SHIFTED CONVOLUTION AND THE TITCHMARSH DIVISOR PROBLEM OVER $\mathbb{F}_q[t]$

J. C. ANDRADE, L. BARY-SOROKER AND Z. RUDNICK

Abstract. In this paper we solve a function field analogue of classical problems in analytic number theory, concerning the auto–correlations of divisor functions, in the limit of a large finite field.

1. Introduction

The goal of this note is to study a function-field analogue of classical problems in analytic number theory, concerning the auto-correlations of divisor functions. First we review the problems over the integers $\mathbb{Z}$ and then we proceed to investigate the same problems over the rational function field $\mathbb{F}_q(t)$.

1.1. **The additive divisor problem and over $\mathbb{Z}$.** Let $d_k(n)$ be the number of representations of n as a product of k positive integers (d_2 is the standard divisor function). Several authors have studied the **additive divisor problem** (other names are "shifted divisor" and "shifted convolution"), which is to get bounds, or asymptotics, for the sum

$$D_k(x;h) := \sum_{n\le x} d_k(n)d_k(n+h), \tag{1.1}$$

where $h \neq 0$ is fixed for this discussion.

The case $k = 2$ (the ordinary divisor function) has a long history: Ingham [13] computed the leading term, and Estermann [8] gave an asymptotic expansion

$$\sum_{n\le x} d_2(n)d_2(n+h) = xP_2(\log x;h) + O(x^{11/12}(\log x)^3), \tag{1.2}$$

Date: January 5, 2015.

2010 *Mathematics Subject Classification.* Primary 11T55; Secondary 11G20 11M38, 11M50, 11N37, 11K65, 20B30.

Key words and phrases. finite fields, function fields, divisor function, shifted convolution, random permutation, cycle structure.

JCA is supported by an IHÉS Postdoctoral Fellowship and an EPSRC William Hodge Fellowship.

The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement n° 320755, and from the Israel Science Foundation (grant No. 925/14).

where

$$P_2(u;h) = \frac{1}{\zeta(2)}\sigma_{-1}(h)u^2 + a_1(h)u + a_2(h), \tag{1.3}$$

with

$$\sigma_w(h) = \sum_{d|h} d^w, \tag{1.4}$$

and $a_1(h)$, $a_2(h)$ are very complicated coefficients.

The size of the remainder term has great importance in applications for various problems in analytic number theory, in particular the dependence on h. See [7, 12] for an improvement of the remainder term.

The higher divisor problem $k \geq 3$ is also of importance, in particular in relation to computing the moments of the Riemann ζ-function on the critical line, see [6, 14]. It is conjectured that

$$D_k(x;h) \sim xP_{2(k-1)}(\log x;h) \qquad \text{as } x \to \infty, \tag{1.5}$$

where $P_{2(k-1)}(u;h)$ is a polynomial in u of degree $2(k-1)$, whose coefficients depend on h (and k). We can get good upper bounds on the additive divisor problem from results in sieve theory on sums of multiplicative functions evaluated at polynomials, for instance as those by Nair and Tenenbaum [23]. The conclusion is that for $h \neq 0$

$$\sum_{n \leq X} d_k(n)d_k(n+h) \ll X(\log X)^{2(k-1)}, \tag{1.6}$$

and we believe this is the right order of magnitude. But even a conjectural description of the polynomials $P_{2(k-1)}(u;h)$ is difficult to obtain, see [6, 14], see § 7.

A variant of the problem about the auto-correlation of the divisor function, is to determine an asymptotic for the more general sum given by

$$D_{k,r}(x;h) := \sum_{n \leq x} d_k(n)d_r(n+h). \tag{1.7}$$

Asymptotics are known for the case $(k,r) = (k,2)$ for any positive integer $k \geq 2$: Linnik [18] showed

$$\begin{aligned} D_{k,2}(x;1) &= \sum_{n \leq x} d_k(n)d_2(n+1) \\ &= \frac{1}{(k-1)!}\prod_p \left(1 - \frac{1}{p} + \frac{1}{p}\left(1 - \frac{1}{p}\right)^{k-1}\right) x(\log x)^k \\ &\quad + O\left(x(\log x)^{k-1}(\log\log x)^{k^4}\right). \end{aligned} \tag{1.8}$$

Motohashi [19, 20, 21] gave an asymptotic expansion

$$D_{k;2}(x,h) = x\sum_{j=0}^{k} f_{k,j}(h)(\log x)^j + O(x(\log x)^{\varepsilon-1}), \tag{1.9}$$

for all $\varepsilon > 0$ where the coefficients $f_{k,j}(h)$ can in principle be explicitly computed. For an improvement in the O–term see [10].

1.2. **The Titchmarsh divisor problem over $\mathbb{Z}$.** A different problem involving the mean value of the divisor function is the **Titchmarsh divisor problem**. The problem is to understand the average behaviour of the number of divisors of a shifted prime, that is the asymptotics of the sum over primes

$$\sum_{p \le x} d_2(p+a) \tag{1.10}$$

where $a \neq 0$ is a fixed integer, and $x \to \infty$. Assuming GRH, Titchmarsh [24] showed in 1931 that

$$\sum_{p \le x} d_2(p+a) \sim C_1 x \tag{1.11}$$

with

$$C_1 = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \prod_{p \mid a} \left(1 - \frac{p}{p^2 - p + 1}\right) \tag{1.12}$$

and this was proved unconditionally by Linnik [18] in 1963.

Fouvry [9] and Bombieri, Friedlander and Iwaniec [3] gave a secondary term

$$\sum_{p \le x} d_2(p+a) = C_1 x + C_2 \operatorname{Li}(x) + O\left(\frac{x}{(\log x)^A}\right), \tag{1.13}$$

for all $A > 1$ and

$$C_2 = C_1 \left(\gamma - \sum_p \frac{\log p}{p^2 - p + 1} + \sum_{p \mid a} \frac{p^2 \log p}{(p-1)(p^2 - p + 1)}\right) \tag{1.14}$$

with γ being the Euler-Mascheroni constant and $\operatorname{Li}(x)$ the logarithmic integral function.

In the following sections we study the additive divisor problem and the Titchmarsh divisor problem over $\mathbb{F}_q[t]$, obtaining definitive analogues of the conjectures described above.

1.3. **The additive divisor problem over $\mathbb{F}_q[t]$.** We denote by $\mathcal{M}_n$ the set of monic polynomials in $\mathbb{F}_q[t]$ of degree n. Note that $\#\mathcal{M}_n = q^n$.

The divisor function $d_k(f)$ is the number of ways to write a monic polynomial f as a product of k monic polynomials:

$$d_k(f) = \#\{(a_1, \dots, a_k), f = a_1 \cdot a_2 \cdots a_k\}, \tag{1.15}$$

where it is allowed to have $a_i = 1$.

The mean value of $d_k(f)$ has an exact formula (see Lemma 2.2):

$$\frac{1}{q^n}\sum_{f\in\mathcal{M}_n} d_k(f) = \binom{n+k-1}{k-1}. \tag{1.16}$$

Note that $\binom{n+k-1}{k-1}$ is a polynomial in n of degree $k-1$ and leading coefficient $1/(k-1)!$. Our first goal is to study the auto-correlation of d_k in the limit $q\to\infty$. We show:

Theorem 1.1. *Fix $n>1$. Then*

$$\frac{1}{q^n}\sum_{f\in\mathcal{M}_n} d_k(f)d_k(f+h) = \binom{n+k-1}{k-1}^2 + O\left(q^{-\frac{1}{2}}\right), \tag{1.17}$$

uniformly for all $0\neq h\in\mathbb{F}_q[t]$ of degree $\deg(h)<n$, as $q\to\infty$.

In light of (1.16), Theorem 1.1 may be interpreted as the statement that $d_k(f)$ and $d_k(f+h)$ become independent in the limit $q\to\infty$ as long as $\deg(h)<n$.

To compare with conjecture (1.5) over $\mathbb{Z}$ we note that $\binom{n+k-1}{k-1}^2$ is a polynomial in n of degree $2(k-1)$ with leading coefficient $1/[(k-1)!]^2$, in agreements with the conjecture, see § 7.2.

The case $h=0$: As an aside, we note that the case $h=0$ is of course dramatically different, indeed one can show that

$$\lim_{q\to\infty}\frac{1}{q^n}\sum_{f\in\mathcal{M}_n} d_k(f)^2 = \binom{n+k^2-1}{k^2-1} \tag{1.18}$$

is a polynomial of degree k^2-1 in n, rather than degree $2(k-1)$ for nonzero shifts.

Our method in fact gives the more general result:

Theorem 1.2. *Let $\mathbf{k}=(k_1,\dots,k_s)$ be a tuple of positive integers and $\mathbf{h}=(h_1,\dots,h_s)$ a tuple of distinct polynomials in $\mathbb{F}_q[t]$. We let*

$$D_{\mathbf{k}}(n;\mathbf{h}) = \sum_{f\in\mathcal{M}_n} d_{k_1}(f+h_1)\cdots d_{k_s}(f+h_s).$$

Then, for fixed $n>1$,

$$\frac{1}{q^n}D_{\mathbf{k}}(n;\mathbf{h}) = \prod_{i=1}^{s}\binom{n+k_i-1}{k_i-1} + O\left(q^{-\frac{1}{2}}\right),$$

uniformly on all tuples $\mathbf{h}=(h_1,h_2,\dots,h_s)$ of distinct polynomials in $\mathbb{F}_q[t]$ of degrees $\deg(h_i)<n$ as $q\to\infty$.

In particular for $\mathbf{k} = (2, k)$ we get

$$\lim_{q\to\infty} \frac{1}{q^n} D_{2,k}(n;h) = (n+1)\binom{n+k-1}{k-1}$$
$$= \frac{1}{(k-1)!}\left(n^k + \frac{k^2-k+2}{2}n^{k-1} + \cdots\right), \tag{1.19}$$

in agreement with (1.8).

1.4. **The Titchmarsh divisor problem over $\mathbb{F}_q[t]$.** Let $\mathcal{P}_n$ be the set of monic irreducible polynomials in $\mathbb{F}_q[t]$ of degree n. By the Prime Polynomial Theorem we have

$$\pi_q(n) := \#\mathcal{P}_n = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

Our next result is a solution of the Titchmarsh divisor problem over $\mathbb{F}_q[t]$ in the limit of large finite field.

Theorem 1.3. *Fix $n > 1$. Then*

$$\frac{1}{\pi_q(n)} \sum_{P\in\mathcal{P}_n} d_k(P+\alpha) = \binom{n+k-1}{k-1} + O\left(q^{-\frac{1}{2}}\right) \tag{1.20}$$

uniformly over all $0 \neq \alpha \in \mathbb{F}_q[t]$ of degree $\deg(\alpha) < n$.

For the standard divisor function ($k = 2$) we find

$$\sum_{P\in\mathcal{P}_n} d_2(P+\alpha) = q^n + \frac{q^n}{n} + O\left(q^{n-\frac{1}{2}}\right), \tag{1.21}$$

which is analogous to (1.13) under the correspondence $x \leftrightarrow q^n$, $\log x \leftrightarrow n$.

1.5. **Independence of cycle structure of shifted polynomials.** We conclude the introduction with a discussion on the connection between shifted polynomials and random permutations and state a result that lies behind the results stated above.

The cycle structure of a permutation σ of n letters is the partition $\lambda(\sigma) = (\lambda_1, \dots, \lambda_n)$ of n if in the decomposition of σ as a product of disjoint cycles, there are λ_j cycles of length j. Note that $\lambda(\sigma)$ is a partition of n is the sense that $\lambda_j \geq 0$ and $\sum_j j\lambda_j = n$. For example, λ_1 is the number of fixed points of σ and $\lambda_n = 1$ if and only if σ is an n-cycle.

For each partition $\lambda \vdash n$, the probability that a random permutation on n letters has cycle structure σ is given by Cauchy's formula [1, Chapter 1]:

$$p(\lambda) = \frac{\#\{\sigma \in S_n : \lambda(\sigma) = \lambda\}}{\#S_n} = \prod_{j=1}^{n} \frac{1}{j^{\lambda_j} \cdot \lambda_j!}. \tag{1.22}$$

For $f \in \mathbb{F}_q[t]$ of positive degree n, we say its cycle structure is $\lambda(f) = (\lambda_1, \dots, \lambda_n)$ if in the prime decomposition $f = \prod_j P_j$ (we allow repetition), we have $\#\{i : \deg(P_i) = j\} = \lambda_j$. Thus we get a partition of n. In analogy with permutation, $\lambda_1(f)$ is the number of roots of f in $\mathbb{F}_q$ (with multiplicity) and f is irreducible if and only if $\lambda_n(f) = 1$.

For a partition $\lambda \vdash n$, we let χ_λ be the characteristic function of $f \in \mathcal{M}_n$ of cycle structure λ:

$$\chi_\lambda(f) = \begin{cases} 1, & \lambda(f) = \lambda \\ 0, & \text{otherwise.} \end{cases} \tag{1.23}$$

The Prime Polynomial Theorem gives the mean values of χ_λ:

$$\frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \chi_\lambda(f) = p(\lambda) + O\left(q^{-1}\right) \tag{1.24}$$

as $q \to \infty$ (see Lemma 2.1). We prove independence of cycle structure of shifted polynomials:

Theorem 1.4. *For fixed positive integers n and s we have*

$$\frac{1}{q^n} \sum_{f \in \mathcal{M}_n} \chi_{\lambda_1}(f + h_1) \cdots \chi_{\lambda_s}(f + h_s) = p(\lambda_1) \cdots p(\lambda_s) + O\left(q^{-\frac{1}{2}}\right),$$

uniformly for all $h_1, \dots, h_s$ distinct polynomials in $\mathbb{F}_q[t]$ of degrees $\deg(h_i) < n$ and on all partitions $\lambda_1, \dots, \lambda_s \vdash n$ as $q \to \infty$.

Remark. *In this theorem $\lambda_1, \cdots, \lambda_s$ are partitions of n and are not the same as the $\lambda_1, \cdots, \lambda_n$ that appears on the definition of $\lambda(f)$ or $\lambda(\sigma)$ where in that case the λ_i's are the number of parts of length i.*

We note that the statistic of Theorem 1.4 is induced from the statistics of cycles structure of tuples of elements in the direct product S_n^s of s copies of the symmetric group on n letters S_n. This plays a role in the proof, where we use that a certain Galois group is S_n^s [2], and we derive the statistic from an explicit Chebotarev theorem. Since we have not found the exact formulation that we need in the literature, we provide a proof in the Appendix.

2. Mean values

For the reader's convenience, we prove in this section some results for which we did not find a good reference. We define the **norm** of a nonzero polynomial $f \in \mathbb{F}_q[t]$ to be $|f| = q^{\deg(f)}$ and set $|0| = 0$.

We start by proving (1.24):

Lemma 2.1. *If $\lambda \vdash n$ is a partition of n and n is a fixed number then*

$$\frac{1}{q^n} \#\{f \in \mathcal{M}_n : \lambda(f) = \lambda\} = p(\lambda)(1 + O(q^{-1})) \tag{2.1}$$

as $q \to \infty$.

Proof. To see this, note that to get a monic polynomial with cycle structure λ, we pick any λ_1 primes of degree 1, λ_2 primes of degree 2, (irrespective of the choice of ordering), and multiply them together. Thus

$$\#\{f \in \mathcal{M}_n : \lambda(f) = \lambda\} = \prod_{j=1}^{n} \frac{\pi_A(j)^{\lambda_j}}{\lambda_j!}\Big(1 + O(\frac{1}{q})\Big) \tag{2.2}$$

where $\pi_A(j)$ is the number of primes of degree j in $A = \mathbb{F}_q[t]$. By the Prime Polynomial Theorem, $\pi_A(j) = \frac{q^j}{j} + O(\frac{q^{j/2}}{j})$ whenever $j \geq 2$ and $\pi_A(1) = q$. Hence $\pi_A(j) = \frac{q^j}{j} + O(\frac{q^{j-1}}{j})$. So

$$\begin{aligned} \#\{f \in \mathcal{M}_n : \lambda(f) = \lambda\} &= \prod_{j=1}^{n} \frac{1}{\lambda_j!}\left(\frac{q^j}{j} + O\left(\frac{q^{j-1}}{j}\right)\right)^{\lambda_j} \\ &= q^{\sum j\lambda_j} \prod_{j=1}^{n} \frac{1}{j^{\lambda_j} \cdot \lambda_j!}(1 + O(q^{-1})) \end{aligned} \tag{2.3}$$

which by (1.22) gives (2.1). ☐

Next we prove (1.16):

Lemma 2.2. *The mean value of $d_k(f)$ is*

$$\frac{1}{q^n} \sum_{f \in \mathcal{M}_n} d_k(f) = \binom{n+k-1}{k-1}. \tag{2.4}$$

Proof. The generating function for $d_k(f)$ is the k-th power of the zeta function associated to the polynomial ring $\mathbb{F}_q[t]$

$$Z(u)^k = \sum_{f \text{ monic}} d_k(f) u^{\deg f} = \sum_{n=0}^{\infty} \sum_{f \in \mathcal{M}_n} d_k(f) u^n. \tag{2.5}$$

Here

$$Z(u) = \sum_{f \text{ monic}} u^{\deg f} = \sum_{n=0}^{\infty} q^n u^n = \frac{1}{1 - qu}. \tag{2.6}$$

Using the Taylor expansion

$$\frac{1}{(1-x)^k} = \sum_{n=0}^{\infty} \binom{n+k-1}{k-1} x^n \tag{2.7}$$

and comparing the coefficients of u^n in (2.5) give

$$q^n \binom{n+k-1}{k-1} = \sum_{f \in \mathcal{M}_n} d_k(f), \tag{2.8}$$

as needed. ☐

3. Proof of Theorem 1.4

In the course of the proof we shall use the following explicit Chebotarev theorem which is a special case of Theorem A.4 of Appendix A:

Theorem 3.1. *Let $\boldsymbol{A} = (A_1, \ldots, A_n)$ be an n-tuple of variables over $\mathbb{F}_q$, let $\mathcal{F}(t) \in \mathbb{F}_q[\boldsymbol{A}][t]$ be monic, separable, and of degree m viewed as a polynomial in t, let L be a splitting field of $\mathcal{F}$ over $K = \mathbb{F}_q(\boldsymbol{A})$, and let $G = \mathrm{Gal}(\mathcal{F}, K) = \mathrm{Gal}(L/K)$. Assume that $\mathbb{F}_q$ is algebraically closed in L. Then there exists a constant $c = c(n, \mathrm{tot.deg}(\mathcal{F}))$ such that for every conjugacy class $C \subseteq G$ we have*

$$\left| \#\{\boldsymbol{a} \in \mathbb{F}_q^n : \mathrm{Fr}_{\boldsymbol{a}} = C\} - \frac{|C|}{|G|} q^n \right| \leq c q^{n-1/2}.$$

Here $\mathrm{Fr}_{\boldsymbol{a}}$ denotes the Frobenius conjugacy class $\left(\frac{S/R}{\phi}\right)$ in G associated to the homomorphism $\phi\colon R \to \mathbb{F}_q$ given by $\boldsymbol{A} \mapsto \boldsymbol{a} \in \mathbb{F}_q^n$, where $R = \mathbb{F}_q[\boldsymbol{A}, \operatorname{disc} \mathcal{F}^{-1}]$ and S is the integral closure of R in the splitting field of $\mathcal{F}$. See Appendix A, in particular (A.11), for more details.

Let $\boldsymbol{A} = (A_1, \ldots, A_n)$ be an n-tuple of variables and set

$$\mathcal{F}_i = T^n + A_1 T^{n-1} + \cdots + A_n + h_i(T) \quad \text{and} \quad \mathcal{F} = \mathcal{F}_1 \cdots \mathcal{F}_s, \tag{3.1}$$

where the h_i's are distinct polynomials. Let L be the splitting field of $\mathcal{F}$ over $K = \mathbb{F}_q(\boldsymbol{A})$ and let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_q$. By [2, Proposition 3.1],

$$G := \mathrm{Gal}(\mathcal{F}, K) = \mathrm{Gal}(L/K) = \mathrm{Gal}(\mathbb{F}L/\mathbb{F}K) = S_n^s.$$

In [2] it is assumed that q is odd, but using [4] that restriction can now be removed for $n > 2$. This in particular implies that $L \cap \mathbb{F} = \mathbb{F}_q$ (since the image of the restriction map $\mathrm{Gal}(\mathbb{F}L/\mathbb{F}K) \to \mathrm{Gal}(L/K)$ is $\mathrm{Gal}(L/L \cap \mathbb{F}K)$, so by the above and Galois correspondence $L \cap (\mathbb{F}K) = K$, and in particular $L \cap \mathbb{F} = K \cap \mathbb{F} = \mathbb{F}_q$). Hence we may apply Theorem 3.1 with the conjugacy class

$$C = \{(\sigma_1, \ldots, \sigma_s) \in G : \lambda_{\sigma_i} = \lambda_i\}$$

to get that

$$|\#\{\boldsymbol{a} \in \mathbb{F}_q^n : \mathrm{Fr}_{\boldsymbol{a}} = C\} - |C|/|G| \cdot q^n| \leq c(s, n) q^{n-1/2}.$$

Since $|C|/|G| = p(\lambda_1) \cdots p(\lambda_s)$ and since $\#\{\boldsymbol{a} \in \mathbb{F}_q^n : \mathrm{disc}_T(\mathcal{F})(\boldsymbol{a}) = 0\} = O_{s,n}(q^{n-1})$, it remains to show that for $\boldsymbol{a} \in \mathbb{F}_q^n$ with $\mathrm{disc}_T(\mathcal{F}(\boldsymbol{a})) \neq 0$ we have $\mathrm{Fr}_{\boldsymbol{a}} = C$ if and only if $\lambda_{\mathcal{F}_i(\boldsymbol{a},T)} = \lambda_i$ for all $i = 1, \ldots, s$.

And indeed, extend the specialization $\boldsymbol{A} \mapsto \boldsymbol{a}$ to a homomorphism Φ of $\mathbb{F}_q[\boldsymbol{A}, \boldsymbol{Y}]$ to $\mathbb{F}$, where $\boldsymbol{Y} = (Y_{ij})$, and $Y_{i1}, \ldots, Y_{in}$ are the roots of $\mathcal{F}_i$. Then $\mathrm{Fr}_{\boldsymbol{a}}$ is, by definition, the conjugacy class of the Frobenius element $\mathrm{Fr}_\Phi \in G$ which is defined by

$$\Phi(\mathrm{Fr}_\Phi(Y_{ij})) = \Phi(Y_{ij})^q. \tag{3.2}$$

Note that Fr_Φ permutes the roots of each $\mathcal{F}_i$ and hence can be identified with a s-tuple of permutations $\mathrm{Fr}_\phi = (\sigma_1, \ldots, \sigma_s) \in G = S_n^s$. Since the $\Phi(Y_{ij})$ are distinct, the cycle structure of σ_i equals the cycle structure of the $\Phi(Y_{ij}) \to \Phi(Y_{ij})^q$, $j = 1, \dots, n$ by (3.2) which in turn equals the cycle structure of the polynomial $\mathcal{F}_i(\boldsymbol{a}, T)$. Hence $\mathrm{Fr}_\Phi \in C$ if and only if $\lambda_{\mathcal{F}_i(\boldsymbol{a},T)} = \lambda_i$ for all i, as needed. □

4. Proof of Theorem 1.1

First we need the following lemma:

Lemma 4.1. *Let $f \in \mathcal{M}_n$ and $h \in \mathbb{F}_q[t]$ such that $\deg(h) < n$. Then we have that*

$$\#\{f \in \mathcal{M}_n : f \text{ and } f+h \text{ are square-free}\} = q^n + O(q^{n-1}). \tag{4.1}$$

Proof. The number of square-free $f \in \mathcal{M}_n$ is $q^n - q^{n-1}$ for $n \geq 2$ (for $n = 1$ it is q), and since $n > \deg(h)$, as f runs over all monic polynomials of degree n so does $f + h$, and hence the number of $f \in \mathcal{M}_n$ such that $f + h$ is square-free is also $q^n - q^{n-1}$. Therefore there are at most $2q^{n-1}$ monic $f \in \mathcal{M}_n$ for which at least one of f, $f + h$ is not square-free, as claimed. □

We denote by $\langle A \rangle$ the mean value of an arithmetic function A over $\mathcal{M}_n$:

$$\langle A \rangle := \frac{1}{q^n} \sum_{f \in \mathcal{M}_n} A(f) \ . \tag{4.2}$$

For this it follows that if A is an arithmetic function on $\mathcal{M}_n$ that is bounded independently of q, then

$$\langle A \rangle = \frac{1}{q^n} \sum_{\substack{f \in \mathcal{M}_n \\ f \text{ and } f+h \text{ square-free}}} A(f) + O\big(q^{n-1}\big). \tag{4.3}$$

Now for square-free f, the divisor function $d_k(f)$ depends only on the cycle structure of f, namely

$$d_k(f) = k^{|\lambda(f)|}, \tag{4.4}$$

where for a partition $\lambda = (\lambda_1, \dots, \lambda_n)$ of n, we denote by $|\lambda| = \sum \lambda_j$ the number of part of λ. Therefore we may apply (4.3) with (4.4) to get

$$\langle d_k(\bullet) d_k(\bullet + h) \rangle = \left\langle k^{|\lambda(\bullet)|} k^{|\lambda(\bullet+h)|} \right\rangle + O(q^{-1}). \tag{4.5}$$

Since the function $k^{\lambda(f)}$ depends only on the cycle structure of f, it follows from Theorem 1.4 that

$$\left\langle k^{|\lambda(\bullet)|} k^{|\lambda(\bullet+h)|} \right\rangle = \left\langle k^{|\lambda(\bullet)|} \right\rangle \left\langle k^{|\lambda(\bullet+h)|} \right\rangle + O(q^{-1/2}) = \left\langle k^{|\lambda(\bullet)|} \right\rangle^2 + O(q^{-1/2}). \tag{4.6}$$

Applying again (4.3) with (4.4) together with Lemma 2.2 we conclude that

$$\left\langle k^{|\lambda(\bullet)|} \right\rangle = \langle d_k(\bullet) \rangle + O(q^{-1}) = \binom{n+k-1}{k-1} + O(q^{-1}). \tag{4.7}$$

Combining (4.5), (4.6), and (4.7) then gives the desired result. □

5. Proof of Theorem 1.2

We argue as in Section 4:

$$\begin{aligned}\left\langle \prod_{i=1}^{s} d_{k_i}(\bullet + h_i)\right\rangle &= \left\langle \prod_{i=1}^{s} k_i^{|\lambda(\bullet+h_i)|}\right\rangle + O(q^{-1})\\ &= \prod_{i=1}^{s}\left\langle k_i^{|\lambda_i(\bullet)|}\right\rangle + O(q^{-1/2})\\ &= \prod_{i=1}^{s}\binom{n+k_i-1}{k_i-1} + O(q^{-1/2}).\end{aligned}$$

(Here the first passage uses (4.3) with (4.4), the last also uses Lemma 2.2, and the middle passage is done by invoking Theorem 1.4.) □

6. Proof of Theorem 1.3

Let $\mathbf{1}_{\mathcal{P}}$ be the characteristic function of the primes of degree n, i.e.

$$\mathbf{1}_{\mathcal{P}}(f) = \chi_{(0,0,\dots,0,1)}(f) = \begin{cases} 1, & \text{if } f \in \mathcal{P}_n \\ 0, & \text{otherwise.}\end{cases} \tag{6.1}$$

The Prime Polynomial Theorem gives that $\langle \mathbf{1}_{\mathcal{P}}\rangle = 1/n + O(q^{-1})$ and we have calculated in Section 4 that $\left\langle k^{|\lambda(\bullet)|}\right\rangle = \binom{n+k-1}{k-1} + O(q^{-1})$. Since these two functions clearly depend only on cycle structures (recall that $\alpha \neq 0$), Theorem 1.4 gives

$$\left\langle \mathbf{1}_{\mathcal{P}}(\bullet)\cdot k^{|\lambda(\bullet)|}\right\rangle = \langle \mathbf{1}_{\mathcal{P}}(\bullet)\rangle \left\langle k^{|\lambda(\bullet)|}\right\rangle = \frac{1}{n}\binom{n+k-1}{k-1} + O(q^{-1/2}). \tag{6.2}$$

Therefore,

$$\begin{aligned}\frac{n}{q^n}\sum_{P\in\mathcal{P}_n} d_k(P+\alpha) &= n\left\langle \mathbf{1}_{\mathcal{P}}(\bullet)\cdot k^{|\lambda(\bullet)|}\right\rangle\\ &= \binom{n+k-1}{k-1} + O(q^{-1/2}),\end{aligned}$$

as needed. □

7. Comparing conjectures and our results

In this section we check the compatibility of the theorems presented in Section § 1.3 with the known results over the integers.

7.1. **Estermann's theorem for $\mathbb{F}_q[t]$.** First we prove the function field analogue of Estermann's result (1.2). For simplicity, we carry it out for $h = 1$.

Theorem 7.1. *Assume that $n \geq 1$. Then*

$$\frac{1}{q^n}\sum_{f\in\mathcal{M}_n} d_2(f)d_2(f+1) = (n+1)^2 - \frac{1}{q}(n-1)^2. \tag{7.1}$$

(Note that q is fixed in this theorem).

We need two auxiliary lemmas before proving Theorem 7.1.

Let $A, B \in \mathbb{F}_q[t]$ be monic polynomials. We want to count the number of monic polynomials solutions $(u,v) \in \mathbb{F}_q[t]^2$ of the linear Diophantine equation

$$Au - Bv = 1, \qquad \deg(Au) = n = \deg(Bv)\ . \tag{7.2}$$

As follows from the Euclidean algorithm, a necessary and sufficient condition for the equation $Au - Bv = 1$ to be solvable in $\mathbb{F}_q[t]$ is $\gcd(A,B) = 1$.

Lemma 7.2. *Given monic polynomials $A, B \in \mathbb{F}_q[t]$, $\gcd(A,B) = 1$, and*

$$n \geq \deg(A) + \deg(B) \tag{7.3}$$

then the set of monic solutions (u,v) of (7.2) forms a nonempty affine subspace of dimension $n - \deg(A) - \deg(B)$, hence the number of solutions is exactly $q^n/|A||B|$.

Proof. We first ignore the degree condition. By the theory of the linear Diophantine equation, given a particular solution $(u_0, v_0) \in \mathbb{F}_q[t]^2$, all other solutions in $\mathbb{F}_q[t]^2$ are of the form

$$(u_0, v_0) + k(B, A) \tag{7.4}$$

where $k \in \mathbb{F}_q[t]$ runs over all polynomials.

Given u_0, we may replace it by $u_1 = u_0 + kB$ where $\deg(u_1) < \deg(B)$ (or is zero), so that we may assume that the particular solution satisfies

$$\deg(u_0) < \deg(B). \tag{7.5}$$

In that case, if $k \neq 0$ then

$$\deg(u_0 + kB) = \deg(kB) \tag{7.6}$$

and $u_0 + kB$ is monic if and only if k is monic. Hence if $k \neq 0$, then

$$\begin{aligned}\deg(u_0 + kB) = n - \deg(A) &\Leftrightarrow \deg(kB) = n - \deg(A) \\ &\Leftrightarrow \deg(k) = n - \deg(A) - \deg(B).\end{aligned} \tag{7.7}$$

Thus the set of solutions of (7.2) is in one-to-one correspondence with the space $\mathcal{M}_{n-\deg(A)-\deg(B)}$ of monic k of degree $n-\deg(A)-\deg(B)$. In particular the number of solutions is $q^n/|A||B|$. $\square$

Let

(7.8)
$$S(\alpha,\beta;\gamma,\delta) := \#\left\{x\in\mathcal{M}_\alpha, y\in\mathcal{M}_\beta, z\in\mathcal{M}_\gamma, u\in\mathcal{M}_\delta : xy-zu=1\right\}.$$

Then we have the following lemma.

Lemma 7.3. *For $\alpha+\beta=n=\gamma+\delta$,*

$$S(\alpha,\beta;\gamma,\delta) = q^n\times\begin{cases}1, & \text{if } \min(\alpha,\beta;\gamma,\delta)=0,\\ 1-\frac{1}{q}, & \text{otherwise.}\end{cases} \tag{7.9}$$

Proof. We have some obvious symmetries from the definition

$$S(\alpha,\beta;\gamma,\delta) = S(\beta,\alpha;\gamma,\delta) = S(\alpha,\beta;\delta,\gamma) \tag{7.10}$$

and hence to evaluate $S(\alpha,\beta;\gamma,\delta)$ it suffices to assume

$$\alpha\le\beta,\quad \gamma\le\delta. \tag{7.11}$$

Assuming (7.11), we write

$$S(\alpha,\beta;\gamma,\delta) = \sum_{\substack{x\in\mathcal{M}_\alpha\\ z\in\mathcal{M}_\gamma\\ \gcd(x,z)=1}} \#\{y\in\mathcal{M}_\beta, u\in\mathcal{M}_\delta : xy-zu=1\} \tag{7.12}$$

Note that $\alpha,\gamma\le n/2$ (since $\alpha+\beta=n$ and $\alpha\le\beta$) and hence $\alpha+\gamma\le\frac{1}{2}(\alpha+\beta+\gamma+\delta)=n$. Thus we may use Lemma 7.2 to deduce that

$$\#\{y\in\mathcal{M}_\beta, u\in\mathcal{M}_\delta : xy-zu=1\} = q^{n-\alpha-\gamma} \tag{7.13}$$

and therefore

$$S(\alpha,\beta;\gamma,\delta) = q^{n-\alpha-\gamma}\sum_{\substack{x\in\mathcal{M}_\alpha\\ z\in\mathcal{M}_\gamma\\ \gcd(x,z)=1}} 1. \tag{7.14}$$

Recall the Möbius inversion formula, which says that for monic f, $\sum_{d|f}\mu(d)$ equals 1 if $f=1$, and 0 otherwise. Hence we may write the coprimality condition $\gcd(x,z)=1$ using the Möbius function as

$$\sum_{d|x,\ d|z}\mu(d) = \begin{cases}1, & \gcd(x,z)=1,\\ 0, & \text{otherwise.}\end{cases} \tag{7.15}$$

and therefore

(7.16)

$$\begin{aligned} S(\alpha,\beta;\gamma,\delta) &= q^{n-\alpha-\gamma} \sum_{\substack{x\in\mathcal{M}_\alpha\\ z\in\mathcal{M}_\gamma}} \sum_{d|x,d|z} \mu(d) \\ &= q^{n-\alpha-\gamma} \sum_{\substack{\deg(d)\le\min(\alpha,\gamma)\\ d \text{ monic}}} \mu(d)\#\{x\in\mathcal{M}_\alpha : d \mid x\}\cdot\#\{z\in\mathcal{M}_\gamma : d\mid z\} \\ &= q^{n-\alpha-\gamma} \sum_{\substack{\deg(d)\le\min(\alpha,\gamma)\\ d \text{ monic}}} \mu(d)\frac{q^\alpha}{|d|}\cdot\frac{q^\gamma}{|d|} \\ &= q^n \sum_{\substack{\deg(d)\le\min(\alpha,\gamma)\\ d \text{ monic}}} \frac{\mu(d)}{|d|^2} \\ &= q^n \sum_{\substack{\deg(d)\le\min(\alpha,\beta;\gamma,\delta)\\ d \text{ monic}}} \frac{\mu(d)}{|d|^2}, \end{aligned}$$

where we have used the fact that $\alpha\le\beta$ and $\gamma\le\delta$.

We next claim that

$$\sum_{\substack{\deg(d)\le\eta\\ d \text{ monic}}} \frac{\mu(d)}{|d|^2} = \begin{cases} 1, & \eta=0,\\ 1-\frac{1}{q}, & \eta\ge 1,\end{cases} \tag{7.17}$$

which when we insert into (7.16) proves the lemma.

To prove (7.17), we sum over d of fixed degree

$$\sum_{\substack{\deg(d)\le\eta\\ d \text{ monic}}} \frac{\mu(d)}{|d|^2} = \sum_{0\le\xi\le\eta} \frac{1}{q^{2\xi}} \sum_{d\in\mathcal{M}_\xi} \mu(d) \tag{7.18}$$

and recall that ([22, Chapter 2 - Exercise 12])

$$\sum_{d\in\mathcal{M}_\xi} \mu(d) = \begin{cases} 1, & \xi=0\\ -q, & \xi=1\\ 0, & \xi\ge 2\end{cases} \tag{7.19}$$

from which (7.17) follows. □

Proof of Theorem 7.1. We write

(7.20)

$$\begin{aligned} \nu &:= \sum_{f\in\mathcal{M}_n} d_2(f)d_2(f+1) \\ &= \#\{x,y,z,u\in\mathbb{F}_q[t] \text{ monic} : xy-zu=1, \quad \deg(xy)=n=\deg(zu)\}. \end{aligned}$$

We partition this into a sum over variables with fixed degree, that is

$$\nu = \sum_{\substack{\alpha+\beta=n\\ \gamma+\delta=n\\ \alpha,\beta,\gamma,\delta\geq 0}} S(\alpha,\beta;\gamma,\delta). \tag{7.21}$$

We now input the results of Lemma 7.3 into (7.21) to deduce that

$$\nu = \sum_{\substack{\alpha+\beta=n\\ \gamma+\delta=n\\ \alpha,\beta,\gamma,\delta\geq 0}} q^n \times \begin{cases} 1, & \min(\alpha,\beta;\gamma,\delta)=0,\\ 1-\frac{1}{q}, & \text{otherwise.}\end{cases} \tag{7.22}$$

Of the $(n+1)^2$ quadruples of non-negative integers $(\alpha,\beta;\gamma,\delta)$ so that $\alpha+\beta = n = \gamma+\delta$, there are exactly $4n$ tuples $(\alpha,\beta;\gamma,\delta)$ for which $\min(\alpha,\beta)=0=\min(\gamma,\delta)$, namely they are

$$(n,0;n,0),\quad (n,0;0,n),\quad (0,n;n,0),\quad (0,n;0,n) \tag{7.23}$$

and the $4(n-1)$ tuples of the form

$$(n,0;i,n-i),(0,n;i,n-i),(i,n-i;n,0),(i,n-i;0,n) \tag{7.24}$$

for $0<i<n$.

Concluding, we have

$$\begin{aligned}\nu &= (4+4(n-1))\cdot q^n + \left[(n+1)^2-(4+4(n-1))\right]\cdot q^n\left(1-\frac{1}{q}\right)\\ &= q^n\left((n+1)^2-\frac{1}{q}(n-1)^2\right)\end{aligned} \tag{7.25}$$

proving the theorem. □

It is easy to check that Theorem 1.1 is compatible with the function field analogue of Estermann's result. Taking $q\to\infty$ in (7.1) we recover the same results as presented in (1.17) with $k=2$.

7.2. **Higher divisor functions.** Next, we want to check compatibility of our result in Theorem 1.1 with what is conjectured over the integers. It is conjectured that

$$D_k(x;h)\sim xP_{2(k-1)}(\log x;h) \qquad \text{as } x\to\infty, \tag{7.26}$$

where $P_{2(k-1)}(u;h)$ is a polynomial in u of degree $2(k-1)$, whose coefficients depend on h (and k). This conjecture appears in the work of Ivić [15], and Conrey and Gonek [6], and from their work, with some effort, we can explicitly write the conjectural leading coefficient for the desired polynomial. The conjecture over $\mathbb{Z}$ states that

$$P_{2(k-1)}(u;h) = \frac{1}{[(k-1)!]^2} A_k(h) u^{2k-2} + \dots, \tag{7.27}$$

where

$$A_k(h) = \sum_{m=1}^{\infty} \frac{c_m(h)}{m^2} C_{-k}^2(m) \tag{7.28}$$

with

$$C_{-k}(m) = m^{1-k} \sum_{a_1=1}^{m} \cdots \sum_{a_k=1}^{m} e\left(\frac{ha_1 \cdots a_k}{m}\right), \tag{7.29}$$

where $e(x) = e^{2\pi i x}$ and $c_m(h)$ is the Ramanujan sum

$$c_m(h) = \sum_{\substack{a=1 \\ (a,m)=1}}^{m} e^{2\pi i \frac{a}{m} h} = \sum_{d|\gcd(m,h)} d\mu\left(\frac{m}{d}\right). \tag{7.30}$$

We now translate the conjecture above to the function field setting using the correspondence $x \leftrightarrow q^n$, $\log x \leftrightarrow n$ and that sum over positive integers correspond to sum over monic polynomials in $\mathbb{F}_q[t]$. Under this correspondence the function field analogue of the above polynomial is given in the following conjecture

Conjecture 7.4. *For q fixed, let $0 \neq h \in \mathbb{F}_q[t]$. Then as $n \to \infty$,*

$$\sum_{f \in \mathcal{M}_n} d_k(f) d_k(f+h) \sim \frac{1}{[(k-1)!]^2} A_{k,q}(h) q^n n^{2k-2}, \tag{7.31}$$

where

$$A_{k,q}(h) = \sum_{\substack{m \in \mathbb{F}_q[t] \\ \text{monic}}} \frac{c_{m,q}(h)(\gcd(m,h))^{2(k-1)}}{|m|^{2(k-1)}} g_{k-1}^2\left(\frac{m}{\gcd(m,h)}\right), \tag{7.32}$$

where $|m| = q^{\deg(m)}$,

$$g_{k-1}(f) = \#\left\{a_1, \dots, a_{k-1} \bmod f : a_1 \dots a_{k-1} \equiv 0 \bmod f\right\}, \tag{7.33}$$

and

$$c_{m,q}(h) = \sum_{d|\gcd(m,h)} |d| \mu\left(\frac{m}{d}\right) \tag{7.34}$$

is the Ramanujan sum over $\mathbb{F}_q[t]$. The sum above is over all monic polynomials $d \in \mathbb{F}_q[t]$ and $\mu(f)$ is the Möbius function for $\mathbb{F}_q[t]$ and $\Phi(m)$ is the $\mathbb{F}_q[t]$-analogue for Euler's totient function.

Remark. *Note that*

$$C_{q,-k}^2(m) = \frac{gcd(m,h)^{2k-1}}{|m|^{k-1}} g_{k-1}^2\left(\frac{m}{gcd(m,h)}\right) \tag{7.35}$$

correspond to $C_{-k}^2(m)$ as given in (7.29).

Remark. *Note that we establish this conjecture for $k = 2$ and $h = 1$ in Theorem 7.1.*

We now check that our Theorem 1.1 is consistent with the conjecture (7.27) and 7.32 for the leading term of the polynomial $P_{2(k-1)}(u;h)$.

The polynomial given by Theorem 1.1 is

$$\binom{n+k-1}{k-1}^2 = \frac{1}{[(k-1)!]^2} n^{2(k-1)} + \dots. \tag{7.36}$$

We wish to show that as $q \to \infty$, $A_{k,q}(h)/[(k-1)!]^2$ matches the leading coefficient of $\binom{n+k-1}{k-1}^2$, that is

$$\lim_{q\to\infty} A_{k,q}(h) = 1. \tag{7.37}$$

Indeed, from (7.34) we note that $|c_{m,q}(h)| = O_h(1)$, and it is easy to see that

$$g_{k-1}(n) \le n^{k-1} d(n)^{k-1} \ll |n|^{k-2+\epsilon}, \quad \forall \epsilon > 0. \tag{7.38}$$

Thus we find

$$A_{k,q}(h) = 1 + O\Big(\sum_{\substack{m\in\mathcal{M} \\ \deg(m)>0}} \frac{1}{|m|^{2-\epsilon}} \Big). \tag{7.39}$$

The series in the O-term is a geometric series:

$$\sum_{\substack{m\in\mathcal{M} \\ \deg(m)>0}} \frac{1}{|m|^{2-\epsilon}} = \sum_{n=1}^{\infty} \frac{1}{q^{n(2-\epsilon)}} \#\mathcal{M}_n = \sum_{n=1}^{\infty} \frac{1}{q^{n(1-\epsilon)}} = \frac{1/q^{1-\epsilon}}{1-1/q^{1-\epsilon}} \tag{7.40}$$

and hence tends to 0 as $q \to \infty$, giving (7.37).

Acknowledgments. We thank an anonymous referee for detailed comments and suggestions.

Appendix A. An explicit Chebotarev theorem

We prove an explicit Chebotarev theorem for function fields over finite fields. This theorem is known to experts, cf. [5, Theorem 4.1], [11, Proposition 6.4.8] or [16, Theorem 9.7.10], however there it is not given explicitly with the uniformity that we need to use. Therefore we provide a complete proof.

A.1. **Frobenius elements.** Let $\mathbb{F}_q$ be a finite field with q elements and algebraic closure $\mathbb{F}$. We denote by Fr_q the Frobenius automorphism $x \mapsto x^q$.

Let R be an integrally closed finitely generated $\mathbb{F}_q$-algebra with fraction field K, let $\mathcal{F} \in R[T]$ be a monic separable polynomial of degree $\deg \mathcal{F} = m$ such that

$$\operatorname{disc} \mathcal{F} \in R^* \tag{A.1}$$

is invertible. Let $\boldsymbol{Y} = (Y_1, \ldots, Y_m)$ be the roots of $\mathcal{F}$, and put

$$S = R[\boldsymbol{Y}], \qquad L = K(\boldsymbol{Y}), \qquad \text{and} \qquad G = \mathrm{Gal}(L/K).$$

We identify G with a subgroup of S_m via the action on $Y_1, \ldots, Y_m$:

$$g(Y_i) = Y_{g(i)}, \qquad g \in G \leq S_m. \tag{A.2}$$

By (A.1) and Cramer's rule, S is the integral closure of R in L and S/R is unramified. In particular, the relative algebraic closure $\mathbb{F}_{q^\mu}$ of $\mathbb{F}_q$ in L is contained in S. For each $\nu \geq 0$ we let

$$G_\nu = \{g \in G : g(x) = x^{q^\nu},\ \forall x \in \mathbb{F}_{q^\mu}\}, \tag{A.3}$$

the preimage of Fr_q^ν in G under the restriction map. Since $\mathrm{Gal}(\mathbb{F}_{q^\nu}/\mathbb{F}_q)$ is commutative, G_ν is stable under conjugation.

For every $\Phi \in \mathrm{Hom}_{\mathbb{F}_q}(S, \mathbb{F})$ with $\Phi(R) = \mathbb{F}_{q^\nu}$ there exists a unique element in G, which we call the *Frobenius element* and denote by

$$\left[\frac{S/R}{\Phi}\right] \in G, \tag{A.4}$$

such that

$$\Phi\left(\left[\frac{S/R}{\Phi}\right] x\right) = \Phi(x)^{q^\nu}, \qquad \forall x \in S. \tag{A.5}$$

Since S is generated by $\boldsymbol{Y}$ over R, it suffices to consider $x \in \{Y_1, \ldots, Y_k\}$ in (A.5). If we further assume that $\Phi \in \mathrm{Hom}_{\mathbb{F}_{q^\mu}}(S, \mathbb{F})$, then (A.5) gives that $\left[\frac{S/R}{\Phi}\right] x = x^{q^\nu}$ for all $x \in \mathbb{F}_{q^\mu}$, hence

$$\Phi(R) = \mathbb{F}_{q^\nu} \Longrightarrow \left[\frac{S/R}{\Phi}\right] \in G_\nu. \tag{A.6}$$

Lemma A.1. *For every $g \in S_m$ and $\nu \geq 1$ there exists $V_{g,\nu} = (v_{ij}) \in \mathrm{GL}_m(\mathbb{F})$ such that such that Fr_{q^ν} acts on the rows of $V_{g,\nu}$ as g acts on $\boldsymbol{Y}$:*

$$v_{ij}^{q^\nu} = v_{g(i)j}. \tag{A.7}$$

Proof. By replacing q by q^ν, we may assume without loss of generality that $\nu = 1$. By relabelling we may assume without loss of generality that

$$g = (s_1\ \cdots\ e_1)(s_2\ \cdots\ e_2)\cdots(s_k\ \cdots\ e_k), \tag{A.8}$$

where $s_1 = 1$, $s_{i+1} = e_i + 1$, and $e_k = m$.

Let V be the block diagonal matrix

$$V = \begin{pmatrix} V_1 & & & \\ & V_2 & & \\ & & \ddots & \\ & & & V_k \end{pmatrix},$$

where

$$V_i = \begin{pmatrix} 1 & \zeta_i & \cdots & \zeta_i^{\lambda_i-1} \\ 1 & \zeta_i^q & \cdots & \zeta_i^{q(\lambda_i-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \zeta_i^{q^{\lambda_i-1}} & \cdots & \zeta_i^{q^{\lambda_i-1}(\lambda_i-1)} \end{pmatrix},$$

is the vandermonde matrix corresponding to an element $\zeta_i \in \mathbb{F}$ of degree $\lambda_i = e_i - s_i$ over $\mathbb{F}_q$. So $\det V_i = \prod_{1\leq j'<j\leq \lambda_i}(\zeta_i^{q^{j'-1}} - \zeta_i^{q^{j-1}}) \neq 0$, hence V is invertible, and by definition Fr_q acts on the rows of V as the permutation g. □

Lemma A.2. *Let $\Phi\colon S\to\mathbb{F}$ with $\Phi(R) = \mathbb{F}_{q^\nu}$ and let $g\in G_\nu$. Then*

$$\left[\frac{S/R}{\Phi}\right] = g \iff V^{-1}\begin{pmatrix}\Phi(Y_1)\\ \vdots \\ \Phi(Y_m)\end{pmatrix} \in \mathbb{F}_{q^\nu}^m, \tag{A.9}$$

where $V = V_{g,\nu}$ is the matrix from Lemma A.1.

Proof. Let $z_1,\dots,z_m\in\mathbb{F}$ be the unique solution of the linear system

$$\Phi(Y_i) = \sum_{j=1}^m v_{ij}z_j, \qquad i=1,\dots m, \tag{A.10}$$

i.e. $\begin{pmatrix}z_1\\ \vdots\\ z_m\end{pmatrix} = V^{-1}\begin{pmatrix}\Phi(Y_1)\\ \vdots \\ \Phi(Y_m)\end{pmatrix}$. If $z_i\in\mathbb{F}_{q^\nu}$, i.e. $z_i^{q^\nu} = z_i$, we get by applying Fr_{q^ν} on (A.10) that

$$\Phi(Y_i)^{q^\nu} = \sum_{j=1}^m v_{ij}^{q^\nu} z_i = \sum_{j=1}^m v_{g(i)j}z_i = \Phi(Y_{g(i)}).$$

Hence $\left[\frac{S/R}{\Phi}\right] = g$ by (A.5).

Conversely, if $\left[\frac{S/R}{\Phi}\right] = g$, then $\Phi(Y_i)^{q^\nu} = \Phi(Y_{g(i)})$ by (A.2) and (A.5). We thus get that Fr_{q^ν} permutes the equations in (A.10), hence Fr_{q^ν} fixes the unique solution of (A.10). That is to say, $z_i^{q^\nu} = z_i$, as needed. □

Next we describe the dependence of the Frobenius element when varying the homomorphisms. For $\phi\in\mathrm{Hom}_{\mathbb{F}_q}(R,\mathbb{F})$ we define

$$\left(\frac{S/R}{\phi}\right) = \left\{\left[\frac{S/R}{\Phi}\right] : \Phi\in\mathrm{Hom}_{\mathbb{F}_{q^\mu}}(S,\mathbb{F}) \text{ prolongs } \phi\right\}. \tag{A.11}$$

Unlike the case when working with ideals, this set is not a conjugacy class in G, since we fix the action on $\mathbb{F}_{q^\mu}$. However as we will prove below, the group G_0 acts regularly on $\left(\frac{S/R}{\phi}\right)$ by conjugation. In particular if $G_0 = G$, or equivalently if $L\cap\mathbb{F} = \mathbb{F}_q$ (with $\mathbb{F}$ denoting an algebraic closure of $\mathbb{F}_q$) then $\left(\frac{S/R}{\phi}\right)$ is a conjugacy class.

To state the result formally, we recall that a group Γ acts *regularly* on a set Ω if the action is free and transitive, i.e. for every $\omega_1, \omega_2 \in \Omega$ there exists a unique $\gamma \in \Gamma$ with $\gamma\omega_1 = \omega_2$.

Lemma A.3. *Let $\phi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F})$ and let H be the subset of $\mathrm{Hom}_{\mathbb{F}_{q^\mu}}(S, \mathbb{F})$ consisting of all homomorphisms prolonging ϕ. Assume that $\phi(R) = \mathbb{F}_{q^\nu}$.*

(1) *The group G_0 defined in* (A.3) *acts regularly on H by $g\colon \Phi \mapsto \Phi \circ g$.*
(2) *for every $g \in G_0$ and $\Phi \in H$ we have*
$$\left[\frac{S/R}{\Phi \circ g}\right] = g^{-1}\left[\frac{S/R}{\Phi}\right] g.$$
(3) *Let $\Phi \in H$, let $g = \left[\frac{S/R}{\Phi}\right]$, $H_g = \{\Psi \in H : \left[\frac{S/R}{\Psi}\right] = g\}$, and $C_{G_0}(g)$ the centralizer of g in G_0. Then $C_{G_0}(g)$ acts regularly on H_g.*
(4) *$\#H_g = \#G_0/\#C = \#G/\mu \cdot \#C$, where C is the conjugacy class of g in G_0.*

Proof. We consider $G_0 \le G$ as subgroups of S_m via the action on $Y_1, \ldots, Y_m$. Let $g \in G_0$ and $\Phi \in H$. Then $g(x) = x$ and $\Phi(x) = x$, thus $\Phi \circ g(x) = x$, for all $x \in \mathbb{F}_{q^\mu}$. Thus $\Phi \circ g \in H$. If $\Phi \circ g = \Phi$, then $\Phi(Y_{g(i)}) = \Phi(Y_i)$ for all i. Since $\operatorname{disc}\mathcal{F} \in R^*$ it follows that $\Phi(\operatorname{disc}\mathcal{F}) \neq 0$, thus Φ maps $\{Y_1, \ldots, Y_m\}$ injectively onto $\{\Phi(Y_1), \ldots, \Phi(Y_m)\}$. We thus get that $Y_{g(i)} = Y_i$, hence g is trivial. This proves that the action is free.

Next we prove that the action is transitive. Let $\Phi, \Psi \in H$. Then $\ker\Phi$ and $\ker\Psi$ are prime ideals of S that lies over the prime ideal $\ker\phi$ of R; hence over the prime $\ker\phi\mathbb{F}_{q^\mu}$ of $R\mathbb{F}_{q^\mu}$. By [17, VII,2.1], there exists $g_1 \in \mathrm{Gal}(L/K\mathbb{F}_{q^\mu}) = G_0$ such that $\ker(\Phi \circ g_1^{-1}) = g_1 \ker\Phi = \ker\Psi$. Replace Φ by $\Phi \circ g_1^{-1}$ to assume without loss of generality that $\ker\Phi = \ker\Psi$. Hence $\Phi = \alpha \circ \Psi$, where α is an automorphism of the image $\Phi(S) = \Psi(S)$ that fixes both $\mathbb{F}_{q^\mu}$ and $\phi(R) = \mathbb{F}_{q^\nu}$. That is to say, $\alpha = \mathrm{Fr}_q^\rho$, where ρ is a common multiple of ν and μ. By (A.5)
$$\Phi(x) = \Psi(x)^{q^\rho} = \Psi\left(\left[\frac{S/R}{\Psi}\right] x\right)^{q^{\rho-\nu}} = \cdots = \Psi\left(\left[\frac{S/R}{\Psi}\right]^{\rho/\nu} x\right),$$
so $\Phi = \Psi \circ g$, where $g = \left[\frac{S/R}{\Psi}\right]^{\rho/\nu}$. Since, for $x \in \mathbb{F}_{q^\mu}$ we have $g(x) = x^{q^\rho}$ and $\mu \mid \rho$, we have $g(x) = x$, so $g \in G_0$. This finishes the proof of (1).

To see (2) note that
$$\begin{aligned}\Phi\left(g\left[\frac{S/R}{\Phi \circ g}\right] x\right) &= \Phi \circ g\left(\left[\frac{S/R}{\Phi \circ g}\right] x\right)\\ &= \Phi \circ g(x)^{q^\nu} = \Phi(gx)^{q^\nu}\\ &= \Phi\left(\left[\frac{S/R}{\Phi}\right] gx\right), \qquad \text{for all } x \in S,\end{aligned}$$
so $g\left[\frac{S/R}{\Phi\circ g}\right] = \left[\frac{S/R}{\Phi}\right] g$ (since Φ is unramified), as claimed.

The rest of the proof is immediate as (3) follows immediately from (1) and (2) and (4) follows from (3). □

By (A.6) and Lemma A.3 it follows that if $\Phi(R) = \mathbb{F}_{q^\nu}$, then $\left(\frac{S/R}{\phi}\right) \subseteq G_\nu$ is an orbit of the action of conjugation from G_0.

Let $C \subseteq G$ be such an orbit, i.e. $C = C_g = \{hgh^{-1} : h \in G_0\}$, $g \in G_\nu$. Then $C \subseteq G_\nu$, since the latter is stable under conjugation (see after (A.3)). The explicit Chebotarev theorem gives the asymptotic probability that $\left(\frac{S/R}{\phi}\right) = C$:

$$P_{\nu,C} = \frac{\#\left\{\phi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F}) : \phi(R) = \mathbb{F}_{q^\nu} \text{ and } \left(\frac{S/R}{\phi}\right) = C\right\}}{\#\{\phi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F}) : \phi(R) = \mathbb{F}_{q^\nu}\}}.$$

Theorem A.4. *Let $\nu \geq 1$, let $C \subseteq G_\nu$ be an orbit of the action of conjugation from G_0. Then*

$$P_{\nu,C} = \frac{\#C}{\#G_\nu} + O_{\deg \mathcal{F}, \mathrm{cmp}(R)}(q^{-1/2}),$$

as $q \to \infty$.

We define $\mathrm{cmp}(R)$ below.

Before proving this theorem, we need to recall the Lang-Weil estimates which play a crucial role in the proof of the theorem and in particular give the asymptotic value of the denominator of $P_{\nu,C}$.

Let U be a closed subvariety of $\mathbb{A}^n_{\mathbb{F}_q}$ that is geometrically irreducible. Lang-Weil estimates give that

$$\#U(\mathbb{F}_q) = q^{\dim U} + O_{n, \deg U}(q^{\dim U - 1/2}). \tag{A.12}$$

Note that both n and $\deg U$ are stable under base change. This may be reformulated in terms of $\mathbb{F}_q$-algebras, to say that if

$$R \cong \mathbb{F}_q[X_1, \ldots, X_n, f_0^{-1}]/(f_1, \ldots, f_k), \tag{A.13}$$

then

$$\#\{\phi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F}) : \phi(R) = \mathbb{F}_q\} = q^{\nu \dim R} + O_{\mathrm{cmp}(R)}(q^{\dim R - \frac{1}{2}}), \tag{A.14}$$

provided $R \otimes \mathbb{F}$ is a domain, where $\mathrm{cmp}(R)$ is a function of $\sum \deg f_i$ and n, taking minimum over all presentations (A.13). By the remark following (A.12), it follows that if two $\mathbb{F}_q$-algebras S and S' become isomorphic over $\mathbb{F}$, then $\mathrm{cmp}(S')$ is bounded in terms of $\mathrm{cmp}(S)$. A final property needed is that if $R \to S$ is a finite map of degree d, then $\mathrm{cmp}(S)$ is bounded in terms of $\mathrm{cmp}(R)$ and d.

Proof. Let $g \in C$, let $V = V_{g,\nu}$ be as in (A.7) and let $S' = R[\boldsymbol{Z}]$, where $\boldsymbol{Z} = V^{-1}\boldsymbol{Y}$. Note that $\boldsymbol{Z}$ is the unique solution of the linear system

$$Y_i = \sum_{j=1}^{n} v_i j Z_j, \qquad i = 1, \ldots, n. \tag{A.15}$$

Let $N = \#\mathrm{Hom}_{\mathbb{F}_q}(S', \mathbb{F}_{q^\nu})$. By (A.9), the number of $\Phi \in \mathrm{Hom}_{\mathbb{F}_q}(S, \mathbb{F})$ with $\left[\frac{S/R}{\Phi}\right] = g$ equals N. By Lemma A.3, for each ϕ there exist exactly $\#G_0/\#C$ homomorphisms $\Phi \in \mathrm{Hom}_{\mathbb{F}_q}(S, \mathbb{F})$ with $\left[\frac{S/R}{\Phi}\right] = g$ prolonging ϕ. Hence,

$$\#\left\{\phi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F}) : \phi(R) = \mathbb{F}_{q^\nu} \text{ and } \left(\frac{S/R}{\phi}\right) = C\right\} = \#C/\#G_0 \cdot N.$$

Since G_ν is a coset of G_0, $\#G_0 = \#G_\nu$. Hence it suffices to prove that $N = q^{\nu \dim R} + O_{\mathrm{cmp}(R), \deg \mathcal{F}}(q^{\nu - 1/2})$: As $R \to S'$ is a finite map of degree $\deg \mathcal{F}$, we get that $\dim R = \dim S'$ and $\mathrm{cmp}(S')$ is bounded in terms of $\mathrm{cmp}(R)$ and $\deg \mathcal{F}$. It suffices to show that $S' \cap \mathbb{F} \subseteq \mathbb{F}_{q^\nu}$ since then by (A.14) we have

$$N = q^{\nu \dim S'} + O_{\mathrm{cmp} S'}(q^{\nu \dim S' - 1/2}) = q^{\nu \dim R} + O_{\mathrm{cmp}(R), \deg F}(q^{\nu \dim R - 1/2}),$$

and the proof is done.

Let L be the fraction field of S and K of R. Since L/K is Galois and $L \cap \mathbb{F} = \mathbb{F}_{q^\mu}$ and since the actions of Fr_{q^ν} and g agrees on $\mathbb{F}_{q^\mu}$, it follows that there exists an automorphism τ of $L\mathbb{F}$ such that $\tau|_L = g$ and $\tau|_{\mathbb{F}} = \mathrm{Fr}_{q^\nu}$. By (A.7) τ permutes the equations (A.15), hence fixes $\boldsymbol{Z}$ and thus S'. In particular, if $x \in S' \cap \mathbb{F}$, then $x^{q^\nu} = \tau(x) = x$, so $x \in \mathbb{F}_{q^\nu}$, as was needed to complete the proof.

$\square$

References

[1] R. Arratia, A.D. Barbour and S. Tavaré, *Logarithmic combinatorial structures: a probabilistic approach.* EMS Monographs in Mathematics. European Mathematical Society (EMS), Zrich, 2003.

[2] L. Bary-Soroker, *Hardy-Littlewood tuple conjecture over large finite fields*, Int. Math. Res. Not., 2012, 1–8 (2012).

[3] E. Bombieri, J. Friedlander and H. Iwaniec, *Primes in arithmetic progressions to large moduli*, Acta Math. 156 (1986), 203–251.

[4] D. Carmon, *The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field in characteristic* 2, preprint.

[5] N. Chavdarov, *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. **87** (1997), no. 1, 151180.

[6] J. B. Conrey and S. M. Gonek, *High Moments of the Riemann Zeta-Function*, Duke Math. J. 107, 577–604 (2001).

[7] J. -M. Deshouillers and H. Iwaniec, *An additive divisor problem.* J. London Math. Soc. (2) 26 (1982), no. 1, 1–14.

[8] T. Estermann, *Über die Darstellungen einer Zahl als Differenz von zwei Produkten.* J. Reine Agnew. Math. 164 (1931): 173–182.

[9] E. Fouvry, *Sur le probleme des diviseurs de titchmarsh*, J. Reine Agnew. Math. 357 (1984), 51–76.

[10] E. Fouvry and G. Tenenbaum, *Sur la corrélation des fonctions de Piltz*, Rev. Mat. Iberoam., Vol. 1, No. 3 (1985), 43–54.

[11] M. D. Fried and M. Jarden, *Field arithmetic.* Third edition. Revised by Jarden. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys

in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], **11**. Springer-Verlag, Berlin, 2008. xxiv+792 pp. ISBN: 978-3-540-77269-9
[12] D. R. Heath–Brown, *The fourth power moment of the Riemann zeta function*, J. London Math. Soc. (3) **38** (1979), 385–422.
[13] A. E. Ingham, *Mean-value theorems in the theory of the Riemann Zeta-function*, Proc. London Math. Soc. (2) 27 (1928), 273–300.
[14] A. Ivić, *On the ternary additive divisor problem and the sixth moment of the zeta-function*, Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995), 205–243, London Math. Soc. Lecture Note Ser., 237, Cambridge Univ. Press, Cambridge, 1997.
[15] A. Ivić, *The general additive divisor problem and moments of the zeta-function*, New trends in probability and statistics, Vol. 4 (Palanga, 1996), 69-89, VSP, Utrecht, 1997.
[16] N. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues, and Monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999.
[17] S. Lang, *Algebra*. Revised third edition. Graduate Texts in Mathematics, **211**. Springer-Verlag, New York, 2002. xvi+914 pp. ISBN: 0-387-95385-X
[18] Ju. V. Linnik, *The dispersion method in binary additive problems*, Transl. Math. Monographs, No. 4, Amer. Math. Soc. (1963).
[19] Y. Motohashi, *An Asymptotic Series for an Additive Divisor Problem*, Math. Z. 170 (1980), 43–63.
[20] Y. Motohashi, *On Some Additive Divisor Problems*, J. Math. Soc. Japan (4) 28 (1976), 605–784.
[21] Y. Motohashi, *On Some Additive Divisor Problems. II*, Proc. Japan Acad., (6) **52** (1976), 279–281.
[22] M. Rosen, *Number theory in function fields*. Graduate Texts in Mathematics, **210**. Springer-Verlag, New York, 2002. xii+358 pp. ISBN: 0-387-95335-3
[23] M. Nair and G. Tenenbaum, *Short sums of certain arithmetic functions*, Acta Math. 180 (1998), no. 1, 119–144.
[24] E. C. Titchmarsh, *A Divisor Problem*, Rend. di Palermo 54 (1931), 414–429.

Institut des Hautes Études Scientifiques (IHÉS), Le Bois-Marie 35, route de Chartres, Bures-sur-Yvette, 91440, France
E-mail address: j.c.andrade@ihes.fr

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel
E-mail address: barylior@post.tau.ac.il

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel
E-mail address: rudnick@post.tau.ac.il