

THE CHEBOTAREV DENSITY THEOREM FOR FUNCTION FIELDS — INCOMPLETE INTERVALS

PÄR KURLBERG, LIOR ROSENZWEIG

ABSTRACT. We prove a Pólya-Vinogradov type variation of the Chebotarev density theorem for function fields over finite fields valid for “incomplete intervals” $I \subset \mathbb{F}_p$, provided $(p^{1/2} \log p)/|I| = o(1)$. Applications include density results for irreducible trinomials in $\mathbb{F}_p[x]$, i.e. the number of irreducible polynomials in the set $\{f(x) = x^d + a_1x + a_0 \in \mathbb{F}_p[x]\}_{a_0 \in I_0, a_1 \in I_1}$ is $\sim |I_0| \cdot |I_1|/d$ provided $|I_0| > p^{1/2+\epsilon}$, $|I_1| > p^\epsilon$, or $|I_1| > p^{1/2+\epsilon}$, $|I_0| > p^\epsilon$, and similarly when x^d is replaced by any monic degree d polynomial in $\mathbb{F}_p[x]$. Under the above assumptions we can also determine the distribution of factorization types, and find it to be consistent with the distribution of cycle types of permutations in the symmetric group S_d .

1. INTRODUCTION

The distribution of primes, and more generally the distribution of factorization types, in “short intervals” in the setting of function fields over finite fields has received considerable attention [5, 6, 3, 2, 14]. For example, in [3], prime equidistribution for the family $\{f(x) + bx + a\}_{a,b \in \mathbb{F}_p}$ was shown for $f \in \mathbb{F}_p[x]$ any monic degree d polynomial (for p large.) For “very short” intervals, i.e., one parameter families of the form $\{f(x) + a\}_{a \in \mathbb{F}_p}$, prime equidistribution does not hold for all f . However, for f suitably “generic”, prime equidistribution does in fact hold for very short intervals. In [14] it was shown that given a monic degree d “Morse polynomial” $f(x) \in \mathbb{F}_p[x]$ (i.e., that $|\{f(\xi) : f'(\xi) = 0\}| = d - 1$; note this holds for generic polynomials, cf. Section 5.1)

$$(1) \quad |\{a \in \mathbb{F}_p : f(x) + a \text{ irreducible}\}| = p/d + O_d(p^{1/2}).$$

More generally, the distribution of factorization types of $f(x) + a$ can also be determined. Writing $f(x) = \prod_{i=1}^l f_i(x)$ with $f_i \in \mathbb{F}_p[x]$ all irreducible and letting $d_i = \deg(f_i)$ we may after rearranging assume that $1 \leq d_1 \leq d_2 \dots \leq d_l$; the *factorization type* (or decomposition type) of f is then given by (d_1, \dots, d_l) . The distribution of factorization

Date: July 3, 2020.

P.K. was partially supported by the Swedish Research Council (2016-03701).

types of $f(x) + a$, for f Morse, is consistent (up to an error of size $O_d(p^{-1/2})$) with the distribution of cycle types of permutations in S_d , the symmetric group on d letters, with respect to the Haar measure. (E.g., for $\sigma = (12) \in S_3$, write out all trivial cycles, i.e., $\sigma = (12)(3)$; the *cycle type* of σ is then $(1, 2)$ if we order according to cycle lengths.)

The connection between factorization types and group theory proceeds via Galois theory and the function field version of the Chebotarev density theorem, made effective by Weil's proof of the Riemann hypothesis for curves. The key point is that for $f(x)$ Morse, $\text{Gal}(f(x) + t/\mathbb{F}_p(t)) \simeq S_d$ and the factorization type for $f(x) + a$ can be read off from the cycle type of the Frobenius class at the prime ideal $(t - a) \subset \mathbb{F}_p[t]$. In particular, $f(x) + a$ being irreducible is equivalent to the Frobenius conjugacy class at the prime $(t - a)$ being generated by a d -cycle, and the proportion of d -cycles in S_d is $1/d$, hence the density $1/d$ in (1).

The purpose of this paper is to show that equidistribution of factorization types also holds for significantly smaller subsets, namely for “incomplete intervals” $I \subset \mathbb{F}_p$, as long as $(p^{1/2} \log p)/|I|$ is small. In fact, in spirit of the Pólya-Vinogradov inequality, we will develop a version of the Chebotarev density theorem for incomplete intervals, allowing us to determine the distribution of Artin symbols, and thus resolve finer invariants than factorization types when $\text{Gal}(f(x) + t/\mathbb{F}_p(t))$ is not the full symmetric group. (Note that the cycle type is in general not enough to determine the conjugacy class, e.g., the three-cycles (123) and (132) are not conjugate in the alternating group A_3 .)

Before stating our main result we introduce some notations. Let p be a (large) prime, let $K := \mathbb{F}_p(t)$, let L/K be a finite normal and separable extension with Galois group $\text{Gal}(L/K)$, and let $O_K = \mathbb{F}_p[t]$ denote the ring of integers in K . Given a prime ideal $\mathfrak{p} \subset O_K$ that does not ramify in L , let $\left(\frac{L/K}{\mathfrak{p}}\right)$ denote the Artin symbol, a certain conjugacy class in $\text{Gal}(L/K)$. (For further details and definitions, cf. [9, Ch. 6].) It will be convenient to use the convention that any prime $\mathfrak{p} \subset O_K$ appearing in an Artin symbol $\left(\frac{L/K}{\mathfrak{p}}\right)$ is implicitly assumed to be unramified.

By an *incomplete interval* I in \mathbb{F}_p we mean a set of the form $I = [M, M + 1, \dots, M + N] \subset \mathbb{F}_p$ for $M \in \mathbb{F}_p$ and $N \in \mathbb{N}$ (in fact, our method applies to arithmetic progressions of the form $\{A \cdot i + B\}_{i \in I}$ where $A, B \in \mathbb{F}_p$ and I is an incomplete interval.) Let Frob_p denote the Frobenius substitution $\alpha \rightarrow \alpha^p$. Define $n \in \mathbb{Z}^+$ such that $\mathbb{F}_{p^n} = L \cap \overline{\mathbb{F}_p}$ is the field of constants in L , and let $m = [L : K\mathbb{F}_{p^n}]$; note that in the

“geometric case”, i.e., when $n = 1$, we have $m = |\text{Gal}(L/K)|$. Further, given $a \in \mathbb{F}_p$, let $\mathfrak{p}_a \subset \mathbb{F}_p[t]$ denote the prime ideal generated by $(t - a)$.

Theorem 1. *Let $C \subset \text{Gal}(L/K)$ be a conjugacy class. If $\tau|_{\mathbb{F}_{p^n}} = \text{Frob}_p|_{\mathbb{F}_{p^n}}$ for all $\tau \in C$, then*

$$\left| \left\{ a \in I : \left(\frac{L/K}{\mathfrak{p}_a} \right) = C \right\} \right| = \frac{|C|}{m} \cdot |I| + O_{[L:K]}(p^{1/2} \log p),$$

On the other hand, if $\tau|_{\mathbb{F}_{p^n}} \neq \text{Frob}_p|_{\mathbb{F}_{p^n}}$ for all $\tau \in C$, then we have

$$\left| \left\{ a \in I : \left(\frac{L/K}{\mathfrak{p}_a} \right) = C \right\} \right| = 0.$$

The result only gives non-trivial information for $|I|$ slightly larger than $p^{1/2} \log p$. Using the Pólya-Vinogradov method of “completing the sum”, the result follows easily from our key technical result, Proposition 2, namely square root cancellation for certain complete sums twisted by additive characters. We remark that by using smoothing (cf. [8, Theorem 1.1]) the error in Theorem 1 is easily improved to $O_{[L:K]}(p^{1/2} \log(10^5 |I| / p^{1/2}))$, hence giving asymptotics as long as $p^{1/2}/|I|$ tends to zero. We leave the details to the interested reader.

Proposition 2. *Let $K = \mathbb{F}_p(t)$ and let L/K be a normal and separable extension with Galois group $\text{Gal}(L/K)$, and let C denote a conjugacy class in $\text{Gal}(L/K)$. If $\psi : \mathbb{F}_p \rightarrow \mathbb{C}^\times$ is a non-trivial additive character then*

$$\left| \sum'_{a \in \mathbb{F}_p : \left(\frac{L/K}{\mathfrak{p}_a} \right) = C} \psi(a) \right| \ll_{[L:K]} p^{1/2},$$

with \sum' denoting the sum restricted to $a \in \mathbb{F}_p$ such that \mathfrak{p}_a is in addition unramified in L .

We remark that the sum is empty unless $\tau|_{\mathbb{F}_{p^n}} = \text{Frob}_p|_{\mathbb{F}_{p^n}}$ for all $\tau \in C$.

1.1. Applications. We now give some explicit examples of families of polynomials for which we can determine the corresponding Galois group. This together with Theorem 1 shows the existence of primes in incomplete intervals. The method proceeds by finding the distribution of Artin symbols, hence also determines the distribution of factorization types, but for simplicity we state it only for the density of irreducible polynomials.

Theorem 3. Let $p > d + 1$ be a (large) prime, and let $f(x) = x^d + \sum_{i=0}^{d-1} a_i x^i \in \mathbb{F}_p[x]$ be a monic polynomial of degree d . There exists subsets $B_1, B_2, B_3 \subset \mathbb{F}_p$ such that $|B_i| = O_d(1)$ for $i = 1, 2, 3$ with the following properties. Given any incomplete interval $I \subset \mathbb{F}_p$, we have:

(1) For $a_1 \in \mathbb{F}_p \setminus B_1$,

$$|\{\alpha \in I : f(x) + \alpha \text{ irreducible }\}| = |I|/d + O_d(p^{1/2} \log p).$$

(2) For $a_0 \in \mathbb{F}_p \setminus B_2$,

$$|\{\alpha \in I : f(x) + \alpha \cdot x \text{ irreducible }\}| = |I|/d + O_d(p^{1/2} \log p).$$

(3) For $a_1 \neq 0, a_0 \in \mathbb{F}_p \setminus B_3$ and any integer $m \in [2, d - 1]$,

$$|\{\alpha \in I : f(x) + \alpha \cdot x^m \text{ irreducible }\}| = |I|/d + O_d(p^{1/2} \log p).$$

An immediate application is a deterministic time algorithm for constructing irreducible degree d polynomials $g(x) \in \mathbb{F}_p[x]$ of quite general shapes, in particular of very sparse form. (The complexity in terms of d is quite bad so we will not make it explicit.) Given any (say monic) degree d polynomial f , consider the family $f(x) + bx + a$. Trying at most $O_d(1)$ values of b , and $O_d(p^{1/2} \log p)$ values of a yields an irreducible polynomial; each such irreducibility test can be done in $O_d(\log p)$ arithmetic operations in \mathbb{F}_p (say using Rabin's test). Hence we can produce an irreducible $g(x)$ in $O_d(p^{1/2} \log^2 p)$ \mathbb{F}_p -operations, or even $O_d(p^{1/2} \log p)$ operations using the earlier described smoothing improvement; note that for existence for irreducibles it is enough to take $|I| \gg_d p^{1/2}$. This is to be compared with Shoup's algorithm [19] which requires $O_d(p^{1/2} \log^3 p)$ \mathbb{F}_p -operations. Ignoring polynomial factors in $\log \log p$, and using fast (FFT-based) \mathbb{F}_p -arithmetic, the bit operation complexities can be obtained by multiplying the above bounds by $\log p$.

Remark. Given polynomials $f, g \in \mathbb{F}_p[x]$ with $\deg(g) < \deg(f) = d$ we can under fairly weak assumptions on f, g , namely that the ratio f/g is Morse, show that (cf. Section 5)

$$|\{\alpha \in I : f(x) + \alpha \cdot g(x) \text{ irreducible }\}| = |I|/d + O_d(p^{1/2} \log p).$$

For f a degree d Morse polynomial, and distinct $h_1, \dots, h_k \in \mathbb{F}_p$, the Galois group of the compositums of the fields generated, over $\mathbb{F}_p(t)$, by the polynomials $f(x) + h_1 + t, \dots, f(x) + h_k + t$ is maximal, i.e., isomorphic to S_d^k (cf. [14]). Theorem 1 then gives equidistribution of cycle types of $\{(f(x) + h_1 + a, \dots, f(x) + h_k + a)\}_{a \in I}$ inside S_d^k , provided $(p^{1/2} \log p)/|I| = o(1)$. Thus, for f Morse we immediately obtain cancellation for function field analogs of Moebius and Chowla

type sums; with μ denoting the function field Moebius μ function, we have

$$\sum_{a \in I} \mu(f + h_1 + a) \cdot \dots \cdot \mu(f + h_k + a) \ll_{k,d} p^{1/2} \log p$$

(cf. [14, 4, 12] for results valid for various longer intervals.)

Another application is asymptotics for function field analogs, for incomplete intervals “centered” at f , assuming $(p^{1/2} \log p)/|I| = o(1)$ and f Morse, of shifted divisors sums (e.g. $\sum_{a \in I} d_r(f + a)d_r(f + 1 + a)$ where d_r is the r -th divisor function) and the Titchmarsh divisor problem (e.g. $\sum_{a \in I} 1_{\text{Prime}}(f + a)d_r(f + 1 + a)$); asymptotics for these sums over “long” intervals, while allowing for very general shifts, were determined in [1].

We next give an example where the cycle type distribution is not enough to determine the distribution of Artin symbols. Let $p \equiv 1 \pmod{3}$ be a (large) prime, and let $h_1, \dots, h_k \in \mathbb{F}_p$ be distinct. Define $f_i(x) = x^3 + h_i + t$ and let L_i denote the splitting field of f_i over $\mathbb{F}_p(t)$, and let L^k denote the compositum of the fields L_1, \dots, L_k . Then (cf. [13, Proposition 8]) $\text{Gal}(L_i/\mathbb{F}_p(t)) \simeq A_3$ for $i = 1, \dots, k$, and $\text{Gal}(L^k/\mathbb{F}_p(t)) \simeq A_3^k$. With $\mathfrak{p}_a = (t - a)$, Theorem 1 implies that the Artin symbols $\left\{ \left(\frac{L^k/\mathbb{F}_p(t)}{\mathfrak{p}_a} \right) : a \in I \right\}$ equidistribute in A_3^k , with relative error of size $(p^{1/2} \log p)/|I|$.

1.2. Discussion. For the full interval $I = \mathbb{F}_p$ and $n = 1$ (the geometric case) Chebotarev’s density theorem for function fields, with error term of size $O_{[L:K]}(p^{1/2})$, easily follows from the work of Reichardt [17] together with Weil’s celebrated proof of the Riemann hypothesis for curves over finite fields [23]. (Reichardt’s error term, for primes of degree v , is of size $O(p^{\Theta \cdot v})$ as $v \rightarrow \infty$, where $\Theta < 1$ is the maximum of the real parts of the roots of the zeta function of L .) The case $I = \mathbb{F}_p$ and $n > 1$ is due to Cohen and Odoni [6] (also cf. [10]). As for incomplete intervals we are only aware of recent results by Entin [7] who determined the distribution of factorization types for various families of polynomials whose coefficients are allowed to vary over incomplete intervals (see below).

In [21] Shparlinski studied the proportion of irreducible monic polynomials in $\mathbb{F}_p[x]$, with coefficients in constrained to lie on points with

integer coordinates inside parallelepipeds, and showed that

$$\begin{aligned} & \left| \left\{ (a_0, \dots, a_{d-1}) \in I_0 \times \dots \times I_{d-1} : x^d + \sum_{i=0}^{d-1} a_i x^i \text{ irreducible} \right\} \right| \\ &= \frac{\prod_{i=0}^{d-1} |I_i|}{d} + O(p^{d-1} \log^{d-1} p), \end{aligned}$$

giving non-trivial information when $\prod_{i=0}^{d-1} |I_i| > p^{d-1+\epsilon}$. (More generally, he also determined the distribution of factorization types.) Further, in [20], he considered sparser families, namely the set of irreducible trinomials in $\mathbb{F}_p[x]$, and showed that

$$\left| \left\{ (a_0, a_1) \in I_0 \times I_1 : x^d + a_1 x + a_0 \text{ irreducible} \right\} \right| \sim |I_0| \cdot |I_1| / d$$

provided $|I_0|, |I_1| > p^{1/4+\epsilon}$ and $|I_0| \cdot |I_1| > p^{1+\epsilon}$, and similarly for trinomials with any prescribed factorization type. Theorem 3 easily implies the same asymptotics, under the weaker conditions $|I_0| > p^\epsilon$, $|I_1| > p^{1/2+\epsilon}$, or $|I_1| > p^\epsilon$, $|I_0| > p^{1/2+\epsilon}$.

Entin [7] determined the distribution of factorization patterns for families of polynomials whose coefficients vary over quite general sets $S \subset \mathbb{F}_p^d$, with relative error of size $\text{irreg}(S)/p^{1/2}$ where $\text{irreg}(S)$ is related to the decay of Fourier coefficients of the characteristic function of S . E.g., for $S = I_0 \times \dots \times I_{d-1}$, $\text{irreg}(S) \ll p^d \log^d p / (\prod_{i=0}^{d-1} |I_i|)$ with relative error small if $\prod_{i=0}^{d-1} |I_i| > p^{d-1/2+\epsilon}$. His method also applies for sparser families: for trinomials the assumption needed for small relative error is $|I_0| \cdot |I_1| > p^{3/2+\epsilon}$; for f Morse and the family $f(x) + a_0$ the relative error is small if $(p^{1/2} \log p) / |I_0| = o(1)$, similar to the conditions in Theorem 3.

1.3. Acknowledgements. We thank A. Granville, E. Kowalski, Z. Rudnick and P. Salberger for helpful discussions. We also thank I. Shparlinski and O. Gorodetsky for valuable comments on an early version of the paper, in particular for suggesting using smoothing to improve the error term in Theorem 1. We further thank I. Shparlinski for pointing out the application of finding irreducible polynomials in sparse families, thus leading to a deterministic way to find irreducibles that is faster than Shoup's algorithm.

2. DEDUCING THEOREM 1 FROM PROPOSITION 2

To simplify the notation, let $F(a) = 1$ if $\left(\frac{L/K}{\mathfrak{p}}\right) = C$, and zero otherwise. For $b \in \mathbb{F}_p$, let $\psi_b(x)$ denote the additive character $\psi_b(x) :=$

$e^{2\pi i bx/p}$. With 1_I denoting the characteristic function of I , we “complete the sum” and write

$$\begin{aligned} |\{a \in I : \left(\frac{L/K}{\mathfrak{p}_a}\right) = C\}| &= \sum_{a \in I} F(a) = \sum_{a \in \mathbb{F}_p} F(a)1_I(a) \\ &= \sum_{a \in \mathbb{F}_p} F(a) \sum_{b \in \mathbb{F}_p} \widehat{1}_I(b)\psi_b(a) = \sum_{b \in \mathbb{F}_p} \widehat{1}_I(b) \sum_{a \in \mathbb{F}_p} F(a)\psi_b(a) \end{aligned}$$

where $\widehat{1}_I(b) := 1/p \sum_{c \in \mathbb{F}_p} 1_I(c)\psi_b(-c)$ is the Fourier transform of 1_I .

Our main term will come from terms with $b = 0$; by [9, Proposition 6.4.8] (note that the genus of L can be bounded in terms of $[L : K]$) we find that

$$\begin{aligned} (2) \quad \frac{|I|}{p} \sum_{a \in \mathbb{F}_p} F(a) &= \frac{|I|}{p} \cdot \left(\frac{|C|}{m} p + O_{[L:K]}(p^{1/2}) \right) \\ &= \frac{|C|}{m} |I| + O_{[L:K]}(|I|p^{-1/2}) \end{aligned}$$

As for the error terms, taking integer representatives b of the elements in \mathbb{F}_p^\times , such that $0 < |b| < p/2$, we find that $\widehat{1}_I(b) \ll 1/b$. Now, by Proposition 2 (note that for $b \not\equiv 0 \pmod{p}$, ψ_b is non-trivial), we have

$$(3) \quad \sum_{b \in \mathbb{F}_p^\times} \left| \sum_{a \in \mathbb{F}_p} F(a)\psi_b(a) \right| \ll_{[L:K]} p^{1/2} \sum_{b=1}^{p/2} 1/b \ll_{[L:K]} p^{1/2} \log p.$$

As $|I| \leq p$, the error term in (3) dominates the error term in (2), hence

$$\frac{|I|}{p} \sum_{a \in \mathbb{F}_p} F(a) = \frac{|C|}{m} |I| + O_{[L:K]}(p^{1/2} \log p).$$

3. ADDITIVE CHARACTERS AND ARTIN-SCHREIER EXTENSIONS

We briefly recall how a non-trivial additive character ψ on \mathbb{F}_p can be realized as a character ψ_K on some cyclic galois group $\text{Gal}(E/K)$, where $K = \mathbb{F}_p(t)$, such that

$$\psi_K \left(\left(\frac{E/K}{\mathfrak{p}_a} \right) \right) = \psi(a), \quad a \in \mathbb{F}_p;$$

and $\mathfrak{p}_a = (t - a) \subset \mathbb{F}_p[t]$ denotes a degree one prime ideal. (Note that $\deg(\mathfrak{p})$, the degree of the prime ideal \mathfrak{p} is defined in terms of the cardinality of the residue field, namely $|\mathcal{O}_K/\mathfrak{p}| = p^{\deg(\mathfrak{p})}$. Also, since E/K is cyclic we can regard the Artin symbol $\left(\frac{E/K}{\mathfrak{p}_a} \right)$ as an element in $\text{Gal}(E/K)$ rather than a conjugacy class.)

The extension E can be constructed as follows: with ξ denoting a root of the polynomial $f(x) = x^p - x - t$, let $E = K(\xi)$. Then E/K is an Artin-Schreier extension of degree p , such that $\text{Gal}(E/K) \simeq \mathbb{F}_p^+$. The extension is unramified except at infinity, where it is wildly ramified.

Specializing at $\mathfrak{p}_a = (t - a)$ for $a = 0$, we find that $x^p - x$ splits completely, and thus $\left(\frac{E/K}{\mathfrak{p}_a}\right)$ is the identity element in $\text{Gal}(E/K)$. Similarly, specializing at $\mathfrak{p}_a = (t - a)$ for $a \in \mathbb{F}_p^\times$, we find that $x^p - x - a$ is irreducible (over \mathbb{F}_p), and thus there is exactly one (unramified) prime $\mathfrak{Q}_a \subset O_E$ above \mathfrak{p}_a , and $O_E/\mathfrak{Q}_a \simeq \mathbb{F}_{p^p}$.

We next turn to identifying the Galois action of the Artin symbol. If ξ is some fixed root of $x^p - x - t$, any Galois element $\sigma \in \text{Gal}(E/K)$ acts via $\xi \rightarrow \xi + \alpha$ for some $\alpha \in \mathbb{F}_p$. Moreover, given such a σ , we can recover α from $\sigma(\xi) - \xi$. Thus, if σ is the Artin map at $\mathfrak{p}_a = (t - a)$, we find that

$$\alpha = \sigma(\xi) - \xi = \xi^p - \xi = a$$

In conclusion, for $a \in \mathbb{F}_p$ the Artin symbol $\left(\frac{E/K}{\mathfrak{p}_a}\right)$ acts as $\xi \rightarrow \xi + a$, hence there is a natural identification of $\text{Gal}(E/K)$ with \mathbb{F}_p^+ so that the image of \mathfrak{p}_a is just $a \in \mathbb{F}_p^+$. In particular, given a non-trivial additive character of \mathbb{F}_p we can define a character ψ_K on $\text{Gal}(E/K)$ such that

$$\psi_K\left(\left(\frac{E/K}{\mathfrak{p}_a}\right)\right) = \psi(a), \quad a \in \mathbb{F}_p.$$

4. PROOF OF PROPOSITION 2

The main bulk of the argument is similar to the one used in [9, Ch 6.4]; below we briefly summarize the argument and only give details when we need to go beyond their results. For easier comparison, we follow their notation and write q rather than p .

Let $K = \mathbb{F}_q(t)$ and let L/K be a normal extension with Galois group $\text{Gal}(L/K)$. Since the constant in the error term is allowed to depend on $[L : K]$, we may assume that $q = p$ is sufficiently large (say $q > [L : K]$) so that L/K is separable, as well as tamely ramified and thus by the Hurwitz genus formula, that the genus bound $g(L) \ll_{[L:K]} 1$ holds. Let $C \subset \text{Gal}(L/K)$ be a conjugacy class. We may also assume that $\tau|_{\mathbb{F}_{q^n}} = \text{Frob}_q|_{\mathbb{F}_{q^n}}$ for all $\tau \in C$, otherwise the Artin symbol never meets C and the sum is empty. We will need some further notations: given field extensions $L/K'/K$, let

$$\begin{aligned} \mathbb{P}'_k(K') := \{\mathfrak{p} \subset O_{K'} : \mathfrak{p} \text{ is a prime ideal,} \\ \text{unramified over } K \text{ and in } L, \deg(\mathfrak{p}) = k\}. \end{aligned}$$

Moreover, for extensions $L'/L/K'/K$, with L'/L unramified, and a conjugacy class $C' \subset \text{Gal}(L'/K')$, let

$$C_k(L'/K', C') := \left\{ \mathfrak{p}' \in \mathbb{P}'_k(K') : \left(\frac{L'/K'}{\mathfrak{p}'} \right) = C' \right\}.$$

Let $\mathbb{F}_{q^n} = L \cap \overline{\mathbb{F}_q}$ denote the field of constants in L , and let $m = [L : K\mathbb{F}_{q^n}]$. Choose some $\tau \in C$ and define $n' = n \cdot \text{ord}(\tau)$, where $\text{ord}(\tau)$ denotes the order τ in $\text{Gal}(L/K)$; note that n' does not depend on the choice of τ since all elements in C have the same order. With $L' := L\mathbb{F}_{q^{n'}}$ we have $[L' : K\mathbb{F}_{q^{n'}}] = [L : K\mathbb{F}_{q^n}] = m$; also note that L'/L is unramified. By [9, Lemma 6.4.4] there exists $\tau' \in \text{Gal}(L'/K)$ such that $\tau'|_L = \tau$ and $\tau'|_{\mathbb{F}_{q^{n'}}} = \text{Frob}_q|_{\mathbb{F}_{q^{n'}}}$; moreover $\text{ord}(\tau') = \text{ord}(\tau) \cdot n = n'$.

With $C' \subset \text{Gal}(L'/K)$ denoting the conjugacy class of τ' , we have (cf. [9, Lemma 6.4.4])

$$C_1(L'/K, C') = C_1(L/K, C),$$

and thus

$$(4) \quad \sum'_{a \in \mathbb{F}_p : \left(\frac{L/K}{\mathfrak{p}a} \right) = C} \psi(a) = \sum_{\mathfrak{p} \in C_1(L/K, C)} \psi_K(\mathfrak{p}) = \sum_{\mathfrak{p} \in C_1(L'/K, C')} \psi_K(\mathfrak{p})$$

Let $K'_{\tau'} \subset L'$ denote the fixed field of τ' . Note that L' does not depend on τ' , whereas $K'_{\tau'}$ does. We will need to keep track of this dependence and will therefore deviate slightly from the notation in Fried-Jarden (in their argument it suffices to work with a fixed τ' , consequently they denote K' for the fixed field of τ' .)

From the proof of [9, Proposition 6.4.8] it follows that $K'_{\tau'} \cap \mathbb{F}_{q^{n'}} = K'_{\tau'} \cap \overline{\mathbb{F}_q} = \mathbb{F}_q$, and $K'_{\tau'}\mathbb{F}_{q^{n'}} = L'$, as well as $[K'_{\tau'} : K] = [L' : K\mathbb{F}_{q^{n'}}] = [L : K\mathbb{F}_{q^n}] = m$. It also follows (in particular see how their Corollary 6.4.3 was used in the proof of Proposition 6.4.8)

$$|C_1(L'/K, C')| = \frac{|C|}{[K'_{\tau'} : K]} \cdot |C_1(L'/K'_{\tau'}, \{\tau'\})| = \frac{|C|}{m} \cdot |C_1(L'/K'_{\tau'}, \{\tau'\})|$$

This equality suggests the existence of some m to 1 map; we will show that this is indeed the case and then obtain a sum over certain degree one primes in $O_{K'}$.

We first show that we can “lift” ψ_K to a suitably invariant character $\psi_{K'_{\tau'}}$, i.e., independent of the choice of prime \mathfrak{p}' above any prime \mathfrak{p} occurring in the sums we wish to estimate. Recall that we have realised the additive character $\psi : \mathbb{F}_q \rightarrow \mathbb{C}^\times$ as a character ψ_K on $\text{Gal}(E/K)$,

for E/K an Artin-Schreier extension E/K , with the property that

$$\psi_K \left(\left(\frac{E/K}{\mathfrak{p}_a} \right) \right) = \psi(a).$$

As $[E : K] = q$ we have, for q sufficiently large (which we may assume to hold since the constant in error term is allowed to depend on $[L : K]$), $\text{Gal}(K'_{\tau'} E/K) \simeq \text{Gal}(K'_{\tau'}/K) \times \text{Gal}(E/K)$, as well as $\text{Gal}(K'_{\tau'} E/K'_{\tau'}) \simeq \text{Gal}(E/K)$, where the latter isomorphism can be defined by restricting $\text{Gal}(K'_{\tau'} E/K'_{\tau'})$ to act on E/K . We can thus define a character $\psi_{K'_{\tau'}}$ by composition. Now, given degree one primes $\mathfrak{p} \in \mathbb{P}'_1(K)$ and $\mathfrak{p}' \in \mathbb{P}'_1(K'_{\tau'})$, with $\mathfrak{p}'|\mathfrak{p}$, we will need, no matter which $\mathfrak{p}'|\mathfrak{p}$ is chosen, that

$$\psi_{K'_{\tau'}}(\mathfrak{p}') = \psi_K(\mathfrak{p}).$$

This in turn is immediate from [15, p. 198, property A3]: since \mathfrak{p}' and \mathfrak{p} are degree one primes, we have $f_{\mathfrak{p}'|\mathfrak{p}} = 1$, and thus

$$\left(\frac{K'_{\tau'} E/K'_{\tau'}}{\mathfrak{p}'} \right) \Big|_E = \left(\frac{E/K}{\mathfrak{p}} \right)^{f_{\mathfrak{p}'|\mathfrak{p}}} = \left(\frac{E/K}{\mathfrak{p}} \right)$$

which shows that the choice of $\mathfrak{p}'|\mathfrak{p}$ indeed does not matter.

Now consider the tower of extensions $L'/K'_{\tau'}/K$. As for their field of constants, we have $L' \cap \overline{\mathbb{F}_q} = \mathbb{F}_{q^{n'}}$, $K'_{\tau'} \cap \overline{\mathbb{F}_q} = \mathbb{F}_q$, $K \cap \overline{\mathbb{F}_q} = \mathbb{F}_q$. Let $\mathfrak{P} \in \mathbb{P}'(L')$, $\mathfrak{p}' \in \mathbb{P}'_1(K'_{\tau'})$, and $\mathfrak{p} \in C_1(L/K, C)$ denote primes such that $\mathfrak{P}|\mathfrak{p}'|\mathfrak{p}$. Then, as $\deg(\mathfrak{p}') = \deg(\mathfrak{p}) = 1$ (see [9, Lemma 6.4.2] and the proof of Proposition 6.4.8) we have $O_{K'}/\mathfrak{p}' \simeq O_K/\mathfrak{p} = \mathbb{F}_q$, and thus $f_{\mathfrak{p}'|\mathfrak{p}} = 1$. Further, as $\left(\frac{L'/K'_{\tau'}}{\mathfrak{p}'} \right) = \{\tau'\}$ and $\text{ord}(\tau') = n'$, we have $O_{L'}/\mathfrak{P} \simeq \mathbb{F}_{q^{n'}}$ and hence $f_{\mathfrak{P}|\mathfrak{p}'} = n'$. Thus, as $[L' : K'_{\tau'}] = n'$, the latter implies that any $\mathfrak{P}|\mathfrak{p}'$ is uniquely determined by \mathfrak{p}' , whereas the former (together with $[K'_{\tau'} : K] = m$) implies that there are exactly m primes $\mathfrak{p}'_1, \dots, \mathfrak{p}'_m$ lying above \mathfrak{p} .

We thus find that

$$(5) \quad \sum_{\mathfrak{p} \in C_1(L'/K, C')} \psi_K(\mathfrak{p}) = \sum_{\tau' \in C'} \sum_{\mathfrak{p} \in \mathbb{P}'_1(K)} \psi_K(\mathfrak{p}) \sum_{\substack{\mathfrak{P} \in \mathbb{P}'_{n'}(L'), \mathfrak{P}|\mathfrak{p}, \\ \left(\frac{L'/K'_{\tau'}}{\mathfrak{P}} \right) = \{\tau'\}}} \frac{1}{m}$$

$$= \frac{1}{m} \sum_{\tau' \in C'} \sum_{\substack{\mathfrak{p}' \in \mathbb{P}'_1(K'_{\tau'}) \\ \left(\frac{L'/K'_{\tau'}}{\mathfrak{p}'} \right) = \{\tau'\}}} \psi_{K'_{\tau'}}(\mathfrak{p}')$$

which, from the proof of [9, Lemma 6.4.6], equals

$$\frac{1}{m} \sum_{\tau' \in C'} \sum_{\mathfrak{p}' \in \mathbb{P}'_1(K'_{\tau'})} \psi_{K'_{\tau'}}(\mathfrak{p}');$$

note that the inner sum amounts to summing an additive character over *all* points on the curve given by the field $K'_{\tau'}$, having field of constants $K'_{\tau'} \cap \overline{\mathbb{F}_q} = \mathbb{F}_q$.

As $|C| = O_{[L:K]}(1)$, it suffices to show that

$$(6) \quad \left| \sum_{\mathfrak{p}' \in \mathbb{P}'_1(K'_{\tau'})} \psi_{K'_{\tau'}}(\mathfrak{p}') \right| \ll_{[L:K]} q^{1/2}.$$

To see this, let $L(s) = L(s, \psi_{K'_{\tau'}}, EK'_{\tau'}/K'_{\tau'})$ denote the Artin L -function attached to the character $\psi_{K'_{\tau'}}$; as $EK'_{\tau'}/K'_{\tau'}$ is abelian it is in fact an L -series attached to a Hecke character.

Taking logarithmic derivatives of $L(s)$, we find that the sum over primes in (6) agrees, apart from ramified primes, with the sum over degree one terms in $-L'(s)/L(s)$. As E/K only ramifies (wildly) at infinity, there are $O_{[L:K]}(1)$ ramified primes, and hence the Riemann hypothesis for curves (due to Weil) gives that the sum is $\ll_{[L:K]} q^{1/2}$, *provided* that we can show that the degree of the L -function only depends on $[L : K]$ (here some care is needed since $[EK'_{\tau'} : K'_{\tau'}] = p$.) To see this, first note that

$$\zeta_{K'_{\tau'}}(s) \cdot \prod_{\psi \in \text{Gal}(\widehat{EK'_{\tau'}}/K'_{\tau'}) \setminus 1} L(s, \psi, EK'_{\tau'}/K'_{\tau'}) = \zeta_{EK'_{\tau'}}(s).$$

Next note that any two non-trivial characters $\psi_1, \psi_2 \in \text{Gal}(\widehat{EK'_{\tau'}}/K'_{\tau'})$ have the same conductor, thus the degrees of the L -functions

$$\{L(s, \psi, EK'_{\tau'}/K'_{\tau'})\}_{\psi \in \text{Gal}(\widehat{EK'_{\tau'}}/K'_{\tau'}) \setminus 1}$$

are the same (cf. [16, Ch. 6].) As there are $p - 1$ non-trivial characters ψ , it is enough to show that the degree of $\zeta_{EK'_{\tau'}}(s)$ is $\ll_{[L:K]} p$. As this degree is linear in $g = g(EK'_{\tau'})$, the genus of $EK'_{\tau'}$, it is in turn enough to show that $g \ll_{[L:K]} p$. This is immediate from Castelnuovos Inequality (cf. [22, Theorem 3.11.3]) since $g(E) \ll 1$, $[E : K] = p$, $g(K'_{\tau'}) \ll_{[K:L]} 1$, and $[K'_{\tau'} : K] \ll_{[L:K]} 1$.

5. CRITERIA FOR MORSE POLYNOMIALS AND GALOIS GROUP S_d

Given an integer $m \in [1, d - 1]$, define

$$f_t(x) := f(x) + tx^m.$$

As long as a few of the small degree coefficients of f avoid sets of $O_d(1)$ “bad coefficients”, the polynomial $f_t(x)$, over $\mathbb{F}_p(t)$, will have maximal Galois group. To see this we recall a very useful criterium.

Proposition 4 (Geyer [11]). *Assume that $\varphi = f/g \in \mathbb{F}_p(x)$ is a Morse function of degree $d = \deg(f) > \deg(g) \geq 0$. Then the Galois group of the covering $\varphi : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ of degree d is the full symmetric group, i.e., $\text{Gal}(f(x) - tg(x)/\mathbb{F}_p(t)) \simeq S_d$.*

Fixing g , Geyer in fact shows that the set of polynomials $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ for which f/g is Morse is a Zariski open dense subset of the affine d -space with coordinates a_0, \dots, a_{d-1} . More precisely, for $\deg(g) > 0$, fixing $a_{d-1}, \dots, a_2, a_1 \in \overline{\mathbb{F}_p}$, write

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_2x^2 + a_1x + u = f_\circ(x) + u$$

with u trancendental over \mathbb{F}_p . Geyer then shows that f/g is Morse provided that

$$(7) \quad \gcd(f'_\circ, g') = 1, \quad f''_\circ \neq 0.$$

In particular, if the conditions in (7) are satisfied, then for all but $O_d(1)$ “bad” specializations of $u = a_0 \in \overline{\mathbb{F}_p}$, the specialized ratio f/g will be Morse.

In particular, for p large the second condition is automatic, and by varying the linear coefficient of f (again avoiding $O_d(1)$ “bad” values) we can ensure that the first condition $(f'_\circ, g') = 1$ holds, showing that $f(x) + t \cdot g(x)$ very often has full Galois group. (Note that $f(x) + t \cdot g(x)$ and $f(x) - t \cdot g(x)$ have the same Galois group over $\mathbb{F}_p(t)$.)

We remark that the Morse criterion is certainly not needed for the Galois group to be maximal. E.g. (cf. [18, Ch. 4.4]) we have

$$\text{Gal}(x^d - x^{d-1} - t/\mathbb{F}_p(t)) \simeq S_d.$$

5.1. Proof of Theorem 3. In [14] it was shown that in the family of polynomials $f^s(x) = f(x) + sx$, f^s is Morse for all but $O_d(1)$ values of $s \in \mathbb{F}_p$ (or even $s \in \overline{\mathbb{F}_p}$). In particular, defining B_1 as the set of s -values for which f^s is not Morse, we have $|B_1| = O_d(1)$ and the first part of Theorem 3 follows from Theorem 1 since $\text{Gal}(f(x) - t/\mathbb{F}_p(t)) \simeq S_d$ for $s \in \mathbb{F}_p \setminus B_1$.

Given Geyer’s criterion, together with Theorem 1, the rest of the proof of Theorem 3 is a simple matter of checking the above conditions.

First, fix an integer $m \in [2, d - 1]$ and take $g(x) = x^m$. Then, for $a_1 \neq 0$, we have $(f'_\circ, g') = 1$; as long as $p > d + 1$ we have $f''_\circ \neq 0$, and hence, for all but $O_d(1)$ choices of $a_0 \in \overline{\mathbb{F}_p}$ (and $a_1 \neq 0$), f/g is Morse

and

$$\mathrm{Gal}(f(x) + tx^m / \mathbb{F}_p(t)) \simeq S_d.$$

Letting B_3 be the union, over $m \in [2, d - 1]$, of these sets of $O_d(1)$ exceptional a_0 -values, the third part follows.

Similarly, for $m = 1$ and $g(x) = x^m = x$ we may, possibly after replacing t by $t + 1$ (changing the interval I to an interval with the same cardinality, and symmetric difference of cardinality 2 with I), assume that $a_1 \neq 0$. Hence for all but $O_d(1)$ choices of a_0 , we find that $\mathrm{Gal}(f(x) + tx + a_0 / \mathbb{F}_p(t)) \simeq S_d$, and the second part follows.

5.2. Further examples. We can also give examples of families of polynomials $f(x)$, with fairly large number of free parameters (about $d/2$ of them), such that the (geometric) Galois group of $f(x) + tx^m$ is not the full symmetric group. For instance, with $m = 0$ and d even, take $f_t(x) = x^d + \sum_{i=0}^{d/2} a_{2i}x^{2i} + t$; the geometric galois group is then a subgroup of a certain wreath product (here the crucial point is that $f_t(x) = g_t(x^2)$, i.e., the family is decomposable.) Similarly, for $m > 0$ and $m|d$, the family

$$f_t(x) = x^d + \sum_{i=0}^{d/m} a_i x^{mi} + tx^m = g_t(x^m)$$

is decomposable.

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] 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.
- [5] S. D. Cohen. Uniform distribution of polynomials over finite fields. *J. London Math. Soc. (2)*, 6:93–102, 1972.
- [6] S. D. Cohen and R. W. K. Odoni. The Farey density of norm subgroups of global fields. II. *Glasgow Math. J.*, 18(1):57–67, 1977.
- [7] A. Entin. Factorization statistics of restricted polynomial specializations over large finite fields. *Preprint*, 2018.

- [8] E. Fouvry, E. Kowalski, P. Michel, C. S. Raju, J. Rivat, and K. Soundararajan. On short sums of trace functions. *Ann. Inst. Fourier (Grenoble)*, 67(1):423–449, 2017.
- [9] 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.
- [10] M. Jarden. The Čebotarev density theorem for function fields: an elementary approach. *Math. Ann.*, 261(4):467–475, 1982.
- [11] M. Jarden and A. Razon. Skolem density problems over large Galois extensions of global fields. In *Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999)*, volume 270 of *Contemp. Math.*, pages 213–235. Amer. Math. Soc., Providence, RI, 2000. With an appendix by Wulf-Dieter Geyer.
- [12] J. Keating and Z. Rudnick. Squarefree polynomials and mobius values in short intervals and arithmetic progressions. *Algebra Number Theory*, 10(2):375–420, 2016.
- [13] P. Kurlberg. Poisson spacing statistics for value sets of polynomials. *International Journal of Number Theory*, 05(03):489–513, 2009.
- [14] P. Kurlberg and L. Rosenzweig. Prime and mobius correlations for very short intervals in $\mathbb{F}_q[x]$. *Preprint*, 2018.
- [15] S. Lang. *Algebraic Number Theory*. Addison-Wesley series in mathematics. Addison-Wesley Publishing Company, 1970.
- [16] W. C. W. Li. *Number theory with applications*, volume 7 of *Series on University Mathematics*. World Scientific Publishing Co., Inc., River Edge, NJ, 1996.
- [17] H. Reichardt. Der Primdivisorsatz für algebraische Funktionenkörper über einem endlichen Konstantenkörper. *Math. Z.*, 40(1):713–719, 1936.
- [18] J.-P. Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. Jones and Bartlett Publishers, Boston, MA, 1992.
- [19] V. Shoup. New algorithms for finding irreducible polynomials over finite fields. *Math. Comp.*, 54(189):435–447, 1990.
- [20] I. E. Shparlinski. On the distribution of irreducible trinomials. *Canad. Math. Bull.*, 54(4):748–756, 2011.
- [21] I. E. Shparlinskiĭ. On primitive elements in finite fields and on elliptic curves. *Mat. Sb.*, 181(9):1196–1206, 1990.
- [22] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.
- [23] A. Weil. *Variétés abéliennes et courbes algébriques*. Actualités Sci. Ind., no. 1064, Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948.

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

DEPARTMENT OF MATHEMATICS, KTH ROYAL INSTITUTE OF TECHNOLOGY,
SE-100 44 STOCKHOLM, SWEDEN
E-mail address: kurlberg@math.kth.se

UNIT OF MATHEMATICS, AFEKA TEL AVIV COLLEGE OF ENGINEERING, MIVTZA
KADESH 38, TEL AVIV, ISRAEL
E-mail address: liorr@afeka.ac.il