Math. Proc. Camb. Phil. Soc. (2025), **179**, 785–819
doi:10.1017/S0305004125101321
First published online 8 August 2025

Moments of random multiplicative functions over function fields

BY MAXIMILIAN C. E. HOFMANN
Department of Mathematics, Stony Brook University, Stony Brook, NY 11794-3651*, U.S.A.*
e-mail: maximilian.hofmann@stonybrook.edu

ANNEMILY HOGANSON
Department of Mathematics, University of Wisconsin-Madison, Madison, WI 53706*, U.S.A.*
e-mail: aghoganson@wisc.edu

SIDDARTH MENON
*Department of Pure Mathematics and Mathematical Statistics, Centre for Mathematical Sciences, University of Cambridge, Cambridge, CB*3 0*WB.*
e-mail: sm2884@cam.ac.uk

WILLIAM VERREAULT AND ASIF ZAMAN
Department of Mathematics, University of Toronto, ON, M5S 2E4*, Canada.*
e-mails: william.verreault@utoronto.ca, asif.zaman@utoronto.ca

(*Received* 09 *September* 2024*; revised* 04 *April* 2025*; accepted* 15 *April* 2025)

Abstract

Granville–Soundararajan, Harper–Nikeghbali–Radziwiłł and Heap–Lindqvist independently established an asymptotic for the even natural moments of partial sums of random multiplicative functions defined over integers. Building on these works, we study the even natural moments of partial sums of Steinhaus random multiplicative functions defined over function fields. Using a combination of analytic arguments and combinatorial arguments, we obtain asymptotic expressions for all the even natural moments in the large field limit and large degree limit, as well as an exact expression for the fourth moment.

2020 Mathematics Subject Classification: 11K65, 11T55 (Primary)

1. *Introduction*

1.1. Background

Let $(f(p))_{p \text{ prime}}$ be a sequence of independent random variables which are uniformly distributed on the complex unit circle. Define $f\colon \mathbb{N} \to \mathbb{C}$ by $f(1) = 1$ and

$$f(n) = f(p_1)^{\alpha_1} \cdots f(p_r)^{\alpha_r},$$

where $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ for distinct primes $p_1, \dots, p_r$ and positive integers $\alpha_1, \dots, \alpha_r$. The function f is a *Steinhaus random multiplicative function* (over the integers $\mathbb{Z}$). Random

© The Author(s), 2025. Published by Cambridge University Press on behalf of Cambridge Philosophical Society.

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

multiplicative functions were first introduced by Wintner [**Win44**] in 1944 as a probabilistic model for the Möbius function in multiplicative number theory. The Steinhaus example is inspired by archimedean characters $n \mapsto n^{it}$ for randomly chosen large values of t, as well as by non-archimedean characters $n \mapsto \chi(n)$ for randomly chosen Dirichlet characters χ modulo q for large prime moduli q (see [**GS01**, section 2] for a related discussion).

For fixed $x \geq 2$, the random variable

$$\sum_{n \leq x} f(n) \tag{1·1}$$

and related subsums have generated substantial interest over the past decade. For a (non-exhaustive) list of examples, see [**BS16**], [**Cai23**], [**CS12**], [**GW24**], [**GW25**], [**Har13**],[**Har19**], [**Har20**], [**Har23**], [**Har24a**], [**Har24b**], [**HL16**], [**HNR15**], [**Hou11**], [**KSX23**], [**LTW13**], [**Mas22**], [**PWX24**], [**SX23**], and [**Xu24**]. While the distribution of (1·1) remains open (see Gorodetsky–Wong [**GW24**] for a recent conjecture), there has been significant progress to describe its moments. Granville–Soundararajan [**GS01**] first gave upper and lower bounds for even natural moments of (1·1). About 15 years later, Granville–Soundararajan (unpublished), Harper–Nikeghbali–Radziwiłł [**HNR15**], and Heap–Lindqvist [**HL16**] independently proved that for $k \in \mathbb{N}$ and $x \geq 3$,

$$\mathbb{E}\Big|\sum_{n \leq x} f(n)\Big|^{2k} = \binom{2k-2}{k-1} c_k \cdot k^{-(k-1)} \mathrm{vol}(\mathcal{B}_k) x^k (\log x)^{(k-1)^2} \Big(1 + O_k\Big(\frac{1}{\log\log x}\Big)\Big), \tag{1·2}$$

where $\mathrm{vol}(\mathcal{B}_k)$ is the volume of the kth Birkhoff polytope, and

$$c_k = \prod_p \Big(1 - \frac{1}{p}\Big)^{k^2} \Big(\sum_{m=0}^{\infty} \binom{m+k-1}{k-1}^2 \frac{1}{p^m}\Big). \tag{1·3}$$

About 10 years prior to this, Conrey–Gamburd [**CG06**] established essentially the same estimate as (1·2) in the equivalent context of integral moments of partial sums of the Riemann ζ-function along the critical line. Morever, the special case $k = 2$ was studied earlier by Ayyad–Cochrane–Zheng [**ACZ96**] and improved by Shi [**Shi08**] who showed that

$$\mathbb{E}\Big|\sum_{n \leq x} f(n)\Big|^4 = \frac{12}{\pi^2} x^2 \log x + cx^2 + O_\varepsilon(x^{547/416+\varepsilon}) \tag{1·4}$$

for $\varepsilon > 0$, where $c = 0.511\ldots$ is an explicit positive constant. Recently, Harper [**Har19**, **Har20**] determined the order of magnitude of $\mathbb{E}|\sum_{n \leq x} f(n)|^{2k}$ for all real numbers $k \geq 0$.

Our interest lies with random multiplicative functions in the *function field setting*, namely the polynomial ring $\mathbb{F}_q[t]$ where $q \geq 2$ is a prime power and $\mathbb{F}_q$ is the finite field with q elements. For an introduction to multiplicative functions over $\mathbb{F}_q[t]$, see Granville–Harper–Soundararajan [**GHS15**] for example. Before presenting our results, we define some notation. Let $\mathcal{M}$ denote the set of all monic polynomials in $\mathbb{F}_q[t]$. Let $\mathcal{M}_N \subseteq \mathcal{M}$ denote the set of monic polynomials of degree exactly N, so $|\mathcal{M}_N| = q^N$. Let $(f(P))_P$ be a sequence of independent random variables indexed by the monic irreducible polynomials P of $\mathbb{F}_q[t]$ and uniformly distributed on the complex unit circle. Define $f\colon \mathcal{M} \to \mathbb{C}$ by $f(1) = 1$ and

$$f(F) = f(P_1)^{\alpha_1} \cdots f(P_r)^{\alpha_r}$$

for $F \in \mathcal{M}$, where $F = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ for distinct monic irreducible polynomials $P_1, \ldots, P_r$ and positive integers $\alpha_1, \ldots, \alpha_r$. The function f is a *Steinhaus random multiplicative function*

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

over the ring $\mathbb{F}_q[t]$. For integers $N \geq 1$, the random variable

$$\sum_{F \in \mathcal{M}_N} f(F) \tag{1·5}$$

is the function field analogue of (1·1). Building on work of Harper [**Har13**] over the integers, Aggarwal–Subedi–Verreault–Zaman–Zheng [**ASV+22**] established a central limit theorem for a variant of (1·5) with few irreducible factors. Otherwise, much less is known about (1·5).

1.2. Results

The purpose of this paper is to obtain asymptotics for the even natural moments of (1·5). Our main result establishes such an estimate as $q^N \to \infty$.

THEOREM 1·1. *Fix $k \in \mathbb{N}$. For any prime power $q \geq 2$ and any integer $N \geq 1$, if f is a Steinhaus random multiplicative function defined over $\mathbb{F}_q[t]$, then*

$$\mathbb{E}\Big|\sum_{F \in \mathcal{M}_N} f(F)\Big|^{2k} = b_k(q)\mathcal{S}_k(N)q^{kN}\left(1 + O_k\left(\frac{(\log N)^k}{qN^{\frac{1}{2}-\frac{3k-2}{4k^2-2k}}}\right)\right), \tag{1·6}$$

where $\mathcal{S}_k(N)$ is the number of $k \times k$ magic squares with magic constant N, and

$$b_k(q) = \prod_{\substack{P \in \mathcal{M} \\ \text{irred.}}}\Big(1 - \frac{1}{q^{\deg P}}\Big)^{k^2}\Big(\sum_{m=0}^{\infty}\binom{m+k-1}{k-1}^2\frac{1}{q^{m \deg P}}\Big). \tag{1·7}$$

Remark. A $k \times k$ magic square with magic constant N is a $k \times k$ matrix with nonnegative integer entries where every row sum and column sum is equal to N. For fixed k, it is a consequence of Ehrhart's theorem [**Ehr77**] that as $N \to \infty$,

$$\mathcal{S}_k(N) = k^{-(k-1)}\mathrm{vol}(\mathcal{B}_k)N^{(k-1)^2}(1 + o(1)). \tag{1·8}$$

The proof of Theorem 1·1 in Section 6 mostly follows the analytic approach of [**HNR15**] and especially [**HL16**] with some novelties, so we shall provide a brief comparison with (1·2). First, the asymptotic of Theorem 1·1 over $\mathbb{F}_q[t]$ and the asymptotic (1·2) over $\mathbb{Z}$ possess similar main terms. Recall the number of integers $n \leq x$ is equal to $\lfloor x \rfloor$, and the number of polynomials $F \in \mathcal{M}_N$ is equal to q^N. By replacing x in (1·2) by q^N and utilizing (1·8), one recovers the same growth rate. Moreover, the arithmetic constants (1·3) and (1·7) have the same structure.

Second, the error term of Theorem 1·1 over $\mathbb{F}_q[t]$ is comparably stronger than (1·2) over $\mathbb{Z}$. Replacing x with q^N again, one might likewise expect the $\log\log x$ factor in (1·2) to become a factor of $\log N$ in the function field setting, but our error term decays by a power of N. These gains are primarily due to a more delicate technical analysis of various oscillatory integrals, and might lead to similar gains in the integer setting.

Third, Theorem 1·1 has complete uniformity in both the q-limit and N-limit. Our adaptation of the analytic approach due to [**HNR15**, **HL16**] handles the case $q^N \to \infty$ provided $N \geq 20$. With more effort, a modified analytic approach might allow for all values of N. Instead, for $N \geq 1$ fixed and $q \to \infty$, we applied a combinatorial approach to prove this special case of Theorem 1·1. We state this theorem separately for the sake of clarity.

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

THEOREM 1·2. *Fix $k, N \in \mathbb{N}$. For any prime power $q \geq 2$, if f is a Steinhaus random multiplicative function defined over $\mathbb{F}_q[t]$, then*

$$\mathbb{E}\left|\sum_{F \in \mathcal{M}_N} f(F)\right|^{2k} = \mathcal{S}_k(N) q^{kN}\left(1 + O_{k,N}\left(\frac{1}{q}\right)\right).$$

Remark. The main term matches (1·6) since $b_k(q) = 1 + O_k(q^{-1})$.

The proof of Theorem 1·2 in Section 4 adapts the GCD matrix construction first introduced by Vaughan–Wooley [**VW95**] and used by Granville–Soundararajan [**GS01**] for moments in the integer setting. Gorodetsky [**Gor24**, section 5·1] outlined this strategy to establish an asymptotic for moments in the function field setting as $q \to \infty$. Our proof follows his outline.

By specializing the analytic (Theorem 1·1) and combinatorial (Theorem 1·2) approaches to the case $k = 2$, we provide two proofs of an exact formula for the fourth moment.

THEOREM 1·3. *For any prime power $q \geq 2$ and integer $N \geq 1$, if f is a Steinhaus random multiplicative function defined over $\mathbb{F}_q[t]$, then*

$$\mathbb{E}\left|\sum_{F \in \mathcal{M}_N} f(F)\right|^{4} = Nq^{2N}\left(1 - \frac{1}{q}\right) + q^{2N}.$$

These two short proofs appear in Sections 3 and 5. In addition to establishing Theorem 1·3, they also have the advantage of outlining the key steps leading to Theorems 1·1 and 1·2 in a simple case. This exact formula in the function field setting can be compared with the asymptotic (1·4) in the integer setting.

1.3. Organisation

Section 2 outlines notation, prepares the starting point for all of our main proofs, and includes some discussion of our methods compared to the proof of (1·2). Sections 3 and 5 respectively contain the combinatorial proof and the analytic proof of the 4th moment formula in Theorem 1·3. These expositions also serve as simplified introductions for the general case with each approach. Section 4 generalises the combinatorial approach to all $2k$th moments in the q-limit and proves Theorem 1·2.

The rest of the paper (Sections 6 to 10) is dedicated to the proof of Theorem 1·1 for all $2k$th moments via an analytic approach. Section 6 proves Theorem 1·1 assuming several key propositions and proceeding with the strategy of Section 5 for $k = 2$. The key propositions are postponed to the subsequent sections. Section 7 establishes analytic theory for the relevant multivariable generating function and its convergence (Proposition 6·1). Section 8 rewrites the $2k$th moment as an integral in terms of this generating function and performs a convenient change of variables (Proposition 6·2). Section 9 extracts the main contribution from this integral and expresses its value in terms of the number of magic squares (Proposition 6·3). Section 10 handles the remaining error term integral by carefully subdividing the region of integration to control the fluctuations in the integrand (Proposition 6·4). The bulk of the contribution comes from a high peak on a narrow region, so this analysis is fairly delicate.

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

2. *Preliminaries*

2.1. Notation

For the sake of clarity, we fix some standard notation and conventions. This repeats some discussion from the introduction. Let $q \geq 2$ be a prime power, and let $\mathbb{F}_q[t]$ be the polynomial ring over the finite field $\mathbb{F}_q$ with q elements. Let $\mathcal{M}$ denote the set of all monic polynomials in $\mathbb{F}_q[t]$ and let $\mathcal{M}_N \subseteq \mathcal{M}$ be the subset of degree N polynomials, so $|\mathcal{M}_N| = q^N$. The letters F and G will always denote monic polynomials, and the letters P and Q will always denote monic irreducible polynomials. The zeta function ζ_q for function fields is defined as

$$\zeta_q(z) = \sum_{N=0}^{\infty} |\mathcal{M}_N| z^N = \prod_P \left(1 - z^{\deg P}\right)^{-1} = \frac{1}{1-qz},$$

where products over P will always run over all irreducible monic polynomials.

A magic square of size k with magic constant N is a $k \times k$ matrix whose entries are nonnegative integers such that the entries of each row and column sum to N. The number of such matrices will be denoted by $\mathcal{S}_k(N)$.

For variables a and b, we write $a \ll b$ or $a = O(b)$ to say that there exists an absolute positive constant C such that $|a| \leq Cb$. If the constant C depends on a parameter, say k, we shall write $a \ll_k b$ or $a = O_k(b)$. If a and b depend on a positive parameter x, then we say that $a = o(b)$ as $x \to \infty$ if the ratio a/b converges to 0 as $x \to \infty$.

Sums of the form

$$\sum_{m_1+\cdots+m_k=m_{k+1}+\cdots+m_{2k}} \cdots \sum$$

will be taken over *non-negative* integers $m_1, \ldots, m_{2k} \geq 0$.

2.2. Setup

For the entirety of the paper, let $f\colon \mathcal{M} \to \mathbb{C}$ be a Steinhaus random multiplicative function over $\mathbb{F}_q[t]$. Our goal is to calculate the $2k$th moments of (1·5) for integers k. All of our proofs begin by reducing to a natural counting problem. By complete multiplicativity and independence of f on distinct irreducibles P, it follows for any $F, G \in \mathcal{M}$ that

$$\mathbb{E}[f(F)\overline{f(G)}] = \mathbb{1}_{\{F=G\}},$$

where $\mathbb{1}_{\mathcal{A}}$ denotes the indicator function of a set $\mathcal{A}$. For the case $k = 1$, this implies that

$$\mathbb{E}\left|\sum_{F \in \mathcal{M}_N} f(F)\right|^2 = \sum_{F,G \in \mathcal{M}_N} \sum \mathbb{E}[f(F)\overline{f(G)}] = \sum_{F,G \in \mathcal{M}_N} \sum \mathbb{1}_{\{F=G\}} = |\mathcal{M}_N| = q^N.$$

Similarly, the $2k$th moments are given by

$$\sum_{F_1,\ldots,F_{2k} \in \mathcal{M}_N} \cdots \sum \mathbb{E}[f(F_1)\ldots f(F_k)\overline{f(F_{k+1})\ldots f(F_{2k})}] = \sum_{F_1,\ldots,F_{2k} \in \mathcal{M}_N} \cdots \sum \mathbb{1}_{\{F_1\ldots F_k = F_{k+1}\ldots F_{2k}\}},$$

leading to the key initial identity:

$$\mathbb{E}\left|\sum_{F \in \mathcal{M}_N} f(F)\right|^{2k} = \#\left\{(F_1, \ldots, F_{2k}) \in \mathcal{M}_N^{2k} \;\middle|\; F_1F_2\cdots F_k = F_{k+1}F_{k+2}\cdots F_{2k}\right\}. \tag{2·1}$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

2.3. Remarks on the integer setting

The moment problem over the integers can be reduced to a counting problem similar to (2·1). More precisely, the left-hand side of (1·2) is equal to

$$\#\Big\{(n_1,\dots,n_{2k})\in\{1,2,\dots,\lfloor x\rfloor\}^{2k}\;\Big|\; n_1\cdots n_k=n_{k+1}\cdots n_{2k}\Big\}. \tag{2·2}$$

Estimating this quantity takes several approaches in the literature. Granville–Soundararajan [**GS01**] give upper and lower bounds for (2·2) via their GCD matrix construction. Our proof of Theorem 1·2 applies this method over $\mathbb{F}_q[t]$ to produce an asymptotic in the q-limit; see also Section 3 for the case $k=2$.

Harper–Nikeghbali–Radziwiłł [**HNR15**] and Heap–Lindqvist [**HL16**] count (2·2) using the analytic theory of multivariable Dirichlet series. They enforce the condition $1\le n_i\le N$ with a suitable bump function, which is written as $2k$ line integrals via Mellin inversion. This essentially rewrites (2·2) as an iterated integral over the multivariable Dirichlet series

$$\sum_{\substack{n_1,n_2,\dots,n_{2k}\\ n_1\cdots n_k=n_{k+1}\cdots n_{2k}}}\cdots\sum \frac{1}{n_1^{s_1}\cdots n_{2k}^{s_{2k}}}. \tag{2·3}$$

By expressing this Dirichlet series as a product of Riemann zeta functions and an Euler product with an expanded region of absolute convergence, they can extract the integral's asymptotic size. Roughly speaking, after a change of variables of the form $s_j\mapsto 1/2+it_j$, they show that the main contribution is concentrated when $t_j\in\mathbb{R}$ is very small for many j. This truncation requires a careful case analysis by subdviding the remaining large region of integration, where the complicated integrand decays rapidly as t_j grows for some fixed j.

Our proof of Theorem 1·1 in Section 6 adapts this strategy to the function field setting. The multivariable Dirichlet series (2·3) over the integers corresponds to a multivariable power series (6·1) over $\mathbb{F}_q[t]$. As established in Section 7, this power series will also factor as a product of zeta functions and another series with expanded radius of convergence. By construction, the quantity (2·1) is a specific coefficient of our multivariable power series, expressed as an iterated integral via Cauchy's integral formula. The case $k=2$ for Theorem 1·3 yields a sufficiently simple series factorisation and integral expression, which we compute directly in Section 5. For $k\ge 3$, we parameterise the resulting integrals, and perform a truncation like Heap–Lindqvist. After an analogous change of variables in Section 8, the main contribution near the origin is extracted in Section 9. The proof concludes in Section 10 with a technical analysis of the integral over the complement of the truncated region.

3. *Fourth moment computation using a combinatorial approach*

We provide a short proof of Theorem 1·3 by counting coprime pairs of monic polynomials of fixed degree. We require the following lemma.

LEMMA 3·1 ([**CSWZ98**, proposition 3]). *The number of coprime pairs of monic polynomials of degree exactly $N\ge 1$ over $\mathbb{F}_q[t]$ is $q^{2N}-q^{2N-1}$.*

Proof of Theorem 1·3. By (2·1), the fourth moment is given by

$$\sum_{\substack{F_1,F_2,G_1,G_2\in\mathcal{M}_N\\ F_1F_2=G_1G_2}}\sum\sum\sum 1.$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

We note that $F_1F_2 = G_1G_2$ if and only if

$$\frac{F_1}{(F_1,G_2)}\frac{F_2}{(F_2,G_1)} = \frac{G_1}{(F_2,G_1)}\frac{G_2}{(F_1,G_2)},$$

where (F,G) denotes the GCD of F and G, which is equivalent to

$$\frac{F_1}{(F_1,G_2)} = \frac{G_1}{(F_2,G_1)} \text{ and } \frac{F_2}{(F_2,G_1)} = \frac{G_2}{(F_1,G_2)}.$$

Letting $A := F_1/(F_1,G_2)$ and $B := G_2/(F_1,G_2)$, we observe that A and B can be any monic, coprime polynomials such that

$$\deg A = \deg B = N - \deg(F_1,G_2) = N - \deg(F_2,G_1),$$

while (F_1,G_2) and (F_2,G_1) can be any monic polynomials of degree $N - \deg A = N - \deg B$. Thus, counting the possible values of (F_1,G_2) and (F_2,G_1) for each possible value of A and B, we have

$$\begin{aligned}\sum_{\substack{F_1,F_2,G_1,G_2\in\mathcal{M}_N\\ F_1F_2=G_1G_2}}\sum\sum\sum 1 &= \sum_{\substack{(A,B)=1\\ \deg A=\deg B\le N}}\sum\sum \left(\sum_{F\in\mathcal{M}_{N-\deg A}} 1\right)^2\\ &= \sum_{\substack{(A,B)=1\\ \deg A=\deg B\le N}}\sum\sum \left(q^{N-\deg A}\right)^2\\ &= \sum_{m=0}^{N} q^{2(N-m)} \sum_{\substack{(A,B)=1\\ \deg A=\deg B=m}}\sum\sum 1\\ &= Nq^{2N}\left(1-\frac{1}{q}\right)+q^{2N},\end{aligned}$$

where the last line follows from Lemma 3·1.

4. *Combinatorial method in the large q limit: proof of Theorem 1·2*

This section is dedicated to the proof of Theorem 1·2 by generalising the combinatorial approach of Section 3. As in the $k = 2$ case, we can divide the equation

$$F_1 \cdots F_k = G_1 \cdots G_k$$

by certain greatest common divisors to reduce the problem of computing the $2k$th moment to a problem of counting sets of polynomials with certain coprimality conditions. For $k > 2$, these coprimality conditions are more complex and, to the best of our knowledge, there are no known exact formulas for counting the number of polynomials satisfying these conditions. For simplicity, rather than describing equivalent conditions to $F_1 \cdots F_k = G_1 \cdots G_k$, we define an injection from

$$\{(F_1,\dots,F_k,G_1,\dots,G_k)\in\mathcal{M}_N^{2k} \mid F_1\cdots F_k = G_1\cdots G_k\} \tag{4·1}$$

to $\mathcal{M}^{k^2}$ and then apply simple bounds to the image of (4·1).

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

We first present the argument for $k = 3$ as an example that will illustrate the general case. We consider

$$F_1\, F_2\, F_3 = G_1\, G_2\, G_3,$$

where $F_i, G_i \in \mathcal{M}_N$. Due to the additional factor compared to the $k = 2$ case, we will require multiple recursive steps to decompose the products. We begin by letting

$$\begin{aligned} A_{12} &= (F_1, G_2) \\ A_{23} &= (F_2, G_3) \\ A_{31} &= (F_3, G_1). \end{aligned}$$

Here the indices are determined by the permutation $\sigma = (1\,2\,3)$, so that $A_{i\sigma(i)} = (F_i, G_{\sigma(i)})$. For the next set of GCDs, we repeat this shift in the indices by letting

$$A_{i\,\sigma^2(i)} = \left(\frac{F_i}{A_{i\,\sigma(i)}}, \frac{G_{\sigma^2(i)}}{A_{\sigma(i)\,\sigma^2(i)}} \right),$$

so that

$$\begin{aligned} A_{13} &= \left(\frac{F_1}{A_{12}}, \frac{G_3}{A_{23}} \right), \\ A_{21} &= \left(\frac{F_2}{A_{23}}, \frac{G_1}{A_{31}} \right), \\ A_{32} &= \left(\frac{F_3}{A_{31}}, \frac{G_2}{A_{12}} \right). \end{aligned}$$

Repeating the shifts a third time, we have

$$A_{i\sigma(i)^3} = A_{ii} = \frac{F_i}{A_{i\sigma(i)} A_{i\sigma^2(i)}} = \frac{G_i}{A_{\sigma^{-1}(i)i} A_{\sigma^{-2}(i)i}},$$

with the last equality following from the fact that for $i \neq j$,

$$\left(\frac{F_i}{A_{i\sigma(i)} A_{i\sigma^2(i)}}, \frac{G_j}{A_{\sigma^{-1}(j)j} A_{\sigma^{-2}(j)j}} \right) = 1.$$

We then have that

$$F_i = A_{i\sigma(i)} A_{i\sigma^2(i)} A_{ii} \qquad \text{and} \qquad G_j = A_{\sigma^{-1}(j)j} A_{\sigma^{-2}(j)j} A_{jj}.$$

Thus, we have mapped $(F_1, F_2, F_3, G_1, G_2, G_3)$ to a unique matrix

$$\begin{bmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix}$$

in which the product of the entries in row i is F_i and the product of the entries in column j is G_j. We will call this matrix the *GCD matrix* of $(F_1, F_2, F_3, G_1, G_2, G_3)$.

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

Now, letting $\deg A_{ij} = a_{ij}$, we note that the matrix containing the degrees of the polynomials in the GCD matrix,

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix},$$

is a magic square since row i must sum to $\deg F_i = N$ and column j must sum to $\deg G_j = N$. We will call this the *GCD degree matrix* of $(F_1, F_2, F_3, G_1, G_2, G_3)$.

For S a magic square of size 3 for the number N, we let $R(S)$ count the number of tuples in

$$\{(F_1, F_2, F_3, G_1, G_2, G_3) \in \mathcal{M}_N^6 \mid F_1F_2F_3 = G_1G_2G_3\}$$

with GCD degree matrix given by S. We then have that

$$\mathbb{E}\Big|\sum_{F\in\mathcal{M}_N} f(F)\Big|^6 = \sum_S R(S),$$

where the sum is taken over all magic squares of size 3 for the number N. We would now like to bound $R(S)$. We first note that $R(S)$ is bounded above by the total number of 3×3 matrices with entries in $\mathcal{M}$ and with the degrees of the entries given by S. Thus $R(S) \le q^{a_{11}+a_{12}+\cdots+a_{32}+a_{33}} = q^{3N}$. To bound $R(S)$ from below, we consider a 3×3 matrix with entries A_{ij} in $\mathcal{M}$ such that the entries are pairwise coprime and the degrees of the entries are given by S. We have that $(A_{i1}A_{i2}A_{i3},\ A_{1j}A_{2j}A_{3j}) = A_{ij}$, so this matrix is the GCD matrix of $(F_1, F_2, F_3, G_1, G_2, G_3)$, where

$$F_i = A_{i1}A_{i2}A_{i3}$$

and

$$G_j = A_{1j}A_{2j}A_{3j}.$$

It follows that $R(S)$ is bounded below by the number of pairwise coprime monic polynomials with degrees equal to the entries of S.

Before establishing an asymptotic for this lower bound, we return for the moment to the general case. For $k \ge 3$, given $\sigma = (1\ 2\ \ldots\ k)$ and $s \le k$, we let

$$A_{i\,\sigma^s(i)} = \Big(\frac{F_i}{\prod_{r<s} A_{i\,\sigma^r(i)}}, \frac{G_{\sigma^s(i)}}{\prod_{r<s} A_{\sigma^{-r}(i)\,\sigma^s(i)}}\Big).$$

As we saw for $k = 3$, we have

$$A_{ii} = A_{i\sigma^k(i)} = \frac{F_i}{\prod_{r<k} A_{i\,\sigma^r(i)}} = \frac{G_i}{\prod_{r<k} A_{\sigma^{-r}(i)\,i}},$$

meaning that

$$F_i = \prod_{h=1}^{k} A_{ih} \qquad \text{and} \qquad G_j = \prod_{h=1}^{k} A_{hj}.$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

In this way, we map $(F_1, \dots, F_k, G_1, \dots, G_k)$ to the GCD matrix

$$\begin{bmatrix} A_{11} & \cdots & A_{1k} \\ \vdots & \ddots & \vdots \\ A_{k1} & \cdots & A_{kk} \end{bmatrix}$$

in which the product of the entries in row i is F_i and the product of the entries in column j is G_j. Letting $\deg A_{ij} = a_{ij}$, we note again that the GCD degree matrix

$$\begin{bmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{k1} & \cdots & a_{kk} \end{bmatrix}$$

is a magic square. We remark that a similar GCD matrix construction was explored by Granville and Soundararajan in [**GS01**] in their study of $2k$th moments in the integer setting.

For S a magic square of size k for the number N, let $R(S)$ count the number of tuples in

$$\{(F_1, \dots, F_k, G_1, \dots, G_k) \in \mathcal{M}_N^{2k} \mid F_1 \cdots F_k = G_1 \cdots G_k\}$$

with GCD degree matrix S, so that

$$\mathbb{E}\Big| \sum_{F \in \mathcal{M}_N} f(F) \Big|^{2k} = \sum_S R(S).$$

As before, the sum is taken over all magic squares of size k for the number N. We observe that $R(S)$ is bounded above by the total number of $k \times k$ matrices with entries in $\mathcal{M}$ and with the degrees of the entries given by S. Thus $R(S) \le q^{\sum_{i=1}^k \sum_{j=1}^k a_{ij}} = q^{kN}$. To bound $R(S)$ from below, we consider a $k \times k$ matrix with pairwise coprime entries A_{ij} in $\mathcal{M}$ such that the degrees of the entries are given by S. We have that

$$\Big(\prod_{h=1}^k A_{ih}, \prod_{h=1}^k A_{hj} \Big) = A_{ij},$$

so this matrix is the GCD matrix of $(F_1, \dots, F_k, G_1, \dots, G_k)$, where

$$F_i = \prod_{h=1}^k A_{ih} \qquad \text{and} \qquad G_j = \prod_{h=1}^k A_{hj}.$$

It follows that $R(S)$ is bounded below by the number of pairwise coprime monic polynomials with degrees equal to the entries of S.

To obtain the q-limit asymptotic and complete the proof of Theorem 1·2, we will need the following result on the number of pairwise coprime polynomials of fixed degrees.

LEMMA 4·1 ([**HJL16**, corollary 3]). *For $(d_1, \dots, d_s) \in \mathbb{N}^s$, the number of monic pairwise coprime polynomials $f_i \in \mathbb{F}_q[t]$ with $\deg(f_i) = d_i$ for $i = 1, \dots, s$ is*

$$q^{d_1 + \cdots + d_s} \left(1 - \frac{s(s-1)}{2} \cdot \frac{1}{q} + O_{s, d_1, \dots, d_s}\left(\frac{1}{q^2} \right) \right).$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

Applying Lemma 4·1 to our lower bound for $R(S)$, we see that

$$R(S) \geq q^{kN}\left(1 - \frac{k^2(k^2-1)}{2} \cdot \frac{1}{q} + O_{k,N}\left(\frac{1}{q^2}\right)\right).$$

Thus $R(S) = q^{kN}\big(1 + O_{k,N}(q^{-1})\big)$, and Theorem 1·2 follows.

5. *Fourth moment using an analytic approach*

We provide another proof of Theorem 1·3 by studying a power series in 4 variables indexed over all 4-tuples of monic polynomials:

$$A(z_1, z_2, z_3, z_4) := \sum_{F_1,\ldots,F_4 \in \mathcal{M}} \sum \sum \sum \mathbb{1}_{\{F_1F_2 = F_3F_4\}} z_1^{\deg F_1} \cdots z_4^{\deg F_4}. \tag{5·1}$$

We will check at the beginning of Section 6 in a more general case that A converges uniformly on compact subsets of $\{(z_1, z_2, z_3, z_4) \in \mathbb{C}^4 : |z_i| < 1/q \text{ for } 1 \leq i \leq 4\}$. By (2·1), calculating the fourth moment $\mathbb{E}|\sum_{F \in \mathcal{M}_N} f(F)|^4$ amounts to computing the coefficient of $z_1^N \cdots z_4^N$ in the above power series.

Observing that the indicator function $\mathbb{1}_{\{F_1F_2=F_3F_4\}}$ is multiplicative (see the Section 6 footnote for a definition of multiplicative), we find that

$$A(z_1, z_2, z_3, z_4) = \prod_P \left(\sum \sum \sum \sum_{m_1+m_2=m_3+m_4} (z_1^{m_1} z_2^{m_2} z_3^{m_3} z_4^{m_4})^{\deg P}\right). \tag{5·2}$$

The product runs over all irreducible monic polynomials and the internal sum iterates over the possible ways to distribute a given irreducible factor P among $F_1, \ldots, F_4$ such that the number of factors of P in F_1F_2 and F_3F_4 are equal. As in [**HL16**], we factor this product as

$$A(z_1, \ldots, z_4) = B(z_1, \ldots, z_4) \prod_{i=1}^{2} \prod_{j=3}^{4} \zeta_q(z_i z_j). \tag{5·3}$$

Here, B is defined implicitly by (5·3), namely

$$B(z_1, z_2, z_3, z_4) = \prod_P \left(\sum \sum \sum \sum_{m_1+m_2=m_3+m_4} \left(z_1^{m_1} z_2^{m_2} z_3^{m_3} z_4^{m_4}\right)^{\deg P}\right) \prod_{i=1}^{2} \prod_{j=3}^{4} \left(1 - (z_i z_j)^{\deg P}\right). \tag{5·4}$$

We note that absolute and uniform convergence of this expression for $|z_i| < 1.1/\sqrt{q}$ will follow by applying Proposition 6·1, which we prove in Section 7, for $k = 2$.

Recall that by the multivariate version of Cauchy's integral formula, obtaining the desired coefficient of A can be done by computing

$$\begin{aligned} &\frac{1}{(2\pi i)^4} \int_{|z_4|=\varepsilon_4} \cdots \int_{|z_1|=\varepsilon_1} \frac{A(z_1, \ldots, z_4)}{z_1^{N+1} \cdots z_4^{N+1}} dz_1 \cdots dz_4 \\ &= \frac{1}{(2\pi i)^4} \int_{|z_4|=\varepsilon_4} \cdots \int_{|z_1|=\varepsilon_1} \frac{B(z_1, \ldots, z_4) \prod_{i=1}^{2} \prod_{j=3}^{4} \zeta_q(z_i z_j)}{z_1^{N+1} \cdots z_4^{N+1}} dz_1 \cdots dz_4, \end{aligned}$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

where we integrate over a polydisc with small radii $0 < \varepsilon_i < q^{-1}$ around the origin. We proceed to find a simple formula for (5·4) which will enable us to explicitly compute the above integral. To do so, we study the local factors of the B-term in the following lemma.

LEMMA 5·1. *If $|z_i z_j| < 1$ for $i \in \{1,2\}$ and $j \in \{3,4\}$, then the following identity holds*:

$$\Big(\sum_{m_1+m_2=m_3+m_4}\sum\sum\sum z_1^{m_1} z_2^{m_2} z_3^{m_3} z_4^{m_4}\Big)\prod_{i=1}^{2}\prod_{j=3}^{4}(1-z_i z_j) = 1 - z_1 z_2 z_3 z_4.$$

Proof. Note that if $|z_i z_j| < 1$ for $i \in \{1,2\}$ and $j \in \{3,4\}$, then

$$\prod_{i=1}^{2}\prod_{j=3}^{4}\frac{1}{1-z_i z_j} = \sum_{k_{13},k_{14},k_{23},k_{24}\geq 0}\sum\sum\sum z_1^{k_{13}+k_{14}} z_2^{k_{23}+k_{24}} z_3^{k_{13}+k_{23}} z_4^{k_{14}+k_{24}}. \tag{5·5}$$

We can thus write the product of (5·5) times $z_1 z_2 z_3 z_4$ as

$$\sum_{k_{13},k_{14},k_{23},k_{24}\geq 0}\sum\sum\sum z_1^{(k_{13}+1)+k_{14}} z_2^{k_{23}+(k_{24}+1)} z_3^{(k_{13}+1)+k_{23}} z_4^{k_{14}+(k_{24}+1)}. \tag{5·6}$$

Subtracting this from (5·5) amounts to multiplying (5·5) by $(1 - z_1 z_2 z_3 z_4)$. Now, notice that the monomial in (5·6) associated to the index $(k_{13}-1, k_{14}, k_{23}, k_{24}-1)$ can be paired with the monomial associated to the index $(k_{13}, k_{14}, k_{23}, k_{24})$ in (5·5) to cancel each other out. This way of pairing terms is not unique, but with this choice the only remaining terms come from monomials in (5·5) where either $k_{13} = 0$ or $k_{24} = 0$.

Now, it suffices to show that given a tuple (m_1, m_2, m_3, m_4) such that

$$m_1 + m_2 = m_3 + m_4,$$

there is a unique tuple $(k_{13}, k_{14}, k_{23}, k_{24})$ with either $k_{13} = 0$ or $k_{24} = 0$ such that

$$(m_1, m_2, m_3, m_4) = (k_{13}+k_{14}, k_{23}+k_{24}, k_{13}+k_{23}, k_{14}+k_{24}).$$

To see this, assume without loss of generality that m_1 is maximal among the m_i. Then $m_1 - m_4 = k_{13} - k_{24} \geq 0$ so we must have $k_{24} = 0$. It then follows that $k_{23} = m_2$, $k_{14} = m_4$, and $k_{13} = m_3 - m_2$.

We then observe

$$\begin{aligned} B(z_1,\ldots,z_4) &= \prod_P \Big(1 - (z_1 z_2 z_3 z_4)^{\deg P}\Big) \\ &= \zeta_q(z_1 z_2 z_3 z_4)^{-1} \\ &= 1 - q z_1 z_2 z_3 z_4. \end{aligned}$$

Substituting our formula for $B(z_1,\ldots,z_4)$, the precise moment for $k = 2$ is therefore

$$\frac{1}{(2\pi i)^4}\int_{|z_4|=\varepsilon_4}\cdots\int_{|z_1|=\varepsilon_1}\frac{(1-qz_1z_2z_3z_4)\prod_{i=1}^{2}\prod_{j=3}^{4}\zeta_q(z_iz_j)}{z_1^{N+1}\cdots z_4^{N+1}}dz_1\cdots dz_4,$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

which we may split using linearity as

$$\frac{1}{(2\pi i)^4}\int_{|z_4|=\varepsilon_4}\cdots\int_{|z_1|=\varepsilon_1}\frac{\prod_{i=1}^{2}\prod_{j=3}^{4}\zeta_q(z_iz_j)}{z_1^{N+1}\cdots z_4^{N+1}}dz_1\cdots dz_4$$
$$-q\frac{1}{(2\pi i)^4}\int_{|z_4|=\varepsilon_4}\cdots\int_{|z_1|=\varepsilon_1}\frac{\prod_{i=1}^{2}\prod_{j=3}^{4}\zeta_q(z_iz_j)}{z_1^{N}\cdots z_4^{N}}dz_1\cdots dz_4.$$

The following proposition will allow us to conclude.

PROPOSITION 5·2. *Fix* $0<\varepsilon<q^{-1}$. *For each integer* $k\geq 1$,

$$\frac{1}{(2\pi i)^{2k}}\int_{|z_{2k}|=\varepsilon}\cdots\int_{|z_1|=\varepsilon}\frac{\prod_{i=1}^{k}\prod_{j=k+1}^{2k}\zeta_q(z_iz_j)}{z_1^{N+1}\cdots z_{2k}^{N+1}}dz_1\cdots dz_{2k}=q^{Nk}\mathcal{S}_k(N). \tag{5·7}$$

Indeed, noting that $\mathcal{S}_2(N)=N+1$, it then follows that the fourth moment equals

$$(N+1)q^{2N}-q\cdot Nq^{2(N-1)}=Nq^{2N}\Big(1-\frac{1}{q}\Big)+q^{2N},$$

as desired.

Proof of Proposition 5·2. Fix $j\in\{k+1,\dots,2k\}$. Note that we can compute the integral over z_j by computing the coefficient of z_j^N in the product

$$\prod_{i=1}^{k}\zeta_q(z_iz_j). \tag{5·8}$$

Recall that $\zeta_q(z)=\sum_{n\geq 0}q^n\cdot z^n$. The coefficient of z_j^N in (5·8) is then just

$$q^N\sum_{m_1+\cdots+m_k=N}\cdots\sum z_1^{m_1}\cdots z_k^{m_k}.$$

Observe that this product is independent of our choice of j, and since the j's are independent of each other in the product, we can integrate out $z_{k+1},\dots,z_{2k}$. In this way we can transform the integral expression in (5·7) into

$$\frac{1}{(2\pi i)^k}\int_{|z_k|=\varepsilon}\cdots\int_{|z_1|=\varepsilon}\frac{q^{Nk}\Big(\sum\limits_{m_1+\cdots+m_k=N}z_1^{m_1}\cdots z_k^{m_k}\Big)^k}{z_1^{N+1}\cdots z_k^{N+1}}dz_1\cdots dz_k.$$

At this point we can directly compute the coefficient of $z_1^N\cdots z_k^N$ in the numerator. Reindexing the sums, we expand it as

$$q^{Nk}\Big(\sum_{m_{1,1}+\cdots+m_{k,1}=N}\cdots\sum z_1^{m_{1,1}}\cdots z_k^{m_{k,1}}\Big)\cdots\Big(\sum_{m_{1,k}+\cdots+m_{k,k}=N}\cdots\sum z_1^{m_{1,k}}\cdots z_k^{m_{k,k}}\Big).$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

This product is precisely

$$\sum_{m_{1,1}+\cdots+m_{k,1}=N} \cdots \sum_{\substack{\vdots \\ m_{1,k}+\cdots+m_{k,k}=N}} z_1^{\sum_{j=1}^k m_{1,j}} \cdots z_k^{\sum_{j=1}^k m_{k,j}}.$$

We observe that the coefficient of $z_1^N \cdots z_k^N$ is given by the number of sets of k^2 integers $m_{i,j}$ such that in the square

$$\begin{bmatrix} m_{1,1} & \cdots & m_{k,1} \\ \vdots & \ddots & \vdots \\ m_{1,k} & \cdots & m_{k,k} \end{bmatrix},$$

each row sums to N (enforcing the condition over the summation) and each column sums to N (ensuring that all exponents are raised to the Nth power). Thus the integral is precisely equal to $q^{Nk}\mathcal{S}_k(N)$.

Remark. Strictly speaking, the above analytic proof of Theorem 1·3 does not require any complex analysis or Cauchy's integral formula. The argument can be reformulated using only formal power series. We chose this approach because it closely parallels the proof of Theorem 1·1 and we hope the reader can benefit from those parallels.

6. *Analytic computation of Steinhaus moments: proof of theorem 1·1*

The remainder of the paper will be dedicated to the proof of Theorem 1·1. We provide a brief outline. This section establishes the theorem assuming some key propositions whose proofs will be postponed to subsequent sections; the strategy closely parallels Section 5. First, we form the formal power series $A(z_1, \ldots, z_{2k})$ for counting solutions to (2·1). We express this series as a product of zeta functions and another power series, denoted $B(z_1, \ldots, z_{2k})$, and then form the contour integral representation of (2·1). Second, using analytic properties of B (Proposition 6·1 is proved in Section 7), we express (2·1) as an iterated integral over an expanded polydisk after a suitable change of variables (Proposition 6·2 is proved in Section 8). Third, we extract the main contribution of this integral in terms of the arithmetic constant $b_k(q)$ and the number of magic squares $\mathcal{S}_k(N)$ (Proposition 6·3 is proved in Section 9). Finally, we compute the size of the residual error term via a delicate analysis of an oscillatory integral (Proposition 6·4 is proved in Section 10), thus establishing the main theorem.

Proof of Theorem 1·1. One can check by hand that the explicit formula for $k = 1$ matches the asymptotics given in Theorem 1·1. We may thus assume $k \geq 2$. Furthermore, note that if N eventually remains bounded by 20 as $q^N \to \infty$, then Theorem 1·1 is already implied by Theorem 1·2. We may therefore also assume that N is at least 20. Both of these assumptions will be convenient for technical estimates later in the proof.

We proceed as in Section 5. Namely, we want to recover the coefficient of $z_1^N \cdots z_{2k}^N$ in the power series

$$A(z_1, \ldots, z_{2k}) := \sum_{F_1, \ldots, F_{2k} \in \mathcal{M}} \cdots \sum \mathbb{1}_{\{F_1 \cdots F_k = F_{k+1} \cdots F_{2k}\}} z_1^{\deg F_1} \cdots z_{2k}^{\deg F_{2k}} \tag{6·1}$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

in $2k$ variables, which is precisely the $2k$th moment by (2·1). Note that this function is dominated by

$$\sum_{F_1,\dots,F_{2k}\in\mathcal{M}} \cdots \sum \left| z_1^{\deg F_1} \cdots z_{2k}^{\deg F_{2k}} \right| = \prod_{i=1}^{2k} \zeta_q(|z_i|),$$

which converges uniformly on compact subsets of $\{(z_1,\dots,z_{2k})\in\mathbb{C}^{2k} : |z_i| < 1/q \text{ for } 1\le i\le 2k\}$.

Since the indicator function is multiplicative[1], we have the product expansion

$$A(z_1,\dots,z_{2k}) = \prod_P \left(\sum_{\substack{m_1+\cdots+m_k \\ =m_{k+1}+\cdots+m_{2k}}} \cdots \sum (z_1^{m_1}\cdots z_{2k}^{m_{2k}})^{\deg P} \right).$$

PROPOSITION 6·1. *Let*

$$B(z_1,\dots,z_{2k}) := \prod_P \left(\sum_{\substack{m_1+\cdots+m_k \\ =m_{k+1}+\cdots+m_{2k}}} \cdots \sum (z_1^{m_1}\cdots z_{2k}^{m_{2k}})^{\deg P} \right) \prod_{i=1}^{k}\prod_{j=k+1}^{2k} (1 - z_i^{\deg P} z_j^{\deg P}).$$

The infinite product $B(z)$ converges absolutely and uniformly on

$$\mathcal{R} := \left\{ (z_1,\dots,z_{2k})\in\mathbb{C}^{2k} : |z_i| < \frac{1.1}{\sqrt{q}} \text{ for } 1\le i\le 2k \right\},$$

and hence $B(z)$ is holomorphic on $\mathcal{R}$. Furthermore, if $z, w\in\mathcal{R}$, then

$$|B(z)| \ll_k 1 \quad \text{and} \quad |B(z)-B(w)| \ll_k \frac{1}{\sqrt{q}}\|z-w\|_\infty.$$

Proof. The proof is postponed to Section 7.

We may thus factor $A(z_1,\dots,z_{2k})$ as

$$A(z_1,\dots,z_{2k}) = B(z_1,\dots,z_{2k}) \prod_{i=1}^{k}\prod_{j=k+1}^{2k} \zeta_q(z_i z_j),$$

where this equation holds when both functions are defined.

By the multivariate version of Cauchy's integral formula, we have

$$\mathbb{E}\left| \sum_{F\in\mathcal{M}_N} f(F) \right|^{2k} = \frac{1}{(2\pi i)^{2k}} \int_{|z_{2k}|=\varepsilon_{2k}} \cdots \int_{|z_1|=\varepsilon_1} \frac{A(z_1,\dots,z_{2k})}{z_1^{N+1}\cdots z_{2k}^{N+1}}\, dz_1\cdots dz_{2k},$$

where $0<\varepsilon_i<q^{-1}$, so that A converges on the closed polydisk with radii ε_i.

[1] For $r\in\mathbb{N}$, a function $\varphi:\mathcal{M}^r\to\mathbb{C}$ is multiplicative if $\varphi(A_1B_1,\dots,A_rB_r)=\varphi(A_1,\dots,A_r)\varphi(B_1,\dots,B_r)$ for every $A_1,\dots,A_r,B_1,\dots,B_r\in\mathcal{M}$ such that $\gcd(A_1\cdots A_r, B_1\cdots B_r)=1$.

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

PROPOSITION 6·2. *Let $c_i \in (1/4, 3/4)$ for $i \in \{2, \dots, 2k\}$. We have the following equality*:

$$\mathbb{E}\Big|\sum_{F\in\mathcal{M}_N} f(F)\Big|^{2k} = \frac{N^{(k-1)^2}}{(2\pi)^{2k-1}} q^{kN} \int_{-\pi N}^{\pi N} \cdots \int_{-\pi N}^{\pi N} \frac{e^{-(c_2+i\theta_2+\cdots+c_{2k}+i\theta_{2k})}}{\prod_{i=2}^{k}\prod_{j=k+1}^{2k} N\left(1-e^{(c_i+i\theta_i+c_j+i\theta_j)/N}\right)} \tag{6·2}$$

$$\times \prod_{j=k+1}^{2k} \frac{d\theta_j}{N\left(1-e^{(c_j+i\theta_j)/N}\right)}$$

$$\times B\left(q^{-1/2}, q^{-1/2}e^{(c_2+i\theta_2)/N}, \dots, q^{-1/2}e^{(c_{2k}+i\theta_{2k})/N}\right)$$

$$\times \; d\theta_2 \cdots d\theta_k.$$

Proof. The proof is postponed to Section 8. The main idea is to use the factorisation of A in terms of B and the zeta functions along with several substitutions to center the integrand around z_1. Finally, we plug in explicit parametrisations of the contour.

Remark. The integral (6·2) is similar to one considered by Heap–Lindqvist in [**HL16**, section 4·2] when computing the moments of truncated characteristic polynomials with secular coefficients, and our proof proceeds similarly. For more discussion on connections with random matrix theory and secular coefficients, we refer the reader to works of Heap–Lindqvist [**HL16**], Conrey–Gamburd [**CG06**], Najnudel–Paquette–Simm [**NPS23**] and Gorodetsky [**Gor24**].

Now, we let $b_k(q) := B(q^{-1/2}, \dots, q^{-1/2})$ so that $0 < b_k(q) \ll_k 1$ by Proposition 6·1. Rewrite

$$\mathbb{E}\Big|\sum_{F\in\mathcal{M}_N} f(F)\Big|^{2k} = b_k(q)q^{kN}(I_k + J_k),$$

where

$$I_k = \frac{N^{(k-1)^2}}{(2\pi)^{2k-1}} \int_{-\pi N}^{\pi N} \cdots \int_{-\pi N}^{\pi N} \frac{e^{-(c_2+i\theta_2+\cdots+c_{2k}+i\theta_{2k})}}{\prod_{i=2}^{k}\prod_{j=k+1}^{2k} N\left(1-e^{(c_i+i\theta_i+c_j+i\theta_j)/N}\right)} \times \prod_{j=k+1}^{2k} \frac{d\theta_j}{N\left(1-e^{(c_j+i\theta_j)/N}\right)}\, d\theta_2 \cdots d\theta_k$$

and

$$J_k = \frac{1}{b_k(q)q^{kN}}\mathbb{E}\Big|\sum_{F\in\mathcal{M}_N} f(F)\Big|^{2k} - I_k.$$

We claim that $b_k(q)q^{kN}I_k$ is our main term.

PROPOSITION 6·3. *We have that $I_k = \mathcal{S}_k(N)$.*

Proof. See Section 9 for a detailed proof and Proposition 1 of [**CG06**] for a similar statement. Our proof more closely follows part of the argument for Theorem 2 in [**CG06**].

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

It remains to show that the error term J_k is $o(\mathcal{S}_k(N))$ as $qN \to \infty$. Since $\mathcal{S}_k(N)/N^{(k-1)^2} \ll_k 1$ (see the remarks after Theorem 1·1), it suffices to estimate the quantity

$$\begin{aligned}\widetilde{J}_k := \frac{1}{(2\pi)^{2k-1}} \int_{-\pi N}^{\pi N} \cdots \int_{-\pi N}^{\pi N} & \frac{e^{-(c_2+i\theta_2+\cdots+c_{2k}+i\theta_{2k})}}{\prod_{i=2}^{k}\prod_{j=k+1}^{2k} N\left(1-e^{(c_i+i\theta_i+c_j+i\theta_j)/N}\right)} \\ & \times \prod_{j=k+1}^{2k} \frac{d\theta_j}{N\left(1-e^{(c_j+i\theta_j)/N}\right)} \\ & \times \left(B(q^{-1/2}, q^{-1/2}e^{(c_2+i\theta_2)/N}, \ldots, q^{-1/2}e^{(c_{2k}+i\theta_{2k})/N}) - b_k(q)\right) \\ & \times d\theta_2 \cdots d\theta_k,\end{aligned} \tag{6·3}$$

and show that $\widetilde{J}_k$ converges to 0 as $qN \to \infty$.

PROPOSITION 6·4. *Fix $k \in \mathbb{N}$ with $k \geq 2$. For $2 \leq X \leq N/10$ and $10X \leq Y \leq N$ (recall the assumption $N \geq 20$),*

$$|\widetilde{J}_k| \ll_k \frac{1}{q}\frac{(\log N)^{2k-1}}{X^{1-1/k}} + \frac{1}{q}(\log N)^{2k-2}\frac{X}{N} + \frac{1}{q}\left(\frac{X}{Y}\right)^{k-1} + \frac{1}{q}\frac{Y}{N}(\log N)^k.$$

Proof. See Section 10 for the proof. The idea is to split up the region of integration. The difference of B-terms will contribute the factor of $1/q$. We will show that if any of the θ_i or θ_j is large, i.e, not $o(N)$, the integral over that part of the region converges to 0 as $N \to \infty$. On the other hand, if we have $\theta_i, \theta_j = o(N)$ for all i,j, the difference $B(\,\cdot\,) - b_k(q)$ will ensure convergence to 0 even for fixed q.

Choosing

$$X = (N\log N)^{\frac{k}{2k-1}} \quad \text{and} \quad Y = \frac{N^{1-1/k}}{X} = \frac{N^{\frac{k^2+k-1}{(2k-1)k}}}{(\log N)^{\frac{k}{2k-1}}},$$

we obtain the final error estimate

$$\frac{1}{q}\left(\frac{(\log N)^{4k^2-5k+2}}{N^{k-1}}\right)^{\frac{1}{2k-1}} + \frac{1}{q}\left(\frac{(\log N)^{2k^2-2k}}{N^{\frac{(k-1)^2}{k}}}\right)^{\frac{1}{2k-1}} \ll_k \frac{1}{q}\frac{(\log N)^k}{N^{\frac{1}{2}-\frac{3k-2}{4k^2-2k}}}.$$

A short computation shows that

$$\begin{aligned} b_k(q) &= B(q^{-1/2}, \ldots, q^{-1/2}) \\ &= \prod_P \sum_{m=0}^{\infty} \Bigg(\sum_{m_1+\cdots+m_k=m} \left(\frac{1}{\sqrt{q}}\right)^{m\deg P}\Bigg)^2 \prod_{i=1}^{k}\prod_{j=k+1}^{2k}\left(1-\left(\frac{1}{q}\right)^{\deg P}\right). \end{aligned}$$

Using stars and bars for the inner sum (cf. [**MV07**, lemma 7·7]), and noting that the second double product no longer depends on i,j, this reduces to

$$\prod_P \sum_{m=0}^{\infty} \left(\binom{m+k-1}{k-1}^2 \left(\frac{1}{\sqrt{q}}\right)^{2m\deg P}\right)\left(1-\left(\frac{1}{q}\right)^{\deg P}\right)^{k^2}.$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

Thus,

$$b_k(q) = \prod_{P\in\mathcal{M}} \left(1 - \left(\frac{1}{q}\right)^{\deg P}\right)^{k^2} \sum_{m=0}^{\infty} \binom{m+k-1}{k-1}^2 \left(\frac{1}{q}\right)^{m \deg P}.$$

This completes the proof of Theorem 1·1 assuming Propositions 6·1 to 6·4.

The last four sections will establish the remaining propositions.

7. *Proof of Proposition 6·1: convergence of B series*

Recall sums over $m_1, \dots, m_{2k}$ will always be over non-negative integers and

$$B(z_1, \dots, z_{2k}) := \prod_P \Big(\sum_{\substack{m_1+\cdots+m_k \\ =m_{k+1}+\cdots+m_{2k}}} \cdots \sum (z_1^{m_1} \cdots z_{2k}^{m_{2k}})^{\deg P} \Big) \prod_{i=1}^{k} \prod_{j=k+1}^{2k} (1 - z_i^{\deg P} z_j^{\deg P}).$$

Our proof proceeds by first looking at the local factors (i.e. for fixed P). Write $\ell := \deg P$ and let

$$F_\ell(z_1, \dots, z_{2k}) := \sum_{\substack{m_1+\cdots+m_k \\ =m_{k+1}+\cdots+m_{2k}}} \cdots \sum z_1^{m_1 \ell} \cdots z_{2k}^{m_{2k}\ell}$$

and

$$G_\ell(z_1, \dots, z_{2k}) := \prod_{i=1}^{k} \prod_{j=k+1}^{2k} (1 - z_i^\ell z_j^\ell).$$

Expanding the sums and products, we get

$$F_\ell(z_1, \dots, z_{2k}) = 1 + \sum_{i=1}^{k} \sum_{j=k+1}^{2k} z_i^\ell z_j^\ell + \sum_{M=2}^{\infty} \left(\sum_{\substack{m_1+\cdots+m_k=M \\ m_{k+1}+\cdots+m_{2k}=M}} \cdots \sum (z_1^{m_1} \cdots z_{2k}^{m_{2k}})^\ell \right)$$

and

$$G_\ell(z_1, \dots, z_{2k}) = 1 - \sum_{i=1}^{k} \sum_{j=k+1}^{2k} z_i^\ell z_j^\ell + \sum_{L=2}^{k^2} \left(\sum_{\substack{n_1+\cdots+n_k=L \\ n_{k+1}+\cdots+n_{2k}=L \\ 0\le n_1,\dots,n_{2k}\le k}} \cdots \sum c(n_1, \dots, n_{2k}) (z_1^{n_1} \cdots z_{2k}^{n_{2k}})^\ell \right)$$

for some constants $c(n_1, \dots, n_{2k})$ depending on $n_1, \dots, n_{2k}$. Consequently,

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

$$(F_\ell \cdot G_\ell)(z_1,\dots,z_{2k}) = 1 + \sum_{M=1}^{\infty}\left(\sum_{\substack{m_1+\cdots+m_k=M\\ m_{k+1}+\cdots+m_{2k}=M}}\cdots\sum (z_1^{m_1}\cdots z_{2k}^{m_{2k}})^\ell\right)$$
$$-\sum_{M=0}^{\infty}\left(\sum_{\substack{m_1+\cdots+m_k=m_{k+1}+\cdots+m_{2k}=M\\ n_1+\cdots+n_k=n_{k+1}+\cdots+n_{2k}=1}}\cdots\sum (z_1^{m_1+n_1}\cdots z_{2k}^{m_{2k}+n_{2k}})^\ell\right)$$
$$+\sum_{M=0}^{\infty}\sum_{L=2}^{k^2}\left(\sum_{\substack{0\le n_1,\dots,n_{2k}\le k\\ m_1+\cdots+m_k=m_{k+1}+\cdots+m_{2k}=M\\ n_1+\cdots+n_k=n_{k+1}+\cdots+n_{2k}=L}}\cdots\sum c(n_1,\dots,n_{2k})(z_1^{m_1+n_1}\cdots z_{2k}^{m_{2k}+n_{2k}})^\ell\right). \quad (7{\cdot}1)$$

Collecting terms, we see that the $M=1$ term in the first series cancels with the $M=0$ term in the second series and that when $m_1'+\cdots+m_k'=m_{k+1}'+\cdots+m_{2k}'\ge 2$, the coefficient of $(z_1^{m_1'}\cdots z_{2k}^{m_{2k}'})^\ell$ is given by

$$c'(m_1',\cdots,m_{2k}') := 1 - \sum_{\substack{0\le n_1,\dots,n_{2k}\le k\\ n_1+\cdots+n_k=n_{k+1}+\cdots+n_{2k}=1\\ m_i'-n_i\ge 0}}\cdots\sum 1 + \sum_{\substack{0\le n_1,\dots,n_{2k}\le k\\ n_1+\cdots+n_k=n_{k+1}+\cdots+n_{2k}\ge 2\\ m_i'-n_i\ge 0}}\cdots\sum c(n_1,\dots,n_{2k}).$$

We observe that

$$c'(m_1',\dots,m_{2k}') \le 1+k^2+\sum_{0\le n_1,\dots,n_{2k}\le k}\cdots\sum |c(n_1,\dots,n_{2k})|,$$

so these constants are uniformly bounded in k. Thus, (7·1) can be rewritten as $1+C_P(z)$, where

$$C_P(z) = \sum_{M=2}^{\infty}\sum_{\substack{m_1+\cdots+m_k=M\\ m_{k+1}+\cdots+m_{2k}=M}}\cdots\sum c'(m_1,\dots,m_{2k}) z_1^{m_1\ell}\cdots z_{2k}^{m_{2k}\ell}. \quad (7{\cdot}2)$$

For simplicity, fix $D = 1.21e^{0.1} > 1$ (this choice is somewhat arbitrary). We now give bounds on the local factor.

LEMMA 7·1. *For $z, w \in \mathcal{R} = \{(z_1,\dots,z_{2k})\in\mathbb{C}^{2k}: |z_i| < 1.1q^{-1/2}$ for $1\le i\le 2k\}$, we have*

$$|C_P(z)| \ll_k \left(\frac{D}{q}\right)^{2\ell}$$

and

$$|C_P(z)-C_P(w)| \ll_k \ell||z-w||_\infty\sqrt{q}\left(\frac{D}{q}\right)^{2\ell}.$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

Proof. For $z \in \mathcal{R}$, we have

$$\begin{aligned}|C_P(z)| &\ll_k \sum_{M=2}^{\infty} \Big(\sum_{\substack{m_1+\cdots+m_k=M \\ m_{k+1}+\cdots+m_{2k}=M}} \cdots \sum 1 \Big) \Big(\frac{1.1}{\sqrt{q}}\Big)^{2M\ell} \\ &= \sum_{M=2}^{\infty} \binom{M+k-1}{k-1}^2 \Big(\frac{(1.1)^2}{q}\Big)^{M\ell} \\ &\ll_k \sum_{M=2}^{\infty} M^{2(k-1)} \Big(\frac{1.21}{q}\Big)^{M\ell}, \end{aligned} \tag{7·3}$$

where the last inequality follows since $\binom{M+k-1}{k-1}^2$ is a polynomial in M of degree at most $2(k-1)$. Observe that $\big(1.21/q\big)^{M\ell} = e^{-0.1M\ell}\big(D/q\big)^{M\ell}$, and further for $M \geq 2$,

$$M^{2(k-1)} e^{-0.1M\ell} \leq M^{2(k-1)} e^{-0.1M} \ll_k 1.$$

We conclude that

$$\sum_{M=2}^{\infty} M^{2(k-1)} \Big(\frac{1.21}{q}\Big)^{M\ell} \ll_k \sum_{M=2}^{\infty} \Big(\frac{D}{q}\Big)^{M\ell} \ll_k \Big(\frac{D}{q}\Big)^{2\ell}, \tag{7·4}$$

where the last estimate comes from bounding the convergent geometric series by its first term. This proves the first estimate in the lemma.

Now, we prove the upper bound for the difference $|C_P(z) - C_P(w)|$. From the definition in (7·2) and using that $|z_i|, |w_i| < 1.1q^{-1/2}$, we find that

$$\begin{aligned}|C_P(z) - C_P(w)| &\ll_k \sum_{M=2}^{\infty} \sum_{\substack{m_1+\cdots+m_k=M \\ m_{k+1}+\cdots+m_{2k}=M}} \cdots \sum \big| (z_1^{m_1} \cdots z_{2k}^{m_{2k}})^{\ell} - (w_1^{m_1} \cdots w_{2k}^{m_{2k}})^{\ell} \big| \\ &\leq \ell \sum_{M=2}^{\infty} \Big(\frac{1.1}{\sqrt{q}}\Big)^{2M(\ell-1)} \sum_{\substack{m_1+\cdots+m_k=M \\ m_{k+1}+\cdots+m_{2k}=M}} \cdots \sum \big| z_1^{m_1} \cdots z_{2k}^{m_{2k}} - w_1^{m_1} \cdots w_{2k}^{m_{2k}} \big|, \end{aligned} \tag{7·5}$$

where we implicitly used the identity $A^n - B^n = (A-B)\sum_{k=0}^{n-1} A^{n-1-k}B^k$.

Now, we claim

$$|z_1^{m_1} \cdots z_{2k}^{m_{2k}} - w_1^{m_1} \cdots w_{2k}^{m_{2k}}| \leq 2M \Big(\frac{1.1}{\sqrt{q}}\Big)^{2M-1} \|z - w\|_{\infty}, \tag{7·6}$$

where $m_1 + \cdots + m_k = m_{k+1} + \cdots + m_{2k} = M$. Observe that when $k = 1$, we can write

$$\begin{aligned}|z_1^{m_1} z_2^{m_2} - w_1^{m_1} w_2^{m_2}| &= |z_1^{m_1} z_2^{m_2} - z_1^{m_1} w_2^{m_2} + z_1^{m_1} w_2^{m_2} - w_1^{m_1} w_2^{m_2}| \\ &\leq |z_1|^{m_1} |z_2^{m_2} - w_2^{m_2}| + |w_2^{m_2}||z_1^{m_1} - w_1^{m_1}| \\ &\leq \Big(\frac{1.1}{\sqrt{q}}\Big)^{m_1} |z_2 - w_2| m_2 \Big(\frac{1.1}{\sqrt{q}}\Big)^{m_2-1} + \Big(\frac{1.1}{\sqrt{q}}\Big)^{m_2} |z_1 - w_1| m_1 \Big(\frac{1.1}{\sqrt{q}}\Big)^{m_1-1} \\ &\leq \|z - w\|_{\infty} (m_1 + m_2) \Big(\frac{1.1}{\sqrt{q}}\Big)^{m_1+m_2-1}. \end{aligned}$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

For any other $k \geq 2$, the claim follows by induction after rewriting

$$\begin{aligned}|z_1^{m_1}\cdots z_{2k}^{m_{2k}} - w_1^{m_1}\cdots w_{2k}^{m_{2k}}| &= |z_1^{m_1}z_2^{m_2}(z_3^{m_3}\cdots z_{2k}^{m_{2k}} - w_3^{m_3}\cdots w_{2k}^{m_{2k}}) \\ &\quad + w_3^{m_3}\cdots w_{2k}^{m_{2k}}(z_1^{m_1}z_2^{m_2} - w_1^{m_1}w_2^{m_2})| \\ &\leq |z_1|^{m_2}|z_2|^{m_2}\cdot(m_3+\cdots+m_{2k})\Big(\frac{1.1}{\sqrt{q}}\Big)^{m_3+\cdots+m_{2k}-1}||z-w||_\infty \\ &\quad + |w_3|^{m_3}\cdots|w_{2k}|^{m_{2k}}\cdot(m_1+m_2)\Big(\frac{1.1}{\sqrt{q}}\Big)^{m_1+m_2-1}||z-w||_\infty \\ &\leq (m_1+\cdots+m_{2k})\Big(\frac{1.1}{\sqrt{q}}\Big)^{m_1+\cdots+m_{2k}-1}||z-w||_\infty,\end{aligned}$$

as required. Thus, the estimate (7·6) implies that (7·5) is

$$\ll \ell\,\|z-w\|_\infty\sqrt{q}\sum_{M=2}^{\infty}M\binom{M+k-1}{k-1}^2\Big(\frac{1.21}{q}\Big)^{M\ell}.$$

At this point, we use the same manipulation as we did in going from (7·3) to (7·4) to recover the estimate

$$|C_P(z)-C_P(w)| \ll_k \ell||z-w||_\infty\sqrt{q}\left(\frac{D}{q}\right)^{2\ell}.$$

Recall that by definition, $B(z)=\prod_P(1+C_P(z))$. By Lemma 7·1 and the observation $D<2\leq q$, if $\ell_0\geq 1$ is sufficiently large depending only on k, then

$$|C_P(z)|\leq\frac{1}{2}\quad\text{whenever }\deg P\geq\ell_0. \tag{7·7}$$

For $\ell_0\geq 1$, define

$$J(z):=\prod_{\substack{P\\ \deg P<\ell_0}}\big(1+C_P(z)\big),\qquad K(z):=\prod_{\substack{P\\ \deg P\geq\ell_0}}\big(1+C_P(z)\big)$$

so that $B(z)=J(z)K(z)$.

LEMMA 7·2. *Assume $\ell_0=\ell_0(k)$ depends only on k and satisfies (7·7). For $z\in\mathcal{R}$,*

$$J(z)\ll_k 1,\qquad K(z)\ll_k 1.$$

In particular, $|B(z)|\ll_k 1$.

Proof. Recall the prime polynomial theorem implies that

$$\pi_q(\ell):=\#\{P\in\mathcal{M}_\ell : P\text{ irreducible}\}\ll\frac{q^\ell}{\ell}, \tag{7·8}$$

so we have

$$\begin{aligned}|J(z)| &= \Big|\prod_{\substack{P\\ \deg P<\ell_0}}(1+C_P(z))\Big| \\ &\ll_k \prod_{\substack{P\\ \deg P<\ell_0}}\Big(1+\frac{D^{2\deg P}}{q^{2\deg P}}\Big)=\prod_{1\leq\ell<\ell_0}\Big(1+\frac{D^{2\ell}}{q^{2l}}\Big)^{\pi_q(\ell)}\end{aligned}$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

$$\leq \prod_{1\leq \ell<\ell_0} \exp\left(O(q^{-\ell}D^{2\ell}/\ell)\right) \ll_k 1.$$

Here, we have used that $(1+1/x)^x < e$ for all $x > 0$ and that $D = 1.21e^{0.1} < \sqrt{2}$.

By our assumption on ℓ_0, we have $|C_P(z)| \leq 1/2$, so we may use the expansion $|\log(1+w)| = O(|w|)$ for $|w| \leq 1/2$. Thus, the prime polynomial theorem (7·8), Lemma 7·1, and the fact that $D < \sqrt{2}$ together imply that

$$|\log(K(z))| \ll \sum_{\substack{P \\ \deg P \geq \ell_0}} |C_P(z)| \ll_k \sum_{\substack{P \\ \deg P \geq \ell_0}} \frac{D^{2\ell}}{q^{2\ell}} \ll_k \sum_{\ell \geq \ell_0} \frac{D^{2\ell}}{q^{2\ell}} \frac{q^\ell}{\ell} \ll_k q^{-\ell_0} \ll_k 1.$$

In particular, $|K(z)| \ll_k 1$.

Lemma 7·2 shows in particular that $|B(z)| \ll_k 1$ as claimed in Proposition 6·1 The remainder of Proposition 6·1 rests on the following consequence of the triangle inequality: for $z, w \in \mathcal{R}$,

$$\begin{aligned} |B(z) - B(w)| &= |J(z)K(z) - J(w)K(w)| \\ &\leq |J(z) - J(w)| \cdot |K(z)| + |K(z) - K(w)| \cdot |J(w)|. \end{aligned} \tag{7·9}$$

Therefore, showing that the differences $|J(z) - J(w)|$ and $|K(w) - K(z)|$ are bounded in terms of k and explicitly in terms of q will allow us to complete the proof of Proposition 6·1.

We now choose a suitable value for ℓ_0 by means of the next lemma.

LEMMA 7·3. *There exists $\ell_0 = \ell_0(k)$ sufficiently large such that (7·7) holds and for $z, w \in \mathcal{R}$,*

$$\left|\log \frac{K(z)}{K(w)}\right| \leq \frac{1}{2} \quad \text{and} \quad \left|\log \frac{K(z)}{K(w)}\right| \ll_k \sqrt{q}||z-w||_\infty \left(\frac{D^2}{q}\right)^{\ell_0}.$$

Proof. By Lemma 7·1, $K(z)$ is an absolutely convergent infinite product inside $\mathcal{R}$. So, it is never zero in that region and we can take its logarithm. Using the Taylor expansion of $\log(1+z)$ for $|z| \leq 1/2$, we find that

$$\begin{aligned} \left|\log \frac{K(z)}{K(w)}\right| &= \left| \sum_{\substack{P \\ \deg P \geq \ell_0}} \left(\log(1+C_P(z)) - \log(1+C_P(w))\right)\right| \\ &= \left| \sum_{\substack{P \\ \deg P \geq \ell_0}} \sum_{n=1}^{\infty} (-1)^{n+1} \frac{C_P(z)^n - C_P(w)^n}{n} \right| \\ &\leq \sum_{\substack{P \\ \deg P \geq \ell_0}} \sum_{n=1}^{\infty} \frac{|C_P(z) - C_p(w)|}{n} \sum_{i=0}^{n-1} |C_P(z)^i C_P(w)^{n-1-i}| \\ &\leq \sum_{\substack{P \\ \deg P \geq \ell_0}} |C_P(z) - C_p(w)|. \end{aligned}$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

Applying Lemma 7·1, as well as the prime polynomial theorem (7·8), we see that

$$\begin{aligned}\sum_{\substack{P\\ \deg P\geq \ell_0}} \big(C_P(z)-C_P(w)\big) &\ll_k \sum_{\ell\geq \ell_0} \ell ||z-w||_\infty \sqrt{q}\Big(\frac{D}{q}\Big)^{2\ell}\frac{q^\ell}{\ell}\\ &= \sqrt{q}||z-w||_\infty \sum_{\ell\geq \ell_0}\Big(\frac{D^2}{q}\Big)^\ell\\ &\ll_k \sqrt{q}||z-w||_\infty\Big(\frac{D^2}{q}\Big)^{\ell_0}.\end{aligned}$$

This is the second estimate that we claimed. Since $||z-w||_\infty \ll 1/\sqrt{q}$ and $D^2/q<1$ for any $q\geq 2$, the first estimate also holds provided $\ell_0=\ell_0(k)$ is taken to be sufficiently large.

We proceed to bound the differences in (7·9), starting with $|K(z)-K(w)|$.

LEMMA 7·4. *If $z,w\in\mathcal{R}$ and $\ell_0=\ell_0(k)$ is sufficiently large according to Lemma 7·3, then*

$$|K(z)-K(w)| \ll_k \sqrt{q}||z-w||_\infty\Big(\frac{D^2}{q}\Big)^{\ell_0}.$$

Proof. We simply observe that

$$|K(z)-K(w)| \ll_k \Big|\frac{K(z)}{K(w)}-1\Big| \ll \Big|\log\frac{K(z)}{K(w)}\Big|,$$

where we used Lemma 7·2 for the first bound, and $e^z=1+O(|z|)$ for $|z|\leq 1/2$ and Lemma 7·3 for the second bound.

The last estimate is an upper bound for the difference $|J(z)-J(w)|$.

LEMMA 7·5. *For $z,w\in\mathcal{R}$, we have that*

$$|J(z)-J(w)| \ll_k \ell_0||z-w||_\infty\frac{D^2}{\sqrt{q}}.$$

Proof. Let $\mathcal{N}$ be some subset of the set of all monic irreducible polynomials P of degree less than ℓ_0. We will show by induction on $|\mathcal{N}|$ that

$$\Big|\prod_{P\in\mathcal{N}}(1+C_P(z))-\prod_{P\in\mathcal{N}}(1+C_P(w))\Big| \ll_k \ell_0\sqrt{q}\sum_{P\in\mathcal{N}}||z-w||_\infty\Big(\frac{D}{q}\Big)^{2\deg P}.$$

If $|\mathcal{N}|=1$, this statement is just Lemma 7·1 and the fact that $\deg P<\ell_0$. In general, we have

$$\begin{aligned}&\Big|\prod_{P\in\mathcal{N}}(1+C_P(z))-\prod_{P\in\mathcal{N}}(1+C_P(w))\Big|\\ &\quad\leq |C_{P_1}(z)-C_{P_1}(w)|\prod_{P\in\mathcal{N}\setminus\{P_1\}}|1+C_P(z)|\\ &\qquad+\Big|(1+C_{P_1}(w))\Big(\prod_{P\in\mathcal{N}\setminus\{P_1\}}(1+C_P(z))-\prod_{P\in\mathcal{N}\setminus\{P_1\}}(1+C_P(w))\Big)\Big|\end{aligned}$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

for any $P_1 \in \mathcal{N}$. Now, we can trivially bound $|1 + C_{P_1}(w)| \ll_k 1$, and by essentially the same argument as in Lemma 7·2, $\left|\prod_{P\in\mathcal{N}\setminus\{P_1\}}(1 + C_P(z))\right| \ll_k 1$. Applying the induction hypothesis and Lemma 7·1, we find that the above is bounded by

$$\ell_0\sqrt{q}\,||z-w||_\infty\Big(\frac{D}{q}\Big)^{2\deg P_1} + \ell_0 \sum_{P\in\mathcal{N}\setminus\{P_1\}} \sqrt{q}\,||z-w||_\infty\Big(\frac{D}{q}\Big)^{2\deg P},$$

up to constants depending only on k, as claimed. In particular, we now get

$$\begin{aligned}|J(z)-J(w)| &\ll_k \ell_0\sqrt{q} \sum_{\substack{P\\ \deg P<\ell_0}} ||z-w||_\infty\Big(\frac{D}{q}\Big)^{2\deg P}\\ &\ll \ell_0\sqrt{q}\sum_{\ell<\ell_0} ||z-w||_\infty\Big(\frac{D}{q}\Big)^{2\ell}\frac{q^\ell}{\ell} \ll \ell_0||z-w||_\infty\frac{D^2}{\sqrt{q}},\end{aligned}$$

by the prime polynomial theorem (7·8). This proves the lemma.

Inserting Lemmas 7·2, 7·4 and 7·5 in (7·9), we obtain

$$|B(z)-B(w)| \ll_k ||z-w||_\infty\Big(\frac{2}{\sqrt{q}}\Big) + ||z-w||_\infty\sqrt{q}\Big(\frac{2}{q}\Big)^{\ell_0} \ll_k \frac{1}{\sqrt{q}}||z-w||_\infty,$$

as desired. This completes the proof of Proposition 6·1.

8. *Proof of Proposition 6·2: integral representation*

Recall that

$$\mathbb{E}\Big|\sum_{F\in\mathcal{M}_N} f(F)\Big|^{2k} = \frac{1}{(2\pi i)^{2k}}\int_{|z_{2k}|=\varepsilon_{2k}}\cdots\int_{|z_1|=\varepsilon_1}\frac{A(z_1,\dots,z_{2k})}{z_1^{N+1}\cdots z_{2k}^{N+1}}\,dz_1\cdots dz_{2k}.$$

Recalling that $\zeta_q(z) = 1/(1-qz)$, we can further rewrite this as

$$\frac{1}{(2\pi i)^{2k}}\int_{|z_{2k}|=\varepsilon_{2k}}\cdots\int_{|z_1|=\varepsilon_1}\frac{(z_1\cdots z_{2k})^{-(N+1)}}{\prod_{i=1}^k\prod_{j=k+1}^{2k}(1-qz_iz_j)}\cdot B(z_1,\dots,z_{2k})\,dz_1\cdots dz_{2k}. \quad (8\cdot1)$$

We make several changes of variables as a means of centering the integral around z_1. In each case the contour integrals can still be taken along circles of small radii around 0. First, we modify z_{k+1} through z_{2k} by sending

$$z_j \mapsto z_1^{-1}q^{-1}z_j \quad \text{for} \quad k+1 \le j \le 2k.$$

This yields the expression

$$\frac{q^{kN}}{(2\pi i)^{2k}}\int\cdots\int\frac{(z_1^{1-k}z_2\cdots z_{2k})^{-(N+1)}}{\prod_{i=2}^k\prod_{j=k+1}^{2k}(1-z_iz_j/z_1)}\cdot\frac{B\left(z_1,\dots,z_1^{-1}q^{-1}z_{2k}\right)}{z_1^k\prod_{j=k+1}^{2k}(1-z_j)}\,dz_1\cdots dz_{2k}.$$

Here, the second product in the denominator of the integrand corresponds to the contribution from the double product in (8·1) in the case where $z_i = z_1$. We may also factor out a q^{kN} by considering the contributions from the numerator of the integrand in (8·1) as well as the changes in the increment.

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

We make the second substitution

$$z_i \mapsto z_1 z_i \quad \text{for} \quad 2 \le i \le k,$$

and our integral becomes

$$\frac{q^{kN}}{(2\pi i)^{2k}} \int \cdots \int \frac{1}{z_1} \frac{(z_2 \cdots z_{2k})^{-(N+1)}}{\prod_{i=2}^{k} \prod_{j=k+1}^{2k} (1 - z_i z_j)} \cdot \frac{B\left(z_1, z_1 z_2, \ldots, z_1^{-1} q^{-1} z_{2k}\right)}{\prod_{j=k+1}^{2k} (1 - z_j)} \, dz_1 \cdots dz_{2k}. \tag{8·2}$$

Before proceeding with our analysis of (8·2), we observe that along this contour, where $|z_1| > 0$, the term $B(z_1, z_1 z_2, \ldots, z_1^{-1} q^{-1} z_{2k})$ is independent of the value of z_1. Indeed,

$$B(z_1, z_1 z_2, \ldots, z_1^{-1} q^{-1} z_{2k}) = \prod_P \sum_{\substack{m_1 + \cdots + m_k = \\ m_{k+1} + \cdots + m_{2k}}} \cdots \sum \left(\frac{z_1^{m_1 + \cdots + m_k}}{z_1^{m_{k+1} + \cdots + m_{2k}}} \right)^{\deg P} (z_2^{m_2} \cdots q^{-m_{2k}} z_{2k}^{m_{2k}})^{\deg P}$$
$$\times \prod_{i=2}^{k} \prod_{j=k+1}^{2k} \left(1 - (q^{-1} z_i z_j)^{\deg P}\right) \prod_{j=k+1}^{2k} \left(1 - (q^{-1} z_j)^{\deg P}\right).$$

Since $m_1 + \cdots + m_k = m_{k+1} + \cdots + m_{2k}$, the z_1 term vanishes and we are left with

$$\prod_P \sum_{\substack{m_1 + \cdots + m_k \\ = m_{k+1} + \cdots + m_{2k}}} \cdots \sum (z_2^{m_2} \cdots q^{-m_{2k}} z_{2k}^{m_{2k}})^{\deg P} \prod_{i=2}^{k} \prod_{j=k+1}^{2k} (1 - (q^{-1} z_i z_j)^{\deg P}) \prod_{j=k+1}^{2k} (1 - (q^{-1} z_j)^{\deg P}),$$

which is clearly independent of z_1. We further note that in (8·2), the only term that depends on z_1 is the $1/z_1$ factor. Thus, we can integrate out z_1 multiplying our expression by $2\pi i$.

In the input of B, we can thus pick any value for z_1, so without loss of generality take $z_1 = q^{-1/2}$. Our integral now becomes

$$\frac{q^{kN}}{(2\pi i)^{2k-1}} \int \cdots \int \frac{(z_2 \cdots z_{2k})^{-(N+1)}}{\prod_{i=2}^{k} \prod_{j=k+1}^{2k} (1 - z_i z_j)} \cdot \frac{B\left(q^{-1/2}, q^{-1/2} z_2 \cdots, q^{-1/2} z_{2k}\right)}{\prod_{j=k+1}^{2k} (1 - z_j)} \, dz_2 \cdots dz_{2k}. \tag{8·3}$$

Despite the changes of variables, the ith integral is still taken around some disk of positive radius ε_i which now only have to satisfy $0 < \varepsilon_i < 1.1$ due to Proposition 6·1 and our choice $z_1 = q^{-1/2}$. For each integral, we can parametrise its contour in terms of its argument θ_i by

$$\gamma(\theta_i) = e^{c_i/N} e^{i\theta_i}.$$

Here, the $c_i \in (1/2, 3/4)$ are some constants, chosen to be independent of N and q. Note the radius satisfies $e^{c_i/N} \le e^{3/80} < 1.1$ as $N \ge 20$ by assumption. Explicitly substituting the contours, we rewrite (8·3) as

$$\frac{q^{kN}}{(2\pi)^{2k-1}} \int_{-\pi}^{\pi} \cdots \int_{-\pi}^{\pi} \frac{e^{-c_2 - \cdots - c_{2k} - iN(\theta_2 + \cdots + \theta_{2k})}}{\prod_{i=2}^{k} \prod_{j=k+1}^{2k} \left(1 - e^{(c_i + c_j)/N + i\theta_i + i\theta_j}\right)} \cdot \prod_{j=k+1}^{2k} \frac{1}{1 - e^{c_j/N + i\theta_j}}$$
$$\times B\left(q^{-1/2}, q^{-1/2} e^{c_2/N + i\theta_2}, \ldots, q^{-1/2} e^{c_{2k}/N + i\theta_{2k}}\right) d\theta_2 \cdots d\theta_{2k}. \tag{8·4}$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

Here, we see some cancellations arising from the derivative term and the original numerator of the integrand from (8·3). Note that the factor of i^{2k-1} cancels with the constant term preceding the integral. At this point, we make the change of variables

$$\theta_j \mapsto \theta_j/N \quad \text{for} \quad j = 2, 3, \ldots, 2k.$$

We will also multiply the numerator and denominator by $N^{(k-1)^2}$, preceding each term in each product of the denominator in (8·4) by N. This ultimately yields

$$\begin{aligned}\frac{N^{(k-1)^2}}{(2\pi)^{2k-1}} q^{kN} \int_{-\pi N}^{\pi N} \cdots \int_{-\pi N}^{\pi N} & \frac{e^{-(c_2+i\theta_2+\cdots+c_{2k}+i\theta_{2k})}}{\prod_{i=2}^{k}\prod_{j=k+1}^{2k} N\left(1-e^{(c_i+i\theta_i+c_j+i\theta_j)/N}\right)} \\ & \times \prod_{j=k+1}^{2k} \frac{d\theta_j}{N\left(1-e^{(c_j+i\theta_j)/N}\right)} \\ & \times B\left(q^{-1/2}, q^{-1/2}e^{(c_2+i\theta_2)/N}, \ldots, q^{-1/2}e^{(c_{2k}+i\theta_{2k})/N}\right) \\ & \times d\theta_2 \cdots d\theta_k,\end{aligned}$$

completing the proof of Proposition 6·2.

9. *Proof of Proposition 6·3: magic squares*

This section is nearly identical to [**CG06**, section 3], but we have included the argument for the sake of completeness. Making the change of variables $\theta_j \mapsto -\theta_j$ for $j = 2, \ldots, 2k$, we turn each integral into a complex line integral along some vertical strip of length $2\pi N$ with real part $-c_j$. Letting $s_j = -c_j + i\theta_j$, our integral becomes

$$\begin{aligned}I_k = \frac{N^{1-2k}}{(2\pi i)^{2k-1}} \int_{-c_{2k}-i\pi N}^{-c_{2k}+i\pi N} \cdots \int_{-c_2-i\pi N}^{-c_2+i\pi N} & \frac{e^{s_2+\cdots+s_{2k}}}{\prod_{i=2}^{k}\prod_{j=k+1}^{2k}\left(1-e^{-(s_i+s_j)/N}\right)} \\ & \times \prod_{j=k+1}^{2k} \frac{ds_j}{\left(1-e^{-s_j/N}\right)} \\ & \times ds_2 \cdots ds_{2k}.\end{aligned}$$

Let $u := (s_2, \ldots, s_k)$ and $v := (s_{k+1}, \ldots, s_{2k})$. Then, using the geometric series formula, the integrand becomes

$$\begin{aligned}& e^{s_2+\cdots+s_{2k}} \prod_{i=2}^{k}\prod_{j=k+1}^{2k} \frac{1}{\left(1-e^{-(s_i+s_j)/N}\right)} \times \prod_{j=k+1}^{2k} \frac{1}{\left(1-e^{-s_j/N}\right)} \\ & = e^{s_2+\cdots+s_{2k}} \prod_{i=2}^{k}\prod_{j=k+1}^{2k} \left(\sum_{a_{ij}\geq 0} (e^{(-s_i-s_j)/N})^{a_{ij}}\right) \prod_{j=k+1}^{2k} \left(\sum_{b_j\geq 0} (e^{-s_j/N})^{b_j}\right) \\ & = e^{s_2+\cdots+s_{2k}} \sum_{\alpha\in\mathbb{N}_0^{k-1},\, \beta\in\mathbb{N}_0^{k}} M_{\alpha,\beta} e^{-\alpha\cdot u/N} e^{-\beta\cdot v/N},\end{aligned}$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

where $\cdot$ denotes the usual dot product and, letting $\alpha=(\alpha_2,\dots,\alpha_k)$ and $\beta=(\beta_{k+1},\dots,\beta_{2k})$, the coefficient $M_{\alpha,\beta}\geq 0$ counts the possible choices for a_{ij} and b_j such that

$$\sum_{j=k+1}^{2k} a_{ij}=\alpha_i \quad \text{for} \quad i=2,\dots,k, \qquad \text{and} \qquad b_j+\sum_{i=2}^{k} a_{ij}=\beta_j \quad \text{for} \quad j=k+1,\dots,2k.$$

The sum is convergent on the compact region of integration. Applying Fubini's theorem, we may thus interchange sum and integral to obtain

$$\begin{aligned}
I_k&=\frac{N^{1-2k}}{(2\pi i)^{2k-1}}\sum_{\substack{\alpha\in\mathbb{N}_0^{k-1},\\ \beta\in\mathbb{N}_0^{k}}} M_{\alpha,\beta}\int_{-c_{2k}-i\pi N}^{-c_{2k}+i\pi N}\cdots\int_{-c_2-i\pi N}^{-c_2+i\pi N} e^{-\alpha\cdot u/N}e^{-\beta\cdot v/N}e^{s_2+\cdots+s_{2k}}ds_2\cdots ds_{2k}\\
&=\frac{N^{1-2k}}{(2\pi i)^{2k-1}}\sum_{\substack{\alpha\in\mathbb{N}_0^{k-1},\\ \beta\in\mathbb{N}_0^{k}}} M_{\alpha,\beta}\Big(\int_{-c_{2k}-i\pi N}^{-c_{2k}+i\pi N} e^{-(\beta_{2k}-N)s_{2k}/N}ds_{2k}\Big)\cdots\Big(\int_{-c_2-i\pi N}^{-c_2+i\pi N} e^{-(\alpha_2-N)s_2/N}ds_2\Big)\\
&=\frac{N^{1-2k}}{(2\pi i)^{2k-1}}\sum_{\substack{\alpha\in\mathbb{N}_0^{k-1},\\ \beta\in\mathbb{N}_0^{k}}} M_{\alpha,\beta}\prod_{\substack{i=2\\ \alpha_i\neq N}}^{k}\frac{N\left(e^{-(\alpha_i-N)(-c_i+i\pi N)/N}-e^{-(\alpha_i-N)(-c_i-i\pi N)/N}\right)}{N-\alpha_i}\prod_{\substack{i=2\\ \alpha_i=N}}^{k}(2\pi iN)\\
&\qquad\times\prod_{\substack{j=k+1\\ \beta_j\neq N}}^{2k}\frac{N\left(e^{-(\beta_j-N)(-c_j+i\pi N)/N}-e^{-(\beta_j-N)(-c_j-i\pi N)/N}\right)}{N-\beta_j}\prod_{\substack{j=k+1\\ \beta_j=N}}^{2k}(2\pi iN).
\end{aligned}$$

Now, observe that

$$e^{-(\alpha_i-N)(-c_i+i\pi N)/N}-e^{-(\alpha_i-N)(-c_i-i\pi N)/N}=e^{(\alpha_i/N-1)c_i}2i\sin\big((-\alpha_i+N)\pi\big),$$

and as $\alpha_i\in\mathbb{Z}$, this (and the corresponding expression for β_j) evaluates to 0 for all i,j. Thus, the only term in the summation that contributes to I_k is $M_{(N,\dots,N),(N,\dots,N)}$, which is just the number of possible choices for a_{ij} and b_j such that

$$\sum_{j=k+1}^{2k} a_{ij}=N \quad \text{for} \quad i=2,\dots,k, \qquad \text{and} \qquad b_j+\sum_{i=2}^{k} a_{ij}=N \quad \text{for} \quad j=k+1,\dots,2k.$$

It follows that we also have

$$\sum_{j=k+1}^{2k} b_j=\sum_{j=k+1}^{2k}\Big(b_j+\sum_{i=2}^{k}a_{ij}\Big)-\sum_{i=2}^{k}\sum_{j=k+1}^{2k}a_{ij}=kN-(k-1)N=N.$$

This gives the desired equality $I_k=\mathcal{S}_k(N)$, establishing Proposition 6·3.

10. *Proof of Proposition 6·4: estimating the error term*

To facilitate notation, we define

$$F(w):=F(w,N):=\frac{1}{N(1-e^{-w/N})}$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

for $w \in \mathbb{C}$. For $i = 2, \dots, 2k$, denote

$$z_i = c_i + i\theta_i, \quad c_i \in \left(\frac{1}{4}, \frac{3}{4}\right), \ \theta_i \in \mathbb{R}.$$

For any Lebesgue-measurable region $R \subset [-\pi N, \pi N]^{2k-1}$, we further define

$$I(R) := \int_R \cdots \int \prod_{i=2}^{k} \prod_{j=k+1}^{2k} |F(z_i + z_j)| \prod_{j=k+1}^{2k} |F(z_j)| \, d\theta_2 \cdots d\theta_{2k}$$

and

$$\Delta(R) := \sup_{(\theta_2,\dots,\theta_{2k}) \in R} \left| B\left(q^{-1/2}, q^{-1/2} e^{(c_2+i\theta_2)/N}, \dots, q^{-1/2} e^{(c_{2k}+i\theta_{2k})/N}\right) - b_k(q) \right|. \quad (10{\cdot}1)$$

To give a brief outline, the proof of Proposition 6·4 will involve splitting the region of integration, $[-\pi N, \pi N]^{2k-1}$, into three regions:

$$R_1 := [-\pi N, \pi N]^{2k-1} \setminus \mathfrak{S}(X), \qquad R_2 := \mathfrak{S}(X) \setminus \mathfrak{S}(X, Y), \qquad R_3 := \mathfrak{S}(X, Y),$$

with $\mathfrak{S}(X)$ and $\mathfrak{S}(X, Y) \subseteq \mathfrak{S}(X)$ specified later by (10·2) and (10·4) and dependent on the parameters X and Y given in the proposition. We observe that the integral $\widetilde{J}_k$ from (6·3) can be bounded by

$$I(R_1)\Delta(R_1) + I(R_2)\Delta(R_2) + I(R_3)\Delta(R_3).$$

In Lemmas 10·3 and 10·4, we will give estimates for $I(R_1)$ and $I(R_2)$, respectively. Here we take the trivial estimates for $\Delta(R_1)$ and $\Delta(R_2)$ coming from Proposition 6·1. In R_3, we loosely estimate $I(R_3)$ in Lemma 10·2 and carefully bound $\Delta(R_3)$ in Lemma 10·5. Combining these estimates yields the desired error term in Proposition 6·4.

We start with some simple upper bounds for F.

LEMMA 10·1. *For $w \in \mathbb{C}$ with $0 < \mathrm{Re}(w) \le N$, we have*

$$|F(w)| \ll \begin{cases} \dfrac{1}{|w|} & \text{if } |\mathrm{Im}(w)| \le \pi N, \\ \dfrac{1}{|w - 2\pi i N|} & \text{if } \pi N \le \mathrm{Im}(w) \le 2\pi N, \\ \dfrac{1}{|w + 2\pi i N|} & \text{if } -2\pi N \le \mathrm{Im}(w) \le -\pi N. \end{cases}$$

Proof. Note that the function

$$\frac{w}{N(1 - e^{-w/N})}$$

is holomorphic on an open set containing $R = \{w \in \mathbb{C} \mid |\mathrm{Im}(w)| \le \pi N, \ 0 \le \mathrm{Re}(w) \le N\}$ since the singularity at 0 is removable. Making the substitution $w \mapsto N \cdot w$, we see that it suffices to show that $w/(1 - e^{-w})$ is bounded on $\tilde{R} = \{w \in \mathbb{C} \mid |\mathrm{Im}(w)| \le \pi, \ 0 \le \mathrm{Re}(w) \le 1\}$. This follows immediately since the above expression is holomorphic on an open set containing $\tilde{R}$. One uses the same argument in the other cases.

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

We will also need the following estimate:

LEMMA 10·2.

$$I([-\pi N, \pi N]^{2k-1}) \ll_k (\log N)^k.$$

Proof. For fixed $i \in \{2, \dots, k\}$, we use Hölder's inequality and the previous lemma to obtain

$$\begin{aligned}\int_{-\pi N}^{\pi N} \prod_{j=k+1}^{2k} |F(z_i + z_j)| d\theta_i &\leq \prod_{j=k+1}^{2k} \Big(\int_{-\pi N}^{\pi N} |F(z_i + z_j)|^k d\theta_i \Big)^{1/k} \\ &\ll_k \prod_{j=k+1}^{2k} \Big(\int_{|\theta_i+\theta_j| \leq \pi N} \frac{1}{|z_i + z_j|^k} d\theta_i \\ &\quad + \int_{-2\pi N \leq \theta_i+\theta_j \leq -\pi N} \frac{1}{|z_i + z_j + 2\pi i N|^k} d\theta_i \\ &\quad + \int_{\pi N \leq \theta_i+\theta_j \leq 2\pi N} \frac{1}{|z_i + z_j - 2\pi i N|^k} d\theta_i \Big)^{1/k}.\end{aligned}$$

Upon applying the inequality $1/|w| \leq \sqrt{2}/(\mathrm{Re}(w) + |\mathrm{Im}(w)|)$ with $\mathrm{Re}(w) > 0$, we have that the above is

$$\begin{aligned}&\ll \prod_{j=k+1}^{2k} \Big(\int_{\mathbb{R}} \frac{1}{(c_i + c_j + |\theta_i + \theta_j|)^k} d\theta_i + \int_{\mathbb{R}} \frac{1}{(c_i + c_j + |\theta_i + \theta_j + 2\pi N|)^k} d\theta_i \\ &\quad + \int_{\mathbb{R}} \frac{1}{(c_i + c_j + |\theta_i + \theta_j - 2\pi N|)^k} d\theta_i \Big)^{1/k},\end{aligned}$$

and this is clearly bounded by a constant independent of N for $k \geq 2$. (Recall that we made this assumption at the very beginning of Section 6.) Thus,

$$\begin{aligned}I([-\pi N, \pi N]^{2k-1}) &\ll_k \int_{-\pi N}^{\pi N} \cdots \int_{-\pi N}^{\pi N} \prod_{j=k+1}^{2k} |F(z_j)| d\theta_{k+1} \cdots d\theta_{2k} \\ &= \prod_{j=k+1}^{2k} \int_{-\pi N}^{\pi N} |F(z_j)| d\theta_j \\ &\ll \prod_{j=k+1}^{2k} \int_0^{\pi N} \frac{1}{c_j + \theta_j} d\theta_j \\ &\ll \prod_{j=k+1}^{2k} \log N = (\log N)^k.\end{aligned}$$

The next few lemmas estimate different regions of the integral I. Let $2 \leq X \leq N/10$ be a parameter. Define the set $\mathfrak{S}(X) \subseteq [-\pi N, \pi N]^{2k-1}$ by

$$\{(\theta_2, \dots, \theta_{2k}) \in [-\pi N, \pi N]^{2k-1} \mid |z_i + z_j| \leq X \text{ for } 2 \leq i \leq k,\ k+1 \leq j \leq 2k\}. \qquad (10·2)$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

We begin by estimating the contribution outside $\mathfrak{S}(X)$.

LEMMA 10·3.

$$I([-\pi N, \pi N]^{2k-1} \setminus \mathfrak{S}(X)) \ll_k \frac{(\log N)^{2k-1}}{X^{1-1/k}} + (\log N)^{2k-2}\frac{X}{N}.$$

Proof. Let $\Omega := \{2, \dots, k\} \times \{k+1, \dots, 2k\}$ with $|\Omega| = k(k-1)$. We say a k-partition $\Lambda_1 \sqcup \Lambda_2 \sqcup \cdots \sqcup \Lambda_k$ of Ω is *weak* if we allow $\Lambda_i = \varnothing$. For every weak 3-partition $\Lambda = (\Lambda_1, \Lambda_2, \Lambda_3)$ of Ω, define the region $R_\Lambda(X)$ to be the set

$$\left\{ (\theta_2, \dots, \theta_{2k}) \in [-\pi N, \pi N]^{2k-1} \;\middle|\; \begin{array}{cc} |z_i+z_j| \le X & \forall\, (i,j) \in \Lambda_1, \\ |z_i+z_j-2\pi iN| \le X \text{ or } |z_i+z_j+2\pi iN| \le X & \forall\, (i,j) \in \Lambda_2, \\ |z_i+z_j| > X \text{ and } |z_i+z_j \pm 2\pi iN| > X & \forall\, (i,j) \in \Lambda_3 \end{array} \right\}.$$

It is easy to see that $[-\pi N, \pi N]^{2k-1}$ is partitioned by $\{R_\Lambda \mid \Lambda \text{ a weak 3-partition of } \Omega\}$ and that $\mathfrak{S}(X) = R_{(\Omega,\varnothing,\varnothing)}(X)$. We further define two projection maps $\pi_i,\ i = 1, 2$ which respectively return the first and second components of a pair of integers, that is, $\pi_1(a, b) = a$ and $\pi_2(a, b) = b$ for $a, b \in \mathbb{Z}$.

It now suffices to prove that

$$I(R_\Lambda(X)) \ll_k \frac{(\log N)^{2k-1-|\pi_2(\Lambda_2)|}}{X^{|\Lambda_3|(1-1/k)}} \left(\frac{X}{N}\right)^{|\pi_2(\Lambda_2)|}, \tag{10·3}$$

because if $\Lambda_2 \neq \varnothing$, then the RHS of the above expression is $\ll_k (\log N)^{2k-2}X/N$. If, on the other hand, $\Lambda_3 \neq \varnothing$, then the RHS is $\ll_k (\log N)^{2k-1}/X^{1-1/k}$, and, since $\mathfrak{S}(X) = R_{(\Omega,\varnothing,\varnothing)}(X)$, at least one of these two cases must occur. Now, fix a weak partition Λ of Ω and write $R_\Lambda := R_\Lambda(X)$. For $(\theta_2, \dots, \theta_{2k}) \in R_\Lambda$, notice that

$$\prod_{i=2}^{k} \prod_{j=k+1}^{2k} |F(z_i + z_j)| \ll_k \frac{1}{X^{|\Lambda_3|}}$$

by assumption and Lemma 10·1. Hence,

$$I(R_\Lambda) \ll_k \frac{1}{X^{|\Lambda_3|(1-1/k)}} \int_{R_\Lambda} \cdots \int \prod_{i=2}^{k} \prod_{j=k+1}^{2k} |F(z_i + z_j)|^{\frac{1}{k}} \prod_{j=k+1}^{2k} |F(z_j)|\, d\theta_2 \cdots d\theta_{2k}.$$

Further note that $R_\Lambda \subset [-\pi N, \pi N]^{k-1} \times \tilde{R}_\Lambda$ where

$$\tilde{R}_\Lambda := \{(\theta_{k+1}, \dots, \theta_{2k}) \in [-\pi N, \pi N]^k \;\big|\; \pi N - X \le |\theta_j| \le \pi N \quad \forall\, j \in \pi_2(\Lambda_2)\}.$$

This inclusion holds because if we had $|\theta_j| < \pi N - X$ for $(i, j) \in \Lambda_2$, then

$$|z_i + z_j \pm 2\pi iN| \ge \big||\theta_i + \theta_j| - 2\pi N\big| \ge 2\pi N - |\theta_i| - |\theta_j| > 2\pi N - \pi N + X - \pi N = X.$$

Consequently, the above gives

$$I(R_\Lambda) \ll_k \frac{1}{X^{|\Lambda_3|(1-1/k)}} \int_{[-\pi N,\pi N]^{k-1} \times \tilde{R}_\Lambda} \cdots \int \prod_{i=2}^{k} \prod_{j=k+1}^{2k} |F(z_i + z_j)|^{\frac{1}{k}} \prod_{j=k+1}^{2k} |F(z_j)|\, d\theta_2 \cdots d\theta_{2k}.$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

By Hölder's inequality,

$$\prod_{i=2}^{k}\int_{-\pi N}^{\pi N}\prod_{j=k+1}^{2k}|F(z_i+z_j)|^{\frac{1}{k}}d\theta_i \le \prod_{i=2}^{k}\prod_{j=k+1}^{2k}\Big(\underbrace{\int_{-\pi N}^{\pi N}|F(z_i+z_j)|d\theta_i}_{\ll \log N}\Big)^{\frac{1}{k}} \ll (\log N)^{k-1}.$$

Finally, we obtain

$$\begin{aligned} I(R_\Lambda) &\ll_k \frac{(\log N)^{k-1}}{X^{|\Lambda_3|(1-1/k)}}\int\cdots\int_{\tilde{R}_\Lambda}\prod_{j=k+1}^{2k}|F(z_j)|d\theta_{k+1}\cdots d\theta_{2k} \\ &\ll_k \frac{(\log N)^{k-1}}{X^{|\Lambda_3|(1-1/k)}}\prod_{j\notin\pi_2(\Lambda_2)}\underbrace{\int_{-\pi N}^{\pi N}|F(z_j)|d\theta_j}_{\ll\log N}\prod_{j\in\pi_2(\Lambda_2)}\Big(\int_{-\pi N}^{-\pi N+X}+\int_{\pi N-X}^{\pi N}\Big)\underbrace{|F(z_j)|}_{\ll\frac{1}{N}}d\theta_j \\ &\ll \frac{(\log N)^{2k-1-|\pi_2(\Lambda_2)|}}{X^{|\Lambda_3|(1-1/k)}}\Big(\frac{X}{N}\Big)^{|\pi_2(\Lambda_2)|}. \end{aligned}$$

Thus, we have shown (10·3).

Let $10X \le Y \le N$ be a parameter. Define the region $\mathfrak{S}(X,Y)\subseteq\mathfrak{S}(X)$ to be the set

$$\left\{(\theta_2,\dots,\theta_{2k})\in[-\pi N,\pi N]^{2k-1}\;\middle|\;\begin{array}{ll}|z_i+z_j|\le X & \forall\ 2\le i\le k,\ k+1\le j\le 2k,\\ |z_j|\le Y & \forall\ k+1\le j\le 2k\end{array}\right\}. \tag{10·4}$$

LEMMA 10·4. *We have*

$$I(\mathfrak{S}(X)\setminus\mathfrak{S}(X,Y))\ll_k\Big(\frac{X}{Y}\Big)^{k-1}.$$

Proof. For $l\in\{k+1,\dots,2k\}$, we define

$$\mathfrak{T}_l(X,Y):=\left\{(\theta_2,\dots,\theta_{2k})\in[-\pi N,\pi N]^{2k-1}\;\middle|\;\begin{array}{ll}|z_i+z_j|\le X & \forall\ 2\le i\le k,\ k+1\le j\le 2k,\\ |z_l|>Y & \end{array}\right\}.$$

We then have $\mathfrak{S}(X)\setminus\mathfrak{S}(X,Y)\subset\bigcup_{l=k+1}^{2k}\mathfrak{T}_l(X,Y)$, and it suffices to prove

$$I(\mathfrak{T}_l(X,Y))\ll_k\Big(\frac{X}{Y}\Big)^{k-1}\quad\forall\ l=k+1,\dots,2k.$$

We claim that

$$\mathfrak{T}_l(X,Y)\subset[-\pi N,\pi N]^{k-1}\times\tilde{\mathfrak{T}}_l(X,Y),$$

where

$$\tilde{\mathfrak{T}}_l(X,Y):=\left\{(\theta_2,\dots,\theta_{2k})\in[-\pi N,\pi N]^{2k-1}\;\middle|\;\begin{array}{ll}|\theta_j-\theta_l|\le 2X & \forall\ k+1\le j\le 2k,\\ |\theta_l|\ge Y/2 & \end{array}\right\}.$$

To prove this, let $(\theta_2,\dots,\theta_{2k})\in\mathfrak{T}_l(X,Y)$. As $|z_l|>Y$, it follows that

$$|\theta_l|\ge Y-|c_l|\ge Y-\frac{3}{4}\ge Y-\frac{X}{2}\ge\frac{Y}{2}.$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

By the triangle inequality, we also have

$$|\theta_j - \theta_l| \le |z_j - z_l| \le |z_j + z_2| + |z_2 + z_l| \le 2X.$$

This proves the claim. Therefore,

$$\begin{aligned} I(\mathfrak{T}_l(X,Y)) &\le I([-\pi N, \pi N]^{k-1} \times \tilde{\mathfrak{T}}_l(X,Y)) \\ &= \int \cdots \int_{\tilde{\mathfrak{T}}_l(X,Y)} \Big(\underbrace{\int_{-\pi N}^{\pi N} \cdots \int_{-\pi N}^{\pi N} \prod_{i=2}^{k} \prod_{j=k+1}^{2k} |F(z_i + z_j)| d\theta_i}_{\ll_k 1 \text{ by Hölder as in (Lemma 10·2)}} \Big) \prod_{j=k+1}^{2k} |F(z_j)| \, d\theta_{k+1} \cdots d\theta_{2k} \\ &\ll_k \int \cdots \int_{\tilde{\mathfrak{T}}_l(X,Y)} \prod_{j=k+1}^{2k} |F(z_j)| \, d\theta_{k+1} \cdots d\theta_{2k} \\ &\ll_k \int_{\frac{Y}{2} \le |\theta_l| \le \pi N} \Big(\prod_{\substack{j=k+1 \\ j \ne l}}^{2k} \int_{|\theta_j - \theta_l| \le 2X} |F(z_j)| \, d\theta_j \Big) |F(z_l)| \, d\theta_l. \end{aligned}$$

Note that for $j \ne l$, $|F(z_j)| \ll |\theta_j|^{-1} \ll |\theta_l|^{-1}$ where the first bound follows from Lemma 10·1 and the second from

$$|\theta_j| \ge |\theta_l| - |\theta_j - \theta_l|$$

and

$$|\theta_j - \theta_l| \le 2X \le \frac{Y}{5} \le \frac{|\theta_l|}{2}.$$

Furthermore, the length of the interval of integration for each j is $O(X)$. Thus,

$$\begin{aligned} I(\mathfrak{T}_l(X,Y)) &\ll_k \int_{|\theta_l| \ge \frac{Y}{2}} \Big(\underbrace{|F(z_l)|}_{\ll \frac{1}{|\theta_l|}} \prod_{\substack{j=k+1 \\ j \ne l}}^{2k} \frac{X}{|\theta_l|} d\theta_l \Big) \\ &\ll_k \int_{|\theta_l| \ge \frac{Y}{2}} \frac{X^{k-1}}{|\theta_l|^k} d\theta_l \ll_k \Big(\frac{X}{Y} \Big)^{k-1}. \end{aligned}$$

This proves the lemma.

For the remaining region $\mathfrak{S}(X,Y)$, we estimate trivially

$$I(\mathfrak{S}(X,Y)) \ll_k (\log N)^k.$$

Here, our savings will come from the fact that the difference

$$B\left(q^{-1/2}, q^{-1/2} e^{(c_2 + i\theta_2)/N}, \ldots, q^{-1/2} e^{(c_{2k} + i\theta_{2k})/N}\right) - b_k(q)$$

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

is small on this region, where all of the exponents $z_i + z_j$ and z_j are small. The next lemma makes this precise. Recall the definition of $\Delta(R)$ from equation (10·1) for any Lebesgue-measurable region R of $[-\pi N, \pi N]^{2k-1}$:

$$\Delta(R) := \sup_{(\theta_2,\dots,\theta_{2k})\in R} \left| B\left(q^{-1/2}, q^{-1/2}e^{(c_2+i\theta_2)/N}, \dots, q^{-1/2}e^{(c_{2k}+i\theta_{2k})/N}\right) - b_k(q)\right|.$$

LEMMA 10·5. *We have*

$$\Delta([-\pi N, \pi N]^{2k-1}) \ll_k \frac{1}{q},$$

and

$$\Delta(\mathfrak{S}(X, Y)) \ll_k \frac{Y}{qN}.$$

Proof. Note that the first bound is an immediate consequence of Proposition 6·1 and

$$\max_{-\pi N\le\theta_i\le N\pi} |e^{c_i/N+i\theta_i/N} - 1| \ll 1.$$

If we have $(\theta_2, \dots, \theta_{2k}) \in \mathfrak{S}(X, Y)$, then $|\theta_i| \le 2Y$ for all $i = 2, \dots, 2k$. Thus, by Proposition 6·1, it again suffices to show that

$$\max_{(\theta_2,\dots,\theta_{2k})\in\mathfrak{S}(X,Y)} ||(q^{-1/2}e^{c_2/N+i\theta_2/N}, \dots, q^{-1/2}e^{c_{2k}/N+i\theta_{2k}/N}) - (q^{-1/2}, \dots, q^{-1/2})||_\infty \ll \frac{Y}{\sqrt{q}N}.$$

Using $|\theta_i| \le 2Y$, we can simplify this statement to

$$\max_{-2Y\le\theta_i\le 2Y} |e^{c_i/N+i\theta_i/N} - 1| \ll \frac{Y}{N} \tag{10·5}$$

for each i. Recalling that for bounded $z \in \mathbb{C}$, we have $|e^z - 1 \ll |z|$, we conclude

$$\begin{aligned} |e^{c_i/N+i\theta_i/N} - 1| &= |e^{c_i/N+i\theta_i/N} - e^{i\theta_i/N} + e^{i\theta_i/N} - 1| \\ &\le |e^{c_i/N} - 1| + |e^{i\theta_i/N} - 1| \\ &\ll_{c_i} \frac{1}{N}(1 + |\theta|). \end{aligned}$$

We now take the maximum over $-2Y \le \theta \le 2Y$ to establish (10·5).

Thus, we obtain the desired bound on the integral $\widetilde{J}_k$:

$$|\widetilde{J}_k| \ll_k \frac{1}{q}\frac{(\log N)^{2k-1}}{X^{1-1/k}} + \frac{1}{q}(\log N)^{2k-2}\frac{X}{N} + \frac{1}{q}\left(\frac{X}{Y}\right)^{k-1} + \frac{Y}{qN}(\log N)^k.$$

The first two terms are a consequence of estimating $I(R_1)$ using Lemma 10·3 and taking the trivial $1/q$ estimate for $\Delta(R_1)$. The third term makes use of Lemma 10·4 to bound $I(R_2)$ and uses the same estimate for $\Delta(R_2)$. Lastly, the fourth term comes from upper bounding $I(R_3)$ by $I([-\pi N, \pi N]^{2k-1})$ and using Lemma 10·5 to bound $\Delta(R_3)$. This completes the proof of Proposition 6·4 and thus the proof of Theorem 1·1.

Acknowledgements. The authors were participants in the Fields Undergraduate Summer Research Program 2023 and are deeply grateful to the Fields Institute for its support. We are

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

thankful to Ofir Gorodetsky for many insightful mathematical and historical remarks on an earlier version of the paper, which improved the exposition and noted our proof gave better q-dependence in Theorem 1·1 than we had initially stated. We also thank Andrew Granville, Winston Heap and the anonymous referee for many helpful comments and their encouragement. AZ was partially supported by NSERC grant RGPIN-2022-04982.

REFERENCES

[ASV+22] D. AGGARWAL, U. SUBEDI, W. VERREAULT, A. ZAMAN and C. ZHENG. Sums of random multiplicative functions over function fields with few irreducible factors. *Math. Proc. Camb. Phil. Soc.* **173**(3) (2022), 715–726.

[ACZ96] A. AYYAD, T. COCHRANE and Z. ZHENG. The congruence $x_1x_2 \equiv x_3x_4 \pmod p$, the equation $x_1x_2 = x_3x_4$, and mean values of character sums. *J. Number Theory* **59**(2) (1996), 398–413.

[BS16] A. BONDARENKO and K. SEIP. Helson's problem for sums of a random multiplicative function. *Mathematika* **62**(1) (2016), 101–110.

[Cai23] R. CAICH. Almost sure upper bound for random multiplicative functions. Preprint: ArXiv:2304.00943 (2023).

[CS12] S. CHATTERJEE and K. SOUNDARARAJAN. Random multiplicative functions in short intervals. *Int. Math. Res. Not. IMRN* **3** (2012), 479–492.

[CG06] B. CONREY and A. GAMBURD. Pseudomoments of the Riemann zeta-function and pseudo-magic squares. *J. Number Theory* **117**(2) (2006), 263–278.

[CSWZ98] S. CORTEEL, C. D. SAVAGE, H. S. WILF and D. ZEILBERGER. A pentagonal number sieve. *J. Combin. Theory Ser. A* **82**(2) (1998), 186–192.

[Ehr77] E. EHRHART. *Polynômes Arithmétiques et Méthode des Polyèdres en Combinatoire. Internat. Ser. Numer. Math.* vol. 35. Birkhäuser Verlag, Basel-Stuttgart (1977).

[Gor24] O. GORODETSKY. Magic squares, the symmetric group and Möbius randomness. *Monatsh. Math.* **204**(1) (2024), 27–46.

[GW24] O. GORODETSKY and M. DICK WONG. Martingale central limit theorem for random multiplicative functions. Preprint: ArXiv:2405.20311 (2024).

[GW25] O. GORODETSKY and M. DICK WONG. A short proof of Helson's conjecture. *Bull. London Math. Soc*. **57**(4) (2025), 1065–1076.

[GHS15] A. GRANVILLE, A. J. HARPER and K. SOUNDARARAJAN. Mean values of multiplicative functions over function fields. *Res. Number Theory* **1**(25) (2015), 18 pages.

[GS01] A. GRANVILLE and K. SOUNDARARAJAN. Soundararajan. Large character sums. *J. Amer. Math. Soc.* **14**(2) (2001), 365–397.

[Har24a] S. HARDY. Almost sure bounds for a weighted Steinhaus random multiplicative function. *J. London Math. Soc. (2)* **110**(3), (e12979), (2024), 27 pages.

[Har24b] S. HARDY. Bounds for exponential sums with random multiplicative coefficient. *Int. Math. Res. Not. IMRN* (22) (2024), 14138–14156.

[Har13] A. J. HARPER. On the limit distributions of some sums of a random multiplicative function. *J. Reine Angew. Math.* **678** (2013), 95–124.

[Har19] A. J. HARPER. Moments of random multiplicative functions, II: High moments. *Algebra Number Theory* **13**(10) (2019), 2277–2321.

[Har20] A. J. HARPER. Moments of random multiplicative functions, I: Low moments, better than squareroot cancellation, and critical multiplicative chaos. *Forum Math. Pi* **8** (e1) (2020), 95 pages.

[Har23] A. J. HARPER. Almost sure large fluctuations of random multiplicative functions. *Int. Math. Res. Not. IMRN* (3) (2023), 2095–2138.

[HNR15] A. J. HARPER, A. NIKEGHBALI and M. RADZIWI. A note on Helson's conjecture on moments of random multiplicative functions. In *Analytic Number Theory* (Springer, Cham, 2015), pp. 145–169.

[HL16] W. P. HEAP and S. LINDQVIST. Moments of random multiplicative functions and truncated characteristic polynomials. *Q. J. Math.* **67**(4) (2016), 683–714.

[HJL16] U. HELMKE, J. JORDAN and J. LIEB. Probability estimates for reachability of linear systems defined over finite fields. *Adv. Math. Commun.* **10**(1) (2016), 63–78.

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press

[Hou11] B. HOUGH. Summation of a random multiplicative function on numbers having few prime factors. *Math. Proc. Cambridge Phil. Soc.* **150**(2) (2011), 193–214.

[KSX23] O. KLURMAN, I. D. SHKREDOV and M. W. XU. On the random Chowla conjecture. *Geom. Funct. Anal.* **33**(3) (2023), 749–777.

[LTW13] Y.-K. LAU, G. TENENBAUM and J. WU. On mean values of random multiplicative functions. *Proc. Amer. Math. Soc.* **141**(2) (2013), 409–420.

[Mas22] D. MASTROSTEFANO. An almost sure upper bound for random multiplicative functions on integers with a large prime factor. *Electron. J. Probab.* **27**(22) (2022), 21 pages.

[MV07] H. L. MONTGOMERY and R. C. VAUGHAN. *Multiplicative Number Theory. I. Classical Theory*. Cambridge Studies in Advanced Math. vol 97 (Cambridge University Press, Cambridge, 2007).

[NPS23] J. NAJNUDEL, E. PAQUETTE and N. SIMM. Secular coefficients and the holomorphic multiplicative chaos. *The Annals of Probability*. **51**(4) (2023), 1193–1248.

[PWX24] M. PANDEY, V. Y. WANG and M. W. XU. Partial sums of typical multiplicative functions over short moving intervals. *Algebra Number Theory* **18**(2) (2024), 389–408.

[Shi08] S. SHI. On the equation $n_1n_2 = n_3n_4$ and mean value of character sums. *J. Number Theory* **128**(2) (2008), 313–321.

[SX23] K. SOUNDARARAJAN and M. W. XU. Central limit theorems for random multiplicative functions. *J. Anal. Math.* **151**(1) (2023), 343–374.

[VW95] R. C. VAUGHAN and T. D. WOOLEY. On a certain nonary cubic form and related equations. *Duke Math. J.* **80**(3) (1995), 669–735.

[Win44] A. WINTNER. Random factorisations and Riemann's hypothesis. *Duke Math. J.* **11** (1944), 267–275.

[Xu24] M. W. XU. Better than square-root cancellation for random multiplicative functions. *Trans. Amer. Math. Soc. Ser. B* **11** (2024), 482–507.

https://doi.org/10.1017/S0305004125101321 Published online by Cambridge University Press