

Mean values of arithmetic functions in short intervals and in arithmetic progressions in the large-degree limit

Ofir Gorodetsky

Abstract

A classical problem in number theory is showing that the mean value of an arithmetic function is asymptotic to its mean value over a short interval or over an arithmetic progression, with the interval as short as possible or the modulus as large as possible.

We study this problem in the function field setting, and prove for a wide class of arithmetic functions (namely factorization functions), that such an asymptotic result holds, allowing the size of the short interval to be as small as a square-root of the size of the full interval, and analogously for arithmetic progressions.

For instance, our results apply for the indicator function of polynomials with a divisor of given degree, and are much stronger than those known for the analogous function over the integers.

As opposed to many previous works, our results apply in the *large-degree limit*, where the base field \mathbb{F}_q is fixed. Our proofs are based on relationships between certain character sums and symmetric functions, and in particular we use results from symmetric function theory due to Egecioglu and Remmel. We also use recent bounds of Bhowmick, Lê and Liu on character sums, which are in the spirit of the Drinfeld–Vlăduț bound.

1 Introduction

An important and challenging class of problems in analytic number theory is showing that the mean value of an arithmetic function in a short interval $[x, x+h] \cap \mathbb{Z}$ is asymptotic to its mean over a long interval. Concretely, this often takes the following form: proving for various $\alpha: \mathbb{N} \rightarrow \mathbb{C}$ that

$$\frac{\sum_{x \leq n \leq x+x^\varepsilon} \alpha(n)}{x^\varepsilon} = \frac{\sum_{n \leq x} \alpha(n)}{x} (1 + o(1)), \quad x \rightarrow \infty \quad (1.1)$$

for $\varepsilon \in (0, 1)$ as small as possible. If the mean value of α tends to 0 and does not have a main term, as happens, for example, for the Möbius function, one should be more careful and instead ask for

$$\frac{\sum_{x \leq n \leq x+x^\varepsilon} \alpha(n)}{x^\varepsilon} = o(1), \quad x \rightarrow \infty \quad (1.2)$$

to hold for $\varepsilon \in (0, 1)$ as small as possible. A related class of problems is showing that the mean value of $\alpha: \mathbb{N} \rightarrow \mathbb{C}$ over integers $1 \leq n \leq x$ which lie in the arithmetic progression $a \bmod q$ ($\gcd(a, q) = 1$) is close to the mean value of α over integers $1 \leq n \leq x$ which are coprime to q . Formally, this often means proving

$$\frac{\sum_{n \leq x, n \equiv a \bmod q} \alpha(n)}{x/\phi(q)} = \frac{\sum_{n \leq x, (n, q)=1} \alpha(n)}{x(\phi(q)/q)} (1 + o(1)), \quad x \rightarrow \infty \quad (1.3)$$

or

$$\frac{\sum_{n \leq x, n \equiv a \bmod q} \alpha(n)}{x/\phi(q)} = o(1), \quad x \rightarrow \infty \quad (1.4)$$

uniformly in $q < x^{1-\varepsilon}$ for $\varepsilon \in (0, 1)$ as small as possible.

Conditionally on the Generalized Riemann Hypothesis (GRH), it is a classical result that in the range $\varepsilon > 1/2$, (1.1) and (1.3) hold for the von Mangoldt function Λ and (1.2) and (1.4) hold for the Möbius function μ . Ramachandra [17] showed that RH implies (1.1) for $\varepsilon > 1/2$ and $\alpha = d_k$, the k th divisor function (k not

necessarily an integer) and some other functions. Kátai [12], building on ideas of Ramachandra, proved that RH also implies (1.1) for $\varepsilon > 1/2$ and α the indicator function of k -almost primes. Some other examples exist [3, 6, 13].

There are close analogues in the function field setting of these results. Because GRH is known in that setting (a theorem due to Weil), they are unconditional. However, both in the number field setting and the function field setting, these results are proven by *ad hoc* arguments, each using GRH in a different way, and in particular the results always require the associated Dirichlet series $\sum \alpha(n)/n^s$ to possess certain structure. In this paper, we prove analogues of (1.1)–(1.4) in the function field setting for $\varepsilon \in (1/2, 1)$ for a wide class of arithmetic functions defined over the polynomial ring $\mathbb{F}_q[T]$, the so-called “factorization functions.” As in previous works, our main tool is GRH for $\mathbb{F}_q(T)$, but we are able to treat all sensible arithmetic functions at once. This leads to interesting applications which are currently out of reach in the number field setting; these are described in §1.3.

1.1 The function field setting

Throughout we fix a prime power q . Let $\mathbb{F}_q[T]$ be the polynomial ring in T over \mathbb{F}_q , $\mathcal{M}_n \subseteq \mathbb{F}_q[T]$ be the subset of monic polynomials of degree n , $\mathcal{P}_n \subseteq \mathcal{M}_n$ be the subset of monic irreducible polynomials of degree n , $\mathcal{M} = \cup_{n \geq 0} \mathcal{M}_n$ be the set of all monic polynomials and $\mathcal{P} = \cup_{n \geq 0} \mathcal{P}_n$ be the set of all monic irreducible polynomials.

To any $f \in \mathcal{M}$ with prime factorization $f = \prod_{i=1}^k P_i^{e_i}$ ($P_i \in \mathcal{P}$ distinct, $e_i \geq 1$), we can associate the following multiset, named the *extended factorization type* of f :

$$\omega_f := \{(\deg(P_i), e_i) : 1 \leq i \leq k\}.$$

(We often omit the word “extended.”) Following Rodgers [19], an arithmetic function $\alpha: \mathcal{M} \rightarrow \mathbb{C}$ is called a *factorization function* if $\alpha(f)$ depends only on ω_f . Some of the most commonly studied arithmetic functions in number theory, when considered in the function field setting, are instances of factorization functions: the von Mangoldt function

$$\Lambda(f) = \begin{cases} \deg(P) & \text{if } f = P^k \text{ for } P \in \mathcal{P} \text{ and } k \geq 1, \\ 0 & \text{otherwise,} \end{cases}$$

the Möbius function

$$\mu(f) = \begin{cases} (-1)^k & \text{if } f = P_1 P_2 \cdots P_k \text{ for distinct } P_i \in \mathcal{P}, \\ 0 & \text{otherwise,} \end{cases}$$

the indicator of squarefrees

$$\mu^2(f) = \begin{cases} 1 & \text{if } f \text{ is squarefree,} \\ 0 & \text{otherwise,} \end{cases}$$

the divisor functions, and many more.

A short interval of size q^{h+1} around $f_0 \in \mathbb{F}_q[T]$ is the subset

$$I(f_0, h) := \{f \in \mathbb{F}_q[T] : \|f - f_0\| \leq q^{h+1}\} = \{f \in \mathbb{F}_q[T] : \deg(f - f_0) \leq h\},$$

where $\|f\| := |\mathbb{F}_q[T]/(f)| = q^{\deg(f)}$ for $f \neq 0$ and $\|0\| := 0$. In addition to short intervals in $\mathbb{F}_q[T]$, we also recall the definition of arithmetic progressions in this setting. Consider a non-zero polynomial $M \in \mathbb{F}_q[T]$ and a polynomial $f_0 \in \mathcal{M}_n$ coprime to M . We define the arithmetic progression of monic polynomials of degree n in the residue class $f_0 \bmod M$ to be

$$\text{AP}(f_0, M) := \{f \in \mathcal{M}_{\deg(f_0)} : f \equiv f_0 \bmod M\},$$

which is a subset of

$$\mathcal{M}_{n;M} := \{f \in \mathcal{M}_n : \gcd(f, M) = 1\}.$$

If $n \geq \deg(M)$, then $|\mathcal{M}_{n;M}| = q^{n-\deg(M)} \phi(M)$, where $\phi(M)$ is Euler’s totient function.

1.2 Main results

For a given arithmetic function $\alpha: \mathcal{M} \rightarrow \mathbb{C}$, let $\langle \alpha \rangle_S$ be the mean value of α over a non-empty finite subset $S \subseteq \mathcal{M}$:

$$\langle \alpha \rangle_S := \frac{1}{|S|} \sum_{f \in S} \alpha(f).$$

We prove the following analogue of (1.1) and (1.2).

Theorem 1.1. *Let $\alpha: \mathcal{M} \rightarrow \mathbb{C}$ be a factorization function. Let $0 \leq h \leq n-1$ and $f_0 \in \mathcal{M}_n$. Then*

$$|\langle \alpha \rangle_{I(f_0, h)} - \langle \alpha \rangle_{\mathcal{M}_n}| \leq \max_{f \in \mathcal{M}_n} |\alpha(f)| q^{\frac{n}{2} - h - 1} e^{O_q(\frac{n \log \log(n+2)}{\log(n+2)})}.$$

The analogous result for arithmetic progressions is the following.

Theorem 1.2. *Let $\alpha: \mathcal{M} \rightarrow \mathbb{C}$ be a factorization function. Let $M \in \mathbb{F}_q[T]$ be a non-zero polynomial and let $f_0 \in \mathcal{M}_n$ be a polynomial coprime to M . Then whenever $n \geq \deg(M)$,*

$$|\langle \alpha \rangle_{\text{AP}(f_0, M)} - \langle \alpha \rangle_{\mathcal{M}_{n;M}}| \leq \max_{f \in \mathcal{M}_{n;M}} |\alpha(f)| q^{\deg(M) - \frac{n}{2}} e^{O_q(\frac{n \log \log(n+2)}{\log(n+2)})}.$$

As long as $\max_{f \in \mathcal{M}_n} |\alpha(f)|$ grows subexponentially in n , Theorems 1.1 and 1.2 give a non-trivial result in the range $\limsup_{n \rightarrow \infty} \frac{h+1}{n} > 1/2$ and $\limsup_{n \rightarrow \infty} (1 - \frac{\deg(M)}{n}) > 1/2$, respectively. These limsups are the function field analogue of the quantity ε discussed before.

We also prove the following results on the variance of the sums $\sum_{f \in I(f_0, h)} \alpha(f)$ and $\sum_{f \in \text{AP}(f_0, M)} \alpha(f)$ as f_0 varies. First, we define the short-interval variance

$$\text{Var}(\alpha; n, h) := \frac{1}{|\mathcal{M}_n|} \sum_{f_0 \in \mathcal{M}_n} \left| \sum_{f \in I(f_0, h)} \alpha(f) - q^{h+1} \langle \alpha \rangle_{\mathcal{M}_n} \right|^2,$$

and the arithmetic progression variance

$$\text{Var}_M(\alpha; n) := \frac{1}{|\mathcal{M}_{n;M}|} \sum_{f_0 \in \mathcal{M}_{n;M}} \left| \sum_{f \in \text{AP}(f_0, M)} \alpha(f) - q^{n - \deg(M)} \langle \alpha \rangle_{\mathcal{M}_{n;M}} \right|^2.$$

Theorem 1.3. *Let $\alpha: \mathcal{M} \rightarrow \mathbb{C}$ be a factorization function. For any $0 \leq h \leq n-1$, we have*

$$\text{Var}(\alpha; n, h) \leq \max_{f \in \mathcal{M}_n} |\alpha(f)|^2 q^{h+1} e^{O_q(\frac{n \log \log(n+2)}{\log(n+2)})}. \quad (1.5)$$

For any non-zero polynomial M with $\deg(M) \leq n$, we have

$$\text{Var}_M(\alpha; n) \leq \max_{f \in \mathcal{M}_{n;M}} |\alpha(f)|^2 \frac{q^n}{\phi(M)} e^{O_q(\frac{n \log \log(n+2)}{\log(n+2)})}. \quad (1.6)$$

The trivial bound for $\text{Var}(\alpha; n, h)$ is $q^{2(h+1)} \max_{f \in \mathcal{M}_n} |\alpha(f)|^2$, and we beat it as long as $\limsup_{n \rightarrow \infty} \frac{h+1}{n}$ is positive, which corresponds to $\varepsilon > 0$ in the number field setting. Similarly, (1.6) beats the trivial bound as long as $\limsup_{n \rightarrow \infty} (1 - \frac{\deg(M)}{n}) > 0$.

1.3 Applications

Let $H(x, y, 2y)$ be number of positive integers up to x which have a divisor in $(y, 2y]$. Ford [7, 8] showed that

$$H(x, y, 2y) \asymp \frac{x}{(\log y)^\delta (\log \log y)^{3/2}}, \quad 3 \leq y \leq \sqrt{x},$$

where $\delta = 1 - \frac{1+\log\log 2}{\log 2}$. Here $A \asymp B$ means $cB \leq A \leq CB$ for absolute positive constants c and C . Ford has a short interval version of this result [7, Theorem 2]:

$$H(x, y, 2y) - H(x - \Delta, y, 2y) \asymp \frac{\Delta}{x} H(x, y, 2y), \quad y_0 \leq y \leq \sqrt{x}, \quad \frac{x}{\log^{10} x} \leq \Delta \leq x, \quad (1.7)$$

where y_0 is a sufficiently large real number. Let $H_q(n, d)$ be the function field analogue of $H(x, y, 2y)$, counting monic polynomials of degree n which have a divisor of degree d . Meisner [16, Theorem 1.2] has recently shown that

$$H_q(n, d) \asymp \frac{q^n}{d^\delta (1 + \log d)^{3/2}}, \quad 1 \leq d \leq \frac{n}{2}.$$

Applying Theorem 1.1 with

$$\alpha_d: \mathcal{M} \rightarrow \mathbb{C}, \quad \alpha_d(f) = \begin{cases} 1 & \text{if } f \text{ has a divisor of degree } d, \\ 0 & \text{otherwise,} \end{cases}$$

we obtain the following

Corollary 1.4. *For any $n \geq 1$, let $f_0 \in \mathcal{M}_n$ and $1 \leq d \leq n$. As $n \rightarrow \infty$, we have*

$$\sum_{\substack{f \in I(f_0, h) \\ f \text{ has a divisor of degree } d}} 1 \sim q^{h+1} \frac{H_q(n, d)}{q^n}$$

uniformly in d , as long as $\limsup_{n \rightarrow \infty} \frac{h}{n} > 1/2$.

Not only is this corollary valid in a much wider range than (1.7), it is an *asymptotic result* and not an estimate. In the integer setting, RH might help in improving the range where (1.7) holds, but it is not clear how to use it to establish an asymptotic formula. We raise the following

Question. Assume RH. Do we have

$$H(x, y, 2y) - H(x - \Delta, y, 2y) = \frac{\Delta}{x} H(x, y, 2y) (1 + o(1)), \quad y_0 \leq y \leq \sqrt{x}, \quad \frac{x}{\log^{10} x} \leq \Delta \leq x,$$

as x tends to infinity?

Our second example is Hooley's Delta function. In his study of Waring's problem, diophantine approximation and other problems [11], Hooley introduced the function

$$\Delta(n) := \max_{u > 0} \sum_{d|n, d \in (u, eu]} 1,$$

and obtained upper and lower bounds on its mean value. Hall and Tenenbaum [9] showed that

$$\frac{1}{x} \sum_{n \leq x} \Delta(n) = O(\log^{A_0} x \sqrt{\log \log x})$$

for an explicit (optimal) constant A_0 , and

$$\frac{1}{x} \sum_{n \leq x} \Delta(n) = \Omega(\log \log x).$$

As far as the author knows, Δ was not studied in short intervals or in arithmetic progressions. The function field analogue of Δ is

$$\Delta_q: \mathcal{M} \rightarrow \mathbb{C}, \quad \Delta_q(f) := \max_{0 \leq i \leq \deg(f)} \sum_{d|f, \deg(d)=i} 1.$$

Let $d_2(f)$ be the usual divisor function, which satisfies $\langle d_2 \rangle_{\mathcal{M}_n} = n + 1$ [20, Proposition 2.5]. It is evident that $\max_{f \in \mathcal{M}_n} \Delta_q(f) \leq \max_{f \in \mathcal{M}_n} d_2(f)$, which is known to grow slower than any power of q^n as n tends to infinity. Also, $\langle \Delta_q \rangle_{\mathcal{M}_n}, \langle \Delta_q \rangle_{\mathcal{M}_{n;M}} \geq 1$, since $\Delta_q \geq 1$. Applying Theorems 1.1 and 1.2 with $\alpha = \Delta_q$, we obtain the following

Corollary 1.5. *For any $n \geq 1$, let $f_0 \in \mathcal{M}_n$. As $n \rightarrow \infty$, we have*

$$\langle \Delta_q \rangle_{I(f_0, h)} \sim \langle \Delta_q \rangle_{\mathcal{M}_n}$$

as long as $\limsup_{n \rightarrow \infty} \frac{h}{n} > 1/2$, and

$$\langle \Delta_q \rangle_{\text{AP}(f_0, M)} \sim \langle \Delta_q \rangle_{\mathcal{M}_{n;M}}$$

as long as $\limsup_{n \rightarrow \infty} \frac{\deg(M)}{n} < 1/2$.

1.4 Previous works

1.4.1 Mean values

In the large- q limit, where the degree n is fixed and the size of the base field \mathbb{F}_q tends to infinity, see Bank *et al.* [1] for a general result on mean values, where completely different methods are employed and do not give a result for growing n .

For some specific functions, one can go beyond some of our mean-value results, see the works of Sawin [21] and Sawin and Shusterman [22].

1.4.2 Variance

In the large- q limit, see Rodgers [19] for a general result on the variance of arithmetic functions. Again, the methods are different than ours and do not allow one to vary n and fix q .

For some specific functions, the work of Ramachandra in the integer setting [17] gives non-trivial mean-value results and variance results, which, although conditional on RH, are much weaker in comparison to ours. For instance, in [17, Equation (11)], an upper bound of the form $O(H^2 X^{-o(1)})$ is obtained for the variance of μ in short intervals (and some other functions), while our upper bound should be compared with $O(HX^{o(1)})$, which is better whenever $X^\varepsilon < H < X^{1-\varepsilon}$. Recently, Matomäki and Radziwiłł [15] proved unconditionally that

$$\frac{1}{X} \int_X^{2X} \left(\sum_{n \in [x, x+H]} \mu(n) \right)^2 dx = o(H^2)$$

which goes beyond Ramachandra's result for μ if H is very small. The methods of [15] apply in general to bounded multiplicative functions, and so they cannot handle e.g. divisor functions or the von Mangoldt function. Our upper bound is qualitatively better in the range $X^\varepsilon < H < X^{1-\varepsilon}$.

2 Results on character sums

Theorems 1.1–1.3 rest on the character sums estimate given in Theorem 2.1 below. The theorem involves Hayes characters, which are a function field analogue of Dirichlet characters defined in §3. Informally, a function $\chi: \mathcal{M} \rightarrow \mathbb{C}$ is called a Hayes character modulo $R_{\ell, M}$ (ℓ a non-negative integer, M a non-zero polynomial) if the following conditions hold: (1) $\chi(fg) = \chi(f)\chi(g)$ for every $f, g \in \mathcal{M}_q$, (2) $\chi(f)$ depends only on the residue of f modulo M and on the first ℓ next-to-leading coefficients of f and (3) $\chi(f) = 0$ if and only if $\gcd(f, M) \neq 1$. Such a χ is called *trivial* if it only assumes the values 0 and 1. For instance, the notion of a Dirichlet character modulo M coincides with that of a Hayes character modulo $R_{0, M}$.

Theorem 2.1. *Let $\alpha: \mathcal{M} \rightarrow \mathbb{C}$ be a factorization function, and let χ be a non-trivial Hayes character modulo $R_{\ell, M}$. We have*

$$\left| \sum_{f \in \mathcal{M}_n} \alpha(f) \chi(f) \right| \leq 7 \max_{f \in \mathcal{M}_{n;M}} |\alpha(f)| q^{\frac{n}{2}} \binom{20(\ell + \deg(M) + 1) + n - 1}{n}. \quad (2.1)$$

If $\ell + \deg(M) = O(n)$, then

$$\left| \sum_{f \in \mathcal{M}_n} \alpha(f) \chi(f) \right| \leq \max_{f \in \mathcal{M}_{n;M}} |\alpha(f)| q^{\frac{n}{2}} e^{O_q\left(\frac{n \log \log(n+2)}{\log(n+2)}\right)}. \quad (2.2)$$

Remark 1. If $\ell + \deg(M)$ is small compared to n , say $\ell + \deg(M) = o(n/\ln n)$, then (2.1) is superior to (2.2). For $\ell + \deg(M)$ which is proportional to n , (2.2) is better than (2.1).

We manage to prove such a theorem, which works for any α , by reducing it to estimating a single character sum, which we now describe.

Let Ω be the set of finite multisets of elements from $\mathbb{N} \times \mathbb{N}$, so that ω_f , the factorization type of a polynomial f , is an element of Ω . For an element $\omega = \{(d_i, e_i) : 1 \leq i \leq k\} \in \Omega$, we define its size to be $|\omega| := \sum_{i=1}^k d_i e_i$ and its length to be $\ell(\omega) := k$. For a factorization function α and a factorization type $\omega \in \Omega$, we denote by $\alpha(\omega)$ the value of α on a polynomial f with $\omega_f = \omega$ if such a polynomial exists, and otherwise set $\alpha(\omega) = 0$. We have, by the triangle inequality,

$$\left| \sum_{f \in \mathcal{M}_n} \alpha(f) \chi(f) \right| = \left| \sum_{\substack{\omega \in \Omega \\ |\omega| = n}} \alpha(\omega) \sum_{\substack{f \in \mathcal{M}_n \\ \omega_f = \omega}} \chi(f) \right| \leq \max_{f \in \mathcal{M}_{n;M}} |\alpha(f)| \sum_{\substack{\omega \in \Omega \\ |\omega| = n}} \left| \sum_{\substack{f \in \mathcal{M}_n \\ \omega_f = \omega}} \chi(f) \right|. \quad (2.3)$$

Thus, it suffices to bound the sum on the right-hand side of (2.3). In order to bound the character sums

$$\sum_{f \in \mathcal{M}_n : \omega_f = \omega} \chi(f),$$

we relate them to products of *monomial symmetric polynomials* evaluated at $\chi(P)$ where P runs over irreducible polynomials of certain degrees, see Lemmas 5.1 and 5.2. We use tools from symmetric function theory in order to be able to use RH efficiently in bounding these evaluations of symmetric polynomials.

Apart from symmetric function theory and RH, we use an additional idea, which first appeared in [2]. Namely, we use the trivial bound in place of RH in some cases, as the trivial bound is superior when the degrees considered are small. This is in the spirit of the Drinfeld–Vlăduț bound, where one bounds the number of points on curves over \mathbb{F}_q when q is fixed and the genus varies.

3 Hayes characters

Here we review the function field analogue of Dirichlet characters, first introduced by Hayes in the paper [10] which is based on his thesis. We call these characters “Hayes characters,” or sometimes “generalized arithmetic progression characters.” Unless otherwise stated, the proofs of the statements in this section appear in Hayes’ original paper. The main difference between Hayes characters and Dirichlet characters is that in the function field setting we can also consider characters modulo the prime at infinity.

3.1 Equivalence relation

Let ℓ be a non-negative integer and M be a non-zero polynomial in $\mathbb{F}_q[T]$. We define an equivalence relation $R_{\ell, M}$ on \mathcal{M} by saying that $A \equiv B \pmod{R_{\ell, M}}$ if and only if A and B have the same first ℓ next-to-leading coefficients and $A \equiv B \pmod{M}$. We adopt throughout the following convention: the j th next-to-leading coefficient of a polynomial $f(T) \in \mathcal{M}$ with $j > \deg(f)$ is considered to be 0. It may be shown that there is a well-defined quotient monoid $\mathcal{M}/R_{\ell, M}$, where multiplication is the usual polynomial multiplication. An element of \mathcal{M} is invertible modulo $R_{\ell, M}$ if and only if it is coprime to M . The units of $\mathcal{M}/R_{\ell, M}$ form an abelian group, having as identity element the equivalence class of the polynomial 1. We denote this unit group by $(\mathcal{M}/R_{\ell, M})^\times$. It may be shown that

$$\left| (\mathcal{M}/R_{\ell, M})^\times \right| = q^\ell \phi(M).$$

3.1.1 Characters

For every character χ of the finite abelian group $(\mathcal{M}/R_{\ell, M})^\times$, we define χ^\dagger with domain \mathcal{M} as follows. If A is invertible modulo $R_{\ell, M}$ and if \mathfrak{c} is the equivalence class of A , then $\chi^\dagger(A) = \chi(\mathfrak{c})$. If A is not invertible, then $\chi^\dagger(A) = 0$.

The set of functions χ^\dagger defined in this way are called the characters of the relation $R_{\ell,M}$, or sometimes “characters modulo $R_{\ell,M}$ ”. We shall abuse language somewhat and write χ instead of χ^\dagger to indicate a character of the relation $R_{\ell,M}$ derived from the character χ of the group $(\mathcal{M}/R_{\ell,M})^\times$. Thus we write χ_0 for the character of $R_{\ell,M}$ which has the value 1 when A is invertible and the value 0 otherwise. We denote by $G(R_{\ell,M})$ the set $\{\chi^\dagger : \chi \in (\widehat{\mathcal{M}/R_{\ell,M}})^\times\}$.

A set of polynomials in \mathcal{M} is called a representative set modulo $R_{\ell,M}$ if the set contains one and only one polynomial from each equivalence class of $R_{\ell,M}$. If $\chi_1, \chi_2 \in G(R_{\ell,M})$, then

$$\frac{1}{q^\ell \phi(M)} \sum_F \chi_1(F) \overline{\chi_2(F)} = \begin{cases} 0 & \text{if } \chi_1 \neq \chi_2, \\ 1 & \text{if } \chi_1 = \chi_2, \end{cases} \quad (3.1)$$

F running through a representative set modulo $R_{\ell,M}$. If $n \geq \ell + \deg(M)$, then \mathcal{M}_n is a disjoint union of $q^{n-\ell-\deg(M)}$ representative sets, and a set of polynomials on which $\chi \in G(R_{\ell,M})$ vanishes. Thus, applying (3.1) with $\chi_2 = \chi_0$, we obtain that for all $n \geq \ell + \deg(M)$,

$$\frac{1}{q^{n-\deg(M)} \phi(M)} \sum_{F \in \mathcal{M}_n} \chi(F) = \begin{cases} 0 & \text{if } \chi \neq \chi_0, \\ 1 & \text{if } \chi = \chi_0. \end{cases} \quad (3.2)$$

We also have, for all $A, B \in \mathcal{M}$ coprime to M ,

$$\frac{1}{q^\ell \phi(M)} \sum_{\chi \in G(R_{\ell,M})} \chi(A) \overline{\chi(B)} = \begin{cases} 1 & \text{if } A \equiv B \pmod{R_{\ell,M}}, \\ 0 & \text{otherwise.} \end{cases} \quad (3.3)$$

We also call the elements of $G(R_{\ell,M})$ “generalized arithmetic progression characters,” because for any $A \in \mathcal{M}_n$, $\chi \in G(R_{\ell,M})$ is constant on the set

$$\{f \in \mathcal{M}_n : f \equiv A \pmod{R_{\ell,M}}\} = \{f \in \mathbb{F}_q[T] : f \equiv A \pmod{M}\} \cap \{f \in \mathcal{M}_n : \deg(f - A) \leq n - \ell - 1\}$$

which is an intersection of an arithmetic progression and a short interval. We set, for future use,

$$\text{GAP}(A; \ell, M) := \{f \in \mathcal{M}_{\deg(A)} : f \equiv A \pmod{R_{\ell,M}}\}.$$

If $\chi \in G(R_{\ell,1})$, we say that χ is a short interval character of ℓ coefficients, and if $\chi \in G(R_{0,M})$, we say that χ is a Dirichlet character modulo M . Every element of $G(R_{\ell,M})$ is a product of an element from $G(R_{\ell,1})$ with an element from $G(R_{0,M})$.

3.1.2 L -Functions

Let $\chi \in G(R_{\ell,M})$. The L -function of χ is the following series in u :

$$L(u, \chi) = \sum_{f \in \mathcal{M}} \chi(f) u^{\deg(f)},$$

which also admits the Euler product

$$L(u, \chi) = \prod_{P \in \mathcal{P}} (1 - \chi(P) u^{\deg(P)})^{-1}. \quad (3.4)$$

If χ is the trivial character χ_0 of $G(R_{\ell,M})$, then

$$L(u, \chi) = \frac{\prod_{P|M} (1 - u^{\deg(P)})}{1 - qu}.$$

Otherwise, the orthogonality relation (3.2) implies that $L(u, \chi)$ is a polynomial in u of degree at most

$$\deg L(u, \chi) \leq \ell + \deg(M) - 1. \quad (3.5)$$

The first one to realize that Weil's proof of the Riemann Hypothesis for Function Fields [24, Theorem 6, p. 134] implies the Riemann Hypothesis for the L -functions of $\chi \in G(R_{\ell,M})$ was Rhin [18, Chapitre 2] in his thesis (cf. [4, Theorem 5.6] and the discussion following it). Hence we know that if we factor $L(u, \chi)$ as

$$L(u, \chi) = \prod_{i=1}^{\deg L(u, \chi)} (1 - \gamma_i(\chi)u), \quad (3.6)$$

then for any i ,

$$|\gamma_i(\chi)| \in \{1, \sqrt{q}\}. \quad (3.7)$$

The following consequence of (3.7) is a basic ingredient in our proofs.

Lemma 3.1. *Let M be a non-zero polynomial in $\mathbb{F}_q[T]$ and ℓ a non-negative integer. Let $\chi \in G(R_{\ell,M})$ and $n \geq 1$. Then*

$$\left| \sum_{P \in \mathcal{P}_n} \chi(P) \right| \leq \begin{cases} \min\{\frac{q^{\frac{n}{2}}}{n}(\ell + \deg(M) + 1), \frac{q^n}{n}\} & \text{if } \chi \neq \chi_0, \\ \frac{q^n}{n} & \text{otherwise.} \end{cases}$$

Proof. The bound $|\sum_{P \in \mathcal{P}_n} \chi(P)| \leq q^n/n$ follows from the bound $|\mathcal{P}_n| \leq q^n/n$ [20, Proposition 2.1]. For $\chi \neq \chi_0$, we obtain the additional bound as follows. We equate (3.4) with (3.6) and take logarithmic derivatives to obtain

$$\left| \sum_{f \in \mathcal{M}_n} \Lambda(f) \chi(f) \right| = \left| \sum_{i=1}^{\deg L(u, \chi)} \gamma_i(\chi)^n \right| \leq (\ell + \deg(M) - 1) q^{\frac{n}{2}}, \quad (3.8)$$

where the last passage used (3.5) and (3.7). We can split (3.8) into the contribution of primes of degree n and proper prime powers:

$$\left| n \sum_{f \in \mathcal{P}_n} \chi(f) + \sum_{d|n, d \neq 1} \frac{n}{d} \sum_{f \in \mathcal{P}_{\frac{n}{d}}} \chi^d(f) \right| \leq (\ell + \deg(M) - 1) q^{\frac{n}{2}}. \quad (3.9)$$

As

$$\left| \sum_{d|n, d \neq 1} \frac{n}{d} \sum_{f \in \mathcal{P}_{\frac{n}{d}}} \chi^d(f) \right| \leq \sum_{d|n, d \neq 1} \frac{n}{d} |\mathcal{P}_{n/d}| \leq \sum_{d|n, d \neq 1} q^{n/d} \leq 2q^{\frac{n}{2}},$$

we obtain from (3.9) and the triangle inequality that

$$\left| n \sum_{f \in \mathcal{P}_n} \chi(f) \right| \leq (\ell + \deg(M) + 1) q^{\frac{n}{2}}.$$

After dividing by n , the lemma is established. \square

3.2 Sums over generalized arithmetic progressions and their variance

For an arithmetic function $\alpha: \mathcal{M} \rightarrow \mathbb{C}$ and $n \geq 1$, define

$$S(n, \alpha) := \sum_{f \in \mathcal{M}_n} \alpha(f). \quad (3.10)$$

The following lemma expresses sums over generalized arithmetic progressions, and the variance of such sums, as sums over characters in $G(R_{\ell,M})$. Special cases of this lemma appeared in a paper of Keating and Rudnick [14].

Lemma 3.2. *Let ℓ be a non-negative integer and $M \in \mathbb{F}_q[T]$ be a non-zero polynomial. Let $n \geq \ell + \deg(M)$. Let $A \in (\mathcal{M}/R_{\ell,M})^\times$ and define $f_A \in \mathcal{M}$ to be some polynomial of degree n in the equivalence class of A modulo $R_{\ell,M}$. Then the following hold.*

1. We have, for all $g \in \mathcal{M}_{n;M}$,

$$\mathbf{1}_{g \in \text{GAP}(f_A; \ell, M)} = \frac{\sum_{\chi \in G(R_{\ell, M})} \bar{\chi}(A) \chi(g)}{\phi(M) q^\ell}.$$

2. For any arithmetic function $\alpha: \mathcal{M} \rightarrow \mathbb{C}$, we have

$$\begin{aligned} \sum_{g \in \text{GAP}(f_A; \ell, M)} \alpha(g) &= \frac{\sum_{\chi \in G(R_{\ell, M})} \bar{\chi}(A) S(n, \alpha \cdot \chi)}{\phi(M) q^\ell} \\ &= q^{n-\ell-\deg(M)} \langle \alpha \rangle_{\mathcal{M}_{n;M}} + \frac{\sum_{\chi_0 \neq \chi \in G(R_{\ell, M})} \bar{\chi}(A) S(n, \alpha \cdot \chi)}{q^\ell \phi(M)}. \end{aligned} \quad (3.11)$$

3. For any arithmetic function $\alpha: \mathcal{M} \rightarrow \mathbb{C}$, the variance of $\{\sum_{g \in \text{GAP}(f; n, \ell; M)} \alpha(g)\}_{f \in \mathcal{M}_{n;M}}$, defined as

$$\text{Var}_M(\alpha; n, n - \ell - 1) := \frac{1}{q^{n-\deg(M)} \phi(M)} \sum_{f \in \mathcal{M}_{n;M}} \left| \sum_{g \in \text{GAP}(f; \ell, M)} \alpha(g) - q^{n-\ell-\deg(M)} \langle \alpha \rangle_{\mathcal{M}_{n;M}} \right|^2,$$

may be expressed as

$$\text{Var}_M(\alpha; n, n - \ell - 1) = \frac{\sum_{\chi_0 \neq \chi \in G(R_{\ell, M})} |S(n, \alpha \cdot \chi)|^2}{q^{2\ell} \phi^2(M)}. \quad (3.12)$$

Proof. The first part of the lemma is a restatement of the orthogonality relation (3.3). For the second part of the lemma, we observe that $\sum_{g \in \text{GAP}(f_A; \ell, M)} \alpha(g) = \sum_{g \in \mathcal{M}_{n;M}} \alpha(g) \cdot \mathbf{1}_{g \in \text{GAP}(f_A; \ell, M)}$, and now we apply the first part of the lemma and interchange the order of summation. Note that

$$\frac{S(n, \alpha \cdot \chi_0)}{\phi(M) q^\ell} = q^{n-\ell-\deg(M)} \langle \alpha \rangle_{\mathcal{M}_{n;M}}. \quad (3.13)$$

To prove the last part of the lemma, we use (3.13) and (3.11) as follows:

$$\begin{aligned} \text{Var}_M(\alpha; n, n - \ell - 1) &= \frac{1}{q^\ell \phi(M)} \sum_{(A \in \mathcal{M}/R_{\ell, M})^\times} \left| \sum_{g \in \text{GAP}(f_A; \ell, M)} \alpha(g) - \frac{S(n, \alpha \cdot \chi_0)}{\phi(M) q^\ell} \right|^2 \\ &= \frac{1}{q^\ell \phi(M)} \sum_{(A \in \mathcal{M}/R_{\ell, M})^\times} \left| \frac{\sum_{\chi_0 \neq \chi \in G(R_{\ell, M})} \bar{\chi}(A) S(n, \alpha \cdot \chi)}{\phi(M) q^\ell} \right|^2 \\ &= \frac{1}{q^{3\ell} \phi^3(M)} \sum_{(A \in \mathcal{M}/R_{\ell, M})^\times} \sum_{\chi_1, \chi_2 \in G(R_{\ell, M}) \setminus \{\chi_0\}} \bar{\chi}_1(A) S(n, \alpha \cdot \chi_1) \chi_2(A) \overline{S(n, \alpha \cdot \chi_2)}. \end{aligned}$$

Interchanging the order of summation and applying (3.1), we conclude the proof. \square

4 Proofs of Theorems 1.1, 1.2 and 1.3

Here we prove the main results of the paper using Lemma 3.2 and Theorem 2.1. By (3.11) with $M = 1$ and $\ell = n - h - 1$, we obtain that

$$|\langle f \rangle_{I(f_0, h)} - \langle f \rangle_{\mathcal{M}_n}| \leq \frac{\sum_{\chi_0 \neq \chi \in G(R_{n-h-1, 1})} |S(n, \alpha \cdot \chi)|}{q^n}.$$

Plugging (2.2) in the sum above, we conclude the proof of Theorem 1.1. By (3.11) with $\ell = 0$, we obtain that

$$|\langle f \rangle_{\text{AP}(f_0, M)} - \langle f \rangle_{\mathcal{M}_{n;M}}| \leq \frac{\sum_{\chi_0 \neq \chi \in G(R_{0, M})} |S(n, \alpha \cdot \chi)|}{q^{n-\deg(M)} \phi(M)}.$$

Plugging (2.2) in the last sum, we conclude the proof of Theorem 1.2. By (3.12) with $M = 1$ and $\ell = n - h - 1$, we obtain that

$$\text{Var}(\alpha; n, h) = \frac{\sum_{\chi_0 \neq \chi \in G(R_{n-h-1,1})} |S(n, \alpha \cdot \chi)|^2}{q^{2(n-h-1)}}.$$

Plugging (2.2) in the sum above, (1.5) is established, and (1.6) is proved similarly, by applying (3.12) with $\ell = 0$. This concludes the proof of Theorem 1.3.

5 Preparation for proof of Theorem 2.1

Here and in subsequent sections, we shall use the notation $[u^n]f(u)$ for the coefficient of u^n in a power series f . We also write $\exp(\bullet)$ for e^\bullet .

5.1 Multiplicativity of character sums

Given $d \geq 1$ and a factorization type

$$\omega = \{(d_i, e_i) : 1 \leq i \leq k\} \in \Omega,$$

we denote by $\omega(d) \subseteq \omega$ the factorization type $\{(d_i, e_i) : 1 \leq i \leq k, d_i = d\}$. By definition, ω is the disjoint union of the $\omega(d)$ -s. Let $\mathbf{1}_\omega$ be the indicator function of polynomials f with $\omega_f = \omega$. The following lemma shows that the character sums $S(n, \chi \cdot \mathbf{1}_\omega)$ (recall (3.10)) enjoy a multiplicative property.

Lemma 5.1. *Let $\omega \in \Omega$ with $|\omega| = n$. Let χ be a Hayes character. Then*

$$S(n, \chi \cdot \mathbf{1}_\omega) = \prod_{d=1}^n S(|\omega(d)|, \chi \cdot \mathbf{1}_{\omega(d)}). \quad (5.1)$$

Proof. Each f with $\omega_f = \omega$ can be written uniquely as $f = \prod_{d=1}^n f_d$ where f_d is divisible only by primes of degree d . We then have $\omega_{f_d} = \omega(d)$, and the lemma follows by expanding the right-hand side of (5.1). \square

5.2 Symmetric function theory

A partition of size n is a finite (possibly empty) non-increasing sequence of positive integers that sum to n . The length of a partition $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$ is the number of its elements and is denoted by $\ell(\lambda) := k$. We write $\lambda \vdash n$ to indicate that λ sums to n . The empty partition is of size and length 0. We denote by \mathbb{Y} the set of all partitions.

An important class of symmetric polynomials is the *monomial symmetric polynomials*. Given a partition $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$ and variables X_1, \dots, X_k , the monomial symmetric polynomial $m_\lambda(X_1, \dots, X_k)$ is the symmetric polynomial

$$m_\lambda(X_1, \dots, X_k) := \sum_{\exists \pi \in S_k : (\lambda'_1, \dots, \lambda'_k) = (\lambda_{\pi(1)}, \dots, \lambda_{\pi(k)})} \prod_{i=1}^k X_i^{\lambda'_i} \in \mathbb{Z}[X_1, \dots, X_k],$$

where the sum is over the *distinct* permutations of λ . It is useful to extend m_λ to the case of a general number of variables X_1, \dots, X_n . If $n < k$, we define $m_\lambda(X_i : 1 \leq i \leq n)$ to be zero. If $n > k$, we set $\lambda_j = 0$ for $j = k + 1, \dots, n$ and define

$$m_\lambda(X_i : 1 \leq i \leq n) := \sum_{\exists \pi \in S_n : (\lambda'_1, \dots, \lambda'_n) = (\lambda_{\pi(1)}, \dots, \lambda_{\pi(n)})} \prod_{i=1}^n X_i^{\lambda'_i} \in \mathbb{Z}[X_1, \dots, X_n],$$

where the sum is over the *distinct* permutations of λ followed by $n - k$ zeros. In particular, m_λ is the elementary symmetric polynomial e_k if $\lambda = (1, 1, \dots, 1)$ with k ones.

The following lemma expresses character sums, of the form appearing in the right-hand side of (5.1), as an evaluation of a monomial symmetric polynomial.

Lemma 5.2. Let $\omega = \{(d, e_i) : 1 \leq i \leq k\} \in \Omega$. Let $\lambda \in \mathbb{Y}$ be the partition whose parts are $\{e_i\}_{i=1}^k$ in non-increasing order. Let χ be a Hayes character. We have

$$S(|\omega|, \chi \cdot \mathbf{1}_\omega) = m_\lambda(\chi(P) : P \in \mathcal{P}_d).$$

Proof. A polynomial f with $\omega_f = \omega$ is necessarily given by a product $\prod_{i=1}^k P_i^{e_i}$ where P_i are distinct elements from \mathcal{P}_d . Equivalently, f may be expressed as $\prod_{P \in \mathcal{P}_d} P^{e(P)}$ where the multiset $\{e(P) : P \in \mathcal{P}_d\}$ is equal to

$$E := \{e_i : 1 \leq i \leq k\} \cup \{0 : 1 \leq i \leq |\mathcal{P}_d| - k\}.$$

Moreover, by unique factorization, this form is unique. Thus,

$$\begin{aligned} S(|\omega|, \chi \cdot \mathbf{1}_\omega) &= \sum_{f \in \mathcal{M}_{|\omega|} : \omega_f = \omega} \chi(f) = \sum_{\substack{e : \mathcal{P}_d \rightarrow \mathbb{N}_{\geq 0} \\ \{e(P) : P \in \mathcal{P}_d\} = E}} \chi \left(\prod_{P \in \mathcal{P}_d} P^{e(P)} \right) \\ &= \sum_{\substack{e : \mathcal{P}_d \rightarrow \mathbb{N}_{\geq 0} \\ \{e(P) : P \in \mathcal{P}_d\} = E}} \prod_{P \in \mathcal{P}_d} (\chi(P))^{e(P)}, \end{aligned}$$

which is just m_λ evaluated at $\{\chi(P) : P \in \mathcal{P}_d\}$, as needed. \square

Another class of symmetric polynomials is the *power sum symmetric polynomials*. Given a positive integer r , the power sum symmetric polynomial $p_r(X_i : 1 \leq i \leq n)$ is the symmetric polynomial

$$p_r(X_i : 1 \leq i \leq n) := \sum_{i=1}^n X_i^r \in \mathbb{Z}[X_1, \dots, X_n].$$

More generally, given a partition $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$, then the power sum symmetric polynomial $p_\lambda(X_i : 1 \leq i \leq n)$ is the symmetric polynomial

$$p_\lambda(X_i : 1 \leq i \leq n) := \prod_{i=1}^k p_{\lambda_i}(X_i : 1 \leq i \leq n).$$

A basic result in symmetric function theory says that whenever $m \geq n$, $\{m_\lambda(X_i : 1 \leq i \leq m)\}_{\lambda \vdash n}$ and $\{p_\lambda(X_i : 1 \leq i \leq m)\}_{\lambda \vdash n}$ are both bases for homogeneous symmetric polynomials of degree n with rational coefficients. In particular, $m_\lambda(X_i : 1 \leq i \leq m)$ can be expressed uniquely as a linear combination of the symmetric polynomials p_μ for partitions μ of size n , that is, there are unique coefficients $c_{\lambda, \mu} \in \mathbb{Q}$ such that

$$m_\lambda(X_i : 1 \leq i \leq m) = \sum_{\mu \vdash n} c_{\lambda, \mu} p_\mu(X_i : 1 \leq i \leq m) \quad (5.2)$$

for all $m \geq n$ ($c_{\lambda, \mu}$ are independent of m). Egecioglu and Remmel [5, pp. 107–111] gave a combinatorial interpretation of $c_{\lambda, \mu}$ which we now describe. We begin with their definition of λ -brick tabloids.

Let $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$ and $\mu = (\mu_1, \mu_2, \dots, \mu_r)$ be two partitions. Recall that the *Young diagram* Y_μ is the diagram which consists of left justified rows of squares of lengths $\mu_1, \mu_2, \dots, \mu_r$ reading from top to bottom. For instance, if $\mu = (4, 3)$ then Y_μ is given by

$$Y_\mu = \begin{array}{|c|c|c|c|} \hline & & & \\ \hline & & & \\ \hline & & & \\ \hline & & & \\ \hline \end{array}.$$

A λ -brick tabloid T of shape μ is a filling of Y_μ with bricks b_1, \dots, b_k of lengths $\lambda_1, \dots, \lambda_k$, respectively, such that

1. each brick b_i covers exactly λ_i squares of Y_μ all of which lie in a single row of Y_μ ,
2. no two brick overlap.

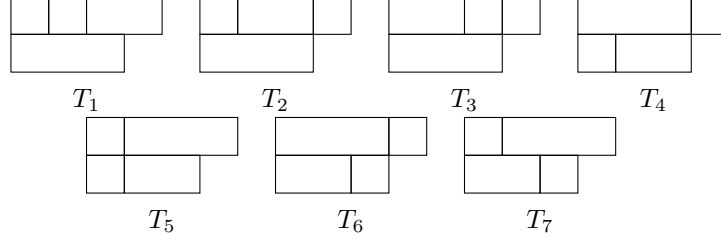
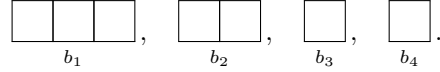


Figure 1: $(3, 2, 1, 1)$ -brick tabloids of shape $(4, 3)$

For example, if $\lambda = (3, 2, 1, 1)$ and $\mu = (4, 3)$, then we must cover Y_μ with the bricks



Here, bricks of the same size are indistinguishable. There are in total seven λ -brick tabloids of shape μ , given in Figure 1.

We let $B_{\lambda, \mu}$ denote the set of λ -brick tabloids of shape μ . We define a weight $w(T)$ for each λ -brick tabloid $T \in B_{\lambda, \mu}$ by

$$w(T) = \prod_{b \in T} w_T(b),$$

where for each brick b in T , $|b|$ denotes the length of b and

$$w_T(b) = \begin{cases} 1 & \text{if } b \text{ is not at the end of a row in } T, \\ |b| & \text{if } b \text{ is at the end of a row in } T. \end{cases}$$

Thus $w(T)$ is the product of the lengths of the rightmost bricks in T . For example, for the seven $(3, 2, 1, 1)$ -brick tabloids of shape $(4, 3)$ given in Figure 1, the weights are computed to be $w(T_1) = 6$, $w(T_2) = 3$, $w(T_3) = 3$, $w(T_4) = 2$, $w(T_5) = 6$, $w(T_6) = 1$ and $w(T_7) = 3$. We let

$$w(B_{\lambda, \mu}) := \sum_{T \in B_{\lambda, \mu}} w(T).$$

Eğecioğlu and Remmel [5, Rel. (11), p. 111] proved that for partitions $\lambda, \mu \vdash n$, we have

$$c_{\lambda, \mu} = (-1)^{\ell(\lambda) - \ell(\mu)} w(B_{\lambda, \mu}) P_\mu, \quad (5.3)$$

where

$$P_\mu := P_{\pi \in S_n}(\pi \text{ has cycle type } \mu).$$

Here $P_{\pi \in S_n}$ is the uniform probability measure on the symmetric group S_n , and we say that π has a cycle type $(\mu_1, \mu_2, \dots, \mu_r)$ if the cycle sizes of π are given by μ_1, \dots, μ_r .

Lemma 5.3. *Let n and k be positive integers. Let $\mu \vdash n$. We have*

$$\sum_{\substack{\lambda \vdash n \\ \ell(\lambda) \leq k}} w(B_{\lambda, \mu}) \leq \sum_{i=0}^k \binom{n}{i}. \quad (5.4)$$

Proof. Write μ as (μ_1, \dots, μ_r) . A λ -brick tabloid of shape μ determines the partition λ uniquely. Indeed, λ can be recovered by reading the lengths of the bricks in each row of the tabloid. Thus, the set $\cup_{\lambda \vdash n, \ell(\lambda) \leq k} B_{\lambda, \mu}$ may be identified with a sequence $\{b_i\}_{i=1}^r$ of positive integers with $\sum_{i=1}^r b_i \leq k$, and a double sequence $\{a_{i,j}\}_{1 \leq i \leq r, 1 \leq j \leq b_i}$ of positive integers with $\sum_{j=1}^{b_i} a_{i,j} = \mu_i$ for each i as follows. The number b_i is set to be the number of blocks in the i th topmost row of the tabloid, and the number $a_{i,j}$ is set to be the length

of the j th leftmost brick in the i -topmost row. Under this identification, $w(B_{\lambda,\mu})$ is given by the product $\prod_{i=1}^r a_{i,b_i}$, and it follows that for any $t \geq 0$, we have

$$\sum_{\substack{\lambda \vdash n \\ \ell(\lambda)=t}} w(B_{\lambda,\mu}) = \sum_{\substack{b_1, \dots, b_r \geq 1 \\ b_1 + \dots + b_r = t}} \sum_{\substack{\forall 1 \leq i \leq r: \\ a_{i,1}, \dots, a_{i,b_i} \geq 1 \\ \sum_{j=1}^{b_i} a_{i,j} = \mu_i}} \prod_{i=1}^r a_{i,b_i}. \quad (5.5)$$

Consider the generating function

$$B(u) := \sum_{\lambda \vdash n} \omega(B_{\lambda,\mu}) u^{\ell(\lambda)}.$$

Letting $c(n_1, n_2, n_3)$ be the number of solutions to $x_1 + x_2 + \dots + x_{n_1} = n_3$ with $x_{n_1} = n_2$ and $x_i \geq 1$, it follows from (5.5) that

$$B(u) = \sum_{\substack{\forall 1 \leq i \leq r: \\ b_i, y_i \geq 1}} \prod_{i=1}^r c(b_i, y_i, \mu_i) y_i u^{b_i} = \prod_{i=1}^r \left(\sum_{b_i, y_i \geq 1} c(b_i, y_i, \mu_i) y_i u^{b_i} \right).$$

As $c(n_1, n_2, n_3)$ is also the number of solutions to $x_1 + \dots + x_{n_1-1} = n_3 - n_2$ in positive integers, a standard combinatorial result says that

$$c(n_1, n_2, n_3) = \begin{cases} \binom{n_3 - n_2 - 1}{n_1 - 2} & \text{if } n_3 \geq n_2 + n_1 - 1, n_1 \geq 2, \\ \mathbf{1}_{n_2 = n_3} & \text{if } n_1 = 1, \\ 0 & \text{otherwise,} \end{cases}$$

so that

$$\begin{aligned} B(u) &= \prod_{i=1}^r \left(\mu_i u + \sum_{y=1}^{\mu_i-1} \sum_{b=2}^{\mu_i-y+1} \binom{\mu_i-y-1}{b-2} y u^b \right) \\ &= \prod_{i=1}^r \left(\mu_i u + \sum_{y=1}^{\mu_i-1} y u^2 (1+u)^{\mu_i-y-1} \right) \\ &= \prod_{i=1}^r ((1+u)^{\mu_i} - 1), \end{aligned}$$

where in the last passage we made use of the identity $\sum_{i=1}^d i x^i = x(dx^{d+1} - (d+1)x^d + 1)/(x-1)^2$ with $d = \mu_i - 1$ and $x = 1/(1+u)$. As the left-hand side of (5.4) is the sum of the first $k+1$ coefficients of $B(u)$, and they are bounded from above by the corresponding coefficients of $\prod_{i=1}^r (1+u)^{\mu_i} = (1+u)^n = \sum_{i=0}^n \binom{n}{i} u^i$, the proof is concluded. \square

5.3 Permutation statistics

We denote the expectation of a function $f: S_n \rightarrow \mathbb{R}$ with respect to the uniform probability measure on S_n by $\mathbb{E}_{\pi \in S_n} f(\pi)$. We denote by $\ell(\pi)$ the number of cycles in a permutation π .

Lemma 5.4. *Let $n \geq 1$, $m \geq 2$ be positive integers. Let $z_1, z_2 \in \mathbb{C}$. Define the following function on S_n :*

$$f(\pi) = \prod_{C \in \pi, m \nmid |C|} z_1 \prod_{C \in \pi, m \mid |C|} z_2 \quad (5.6)$$

where the product is over the disjoint cycles of π . Then

$$\mathbb{E}_{\pi \in S_n} f(\pi) = [u^n] (1-u)^{-z_1} (1-u^m)^{(-z_2+z_1)/m}.$$

Proof. The exponential formula for permutations [23, Corollary 5.1.9] states the following. Given a function $g: \mathbb{N} \rightarrow \mathbb{C}$, we construct a corresponding function on permutations (on arbitrary number of elements) as follows:

$$G(\pi) = \prod_{C \in \pi} g(|C|),$$

where the product is over the disjoint cycles of π . We then have the following identity of formal power series:

$$1 + \sum_{i \geq 1} (E_{\pi \in S_i} G(\pi)) u^i = \exp\left(\sum_{j \geq 1} \frac{g(j)}{j} u^j\right).$$

Applying the identity with

$$g(j) = \begin{cases} z_1 & \text{if } m \nmid j, \\ z_2 & \text{otherwise,} \end{cases}$$

we find that $G(\pi) = f(\pi)$ for every $\pi \in S_n$, and the lemma follows by a short computation. \square

5.4 Bounds on certain finite sums

Lemma 5.5. *Let $x \geq 2$ be a real number and n be a positive integer. Then*

1. $\sum_{d_1 d_2 = n} 2^{d_1} x^{d_2} \leq 8x^n$.
2. *If furthermore $x \geq 4$, $\sum_{d_1 d_2 = n, d_2 < n} 2^{d_1} x^{d_2} \leq 10x^{n/2}$.*

Proof. We begin with the first part. We may assume $n > 1$. Consider the function $f(t) = 2^{\frac{n}{t}} x^t$ on $[1, n]$. Its derivative is

$$f'(t) = f(t) \left(\log x - \frac{n \log 2}{t^2} \right),$$

so that f is either increasing from 1 to n (if $n \log 2 / \log x \leq 1$), or decreasing from 1 to $\sqrt{n \log 2 / \log x}$ and increasing from $\sqrt{n \log 2 / \log x}$ to n (otherwise). As $f(1) = 2^n x \leq 2x^n = f(n)$, it follows that

$$\sum_{d_1 d_2 = n} 2^{d_1} x^{d_2} = \sum_{d_2 | n} f(d_2) \leq 4x^n + (n-2) \max\{f(2), f(n/2)\} \cdot \mathbf{1}_{n \text{ not a prime}}.$$

If n is a prime, we are done. Otherwise, it suffices to show that $(n-2)2^2 x^{n/2} \leq 4x^n$ and that $(n-2)2^{n/2} x^2 \leq 4x^n$. For $n = 4, 5$, these are easy to verify, and for larger n they follow by induction. This establishes the first part of the lemma. The proof of the second part follows similar lines and is therefore omitted. \square

The following variant of Lemma 5.5 is also needed. We omit the similar proof.

Lemma 5.6. *Let $x \in \{\sqrt{2}, \sqrt{3}, 2, 3\}$. For any positive integer n , we have*

$$\sum_{d_1 d_2 = n, d_1 \neq n} 2^{d_1} x^{d_2} \leq 7x^n.$$

For $x = 2, 3$ we also have $\sum_{d_1 d_2 = n, 1 < d_2 < n} 2^{d_1} x^{d_2} + 1.4^n x \leq 14x^{n/2}$.

Lemma 5.7. *For any $n \geq 1$, we have $\sum_{i=0}^3 \binom{n}{i} \leq 7 \cdot 1.4^n$.*

Proof. For $n \leq 9$, this is checked by a short computation. For $n \geq 10$, we have $\sum_{i=0}^3 \binom{n}{i} = (n^3 + 5n + 6)/6 \leq 2n^3$, and an inductive argument shows that $2n^3 \leq 7 \cdot 1.4^n$. \square

5.5 Bounds on coefficients of a generating function

Lemma 5.8. *Let $t, r \geq 2$. Set $L := \lfloor 2 \log_t r \rfloor$ and*

$$Z(u) := \exp \left(\sum_{1 \leq k \leq L} \frac{20t^k}{k} u^k + \sum_{k > L} 20(r+1) \frac{t^{\frac{k}{2}}}{k} u^k \right).$$

Then

$$|[u^n]Z(u)| \leq t^{\frac{n}{2}} \binom{20(r+1) + n - 1}{n} \quad (5.7)$$

for all $n \geq 1$. If $r \geq \max\{200000, t^{\log^2 t}\}$, we have

$$|[u^n]Z(u)| \leq t^{\frac{n}{2}} t^{\frac{n \log \log r}{\log r}} \exp(140 \frac{(r+1)}{(\log r)^2} t) \quad (5.8)$$

for all $n \geq 1$. If $r = O(n)$, we have

$$|[u^n]Z(u)| \leq t^{\frac{n}{2} + O_t(\frac{n \log \log(n+2)}{\log(n+2)})}. \quad (5.9)$$

Proof. We work with the modified function

$$\tilde{Z}(u) := Z(u/\sqrt{t}),$$

so that

$$[u^n]Z(u) = t^{n/2} [u^n] \tilde{Z}(u).$$

As $t^{k/2} \leq r+1$ for $k \leq L$, we have

$$\left| [u^n] \tilde{Z}(u) \right| \leq \left| [u^n] \exp \left(\sum_{k \geq 1} 20(r+1) \frac{u^k}{k} \right) \right| = [u^n] (1-u)^{-20(r+1)},$$

which establishes (5.7). As \tilde{Z} has non-negative coefficients and radius of convergence 1, we have

$$|[u^n] \tilde{Z}(u)| \leq \sum_{i \geq 0} R^{i-n} [u^i] \tilde{Z}(u) = \frac{\tilde{Z}(R)}{R^n}$$

for every $R \in (0, 1)$. If $R \in (1.2/\sqrt{t}, 1)$, we can bound $\sum_{1 \leq k \leq L} 20t^{k/2} R^k/k$ from above by

$$\sum_{1 \leq k \leq L} \frac{20t^{k/2}}{k} R^k \leq \frac{20(R\sqrt{t})^L}{1 - 1/(R\sqrt{t})} \leq 120(r+1)R^L,$$

and the sum $\sum_{k > L} 20(r+1)R^k/k$ by

$$\sum_{k > L} 20(r+1) \frac{R^k}{k} \leq \frac{20(r+1)}{L+1} \frac{R^L}{1-R}.$$

Thus, for every $R \in (1.2/\sqrt{t}, 1)$,

$$|[u^n] \tilde{Z}(u)| \leq \exp \left(20(r+1)R^L \left(6 + \frac{1}{(L+1)(1-R)} \right) - n \log R \right). \quad (5.10)$$

Assume $r \geq 200000$ and choose $R = t^{-\frac{\log \log r}{\log r}}$ in (5.10). We then have

$$-n \log R = n \frac{\log \log r}{\log r} \log t, \quad R^L \leq t^{-\frac{\log \log r}{\log r} (2 \log_t r - 1)} = \frac{t^{\frac{\log \log r}{\log r}}}{(\log r)^2} \leq \frac{t}{(\log r)^2}. \quad (5.11)$$

Assuming further $r \geq t^{\log^2 t}$, we have $\frac{\log t \log \log r}{\log r} \in (0, 1)$, which implies $R \leq 1 - \log t \log \log r / (2 \log r)$, and so

$$\frac{1}{(L+1)(1-R)} \leq \frac{\log t}{2 \log r} \frac{2 \log r}{\log t \log \log r} \leq 1. \quad (5.12)$$

Plugging (5.11) and (5.12) in (5.10), we obtain (5.8). To prove (5.9), use (5.8) if $r \geq \max\{200000, t^{\log^2 t}, \sqrt{n}\}$, and otherwise use (5.7) together with the bound $\binom{n+k}{n} \leq (n+k)^{\min\{n, k\}}$. \square

6 Proof of Theorem 2.1

By (2.3), it suffices to bound

$$\sum_{\substack{\omega \in \Omega \\ |\omega| = n}} |S(n, \chi \cdot \mathbf{1}_\omega)|,$$

where $\mathbf{1}_\omega$ is the indicator function of polynomials f with $\omega_f = \omega$ (see (3.10) for the definition of S). Let

$$\Omega_d \subseteq \Omega$$

be the subset of factorization types containing only pairs $(x, y) \in \mathbb{N}^2$ with $x = d$. The elements of Ω_d , for each d , may be parametrized by partitions – to each $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k) \in \mathbb{Y}$, we associate

$$\omega_{\lambda, d} := \{(d, \lambda_1), \dots, (d, \lambda_k)\} \in \Omega_d.$$

Note that $|\omega_{\lambda, d}| = d|\lambda|$. By Lemma 5.1, $\sum_{\omega \in \Omega, |\omega| = n} |S(n, \chi \cdot \mathbf{1}_\omega)|$ is the coefficient of u^n in the following power series:

$$F_\chi(u) := \prod_{d \geq 1} F_d(u^d)$$

where

$$F_d(u) := \sum_{\lambda \in \mathbb{Y}} |S(d|\lambda|, \chi \cdot \mathbf{1}_{\omega_{\lambda, d}})| u^{|\lambda|}.$$

The terms with $\ell(\lambda) > |\mathcal{P}_d|$ do not contribute to $F_d(u)$, as there is no factorization type with more than $|\mathcal{P}_d|$ distinct primes of degree d . By Lemma 5.2 and (5.2), for each $\lambda \in \mathbb{Y}$ and $d \geq 1$, we have

$$S(d|\lambda|, \chi \cdot \mathbf{1}_{\omega_{\lambda, d}}) = \sum_{\mu \vdash |\lambda|} c_{\lambda, \mu} p_\mu(\chi(P) : P \in \mathcal{P}_d). \quad (6.1)$$

Let $\text{ord}(\chi) \geq 2$ be the order of χ . Writing μ as $(\mu_1, \mu_2, \dots, \mu_r)$, we may bound $p_\mu(\chi(P) : P \in \mathcal{P}_d)$ using Lemma 3.1 as follows:

$$\begin{aligned} |p_\mu(\chi(P) : P \in \mathcal{P}_d)| &= \prod_{i=1}^r |p_{\mu_i}(\chi(P) : P \in \mathcal{P}_d)| \\ &\leq \prod_{\substack{1 \leq i \leq r \\ \text{ord}(\chi) \nmid \mu_i}} \left(\min \left\{ \frac{q^{\frac{d}{2}}}{d} (\ell + \deg(M) + 1), \frac{q^d}{d} \right\} \right) \prod_{\substack{1 \leq i \leq r \\ \text{ord}(\chi) \mid \mu_i}} \left(\frac{q^d}{d} \right). \end{aligned} \quad (6.2)$$

From (6.1), (6.2), (5.6) and (5.3), we have for all $n \geq 1$

$$\begin{aligned} \sum_{\substack{\lambda \vdash n \\ \ell(\lambda) \leq |\mathcal{P}_d|}} |S(d|\lambda|, \chi \cdot \mathbf{1}_{\omega_{\lambda, d}})| &\leq \sum_{\substack{\lambda, \mu \vdash n \\ \ell(\lambda) \leq |\mathcal{P}_d|}} |c_{\lambda, \mu}| \prod_{\substack{1 \leq i \leq \ell(\mu) \\ \text{ord}(\chi) \nmid \mu_i}} \left(\min \left\{ \frac{q^{\frac{d}{2}}}{d} (\ell + \deg(M) + 1), \frac{q^d}{d} \right\} \right) \prod_{\substack{1 \leq i \leq \ell(\mu) \\ \text{ord}(\chi) \mid \mu_i}} \left(\frac{q^d}{d} \right) \\ &= E_{\pi \in S_n} f(\pi) \left(\sum_{\substack{\lambda \vdash n \\ \ell(\lambda) \leq |\mathcal{P}_d|}} w(B_{\lambda, \mu_\pi}) \right), \end{aligned} \quad (6.3)$$

where f is defined as in (5.6) with $m := \text{ord}(\chi)$ and

$$z_1 = z_{1, d} := \min \left\{ \frac{q^{\frac{d}{2}}}{d} (\ell + \deg(M) + 1), \frac{q^d}{d} \right\}, \quad z_2 = z_{2, d} := \frac{q^d}{d},$$

and μ_π is the partition of n whose parts are the cycle sizes of π . By Lemma 5.3 and (6.3), the coefficients of F_d are bounded from above by the coefficients of

$$G_d(u) := 1 + \sum_{n \geq 1} \left(\sum_{i=0}^{|\mathcal{P}_d|} \binom{n}{i} \right) E_{\pi \in S_n} f(\pi) u^n.$$

If $q \geq 4$, we do the following. Replacing $\sum_{i=0}^{|\mathcal{P}_q|} \binom{n}{i}$ with 2^n , we use Lemma 5.4 to bound the coefficients of G_d from above by the coefficients of

$$H_d(u) := (1 - 2u)^{-z_{1,d}} (1 - (2u)^{\text{ord}(\chi)})^{(-z_{2,d} + z_{1,d})/\text{ord}(\chi)},$$

and so the coefficients of F_χ are bounded from above by the coefficients of

$$H_\chi(u) := \prod_{d \geq 1} H_d(u^d).$$

Summarizing,

$$\begin{aligned} \sum_{\omega \in \Omega, |\omega|=n} |S(n, \chi \cdot \mathbf{1}_\omega)| &= [u^n] F_\chi(u) \leq [u^n] H_\chi(u) \\ &= [u^n] \prod_{d \geq 1} (1 - 2u^d)^{-z_{1,d}} (1 - 2^{\text{ord}(\chi)} u^{d \text{ord}(\chi)})^{(-z_{2,d} + z_{1,d})/\text{ord}(\chi)}. \end{aligned} \quad (6.4)$$

The logarithm of the power series H_χ is given by

$$\log H_\chi(u) = \sum_{i,d \geq 1} \frac{2^i u^{di}}{i} z_{1,d} + \sum_{i,d \geq 1} \frac{2^{i \text{ord}(\chi)} u^{di \text{ord}(\chi)}}{i} \frac{z_{2,d} - z_{1,d}}{\text{ord}(\chi)},$$

so that

$$[u^k] \log H_\chi(u) = \frac{1}{k} \sum_{di=k} 2^i (z_{1,d} d) + \frac{\mathbf{1}_{\text{ord}(\chi)|k}}{k} \cdot \sum_{di=\frac{k}{\text{ord}(\chi)}} 2^{i \text{ord}(\chi)} (z_{2,d} - z_{1,d}) d.$$

Set

$$L := \lfloor 2 \log_q(\ell + \deg(M) + 1) \rfloor.$$

For $d \leq L$, we have $z_{1,d} = z_{2,d} = q^d/d$, so that by the first part of Lemma 5.5 with $x = q$,

$$[u^k] \log H_\chi(u) \leq \frac{1}{k} \sum_{di=k} 2^i q^d \leq \frac{8q^k}{k}.$$

for all $1 \leq k \leq L$. As $z_{2,d} - z_{1,d} \leq q^d/d$ and $z_{1,d} \leq q^{\frac{d}{2}}(\ell + \deg(M) + 1)/d$, we also have, by the first part of Lemma 5.5 with $x = \sqrt{q}$ and the second part of the lemma with $x = q$, that

$$\begin{aligned} [u^k] \log H_\chi(u) &\leq \frac{(\ell + \deg(M) + 1)}{k} \sum_{di=k} 2^i q^{\frac{d}{2}} + \frac{\mathbf{1}_{\text{ord}(\chi)|k}}{k} \cdot \sum_{di=\frac{k}{\text{ord}(\chi)}} 2^{i \text{ord}(\chi)} q^d \\ &\leq 8(\ell + \deg(M) + 1) \frac{q^{\frac{k}{2}}}{k} + 10 \frac{q^{\frac{k}{2}}}{k} \leq 10(\ell + \deg(M) + 2) \frac{q^{\frac{k}{2}}}{k} \end{aligned} \quad (6.5)$$

for all $k \geq 1$. From (6.4) and (6.5), we have

$$\sum_{\omega \in \Omega, |\omega|=n} |S(n, \chi \cdot \mathbf{1}_\omega)| \leq [u^n] \exp\left(\sum_{1 \leq k \leq L} \frac{10q^k}{k} u^k + \sum_{k > L} 10(\ell + \deg(M) + 2) \frac{q^{\frac{k}{2}}}{k} u^k\right),$$

and by Lemma 5.8 with $t = q$, $r = \ell + \deg(M) + 1$, we have the estimates

$$\sum_{\omega \in \Omega, |\omega|=n} |S(n, \chi \cdot \mathbf{1}_\omega)| \leq q^{\frac{n}{2}} \binom{20(\ell + \deg(M) + 2) + n - 1}{n}$$

and, if $\ell + \deg(M) = O(n)$,

$$\sum_{\omega \in \Omega, |\omega|=n} |S(n, \chi \cdot \mathbf{1}_\omega)| \leq q^{\frac{n}{2}} e^{O_q\left(\frac{n \log \log(n+2)}{\log(n+2)}\right)}.$$

The theorem is established for $q \geq 4$. We now suppose $q \in \{2, 3\}$. We define $\widetilde{H}_d := H_d$ for $d \geq 2$, while for $d = 1$

$$\widetilde{H}_1(u) := 1 + \sum_{n \geq 1} 1.4^n \mathbb{E}_{\pi \in S_n} f(\pi) u^n = (1 - 1.4u)^{-z_{1,1}} (1 - (1.4u)^{\text{ord}(\chi)})^{(-z_{2,1} + z_{1,1})/\text{ord}(\chi)},$$

where in the last passage we used Lemma 5.4. As $|\mathcal{P}_1| = q \leq 3$ for $q \in \{2, 3\}$, it follows that $\sum_{i=0}^{|\mathcal{P}_1|} \binom{n}{i} \leq \sum_{i=0}^3 \binom{n}{i}$, which is at most $7 \cdot 1.4^n$ by Lemma 5.7. Thus the coefficients of G_1 are bounded from above by those of \widetilde{H}_1 times 7, and so the coefficients of F_χ are bounded from above by those of

$$\widetilde{H}_\chi(u) := \prod_{d \geq 1} \widetilde{H}_d(u^d),$$

times 7. As in the case $q \geq 4$, we proceed to upper bound the coefficients of $\log \widetilde{H}_\chi$. For $d \leq L$, we have $z_{1,d} = z_{2,d} = q^d/d$, so that by Lemma 5.6 with $x = q$,

$$[u^k] \log \widetilde{H}_\chi(u) \leq \frac{1}{k} \left(1.4^k q + \sum_{di=k, d \neq 1} 2^i q^d \right) \leq 10 \frac{q^k}{k},$$

for all $1 \leq k \leq L$, where we used $1.4 < q \leq 3$. For any $k \geq 1$, we have by Lemma 5.6 that

$$\begin{aligned} [u^k] \log \widetilde{H}_\chi(u) &\leq \frac{(\ell + \deg(M) + 1)}{k} \left(1.4^k q^{\frac{1}{2}} + \sum_{di=k, d \neq 1} 2^i q^{\frac{d}{2}} \right) + \frac{\mathbf{1}_{\text{ord}(\chi)} |k|}{k} \left(\sum_{di=\frac{k}{\text{ord}(\chi)}, d \neq 1} 2^i \text{ord}(\chi) q^d + 1.4^k q \right) \\ &\leq \frac{(\ell + \deg(M) + 1)}{k} \left(2 \cdot 1.4^k + 7q^{\frac{k}{2}} \right) + 14 \frac{q^{\frac{k}{2}}}{k} \leq 20(\ell + \deg(M) + 2) \frac{q^{\frac{k}{2}}}{k}. \end{aligned}$$

From this point we continue as in the case $q \geq 4$ and conclude the proof of the theorem.

Acknowledgements

The author would like to express his gratitude to Darij Grinberg for pointing out to him the work of Egecioğlu and Remmel [5]. The author would like to thank Dimitris Koukoulopoulos for a discussion on $H(x, y, 2y)$ and to Brad Rodgers, Ze'ev Rudnick, Will Sawin and the anonymous referees for useful comments and suggestions. The author was supported by the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement no. 320755.

References

- [1] E. Bank, L. Bary-Soroker, and L. Rosenzweig. Prime polynomials in short intervals and in arithmetic progressions. *Duke Math. J.*, 164(2):277–295, 2015.
- [2] A. Bhowmick, T. H. Lê, and Y.-R. Liu. A note on character sums in finite fields. *Finite Fields Appl.*, 46:247–254, 2017.
- [3] Z. Cui and J. Wu. The Selberg-Delange method in short intervals with an application. *Acta Arith.*, 163(3):247–260, 2014.
- [4] G. W. Effinger and D. R. Hayes. *Additive number theory of polynomials over a finite field*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1991. Oxford Science Publications.
- [5] O. Egecioğlu and J. B. Remmel. Brick tabloids and the connection matrices between bases of symmetric functions. *Discrete Appl. Math.*, 34(1-3):107–120, 1991. Combinatorics and theoretical computer science (Washington, DC, 1989).

- [6] B. Feng and Z. Cui. DDT theorem over square-free numbers in short interval. *Frontiers of Mathematics in China*, 12(2):367–375, Apr 2017.
- [7] K. Ford. The distribution of integers with a divisor in a given interval. *Ann. of Math. (2)*, 168(2):367–433, 2008.
- [8] K. Ford. Integers with a divisor in $(y, 2y]$. In *Anatomy of integers*, volume 46 of *CRM Proc. Lecture Notes*, pages 65–80. Amer. Math. Soc., Providence, RI, 2008.
- [9] R. R. Hall and G. Tenenbaum. On the average and normal orders of Hooley’s Δ -function. *J. London Math. Soc. (2)*, 25(3):392–406, 1982.
- [10] D. R. Hayes. The distribution of irreducibles in $\text{GF}[q, x]$. *Trans. Amer. Math. Soc.*, 117:101–127, 1965.
- [11] C. Hooley. On a new technique and its applications to the theory of numbers. *Proc. London Math. Soc. (3)*, 38(1):115–151, 1979.
- [12] I. Kátai. A remark on a paper of K. Ramachandra. In *Number theory (Ootacamund, 1984)*, volume 1122 of *Lecture Notes in Math.*, pages 147–152. Springer, Berlin, 1985.
- [13] I. Kátai and M. V. Subbarao. Some remarks on a paper of Ramachandra. *Liet. Mat. Rink.*, 43(4):497–506, 2003.
- [14] J. Keating and Z. Rudnick. Squarefree polynomials and Möbius values in short intervals and arithmetic progressions. *Algebra Number Theory*, 10(2):375–420, 2016.
- [15] K. Matomäki and M. Radziwiłł. Multiplicative functions in short intervals. *Ann. of Math. (2)*, 183(3):1015–1056, 2016.
- [16] P. Meisner. Erdős’ multiplication table problem for function fields and symmetric groups. *arXiv preprint arXiv:1804.08483*, 2018.
- [17] K. Ramachandra. Some problems of analytic number theory. *Acta Arith.*, 31(4):313–324, 1976.
- [18] G. Rhin. Répartition modulo 1 dans un corps de séries formelles sur un corps fini. *Dissertationes Math. (Rozprawy Mat.)*, 95, 1972.
- [19] B. Rodgers. Arithmetic functions in short intervals and the symmetric group. *Algebra Number Theory*, 12(5):1243–1279, 2018.
- [20] M. Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.
- [21] W. Sawin. Square-root cancellation for sums of factorization functions over short intervals in function fields. *arXiv preprint arXiv:1809.05137*, 2018.
- [22] W. Sawin and M. Shusterman. On the Chowla and twin primes conjectures over $\mathbb{F}_q[t]$. *arXiv preprint arXiv:1808.04001*, 2019.
- [23] R. P. Stanley. *Enumerative combinatorics. Vol. 2*, volume 62 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1999. With a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin.
- [24] A. Weil. *Basic number theory*. Springer-Verlag, New York-Berlin, third edition, 1974. Die Grundlehren der Mathematischen Wissenschaften, Band 144.

RAYMOND AND BEVERLY SACKLER SCHOOL OF MATHEMATICAL SCIENCES, TEL AVIV UNIVERSITY, TEL AVIV 69978, ISRAEL
 E-mail address: ofir.goro@gmail.com