PRIME AND MÖBIUS CORRELATIONS FOR VERY SHORT INTERVALS IN $\mathbb{F}_q[x]$.

PÄR KURLBERG, LIOR ROSENZWEIG

ABSTRACT. We investigate function field analogs of the distribution of primes, and prime k-tuples, in "very short intervals" of the form $I(f) := \{f(x) + a : a \in \mathbb{F}_p\}$ for $f(x) \in \mathbb{F}_p[x]$ and p prime, as well as cancellation in sums of function field analogs of the Möbius μ function and its correlations (similar to sums appearing in Chowla's conjecture). For generic f, i.e., for f a Morse polynomial, the error terms are roughly of size $O(\sqrt{p})$ (with typical main terms of order p). For non-generic f we prove that independence still holds for "generic" set of shifts. We can also exhibit examples for which there is no cancellation at all in Möbius/Chowla type sums (in fact, it turns out that (square root) cancellation in Möbius sums is *equivalent* to (square root) cancellation in Chowla type sums), as well as intervals where the heuristic "primes are independent" fails badly. The results are deduced from a general theorem on correlations of arithmetic class functions; these include characteristic functions on primes, the Möbius μ function, and divisor functions (e.g., function field analogs of the Titchmarsh divisor problem can be treated.) We also prove analogous, but slightly weaker, results in the more delicate fixed characteristic setting, i.e., for $f(x) \in \mathbb{F}_q[x]$ and intervals of the form $f(x) + a$ for $a \in \mathbb{F}_q$, where p is fixed and $q = p^l$ grows.

1. INTRODUCTION

Given a prime p, let $\mathbb{F}_p$ denote the finite field with p elements, and let

$$M_d = M_d(\mathbb{F}_p) := \{f \in \mathbb{F}_p[x] : f \text{ is monic and } \deg(f) = d\}$$

denote the set of monic polynomials of degree d. Gauss gave an exact formula for the number of prime, or irreducible, polynomials in $M_d(\mathbb{F}_p)$,

The authors were partially supported by grants from the Göran Gustafsson Foundation for Research in Natural Sciences and Medicine,and the Swedish Research Council (621-2011-5498, 2016-03701).

namely

$$|\{f \in M_d(\mathbb{F}_p) : \ f \text{ is prime } \}| = \frac{1}{d}\sum_{e|d}\mu(d/e)p^e = \frac{p^d}{d}\cdot(1+O(p^{-d/2}));$$

since $|M_d(\mathbb{F}_p)| = p^d$ this can be viewed as a function field analog of the Prime Number Theorem as p^d tends to infinity, with $1/d$ playing the role of the "prime density", with square root cancellation in the error term. In this paper, we shall be concerned with "short interval" analogs of Gauss' result, various generalizations to prime k-tuples, square root cancellation in Möbius μ sums, as well as sums appearing in Chowla's conjecture (these will be described in detail below.) Given $f \in \mathbb{F}_p[x]$ we define a *very short interval* around f as the set

$$I(f) := \{f(x) + a : a \in \mathbb{F}_p\};$$

clearly $|I(f)| = p$. In order to avoid trivialities we will from now on assume that $\deg(f) \geq 2$. Further, as we are mainly interested in the large p limit, we will assume that $p > d$ unless otherwise noted (cf. Section 7 for results when p is fixed but $q = p^l$ grows.)

1.1. **Results for generic intervals.** An element $f \in M_d(\mathbb{F}_p)$ is said to be a *Morse polynomial* provided that f has $d-1$ distinct critical values, i.e., $|\{f(\xi) : f'(\xi) = 0\}| = d-1$. A basic fact (cf. Section 2.2) is that f is Morse for a *generic* choice of coefficients; in particular, given $f(x) \in M_d(\mathbb{F}_p)$, the polynomials $f(x) + sx$ will be Morse for all but $O_d(1)$ elements $s \in \mathbb{F}_p$. Our first result is that an analog of the Hardy-Littlewood prime k-tuple conjecture holds for *almost all* very short intervals, namely the ones "centered" at Morse polynomials. For simplicity we state the result only for simultaneous prime specialization, but in fact any set of k factorization patterns can be treated, cf. Section 1.1.1.

Theorem 1. *Assume that $f \in M_d(\mathbb{F}_p)$ is a Morse polynomial, and $d \geq 2$. We then have*

$$|\{g \in I(f) : \ g \text{ is prime } \}| = \frac{p}{d} + O_d(\sqrt{p}) \tag{1}$$

Moreover, given k distinct shifts $h_1, h_2, \dots, h_k \in \mathbb{F}_p$, we have

$$|\{g \in I(f) : \ g+h_1, g+h_2, \dots, g+h_k \text{ are prime } \}| = \frac{p}{d^k} + O_{d,k}(\sqrt{p}) \tag{2}$$

The latter assertion is a natural function field analogue of the prime k-tuple conjecture for integers in short intervals. However, unlike

the integer case, for f Morse there are *no* fluctuations in the Hardy-Littlewood constants as $h_1, \dots, h_k$ varies over distinct elements. This result is generalized in the non-Morse case for "generic" shifts, where in Theorem 4 we show that this type of "prime independence" is valid also in the case where the "prime distribution" is not the generic one. Even so, interestingly, large variations do occur in the non-Morse case (cf. Section 1.4), and, very surprisingly, there are non-Morse examples where "prime independence" breaks down completely for certain rare shifts (cf. Section 1.4.6.)

We remark that an easy consequence of (1) is a prime number theorem for progressions that is valid for "very large" Morse moduli: given $b \in \mathbb{F}_p^\times$ and a Morse polynomial $q(x) \in M_d(\mathbb{F}_p)$,

$$|\{a \in \mathbb{F}_p : a \cdot q(x) + b \text{ is prime}\}| = p/d + O_d(\sqrt{p}).$$

The distribution of primes, and prime k-tuples, in "short intervals", i.e., sets of the form $I(f,1) := \{f(x) + a_1 x + a_0 : a_0, a_1 \in \mathbb{F}_q\}$, or more generally, sets of the form $I(f,m) := \{f(x) + \sum_{n=0}^{m} a_n x^n : a_0, \dots, a_m \in \mathbb{F}_q\}$ for $1 \le m < \deg(f)$, has received considerable attention in the large field limit, i.e., where $q = p^k \to \infty$ (in particular allowing for p fixed). That (1) holds for f "in general" (i.e., when $f(x) - t$ has Galois group S_d over $\overline{\mathbb{F}_q}(t)$) goes back to Cohen's pioneering work [8]; in [9] he showed that it holds for the short interval $I(f,1)$ provided $f \in M_d(\mathbb{F}_q)$ and $p > d$. In [4] Bary-Soroker removed this size condition for p odd, and allowed for more general shifts. In [3], the second author, together with Bank and Bary-Soroker, show that for any prime power q, for *all* polynomials f, and $m \ge 3$

$$|\{g \in I(f,m) : g \text{ is prime}\}| = \frac{q^{m+1}}{\deg(f)} + O_{\deg f}(q^{m+1/2});$$

in fact, under minor restrictions on f and q one may take $m = 2$ or even $m = 1$ (it is also implicit that (1) holds for f Morse.) An analog of the prime k-tuple conjecture for the "long" interval $M_d(\mathbb{F}_p)$ was shown by Pollack [20] provided that $(2p, d) = 1$. This co-primality condition was removed by Bary-Soroker [4]; Bank and Bary-Soroker then treated the case of short intervals (i.e., $I(f,m)$, $m \ge 2$) and q odd in [2]. We also mention that Entin [11] has shown prime k-tuple equidistribution for short intervals in a more general setting, namely for "Bateman-Horn" type specializations (e.g., for nonassociate, separable and irreducible polynomials $F_1(x,t), \dots, F_k(x,t) \in \mathbb{F}_q[x,t]$, he obtains the asymptotics for simultaneous irreducibility of the k specialized polynomials $F_1(g(t),t), \dots, F_k(g(t),t)$, for $g \in I(f,m)$); cf. [10] for recent further developments. For a nice survey of recent results

on function field analogs of similar questions in classical number theory, including analogs of cancellation in Möbius μ and Chowla sums described below, see [21].

A function field analog of the Möbius μ function on $M_d(\mathbb{F}_p)$ can be defined as follows: given a squarefree polynomial $g \in M_d(\mathbb{F}_p)$, write g as a product of l distinct monic irreducibles, i.e., $g = \prod_{i=1}^{l} g_i$, and define $\mu(g) := (-1)^l$; if g is not squarefree we set $\mu(g) = 0$. We then find that there is square root cancellation in Möbius sums, as well as in the auto-correlation type sums appearing in Chowla's conjecture (cf. [7]), for very short intervals in the large p limit.

Theorem 2. *Assume that $f \in M_d(\mathbb{F}_p)$ is Morse, and $d \geq 2$. Then*

$$\sum_{g \in I(f)} \mu(g) = O_d(\sqrt{p}). \tag{3}$$

More generally, given distinct elements $h_1, h_2, \ldots, h_k \in \mathbb{F}_p$, we have

$$\sum_{g \in I(f)} \left(\prod_{i=1}^{k} \mu(g + h_i) \right) = O_{d,k}(\sqrt{p}). \tag{4}$$

In Theorem 5 we show that for general f (i.e., non-Morse) square root cancellation in (3) is *equivalent* to square root cancellation in (4); moreover either there is square root cancellation, or there is *no cancellation at all*. See Section 1.3 for more details, as well as examples of intervals on which μ has constant sign.

In [6], Carmon and Rudnick showed that Chowla type sums over $M_d(\mathbb{F}_q)$ has square root cancellation as $q \to \infty$, provided q is odd; in [5], Carmon treated even q. In [16] Keating and Rudnick proved square root cancellation for Möbius sum over intervals of type $I(f, m)$ for $m \geq 2$; they also gave examples of polynomials f for which the Möbius sum over $I(f, 1)$ has no cancellation at all. We also note that Entin [11] can treat cancellation in short Chowla type sums in the more general Bateman-Horn type setting described earlier, and Sawin and Shusterman breakthrough result solving the twin prime Conjecture [23], and the quadratic Bateman-Horn Conjecture [24] for (large enough) prime powers.

1.1.1. *Class function correlations.* The above results are easily deduced from a more general result valid for functions induced from class functions on S_d, the symmetric group on d letters. Briefly, for squarefree $g \in M_d(\mathbb{F}_p)$ we associate a conjugacy class σ_g in S_d as follows: factoring g into prime polynomials, i.e., writing $g = \prod_{i=1}^{l} P_i$, choose l *disjoint* cycles $c_1, \ldots, c_l \in S_d$ such that the length of c_i equals $\deg(P_i)$

for $1 \leq i \leq l$; we then define σ_g as the conjugacy class generated by $\prod_{i=1}^{l} c_i$.

Now, given a class function ϕ on S_d (i.e. $\phi(\sigma)$ only depends on the conjugacy class of σ), the above construction allows us to define a function, also denoted ϕ, on the set of squarefree elements in $M_d(\mathbb{F}_p)$. As the number of non-squarefree polynomials in $I(f)$, for $f \in M_d$ is $O_d(1)$ (cf. (9)) we may then choose any bounded extension of ϕ to $M_d(\mathbb{F}_p)$. In order to simplify statements we will in what follows always assume that the supremum norms of all class functions, and their extensions, are bounded by some absolute constant.

Theorem 3. *Assume that $f \in M_d(\mathbb{F}_p)$ is a Morse polynomial, and $d \geq 2$. Further, let $\phi_1, \dots, \phi_k$ be class functions on S_d, extended as above to functions on $M_d(\mathbb{F}_p)$ .Then there exists constants $\{c(\phi_i)\}_{i=1}^{k}$, given by*

$$c(\phi_i) = \frac{1}{|S_d|} \sum_{\sigma \in S_d} \phi_i(\sigma), \quad i = 1, \dots, k.$$

such that

$$\sum_{g \in I(f)} \phi_i(g) = p \cdot c(\phi_i) + O_d(\sqrt{p})$$

for $i = 1, \dots, k$. Moreover, given distinct elements $h_1, h_2, \dots, h_k \in \mathbb{F}_p$, we have

$$\sum_{g \in I(f)} \left(\prod_{i=1}^{k} \phi_i(g + h_i) \right) = p \cdot \prod_{i=1}^{k} c(\phi_i) + O_{d,k}(\sqrt{p}). \tag{5}$$

We remark that Theorem 3 does *not* hold in the large q limit, cf. Section 7 for further details, together with a suitably weakened independence result valid for the large q limit.

When detecting factorization patterns the constants $c(\phi_i)$ can be given a simple combinatorial interpretation. Namely, given a desired factorization pattern of $g \in M_d(\mathbb{F}_p)$, associate an S_d-conjugacy class C as described above. This in turn can be interpreted as a partition of d, i.e., $d = \sum_{j \geq 1} d_j j$ (e.g., for the partition $4 = 2 + 1 + 1$, $d_1 = 2$, $d_2 = 1$, and $d_j = 0$ for $j > 2$). With $\phi = 1_C$, where 1_C denotes the characteristic function of the conjugacy class C, we have

$$c(\phi) = \frac{|C|}{|S_d|} = \frac{1}{\prod_j (j^{d_j}(d_j!))}$$

(since $|C| = \frac{|S_d|}{\prod_j j^{d_j}(d_j!)}$.) For example, if $C = \{\sigma \in S_d : \sigma \sim (123 \dots d)\}$, we find that $1_C = 1_{\text{Prime}}$ (the characteristic function on the set of prime polynomials), and $c(1_{\text{Prime}}) = |C|/|S_d| = (d-1)!/d! = 1/d$.

Other interesting examples of class functions include the Möbius μ function, as well as the function field analog of divisor functions d_r for integer $r \geq 2$; e.g., $d_2(g)$ is the number of ways to decompose g as a product of two monic polynomials. In particular, Theorems 1 and 2 are immediate consequences of Theorem 3. In similar fashion we can treat short interval function field analogs of the "shifted divisor problem", e.g., the sum $\sum_{g\in I(f)} d_r(g)d_r(g+1)$, as well as the Titchmarsh divisor problem, e.g., sums of the form $\sum_{g\in I(f)} 1_{\text{Prime}}(g)d_r(g+1)$. These results can be viewed as very short interval versions of recent results [1] by Andrade, Bary-Soroker and Rudnick for the full interval $M_d(\mathbb{F}_q)$.

We remark that Theorem 3 is, via the Chebotarev density theorem, Galois theoretic at heart (cf. Section 2.3): to each polynomial $f(x) + h_i + t$ we can associate a field extension $L_{h_i}/\mathbb{F}_p(t)$ with Galois group $G_{h_i} = \text{Gal}(L_{h_i}/\mathbb{F}_p(t)) \simeq S_d$, and the independence implicit in (5) boils down to linear independence of the field extensions $L_{h_1}, L_{h_2}, \dots, L_{h_k}$. In particular, with L^k denoting the compositium of $L_{h_1}, \dots, L_{h_k}$, we have $\text{Gal}(L^k/\mathbb{F}_p(t)) \simeq (S_d)^k$.

1.2. **Independence results for non-generic intervals.** For non-Morse polynomials the situation is more complicated since G_{h_i} might be smaller than S_d, and $\text{Gal}(L^k/\mathbb{F}_p(t))$ is in general *not* a product of groups. However, while independence can fail for non-Morse polynomials (cf. Section 1.4.6), we can still show that independence holds for "generic" choices of distinct shifts $h_1, \dots, h_k \in \mathbb{F}_p$ and p large.

Theorem 4. *Let $d \geq 2$, and let $\phi_1, \dots, \phi_k$ be class functions on S_d, extended as before to functions on $M_d(\mathbb{F}_p)$. Then for $f \in M_d(\mathbb{F}_p)$,*

$$\sum_{g\in I(f)} \phi_i(g) = p \cdot c_i + O_d(\sqrt{p}),$$

where c_i is explicitly given in (6)*. Moreover, there exists a set $B(f) \subset \mathbb{F}_p$, of cardinality at most $(d-1)^2$, with the following property: given distinct elements $h_1, h_2, \dots, h_k \in \mathbb{F}_p$ such that $h_i - h_j \notin B(f)$ for $i \neq j$, we have*

$$\sum_{g\in I(f)} \left(\prod_{i=1}^{k} \phi_i(g+h_i) \right) = p \cdot \prod_{i=1}^{k} c_i + O_{d,k}(\sqrt{p}).$$

Note that the number of distinct shifts $h_1, \dots, h_k \in \mathbb{F}_p$ such that $h_i - h_j \in B(f)$ is $O_{k,d}(p^{k-1})$, hence independence holds for most choices of shifts.

Determining the constants c_i is delicate (E.g., some factorization patterns might not occur at all, cf. Section 1.4). and requires some

knowledge about $G_{h_1} = \mathrm{Gal}(L_{h_1}/\mathbb{F}_p(t))$ (it turns out that the isomorphism class of G_{h_i} does not change with h_i.) With $l_{h_1} := L_{h_1} \cap \overline{\mathbb{F}_p}$ denoting the field of constants in L_{h_1}, let $G_{h_1,\mathrm{geom}} := \mathrm{Gal}(L_{h_1}/l_{h_1}(t))$ denote the "geometric part" of G_{h_1}. After making a *non-canonical* labeling of the roots of $f(x) + h_1 + t$ and $f(x) + h_i + t$ (regarded as polynomials with coefficients in $\mathbb{F}_p(t)$), we obtain an identification and inclusion $G_{h_i} \simeq G_{h_1} \subset S_d$ and can write

$$c_i = \frac{1}{|G_{h_1,\mathrm{geom}}|} \sum_{\sigma \in \tau \cdot G_{h_1,\mathrm{geom}}} \phi_i(\sigma) \tag{6}$$

where $\tau \in G_{h_1}$ is any element such that $\tau|_{l_{h_1}}$ acts as Frobenious on the finite field extension $l_{h_1}/\mathbb{F}_p$, i.e., $\tau(\alpha) = \alpha^p$ for $\alpha \in l_{h_1}$. For some examples where class function constants are computed using Galois theory, see Sections 1.4.3 and 1.4.4.

The independence can also be explained in terms of Galois theory. Briefly, after making non-canonical identifications $G_{h_i} \simeq G_{h_1}$ for $i = 2, 3, \dots, k$, we obtain inclusions

$$\mathrm{Gal}(L^k/\mathbb{F}_p(t)) \subset \prod_{i=1}^{k} G_{h_i} \subset (G_{h_1})^k$$

and the independence amounts to Frobenius equidistribution inside the coset $(\tau \cdot G_{h_1,\mathrm{geom}})^k$. We note that the methods (cf. the remark after Proposition 12) allows us to take $\phi_1, \dots, \phi_k$ to be class functions on $G_{h_1}, \dots, G_{h_k}$, rather than on S_d, and this sometimes allows for going beyond factorization patterns. E.g., the cycles (123) and (132) are conjugate in S_3, but not in A_3 (the latter group is abelian); when $G_{h_i} \simeq A_3$, after a non-canonical labeling of the roots, we can distinguish the two cases in terms of the Frobenious action on the roots. Another example is given in Section 1.4.5.

A more detailed discussion, in particular regarding the set $B(f)$ can be found in Sections 2.3 and 2.4.

1.3. **Lack of cancellation in Möbius and Chowla sums.** An unexpected phenomena is the existence of elements $f \in M_d(\mathbb{F}_p)$ for which there is *no cancellation* in short interval Möbius sum, i.e.,

$$\left| \sum_{g \in I(f)} \mu(g) \right| = p + O_d(1).$$

For example, for d odd and $p \equiv 1 \mod d$, take $f(x) = x^d$ (cf. Sections 1.4.2 and 5.1.1). Even more surprising, as noted in [16], for $f(x) = x^{2p}$ there is complete lack of cancellation for the sum over the

longer interval $I(f,1)$. In fact, either there is square root cancellation in both the Möbius sum as well as the Chowla sum, or there is essentially no cancellation whatsoever in either sum (cf. Theorem 2.)

Theorem 5. *Let $f \in M_d(\mathbb{F}_p)$ for $d \geq 2$, and let $h_1, \dots, h_k \in \mathbb{F}_p$ be distinct elements. Then one of the following occurs: either both*

$$\left|\sum_{g\in I(f)} \mu(g)\right| = p + O_d(1), \quad \left|\sum_{g\in I(f)} \left(\prod_{i=1}^{k} \mu(g+h_i)\right)\right| = p + O_{k,d}(1)$$

holds, or both

$$\left|\sum_{g\in I(f)} \mu(g)\right| = O_d(\sqrt{p}), \quad \left|\sum_{g\in I(f)} \left(\prod_{i=1}^{k} \mu(g+h_i)\right)\right| = O_{k,d}(\sqrt{p})$$

holds.

We remark that lack of cancellation is equivalent to the "geometric part" of a certain Galois group being contained in the alternating group A_d. More details on this, as well as the proof of Theorem 5 can be found in Section 5. Moreover, we note that Theorem 5 is *not true* in the large q limit (i.e., for p fixed), cf. Section 7.

1.4. **Further examples of degenerate intervals.** We next give some additional examples of short intervals exhibiting irregular behavior. For more details regarding these examples, see Section 6.

1.4.1. *Prime density fluctuations.* Let $f(x) = x^3$ and take $\phi_1 = \phi_2 = 1_{\text{Prime}}$. Here the constants vary with p, namely $c(1_{\text{Prime}}, p) = 2/3$ for $p \equiv 1 \mod 3$, whereas $c(1_{\text{Prime}}, p) = 0$ for $p \equiv 2 \mod 3$. In fact, there are *no primes* in $I(f)$ if $p \equiv 2 \mod 3$, and in this case the second part of Theorem 4 is trivial. On the other hand, it can be shown that $B(f) = \emptyset$ and hence, for $p \equiv 1 \mod 3$ and $h \not\equiv 0 \mod p$,

$$\sum_{g\in I(f)} 1_{\text{Prime}}(g) 1_{\text{Prime}}(g+h) = (2/3)^2 \cdot p + O(\sqrt{p}). \tag{7}$$

In other words, after taking into account the larger than expected prime density (for generic degree 3 polynomials it is 1/3), the short interval contains the expected number of twin primes (and similarly for prime k-tuples) — the heuristic "primes are independent" indeed holds in $I(f)$ as $p \to \infty$, even though $f(x) = x^3$ is *not* Morse.

1.4.2. *Lack of cancellation in Möbius sums.* Again we take $f(x) = x^3$ and, as noted before, for $p \equiv 1 \mod 3$, either $f(x)+a$ splits completely or is irreducible. In either case, $f(x) + a$ factors into an odd number of irreducibles and hence $\mu(f(x) + a) = -1$ if $f(x) + a$ is square free, i.e., for all nonzero $a \in \mathbb{F}_p$. If $p \equiv 2 \mod 3$, $x^3 + a$ is a permutation for all $a \in \mathbb{F}_p$. Consequently for all nonzero a, $f(x) + a$ has one linear factor, and one irreducible quadratic factor, and thus $\mu(x^3+a) = 1$ for all nonzero $a \in \mathbb{F}_p$.

1.4.3. *Class function constants via Galois theory.* To illustrate how averages over cosets of the geometric part of G_0 determines the class function constants (cf. (6)) we return to the example $f(x) = x^3$. Then $L_0 = \mathbb{F}_p(t, \zeta_3, \sqrt[3]{-t})$, where ζ_3 denotes a non-trivial third root of unity, and $l_0 = L_0 \cap \overline{\mathbb{F}_p} = \mathbb{F}_p(\zeta_3)$. If $p \equiv 1 \mod 3$, we have $\zeta_3 \in \mathbb{F}_p$, hence $l_0 = \mathbb{F}_p$, and $G_0 = G_{0,\mathrm{geom}} \simeq A_3$. Letting ϕ_1, ϕ_2, ϕ_3 denote characteristic functions of the three S_3-conjugacy classes $\{()\}$, $\{(123), (132)\}$, and $\{(12), (13), (23)\}$, the corresponding class function constants given by Theorem 4 and (6) is then given by $c_1 = 1/3, c_2 = 2/3, c_3 = 0$ (the key point is that Frobenious equidistributes in A_3.)

If $p \equiv 2 \mod 3$, then $l_0 = \mathbb{F}_p(\zeta_3) = \mathbb{F}_{p^2}$, and thus $G_0 \simeq S_3$ and $G_{0,\mathrm{geom}} \simeq A_3$. Further, as the action of the Frobenious map $\alpha \to \alpha^p$ must act nontrivially on l_0, the image of Frobenious equidistributes in the single conjugacy class given by the non-trival coset of A_3 (in S_3), consisting of the three transpositions $\{(12), (13), (23)\}$. Hence, for $p \equiv 2 \mod 3$, we have $c_1 = c_2 = 0, c_3 = 1$.

1.4.4. *Class function constants and "missing" factorization patterns.* Let p be a large prime and let $f(x) = x^4-2x^2$. Then $\mathrm{Gal}(f(x)+t, \mathbb{F}_p(t))$ is isomorphic to D_4, the dihedral group with 8 elements. Regarding D_4 as a subgroup of S_4, the elements of D_4, in cycle notation, are

$$\{(1,4)(2,3), (1,3)(2,4), (1,3), (2,4), (1,2)(3,4), (1,2,3,4), (1,4,3,2)\}.$$

Parametrizing the factorization patterns of $f(x) + a$, for $a \in \mathbb{F}_p$, by partitions of 4, we find that the different factorization patterns occurs with the following frequencies: $4 = 1+1+1+1$: $1/8$, $4 = 2+1+1$: $2/8$, $4 = 3 + 1$: $0/8$, $4 = 2 + 2$: $3/8$, and finally $4 = 4$: $2/8$. In particular, $f(x) + a$ *cannot* split into a linear and a cubic (irreducible) factor.

Let $\phi_1, \dots, \phi_5$ denote class functions (in S_4) that equals one on all permutations corresponding to the factorization pattern given by the 5 different partitions of 4 (see above), and zero otherwise. The corresponding class function constants in Theorem 4 are then the same as the corresponding frequencies listed above, and thus $c_1 = 1/8$, $c_2 = 2/8$, $c_3 = 0$, $c_4 = 3/8$, and $c_5 = 2/8$.

1.4.5. *Going beyond factorization patterns.* Again take $f(x) = x^4 - 2x^2$; as noted above we then have $\mathrm{Gal}(f(x)+t, \mathbb{F}_p(t)) \simeq D_4$. The elements of D_4 that are products of two disjoint transpositions fall into two D_4 conjugacy classes, namely $\{(1,2)(3,4),(1,4)(2,3)\}$ and $\{(1,3)(2,4)\}$; these two cases (after labeling the roots) can then be distinguished if we take class functions on D_4 rather than on S_4.

1.4.6. *Breakdown of independence of primes.* For general f the issue of independence for "bad shifts" appears delicate, but we can give an explicit example of a polynomial $f \in M_4(\mathbb{F}_p)$ for which the interval $I(f)$ has the expected prime density, yet prime independence breaks down for a few "bad" shifts h — there can be large fluctuations in the Hardy-Littlewood constants for f non-Morse.

Again let $f(x) = x^4 - 2x^2$ and first consider primes $p \equiv 1 \mod 4$; abusing notation we will let $f = f_p$ denote the reduction of f modulo p. Then

$$\sum_{g \in I(f)} 1_{\mathrm{Prime}}(g) = \frac{1}{4} \cdot p + O(\sqrt{p}) \tag{8}$$

and for $h \in \mathbb{F}_p \setminus \{0, \pm 1\}$ we have

$$\sum_{g \in I(f)} 1_{\mathrm{Prime}}(g) \cdot 1_{\mathrm{Prime}}(g+h) = \frac{1}{4^2} \cdot p + O(\sqrt{p}),$$

i.e., prime independence holds. However, for $h = \pm 1$, we have

$$\sum_{g \in I(f)} 1_{\mathrm{Prime}}(g) \cdot 1_{\mathrm{Prime}}(g+h) = \frac{1}{8} \cdot p + O(\sqrt{p})$$

and independence is clearly violated.

On the other hand, for $p \equiv 3 \mod 4$, the prime density is still $1/4$ (e.g., (8) holds), but if $h = \pm 1$, then

$$\sum_{g \in I(f)} 1_{\mathrm{Prime}}(g) \cdot 1_{\mathrm{Prime}}(g+h) = O(\sqrt{p});$$

in a sense independence is violated in the worst possible way as the "twin prime constant" is *zero*.

We remark that the p-averaged twin prime constant (asymptotically $p \equiv 1 \mod 4$ holds for half the primes) equals $1/2 \cdot 1/8 + 1/2 \cdot 0 = 1/4^2$, i.e., we arrive at the expected "independent" density — this is no coincidence, cf. Section 6.2.

1.5. **Acknowledgments.** We thank L. Bary-Soroker, A. Granville, and Z. Rudnick for stimulating and fruitful discussions, as well as their comments on an early draft, and L. Klurman for pointing out the application to primes in progressions to very large moduli.

2. Preliminaries

2.1. **Squarefree polynomials in very short intervals.** As we are concerned with class functions on very short intervals we begin by recording the useful fact that almost all $g \in I(f)$ are squarefree, for $f \in M_d(\mathbb{F}_q)$ and q large. In fact, given $f \in M_d$ and distinct shifts $h_1, \dots, h_k \in \mathbb{F}_q$,

$$|\{g \in I(f) : g + h_1, \dots, g + h_k \text{ are squarefree}\}| = q + O_{k,d}(1) \tag{9}$$

To see this it is enough to verify that $(f + h, f') = 1$ for all but $O_d(1)$ choices of $h \in \mathbb{F}_q$, but this is clear as $f'(\xi) = 0$ for at most $d-1$ values of $\xi \in \overline{\mathbb{F}_q}$, so the number of h so that $f(\xi) + h = 0$ is at most $d - 1$.

2.2. **Morse polynomials are generic.** As recalled in the introduction, a polynomial of degree d is called a Morse polynomial if the set of critical values is of cardinality $d-1$. It turns out that for f a Morse polynomial, the Galois group of $f(x) - t$ is maximal (over $\mathbb{Q}(t)$ this goes back to Hilbert [14].)

Proposition 6 (Cf. [25], Theorem 4.4.5)**.** *Assume that* $(q, 2d) = 1$ *and that* $f \in M_d(\mathbb{F}_q)$ *is a Morse polynomial. Then* $\mathrm{Gal}(f(x) - t/\mathbb{F}_q(t)) \simeq S_d$.

We remark that Geyer, in the appendix of [15], also treats the case $(q, d) = 1$ by introducing a more general notion of Morseness, namely assuming non-vanishing of the second Hasse-Schmidt derivative of f. Moreover, he also gives a beautiful Galois theoretic proof that "generic" polynomials are Morse.

Proposition 7. *Let* $f(x) \in M_d(\mathbb{F}_q)$ *with* $f''(x) \neq 0$*, and assume that* $(q, 2d) = 1$*. Then, for all but* $O_d(1)$ *values of* $s \in \overline{\mathbb{F}_q}$*, the polynomial* $f_s(x) = f(x) + sx$ *is a Morse polynomial.*

Although not stated this way, Proposition 7 is in fact proved in the last page of the proof of Proposition 4.3 in [15].

Similar criteria for showing that $\mathrm{Gal}(f(x) + tx^m/\mathbb{F}_p(t)) \simeq S_d$ for "generic" f and integer $m \in [1, d-1]$ can be found in [18, Section 5].

2.3. **Galois theory and the Chebotarev density theorem.** For the convenience of the reader, we collect here some results about Galois groups of function fields over finite fields. Before doing so, we begin with the following notations, similar to the ones used in [13, 17].

For $f \in M_d(\mathbb{F}_p)$ and $h \in \mathbb{F}_p$, define $F_h(x,t) \in \mathbb{F}_p[x,t]$ by

$$F_h(x,t) := f(x) + h + t.$$

Set $K_h = \mathbb{F}_p(t)[x]/(F_h(x,t))$, let L_h denote its Galois closure, and let $l_h := L_h \cap \overline{\mathbb{F}_p}$ be the corresponding field of constants. As l_h is independent of h (cf. [17, Lemma 5]), it is convenient to define $l = l_0$.

Given k distinct shifts $h_1, \dots, h_k \in \mathbb{F}_p$, let $L^k := L_{h_1} \cdot L_{h_2} \dots \cdot L_{h_k}$ be the compositum of the fields $L_{h_1}, \dots, L_{h_k}$, and let $G^k = \mathrm{Gal}(L^k/\mathbb{F}_p(t))$. Note that G^k is *not necessarily* a product of groups. We also define $G_{h_i} := \mathrm{Gal}(L_{h_i}/\mathbb{F}_p(t))$ for $i = 1, \dots, k$; after labeling the roots of $F_h(x,t)$ we obtain a natural inclusion $G_h \hookrightarrow S_d$; similarly we obtain a natural inclusion $G^k \hookrightarrow S_d^k$.

Let $l^k := L^k \cap \overline{\mathbb{F}_p}$ denote the field of constants in L^k,

and let $G^k_{\mathrm{geom}} := \mathrm{Gal}(L^k/l^k(t))$ denote the geometric part of G^k. Similarly let $G_{h_i,\mathrm{geom}} := \mathrm{Gal}(L_{h_i}/l_{h_i}(t)) = \mathrm{Gal}(L_{h_i}/l(t))$ denote the geometric parts of G_{h_i}, for $i = 1, \dots, k$. (Here we use that l_h does not depend on h, and that $l = l_0$.)

The set of critical values of f is given by

$$R_f := \{f(\xi) : \xi \in \overline{\mathbb{F}_p}, f'(\xi) = 0\};$$

we then put

$$B(f) := ((R_f - R_f) \setminus \{0\}) \cap \mathbb{F}_p,$$

where $R_f - R_f$ denotes the set of differences $\{r_1 - r_2 : r_1, r_2 \in R_f\}$.

We shall make use of the following properties of the Artin symbol.

Let $F(x,t) \in \mathbb{F}_q[x,t]$ be a separable irreducible polynomial, and let L denote its splitting field over $\mathbb{F}_q(t)$.

For all but finitely many $a \in \mathbb{F}_q$, the prime ideal $\mathfrak{p}_a = (t-a) \subset \mathbb{F}_q[t]$ is unramified in L, yielding a well defined conjugacy class $(\frac{L/\mathbb{F}_q(t)}{\mathfrak{p}_a}) \in \mathrm{Gal}(L/\mathbb{F}_q(t))$ — the Artin symbol. Moreover, for these choices of a the splitting type, or the cycle pattern, of the polynomial $F(x,a)$ (i.e., when specializing $t \to a \in \mathbb{F}_q$) is the same as the cycle pattern of $(\frac{L/\mathbb{F}_q(t)}{\mathfrak{p}_a})$, interpreted as a permutation on the roots of $F(x,t)$. Further, given a conjugacy class $\mathcal{C} \subset \mathrm{Gal}(L/\mathbb{F}_q(T))$, the density of prime ideals for which Artin symbol lies in $\mathcal{C}$ is given by the Chebotarev density Theorem.

Proposition 8 ([12], Proposition 6.4.8.)**.** *Let K be a function field over $\mathbb{F}_q$, let $d = [K : \mathbb{F}_q(t)]$, let L/K be a finite Galois extension, and let*

$\mathcal{C}$ be a conjugacy class in $\mathrm{Gal}(L/K)$. *With* $\mathbb{F}_{q^n}$ *denoting the algebraic closure of* $\mathbb{F}_q$ *in* L, *let* $m = [L : K\mathbb{F}_{q^n}]$. *Let* b *be a positive integer with* $res_{\mathbb{F}_{q^n}}\tau = res_{\mathbb{F}_{q^n}}\mathrm{Frob}_q^b$ *for each* $\tau \in \mathcal{C}$. *Let* k *be a positive integer. If* $k \not\equiv b \mod n$, *then* $C_k(L/K, \mathcal{C})$ *is empty. If* $k \equiv b \mod n$, *then*

$$\left| |C_k(L/K,\mathcal{C})| - \frac{|\mathcal{C}|}{km}q^k \right| < \frac{2|\mathcal{C}|}{km}((m+g_L)q^{k/2}+m(2g_K+1)q^{k/4}+g_L+dm).$$

Here $\mathrm{Frob}_q \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ is the Frobenius map given by $\mathrm{Frob}_q(\alpha) = \alpha^q$, g_L, g_K are the genera of the fields L, K, and

$$C_k(L/K,\mathcal{C}) = \{\mathfrak{p} \subset O_K : \deg(\mathfrak{p}) = k,\ \mathfrak{p} \text{ unramified}, \left(\frac{L/K}{\mathfrak{p}}\right) = \mathcal{C}\}$$

where $O_K \subset K$ is the integral closure of $\mathbb{F}_q[t]$ in K. In our applications we will always take $K = \mathbb{F}_q(t)$ and in this case $O_K = \mathbb{F}_q[t]$.

For a squarefree polynomial $f \in M_d(\mathbb{F}_q)$, define a conjugacy class $\sigma = \sigma_f \subset S_d$ by the Frobenius action $\alpha \mapsto \alpha^q$ on the roots of f.

Further, if we let $f_a(x) := f(x) + a$, the conjugacy classes σ_{f_a} (as $a \in \mathbb{F}_p$ ranges over elements such that f_a is squarefree) is the same as the Artin symbols $(\frac{L/K}{\mathfrak{p}_a})$ as $a \in \mathbb{F}_p$ ranges over elements for which the prime ideal $\mathfrak{p}_a := (t - a)$ is unramified, if we take $K = \mathbb{F}_p(t)$ and $L = L_0$ with notation as above (also note that $m = |G_{0,\mathrm{geom}}|$ in this case.)

We next collect some crucial facts about the Galois extensions introduced above. Given a finite extension $\mathbb{E}/\mathbb{F}_p$ it will be convenient to let $\mathrm{Frob}_{\mathbb{E}}$ denote the map $\alpha \to \alpha^{|\mathbb{E}|}$.

Proposition 9 ([17], Section 2)**.** *Let* $f \in M_d(\mathbb{F}_p)$. *Then*

(1) *For any* $h \in \mathbb{F}_p$, $l_h = l_0$ *and* $G_h \simeq G_0$.
(2) *If* $\mathbf{h} = (h_1, \ldots, h_k)$ *is such that* $h_i - h_j \notin B(f)$, *then the field extensions* $L_{h_1}/l(T), \ldots, L_{h_k}/l(T)$ *are linearly disjoint, where* $l = l_0$ *is the field of constants of* L^k. *In particular,*

$$G_{geom}^k = \prod_{i=1}^k G_{h_i,geom} \simeq (G_{0,geom})^k$$

(3) *For* $\mathbf{h} = (h_1, \ldots, h_k)$ *such that* $h_i - h_j \notin B(f)$, *let* $\mathcal{C} \subset G^k$ *be a conjugacy class of the form* $\mathcal{C} = \mathcal{C}_1 \times \ldots \mathcal{C}_k$, *where each* $\mathcal{C}_i$ *is the corresponding conjugacy class in* G_{h_i} *(i.e., where* $G^k < G_{h_1} \times \cdots \times G_{h_k}$ *and* $\mathcal{C}_i = \pi_i(\mathcal{C})$ *is the image of* $\mathcal{C}$ *under the* i*-th projection.) Then*

$$\left\{\gamma \in G^k : \gamma|_{l^k} = \mathrm{Frob}_{l^k}, \gamma|_{L_{h_i}} \in \mathcal{C}_{h_i}\ \forall i = 1, \ldots, k\right\}$$

is in $1-1$ *correspondence with*

$$\prod_{i=1}^{k} \{\gamma \in G_0 : \gamma|_l = \mathrm{Frob}_l, \gamma \in \mathcal{C}_i\}$$

which, if we let $\delta \in G_0$ *denote any element such that* $\delta|_l = \mathrm{Frob}_l$, *is in* $1-1$ *correspondence with*

$$\prod_{i=1}^{k} \left((\delta \cdot G_{0,geom}) \cap \mathcal{C}_i\right),$$

Proof. The proof of the proposition is the content of Lemma 5, Proposition 8, and (the proof of) Lemma 10 in [17]. We note that in Proposition 8 and Lemma 10, the first author shows that if $R_f+h_1, \dots, R_f+h_k$ are pairwise disjoint (more precisely, he considers $h_1 = 0$, and $F_h(x,t) = f(x)-(h+t)$, and therefore the sets are of the form $R_f - h_i$), then linear disjointedness holds, and from that also Lemma 10. We note that the sets are indeed pairwise disjoint if $h_i - h_j \notin B(f)$ for $i \neq j$. □

To prove independence when disjoint ramification does not hold, we need the following key result (cf. [13], Proposition 17 and Lemma 16.)

Proposition 10. *If* $f \in M_d(\mathbb{F}_p)$ *is a Morse polynomial and* $h_1, \dots, h_k \in \mathbb{F}_p$ *are distinct then* $G^k = S_d^k$ *provided that* $p > 4^{k+d-1} + 1$.

2.4. **Class functions.** As mentioned in the introduction, any class function on S_d can be viewed as an arithmetic class function on the set of squarefree polynomials in $M_d(\mathbb{F}_p)$; we then consider any bounded (by some absolute constant) extension to the set of all polynomials in $M_d(\mathbb{F}_p)$.

Proposition 11. *Let* $f \in M_d(\mathbb{F}_p)$, $d \geq 2$ *and let* ϕ *be a class function on* S_d. *Choose* $\gamma \in G_0$ *such that* $\gamma|_l$ *acts via* $\alpha \to \alpha^p$, *and let* $G_{0,geom}$ *denote the geometric part of* G_0. *Then*

$$\sum_{g \in I(f)} \phi(g) = c(\phi) \cdot p + O_d(\sqrt{p})$$

where

$$c(\phi) = \frac{1}{|G_{0,geom}|} \sum_{\sigma \in \gamma \cdot G_{0,geom}} \phi(\sigma)$$

Proof. The contribution from non-squarefree $g \in I(f)$ is $O_d(1)$ (cf. (9).) The result now follows from the Chebotarev density theorem. □

Remark: If f is Morse and $h \in \mathbb{F}_p$, then $G_{h,\text{geom}} = S_d$. In the non-Morse case, the set of possible constants $C(\phi, d)$ can be shown to only depend on ϕ and d by noting that $C(\phi, d)$ is a subset of

(10)
$$\left\{ \frac{1}{|H|} \sum_{\sigma \in \gamma H} \phi(\sigma) : \gamma \in S_d,\ H < S_d \text{ acts transitively on } \{1, \ldots, \mathrm{d}\} \right\}$$

As an immediate consequence of the Chebotarev density theorem we can give a more precise description of what the constants might be for several shifts, when independence is allowed to break down.

Proposition 12. *Let $\phi_1, \ldots, \phi_k$ be class functions on S_d and let $h_1, \ldots, h_k \in \mathbb{F}_p$ be distinct shifts. Choosing $\gamma \in G^k$ such that $\gamma|_{l^k}$ acts via $\alpha \to \alpha^p$, we have*

$$\sum_{g \in I(f)} \left(\prod_{i=1}^{k} \phi_i(g + h_i) \right) = c \cdot p + O_{d,k}(\sqrt{p})$$

where

$$c = \frac{1}{|G^k_{geom}|} \cdot \sum_{\sigma \in \gamma \cdot G^k_{geom}} \left(\prod_{i=1}^{k} \phi_i(\sigma_i) \right),$$

and $(\sigma_1, \ldots, \sigma_k) \in S_d^k$ denotes the image of $\sigma \in G^k$ under the natural inclusion $G^k \hookrightarrow S_d^k$.

Remark. *In order to go beyond factorization patterns (to distinguish conjugacy classes having the same factorization pattern), note that the proof gives a slightly more general version of Proposition 12, where $\phi_1, \ldots, \phi_k$ are class functions on $G_{h_1}, \ldots, G_{h_k}$, and using the inclusion $G^k \subset G_{h_1} \times G_{h_2} \times \cdots \times G_{h_k}$ to map $\sigma \in G^k$ to $(\sigma_1, \ldots, \sigma_k) \in G_{h_1} \times G_{h_2} \times \cdots \times G_{h_k}$.*

3. Proofs of Theorems 3 and 4

We begin with proving Theorem 3. The first part of the Theorem is an immediate corollary of Propositions 6 and 11. Indeed, for $f \in M_d(\mathbb{F}_p)$ Morse, $G_0 = G_{0,\text{geom}} = S_d$, and the sums in Theorem 3 and in Proposition 11 are the same. As for the second part, for p sufficiently large, Proposition 10 gives that $G^k = G^k_{\text{geom}} = S_d^k$. By Proposition 12,

$$\sum_{g \in I(f)} \left(\prod_{i=1}^{k} \phi_i(g + h_i) \right) = c \cdot p + O_{d,k}(\sqrt{p})$$

where

$$c = \frac{1}{|S_d^k|} \cdot \sum_{\sigma \in S_d^k} \left(\prod_{i=1}^{k} \phi_i(\sigma_i) \right) = \prod_{i=1}^{k} c(\phi_i),$$

and $c(\phi_i) = \frac{1}{|S_d|} \sum_{\sigma \in S_d} \phi_i(\sigma)$ for $i = 1, \dots k$.

The proof of Theorem 4 is similar. The first part follows from Proposition 11; letting $c_i = \frac{1}{|G_{0,\mathrm{geom}}|} \sum_{\sigma \in \tilde{\gamma} \cdot G_{0,\mathrm{geom}}} \phi_i(\sigma)$ it is clear that $C(\phi_i, d)$, the set of possible values of c_i, is clearly a subset of the finite set given in (10). As for the second part, we note that, by part (2) of Proposition 9, $G_{\mathrm{geom}}^k = (G_{0,\mathrm{geom}})^k$ and it follows that the constant in front of p is

$$c = \frac{1}{|G_{\mathrm{geom}}^k|} \cdot \sum_{\sigma \in \gamma \cdot G_{\mathrm{geom}}^k} \left(\prod_{i=1}^{k} \phi_i(\sigma_i) \right) =$$

$$= \frac{1}{|G_{0,\mathrm{geom}}|^k} \prod_{i=1}^{k} \left(\sum_{\sigma \in \tilde{\gamma} \cdot G_{0,\mathrm{geom}}} \phi_i(\sigma) \right) = \prod_{i=1}^{k} c_i,$$

where $\gamma \in G^k$ is some element such that $\gamma|_{l^k} = \mathrm{Frob}_{l^k}$, and $\tilde{\gamma}$ denotes the image of γ under the projection from G^k to G_0.

4. Proof of Theorem 1

Recall that $f \in M_d(\mathbb{F}_p)$ denotes a Morse polynomial. We begin by showing that the characteristic function on prime polynomials is a class function. With

$$1_{d\text{-cycle}}(\sigma) = \begin{cases} 1 & \sigma = (i_1 \cdots i_d) \text{ is a } d\text{-cycle} \\ 0 & \text{otherwise} \end{cases}$$

the function

$$\phi(f) = \begin{cases} 1_{d\text{-cycles}}(\sigma_f) & f \text{ is squarefree} \\ 0 & \text{otherwise} \end{cases}$$

on $M_d(\mathbb{F}_p)$ is a class function, which equals 1_{Prime} since a polynomial is irreducible if and only if σ_f is a d-cycle. Hence $c(1_{\mathrm{Prime}})$ is the density of d-cycles in S_d, namely $\frac{1}{d}$, and Theorem 1 now follows from Theorem 3.

In a similar way, the "Titchmarsh divisor problem", and the "shifted divisor problem" for very short intervals $I(f)$ may be treated. The former consider sums of the form

$$\sum_{g \in I(f)} 1_{\mathrm{Prime}} d_r(f+h)$$

where $d_r(f)$ is the number of ways to decompose f as a product of r monic polynomials, and the latter concerns sums of the form

$$\sum_{g\in I(f)} d_{r_1}(f+h_1)\cdots d_{r_k}(f+h_k)$$

where $r_1,\dots,r_k$ are positive integers, and $h_1,\dots h_k\in\mathbb{F}_p$ are distinct. Once again, $d_r(f)$ is a class function, since for f squarefree, $d_r(f)=d_r(\sigma_f)$, where $d_r(\sigma)$ is the number of ways to decompose the permutation σ as a product of r disjoint cycles (here we allow for empty cycles.) We can therefore apply Theorem 3 for these sums and get that for distinct $h_1,\dots,h_k\in\mathbb{F}_p$,

$$\sum_{g\in I(f)} d_{r_1}(f+h_1)\cdots d_{r_k}(f+h_k)=\prod_{i=1}^{k}\binom{n+r_i-1}{r_i-1}p+O(p^{1/2}) \tag{11}$$

(the constants are derived in [1, Lemma 2.2]), and for all nonzero $h\in\mathbb{F}_p$

$$\sum_{g\in I(f)} 1_{\text{Prime}}\cdot d_r(f+h)=\frac{1}{n}\binom{n+r-1}{r-1}p+O(p^{1/2}). \tag{12}$$

5. Möbius and Chowla type sums in very short intervals

In this section we give proofs of Theorems 2 and 5. We begin with a discussion of the Möbius μ function for function fields.

Given a polynomial $f\in M_d(\mathbb{F}_p)$, let $\omega(f)$ denote the number of distinct irreducible divisors of f. It is natural to define the function field Möbius μ-function by $\mu(f):=(-1)^{\omega(f)}$ for f squarefree; otherwise we set $\mu(f)=0$. For p large and $f\in M_d(\mathbb{F}_p)$, essentially all $g\in I(f)$ are squarefree (cf. (9)), and hence μ is a class function in the sense previously discussed.

Given $\sigma\in S_d$, let $c(\sigma)$ denote the number of cycles in the cycle representation of σ, *including all* 1*-cycles*, e.g., for $(12)\in S_4$ we write $(12)=(12)(3)(4)$ and find that $c(\sigma)=3$. Thus $\mu(f)$, for f squarefree, is given by $(-1)^{c(\sigma_f)}$. It is convenient to abuse notation and define $\mu(\sigma):=(-1)^{c(\sigma)}$ for $\sigma\in S_d$. It turns out that $(-1)^{c(\sigma)}$ is closely related to $\operatorname{sgn}(\sigma)$, the sign of σ regarded as a permutation:

$$\mu(\sigma)=(-1)^{c(\sigma)}=(-1)^d\cdot\operatorname{sgn}(\sigma)$$

To see this consider the disjoint cycle decomposition $\sigma=\prod_{i=1}^{L}c_i$ (including one-cycles). We then have $\mu(\sigma)=(-1)^L$. Now, with L_1 denoting the number of even length cycles, and L_2 the number of odd length cycles, we trivially have $L=L_1+L_2$ and moreover that $\operatorname{sgn}(\sigma)=(-1)^{L_1}$. As the sum of the length of all cycles $c_1,\dots,c_L$ equals

d (here it is crucial to include one-cycles), we find that L_2 and d has the same parity. Hence

$$\operatorname{sgn}(\sigma) = (-1)^{L_1} = (-1)^{L_1+L_2+d} = (-1)^{L+d} = \mu(\sigma)(-1)^d$$

and we find that $\mu(\sigma) = \pm \operatorname{sgn}(\sigma)$, where the sign is given by the parity of d.

Now, if f is Morse, we have $G_0 = G_{\text{geom}} = S_d$, hence (cf. Theorem 4

$$c(\mu) = \frac{1}{|G|}\sum_{\sigma\in G_0}\mu(\sigma) = \frac{(-1)^d}{|S_d|}\sum_{\sigma\in S_d}\operatorname{sgn}(\sigma) = 0.$$

Thus Theorem 2 immediately follows from Theorem 3.

5.1. **The non-Morse case.** We begin by characterizing short intervals on which there is no cancellation in the sum $\sum_{g\in I(f)}\mu(g)$. Fix $\gamma \in G_0$ such that $\gamma|_l$ acts as $\alpha \to \alpha^p$.

First case: We begin by considering the case $G_{0,\text{geom}} \subset A_d$ (with $A_d \subset S_d$ denoting the alternating group.) Since μ is a class function, (6) gives that

$$c(\mu) = \frac{1}{|G_{0,\text{geom}}|}\sum_{\sigma\in\gamma\cdot G_{0,\text{geom}}}\mu(\sigma)$$

and since sgn is trivial on $G_{0,\text{geom}} \subset A_d$, we find that $\mu(g)$ has *constant sign* for $g \in I(f)$, with the possible exception of $O(1)$ non-squarefree g. Hence $|\sum_{g\in I(f)}\mu(g)| = p + O_d(\sqrt{p})$.

Second case: If $G_{0,\text{geom}}$ is not contained in A_d, there exist at least one odd permutation $\tau \in G_{0,\text{geom}}$; in particular, $\sum_{\sigma\in G_{0,\text{geom}}}\operatorname{sgn}(\sigma) = 0$. Thus,

$$c(\mu) = \frac{1}{|G_{0,\text{geom}}|}\sum_{\sigma\in\gamma G_{0,\text{geom}}}\mu(\sigma) = \frac{(-1)^d\operatorname{sgn}(\gamma)}{|G_{0,\text{geom}}|}\sum_{\sigma\in G_{0,\text{geom}}}\operatorname{sgn}(\sigma) = 0,$$

and hence Theorem 3 gives that

$$\sum_{g\in I(f)}\mu(g) = O(\sqrt{p})$$

In summary, there is (square root) cancellation in $\sum_{g\in I(f)}\mu(g)$ if and only if there is sign cancellation in $\sum_{\sigma\in G_{0,\text{geom}}}\operatorname{sgn}(\sigma)$.

5.1.1. *Cancellation in Chowla sums.* We first note that if $h_1,\dots,h_k \in \mathbb{F}_p$ are distinct elements such that $h_i - h_j \notin B(f)$ ("the uncorrelated case"), Theorem 5 follows immediately from Theorem 4.

If $h_i - h_j \in B(f)$ ("the correlated case") we argue as follows. As we have seen, no cancellation in the Möbius sum $\sum_{g\in I(f)}\mu(g+h_1)$ (which in turn happens if and only if there is no cancellation in the unshifted

sum $\sum_{g\in I(f)}\mu(g)$, or in any other shifted sum $\sum_{g\in I(f)}\mu(g+h_i)$, $i=2,\dots,k$) is equivalent to $G_{h_i,\mathrm{geom}}\subset A_d$ for all i. In particular, $G^k_{\mathrm{geom}}\subset\prod_{i=1}^k G_{h_i,\mathrm{geom}}\subset A_d^k$. Since $\sum_{g\in I(f)}\prod_{i=1}^k\mu(g+h_i)=c\cdot p+O_{d,k}(\sqrt{p})$ where

$$c=\frac{1}{|G^k_{\mathrm{geom}}|}\cdot\sum_{(\sigma_1,\dots,\sigma_k)\in\gamma\cdot G^k_{\mathrm{geom}}}\left(\prod_{i=1}^k\mu(\sigma_i)\right),$$

(cf. Proposition 12 and use the natural embedding $G^k\hookrightarrow S_d^k$) we find that there is no cancellation in the Chowla sum.

On the other hand, if there is cancellation in the short Möbius sum, there must be some odd permutation in $G_{h_1,\mathrm{geom}}$, and this in fact implies that the same holds for G^k_{geom}, provided p is sufficiently large (in terms of k.) To see this, define $R_{\mathrm{odd}}\subset R_f$ as the set of critical values of f giving rise to odd permutations in $G_{h_1,\mathrm{geom}}$. Then, as $G_{h_1,\mathrm{geom}}$ is generated by the inertia subgroups of points outside ∞, and their conjugates (cf. [25, Proposition 4.4.6]), R_{odd} is nonempty. By [13, Lemma 16] (in particular, take $H=\{-h_1,-h_2,\dots,-h_k\}$, $S=R_{\mathrm{odd}}$ and note that we may assume that $p>4^{k+d}\geq 4^{k+|R_{\mathrm{odd}}|}$ since the implied constants in the error terms are allowed to depend on d and k) there must be some element in the multi-set generated by $R_{\mathrm{odd}}+h_1,\dots,R_{\mathrm{odd}}+h_k$ that has *odd* parity, and hence G^k_{geom} contains an odd element given by a product of an odd number of odd permutations. Thus the elements of G^k_{geom} do not have constant sign, and hence there is square root cancellation in the Chowla sum also in this case.

To see that $G_{0,\mathrm{geom}}\subset A_d$ does indeed occur (for p large and d fixed; for interesting examples when $p|d$, see [6]), we can take $f(x)=x^l$ and $p\equiv 1 \mod l$ for some odd prime l; then $G=G_{\mathrm{geom}}$ is cyclic of order l, and all nontrivial elements are given by *even* l-cycles.

6. Examples of degenerate intervals — further details

6.1. **Prime density fluctuations.** We take $f(x)=x^3$, $\phi_1=\phi_2=1_{\mathrm{Prime}}$. As $I(f)=\{x^3-t,t\in\mathbb{F}_p\}$ it is enough to consider splitting patterns of $x^3-t=0$. For primes $p\equiv 1 \mod 3$, x^3-t has either zero or three roots in $\mathbb{F}_p$; the latter happens if and only if t is a cube of some element in $\mathbb{F}_p$, and there are $1+(p-1)/3$ such elements. Hence $c(1_{\mathrm{Prime}},p)=2/3$ for $p\equiv 1 \mod 3$. On the other hand, for $p\equiv 2 \mod 3$, the map $x\to x^3$ is a permutation of the elements in $\mathbb{F}_p$, hence $x^3-t=0$ has one root in $\mathbb{F}_p$ no matter what t is. In particular, $c(1_{\mathrm{Prime}},p)=0$ for $p\equiv 2 \mod 3$.

Since x^3 only has one critical value, $|R_f| = 1$ and hence $(h_1 + R_f) \cap (h_2 + R_f) = \emptyset$ unless $h_1 = h_2$; in particular $B(f) = (R_f - R_f) \setminus \{0\} = \emptyset$, and (7) follows from Theorem 4.

6.2. **Breakdown of independence of primes.** Take $f(x) = x^4 - 2x^2$, and let p be a large prime. The following was shown in [13, Section 4.2]: $G \simeq D_4$, and for $h_1 = 0, h_2 = 1$, we have $G^2 = \mathrm{Gal}(L^2/\mathbb{F}_p(T))$ (where L^2 denotes the compositum $L_{h_1}L_{h_2}$), and G^2 genuinely depends on p. Namely, for $p \equiv 3 \mod 4$ we have $G^2 \simeq D_4 \times D_4$, whereas for $p \equiv 1 \mod 4$, $G^2 = G^2_{\mathrm{geom}} = H$ is a certain index two subgroup of $D_4 \times D_4$. More precisely,

$$H = \langle (6,7), (2,3)(5,6)(7,8), (1,2)(3,4) \rangle \subset D_4 \times D_4,$$

where we have identified the first copy of D_4 as permutation of $\{1,2,3,4\}$, and the second copy as a permutation of $\{5,6,7,8\}$. As

$$D_4 = \{(1,4)(2,3), (1,3)(2,4), (1,3), (2,4), (1,2)(3,4), (1,2,3,4), (1,4,3,2)\}$$

(note that D_4 contains exactly two 4-cycles) the Chebotarev density theorem gives that

$$c(1_{\mathrm{Prime}}) = 2/|D_4| = 2/8 = 1/4$$

A tedious but straightforward calculation gives that $|H| = 32$ and that there are exactly four elements in H corresponding to both $f(x)+t$ and $f(x) + 1 + t$ being prime for $t \in \mathbb{F}_p$, namely $(1,3,4,2)(5,7,8,6)$, $(1,3,4,2)(5,6,8,7)$, $(1,2,4,3)(5,6,8,7)$, and $(1,2,4,3)(5,7,8,6)$. Hence the "twin prime density" for the shift $h = 1$ equals $4/|H| = 4/32 = 1/8 \neq 1/4^2$. Similarly, the density for the shift $h = -1$ also equals $1/8$.

As mentioned above, for $p \equiv 3 \mod 4$, the compositum L^2 of L_0 and L_1 was shown to have maximal Galois group, namely $G^2 \simeq D_4 \times D_4$; further the field of constants of the compositum was shown to equal $\mathbb{F}_p[i]$ (where $i^2 = 1$). Thus, if $\sigma \in G$ is any element such that $\sigma(i) = -i$, we find that Frobenius takes values in the coset $\sigma H \subset D_4 \times D_4$. In particular, as all elements of G consisting of two 4-cycles in $D_4 \times D_4$ are contained in H, there are no such elements in the coset σH. Consequently the Chebotarev density for $(g, g+1)$ both being prime is *zero* for $p \equiv 3 \mod 4$ and $g \in I(f)$ (even though $c(1_{\mathrm{Prime}}) = 1/4$.)

On the other hand, the critical points of f (i.e., zeros of f') are $\{0, -1, 1\}$, and thus the critical values of f are given by $R_f = \{0, -1\}$. Hence $B(f) = (R_f - R_f) \setminus \{0\} = \{-1, 1\}$, and thus Theorem 4 gives independence in the sense that the simultaneous prime density for $g, g+h$ equals $1/4^2$ for $h \neq 0, \pm 1$ and $g \in I(f)$.

The "coincidence" of getting the expected twin prime density when averaging over all primes p can be explained as follows. We lift the

setup to $\mathbb{Q}$ and consider $G = \mathrm{Gal}(f(x)+t, f(x)+1+t/\mathbb{Q}(t))$. Then $G \simeq D_4 \times D_4$, and the constant field extension is $\mathbb{Q}(i)$. Thus, if we first average over primes p, and then over $t \in \mathbb{F}_p$, the Frobenius element equidistributes in all of G (for $p \equiv 1 \mod 4$ it equidistributes in H, and for $p \equiv 3 \mod 4$ it equidistributes in the nontrivial coset of H, and G is the union of these two cosets.) In particular, as there are 4 elements in G whose cycle structure corresponds two simultaneous prime specialization, we find that the p-averaged twin prime density equals $4/|G| = 4/64 = 1/4^2$, "as expected".

7. The large q limit

The previous results can be extended to the setting of very short intervals in $M_d(\mathbb{F}_q)$ for $q = p^l$ as long as p grows (the key point is that the proof of Lemma 16 in [13] also works for $\mathbb{F}_q$ provided p is sufficiently large).

The setting of p fixed and letting l grow is more complicated. We first note there is an obvious obstruction to $f(x) + sx$ being Morse for *any* value of $s \in \mathbb{F}_q$ in case $p|\deg(f)$ — clearly $\deg(f') < d-1$ and hence there are at most $d-2$ critical values. However, even if we assume $(\deg(f), p) = 1$ there are other obstructions for the the Galois group being maximal (i.e., that $G^k_{\mathrm{geom}} = S_d^k$), *even though* $G_{h_i} = S_d$ for $1 \le i \le k$. For example, consider the family $f_s(x) = x^3 + sx$ for $s \in \mathbb{F}_q$ where $q = p^l$ and $p > 3$ is fixed. For all but $O(1)$ choices of s, $f_s(x)$ is Morse, and $f_s'(x) = 3x^2 + s$ is a quadratic with two distinct roots in $\mathbb{F}_{q^2}$, and it is easy to see that $R_{f_s} = \{\alpha_s, -\alpha_s\}$ for some $\alpha_s \in \mathbb{F}_{q^2}$. Taking $k = p$ and letting $h_i = i\alpha_s$ for $1 \le i \le k$, we find that the multiset-union of $R + h_1, R + h_2, \dots, R + h_k$, as a set is a linear $\mathbb{F}_p$-subspace in $\mathbb{F}_{q^2}$, with each element having multiplicity two (since $|R| = 2$). Consequently G^k_{geom} contains only *even* permutations. In particular, the equivalence between cancellation in Möbius sums and Chowla sums (cf. Theorem 5) does not hold in the large q limit. A more subtle example of independence breaking down can also be given. For $f(x) = x^4 + x^3 + 3x^2 \in M_4(\mathbb{F}_7)$, the critical values are given by $R = \{0, 1, 3\}$; taking $(h_1, \dots, h_4) = (0, 1, 2, 4)$ we find that the multiset union of $h_i + R$ has multiplicity two on its support. This type of example cannot occur for p large, but if we fix p and consider polynomials of the form $f_s(x) = f(x) + sx$, $s \in \mathbb{F}_{7^l}$ for growing l, it is clear that the above phenomena occur at least once (for $s = 0$.) However, if we *fix* $h_1, \dots, h_k$, in some extension of $\mathbb{F}_p$, this can only happen for $O_{d,k}(1)$ values $s \in \overline{\mathbb{F}_q}$ (but note that this set of "exceptional" s-values depends on the shifts $h_1, \dots, h_k$.)

Theorem 13. *Fix distinct elements $h_1,\dots,h_k \in \overline{\mathbb{F}_p}$, and let $f_0 \in M_d(\overline{\mathbb{F}_p})$ with $(p, d(d-1)) = 1$, and let $q = p^l$ for some $l \geq 1$ large enough so that $f_0 \in \mathbb{F}_q[x]$ and $h_1,\dots,h_k \in \mathbb{F}_q$. Given $s \in \mathbb{F}_q$, let $f_s(x) = f_0(x) + sx$ and for $i = 1,\dots,k$, let $K_i/\mathbb{F}_q(t)$ denote the field extension generated by $f_s(x)+h_i+t$, let L_i denote the Galois closure of K_i, and let L^k denote the compositum of $L_1,\dots,L_k$. Then, for all but $O_{d,k}(1)$ values of $s \in \mathbb{F}_q$, f_s is Morse, and we have $\mathrm{Gal}(L^k/\mathbb{F}_q(t)) \simeq S_d^k$.*

Before giving the proof of Theorem 13 we deduce an immediate corollary, namely a somewhat weaker "large q" analogue of Theorems 1, 2 and 3. To do so we need some additional notation: given $f \in M_d(\mathbb{F}_q)$, let $I_{\mathbb{F}_q}(f) := \{f(x) + a : a \in \mathbb{F}_q\}$, and as usual, for $s \in \mathbb{F}_q$ let $f_s(x) = f(x) + sx$.

Corollary 14. *Fix distinct elements $h_1,\dots,h_k \in \overline{\mathbb{F}_p}$, and let $f_0 \in M_d(\overline{\mathbb{F}_p})$ with $(p, d(d-1)) = 1$. There exists a subset $S_{bad} \subset \overline{\mathbb{F}_p}$, depending on f_0 and $h_1,\dots,h_k$, with the following properties:*

1. *$|S_{bad}| = O_{d,k}(1)$.*
2. *Let $q = p^l$ be any prime power such that $h_1,\dots,h_k \in \mathbb{F}_q$ and $f_0 \in \mathbb{F}_q[x]$. Then, for $s \in \mathbb{F}_q \setminus S_{bad}$, Theorems 1, 2, and 3 hold for the very short interval $I_{\mathbb{F}_q}(f_s)$. For example, if $s \in \mathbb{F}_q \setminus S_{bad}$, then*

$$|\{g \in I_{\mathbb{F}_q}(f_s) : \ g+h_1,\dots,g+h_k \text{ are irreducible }\}| = \frac{q}{d^k} + O_{d,k}(\sqrt{q}),$$

and

$$\sum_{g \in I_{\mathbb{F}_q}(f_s)} \left(\prod_{i=1}^{k} \mu(g+h_i) \right) = O_{d,k}(\sqrt{q}).$$

As for the proof of Theorem 13, we first show that critical values having constant difference is a rare occurrence.

Proposition 15. *Let $f \in M_d(\mathbb{F}_q)$ where $q = p^l$, and assume that $p \nmid d(d-1)$. With s transcendental over $\overline{\mathbb{F}_p}$, denote $f_s(x) := f(x) + sx$, and let τ_1, τ_2 be distinct roots of $f_s'(x) = f'(x) + s = 0$. Then $f_s(\tau_1) - f_s(\tau_2) \notin \overline{\mathbb{F}_p}$.*

Proof. Assume by contradiction that $c = f_s(\tau_1) - f_s(\tau_2) \in \overline{\mathbb{F}_p}$, and define $\mathbb{E} = \mathbb{F}_q(c)$. Now, $f_s(x) = f(x) + sx$ and $f_s'(x) = f'(x) + s$ are irreducible polynomials over $\mathbb{E}(s)$, so for both $i = 1, 2$, $[\mathbb{E}(\tau_i) : \mathbb{E}(s)] = d - 1$, and $[\mathbb{E}(\tau_i) : \mathbb{E}(f_s(\tau_i))] = d$. Since the degrees of both extensions are co-prime we find that $\mathbb{E}(\tau_i) = \mathbb{E}(s, f_s(\tau_i))$, and thus, since we assume that $f_s(\tau_1) = f_s(\tau_2) + c$, we find that $\mathbb{E}(\tau_1) = \mathbb{E}(\tau_2)$.

This implies that there exist $A, B, C, D \in \mathbb{E}$ such that $\tau_2 = \frac{A\tau_1+B}{C\tau_1+D}$. We claim that $C = 0$, otherwise (note that $f'(\tau_i) = -s$ for $i = 1, 2$)

(13)
$$f(\tau_1)-f'(\tau_1)\tau_1 = f(\tau_1)+s\tau_1 = f_s(\tau_1) = f_s(\tau_2)+c = f(\tau_2)+s\tau_2+c = f(\tau_2) - f'(\tau_2)\tau_2 + c = f(\frac{A\tau_1+B}{C\tau_1+D}) - \frac{A\tau_1+B}{C\tau_1+D}f'(\frac{A\tau_1+B}{C\tau_1+D}) + c,$$

and after clearing denominators we find that τ_1 is a root of a polynomial of degree $2d$ (here we use $p \nmid d-1$ so that $\deg(f(x)-xf'(x)) = d$), with coefficients in $\overline{\mathbb{F}_p}$, contradicting that τ_1 is transcendental. Therefore $C = 0$, and thus $\tau_2 = A\tau_1 + B$ for some $A, B \in \mathbb{E}$. Denote $h(x) = f(x) - xf'(x)$. Then $h(x) - c = h(Ax + B)$. Let R_h be the multiset of critical values of h, and A_h the set of critical points of h. For any $a \in A_h$, $(a-B)/A$ is a critical point of $h(Ax+B)$, and $h(a)$ is a critical value of $h(Ax + B)$. Therefore R_h is the multiset of critical values also for $h(Ax+B)$. On the other hand, by the equality $h(x)-c = h(Ax+B)$, we find that $R_h = R_h - c$. By [15] (cf. Claim D' in the proof of Proposition 4.3), critical values are distinct and hence $c \neq 0$. We thus find that there exists a nontrivial $\mathbb{F}_p$-action on the multiset R_h, and therefore p divides the multiset cardinality of R_h, i.e., p divides $\deg(h') = d - 1$, contradicting the assumption that $p \nmid d - 1$. □

Corollary 16. *For $f \in M_d(\mathbb{F}_q)$ such that $(q, d(d-1)) = 1$, and any set of k distinct elements $H = \{h_1, \dots, h_k\} \subset \mathbb{F}_q$, the set $B(f_s) \cap (H - H)$ is empty for all but $O_{d,k}(1)$ values of s, where $B(f_s) = (R_{f_s} - R_{f_s}) \setminus \{0\}$.*

Proof. By Proposition 15, for s transcendental over $\mathbb{F}_p$, $h_i \neq h_j$, and $\tau_i \neq \tau_j$ denoting any two distinct roots of $f_s'(x)$,

$$f_s(\tau_i) - f_s(\tau_j) - (h_i - h_j) \neq 0$$

Let

$$\Pi(s) := \prod_{h_i \neq h_j} \prod_{\tau_i \neq \tau_j} (f_s(\tau_i) - f_s(\tau_j) - (h_i - h_j))$$

Then $\Pi(s) \neq 0$, and as $\Pi(s)$ is a symmetric polynomial in the roots of $f_s'(x) = 0$, it is a polynomial in s, of degree bounded in terms of d and k. Since $B(f_s) \cap (H - H) \neq \emptyset$ is equivalent to $\Pi(s) = 0$, the result follows. □

Theorem 13 now follows easily as the extensions $L_1, \dots, L_k$ are linearly disjoint by Corollary 16.

References

[1] J. C. Andrade, L. Bary-Soroker, and Z. Rudnick. Shifted convolution and the titchmarsh divisor problem over $\mathbb{F}_q[t]$. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 373(2040), 2015.

[2] E. Bank and L. Bary-Soroker. Prime polynomial values of linear functions in short intervals. *Journal of Number Theory*, 151(Supplement C):263 – 275, 2015.

[3] E. Bank, L. Bary-Soroker, and L. Rosenzweig. Prime polynomials in short intervals and in arithmetic progressions. *Duke Math. J.*, 164(2):277–295, 02 2015.

[4] L. Bary-Soroker. Hardy–littlewood tuple conjecture over large finite fields. *International Mathematics Research Notices*, 2014(2):568–575, 2014.

[5] D. Carmon. The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field in characteristic 2. *Philos. Trans. Roy. Soc. A*, 373(2040):20140311, 14, 2015.

[6] D. Carmon and Z. Rudnick. The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field. *Q. J. Math.*, 65(1):53–61, 2014.

[7] S. Chowla. *The Riemann Hypothesis and Hilbert's Tenth Problem*. Mathematics and its applications. Gordon and Breach, 1987.

[8] S. D. Cohen. The distribution of polynomials over finite fields. *Acta Arith.*, 17:255–271, 1970.

[9] S. D. Cohen. Uniform distribution of polynomials over finite fields. *J. London Math. Soc. (2)*, 6:93–102, 1972.

[10] A. Entin. Monodromy of Hyperplane Sections of Curves and Decomposition Statistics over Finite Fields. *International Mathematics Research Notices*, 2021(14):10409–10441, 07 2019.

[11] A. Entin. On the Bateman-Horn conjecture for polynomials over large finite fields. *Compos. Math.*, 152(12):2525–2544, 2016.

[12] M. Fried and M. Jarden. *Field Arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics. Springer Berlin Heidelberg, 2006.

[13] A. Granville and P. Kurlberg. Poisson statistics via the chinese remainder theorem. *Advances in Mathematics*, 218(6):2013 – 2042, 2008.

[14] D. Hilbert. Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten. *J. Reine Angew. Math.*, 110:104–129, 1892.

[15] M. Jarden and A. Razon. Skolem density problems over large. In *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry: Workshop on Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry, November 2-5, 1999, Ghent University, Belgium*, volume 270, page 213. American Mathematical Soc., 2000.

[16] J. Keating and Z. Rudnick. Squarefree polynomials and möbius values in short intervals and arithmetic progressions. *Algebra Number Theory*, 10(2):375–420, 2016.

[17] P. Kurlberg. Poisson spacing statistics for value sets of polynomials. *International Journal of Number Theory*, 05(03):489–513, 2009.

[18] P. Kurlberg and L. Rosenzweig. The chebotarev density theorem for function fields — incomplete intervals. *Finite Fields and Their Applications*, 73:101838, 2021.
[19] W. Li. *Number Theory with Applications*. Series on University Mathematics. 1996.
[20] P. Pollack. Simultaneous prime specializations of polynomials over finite fields. *Proc. Lond. Math. Soc. (3)*, 97(3):545–567, 2008.
[21] Z. Rudnick. Some problems in analytic number theory for polynomials over a finite field. In *Proc. International Congress of Math (Seoul)*, volume 2, pages 443–460.
[22] A. Selberg. On the normal density of primes in small intervals, and the difference between consecutive primes. *Arch. Math. Naturvid.*, 47(6):87–105, 1943.
[23] W. Sawin and M. Shusterman. On the chowla and twin primes conjectures over $\mathbb{F}_q[t]$, 2018.
[24] W. Sawin and M. Shusterman. Möbius cancellation on polynomial sequences and the quadratic bateman–horn conjecture over function fields. *Inventiones mathematicae*, pages 1–177, 2022.
[25] J.-P. Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. Jones and Bartlett Publishers, Boston, MA, 1992.
[26] A. Weil. *Basic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013.

URL: `www.math.kth.se/~kurlberg`

Department of Mathematics, KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
Email address: `kurlberg@math.kth.se`

Unit of Mathematics, Afeka Tel Aviv College of Engineering, Mivtza Kadesh 38, Tel Aviv, Israel
Email address: `liorr@afeka.ac.il`