This is a ``preproof'' accepted article for *Canadian Mathematical Bulletin*
This version may be subject to change during the production process.
DOI: 10.4153/S0008439525000025

Canad. Math. Bull. Vol. **00** (0), 2020 pp. 1–15
http://dx.doi.org/10.4153/xxxx
© Canadian Mathematical Society 2020

A Function Field Analogue of Jacobi's Theorem on Sums of Squares and its Moments

Wentang Kuo, Yu-Ru Liu and Yash Totani

Abstract. **In this paper, we establish a function field analogue of Jacobi's theorem on sums of squares and analyze its moments. Our approach involves employing two distinct techniques to derive the main results concerning asymptotic formulas for the moments. The first technique utilizes Dirichlet series framework to derive asymptotic formulas in the limit of large finite fields, specifically when the characteristic of $\mathbb{F}_q[T]$ becomes large. The second technique involves effectively partitioning the set of polynomials of a fixed degree, providing asymptotic formulas in the limit of large polynomial degree.**

1 Introduction

The problem of representing integers as sums of squares has garnered extensive attention in mathematical research. Jacobi's theorem on sums of two squares provides a fundamental result in this domain, stating that the number of ways $r_2(n)$ to express a positive integer n as a sum of two squares is given by

$$r_2(n) = 4\left(d_1(n) - d_3(n)\right),$$

where $d_i(n)$ is the number of divisors of n congruent to i modulo 4 for $i = 1, 3$. Let the letters p, q represent primes congruent to $1, -1$ modulo 4 respectively. An equivalent formulation of Jacobi's theorem can be stated as follows. Let $n \in \mathbb{N} = \{1, 2, 3 \cdots\}$ have the factorisation

$$n = 2^a \prod_{i=1}^{k} p_i^{b_i} \prod_{j=1}^{l} q_j^{c_j}$$

for positive integers b_i, c_j for $1 \le i \le k$, $1 \le j \le l$. Then, as in [4, Theorem 278],

$$r_2(n) = \begin{cases} 4\prod_{i=1}^{k}(b_i+1) & \text{if } c_j \text{ is even for all } j \le l, \\ 0 & \text{otherwise.} \end{cases}$$

In [4], Hardy and Littlewood present a formula for the Dirichlet series corresponding to $r_2(n)$ in terms of $\zeta(s)$ and $L_{-4}(s)$. Here $\zeta(s)$ is the Riemann zeta function and $L_{-4}(s)$

2020 Mathematics Subject Classification: 11T55, 11N37.
Keywords: sums of squares, quadratic forms, Jacobi's theorem, number of representations, polynomial rings.

https://doi.org/10.4153/S0008439525000025 Published online by Cambridge University Press

is the L-function corresponding to the Kronecker symbol $\left(\frac{-4}{n}\right)$. The formula states

$$\sum_{n=1}^{\infty} \frac{r_2(n)}{n^s} = 4\zeta(s)L_{-4}(s).$$

The Gauss circle problem, which seeks to determine the number of integer lattice points inside a circle of radius r centered at the origin, is linked to the study of the first moment of $r_2(n)$. Sierpinski's result [6, Satz 509] provides insight into the first moment of $r_2(n)$ indicating that

$$\sum_{n \le x} r_2(n) = \pi x + O(x^{1/3}).$$

While it is conjectured that the exponent in the error term could be $1/4+\epsilon$, this conjecture remains elusive. Borwein and Choi [2] derived the following asymptotic expression for the second moment of $r_2(n)$.

$$\sum_{n \le x} r_2^2(n) = 4x \log x + 4\alpha x + O(x^{2/3}),$$

where $\alpha = 2.0166\cdots$. Their approach hinges on a Dirichlet series representation for $r_2^2(n)$:

$$\sum_{n=1}^{\infty} \frac{r_2^2(n)}{n^s} = \frac{(4\zeta(s)L_{-4}(s))^2}{(1+2^{-s}\zeta(2s))}.$$

Connors and Keating [3] explore higher moments of $r_2(n)$ to analyze accidental degeneracies in energy levels for square billiards, quantifying deviations from a Poisson distribution. In addition to its connections with the aforementioned issues, the exploration of moments in the representation theory of quadratic forms is inherently intriguing.

An integer can be expressed as a sum of two squares if and only if it is the norm of a Gaussian integer, meaning it is the norm of an element in the ring $\mathbb{Z}[i]$. A natural analogue over $\mathbb{F}_q[T]$ is to consider norms of the extension ring $\mathbb{F}_q[\sqrt{-T}]$. Let $\mathcal{M}_{n,q}$ denote the set of monic polynomials of degree n with coefficients in $\mathbb{F}_q$. For $f \in \mathcal{M}_{n,q}$, define

$$b_q(f) = \begin{cases} 1, & f = \alpha^2 + T\beta^2 \ \text{ for } \ \alpha, \beta \in \mathbb{F}_q[T], \\ 0, & \text{otherwise.} \end{cases}$$

The counting function $B_q(n) = \sum_{f \in \mathcal{M}_{n,q}} b_q(f)$ was examined by Bary-Soroker, Smilansky and Wolf in [1], drawing parallels to Landau's theorem on sums of squares. For $f \in \mathcal{M}_{n,q}$, let

$$r_2^*(f) = \#\{(\alpha, \beta), \alpha, \beta \in \mathbb{F}_q[T] : f = \alpha^2 + T\beta^2\}.$$

In this article, we investigate the function $r_2^*(f)$ and its moments for polynomial rings $\mathbb{F}_q[T]$, where q is a prime power. A key focus will be comparing these results with the known results for $r_2(n)$.

When $\mathbb{F}_q$ has characteristic 2, the Frobenius map $\phi : \mathbb{F}_q \to \mathbb{F}_q$ defines an isomorphism, making the study trivial. When $\mathbb{F}_q$ has odd characteristic, the formula for $r_2^*(f)$ is analogous to the one we get in the classical case. We obtain

https://doi.org/10.4153/S0008439525000025 Published online by Cambridge University Press

***Theorem* 1.1** *Let $f = T^a P_1^{c_1} P_2^{c_2} \dots P_k^{c_k} Q_1^{2d_1} \dots Q_l^{2d_l}$ be the prime factorisation of $f \in \mathcal{M}_{n,q}$ such that $\left(\frac{P_i}{T}\right) = 1$ and $\left(\frac{Q_j}{T}\right) = -1, \forall i, j$. Then*

$$r_2^*(f) = 2 \prod_{i=1}^{k} (c_i + 1).$$

The main difference between the classical and the function field analogue seems to be a factor of 2 reflecting the number of units in the ring of integers. The ring $\mathbb{Z}[i]$ has four units of norm 1, whereas $\mathbb{F}_q[\sqrt{-T}]$ only has two units of norm 1.

Let $\mathcal{M}$ be the set of monic polynomials, and let $\zeta_q(s)$ be the zeta function of $\mathbb{F}_q[T]$. Analogous to the Dirichlet series in the classical case, we find that the Dirichlet series for r_2^* has the form

$$\sum_{f \in \mathcal{M}} \frac{r_2^*(f)}{|f|^s} = 2\zeta_q(s).$$

The Dirichlet series for the square of r_2^* is computed as

$$\sum_{f \in \mathcal{M}} \frac{(r_2^*)^2(f)}{|f|^s} = \frac{4\zeta_q^2(s)}{\zeta_q(2s)(1 + q^{-s})}.$$

See Theorem 3.1 and Theorem 3.2 for more details. We note that the L-series $L_\chi(s)$ corresponding to the quadratic character $\chi(f) = \left(\frac{f}{T}\right)$ is trivially equal to 1 (see section 4). This simplifies the above formulae even further in contrast.

Employing the Dirichlet series described above, we derive the following formulae.

***Theorem* 1.2** *Let $\mathbb{F}_q$ be a field of odd characteristic. The first and the second moments for $r_2^*(f)$ are given by*

$$\sum_{f \in \mathcal{M}_{n,q}} r_2^*(f) = 2q^n,$$

and

$$\sum_{f \in \mathcal{M}_{n,q}} (r_2^*)^2(f) = 4(n+1)q^n + 4\sum_{k=1}^{n-1} (-1)^k (2n - 2k + 1) q^{n-k} + 4(-1)^n.$$

The absence of error terms in the formulae can be attributed to the fact that the L-function $L_\chi(s)$ is constant and equal to 1. While the Dirichlet series approach proves effective for the first and second moments, it encounters limitations with higher moments.

For higher moments, we split the study into two scenarios. First, in the large degree limit, we fix q and obtain asymptotic formulas as n gets large. In this scenario, asymptotic formulae are obtained rather than exact formulae, as the Dirichlet series cannot be represented solely in terms of the zeta function $\zeta_q(s)$ and the L-function $L_\chi(s)$. Utilizing techniques similar to those in [3], we investigate the Dirichlet series for the i-th power of r_2^*, leading to the following results.

https://doi.org/10.4153/S0008439525000025 Published online by Cambridge University Press

***Theorem* 1.3** *Let $\mathbb{F}_q$ be a field of odd characteristic. For a fixed q and $i \in \mathbb{N}$ with $i \geq 3$, the i-th moment for r_2^* is given by*

$$\sum_{f \in \mathcal{M}_{n,q}} (r_2^*)^i(f) = -B_i(1)2^i \binom{n + 2^{i-1} - 1}{n} q^n + O(q^{n-1}),$$

where $B_i(1)$ is a fixed constant depending on i and q obtained from the Dirichlet series for $(r_2^*)^i$. The error term has a dependence on i and q.

Explicitly describing the constant $B_i(1)$ using the above methods is a non-trivial problem.

In the second scenario, we obtain asymptotic formulas in the large finite field limit, i.e., when n is fixed and q gets large. Inspired by the techniques in [1], we obtain the main result of this paper, which provides a second-order term for the higher moments. We make a note that in the integer setting, such formulae are not known.

***Theorem* 1.4** *Let $\mathbb{F}_q$ be a field of odd characteristic and $f \in \mathcal{M}_{n,q}$. For $i \in \mathbb{N}$, the i^{th} moment for r_2^* for a fixed n is given by*

$$\sum_{f \in \mathcal{M}_{n,q}} (r_2^*)^i(f) = 2^i \gamma_{i,n} q^n - \alpha_{i,n} q^{n-1} + O(q^{n-2}),$$

where

$$\alpha_{i,n} = \left(2^{2i-1} - 2^i\right) \gamma_{i,n-1} + \left(2^{2i-1} + 2^{3i-2} - 2^{i-1} - 2^{i-1}3^i\right) \gamma_{i,n-2}$$

and $\gamma_{i,n}$ is the binomial coefficient

$$\gamma_{i,n} = \binom{n + 2^{(i-1)} - 1}{n}.$$

The error term has a dependence on i and n.

Specifically, for $i = 1, 2$, the first two terms of the result align with the first and second moments outlined in Theorem 1.2.

2 Number of representations in the form $A^2 + TB^2$

Fix an odd prime power q. Define the embedding $\mathbb{F}_q[T] \subset \mathbb{F}_q[S]$, where $S = \sqrt{-T}$. There are two automorphisms of $\mathbb{F}_q[S]$ that fix $\mathbb{F}_q[T]$ defined by the actions $S \to \pm S$. The norm map

$$N : \mathbb{F}_q[S] \to \mathbb{F}_q[T]$$

is given by

$$N(A + SB) = (A + SB)(A - SB) = A^2 + TB^2, A, B \in \mathbb{F}_q[T].$$

https://doi.org/10.4153/S0008439525000025 Published online by Cambridge University Press

For $f \in \mathcal{M}_{n,q}$, we define the Legendre symbol $\left(\frac{f}{T}\right)$ as follows.

$$\left(\frac{f}{T}\right) = \begin{cases} 1 & f \text{ is a square modulo } T,\ T \nmid f \\ -1 & f \text{ is a non-square modulo } T,\ T \nmid f \\ 0 & T \mid f \end{cases}$$

Then, by [1, Theorem 2.5], $b_q(f) = 1$ if and only if every monic irreducible polynomial Q with $\left(\frac{Q}{T}\right) = -1$ appears with even multiplicity in the prime factorisation of f. Before we proceed any further, we reserve the letters P and Q for monic irreducibles in $\mathbb{F}_q[T]$ with $\left(\frac{P}{T}\right) = 1$ and $\left(\frac{Q}{T}\right) = -1$ respectively. It is clear that the irreducible element T is not in any of the categories we mentioned since $\left(\frac{T}{T}\right) = 0$. We are now ready to prove Theorem 1.1.

Proof From the definitions, we see that $b_q(f) = 1$ if and only if $f = N(h)$ for some $h \in \mathbb{F}_q[S]$. So the question is how many elements in $\mathbb{F}_q[S]$ have norm f. Let us see what happens when f is a prime power.

We know from [1, Proposition 2.4] that $\pm Q$ are the only primes of norm Q^2. We deduce that if $f = Q^{2d}$, where $\left(\frac{Q}{T}\right) = -1$, then $\pm Q^d$ are the only elements in $\mathbb{F}_q[S]$ with norm f.

If $f = P^c$, where $\left(\frac{P}{T}\right) = 1$, then there are exactly $2(c+1)$ elements with norm f. To see this, if $N(q+rS) = P$, then $N(q-rS) = P$ as well. and hence $N(\pm(q+rS)^i(q-rS)^{c-i}) = P^i$ for all $0 \le i \le c$. The last thing we should check is the uniqueness of elements of norm P. If,

$$N(q+rS) = N(t+uS) = P$$

for $q, r, t, u \in \mathbb{F}_q[T]$. Then,

$$(q+rS)(q-rS) = (t+uS)(t-uS),$$

each of the factors being an irreducible polynomial in $\mathbb{F}_q[S]$ (the irreducibilty comes from [1, Lemma 2.1]). Without loss of generality, assume that

$$q + rS = c(t + uS)$$

for some $c \in \mathbb{F}_q$. Taking the norms and observing that P is monic, we get that c has to be an element of order 2 and the only elements of order 2 in $\mathbb{F}_q$ are ± 1. Hence, the result is evident. ∎

3 First and second Moments of r_2^* using Dirichlet series

In this section, we will study the Dirichlet series to arrive at the first and second moments of r_2^*. For $f = T^c P_1^{a_1} P_2^{a_2} \ldots P_k^{a_k} Q_1^{2c_1} Q_2^{2c_2} \ldots Q_r^{2c_r}$, we have $r_2^*(f) = 2\prod_{i=1}^{k}(a_i+1)$. Let $\delta_2(f) = \frac{r_2^*(f)}{2}$. Then $\delta_2(f)$ is a multiplicative function. Let $\mathcal{M}$ and $\mathcal{P}$ be the set of monic polynomials and the set of monic irreducibles in $\mathbb{F}_q[T]$ respectively. We want to study the Dirichlet series

$$L_i(s) = \sum_{f \in \mathcal{M}} \delta_2^i(f)|f|^{-s}$$

https://doi.org/10.4153/S0008439525000025 Published online by Cambridge University Press

for $i = 1, 2$, where $|f| = q^{\deg(f)}$. Since $\delta_2(f)$ is multilplicative, we have a product of local factors

$$L_i(s) = \prod_{R\in\mathcal{P}}\left(\sum_{k=0}^{\infty}\delta_2^i(R^k)|R|^{-ks}\right),$$

where

$$\delta_2^i\left(R^k\right) = \begin{cases}(k+1)^i & \text{if } \left(\frac{R}{T}\right)=1,\\ 1 & \text{if } R=T,\\ 1 & \text{if } \left(\frac{R}{T}\right)=-1 \text{ and } 2\mid k,\\ 0 & \text{if } \left(\frac{R}{T}\right)=-1 \text{ and } 2\nmid k.\end{cases}$$

Let χ be the quadratic character given by $\chi(f) = \left(\frac{f}{T}\right)$. The associated L series is

$$L_\chi(s) = \sum_{f\in\mathcal{M}}\chi(f)|f|^{-s} = \prod_{\left(\frac{P}{T}\right)=1}(1-|P|^{-s})^{-1}\prod_{\left(\frac{Q}{T}\right)=-1}(1+|Q|^{-s})^{-1}. \tag{3.1}$$

Since χ is defined modulo a linear polynomial, $L_\chi(s) = 1$. The zeta function in $\mathbb{F}_q$ is given by

$$\begin{aligned}\zeta_q(s) &= \sum_{f\in\mathcal{M}}|f|^{-s} = (1-q^{-s})^{-1}\prod_{\left(\frac{P}{T}\right)=1}(1-|P|^{-s})^{-1}\prod_{\left(\frac{Q}{T}\right)=-1}(1-|Q|^{-s})^{-1}\\ &= \frac{1}{1-q^{1-s}}.\end{aligned} \tag{3.2}$$

See [7, Chapter 2, equation 1] for a proof.

Theorem 3.1 *We have*

$$L_1(s) = \zeta_q(s),$$

where $\zeta_q(s)$ is the zeta function in $\mathbb{F}_q[T]$.

Proof From the Euler product and the description of $\delta_2(P^k)$ provided above, we get

$$\begin{aligned}L_1(s) &= \left(\sum_{k=0}^{\infty}|T|^{-ks}\right)\prod_{\left(\frac{P}{T}\right)=1}\left(\sum_{k=0}^{\infty}(k+1)|P|^{-ks}\right)\prod_{\left(\frac{Q}{T}\right)=-1}\left(\sum_{k=0}^{\infty}|Q|^{-2ks}\right)\\ &= (1-q^{-s})^{-1}\prod_{\left(\frac{P}{T}\right)=1}(1-|P|^{-s})^{-2}\prod_{\left(\frac{Q}{T}\right)=-1}\left(1-|Q|^{-2s}\right)^{-1}.\end{aligned} \tag{3.3}$$

Comparing (3.3), (3.1) and (3.2), we get

$$L_1(s) = L_\chi(s)\zeta_q(s) = \zeta_q(s).$$

■

Theorem 3.2 *We have*

$$L_2(s) = \frac{\zeta_q^2(s)}{\zeta_q(2s)(1+q^{-s})}.$$

https://doi.org/10.4153/S0008439525000025 Published online by Cambridge University Press

Proof From the Euler product and the description of $\delta_2(R^k)$ provided at the beginning of the section, we get

$$\begin{aligned}
L_2(s) &= \left(\sum_{k=0}^{\infty} |T|^{-ks}\right) \prod_{\left(\frac{P}{T}\right)=1} \left(\sum_{k=0}^{\infty} (k+1)^2 |P|^{-ks}\right) \prod_{\left(\frac{Q}{T}\right)=-1} \left(\sum_{k=0}^{\infty} |Q|^{-2ks}\right) \\
&= (1-q^{-s})^{-1} \prod_{\left(\frac{P}{T}\right)=1} \left(2\,(1-|P|^{-s})^{-3} - (1-|P|^{-s})^{-2}\right) \prod_{\left(\frac{Q}{T}\right)=-1} \left(1-|Q|^{-2s}\right)^{-1} \\
&= \zeta_q(s) L_\chi(s) \left[\prod_{\left(\frac{P}{T}\right)=1} \left(2\,(1-|P|^{-s})^{-1} - 1\right)\right] \\
&= \zeta_q(s) L_\chi(s) \prod_{\left(\frac{P}{T}\right)=1} \frac{(1+|P|^{-s})}{(1-|P|^{-s})} \\
&= \zeta_q(s) L_\chi(s) \prod_{\left(\frac{P}{T}\right)=1} \frac{(1-|P|^{-2s})}{(1-|P|^{-s})^2}.
\end{aligned}$$

Here we used the fact that

$$\frac{2}{(1-x)^3} - \frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1)^2 x^k.$$

We now multiply and divide the equation by $\prod_{\left(\frac{Q}{T}\right)=-1}(1-|Q|^{-2s})$. We get

$$L_2(s) = \zeta_q(s) L_\chi(s) \prod_{\left(\frac{P}{T}\right)=1} \frac{(1-|P|^{-2s})}{(1-|P|^{-s})^2} \prod_{\left(\frac{Q}{T}\right)=-1} \frac{(1-|Q|^{-2s})}{(1+|Q|^{-s})(1-|Q|^{-s})}.$$

Using the fact that

$$\zeta_q(2s) = (1-q^{-2s})^{-1} \prod_{\left(\frac{P}{T}\right)=1} \left(1-|P|^{-2s}\right)^{-1} \prod_{\left(\frac{Q}{T}\right)=-1} \left(1-|Q|^{-2s}\right)^{-1},$$

we see that

$$L_2(s) = \frac{\zeta_q(s) L_\chi(s)}{\zeta_q(2s)(1-q^{-2s})} \prod_{\left(\frac{P}{T}\right)=1} (1-|P|^{-s})^{-2} \prod_{\left(\frac{Q}{T}\right)=-1} (1+|Q|^{-s})^{-1}(1-|Q|^{-s})^{-1}.$$

Further, using (3.1) and (3.2), we get

$$L_2(s) = \frac{\zeta_q^2(s) L_\chi^2(s)(1-q^{-s})}{\zeta_q(2s)(1-q^{-2s})}.$$

Making use of the fact that $L_\chi(s) = 1$, we have the result. ∎

Using the Dirichlet series $L_i(s)$ for $i = 1, 2$, we prove Theorem 1.2.

2024/12/28 21:50
https://doi.org/10.4153/S0008439525000025 Published online by Cambridge University Press

Proof For the first moment, we have from Theorem 3.1 that

$$L_1(s) = \zeta_q(s).$$

Expanding to retrieve the coefficient of q^{-ns}, we get

$$L_1(s) = \sum_{n=1}^{\infty} \frac{q^n}{q^{-ns}}.$$

Hence we get that

$$\sum_{f \in \mathcal{M}_{n,q}} \delta_2(f) = q^n.$$

Now, since $r_2^*(f) = 2\delta_2(f)$, we have the first moment. For the second moment, we have from Theorem 3.2 that

$$L_2(s) = \frac{\zeta_q^2(s)}{\zeta_q(2s)(1+q^{-s})}.$$

We know that

$$\zeta_q(s) = \frac{1}{1-q^{1-s}} = \sum_{n=0}^{\infty} \frac{q^n}{q^{ns}}.$$

Raising to the power of 2, we get

$$\zeta_q^2(s) = \left(\frac{1}{1-q^{1-s}}\right)^2 = \sum_{n=0}^{\infty} \frac{(n+1)q^n}{q^{ns}}.$$

Lastly, we note that

$$\frac{1}{(1+q^{-s})} = \sum_{n=0}^{\infty} \frac{(-1)^n}{q^{ns}}.$$

Combining all of the above, we get

$$L_2(s) = \frac{\zeta_q^2(s)}{\zeta_q(2s)(1+q^{-s})} = \left(\sum_{n=0}^{\infty} \frac{(n+1)q^n}{q^{ns}}\right)\left(\sum_{n=0}^{\infty} \frac{(-1)^n}{q^{ns}}\right)\left(1-q^{1-2s}\right).$$

Extracting the coefficient of q^{-ns} from the right hand side and using the fact that $r_2^*(f) = 2\delta_2(f)$, we have the second moment. ∎

We make a note that the formulae obtained for the first and second moments in this section have no associated error and hence work for all values of q and n.

4 Higher Moments of r_2^* in the large degree limit

In this section, we will first compute the L-series corresponding to δ_2^i for $i \geq 3$. We then make some remarks about the higher moments of r_2^* from the aforementioned L functions. We use the approach taken by Connors and Keating in [3]. The L-series $L_i(s)$

https://doi.org/10.4153/S0008439525000025 Published online by Cambridge University Press

for $\delta_2^i(f)$ is given by

$$L_i(s) = \left(\sum_{k=0}^{\infty} |T|^{-ks}\right) \prod_{\left(\frac{P}{T}\right)=1} \left(\sum_{k=0}^{\infty} (k+1)^i |P|^{-ks}\right) \prod_{\left(\frac{Q}{T}\right)=-1} \left(\sum_{k=0}^{\infty} |Q|^{-2ks}\right)$$
$$= (1-q^{-s})^{-1} \prod_{\left(\frac{P}{T}\right)=1} \left(\sum_{k=0}^{\infty} (k+1)^i |P|^{-ks}\right) \prod_{\left(\frac{Q}{T}\right)=-1} \left(1 - |Q|^{-2s}\right)^{-1}.$$

To further simplify this, we want to simplify the expression

$$\sum_{k=0}^{\infty} (k+1)^i |P|^{-ks}.$$

To this aim, we define

$$\gamma_i(x) := \sum_{k=0}^{\infty} (k+1)^i x^k.$$

Then, $\gamma_i(x)$ satisfies the recurrence

$$\frac{d}{dx}\left(x\gamma_{i-1}(x)\right) = \gamma_i(x). \tag{4.1}$$

Hence, we can write

$$\gamma_i(x) = \frac{1 + a_i x + \tilde{i}(x)}{(1-x)^{i+1}}, \tag{4.2}$$

where a_i are integers and $\tilde{i}(x)$ is a polynomial in x with least exponent term x^2. Before we move to estimating $L_i(s)$, we compute the leading coefficient a_i as it will prove to be useful. Substituting the form of $\gamma_i(x)$ given in (4.2) in the recurrence relation (4.1), we get

$$\gamma_{i+1}(x) = \frac{d}{dx}\left(\frac{x\left(1 + a_i x + \tilde{i}(x)\right)}{(1-x)^{i+1}}\right)$$
$$= \frac{(1-x)^{i+1}[1 + 2a_i x + x\tilde{i}'(x) + \tilde{i}(x)] + (1-x)^i (i+1)[x + a_i x^2 + x\tilde{i}(x)]}{(1-x)^{2i+2}}.$$

The coefficient of x in the numerator is $(2a_i + i)$. Hence, a_i satisfies the recurrence $a_{i+1} = 2a_i + i$. Using induction, we see that

$$a_i = 2^i - i - 1.$$

Coming back to our estimation of $L_i(s)$, we have

$$L_i(s) = (1-q^{-s})^{-1} \prod_{\left(\frac{P}{T}\right)=1} \left(\sum_{k=0}^{\infty} (k+1)^i |P|^{-ks}\right) \prod_{\left(\frac{Q}{T}\right)=-1} \left(1 - |Q|^{-2s}\right)^{-1}$$
$$= (1-q^{-s})^{-1} \prod_{\left(\frac{P}{T}\right)=1} \left(1 + a_i|P|^{-s} + b_i|P|^{-2s} + \cdots\right)\left(1 - |P|^{-s}\right)^{-(i+1)} \prod_{\left(\frac{Q}{T}\right)=-1} \left(1 - |Q|^{-2s}\right)^{-1}.$$

2024/12/28 21:50
https://doi.org/10.4153/S0008439525000025 Published online by Cambridge University Press

The product

$$\prod_{(\frac{P}{T})=1}\left(1+a_i|P|^{-s}+b_i|P|^{-2s}+\cdots\right)$$

does not converge near $s=1$ when $a_i \neq 0$. Hence, we define

$$A_i(s)=\prod_{(\frac{P}{T})=1}\left(1+a_i|P|^{-s}+b_i|P|^{-2s}+\cdots\right)\left(1-|P|^{-s}\right)^{a_i}.$$

Note that by construction,

$$A_i(s)=\prod_{(\frac{P}{T})=1}\left(1+c_i|P|^{-2s}+\cdots\right)$$

for some c_i and hence $A_i(s)$ converges at $s=1$ since it does not have any linear term. Therefore, we have

$$\begin{aligned} L_i(s)&=(1-q^{-s})^{-1}\prod_{(\frac{P}{T})=1}(1-|P|^{-s})^{-(i+1+a_i)}\prod_{(\frac{Q}{T})=-1}\left(1-|Q|^{-2s}\right)^{-1}A_i(s)\\ &=(1-q^{-s})^{-1}\prod_{(\frac{P}{T})=1}(1-|P|^{-s})^{-2^i}\prod_{(\frac{Q}{T})=-1}\left(1-|Q|^{-2s}\right)^{-1}A_i(s). \end{aligned} \tag{4.3}$$

Now,

$$\zeta_q(s)=\zeta_q(s)L_\chi(s)=(1-q^{-s})^{-1}\prod_{(\frac{P}{T})=1}(1-|P|^{-s})^{-2}\prod_{(\frac{Q}{T})=-1}\left(1-|Q|^{-2s}\right)^{-1}.$$

Hence

$$\zeta_q^{2^{i-1}}(s)=(1-q^{-s})^{-2^{i-1}}\prod_{(\frac{P}{T})=1}(1-|P|^{-s})^{-2^i}\prod_{(\frac{Q}{T})=-1}\left(1-|Q|^{-2s}\right)^{-2^{i-1}}.$$

Using this in equation (4.3), we get

$$\begin{aligned} L_i(s)&=\zeta_q^{2^{i-1}}(s)(1-q^{-s})^{2^{i-1}-1}\prod_{(\frac{Q}{T})=-1}\left(1-|Q|^{-2s}\right)^{2^{i-1}-1}A_i(s)\\ &=\zeta_q^{2^{i-1}}(s)B_i(s), \end{aligned} \tag{4.4}$$

where

$$B_i(s)=(1-q^{-s})^{2^{i-1}-1}\prod_{(\frac{Q}{T})=-1}\left(1-|Q|^{-2s}\right)^{2^{i-1}-1}A_i(s).$$

Note that $B_i(s)$ is non-singular for $\mathrm{Re}(s)\geq 1$. Now, we will use the L-series $L_i(s)$ to prove Theorem 1.3.

Proof We note from (4.4) that

$$\begin{aligned} L_i(s)&=\zeta_q^{2^{i-1}}(s)B_i(s)\\ &=\frac{B_i(s)}{(1-qu)^{2^{i-1}}}, \end{aligned}$$

where $u=q^{-s}$. Abusing the use of notations, we will write $\mathcal{L}_i(u)$ and $\mathcal{B}_i(u)$ in place of $L_i(s)$ and $B_i(s)$. Now, by Perron's formula

$$\sum_{f\in\mathcal{M}_{n,q}}\delta_2^i(f)=\frac{1}{2\pi i}\oint_{|u|=q^{-1-\epsilon}}\frac{\mathcal{B}_i(u)}{(1-qu)^{2^{i-1}}u^{n+1}}du.$$

2024/12/28 21:50
https://doi.org/10.4153/S0008439525000025 Published online by Cambridge University Press

We have a pole of order 2^{i-1} at $u = q^{-1}$. Hence we enlarge our contour to collect the residue at the pole. Hence

$$\sum_{f\in\mathcal{M}_{n,q}} \delta_2^i(f) = \frac{1}{2\pi i}\oint_{|u|=q^{-\epsilon}} \frac{\mathcal{B}_i(u)}{(1-qu)^{2^{i-1}}u^{n+1}}du - \operatorname{Res}\left(\frac{\mathcal{B}_i(u)}{(1-qu)^{2^{i-1}}u^{n+1}}; u = q^{-1}\right). \tag{4.5}$$

We know that $\mathcal{B}_i$ converges absolutely when $|u| < q^{-1}$. Also

$$|qu-1| > q^{1-\epsilon} - 1 \gg 1.$$

Hence

$$\frac{1}{(1-qu)^{2^{i-1}}} \ll 1.$$

So we get

$$\frac{1}{2\pi i}\oint_{|u|=q^{-\epsilon}} \frac{\mathcal{B}_i(u)}{(1-qu)^{2^{i-1}}u^{n+1}}du \ll \oint_{|u|=q^{-\epsilon}} \frac{1}{u^{n+1}}du \ll q^{n\epsilon}.$$

For the next step, we have to compute the residue in (4.5). To do just that, we make a note that for a memomorphic function $f(z)$ with a pole of order r at $z = z_0$, the residue is given by

$$\operatorname{Res}(f(z), z_0) = \frac{1}{(r-1)!}\lim_{z\to z_0}\frac{d^{r-1}}{dz^{r-1}}\left((z-z_0)^r f(z)\right).$$

Let

$$g(u) = \frac{\mathcal{B}_i(u)}{(1-qu)^{2^{i-1}}u^{n+1}}.$$

Hence using the above formula for the residue, we get

$$\begin{aligned}
\operatorname{Res}(g(u), q^{-1}) &= \frac{1}{(2^{i-1}-1)!}\lim_{u\to q^{-1}}\frac{d^{2^{i-1}-1}}{du^{2^{i-1}-1}}\left((u-q^{-1})^{2^{i-1}}g(u)\right)\\
&= \frac{1}{(2^{i-1}-1)!}\lim_{u\to q^{-1}}\frac{1}{q^{2^{i-1}}}\frac{d^{2^{i-1}-1}}{du^{2^{i-1}-1}}\left(\frac{\mathcal{B}_i(u)}{u^{n+1}}\right)\\
&= \frac{1}{(2^{i-1}-1)!}\lim_{u\to q^{-1}}\sum_{j=0}^{2^{i-1}-1}\frac{1}{q^{2^{i-1}}}\frac{d^j}{du^j}\left(\frac{1}{u^{n+1}}\right)\frac{d^{2^{i-1}-1-j}}{du^{2^{i-1}-1-j}}\mathcal{B}_i(u).
\end{aligned}$$

The last line follows by using the product rule. Noting that the $j = 0$ term corresponds to the leading order term of the residue, we get

$$\begin{aligned}
\operatorname{Res}(g(u), q^{-1}) &= \frac{1}{(2^{i-1}-1)!}\frac{1}{q^{2^{i-1}}}\left(\mathcal{B}_i(q^{-1})\frac{-(n+2^{i-1}-1)!}{n!}q^{n+2^{i-1}} + O(q^{n+2^{i-1}-1})\right)\\
&= -\mathcal{B}_i(q^{-1})\binom{n+2^{i-1}-1}{n}q^n + O(q^{n-1}),
\end{aligned}$$

where $\binom{s}{t}$ is the binomial coefficent s choose t. Plugging it back into (4.5) and using the relation $r_2^*(f) = 2\delta(f)$ gives us the result. ∎

5 Higher Moments of r_2^* in the large finite field limit

In this section, we use another approach to estimate the moments. We define the set $\mathcal{F}_n \subset \mathcal{M}_{n,q}$ consisting of all $f \in \mathcal{M}_{n,q}$ such that $b_q(f) = 1$. By the definition of $\mathcal{F}_n$, it is clear that

$$\sum_{f\in\mathcal{M}_{n,q}} (r_2^*)^i(f) = \sum_{f\in\mathcal{F}_n} (r_2^*)^i(f).$$

2024/12/28 21:50
https://doi.org/10.4153/S0008439525000025 Published online by Cambridge University Press

for each $i \in \mathbb{N}$. Partitioning $\mathcal{F}_n$ as in [1], we define

$$\begin{aligned}
\mathcal{F}_{1,n} &= \left\{ f \in \mathcal{F}_n : f = P_1P_2\ldots P_r, P_i \neq P_j \quad \forall i \neq j, r \geq 0 \right\}, \\
\mathcal{F}_{2,n} &= \left\{ f \in \mathcal{F}_n : f = TP_1P_2\ldots P_r, P_i \neq P_j \quad \forall i \neq j, r \geq 0 \right\}, \\
\mathcal{F}_{3,n} &= \left\{ f \in \mathcal{F}_n : f = P_1P_2\ldots P_rQ_1^2, \deg Q_1 = 1, P_i \neq P_j \quad \forall i \neq j, r \geq 0 \right\}, \\
\mathcal{F}_{4,n} &= \left\{ f \in \mathcal{F}_n : f = P_1^2P_2\ldots P_r, \deg P_1 = 1, P_i \neq P_j \quad \forall i \neq j, r \geq 0 \right\}, \\
\mathcal{F}_{5,n} &= \left\{ f \in \mathcal{F}_n : f = TP_1P_2\ldots P_rQ_1^2, \deg Q_1 = 1, P_i \neq P_j \quad \forall i \neq j, r \geq 0 \right\}, \\
\mathcal{F}_{6,n} &= \mathcal{F}_n \setminus \bigcup_{i=1}^{5} \mathcal{F}_{i,n}.
\end{aligned}$$

The motive behind the partitioning is that the major contribution to the moments of $r_2^*(f)$ comes from specific types of polynomials described in the partitions. To show this, we will estimate the sum for each of the subsets of $\mathcal{F}_n$. Before the estimation, we state the version of the Chebotarev density theorem we will be using.

***Lemma* 5.1** *[1, Lemma 3.2] Let*

$$\pi_{q;\alpha}(n) := \# \left\{ R \in \mathcal{M}_{n,q} : \left(\frac{R}{T}\right) = \alpha, \alpha = \pm 1, R \textit{ irreducible} \right\} = \frac{q^n}{2n} + O\left(q^{\lfloor n/2 \rfloor}\right).$$

Then, we have

$$\begin{aligned}
\pi_{q;\alpha}(1) &= \frac{q-1}{2}, \\
\pi_{q;\alpha}(2) &= \frac{1}{4}q^2 - \frac{1+\alpha}{4}q + \frac{\alpha}{4}, \textit{and} \\
\pi_{q;\alpha}(n) &= \frac{q^n}{2n} + O\left(q^{n-2}\right), n \geq 3.
\end{aligned}$$

Let us introduce some notations before we proceed. Let $\lambda \vdash n$ denote a partition $(\lambda_1, \lambda_2, ..., \lambda_n)$ of n such that $\sum_{j=1}^n j\lambda_j = n$, i.e., λ_j is the number of times j appears in the partition. In the next few results, certain coefficients show up often. We define

$$\gamma_{i,n} = \sum_{\lambda \vdash n} \prod_{j=1}^{n} \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!}.$$

***Proposition* 5.1** *We have*

$$\sum_{f \in \mathcal{F}_{1,n}} (r_2^*)^i(f) = 2^i\gamma_{i,n}q^n - 2^i\left(2^{(i-1)}\gamma_{i,n-1} + \left(2^{(i-1)} + 2^{2(i-1)}\right)\gamma_{i,n-2}\right)q^{n-1} + O(q^{n-2}).$$

Proof Say $f \in \mathcal{F}_{1,n}$. We have $f = P_1P_2....P_k$ for primes P_j, $j \leq k$. The degrees of P_i form a partition of n say $(\lambda_1, \lambda_2, \cdots, \lambda_n)$, where λ_j is the number of primes in the factorisation with degree j. Since every prime in the factorisation has exponent 1, Theorem 1.1 gives

$$r_2^*(f) = 2 \cdot 2^{\lambda_1+\lambda_2+\cdots+\lambda_n}.$$

Hence, we have

$$\sum_{f \in \mathcal{F}_{1,n}} (r_2^*)^i(f) = 2^i \sum_{\lambda \vdash n} \prod_{j=1}^{n} \binom{\pi_{q;1}(j)}{\lambda_j} 2^{i\lambda_j}.$$

https://doi.org/10.4153/S0008439525000025 Published online by Cambridge University Press

Note that the term $\binom{\pi_{q;1}(j)}{\lambda_j}$ denotes the number of ways to choose λ_j primes of degree j. From Lemma 5.1, we have

$$\begin{aligned}\binom{\pi_{q;1}(1)}{\lambda_1}2^{i\lambda_1} &= \frac{2^{(i-1)\lambda_1}}{\lambda_1!}q^{\lambda_1} - \frac{2^{(i-1)\lambda_1}\lambda_1^2}{\lambda_1!}q^{\lambda_1-1} + O\left(q^{\lambda_1-2}\right),\\ \binom{\pi_{q;1}(2)}{\lambda_2}2^{i\lambda_2} &= \frac{2^{(i-1)\lambda_2}}{2^{\lambda_2}\lambda_2!}q^{2\lambda_2} - \frac{2^{(i-1)\lambda_2}2\lambda_2}{2^{\lambda_2}\lambda_2!}q^{2\lambda_2-1} + O\left(q^{2\lambda_2-2}\right), \text{ and}\\ \binom{\pi_{q;1}(j)}{\lambda_j}2^{i\lambda_j} &= \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!}q^{j\lambda_j} + O\left(q^{j\lambda_j-2}\right).\end{aligned}$$

Hence, we get

$$\prod_{j=1}^{n}\binom{\pi_{q;1}(j)}{\lambda_j}2^{i\lambda_j} = \prod_{j=1}^{n}\frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!}q^n - \left(\lambda_1^2\prod_{j=1}^{n}\frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!} + 2\lambda_2\prod_{j=1}^{n}\frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!}\right)q^{n-1} + O(q^{n-2}).$$

Hence

$$\sum_{\lambda\vdash n}\prod_{j=1}^{n}\binom{\pi_{q;1}(j)}{\lambda_j}2^{i\lambda_j} = \gamma_{i,n}q^n - \sum_{\lambda\vdash n}\left(\lambda_1^2\prod_{j=1}^{n}\frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!} + 2\lambda_2\prod_{j=1}^{n}\frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!}\right)q^{n-1} + O(q^{n-2}). \tag{5.1}$$

Define C_λ and D_λ as

$$C_\lambda = \left(\lambda_1^2\prod_{j=1}^{n}\frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!}\right),\ D_\lambda = \left(2\lambda_2\prod_{j=1}^{n}\frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!}\right).$$

Also, define the partitions μ and ν as follows: μ is a partition of $n-1$ given by $(\lambda_1-1, \lambda_2, .., \lambda_{n-1})$ and ν is a partition of $n-2$ given by $(\lambda_1-2, \lambda_2, .., \lambda_{n-2})$. If $\lambda_1 = 0$, then $C_\lambda = 0$ and hence such partitions do not contribute to our sum. If $\lambda_1 = 1$, then $\lambda_n = 0$ and

$$C_\lambda = 2^{(i-1)}\left(\prod_{j=1}^{n-1}\frac{2^{(i-1)\mu_j}}{j^{\mu_j}\mu_j!}\right),$$

where μ is a partition of $n-1$. So, when λ runs through all the partitions of n with $\lambda_1 = 1$, μ runs through all partitions of $n-1$ with $\mu_1 = 0$. If $\lambda_1 \geq 2$, $\lambda_{n-1} = \lambda_n = 0$ and

$$C_\lambda = \left(\lambda_1^2\prod_{j=1}^{n}\frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!}\right) = \left(\lambda_1\prod_{j=1}^{n}\frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!}\right) + \left(\lambda_1(\lambda_1-1)\prod_{j=1}^{n}\frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!}\right).$$

Hence

$$C_\lambda = 2^{(i-1)}\left(\prod_{j=1}^{n-1}\frac{2^{(i-1)\mu_j}}{j^{\mu_j}\mu_j!}\right) + 2^{2(i-1)}\left(\prod_{j=1}^{n-2}\frac{2^{(i-1)\nu_j}}{j^{\nu_j}\nu_j!}\right),$$

where μ is a partition of $n-1$ and ν is a partition of $n-2$. In this case, when λ runs through all partitions of n with $\lambda_1 \geq 2$, μ runs through all partitions of $n-1$ with $\mu_1 \geq 1$ and ν run through all partitions of $n-2$. So overall, as λ runs through all partitions of n, μ and ν runs through all the partitions of $n-1$ and $n-2$. Hence

$$\begin{aligned}\sum_{\lambda\vdash n}C_\lambda &= 2^{(i-1)}\sum_{\mu\vdash(n-1)}\left(\prod_{j=1}^{m-1}\frac{2^{(i-1)\mu_j}}{j^{\mu_j}\mu_j!}\right) + 2^{2(i-1)}\sum_{\nu\vdash(n-2)}\left(\prod_{j=1}^{n-2}\frac{2^{(i-1)\nu_j}}{j^{\nu_j}\nu_j!}\right)\\ &= 2^{(i-1)}\gamma_{i,n-1} + 2^{2(i-1)}\gamma_{i,n-2}.\end{aligned} \tag{5.2}$$

https://doi.org/10.4153/S0008439525000025 Published online by Cambridge University Press

If $\lambda_2 = 0$, then $D_\lambda = 0$ and hence such partitions do not contribute to the sums. If $\lambda_2 \geq 1, \lambda_{n-1} = \lambda_n = 0$. Hence

$$D_\lambda = \left(2\lambda_2 \prod_{j=1}^{n} \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!}\right) = 2^{(i-1)} \prod_{j=1}^{n-2} \frac{2^{(i-1)\nu_j}}{j^{\nu_j}\nu_j!},$$

where ν is a partition of $n-2$ given by $(\lambda_1, \lambda_2 - 1, .., \lambda_{n-2})$. We see that as λ runs through all partitions of n, ν runs through all partitions of $n-2$. Hence

$$\sum_{\lambda \vdash n} D_\lambda = 2^{(i-1)} \sum_{\nu \vdash (n-2)} \left(\prod_{j=1}^{n-2} \frac{2^{(i-1)\nu_j}}{j^{\nu_j}\nu_j!}\right) = 2^{(i-1)}\gamma_{i,n-2}. \tag{5.3}$$

Finally using (5.2) and (5.3) in (5.1), we have our result. ■

***Proposition* 5.2** *We have*

$$\sum_{f \in \mathcal{F}_{2,n}} (r_2^*)^i(f) = 2^i \gamma_{i,n-1} q^{n-1} + O(q^{n-2}),$$

Proof We exploit the one to one correspondence between $\mathcal{F}_{2,n}$ and $\mathcal{F}_{1,n-1}$. For $f \in \mathcal{F}_{2,n}$, the degrees of P_i form a partition of $n-1$ and so we have

$$\sum_{f \in \mathcal{F}_{2,n}} (r_2^*)^i(f) = 2^i \sum_{\lambda \vdash n-1} \prod_{j=1}^{n-1} \binom{\pi_{q;1}(j)}{\lambda_j} 2^{i\lambda_j}.$$

Using (5.1), we have the result. ■

***Proposition* 5.3** *We have*

$$\sum_{f \in \mathcal{F}_{3,n}} (r_2^*)^i(f) = 2^{(i-1)}\gamma_{i,n-2} q^{n-1} + O(q^{n-2}).$$

Proof Say $f = P_1 P_2 ... P_r Q_1^2 \in \mathcal{F}_{3,n}$ with degree of Q_1 being 1. Let Q be fixed. Then the degrees of P_i form a partition of $n-2$ and for a fixed Q, we have a correspondence between $\mathcal{F}_{3,n}$ and $\mathcal{F}_{1,n-2}$. So we have

$$\sum_{f \in \mathcal{F}_{3,n}, Q \text{ fixed}} (r_2^*)^i(f) = 2^i \gamma_{i,n-2} q^{n-2} + O(q^{n-3}).$$

Note that the choice of Q does not influence the function $r_2^*(f)$. We have $\frac{q-1}{2}$ choices for Q. Hence

$$\sum_{f \in \mathcal{F}_{3,n}} (r_2^*)^i(f) = \frac{q-1}{2}\left(2^i \gamma_{i,n-2} q^{n-2} + O(q^{n-3})\right) = 2^{(i-1)}\gamma_{i,n-2} q^{n-1} + O(q^{n-2}).$$

■

***Proposition* 5.4** *We have*

$$\sum_{f \in \mathcal{F}_{4,n}} (r_2^*)^i(f) = \frac{6^i}{2}\gamma_{i,n-2} q^{n-1} + O(q^{n-2}).$$

2024/12/28 21:50
https://doi.org/10.4153/S0008439525000025 Published online by Cambridge University Press

Proof For $f \in \mathcal{F}_{4,n}$, say $f = P_1^2 P_2..P_r$ with degree of P_1 being 1, the degrees of $P_2, P_3, ..P_r$ form a partition $\lambda = (\lambda_1, \lambda_2, ..., \lambda_{n-2})$ of $n-2$ where λ_1 is the number of linear terms in the factorisation excluding P_1. Also,

$$r_2^*(f) = 6 \cdot 2^{\lambda_1+\lambda_2+\cdots\lambda_{n-2}}.$$

Hence

$$\sum_{f\in\mathcal{F}_{4,n}} (r_2^*)^i(f) = \binom{q-1}{2} 6^i \sum_{\lambda\vdash n-2} \binom{\pi_{q;1}(1)-1}{\lambda_1} 2^{i\lambda_1} \prod_{j=2}^{n-2} \binom{\pi_{q;1}(j)}{\lambda_j} 2^{i\lambda_j}.$$

Similar analysis gives the result. ■

***Proposition* 5.5** *We have*

$$\sum_{f\in\mathcal{F}_{5,n}\cup\mathcal{F}_{6,n}} (r_2^*)^i(f) = O(q^{n-2}).$$

Proof Exploiting the one to one correspondence between $\mathcal{F}_{5,n}$ and $\mathcal{F}_{3,n-1}$, we have from Proposition 5.3 that

$$\sum_{f\in\mathcal{F}_{5,n}} (r_2^*)^i(f) = O(q^{n-2}).$$

Also, from [1, Lemma 3.1], the size of the set $\mathcal{F}_{6,n}$ is bounded above by $\frac{7}{3}q^{n-2}$. Hence, the result is evident. ■

The coefficients $\gamma_{i,n}$ also arise naturally in the study of Ewens sampling formula which describes the probabilities associated with the number of different alleles observed in a sample. Using the sampling formula, we get that

$$\gamma_{i,n} = \sum_{\lambda\vdash n} \prod_{j=1}^{n} \frac{2^{(i-1)\lambda_j}}{j^{\lambda_j}\lambda_j!} = \frac{(n+2^{(i-1)}-1)!}{n!(2^{(i-1)}-1)!} = \binom{n+2^{(i-1)}-1}{n}.$$

Refer to [5] for more details. Finally, we prove Theorem 1.4.

Proof From the definition of $\mathcal{F}_n$,

$$\sum_{f\in\mathcal{M}_{n,q}} (r_2^*)^i(f) = \sum_{f\in\mathcal{F}_n} (r_2^*)^i(f).$$

Splitting the sum over partitions of $\mathcal{F}_n$ and using the estimates obtained in Proposition 5.1 to Proposition 5.5, we get the result. ■

References

[1] L. Bary-Soroker, Y. Smilansky A. Wolf, *On the function field analogue of Landau's theorem on sums of squares*, Finite Fields Appl. **39** (2016), 195–215.
[2] J. M. Borwein K. S. Choi, *On Dirichlet series for sums of squares*, Ramanujan J.7 (2003), 95–127.
[3] R. D. Connors J. P. Keating, *Degeneracy moments for the square billiard*, J. Phys. A **32** (1999), 555–562.
[4] G. H. Hardy E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, Oxford (2008).
[5] S. Karlin J. McGregor, *Addendum to a paper of W. Ewens*, Theoret. Population Biol. **3** (1972), 113–116.
[6] E. Landau, *Vorlesungen über Zahlentheorie*, Chelsea Publishing Co., New York (1969).
[7] M. Rosen, *Number theory in function fields*, Springer-Verlag, New York (2002).

Department of Pure Mathematics, University of Waterloo, Waterloo, ON, N2L3G1
e-mail: *wtkuo@uwaterloo.ca, yrliu@uwaterloo.ca, ytotani@uwaterloo.ca.*

2024/12/28 21:50
https://doi.org/10.4153/S0008439525000025 Published online by Cambridge University Press