

Algebra & Number Theory

Volume 12

2018

No. 5

**Arithmetic functions in short intervals
and the symmetric group**

Brad Rodgers



Arithmetic functions in short intervals and the symmetric group

Brad Rodgers

We consider the variance of sums of arithmetic functions over random short intervals in the function field setting. Based on the analogy between factorizations of random elements of $\mathbb{F}_q[T]$ into primes and the factorizations of random permutations into cycles, we give a simple but general formula for these variances in the large q limit for arithmetic functions that depend only upon factorization structure. From this we derive new estimates, quickly recover some that are already known, and make new conjectures in the setting of the integers.

In particular we make the combinatorial observation that any function of this sort can be explicitly decomposed into a sum of functions u and v , depending on the size of the short interval, with u making a negligible contribution to the variance, and v asymptotically contributing diagonal terms only.

This variance evaluation is closely related to the appearance of random matrix statistics in the zeros of families of L -functions and sheds light on the arithmetic meaning of this phenomenon.

1. Historical background and motivation

The purpose of this paper is to explore a connection between two well-known phenomena in number theory: that the zeros of a family of L -functions distribute like the eigenvalues of a random matrix and that the prime factors of a random integer distribute like the cycles of a random permutation. We use this connection to give a general yet simple description for the statistical behavior of sums of arithmetic functions over short intervals. The results that we ultimately prove will make use of a function field analogy: they concern arithmetic functions defined on $\mathbb{F}_q[T]$ rather than the integers and we will require that $q \rightarrow \infty$. We begin this section however with a discussion of some historical conjectures and heuristics from the integers that motivate what follows. A statement of the most important results we prove may be found at the beginning of [Section 3](#) — our main results are [Theorems 3.1](#) and [3.2](#) along with [Corollary 3.5](#). Key use is made of a combinatorial variant of the explicit formula of Weil, [Theorem 7.1](#), which may be of independent interest.

We recall the following conjectures:

Conjecture 1.1 [[Good and Churchhouse 1968](#)]. As $X \rightarrow \infty$, for $H = X^\delta$ with $\delta \in (0, 1)$,

$$\frac{1}{X} \int_X^{2X} \left(\sum_{x \leq n \leq x+H} \mu(n) \right)^2 dx \sim \frac{6}{\pi^2} H.$$

MSC2010: primary 11M50; secondary 11N37, 11T55.

Keywords: arithmetic in function fields, random matrices, the symmetric group.

Conjecture 1.2 [Goldston and Montgomery 1987]. As $X \rightarrow \infty$ for $H = X^\delta$ with $\delta \in (0, 1)$,

$$\frac{1}{X} \int_X^{2X} \left(\sum_{x \leq n \leq x+H} \Lambda(n) - H \right)^2 dx \sim H(\log X - \log H).$$

In both conjectures, we consider random $x \in [X, 2X]$ and seek to compute the variance of the sum of an arithmetic function, $\mu(n)$ or $\Lambda(n)$, over the random short interval $[x, x + H]$. Here $\mu(n)$ is the Möbius function, which oscillates around the value 0, and $\Lambda(n)$ is the von Mangoldt function which has an average value of 1, by the prime number theorem. Similar conjectures can be made for, for instance, the higher order von Mangoldt functions $\Lambda_j(n)$ [Rodgers 2015] or the k -fold divisor function $d_k(n)$ [Keating et al. 2018], the latter of which is conjectured to display a very curious series of “phase changes” as the parameter δ varies. These conjectures are known to be closely related to the conjectural phenomenon that the zeros of families of L -functions tends to distribute like the eigenvalues of certain random matrices (see [Katz and Sarnak 1999] for an exposition on the latter phenomenon).

In the past few years, beginning with the work of Keating and Rudnick [2014], function field variants of these conjectures have been proved. (In some cases the function field theorems have in fact motivated new conjectures.) In order to state these function field results, we make use of a well-known dictionary between the integers \mathbb{Z} and the ring of polynomials over a finite field, that is $\mathbb{F}_q[T]$. To review this dictionary and fix some of our notation:

- The collection of monic polynomials, \mathcal{M} , takes the place of positive integers.
- The degree, $\deg(f)$, of $f \in \mathcal{M}$ takes the place of $\log n$ for $n \in \mathbb{N}$.
- The collection of degree n monic polynomials, \mathcal{M}_n , takes the place of integers lying in a dyadic interval $[X, 2X]$.
- Irreducible polynomials take the role of primes.
- For $f \in \mathcal{M}$ and $h < \deg(f)$, the set $I(f; h) := \{g \in \mathcal{M} : \deg(f - g) \leq h\}$ is a short interval around the polynomial f , playing the role of $[x, x + H]$. (Here h may be thought of as corresponding to $\log H$.)

The reader should verify that $|\mathcal{M}_n| = q^n$, while $|I(f; h)| = q^{h+1}$. (Note that in the notation above, we have suppressed a dependence on the parameter q .)

This set up is explained more extensively in, for instance, the ICM address of Rudnick [2014] or the book of Rosen [2015]. We have the following analogues of Conjectures 1.1 and 1.2:

Theorem 1.3 [Rudnick 2014; Bae et al. 2015]. For fixed $0 \leq h \leq n - 5$, as $q \rightarrow \infty$,

$$\frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \left| \sum_{g \in I(f; h)} \mu(g) \right|^2 \sim q^{h+1}. \quad (1)$$

Theorem 1.4 [Keating and Rudnick 2014]. For fixed $0 \leq h \leq n - 5$, as $q \rightarrow \infty$,

$$\frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \left| \sum_{g \in I(f; h)} \Lambda(g) - q^{h+1} \right|^2 \sim q^{h+1}(n - h - 2). \quad (2)$$

For $g \in \mathcal{M}$, the Möbius function $\mu(g)$ is defined in analogy with the integers by $\mu(g) = (-1)^\ell$ if g is squarefree (that is g has no repeated factors) and $g = P_1 \cdots P_\ell$ in its prime factorization, and $\mu(g) = 0$ if g is squareful¹ (that is g is not squarefree). Likewise $\Lambda(g) = \deg(P)$ if $g = P^k$ for a prime P and a power $k \geq 1$, and $\Lambda(g) = 0$ otherwise.

We introduce a notation to write these results more succinctly. For a function $\eta : \mathcal{M}_n \rightarrow \mathbb{C}$, we define its mean value by

$$\mathbb{E}_{f \in \mathcal{M}_n} \eta(f) := \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \eta(f), \tag{3}$$

and its variance by

$$\text{Var}_{f \in \mathcal{M}_n} (\eta(f)) := \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} |\eta(f) - \mathbb{E}_{\mathcal{M}_n} \eta|^2. \tag{4}$$

Note that both the mean value and variance typically depend on the size of the field q . As a test of notation, the reader may easily verify that

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} 1 \right) = 0. \tag{5}$$

Likewise we see that (1) may be rewritten

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} \mu(g) \right) \sim q^{h+1}, \tag{6}$$

and (2)

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} \Lambda(g) \right) \sim q^{h+1}(n - h - 2), \tag{7}$$

as $q \rightarrow \infty$.

We may add another recent result to this list, due to Keating, the author, Roditty-Gershon, and Rudnick [Keating et al. 2018], for the k -fold divisor function, which is defined in analogy with the integers by $d_k(f) := |\{(a_1, \dots, a_k) \in \mathcal{M}^k : f = a_1 \cdots a_k\}|$.

Theorem 1.5. *For fixed positive integer k , and fixed $0 \leq h \leq n - 5$, as $q \rightarrow \infty$,*

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} d_k(g) \right) = q^{h+1} \mathcal{I}_k(n, n - h - 2) + O(q^{h+1/2}), \tag{8}$$

where $\mathcal{I}_k(m, N)$ is the count of lattice points $(x_{ij}) \in (\mathbb{Z})^{k^2}$ satisfying each of the following conditions:

- (i) $0 \leq x_{ij} \leq N$ for all $1 \leq i, j \leq k$.
- (ii) $x_{11} + \cdots + x_{kk} = m$.

¹There is a closely related terminology “square-full”, which means something quite different — namely that for prime P , if $P | g$, we have $P^2 | g$ also. The distinction is important to keep in mind. Square-full numbers will not play a role in this paper.

(iii) The array x_{ij} is weakly decreasing across columns and down rows. That is,

$$\begin{array}{cccc}
 x_{11} & \geq & x_{12} & \geq \cdots \geq & x_{1k} \\
 | \vee & & | \vee & & | \vee \\
 x_{21} & \geq & x_{22} & \geq \cdots \geq & x_{2k} \\
 | \vee & & | \vee & & | \vee \\
 \vdots & & \vdots & \ddots & \vdots \\
 | \vee & & | \vee & & | \vee \\
 x_{k1} & \geq & x_{k2} & \geq \cdots \geq & x_{kk}.
 \end{array}$$

Of the evaluations (5)–(8), only (5) may be proved easily (in fact trivially). Nonetheless, the estimate in (6), while deep, at least has a heuristic meaning that is easy to understand; it is just the claim that in expanding the variance into a sum over two indices, the Möbius function is so oscillatory that off-diagonal terms make no contribution. That is, (6) may be understood heuristically in the following way:

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} \mu(g) \right) = \frac{q^{h+1}}{q^n} \sum_{\substack{g_1, g_2 \\ \text{deg}(g_1 - g_2) \leq h}} \mu(g_1)\mu(g_2) \approx \frac{q^{h+1}}{q^n} \sum_{\substack{g_1, g_2 \in \mathcal{M}_n \\ g_1 = g_2}} \mu(g_1)\mu(g_2).$$

See for instance [Ng 2008] for a broader application of this heuristic in the setting of the integers, and see [Carmon and Rudnick 2014; Carmon 2015] for estimates of off-diagonal sums of the Möbius function in the function field setting.

The evaluation of the k -fold divisor function in (8) is obviously of a more complicated sort, even heuristically. In particular it may be seen that $\mathcal{I}_k(n; n - h - 2)$ is a piecewise polynomial, and for $k \geq 3$ as h ranges from 0 to $n - 5$, it exhibits several phase changes in its behavior in various ranges of h (see [Keating et al. 2018, §4]). The arithmetic reason for these phase changes in particular is rather mysterious.

Nonetheless, we make the following claim: (8) may be understood arithmetically as nothing more complicated than a combination of the phenomena that give rise to (5) and (6). For any degree n and short interval size h , we will observe that we may decompose

$$d_k(f) = u(f) + v(f),$$

where u and v are arithmetic functions, with $u(f)$ regular enough within the specified short intervals that (in analogy with (5)),

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} u(g) \right) = o(q^{h+1}), \tag{9}$$

while $v(f)$ is oscillatory and

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} v(g) \right) \sim q^{h+1} \cdot \frac{1}{q^{n+1}} \sum_{g \in \mathcal{M}_n} |v(g)|^2. \tag{10}$$

That is, as with the Möbius function, only diagonal terms contribute to its variance, in analogy with (6).

From Cauchy–Schwarz, it follows that

$$\mathrm{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f; h)} d_k(g) \right) \sim q^{h+1} \cdot \frac{1}{q^n} \sum_{g \in \mathcal{M}_n} |v(g)|^2.$$

This decomposition is explicit, based on symmetric function theory, and is given below — the quantity $\mathcal{I}_k(n; n - h - 2)$ may be recovered from it. That (9) holds for our function u will be a relatively shallow fact (having to do with the number of zeros of a certain family of L -functions), and one may think of u as being the largest piece of d_k with enough regularity that (9) holds for this reason. The intricacies of the variance estimate in (8) may thus be thought of as resulting from the fact that this decomposition changes for various values of n and h .

Such a decomposition is not limited to the k -fold divisor function. Any arithmetic functions whose value depends only upon the factorization type of its argument may be decomposed in this way and the variance of its sum over short intervals may thus be evaluated. What we mean by factorization type is defined formally below; roughly this is the size of all prime factors, listed with multiplicity. The functions $\mu(f)$, $\Lambda(f)$, $\Lambda_j(f)$, and $d_k(f)$ are all examples to which the result may be applied.

The evaluation of variance for such a general class of function is closely related to the known phenomena that the zeros of L -functions distribute like the eigenvalues of a random matrix. Indeed, the result we prove may be seen to be an equivalent restatement of an equidistribution result of Katz, [Theorem 4.2](#) below. (We make use of Katz’s theorem in our proof, and so we *do not* arrive at an independent proof of it however.)

We will use this general variance evaluation to recover several of the results that have been mentioned above with relatively little extra work and to derive new results that seem difficult by other means. New conjectures in the setting of the integers are put forward based on these results. Perhaps of particular interest, we consider sums of the function $\omega(n)$, counting prime factors; based on a function field model, we conjecture that the variance of sums of this function is somewhat smaller than a naive heuristic would lead one to believe.

In addition to yielding a pleasant general formula, the decomposition results of this paper help elucidate why random matrix universality should make an appearance in number theory. A complementary perspective as to the arithmetic reasons for the appearance of random matrix theory in number theory, dealing with the integers themselves, has appeared in the work of Bogomolny and Keating [[1995](#); [1996](#)] and in work of Conrey and Keating [[2015a](#); [2015b](#); [2015c](#); [2016](#)]. It would be very interesting to see if the combinatorial decompositions in the present paper can be extended to the setting of the integers in a way consistent with various conjectures that have been made there.

We finally note a recent application of our main results to algebraic geometry proper; by combining [Theorem 3.1](#) with other work of their own, Hast and Matei [[2016](#)] have given a geometric interpretation of this result. Indeed, it may be possible and it would be interesting to prove [Theorem 3.1](#) of this paper directly through algebro-geometric means.

2. The symmetric group and factorization type

2A. The decomposition described in [Section 1](#) and the corresponding estimates for variance hinge upon a well-known analogy between the prime factors of a random integer or element of $\mathbb{F}_q[T]$ and the cycles of a random permutation. (Later an application of symmetric function theory to the zeros of L -functions will play an equally important and dual role.)

We begin by recalling how it is that factorizations over $\mathbb{F}_q[T]$ resemble the cycles of permutations.

Recall that \mathcal{M}_n , the collection of monic polynomials of degree n , consists of q^n elements. Recall also that a partition λ of a positive integer n is defined to be a sequence of nonincreasing positive integers $(\lambda_1, \lambda_2, \dots, \lambda_k)$ such that for $|\lambda| := \lambda_1 + \dots + \lambda_k$ we have $|\lambda| = n$. We will also use the notation $\lambda \vdash n$ to indicate that λ is a partition of n .

Definition 2.1. For an element f of \mathcal{M}_n that is squarefree, if f has prime factorization $f = P_1 P_2 \cdots P_k$ with $\deg P_1 \geq \deg P_2 \geq \dots$, we define the *factorization type* to be the partition of n given by

$$\tau_f = (\deg P_1, \dots, \deg P_k).$$

For f that is not squarefree (i.e., squareful) we adopt the convention that $\tau_f = \emptyset$ (the empty partition).

In the above definition we have fixed our attention on the squarefrees because as $q \rightarrow \infty$ nearly all elements of \mathcal{M}_n are squarefree [[Carlitz 1932](#), §6]; see also [[Rosen 2002](#), Proposition 2.3] or [[Weiss 2013](#), Theorem 4.1]:

$$\frac{1}{q^n} \#\{f \in \mathcal{M}_n : f \text{ squarefree}\} = 1 - O\left(\frac{1}{q}\right). \quad (11)$$

Note that likewise any element σ of the symmetric group \mathfrak{S}_n on n elements can be written uniquely as a product of disjoint cycles: $\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$. Denote the lengths of the cycles by $|\sigma_i|$. For instance $|(245)| = 3$, where we have used cycle notation to represent the permutation.

Definition 2.2. For an element $\sigma \in \mathfrak{S}_n$, with $\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$ and $|\sigma_1| \geq |\sigma_2| \geq \dots$ we define the *cycle type* to be the partition of n given by

$$\tau_\sigma = (|\sigma_1|, \dots, |\sigma_k|).$$

It is well known that as $q \rightarrow \infty$ the distribution over \mathcal{M}_n of factorization types tends to the distribution of cycle types in \mathfrak{S}_n [[Andrade et al. 2015](#)]:

Proposition 2.3. For a partition $\lambda \vdash n$,

$$\lim_{q \rightarrow \infty} \mathbb{P}_{f \in \mathcal{M}_n}(\tau_f = \lambda) = \mathbb{P}_{\sigma \in \mathfrak{S}_n}(\tau_\sigma = \lambda).$$

Here and in what follows we have used elementary probabilistic notation, for instance

$$\mathbb{P}_{f \in \mathcal{M}_n}(\tau_f = \lambda) := \frac{1}{q^n} \#\{f \in \mathcal{M}_n : \tau_f = \lambda\}.$$

There is a well-known expression for the probability that a random permutation has a cycle structure λ , due to Cauchy. We use the standard partition frequency notation $\lambda = \langle 1^{m_1} 2^{m_2} \dots j^{m_j} \rangle$; this means for $\lambda = (\lambda_1, \lambda_2, \dots)$, that m_1 of the parts of λ are equal to 1, m_2 are equal to 2, etc. So if $\tau_\sigma = \langle 1^{m_1} 2^{m_2} \dots j^{m_j} \rangle$, σ has m_1 1-cycles, m_2 2-cycles, etc. With this notation, Cauchy’s result is that

$$\mathbb{P}_{\sigma \in \mathfrak{S}_n}(\tau_\sigma = \lambda) = \mathbf{p}(\lambda), \quad \text{where } \mathbf{p}(\lambda) := \prod_{i=1}^j \frac{1}{i^{m_i} m_i!}. \tag{12}$$

It is worth mentioning a recent result of Andrade, Bary-Soroker, and Rudnick [Andrade et al. 2015] that has generalized this picture. They show that the factorization types of a random polynomial f and a shift $f + \alpha$ become independent as $q \rightarrow \infty$:

Theorem 2.4 (Andrade, Bary-Soroker, and Rudnick). *For partitions λ and $\nu \vdash n$, uniformly for $\deg(\alpha) < n$,*

$$\mathbb{P}_{f \in \mathcal{M}_n}(\tau_f = \lambda, \tau_{f+\alpha} = \nu) = \mathbf{p}(\lambda)\mathbf{p}(\nu) + O(q^{-1/2}).$$

In fact they demonstrate this independence even for multiple shifts: the factorization types of $f + \alpha_1, f + \alpha_2, \dots, f + \alpha_k$ become independent as well.

2B. In this paper we will be concerned with the distribution of arithmetic functions $a : \mathcal{M} \mapsto \mathbb{C}$ such that $a(f)$ depends only upon the size and exponents of the prime factors of f . To make a more formal definition, if f has prime factorization $P_1^{e_1} \dots P_k^{e_k}$, with P_1, \dots, P_k monic primes, we call the data $(\deg P_1, e_1; \dots; \deg P_k, e_k)$, the *extended factorization type* of f . We will be concerned with functions a such that $a(f)$ is defined for all monic $f \in \mathbb{F}_q[T]$ for all q and such that the value $a(f)$ depends only on the extended factorization type of f ; we call such functions *factorization functions*. The class of factorization functions includes, for instance, the Möbius function $\mu(f)$, the von Mangoldt function $\Lambda(f)$, the count-of-divisors function $d(f)$, the indicator function of degree n polynomials $\mathbf{1}[\deg(f) = n]$, the indicator function of squarefree polynomials $\mu(n)^2$, etc. It does not include Dirichlet characters, for instance.

It is evident that for each n , the linear space of factorization functions supported on degree n polynomials is of finite dimension. The space of factorization functions supported on degree n squarefree polynomials is likewise of (smaller) finite dimension. In invoking the symmetric group, Proposition 2.3 and Theorem 2.4 suggest that the space of factorization functions has an important basis that may provide useful information: namely the irreducible characters of \mathfrak{S}_n .

In describing how such characters may be applied to elements of $\mathbb{F}_q[T]$, we suppose the reader is familiar with the most basic outlines of representation theory over \mathfrak{S}_n , along the lines of, for instance, Chapter 4 of [Fulton and Harris 1991]. We recall that the space of class functions of \mathfrak{S}_n are those functions $a(\sigma)$ with a value depending only on the cycle type the permutation σ and that a basis for such functions is given by the irreducible characters, for which we use the notation²

$$X^\lambda(\sigma).$$

²We use the letter X rather than the more traditional χ to distinguish these characters from Dirichlet characters which will make an appearance later on.

If σ has cycle type τ , sometimes instead of $X^\lambda(\sigma)$ we write $X^\lambda(\tau)$, since X^λ depends only on cycle type. Such characters are indexed by partitions $\lambda \vdash n$, and there is a one-to-one correspondence between irreducible characters of \mathfrak{S}_n and partitions of n . These characters satisfy the orthogonality relation:

$$\mathbb{E}_{\sigma \in \mathfrak{S}_n} X^{\lambda_1}(\sigma) X^{\lambda_2}(\sigma) = \delta_{\lambda_1 = \lambda_2}. \quad (13)$$

For an element $f \in \mathbb{F}_q[T]$, for $\lambda \vdash n$, we define

$$X^\lambda(f) := \begin{cases} X^\lambda(\tau_f) & \text{if } \deg(f) = n \text{ and } f \text{ is squarefree,} \\ 0 & \text{otherwise.} \end{cases}$$

It is easy to see from this definition that for any factorization function a , there exists a unique decomposition

$$a(f) = \sum_{\lambda} \hat{a}_{\lambda} X^{\lambda}(f) + b(f), \quad (14)$$

where $b(f)$ is a function supported on the squarefuls, \hat{a}_{λ} are constants that depend on the function a and are defined by this relation, and the sum is over all partitions. (Note that for any particular f of degree n , the sum in (14) will be a finite sum over $\lambda \vdash n$, all other terms in the summand being 0.)

Note that from [Proposition 2.3](#) and the orthogonality relation (13) we may equivalently define the coefficients \hat{a}_{λ} for $\lambda \vdash n$ by

$$\hat{a}_{\lambda} := \lim_{q \rightarrow \infty} \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} a(f) X^{\lambda}(f).$$

For instance, since $X^{(n)}$ is the trivial character, we have $\mathbb{E}_{f \in \mathcal{M}_n} a(f) \rightarrow \hat{a}_{(n)}$, as $q \rightarrow \infty$.³

Hast and Matei [2016, Theorem 4.4] have considered a class of functions called arithmetic functions of von Mangoldt type, which is similar to the class of factorization functions defined here (see [Hast and Matei 2016] for details of the definition). For this class of functions, Hast and Matei prove what may be thought of as a first-order short interval analogue of Andrade, Bary-Soroker, and Rudnick's result in [Theorem 2.4](#). Rewritten in the notation used above:

Theorem 2.5. *For a fixed arithmetic function of von Mangoldt type $a(f)$, and fixed $n \geq 4$, $1 \leq h \leq n - 3$,*

$$\mathbb{E}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f; h)} a(g) \right)^2 = q^{2(h+1)} (\mathbb{E}_{f \in \mathcal{M}_n} a(f))^2 + O(q^{(h+1)}), \quad (15)$$

as $q \rightarrow \infty$.

This is sufficient to recover the upper bound of $O(q^{h+1})$ for the variance computed by [Theorem 1.4](#) of Keating and Rudnick, though not the constant $n - h - 2$.

This result of Hast and Matei is of interest perhaps especially because their methods are rather different than ours — in particular they do not require any of the facts about L -functions that we will make use of in what follows. Other related recent papers with a perspective similar to Hast and Matei's, making use of

³Alternatively, if $\lambda \vdash n$, and $A : S_n \rightarrow \mathbb{C}$ is the function induced by a , then \hat{a}_{λ} is also equal to the Fourier coefficient of A .

the connection between polynomials over a finite field and the symmetric group to investigate arithmetic functions defined on \mathcal{M} , include [Church et al. 2014; Gadish 2017].

3. A statement of main results

3A. We are now in a position to state our main results.

Theorem 3.1. For $a(f)$ a fixed factorization function, and fixed h and n with $0 \leq h \leq n - 5$,

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} a(g) \right) = q^{h+1} \sum_{\substack{\lambda \vdash n \\ \lambda_1 \leq n-h-2}} |\hat{a}_\lambda|^2 + O(q^{h+1/2}). \tag{16}$$

Here the coefficients \hat{a}_λ are defined by the expansion (14), and the sum in (16) is over all partitions $(\lambda_1, \lambda_2, \dots)$ of n such that λ_1 (and therefore every λ_i) is no more than $n - h - 2$.

In (16), the implied constant of the error term depends on h, n and the factorization function itself, so the result is only of interest as $q \rightarrow \infty$.

In Section 9 we compute the coefficients in the expansion (14) for the factorization functions $\mu(f)$, $\Lambda(f)$, $\Lambda_j(f)$ and $d_k(f)$. These expansions, applied in Theorem 3.1 are sufficient to recover estimates for the variance of sums of these arithmetic functions over short intervals which we have cited in Theorems 1.3, 1.4, and 1.5.

Likewise we consider the arithmetic functions $\omega(f)$, counting the number of prime factors of f , and likewise the function $\mu(f)\omega(f)$. The short interval variance of these functions is computed in Section 9 by using Theorem 3.1, and this leads us to make a conjecture in the setting of the integers which seems perhaps somewhat surprising.

Note also that Theorem 3.1 gives us a nontrivial upper bound for the variance of arithmetic functions supported on the squarefrees, though the upper bound is one which may be far from optimal. Work of Keating and Rudnick [2016] and Roditty-Gershon [2017] considers some related questions about the squarefrees (and indeed square-fulls) more carefully to get asymptotics, not only upper bounds.

The variance evaluation in Theorem 3.1 comes in part from a combinatorial analysis of random matrix integrals. In particular the already mentioned function field equidistribution theorem of Katz plays an important role in the proof.

A likewise central role is played by a combinatorial analogue of the explicit formula of Weil, relating the zeros of an L -function to certain arithmetic functions. In particular, in Section 7 and especially Theorem 7.1 we show that Schur functions of zeros of L -functions are closely related to the characters $X^\lambda(f)$ defined above.

We note the conjectural appearance of the symmetric group in other closely related contexts, for example in Dehaye’s work [≥ 2018] on moments of the Riemann zeta function. It would be of interest to pursue this connection further.

3B. The same result may be stated perhaps more strikingly along the lines advertised in Section 1. Let \mathcal{F}_n be the linear space of factorization functions supported on \mathcal{M}_n , and define \mathcal{U}_n^h to be the subspace of

factorization functions for which variance is negligible; that is,

$$\mathcal{U}_n^h := \left\{ u \in \mathcal{F}_n : \lim_{q \rightarrow \infty} \text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} u(g) \right) = o(q^{h+1}) \right\}. \tag{17}$$

We may endow \mathcal{F}_n with an inner product: for $a_1, a_2 \in \mathcal{F}_n$, we define

$$\langle a_1, a_2 \rangle := \lim_{q \rightarrow \infty} \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} a_1(f) \overline{a_2(f)}. \tag{18}$$

This inner product is degenerate, but only on factorization functions supported on the squarefuls. If we decompose $\mathcal{F}_n = \mathcal{G}_n \oplus \mathcal{B}_n$, where \mathcal{G}_n is the space of factorization functions supported on squarefree monic polynomials of degree n , and \mathcal{B}_n is the space supported on squarefuls, then the equidistribution of factorization types imply that this is a proper inner product when restricted to \mathcal{G}_n .

We will show that $\mathcal{B}_n \subseteq \mathcal{U}_n^h$, and so if we define \mathcal{V}_n^h to be the orthogonal complement to \mathcal{U}_n^h inside \mathcal{G}_n , we have

$$\mathcal{F}_n = \mathcal{U}_n^h \oplus \mathcal{V}_n^h.$$

We will observe the following restatement of [Theorem 3.1](#),

Theorem 3.2. *Let $0 \leq h \leq n - 5$ be fixed and v be a fixed factorization function from the subspace \mathcal{V}_n^h . Then*

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} v(g) \right) = q^{h+1} \langle v, v \rangle + O(q^{h+1/2}).$$

That is, for \mathcal{V}_n^h , only diagonal terms contribute to the variance, while by definition for \mathcal{U}_n^h the variance is of lower order.

Thus, this theorem implies an estimate for the variance of an arbitrary factorization function $a \in \mathcal{F}_n$, since there is a unique decomposition $a = u + v$ with $u \in \mathcal{U}_n^h$ and $v \in \mathcal{V}_n^h$. Indeed,

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} u(g) \right) = o(q^{h+1}),$$

so (using Cauchy–Schwarz to bound covariance),

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} a(g) \right) = q^{h+1} \langle v, v \rangle + o(q^{h+1}). \tag{19}$$

The spaces \mathcal{U}_n^h and \mathcal{V}_n^h can be characterized explicitly.

Proposition 3.3. *We have*

$$\mathcal{U}_n^h = \mathcal{A}_n^h \oplus \mathcal{B}_n,$$

where

$$\mathcal{A}_n^h := \text{span}\{X^\lambda(f) : \lambda \vdash n, \lambda_1 \geq n - h - 1\},$$

$$\mathcal{B}_n := \{b(f) : b \in \mathcal{F}_n \text{ is supported on squareful elements}\}.$$

Furthermore

$$\mathcal{V}_n^h = \text{span}\{X^\lambda(f) : \lambda \vdash n, \lambda_1 \leq n - h - 2\}.$$

This explicit decomposition is what connects Theorems 3.1 and 3.2. It is worthwhile to emphasize once again an interpretation of this result; the determination that the variance of short interval sums of functions lying in \mathcal{U}_n^h is negligible will be a relatively simple fact to verify — we will see that functions lying in this space are forced to be regular across short intervals owing in the end to a paucity of zeros of L -functions. The theorem tells us that outside this first obstruction, factorization functions otherwise behave in an oscillatory fashion, akin to the Möbius function, when summed in a short interval.

There is another appealing way to write this decomposition, based on a suggestion by J. Ellenberg:

Proposition 3.4. *Define the space \mathcal{U}_n^h as in the start of this subsection. Then \mathcal{U}_n^h consists of functions $u(f)$ that can be written in the form*

$$u(f) = \sum_{\substack{\delta \mid f \\ \deg(\delta) \leq h+1}} \alpha(\delta) + b(f), \quad \text{for all } f \in \mathcal{M}_n, \tag{20}$$

where $\alpha(\delta)$ is a factorization function and $b(f)$ is a factorization function supported on the squarefuls.

Here the sum is over all monic polynomials δ dividing f with degree no more than $h + 1$.

Indeed, it will again follow quite easily that for all factorization functions that can be represented as truncated divisor sums in this way, the value of their sums over short intervals will remain basically constant no matter the choice of short interval, so that these sums have negligible variance. The space \mathcal{V}_n^h remains defined as the complement of \mathcal{U}_n^h , and so an interpretation of this decomposition remains the same — outside an “easy-to-find” obstruction, functions otherwise behave in an oscillatory fashion when summed in a short interval.

As a corollary of Theorem 3.2 and Proposition 3.4, we have

Corollary 3.5. *For $a(f)$ a fixed factorization function and fixed h and n with $0 \leq h \leq n - 5$,*

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} a(g) \right) = q^{h+1} \inf_{\alpha \in \mathcal{F}} \left\| a(f) - \sum_{\substack{\delta \mid f \\ \deg(\delta) \leq h+1}} \alpha(\delta) \right\|^2 + O(q^{h+1/2}), \tag{21}$$

where \mathcal{F} is the space of all factorization functions and $\|\cdot\|$ is the norm induced by the inner product (18).

Rather curiously, the minimization problem arising in the computing the right-hand side of (21) has some similarity to those which arise in connection to the Selberg sieve.

We turn to a proof of these decompositions and Theorem 3.2 in Section 11.

3C. Because Theorem 3.1 allows us to compute variances for general factorization functions, it is also straightforward to use it to compute covariance. We record a general formula for covariance in Section 10 and draw out some interesting consequences that appear to be new in the literature.

3D. A similar set of results could be developed for factorization functions in arithmetic progressions rather than short intervals, though we don’t do so here.

3E. In the next two sections we recall some background material regarding Dirichlet characters, L -functions, and symmetric function theory. We turn to the substantial portion of the proof of [Theorem 3.1](#) in [Section 8](#).

4. Background on Dirichlet characters and zeros of L -functions

4A. We recall a few of the basic facts about Dirichlet characters defined over $\mathbb{F}_q[T]$ that we will use. Our notation is the same as that from [\[Rosen 2002; Keating and Rudnick 2014; Rudnick 2014; Rodgers 2015; Keating et al. 2018\]](#) and a reader familiar with the facts from any one of those may skip this section and refer back to it as it is referenced.

In $\mathbb{F}_q[T]$, we will make use of the family of primitive even characters modulo the element T^M for powers $M \geq 1$. We call a character χ *even* if for all $c \in \mathbb{F}_q$ and all $f \in \mathbb{F}_q[T]$, we have $\chi(cf) = \chi(f)$. Recall that the number of Dirichlet characters modulo T^M is

$$\Phi(T^M) = q^M \left(1 - \frac{1}{q}\right), \tag{22}$$

the number of primitive Dirichlet characters is

$$\Phi_{\text{prim}}(T^M) = q^M \left(1 + O\left(\frac{1}{q}\right)\right), \tag{23}$$

the number of even Dirichlet characters is

$$\Phi^{\text{ev}}(T^M) = q^{M-1}, \tag{24}$$

and the number of even primitive characters is

$$\Phi_{\text{prim}}^{\text{ev}}(T^M) = q^{M-1} \left(1 + O\left(\frac{1}{q}\right)\right). \tag{25}$$

We recall that the L -function of a Dirichlet character χ is defined for $|u| < 1/q$ by

$$\mathcal{L}(u, \chi) := \sum_{f \text{ monic}} \chi(f) u^{\deg(f)} = \prod_{\substack{P \text{ monic,} \\ \text{irreducible}}} \frac{1}{1 - \chi(P) u^{\deg(P)}},$$

and that for χ nontrivial that $\mathcal{L}(u, \chi)$ is a polynomial in u , defined for $|u| \geq 1/q$ by analytic continuation. The Riemann hypothesis, in this context a theorem of Weil [\[1967\]](#), states that all roots of $\mathcal{L}(u, \chi)$ lie on the circles $|u| = q^{-1/2}$ or $|u| = 1$. If χ is a nontrivial character modulo a polynomial Q of degree M , then $\mathcal{L}(u, \chi)$ has no more than $M - 1$ roots, and as a well-known consequence of this and the Riemann hypothesis,

$$\sum_{f \in \mathcal{M}_n} \Lambda(f) \chi(f) = O_M(q^{n/2}). \tag{26}$$

4B. In the case that χ is a primitive character we can succinctly say more. In this case for χ modulo T^M , the polynomial $\mathcal{L}(u, \chi)$ has exactly $M - 1$ roots. Define the function λ_χ to be 1 if χ is even, and 0 otherwise. When χ is even, $\mathcal{L}(u, \chi)$ has a simple zero at $u = 1$, otherwise all zeros of this polynomial lie on the circle $|u| = q^{-1/2}$. We can record this information in a single equation; we have for primitive

characters χ and $N := \deg Q - 1 - \lambda_\chi$,

$$\mathcal{L}(u, \chi) = (1 - \lambda_\chi u) \prod_{j=1}^N (1 - q^{1/2} e^{i2\pi \vartheta_j} u) = (1 - \lambda_\chi u) \det(1 - q^{1/2} u \Theta_\chi), \tag{27}$$

where $e^{i2\pi \vartheta_1}, \dots, e^{i2\pi \vartheta_N}$ lie on the unit circle and are determined by the character χ and

$$\Theta_\chi := \text{diag}(e^{i2\pi \vartheta_1}, \dots, e^{i2\pi \vartheta_N})$$

is known as the unitarized Frobenius matrix. From logarithmic differentiation we also have the *explicit formula*,

$$\sum_{f \in \mathcal{M}_n} \Lambda(f) \chi(f) = -q^{n/2} \text{Tr } \Theta_\chi^n - \lambda_\chi. \tag{28}$$

To control the distribution of zeros, a theorem of Katz will be important for us, as it has been in all investigations of this sort since Keating and Rudnick’s [2014]. We let $\text{PU}(m)$ be the projective unitary group, the quotient of the unitary group $U(m)$ by unit modulus scalars, endowed with Haar measure, and $\text{PU}(m)^\#$ be the space of conjugacy classes of $\text{PU}(m)$, with inherited measure.

Theorem 4.1 [Katz 2013, Theorem 8.1]. *Fix $M \geq 5$. Over the family of even primitive characters $\chi \pmod{T^M}$, the conjugacy classes of the unitarized Frobenii Θ_χ become equidistributed in $\text{PU}(M - 2)^\#$ as $q \rightarrow \infty$.*

More computationally the meaning of the theorem is as follows: for any continuous class function $\phi : U(M - 2) \rightarrow \mathbb{C}$ such that $\phi(e^{i2\pi\theta} g) = \phi(g)$ for all unit scalars $e^{i2\pi\theta}$ and unitary matrices g , we have

$$\lim_{q \rightarrow \infty} \mathbb{E}_{\chi(T^M)_{\text{prim, ev}}} \phi(\Theta_\chi) = \int_{U(M-2)} \phi(g) dg,$$

as $q \rightarrow \infty$, where for typographical reasons we have written

$$\mathbb{E}_{\chi(T^M)_{\text{prim, ev}}} \phi(\Theta_\chi) := \frac{1}{\Phi_{\text{prim}}^{\text{ev}}(T^M)} \sum_{\substack{\chi(T^M) \\ \text{prim, ev}}} \phi(\Theta_\chi).$$

Indeed, Katz also considers the rate of convergence in this result, at least for a sufficiently simple function ϕ .

Theorem 4.2 [Katz 2013, Theorem 8.2]. *Fix $M \geq 5$. For a fixed class function $\phi : U(M - 2) \rightarrow \mathbb{C}$ as described above such that the map induced by ϕ from $\text{PU}(M - 2)$ to \mathbb{C} is a linear combination of irreducible characters of $\text{PU}(M - 2)$:*

$$\mathbb{E}_{\chi(T^M)_{\text{prim, ev}}} \phi(\Theta_\chi) = \int_{U(M-2)} \phi(g) dg + O(q^{-1/2}).$$

4C. The reason we will be interested in characters modulo T^M is the following involution used by Keating and Rudnick.

We let \mathcal{P}_n be the collection of degree n polynomials in $\mathbb{F}_q[T]$ and $\mathcal{P}_n^\natural := \{f \in \mathcal{P}_n : (f, T) = 1\}$. Equivalently \mathcal{P}_n^\natural is the collection of degree n polynomials with a constant coefficient that is nonzero. Our

involution is the mapping $f \mapsto f^*$ from \mathcal{P}_n^{\natural} to itself defined by

$$(a_0 + a_1T^1 + \cdots + a_nT^n)^* = a_n + a_{n-1}T + \cdots + a_0T^n. \quad (29)$$

It is straightforward to check that for f with nonzero constant coefficient,

$$(f^*)^* = f,$$

and for f and g with nonzero constant coefficient,

$$(fg)^* = f^*g^*.$$

If we extend the definition of factorization type to \mathcal{P}_n , so that for $f \in \mathcal{P}_n$ and for that scalar $c \in \mathbb{F}_q$ such that $cf \in \mathcal{M}_n$, the factorization type of f is defined to be the factorization type of cf , it follows that for $f \in \mathcal{P}_n^{\natural}$,

$$\tau_f = \tau_{f^*}. \quad (30)$$

This involution is useful for us because for $g_1, g_2 \in \mathcal{P}_n^{\natural}$,

$$\deg(g_1 - g_2) \leq h$$

if any only if

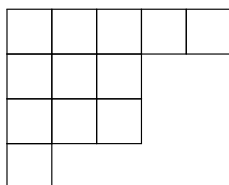
$$g_1^* - g_2^* \equiv 0 \pmod{T^{n-h}}.$$

This equivalence is easily checked. It is because of this that we may use Dirichlet characters and their L -functions to study short interval sums.

5. Background on symmetric function theory

5A. We recall some notation and well-known facts from symmetric function theory that we will use in what follows. A standard reference and introduction to the material we recall here is [Stanley 1999, Chapter 7].

We have already defined partitions and discussed their basic notation in Section 2A. One additional way to represent partitions is as a Young diagram. This is an array of left-justified boxes, with the number of boxes in each row weakly decreasing. For a partition λ , the Young diagram corresponding to λ has λ_1 boxes in its first row, λ_2 boxes in its second row, etc. For instance, the Young diagram with shape $(5, 3, 3, 1)$ is as follows:



The *dual partition* λ' is defined to be $(\lambda'_1, \lambda'_2, \dots)$ where λ'_i is the number of boxes in the i -th column of the Young diagram corresponding to λ . So in our example above $(5, 3, 3, 1)' = (4, 3, 3, 1, 1)$.

The *length of a partition*, $\ell(\lambda)$, is defined to be k , where $\lambda = (\lambda_1, \dots, \lambda_k)$. For instance $\ell(5, 3, 3, 1) = 4$.

Young diagrams may be used to write down a relatively simple expression for characters of the symmetric group in the form of the famous Murnaghan–Nakayama rule. We quickly recall it here, taking from the presentation in [Stanley 1999, §7.17], which is recommended for those who have not seen this result before. As a prerequisite, we define *Young tableaux of shape* λ to be arrays of numbers, weakly increasing across rows and down columns, written in the squares of a Young diagram of λ . A *border strip tableau of shape* λ and *type* τ is a Young tableau such that among the entries the number i occurs exactly τ_i times, and for each i the set of squares in which i has been written form a *border strip*—that is, a connected collection of squares with no square upward and to the left of any others. The *height* of a border strip is one less than the number of rows that contain it, and the height $h(T)$ of a tableau T composed of border strips is the sum of the heights of the border strips.

Theorem 5.1 (Murnaghan–Nakayama rule). *For λ a partition of n and τ the type of a permutation from \mathfrak{S}_n*

$$X^\lambda(\tau) = \sum_T (-1)^{h(T)}, \tag{31}$$

where the sum is over all border strip tableaux T of shape λ and type τ .

Remark. A reader unfamiliar with characters of the symmetric group but nonetheless comfortable with the statement of the Murnaghan–Nakayama rule may take (31) as their definition the symmetric group’s characters.

5B. We will need to work with symmetric polynomials in m variables. Two bases for these polynomials that will be important for us are the power sum symmetric functions and Schur functions. Both bases are indexed by partitions.

For *power sum symmetric functions* in the variables $\omega_1, \dots, \omega_m$ we recall the definition that for an integer n ,

$$p_n = p_n(\omega_1, \dots, \omega_m) := \omega_1^n + \dots + \omega_m^n,$$

and for a partition $\lambda = (\lambda_1, \dots, \lambda_k)$, we define

$$p_\lambda := p_{\lambda_1} \cdots p_{\lambda_k}.$$

It is an elementary fact [Stanley 1999, Corollary 7.7.2] that any symmetric polynomial in the variables $\omega_1, \dots, \omega_m$ can be expressed uniquely as a linear combination of the functions p_λ .

Schur functions in the variables $\omega_1, \dots, \omega_m$ have the following as their classical definition. For a partition λ with $\ell(\lambda) \leq m$, set

$$s_\lambda = s_\lambda(\omega_1, \dots, \omega_m) := \frac{\det(\omega_i^{\lambda_j + m - j})_{i,j=1}^m}{\det(\omega_i^{n-j})_{i,j=1}^m}.$$

If $\ell(\lambda) < m$, we extend λ with 0's in the extra places so that the above definition still makes sense — i.e., $\lambda = (\lambda_1, \dots, \lambda_k, 0, \dots, 0)$. If $\ell(\lambda) > m$, we set $s_\lambda = 0$.

It is well-known (though not completely obvious at first glance) that s_λ defined as above is a symmetric polynomial with integer coefficients. As with power sums, any symmetric polynomial in the variables $\omega_1, \dots, \omega_m$ can be expressed uniquely as a linear combination of the functions s_λ . Proofs of these facts may be found in [Stanley 1999, Chapter 7].

For these symmetric polynomials we have the following important identities:

Theorem 5.2 (Frobenius). *For $\lambda \vdash n$,*

$$s_\lambda = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} X^\lambda(\sigma) p_\sigma = \sum_{\nu \vdash n} \mathbf{p}(\nu) X^\lambda(\nu) p_\nu. \quad (32)$$

Likewise,

$$p_\nu = \sum_{\lambda \vdash n} X^\lambda(\nu) s_\lambda. \quad (33)$$

Proof. Equation (32) is Theorem 7.17.3 of [Stanley 1999], while (33) is Corollary 7.17.4. □

We can also express s_λ in terms of the elementary symmetric functions, defined by

$$e_n = e_n(\omega_1, \dots, \omega_m) := \sum_{i_1 < \dots < i_n} \omega_{i_1} \cdots \omega_{i_n},$$

with the conventions $e_0 = 1$ and $e_n(\omega_1, \dots, \omega_m) = 0$ for $n > m$.

Theorem 5.3 (Jacobi–Trudi). *For $\lambda_1 \leq k$,*

$$s_\lambda = \det(e_{\lambda'_i - i + j})_{i,j=1}^k.$$

Proof. This is a special case of Corollary 7.16.2 of [Stanley 1999]. □

Remark. This is often known as the *dual* Jacobi–Trudi identity because there is an equivalent formula in terms of the complete homogeneous symmetric functions; see [Stanley 1999, Theorem 7.16.1].

5C. One of the many results that is derived in the literature from Theorem 5.2 is an identity for characters of the symmetric group indexed by partitions that are dual to each other. We cite it here because we will use it later.

Proposition 5.4. *For $\sigma \in \mathfrak{S}_n$ and $\lambda \vdash n$,*

$$X^{\lambda'}(\sigma) = (-1)^{n-\ell(\sigma)} X^\lambda(\sigma).$$

Here $\ell(\sigma) := \ell(\tau_\sigma)$.

Proof. This is example 2 of section I.7 in [Macdonald 1995]. □

5D. One of the reasons we are interested in Schur functions is their appearance in random matrix theory. It is well known that they satisfy the following orthogonality relation.

Theorem 5.5. For partitions λ and ν ,

$$\int_{U(m)} s_\lambda(g) \overline{s_\nu(g)} dg = \delta_{\lambda\nu} \cdot \delta_{\ell(\lambda), \ell(\nu) \leq m}.$$

Moreover, if λ and ν are partitions of the same number (that is $|\lambda| = |\nu|$)

$$\int_{\text{PU}(m)} s_\lambda(g) \overline{s_\nu(g)} dg = \delta_{\lambda\nu} \cdot \delta_{\ell(\lambda), \ell(\nu) \leq m}.$$

Here $s_\lambda(g)$ and $s_\nu(g)$ are Schur functions whose entries are the m eigenvalues of the matrix g . A more or less self-contained proof may be found in [Gamburd 2007] as well as in more standard texts on representation theory.

6. A basis for factorization functions, and a bound for character sums

6A. We turn in this section to a proof of Theorem 3.1. Our strategy will be a familiar one, similar in its broad outlines to the original proof of Keating and Rudnick. By making use of the involution described in Section 4, we transfer a short interval sum to an average over sums of Dirichlet characters against factorization functions. These are in turn evaluated by using an equidistribution result of Katz and the combinatorial analysis of Section 7. This combinatorial analysis is perhaps the most important observation of the paper. In terms of technique, some new issues arise that have not appeared in the past just because we work with factorization functions in general.

6B. We begin by noting some ways to build factorization functions out of simpler functions. For two arithmetic functions ϕ_1 and ϕ_2 we define the convolution in the usual way,

$$\phi_1 \star \phi_2(f) := \sum_{\substack{f_1 f_2 = f \\ f_1, f_2 \in \mathcal{M}}} \phi_1(f_1) \phi_2(f_2).$$

It is clear that if ϕ_1 and ϕ_2 are factorization functions, then $\phi_1 \star \phi_2$ will be a factorization function as well.

For integers $m, e \geq 1$ we define the factorization function

$$\iota_{m,e}(f) = \begin{cases} 1 & \text{if } f = P^e \text{ with } \deg(P) = m, \\ 0 & \text{otherwise.} \end{cases}$$

Thus $\iota_{m,e}$ is the indicator function of e -th powers of m -th degree primes and is supported on \mathcal{M}_{me} . We generalize it in the following way: for an array $(\mathbf{m}, \mathbf{e}) = (m_1, e_1; m_2, e_2; \dots; m_\ell, e_\ell)$ we define

$$\iota_{(\mathbf{m}, \mathbf{e})} = \iota_{m_1, e_1} \star \iota_{m_2, e_2} \star \dots \star \iota_{m_\ell, e_\ell}. \tag{34}$$

Proposition 6.1. Any factorization function supported on \mathcal{M}_n is a linear combination of the functions $\iota_{(\mathbf{m}, \mathbf{e})}$. (Necessarily $m_1 e_1 + \dots + m_\ell e_\ell = n$).

Proof. Let $\mathcal{M}_{n,L}$ be the collection of elements of \mathcal{M}_n with extended factorization type $(m_1, e_1; \dots; m_\ell, e_\ell)$ for $\ell \leq L$ and $\mathcal{F}_{n,L}$ be the collection of factorization function supported on $\mathcal{M}_{n,L}$. We suppose the proposition is true for all factorization functions supported on $\mathcal{M}_{r,L}$ with $r \leq n$ and show that it is true for $\mathcal{M}_{n,L+1}$. Since it is obviously true (check) for $\mathcal{M}_{n,1}$ for all n , this will verify the claim by induction.

We introduce indicator functions $I_{(m,e)}$ of the extended factorization type (m, e) ; that is for $f \in \mathcal{M}$, we set $I_{(m_1,e_1;\dots;m_\ell,e_\ell)}(f) = 1$ if f has extended factorization type $(m_1, e_1; \dots; m_\ell, e_\ell)$ and we set $I_{(m_1,e_1;\dots;m_\ell,e_\ell)}(f) = 0$ otherwise. Clearly

$$\mathcal{F}_{n,L+1} = \text{span}\{I_{(m_1,e_1;\dots;m_\ell,e_\ell)} : m_1e_1 + \dots + m_\ell e_\ell = n, \ell \leq L + 1\},$$

so to prove our claim we need only show that each

$$I_{(m_1,e_1;\dots;m_{L+1},e_{L+1})} \tag{35}$$

is a linear combination of functions $\iota_{(m,e)}$. Suppose v of the terms $(m_1, e_1), \dots, (m_L, e_L)$ in (35) are equal to (m_{L+1}, e_{L+1}) . (We allow v to be 0.) By inspection of elements of $\mathcal{M}_{n,L+1}$ we see that

$$I_{(m_1,e_1;\dots;m_L,e_L)} \star \iota_{m_{L+1},e_{L+1}} - (v + 1)I_{(m_1,e_1;\dots;m_{L+1},e_{L+1})} \tag{36}$$

is supported on $\mathcal{M}_{n,L}$. By inductive hypothesis then (36) is a linear combination of terms $\iota_{(m,e)}$. Likewise by inductive hypothesis, $I_{(m_1,e_1;\dots;m_L,e_L)}$ is a linear combination of such terms, so $I_{(m_1,e_1;\dots;m_L,e_L)} \star \iota_{m_{L+1},e_{L+1}}$ will be as well. Returning to (36), since $v + 1 \neq 0$, this shows that $I_{(m_1,e_1;\dots;m_{L+1},e_{L+1})}$ is therefore a linear combination of such terms, so that as claimed all factorization functions on $\mathcal{M}_{n,L+1}$ are linear combinations of such terms also. \square

6C. We have indicated that we must work with Dirichlet characters modulo T^M for some power M . Note that for any nontrivial Dirichlet character χ modulo T^M , we have, by excluding powers of primes from the sum in the first line below and using the Riemann hypothesis in the form (26) in the second,

$$\sum_{f \in \mathcal{M}_n} \iota_{n,1}(f)\chi(f) = \frac{1}{n} \sum_{f \in \mathcal{M}_n} \Lambda(f)\chi(f) + O(q^{n/2}) = O_M(q^{n/2}).$$

Thus for any $e \geq 2$, as long as $\chi^e \neq \chi_0$,

$$\sum_{f \in \mathcal{M}_{me}} \iota_{m,e}(f)\chi(f) = \sum_{f \in \mathcal{M}_m} \iota_{m,1}(f)\chi^e(f) = O_M(q^{m/2}).$$

For $e \geq 3$, trivially

$$\sum_{f \in \mathcal{M}_{me}} \iota_{m,e}(f)\chi(f) = O(q^m).$$

Note that for $m \geq 1, e \geq 2$, we have $\frac{m}{2} \leq \frac{me}{2} - \frac{1}{2}$, and for $m \geq 1, e \geq 3$, we have likewise $m \leq \frac{me}{2} - \frac{1}{2}$. Thus combining the two estimates above, we see that unless $\chi^2 = \chi_0$, we have for $e \geq 2$,

$$\sum_{f \in \mathcal{M}_{me}} \iota_{m,e}(f)\chi(f) = O(q^{me/2-1/2}).$$

Hence recalling the definition (34), unless $\chi^2 = \chi_0$, if some $e_i \geq 2$,

$$\sum_{f \in \mathcal{M}_n} \iota_{\mathbf{m},e}(f)\chi(f) = O_{M,n}(q^{n/2-1/2}), \tag{37}$$

where $n = m_1e_1 + \dots + m_ke_k$.

We have thus obtained

Lemma 6.2. *If b is a fixed factorization function supported on the squarefuls, for χ a Dirichlet character modulo T^M , as long as $\chi^2 \neq \chi_0$,*

$$\sum_{f \in \mathcal{M}_n} b(f)\chi(f) = O_{M,n}(q^{n/2-1/2}).$$

Proof. For such b , the function $b(f)\mathbf{1}_{\mathcal{M}_n}(f)$ is necessarily a linear combination of functions $\iota_{\mathbf{m},e}$, where in each case some $e_i \geq 2$. □

In the case that $\chi^2 = \chi_0$, we may genuinely have a worse bound, but it is easy to see in the same way that as long as $\chi \neq \chi_0$ for $\chi \pmod{T^M}$, the bound in Lemma 6.2 may be replaced by $O_{M,n}(q^{n/2})$. Indeed, for such an estimate, it is easy to see that we have no need that our factorization function be supported on the squarefuls as it was in Lemma 6.2.

Lemma 6.3. *If a is a fixed factorization function, for χ a nontrivial Dirichlet character modulo T^M ,*

$$\sum_{f \in \mathcal{M}_n} a(f)\chi(f) = O_{n,M}(q^{n/2}).$$

Note that a character satisfies $\chi^2 = \chi_0$ only if it is real. Fortunately there are not many real characters modulo T^M .

Lemma 6.4. *Over $\mathbb{F}_q[T]$, the number of nontrivial real characters modulo T^M is $O(1)$ if $2 \nmid q$, and $O(q^{\lfloor M/2 \rfloor})$ if $2 \mid q$.*

Proof. Let \widehat{G} be the group of characters. Real characters χ are characterized by having $\chi^2 = \chi_0$. As $\widehat{G} \cong (\mathbb{F}_q[T]/(T^M))^*$, the number of real characters is equal to the number of $f \in \mathbb{F}_q[T]$ with $(f, T^M) = 1$ and $\deg(f) < M$ such that

$$f^2 \equiv 1 \pmod{T^M}. \tag{38}$$

Yet if $2 \nmid q$, we have $(f - 1, f + 1) = 1$ and so (38) implies $f \equiv \pm 1 \pmod{T^M}$, which is satisfied by only two such f . Hence in this case there are at most two real characters modulo T^M , and thus at most one nontrivial real character.

If $2 \mid q$, the situation is more complicated. If $f = a_0 + \dots + a_{M-1}T^{M-1}$, we have

$$f^2 = a_0^2 + a_1^2T^2 + \dots + a_{M-1}^2T^{2(M-1)},$$

so that each solution $f^2 \equiv 1 \pmod{T^M}$ entails $\lfloor (M - 1)/2 \rfloor + 1$ linear equations,

$$a_0^2 = 1, a_1^2 = 0, \dots, a_{\lfloor (M-1)/2 \rfloor}^2 = 0$$

of which there is only one solution. The remaining $M - 1 - \lfloor (M - 1)/2 \rfloor = \lfloor M/2 \rfloor$ coefficients $a_{\lfloor (M-1)/2 \rfloor + 1}, \dots, a_{M-1}$ may vary freely, but this leads to only $q^{\lfloor M/2 \rfloor}$ different solutions. \square

Remark. I thank Ofir Gorodetsky for suggesting this proof of [Lemma 6.4](#) to me.

7. Schur functions of zeros

7A. We have noted the explicit formula [\(28\)](#), which establishes a correspondence between the von Mangoldt function $\Lambda(f)$ and the traces of powers of unitarized Frobenius matrices. Written another way, let χ be a primitive character modulo T^m . For $p_n(\Theta_\chi)$ the symmetric power sum of the unitarized zeros $\{e^{i2\pi\vartheta_1}, \dots, e^{i2\pi\vartheta_{m-2}}\}$ of $\mathcal{L}(u, \chi)$, the explicit formula is just the statement that

$$p_n(\Theta_\chi) = \frac{-1}{q^{n/2}} \sum_{f \in \mathcal{M}_n} \Lambda(f)\chi(f) + O(1/q^{n/2}) = \frac{-n}{q^{n/2}} \sum_{\substack{P \in \mathcal{M}_n \\ \text{prime}}} \chi(P) + O(q^{-1/2}) \tag{39}$$

for $\chi^2 \neq \chi_0$. (We require $\chi^2 \neq \chi$ in order to absorb higher prime powers into the error term.) By multiplying these power sums together, from unique factorization and a simple counting argument, it follows that for the partition $\nu = \langle 1^{m_1} 2^{m_2} \dots j^{m_j} \rangle$, with $\nu \vdash n$,

$$p_\nu(\Theta_\chi) = \frac{1}{q^{n/2}} \prod_{i=1}^j i^{m_i} m_i! \sum_{f \in \mathcal{M}_n} \mathbf{1}_\nu(\tau_f) \mu(f) \chi(f) + O(q^{-1/2}).$$

We have used the Riemann hypothesis bound [\(26\)](#) to retain this error term from [\(39\)](#). Note that the coefficient $\prod i^{m_i} m_i!$ here is $1/p(\nu)$, defined in [\(12\)](#) from our introductory remarks about the symmetric group. By applying the Frobenius formula, [Theorem 5.2](#), we see that for the Schur function with arguments $\{e^{i2\pi\vartheta_1}, \dots, e^{i2\pi\vartheta_{m-2}}\}$,

$$s_\lambda(\Theta_\chi) = \frac{1}{q^{n/2}} \sum_{f \in \mathcal{M}_n} \mu(f) X^\lambda(f) \chi(f) + O(q^{-1/2}).$$

Because $\mu(f) X^\lambda(f) = (-1)^{\ell(\tau_f)} X^\lambda(\tau_f) = (-1)^n X^{\lambda'}(\tau_f)$ by [Proposition 5.4](#), we have thus shown:

Theorem 7.1. *For χ a primitive character modulo T^m with $\chi^2 \neq \chi_0$,*

$$s_\lambda(\Theta_\chi) = \frac{(-1)^n}{q^{n/2}} \sum_{f \in \mathcal{M}_n} X^{\lambda'}(f) \chi(f) + O_{n,m}(q^{-1/2}).$$

7B. Note that in the above theorem, there is no explicit reference to the degree m of the polynomial T^m . Nonetheless, if χ is primitive and even, $s_\lambda(\Theta_\chi)$ is a polynomial in $m - 2$ variables, and so we must have $s_\lambda(\Theta_\chi) = 0$ for $\ell(\lambda) > m - 2$. We have thus observed

Corollary 7.2. *If $\ell(\lambda') = \lambda_1 > m - 2$,*

$$\sum_{f \in \mathcal{M}_n} X^{\lambda'}(f) \chi(f) = O(q^{(n-1)/2}),$$

uniformly for χ a primitive even character modulo T^m .

Remark. A similar statement to the above can of course be written down for odd primitive characters.

As another consequence of [Theorem 7.1](#),

Corollary 7.3. For partitions $\lambda, \nu \vdash n$ and $m \geq 5$,

$$\mathbb{E}_{\chi(T^m)_{\text{prim, ev}}} \left(\frac{1}{q^{n/2}} \sum_{f \in \mathcal{M}_n} X^\lambda(f) \chi(f) \right) \overline{\left(\frac{1}{q^{n/2}} \sum_{f \in \mathcal{M}_n} X^\nu(f) \chi(f) \right)} = \delta_{\lambda, \nu} \cdot \delta_{\ell(\lambda'), \ell(\nu') \leq m-2} + O(q^{-1/2}). \quad (40)$$

Proof. By [Theorem 7.1](#), the left-hand side of (40) can be written

$$\frac{1}{\Phi_{\text{prim}}^{\text{ev}}(T^m)} \sum_{\chi(T^m)_{\text{prim, ev}}} (s_{\lambda'}(\Theta_\chi) + O(q^{-1/2})) \overline{(s_{\nu'}(\Theta_\chi) + O(q^{-1/2}))} + O\left(\frac{q^{\lfloor m/2 \rfloor}}{\Phi_{\text{prim}}^{\text{ev}}(T^m)}\right), \quad (41)$$

using [Lemmas 6.3](#) and [6.4](#) to bound the contribution of characters with $\chi^2 = \chi_0$. For $m \geq 5$, recalling the value of $\Phi_{\text{prim}}^{\text{ev}}(T^m)$ given in [\(25\)](#), we certainly have

$$\frac{q^{\lfloor m/2 \rfloor}}{\Phi_{\text{prim}}^{\text{ev}}(T^m)} = O(q^{-1/2}),$$

and using the equidistribution [Theorem 4.2](#) to treat the main term, we see that (41) reduces to

$$\int_{U(m-2)} s_{\lambda'} \overline{s_{\nu'}} dg + O(q^{-1/2}).$$

(Note that the symmetric polynomial $s_{\lambda'} \overline{s_{\nu'}}$, homogeneous under unimodular multiplication, is a linear combination of characters of $\text{PU}(M-2)$.) This agrees with the right-hand side of (40) by the orthonormality of Schur functions ([Theorem 5.5](#)). □

7C. We will later need the following result, which is essentially the “easy” case of [Corollary 7.3](#).

Lemma 7.4. For a_1 and a_2 , factorization functions supported on \mathcal{M}_n , and m sufficiently large (depending on n),

$$\lim_{q \rightarrow \infty} \mathbb{E}_{\chi(T^m)_{\text{prim, ev}}} \left(\frac{1}{q^{n/2}} \sum_{f \in \mathcal{M}_n} a_1(f) \chi(f) \right) \overline{\left(\frac{1}{q^{n/2}} \sum_{f \in \mathcal{M}_n} a_2(f) \chi(f) \right)} = \langle a_1, a_2 \rangle, \quad (42)$$

with the inner product defined by [\(18\)](#).

Proof. This is not a deep result, following from nothing more sophisticated than orthogonality relations for characters averaged in this way.

Nonetheless, it is less work for us at this point to make use of [Corollary 7.3](#) and note the following, for $m \geq \min(5, n+2)$: if a_1 or a_2 is supported on the squarefuls, then (42) is true (with the right-hand side obviously equal to 0), owing to [Lemmas 6.2](#) and [6.3](#) (with contributions of characters $\chi^2 = \chi_0$ in the average dealt with as in the proof of [Corollary 7.3](#)). Moreover, if these functions are characters of the symmetric group, $a_1(f) = X^\lambda(f)$ and $a_2(f) = X^\nu(f)$, then (42) is true by [Corollary 7.3](#). Since any factorization function can be written as a linear combination of characters and some function supported on the squarefuls, this verifies (42) in general. □

8. A proof of Theorem 3.1

8A. Because we will be using characters modulo powers of T , we must work with polynomials f that are coprime to T . We recall our definition \mathcal{P}_n^\natural and make a similar definition for monic polynomials

$$\mathcal{P}_n^\natural := \{f \in \mathcal{P}_n : f(0) \neq 0\} \quad \text{and} \quad \mathcal{M}_n^\natural := \{f \in \mathcal{M}_n : f(0) \neq 0\}.$$

In addition we define for $f \in \mathcal{M}_n$,

$$\tilde{a}(f) := a(f) - E(a; n), \quad \text{with } E(a; n) := \frac{1}{|\mathcal{M}_n|} \sum_{g \in \mathcal{M}_n} a(g)$$

and for $f \in \mathcal{M}_n^\natural$,

$$\tilde{a}^\natural(f) := a(f) - E^\natural(a; n), \quad \text{with } E^\natural(a; n) := \frac{1}{|\mathcal{M}_n^\natural|} \sum_{g \in \mathcal{M}_n^\natural} a(g).$$

With these conventions, our proof of Theorem 3.1 may be broken into five pieces.

Step 1: In the first place, we reduce the variance of short interval sums, restricted to \mathcal{M}_n^\natural , to a sum over Dirichlet characters.

Lemma 8.1. *For any factorization function a ,*

$$\sum_{f \in \mathcal{M}_n} \left| \sum_{\substack{g \in I(f; h) \\ g \in \mathcal{M}_n^\natural}} \tilde{a}^\natural(g) \right|^2 = \frac{q^{h+1}(q-1)}{\Phi(T^{n-h})} \sum_{\substack{\chi \neq \chi_0(T^{n-h}) \\ \text{even}}} \left| \sum_{g \in \mathcal{M}_n} a(g)\chi(g) \right|^2.$$

for $0 \leq h \leq n - 1$.

The proof is a straightforward modification of Steps 1 and 2 in [Rodgers 2015], and we refer the reader to that paper for details. In summary: one transfers the short interval sum to a sum over Dirichlet characters by making use of the involution described in Section 4 of this paper.

Step 2: We next bound the sums in Lemma 8.1 for all factorization functions that are supported on the squarefuls.

Lemma 8.2. *For a fixed factorization b function supported on the squarefuls,*

$$\sum_{f \in \mathcal{M}_n} \left| \sum_{\substack{g \in I(f; h) \\ g \in \mathcal{M}_n^\natural}} \tilde{b}^\natural(g) \right|^2 = O_{n,h}(q^h q^n). \tag{43}$$

for $0 \leq h \leq n - 4$.

Proof. Clearly by Lemma 8.1 we need only show that

$$\frac{q-1}{\Phi(T^{n-h})} \sum_{\substack{\chi \neq \chi_0(T^{n-h}) \\ \text{even}}} \left| \sum_{g \in \mathcal{M}_n} b(g)\chi(g) \right|^2 = O_{n,h}(q^{n-1}). \tag{44}$$

From Lemma 6.2, we note that for nonreal characters χ modulo T^{n-h} , uniformly

$$\left| \sum_{g \in \mathcal{M}_n} b(f)\chi(f) \right| = O_{n,h}(q^{n/2-1/2}),$$

while from Lemma 6.4 there are at most $O(q^{(n-h)/2})$ real nontrivial characters, and for such a character by Lemma 6.3 this sum is $O_{n,h}(q^{n/2})$. Hence the left-hand side of (44) is at most

$$\frac{q-1}{\Phi(T^{n-h})} (\Phi_{\text{ev}}(T^{n-h}) \cdot O_{n,h}(q^{n-1}) + O_{n,h}(q^n q^{(n-h)/2})) = O_{n,h}(q^{n-1}). \quad \square$$

In a similar same manner, we obtain a more general bound for factorization functions that needn't be supported on the squarefuls.

Lemma 8.3. *For a fixed factorization function a ,*

$$\sum_{f \in \mathcal{M}_n} \left| \sum_{\substack{g \in I(f;h) \\ f \in \mathcal{M}_n^{\natural}}} \tilde{a}^{\natural}(g) \right|^2 = O_{n,h}(q^{h+1}q^n),$$

for $0 \leq h \leq n$.

Proof. This follows from Lemmas 8.1 and 6.3. □

Step 3: We show that the variances of sums over \mathcal{M}_n^{\natural} we have computed in Lemma 8.1 are not far from those of sums over \mathcal{M}_n , which we are ultimately after.

Lemma 8.4. *For a fixed factorization function a ,*

$$\sum_{f \in \mathcal{M}_n} \left| \sum_{g \in I(f;h)} \tilde{a}(g) \right|^2 = \sum_{f \in \mathcal{M}_n} \left| \sum_{\substack{g \in I(f;h) \\ f \in \mathcal{M}_n^{\natural}}} \tilde{a}^{\natural}(g) \right|^2 + O_{h,n}(q^{h+1/2}q^n),$$

for $0 \leq h \leq n$.

Note, in comparison with the error term, that we expect the left-hand side to usually be of order $q^n q^{h+1}$.

Proof. We make use of a mapping of polynomials $f \mapsto f^{[i]}$ defined by

$$(a_0 + a_1T + \dots + a_nT^n)^{[i]} = a_i + a_{i+1}T + \dots + a_nT^{n-i},$$

so that if $T^i \mid f$,

$$f = T^i f^{[i]}.$$

For $f \in \mathcal{M}_n$, we may partition $I(f; h)$ into the disjoint union

$$I(f; h) = \left(\bigcup_{i=0}^h \{T^i g \in I(f; h) : g \in \mathcal{M}_{n-i}^{\natural}\} \right) \cup \{T^{h+1} f^{[h+1]}\}. \quad (45)$$

For $g \in \mathcal{M}_{n-i}^{\natural}$, we define the function

$$a_{[i]}(g) := a(T^i g),$$

with

$$\tilde{a}_{[i]}(g) := a_{[i]}(g) - E^{\natural}(a_{[i]}; n - i), \quad \text{with} \quad E^{\natural}(a_{[i]}; n - i) = \frac{1}{|\mathcal{M}_{n-i}^{\natural}|} \sum_{g \in \mathcal{M}_{n-i}^{\natural}} a_{[i]}(g).$$

From the partitioning (45), it is easy to see that for $f \in \mathcal{M}_n$,

$$\sum_{g \in I(f; h)} a(f) = \sum_{\substack{g \in I(f; h) \\ g \in \mathcal{M}_n^{\natural}}} a(g) + \sum_{\substack{g \in I(f^{[1]}; h-1) \\ g \in \mathcal{M}_{n-1}^{\natural}}} a_{[1]}(g) + \cdots + \sum_{\substack{g \in I(f^{[h]}; 0) \\ g \in \mathcal{M}_{n-h}^{\natural}}} a_{[h]}(g) + \underbrace{a(T^{h+1} f^{[h+1]})}_{=O_{n,h}(1)}. \quad (46)$$

Using that

$$|\mathcal{M}_n^{\natural}| = q^{n-1}(q - 1), \quad \text{and} \quad |\{g \in I(f; h) : g \in \mathcal{M}_n^{\natural}\}| = q^h(q - 1),$$

one may verify (with a little work, but straightforwardly) that

$$\sum_{g \in I(f; h)} E(a; n) = \frac{q^{h+1}}{q^n} \sum_{g \in \mathcal{M}_n} a(g) = \sum_{k=0}^h \sum_{\substack{g \in I(f^{[k]}; h-k) \\ g \in \mathcal{M}_{n-k}^{\natural}}} E^{\natural}(a_{[k]}; n - k) + \underbrace{\frac{q^{h+1}}{q^n} \sum_{g \in \mathcal{M}_{n-h-1}} a(T^{h+1} g)}_{=O_{n,h}(1)}. \quad (47)$$

Thus combining (46) and (47), we have uniformly for $f \in \mathcal{M}_n$,

$$\sum_{g \in I(f; h)} \tilde{a}(g) = \sum_{\substack{g \in I(f; h) \\ g \in \mathcal{M}_n^{\natural}}} \tilde{a}^{\natural}(g) + \sum_{\substack{g \in I(f^{[1]}; h-1) \\ g \in \mathcal{M}_{n-1}^{\natural}}} \tilde{a}_{[1]}^{\natural}(g) + \cdots + \sum_{\substack{g \in I(f^{[h]}; 0) \\ g \in \mathcal{M}_{n-h}^{\natural}}} \tilde{a}_{[h]}^{\natural}(g) + O_{n,h}(1). \quad (48)$$

For each i , the function $a_{[i]}$ defined on \mathcal{M}_{n-i} extends uniquely to a factorization function defined on all of \mathcal{M}_{n-i} . Hence, using Lemma 8.3 to pass to the second line below,

$$\sum_{f \in \mathcal{M}_n} \left| \sum_{\substack{g \in I(f^{[i]}; h-i) \\ g \in \mathcal{M}_{n-i}^{\natural}}} \tilde{a}_{[i]}^{\natural}(g) \right|^2 = q^i \sum_{f \in \mathcal{M}_{n-i}} \left| \sum_{g \in I(f; h-i)} \tilde{a}_{[i]}^{\natural}(g) \right|^2 \ll_{n,h} q^i q^{h-i+1} q^{n-i}.$$

This quantity is no more than $q^h q^n$ for $i \geq 1$, and for $i = 0$ it is of course equal to $q^{h+1} q^n$.

Therefore, squaring the identity (48) and summing over $g \in \mathcal{M}_n$, then using Cauchy–Schwarz and (49) to bound all terms but one on the right,

$$\sum_{f \in \mathcal{M}_n} \left| \sum_{g \in I(f; h)} \tilde{a}(g) \right|^2 = \sum_{f \in \mathcal{M}_n} \left| \sum_{\substack{g \in I(f; h) \\ g \in \mathcal{M}_n^{\natural}}} \tilde{a}^{\natural}(g) \right|^2 + O_{n,h}(q^n q^{h+1/2}),$$

as claimed. □

Step 4: Recall the “factorization Fourier expansion” (14):

$$a(f) = A(f) + b(f), \tag{49}$$

with

$$A(f) := \sum_{\lambda} \hat{a}_{\lambda} X^{\lambda}(f),$$

where $b(f)$ is a function supported on the squarefuls. We use this to reduce variance for the function $a(f)$ to finding the covariance of characters $X^{\lambda}(f)$.

We introduce the shorthand, for partitions $\lambda, \nu \vdash n$,

$$\Delta_{\lambda, \nu}(m) := \mathbb{E}_{\chi(T^m)_{\text{prim, ev}}} \left(\sum_{f \in \mathcal{M}_n} X^{\lambda}(f) \chi(f) \right) \overline{\left(\sum_{g \in \mathcal{M}_n} X^{\nu}(g) \chi(g) \right)}. \tag{50}$$

Note that by Corollary 7.3, for $m \geq 5$,

$$\Delta_{\lambda, \nu}(m) = \delta_{\lambda \nu} \delta_{\ell(\lambda'), \ell(\nu') \leq m-2} + O(q^{-1/2}) = \delta_{\lambda \nu} \delta_{\lambda_1, \nu_1 \leq m-2} + O(q^{-1/2}). \tag{51}$$

Lemma 8.5. For a fixed factorization function a , with $0 \leq h \leq n - 4$,

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f; h)} a(g) \right) = q^{h+1} \sum_{\mu, \nu \vdash n} \Delta_{\lambda, \nu}(n-h) \hat{a}_{\lambda} \overline{\hat{a}_{\nu}} + O_{n, h}(q^{h+1/2}). \tag{52}$$

Proof. The variance in (52) is given by

$$\frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \left| \sum_{g \in I(f; h)} \tilde{a}(g) \right|^2 = \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \left| \sum_{g \in I(f; h)} \tilde{A}^{\natural}(g) \right|^2 + O_{n, h}(q^{h+1/2}),$$

where we have reduced to a sum of terms $\tilde{A}^{\natural}(g)$ by using Lemma 8.4 and then Lemmas 8.2 and 8.3 to absorb a sum of terms $b^{\natural}(g)$ into the error term.

In turn from Lemma 8.1,

$$\begin{aligned} \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \left| \sum_{g \in I(f; h)} \tilde{A}^{\natural}(g) \right|^2 &= \frac{q^{h+1}(q-1)}{q^n \Phi(T^{n-h})} \sum_{\substack{\chi \neq \chi_0(T^{n-h}) \\ \text{even}}} \left| \sum_{g \in \mathcal{M}_n} A(g) \chi(g) \right|^2 \\ &= \frac{q^{h+2}}{q^n q^{n-h}} \left(\sum_{\substack{\chi(T^{n-h}) \\ \text{prim, ev}}} \left| \sum_{g \in \mathcal{M}_n} A(g) \chi(g) \right|^2 + O_{n, h}(q^n \cdot q^{n-h-2}) \right). \end{aligned}$$

The second line has followed by taking nonprimitive even characters from the sum and bounding their contribution by Lemma 6.3. The above quantity simplifies to

$$q^{h+1} \mathbb{E}_{\chi(T^{n-h})_{\text{prim, ev}}} \left| \sum_{g \in \mathcal{M}_n} A(g) \chi(g) \right|^2 + O_{n, h}(q^h),$$

and Lemma 8.5 follows by expanding $A(g)$ into a linear combination of characters X^λ (recall A is defined by (49)) and then expanding the square above. □

With this lemma in place, Theorem 3.1 now follows by applying (51).

9. Factorization Fourier expansions

9A. We list some examples of the expansion (14) for the arithmetic functions we considered in Section 1. In this way we recover Theorems 1.3, 1.4, and 1.5, estimating variance over short intervals of the Möbius function, the von Mangoldt function, and the k -fold divisor function. We also consider the function ω , which as usual counts distinct prime factors, and this leads to a new result for the variance of $\omega(f)$ and $\mu(f)\omega(f)$ summed over short intervals.

Proposition 9.1. For $f \in \mathcal{M}_n$,

$$\mu(f) = (-1)^n X^{(1^n)}(f).$$

Remark. Applied to Theorem 3.1 this recovers Theorem 1.3, for $\mu(f)$.

Proof. Both $\mu(f)$ and $X^{(1^n)}(f)$ will be zero unless f is squarefree. But for $f = p_1 \cdots p_\ell$, with all factors distinct, $\mu(f) = (-1)^\ell$, while it may be checked $X^{(1^n)}(f) = (-1)^{\deg(p_1)-1} \cdots (-1)^{\deg(p_\ell)-1}$. As $(-1)^{\deg(p_1)} \cdots (-1)^{\deg(p_\ell)} = (-1)^n$, this verifies the claim. □

Proposition 9.2. For $f \in \mathcal{M}_n$,

$$\mu(f)^2 = X^{(n)}(f).$$

Proof. As $X^{(n)}$ is the trivial character, this is clear. □

Proposition 9.3. For $f \in \mathcal{M}_n$,

$$\Lambda(f) = \sum_{r=1}^n (-1)^{n-r} X^{(r, 1^{n-r})}(f) + b(f),$$

for a function $b(f)$ that is supported on the squarefuls.

Remark. This recovers Theorem 1.4, for $\Lambda(f)$.

If we define the function,

$$\Lambda_j(f) := \sum_{\substack{g|f \\ g \text{ monic}}} \mu(g) \deg(f/g)^j, \tag{53}$$

the proposition above is special case of:

Proposition 9.4. For $f \in \mathcal{M}_n$,

$$\Lambda_j(f) = \sum_{r=1}^n (-1)^{n-r} (r^j - (r-1)^j) X^{(r, 1^{n-r})}(f) + b(f),$$

for a function $b(f)$ that is supported on the squarefuls.

Remark. This recovers an estimate for the covariance of almost-primes in short intervals, proved in [Rodgers 2015].

Note that, using (53),

$$\Lambda_j(f) = \sum_{r=1}^n (r^j - (r-1)^j) \sum_{\substack{g|f \\ \deg(g) \leq n-r \\ g \text{ monic}}} \mu(g),$$

so we have that Proposition 9.4 is a corollary of:

Proposition 9.5. For $f \in \mathcal{M}_n$, with $n = r + s$ and $0 \leq s < n$,

$$\sum_{\substack{g|f \\ \deg(g) \leq s \\ g \text{ monic}}} \mu(g) = (-1)^s X^{(r,1^s)}(f) + b(f),$$

for a function $b(f)$ that is supported on the squarefals.

Proof. We will need to make use of the Murnaghan–Nakayama rule, quoted in Theorem 5.1.

We may suppose that f is squarefree (otherwise the proposition is trivial), and let $f = p_1 \cdots p_\ell$ with $\deg p_i = \tau_i$, $\tau_1 \geq \tau_2 \geq \cdots$. We apply the Murnaghan–Nakayama rule to the type $\tau_f = (\tau_1, \dots, \tau_\ell)$ and Young diagram of $(r, 1^s)$. For any border-strip tableau, let $I \subset \{2, \dots, \ell\}$ be the collection of numbers that appear in rows 2 through s of the Young diagram of $(r, 1^s)$. Writing

$$\tau_I := \sum_{i \in I} \tau_i,$$

to form a valid border-strip tableau, it is easy to see that we require only that $\tau_I \leq s$ and $\tau_1 + \tau_I \geq s + 1$. Hence, applying the rule,

$$X^{(r,1^s)}(f) = \sum_{\substack{I \subset \{2, \dots, \ell\} \\ \tau_I \leq s \\ \tau_1 + \tau_I \geq s + 1}} (-1)^{\tau_I - |I|} (-1)^{(s+1) - \tau_I - 1} = (-1)^s \sum_{\substack{I \subset \{2, \dots, \ell\} \\ s - \tau_1 < \tau_I \leq k}} (-1)^{|I|}. \tag{54}$$

Yet,

$$\sum_{\substack{g|f \\ \deg(g) \leq s \\ g \text{ monic}}} \mu(g) = \sum_{J \subset \{1, \dots, \ell\}} (-1)^{|J|} \tag{55}$$

By breaking the right-hand sum into parts for which 1 is an element of J or not, we see that (55) is equal to

$$\sum_{\substack{I \subset \{2, \dots, \ell\} \\ \tau_I \leq s}} (-1)^{|I|} + \sum_{\substack{I \subset \{2, \dots, \ell\} \\ \tau_I + \tau_1 \leq s}} (-1)^{|I|+1} = \sum_{\substack{I \subset \{2, \dots, \ell\} \\ s - \tau_1 < \tau_I \leq s}} (-1)^{|I|}.$$

Comparing this with (54) yields the result. □

Proposition 9.6. For $f \in \mathcal{M}_n$,

$$d_k(f) = \sum_{\substack{\lambda \vdash n \\ \ell(\lambda) \leq k}} s_\lambda(\underbrace{1, \dots, 1}_k) X^\lambda(f) + b(f), \tag{56}$$

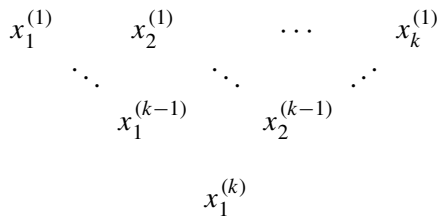
for a function $b(f)$ that is supported on the squarefuls. Moreover, we have the following equivalent expressions for $s_\lambda(1, \dots, 1)$:

$$(i) \quad s_\lambda(\underbrace{1, \dots, 1}_k) = \prod_{1 \leq i < j \leq k} \frac{\lambda_i - \lambda_j + j - i}{j - i}, \tag{57}$$

with the convention that $\lambda_{\ell(\lambda)+1} = \dots = \lambda_k = 0$ if $\ell(\lambda) < k$.

$$(ii) \quad s_\lambda(\underbrace{1, \dots, 1}_k) = \text{GT}_k(\lambda), \tag{58}$$

where $\text{GT}_k(\lambda)$ is the number of triangular arrays of nonnegative integers



with entries weakly decreasing left-to-right down diagonals and weakly increasing left-to-right up diagonals (that is, $x_j^{(i)} \geq x_j^{(i+1)} \geq x_{j+1}^{(i)}$), and in the top row, $x_i^{(1)} = \lambda_i$, with again the convention if $\ell(\lambda) < k$ that $\lambda_{\ell(\lambda)+1} = \dots = \lambda_k = 0$.

$$(iii) \quad s_\lambda(\underbrace{1, \dots, 1}_k) = \prod_{u \in \lambda} \frac{k + c(u)}{h(u)}, \tag{59}$$

where the product is over all squares u of the Young diagram of λ , and where if we label the squares u by the coordinates (i, j) with $1 \leq j \leq \lambda_i$, the content $c(u)$ is defined by

$$c(u) = i - j,$$

and the hook length $h(u)$ is defined by

$$h(u) = \lambda_i + \lambda'_j - i - j + 1.$$

(See [Stanley 1999, p. 373] for a lengthier account of these definitions.)

Remark. Using the representation (ii), this recovers the variance of the k -fold divisor function given in Theorem 1.5.

Proof. It will again be sufficient to consider f squarefree. We note that for p prime, $d_k(p) = k$, so for $f = p_1 \cdots p_\ell$ with all prime factors distinct,

$$d_k(f) = k^\ell = k^{\ell(\tau)},$$

where τ is the factorization type of f . On the other hand,

$$k^{\ell(\tau)} = p_\tau \underbrace{(1, \dots, 1)}_k = \sum_{\lambda \vdash n} s_\lambda \underbrace{(1, \dots, 1)}_k X^\lambda(\tau), \tag{60}$$

by [Theorem 5.2](#) of Frobenius. This proves [\(56\)](#).

For the formula given in (i), note that for $\ell(\lambda) > k$, we have $s_\lambda(1, \dots, 1) = 0$, while for $\ell(\lambda) \leq k$, the identity [\(57\)](#) is [\[Fulton 1997, Example 6, Chapter 6\]](#).

For the formula given in (ii), note that $s_\lambda(1, \dots, 1)$ is equal to the number of semistandard Young tableaux of shape λ with entries 1 through k (see [\[Stanley 1999, §7.10\]](#)), and by a well-known bijection (again, see [\[Stanley 1999, §7.10\]](#)) this is equal to $\text{GT}_k(\lambda)$. (For readers familiar with the terminology, $\text{GT}_k(\lambda)$ is a count of Gelfand–Tsetlin patterns.)

For the formula given in (iii), this is [Corollary 7.21.4](#) of [\[Stanley 1999\]](#). □

Proposition 9.7. *Let $\omega(f)$ be the number of distinct primes that divide f . Then for $f \in \mathcal{M}_n$,*

$$\omega(f) = H_n X^{(n)}(f) + \sum_{\lambda} (-1)^v \left(\frac{1}{\lambda_2 + v} - \frac{1}{\lambda_1 + v + 1} \right) X^{(\lambda_1, \lambda_2, 1^v)}(f) + b(f), \tag{61}$$

where the sum is over all partitions $\lambda = (\lambda_1, \lambda_2, 1^v) \vdash n$ with $\lambda_2 \geq 1$ and $v \geq 0$, where $b(f)$ is a function supported on the squarefuls, and where

$$H_n := \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}.$$

Remark. The mean value as $q \rightarrow \infty$ of $\omega(f)$ for $\deg(f) = n$ is H_n . Because $X^{(n)}(f) = 1$ for all squarefree f , the expression [\(61\)](#) may be thought of as characterizing the oscillation of $\omega(f)$ around this value.

Proof. We use the identity [\(60\)](#) from the last proof, along with the representation [\(59\)](#) for $s_\lambda(1, \dots, 1)$. Taken together these imply for $\tau \vdash n$ and positive integer k ,

$$k^{\ell(\tau)} = \sum_{\lambda \vdash n} \prod_{u \in \lambda} \frac{k + c(u)}{h(u)} X^\lambda(\tau). \tag{62}$$

Though we have only demonstrated [\(62\)](#) for an integer k , both the left- and right-hand side of this identity are polynomials in k , and therefore [\(62\)](#) must hold for all $k \in \mathbb{C}$. Differentiating [\(62\)](#) and setting $k = 1$ requires some slightly tedious book-keeping, but is otherwise straightforward and gives us

$$\ell(\tau) = H_n X^{(n)}(\tau) + \sum_{\lambda} (-1)^v \left(\frac{1}{\lambda_2 + v} - \frac{1}{\lambda_1 + v + 1} \right) X^{(\lambda_1, \lambda_2, 1^v)}(\tau). \tag{63}$$

Applying this to the factorization types of $f \in \mathcal{M}_n$ gives the proposition. □

Proposition 9.8. For $f \in \mathcal{M}_n$,

$$\mu(f)\omega(f) = (-1)^n \left[H_n X^{(1^n)}(f) + \sum (-1)^v \left(\frac{1}{j+v+1} - \frac{1}{i+j+v+2} \right) X^{(v+2, 2^j, 1^i)}(f) \right] + b(f), \tag{64}$$

where the sum is over all partitions $(v+2, 2^j, 1^i) \vdash n$, with $i, j, v \geq 0$, and $b(f)$ is a function supported on the squarefals.

Proof. For f squarefree with factorization type τ , note that $\mu(f)\omega(f) = (-1)^{\ell(\tau)}\ell(\tau)$. But by applying Proposition 5.4 to the identity (63), we may decompose $(-1)^{\ell(\tau)}\ell(\tau)$ into a sum over irreducible characters associated to dual partitions. This decomposition yields (64). \square

9B. By applying Theorem 3.1 to Propositions 9.7 and 9.8 we straightforwardly obtain the following results:

Corollary 9.9. For fixed $0 \leq h \leq n - 5$,

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} \omega(g) \right) = q^{h+1} \sum_{1 \leq \lambda_2 \leq \lambda_1 \leq n-h-2} \sum_{\lambda_1 + \lambda_2 \leq n} \left(\frac{1}{n-\lambda_1} - \frac{1}{n-\lambda_2+1} \right)^2 + O(q^{h+1/2}). \tag{65}$$

Corollary 9.10. For fixed $0 \leq h \leq n - 5$,

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} \mu(g)\omega(g) \right) = q^{h+1} \left[H_n^2 + \sum_{h+2 \leq i+2j \leq n-2} \sum \left(\frac{1}{n-i-j-1} - \frac{1}{n-j} \right)^2 \right] + O(q^{h+1/2}). \tag{66}$$

9C. Because the double-indexed sum in the asymptotic formula of (66) remains bounded for $n \rightarrow \infty$ and $h \sim \delta n$ with $\delta > 0$, and because $H_n \sim \log n = \log \deg(f)$ for $f \in \mathcal{M}_n$, one may think of Corollary 9.10 as a function field analogue of the following conjecture over the integers (which is intuitive enough on its own):

Conjecture 9.11. For $H = X^\delta$ with fixed $\delta \in (0, 1)$, as $X \rightarrow \infty$, we have

$$\frac{1}{X} \int_X^{2X} \left(\sum_{x \leq n \leq x+H} \mu(n)\omega(n) \right)^2 dx \sim H (\log \log X)^2.$$

Corollary 9.9 has a rather more striking interpretation. In (65) the double indexed sum remains bounded for $h \sim \delta n$ with $\delta \in (0, 1)$ fixed; indeed the reader may check that

$$\sum_{1 \leq \lambda_2 \leq \lambda_1 \leq n-h-2} \sum_{\lambda_1 + \lambda_2 \leq n} \left(\frac{1}{n-\lambda_1} - \frac{1}{n-\lambda_2+1} \right)^2 \sim p(\delta) < +\infty \tag{67}$$

as $n \rightarrow \infty$ for⁴

$$p(\delta) := \int_{\substack{x+y \geq 1 \\ \delta \leq x \leq y \leq 1}} \left(\frac{1}{x} - \frac{1}{y} \right)^2 dx dy.$$

⁴One can further reduce the integral to see

$$p(\delta) = \begin{cases} \log((1-\delta)/\delta) + \delta - \text{Li}_2(1-\delta) + \text{Li}_2(\delta) - \log(1-\delta) \log(\delta) & \text{for } \delta \leq 1/2, \\ (1-\delta)/\delta - (1-\delta) - \log(\delta)^2 & \text{for } \delta > 1/2, \end{cases}$$

where Li_2 is the dilogarithm. Note the phase change at $\delta = \frac{1}{2}$.

Because this is bounded it is reasonable to suppose:

Conjecture 9.12. For $H = X^\delta$ with fixed $\delta \in (0, 1)$ as $X \rightarrow \infty$ we have

$$\frac{1}{X} \int_X^{2X} \left(\sum_{x \leq n \leq x+H} \omega(n) \right)^2 dx - \left(\frac{1}{X} \int_X^{2X} \sum_{x \leq n \leq x+H} \omega(n) dx \right)^2 = O_\delta(H). \tag{68}$$

There is a sense in which an estimate of the sort in [Conjecture 9.12](#) would be surprising, since the Erdős–Kac theorem [[1940](#)] predicts that diagonal terms make a contribution of size $H \log \log X$. Clearly that $\delta \in (0, 1)$ remain fixed is important for anything like [Conjecture 9.12](#) to be true — the consideration of diagonal terms shows that we cannot have such an estimate if $\delta \rightarrow 0$ as $X \rightarrow \infty$. Nonetheless the function field analogy remains, and it would be interesting to study in greater depth whether [Conjecture 9.12](#) is true.⁵

Rather more ambitiously, one may even guess that the right-hand side of (68) can be replaced by

$$p(\delta)H + o_\delta(H).$$

10. Covariance

10A. In analogy with the definition of variance, (4), we define the covariance of two arithmetic functions η_1 and η_2 by

$$\text{Covar}_{f \in \mathcal{M}_n}(\eta_1(f), \eta_2(f)) := \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} (\eta_1(f) - \mathbb{E}_{\mathcal{M}_n} \eta_1) \overline{(\eta_2(f) - \mathbb{E}_{\mathcal{M}_n} \eta_2)}.$$

Because [Theorem 3.1](#) holds for a general factorization function a , it implies by a standard argument a corresponding result for covariance.

Theorem 10.1. For $a(f)$ and $b(f)$ fixed factorization functions and for fixed $0 \leq h \leq n - 5$,

$$\text{Covar}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} a(g), \sum_{g \in I(f;h)} b(g) \right) = q^{h+1} \sum_{\substack{\lambda \vdash n \\ \lambda_1 \leq n-h-2}} \hat{a}_\lambda \overline{\hat{b}_\lambda} + O(q^{h+1/2}).$$

One consequence of this is worthwhile to draw out. Since $\mu(g) = X^{(1^n)}(g)$, we see directly that:

Corollary 10.2. For $a(f)$ a fixed factorization function and for fixed $0 \leq h \leq n - 5$,

$$\text{Covar}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} a(g), \sum_{g \in I(f;h)} \mu(g) \right) = q^{h+1} \hat{a}_{(1^n)} + O(q^{h+1/2}) = q^{h+1} \cdot \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \mu(g) a(g) + o(q^{h+1}).$$

That is to say, the Möbius function oscillates to such an extent that in estimating its short-interval-sum covariance against any factorization function, only diagonal terms contribute. It is easy to see that (up to values on the squarefuls) the Möbius function is unique among factorization functions in this regard.

⁵Andrew Granville (personal communication) has shown a variant of this conjecture is true for a restricted range of δ , when $\omega(n)$ is replaced by $\omega_y(n)$, a count of prime factors of n less than $y = X^{1/2-\epsilon}$.

For example, [Corollary 10.2](#) implies

$$\text{Covar}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} \Lambda(g), \sum_{g \in I(f;h)} \mu(g) \right) \sim -q^{h+1},$$

as $q \rightarrow \infty$. Over the integers we have the following analogy:

Conjecture 10.3. For $H = X^\delta$ with $\delta \in (0, 1)$,

$$\frac{1}{X} \int_X^{2X} \left(\sum_{x \leq n \leq x+H} \Lambda(n) - H \right) \left(\sum_{x \leq n \leq x+H} \mu(n) \right) dx \sim -H,$$

as $X \rightarrow \infty$.

11. Decompositions: proofs of [Theorem 3.2](#) and [Corollary 3.5](#)

11A. We now turn to the decomposition of the space of factorization functions \mathcal{F} into \mathcal{U}_n^h and \mathcal{V}_n^h and the corresponding evaluation of variance described in [Theorem 3.2](#). Recall that \mathcal{U}_n^h is the linear space of functions defined by (17) and \mathcal{V}_n^h is orthogonal complement supported on squarefuls. We first demonstrate the explicit characterization of the spaces \mathcal{U}_n^h and \mathcal{V}_n^h given by [Proposition 3.3](#).

Proof of [Proposition 3.3](#). Let \mathcal{A}_n^h and \mathcal{B}_n^h be as in the proposition and

$$\mathcal{C}_n^h := \text{span}\{X^\lambda(f) : \lambda \vdash n, \lambda_1 \leq n - h - 2\}.$$

Note that \mathcal{C}_n^h is supported on the squarefrees, and

$$\mathcal{F} = (\mathcal{A}_n^h \oplus \mathcal{B}_n^h) \oplus \mathcal{C}_n^h.$$

Moreover, by the equidistribution of factorization types and cycles types and the orthogonality of characters X^λ , \mathcal{A}_n^h is orthogonal to \mathcal{C}_n^h .

[Theorem 3.1](#) implies that $\mathcal{A}_n^h \oplus \mathcal{B}_n^h \subset \mathcal{U}_n^h$, and likewise that $\mathcal{C}_n^h \cap \mathcal{U}_n^h = \{0\}$, so that no function outside of $\mathcal{A}_n^h \oplus \mathcal{B}_n^h$ lies in \mathcal{U}_n^h ; that is, $\mathcal{A}_n^h \oplus \mathcal{B}_n^h = \mathcal{U}_n^h$. \mathcal{V}_n^h , defined to be the orthogonal complement supported on squarefuls, is thus identical with \mathcal{C}_n^h , which proves the proposition. □

Proof of [Theorem 3.2](#). Note that for $v \in \mathcal{V}_n^h$ with

$$v(f) = \sum_{\lambda_1 \leq n-h-2} \hat{v}_\lambda X^\lambda(f),$$

we have

$$\langle v, v \rangle = \lim_{q \rightarrow \infty} \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} v(f) \overline{v(f)} = \sum_{\lambda_1 \leq n-h-2} |\hat{v}_\lambda|^2,$$

by again making use of the equidistribution of factorization types and cycle types ([Proposition 2.3](#)). Combined with [Theorem 3.1](#), this gives the result. □

11B. We now turn to [Proposition 3.4](#) and [Corollary 3.5](#).

Proof of Proposition 3.4. We note first that for any factorization function α , it is simple to see that

$$w(f) := \sum_{\substack{\delta | f \\ \deg(\delta) \leq h+1}} \alpha(\delta), \quad (\text{defined for } f \in \mathcal{M}_n)$$

lies in \mathcal{U}_n^h . (Recall that \mathcal{U}_n^h is defined by (17).) For in this case, for any $f \in \mathcal{M}_n$,

$$\sum_{g \in I(f;h)} q(g) = \sum_{\deg(\delta) \leq h+1} \alpha(\delta) \sum_{\substack{g \in I(f;h) \\ \delta | g}} 1 = \sum_{\deg(\delta) \leq h+1} \alpha(\delta) q^{h+1-\deg(\delta)}.$$

This does not depend on f , so that

$$\text{Var}_{f \in \mathcal{M}_n} \left(\sum_{g \in I(f;h)} w(g) \right) = 0,$$

implying $w \in \mathcal{U}_n^h$. Since we already know any factorization function $b \in \mathcal{F}_n$ supported on the squarefuls lies in the linear space \mathcal{U}_n^h , and function of the form $w(f) + b(f)$ must therefore lie in \mathcal{U}_n^h .

Hence to complete the proof of the proposition, we need only show that all functions in \mathcal{U}_n^h are of this form. Having already characterized \mathcal{U}_n^h in terms of characters of the symmetric group in [Proposition 3.3](#), we will have done so if we show that for $\lambda \vdash n$ with $\lambda_1 \geq n - h - 1$, there exists a factorization function α and a factorization function b supported on the squarefuls such that

$$X^\lambda(f) = \sum_{\substack{\delta | f \\ \deg(\delta) \leq h+1}} \alpha(\delta) + b(f), \quad (\text{for all } f \in \mathcal{M}_n).$$

The remainder of this proof is devoted to a demonstration in four steps of this claim.

Step 1: Let m be arbitrary. For an even primitive character χ modulo T^m , from the identity

$$\left(1 - \frac{u}{\sqrt{q}}\right) \prod_{j=1}^{m-2} (1 - ue^{i2\pi \vartheta_j}) = \mathcal{L}\left(\frac{u}{\sqrt{q}}, \chi\right) = \sum_{n \geq 0} u^n \frac{1}{q^{n/2}} \sum_{f \in \mathcal{M}_n} \chi(f),$$

we have the following expression for elementary symmetric functions in the normalized roots of the \mathcal{L} -function:

$$e_n(\Theta_\chi) = \frac{(-1)^n}{q^{n/2}} \sum_{f \in \mathcal{M}_n} \chi(f) + O_{n,m}(q^{-1/2}). \tag{69}$$

Step 2: We note for $n_1 + \dots + n_k = n$,

$$\begin{aligned} e_{n_1}(\Theta_\chi) \cdots e_{n_k}(\Theta_\chi) &= \frac{(-1)^n}{q^{n/2}} \left(\sum_{f_1 \in \mathcal{M}_{n_1}} \chi(f_1) + O_{n,m}(q_{-1/2}) \right) \cdots \left(\sum_{f_k \in \mathcal{M}_{n_k}} \chi(f_k) + O_{n,m}(q_{-1/2}) \right) \\ &= \frac{(-1)^n}{q^{n/2}} \sum_{\substack{f_1 \in \mathcal{M}_{n_1} \\ g \in \mathcal{M}_{n_2+\dots+n_k}}} \chi(f_1 g) \alpha(g) + O_{n,m}(q^{-1/2}), \end{aligned}$$

where

$$\alpha(g) := \sum_{\substack{f_2 \cdots f_k = g \\ f_2 \in \mathcal{M}_2, \dots, f_k \in \mathcal{M}_k}} 1$$

is a factorization function supported on $\mathcal{M}_{n_2 + \dots + n_k}$. In particular, we have that if $n_1 \geq n - h - 1$ (so $n_2 + \dots + n_k \leq h + 1$) then

$$e_{n_1} \cdots e_{n_k} = \frac{(-1)^n}{q^{n/2}} \sum_{f \in \mathcal{M}_n} \chi(f) \sum_{\delta | f} \alpha(\delta) + O_{n,m}(q^{-1/2}), \tag{70}$$

for a factorization function $\alpha(\delta)$ supported on the set of δ with $\deg(\delta) \leq h + 1$.

Step 3: From an expansion of the determinant in the Jacobi–Trudi identity, we see for $\lambda \vdash n$ that $s_{\lambda'}$ is a linear combination of terms $e_{n_1} \cdots e_{n_k}$ with $n_1 + \dots + n_k = n$ and (from the top row of the determinant) $n_1 \geq \lambda_1$ always. Hence via step 2, if $\lambda_1 \geq n - h - 1$,

$$s_{\lambda'}(\Theta_{\chi}) = \frac{(-1)^n}{q^{n/2}} \sum_{f \in \mathcal{M}_n} \chi(f) \sum_{\delta | f} \alpha(\delta) + O_{n,m}(q^{-1/2}), \tag{71}$$

for a factorization function $\alpha(\delta)$ supported on δ with $\deg(\delta) \leq h + 1$, since linear combinations of terms of the form $\sum_{\delta | f} \alpha(\delta)$ remain of this form.

Yet from [Theorem 7.1](#)

$$s_{\lambda'}(\Theta_{\chi}) = \frac{(-1)^n}{q^{n/2}} \sum_{f \in \mathcal{M}_n} X^{\lambda}(f) \chi(f) + O(q^{-1/2}). \tag{72}$$

Hence pairing [\(71\)](#) and [\(72\)](#) we have

$$\frac{1}{q^{n/2}} \sum_{f \in \mathcal{M}_n} \chi(f) \left(X^{\lambda}(f) - \sum_{\substack{\delta | f \\ \deg(\delta) \leq h+1}} \alpha(\delta) \right) = O_{n,m}(q^{-1/2}). \tag{73}$$

Step 4: In [\(73\)](#), m is arbitrary; take m sufficiently large depending on n , with the intention of using [Lemma 7.4](#). We have upon squaring and averaging,

$$\mathbb{E}_{\chi(T^m)} \left| \frac{1}{q^{n/2}} \sum_{f \in \mathcal{M}_n} \chi(f) \left(X^{\lambda}(f) - \sum_{\substack{\delta | f \\ \deg(\delta) \leq h+1}} \alpha(\delta) \right) \right|^2 \rightarrow 0,$$

as $q \rightarrow \infty$. But then from [Lemma 7.4](#),

$$\left\| X^{\lambda}(f) - \sum_{\substack{\delta | f \\ \deg(\delta) \leq h+1}} \alpha(\delta) \right\| = 0,$$

for $\|\cdot\|$ the norm induced by our inner product. Since this inner product is nondegenerate on functions supported on the squarefrees, we must have

$$X^\lambda(f) = \sum_{\substack{\delta|f \\ \deg(\delta)\leq h+1}} \alpha(\delta) + b(f),$$

for some function $b(f)$ supported on the squarefuls, as claimed. □

Proof of Corollary 3.5. This follows immediately from Theorem 3.2 and Proposition 3.4. For in the identity (19), the function $v(f)$ is a projection of the function $a(f)$ to the subspace \mathcal{V}_n^h , but then

$$\langle v, v \rangle = \|\text{Proj}_{\mathcal{V}_n^h}(a)\|^2 = \inf_{u \in \mathcal{U}_n^h} \|a - u\|^2 = \inf_{\alpha \in \mathcal{F}} \left\| a(f) - \sum_{\substack{\delta|f \\ \deg(\delta)\leq h+1}} \alpha(\delta) \right\|^2.$$

□

11C. It is worthwhile to reflect one last time on the dichotomy between \mathcal{U}_n^h and \mathcal{V}_n^h . Theorem 7.1 gives us another way to characterize them. \mathcal{U}_n^h is just the collection of those factorization functions u for which

$$\sum_{f \in \mathcal{M}_n} u(f)\chi(f) = O(q^{n/2-1/2}), \tag{74}$$

uniformly for all even primitive characters modulo T^{n-h} . The reason that Theorem 7.1 implies (74) is very simply that $\mathcal{L}(u, \chi)$ always has $n - h - 2$ nontrivial zeros. Contrariwise, Theorem 3.2 and Proposition 3.3 tell us that for those factorization functions which do not have enough structure to belong to \mathcal{U}_n^h their variance may be computed according to the most naive heuristic of randomness. Indeed, one last reformulation of Theorem 3.2 may be seen to be the following: for $v_1, v_2 \in \mathcal{V}_n^n$,

$$\mathbb{E}_{\chi(T^{n-h})} \sum_{\substack{\text{prim, ev} \\ f, g \in \mathcal{M}_n \\ f \neq g}} v_1(f)\chi(f)\overline{v_2(g)\chi(g)} = o(q^n). \tag{75}$$

It would be interesting to see whether a modification of this picture is consistent with conjectures that have been made in other settings (e.g., in the fixed q large n limit, or over number fields), or indeed with statistics in orthogonal and symplectic families.

Acknowledgments

For helpful discussions, I thank a number of people, including Efrat Bank, Dan Bump, Reda Chhaibi, Paul-Olivier Dehaye, Andrew Granville, Jeff Lagarias, Zeev Rudnick, Will Sawin, and especially Ofir Gorodetsky, who made a number of careful suggestions and corrections to an earlier draft that have greatly improved the paper. I also want to thank Jordan Ellenberg, Daniel Hast, and Vlad Matei; the decomposition of Proposition 3.4 came out of discussions with them during a visit to Madison. A discussion on the website MathOverflow, available at <http://mathoverflow.net/q/233167>, was useful for

finding a reference. Part of this work was done while I was a postdoctoral fellow at the University of Zürich, and I thank that institution for its hospitality. Finally I thank the anonymous referee for a very attentive reading of the manuscript and a number of corrections and comments.

References

- [Andrade et al. 2015] J. C. Andrade, L. Bary-Soroker, and Z. Rudnick, “Shifted convolution and the Titchmarsh divisor problem over $\mathbb{F}_q[t]$ ”, *Philos. Trans. Roy. Soc. A* **373**:2040 (2015), art. id. 20140308. [MR](#) [Zbl](#)
- [Bae et al. 2015] S. Bae, B. Cha, and H. Jung, “Möbius function in short intervals for function fields”, *Finite Fields Appl.* **34** (2015), 235–249. [MR](#) [Zbl](#)
- [Bogomolny and Keating 1995] E. B. Bogomolny and J. P. Keating, “Random matrix theory and the Riemann zeros, I: Three- and four-point correlations”, *Nonlinearity* **8**:6 (1995), 1115–1131. [MR](#) [Zbl](#)
- [Bogomolny and Keating 1996] E. B. Bogomolny and J. P. Keating, “Random matrix theory and the Riemann zeros, II: n -point correlations”, *Nonlinearity* **9**:4 (1996), 911–935. [MR](#) [Zbl](#)
- [Carlitz 1932] L. Carlitz, “The arithmetic of polynomials in a Galois field”, *Amer. J. Math.* **54**:1 (1932), 39–50. [MR](#) [Zbl](#)
- [Carmon 2015] D. Carmon, “The autocorrelation of the Möbius function and Chowla’s conjecture for the rational function field in characteristic 2”, *Philos. Trans. Roy. Soc. A* **373**:2040 (2015), art. id. 20140311. [MR](#) [Zbl](#)
- [Carmon and Rudnick 2014] D. Carmon and Z. Rudnick, “The autocorrelation of the Möbius function and Chowla’s conjecture for the rational function field”, *Q. J. Math.* **65**:1 (2014), 53–61. [MR](#) [Zbl](#)
- [Church et al. 2014] T. Church, J. S. Ellenberg, and B. Farb, “Representation stability in cohomology and asymptotics for families of varieties over finite fields”, pp. 1–54 in *Algebraic topology: applications and new directions*, edited by U. Tillmann et al., *Contemp. Math.* **620**, Amer. Math. Soc., Providence, RI, 2014. [MR](#) [Zbl](#)
- [Conrey and Keating 2015a] B. Conrey and J. P. Keating, “Moments of zeta and correlations of divisor-sums, I”, *Philos. Trans. Roy. Soc. A* **373**:2040 (2015), art. id. 20140313. [MR](#) [Zbl](#)
- [Conrey and Keating 2015b] B. Conrey and J. P. Keating, “Moments of zeta and correlations of divisor-sums, II”, pp. 75–85 in *Advances in the theory of numbers*, edited by A. Alaca et al., *Fields Inst. Commun.* **77**, Fields Inst. Res. Math. Sci., Toronto, 2015. [MR](#) [Zbl](#)
- [Conrey and Keating 2015c] B. Conrey and J. P. Keating, “Moments of zeta and correlations of divisor-sums, III”, *Indag. Math. (N.S.)* **26**:5 (2015), 736–747. [MR](#) [Zbl](#)
- [Conrey and Keating 2016] B. Conrey and J. P. Keating, “Pair correlation and twin primes revisited”, *Proc. A.* **472**:2194 (2016), art. id. 20160548. [MR](#) [Zbl](#)
- [Dehaye \geq 2018] P.-O. Dehaye, “Combinatorics of lower order terms in the moments conjecture for the Riemann zeta function”, in preparation.
- [Erdős and Kac 1940] P. Erdős and M. Kac, “The Gaussian law of errors in the theory of additive number theoretic functions”, *Amer. J. Math.* **62** (1940), 738–742. [MR](#) [Zbl](#)
- [Fulton 1997] W. Fulton, *Young tableaux: with applications to representation theory and geometry*, Lond. Math. Soc. Student Texts **35**, Cambridge Univ. Press, 1997. [MR](#) [Zbl](#)
- [Fulton and Harris 1991] W. Fulton and J. Harris, *Representation theory*, Graduate Texts in Math. **129**, Springer, 1991. [MR](#) [Zbl](#)
- [Gadish 2017] N. Gadish, “A trace formula for the distribution of rational G -orbits in ramified covers, adapted to representation stability”, *New York J. Math.* **23** (2017), 987–1011. [MR](#) [Zbl](#)
- [Gamburd 2007] A. Gamburd, “Some applications of symmetric functions theory in random matrix theory”, pp. 143–170 in *Ranks of elliptic curves and random matrix theory*, edited by J. B. Conrey et al., *Lond. Math. Soc. Lecture Note Ser.* **341**, Cambridge Univ. Press, 2007. [MR](#) [Zbl](#)
- [Goldston and Montgomery 1987] D. A. Goldston and H. L. Montgomery, “Pair correlation of zeros and primes in short intervals”, pp. 183–203 in *Analytic number theory and Diophantine problems* (Stillwater, OK, 1984), edited by A. C. Adolphson et al., *Progr. Math.* **70**, Birkhäuser, Boston, 1987. [MR](#) [Zbl](#)

- [Good and Churchhouse 1968] I. J. Good and R. F. Churchhouse, “The Riemann hypothesis and pseudorandom features of the Möbius sequence”, *Math. Comp.* **22**:104 (1968), 857–861. [MR](#) [Zbl](#)
- [Hast and Matei 2016] D. Hast and V. Matei, “Higher moments of arithmetic functions in short intervals: a geometric perspective”, preprint, 2016. [arXiv](#)
- [Katz 2013] N. M. Katz, “Witt vectors and a question of Keating and Rudnick”, *Int. Math. Res. Not.* **2013**:16 (2013), 3613–3638. [MR](#) [Zbl](#)
- [Katz and Sarnak 1999] N. M. Katz and P. Sarnak, “Zeroes of zeta functions and symmetry”, *Bull. Amer. Math. Soc. (N.S.)* **36**:1 (1999), 1–26. [MR](#) [Zbl](#)
- [Keating and Rudnick 2014] J. P. Keating and Z. Rudnick, “The variance of the number of prime polynomials in short intervals and in residue classes”, *Int. Math. Res. Not.* **2014**:1 (2014), 259–288. [MR](#) [Zbl](#)
- [Keating and Rudnick 2016] J. Keating and Z. Rudnick, “Squarefree polynomials and Möbius values in short intervals and arithmetic progressions”, *Algebra Number Theory* **10**:2 (2016), 375–420. [MR](#) [Zbl](#)
- [Keating et al. 2018] J. P. Keating, B. Rodgers, E. Roditty-Gershon, and Z. Rudnick, “Sums of divisor functions in $\mathbb{F}_q[t]$ and matrix integrals”, *Math. Z.* **288**:1-2 (2018), 167–198. [MR](#) [Zbl](#)
- [Macdonald 1995] I. G. Macdonald, *Symmetric functions and Hall polynomials*, 2nd ed., Oxford Univ. Press, 1995. [MR](#) [Zbl](#)
- [Ng 2008] N. Ng, “The Möbius function in short intervals”, pp. 247–258 in *Anatomy of integers*, edited by J.-M. De Koninck et al., CRM Proc. Lecture Notes **46**, Amer. Math. Soc., Providence, RI, 2008. [MR](#) [Zbl](#)
- [Rodgers 2015] B. Rodgers, “The covariance of almost-primes in $\mathbb{F}_q[T]$ ”, *Int. Math. Res. Not.* **2015**:14 (2015), 5976–6004. [MR](#) [Zbl](#)
- [Roditty-Gershon 2017] E. Roditty-Gershon, “Square-full polynomials in short intervals and in arithmetic progressions”, *Res. Number Theory* **3** (2017), art. id. 3. [MR](#) [Zbl](#)
- [Rosen 2002] M. Rosen, *Number theory in function fields*, Graduate Texts in Math. **210**, Springer, 2002. [MR](#) [Zbl](#)
- [Rudnick 2014] Z. Rudnick, “Some problems in analytic number theory for polynomials over a finite field”, pp. 443–459 in *Proceedings of the International Congress of Mathematicians, II* (Seoul, 2014), edited by S. Y. Jang et al., Kyung Moon Sa, Seoul, 2014. [MR](#) [Zbl](#)
- [Stanley 1999] R. P. Stanley, *Enumerative combinatorics, II*, Cambridge Studies in Adv. Math. **62**, Cambridge Univ. Press, 1999. [MR](#) [Zbl](#)
- [Weil 1967] A. Weil, *Basic number theory*, Die Grundlehren der Math. Wissenschaften **144**, Springer, 1967. [MR](#) [Zbl](#)
- [Weiss 2013] B. L. Weiss, “Probabilistic Galois theory over p -adic fields”, *J. Number Theory* **133**:5 (2013), 1537–1563. [MR](#) [Zbl](#)

Communicated by Peter Sarnak

Received 2017-09-30 Revised 2018-01-29 Accepted 2018-03-18

rbrad@umich.edu

*Department of Mathematics, University of Michigan, Ann Arbor, MI,
United States*

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Richard E. Borcherds	University of California, Berkeley, USA	Martin Olsson	University of California, Berkeley, USA
Antoine Chambert-Loir	Université Paris-Diderot, France	Raman Parimala	Emory University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Jonathan Pila	University of Oxford, UK
Brian D. Conrad	Stanford University, USA	Anand Pillay	University of Notre Dame, USA
Samit Dasgupta	University of California, Santa Cruz, USA	Michael Rapoport	Universität Bonn, Germany
Hélène Esnault	Freie Universität Berlin, Germany	Victor Reiner	University of Minnesota, USA
Gavril Farkas	Humboldt Universität zu Berlin, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Joseph H. Silverman	Brown University, USA
Sergey Fomin	University of Michigan, USA	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Christopher Skinner	Princeton University, USA
Andrew Granville	Université de Montréal, Canada	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Joseph Gubeladze	San Francisco State University, USA	J. Toby Stafford	University of Michigan, USA
Roger Heath-Brown	Oxford University, UK	Pham Huu Tiep	University of Arizona, USA
Craig Huneke	University of Virginia, USA	Ravi Vakil	Stanford University, USA
Kiran S. Kedlaya	Univ. of California, San Diego, USA	Michel van den Bergh	Hasselt University, Belgium
János Kollár	Princeton University, USA	Marie-France Vignéras	Université Paris VII, France
Philippe Michel	École Polytechnique Fédérale de Lausanne	Kei-Ichi Watanabe	Nihon University, Japan
Susan Montgomery	University of Southern California, USA	Shou-Wu Zhang	Princeton University, USA
Shigefumi Mori	RIMS, Kyoto University, Japan		

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor


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

The subscription price for 2018 is US \$340/year for the electronic version, and \$535/year (+\$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

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

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2018 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 12 No. 5 2018

Semistable Chow–Hall algebras of quivers and quantized Donaldson–Thomas invariants HANS FRANZEN and MARKUS REINEKE	1001
Certain abelian varieties bad at only one prime ARMAND BRUMER and KENNETH KRAMER	1027
Characterization of Kollár surfaces GIANCARLO URZÚA and JOSÉ IGNACIO YÁÑEZ	1073
Représentations de réduction unipotente pour $SO(2n + 1)$, III: Exemples de fronts d’onde JEAN-LOUP WALDSPURGER	1107
Correspondences without a core RAJU KRISHNAMOORTHY	1173
Local topological algebraicity with algebraic coefficients of analytic sets or functions GUILLAUME ROND	1215
Polynomial bound for the nilpotency index of finitely generated nil algebras MÁTYÁS DOMOKOS	1233
Arithmetic functions in short intervals and the symmetric group BRAD RODGERS	1243
Cohomology for Drinfeld doubles of some infinitesimal group schemes ERIC M. FRIEDLANDER and CRIS NEGRON	1281