C is a Tate curve $\mathbb{K}^*/q^{\mathbb{Z}}$ for some q and that the map $\phi : C \to (\mathbb{K}^*)^n$ is given by $u \mapsto \big(\phi(u; Z_1^+, Z_1^-), \dots, \phi(u; Z_n^+, Z_n^-)\big)$ for some $Z_1^\pm, \dots, Z_n^\pm$.

By our combinatorial construction of $\daleth(q, Z_\bullet^\pm)$, the length of the loop of $\daleth$ is $v(q) = -v(j(C))$. Lemma 5.2 ensures that f is injective, and thus the loop of $\daleth$ and the loop of Γ have the same length.

Now, assume that κ has characteristic zero and (for the sake of contradiction) that (ι, Γ, m) is not well spaced. After a change of coordinates, we may assume that H is the n-th coordinate hyperplane. Assume for the sake of contradiction that x is the boundary vertex of $\Gamma \cap H$ which is closest to the loop of Γ, and let R denote the distance from x to the loop of Γ. Then x is trivalent by hypothesis. One of the edges of x is between x and the loop of Γ; this edge is contained in H, so its n-th component is 0. Let the n-th components of the other two edges be a and $-a$ for some positive integer a. Let $\{z_1^+, \dots, z_a^+\}$ and $\{z_1^-, \dots, z_a^-\}$ be the elements of Z_n^+ and Z_n^- respectively which are beyond these edges. Then we have $v(z_i^+/z_j^+ - 1) > R$

for any indices i and j from 1 to a and similarly $v(z_i^-/z_j^- - 1) > R$. On the other hand, $v(z_i^+/z_j^- - 1) = R$. So

$$\prod_{i=1}^{a}(z_i^+/z_i^-) = (z_1^+/z_1^-)^a(1+t^R c)$$

for some c with $v(c) > 0$ and thus $v\bigl(\prod_{i=1}^{a}(z_i^+/z_i^-) - 1\bigr) = R$. We have used that κ has characteristic zero to deduce that if $v(u-1) > 0$, then $v(u^a - 1) = v(u-1)$.

Pair off the elements of $Z_n^+ \setminus \{z_1^+, \dots, z_a^+\}$ with elements of $Z_n^- \setminus \{z_1^-, \dots, z_a^-\}$ that lie in the same component of $\Gamma \setminus (H \cap \Gamma)$; this is possible by the same argument as in the proof of Lemma 8.2. We write the pairs as (z_i^+, z_i^-) for $i > a$. Then in each pair (z^+, z^-), we have $v(z^+/z^- - 1) > R$. But we are supposed to have $\prod_{z\in Z_n^+} z / \prod_{z \in Z_n^-} z = 1$, so $\prod_{i=1}^{a}(z_i^+/z_i^-) = \bigl(\prod_{i>a}(z_i^+/z_i^-)\bigr)^{-1}$. Then the left-hand side differs from 1 by an element of valuation R while the right-hand side differs from 1 by an element of valuation greater than R, a contradiction. □

Acknowledgements

This paper, which has been several years in preparation, stems from portions of my Ph.D. dissertation. I am extremely grateful to my advisor Bernd Sturmfels, for his guidance in the writing of the dissertation and afterwards. I want to thank Paul Hacking, Hannah and Thomas Markwig, Grigory Mikhalkin, Sam Payne and Jenia Tevelev for many discussions of my work and theirs, including informing me of many results which were unpublished at the time. Finally, I was aided by several extremely careful referees. During much of the writing of this paper, I have been supported by a research fellowship from the Clay Mathematics Institute.

References

[Baker and Norine 2007] M. Baker and S. Norine, "Riemann–Roch and Abel–Jacobi theory on a finite graph", *Adv. Math.* **215**:2 (2007), 766–788. MR 2008m:05167 Zbl 1124.05049

[Baker et al. 2012] M. Baker, S. Payne, and J. Rabinoff, "Nonarchimedean geometry, tropicalization, and metrics on curves", preprint, 2012. arXiv 1104.0320

[Bieri and Groves 1984] R. Bieri and J. R. J. Groves, "The geometry of the set of characters induced by valuations", *J. Reine Angew. Math.* **347** (1984), 168–195. MR 86c:14001 Zbl 0526.13003

[Bogart et al. 2007] T. Bogart, A. N. Jensen, D. Speyer, B. Sturmfels, and R. R. Thomas, "Computing tropical varieties", *J. Symbolic Comput.* **42**:1-2 (2007), 54–73. MR 2007j:14103 Zbl 1121.14051

[Draisma 2008] J. Draisma, "A tropical approach to secant dimensions", *J. Pure Appl. Algebra* **212**:2 (2008), 349–363. MR 2008j:14102 Zbl 1126.14059

[Einsiedler et al. 2006] M. Einsiedler, M. Kapranov, and D. Lind, "Non-Archimedean amoebas and tropical varieties", *J. Reine Angew. Math.* **601** (2006), 139–157. MR 2007k:14038 Zbl 1115.14051

[Fulton 1993] W. Fulton, *Introduction to toric varieties*, Annals of Mathematics Studies **131**, Princeton University Press, 1993. MR 94g:14028 Zbl 0813.14039

[Fulton and Sturmfels 1997] W. Fulton and B. Sturmfels, "Intersection theory on toric varieties", *Topology* **36**:2 (1997), 335–353. MR 97h:14070 Zbl 0885.14025

[Gathmann and Kerber 2008] A. Gathmann and M. Kerber, "A Riemann–Roch theorem in tropical geometry", *Math. Z.* **259**:1 (2008), 217–230. MR 2009a:14014 Zbl 1187.14066

[Gathmann et al. 2009] A. Gathmann, M. Kerber, and H. Markwig, "Tropical fans and the moduli spaces of tropical curves", *Compos. Math.* **145**:1 (2009), 173–195. MR 2009m:14085 Zbl 1169.51021

[Helm and Katz 2012] D. Helm and E. Katz, "Monodromy filtrations and the topology of tropical varieties", *Canad. J. Math.* **64**:4 (2012), 845–868. MR 2957233 Zbl 06064256

[Katz 2012] E. Katz, "Lifting tropical curves in space and linear systems on graphs", *Adv. Math.* **230**:3 (2012), 853–875. MR 2921163 Zbl 06059012

[Kerber and Markwig 2009] M. Kerber and H. Markwig, "Counting tropical elliptic plane curves with fixed j-invariant", *Comment. Math. Helv.* **84**:2 (2009), 387–427. MR 2010c:14079 Zbl 1205.14071

[Mikhalkin 2005] G. Mikhalkin, "Enumerative tropical algebraic geometry in $\mathbb{R}^2$", *J. Amer. Math. Soc.* **18**:2 (2005), 313–377. MR 2006b:14097 Zbl 1092.14068

[Mikhalkin 2006] G. Mikhalkin, "Tropical geometry and its applications", pp. 827–852 in *International Congress of Mathematicians* (Madrid, 2006), vol. 2, edited by M. Sanz-Solé et al., Eur. Math. Soc., Zürich, 2006. MR 2008c:14077 Zbl 1103.14034 arXiv math/0601041

[Mikhalkin 2007] G. Mikhalkin, "Moduli spaces of rational tropical curves", pp. 39–51 in *Proceedings of Gökova Geometry-Topology Conference 2006* (Gökova, 2006), edited by S. Akbulut et al., International Press, Somerville, MA, 2007. MR 2009i:14014 Zbl 1203.14027 arXiv 0704.0839

[Morgan and Shalen 1984] J. W. Morgan and P. B. Shalen, "Valuations, trees, and degenerations of hyperbolic structures, I", *Ann. of Math.* (2) **120**:3 (1984), 401–476. MR 86f:57011 Zbl 0583.57005

[Nishinou 2010] T. Nishinou, "Correspondence theorems for tropical curves", preprint, 2010. arXiv 0912.5090

[Nishinou and Siebert 2006] T. Nishinou and B. Siebert, "Toric degenerations of toric varieties and tropical curves", *Duke Math. J.* **135**:1 (2006), 1–51. MR 2007h:14083 Zbl 1105.14073 arXiv math/0409060

[Payne 2009a] S. Payne, "Analytification is the limit of all tropicalizations", *Math. Res. Lett.* **16**:3 (2009), 543–556. MR 2010j:14104 Zbl 1193.14077

[Payne 2009b] S. Payne, "Fibers of tropicalization", *Math. Z.* **262**:2 (2009), 301–311. MR 2010c:14081 Zbl 1222.14130

[Roquette 1970] P. Roquette, *Analytic theory of elliptic functions over local fields*, Hamburger Mathematische Einzelschriften (N.F.) **1**, Vandenhoeck and Ruprecht, Göttingen, 1970. MR 41 #5376 Zbl 0194.52002

[Shustin and Tyomkin 2006] E. Shustin and I. Tyomkin, "Patchworking singular algebraic curves, I", *Israel J. Math.* **151** (2006), 125–144. MR 2007b:14056 Zbl 1128.14019

[Speyer and Sturmfels 2004] D. Speyer and B. Sturmfels, "The tropical Grassmannian", *Adv. Geom.* **4**:3 (2004), 389–411. MR 2005d:14089 Zbl 1065.14071

[Sturmfels 1996] B. Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series **8**, American Mathematical Society, Providence, RI, 1996. MR 97b:13034 Zbl 0856.13020

[Sturmfels 2002] B. Sturmfels, *Solving systems of polynomial equations*, CBMS Regional Conference Series in Mathematics **97**, American Mathematical Society, Providence, RI, 2002. MR 2003i:13037 Zbl 1101.13040

[Sturmfels and Yu 2008] B. Sturmfels and J. Yu, "Tropical implicitization and mixed fiber polytopes", pp. 111–131 in *Software for algebraic geometry* (Minneapolis, MN, 2006), edited by M. E. Stillman et al., IMA Vol. Math. Appl. **148**, Springer, New York, 2008. MR 2009m:14089 Zbl 1143.14313

[Sturmfels et al. 2007] B. Sturmfels, J. Tevelev, and J. Yu, "The Newton polytope of the implicit equation", *Mosc. Math. J.* **7**:2 (2007), 327–346. MR 2008f:14073 Zbl 1133.13026 arXiv math/0607368

Communicated by Bernd Sturmfels
Received 2013-06-12 Revised 2013-12-20 Accepted 2014-01-29

speyer@umich.edu *Department of Mathematics, University of Michigan, 2844 East Hall, 530 Church Street, Ann Arbor, MI 48109-1043, United States*

ALGEBRA AND NUMBER THEORY 8:4 (2014)
dx.doi.org/10.2140/ant.2014.8.999

Pair correlation of angles between reciprocal geodesics on the modular surface

Florin P. Boca, Vicențiu Pașol,
Alexandru A. Popa and Alexandru Zaharescu

The existence of the limiting pair correlation for angles between reciprocal geodesics on the modular surface is established. An explicit formula is provided, which captures geometric information about the length of reciprocal geodesics, as well as arithmetic information about the associated reciprocal classes of binary quadratic forms. One striking feature is the absence of a gap beyond zero in the limiting distribution, contrasting with the analog Euclidean situation.

1. Introduction

Let $\mathbb{H}$ denote the upper half-plane and $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ the modular group. Consider the modular surface $X = \Gamma\backslash\mathbb{H}$, and let $\Pi : \mathbb{H} \to X$ be the natural projection. The angles on the upper half-plane $\mathbb{H}$ considered in this paper are the same as the angles on X between the closed geodesics passing through $\Pi(i)$ and the image of the imaginary axis. These geodesics were first introduced in connection with the associated "self-inverse classes" of binary quadratic forms in the classical work of Fricke and Klein [1892, p. 164], and the primitive geodesics among them were studied recently and called reciprocal geodesics by Sarnak [2007]. The aim of this paper is to establish the existence of the pair correlation measure of their angles and to explicitly express it.

For $g \in \Gamma$, denote by $\theta_g \in [-\pi, \pi]$ the angle between the vertical geodesic $[i, 0]$ and the geodesic ray $[i, gi]$. For $z_1, z_2 \in \mathbb{H}$, let $d(z_1, z_2)$ denote the hyperbolic distance, and set

$$\|g\|^2 = 2\cosh d(i, gi) = a^2 + b^2 + c^2 + d^2 \quad \text{for } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}).$$

MSC2010: primary 11K36; secondary 11J71, 11M36, 11P21, 37D40.
Keywords: modular surface, reciprocal geodesics, pair correlation, hyperbolic lattice points, hyperbolic lattice angles.

It was proved by Nicholls [1983] (see also [Nicholls 1989, Theorem 10.7.6]) that for any discrete subgroup Γ of finite covolume in $\mathrm{PSL}_2(\mathbb{R})$, the angles θ_γ are uniformly distributed, in the sense that for any fixed interval $I \subseteq [-\pi, \pi]$,

$$\lim_{R\to\infty} \frac{\#\{\gamma \in \Gamma : \theta_\gamma \in I, d(i, \gamma i) \leqslant R\}}{\#\{\gamma \in \Gamma : d(i, \gamma i) \leqslant R\}} = \frac{|I|}{2\pi}.$$

Effective estimates for the rate of convergence that allow one to take $|I| \asymp e^{-cR}$ as $R \to \infty$ for some constant $c = c_\Gamma > 0$ were proved for $\Gamma = \Gamma(N)$ by one of us [Boca 2007], and in general situations by Risager and Truelsen [2010] and by Gorodnik and Nevo [2012]. Other related results concerning the uniform distribution of real parts of orbits in hyperbolic spaces were proved by Good [1983], and more recently by Risager and Rudnick [2009].

The statistics of spacings, such as the pair correlation or the nearest neighbor distribution (also known as the gap distribution) measure the fine structure of sequences of real numbers in a more subtle way than the classical Weyl uniform distribution. Very little is known about the spacing statistics of closed geodesics. In fact, the only result that we are aware of, due to Pollicott and Sharp [2006], concerns the correlation of differences of lengths of pairs of closed geodesics on a compact surface of negative curvature, ordered with respect to the word length on the fundamental group.

This paper investigates the pair correlation of angles θ_γ with $d(i, \gamma i) \leqslant R$, or equivalently with $\|\gamma\|^2 \leqslant Q^2 = e^R \sim 2\cosh R$ as $Q \to \infty$. As explained in Section 2, these are exactly the angles between reciprocal geodesics on the modular surface.

The Euclidean analog of this problem considers the angles between the line segments connecting the origin $(0, 0)$ with all integer points (m, n) satisfying $m^2 + n^2 \leqslant Q^2$ as $Q \to \infty$. When only primitive lattice points are being considered (rays are counted with multiplicity one), the problem reduces to the study of the pair correlation of the sequence of Farey fractions with the L^2 norm $\|m/n\|_2^2 = m^2 + n^2$. Its pair correlation function is plotted on the left of Figure 1. When Farey fractions are ordered by their denominator, the pair correlation is shown to exist and it is explicitly computed in [Boca and Zaharescu 2005]. A common important feature is the existence of a gap beyond zero for the pair correlation function. This is an ultimate reflection of the fact that the area of a nondegenerate triangle with integer vertices is at least $\frac{1}{2}$, which corresponds to the familiar inequality $|b/d - a/c| \geqslant 1/cd$ satisfied by two lattice points $P = (a, b)$ and $Q = (c, d)$ with $\mathrm{Area}(\triangle OPQ) > 0$.

For the hyperbolic lattice centered at i, it is convenient to start with the (nonuniformly distributed) numbers $\tan(\theta_\gamma/2)$ with multiplicities, rather than the angles θ_γ themselves. Employing obvious symmetries explained in Section 3, it is further convenient to restrict to a set of representatives $\Gamma_{\mathbf{I}}$ consisting of matrices γ with nonnegative entries such that the point γi is in the first quadrant in Figure 2. The pair correlation measures of the finite set $\mathfrak{A}_Q$ of elements θ_γ with $\gamma \in \Gamma_{\mathbf{I}}$ and $\|\gamma\| \leqslant Q$ (counted with multiplicities) is defined as

$$R_Q^{\mathfrak{A}}(\xi) = \frac{1}{B_Q}\#\Big\{(\gamma,\gamma') \in \Gamma_{\mathbf{I}}^2 : \|\gamma\|, \|\gamma'\| \leqslant Q,\ \gamma' \neq \gamma,\ 0 \leqslant \frac{2}{\pi}\big(\theta_{\gamma'} - \theta_\gamma\big) \leqslant \frac{\xi}{B_Q}\Big\},$$

where $B_Q \sim \frac{3}{8}Q^2$ denotes the number of elements $\gamma \in \Gamma_{\mathbf{I}}$ with $\|\gamma\| \leqslant Q$. As it will be used in the proof, we similarly define the pair correlation measure $R_Q^{\mathfrak{T}}(\xi)$ of the set $\mathfrak{T}_Q$ of elements $\tan(\theta_\gamma/2)$ with $\gamma \in \Gamma_{\mathbf{I}}$ and $\|\gamma\| \leqslant Q$.

One striking feature, illustrated by the numerical calculations in Figure 1, points to the absence of a gap beyond zero in the limiting distribution, in contrast with the analog Euclidean situation.

The main result of this paper is the proof of existence and explicit computation of the pair correlation measure $R_2^{\mathfrak{A}}$ given by

$$R_2^{\mathfrak{A}}(\xi) = R_2^{\mathfrak{A}}\big((0,\xi]\big) := \lim_{Q\to\infty} R_Q^{\mathfrak{A}}(\xi), \tag{1-1}$$

and similarly for $R_2^{\mathfrak{T}}$, thus answering a question raised in [Boca 2007].

To give a precise statement, consider $\mathfrak{S}$, the free semigroup on two generators $L = \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$ and $R = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$. Repeated application of the Euclidean algorithm shows that $\mathfrak{S} \cup \{I\}$ coincides with the set of matrices in $\mathrm{SL}_2(\mathbb{Z})$ with nonnegative entries. The explicit formula for $R_2^{\mathfrak{T}}(\xi)$ is given as a series of volumes summed over $\mathfrak{S}$, plus a finite sum of volumes, and it is stated in Theorem 2 (Section 7). The formula for $R_2^{\mathfrak{T}}(\xi)$ leads to an explicit formula for $R_2^{\mathfrak{A}}(\xi)$, which we state here, partly because the pair correlation function for the angles θ_γ is more interesting, being equidistributed, and partly because the formula we obtain is simpler.

Theorem 1. *The pair correlation measure $R_2^{\mathfrak{A}}$ on $[0,\infty)$ exists and is given by the C^1 function*

$$R_2^{\mathfrak{A}}\Big(\frac{3}{4\pi}\xi\Big) = \frac{8}{3\zeta(2)}\bigg(\sum_{M\in\mathfrak{S}} B_M(\xi) + \sum_{\ell\in[0,\xi/2)}\ \sum_{K\in[1,\xi/2)} A_{K,\ell}(\xi)\bigg). \tag{1-2}$$

For $M \in \mathfrak{S}$, letting $U_M = \|M\|^2/\sqrt{\|M\|^4 - 4}$, θ_M as above, and $f_+ = \max\{f,0\}$, we have

$$B_M(\xi) = \frac{\pi}{4}\int_0^{\pi/2} \frac{\big(1/\sqrt{\|M\|^4-4} - \sin(2\theta-\theta_M)/\xi\big)_+}{U_M + \cos(2\theta-\theta_M)}\,d\theta.$$

For integers $\ell \in [0,\xi/2)$, $K \in [1,\xi/2)$, we have

$$A_{K,\ell}(\xi) = \int_0^{\pi/4} A_{K,\ell}\Big(\frac{\xi}{2\cos^2 t}, t\Big)\frac{dt}{\cos^2 t},$$

where $A_{K,\ell}(\xi, t)$ is the area of the region defined by those $re^{i\theta} \in [0,1]^2$ such that

$$L_{\ell+1}(e^{i\theta}) > 0, \qquad \frac{F_{K,\ell}(\theta)}{\xi} \leqslant r^2 \leqslant \frac{\cos^2 t}{\max\{1, L_\ell^2(e^{i\theta}) + L_{\ell+1}^2(e^{i\theta})\}}, \tag{1-3}$$

with $e^{i\theta} = (\cos\theta, \sin\theta)$, the piecewise linear functions L_i as defined in (5-5), and

$$F_{K,\ell}(\theta) := \cot\theta + \sum_{i=1}^{\ell} \frac{1}{L_{i-1}(e^{i\theta})L_i(e^{i\theta})} + \frac{L_{\ell+1}(e^{i\theta})}{L_\ell(e^{i\theta})\big(L_\ell^2(e^{i\theta}) + L_{\ell+1}^2(e^{i\theta})\big)}.$$

Rates of convergence in (1-1) are effectively described in the proof of Theorem 2 and in Proposition 15.

When $\xi \leqslant 2$, the second sum in (1-2) disappears and the derivative $B_M'(\xi)$ is explicitly computed in Lemma 17, yielding an explicit formula for the pair correlation density function $g_2^{\mathfrak{A}}(\xi) = dR_2^{\mathfrak{A}}(\xi)/d\xi$, which matches the graph in Figure 1.

Corollary 1. *For $0 < \xi \leqslant 2$ we have*

$$g_2^{\mathfrak{A}}\Big(\frac{3}{4\pi}\xi\Big) = \frac{16}{3\xi^2} \sum_{M \in \mathfrak{S}} \ln\bigg(\frac{\|M\|^2 + \sqrt{\|M\|^4 - 4}}{\|M\|^2 + \sqrt{\|M\|^4 - 4 - \xi^2}}\bigg).$$

A formula valid for $0 < \xi \leqslant 4$ is given in (8-11) after computing $A_{0,K}'(\xi)$.

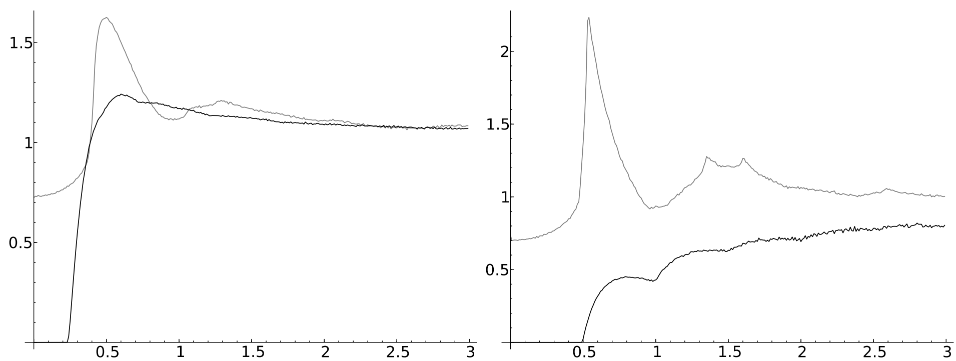


Figure 1. The pair correlation functions $g_2^{\mathfrak{T}}$ (left) and $g_2^{\mathfrak{A}}$ (right), plotted in gray, compared with the pair correlation function of Farey fractions with L^2 norm (left), and of the angles (with multiplicities) of lattice points in Euclidean balls (right). The graphs are obtained by counting the pairs in their definition, using $Q = 4000$, for which $B_Q = 6000203$. We used Magma [Bosma et al. 1997] for the numerical computations, and SAGE [Stein et al. 2012] for plotting the graphs.

The computation is performed in Section 8.2, and it identifies the first spike in the graph of $g_2^{\mathfrak{A}}(x)$ at $x=(3/4\pi)\sqrt{5}$. A proof of an explicit formula for the pair correlation density $g_2^{\mathfrak{A}}(x)$ valid for all x, and working also when the point i is replaced by the other elliptic point $\rho=e^{\pi i/3}$, will be given in [Boca et al. 2013].

Since the series in Corollary 1 is dominated by the absolutely convergent sum $\sum_M \xi^2\|M\|^{-4}$, we can take the limit as $\xi\to 0$:

$$g_2^{\mathfrak{A}}(0)=\frac{2}{3}\sum_{M\in\mathfrak{S}}\left(\frac{\|M\|^2}{\sqrt{\|M\|^4-4}}-1\right)=0.7015\ldots$$

Remarkably, the previous two formulas, as well as (1-2) for $\xi\leqslant 2$, can be written geometrically as a sum over the primitive closed geodesics $\mathscr{C}$ on X which pass through the point $\Pi(i)$, where the summand depends only on the length $\ell(\mathscr{C})$:

$$g_2^{\mathfrak{A}}(0)=\frac{8}{3}\sum_{\mathscr{C}}\sum_{n\geqslant 1}\frac{1}{e^{n\ell(\mathscr{C})}-1}.$$

This is proved in Section 2, where we also give an arithmetic version based on an explicit description of the reciprocal geodesics $\mathscr{C}$ due to Sarnak [2007].

For the rest of the introduction we sketch the main ideas behind the proof, describing also the organization of the article. After reducing to angles in the first quadrant in Section 3, we show that the pair correlation of the quantities $\Psi(\gamma)=\tan(\theta_\gamma/2)$ is identical to that of $\Phi(\gamma)=\operatorname{Re}(\gamma i)$. We are led to estimating the cardinality of the set

$$\bigl\{(\gamma,\gamma')\in\Gamma_{\mathbf{I}}^2:\|\gamma\|,\|\gamma'\|\leqslant Q,\ \gamma'\neq\gamma,\ 0\leqslant Q^2(\Phi(\gamma')-\Phi(\gamma))\leqslant\xi\bigr\}.$$

For a matrix $\gamma=\left(\begin{smallmatrix}p' & p\\ q' & q\end{smallmatrix}\right)$ with nonnegative entries, $\|\gamma\|\leqslant Q$, and $q,q'>0$, consider the associated Farey interval $[p/q,\,p'/q']$, which contains $\Phi(\gamma)$. In Section 4, we break the set of pairs (γ,γ') above in two parts, depending on whether one of the associated Farey intervals contains the other, or the two intervals intersect at most at one endpoint. In the first case we have $\gamma=\gamma' M$ or $\gamma'=\gamma M$ with $M\in\mathfrak{S}$, while in the second we have a similar relation depending on the number ℓ of consecutive Farey fractions there are between the two intervals. The first case contributes to the series over $\mathfrak{S}$ in (1-2), while the second case contributes to the sum over K,ℓ. The triangle map T whose iterates define the piecewise linear functions $L_i(x,y)$, first introduced in [Boca et al. 2001], makes its appearance in the second case, being related to the denominator of the successor function for Farey fractions.

To estimate the number of pairs $(\gamma,\gamma M)$ in the first case, a key observation is that for each $M\in\Gamma$ there exists an explicit elementary function $\Xi_M(x,y)$, given by (5-1), such that

$$\Phi(\gamma)-\Phi(\gamma M)=\Xi_M(q',q)$$

for γ as above. Together with estimates for the number of points in two dimensional regions based on bounds on Kloosterman sums (Lemma 7), this allows us to estimate the number of pairs $(\gamma, \gamma M)$ with fixed $M \in \mathfrak{S}$, in terms of the volume of a three dimensional body $S_{M,\xi}$ given in (7-14). The absence of a gap beyond zero in the pair correlation measure arises as a result of this estimate. The details of the calculation are given in Section 7, leading to an explicit formula for $R_2^{\mathfrak{T}}$ (Theorem 2).

Finally in Section 8 we pass to the pair correlation of the angles θ_γ, obtaining the formulas of Theorem 1 and Corollary 1.

In this paper we focus on the full modular lattice centered at i, both because of the arithmetic connection with reciprocal geodesics, and because in this case the connection between unimodular matrices and Farey intervals is most transparent. It is this connection and the intuition provided by the repulsion of Farey fractions that guides our argument, and leads to the explicit formula for the pair correlation function, which is the first of this kind for hyperbolic lattices.

In a subsequent paper [Boca et al. 2013], we abstract some of this intuition and propose a *different* conjectural formula for the pair correlation function of an arbitrary lattice in $\mathrm{PSL}_2(\mathbb{R})$, centered at a point on the upper half plane, which we prove for the full level lattice centered at elliptic points. While the formula in that paper is more general, the method of proof, and the combinatorial-geometric intuition behind it, is reflected more accurately in the formula of Theorem 1: the infinite sum in the formula corresponds to pairs of matrices where there is no repulsion between their Farey intervals, while the finite sum corresponds to pairs of matrices where there is repulsion. The approach used in [Boca et al. 2013] builds on the estimates and method of the present paper.

A proof of that paper's conjecture by spectral methods has been proposed in a preprint by Kelmer and Kontorovich [2013]. By comparison, our approach is entirely elementary (using only standard bounds on Kloosterman sums), and via the repulsion argument it provides a natural way of approximating the pair correlation function. A key insight in the present paper, which is also the starting point of [Boca et al. 2013] and [Kelmer and Kontorovich 2013], is that instead of counting pairs $(\gamma, \gamma') \in \Gamma \times \Gamma$ in the definition of the pair correlation measure, we fix a matrix M, count pairs $(\gamma, \gamma M)$, and sum over M. The same approach may prove useful for the pair correlation problem for lattices in other groups as well.

2. Reciprocal geodesics on the modular surface

In this section we recall the definition of reciprocal geodesics and explain how the pair correlation of the angles they make with the imaginary axis is related to the pair correlation considered in the introduction. We also show that the sums over the semigroup $\mathfrak{S}$ appearing in the introduction can be expressed geometrically in terms of sums over primitive reciprocal geodesics. A description of the trajectory of reciprocal geodesics on the fundamental domain seems to have first appeared in the classical work of Fricke and Klein [1892, p.164], where it is shown that they consist of two closed loops, one the reverse of the other. There the terminology "sich selbst inverse Classe" is used for the equivalence classes of quadratic forms corresponding to reciprocal conjugacy classes of hyperbolic matrices.

Oriented closed geodesics on X are in one-to-one correspondence with conjugacy classes $\{\gamma\}$ of hyperbolic elements $\gamma \in \Gamma$. To a hyperbolic element $\gamma \in \Gamma$ one attaches its axis a_γ on $\mathbb{H}$, namely the semicircle whose endpoints are the fixed points of γ on the real axis. The part of the semicircle between z_0 and γz_0, for any $z_0 \in a_\gamma$, projects to a closed geodesic on X, with multiplicity one if and only if γ is a primitive matrix (not a power of another hyperbolic element of Γ). The group that fixes the semicircle a_γ (or equivalently its endpoints on the real axis) is generated by one primitive element γ_0.

We are concerned with (oriented) closed geodesics passing through $\Pi(i)$ on X. Since the axis of a hyperbolic element A passes through i if and only if A is symmetric, the closed geodesics passing through $\Pi(i)$ correspond to the set $\mathcal{R}$ of hyperbolic conjugacy classes $\{\gamma\}$ which contain a symmetric matrix. The latter are exactly the reciprocal geodesics considered in [Sarnak 2007], where only primitive geodesics are considered.

The reciprocal geodesics can be parametrized in a two-to-one manner by the set $\mathfrak{S} \subset \Gamma$, defined in the introduction, which consists of matrices distinct from the identity with nonnegative entries. To describe this correspondence, let $\mathcal{A} \subset \Gamma$ be the set of symmetric hyperbolic matrices with positive entries. Then we have maps

$$\mathfrak{S} \to \mathcal{A} \to \mathcal{R} \tag{2-1}$$

where the first map takes $\gamma \in \mathfrak{S}$ to $A = \gamma\gamma^t$, and the second takes the hyperbolic symmetric A to its conjugacy class $\{A\}$. The first map is bijective, while the second is two-to-one and onto, as follows from [Sarnak 2007]. More precisely, if $A = \gamma\gamma^t \in \mathcal{A}$ is a primitive matrix, then $B = \gamma^t\gamma \neq A$ is the only other matrix in $\mathcal{A}$ conjugate to A, and $\{A^n\} = \{B^n\}$ for all $n \geqslant 0$.

Note also that $\|\gamma\|^2 = \operatorname{Tr}(\gamma\gamma^t)$, and if A is hyperbolic with $\operatorname{Tr}(A) = T$, then the length of the geodesic associated to $\{A\}$ is $2 \ln N(A)$ with $N(A) = \frac{1}{2}(T + \sqrt{T^2 - 4})$.

Lemma 2. *Let $A \in \Gamma$ be a hyperbolic symmetric matrix and let $\gamma \in \Gamma$ such that $A = \gamma\gamma^t$. Then the point γi is halfway (in hyperbolic distance) between i and Ai on the axis of A.*

Proof. We have $d(i, \gamma i) = d(i, \gamma^t i) = d(\gamma i, Ai)$ where the first equality follows from the hyperbolic distance formula and the second since Γ acts by isometries on $\mathbb{H}$. Using formula (3-3), one checks that the angles of i, γi and i, Ai are equal, hence γi is indeed on the axis of A. $\square$

We can now explain the connection between the angles θ_γ in the first and second quadrant in Figure 2, and the angles made by the reciprocal geodesics with the image $\Pi(i \to i\infty) = \Pi(i \to 0)$. Namely, points in the first and second quadrant are parametrized by γi with $\gamma \in \mathfrak{S}$, and by the lemma the reciprocal geodesic corresponding to $A = \gamma\gamma^t \in \mathscr{A}$ consists of the loop $\Pi(i \to \gamma i)$, followed by $\Pi(i \to \gamma^t i)$ (which is the same as the reverse of the first loop). Therefore to each reciprocal geodesic corresponding to $A = \gamma\gamma^t \in \mathscr{A}$ correspond two angles, those attached to γi and $\gamma^t i$ in Figure 2, measured in the first or second quadrant so that all angles are between 0 and $\pi/2$.

In conclusion, the angles made by the reciprocal geodesics on X with the fixed direction $\Pi(i \to i\infty)$ consist of the angles in the first quadrant considered before, each appearing twice. Ordering the points γi in the first quadrant by $\|\gamma\|$ corresponds to ordering the geodesics by their length. Therefore the pair correlation measure of the angles of reciprocal geodesics is $2R_2^{\mathfrak{A}}(\xi/2)$, where $R_2^{\mathfrak{A}}$ was defined in the introduction.

The parametrization (2-1) of reciprocal geodesics allows one to rewrite the series appearing in the formula for $g_2^{\mathfrak{A}}(0)$ in the introduction, as a series over the primitive reciprocal classes $\mathscr{R}^{\text{prim}}$:

$$\sum_{M \in \mathfrak{S}} \left(\frac{\|M\|^2}{\sqrt{\|M\|^4 - 4}} - 1 \right) = \sum_{A \in \mathscr{A}} \frac{2}{N(A)^2 - 1} = 4 \sum_{\{\gamma\} \in \mathscr{R}^{\text{prim}}} \sum_{n \geqslant 1} \frac{1}{N(\gamma)^{2n} - 1},$$

where we have used the fact that for a hyperbolic matrix A of trace T we have

$$\sqrt{T^2 - 4} = N(A) - N(A)^{-1} \quad \text{and} \quad N(A^n) = N(A)^n.$$

One can rewrite the sum further using the arithmetic description of primitive reciprocal geodesics given in [Sarnak 2007]. Namely, let $\mathscr{D}_{\mathscr{R}}$ be the set of nonsquare positive discriminants $2^\alpha D'$ with $\alpha \in \{0, 2, 3\}$ and D' odd divisible only by primes $p \equiv 1 \pmod 4$. Then the set of primitive reciprocal classes $\mathscr{R}^{\text{prim}}$ decomposes as a disjoint union of finite sets:

$$\mathscr{R}^{\text{prim}} = \bigcup_{d \in \mathscr{D}_{\mathscr{R}}} \mathscr{R}_d^{\text{prim}},$$

with $|\mathscr{R}_d^{\text{prim}}| = \nu(d)$, the number of genera of binary quadratic forms of discriminant d. If $d \in \mathscr{D}_{\mathscr{R}}$ has exactly λ odd prime factors, $\nu(d)$ equals 2^λ if 8 divides d and $2^{\lambda-1}$ otherwise. Each class $\{\gamma\} \in \mathscr{R}_d^{\text{prim}}$ has

$$N(\gamma) = \alpha_d = \tfrac{1}{2}(u_0 + v_0\sqrt{d}),$$

with (u_0, v_0) the minimal positive solution to Pell's equation $u^2 - dv^2 = 4$. We then have

$$\sum_{\{\gamma\}\in\mathcal{R}^{\mathrm{prim}}} \sum_{n\geqslant 1} \frac{1}{N(\gamma)^{2n}-1} = \sum_{d\in\mathcal{D}_{\mathcal{R}}} \sum_{n\geqslant 1} \frac{\nu(d)}{\alpha_d^{2n}-1}.$$

In the same way, by Lemma 13 the pair correlation measure $R_2^{\mathfrak{T}}(\xi)$ in Theorem 1 can be written for $\xi \leqslant 1$ as a sum over classes $\{\gamma\} \in \mathcal{R}^{\mathrm{prim}}$, where each summand depends only on ξ and $N(\gamma)$.

3. Reduction to the first quadrant

In this section we establish notation in use throughout the paper, and we reduce the pair correlation problem to angles in the first quadrant. A similar reduction can be found in [Chamizo 2006], in the context of visibility problems for the hyperbolic lattice centered at i.

For each matrix $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$, define the quantities

$$X_g = a^2+b^2, \quad Y_g = c^2+d^2, \quad Z_g = ac+bd, \quad T_g = X_g+Y_g = \|g\|^2,$$
$$\Phi(g) = \mathrm{Re}(gi) = \frac{Z_g}{Y_g}, \quad \epsilon_g = \epsilon_{T_g} = \tfrac{1}{2}\big(T_g - \sqrt{T_g^2-4}\big). \tag{3-1}$$

The upper half-plane $\mathbb{H}$ is partitioned into four quadrants:

$$\mathbf{I} = \{z\in\mathbb{H} : \mathrm{Re}\, z > 0,\, |z|<1\}, \quad \mathbf{II} = \{z\in\mathbb{H} : \mathrm{Re}\, z > 0,\, |z|>1\},$$
$$\mathbf{III} = \{z\in\mathbb{H} : \mathrm{Re}\, z < 0,\, |z|>1\}, \quad \mathbf{IV} = \{z\in\mathbb{H} : \mathrm{Re}\, z < 0,\, |z|<1\}.$$

Note that all the points gi for $g\in\Gamma$ lie in one of the four *open* quadrants, with the exception of i itself. This follows from the relation

$$X_g Y_g - Z_g^2 = 1, \tag{3-2}$$

which will be often used.

In this section, simply take $X = X_g$, $Y = Y_g$, $Z = Z_g$, $\theta = \theta_g$. A direct calculation shows that the center of the circle through i and gi is $\alpha = (X-Y)/(2Z)$, leading to

$$\tan\theta_g = -\frac{1}{\alpha} = \frac{2Z_g}{Y_g - X_g} \quad \text{for all } \theta_g \in [-\pi, \pi].$$

Plugging this into

$$\tan\frac{\theta}{2} = \frac{\tan\theta}{1+\sqrt{1+\tan^2\theta}} \text{ if } |\theta| < \frac{\pi}{2} \quad\text{or}\quad \tan\frac{\theta}{2} = -\frac{1+\sqrt{1+\tan^2\theta}}{\tan\theta} \text{ if } \frac{\pi}{2} < |\theta| < \pi,$$

and employing (3-2) and the equivalences $|gi|<1 \iff X<Y$ and $\mathrm{Re}(\gamma i) > 0 \iff Z>0$, we find the useful formulas

$$\Psi(g) := \tan\frac{\theta_g}{2} = \frac{\sqrt{T_g^2-4}+X_g-Y_g}{2Z_g} = \frac{X_g-\epsilon_g}{Z_g} = \frac{Z_g}{Y_g-\epsilon_g} \tag{3-3}$$

for all $\theta_g \in [-\pi,\pi]$.

We set $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)$, $\tilde{\gamma} = \left(\begin{smallmatrix} d & c \\ b & a\end{smallmatrix}\right)$, $s = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0\end{smallmatrix}\right)$. Let $\gamma \in \Gamma$, $\gamma \neq I, s$. For γi to be in the right half-plane we need $\mathrm{Re}(\gamma i) > 0$. This is equivalent to $ac+bd > 0$, and implies that $ac \geqslant 0$ and $bd \geqslant 0$ because $abcd = bc + (bc)^2 \geqslant 0$. Since $ac \geqslant 0$, without loss of generality we will assume that $a \geqslant 0$ and $c \geqslant 0$ (otherwise consider $-\gamma$ instead). Without loss of generality, we will assume that $b \geqslant 0$, $d \geqslant 0$ as well (otherwise, we consider $-\gamma s = \left(\begin{smallmatrix} -b & a \\ -d & c\end{smallmatrix}\right)$ instead, since $\gamma i = \gamma s i$). Thus γ has only nonnegative entries.

If $a,b,c,d \geqslant 0$ and $ad-bc=1$, then c/a and d/b are both $\leqslant 1$ or both $\geqslant 1$ (since open intervals between consecutive Farey fractions are either nonintersecting or one contains the other). Since $\gamma i \in \mathbf{I} \iff a^2+b^2 < c^2+d^2$, it follows that both a/c and b/d are $\leqslant 1$ for $\gamma i \in \mathbf{I}$. We conclude that among the eight matrices $\pm\gamma$, $\pm\gamma s$, $\pm\tilde{\gamma}$, $\pm\tilde{\gamma}s$, which have symmetric angles (see Figure 2), the one for which γi is in quadrant $\mathbf{I}$ can be chosen such that

$$a,b,c,d \geqslant 0 \quad \text{and} \quad 0 \leqslant \frac{b}{d} < \frac{a}{c} \leqslant 1.$$

The set of such matrices γ is denoted $\Gamma_{\mathbf{I}}$.

Consider the subset $\mathfrak{R}_Q$ of $\Gamma_{\mathbf{I}}$ consisting of matrices with entries at most Q:

$$\mathfrak{R}_Q := \left\{ \begin{pmatrix} p' & p \\ q' & q \end{pmatrix} \in \Gamma : 0 \leqslant p, p', q, q' \leqslant Q,\ \frac{p}{q} < \frac{p'}{q'} \leqslant 1 \right\},$$

and its subset $\widetilde{\mathfrak{R}}_Q$ consisting of those γ with $\|\gamma\| \leqslant Q$. The cardinality B_Q of $\widetilde{\mathfrak{R}}_Q$ is estimated in Corollary 8 as $B_Q \sim 3Q^2/8$, in agreement with formula (58) in [Sarnak 2007] for the number of reciprocal geodesics of length at most $x = Q^2$.

Let $\mathscr{F}_Q$ be the set of Farey fractions p/q with $0 \leqslant p \leqslant q \leqslant Q$ and $(p,q)=1$. The *Farey tessellation* (Figure 3) consists of semicircles on the upper half-plane

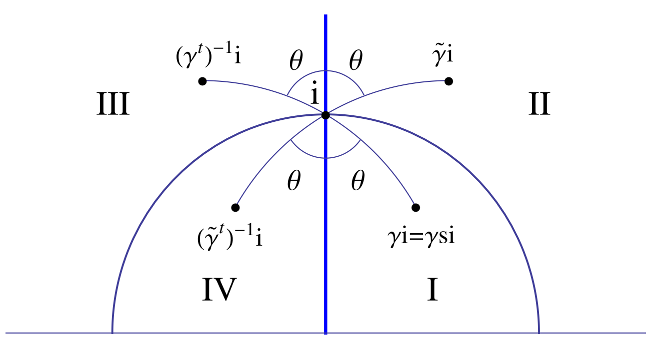


Figure 2. Two symmetric geodesics through i.

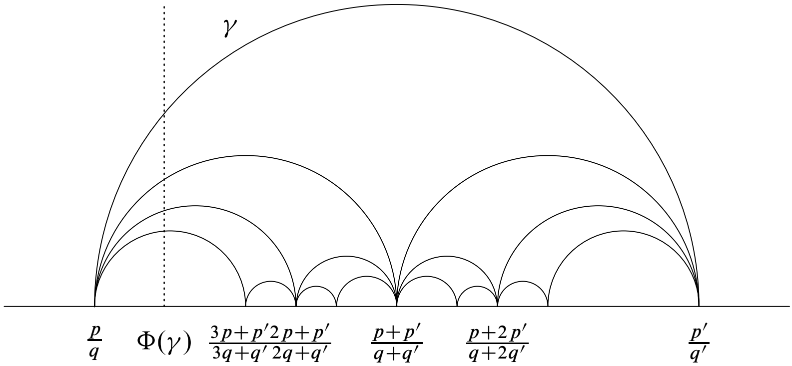


Figure 3. The Farey tessellation.

connecting Farey fractions $0 \leqslant p/q < p'/q' \leqslant 1$ with $p'q - pq' = 1$. We associate to matrices $\gamma \in \mathfrak{R}_Q$ with entries as above the arc in the Farey tessellation connecting p/q and p'/q', and conclude that

$$\#\mathfrak{R}_Q = 2\#\mathscr{F}_Q - 3 = \frac{Q^2}{\zeta(2)} + O(Q \ln Q).$$

4. The coincidence of the pair correlations of Φ and Ψ

In this section we show that the limiting pair correlations of the sets $\{\Psi(\gamma)\}$ and $\{\Phi(\gamma)\}$ ordered by $\|\gamma\| \to \infty$ do coincide. The proof uses properties of the Farey tessellation, via the correspondence between elements of $\mathfrak{R}_Q$ and arcs in the Farey tessellation defined at the end of Section 3.

For $\gamma = \left(\begin{smallmatrix} p' & p \\ q' & q \end{smallmatrix}\right)$, set $\gamma_- = p/q$, $\gamma_+ = p'/q'$. From (3-1), (3-3), and the inequalities $X_\gamma < Z_\gamma < Y_\gamma$, $2Y_\gamma > T_\gamma$ and $\epsilon_\gamma < 1/T_\gamma$, we have:

$$\Psi(\gamma) - \Phi(\gamma) = \frac{Z_\gamma}{Y_\gamma(\epsilon_\gamma^{-1} Y_\gamma - 1)} \ll \frac{1}{\|\gamma\|^4}, \tag{4-1}$$

$$\gamma_- < \Phi(\gamma) < \Psi(\gamma) < \gamma_+. \tag{4-2}$$

Denote by $\mathscr{R}_Q^{\Psi}(\xi)$ (resp. $\mathscr{R}_Q^{\Phi}(\xi)$) the number of pairs $(\gamma, \gamma') \in \widetilde{\mathfrak{R}}_Q^2$, $\gamma \neq \gamma'$, such that $0 \leqslant \Psi(\gamma) - \Psi(\gamma') \leqslant \xi/Q^2$ (resp. $0 \leqslant \Phi(\gamma) - \Phi(\gamma') \leqslant \xi/Q^2$). For fixed $\beta \in \left(\frac{2}{3}, 1\right)$, consider also

$$\mathcal{N}_{Q,\xi,\beta}^{\Psi} := \#\left\{(\gamma, \gamma') \in \widetilde{\mathfrak{R}}_Q^2 : Q^2|\Psi(\gamma) - \Psi(\gamma')| \leqslant \xi,\ \|\gamma\| \leqslant Q^\beta\right\},$$

and the similarly defined $\mathcal{N}_{Q,\xi,\beta}^{\Phi}$. The trivial inequality

$$\begin{aligned} \mathscr{R}_Q^{\Phi}(\xi) &\leqslant 2\mathcal{N}_{Q,\xi,\beta}^{\Phi} \\ &\quad + \#\left\{(\gamma, \gamma') \in \widetilde{\mathfrak{R}}_Q^2 : \gamma \neq \gamma',\ Q^2|\Phi(\gamma) - \Phi(\gamma')| \leqslant \xi,\ \|\gamma\|, \|\gamma'\| \geqslant Q^\beta\right\} \end{aligned}$$

and the estimate in (4-1) show that there exists a universal constant $\kappa > 0$ such that

$$\begin{aligned}\mathcal{R}_Q^{\Phi}(\xi) &\leqslant 2\mathcal{N}_{Q,\xi,\beta}^{\Phi} \\ &+ \#\big\{(\gamma,\gamma') \in \widetilde{\mathfrak{R}}_Q^2 : \gamma \neq \gamma',\ -2\kappa Q^{-4\beta} \leqslant \Psi(\gamma) - \Psi(\gamma') \leqslant \xi Q^{-2} + 2\kappa Q^{-4\beta}\big\},\end{aligned}$$

showing that

$$\mathcal{R}_Q^{\Phi}(\xi) \leqslant 2\mathcal{N}_{Q,\xi,\beta}^{\Phi} + \mathcal{R}_Q^{\Psi}(2\kappa Q^{2-4\beta}) + \mathcal{R}_Q^{\Psi}(\xi + 2\kappa Q^{2-4\beta}). \tag{4-3}$$

In a similar way we show that

$$\mathcal{R}_Q^{\Psi}(\xi) \leqslant 2\mathcal{N}_{Q,\xi,\beta}^{\Psi} + \mathcal{R}_Q^{\Phi}(2\kappa Q^{2-4\beta}) + \mathcal{R}_Q^{\Phi}(\xi + 2\kappa Q^{2-4\beta}). \tag{4-4}$$

We first prove that $\mathcal{N}_{Q,\xi,\beta}^{\Phi}$ and $\mathcal{N}_{Q,\xi,\beta}^{\Psi}$ are much smaller than Q^2. For this goal and for later use, it is important to divide pairs $(\gamma,\gamma') \in \mathfrak{R}_Q^2$ in three cases, depending on the relative position of their associated arcs in the Farey tessellation (it is well known that two arcs in the Farey tessellation are nonintersecting):

(i) The arcs corresponding to γ and γ' are *exterior*, i.e., $\gamma_+ \leqslant \gamma'_-$ or $\gamma'_+ \leqslant \gamma_-$.

(ii) $\gamma' \lesssim \gamma$, i.e., $\gamma_- \leqslant \gamma'_- < \gamma'_+ \leqslant \gamma_+$.

(iii) $\gamma \lesssim \gamma'$, i.e., $\gamma'_- \leqslant \gamma_- < \gamma_+ \leqslant \gamma'_+$.

Proposition 3. $\mathcal{N}_{Q,\xi,\beta}^{\Phi} \ll Q^{1+\beta} \ln Q$ *and* $\mathcal{N}_{Q,\xi,\beta}^{\Psi} \ll Q^{1+\beta} \ln Q$.

Proof. $\mathcal{N}_{Q,\xi,\beta}^{\Phi}$ and $\mathcal{N}_{Q,\xi,\beta}^{\Psi}$ are increasing as an effect of enlarging $\widetilde{\mathfrak{R}}_Q$ to $\mathfrak{R}_Q$, so for this proof we will replace $\widetilde{\mathfrak{R}}_Q$ by $\mathfrak{R}_Q$. We only consider $\mathcal{N}_{Q,\xi,\beta}^{\Phi}$ here. The proof for the bound on $\mathcal{N}_{Q,\xi,\beta}^{\Psi}$ is identical. Both rely on (4-1) and (4-2).

Set $K = [\xi] + 1$. From (4-2) and the fact that $|r' - r| \geqslant 1/Q^2$ for all $r, r' \in \mathcal{F}_Q$ such that $r \neq r'$, it follows that

$$\#(\mathcal{F}_Q \cap [\gamma_+, \gamma'_-]) \leqslant K + 1$$

if $\gamma_+ \leqslant \gamma'_-$ and $|\Phi(\gamma') - \Phi(\gamma)| \leqslant \xi/Q^2$. In particular, $\gamma'_- = \gamma_+$ when $0 < \xi < 1$.

We now consider the three cases listed before the statement of the proposition:

(i) The arcs corresponding to γ and γ' are exterior. Without loss of generality, assume that $\gamma_+ \leqslant \gamma'_-$. If i is such that $\gamma_+ = \gamma_i$, the i-th element of $\mathcal{F}_Q$, then

$$\gamma'_- = \gamma_{i+r} = \frac{p_{i+r}}{q_{i+r}}$$

for some r with $0 \leqslant r < K$. The equality $p'_+ q'_- - p'_- q'_+ = 1$ shows that if $\gamma'_- = p'_-/q'_-$ is fixed, then q'_+ (and therefore $\gamma'_+ = p'_+/q'_+$) is uniquely determined in intervals of length at most q'_-. Since $q'_\pm \leqslant Q$, it follows that the number of choices for q'_+ is actually at most $(Q/q'_-) + 1 = (Q/q_{i+r}) + 1$.

When $0 < \xi < 1$ one must have $\gamma'_- = \gamma_+$. Knowing q_- and q_+ would uniquely determine the matrix γ. Then there will be at most $(Q/q_+)+1$ choices for γ', so the total contribution of this case to $\mathcal{N}^{\Phi}_{Q,\xi,\beta}$ is at most

$$\sum_{1\leqslant q_-\leqslant Q^\beta} \sum_{1\leqslant q_+\leqslant Q^\beta} \Bigl(\frac{Q}{q_+}+1\Bigr) \ll Q^{1+\beta} \ln Q.$$

When $\xi \geqslant 1$ denote by $q_i, q_{i+1}, \dots, q_{i+K}$ the denominators of $\gamma_i, \gamma_{i+1}, \dots, \gamma_{i+K}$. Since $q_i < Q^\beta$, we have

$$\gamma_{i+K} - \gamma_i \leqslant \frac{K}{Q} \leqslant \frac{1}{Q^\beta} \leqslant \frac{1}{q_i} \leqslant 1-\gamma_i,$$

showing that $i+K < \#\mathcal{F}_Q$ so long as $Q \gg_\xi 1$. As noticed in [Hall and Tenenbaum 1984],

$$q_{j+2} = \Bigl[\frac{Q+q_j}{q_{j+1}}\Bigr] q_{j+1} - q_j.$$

As in [Boca et al. 2001], consider

$$\kappa(x, y) := \Bigl[\frac{1+x}{y}\Bigr] \quad \text{and} \quad \mathcal{T}_k = \{(x, y) \in (0, 1]^2 : x+y > 1, \kappa(x, y) = k\}.$$

Let Q be large enough so that $\delta_0 := Q^{\beta-1} < 1/(2K+3)$. Then $q_i/Q < \delta_0$, and it is plain (see also [ibid.]) that

$$\frac{q_{i+1}}{Q} > 1-\delta_0, \quad \kappa\Bigl(\frac{q_i}{Q}, \frac{q_{i+1}}{Q}\Bigr) = 1,$$

and

$$\kappa\Bigl(\frac{q_{i+1}}{Q}, \frac{q_{i+2}}{Q}\Bigr) = \cdots = \kappa\Bigl(\frac{q_{i+K}}{Q}, \frac{q_{i+K+1}}{Q}\Bigr) = 2,$$

because $q_{i+1}, q_{i+2}, \dots, q_{i+K+1}$ must form an arithmetic progression. Hence

$$\Bigl(\frac{q_i}{Q}, \frac{q_{i+1}}{Q}\Bigr) \in \mathcal{T}_1 \quad \text{and} \quad \Bigl(\frac{q_{i+1}}{Q}, \frac{q_{i+2}}{Q}\Bigr), \dots, \Bigl(\frac{q_{i+K}}{Q}, \frac{q_{i+K+1}}{Q}\Bigr) \in \mathcal{T}_2,$$

showing in particular that $\min\{q_{i+1}, \dots, q_{i+K}\} > Q/3$. Therefore, we find that $\max\{Q/q_{i+1}, \dots, Q/q_{i+K}\} < 3$, and the contribution of this case to $\mathcal{N}^{\Phi}_{Q,\xi,\beta}$ is at most

$$\sum_{1\leqslant q_-\leqslant Q^\beta} \sum_{1\leqslant q_+\leqslant Q^\beta} 4K \ll_\xi Q^{2\beta}.$$

(ii) $\gamma' \lessapprox \gamma$. Let i be the unique index for which $\gamma_i < \Phi(\gamma) < \gamma_{i+1}$ with $\gamma_i < \gamma_{i+1}$ successive elements in $\mathcal{F}_Q$. Since $|\Phi(\gamma') - \Phi(\gamma)| \leqslant \xi/Q^2$, either $\gamma'_- < \Phi(\gamma) < \gamma'_+$ or there exists $0 \leqslant r \leqslant K$ with $\gamma'_+ = \gamma_{i-r}$ or with $\gamma'_- = \gamma_{i+r}$. In both situations the arc corresponding to the matrix γ' will cross at least one of the vertical lines above $\gamma_{i-K}, \dots, \gamma_i, \gamma_{i+1}, \dots, \gamma_{i+K}$. A glance at the Farey tessellation provides an upper bound for this number $N_{\gamma,K}$ of arcs $\gamma' \in \mathfrak{R}_Q$. Actually, one sees that the set $\mathcal{C}_{\gamma,L}$ consisting of $2+2^2+\cdots+2^L$ arcs obtained from γ by iterating the mediant construction $L = [Q/\min\{q_-, q_+\}] + 1$ times (γ is not enclosed in $\mathscr{C}_{\gamma,L}$) contains the set $\{\gamma' \in \mathfrak{R}_Q : \gamma' \lessapprox \gamma, \gamma' \neq \gamma\}$. The former set contains at most L arcs that are intersected by each vertical direction, and so $N_{\gamma,K} \leqslant (2K+1)L$. Therefore, the contribution of this case to $\mathscr{N}^{\Phi}_{Q,\xi,\beta}$ is (first choose γ, then γ') at most

$$\sum_{1\leqslant q\leqslant Q^\beta} \sum_{1\leqslant q'\leqslant Q^\beta} (2K+1)\Big(\frac{Q}{\min\{q,q'\}}+1\Big) \ll_\xi Q^{1+\beta}\ln Q.$$

(iii) $\gamma \lessapprox \gamma'$. We necessarily have $\gamma = \gamma' M$, with $M \in \mathfrak{S}$. In particular, this yields $\gamma'_\pm \in \mathscr{F}_{Q^\beta}$. Considering the subtessellation defined only by arcs connecting points from $\mathscr{F}_{Q^\beta}$, one sees that the number of arcs intersected by a vertical line $x = \alpha$ with

$$\gamma_- = \frac{p}{q} < \alpha < \gamma_+ = \frac{p'}{q'}, \quad \text{where } \gamma = (\gamma_-, \gamma_+) \in \mathscr{F}_{Q^\beta},$$

is equal to $s(q,q')$, the sum of digits in the continued fraction expansion of $q/q' < 1$ when $q < q'$, and respectively to $s(q',q)$ when $q' < q$. A result from [Yao and Knuth 1975] yields in particular that

$$\sum_{0<q<q'\leqslant Q^\beta} s(q,q') \ll Q^{2\beta}\ln^2 Q,$$

and therefore

$$\#\{(\gamma,\gamma') \in \mathfrak{R}^2_{Q^\beta} : \gamma \lessapprox \gamma'\} \leqslant 1 + 2\sum_{0<q<q'\leqslant Q^\beta} s(q,q') \ll Q^{2\beta}\ln^2 Q.$$

This completes the proof of the proposition. □

Proposition 3 and inequalities (4-3) and (4-4) imply:

Corollary 4. *For each* $\beta \in \big(\frac{2}{3}, 1\big)$,

$$\mathscr{R}^{\Psi}_Q(\xi) = \mathscr{R}^{\Phi}_Q\big(\xi + O_\xi(Q^{2-3\beta})\big) + \mathscr{R}^{\Phi}_Q\big(O_\xi(Q^{2-3\beta})\big) + O_\xi(Q^{1+\beta}\ln Q).$$

5. A decomposition of the pair correlation of $\{\Phi(\gamma)\}$

To estimate $\mathscr{R}^{\Phi}_Q(\xi)$, recall the correspondence between elements of $\mathfrak{R}_Q$ and arcs in the Farey tessellation from the end of Section 3. We consider the following two possibilities for the arcs associated to a pair $(\gamma,\gamma') \in \widetilde{\mathfrak{R}}^2_Q$:

(i) One of the arcs corresponding to γ and γ' contains the other.

(ii) The arcs corresponding to γ and γ' are exterior (possibly tangent).

Denoting by $R^{\Cap}_Q(\xi)$ and $R^{\cap\cap}_Q(\xi)$ the number of pairs in each case, we have

$$\mathscr{R}^{\Phi}_Q(\xi) = R^{\Cap}_Q(\xi) + R^{\cap\cap}_Q(\xi).$$

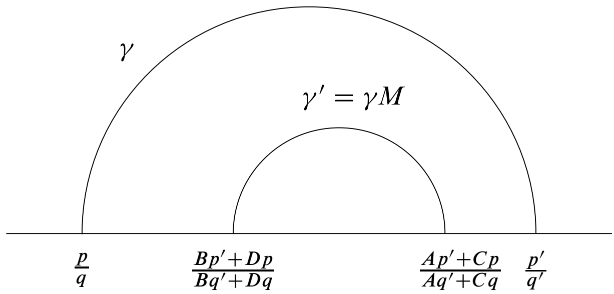


Figure 4. The case $\gamma' \lessapprox \gamma$.

5.1. ***One of the arcs contains the other.*** In this case we have either $\gamma = \gamma' M$ or $\gamma' = \gamma M$ with $M \in \mathfrak{S}$ (see also Figure 4). For each $M \in \Gamma$ define

$$\Xi_M(x, y) = \frac{xy(Y_M - X_M) + (x^2 - y^2)Z_M}{(x^2 + y^2)(x^2 X_M + y^2 Y_M + 2xyZ_M)}, \tag{5-1}$$

where X_M, Y_M, Z_M are defined in (3-1). For $\gamma = \left(\begin{smallmatrix} p' & p \\ q' & q \end{smallmatrix}\right)$, a direct calculation shows

$$\Phi(\gamma) - \Phi(\gamma M) = \Xi_M(q', q). \tag{5-2}$$

Two remarks are in order now. First, notice that $X_M \neq Y_M$ for any $M \in \mathfrak{S}$ because of (3-2) and since $X_M, Y_M, Z_M \geqslant 1$. Secondly, we also have

$$\Phi(\gamma) \neq \Phi(\gamma M). \tag{5-3}$$

Suppose, ad absurdum, that $\Phi(\gamma) = \Phi(\gamma M)$. Then (5-2) and (5-1) yield

$$\frac{2Z_M}{Y_M - X_M} = \frac{2qq'}{q^2 - q'^2},$$

that is, $\tan \theta_M = \tan 2\theta$, where $\theta = \tan^{-1}(q'/q) \in (0, \pi)$ and $\theta_M \in (0, \pi)$ because $Z_M > 0$. This gives

$$\frac{X_M - \epsilon_M}{Z_M} = \tan\left(\frac{\theta_M}{2}\right) = \tan \theta \in \mathbb{Q},$$

hence $\sqrt{(X_M + Y_M)^2 - 4} = X_M + Y_M - 2\epsilon_M \in \mathbb{Q}$, which is not possible because $X_M + Y_M \geqslant 3$.

From (5-2) and (5-3) we now infer:

Lemma 5. *Using the notation introduced before Proposition 3, the number of pairs $(\gamma, \gamma') \in \widetilde{\mathfrak{R}}_Q^2$, $\gamma \neq \gamma'$, with $0 \leqslant \Phi(\gamma) - \Phi(\gamma') \leqslant \xi/Q^2$ and $\gamma \lessapprox \gamma'$ or $\gamma' \lessapprox \gamma$, is given by*

$$R_Q^{\Cap}(\xi) = \#\left\{(\gamma, \gamma M) \in \widetilde{\mathfrak{R}}_Q^2 : \gamma = \begin{pmatrix} p' & p \\ q' & q \end{pmatrix},\ M \in \mathfrak{S},\ |\Xi_M(q', q)| \leqslant \frac{\xi}{Q^2}\right\}.$$

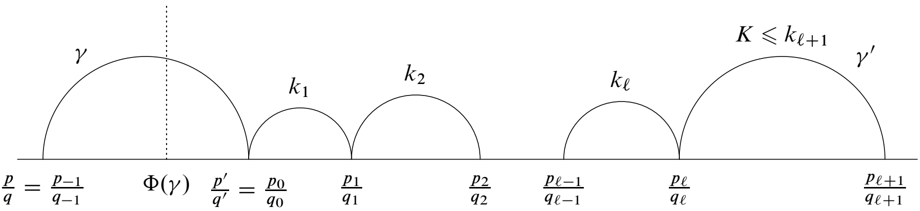


Figure 5. The case where γ and γ' are exterior.

5.2. ***Exterior arcs.*** In this case we have $\gamma, \gamma' \in \widetilde{\mathfrak{R}}_Q$, $\gamma'_- \geqslant \gamma_+$. Let $\ell \geqslant 0$ be the number of Farey arcs in $\mathscr{F}_Q$ connecting the arcs corresponding to γ, γ' (see Figure 5). In other words, writing $\gamma = \left(\begin{smallmatrix} p' & p \\ q' & q \end{smallmatrix}\right)$ and $\gamma' = \left(\begin{smallmatrix} p_{\ell+1} & p_\ell \\ q_{\ell+1} & q_\ell \end{smallmatrix}\right)$, we have that $p_0/q_0 := p'/q'$, $p_1/q_1, \ldots, p_\ell/q_\ell$ are consecutive elements in $\mathscr{F}_Q$. Setting also $p_{-1}/q_{-1} := p/q$, it follows that $q_i = k_i q_{i-1} - q_{i-2}$, where $k_i \in \mathbb{N}$, $i = 1, \ldots, \ell$, and

$$k_i = \left[\frac{Q + q_{i-2}}{q_{i-1}}\right] \quad \text{for } 2 \leqslant i \leqslant \ell.$$

The fractions p_ℓ/q_ℓ and $p_{\ell+1}/q_{\ell+1}$ are not necessarily consecutive in $\mathscr{F}_Q$, but we have $q_{\ell+1} = K q_\ell - q_{\ell-1}$,

$$K \leqslant k_{\ell+1} = \left[\frac{Q + q_\ell}{q_{\ell+1}}\right].$$

It follows that $\gamma' = \gamma M$ with

$$M = \begin{pmatrix} k_1 & 1 \\ -1 & 0 \end{pmatrix} \cdots \begin{pmatrix} k_\ell & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} K & 1 \\ -1 & 0 \end{pmatrix}.$$

We have $\ell < \xi$ because

$$\Phi(\gamma') - \Phi(\gamma) > \sum_{i=1}^{\ell} \frac{1}{q_{i-1} q_i} \geqslant \frac{\ell}{Q^2}.$$

It is also plain to see that

$$\frac{p'}{q'} - \Phi(\gamma) = \frac{q}{q'(q^2 + q'^2)}, \qquad \Phi(\gamma') - \frac{p_\ell}{q_\ell} = \frac{q_{\ell+1}}{q_\ell (q_\ell^2 + q_{\ell+1}^2)}. \tag{5-4}$$

The last equality in (5-4) and $q_\ell^2 + q_{\ell+1}^2 \leqslant Q^2$ yield, for $\ell \geqslant 1$,

$$\begin{aligned} \frac{\xi}{Q^2} \geqslant \Phi(\gamma') - \Phi(\gamma) &\geqslant \frac{1}{q_{\ell-1} q_\ell} + \frac{q_{\ell+1}}{q_\ell (q_\ell^2 + q_{\ell+1}^2)} \\ &\geqslant \frac{1}{q_{\ell-1} q_\ell} + \frac{K q_\ell - q_{\ell-1}}{q_\ell Q^2} = \frac{K}{Q^2} + \frac{Q^2 - q_{\ell-1}^2}{q_{\ell-1} q_\ell Q^2} \geqslant \frac{K}{Q^2}, \end{aligned}$$

while if $\ell = 0$ we have

$$\Phi(\gamma') - \Phi(\gamma) = \frac{K(q'^2 + q q_1)}{(q^2 + q'^2)(q'^2 + q_1^2)} \geqslant \frac{K}{Q^2},$$

showing that $K < \xi$. Notice also that (5-4) yields

$$\Phi(\gamma') - \Phi(\gamma) = \frac{q}{q'(q^2+q'^2)} + \sum_{i=1}^{\ell} \frac{1}{q_{i-1}q_i} + \frac{q_{\ell+1}}{q_\ell(q_\ell^2+q_{\ell+1}^2)}.$$

Let $\mathcal{T} = \{(x, y) \in (0, 1]^2 : x + y > 1\}$ and consider the map

$$T : (0, 1]^2 \to \mathcal{T}, \quad T(x, y) = \Big(y, \Big[\frac{1+x}{y}\Big]y - x\Big),$$

whose restriction to $\mathcal{T}$ is bijective and area-preserving [Boca et al. 2001]. Consider the iterates $T^i = (L_{i-1}, L_i)$ and the functions $K_i = [(1+L_{i-2})/L_{i-1}]$ if $i = 1, \dots, \ell$, $K_{\ell+1} = K$, and $L_{\ell+1} = K L_\ell - L_{\ell-1}$. One has:

$$\begin{aligned}
&\bullet\ L_{-1}(x, y) = x \text{ and } L_0(x, y) = y \text{ for } (x, y) \in (0, 1]^2;\\
&\bullet\ 0 < L_i(x, y) \leqslant 1 \text{ for } i \geqslant 0 \text{ and } (x, y) \in \mathcal{T};\\
&\bullet\ L_{i-1}(x, y) + L_i(x, y) > 1 \text{ for } i = 1, \dots, \ell \text{ and } (x, y) \in \mathcal{T};\\
&\bullet\ L_i(x, y) = K_i(x, y)L_{i-1}(x, y) - L_{i-2}(x, y)\\
&\qquad\qquad \text{for } i = 1, \dots, \ell+1 \text{ and } (x, y) \in \mathcal{T};\\
&\bullet\ (q_{i-1}, q_i) = QT^i\Big(\frac{q}{Q}, \frac{q'}{Q}\Big)\\
&\qquad\qquad = \Big(QL_{i-1}\Big(\frac{q}{Q}, \frac{q'}{Q}\Big), QL_i\Big(\frac{q}{Q}, \frac{q'}{Q}\Big)\Big) \text{ for } i = 0, 1, \dots, \ell;\\
&\bullet\ q_{\ell+1} = Kq_\ell - q_{\ell-1} = Q\Big(KL_\ell\Big(\frac{q}{Q}, \frac{q'}{Q}\Big) - L_{\ell-1}\Big(\frac{q}{Q}, \frac{q'}{Q}\Big)\Big).
\end{aligned} \tag{5-5}$$

Define also the function $\Upsilon_{\ell,K} : (0, 1]^2 \to (0, \infty)$ by

$$\Upsilon_{\ell,K} = \frac{L_{-1}}{L_0(L_{-1}^2+L_0^2)} + \sum_{i=1}^{\ell} \frac{1}{L_{i-1}L_i} + \frac{L_{\ell+1}}{L_\ell\big(L_\ell^2+L_{\ell+1}^2\big)}. \tag{5-6}$$

We have proved the following statement:

Lemma 6. *The number $R_Q^{\cap\cap}(\xi)$ of pairs (γ, γ') of exterior (possibly tangent) arcs in $\widetilde{\mathfrak{R}}_Q$ for which $0 < \Phi(\gamma') - \Phi(\gamma) \leqslant \xi/Q^2$ is given by*

$$R_Q^{\cap\cap}(\xi) = \sum_{\substack{\ell\in[0,\xi)\\ K\in[1,\xi)}} d_{\ell K},$$

where the sums are over integers in the given intervals, $d_{\ell K}$ is the number of matrices $\left(\begin{smallmatrix} p' & p\\ q' & q\end{smallmatrix}\right)$ such that the following hold:

$$\begin{gathered}0 \leqslant p \leqslant q, \quad 0 \leqslant p' \leqslant q', \quad p'q - pq' = 1, \\ p^2 + p'^2 + q^2 + q'^2 \leqslant Q^2, \quad 0 < Kq_\ell - q_{\ell-1} \leqslant Q, \\ p_\ell^2 + q_\ell^2 + (Kp_\ell - p_{\ell-1})^2 + (Kq_\ell - q_{\ell-1})^2 \leqslant Q^2, \\ \Upsilon_{\ell,K}\big(q/Q, q'/Q\big) \leqslant \xi,\end{gathered} \tag{5-7}$$

and $q_{-1} = q$, $q_0 = q'$.

6. A lattice point estimate

Lemma 7. *Suppose that* Ω *is a region in* $\mathbb{R}^2$ *of area* $A(\Omega)$ *and rectifiable boundary of length* $\ell(\partial\Omega)$. *For any integer* r *with* $(r, q) = 1$ *and* $1 \leqslant L \leqslant q$, *we have*

$$\mathcal{N}_{\Omega,q,r} := \#\big\{(a, b) \in \Omega \cap \mathbb{Z}^2 : ab \equiv r \pmod q\big\} = \frac{\varphi(q)}{q^2} A(\Omega) + \mathscr{E}_{\Omega,L,q},$$

where, for each $\varepsilon > 0$,

$$\mathscr{E}_{\Omega,L,q} \ll_\varepsilon \frac{q^{1/2+\varepsilon} A(\Omega)}{L^2} + \left(1 + \frac{\ell(\partial\Omega)}{L}\right)\left(\frac{L^2}{q} + q^{1/2+\varepsilon}\right).$$

Proof. Replacing $\mathbb{Z}^2$ by $L\mathbb{Z}^2$ in the estimate

$$\big\{(m, n) \in \mathbb{Z}^2 : (m, m+1) \times (n, n+1) \cap \partial\Omega \neq \varnothing\big\} \ll 1 + \ell(\partial\Omega),$$

(for a proof see [Narkiewicz 1983, Theorem 5.9]) we find that the number of squares $S_{m,n} = [Lm, L(m+1)] \times [Ln, L(n+1)]$ such that $\mathring{S}_{m,n} \cap \partial\Omega$ is nonempty is $\ll 1 + (1/L)\ell(\partial\Omega)$. Therefore

$$\#\big\{(m, n) \in \mathbb{Z}^2 : (Lm, L(m+1)) \times (Ln, L(n+1)) \subseteq \Omega\big\} = \frac{A(\Omega)}{L^2} + O\Big(1 + \frac{\ell(\partial\Omega)}{L}\Big).$$

Weil's estimates [1948] on Kloosterman sums, extended to composite moduli in [Hooley 1957] and [Estermann 1961], show that each such square contains $(\varphi(q)/q^2)L^2 + O_\varepsilon(q^{1/2+\varepsilon})$ pairs of integers (a, b) with $ab \equiv r \pmod q$ (see, e.g., [Boca et al. 2000, Lemma 1.7] for details). Combining these two estimates, we find

$$\mathcal{N}_{\Omega,q,r} = \left(\frac{A(\Omega)}{L^2} + O\Big(1 + \frac{\ell(\partial\Omega)}{L}\Big)\right)\left(\frac{\varphi(q)}{q^2}L^2 + O\big(q^{1/2+\varepsilon}\big)\right) = \frac{\varphi(q)}{q^2}A(\Omega) + \mathscr{E}_{\Omega,q,L},$$

as desired. $\square$

Corollary 8.
$$\#\widetilde{\mathfrak{R}}_Q = \frac{3Q^2}{8} + O_\varepsilon(Q^{11/6+\varepsilon}).$$

Proof. Note first that one can substitute pq'/q for $p' = (1 + pq')/q$ in the definition of $\widetilde{\mathfrak{R}}_Q$, replacing the inequality $\|\gamma\|^2 \leqslant Q^2$ by $(q^2 + q'^2)(q^2 + p^2) \leqslant Q^2q^2$, without altering the error term. Applying Lemma 7 with

$$\Omega_q = \{(u, v) \in [0, q] \times [0, Q] : (q^2 + u^2)(q^2 + v^2) \leqslant Q^2q^2\} \quad \text{and} \quad L = q^{5/6},$$

and using $A(\Omega_q) \leqslant Qq$ and $\ell(\Omega_q) \leqslant 2(Q+q) \leqslant 4Q$, we infer that

$$\#\widetilde{\mathfrak{R}}_Q = \sum_{q=1}^{Q} \frac{\varphi(q)}{q} \cdot \frac{A(\Omega_q)}{q} + O_\varepsilon(Q^{11/6+\varepsilon}).$$

Standard Möbius summation (see, e.g., [Boca et al. 2000, Lemma 2.3]) applied to the decreasing function $h(q) = (1/q)A(\Omega_q)$ with $\|h\|_\infty \leqslant Q$ and the change of variable $(q, u, v) = (Qx, Qxy, Qz)$ further yield

$$\#\widetilde{\mathfrak{R}}_Q = \frac{Q^2}{\zeta(2)} \operatorname{Vol}(S) + O_\varepsilon(Q^{11/6+\varepsilon}),$$

where

$$S = \{(x, y, z) \in [0, 1]^3 : (1 + y^2)(x^2 + z^2) \leqslant 1\}.$$

The substitution $y = \tan\theta$ yields

$$\operatorname{Vol}(S) = \int_0^{\pi/4} \frac{d\theta}{\cos^2\theta} A\big(\{(x, z) \in [0, 1]^2 : x^2 + z^2 \leqslant \cos^2\theta\}\big) = \frac{\pi^2}{16},$$

completing the proof of the corollary. □

The error bound in Corollary 8 can be improved using spectral methods (see Corollary 12.2 in [Iwaniec 2002]). We have given the proof since it is the prototype of applying Lemma 7 to the counting problems of the next section.

7. Pair correlation of $\{\Phi(\gamma)\}$

The main result of this section is Theorem 2, where we obtain explicit formulas for the pair correlation of the quantities $\{\Phi(\gamma)\}$ in terms of volumes of three-dimensional bodies. The discussion is divided in two cases, as in Section 5.

7.1. ***One of the arcs contains the other.*** The formula for $R_Q^{\Cap}$ in Lemma 5 provides

$$R_Q^{\Cap}(\xi) = \sum_{M \in \mathfrak{S}} \mathcal{N}_{M,Q}(\xi), \tag{7-1}$$

where $\mathcal{N}_{M,Q}(\xi)$ denotes the number of matrices $\gamma = \left(\begin{smallmatrix} p' & p \\ q' & q \end{smallmatrix}\right)$ for which

$$0 \leqslant p \leqslant q, \quad 0 \leqslant p' \leqslant q', \quad p'q - pq' = 1, \quad |\Xi_M(q', q)| \leqslant \frac{\xi}{Q^2}, \quad \|\gamma M\| \leqslant Q. \tag{7-2}$$

The first goal is to replace in (7-2) the inequality $\|\gamma M\| \leqslant Q$ by a more tractable one. Taking γ of the given form and substituting $p = (p'q - 1)/q'$ we write, using the notation from (3-1):

$$\|\gamma M\|^2 = \left(\frac{p'^2}{q'^2} + 1\right)\left(q'^2 X_M + q^2 Y_M + 2qq' Z_M\right) - \frac{(p'q + pq')Y_M + 2p'q' Z_M}{q'^2}. \tag{7-3}$$

The quantity $\mathcal{N}_{M,Q}(\xi)$ can be conveniently related to $\tilde{\mathcal{N}}_{M,Q}(\xi)$, the number of integer triples (q', q, p') such that

$$\begin{gathered} 0 < p' \leqslant q' \leqslant Q, \quad 0 < q \leqslant Q, \quad p'q \equiv 1 \pmod{q'}, \\ |\Xi_M(q', q)| \leqslant \frac{\xi}{Q^2}, \quad Y_{\gamma M} = q'^2 X_M + q^2 Y_M + 2qq' Z_M \leqslant \frac{Q^2 q'^2}{p'^2 + q'^2}. \end{gathered} \tag{7-4}$$

We next prove that, given $c_0 \in \left(\frac{1}{2}, 1\right)$, for all $M \in \mathfrak{S}$ and $Q \geqslant 1$ with $Y_M < X_M \leqslant Q^{2c_0}$ and all $\xi > 0$,

$$\tilde{\mathcal{N}}_{M,Q}(\xi) \leqslant \mathcal{N}_{M,Q}(\xi) \leqslant \tilde{\mathcal{N}}_{M,Q(1+\sqrt{2}Q^{c_0-1})}\big(\xi(1+\sqrt{2}Q^{c_0-1})^2\big). \tag{7-5}$$

For the first inequality, note that if the integral triple (q', q, p') satisfies (7-4) then by (7-3) we have

$$\|\gamma M\|^2 \leqslant \frac{p'^2 + q'^2}{q'^2} Y_{\gamma M} \leqslant Q^2,$$

and thus if we define $p := (p'q - 1)/q'$ then (7-2) holds. For the second inequality, take γ as in (7-2). Using (7-3) we then have

$$\frac{p'^2 + q'^2}{q'^2} Y_{\gamma M} \leqslant Q^2 + \frac{(p'q + pq')Y_M + 2p'q'Z_M}{q'^2} \leqslant Q^2 + 2qY_M + 2Z_M.$$

Using also that $Z_M \leqslant Q^{2c_0}$ and $qY_M = \sqrt{q^2 Y_M}\sqrt{Y_M} \leqslant \sqrt{Y_{\gamma M}}\sqrt{Y_M} \leqslant Q^{1+c_0}$, we conclude that

$$\frac{p'^2 + q'^2}{q'^2} Y_{\gamma M} \leqslant Q^2 + 2Q^{1+c_0} + 2Q^{2c_0} \leqslant Q^2(1+\sqrt{2}Q^{c_0-1})^2.$$

Also

$$|\Xi_M(q', q)| \leqslant \frac{\xi}{Q^2} = \frac{\xi(1+\sqrt{2}Q^{c_0-1})^2}{Q^2(1+\sqrt{2}Q^{c_0-1})^2}.$$

Hence (q', q, p') satisfies (7-4) with the pair (Q, ξ) replaced by $(Q + \sqrt{2}\,Q^{c_0}, \xi(1+\sqrt{2}\,Q^{c_0-1})^2)$. This proves (7-5).

Next we show that $\mathcal{N}_{M,Q}(\xi)$ vanishes when $\max\{X_M, Y_M\} \geqslant Q^{2c_0}$ and Q is large enough.

Lemma 9. *Let $c_0 \in \left(\frac{1}{2}, 1\right)$. There exists $Q_0(\xi)$ such that whenever $M \in \mathfrak{S}$, $\max\{X_M, Y_M\} \geqslant Q^{2c_0}$, and $Q \geqslant Q_0(\xi)$,*

$$\mathcal{N}_{M,Q}(\xi) = \tilde{\mathcal{N}}_{M,Q}(\xi) = 0.$$

Proof. We show there are no coprime positive integer lattice points (q', q) for which

$$|\Xi_M(q', q)| \leqslant \frac{\xi}{Q^2}, \quad Y_{\gamma M} = q'^2 X_M + q^2 Y_M + 2qq' Z_M \leqslant Q^2. \tag{7-6}$$

Noting from (7-3) that $Y_{\gamma M} \leqslant \|\gamma M\|^2$, this will ensure that $\mathcal{N}_{M,Q}(\xi) = 0$. The equality $\tilde{\mathcal{N}}_{M,Q}(\xi) = 0$ follows as well from (7-4).

Suppose (q', q) is as in (7-6), write $q'i + q = (q, q') = (r\cos\theta, r\sin\theta)$, $\theta \in (0, \pi/2)$, and consider $(X, Y, Z) = (X_M, Y_M, Z_M)$, $T = \|M\|^2 = X + Y$, and $U_M = \coth d(i, Mi) = T/\sqrt{T^2-4}$. Since

$$\sin\theta_M = \frac{2Z}{\sqrt{T^2-4}} \quad \text{and} \quad \cos\theta_M = \frac{Y-X}{\sqrt{T^2-4}},$$

the inequalities in (7-6) can be described as

$$\frac{1}{\xi}\cdot\frac{|\sin(\theta_M - 2\theta)|}{U_M + \cos(\theta_M - 2\theta)} \leqslant \frac{r^2}{Q^2} \leqslant \frac{2}{\big(U_M + \cos(\theta_M - 2\theta)\big)\sqrt{T^2-4}}. \tag{7-7}$$

Denoting $\delta_M = \theta_M/2 - \theta$, from the first and last fraction in (7-7) we infer $|\sin 2\delta_M| \ll 1/T$. Therefore δ_M is close to 0, or to $\pm\pi/2$. When δ_M is close to 0 we have

$$|\tan\delta_M| \ll |\delta_M| \ll |\sin 2\delta_M| \ll \frac{1}{T}.$$

When δ_M is close to $\pm\pi/2$ we similarly have $|\delta_M \mp \pi/2| \ll \frac{1}{T}$, which is seen to be impossible. Indeed, the inequality

$$\frac{|\tan\delta_M|}{1 + \dfrac{U_M - 1}{1+\cos 2\delta_M}} = \frac{|\sin 2\delta_M|}{U_M + \cos 2\delta_M} \leqslant \xi$$

shows that it suffices to bound from above $(U_M - 1)/(1+\cos 2\delta_M)$, which would imply that $|\tan\delta_M| \ll \xi$, thus contradicting $|\delta_M \mp \frac{\pi}{2}| \ll 1/T$. Since Z is a positive integer, we have $\sin\theta_M \gg 1/T$. Since $\cos\theta, \sin\theta > 0$ and $\theta_M \in (0, \pi)$, we have

$$\begin{aligned} 1 + \cos 2\delta_M = 1 + \cos(\theta_M - 2\theta) &\geqslant 1 + \cos 2\theta\cos\theta_M \\ &\geqslant 1 - |\cos\theta_M| = 1 - \sqrt{1 - \sin^2\theta_M} \gg \frac{1}{T^2}. \end{aligned}$$

As $U_M - 1 \ll 1/T^2$, it follows that $(U_M - 1)/(1+\cos 2\delta_M) \ll 1$, a contradiction.

We have thus shown that $|\delta_M| \leqslant |\tan\delta_M| \ll 1/T$; more precisely, there exists a function $\Theta_0(\xi)$, continuous in ξ, such that $|\delta_M| \leqslant \Theta_0(\xi)/T$.

Case I: $Y > X$. Then $0 < \theta_M/2 < \pi/4$ and $Z = \sqrt{XY - 1} < Y$. Since

$$|\delta_M| \ll \frac{1}{T} \ll Q^{-2c_0},$$

one has $0 < \theta < \pi/3$ for large Q. Employing the formula $\tan(\theta_M/2) = Z/(Y - \epsilon_T)$ with ϵ_T as in (3-1), we infer

$$\left|\frac{AC+BD}{C^2+D^2-\epsilon_T} - \frac{q'}{q}\right| = |\tan\delta_M|\cdot\left|1 + \tan\theta\,\tan\frac{\theta_M}{2}\right| \ll \frac{1}{T}. \tag{7-8}$$

Combining (7-8) with

$$0 < \frac{Z}{Y-\epsilon_T} - \frac{Z}{Y} \ll \frac{1}{T} \quad \text{and} \quad \left|\frac{Z}{Y} - \frac{A+B}{C+D}\right| \leqslant \frac{1}{C^2+D^2} \ll \frac{1}{T},$$

we arrive at

$$\left|\frac{A+B}{C+D} - \frac{q'}{q}\right| \ll \frac{1}{T} \leqslant Q^{-2c_0}. \tag{7-9}$$

If nonzero, the left-hand side in (7-9) must be at least $1/q(C+D)$. But

$$q(C+D) \leqslant q\sqrt{2(C^2+D^2)} \leqslant Q\sqrt{2},$$

and so $Q^{2c_0} \ll Q$, a contradiction. The remaining case, in which $q = C+D$ and $q' = A+B$, is not possible because $Q^{2c_0} \leqslant (C+D)^2 = q(C+D) \leqslant Q\sqrt{2}$.

Case II: $X > Y$. Then $\pi/4 < \theta_M/2 < \pi/2$ and $Y \leqslant \sqrt{XY-1} = Z$. As $|\delta_M| \ll Q^{-2c_0}$, we must have $0 < \pi/2 - \theta < \pi/3$ for large values of Q. This time we have

$$\begin{aligned}\left|\frac{Y-\varepsilon_T}{Z} - \frac{q}{q'}\right| &= \left|\tan\left(\frac{\pi}{2} - \frac{\theta_M}{2}\right) - \tan\left(\frac{\pi}{2} - \theta\right)\right| \\ &= |\tan\delta_M| \cdot \left|1 + \tan\left(\frac{\pi}{2} - \frac{\theta_M}{2}\right)\tan\left(\frac{\pi}{2} - \theta\right)\right| \\ &\leqslant (1+\sqrt{3})\,|\tan\delta_M| \ll \frac{1}{T},\end{aligned}$$

which leads (since $D \geqslant C$ if and only if $B \geqslant A$) to

$$\begin{aligned}\left|\frac{C+D}{A+B} - \frac{q}{q'}\right| &\ll \frac{1}{T} + \frac{\epsilon_T}{Z} + \left|\frac{Y}{Z} - \frac{C+D}{A+B}\right| \ll \frac{1}{T} + \frac{|D-C|}{(A+B)(AC+BD)} \\ &\leqslant \frac{1}{T} + \frac{1}{(A+B)^2} \leqslant \frac{1}{T} + \frac{1}{X} \ll \frac{1}{T} \ll Q^{-2c_0}.\end{aligned} \tag{7-10}$$

As in Case I, this is not possible because $q'(A+B) \leqslant q'\sqrt{2X} \leqslant Q\sqrt{2}$ and $(A+B)^2 \geqslant Q^{2c_0}$. $\square$

Our next goal is to apply Lemma 7, assuming $Y_M < X_M \ll Q^{2c_0}$ and taking $r = 1$, to the set $\Omega = \Omega_{M,q',\xi}$ of pairs $(u, v) \in (0, Q] \times (0, q']$ that satisfy

$$|\Xi_M(q', u)| \leqslant \frac{\xi}{Q^2} \quad \text{and} \quad q'^2 X_M + u^2 Y_M + 2uq' Z_M \leqslant \frac{Q^2 q'^2}{v^2+q'^2}. \tag{7-11}$$

Lemma 10. *There exist continuous functions $T_0(\xi)$ and $C(\xi)$ such that, for any matrix $M \in \mathfrak{S}$ with $Y_M < X_M$ and $T = \|M\|^2 > T_0(\xi)$, the projection on the first coordinate of the set $\Omega_{M,q',\xi}$ is contained in the interval* $(0, C(\xi)q']$.

Proof. Using polar coordinates $(u, q') = (r\cos\theta, r\sin\theta)$, $\theta \in (0, \pi/2)$, we see that inequalities (7-11) imply (7-7). This shows that for the purpose of this lemma we can replace $\Omega_{M,q',\xi}$ by the set of $(u, v) \in (0, Q] \times (0, q']$ satisfying (7-7). Therefore we can use all estimates from the first part of the proof of Lemma 9 (because they only rely on (7-7), the integrality of q being used only at the end).

Note also that $Y = Y_M < X = X_M$ and $Z^2 = XY - 1$ yield $Y \leqslant Z$. Replacing q by u in the first part of the proof of Lemma 9, so that $\tan\theta = u/q'$, $\theta \in (0, \pi/2)$, we see (compare the last line before Case 1) that $|\delta_M| \leqslant \Theta(\xi)/T$ for some continuous function Θ. Next we look into the first estimates in Case 2 and see that there exists a function $T_0(\xi)$, depending continuously on ξ, such that, for any M with $T = \|M\|^2 > T_0(\xi)$, one has $0 < \pi/2 - \theta < \pi/3$ and

$$\left| \frac{u}{q'} - \frac{Y - \epsilon_T}{Z} \right| \leqslant (1 + \sqrt{3})\, |\tan \delta_M| \,.$$

In conjunction with the bound on δ_M, this shows the existence of a continuous function $C_0(\xi)$ such that

$$\left| u - \frac{Y - \epsilon_T}{Z} q' \right| \leqslant C_0(\xi) q',$$

showing that $u \leqslant (1 + C_0(\xi)) q'$. □

Although this will not be used in this paper, we remark that if γ is as in (7-2), then (7-4) is satisfied by the triple (q', q, p') with the pair (Q, ξ) replaced by $(Q + \sqrt{2} Q^{c_0}, \xi(1 + \sqrt{2} Q^{c_0 - 1})^2)$, by the proof of (7-5). Therefore Lemma 10 shows that $q/q' \ll_\xi 1$ (with a different implicit constant than $C(\xi)$ from Lemma 10).

Next notice that, as $Q \to \infty$,

$$\sum_{\substack{M \in \mathfrak{S} \\ \max\{X_M, Y_M\} \leqslant Q^{2c_0}}} \max\{X_M, Y_M\}^{-\sigma} \ll_\sigma Q^{(2-2\sigma)c_0}, \quad 0 < \sigma < 1. \tag{7-12}$$

This follows immediately from[1]

$$\sum_{\substack{M \in \mathfrak{S} \\ Y_M < X_M \leqslant Q^{2c_0}}} X_M^{-\sigma} \leqslant \sum_{1 \leqslant A^2 + B^2 \leqslant Q^{2c_0}} (A^2 + B^2)^{-\sigma}$$
$$\leqslant \iint_{x^2 + y^2 \leqslant 2Q^{2c_0}} (x^2 + y^2)^{-\sigma}\, dx\, dy \ll_\sigma Q^{(2-2\sigma)c_0}.$$

Assume now that $Y_M < X_M \leqslant Q^{2c_0}$. When $T = \|M\|^2 > T_0(\xi)$ we apply Lemma 10. The definition of Ω, seen after some obvious scaling as a section subset in the body $S_{M,\xi}$ defined by the conditions in (7-14) below, shows that the range of u consists of a union of intervals in $[0, Q]$ with a (universally) bounded number of components and of total Lebesgue measure $\ll_\xi q'$. This gives

$$A(\Omega) \ll_\xi \frac{Qq'}{\sqrt{X_M}} \quad \text{and} \quad \ell(\partial\Omega) \ll_\xi q' + q' \ll \frac{Q}{\sqrt{X_M}}.$$

[1]Here A and B determine uniquely the matrix $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$.

Taking $L=(q')^{5/6}$, we find $Q \gg X_M^{1/2}(q')^{1/6}$, and the error provided by Lemma 7 is $\mathscr{E}_{\Omega,L,q'} \ll_\varepsilon Q(q')^{-1/6+\varepsilon} X_M^{-1/2}$. Note also that in this case $A \geqslant C$ and $B \geqslant D$. As a result, applying (7-12) with $\sigma=\frac{11}{12}$, the error is seen to add up to

$$\sum_{\substack{A^2+B^2 \leqslant Q^{2c_0} \\ \|M\|^2 > T_0(\xi)}} \sum_{q' \leqslant Q/\sqrt{X_M}} \mathscr{E}_{\Omega,q'^{5/6},q'} \ll_\varepsilon Q \sum_{A^2+B^2 \leqslant Q^{2c_0}} \frac{1}{X_M^{1/2}} \left(\frac{Q}{X_M^{1/2}}\right)^{5/6+\varepsilon} \ll_\varepsilon Q^{(11+c_0)/6+\varepsilon}.$$

Lemma 7 now provides

$$\widetilde{\mathscr{N}}_M(Q,\xi) = \sum_{1 \leqslant q' \leqslant Q/\sqrt{X_M}} \frac{\varphi(q')}{q'^2} A(\Omega_{M,q',\xi}) + O_\varepsilon(Q^{(11+c_0)/6+\varepsilon}). \tag{7-13}$$

The situation $\|M\|^2 \leqslant T_0(\xi)$ (in this case there are $O_\xi(1)$ choices for M) is directly handled by Lemma 7. The same choice for L provides $\mathscr{E}_{\Omega,q'^{5/6},q'} \ll_\varepsilon Q(q')^{-1/6+\varepsilon}$. These error terms sum up to $O_{\varepsilon,\xi}(Q^{11/6+\varepsilon})$ in this situation.

Next we will apply Möbius summation (see, e.g., [Boca et al. 2000, Lemma 2.3]) to the function $h_1(q')=(1/q')A(\Omega_{M,q',\xi})$. Note that $(1/Q)h_1(q')$ represents the area of the cross-section of the body $S_{M,\xi}$ by the plane $x=q'/Q$, where $S_{M,\xi}$ consists of those $(x,y,z) \in [0,1]^3$ such that

$$|\Xi_M(x,y)| \leqslant \xi \quad \text{and} \quad x^2 X_M + y^2 Y_M + 2xyZ_M \leqslant \frac{1}{1+z^2}. \tag{7-14}$$

The intersection of the projection of $S_{M,\xi}$ onto the plane $z=0$ with a vertical line $x=c$ is bounded by a quartic and an ellipse, showing that the cross-section function $c \mapsto A_{M,\xi}(c) := \operatorname{Area}(S_{M,\xi} \cap \{x=c\})$ is continuous and piecewise C^1 on $[0,1]$ and the number of critical points of $A_{M,\xi}$ is bounded by a universal constant C independently of M and ξ. The graph on the right of Figure 6 illustrates one of the possible cases that can arise, when $A_{M,\xi}(c)$ has the most number of critical points, showing that we can take $C=3$.

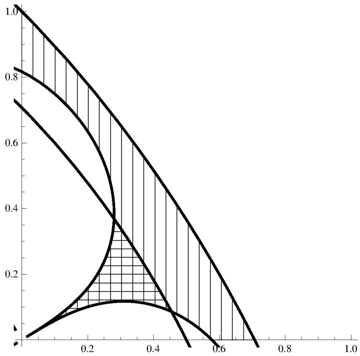
In particular, the total variation of h_1 on $[0,Q]$ is bounded above by

$$(C+1)\big(\sup_{[0,Q]} h_1 - \inf_{[0,Q]} h_1\big) \ll \|h_1\|_\infty \ll_\xi \frac{Q}{\sqrt{X_M}},$$

and so we infer

$$\sum_{1 \leqslant q' \leqslant Q/\sqrt{X_M}} \frac{\varphi(q')}{q'^2} A(\Omega_{M,q',\xi}) = \frac{1}{\zeta(2)} \int_0^{Q/\sqrt{X_M}} h_1(q')\,dq' + O\left(\frac{Q}{\sqrt{X_M}} \ln Q\right).$$

Using also the change of variables $(q',u,v)=(Qx,Qy,Qxz)$, $(x,y,z) \in [0,1]^3$,



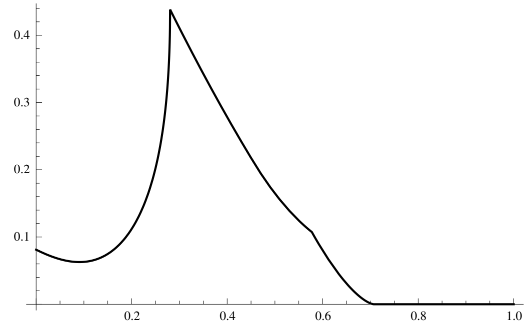


Figure 6. Left: cross-sections of $S_{M,\xi}$ for $z=0$ (vertical hatching) and $z=1$ (horizontal hatching). Right: the function $c \mapsto A_{M,\xi}(c)$, for $M=R$ and $\xi=1.5$.

(7-13), (7-5) and (7-12), we find that the contribution to $R_Q^{\Cap}(\xi)$ of matrices M with $Y_M < X_M$ is

$$\frac{1}{\zeta(2)} \sum_{\substack{M\in\mathfrak{S}\\ Y_M<X_M\leqslant Q^{2c_0}}} \left(\int_0^{\frac{Q}{\sqrt{X_M}}} A(\Omega_{M,q',\xi}) \frac{dq'}{q'} + O\left(\frac{Q\ln Q}{X_M^{1/2}}\right)\right) + O_{\varepsilon,\xi}\left(Q^{(11+c_0)/6+\varepsilon}\right)$$
$$= \frac{Q^2}{\zeta(2)} \sum_{\substack{M\in\mathfrak{S}\\ Y_M<X_M\leqslant Q^{2c_0}}} \operatorname{Vol}(S_{M,\xi}) + O_{\varepsilon,\xi}\left(Q^{1+c_0+\varepsilon} + Q^{(11+c_0)/6+\varepsilon}\right). \quad (7\text{-}15)$$

With $\eta = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, notice the following important symmetries:

$$\eta M \eta = \begin{pmatrix} D & C \\ B & A \end{pmatrix} \quad \text{and} \quad \Xi_{\eta M \eta}(y,x) = -\Xi_M(x,y). \quad (7\text{-}16)$$

This shows that the reflection $(x,y,z) \mapsto (y,x,z)$ maps $S_{M,\xi}$ bijectively onto $S_{\eta M\eta,\xi}$.

The situation $X_M < Y_M$ is handled similarly using (7-16), which results in reversing the roles of q and q' with Lemma 7 applied for $r=-1$.

Now we give upper bounds for $\operatorname{Vol}(S_{M,\xi})$. Let $(x,y,z) = (r\cos t, r\sin t, z) \in S_{M,\xi}$. The proof of (7-9) and (7-10) does not use the integrality of q' and q, so denoting

$$\omega_M = \frac{C+D}{A+B} < 1 \quad \text{if } Y_M < X_M \quad \text{and} \quad \omega_M = \frac{A+B}{C+D} < 1 \quad \text{if } X_M < Y_M,$$

we find that

$$y \ll x \ll X_M^{-1/2} \ll T^{-1} \quad \text{and} \quad \left|\frac{y}{x} - \omega_M\right| \ll \frac{1}{T}$$

in the former case, and

$$x \ll y \ll Y_M^{-1/2} \ll T^{-1} \quad \text{and} \quad \left|\frac{x}{y} - \omega_M\right| \ll \frac{1}{T}$$

in the latter case. Writing the area in polar coordinates, we find $r^2 \ll T^{-1}$ and

$$\begin{aligned} \operatorname{Vol}(S_{M,\xi}) &\leqslant A\big(\{(x,y)\in[0,1]^2 : \exists z\in[0,1],\,(x,y,z)\in S_{M,\xi}\}\big) \\ &\leqslant \frac{1}{2}\int_{\omega_M-\xi T_M^{-1}}^{\omega_M+\xi T_M^{-1}} 2T_M^{-1}\,dt = \frac{2\xi}{T_M^2} = \frac{2\xi}{\|M\|^4}. \end{aligned} \tag{7-17}$$

The bound (7-17) and an argument similar to the proof of (7-12) yields

$$\sum_{M\in\mathfrak{S}} \operatorname{Vol}(S_{M,\xi}) < \infty \quad \text{and} \quad \sum_{\substack{M\in\mathfrak{S}\\ \max\{X_M,Y_M\}\geqslant Q^{2c_0}}} \operatorname{Vol}(S_{M,\xi}) \ll_\xi Q^{-2c_0}. \tag{7-18}$$

From (7-15), (7-18) and $c_0\in\big(\tfrac{1}{2},1\big)$, we infer

$$R_Q^{\Cap}(\xi) = \frac{Q^2}{\zeta(2)}\sum_{M\in\mathfrak{S}} \operatorname{Vol}(S_{M,\xi}) + O_\varepsilon(Q^{(11+c_0)/6+\varepsilon}). \tag{7-19}$$

The volume of $S_{M,\xi}$ can be evaluated in closed form using the substitution $z=\tan t$:

$$\operatorname{Vol}(S_{M,\xi}) = \int_0^{\pi/4} B_M(\xi,t)\frac{dt}{\cos^2 t}, \tag{7-20}$$

where $B_M(\xi,t)$ is the area of the region consisting of those $(r\cos\theta, r\sin\theta)\in[0,1]^2$ such that

$$\frac{1}{\xi}\cdot\frac{|\sin(2\theta-\theta_M)|}{U_T+\cos(2\theta-\theta_M)} \leqslant r^2 \leqslant \frac{1}{\sqrt{T^2-4}}\cdot\frac{2\cos^2 t}{U_T+\cos(2\theta-\theta_M)}, \tag{7-21}$$

with $\theta_M\in(0,\pi/2)$ having $\sin\theta_M = 2Z_M/\sqrt{T^2-4}$ and $U_T = T/\sqrt{T^2-4}$ (for brevity we write $T=T_M$).

The following elementary fact will be useful to prove the differentiability of the volumes as functions of ξ.

Lemma 11. *Assume that $G, H : K\to\mathbb{R}$ are continuous functions on a compact set $K\subset\mathbb{R}^k$, and denote $x_+=\max\{x,0\}$. Then the formula*

$$V(\xi) := \int_K (\xi - G(v))_+ H(v)\,dv, \qquad \xi\in\mathbb{R},$$

defines a C^1 map on $\mathbb{R}$, and

$$V'(\xi) = \int_{G<\xi} H(v)\,dv.$$

Using Equation (7-20), we find that

$$\operatorname{Vol}(S_{M,\xi}) = \frac{1}{2}\int_0^{\pi/4} dt \int_0^{\pi/2} d\theta\, \frac{\big(2/\sqrt{T^2-4} - |\sin(2\theta-\theta_M)|/(\xi\cos^2 t)\big)_+}{U_T+\cos(2\theta-\theta_M)}, \tag{7-22}$$

and applying Lemma 11, we obtain:

Corollary 12. *The function* $\xi \mapsto \mathrm{Vol}(S_{M,\xi})$ *is* C^1.

For a smaller range for ξ we have the following explicit formula:

Lemma 13. *Suppose that* $\xi \leqslant Z_M$. *The volume of* $S_{M,\xi}$ *only depends on* ξ *and* $T = \|M\|^2$:

$$\mathrm{Vol}(S_{M,\xi}) = \int_0^{\frac{\pi}{4}} \tan^{-1}\left(\frac{\sqrt{\Delta}-\sqrt{\Delta-4\xi^2\cos^4 t}}{2\alpha\xi\cos^2 t}\right) + \frac{1}{2\xi\cos^2 t}\ln\left(1-\frac{\sqrt{\Delta}-\sqrt{\Delta-4\xi^2\cos^4 t}}{2\alpha}\right)dt,$$

where $\Delta = T^2-4$ *and* $\alpha = \frac{1}{2}(T+\sqrt{T^2-4})$.

Proof. The two polar curves defined by (7-21) intersect for

$$|\sin(2\theta-\theta_M)| = \frac{2\xi}{\sqrt{T^2-4}}\cos^2 t,$$

that is, for $\theta_\pm = \theta_M/2 \pm \alpha$ with $\alpha = \alpha(\xi, t) \in (0, \pi/4)$ such that

$$\sin 2\alpha = \frac{2\xi}{\sqrt{T^2-4}}\cos^2 t.$$

Since $\sin\theta_M = 2Z/\sqrt{T^2-4}$, the assumption $\xi \leqslant Z$ ensures that $\alpha < \theta_M$. Thus $\theta_\pm \in [0, \pi/2)$, and the change of variables $\theta = \theta_M/2 + u$ yields

$$B_{M,\xi}(t) = \frac{1}{2}\int_{-\alpha}^{\alpha}\left(\frac{2\cos^2 t}{\sqrt{T^2-4}}\cdot\frac{1}{U_T+\cos(2u)} - \frac{|\sin(2u)|}{\xi(U_T+\cos(2u))}\right)du.$$

The integrand is even and both integrals can be computed exactly, yielding the formula above. □

In particular, Lemma 13 yields $\mathrm{Vol}(S_{M,\xi}) \ll \xi/T^2$, providing an alternative proof for (7-17).

7.2. ***Exterior arcs.*** Referring to the notation of Section 5.2, we first replace the inequalities

$$p^2+p'^2+q^2+q'^2 \leqslant Q^2 \quad \text{and} \quad p_\ell^2+q_\ell^2+(Kp_\ell-p_{\ell-1})^2+(Kq_\ell-q_{\ell-1})^2 \leqslant Q^2$$

in (5-7) by simpler ones. Using $p'q-pq'=1$, we can replace p by $p'q/q'$ in the former, while $p_{\ell-1}$ can be replaced by $p_\ell q_{\ell-1}/q_\ell$ in the latter. As a result, these two inequalities can be substituted in (5-7) by

$$\begin{aligned}\left(1+\frac{p'^2}{q'^2}\right)(q^2+q'^2) &\leqslant Q^2\big(1+O(Q^{-1})\big),\\ \left(1+\frac{p_\ell^2}{q_\ell^2}\right)\big(q_\ell^2+(Kq_\ell-q_{\ell-1})^2\big) &\leqslant Q^2\big(1+O(Q^{-1})\big).\end{aligned} \tag{7-23}$$

Since $p_\ell/q_\ell = p'/q' + O(\ell/Q)$ and $q_\ell^2 + (Kq_\ell - q_{\ell-1})^2 \leqslant 2Q^2$, the second inequality in (7-23) can be also written as

$$\Big(1+\frac{p'^2}{q'^2}\Big)\big(q_\ell^2 + (Kq_\ell - q_{\ell-1})^2\big) \leqslant Q^2\big(1+O(Q^{-1})\big),$$

leading to

$$R_Q^{\cap\cap}(\xi) = \sum_{\substack{\ell\in[0,\xi)\\ K\in[1,\xi)}} \sum_{q'<Q} \mathcal{N}^{\cap\cap}_{Q+O(Q^{1/2}),q',K,\ell}(\xi),$$

where $\mathcal{N}^{\cap\cap}_{Q,q',K,\ell}(\xi)$ denotes the number of integer lattice points (p', q) such that

$$0 \leqslant p' \leqslant q', \quad 0 \leqslant q \leqslant Q, \quad p'q \equiv 1 \pmod{q'}, \quad 0 < Kq_\ell - q_{\ell-1} \leqslant Q,$$
$$\Upsilon_{\ell,K}\Big(\frac{q}{Q}, \frac{q'}{Q}\Big) \leqslant \xi, \quad p'^2 + q'^2 \leqslant \frac{Q^2 q'^2}{\max\{q^2+q'^2, q_\ell^2 + (Kq_\ell - q_{\ell-1})^2\}}. \tag{7-24}$$

Applying Lemma 7 to the set $\Omega = \Omega^{\cap\cap}_{q',K,\ell,\xi}$ of elements (u, v) for which

$$u \in [0, Q], \quad v \in [0, q'], \quad L_i\Big(\frac{u}{Q}, \frac{q'}{Q}\Big) > 0 \text{ for } i = 0, 1, \dots, \ell,$$
$$0 < KL_\ell\Big(\frac{u}{Q}, \frac{q'}{Q}\Big) - L_{\ell-1}\Big(\frac{u}{Q}, \frac{q'}{Q}\Big) \leqslant 1, \quad \Upsilon_{\ell,K}\Big(\frac{u}{Q}, \frac{q'}{Q}\Big) \leqslant \xi,$$
$$v^2 + q'^2 \leqslant \frac{Q^2q'^2}{\max\big\{u^2+q'^2, Q^2L_\ell^2\big(\frac{u}{Q}, \frac{q'}{Q}\big) + Q^2\big(KL_\ell\big(\frac{u}{Q}, \frac{q'}{Q}\big) - L_{\ell-1}\big(\frac{u}{Q}, \frac{q'}{Q}\big)\big)^2\big\}},$$

with $A(\Omega) \leqslant Qq'$, $\ell(\partial\Omega) \ll Q$, $L = (q')^{5/6}$, we find

$$\mathcal{N}^{\cap\cap}_{Q,q',K,\ell}(\xi) = \frac{\varphi(q')}{q'} \cdot \frac{A\big(\Omega^{\cap\cap}_{q',K,\ell,\xi}\big)}{q'} + O_\varepsilon(Q(q')^{-1/6+\varepsilon}).$$

This leads in turn to

$$R_Q^{\cap\cap}(\xi) = \mathcal{M}_Q^{\cap\cap}(\xi) + O_{\xi,\varepsilon}(Q^{11/6+\varepsilon}),$$

where

$$\mathcal{M}_Q^{\cap\cap}(\xi) = \sum_{\substack{\ell\in[0,\xi)\\ K\in[1,\xi)}} \sum_{q'\leqslant Q} \frac{\varphi(q')}{q'} \cdot \frac{A(\Omega^{\cap\cap}_{q',K,\ell,\xi})}{q'}.$$

For fixed integers $K \in [1, \xi)$, $\ell \in [0, \xi)$, consider the subset $T_{K,\ell,\xi}$ of $[0, 1]^3$ consisting of those $(x, y, z) \in [0, 1]^3$ such that

$$\begin{gathered} 0 < L_{\ell+1}(x, y) = KL_\ell(x, y) - L_{\ell-1}(x, y) \leqslant 1, \quad \Upsilon_{\ell,K}(x, y) \leqslant \xi, \\ \max\big\{x^2+y^2, L_\ell^2(x, y) + L_{\ell+1}^2(x, y)\big\} \leqslant \frac{1}{1+z^2}, \end{gathered} \tag{7-25}$$

with L_i and $\Upsilon_{\ell,K}$ as in (5-5) and (5-6).

Möbius summation is now applied to $h_2(q') = (1/q')A(\Omega^{\cap\cap}_{q',K,\ell,\xi})$. The quantity $(1/Q)h_2(q')$ represents the area of the cross-section of the body $T_{K,\ell,\xi}$ by the plane $x = q'/Q$. This shows that h_2 is continuous and piecewise C^1 on $[0, Q]$, and furthermore the number of critical points of h_2 is bounded uniformly in ξ (and independently of Q). Hence the total variation of h_2 on $[0, Q]$ is $\ll_\xi \|h_2\|_\infty \leqslant Q$. Employing also the change of variables $(q', u, v) = (Qx, Qy, Qxz)$, where $(x, y, z) \in [0, 1]^3$, we find

$$\begin{aligned}\mathcal{M}^{\cap\cap}_Q(\xi) &= \frac{1}{\zeta(2)} \sum_{\substack{\ell\in[0,\xi)\\ K\in[1,\xi)}} \left(\int_0^Q \frac{dq'}{q'} A\big(\Omega^{\cap\cap}_{q',K,\ell,\xi}\big) + O(Q) \right)\\ &= \frac{Q^2}{\zeta(2)} \sum_{\substack{\ell\in[0,\xi)\\ K\in[1,\xi)}} \operatorname{Vol}(T_{K,\ell,\xi}) + O_\xi(Q),\end{aligned}$$

and so

$$R^{\cap\cap}_Q(\xi) = \frac{Q^2}{\zeta(2)} \sum_{\substack{\ell\in[0,\xi)\\ K\in[1,\xi)}} \operatorname{Vol}(T_{K,\ell,\xi}) + O_{\xi,\varepsilon}(Q^{11/6+\varepsilon}). \tag{7-26}$$

To show that $\xi \mapsto \operatorname{Vol}(T_{K,\ell,\xi})$ is C^1 on $[1, \infty)$, we make the change of variables $(x, y, z) = (\cos\theta, \sin\theta, \tan t)$ to obtain

$$\operatorname{Vol}(T_{K,\ell,\xi}) = \int_0^{\pi/4} A_{K,\ell}(\xi, t)\, \frac{dt}{\cos^2 t}, \tag{7-27}$$

where $A_{K,\ell}(\xi, t)$ is the area of the region defined by the conditions in (1-3). Now notice that $K_i(x, y) \leqslant \xi$ when $1 \leqslant i \leqslant \ell$, as a result of (omitting the arguments of the functions)

$$K_i = \frac{L_i + L_{i-2}}{L_{i-1}} \leqslant \frac{1}{L_{i-2}L_{i-1}} + \frac{1}{L_{i-1}L_i} < \Upsilon_{\ell,K} \leqslant \xi.$$

Similarly,

$$K_1 = \frac{L_{-1} + L_1}{L_0} \leqslant \frac{L_{-1}}{L_0} + \frac{1}{L_0 L_1} < \Upsilon_{\ell,K} \leqslant \xi.$$

Thus the projection of $T_{K,\ell,\xi}$ on the first two coordinates is included into the union of disjoint cylinders $\mathcal{T}_{\boldsymbol{k}} := \mathcal{T}_{k_1} \cap T^{-1}\mathcal{T}_{k_2} \cap \cdots \cap T^{-\ell+1}\mathcal{T}_{k_\ell}$ with $\mathcal{T}_k = \{(x, y) : K_1(x, y) = k\}$ and $\boldsymbol{k} = (k_1, \dots, k_\ell) \in [1, \xi)^\ell$. On each set $\mathcal{T}_{\boldsymbol{k}}$ all maps $L_1, \dots, L_\ell, L_{\ell+1}$ are linear, say $L_i(x, y) = A_i x + B_i y$, with integers A_i, B_i depending only on $k_1, \dots, k_i$ for $i \leqslant \ell$ and $A_{\ell+1}, B_{\ell+1}$ depending only on $\boldsymbol{k}$ and K. Therefore the function $F_{K,\ell}(\theta)$ is continuous on each region $\mathcal{T}_{\boldsymbol{k}}$, and applying Lemma 11 we conclude that the function $\xi \mapsto \operatorname{Vol}(T_{K,\ell,\xi})$ is C^1 on $[1, \infty]$, being a sum of $[\xi]^\ell$ volumes, as functions $\to$ each of which is C^1 each of which is C^1 as a function of ξ.

Remark 14. The region $T_{K,\ell,\xi}$ can be simplified further. For each integer $J \in [1, \xi)$, the map

$$\Psi_J : (u, v) \mapsto (J L_\ell(u, v) - L_{\ell-1}(u, v), L_\ell(u, v))$$

is an area preserving injection on $\mathcal{T}$, since it is the composition of T^ℓ in (5-5) followed by the linear transformation $(u, v) \mapsto (Jv - u, v)$. Note that under this map (omitting the arguments (u, v) of the functions below):

$$L_1 \to \left[\frac{1 + J L_\ell - L_{\ell-1}}{L_\ell}\right] - (J L_\ell - L_{\ell-1}) = L_{\ell-1}$$

(using $L_{\ell-1} + L_\ell > 1$), and by induction it follows similarly that $L_i \to L_{\ell-i}$ for $0 \leqslant i \leqslant \ell$. Also we have that $\Psi_J(u, v) = (x, y) \in [0, 1]^2$ if and only if $x = J L_\ell - L_{\ell-1} \in [0, 1]$ and $J = [(1 + x)/y]$.

Let us decompose the region $T_{K,\ell,\xi}$ into a disjoint union of regions $T_{K,J;\ell,\xi}$, $1 \leqslant J < \xi$, obtained by adding the condition $[(1 + x)/y] = J$. By the discussion of the previous paragraph, the map (Ψ_J, Id_z) is a volume preserving bijection taking $U_{K,J;\ell,\xi}$ onto $T_{K,J;\ell,\xi}$, where $U_{K,J;\ell,\xi}$ is the set of all $(x, y, z) \in [0, 1]^3$ such that

$$\begin{gathered} x + y > 1, \quad J L_\ell - L_{\ell-1} > 0, \quad K L_0 - L_1 > 0, \quad \Upsilon_{\ell,K,J} \leqslant \xi, \\ L_0^2 + (K L_0 - L_1)^2 \leqslant \frac{1}{1 + z^2}, \quad L_\ell^2 + (J L_\ell - L_{\ell-1})^2 \leqslant \frac{1}{1 + z^2}. \end{gathered}$$

Here $L_i = L_i(x, y)$ and

$$\Upsilon_{\ell,K,J}(x, y) = \frac{J L_\ell - L_{\ell-1}}{L_\ell(L_\ell^2 + (J L_\ell - L_{\ell-1})^2)} + \sum_{i=1}^{\ell} \frac{1}{L_{i-1} L_i} + \frac{K L_0 - L_1}{L_0(L_0^2 + (K L_0 - L_1)^2)}.$$

For $\alpha \geqslant 1$, the transformation $(\Psi_\alpha, \mathrm{Id}_z)$ maps bijectively the part of $U_{K,J;\ell,\xi}$ for which $[(1 + L_{\ell-1})/L_\ell] = \alpha$ onto the part of $U_{J,K;\ell,\xi}$ for which $[(1 + x)/y] = \alpha$. Therefore $\mathrm{Vol}(U_{K,J;\ell,\xi}) = \mathrm{Vol}(U_{J,K;\ell,\xi})$ and the sum of volumes appearing in (7-28) can be written more symmetrically:

$$\sum_{K \in [1,\xi)} \mathrm{Vol}(T_{K,\ell,\xi}) = \sum_{K,J \in [1,\xi)} \mathrm{Vol}(U_{K,J;\ell,\xi}).$$

As an example of using this formula, if $1 < \xi \leqslant 2$ and $\ell = 1$, we can only have $K = J = 1$ and the inequalities $J L_1 - L_0 > 0$, $K L_0 - L_1 > 0$ cannot be both satisfied, so $U_{1,1;1,\xi}$ is empty. Therefore the only contribution from the T bodies in (7-28) comes from $T_{1,0,\xi}$ if $\xi \in (1, 2]$.

We can now prove the main theorem on the pair correlation of the quantities $\tan(\theta_\gamma/2)$.

Theorem 2. *The pair correlation measure $R_2^{\mathfrak{T}}$ exists on* $[0,\infty)$. *It is given by the C^1 function*

$$R_2^{\mathfrak{T}}\left(\tfrac{3}{8}\xi\right)=\frac{8}{3\zeta(2)}\left(\sum_{M\in\mathfrak{S}}\operatorname{Vol}(S_{M,\xi})+\sum_{\ell\in[0,\xi)}\sum_{K\in[1,\xi)}\operatorname{Vol}(T_{K,\ell,\xi})\right),\tag{7-28}$$

where the three-dimensional bodies $S_{M,\xi}$ are defined by the conditions in (7-14) and the bodies $T_{K,\ell,\xi}$ are defined by the conditions in (7-25).

Proof. By (7-19) and (7-26), with $c_0\in\left(\frac{1}{2},1\right)$ and $G(\xi)$ denoting the sum of all volumes in (7-28), we infer that

$$\mathcal{R}_Q^{\Phi}(\xi)=\frac{Q^2}{\zeta(2)}G(\xi)+O_{\xi,\varepsilon}(Q^{(11+c_0)/6+\varepsilon}).\tag{7-29}$$

It follows that the function G is C^1 on $[0,\infty)$ as a result of $\xi\mapsto\operatorname{Vol}(S_{M,\xi})$ being C^1 on $[0,\infty)$, and of $\xi\mapsto\operatorname{Vol}(T_{K,\ell,\xi})$ being C^1 on $[1,\infty)$. Corollary 4 and (7-29) now yield, for $\beta\in\left(\frac{2}{3},1\right)$,

$$\mathcal{R}_Q^{\Psi}(\xi)$$
$$=\frac{Q^2}{\zeta(2)}\left(G(\xi+O(Q^{2-3\beta}))+G(O(Q^{2-3\beta}))\right)+O_{\xi,\varepsilon}(Q^{1+\beta}\ln Q+Q^{(11+c_0)/6+\varepsilon}).$$

Employing again the differentiability of G and $G(0)=0$, and taking $\beta=\frac{3}{4}$, $c_0=\frac{1}{2}+\varepsilon$, this provides

$$\mathcal{R}_Q^{\Psi}(\xi)=\frac{Q^2}{\zeta(2)}G(\xi)+O_{\xi,\varepsilon}(Q^{23/12+\varepsilon}).\tag{7-30}$$

Equation (7-28) now follows from (7-30) and Corollary 8. □

8. Pair correlation of $\{\theta_\gamma\}$

8.1. ***Proof of Theorem 1.*** In this section we pass to the pair correlation of the angles $\{\theta_\gamma\}$, estimating

$$\mathcal{R}_Q^{\theta}(\xi):=\#\left\{(\gamma,\gamma')\in\widetilde{\mathfrak{R}}_Q^2:0\leqslant Q^2(\theta_{\gamma'}-\theta_\gamma)\leqslant\xi\right\}.$$

Define the pair correlation kernel $F(\xi,t)$ as follows:

$$F(\xi,t)=\sum_{M\in\mathfrak{S}}B_M(\xi,t)+\sum_{\substack{\ell\in[0,\xi)\\K\in[1,\xi)}}A_{K,\ell}(\xi,t),\tag{8-1}$$

where $B_M(\xi,t)$ and $A_{K,\ell}(\xi,t)$ are the areas from (7-20) and (7-27), respectively, so that by (7-30) we have

$$\mathcal{R}_Q^{\Psi}(\xi)=\frac{Q^2}{\zeta(2)}\int_0^{\pi/4}F(\xi,t)\frac{dt}{\cos^2 t}+O_{\xi,\varepsilon}(Q^{(11+c_0)/6+\varepsilon}).$$

Proposition 15. $\mathcal{R}^{\theta}_{Q}(\xi) = \dfrac{Q^2}{\zeta(2)} \displaystyle\int_0^{\pi/4} F\Big(\frac{\xi}{2\cos^2 t}, t\Big)\frac{dt}{\cos^2 t} + O_{\xi,\varepsilon}(Q^{47/24+\varepsilon}).$

Before giving the proof, note that Theorem 1 follows from the proposition as $Q \to \infty$, taking into account the different normalization in the definitions of $\mathcal{R}^{\theta}_{Q}(\xi)$ and $R^{\mathfrak{A}}_{Q}(\xi)$, and defining, in view of Proposition 15 and (8-1),

$$B_M(\xi) := \int_0^{\frac{\pi}{4}} B_M\Big(\frac{\xi}{2\cos^2 t}, t\Big)\frac{dt}{\cos^2 t}, \quad A_{K,\ell}(\xi) := \int_0^{\frac{\pi}{4}} A_{K,\ell}\Big(\frac{\xi}{2\cos^2 t}, t\Big)\frac{dt}{\cos^2 t}.$$

From the definitions of $B_M(\xi,t)$, $A_{K,\ell}(\xi,t)$ in the equations following (7-20), (7-27), it is clear that

$$B_M\Big(\frac{\xi}{2\cos^2 t}, t\Big) = B_M\Big(\frac{\xi}{2}, 0\Big)\cos^2 t, \quad A_{K,0}\Big(\frac{\xi}{2\cos^2 t}, t\Big) = A_{K,0}\Big(\frac{\xi}{2}, 0\Big)\cos^2 t,$$

hence one has

$$B_M(\xi) = \frac{\pi}{4} B_M\Big(\frac{\xi}{2}, 0\Big), \quad A_{K,0}(\xi) = \frac{\pi}{4} A_{K,0}\Big(\frac{\xi}{2}, 0\Big), \tag{8-2}$$

which together with (7-22) yields the formula for $B_M(\xi)$ given in Theorem 1. Note that the range of summation in Theorem 1 restricts to $K < \xi/2$, $\ell < \xi/2$, compared with the range in (8-1). Indeed, from the description of $A_{K,\ell}(\xi/2\cos^2 t, t)$ following (7-27), we see that $\ell < \Upsilon_{\ell,K} \leqslant \xi/2$, while for K we have

$$K < \frac{1}{L_{\ell-1}L_\ell} + \frac{KL_\ell - K_{\ell-1}}{L_\ell} < \Upsilon_{\ell,K} \leqslant \frac{\xi}{2},$$

and similarly for $\ell = 0$.

Proof of Proposition 15. Consider $I = [\alpha, \beta)$ with $N = [Q^d]$, $|I| = N^{-1} \sim Q^{-d}$, $I^+ = [\alpha - Q^{-d'}, \beta + Q^{-d'}]$, and $I^- = [\alpha + Q^{-d'}, \beta - Q^{-d'}]$, where

$$0 < d = \tfrac{1}{24} < d' = \tfrac{1}{12} < 1.$$

Partition the interval $[0, 1)$ into the union of N intervals $I_j = [\alpha_j, \alpha_{j+1})$, with $|I_j| = N^{-1}$ as above. Associate the intervals $I_j^{\pm}$ to I_j as described above. Set

$$\begin{aligned}
&\mathfrak{R}^{\sharp}_{Q} := \{(\gamma,\gamma') \in \widetilde{\mathfrak{R}}^{2}_{Q} : \gamma \neq \gamma'\},\\
&\mathcal{R}^{\theta}_{I,Q}(\xi) := \#\big\{(\gamma,\gamma') \in \mathfrak{R}^{\sharp}_{Q} : 0 \leqslant Q^2(\theta_{\gamma'} - \theta_{\gamma}) \leqslant \xi,\ \Psi(\gamma), \Psi(\gamma') \in I\big\},\\
&\mathcal{R}^{\theta,\natural}_{I,Q}(\xi) := \#\big\{(\gamma,\gamma') \in \mathfrak{R}^{\sharp}_{Q} : 0 \leqslant Q^2(\theta_{\gamma'} - \theta_{\gamma}) \leqslant \xi,\ \Psi(\gamma) \in I\big\}\ \big(\geqslant \mathcal{R}^{\theta}_{I,Q}(\xi)\big),\\
&\mathcal{R}^{\Psi}_{I,Q}(\xi) := \#\big\{(\gamma,\gamma') \in \mathfrak{R}^{\sharp}_{Q} : 0 \leqslant Q^2(\Psi(\gamma') - \Psi(\gamma)) \leqslant \xi,\ \Psi(\gamma), \Psi(\gamma') \in I\big\},\\
&\mathcal{R}^{\Psi,\flat}_{I,Q}(\xi) := \#\big\{(\gamma,\gamma') \in \mathfrak{R}^{\sharp}_{Q} : 0 \leqslant Q^2(\Psi(\gamma') - \Psi(\gamma)) \leqslant \xi,\ \gamma_-, \gamma_+ \in I\big\},\\
&\mathcal{R}^{\Phi,\flat}_{I,Q}(\xi) := \#\big\{(\gamma,\gamma') \in \mathfrak{R}^{\sharp}_{Q} : 0 \leqslant Q^2(\Phi(\gamma') - \Phi(\gamma)) \leqslant \xi,\ \gamma_-, \gamma_+ \in I\big\}.
\end{aligned}$$

Expressing $\theta_{\gamma'} - \theta_\gamma$ and $\Psi(\gamma') - \Psi(\gamma)$ via the mean value theorem, we find

$$\mathcal{R}^{\Psi}_{I,Q}\big(\tfrac{1}{2}(1+\alpha^2)\xi\big) \leqslant \mathcal{R}^{\theta}_{I,Q}(\xi) \leqslant \mathcal{R}^{\Psi}_{I,Q}\big(\tfrac{1}{2}(1+\beta^2)\xi\big). \tag{8-3}$$

Lemma 16. *The following estimates hold*:

(i) $$\sum_{j=1}^{N} \mathcal{R}^{\theta}_{I_j,Q}(\xi) \leqslant \mathcal{R}^{\theta}_{Q}(\xi) = \sum_{j=1}^{N} \mathcal{R}^{\theta,\natural}_{I_j,Q}(\xi) \leqslant \sum_{j=1}^{N} \mathcal{R}^{\theta}_{I_j^+,Q}(\xi) + O(Q^{15/8}\ln^2 Q).$$

(ii) $\mathcal{R}^{\Psi}_{I,Q}(\xi) = \mathcal{R}^{\Psi,\flat}_{I,Q}(\xi) + O(Q^{1+d'}\ln^2 Q)$.

Proof. The first inequality in (i) is trivial. For the second one, note first that the total number of pairs (γ,γ') with $0 \leqslant \theta_{\gamma'} - \theta_\gamma \leqslant \xi Q^{-2}$ and $qq' \leqslant Q^{d'}$, with $\gamma_- = p/q$ and $\gamma_+ = p'/q'$, is $\ll_\xi Q^d(Q^{d'}\ln Q)(Q\ln Q)$. For γ with $qq' > Q^{-d'}$, use $\Psi(\gamma') - \beta \leqslant \Psi(\gamma') - \Psi(\gamma) \leqslant 1/qq' \leqslant Q^{-d'}$, so $\Psi(\gamma') \in I_j^+$. The proof of (ii) is analogous. □

Lemma 16 and (8-3) yield

$$\sum_{j=1}^{N} \mathcal{R}^{\Psi}_{I_j,Q}\big(\tfrac{1}{2}(1+\alpha_j^2)\xi\big) \leqslant \mathcal{R}^{\theta}_{Q}(\xi) \leqslant \sum_{j=1}^{N} \mathcal{R}^{\Psi}_{I_j^+,Q}\big(\tfrac{1}{2}(1+\alpha_{j+1}^2)\xi\big) + O_\varepsilon(Q^{15/8+\varepsilon}).$$

To estimate $\mathcal{R}^{\Phi}_{I,Q}(\xi)$ we repeat the previous arguments for a short interval I as above. Adding everywhere the condition $\gamma_-, \gamma_+ \in I$, we modify $\mathcal{R}^{\Cap}_{Q}$ by $\mathcal{R}^{\Cap}_{I,Q}$ and $R^{\Cap}_{Q}$ by $R^{\Cap}_{I,Q}$ in Lemma 5, $\mathcal{R}^{\cap\cap}_{Q}$ by $\mathcal{R}^{\cap\cap}_{I,Q}$ and $R^{\cap\cap}_{Q}$ by $R^{\cap\cap}_{I,Q}$ in Lemma 6. The additional condition $p/q,\ p'/q' \in I$ is inserted in (7-2). The condition $0 \leqslant p' \leqslant q'$ is replaced by $q'\alpha \leqslant p' < q'\beta$ in (7-4) and (7-24), and $0 \leqslant p \leqslant q$ is replaced by $q\alpha \leqslant p < q\beta$ in (7-4). The condition $v \in [0, q']$ is replaced by $v \in [q'\alpha, q'\beta)$ in the definition of $\Omega_{M,q',\xi}$, and $\Omega^{\cap\cap}_{q',\ell,K,\xi}$. The bodies $S_{M,\xi}$ and $T_{K,\ell,\xi}$ are substituted, respectively, by $S_{I,M,\xi}$ and $T_{I,K,\ell,\xi}$ after replacing the condition $z \in [0,1]$ in their definitions by $z \in [\alpha,\beta)$. The analogs of (7-20) and (7-27) hold:

$$\operatorname{Vol}(S_{I,M,\xi}) = \int_I B_M(\xi,t)\frac{dt}{\cos^2 t}, \qquad \operatorname{Vol}(T_{I,K,l,\xi}) = \int_I A_{K,\ell}(\xi,t)\frac{dt}{\cos^2 t}. \tag{8-4}$$

The approach from Section 7 under the changes specified in the previous paragraph leads to

$$R^{\Phi,\flat}_{I,Q}(\xi) = R^{\Cap}_{I,Q}(\xi) + R^{\cap\cap}_{I,Q}(\xi) = \frac{Q^2}{\zeta(2)}\int_{\tan^{-1} I} F(\xi,t)\frac{dt}{\cos^2 t} + O_{\xi,\varepsilon}(Q^{23/12+\varepsilon}), \tag{8-5}$$

with the pair correlation kernel $F(\xi,t)$ defined by (8-1). We also have

$$R^{\Phi,\flat}_{I^+,Q}(\xi) = R^{\Phi,\flat}_{I,Q}(\xi) + O_{\xi,\varepsilon}(Q^{23/12+\varepsilon} + Q^{2-d'}). \tag{8-6}$$

The analogs of Lemmas 5 and 6 yield, upon (8-5) and (8-6),

$$\mathcal{R}^{\Phi,\flat}_{I,Q}(\xi)=\frac{Q^2}{\zeta(2)}\int_{\tan^{-1}I}F\big(\xi+O(Q^{-1/3}),t\big)\frac{dt}{\cos^2 t}+O_{\xi,\varepsilon}(Q^{23/12+\varepsilon})=\mathcal{R}^{\Phi,\flat}_{I^+,Q}(\xi). \tag{8-7}$$

The analog of Corollary 4 and (8-7) yield

$$\begin{aligned}\mathcal{R}^{\Psi,\flat}_{I,Q}(\xi)&=\mathcal{R}^{\Phi,\flat}_{I,Q}(\xi+O(Q^{-1/4}))+\mathcal{R}^{\Phi,\flat}_{I,Q}(O(Q^{-1/4}))+O_\varepsilon(Q^{7/4+\varepsilon})\\&=\frac{Q^2}{\zeta(2)}\int_{\tan^{-1}I}\big(F(\xi+O(Q^{-1/4}),t)+F(Q^{-1/4},t)\big)\big)\frac{dt}{\cos^2 t}+O_{\xi,\varepsilon}(Q^{23/12+\varepsilon})\\&=\mathcal{R}^{\Psi,\flat}_{I^+,Q}(\xi).\end{aligned} \tag{8-8}$$

As shown in Section 7, the function F is C^1 in ξ, thus (8-8) gives actually[2]

$$\mathcal{R}^{\Psi,\flat}_{I,Q}(\xi)=\frac{Q^2}{\zeta(2)}\int_{\tan^{-1}I}F(\xi,t)\frac{dt}{\cos^2 t}+O_{\xi,\varepsilon}(Q^{23/12+\varepsilon})=\mathcal{R}^{\Psi,\flat}_{I^+,Q}(\xi). \tag{8-9}$$

Lemma 16(i), (8-9), and the fact that $F\in C^1[0,\infty)$ yield

$$\mathcal{R}^{\Psi}_{I,Q}(\xi)=\frac{Q^2}{\zeta(2)}\int_{\tan^{-1}I}F(\xi,t)\frac{dt}{\cos^2 t}+O_{\xi,\varepsilon}(Q^{23/12+\varepsilon}+Q^{2-d'})=\mathcal{R}^{\Psi}_{I^+,Q}(\xi). \tag{8-10}$$

Let also $\omega_j=\tan^{-1}\alpha_j$. From (8-10) and (8-3) we further infer

$$\begin{aligned}\frac{Q^2}{\zeta(2)}\int_{\omega_j}^{\omega_{j+1}}&F\Big(\tfrac12(1+\alpha_j^2)\xi,t\Big)\frac{dt}{\cos^2 t}+O_{\xi,\varepsilon}(Q^{23/12+\varepsilon}+Q^{2-d'})\\&\leqslant\mathcal{R}^{\theta}_{I_j,Q}(\xi)\leqslant\mathcal{R}^{\theta}_{I_j^+,Q}(\xi)\\&\leqslant\frac{Q^2}{\zeta(2)}\int_{\omega_j}^{\omega_{j+1}}F\big(\tfrac12(1+\alpha_{j+1}^2)\xi,t\big)\frac{dt}{\cos^2 t}+O_{\xi,\varepsilon}(Q^{23/12+\varepsilon}+Q^{2-d'}).\end{aligned}$$

Employing also

$$\int_{\omega_j}^{\omega_{j+1}}F\big(\tfrac12(1+\alpha_j^2)\xi,t\big)\frac{dt}{\cos^2 t}=\int_{\omega_j}^{\omega_{j+1}}\Big(F\big(\tfrac12(1+\tan^2 t)\xi,t\big)+O(\omega_{j+1}-\omega_j)\Big)\frac{dt}{\cos^2 t}$$

and $(\omega_{j+1}-\omega_j)^2\leqslant Q^{-2d}$, we find that

$$\mathcal{R}^{\theta}_{I_j,Q}(\xi)=\frac{Q^2}{\zeta(2)}\int_{\omega_j}^{\omega_{j+1}}F\big(\tfrac12(1+\tan^2 t)\xi,t\big)\frac{dt}{\cos^2 t}+O_{\xi,\varepsilon}(Q^{23/12+\varepsilon})=\mathcal{R}^{\theta}_{I_j^+,Q}(\xi).$$

This, together with Lemma 16(i), yields the equality from Proposition 15. □

[2]The argument from Section 7 applies before integrating with respect to t on $[0,\pi/4]$, showing that F is C^1.

8.2. ***Explicit formula for $g_2^{\mathfrak{A}}$.*** Next we compute the derivatives $B'_M(\xi)$, thus proving Corollary 1. We also obtain the explicit formula (8-11) for $g_2^{\mathfrak{A}}$ on a larger range than in Corollary 1, after computing the derivative $A'_{K,0}(\xi)$.

Lemma 17. *For $M \in \mathfrak{S}$, let $T = T_M$, $Z = Z_M$ as in (3-1). The derivative $B'_M(\xi)$ is given by*

$$\begin{cases} \dfrac{\pi}{4\xi^2} \ln\left(\dfrac{T+\sqrt{T^2-4}}{T+\sqrt{T^2-4-\xi^2}}\right) & \text{if } \xi \leqslant 2Z, \\[2ex] \dfrac{\pi}{8\xi^2} \ln\left(\dfrac{(T+\sqrt{T^2-4})^2(T-\sqrt{T^2-4-\xi^2})}{(4+4Z^2)(T+\sqrt{T^2-4-\xi^2})}\right) & \text{if } 2Z \leqslant \xi \leqslant \sqrt{T^2-4}, \\[2ex] \dfrac{\pi}{8\xi^2} \ln\left(\dfrac{(T+\sqrt{T^2-4})^2}{4+4Z^2}\right) & \text{if } \xi \geqslant \sqrt{T^2-4}. \end{cases}$$

Proof. Using (8-2), we proceed as in the proof of Lemma 13:

$$B_M(\xi) = \frac{\pi}{4\xi} \int_0^{\pi/2} \left(\frac{\xi}{\sqrt{T^2-4}} \cdot \frac{1}{U_T + \cos(2\theta-\theta_M)} - \frac{|\sin(2\theta-\theta_M)|}{U_T+\cos(2\theta-\theta_M)} \right)_+ d\theta,$$

where $U_T = T/\sqrt{T^2-4}$, and $\theta_M \in (0, \pi/2)$ has $\sin\theta_M = 2Z/\sqrt{T^2-4}$. Applying Lemma 11, we obtain

$$B'_M(\xi) = \frac{\pi}{4\xi^2} \int_I \frac{|\sin(2\theta-\theta_M)|}{U_T+\cos(2\theta-\theta_M)}\, d\theta,$$

with $I = \{\theta \in (0, \pi/2) : |\sin(2\theta-\theta_M)| < \xi/\sqrt{T^2-4}\}$. Clearly $I = (0, \pi/2)$ when $\xi > \sqrt{T^2-4}$, and if $\xi \leqslant \sqrt{T^2-4}$, let $\alpha = \alpha(\xi) \in (0, \pi/4)$ be such that $\sin 2\alpha = \xi/\sqrt{T^2-4}$. Then

$$\begin{aligned} \xi \leqslant 2Z &\iff \alpha \leqslant \theta_M/2 \iff I = [\theta_M/2-\alpha, \theta_M/2+\alpha], \\ 2Z \leqslant \xi \leqslant \sqrt{T^2-4} &\iff \alpha \in [\theta_M/2, \pi/4] \\ &\iff I = [0, \theta_M/2+\alpha] \cup [\pi/2+\theta_M/2-\alpha, \pi/2], \end{aligned}$$

and the integral is easy to compute. For $M = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\xi = 3$, the region with area $B_M(\xi/2, 0)$ is the one hatched vertically in Figure 6. □

A similar computation using (8-2) shows that $A'_{K,0}(\xi)$ is given by

$$\frac{\pi}{4\xi^2} \cdot \begin{cases} 0 & \text{if } \xi \leqslant 2K, \\ \ln(1+K^2) + \ln\left(\dfrac{(1+x_1^2)(1+(x_2-K)^2)}{(1+x_2^2)(1+(x_1-K)^2)}\right) & \text{if } \xi \in [2K, K\sqrt{K^2+4}], \\ \ln(1+K^2) & \text{if } \xi \geqslant K\sqrt{K^2+4}, \end{cases}$$

where $x_2 > x_1$ are the roots of

$$x^2(\xi+2K) - 2xK(\xi+K) + \xi(K^2+1) - 2K = 0.$$

By the last paragraph in Remark 14, the body $T_{1,1,\xi}$ is empty, so $A_{1,1}(\xi)=0$, and we have an explicit formula on a larger range than in the introduction:

$$g_2^{\mathfrak{A}}\Big(\frac{3}{4\pi}\xi\Big)=\frac{32\pi}{9\zeta(2)}\bigg(\sum_{M\in\mathfrak{S}}B'_M(\xi)+A'_{1,0}(\xi)\bigg),\quad 0<\xi\leqslant 4. \tag{8-11}$$

We can now explain the presence of the spikes in the graph of $g_2^{\mathfrak{A}}$ in Figure 1. The function $B'_M(\xi)$ is not differentiable at $\xi=2F$ and $\sqrt{T^2-4}$, while the function $A'_{K,0}(\xi)$ is not differentiable at $\xi=2K$ and $\sqrt{(K^2+2)^2-4}$. At the point $\xi=\sqrt{5}$, two of the functions $B'_M(\xi)$, as well as $A'_{1,0}(\xi)$, have infinite slopes on the left, which gives the spike on the graph of $g_2^{\mathfrak{A}}(x)$ at $x=(3/4\pi)\sqrt{5}$.

Acknowledgments

We thank the referees for their constructive comments, which led to improvements and clarifications in the presentation. Boca and Popa were supported in part by the CNCS - UEFISCDI grant PN-II-RU-TE-2011-3-0259. Paşol was supported in part by grant CNCSIS RU-TE-2011-3-0053. Popa was supported in part by European Community's Marie Curie grant PIRG05-GA-2009-248569. Zaharescu was supported in part by NSF grant DMS-0901621.

References

[Boca 2007] F. P. Boca, "Distribution of angles between geodesic rays associated with hyperbolic lattice points", *Q. J. Math.* **58**:3 (2007), 281–295. MR 2008j:11142 Zbl 1197.11134

[Boca and Zaharescu 2005] F. P. Boca and A. Zaharescu, "The correlations of Farey fractions", *J. London Math. Soc.* (2) **72**:1 (2005), 25–39. MR 2006h:11086 Zbl 1089.11037

[Boca et al. 2000] F. P. Boca, C. Cobeli, and A. Zaharescu, "Distribution of lattice points visible from the origin", *Comm. Math. Phys.* **213**:2 (2000), 433–470. MR 2001j:11094 Zbl 0989.11049

[Boca et al. 2001] F. P. Boca, C. Cobeli, and A. Zaharescu, "A conjecture of R. R. Hall on Farey points", *J. Reine Angew. Math.* **535** (2001), 207–236. MR 2002f:11127 Zbl 1006.11053

[Boca et al. 2013] F. P. Boca, A. A. Popa, and A. Zaharescu, "Pair correlation of hyperbolic lattice angles", preprint, 2013. arXiv 1302.5067

[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 1484478 Zbl 0898.68039

[Chamizo 2006] F. Chamizo, "Non–Euclidean visibility problems", *Proc. Indian Acad. Sci. Math. Sci.* **116**:2 (2006), 147–160. MR 2006m:52012 Zbl 1126.11033

[Estermann 1961] T. Estermann, "On Kloosterman's sum", *Mathematika* **8** (1961), 83–86. MR 23 #A3716 Zbl 0114.26302

[Fricke and Klein 1892] R. Fricke and F. Klein, *Vorlesungen über die Theorie der Elliptischen Modulfunktionen, II*, Teubner, Leipzig, 1892.

[Good 1983] A. Good, "On various means involving the Fourier coefficients of cusp forms", *Math. Z.* **183**:1 (1983), 95–129. MR 84g:10052 Zbl 0497.10015

[Gorodnik and Nevo 2012] A. Gorodnik and A. Nevo, "Counting lattice points", *J. Reine Angew. Math.* **663** (2012), 127–176. MR 2889708 Zbl 1248.37011

[Hall and Tenenbaum 1984] R. R. Hall and G. Tenenbaum, "On consecutive Farey arcs", *Acta Arith.* **44**:4 (1984), 397–405. MR 86e:11087 Zbl 0553.10011

[Hooley 1957] C. Hooley, "An asymptotic formula in the theory of numbers", *Proc. London Math. Soc.* (3) **7** (1957), 396–413. MR 19,839c Zbl 0079.27301

[Iwaniec 2002] H. Iwaniec, *Spectral methods of automorphic forms*, 2nd ed., Graduate Studies in Mathematics **53**, Amer. Math. Soc., Providence, RI, 2002. MR 2003k:11085 Zbl 1006.11024

[Kelmer and Kontorovich 2013] D. Kelmer and A. Kontorovich, "On the pair correlation density for hyperbolic angles", preprint, 2013. arXiv 1308.0754

[Narkiewicz 1983] W. Narkiewicz, *Number theory*, World Scientific, Singapore, 1983. MR 85j:11002 Zbl 0528.10001

[Nicholls 1983] P. Nicholls, "A lattice point problem in hyperbolic space", *Michigan Math. J.* **30**:3 (1983), 273–287. MR 85f:11071 Zbl 0537.30033

[Nicholls 1989] P. J. Nicholls, *The ergodic theory of discrete groups*, London Mathematical Society Lecture Note Series **143**, Cambridge University Press, 1989. MR 91i:58104 Zbl 0674.58001

[Pollicott and Sharp 2006] M. Pollicott and R. Sharp, "Correlations for pairs of closed geodesics", *Invent. Math.* **163**:1 (2006), 1–24. MR 2007a:37036 Zbl 1081.37016

[Risager and Rudnick 2009] M. S. Risager and Z. Rudnick, "On the statistics of the minimal solution of a linear Diophantine equation and uniform distribution of the real part of orbits in hyperbolic spaces", pp. 187–194 in *Spectral analysis in geometry and number theory* (Nagoya, 2007), edited by M. Kotani et al., Contemp. Math. **484**, Amer. Math. Soc., Providence, RI, 2009. MR 2010b:11076 Zbl 1189.11036

[Risager and Truelsen 2010] M. S. Risager and J. L. Truelsen, "Distribution of angles in hyperbolic lattices", *Q. J. Math.* **61**:1 (2010), 117–133. MR 2011i:11102 Zbl 1194.11081

[Sarnak 2007] P. Sarnak, "Reciprocal geodesics", pp. 217–237 in *Analytic number theory* (Göttingen, 2005), edited by W. Duke and Y. Tschinkel, Clay Math. Proc. **7**, Amer. Math. Soc., Providence, RI, 2007. MR 2009a:11184 Zbl 1198.11039

[Stein et al. 2012] W. A. Stein et al., Sage Mathematics Software (Version 5.0.1), 2012, Available at http://www.sagemath.org.

[Weil 1948] A. Weil, "On some exponential sums", *Proc. Nat. Acad. Sci. U. S. A.* **34** (1948), 204–207. MR 10,234e Zbl 0032.26102

[Yao and Knuth 1975] A. C. Yao and D. E. Knuth, "Analysis of the subtractive algorithm for greatest common divisors", *Proc. Nat. Acad. Sci. U.S.A.* **72**:12 (1975), 4720–4722. MR 54 #5102 Zbl 0315.10005

Communicated by Brian Conrad
Received 2013-09-03 Revised 2013-10-21 Accepted 2013-11-22

fboca@illinois.edu — *Department of Mathematics, University of Illinois, 1409 W. Green Street, Urbana, IL 61801, United States*

vicentiu.pasol@imar.ro — *Simion Stoilow Institute of Mathematics of the Romanian Academy, P.O. Box 1-764, 014700 Bucharest, Romania*

alexandru.popa@imar.ro — *Simion Stoilow Institute of Mathematics of the Romanian Academy, P.O. Box 1-764, 014700 Bucharest, Romania*

zaharesc@illinois.edu — *Department of Mathematics, University of Illinois, 1409 W. Green Street, Urbana, IL 61801, United States*

ALGEBRA AND NUMBER THEORY 8:4 (2014)
dx.doi.org/10.2140/ant.2014.8.1037

Étale contractible varieties in positive characteristic

Armin Holschbach, Johannes Schmidt and Jakob Stix

Unlike in characteristic 0, there are no nontrivial smooth varieties over an algebraically closed field k of characteristic $p > 0$ that are contractible in the sense of étale homotopy theory.

1. Introduction

Homotopy theory is founded on the idea of contracting the interval, either as a space, or as an actual homotopy, that is, a path in a space of maps. In algebraic geometry, the affine line $\mathbb{A}^1_k$ serves as an algebraic equivalent of the interval, at least in characteristic 0, where $\mathbb{A}^1_k$ is contractible.

Matters differ in characteristic $p > 0$, where $\pi_1(\mathbb{A}^1_k)$ is an infinite group: a group G occurs as a finite quotient of $\pi_1(\mathbb{A}^1_k)$ precisely if G is a quasi-p-group due to Abhyankar's conjecture for the affine line as proven by Raynaud. This raises the question whether there is an étale contractible variety in positive characteristic.

Theorem 1. *Let k be an algebraically closed field of characteristic $p > 0$. A smooth variety U/k is étale contractible if and only if $U = \mathrm{Spec}(k)$ is the point.*

It turns out that our discussion in positive characteristic depends only on H^1 and H^2. By the étale Hurewicz and Whitehead theorems (see [Artin and Mazur 1969, §4]), we might therefore replace "étale contractible" with "étale 2-connected" in Theorem 1. Further, our proof covers more than just smooth varieties. Here is the more precise result, which proves Theorem 1 because smooth varieties have big Cartier divisors.

Theorem 2. *Let k be an algebraically closed field of characteristic $p > 0$ and let U/k be a normal variety such that*

(i) *the group $\mathrm{H}^1_{\text{ét}}(U, \mathbb{F}_p)$ vanishes,*

(ii) *there is a prime number $\ell \neq p$ such that $\mathrm{H}^2_{\text{ét}}(U, \mu_\ell) = 0$,*

Supported by DFG-Forschergruppe 1920, "Symmetrie, Geometrie und Arithmetik", Heidelberg–Darmstadt.
MSC2010: 14F35.
Keywords: étale homotopy theory, étale contractible.

(iii) *U has a big Cartier divisor or* $\dim U \leq 2$.

Then U has dimension 0.

In order to show the range of varieties to which Theorem 2 applies, we list in Proposition 4 properties of varieties that imply the existence of big Cartier divisors, including quasiprojective varieties and locally $\mathbb{Q}$-factorial (in particular smooth) varieties. The proof of Theorem 2 in the presence of a big Cartier divisor will be given in Section 2.3. The case of normal surfaces will be treated in Section 3.

In the proof of Theorem 2, one would like to work with a compactification $U \subseteq X$ and the geometry of line bundles on U versus X. For that strategy to work, we need a compactification that is locally factorial along $Y = X \setminus U$. Since in characteristic $p > 0$, resolution of singularities is presently absent in dimension ≥ 4, we resort to desingularisation by alterations due to de Jong. Unfortunately, the alteration typically destroys the étale contractibility assumption. We first deduce more *coherent* properties from étale 2-connectedness that transfer to the alteration.

The key difference with characteristic 0 comes from Artin–Schreier theory relating $\mathrm{H}^1_{\text{ét}}(U, \mathbb{F}_p)$ to regular functions on U.

Remark 3. Let us illustrate the situation in characteristic 0 in contrast to Theorem 1.

(1) There are contractible complex smooth surfaces other than $\mathbb{A}^2_{\mathbb{C}}$. The first such example is due to Ramanujam [1971, §3]; see also [tom Dieck and Petrie 1990] for explicit equations. All of them are affine and have rational smooth projective completions.

(2) Smooth varieties $U/\mathbb{C}$ different from affine space $\mathbb{A}^n_{\mathbb{C}}$ but with $U(\mathbb{C})$ diffeomorphic to $\mathbb{C}^n$ are known as exotic algebraic structures on $\mathbb{C}^n$. These varieties are contractible and we recommend the Bourbaki talk on $\mathbb{A}^n$ by Kraft [1996], or the survey by Zaĭdenberg [1999]. A remarkable nonaffine (but quasiaffine) example U was obtained by Winkelmann [1990] as a quotient $U = \mathbb{A}^5/\mathbb{G}_{\mathrm{a}}$, and more concretely as the complement in a smooth projective quadratic hypersurface in $\mathbb{P}^5_{\mathbb{C}}$ of the union of a hyperplane and a smooth surface.

(3) The notion of $\mathbb{A}^1$-contractibility is a priori stronger than contractibility in the complex topology. Asok and Doran [2007] construct, for every $d \geq 6$, continuous families of pairwise nonisomorphic, nonaffine smooth varieties of dimension d that are even $\mathbb{A}^1$-contractible.

Notation. Throughout the note, k will be an algebraically closed field. By definition, a variety over k is a separated scheme of finite type over k. We will denote the étale fundamental group by π_1 and its maximal abelian quotient by π_1^{ab}. The sheaf μ_ℓ for ℓ different from the characteristic denotes the (locally) constant sheaf of ℓ-th roots of unity.

2. Big Cartier divisors

2.1. *Existence of big divisors.* Recall that a Cartier divisor D on a normal (but not necessarily proper) variety U/k is big if the rational map associated to the linear system $|mD|$ is generically finite for $m \gg 0$.

Proposition 4. *Let k be an algebraically closed field and let U/k be a normal variety such that one of the following holds*:

(a) *U is quasiprojective.*

(b) *U is a product of varieties with big divisors.*

(c) *U is locally $\mathbb{Q}$-factorial everywhere.*

Then U has a big Cartier divisor.

Proof. Since any ample divisor is big, the conclusion holds if we assume (a). In case (b), the sum of the pullbacks of big Cartier divisors on the factors is again big.

If (c) holds, then we first choose a dense affine open $V \subseteq U$ and an effective big Cartier divisor D on V by (a). Let $B = U \setminus V$ be the boundary, in fact a Weil divisor since V is affine, and let D' be the Zariski closure of D as a Weil divisor on U. By assumption, mD' and mB are both effective Cartier divisors for $m \gg 0$, and there are sections $s_0, \dots, s_d \in \mathrm{H}^0(V, mD)$ such that the induced map $V \to \mathbb{P}^d_k$ is generically finite. For $r \gg 0$, the sections s_i extend to sections of

$$\mathrm{H}^0(U, mD + mrB),$$

so that $mD + mrB$ is the desired big Cartier divisor on U. □

2.2. *Geometry of varieties with vanishing* $\mathbf{H^1}$ *and* $\mathbf{H^2}$. Let ℓ be a prime number different from the characteristic of k and let U/k be a variety with $\mathrm{H}^2_{\text{ét}}(U, \mu_\ell) = 0$. It follows from the Kummer sequence in étale cohomology that $\mathrm{Pic}(U)$ is an ℓ-divisible abelian group.

The following crucially depends on k being a field of positive characteristic.

Proposition 5. *Let k be of characteristic $p > 0$. If U/k is a connected reduced variety such that $\pi_1^{\mathrm{ab}}(U) \otimes \mathbb{F}_p$ is finite, then* $\mathrm{H}^0(U, \mathbb{O}_U) = k$.

Proof. We argue by contradiction. If $f : U \to \mathbb{A}^1_k$ is a dominant map, then the induced map

$$f_* : \pi_1^{\mathrm{ab}}(U) \otimes \mathbb{F}_p \to \pi_1^{\mathrm{ab}}(\mathbb{A}^1_k) \otimes \mathbb{F}_p$$

has image of finite index in the infinite group $\pi_1^{\mathrm{ab}}(\mathbb{A}^1_k) \otimes \mathbb{F}_p$, a contradiction. □

By the duality $\mathrm{H}^1_{\text{ét}}(U, \mathbb{F}_p) = \mathrm{Hom}(\pi_1^{\mathrm{ab}}(U), \mathbb{F}_p)$, the vanishing of $\mathrm{H}^1_{\text{ét}}(U, \mathbb{F}_p)$ implies the assumption of Proposition 5.

2.3. ***Using alterations.*** Section 2.2 reduces the proof of Theorem 2 in the presence of a big Cartier divisor to the following proposition.

Proposition 6. *Let k be an algebraically closed field and let U/k be a connected normal variety with a big Cartier divisor and such that*

(i) $\mathrm{H}^0(U, \mathcal{O}_U) = k$ *and*

(ii) *there is a prime number ℓ such that* $\mathrm{Pic}(U)$ *is ℓ-divisible.*

Then U has dimension 0.

Proof. By [de Jong 1996, Theorem 7.3], there exists an alteration, that is, a generically finite projective map $h : \tilde{U} \to U$ such that $\tilde{U}$ can be embedded into a connected smooth projective variety $\tilde{X}$.

Step 1. The maximal open $V \subset U$, such that the restriction $\tilde{V} = h^{-1}(V) \to V$ is a finite map, has boundary $U \setminus V$ of codimension at least 2, since U is normal.

The k-algebra $\mathrm{H}^0(\tilde{V}, \mathcal{O}_{\tilde{V}})$ is an integral domain inside the function field of $\tilde{V}$. The minimal polynomial for $s \in \mathrm{H}^0(\tilde{V}, \mathcal{O}_{\tilde{V}})$ with respect to the function field of V has coefficients that are regular functions on V by normality and uniqueness of the minimal polynomial. Hence these coefficients are elements of $\mathrm{H}^0(V, \mathcal{O}_V) = \mathrm{H}^0(U, \mathcal{O}_U) = k$, and so

$$\mathrm{H}^0(\tilde{V}, \mathcal{O}_{\tilde{V}}) = k.$$

Step 2. By the theorem of the base [Kleiman 1971, Theorem 5.1], the Néron–Severi group

$$\mathrm{NS}(\tilde{X}) = \mathrm{Pic}(\tilde{X}) / \mathrm{Pic}^0(\tilde{X})$$

is a finitely generated abelian group. Since the restriction map $\mathrm{Pic}(\tilde{X}) \twoheadrightarrow \mathrm{Pic}(\tilde{U})$ is surjective, the induced composite map

$$h^* : \mathrm{Pic}(U) \to \mathrm{coker}\big(\mathrm{Pic}^0(\tilde{X}) \to \mathrm{Pic}(\tilde{U})\big) \tag{2-1}$$

maps an ℓ-divisible group to a finitely generated abelian group, and hence has finite image.

Step 3. Let D be a big Cartier divisor on U. Since $h : \tilde{U} \to U$ is generically finite, the divisor h^*D is also a big Cartier divisor. Moreover, as in the proof of Proposition 4, there is a big divisor $\tilde{D}$ on $\tilde{X}$ that restricts to h^*D on $\tilde{U}$. Upon replacing D and $\tilde{D}$ by a positive multiple, we may assume, by the finiteness of the image of the map (2-1), that $\tilde{D}$ is algebraically and thus numerically equivalent to a divisor B on $\tilde{X}$ that is supported in $\tilde{X} \setminus \tilde{U}$.

Since bigness on projective varieties only depends on the numerical equivalence class, see [Lazarsfeld 2004, Corollary 2.2.8], the divisor B is also big. Restriction to $\tilde{V}$ yields

$$\bigcup_{n \geq 0} \mathrm{H}^0(\tilde{X}, \mathcal{O}_{\tilde{X}}(nB)) \subseteq \mathrm{H}^0(\tilde{V}, \mathcal{O}_{\tilde{V}}) = k,$$

by Step 1 above. We conclude that $\dim U = \dim \tilde{X} = 0$ by the bigness of B. □

2.4. *Complementing example.* We illustrate the importance of the presence of a big divisor in Theorem 2 or Proposition 6 by an example from toric geometry.

We first recall two facts about complete toric varieties that are standard analytically over $\mathbb{C}$ and that have étale counterparts for toric varieties over arbitrary algebraically closed base fields, in particular of characteristic $p > 0$.

Lemma 7. *Let k be an algebraically closed field. Any complete toric variety X/k is étale simply connected*: $\pi_1(X) = \mathbf{1}$.

Proof. By toric resolution, see [Fulton 1993, §2.6], there is a resolution of singularities $\tilde{X} \to X$ with a smooth projective toric variety $\tilde{X}$. Birational invariance of the étale fundamental group shows $\pi_1(\tilde{X}) = \pi_1(\mathbb{P}^n_k) = \mathbf{1}$, and the surjection $\pi_1(\tilde{X}) \twoheadrightarrow \pi_1(X)$ shows that X is étale 1-connected. □

Lemma 8. *Let k be an algebraically closed field of characteristic p, and let X/k be a complete toric variety. Then for all $\ell \neq p$ we have*

$$\mathrm{H}^2_{\text{ét}}(X, \mathbb{Z}_\ell(1)) \simeq \mathrm{Pic}(X) \otimes \mathbb{Z}_\ell.$$

Proof. In the context of toric varieties over $\mathbb{C}$ and with respect to singular cohomology, this is [Fulton 1993, Corollary in 3.4]. The ℓ-adic case for toric varieties over an algebraically closed field k of characteristic $\neq \ell$ follows with a parallel proof. □

Example 9. Let $U = X$ be a complete normal nonprojective toric variety X of dimension 3 with trivial Picard group. Such toric varieties have been constructed in [Eikelberg 1992, Example 3.5; Fulton 1993, pp. 25–26, 65]. These sources construct X over $\mathbb{C}$ but the constructions work mutatis mutandis over any algebraically closed base field k. Then

(i) $\mathrm{H}^1_{\text{ét}}(X, \mathbb{F}_p) = 0$ by Lemma 7, and

(ii) $\mathrm{H}^2_{\text{ét}}(X, \mathbb{Z}_\ell(1)) = 0$ for all $\ell \neq p$ by Lemma 8, and since there is nontrivial torsion in ℓ-adic cohomology only for finitely many primes [Gabber 1983], we conclude that $\mathrm{H}^2(X, \mu_\ell) = 0$ for almost all $\ell \neq p$.

Therefore the assumptions of Theorem 2 hold, with the exception of the presence of a big Cartier divisor. Nevertheless, these toric varieties are not étale contractible since $\mathrm{H}^6_{\text{ét}}(X, \mathbb{Z}_\ell(3)) = \mathbb{Z}_\ell$.

3. Normal surfaces

In this section, Proposition 10 completes the proof of Theorem 2 for surfaces. Not every normal surface admits a big Cartier divisor, so something needs to be done. Examples of proper normal surfaces with trivial Picard group, in particular without big divisors, can be found in [Nagata 1958; Schröer 1999]. However, on a hypothetical normal 2-contractible surface, a specialisation argument allows us to conclude the existence of a big Cartier divisor in general.

Proposition 10. *There is no normal connected surface U/k over an algebraically closed field k of characteristic $p > 0$ such that*

(i) $\mathrm{H}^1_{\text{ét}}(U, \mathbb{F}_p) = 0$ *and*

(ii) $\mathrm{H}^2_{\text{ét}}(U, \mu_\ell) = 0$ *for some prime number $\ell \neq p$.*

Proof. We argue by contradiction and assume that U is a surface as in the proposition. By Nagata's embedding theorem and resolution of singularities for surfaces, U is a dense open in a normal proper surface X/k with boundary $Y = X \setminus U$ being a normal crossing divisor. Hence, X is smooth in a neighbourhood of Y.

By limit arguments, we may spread out over an integral scheme S of finite type over $\mathbb{F}_p$, that is, there is a proper flat $f : \mathscr{X} \to S$, a relative Cartier divisor $\mathscr{Y}$ in $\mathscr{X}/S$ with normal crossing relative to S and complement $\mathscr{U} = \mathscr{X} \setminus \mathscr{Y}$ such that

(a) all fibres are normal proper surfaces;

(b) there is a point $\eta : \mathrm{Spec}(k) \to S$ over the generic point of S such that the fibre over η agrees with the original $\mathscr{X}_\eta = X$ together with $\mathscr{U}_\eta = U$ and $\mathscr{Y}_\eta = Y$;

(c) the set of irreducible components of the fibres of $\mathscr{Y}$ forms a constant system, and each component of $\mathscr{Y}$ is a Cartier divisor; and

(d) the higher direct image $\mathrm{R}^2 f|_{\mathscr{U}*}\mu_\ell$ is locally constant and commutes with arbitrary base change by [Deligne 1977, Finitude, Theorem 1.9].

Since the generic stalk $(\mathrm{R}^2 f|_{\mathscr{U}*}\mu_\ell)_\eta = \mathrm{H}^2_{\text{ét}}(U, \mu_\ell) = 0$ vanishes, we conclude that for all geometric points $\bar{s} \in S$, we have $\mathrm{H}^2_{\text{ét}}(\mathscr{U}_{\bar{s}}, \mu_\ell) = 0$, where $\mathscr{U}_{\bar{s}}$ is the fibre of $\mathscr{U} \to S$ in $\bar{s}$. As in the proof of Proposition 6, this implies that for every Cartier divisor D on $\mathscr{X}_{\bar{s}}$, there are an $m \geq 1$ and a Cartier divisor E on $\mathscr{X}_{\bar{s}}$ supported in $\mathscr{Y}_{\bar{s}}$ such that $mD \equiv E$ are numerically equivalent.

We apply this insight to a geometric fibre $\mathscr{X}_{\bar{t}}$ above a closed point $t \in S$. Since by [Artin 1962, Corollary 2.11], all proper normal surfaces over the algebraic closure of a finite field are projective, we conclude that there is a very ample Cartier divisor $H_{\bar{t}}$ on $\mathscr{X}_{\bar{t}}$ with support contained in $\mathscr{Y}_{\bar{t}}$.

Let $\mathscr{H} \hookrightarrow \mathscr{X}$ be the relative Cartier divisor with support in $\mathscr{Y}$ that specialises to $H_{\bar{t}}$. By [Grothendieck 1961, Théorème 4.7.1], the divisor $\mathscr{H}$ is ample relative to S in an open neighbourhood of $t \in S$. Consequently, the normal proper surface X is projective, and in particular, U admits a big divisor. The part of Theorem 2 proven in Section 2.3 leads to a contradiction. $\square$

Remark 11. It follows from the proof of Proposition 10 that any proper nonprojective normal surface X with trivial Picard group, in particular the examples of [Nagata 1958; Schröer 1999], must have $\mathrm{H}^2_{\text{ét}}(X, \mu_\ell) \neq 0$ and a fortiori must contain nontrivial ℓ-torsion classes in the cohomological Brauer group $\mathrm{Br}(X)$ for all ℓ different from the characteristic. The existence of nontrivial torsion classes in $\mathrm{Br}(X)$ under the above assumptions was proven by different methods in [Schröer 2001, proof of Theorem 4.1].

Acknowledgments

We would like to thank Alexander Schmidt and Malte Witte for comments on an earlier version of the paper.

References

[Artin 1962] M. Artin, "Some numerical criteria for contractability of curves on algebraic surfaces", *Amer. J. Math.* **84** (1962), 485–496. MR 26 #3704 Zbl 0105.14404

[Artin and Mazur 1969] M. Artin and B. Mazur, *Etale homotopy*, Lecture Notes in Mathematics **100**, Springer, Berlin, 1969. MR 39 #6883 Zbl 0182.26001

[Asok and Doran 2007] A. Asok and B. Doran, "On unipotent quotients and some $\mathbb{A}^1$-contractible smooth schemes", *Int. Math. Res. Pap.* **2007**:2 (2007), rpm005. MR 2008f:14061 Zbl 1157.14032

[Deligne 1977] P. Deligne, *Cohomologie étale: Séminaire de Géométrie Algébrique du Bois-Marie (SGA $4\frac{1}{2}$)*, Lecture Notes in Mathematics **569**, Springer, Berlin, 1977. MR 57 #3132 Zbl 0349.14008

[tom Dieck and Petrie 1990] T. tom Dieck and T. Petrie, "Contractible affine surfaces of Kodaira dimension one", *Japan. J. Math.* (*N.S.*) **16**:1 (1990), 147–169. MR 91j:14027 Zbl 0721.14018

[Eikelberg 1992] M. Eikelberg, "The Picard group of a compact toric variety", *Results Math.* **22**:1-2 (1992), 509–527. MR 93g:14060 Zbl 0786.14031

[Fulton 1993] W. Fulton, *Introduction to toric varieties*, Annals of Mathematics Studies **131**, Princeton University Press, 1993. MR 94g:14028 Zbl 0813.14039

[Gabber 1983] O. Gabber, "Sur la torsion dans la cohomologie l-adique d'une variété", *C. R. Acad. Sci. Paris Sér. I Math.* **297**:3 (1983), 179–182. MR 85f:14018 Zbl 0574.14019

[Grothendieck 1961] A. Grothendieck, "Éléments de géométrie algébrique, III: Étude cohomologique des faisceaux cohérents, I", *Inst. Hautes Études Sci. Publ. Math.* 11 (1961), 167. MR 36 #177c Zbl 0118.36206

[de Jong 1996] A. J. de Jong, "Smoothness, semi-stability and alterations", *Inst. Hautes Études Sci. Publ. Math.* 83 (1996), 51–93. MR 98e:14011 Zbl 0916.14005

[Kleiman 1971] S. Kleiman, "Les théorèmes de finitude pour le foncteur de Picard: Exposé XIII", pp. 616–666 in *Théorie des intersections et théorème de Riemann–Roch: Séminaire de Géométrie Algébrique du Bois–Marie 1966–1967* (SGA 6), edited by P. Berthelot et al., Lecture Notes in Mathematics **225**, Springer, Berlin, 1971. MR 50 #7133 Zbl 0227.14007

[Kraft 1996] H. Kraft, "Challenging problems on affine n-space", pp. 295–317 in *Séminaire Bourbaki* 1994/95 (Exposé 802 No. 5), Astérisque **237**, Société Mathématique de France, Paris, 1996. MR 97m:14042 Zbl 0892.14003

[Lazarsfeld 2004] R. Lazarsfeld, *Positivity in algebraic geometry, I: Classical setting: Line bundles and linear series*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **48**, Springer, Berlin, 2004. MR 2005k:14001a Zbl 1093.14501

[Nagata 1958] M. Nagata, "Existence theorems for nonprojective complete algebraic varieties", *Illinois J. Math.* **2** (1958), 490–498. MR 20 #3875 Zbl 0081.37503

[Ramanujam 1971] C. P. Ramanujam, "A topological characterisation of the affine plane as an algebraic variety", *Ann. of Math.* (2) **94** (1971), 69–88. MR 44 #4010 Zbl 0218.14021

[Schröer 1999] S. Schröer, "On non-projective normal surfaces", *Manuscripta Math.* **100**:3 (1999), 317–321. MR 2001c:14067 Zbl 0987.14031

[Schröer 2001] S. Schröer, "There are enough Azumaya algebras on surfaces", *Math. Ann.* **321**:2 (2001), 439–454. MR 2002i:14023 Zbl 1053.14017

[Winkelmann 1990] J. Winkelmann, "On free holomorphic $\mathbf{C}$-actions on $\mathbf{C}^n$ and homogeneous Stein manifolds", *Math. Ann.* **286**:1-3 (1990), 593–612. MR 90k:32094 Zbl 0708.32004

[Zaĭdenberg 1999] M. Zaĭdenberg, "Exotic algebraic structures on affine spaces", *Algebra i Analiz* **11**:5 (1999), 3–73. In Russian; translated in *St. Petersburg Math. J.* **11**:5 (2000), 703–760. MR 2001d:14069 Zbl 1002.14020

Communicated by Barry Mazur
Received 2013-10-31 Revised 2013-12-03 Accepted 2014-01-22

holschbach@mathi.uni-heidelberg *Mathematisches Institut, Universität Heidelberg, Im Neuenheimer Feld 288, 69120 Heidelberg, Germany*

jschmidt@mathi.uni-heidelberg.de *Mathematisches Institut, Universität Heidelberg, Im Neuenheimer Feld 288, 69120 Heidelberg, Germany*

stix@math.uni-frankfurt.de *Institut für Mathematik, Johann Wolfgang Goethe-Universität, Robert-Mayer-Strasse 6-8, 60325 Frankfurt am Main, Germany*

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 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 LaTeX but submissions in other varieties of TeX, 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 BibTeX 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 8 No. 4 2014