Math. Z. (2018) 288:167–198
https://doi.org/10.1007/s00209-017-1884-1

Mathematische Zeitschrift

Sums of divisor functions in $\mathbb{F}_q[t]$ and matrix integrals

J. P. Keating[1] · B. Rodgers[2] · E. Roditty-Gershon[1] · Z. Rudnick[3]

Received: 6 March 2017 / Accepted: 6 March 2017 / Published online: 28 March 2017
© Springer-Verlag Berlin Heidelberg 2017

Abstract We study the mean square of sums of the kth divisor function $d_k(n)$ over short intervals and arithmetic progressions for the rational function field over a finite field of q elements. In the limit as $q \to \infty$ we establish a relationship with a matrix integral over the unitary group. Evaluating this integral enables us to compute the mean square of the sums of $d_k(n)$ in terms of a lattice point count. This lattice point count can in turn be calculated in terms of a certain piecewise polynomial function, which we analyse. Our results suggest general conjectures for the corresponding classical problems over the integers, which agree with the few cases where the answer is known.

JPK gratefully acknowledges support under EPSRC Programme Grant EP/K034383/1 LMF: L-Functions and Modular Forms, a grant from Leverhulme Trust, a Royal Society Wolfson Merit Award, a Royal Society Leverhulme Senior Research Fellowship, and by the Air Force Office of Scientific Research, Air Force Material Command, USAF, under grant number FA8655-10-1-3088. ZR is similarly grateful for support from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007–2013)/ERC Grant Agreement No. 320755, and from the Israel Science Foundation (Grant No. 925/14).

✉ J. P. Keating
j.p.keating@bristol.ac.uk

B. Rodgers
rbrad@umich.edu

E. Roditty-Gershon
er14265@bristol.ac.uk

Z. Rudnick
rudnick@post.tau.ac.il

1 School of Mathematics, University of Bristol, Bristol BS8 1TW, UK

2 Department of Mathematics, University of Michigan, 530 Church St., Ann Arbor, MI 48109, USA

3 Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, 69978 Tel Aviv, Israel

1 Introduction

The goal of this paper is to study the mean square of sums of divisor functions over short intervals, for the rational function field over a finite field, and to use the results obtained to gain insight into the corresponding classical problem over the integers.

1.1 Classical theory

The k-th divisor function $d_k(n)$ gives the number of ways of writing a (positive) integer as a product of k positive integers:

$$d_k(n) := \#\{(a_1, \dots, a_k) : n = a_1 \cdot \dots \cdot a_k, \quad a_1, \dots, a_k \geq 1\}, \tag{1.1}$$

the classical divisor function being $d(n) = d_2(n)$.

Dirichlet's divisor problem addresses the size of the remainder term $\Delta_2(x)$ in partial sums of the divisor function

$$\Delta_2(x) := \sum_{n \leq x} d_2(n) - x\Big(\log x + (2\gamma - 1)\Big), \tag{1.2}$$

where γ is the Euler–Mascheroni constant. For the higher divisor functions one defines a remainder term $\Delta_k(x)$ similarly as the difference between the partial sums $\sum_{n \leq x} d_k(n)$ and a smooth term $x P_{k-1}(\log x)$ where $P_{k-1}(u)$ is a certain polynomial of degree $k-1$; see, for example, [39] Chapter XII.

The mean square of $\Delta_k(x)$ was computed by Crámer [10] for $k = 2$, and by Tong [40] for $k \geq 3$ (assuming the Riemann Hypothesis (RH) if $k \geq 4$), to be

$$\frac{1}{X} \int_X^{2X} \Delta_k(x)^2 dx \sim c_k X^{1-\frac{1}{k}}, \tag{1.3}$$

for a certain constant[1] c_k. Heath-Brown [18] showed that $\Delta_k(x)/x^{\frac{1}{2}-\frac{1}{2k}}$ has a limiting value distribution (for $k \geq 4$ one needs to assume RH); it is non-Gaussian.

1.2 The divisor function in short intervals

Let

$$\Delta_k(x; H) = \Delta_k(x + H) - \Delta_k(x) \tag{1.4}$$

be the remainder term for sums of d_k over short intervals $[x, x + H]$. Our main concern is to understand its mean square.

For relatively long intervals, Lester [30] proves an asymptotic (assuming RH for $k > 3$) similar to the result (1.3):

$$\frac{1}{X} \int_X^{2X} \Big(\Delta_k(x, H)\Big)^2 dx \sim 2c_k X^{1-\frac{1}{k}}, \quad X^{1-\frac{1}{k}+o(1)} < H < X^{1-o(1)}. \tag{1.5}$$

The interesting range for us is that of shorter intervals: $H < X^{1-\frac{1}{k}}$. For $k = 2$, Jutila [21], Coppola and Salerno [9], and Ivić [19,20] show that, for $X^{\epsilon} < H < X^{1/2-\epsilon}$, the mean

[1] Adapted to our averaging method, Tong's constant is $c_k = \frac{2^{2-1/k}-1}{(4k-2)\pi^2} \sum_{n=1}^{\infty} \frac{d_k(n)^2}{n^{1+\frac{1}{k}}}$.

square of $\Delta_2(x, H)$ is asymptotically equal to

$$\frac{1}{X}\int_X^{2X}\Big(\Delta_2(x,H)\Big)^2 dx \sim H F_3\left(\log\frac{X^{1/2}}{H}\right) \tag{1.6}$$

for a certain cubic polynomial F_3. In that regime, Lester and Yesha [31] showed that $\Delta_2(x, H)$, normalized to have unit mean-square using (1.6), has a Gaussian value distribution, at least for a narrow range of H below $X^{1/2}$, the conjecture being that this should hold for $X^\epsilon < H < X^{1/2-\epsilon}$ for any $\epsilon > 0$.

For $k \geq 3$, Milinovich and Turnage-Butterbaugh [32, p. 182] give an upper bound, assuming RH, of

$$\frac{1}{X}\int_X^{2X}\Big(\Delta_k(x,H)\Big)^2 dx \ll H(\log X)^{k^2+o(1)}\,, \quad X^\epsilon < H < X^{1-\epsilon} \tag{1.7}$$

In concurrent work, Lester [30] shows that for $k \geq 3$, assuming the Lindelöf Hypothesis, if $h(x) = (\frac{x}{X})^{1-\frac{1}{k}} X^\delta$,

$$\frac{1}{X}\int_X^{2X}\Big(\Delta_k(x,h(x))\Big)^2 dx \sim a_k \cdot \frac{k^{k^2-1}}{\Gamma(k^2)}\left(1-\frac{1}{k}-\delta\right)^{k^2-1} \cdot \frac{2^{2-\frac{1}{k}}-1}{2-\frac{1}{k}} X^\delta \cdot (\log X)^{k^2-1}, \tag{1.8}$$

provided $1-\frac{1}{k-1} < \delta < 1-\frac{1}{k}$, where

$$a_k = \prod_p \left\{\left(1-\frac{1}{p}\right)^{k^2}\sum_{j=0}^{\infty}\left(\frac{\Gamma(k+j)}{\Gamma(k)j!}\right)^2\frac{1}{p^j}\right\} = \prod_p\left\{\left(1-\frac{1}{p}\right)^{(k-1)^2}\sum_{j=0}^{k-1}\binom{k-1}{j}^2 p^{-j}\right\}. \tag{1.9}$$

For $k = 3$ and $\frac{7}{12} < \delta < \frac{2}{3}$, the result is unconditional.

1.3 A conjecture

We did not find any conjecture in the literature for the order of growth of the mean-square of $\Delta_k(x; H)$ for small H. Based on Theorems 1.4 and 1.5, we believe the following:

Conjecture 1.1 *If $0 < \delta < 1-\frac{1}{k}$ is fixed, then for $H = X^\delta$,*

$$\frac{1}{X}\int_X^{2X}\Big(\Delta_k(x,H)\Big)^2 dx \sim a_k \mathcal{P}_k(\delta) H(\log X)^{k^2-1}\,, \quad X \to \infty \tag{1.10}$$

where a_k is given by (1.9), and $\mathcal{P}_k(\delta)$ is a piecewise polynomial function of δ, of degree k^2-1, given by

$$\mathcal{P}_k(\delta) = (1-\delta)^{k^2-1}\gamma_k\left(\frac{1}{1-\delta}\right). \tag{1.11}$$

Here

$$\gamma_k(c) = \frac{1}{k!\,G(1+k)^2}\int_{[0,1]^k}\delta_c(w_1+\cdots+w_k)\prod_{i<j}(w_i-w_j)^2\,d^k w, \tag{1.12}$$

where $\delta_c(x) = \delta(x-c)$ is the delta distribution translated by c, and G is the Barnes G-function, so that for positive integers k, $G(1+k) = 1!\cdot 2!\cdot 3!\cdots(k-1)!$.

For $1-\frac{1}{k-1}<\delta<1-\frac{1}{k}$, (1.11) reduces to the simpler form

$$\mathcal{P}_k(\delta)=\frac{k^{k^2-1}}{(k^2-1)!}\left(1-\frac{1}{k}-\delta\right)^{k^2-1}, \tag{1.13}$$

rendering visible the compatibility of Conjecture 1.1 with Lester's result (1.8), which corresponds to taking $H=X^\delta$, with δ in this range. Note that in (1.8), the length of the interval $h(x)=(\frac{x}{X})^{1-\frac{1}{k}}X^\delta$ varies with x, and this slight difference in conventions is responsible for the factor of $\frac{2^{2-\frac{1}{k}}-1}{2-\frac{1}{k}}$ in (1.8), since the mean value of $h(x)$ over $[X,2X]$ is

$$\frac{1}{X}\int_X^{2X}h(x)dx=\frac{2^{2-\frac{1}{k}}-1}{2-\frac{1}{k}}X^\delta. \tag{1.14}$$

We also note that in the restricted range $0\le\delta\le 1/2$, this conjecture and the polynomial $\mathcal{P}_k(\delta)$ may be seen to be closely connected to a conjecture regarding the mean values of Dirichlet polynomials made by Conrey and Gonek (Conjecture 4 of [6]).

As will be explained later, $\gamma_k(c)$ is a piecewise polynomial function of c, satisfying $\gamma_k(c)=\gamma_k(k-c)$, that relates to the asymptotics of a lattice counting problem (Theorem 1.4). This lattice counting problem itself emerges from the evaluation of a matrix integral over the unitary group. We also note that it is possible to write down conjectures for the lower order terms in the asymptotic expansion (1.1): the right-hand side is, up to terms that are $o(1)$, a polynomial in $\log X$ whose coefficients can be computed. This is explained in Sect. 5.

1.4 Divisor functions in $\mathbb{F}_q[x]$

We study the problem of the sum of divisor functions $d_k(f)$ over short intervals for $\mathbb{F}_q[x]$. The divisor functions $d_k(f)$ for a monic polynomial f are defined in analogy to (1.1) and give the number of decompositions $f=f_1f_2\cdots f_k$ with f_i monic. In particular $d_2=d$ is the classical divisor function.

We denote by $\mathcal{M}_n$ the set of monic polynomials of degree n. A "short interval" in $\mathbb{F}_q[x]$ is a set of the form

$$I(A;h)=\{f:||f-A||\le q^h\} \tag{1.15}$$

where $A\in\mathcal{M}_n$ has degree n, $0\le h\le n-2$ and the norm is

$$||f||:=\#\mathbb{F}_q[t]/(f)=q^{\deg f}. \tag{1.16}$$

The cardinality of such a short interval is

$$\#I(A;h)=q^{h+1}=:H. \tag{1.17}$$

Set

$$\mathcal{N}_{d_k}(A;h):=\sum_{f\in I(A;h)}d_k(f). \tag{1.18}$$

The mean value is (c.f. [1])

$$\frac{1}{q^n}\sum_{A\in\mathcal{M}_n}\mathcal{N}_{d_k}(A;h)=\frac{q^{h+1}}{q^n}\sum_{f\in\mathcal{M}_n}d_k(f)=q^{h+1}\binom{n+k-1}{k-1}. \tag{1.19}$$

In analogy with (1.2) and (1.4) we set

$$\Delta_k(A;h) := \mathcal{N}_{d_k}(A;h) - q^{h+1}\binom{n+k-1}{k-1}. \tag{1.20}$$

We will show below (Theorem 1.2) that

$$\mathcal{N}_{d_k}(A;h) = q^{h+1}\binom{n+k-1}{k-1}, \quad h > \left(1-\frac{1}{k}\right)n-1 \tag{1.21}$$

so that $\Delta_k(A;h) = 0$ for $h > (1-\frac{1}{k})n-1$. The corresponding range over the integers is $X^{1-\frac{1}{k}} < H < X$, where we have a bound of $O(X^{1-\frac{1}{k}})$ for the mean square, see (1.5).

Our principal result gives the mean square of $\Delta_k(A;h)$ (which is the variance of $\mathcal{N}_{d_k}(A;h)$), in the limit $q \to \infty$, in terms of a matrix integral. Let U be an $N \times N$ matrix. The *secular coefficients* $\mathrm{Sc}_j(U)$ are the coefficients of the characteristic polynomial of U:

$$\det(I + xU) = \sum_{j=0}^{N} \mathrm{Sc}_j(U)x^j. \tag{1.22}$$

Thus $\mathrm{Sc}_0(U) = 1$, $\mathrm{Sc}_1(U) = \operatorname{tr} U$, $\mathrm{Sc}_N(U) = \det U$. The secular coefficients are the elementary symmetric functions in the eigenvalues $\lambda_1, \ldots, \lambda_N$ of U:

$$\mathrm{Sc}_r(U) = \sum_{1 \le i_1 < \cdots < i_r \le N} \lambda_{i_1} \cdot \cdots \cdot \lambda_{i_r}, \tag{1.23}$$

and give the character of the exterior power representation on $\wedge^j \mathbb{C}^N$:

$$\mathrm{Sc}_j(U) = \operatorname{tr} \wedge^j(U). \tag{1.24}$$

It is well known that $\wedge^j$ are distinct irreducible representations of the unitary group $U(N)$, and hence one gets the mean values

$$\int_{U(N)} \mathrm{Sc}_j(U)dU = 0, \quad j = 1, \ldots, N \tag{1.25}$$

and

$$\int_{U(N)} \mathrm{Sc}_j(U)\overline{\mathrm{Sc}_k(U)}dU = \delta_{j,k}, \tag{1.26}$$

where the integrals are with respect to the Haar probability measure.

Define the matrix integrals over the group $U(N)$ of $N \times N$ unitary matrices

$$I_k(m;N) := \int_{U(N)} \Big| \sum_{\substack{j_1+\cdots+j_k=m \\ 0 \le j_1,\ldots,j_k \le N}} \mathrm{Sc}_{j_1}(U)\ldots\mathrm{Sc}_{j_k}(U)\Big|^2 dU. \tag{1.27}$$

Then the variance

$$\mathrm{Var}(\mathcal{N}_{d_k}) := \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} |\Delta_k(A;h)|^2 \tag{1.28}$$

satisfies

Theorem 1.2 *If* $0 \le h \le \min(n-5, (1-\frac{1}{k})n-2)$, *then as* $q \to \infty$

$$\mathrm{Var}(\mathcal{N}_{d_k}) = H \cdot I_k(n; n-h-2) + O\Big(\frac{H}{\sqrt{q}}\Big). \tag{1.29}$$

In the remaining cases,

$$\mathrm{Var}(\mathcal{N}_{d_k}) = O\Big(\frac{H}{\sqrt{q}}\Big), \quad h = \left\lfloor \left(1-\frac{1}{k}\right) n \right\rfloor - 1 \tag{1.30}$$

and

$$\mathrm{Var}(\mathcal{N}_{d_k}) = 0, \quad \left\lfloor \left(1-\frac{1}{k}\right) n \right\rfloor \le h \le n. \tag{1.31}$$

In the case $(1-\frac{1}{k-1})n < h+2 \le (1-\frac{1}{k})n$, the matrix integral takes a simple form, c.f. Theorem 1.3 below.

1.5 Matrix integrals

For $(k-1)N < m < kN$, we obtain a simple formula for the matrix integral:

Theorem 1.3 *For* $(k-1)N < m < kN$,

$$I_k(m; N) = \binom{kN - m + k^2 - 1}{k^2 - 1}. \tag{1.32}$$

We are also able to give a closed form, albeit more complicated, formula for the matrix integral for any range of the parameters in terms of a lattice point count:

Theorem 1.4 *The quantity* $I_k(m; N)$ *is equal to the count of lattice points* $x = (x_i^{(j)}) \in \mathbb{Z}^{k^2}$ *satisfying each of the relations*

(i) $0 \le x_i^{(j)} \le N$ *for all* $1 \le i, j \le k$
(ii) $x_1^{(k)} + x_2^{(k-1)} + \cdots + x_k^{(1)} = kN - m$, *and*
(iii) $x \in A_k$,

where A_k *is the collection of* $k \times k$ *matrices whose entries satisfy the following system of inequalities:*

$$\begin{array}{ccccccc}
x_1^{(1)} & \le & x_1^{(2)} & \le & \cdots & \le & x_1^{(k)} \\
\vee\!| & & \vee\!| & & & & \vee\!| \\
x_2^{(1)} & \le & x_2^{(2)} & \le & \cdots & \le & x_2^{(k)} \\
\vee\!| & & \vee\!| & & & & \vee\!| \\
\vdots & & \vdots & & \ddots & & \vdots \\
\vee\!| & & \vee\!| & & & & \vee\!| \\
x_k^{(1)} & \le & x_k^{(2)} & \le & \cdots & \le & x_k^{(k)}
\end{array}$$

We note in passing that the above count of lattice points also may be interpreted as a count of plane partitions (see [38], Section 7.20 for an introduction to the latter).

For the standard divisor function ($k = 2$), if $h \le n/2 - 2$ and $n \ge 5$ we thus find that as $q \to \infty$,

$$\frac{1}{q^n} \sum_{A \in \mathcal{M}_n} |\Delta_2(A; h)|^2 \sim H \frac{(n-2h+5)(n-2h+6)(n-2h+7)}{6}. \tag{1.33}$$

This is consistent with (1.6), which leads us to expect a cubic polynomial in $\frac{n}{2} - h$.

For the range $(1 - \frac{1}{k-1})n < h + 2 < (1 - \frac{1}{k})n$, (1.32) gives

$$\begin{aligned} \frac{1}{q^n} \sum_{A \in \mathcal{M}_n} |\Delta_k(A; h)|^2 &\sim H \binom{k(n-h-2) - n + k^2 - 1}{k^2 - 1} \\ &= H\, Q_{k^2-1}\left(\left(1 - \frac{1}{k}\right)n - (h+1)\right), \end{aligned} \tag{1.34}$$

where $Q_{k^2-1}(u)$ is a polynomial of degree $k^2 - 1$, given by

$$Q_{k^2-1}(u) := \frac{\prod_{j=1}^{k^2-1}(k(u-1)+j)}{\Gamma(k^2)} = \frac{k^{k^2-1}}{\Gamma(k^2)} u^{k^2-1} + \cdots. \tag{1.35}$$

As this range corresponds to $X^{1-\frac{1}{k-1}} < H < X^{1-\frac{1}{k}}$ over the integers, the result (1.34), (1.35) is comparable with Lester's result (1.8) [c.f. the remark after (1.13)].

We use these results to model the situation over the integers for the range $H < X^{1-\frac{1}{k-1}}$, leading to Conjecture 1.1. To do so we derive asymptotics of $I_k(m; N)$ for $m \approx N$.

Theorem 1.5 *Let $c := m/N$. Then for $c \in [0, k]$,*

$$I_k(m; N) = \gamma_k(c) N^{k^2-1} + O_k\left(N^{k^2-2}\right), \tag{1.36}$$

with $\gamma_k(c)$ defined by (1.12).

The matrix integral satisfies a functional equation $I_k(m; N) = I_k(kN - m; N)$ (see Lemma 4.1), from which it follows that

$$\gamma_k(c) = \gamma_k(k - c). \tag{1.37}$$

It follows from an alternative analysis of $I_k(m; N)$ that we also have

Theorem 1.6

$$\gamma_k(c) = \sum_{0 \le \ell < c} \binom{k}{\ell}^2 (c-\ell)^{(k-\ell)^2+\ell^2-1} g_{k,\ell}(c-\ell) \tag{1.38}$$

where $g_{k,\ell}(c-\ell)$ are (complicated) polynomials in $c - \ell$.

From this we see that

Corollary 1.7 *For a fixed k, $\gamma_k(c)$ is a piecewise polynomial function of c. Specifically, it is a fixed polynomial for $r \le c < r + 1$ (r integer), and each time the value of c passes through an integer it becomes a different polynomial.*

For example,

$$\gamma_2(c) = \frac{1}{2!} \int\limits_{\substack{0 \le w_1 \le 1 \\ 0 \le c - w_1 \le 1}} (w_1 - (c - w_1))^2\, dw_1 = \begin{cases} \frac{c^3}{3!}, & 0 \le c \le 1 \\ \frac{(2-c)^3}{3!}, & 1 \le c \le 2, \end{cases}$$

and similarly

$$\gamma_3(c) = \begin{cases} \frac{1}{8!}c^8, & 0 < c < 1 \\ \frac{1}{8!}(3-c)^8, & 2 < c < 3, \end{cases}$$

while for $1 < c < 2$ we get

$$\gamma_3(c) = \frac{1}{8!}\Big(-2c^8 + 24c^7 - 252c^6 + 1512c^5 - 4830c^4 + 8568c^3 - 8484c^2 + 4392c - 927\Big).$$

1.6 Arithmetic progressions

A similar theory can be developed for sums of divisor functions along arithmetic progressions, see Sect. 3.

2 The divisor functions in short intervals

Our first goal is to provide proofs for Theorem 1.2 and the other results on sums of d_k in short intervals.

2.1 An expression for the variance

To begin the proof of Theorem 1.2, we express the variance of the short interval sums $\mathcal{N}_{d_k}$ in terms of sums of divisor functions, twisted by primitive even Dirichlet characters. Recall that a Dirichlet character is *even* if $\chi(cf) = \chi(f)$ for all $c \in \mathbb{F}_q^\times$, and is *odd* otherwise. The number of even characters modulo T^{n-h} is $\Phi(T^{n-h})/(q-1) = q^{n-h-1}$ (see e.g. [25, §3.3]). We denote by $\Phi^*_{ev}(T^{n-h}) = q^{n-h-2}(q-1)$ the number of primitive even characters modulo T^{n-h}.

For a Dirichlet character χ modulo T^{n-h}, set

$$\mathcal{M}(n; d_k\chi) := \sum_{f \in \mathcal{M}_n} d_k(f)\chi(f). \tag{2.1}$$

Lemma 2.1 *As $q \to \infty$*

$$\mathrm{Var}(\mathcal{N}_{d_k}) = \frac{H}{q^n}\frac{1}{\Phi^*_{ev}(T^{n-h})} \sum_{\substack{\chi \bmod T^{n-h} \\ \chi \text{ even primitive}}} |\mathcal{M}(n; d_k\chi)|^2 + O\Big(\frac{H}{\sqrt{q}}\Big). \tag{2.2}$$

Proof To compute the variance, we use [26, Lemma 5.4], which gives an expression for the variance of sums over short intervals of certain arithmetic functions α which are "even" ($\alpha(cf) = \alpha(f)$ for $c \in \mathbb{F}_q^\times$), multiplicative, and symmetric under the map $f^*(t) := t^{\deg f} f(\frac{1}{t})$, in the sense that

$$\alpha(f^*) = \alpha(f), \quad \text{if } f(0) \neq 0. \tag{2.3}$$

Since the divisor functions d_k clearly satisfy all these conditions, we may use [26, Lemma 5.3] (compare [25, §4.5]) to obtain

$$\mathrm{Var}(\mathcal{N}_{d_k}) = \frac{H}{q^n} \sum_{m_1,m_2=0}^{n} d_k(T^{n-m_1})\overline{d_k(T^{n-m_2})} \times \frac{1}{\Phi_{ev}(T^{n-h})} \sum_{\substack{\chi \bmod T^{n-h} \\ \chi\neq\chi_0 \text{ even}}} \mathcal{M}(m_1; d_k\chi)\overline{\mathcal{M}(m_2; d_k\chi)} \tag{2.4}$$

To compute $\mathcal{M}(n; d_k\chi)$, we introduce the generating function

$$\sum_{m=0}^{\infty} \mathcal{M}(m; d_k\chi)u^m = \sum_{f \text{ monic}} \chi(f)d_k(f)u^{\deg f} = L(u,\chi)^k. \tag{2.5}$$

Hence $\mathcal{M}(n; d_k\chi)$ is the coefficient of u^n in $L(u,\chi)^k$. Now for even $\chi \neq \chi_0$, we write $L(u,\chi) = (1-u)P(u,\chi)$ and by the Riemann Hypothesis for curves, $P(u,\chi) = \prod_{j=1}^{n-h-2}(1-\alpha_j u)$ with the inverse zeros satisfying $|\alpha_j| \leq \sqrt{q}$. Hence we have a bound

$$|\mathcal{M}(m; d_k\chi)| \ll_{n,k} q^{m/2}. \tag{2.6}$$

Therefore in the sum (2.4), the terms with $m_1 + m_2 < 2n$ (i.e., $(m_1, m_2) \neq (n,n)$) will contribute $O(\frac{H}{q^n}q^{n-\frac{1}{2}}) = O(H/\sqrt{q})$ (the coefficients $d_k(T^{n-m}) = \binom{n-m+k-1}{k-1}$ do not depend on q). Thus

$$\mathrm{Var}(\mathcal{N}_{d_k}) = \frac{H}{q^n}\frac{1}{\Phi_{ev}(T^{n-h})} \sum_{\substack{\chi \bmod T^{n-h} \\ \chi\neq\chi_0 \text{ even}}} |\mathcal{M}(n; d_k\chi)|^2 + O\Big(\frac{H}{\sqrt{q}}\Big). \tag{2.7}$$

For the same reason, the non-primitive even characters, whose number is $\ll \Phi_{ev}(T^{n-h})/q$ (see [25, §3.3]), contribute $O(H/q)$ to the variance. Thus we are left with

$$\mathrm{Var}(\mathcal{N}_{d_k}) = \frac{H}{q^n}\frac{1}{\Phi^*_{ev}(T^{n-h})} \sum_{\substack{\chi \bmod T^{n-h} \\ \chi \text{ even primitive}}} |\mathcal{M}(n; d_k\chi)|^2 + O\Big(\frac{H}{\sqrt{q}}\Big). \tag{2.8}$$

□

2.2 The sums $\mathcal{M}(n; d_k\chi)$

We need some information on $\mathcal{M}(n; d_k\chi)$ for χ even and primitive. By the Riemann Hypothesis (Weil's theorem), for χ even and primitive modulo T^{n-h}, we write

$$L(u,\chi) = (1-u)\det\left(I - uq^{1/2}\Theta_\chi\right) \tag{2.9}$$

with $\Theta_\chi \in U(n-h-2)$ a unitary matrix of size $n-h-2$.

Lemma 2.2 *For χ even, primitive modulo T^{n-h}, the following hold.*

- *If $n \leq k(n-h-2)$, that is $h \leq (1-\frac{1}{k})n - 2$, then*

$$\mathcal{M}(n, \chi d_k) = (-1)^n q^{n/2} \sum_{\substack{j_1+\cdots+j_k=n \\ j_1,\ldots,j_k\leq n-h-2}} \prod \mathrm{Sc}_{j_i}(\Theta_\chi) + O\left(q^{n-\frac{1}{2}}\right) \tag{2.10}$$

- *For $k(n-h-2) < n \leq k(n-h-1)$, i.e., $h = \lfloor(1-\frac{1}{k})n\rfloor - 1$, we get*

$$\mathcal{M}(n, d_k\chi) = O\left(q^{\frac{n-1}{2}}\right). \tag{2.11}$$

- *For $n > k(n-h-1)$, that is $h > (1-\frac{1}{k})n-1$, we get $\mathcal{M}(n, d_k\chi) = 0$.*

Proof For a primitive even character, the L-function is

$$\begin{aligned} L(u,\chi) &= (1-u)\det\left(I - u\sqrt{q}\Theta_\chi\right) \\ &= (1-u)\sum_{j=0}^{n-h-2}(-1)^j q^{j/2}\,\mathrm{Sc}_j(\Theta_\chi)u^j. \end{aligned} \tag{2.12}$$

To simplify notation in the calculations below, we write

$$N = n-h-2\,, \tag{2.13}$$

$$a_j = (-1)^j q^{j/2}\,\mathrm{Sc}_j(\Theta_\chi), \quad 0 \le j \le N, \quad a_{-1} = 0 = a_{N+1}\,, \tag{2.14}$$

and set

$$b_j := a_j - a_{j-1}, \quad j = 0, \ldots, N+1 \tag{2.15}$$

so that for χ even, primitive

$$L(u,\chi) = \sum_{j=0}^{N+1} b_j u^j \tag{2.16}$$

and

$$L(u,\chi)^k = \sum_{j_1,\ldots,j_k=0}^{N+1} b_{j_1}\cdot\cdots\cdot b_{j_k} u^{j_1+\cdots+j_k}. \tag{2.17}$$

Therefore the coefficient of u^n in the expansion of $L(u,\chi)^k$ for χ even and primitive is

$$\mathcal{M}(n, d_k\chi) = \sum_{\substack{j_1+\cdots+j_k=n \\ 0\le j_1,\ldots,j_k\le N+1}} b_{j_1}\cdot\cdots\cdot b_{j_k}. \tag{2.18}$$

Note that

$$b_j = a_j + O\left(q^{\frac{j-1}{2}}\right), \quad 0 \le j \le N \tag{2.19}$$

while

$$|b_{N+1}| \ll q^{N/2}. \tag{2.20}$$

Hence for a k-tuple $(j_1, \ldots, j_k)$ where one of the $j_i = N+1$ we have an upper bound

$$|b_{j_1}\cdot\cdots\cdot b_{j_k}| \ll q^{\frac{n-1}{2}}. \tag{2.21}$$

Thus if $n > kN$, and $j_1 + \cdots + j_k = n$, there is at least one index i so that $j_i = N+1$ and in that case

$$|\mathcal{M}(n, d_k\chi)| \ll q^{\frac{n-1}{2}}, \quad kN < n \le k(N+1). \tag{2.22}$$

For $n \le kN$, there will always be a k-tuple of $0 \le j_1, \ldots, j_k \le N$ with $j_1 + \cdots + j_k = n$, and so for $n \le kN$

$$\begin{aligned} \mathcal{M}(n, d_k\chi) &= \sum_{\substack{j_1+\cdots+j_k=n \\ 0\le j_1,\ldots,j_k\le N}} b_{j_1}\cdot\cdots\cdot b_{j_k} + O\left(q^{\frac{n-1}{2}}\right) \\ &= (-1)^n q^{n/2} \sum_{\substack{j_1+\cdots+j_k=n \\ 0\le j_1,\ldots,j_k\le N}} \mathrm{Sc}_{j_1}(\Theta_\chi)\cdot\cdots\cdot \mathrm{Sc}_{j_k}(\Theta_\chi) + O\left(q^{\frac{n-1}{2}}\right). \end{aligned} \tag{2.23}$$

This concludes the proof. □

2.3 Proof of Theorem 1.2

Inserting Lemma 2.2 into (2.2) we find that for $h \le (1-\frac{1}{k})n-2$,

$$\mathrm{Var}(\mathcal{N}_{d_k}) = \frac{H}{\Phi^*_{ev}(T^{n-h})} \sum_{\substack{\chi \bmod T^{n-h} \\ \text{even primitive}}} \Bigg| \sum_{\substack{j_1+\cdots+j_k=n \\ 0\le j_1,\ldots,j_k\le n-h-2}} \mathrm{Sc}_{j_1}(\Theta_\chi)\cdot\cdots\cdot \mathrm{Sc}_{j_k}(\Theta_\chi)\Bigg|^2 + O\Big(\frac{H}{\sqrt{q}}\Big). \tag{2.24}$$

We now apply Katz's equidistribution theorem for primitive even characters modulo T^N [23], which says that the corresponding Frobenii Θ_χ are equidistributed in the projective unitary group $PU(N-2)$ if $N \ge 5$, to replace the average over primitive even characters by a matrix integral over $PU(n-h-2)$, with an error of $O(1/\sqrt{q})$. This gives

$$\mathrm{Var}(\mathcal{N}_{d_k}) = H\cdot I_k(n; n-h-2) + O\Big(\frac{H}{\sqrt{q}}\Big), \quad 0 \le h \le \min\Big(n-5, \Big(1-\frac{1}{k}\Big)n-2\Big) \tag{2.25}$$

which proves the main statement of our theorem.

In the remaining cases, Lemma 2.2 gives

$$\mathrm{Var}(\mathcal{N}_{d_k}) = O\Big(\frac{H}{\sqrt{q}}\Big), \quad h = \Big\lfloor \Big(1-\frac{1}{k}\Big)n \Big\rfloor - 1 \tag{2.26}$$

and

$$\mathrm{Var}(\mathcal{N}_{d_k}) = 0, \quad \Big\lfloor \Big(1-\frac{1}{k}\Big)n \Big\rfloor \le h \le n. \tag{2.27}$$

This concludes the proof of Theorem 1.2. □

3 The divisor function in arithmetic progressions

3.1 Arithmetic progressions

We now turn to sums of divisor functions over arithmetic progressions. Set

$$\mathcal{S}_{d_k}(A) = \mathcal{S}_{d_k;X;Q}(A) = \sum_{\substack{n\le X \\ n=A \bmod Q}} d_k(n). \tag{3.1}$$

For the standard divisor function ($k=2$), it is known that individually, if $Q < X^{2/3-\epsilon}$,

$$\mathcal{S}_{d_2}(A) = \frac{X p_Q(\log X)}{\Phi(Q)} + O\left(X^{1/3+o(1)}\right) \tag{3.2}$$

for some linear polynomial p_Q. This is apparently due to Selberg (unpublished). For recent work on asymptotics of sums of d_3 over arithmetic progressions, see [16] and the literature cited therein.

The variance $\mathrm{Var}(\mathcal{S}_{d_2;X;Q})$ of $\mathcal{S}_{d_2}$ has been studied by Motohashi [33], Blomer [3], Lau and Zhao [29], the result being [29] (we assume Q prime for simplicity):

i) if $1 \le Q < X^{1/2+\epsilon}$ then

$$\mathrm{Var}(\mathcal{S}_{d_2;X;Q}) \ll X^{1/2} + \left(\frac{X}{Q}\right)^{2/3+\epsilon} \tag{3.3}$$

ii) for $X^{1/2} < Q < X$,

$$\mathrm{Var}(\mathcal{S}_{d_2;X;Q}) = \frac{X}{Q} p_3\left(\log \frac{Q^2}{X}\right) + O\left(\left(\frac{X}{Q}\right)^{5/6} (\log X)^3\right) \tag{3.4}$$

where p_3 is a polynomial of degree 3 with positive leading coefficient. See also the recent papers by Fouvry, Ganguli, Kowalski, Michel [15] and by Lester and Yesha [31] discussing higher moments.

For $k \ge 3$, Kowalski and Ricotta [28] considered smooth analogues of the divisor sums $\mathcal{S}_{d_k;X;Q}(A)$, and among other things computed the variance[2] for $Q^{k-\frac{1}{2}+\epsilon} < X < Q^{k-\epsilon}$.

We turn to $\mathbb{F}_q[x]$. For $Q \in \mathbb{F}_q[x]$ squarefree of degree at least 2, and A co-prime to Q, set

$$\mathcal{S}_{d_k,n,Q}(A) := \sum_{\substack{f \in \mathcal{M}_n \\ f = A \bmod Q}} d_k(f). \tag{3.5}$$

Our main result here concerns the variance

$$\mathrm{Var}_Q(\mathcal{S}_{d_k,n,Q}) := \frac{1}{\Phi(Q)} \sum_{\substack{A \bmod Q \\ \gcd(A,Q)=1}} \left|\mathcal{S}_{d_k,n,Q}(A) - \langle \mathcal{S}_{d_k,n,Q}\rangle\right|^2 \tag{3.6}$$

in the range $n \le k(\deg Q - 1)$.

Theorem 3.1 *If Q is squarefree, and $n \le k(\deg Q - 1)$, then the variance is given by*

$$\lim_{q\to\infty} \frac{\mathrm{Var}_Q(\mathcal{S}_{d_k,n,Q})}{q^n/|Q|} = I_k(n; \deg Q - 1). \tag{3.7}$$

In particular, for the classical divisor function $d = d_2$, we get a result consistent with (3.4).

Corollary 3.2 *If Q is squarefree,* $\deg Q \ge 2$ *and $n \le 2(\deg Q - 1)$, then*

$$\lim_{q\to\infty} \frac{\mathrm{Var}_Q(\mathcal{S}_{d_2,n,Q})}{q^n/|Q|} = \begin{cases} Pol_3(n), & n \le \deg Q - 1 \\ Pol_3(2(\deg Q - 1) - n), & \deg Q \le n \le 2(\deg Q - 1), \end{cases} \tag{3.8}$$

where $Pol_3(x) = \binom{x+3}{3} = (x+1)(x+2)(x+3)/6$.

As in the short interval case, we are led to a conjecture on the asymptotics of the variance over the integers. For simplicity, we stick with the case that the modulus Q is prime:

Conjecture 3.3 *For Q prime, $Q^{1+\epsilon} < X < Q^{k-\epsilon}$, as $X \to \infty$,*

$$\mathrm{Var}(\mathcal{S}_{d_k;X;Q}) \sim \frac{X}{Q} a_k \gamma_k\left(\frac{\log X}{\log Q}\right)(\log Q)^{k^2-1}$$

where a_k is given by (1.9) and $\gamma_k(c)$ is given by (1.12).

[2] The statement of [28, Theorem A], which deals with all moments, includes a term which is not small for the second moment; however the actual proof, see [28, Equation 9.8 and below] does give a good remainder.

3.2 Proof of Theorem 3.1

We start with the following expansion, using the orthogonality relation for Dirichlet characters to pick out an arithmetic progression [26, §4.1]:

$$\mathcal{S}_{d_k,n,Q}(A) = \frac{1}{\Phi(Q)} \sum_{\substack{f\in\mathcal{M}_n \\ (f,Q)=1}} d_k(f) + \frac{1}{\Phi(Q)} \sum_{\chi\neq\chi_0} \overline{\chi(A)}\mathcal{M}(n; d_k\chi) \tag{3.9}$$

where $\mathcal{M}(n; d_k\chi)$, given by (2.1), is the coefficient of u^n in the expansion of $L(u,\chi)^k$. Since $L(u,\chi)$ is a polynomial of degree $\leq \deg Q-1$ for $\chi\neq\chi_0$, we see that $\mathcal{S}_{d_k,n,Q}$ is independent of A for $n > k(\deg Q-1)$:

$$\mathcal{S}_{d_k,n,Q}(A) = \frac{1}{\Phi(Q)} \sum_{\substack{f\in\mathcal{M}_n \\ (f,Q)=1}} d_k(f) \sim \frac{q^n\binom{n+k-1}{k-1}}{\Phi(Q)}. \tag{3.10}$$

Thus for any n, the mean value (averaging over A coprime to Q) is

$$\left\langle \mathcal{S}_{d_k,n,Q}\right\rangle \sim \frac{q^n\binom{n+k-1}{k-1}}{\Phi(Q)}. \tag{3.11}$$

The interesting range is $n \leq k(\deg Q-1)$, which we assume from now on. To compute the variance, we use (3.9) and the orthogonality relations for Dirichlet characters as in [25,26] to find

$$\mathrm{Var}(\mathcal{S}_{d_k,n,Q}) = \frac{1}{\Phi(Q)^2} \sum_{\chi\neq\chi_0} |\mathcal{M}(n; d_k\chi)|^2. \tag{3.12}$$

We first dispose of the contribution of even characters, whose number is $\Phi_{ev}(Q) = \Phi(Q)/(q-1)$: As in (2.6), we have a bound for $\chi\neq\chi_0$

$$|\mathcal{M}(n, d_k\chi)| \ll_n q^{n/2}. \tag{3.13}$$

Therefore the even characters contribute at most

$$\ll_n \frac{1}{\Phi(Q)^2}\Phi_{\mathrm{ev}}(Q)q^n \ll \frac{1}{q}\frac{q^n}{\Phi(Q)}\ , \tag{3.14}$$

which is negligible relative to the main term that we find which is of order $q^n/\Phi(Q)$. The same argument bounds the contribution of odd non-primitive characters if Q is non-prime. Thus

$$\mathrm{Var}(\mathcal{S}_{d_k,n,Q}) = \frac{1}{\Phi(Q)^2} \sum_{\chi \text{ odd and primitive}} |\mathcal{M}(n; d_k\chi)|^2 + O\Big(\frac{1}{q}\cdot\frac{q^n}{\Phi(Q)}\Big). \tag{3.15}$$

To handle the odd primitive characters χ, we use the Riemann Hypothesis (Weil's theorem) to write

$$L(u,\chi) = \det(I - uq^{1/2}\Theta_\chi), \tag{3.16}$$

with the unitarized Frobenius $\Theta_\chi \in U(\deg Q-1)$. Hence for $2 \leq n \leq k(\deg Q-1)$,

$$\mathcal{M}(n; d_k\chi) = (-1)^n q^{n/2} \sum_{\substack{j_1+\cdots+j_k=n \\ 0\leq j_1,\ldots,j_k\leq \deg Q-1}} \mathrm{Sc}_{j_1}(\Theta_\chi)\cdot\cdots\cdot\mathrm{Sc}_{j_k}(\Theta_\chi). \tag{3.17}$$

Inserting (3.17) into (3.15) and using (3.17) and Katz's equidistribution theorem [22] (here we require Q squarefree) we get for $\deg Q \geq 2$ and $2 \leq n \leq k(\deg Q - 1)$

$$\lim_{q\to\infty} \frac{\mathrm{Var}(\mathcal{S}_{d_k,n,Q})}{q^n/|Q|} = \int\limits_{U(\deg Q-1)} \Big| \sum_{\substack{j_1+\cdots+j_k=n \\ 0\leq j_1,\ldots,j_k\leq \deg Q-1}} \mathrm{Sc}_{j_1}(U)\ldots\mathrm{Sc}_{j_k}(U)\Big|^2 dU \tag{3.18}$$
$$= I_k(n, \deg Q - 1),$$

proving Theorem 3.1.

Note that If $n < \deg Q$, then we of course do not need these powerful equidistribution results, since there is at most *one* f with $\deg f = n$ and $f = A \bmod Q$, which allows one to obtain the claim in an elementary manner.

4 Matrix integral

Our goal in this section is to evaluate the matrix integral (1.27). We start by looking at the following products:

$$\det(I - xU)^k \det(I - yU^*)^k = \left(\sum_{j=1}^{N} Sc_j(U)(-x)^j\right)^k \left(\sum_{i=1}^{N} Sc_i(U^*)(-y)^i\right)^k. \tag{4.1}$$

We will be interested in the expected value over the unitary group of the above. Due to the invariance of Haar measure of $U(N)$ under multiplication by unit scalars, we are left with only the diagonal terms, i.e.,

$$\int\limits_{U(N)} \det(I - xU)^k \det(I - yU^*)^k dU = \sum_{0\leq m\leq kN} I_k(m, N)(xy)^m. \tag{4.2}$$

This integral therefore serves as a generating series for the function $I_k(m; N)$. Note that we may switch the sign of both x and y and retain the same right hand side.

4.1 Evaluation in a certain range

We now give the proof of Theorem 1.3. For the range $m \leq N$, we will apply the method of Diaconis-Gamburd [13] to obtain

$$I_k(m; N) = \binom{m + k^2 - 1}{k^2 - 1}, \quad m \leq N. \tag{4.3}$$

When $(k - 1)N \leq m \leq kN$ we have a functional equation which allows us to compute the integral in this range.

4.1.1 The functional equation

Lemma 4.1 *For $0 \leq m \leq kN$, the following functional equation holds:*

$$I_k(m; N) = I_k(kN - m; N). \tag{4.4}$$

Proof We use the functional equation of the characteristic polynomial of a unitary matrix

$$\det(I + xU) = x^N \det(U) \det(I + x^{-1}U^*), \tag{4.5}$$

which implies that

$$\mathrm{Sc}_j(U) = \det(U)\,\mathrm{Sc}_{N-j}(U^*) = \det(U)\overline{\mathrm{Sc}_{N-j}(U)}. \tag{4.6}$$

Therefore

$$\begin{aligned}\mathrm{Sc}_{j_1}(U)\cdots\mathrm{Sc}_{j_k}(U)&\overline{\mathrm{Sc}_{l_1}(U)\cdots\mathrm{Sc}_{l_k}(U)}\\ &= \mathrm{Sc}_{N-l_1}(U)\cdots\mathrm{Sc}_{N-l_k}(U)\overline{\mathrm{Sc}_{N-j_1}(U)\cdots\mathrm{Sc}_{N-j_k}(U)}.\end{aligned}$$

We change variables

$$m' = kN - m, \quad j_i' = N - j_i, \quad l_i' = N - l_i \tag{4.7}$$

and so obtain

$$\Big|\sum_{\substack{j_1+\cdots j_k=m\\ 0\le j_1,\ldots,j_k\le N}} \mathrm{Sc}_{j_1}(U)\ldots\mathrm{Sc}_{j_k}(U)\Big|^2 = \Big|\sum_{\substack{j_1'+\cdots j_k'=m'\\ 0\le j_1',\ldots,j_k'\le N}} \mathrm{Sc}_{j_1'}(U)\ldots\mathrm{Sc}_{j_k'}(U)\Big|^2, \tag{4.8}$$

which implies (4.4). □

4.1.2 Review of Diaconis and Gamburd [13]

Let $A = (a_{i,j})$ be an $m \times n$ matrix with non-negative integer entries. Let $r_i = \sum_j a_{i,j}$ be the sum of the entries in the i-th row, and $c_j = \sum_i a_{i,j}$ be the sum of the entries in the j-th column. Set

$$\mathrm{row}(A) = (r_1, \ldots, r_m), \quad \mathrm{col}(A) = (c_1, \ldots, c_n). \tag{4.9}$$

Let $\lambda = (\lambda_1, \ldots, \lambda_r) \in \mathbb{N}^r$ with $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_r$ be a partition of n, so $n = \sum_i \lambda_i$. Denote by $m_i = m_i(\lambda)$ the number of part of λ equal to i, so an alternative notation is

$$\lambda = \langle 1^{m_1} 2^{m_2} \ldots \rangle. \tag{4.10}$$

Given two partitions $\mu = (\mu_1, \ldots, \mu_m)$ and $\tilde{\mu} = (\tilde{\mu}_1, \ldots, \tilde{\mu}_n)$, denote by $N_{\mu,\tilde{\mu}}$ the number of $m \times n$ matrices A with non-negative integer entries so that $\mathrm{row}(A) = \mu$ and $\mathrm{col}(A) = \tilde{\mu}$. For instance if $\mu = (2, 1, 1) = \langle 1^2 2^1 \rangle$ and $\tilde{\mu} = (3, 1) = \langle 1^1 3^1 \rangle$ then $N_{\mu,\tilde{\mu}} = 3$ with the corresponding matrices A being

$$\begin{pmatrix} 2 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}$$

We quote a result of Diaconis and Gamburd:

Theorem 4.2 [13] *Let a_i, b_j be non-negative integers, $1 \le i, j \le \ell$. Then for $\max(\sum_{j=1}^{\ell} j a_j, \sum_{j=1}^{\ell} j b_j) \le N$,*

$$\int_{U(N)} \prod_{j=1}^{\ell} (\mathrm{Sc}_j(U))^{a_j} \overline{\mathrm{Sc}_j(U)}^{b_j}\, dU = N_{\mu,\tilde{\mu}} \tag{4.11}$$

where $\mu = \langle 1^{a_1} 2^{a_2} \ldots \ell^{a_\ell} \rangle$, $\tilde{\mu} = \langle 1^{b_1} 2^{b_2} \ldots \ell^{b_\ell} \rangle$.

4.1.3 Back to the variance calculation

There is a slight reformulation of Theorem 4.2 that will be useful to have stated. Let $\mu = (j_1, \ldots, j_k)$ and $\tilde{\mu} = (\tilde{j}_1, \ldots, \tilde{j}_k)$ be arrays of non-negative integers (we now impose no condition that they be weakly decreasing), and we generalize $N_{\mu,\tilde{\mu}}$ in the obvious manner, so that it is the count of $k \times k$ matrices A with non-negative integer entries such that $\mathrm{row}(A) = \mu$ and $\mathrm{col}(A) = \tilde{\mu}$. Note that, by permuting rows and then columns of the matrix A, if the arrays μ and ν are rearrangements of each other, and likewise for $\tilde{\mu}$ and $\tilde{\nu}$,

$$N_{\mu,\tilde{\mu}} = N_{\nu,\tilde{\nu}}.$$

Thus Theorem 4.2 may be reformulated as the statement that for $\max(\sum j_i, \sum \tilde{j}_i) \leq N$,

$$\int_{U(N)} \prod_i \mathrm{Sc}_{j_i}(U)\overline{\mathrm{Sc}_{\tilde{j}_i}(U)}\, dU = N_{\mu,\tilde{\mu}}. \tag{4.12}$$

The reformulation is useful for us because in the proof that follows we will be working with arrays that are not ordered.

Proof of Theorem 1.3 For $m \leq N$, note that in the definition (1.27), the restriction that $j_i \leq N$ plays no role. Hence,

$$I_k(m; N) := \int_{U(N)} \left| \sum_{j_1+\cdots+j_k=m} \mathrm{Sc}_{j_1}(U) \ldots \mathrm{Sc}_{j_k}(U) \right|^2 dU.$$

We may expand the square, and, because in the range of summation over j_i we have $j_1 + \cdots + j_k = m \leq N$, we may apply (4.12) to see that the above expression is just

$$\sum_{\substack{j_1+\cdots+j_k=m \\ \tilde{j}_1+\cdots+\tilde{j}_k=m}} N_{\mu,\tilde{\mu}}.$$

But this sum is just the count of all $k \times k$ matrices comprised of non-negative integer entries with the total sum of the entries being m. This in turn is just the number of ways of writing $a_1 + \cdots + a_{k^2} = m$. Therefore, for this range of $m \leq N$, $I_k(m; N)$ is the binomial coefficient

$$I_k(m; N) = \binom{m + k^2 - 1}{k^2 - 1}.$$

One way to see so is to note that it is the coefficient of x^m in

$$\sum_{a_i \geq 0} x^{a_1+\cdots+a_{k^2}} = \frac{1}{(1-x)^{k^2}}.$$

Finally, to deal with the case $(k-1)N \leq m \leq kN$, we use the functional equation, Lemma 4.1. □

4.2 Evaluation in other ranges

It was shown in the previous section how to evaluate $I_k(m; N)$ in the ranges $m \leq N$ and $(k-1)N \leq m \leq kN$. Our goal here is to illustrate a general method for computing it in all other ranges.

By (4.2), we are looking to find the coefficient of x^m in the expansion of

$$P_k(x) = \int_{U(N)} \det(I - U^* x)^k \det(I - U)^k dU. \tag{4.13}$$

This can be calculated using the following theorem:

Theorem 4.3 [7,8] *Let A and B be finite collections of complex numbers. Then*

$$\int_{U(N)} \prod_{\alpha\in A} \det\left(I - U^* e^{-\alpha}\right) \prod_{\beta\in B} \det(I - U e^{-\beta})\, dU$$
$$= \sum_{\substack{S\subseteq A\\ T\subseteq B\\ |T|=|S|}} e^{-N\left(\sum_{\hat\alpha\in s}\hat\alpha + \sum_{\hat\beta\in T}\hat\beta\right)} Z(\overline{S} + T^-, \overline{T} + S^-) \tag{4.14}$$

where

$$\overline{S} = A - S, \quad \overline{T} = B - T, \quad S^- = \{-\hat\alpha, \hat\alpha \in S\}, \quad T^- = \{-\hat\beta, \hat\beta \in T\}$$

and

$$Z(A, B) = \prod_{\substack{\alpha\in A\\ \beta\in B}} z(\alpha + \beta)$$

with $z(x) = \frac{1}{1-e^{-x}}$.

For example, we find

$$\begin{aligned} P_2(x) =& \frac{1}{(1-x)^4}\Big[1 + x^{2N+4} - (2+N)^2 x^{1+N} \\ &+ 2(3 + 4N + N^2)x^{N+2} - (2+N)^2 x^{N+3}\Big]. \end{aligned} \tag{4.15}$$

Note that $P_2(x)$ satisfies $x^{2N} P_2(x)(1/x) = P_2(x)(x)$, which corresponds to the functional equation $I_2(m; N) = I_2(2N - m; N)$. Evaluating the coefficient of x^m we recover

$$I_2(m; N) = \begin{cases} \binom{m+3}{3} & \text{if } m \le N \\ \binom{2N-m+3}{3} & \text{if } N \le m \le 2N, \end{cases} \tag{4.16}$$

as proved in the previous section.

Similarly

$$\begin{aligned} P_3(x) =& \frac{1}{(1-x)^9}\Big[1 - x^{3N+9} + (3+N)^2\left(4 + 5N + N^2\right)\left(x^{2+N} - x^{N+7}\right) \\ &+ \frac{1}{4}(3+N)^2(2+N)^2\left(x^{2N+8} - x^{N+1}\right) \\ &+ (3+N)^2\left(10 + 7N + N^2\right)\left(x^{N+4} - x^{2N+5}\right) \\ &+ (3+N)^2(N+4)^2(1/4)\left(x^{2N+4} - x^{N+5}\right) \\ &+ \frac{3}{2}\left(56 + 90N + 51N^2 + 12N^3 + N^4\right)\left(x^{2N+6} - x^{N+3}\right)\Big] \end{aligned}$$

Again $P_3(x)$ satisfies $x^{3n}P_3(x)(1/x) = P_3(x)(x)$, corresponding to the functional equation $I_3(m;N) = I_3(3N-m;N)$. Hence

$$I_3(m;N) = \begin{cases} \binom{m+8}{8} & \text{if } m \le N+3 \\ \mathrm{Poly}_8(m) & \text{if } N+3 < m < 2N-3 \\ \binom{3N-m+8}{8} & \text{if } 2N-3 \le m \le 3N. \end{cases} \tag{4.17}$$

where $\mathrm{Poly}_8(m)$ is a polynomial in m of degree 8, and is given by

$$\begin{aligned} \mathrm{Poly}_8(m) = &\binom{m+8}{8} - (3+N)^2(N+4)^2(1/4)\binom{m-N+3}{8} \\ &+ (3+N)^2\left(10+7N+N^2\right)\binom{m-N+4}{8} \\ &- \frac{3}{2}\left(56+90N+51N^2+12N^3+N^4\right)\binom{m-N+5}{8} \\ &+ (3+N)^2\left(4+5N+N^2\right)\binom{m-N+6}{8} \\ &- \frac{1}{4}(3+N)^2(2+N)^2\binom{m-N+7}{8}. \end{aligned}$$

This method obviously extends to larger values of k, but in practice is effective only when k is relatively small.

4.3 Large N asymptotics: a symmetric function theory approach

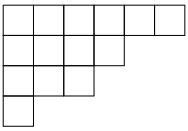
In this subsection, we give a proof of Theorem 1.5, determining the asymptotic behavior of $I_k(m;N)$ when m and N grow in ratio to one another. We begin however with a proof of Theorem 1.4, the characterization of $I_k(m;N)$ in terms of a count of lattice points. It is then in part by estimating this lattice count that we obtain the coefficient $\gamma_k(c)$ in Theorem 1.5.

4.3.1 Some preliminaries from symmetric function theory

The proof below of Theorems 1.4 and 1.5 requires some knowledge from symmetric function theory. In order to make our presentation self-contained, in this section we recall for the reader a few concepts that will be necessary. In particular Schur functions, defined below, will play a key role. The reader already familiar with this material may skip ahead to the next subsection. (Standard references for this material include [4,17,38]; for readers with a background in analytic number theory, [17] is perhaps the quickest general introduction.)

Recall (from 4.1.2), a *partition* λ is a sequence $(\lambda_1, \dots, \lambda_k)$ of positive integers satisfying $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_k$. The *length* $\ell(\lambda)$ of such a partition is defined by $\ell(\lambda) := k$. If 1 appears among the numbers $\lambda_1, \dots, \lambda_k$ a total of m_1 times, 2 appears m_2 times, and so on, we also write $\lambda = \langle 1^{m_1} 2^{m_2} \cdots \rangle$.

A *Young diagram* is a collection of boxes arranged in left-justified rows, with a weakly decreasing number of boxes in each row. The partition $(\lambda_1, \dots, \lambda_k)$ corresponds to a Young diagram with λ_1 boxes in the first row, λ_2 boxes in the second, and so on to λ_k boxes in the kth row. For instance, the partition $(6, 4, 3, 1)$ corresponds to the Young diagram



For λ a partition, a *semistandard Young tableau (SSYT)* of shape λ is an array $T = (T_{ij})_{1\le i\le \ell(\lambda), 1\le j\le \lambda_i}$ of positive integers such that $T_{i,j} \le T_{i,j+1}$ and $T_{ij} < T_{i+1,j}$. It is common to write SSYTs in a Young diagram, as for example

1	1	2	3	3	7
2	3	3	4		
4	4	6			
7					

This is a SSYT of shape $(6, 4, 3, 1)$. Note that the condition $T_{i,j} \le T_{i,j+1}$ translates to the array T weakly increasing in every row and $T_{i,j} < T_{i+1,j}$ to strictly increasing in every column.

We say T has *type* $a = (a_1, a_2, \ldots)$ if T has $a_i = a_i(T)$ parts equal to i. The SSYT above has type $(2, 2, 4, 3, 0, 1, 2)$. It is common to use the notational abbreviation

$$x^T = x_1^{a_1(T)} x_2^{a_2(T)} \cdots ,$$

so for the example SSYT above,

$$x^T = x_1^2 x_2^2 x_3^4 x_4^3 x_6 x_7.$$

We finally come to the combinatorial definition of Schur functions.

Definition 4.4 For a partition λ, the Schur function in the variables $x_1, \ldots, x_r$ indexed by λ is a multivariable polynomial defined by

$$s_\lambda(x_1, \ldots, x_r) := \sum_T x_1^{a_1(T)} \cdots x_r^{a_r(T)},$$

where the sum is over all SSYTs T whose entries belong to the set $\{1, \ldots, r\}$ (i.e., $a_i(T) = 0$ for $i > r$).

For example, the SSYTs of shape $(2, 1)$ whose entries belong to the set $\{1, 2, 3\}$ are

$$\begin{array}{|c|c|}\hline 1&1\\\hline 2\\\cline{1-1}\end{array}\quad \begin{array}{|c|c|}\hline 1&2\\\hline 2\\\cline{1-1}\end{array}\quad \begin{array}{|c|c|}\hline 1&3\\\hline 2\\\cline{1-1}\end{array}\quad \begin{array}{|c|c|}\hline 1&1\\\hline 3\\\cline{1-1}\end{array}\quad \begin{array}{|c|c|}\hline 1&2\\\hline 3\\\cline{1-1}\end{array}\quad \begin{array}{|c|c|}\hline 1&3\\\hline 3\\\cline{1-1}\end{array}\quad \begin{array}{|c|c|}\hline 2&2\\\hline 3\\\cline{1-1}\end{array}\quad \begin{array}{|c|c|}\hline 2&3\\\hline 3\\\cline{1-1}\end{array}$$

and so

$$s_{(2,1)}(x_1, x_2, x_3) = x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2 + 2x_1 x_2 x_3.$$

4.3.2 A proof of Theorems 1.4 and 1.5

Proof of Theorem 1.4 Our starting point is again Eq. 4.2, which in this case we evaluate using a result of Bump and Gamburd [5, Prop. 4].

Theorem 4.5 [5] *Let $\alpha_1, \ldots, \alpha_{L+L'}$ be complex numbers. Then,*

$$\int_{U(N)} \prod_{\ell=1}^{L} \det(1 + \alpha_\ell^{-1} U^{-1}) \prod_{\ell'=1}^{L'} \det(1 + \alpha_{L+\ell'} U)\, dU = \frac{s_{\langle N^L\rangle}(\alpha_1, \ldots, \alpha_{L+L'})}{\alpha_1^N \cdots \alpha_L^N}.$$

Here $s_{\langle N^L\rangle}$ is a Schur function indexed by the partition $\langle N^L\rangle$.

By specializing this theorem, we see that

$$\int_{U(N)} \det(1+\alpha U)^k \det(1+\beta U^{-1})^k \, dU = \alpha^{kN} s_{\langle N^k \rangle}(\underbrace{\alpha^{-1}, \ldots, \alpha^{-1}}_{k \text{ terms}}, \underbrace{\beta, \ldots, \beta}_{k \text{ terms}}). \tag{4.18}$$

Expanding the Schur function as a polynomial and labeling the coefficients, we have

$$\alpha^{kN} s_{\langle N^k \rangle}(\underbrace{\alpha^{-1}, \ldots, \alpha^{-1}}_{k \text{ terms}}, \underbrace{\beta, \ldots, \beta}_{k \text{ terms}}) = \sum c_{ij} \alpha^i \beta^j.$$

By comparison with (4.2), we see that $I_k(m; N) = c_{mm}$.

From the combinatorial definition of Schur functions (Definition 4.4 above), we see that c_{mm} is the number of semistandard Young tableau (SSYT) T such that if, as before, a_i denotes the number of i's in T,

$$a_{k+1} + \cdots + a_{2k} = m,$$

and $a_i = 0$ for $i > 2k$.

We parametrize such tableaux T by letting $y_r^{(s)} = y_r^{(s)}(T)$ be the rightmost position of the entry s in row r; if s does not occur in row r, inductively define $y_r^{(s)} = y_r^{(s-1)}$, with $y_r^{(1)} = 0$ if the entry 1 does not occur in row r. So, for instance, in the SSYT T on the partition (7^2) with entries ranging from 1 to 4 given by

$$T = \begin{array}{|c|c|c|c|c|c|c|} \hline 1 & 1 & 1 & 2 & 3 & 3 & 3 \\ \hline 2 & 2 & 2 & 4 & 4 & 4 & 4 \\ \hline \end{array}$$

we have

$$\begin{pmatrix} y_1^{(1)} & y_1^{(2)} & y_1^{(3)} & y_1^{(4)} \\ y_2^{(1)} & y_2^{(2)} & y_2^{(3)} & y_2^{(4)} \end{pmatrix} = \begin{pmatrix} 3 & 4 & 7 & 7 \\ 0 & 3 & 3 & 7 \end{pmatrix}.$$

Note that here $y_2^{(1)} = 0$ and $y_1^{(3)} = y_1^{(4)} = y_2^{(4)} = 7$. That these entries should take these values is necessarily the case; if the 2nd row began with 1, then T could not be made to be strictly increasing in columns, and for the same reason the 1st row may not end with 4.

Moreover, note that because rows increase weakly,

$$y_r^{(s)} \le y_r^{(s+1)}, \tag{4.19}$$

and because columns increase strongly,

$$y_{r+1}^{(s+1)} \le y_r^{(s)}. \tag{4.20}$$

With these restrictions (4.19) and (4.20) in place, there is a bijection between arrays

$$\begin{pmatrix} y_1^{(1)} & y_1^{(2)} & \cdots & y_1^{(k)} & N & \cdots & \cdots & N \\ 0 & y_2^{(2)} & \cdots & y_2^{(k)} & y_2^{(k+1)} & N & \cdots & N \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & y_k^{(k)} & y_k^{(k+1)} & \cdots & y_k^{(2k-1)} & N \end{pmatrix}$$

with $y_r^{(s)} \in [0, N] \cap \mathbb{Z}$ and SSYT of $\langle N^k \rangle$ with entries ranging from 1 to $2k$.

It is easy to see that those SSYT for which $a_{k+1}+\cdots+a_{2k}=m$ correspond to those arrays in which $(N-y_1^{(k)})+(N-y_2^{(k)})+\cdots+(N-y_k^{(k)})=m$. By re-indexing $x_r^{(s)}=y_r^{(s+r-1)}$, we obtain the proposition.

With Theorem 1.4 in hand, getting an expression for $\gamma_k(c)$ in Theorem 1.5, as we will see, is a more or less standard argument in counting lattice points. On the other hand, in order to simplify the expression we get to (1.12), it will be useful to have done the following computation beforehand.

Lemma 4.6 *As usual, define the Vandermonde determinant by*

$$\Delta(w_1,w_2,\ldots,w_k):=\prod_{i>j}(w_i-w_j),$$

and for $\beta\in\mathbb{R}^{k+1}$ satisfying $\beta_1\le\beta_2\le\cdots\le\beta_{k+1}$, define

$$I(\beta)=\{\alpha\in\mathbb{R}^k:\beta_1\le\alpha_1\le\beta_2\le\alpha_2\le\cdots\le\alpha_k\le\beta_{k+1}\}.$$

Then

$$\int_{\alpha\in I(\beta)}\Delta(\alpha_1,\alpha_2,\ldots,\alpha_k)\,d^k\alpha=\frac{1}{k!}\Delta(\beta_1,\ldots,\beta_{k+1}). \tag{4.21}$$

Proof Because of the well known identity $\Delta(w)=\det(w_\mu^{\nu-1})$, we see that the left hand side of (4.21) is just

$$\int_{\alpha\in I(\beta)}\det\begin{pmatrix}1&1&\cdots&1\\ \alpha_1&\alpha_2&\cdots&\alpha_k\\ \vdots&\vdots&\ddots&\vdots\\ \alpha_1^{k-1}&\alpha_2^{k-1}&\cdots&\alpha_k^{k-1}\end{pmatrix}d^k\alpha$$
$$=\det\begin{pmatrix}\beta_2-\beta_1&\beta_3-\beta_2&\cdots&\beta_{k+1}-\beta_k\\ (\beta_2^2-\beta_1^2)/2&(\beta_3^2-\beta_3^2)/2&\cdots&(\beta_{k+1}^2-\beta_k^2)/2\\ \vdots&\vdots&\ddots&\vdots\\ (\beta_2^k-\beta_1^k)/k&(\beta_3^k-\beta_2^k)/k&\cdots&(\beta_{k+1}^k-\beta_k^k)/k\end{pmatrix}$$

by integrating one variable at a time and using multilinearity. But again applying multilinearity (twice), we see that this is just

$$\frac{1}{k!}\sum_{\varepsilon\in\{0,1\}^k}(-1)^{k-|\varepsilon|}\det\begin{pmatrix}\beta_{1+\varepsilon_1}&\beta_{2+\varepsilon_2}&\cdots&\beta_{k+\varepsilon_k}\\ \beta_{1+\varepsilon_1}^2&\beta_{2+\varepsilon_2}^2&\cdots&\beta_{k+\varepsilon_k}^2\\ \vdots&\vdots&\ddots&\vdots\\ \beta_{1+\varepsilon_1}^k&\beta_{2+\varepsilon_2}^k&\cdots&\beta_{k+\varepsilon_k}^k\end{pmatrix},$$

where $|\varepsilon|$ is the number of i such that $\varepsilon_i=1$. Clearly the determinant in the summand will be 0 unless ε is one of the $k+1$ possibilities: $(1,1,1,\ldots,1)$, $(0,1,1,\ldots,1)$, $(0,0,1,\ldots,1)$, …, $(0,0,0,\ldots,0)$. Thus the sum above is just a Laplace expansion of

$$\frac{1}{k!}\det\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_{k+1} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^k & \beta_2^k & \cdots & \beta_{k+1}^k \end{pmatrix}$$

as claimed. □

Proof of Theorem 1.5 We demonstrate first that (1.36) of Theorem 1.5 holds with $\gamma_k(c)$ given by

$$\gamma_k(c) = \int_{[0,1]^{k^2}} \delta_c\left(u_1^{(k)} + u_2^{(k-1)} + \cdots + u_k^{(1)}\right) \mathbf{1}_{A_k}(u)\, d^{k^2}u, \tag{4.22}$$

where $\mathbf{1}_{A_k}$ is the indicator function of the set A_k (defined in the statement of Theorem 1.4).□

The truth of this should come as no surprise; we have just approximated a lattice count with a continuous approximation. Later we show that this integral is equal to the right hand side of (1.12).

Our proof of this first part is standard. For notational reasons let $S = \{(i, j) : 1 \le i, j \le k : (i, j) \ne (1, k)\}$, and let V_c be the convex region contained in $\mathbb{R}^{k^2-1} = \{(u_i^{(j)})_{(i,j)\in S} : u_i^{(j)} \in \mathbb{R}\}$ defined by the following system of inequalities:

(i) $0 \le u_i^{(j)} \le 1$, for all $(i, j) \in S$,
(ii) for $u_1^{(k)} := c - (u_2^{(k-1)} + \cdots + u_k^{(1)})$, we have $0 \le u_1^{(k)} \le 1$, and
(iii) the matrix $(u_i^{(j)})_{1\le i,j\le k}$ lies in the set A_k.

This region is convex because it is the intersection of half planes. Note moreover that for all $c \in [0, k]$, the region V_c is contained in $[0, 1]^{k^2-1}$, and therefore contained in a closed ball of radius $\sqrt{k^2 - 1}$.

Theorems 1.4 and Lemma 4.1 show that

$$I_k(m; N) = \#\left(\mathbb{Z}^{k^2-1} \cap (N \cdot V_c)\right), \tag{4.23}$$

where $N \cdot V_c = \{Nx : x \in V_c\}$ is the dilate of V_c by a factor of N.

We will need to reference the well known principle that a count of lattice points in a region can be approximated by the volume of the region (at least in ordinary circumstances). A result of the sort we quote below dates back to Davenport [11,12]; the clean formulation we have cited here may be found in [35, Section 2].

Theorem 4.7 *If $S \subset \mathbb{R}^\ell$ is a convex region contained in a closed ball of radius ρ, then*

$$\#(S \cap \mathbb{Z}^\ell) = \mathrm{vol}_\ell(S) + O\left(\rho^{\ell-1}\right), \tag{4.24}$$

where the implicit constant depends only on ℓ.

Applying (4.24), with $\ell = k^2 - 1$, we see

$$I_k(m; N) = \mathrm{vol}(N \cdot V_c) + O_k\left(N^{k^2-2}\right).$$

Yet clearly

$$\mathrm{vol}(N \cdot V_c) = N^{k^2-1} \int\limits_{[0,1]^{k^2}} \delta_c\left(u_1^{(k)} + \cdots + u_k^{(1)}\right) \mathbf{1}_{A_k}(u)\, d^{k^2}u,$$

which implies (1.36), with $\gamma_k(c)$ given by (4.22).

It remains to show that this integral can be reduced to the expression defined in (1.12). Here we make use of Lemma 4.6. We have, by applying it inductively,

$$\begin{aligned}
\gamma_k(c) &= \int_{[0,1]^{k^2}} \delta_c(u_1^{(k)} + \cdots + u_k^{(k)}) \cdot \mathbf{1} \begin{bmatrix} u_1^{(1)} & \le & u_1^{(2)} & \le & \cdots & & \cdots & & \cdots \\ \vee\!| & & \vee\!| & & & & & & \\ u_2^{(1)} & \le & u_2^{(2)} & \le & \cdots & & \cdots & & \cdots \\ \vee\!| & & \vee\!| & & & & & & \\ \vdots & & \vdots & & \ddots & & \vdots & & \vdots \\ & & & & & & \vee\!| & & \vee\!| \\ \cdots & & \cdots & & \cdots & \le & u_{k-1}^{(k-1)} & \le & u_{k-1}^{(k)} \\ & & & & & & \vee\!| & & \vee\!| \\ \cdots & & \cdots & & \cdots & \le & u_k^{(k-1)} & \le & u_k^{(k)} \end{bmatrix} d^{k^2}u \\
&= \int_{[0,1]^{k^2-2}} \delta_c(u_1^{(k)} + \cdots + u_k^{(1)}) \cdot \mathbf{1} \begin{bmatrix} & & u_1^{(2)} & \le & \cdots & & \cdots & & \cdots \\ & & \vee\!| & & & & & & \\ u_2^{(1)} & \le & u_2^{(2)} & \le & \cdots & & \cdots & & \cdots \\ \vee\!| & & \vee\!| & & & & & & \\ \vdots & & \vdots & & \ddots & & \vdots & & \vdots \\ & & & & & & \vee\!| & & \vee\!| \\ \cdots & & \cdots & & \cdots & \le & u_{k-1}^{(k-1)} & \le & u_{k-1}^{(k)} \\ & & & & & & \vee\!| & & \\ \cdots & & \cdots & & \cdots & \le & u_k^{(k-1)} & & \end{bmatrix} \\
&\qquad \times \frac{\Delta(u_1^{(2)}, u_2^{(1)})}{1!} \frac{\Delta(u_{k-1}^{(k)}, u_k^{(k-1)})}{1!}\, d^{k^2-2}u \\
&= \cdots \\
&= \int_{[0,1]^k} \delta_c(u_1^{(k)} + \cdots + u_k^{(1)}) \cdot \mathbf{1}(u_k^{(1)} \le u_{k-1}^{(2)} \le \cdots \le u_1^{(k)}) \\
&\qquad \times \frac{\Delta(u_1^{(k)}, u_2^{(k-1)}, \ldots, u_k^{(1)})}{1! \cdot 2! \cdots (k-1)!} \cdot \frac{\Delta(u_1^{(k)}, u_2^{(k-1)}, \ldots, u_k^{(1)})}{1! \cdot 2! \cdots (k-1)!}\, d^k u \\
&= \frac{1}{k!\, G(1+k)^2} \int_{[0,1]^k} \delta_c(w_1 + \cdots + w_k) \Delta(w)^2\, d^k w,
\end{aligned}$$

with the last step following from symmetry. □

We note for the reader familiar with Gelfand–Tsetlin patterns that what we have done in these last few steps is to compute the volume of what is called a Gelfand–Tsetlin polytope. A computation of this volume has appeared before in the literature (see [2] for a proof using representation theory, or [34] for a proof using the Harish–Chandra–Itzykson–Zuber integral), but the elementary proof we give here based on Lemma 4.6 seems to be new.

4.3.3 Ehrhart theory

Theorem 1.4 also allows us to say something about the algebraic character of the quantities we have been discussing.

Corollary 4.8 *Let $c = p/q$ be fixed rational number and k be a fixed integer. If N is a multiple of q, then $I_k(cN, N) = P_{c,k}(N)$, where $P_{c,k}$ is a polynomial of degree $k^2 - 1$.*

Proof This corollary follows from an application of the following theorem of Ehrhart [14]:

Theorem 4.9 *If E is a convex lattice polytope in $\mathbb{R}^n$ (that is, a polytope whose vertices are all integer coordinates), then there is a polynomial P of degree n, such that for all $\ell \in \mathbb{N}_{>0}$,*

$$\#(\mathbb{Z}^n \cap (\ell \cdot E)) = P(\ell).$$

Returning to the corollary at hand, we have from (4.23), when $N = q\ell$,

$$I_k(cN; N) = \#(\mathbb{Z}^{k^2-1} \cap (\ell \cdot [q \cdot V_c])).$$

But then it is straightforward to verify that $qV_c = qV_{p/q}$ is a convex lattice polytope in $\mathbb{R}^{k^2-1}$, so that $I_k(cN; N)$ is a polynomial in ℓ and therefore in N. □

4.4 Large N asymptotic: the complex analysis approach

In this subsection we prove Theorem 1.6. The approach we take is based on the following expression, proved in [7] (Lemma 2.1).

Theorem 4.10 [7] *Let α_i, β_j be complex numbers. Then,*

$$\begin{aligned}
&\int_{U(N)} \prod_{i=1}^{r} \det(I - U^* e^{-\alpha_i}) \prod_{j=1}^{r} \det(I - U e^{-\beta_j}) dU \\
&\quad = \frac{(-1)^r e^{N(\alpha_1+\cdots+\alpha_r)}}{(2\pi i)^{2r}(r!)^2} \oint \cdots \oint e^{-N(z_{r+1}+\cdots+z_{2r})} \prod_{\substack{1\le l\le r \\ r+1\le q\le 2r}} (1 - e^{z_q - z_l})^{-1} \\
&\qquad \times \frac{\Delta(z_1, \ldots, z_{2r})^2}{\prod_{i=1}^{2r}\prod_{j=1}^{r}(z_i - \alpha_j)(z_i - \beta_j)} dz_1 \cdots dz_{2r},
\end{aligned}$$

where $\Delta(z_1, \ldots, z_{2r}) = \prod_{i<j}(z_j - z_i)$ is the vandermonde determinant, and the contour integrals enclose the variables α_i, β_j.

From the definition (4.13), we have

$$\begin{aligned}
P_k(x) = &\frac{(-1)^k x^{kN}}{(2\pi i)^{2k}(k!)^2} \oint \cdots \oint e^{-N(z_{k+1}+\cdots+z_{2k})} \prod_{\substack{1\le l\le k \\ k+1\le q\le 2k}} (1 - e^{z_q - z_l})^{-1} \\
&\times \frac{\Delta(z_1, \ldots, z_{2k})^2}{\prod_{i=1}^{2k}((z_i - a)z_i)^k} dz_1 \cdots dz_{2k}
\end{aligned} \tag{4.25}$$

where $a = \log x$.

We set $m = cN$ and will consider when $0 \le c \le k$ is fixed and $N \to \infty$ in such a way that cN is an integer. We will then need to compute the coefficient of x^{cN} in $P_k(x)$.

We first shrink the contour in (4.10) into small circles centered at 0 and a. This leads to a sum of 2^{2k} multiple integrals, each surrounding either 0 or a; c.f. the calculation in [24]. Taking into account symmetries between the variables and counting the number of ways of picking ℓ of the first k contours to surround a, and $k - \ell$ of the second k contours to surround a, we find

$$P_k(x) = \sum_{\ell=0}^{k} \binom{k}{\ell}^2 P_{k,\ell}(x) \tag{4.26}$$

where $P_{k,\ell}(x)$ is the integral with contours $z_1, \dots, z_\ell, z_{k+\ell+1}, \dots, z_{2k}$ along small circles surrounding $a = \log x$ and $z_{\ell+1}, \dots, z_{k+\ell}$ along small circles surrounding 0. The remaining integrals where there are different numbers of contours surrounding a and 0 do not contribute, as follows from Lemma 4.11, which we prove below.

Next we change variables

$$z_j = \epsilon_j a + \frac{v_j}{N}$$

where

$$\epsilon_j = \begin{cases} 1, & j = 1, \dots, \ell \text{ or } j = k+\ell+1, \dots, 2k \\ 0, & \ell+1 \le j \le k+\ell \end{cases}.$$

This gives that the integrand of $P_{k,\ell}(x)$ is, up to terms of order $1/N$ smaller,

$$\frac{x^{-N(k-\ell)}}{N^{2k}} \frac{e^{-(v_{k+1}+\dots+v_{2k})} \prod_{\substack{i<j \\ \epsilon_i \neq \epsilon_j}} a^2 \prod_{\substack{i<j \\ \epsilon_i = \epsilon_j}} \left(\frac{v_i - v_j}{N}\right)^2 dv_1 \dots dv_{2k}}{\prod_{\substack{t \le k < q \\ \epsilon_t = \epsilon_q}} \frac{v_q - v_t}{N} \prod_{\substack{t \le k < q \\ \epsilon_t \neq \epsilon_q}} \left(1 - x^{\epsilon_q - \epsilon_t} e^{\frac{v_q - v_t}{N}}\right) a^{2k^2} (-1)^{k^2} \prod_{j=1}^{2k} \left(\frac{v_j}{N}\right)^k}. \tag{4.27}$$

The number of pairs $i < j$ with $\epsilon_i \neq \epsilon_j$ is k^2, hence $\prod_{\substack{i<j \\ \epsilon_i \neq \epsilon_j}} a^2 = a^{2k^2}$; and the number of pairs $i < j$ with $\epsilon_i = \epsilon_j$ is $\binom{2k}{2} - k^2 = k^2 - k$, so that

$$\prod_{\substack{i<j \\ \epsilon_i = \epsilon_j}} \left(\frac{v_i - v_j}{N}\right)^2 = \frac{1}{N^{2(k^2-k)}} \prod_{\substack{i<j \\ \epsilon_i = \epsilon_j}} (v_i - v_j)^2.$$

The number of pairs (t, q) with $1 \le t \le k < q \le 2k$ and $\epsilon_t = \epsilon_q$ is $2\ell(k-\ell)$, hence

$$\prod_{\substack{t \le k < q \\ \epsilon_t = \epsilon_q}} \frac{v_q - v_t}{N} = \frac{1}{N^{2\ell(k-\ell)}} \prod_{\substack{t \le k < q \\ \epsilon_t = \epsilon_q}} (v_q - v_t).$$

Therefore (4.27) is equal to

$$(-1)^k x^{-N(k-\ell)} N^{2\ell(k-\ell)} \frac{e^{-(v_{k+1}+\dots+v_{2k})} \prod_{\substack{i<j \\ \epsilon_i = \epsilon_j}} (v_i - v_j)^2 \prod_{j=1}^{2k} \frac{dv_j}{v_j^k}}{\prod_{\substack{t \le k < q \\ \epsilon_t \neq \epsilon_q}} \left(1 - x^{\epsilon_q - \epsilon_t} e^{\frac{v_q - v_t}{N}}\right) \prod_{\substack{t \le k < q \\ \epsilon_t = \epsilon_q}} (v_q - v_t)}.$$

In the denominator, we rewrite the expression $\prod_{\substack{t \le k < q \\ \epsilon_t \neq \epsilon_q}} (1 - x^{\epsilon_q - \epsilon_t} e^{\frac{v_q - v_t}{N}})$ by noting that $x^{\epsilon_q - \epsilon_t}$ is x if $\epsilon_q = 1, \epsilon_t = 0$, which happens when $t = \ell+1, \dots, k$ and $q = k+\ell+1, \dots, 2k$, and it equals x^{-1} if $\epsilon_q = 0$ and $\epsilon_t = 1$, which happens when $t = 1, \dots, \ell$ and $q = k+1, \dots k+\ell$. Thus

$$\prod_{\substack{t \le k < q \\ \epsilon_t \neq \epsilon_q}} \left(1 - x^{\epsilon_q - \epsilon_t} e^{\frac{v_q - v_t}{N}}\right) = \prod_{t=\ell+1}^{k} \prod_{q=k+\ell+1}^{2k} \left(1 - x e^{\frac{v_q - v_t}{N}}\right) \prod_{t=1}^{\ell} \prod_{q=k+1}^{k+\ell} \left(1 - x^{-1} e^{\frac{v_q - v_t}{N}}\right)$$

$$= (-1)^\ell x^{-\ell^2} \prod_{\substack{1 \le t \le k \\ k+1 \le q \le 2k \\ \epsilon_t \neq \epsilon_q}} \left(1 - x e^{(\epsilon_q - \epsilon_t) \frac{v_q - v_t}{N}}\right) \prod_{t=1}^{l} \prod_{q=k+1}^{k+\ell} e^{\frac{v_t - v_q}{N}}.$$

Multiplying by the common pre-factor of $\frac{(-1)^k x^{kN}}{(k!)^2}$ gives that, up to a term of order $1/N$ smaller,

$$P_{k,\ell}(x) \sim (-1)^\ell \frac{x^{\ell(N+\ell)} N^{2\ell(k-\ell)}}{(k!)^2} \frac{1}{(2\pi i)^{2k}}$$

$$\oint \dots \oint \prod_{\substack{1\le t\le k\\ k+1\le q\le 2k\\ \epsilon_t\ne\epsilon_q}} \left(1 - x e^{(\epsilon_q-\epsilon_t)\frac{v_q-v_t}{N}}\right)^{-1} \prod_{t=1}^{l} \prod_{q=k+1}^{k+\ell} \left(e^{\frac{v_t-v_q}{N}}\right) e^{-(v_{k+1}+\dots+v_{2k})}$$

$$\prod_{\substack{1\le t\le \ell,\ k+l+1\le q\le 2k\\ \text{or}\\ \ell+1\le t\le k,\ k+1\le q\le k+\ell}} (v_q - v_t) \prod_{\substack{1\le i<j\le \ell\\ \text{or}\\ k+\ell+1\le i<j\le 2k\\ \text{or}\\ \ell+1\le i<j\le k\\ \text{or}\\ k+1\le i<j\le k+\ell}} (v_j - v_i)^2 \prod_{j=1}^{2k} \frac{dv_j}{v_j^k} \tag{4.28}$$

We need to pick out the coefficient of x^{cN} in $P_{k,\ell}(x)$. (This coefficient is automatically 0 if $\ell(N+\ell) > cN$, so we need only consider $\ell < c$.) We therefore need to find the coefficient of $x^{cN-\ell(N+\ell)} = x^{(c-\ell)N-\ell^2}$ in

$$\prod_{\substack{1\le t\le k\\ k+1\le q\le 2k\\ \epsilon_t\ne\epsilon_q}} \left(1 - x e^{(\epsilon_q-\epsilon_t)\frac{v_q-v_t}{N}}\right)^{-1}. \tag{4.29}$$

We can expand the above to get

$$\sum_{m=0}^{\infty} \sum_{\substack{b_1+\dots+b_{\ell^2+(k-\ell)^2}=m\\ b_i\ge 0}} x^m \exp\left(\sum b_{q,t}(\epsilon_q-\epsilon_t)\frac{v_q-v_t}{N}\right). \tag{4.30}$$

If we consider the pre-factor of $\prod_{t=1}^{\ell}\prod_{q=k+1}^{k+\ell} e^{\frac{v_t-v_q}{N}}$, then the required coefficient is

$$\operatorname{tr}\operatorname{Sym}^{(c-\ell)N} \exp\left(\frac{1}{N}V\right) \tag{4.31}$$

where $V := \operatorname{diag}(v_q - v_t)$ for q and t such that $1 \le t \le k, \quad k+1 \le q \le 2k$ and $\epsilon_t \ne \epsilon_q$.

Next, we use Lemma 4.12, proved below, to deduce that the expression (4.31) is

$$((c-\ell)N)^{k^2-2\ell(k-\ell)-1} J_\ell((c-\ell)\vec{v}) \tag{4.32}$$

with

$$J_\ell(v_1,\dots,v_{2k}) = \int_{\substack{\sum x_{t,q}=1\\ x_{tq}\ge 0}} e^{\sum x_{tq}(\epsilon_q-\epsilon_t)(v_q-v_t)} \prod dx_{tq} \tag{4.33}$$

where the $\ell^2 + (k-\ell)^2$ variables x_{tq} have indices $1 \le t \le k, k+1 \le q \le 2k$ with $\epsilon_t \ne \epsilon_q$, that is either $1 \le t \le \ell, k+1 \le q \le k+\ell$ or $\ell+1 \le t \le k, k+\ell+1 \le q \le 2k$.

Since $P_{k,\ell}(x)$ also has a factor of $N^{2\ell(k-\ell)}$, we get a total contribution of $N^{k^2-1}(c-\ell)^{k^2-2\ell(k-\ell)-1} g_{k,\ell}(c-\ell)$ where

$$g_{k,\ell}(c-\ell) = \frac{(-1)^\ell}{(k!)^2} \frac{1}{(2\pi i)^{2k}} \oint \dots \oint J_\ell((c-\ell)\vec{v})$$

$$e^{-(v_{k+1}+\cdots+v_{2k})} \prod_{\substack{1\le t\le \ell,\ k+\ell+1\le q\le 2k \\ \text{or} \\ \ell+1\le t\le k,\ k+1\le q\le k+\ell}} (v_q - v_t) \prod_{\substack{1\le i<j\le \ell \\ \text{or} \\ k+\ell+1\le i<j\le 2k \\ \text{or} \\ \ell+1\le i<j\le k \\ \text{or} \\ k+1\le i<j\le k+\ell}} (v_j - v_i)^2 \prod_{j=1}^{2k} \frac{dv_j}{v_j^k}. \tag{4.34}$$

The prefactor $g_{k,\ell}(c-\ell)$ depends polynomially on $c-\ell$, because to compute it we need to compute derivatives of $J_\ell((c-\ell)\vec{v})$ at $\vec{v}=0$, which are clearly polynomial in $(c-\ell)$. An examination of (4.34) shows that the degree of $g_{k,\ell}$ is $2\ell(k-\ell)$.

Summing these over $0\le \ell < c$ gives an expression of the form $\gamma_k(c)N^{k^2-1}$, where

$$\gamma_k(c) = \sum_{0\le \ell<c} \binom{k}{\ell}^2 (c-\ell)^{k^2-2\ell(k-\ell)-1} g_{k,\ell}(c-\ell), \tag{4.35}$$

as was to be proved.

It remains now to prove the two lemmas we have used. This we do in the following subsections.

4.4.1 Vanishing of an integral

Denote by $P_k(x; a\epsilon_1, \ldots, a\epsilon_{2k})$ the integral $P_k(x)$ over the circular contours centered in $a\epsilon_i$ when ϵ_i can be either zero or one.

Lemma 4.11 *Let the number of ϵ_i which are equal to* 1 *and the number which are equal to* 0 *be different. Then the integral $P_k(x; a\epsilon_1, \ldots, a\epsilon_{2k})$ is identically zero.*

Proof We consider the case in which there are more zeros then ones. The case in which there are more ones then zeros, can be deduced in the same way. We can choose (without loss of generality) $\epsilon_1, \ldots, \epsilon_{k+1}$ to be zero.

Denote

$$G(z_1, \ldots, z_{k+1}) := e^{-N(z_{k+1}+\cdots+z_{2k})} \times \prod_{\substack{1\le l\le k \\ k+1\le q\le 2k}} (1-e^{z_q-z_l})^{-1} \frac{\Delta(z_1, \ldots, z_{2k})}{\prod_{i=1}^{2k}(z_i-a)^k \prod_{i=k+2}^{2k}(z_i)^k}$$

This function is analytic around zero. The poles that arise when $z_q = z_l$ cancel with the Vandermonde determinant. Next, we use the residue theorem in order to compute the integral. Consider the Vandermonde determinant expansion:

$$\Delta(z_1, \ldots, z_{2k}) = \sum_{\sigma\in S_{2k}} \mathrm{Sgn}(\sigma) \left(\prod_{i=1}^{2k} (z_i)^{\sigma(i)-1} \right).$$

By the residue theorem we need to show that the coefficient of $\prod_{i=1}^{k+1}(z_i)^{k-1}$ in the product $G(z_1, \ldots, z_{k+1})\Delta(z_1, \ldots, z_{2k})$ is zero. For this purpose, since $G(z_1, \ldots, z_{k+1})$ is analytic around zero, it is enough to show that there is no monomial term in the expansion of $\Delta(z_1, \ldots, z_{2k})$ of the form $\prod_{i=1}^{k+2}(z_i)^{\sigma(i)-1}$ with $\sigma(i)-1 \le k-1$ for $i = 1, \ldots, k+1$. Since σ is a permutation this is clearly the case. □

4.4.2 A lemma on geometric sums

Let $V = \mathrm{diag}(v_1, \ldots, v_d)$ be a diagonal $d \times d$ matrix, and M a large parameter. We want to compute the asymptotic behaviour of

$$\mathrm{tr}\,\mathrm{Sym}^M \exp\left(\frac{1}{M}V\right) = \sum_{\substack{k_1+\cdots+k_d=M \\ k_1,\ldots,k_d\geq 0}} \exp\left(\frac{1}{M}\sum_{j=1}^{d} k_j v_j\right). \tag{4.36}$$

This is the coefficient of x^M in the power series expansion of

$$\det\left(I - x\exp\left(\frac{1}{M}V\right)\right)^{-1} = \frac{1}{\prod_{j=1}^{d}(1 - e^{v_j/M}x)}.$$

Lemma 4.12 *As $M \to \infty$,*

$$\mathrm{tr}\,\mathrm{Sym}^M \exp\left(\frac{1}{M}V\right) = M^{d-1} \iint\limits_{\substack{x_1+\cdots+x_d=1 \\ x_j\geq 0}} e^{\sum x_j v_j} dx_1 \ldots dx_d + O(M^{d-2}).$$

Proof Dividing by M^{d-1} we get a Riemann sum

$$\frac{1}{M^{d-1}} \sum_{\substack{k_1+\cdots+k_d=M \\ k_1,\ldots,k_d\geq 0}} e^{\frac{1}{M}\sum_{j=1}^{d} k_j v_j} = \iint\limits_{\substack{x_1+\cdots+x_d=1 \\ x_j\geq 0}} e^{\sum x_j v_j} dx_1 \ldots dx_d + O\left(\frac{1}{M}\right)$$

□

4.4.3 Example: leading coefficient in the range $0 < c \leq 1$

The leading coefficient in $I_k(cN, N)$ (i.e., the coefficient of N^{k^2-1}) when $0 < c \leq 1$, can be obtained from (4.3). Thus for $0 < c \leq 1$, we have $\gamma_k(c) = \frac{c^{k^2-1}}{(k^2-1)!}$. We now verify that the complicated expression that we got in this section for the leading coefficient $\gamma_k(c)$, agrees with the above. Note that because of the functional equation, Lemma 4.1, we can conclude that this holds also in the range $(k-1)N \leq c \leq kN$

The leading coefficient of $I_k(cN, N)$ when $0 < c \leq 1$ is $\gamma_k(c) = c^{k^2-1} g_{k,0}(c)$ where

$$\begin{aligned} g_{k,0}(c) &= \frac{1}{(k!)^2} \frac{1}{(2\pi i)^{2k}} \oint \dots \oint J_0(c\vec{v}) e^{-(v_{k+1}+\dots+v_{2k})} \\ &\quad \times \prod_{\substack{1 \leq i < j \leq k \\ \text{or} \\ k+1 \leq i < j \leq 2k}} (v_j - v_i)^2 \prod_{j=1}^{2k} \frac{dv_j}{v_j^k} \\ &= \frac{1}{(k!)^2} \frac{1}{(2\pi i)^{2k}} \oint \dots \oint J_0(c\vec{v}) e^{-(v_{k+1}+\dots+v_{2k})} \\ &\quad \times \Delta(v_1, \dots, v_k)^2 \Delta(v_{k+1}, \dots, v_{2k})^2 \prod_{j=1}^{2k} \frac{dv_j}{v_j^k}. \end{aligned} \tag{4.37}$$

By the residue theorem, in order to compute $g_{k,0}(c)$ we need to find the coefficient of $\prod_{j=1}^{2k} v_j^{k-1}$ in the expansion of

$$J_0(c\vec{v}) e^{-(v_{k+1}+\dots+v_{2k})} \Delta(v_1, \dots, v_k)^2 \Delta(v_{k+1}, \dots, v_{2k})^2.$$

Consider the vandermonde determinant expansion:

$$\Delta(v_1, \dots, v_k)^2 = \sum_{\sigma, \sigma' \in S_k} \mathrm{Sgn}(\sigma) \mathrm{Sgn}(\sigma') \prod_{i=1}^{k} (v_i)^{\sigma(i)+\sigma'(i)-2}. \tag{4.38}$$

We are looking for terms of the form $\prod_{i=1}^{k} (v_i)^{\sigma(i)+\sigma'(i)-2}$ with $\sigma(i)+\sigma'(i)-2 \leq k-1$ for all $1 \leq i \leq k$. Since $\sigma(i)$ and $\sigma'(i)$ are permutations, the only such term is $k! \prod_{i=1}^{k} (v_i)^{k-1}$. In the same way, the only possible contribution from $\Delta(v_{k+1}, \dots, v_{2k})^2$ to the integral comes from the term $k! \prod_{i=k+1}^{2k} (v_i)^{k-1}$. That means that the term $J_0(c\vec{v}) e^{-(v_{k+1}+\dots+v_{2k})}$ can contribute only a constant. Therefore, the calculation comes down to verifying that $J_0(c\vec{v}) = \frac{1}{(k^2-1)!}$ when $\vec{v} = 0$. This is indeed the case, since when $\vec{v} = 0$, $J_0(c\vec{v})$ is the volume of a $k^2 - 1$ dimensional simplex, which is $\frac{1}{(k^2-1)!}$ as required.

5 Justification of Conjecture 1.1

Our final goal is to sketch briefly a justification for Conjecture 1.1 without reference to the function field results in the body of the paper. In addition, we indicate how to generate a conjecture for the lower order terms in the asymptotic expansion (1.1), as noted at the end of Sect. 1.3.

We start by defining

$$Q_k(\alpha, T) = \frac{1}{T(\log T)^{k^2}} \int_0^T \zeta\left(\frac{1}{2} + \frac{i\alpha}{\log T} + \mathrm{i}t\right)^k \zeta\left(\frac{1}{2} + \frac{i\alpha}{\log T} - \mathrm{i}t\right)^k dt. \tag{5.1}$$

We have the Riemann–Stieljes integral identity,

$$\zeta^k(1/2 + i\alpha/\log T + it) = \int_{-\infty}^{\infty} e^{-i\alpha x/\log T} e^{-ixt} e^{-x/2} d\Delta_k(e^x).$$

Substituting this into (5.1) and swapping the order of integration, we find that

$$Q_k(\alpha, T) \sim \frac{T}{(\log T)^{k^2-1}} \int_{-\infty}^{\infty} e^{-2i\alpha u} \frac{1}{T^u} \Delta_k^2 \left(T^u;\ T^{u-1}\right) du.$$

Hence, by Fourier inversion, on average

$$\frac{T^{1-v}}{(\log T)^{k^2-1}} \Delta_k^2(T^v;\ T^{v-1}) \sim \int_{-\infty}^{\infty} Q_k(\pi\beta, T) \mathrm{e}^{2\pi i\beta v} d\beta. \tag{5.2}$$

Conjecture 1.1 now follows from a conjecture of Kösters [27]:

$$\lim_{T\to\infty} Q_k(\alpha, T) = a_k \lim_{N\to\infty} W_k(\alpha, N), \tag{5.3}$$

where we write

$$W_k(\alpha, N) = \frac{1}{N^{k^2}} \int_{U(N)} \det\left(1 - e^{-i\alpha/N} U\right)^k \det\left(1 - e^{-i\alpha/N} U^*\right)^k dU$$

and a_k is given by (1.9). (This is a matter of coupling Eq. (1.2) and Conjecture 1.2 of [27].) We then have, using (4.2) to expand the random matrix integral,

$$\begin{aligned} W_k(\alpha, N) &= \frac{1}{N^{k^2}} \sum_{0\le m\le kN} I_k(m; N) e^{-2i\alpha m/N} \\ &= \frac{1}{N^{k^2}} \sum_{0\le m\le kN} e^{-2i\alpha m/N} \left(\gamma_k(m/N) N^{k^2-1} + O_k(N^{k^2-2})\right) \\ &\sim \frac{1}{N} \sum_{m\ge 0} e^{-2i\alpha m/N} \gamma_k(m/N) \mathbf{1}_{[0,k]}(m/N) \\ &\sim \int_0^k e^{-2i\alpha u} \gamma_k(u)\, du, \end{aligned} \tag{5.4}$$

as the last sum is a Riemann sum.

Setting $X = T^u$ and $H = T^{u-1}$ in (5.2) implies that for $x \approx X$, on average

$$\frac{\Delta_k^2(x;\ H)}{H\left(\frac{\log X}{u}\right)^{k^2-1}} \sim a_k \gamma_k(u).$$

We may impose $H = X^\delta$ by setting $u = 1/(1-\delta)$. The restriction that $u \in [0, k]$ becomes $\delta \in [0, 1 - 1/k]$ and the Conjecture follows.

The expression (5.3) follows from conjectures in [8] which relate $Q_k(\alpha, T)$ to a combinatorial sum, like that in Theorem 4.3, and to a multiple contour integral, like that in Theorem 4.10, which include arithmetic factors [27]. Specifically, it follows from a leading-order asymptotic evaluation of the multiple contour integral that is similar to the calculation given here in Sect. 4.4. A calculation of lower order terms, as in Sect. 4.2 of the present paper, leads to a polynomial of order $k^2 - 1$ in the variable $\log X$ for the second moment of Δ_k.

References

1. Andrade, J.C., Bary-Soroker, L., Rudnick, Z.: Shifted convolution and the Titchmarsh divisor problem over $\mathbb{F}_q[T]$. Philos. Trans. A **373**, 20140308–20140318 (2040)
2. Baryshnikov, Y.: GUEs and queues. Probab. Theory Rel. Fields **119**, 256–274 (2001)
3. Blomer, V.: The average value of divisor sums in arithmetic progressions. Q. J. Math. **59**, 275–286 (2008)
4. Bump, D.: Lie groups. Graduate texts in mathematics, vol. 225. Springer, New York (2004)
5. Bump, D., Gamburd, A.: On the averages of characteristic polynomials from classical groups Comm. Math. Phys. **265**(1), 227–274 (2006)
6. Conrey, J.B., Gonek, S.M.: High moments of the Riemann zeta-function. Duke Math. J. **107**(3), 577–604 (2001)
7. Conrey, J.B., Farmer, D.W., Keating, J.P., Rubinstein, M.O., Snaith, N.C.: Autocorrelation of random matrix polynomials. Commun. Math. Phys. **237**, 365–395 (2003)
8. Conrey, J.B., Farmer, D.W., Keating, J.P., Rubinstein, M.O., Snaith, N.C.: Integral moments of L-functions. Proc. Lond. Math. Soc. **91**(3), 33–104 (2005)
9. Coppola, G., Salerno, S.: On the symmetry of the divisor function in almost all short intervals. Acta Arith. **113**(2), 189–201 (2004)
10. Cramér, H.: Über zwei Sätze des Herrn G. H. Hardy. Math. Z **15**(1), 201–210 (1922)
11. Davenport, H.: On a principle of Lipschitz. J. Lond. Math. Soc. **26**, 179–183 (1951)
12. Davenport, H.: Corrigendum: on a principle of Lipschitz. J. Lond. Math. Soc. **39**, 580 (1964)
13. Diaconis, P., Gamburd, A.: Random matrices, magic squares and matching polynomials. Electron. J. Comb. 11(2), 26 (2004/06) (**Research Paper 2**)
14. Ehrhart, E.: Sur un probleme de geometrie diophantienne lineaire II. J. Reine Angew. Math. **227**, 2549 (1967)
15. Fouvry, É., Ganguly, S., Kowalski, E., Michel, P.: Gaussian distribution for the divisor function and Hecke eigenvalues in arithmetic progressions. Comment. Math. Helv. **89**(4), 979–1014 (2014)
16. Fouvry, É., Ganguly, S., Kowalski, E., Michel, P.: On the exponent of distribution of the ternary divisor function. Mathematika, 1–24 (2015). doi:10.1112/S0025579314000096, arXiv:1304.3199 [math.NT]
17. Gamburd, A.: Some applications of symmetric functions theory in random matrix theory. LMS Lect. Note Ser. **341**, 143–170 (2007)
18. Heath-Brown, D.R.: The distribution and moments of the error term in the Dirichlet divisor problem. Acta Arith. **60**(4), 389–415 (1992)
19. Ivić, A.: On the mean square of the divisor function in short intervals. J. Théor. Nombres Bordeaux **21**(2), 251–261 (2009)
20. Ivić, A.: On the divisor function and the Riemann zeta-function in short intervals. Ramanujan J. **19**(2), 207–224 (2009)
21. Jutila, M.: On the divisor problem for short intervals. Studies in honour of Arto Kustaa Salomaa on the occasion of his fiftieth birthday. Ann. Univ. Turku. Ser. A **I**(186), 23–30 (1984)
22. Katz, N.M.: On a question of Keating and Rudnick about primitive Dirichlet characters with squarefree conductor. Int. Math. Res. Not. **2013**(14), 3221–3249 (2013)
23. Katz, N.M.: Witt vectors and a question of Keating and Rudnick. Int. Math. Res. Not. **2013**(16), 3613–3638 (2013)
24. Keating, J.P.: Symmetry transitions in random matrix theory and L-Functions. Commun. Math. Phys. **281**, 499–528 (2008)
25. Keating, J.P., Rudnick, Z.: The variance of the number of prime polynomials in short intervals and in residue classes. Int. Math. Res. Not. (2012). doi:10.1093/imrn/rns220
26. Keating, J.P., Rudnick, Z.: Squarefree polynomials and Möbius values in short intervals and arithmetic progressions. Algebra Number Theory **10**(2), 375–420 (2016)
27. Kösters, H.: On the occurrence of the sine kernel in connection with the shifted moments of the Riemann zeta function. J. Number Theory **130**, 2596–2609 (2010)
28. Kowalski, E., Ricotta, G.: Fourier coefficients of GL(N) automorphic forms in arithmetic progressions. Geom. Funct. Anal. **24**, 1229–1297 (2014)
29. Lau, Y.K., Zhao, L.: On a variance of Hecke eigenvalues in arithmetic progressions. J. Number Theory **132**(5), 869–887 (2012)
30. Lester, S.: On the variance of sums of divisor functions in short intervals. Proc. Amer. Math. Soc. **144**(12), 5015–5027 (2016)
31. Lester, S., Yesha, N.: On the distribution of the divisor function and Hecke eigenvalues. Israel J. Math. **212**(1), 443–472 (2016)
32. Milinovich, M.B., Turnage-Butterbaugh, C.L.: Moments of products of automorphic L-functions. J. Number Theory **139**, 175–204 (2014)

33. Motohashi, Y.: On the distribution of the divisor function in arithmetic progressions. Acta Arith. **22**, 175–199 (1973)
34. Olshanksi, G.: Projections of orbital measures, Gelfand–Tsetlin polytopes, and splines. J. of Lie Theory **23**(4), 1011–1022 (2013)
35. Schmidt, W.M.: Northcott's theorem on heights II. The quadratic case. Acta Arith. **70**(4), 343–375 (1995)
36. Shiu, P.: A Brun–Titchmarsh theorem for multiplicative functions. J. Reine Angew. Math. **313**, 161–170 (1980)
37. Soundararajan, K.: Moments of the Riemann zeta function. Ann. Math. **170**(2), 981–993 (2009)
38. Stanley, R.P.: Enumerative combinatorics. Volume 2, Cambridge Studies in Advanced Mathematics, vol. 62. Cambridge University Press, Cambridge (1999)
39. Titchmarsh, E.C.: The theory of the Riemann zeta-function, 2nd edn. In: Heath-Brown, D.R. (ed.) Oxford University Press, New York (1986)
40. Tong, K.C.: On divisor problems III. Acta Math. Sin. **6**, 515–541 (1956)