CHEBOTAREV DENSITY THEOREM IN SHORT INTERVALS FOR EXTENSIONS OF $\mathbb{F}_q(T)$

LIOR BARY-SOROKER, OFIR GORODETSKY, TAELIN KARIDI, AND WILL SAWIN

Abstract. An old open problem in number theory is whether Chebotarev density theorem holds in short intervals. More precisely, given a Galois extension E of $\mathbb{Q}$ with Galois group G, a conjugacy class C in G and an $1 \geq \varepsilon > 0$, one wants to compute the asymptotic of the number of primes $x \leq p \leq x + x^\varepsilon$ with Frobenius conjugacy class in E equal to C. The level of difficulty grows as ε becomes smaller. Assuming the Generalized Riemann Hypothesis, one can merely reach the regime $1 \geq \varepsilon > 1/2$. We establish a function field analogue of Chebotarev theorem in short intervals for any $\varepsilon > 0$. Our result is valid in the limit when the size of the finite field tends to ∞ and when the extension is tamely ramified at infinity. The methods are based on a higher dimensional explicit Chebotarev theorem, and applied in a much more general setting of arithmetic functions, which we name G-factorization arithmetic functions.

1. Introduction

The goal of this paper is to provide support to an open problem in the distribution of primes with a given Frobenius conjugacy class. We do this by resolving a function field version of the problem. We start by introducing the problem in number fields, and then we present our results.

1.1. The Chebotarev Density Theorem in short intervals.

One of the main theorems in algebraic number theory is the Chebotarev Density Theorem about the distribution of Frobenius conjugacy classes in Galois extensions of global fields. To keep the presentation as simple as possible, we fix the base field to be $\mathbb{Q}$. Let E be a finite Galois extension of $\mathbb{Q}$ with Galois group $G = \mathrm{Gal}(E/\mathbb{Q})$ and with ring of integers $\mathcal{O}_E$. For a prime number p, we define

$$\left(\frac{E/\mathbb{Q}}{p}\right) \subseteq G,$$

2010 *Mathematics Subject Classification.* Primary 11N05; Secondary 11T06, 12F10.

LBS was partially supported by a grant of the Israel Science Foundation. Part of the work was done while LBS was a member of Simons CRM Scholar-in-Residence Program.

The research of OG was supported by the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement n° 320755.

This research was partially conducted during the period WS served as a Clay Research Fellow, and partially conducted during the period he was supported by Dr. Max Rössler, the Walter Haefner Foundation and the ETH Zurich Foundation.

to be the set of all $\sigma \in G$ for which there exists a prime $\mathfrak{P}$ of E lying above p such that

$$\sigma(x) \equiv x^p \mod \mathfrak{P},$$

for all $x \in \mathcal{O}_E$. If p is unramified in E, then $\left(\frac{E/\mathbb{Q}}{p}\right)$ is called the *Frobenius* at p and it is a conjugacy class in G.

The Chebotarev Density Theorem says that as p varies, the Frobenius equidistributes in the set of conjugacy classes (with the obvious weights). More precisely, let

$$\pi(x) = \#\{p \leq x : p \text{ prime number}\}$$

be the prime counting function. By the Prime Number Theorem, we know that $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$ well approximates $\pi(x)$; that is to say, for any $A > 1$ we have

$$\pi(x) = \mathrm{Li}(x) + O_A(x/(\log x)^A), \qquad x \to \infty.$$

For a conjugacy class $C \subseteq G$, let

$$\pi_C(x;E) = \#\left\{p \leq x : p \text{ prime number and } \left(\frac{E/\mathbb{Q}}{p}\right) = C\right\}$$

be the function that counts primes with Frobenius equals to C. The Chebotarev Density Theorem [35, Theorem 2.2, Chapter I] says that

$$\pi_C(x;E) \sim \frac{|C|}{|G|}\mathrm{Li}(x), \qquad x \to \infty. \tag{1}$$

This theorem is a vast generalization of the Prime Number Theorem for arithmetic progressions which follows from (1) applied to cyclotomic fields.

It is both natural and important for applications to consider the Chebotarev Density Theorem in short intervals. Balog and Ono [2] studied the non-vanishing of Fourier coefficients of modular forms in short intervals. For this application they prove that

$$\pi_C(x+y;E) - \pi_C(x;E) \sim \frac{|C|}{|G|}\frac{y}{\log x}, \qquad x \to \infty, \tag{2}$$

for $x^{1-1/c(E)+\varepsilon} \leq y \leq x$, and where $c(E) > 0$ is a constant depending only on E (and in fact only on $[E:\mathbb{Q}]$). Thorner [38, Corollary 1.1] improves the range of y for which (2) holds true.

Naively, we expect that (2) holds for any $y = y(x) \leq x$ that grows 'sufficiently fast'. From (1), it follows that the average gap between primes with $\left(\frac{E/\mathbb{Q}}{p}\right) = C$ is $\frac{|G|}{|C|}\log x$. Thus it makes sense to only consider y-s satisfying $\lim_{x\to\infty} \frac{y}{\log x} = \infty$. The Maier phenomenon [24] about primes tells us that (2) fails unless $y \gg (\log x)^A$ for all $A > 1$. A folklore conjecture says that for any fixed $\varepsilon > 0$ and $y = x^\varepsilon$ the asymptotic formula (2) holds true:

Conjecture 1.1. *Let $E/\mathbb{Q}$ be a Galois extension with Galois group G, $1 \geq \varepsilon > 0$, and $C \subseteq G$ a conjugacy class. Then*

$$\pi_C(x + x^\varepsilon; E) - \pi_C(x; E) \sim \frac{|C|}{|G|}\frac{x^\varepsilon}{\log x}, \qquad x \to \infty.$$

When $E = \mathbb{Q}$, Conjecture 1.1 reduces to primes in short intervals, and we refer the reader to the excellent survey [36] for further reading on this case.

One approach for Conjecture 1.1 is to study the error term in Chebotarev Density Theorem. Let

$$\Delta_{E;C}(x) = \pi_C(x, E) - \frac{|C|}{|G|}\mathrm{Li}(x)$$

and let d_E be the absolute value of the discriminant of E. Under the Riemann Hypothesis for the Dedekind zeta function ζ_E of E, Lagarias and Odlyzko [20] gave the bound

$$\Delta_{E;C}(x) = O(|C|x^{1/2}(\log x + \frac{\log d_E}{|G|})), \tag{3}$$

where the implied constant is effective and absolute. We borrow the above formulation from [34, Theorem. 4]. See [15, Cor. 1] for a calculation of the implied constants and [25, Cor. 3.7] for an improved dependence on $|C|$.

From (3), in particular conditionally on the Riemann Hypothesis for ζ_E, one immediately gets Conjecture 1.1 for any $\varepsilon > 1/2$. As discussed above, there are unconditional results. However, the case $\varepsilon \leq 1/2$ falls beyond the Generalized Riemann Hypothesis.

1.2. The Chebotarev Density Theorem in function fields.

The function field Chebotarev Density Theorem has a long history, starting with Reichardt [30] who first established it. Lang [21] gave a square-root cancellation, based on the Riemann Hypothesis for curves over finite fields, and explicit estimates were given by Cohen and Odoni in the appendix to [10] and by Halter-Koch [16, Satz 2]. Fried and Jarden [13, Proposition 6.4.8] and Murty and Scherk [19] gave explicit bounds on the error term.

However, unlike the number field case, there are two obstructions in the Chebotarev Density Theorem. One obstruction comes from the arithmetic part of the Frobenius and the other appears when considering short intervals. For a more concise presentation of the obstruction we introduce some notation.

Let q be a power of a prime number p, let $\mathbb{F}_q$ be the finite field of q elements, and let $\mathbb{F}_q(T)$ be the field of rational functions over $\mathbb{F}_q$. We define $\mathcal{P}_{n,q}$ as the set of primes of $\mathbb{F}_q(T)$ of degree n. If $n > 1$, we identify $\mathcal{P}_{n,q}$ with the set of monic irreducible polynomials in the ring of polynomials $\mathbb{F}_q[T]$, and we identify $\mathcal{P}_{1,q}$ with the degree-1 monic polynomials and $1/T$ ‘the infinite prime’. The prime polynomial theorem says that

$$\pi_q(n) = \#\mathcal{P}_{n,q} = \frac{q^n}{n}(1 + O(q^{-n/2})),$$

and so we use $\frac{q^n}{n}$ as an estimate for $\pi_q(n)$.

Given a Galois extension $E/\mathbb{F}_q(T)$ with Galois group $G = \mathrm{Gal}(E/\mathbb{F}_q(T))$, for each $P \in \mathcal{P}_{n,q}$ we define the *Frobenius at* P,

$$\left(\frac{E/\mathbb{F}_q(T)}{P}\right) \subseteq G, \tag{4}$$

as in the number field setting: it is the set of $\sigma \in G$ for which there exists a prime $\mathfrak{P}$ of E lying above P such that

$$\sigma(x) \equiv x^{|P|} \mod \mathfrak{P},$$

for all $x \in E$ which are integral at $\mathfrak{P}$ and where $|P| = q^n$. As before, if P is unramified in E, then $\left(\frac{E/\mathbb{F}_q(T)}{P}\right)$ is a conjugacy class in G. Given a conjugacy class $C \subseteq G$, we set

$$\pi_{C;q}(n;E) = \#\left\{P \in \mathcal{P}_{n,q} : \left(\frac{E/\mathbb{F}_q(T)}{P}\right) = C\right\},$$

the function that counts primes with Frobenius C.

To describe the obstruction for a conjugacy class to be a Frobenius of a prime of degree n, we introduce the restriction map. Let $\mathbb{F}_{q^\nu}$ be the field of scalars of E, that is, the algebraic closure of $\mathbb{F}_q$ in E. Let $\phi\colon \mathbb{F}_{q^\nu} \to \mathbb{F}_{q^\nu}$, $\phi(x) = x^q$ be the generator of the cyclic group $G_0 = \mathrm{Gal}(\mathbb{F}_{q^\nu}/\mathbb{F}_q)$. We have the restriction of automorphisms map $G \twoheadrightarrow G_0$, which is surjective. Since G_0 is abelian, if $C \subseteq G$ is a conjugacy class, then all $\sigma \in C$ map to the same power ϕ_C of ϕ. Then the Chebotarev Density Theorem for function fields says that if $\phi_C = \phi^n$, then

$$\left|\pi_{C;q}(n;E) - \nu\frac{|C|}{|G|}\frac{q^n}{n}\right| \ll \nu\frac{|C|}{|G|}\max\{\mathrm{genus}(E), \frac{|G|}{\nu}\}\frac{q^{n/2}}{n} \tag{5}$$

and otherwise $\pi_{C;q}(n;E) = 0$. The implied constant is absolute.

Next we turn to short intervals. Following Keating and Rudnick [18, §2.1], we define a short interval around a polynomial f of degree n with parameter $0 \le m < n$ to be

$$I(f,m) = \{f + g : \deg g \le m\}.$$

The size of the interval is

$$\#I(f,m) = q^{m+1}.$$

To compare with the number field interval $\{x \le n \le x + x^\varepsilon\}$, we see that x corresponds to $|f| = q^n$ and x^ε corresponds to q^{m+1}, so $\varepsilon = \frac{m+1}{n}$. Having the analogy with number fields in mind, one would naively expect that (5) implies a

Chebotarev Density Theorem for the short interval $I(f,m)$ whenever $m+1>n/2$ (i.e., $\varepsilon>1/2$). However, there seems to be no direct such implication. Letting

$$\pi_{C;q}(I(f,m);E)=\#\left\{P\in P_{n,q}\cap I(f,m):\left(\frac{E/\mathbb{F}_q(T)}{P}\right)=C\right\},$$

then unlike in the number field case, we cannot express $\pi_{C;q}(I(F,m);E)$ as the difference of values of $\pi_{C;q}(n;E)$ in order to utilize the error term (5).

In fact, there is an obstruction to Chebotarev in short intervals coming from the fact that E is not necessarily linearly disjoint from the cyclotomic field L_{n-m-1} associated to a power of the infinite prime (see [32, Chapter 12]). Thus one needs to modify the asymptotic formula according to the intersection of E and L_{n-m-1}. Applying (5) to the compositum of EL_{n-m-1} would yield a Chebotarev in short intervals for $\varepsilon>1/2$. We note that the extensions L_{n-m-1} are wildly ramified at the infinite prime.

Our main result is a Chebotarev Density Theorem for short intervals with any $\varepsilon>0$ for extensions that are tamely ramified at the infinite prime. Thus the result goes beyond the Riemann Hypothesis. For simplicity of presentation we consider only geometric extensions. We indicate at the end of the paper how to handle non-geometric extensions.

Theorem 1.2. *For every $B>0$ there exists a constant M_B satisfying the following property. Let q be a prime power. Let $n>m\geq 2$ if q is odd and $n>m\geq 3$ otherwise. Let G be a finite group and let $E/\mathbb{F}_q(T)$ be a geometric G-extension. Assume that the infinite prime is tamely ramified in the fixed field E^{ab} in E of the commutator of G. Further assume that* $\operatorname{genus}(E),n,|G|\leq B$. *Let $f\in\mathbb{F}_q[T]$ be monic of degree n. Then*

$$\left|\frac{1}{q^{m+1}}\pi_{C;q}(I(f,m);E)-\frac{|C|}{|G|}\frac{1}{n}\right|\leq M_Bq^{-1/2}.$$

It follows in particular that for any $\varepsilon>0$ we have

$$\lim_{n\to\infty}\lim_{q\to\infty}\max_{f,E}\left|\frac{1}{q^{m+1}}\pi_{C;q}(I(f,m);E)-\frac{|C|}{|G|}\frac{1}{n}\right|=0, \tag{6}$$

where E runs over all G-Galois extensions of $\mathbb{F}_q(T)$ of bounded genus that are tamely ramified at infinity and $f\in\mathbb{F}_q[T]$ runs over all monic polynomials of degree n. Hence we have proved a version of Conjecture 1.1 in the function field setting.

It would be desirable to change the order of the limits in (6). As explained above, for $\varepsilon>1/2$ this follows from the Riemann Hypothesis for curves. For $\varepsilon\leq\frac{1}{2}$, it is open and we know of no approach to attack it. A yet more challenging task is to fix q and take $n\to\infty$, and also here the problem is open, and we know of no approach to attack it.

Our method gives more general results, and may be applied for instance to problems about norms. In Theorem 5.1 we count, in the large-q limit, how many polynomials $g \in I(f,m)$ satisfy $(g) = \mathrm{Norm}_{E/\mathbb{F}_q(T)} I$ for some ideal I in $\mathcal{O}_E$. Our most general result is given in Theorem 4.3, for which the terminology of §3–4 is needed.

It would be interesting to generalize our results to a function field of a general curve in place of $\mathbb{F}_q(T)$.

2. Methods

We outline our approach when E is a geometric extension of $\mathbb{F}_q$, which, under the notation used in (5), means that $\nu = 1$. We introduce a general notion of G-factorization arithmetic functions (Definition 3.1), which are arithmetic functions on $\mathbb{F}_q[T]$, whose value on a polynomial $f(T)$ depends only on the Frobenius at the prime factors of $f(T)$. These functions are closely related to Serre's Frobenian functions [33] and to the extensions by Odoni [27, 28] and Coleman [11].

Given a short interval, we relate such an arithmetic function ψ to a class function ψ' on a *subgroup* of the wreath product $G \wr S_n$ using a higher dimensional function field Chebotarev Density Theorem. The main property of this association is that the expected value of ψ on the short interval is asymptotically equal to the average of ψ' on the subgroup, as $q \to \infty$ (Theorem 4.3). The main technical part of the work is to compute the subgroup: it equals to the wreath product $G \wr S_n$ itself.

Applying the above to the indicator function of primes with Frobenius C (Example 3.2) reduces Theorem 1.2 to either a combinatorial computation in $G \wr S_n$ or the classical Chebotarev Density Theorem.

Finally, for the subgroup computation, we take an algebraic approach, using elementary group theory and Artin-Schreier and Kummer theories. Our methods are in the spirit of the works [9, 4, 3] which assume $\mathrm{genus}(E) = 0$ and G cyclic.

3. G-factorization arithmetic functions

For a finite group G we consider the space

$$\hat{\Omega}_G = \{\sigma I : \sigma \in G,\ I \leq G\}$$

of all cosets of subgroups. The group G acts on $\hat{\Omega}_G$ by conjugation and we write

$$\Omega_G = \hat{\Omega}_G / G$$

for the set of conjugacy classes of cosets of subgroups. If $I = 1$ is the trivial subgroup, we identify $\sigma I \in \hat{\Omega}_G$ with σ. So the image of σI in Ω_G is the conjugacy class $C = \{\tau^{-1}\sigma\tau : \tau \in G\}$ of σ.

We want to encode the combinatorial data of degrees, multiplicities, and the Frobenius at the prime factors of a polynomial. A G**-factorization type** is a function

$$\lambda \colon \mathbb{N} \times \mathbb{N} \times \Omega_G \to \mathbb{Z}_{\geq 0}$$

with finite support. We define $\Lambda = \Lambda_G$ to be the set of all G-factorization types. For $\lambda \in \Lambda$ we let

$$\deg(\lambda) = \sum_{d,e,\omega} \lambda(d,e,\omega) de,$$

where the sum runs over $d, e \in \mathbb{N}$ and $\omega \in \Omega_G$. For a monic polynomial $f \in \mathbb{F}_q[T]$ with prime factorization $f = P_1^{e_1} \cdots P_r^{e_r}$ and for a G-Galois extension $E/\mathbb{F}_q(T)$ we define

$$\lambda_{f;E/\mathbb{F}_q(T)}(d,e,\omega) = \#\left\{ i : \deg P_i = d,\ e_i = e,\ \left(\frac{E/\mathbb{F}_q(T)}{P_i}\right) = \omega \right\}.$$

When there is no risk of confusion we simplify the notation and write λ_f for $\lambda_{f;E/\mathbb{F}_q(T)}$. Obviously, we have that $\deg(f) = \deg(\lambda_f)$.

Definition 3.1. A **G-factorization arithmetic function** is a function on G-factorization types. We denote by

$$\Lambda^* = \{\psi \colon \Lambda \to \mathbb{C}\}$$

the space of G-factorization arithmetic functions.

Given a G-Galois extension $E/\mathbb{F}_q(T)$, each $\psi \in \Lambda^*$ induces an arithmetic function $\psi_{E/\mathbb{F}_q(T)}$ on $\mathbb{F}_q[T]$ by setting

$$\psi_{E/\mathbb{F}_q(T)}(f) = \psi(\lambda_{f;E/\mathbb{F}_q(T)}),$$

for monic $f \in \mathbb{F}_q[T]$. By abuse of notation, $\psi_{E/\mathbb{F}_q(T)}$ is also called G-factorization arithmetic function.

Definition 3.1 vastly extends some families of arithmetic functions – see [31, 5] for similar definitions in the cases $E = \mathbb{F}_q(T)$ ($G = \{e\}$) and $E = \mathbb{F}_q(\sqrt{-T})$ ($G = \mathbb{Z}/2\mathbb{Z}$).

The following example of a G-factorization arithmetic function is crucial for our main result.

Example 3.2. Fix a conjugacy class $C \subseteq G$. Consider the G-factorization arithmetic function

$$1_C(\lambda) = \begin{cases} 1, & \text{if } \lambda(d,e,\omega) > 0 \Rightarrow \omega = C \text{ and } d = \deg \lambda, \\ 0, & \text{otherwise.} \end{cases}$$

For any G-Galois extension $E/\mathbb{F}_q(T)$ and monic $f \in \mathbb{F}_q[T]$ we have

$$1_{C,E/\mathbb{F}_q(T)}(f) = \begin{cases} 1, & \text{if } f \text{ is irreducible and } \left(\frac{E/\mathbb{F}_q(T)}{f}\right) = C, \\ 0, & \text{otherwise.} \end{cases}$$

4. G-factorization arithmetic functions on wreath products

Recall the construction of the **permutational wreath product**: Let S_n be the symmetric group on $X = \{1, 2, \ldots, n\}$ (with left action $(\sigma, x) \mapsto \sigma.x$), let G be a finite group, and let

$$G^X := \{\xi \colon X \to G\}$$

be the group of functions from X to G with pointwise multiplication. Then S_n acts (from the right) on G^X by

$$\xi^\sigma(x) = \xi(\sigma.x), \qquad \sigma \in S_n,\ x \in X.$$

The corresponding semidirect product

$$G \wr S_n := G^X \rtimes S_n$$

is the wreath product of G and S_n. For the reader's convenience we recall that the multiplication is given by

$$(\xi_1, \sigma_1)(\xi_2, \sigma_2) = (\xi_1 \xi_2^{\sigma_1^{-1}}, \sigma_1\sigma_2), \qquad \xi_1, \xi_2 \in G^X,\ \sigma_1, \sigma_2 \in S_n.$$

The imprimitive action of $G \wr S_n$ on the set $G \times X$, given explicitly by

$$(\xi, \sigma).(g, x) = (\xi(\sigma.x)g, \sigma.x), \qquad \xi \in G^X,\ \sigma \in S_n,\ g \in G,\ x \in X, \tag{7}$$

makes $G \wr S_n$ into a transitive permutation group.

For $(\xi, \sigma) \in G \wr S_n$ we attach a G-factorization type: Let $\sigma = \sigma_1 \cdots \sigma_r$ be the factorization of σ to disjoint cycles. We include the trivial cycles so that $\sum_{i=1}^r \operatorname{ord}(\sigma_i) = n$. For each $i = 1, \ldots, r$, if we write $\sigma_i = (j_1\ \cdots\ j_d)$, then we set $C_{(\xi,\sigma),\sigma_i}$ to be the conjugacy class in G of the element

$$\xi(j_d) \cdots \xi(j_1).$$

The conjugacy class $C_{(\xi,\sigma),\sigma_i}$ is well defined, since $\xi(j_a) \cdots \xi(j_1)\xi(j_d) \cdots \xi(j_{a+1})$ is conjugate to $\xi(j_d) \cdots \xi(j_1)$. Now we set

$$\lambda_{(\xi,\sigma)}(d, e, \omega) = \begin{cases} 0, & \text{if } e > 1, \\ \#\{i : \operatorname{ord}(\sigma_i) = d,\ C_{(\xi,\sigma),\sigma_i} = w\}, & \text{if } e = 1. \end{cases} \tag{8}$$

Any $\psi \in \Lambda^*$ induces a function $\psi_{G \wr S_n} \colon G \wr S_n \to \mathbb{C}$ by

$$\psi_{G \wr S_n}((\xi, \sigma)) = \psi(\lambda_{(\xi,\sigma)})$$

and we refer to such functions on $G \wr S_n$ as G-factorization arithmetic functions as well. Below we show that the set of G-factorization arithmetic functions on $G \wr S_n$ actually coincides with the set of class functions.

Example 4.1. Recall the G-factorization arithmetic function 1_C from Example 3.2. Then, for $(\xi, \sigma) \in G \wr S_n$ we have

$$1_C(\xi, \sigma) = \begin{cases} 1, & \text{if } \sigma \text{ is an } n\text{-cycle and } C_{(\xi,\sigma),\sigma} = C, \\ 0, & \text{otherwise.} \end{cases}$$

Next, we prove that conjugation in $G\wr S_n$ preserve the G-factorization type. Let $\tau\in S_n$ and identify it with $(1,\tau)\in G\wr S_n$. Then $\tau\sigma\tau^{-1}=\rho_1\cdots\rho_r$ with $\rho_i=\tau\sigma_i\tau^{-1}$. If $\sigma_i=(j_1\ \cdots\ j_d)$, then $\rho_i=(\tau(j_1)\ \cdots\ \tau(j_d))$. Now, as $\tau(\xi,\sigma)\tau^{-1}=(\xi^{\tau^{-1}},\tau\sigma\tau^{-1})$ we have that

$$\xi^{\tau^{-1}}(\tau(j_d))\cdots\xi^{\tau^{-1}}(\tau(j_1))=\xi(j_d)\cdots\xi(j_1) \tag{9}$$

and so $C_{(\xi,\sigma),\sigma_i}=C_{\tau(\xi,\sigma)\tau^{-1},\rho_i}$. We thus conclude that

$$\lambda_{(\xi,\rho)}=\lambda_{\tau(\xi,\rho)\tau^{-1}}.$$

Similarly, if $\eta\in G^X$ and we identify it with $(\eta,1)\in G\wr S_n$, then

$$\eta(\xi,\sigma)\eta^{-1}=(\eta\xi\eta^{-\sigma^{-1}},\sigma) \tag{10}$$

and we have

$$\begin{aligned}&(\eta\xi\eta^{-\sigma^{-1}})(j_d)\cdots(\eta\xi\eta^{-\sigma^{-1}}(j_1))\\&\quad=\eta(j_d)\xi(j_d)\eta(j_{d-1})^{-1}\cdot\eta(j_{d-1})\cdots\eta(j_1)^{-1}\cdot\eta(j_1)\xi(j_1)\eta(j_d)^{-1}\\&\quad=\eta(j_d)\xi(j_d)\cdots\xi(j_1)\eta(j_d)^{-1}.\end{aligned}$$

Here we used that $\sigma_i^{-1}=(j_d\ \cdots\ j_1)$. In particular, $C_{(\xi,\sigma),\sigma_i}=C_{\eta(\xi,\sigma)\eta^{-1},\sigma_i}$ and thus

$$\lambda_{(\xi,\rho)}=\lambda_{\eta(\xi,\rho)\eta^{-1}}.$$

We thus deduce that if (ξ,σ) and (η,ρ) are conjugate, then $\lambda_{(\xi,\rho)}=\lambda_{(\eta,\rho)}$.

The converse is also true. Indeed, $\lambda_{(\xi,\sigma)}=\lambda_{(\zeta,\rho)}$ implies that we have r conjugacy classes $C_1,\dots,C_r$ (possibly with repetitions) and factorization to disjoint cycles $\rho=\rho_1\cdots\rho_r$ and $\sigma=\sigma_1\cdots\sigma_r$ such that $\operatorname{ord}(\sigma_i)=\operatorname{ord}(\rho_i)$ and

$$C_{(\xi,\sigma),\sigma_i}=C_i=C_{(\zeta,\rho),\rho_i}.$$

Without loss of generality we may assume that $\sigma=\rho$ and $\sigma_i=\rho_i$ for all i (indeed, conjugate by $\tau\in S_n$ such that $\tau\sigma_i\tau^{-1}=\rho_i$ for all i and use (9)). Thus, if $\sigma_i=(j_1\ \cdots\ j_d)$, then

$$g\xi(j_d)\cdots\xi(j_1)g^{-1}=\zeta(j_d)\cdots\zeta(j_1)$$

for some $g\in G$. By (10) it suffices to find $\eta\in G^X$ such that $\eta\xi\eta^{-\sigma^{-1}}=\zeta$. Defining

$$\eta(j_d)=g\quad\text{and}\quad\eta(j_a)=\zeta^{-1}(j_{a+1})\eta(j_{a+1})\xi(j_{a+1}),\ 1\le a\le d-1$$

on the orbits of σ_i, for each σ_i gives the desired solution. We thus proved

Lemma 4.2. *The elements (ξ,σ), $(\zeta,\rho)\in G\wr S_n$ are conjugate if and only if $\lambda_{(\xi,\sigma)}=\lambda_{(\zeta,\rho)}$.*

In particular, every class function on $G\wr S_n$ may be realized as a G-factorization arithmetic function.

We prove the following general theorem which connects the averages of a G-factorization arithmetic function on a short interval to the average on the wreath product. A piece of notation is needed: for a non-empty finite set X and a function ψ on X we denote the mean value by

$$\langle \psi(f) \rangle_{f\in X} := \frac{1}{\#X}\sum_{f\in X}\psi(f).$$

Theorem 4.3. *For every $B>0$ there exists a constant M_B satisfying the following property. Let q be a prime power. Let $n>m\geq 2$ if q is odd and $n>m\geq 3$ otherwise. Let G be a finite group and let $E/\mathbb{F}_q(T)$ be a geometric G-extension. Assume that the infinite prime is tamely ramified in the fixed field E^{ab} in E of the commutator of G. Let $f_0\in\mathbb{F}_q[T]$ be monic of degree n, and $\psi\in\Lambda^*$. Assume that* $\mathrm{genus}(E), n, |G|\leq B$. *Then*

$$\left| \left\langle \psi_{E/\mathbb{F}_q(T)}(f) \right\rangle_{\deg(f-f_0)\leq m} - \langle \psi_{G\wr S_n}(\tau)\rangle_{\tau\in G\wr S_n} \right| \leq M_B q^{-1/2} \max_{\deg(\lambda)=n} |\psi(\lambda)|.$$

We postpone the proof of Theorem 4.3 to §7.

5. Applications of Theorem 4.3

From Theorem 4.3 it follows immediately that in the large-q limit, the average on a short interval is the same as on the 'long interval' — the set of all degree-n monics

$$M_{n,q} = I(T^n, n-1).$$

Moreover, Theorem 4.3 reduces the computations of averages of arithmetic functions to combinatorics of group theory. This also works vice versa.

5.1. Proof of Theorem 1.2.

We give two proofs to exemplify the ways to apply Theorem 4.3.

First proof: The assumptions allow us to apply Theorem 4.3 with the G-factorization arithmetic function 1_C, and to get that the average on a short interval is the same as over a long interval. The latter is given by (5), as needed.

Second proof: The assumptions allow us to apply Theorem 4.3 with the G-factorization arithmetic function 1_C, and to get that the average on a short interval is the same as on the wreath product. We compute the latter: Using Example 4.1, we find that $1_C(\xi,\sigma)\neq 0$ implies that $\sigma=(j_1\ \cdots\ j_n)$ is an n-cycle and $\xi(j_n)\cdots\xi(j_1)\in C$. So we may choose $\xi(j_1),\ldots,\xi(j_{n-1})$ arbitrarily and then we have $|C|$ choices for $\xi(j_n)$. So

$$\langle 1_C(\xi,\sigma)\rangle_{(\xi,\sigma)\in G\wr S_n} = \frac{(n-1)!|G|^{n-1}|C|}{n!|G|^n} = \frac{1}{n}\frac{|C|}{|G|},$$

as needed. □

5.2. **Norms in short intervals.** Here we discuss two G-factorization arithmetic functions related to norms, and our results on their mean value in short intervals. For a function field $E/\mathbb{F}_q(T)$, we define the following arithmetic functions. For $f \in M_{n,q}$, we define

$$b_{E/\mathbb{F}_q(T)}(f) = \begin{cases} 1, & \text{if } \exists I \subseteq \mathcal{O}_E : (f) = \mathrm{Norm}_{E/\mathbb{F}_q(T)}(I), \\ 0, & \text{otherwise,} \end{cases}$$
$$r_{E/\mathbb{F}_q(T)}(f) = \#\{I \text{ ideal in } \mathcal{O}_E : \mathrm{Norm}_{E/\mathbb{F}_q(T)}(I) = (f)\}.$$

The number field versions of r, b were studied extensively: Let $E/\mathbb{Q}$ be a finite extension. Odoni [26, Thm. 1] computed the asymptotic of the mean value of $b_{E/\mathbb{Q}}$. When $E/\mathbb{Q}$ is Galois, the work of Ramachandra [29] gives the mean value of $b_{E/\mathbb{Q}}$ in $[x, x + x^{\varepsilon}]$ for some $0 < \varepsilon < 1$.

Weber [39] computed the mean value of $r_{E/\mathbb{Q}}$, and studied the error term. We refer to Bourgain and Watt [7, Thm. 2] for the state-of-the-art result on the error term when $E = \mathbb{Q}(i)$, and to Lao [22] for more general E. These results in particular gives the expected asymptotics for the mean value of $r_{E/\mathbb{Q}}$ in $[x, x + x^{\varepsilon}]$ for some $0 < \varepsilon < 1$.

In Appendix A, we prove a function field analogue of Odoni's result on the average of $b_{E/\mathbb{F}_q(T)}$ in long intervals when $E/\mathbb{F}_q(T)$ is Galois. This is to be done in the most general limit $q^n \to \infty$. Appendix A also treats $r_{E/\mathbb{F}_q(T)}$ for which the rationality of the corresponding Dedekind zeta function gives a closed formula for the mean value.

The result to be presented is a computation of the mean values in short intervals.

Theorem 5.1. *For every $B > 0$ there exists a constant M_B satisfying the following property. Let q be a prime power. Let $n > m \geq 2$ if q is odd and $n > m \geq 3$ otherwise. Let G be a finite group and let $E/\mathbb{F}_q(T)$ be a geometric G-extension which has is tamely ramified at the infinite prime. Let $f_0 \in \mathbb{F}_q[T]$ monic of degree n. Assume that* $\mathrm{genus}(E), n, |G| \leq B$. *Then*

$$\left\langle b_{E/\mathbb{F}_q(T)}(f) \right\rangle_{\deg(f-f_0)\leq m} = 1 + O_B(q^{-1/2}),$$
$$\left\langle r_{E/\mathbb{F}_q(T)}(f) \right\rangle_{\deg(f-f_0)\leq m} = \binom{n + \frac{1}{|G|} - 1}{n} + O_B(q^{-1/2}).$$

To see how Theorem 5.1 is deduced from Theorem 4.3 we need to express r, b as G-factorization arithmetic functions (Example 5.3) and to compute the mean value on the wreath product, or alternatively apply the results from Appendix A.

Let $E/\mathbb{F}_q(T)$ be a Galois extension. Given a prime polynomial $P \in \mathbb{F}_q[T]$, we denote by $g(P; E)$, $f(P; E)$ and $e(P; E)$ the number of distinct primes in E lying above P, the inertia degree of P in E and the ramification index of P, respectively.

Lemma 5.2. *Let $E/\mathbb{F}_q(T)$ be a geometric G-extension.*

(1) The functions $b_{E/\mathbb{F}_q(T)}$ and $r_{E/\mathbb{F}_q(T)}$ are multiplicative.

(2) Let $f \in M_{n,q}$ with prime factorization $f = \prod_{i=1}^k P_i^{a_i}$. Then

$$b_{E/\mathbb{F}_q(T)}(f) = \begin{cases} 1, & \text{if } f(P_i;E) \mid a_i \text{ for all } i, \\ 0, & \text{otherwise,} \end{cases} \tag{11}$$

and if we put $b_i = a_i/f(P_i;E)$ and $g_i = g(P_i;E)$, then we have

$$r_{E/\mathbb{F}_q(T)}(f) = b_{E/\mathbb{F}_q(T)}(f) \cdot \prod_{i=1}^k \binom{b_i + g_i - 1}{g_i - 1}. \tag{12}$$

Proof. Let P be a prime polynomial and let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_E$ lying above P. Then

$$\mathrm{Norm}_{E/\mathbb{F}_q(T)}\mathfrak{P} = (P)^{f(P;E)}.$$

By multiplicativity of the norm map and by unique factorization in $\mathcal{O}_E$, it follows that the image of $\mathrm{Norm}_{E/\mathbb{F}_q(T)}$ on the non-zero ideals in $\mathcal{O}_E$ is the semigroup generated by $\{(P)^{f(P;E)}\}_{P \in \mathcal{P}_q}$, which establishes (11). It now immediately follows that $b_{E/\mathbb{F}_q(T)}$ is multiplicative.

If f_1 and f_2 are relatively prime polynomials, then from unique factorization of ideals in $\mathcal{O}_E$, every ideal I of $\mathcal{O}_E$ with $\mathrm{Norm}_{E/\mathbb{F}_q(T)}I = (f_1 f_2)$ has a unique factorization $I = I_1 I_2$, with $\mathrm{Norm}_{E/\mathbb{F}_q(T)}I_j = (f_j)$. Indeed, if $I = \prod \mathfrak{P}_i^{a_i}$ take I_j be the product of $\mathfrak{P}_i^{a_i}$ with $\mathfrak{P}_i \mid f_j$. Thus,

$$r_{E/\mathbb{F}_q(T)}(f_1 f_2) = \sum_{\mathrm{Norm}_{E/\mathbb{F}_q(T)}I = (f_1 f_2)} 1 = \sum_{\substack{\mathrm{Norm}_{E/\mathbb{F}_q(T)}I_1 = (f_1) \\ \mathrm{Norm}_{E/\mathbb{F}_q(T)}I_2 = (f_2)}} 1 = r_{E/\mathbb{F}_q(T)}(f_1) r_{E/\mathbb{F}_q(T)}(f_2).$$

This implies that $r_{E/\mathbb{F}_q(T)}$ is multiplicative. In particular, it suffices to prove (12) for $f = P^a$ a prime power.

If $f(P;E) \nmid a$, then $b_{E/\mathbb{F}_q(T)}(P^a) = 0$, hence also $r_{E/\mathbb{F}_q(T)}(P^a) = 0$. Assume now that $f(P;E) \mid a$ and let $b = a/f(P;E)$. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ be the primes of $\mathcal{O}_E$ lying above P. Since $\mathrm{Norm}_{E/\mathbb{F}_q(T)}\mathfrak{P}_j = P^{f(P;E)}$, the solutions to $\mathrm{Norm}_{E/\mathbb{F}_q(T)}I = P^a$, are of the form $I = \prod_{j=1}^g \mathfrak{P}_j^{c_j}$ with $c_j \geq 0$ and $\sum_{j=1}^g c_j = b$. As there are $\binom{b+g-1}{g-1}$ many such sequences of c_j, the proof is done. □

Lemma 5.2 allows us to realize $b_{E/\mathbb{F}_q(T)}$, $r_{E/\mathbb{F}_q(T)}$ as G-factorization arithmetic functions.

Example 5.3. Let $\omega \in \Omega_G$, and let $\Sigma \in \omega$. So Σ is a coset of a subgroup of G, say $\Sigma = \sigma I$. Let $e_\omega = |I|$, $f_\omega = [\langle \sigma, I \rangle : I]$, and $g_w = |G|/e_w f_w$. Now we define the G-factorization arithmetic functions

$$\begin{aligned} b(\lambda) &= \begin{cases} 1, & \text{if } \lambda(d,a,\omega) > 0 \Rightarrow f_\omega \mid a, \\ 0, & \text{otherwise.} \end{cases} \\ r(\lambda) &= b(\lambda) \cdot \prod_{(d,a,w)} \binom{a/f_w + g_w - 1}{g_w - 1}^{\lambda(d,a,w)} \end{aligned} \tag{13}$$

Let $E/\mathbb{F}_q(T)$ be a geometric G-Galois extension. Then

$$b_{E/\mathbb{F}_q(T)}(f) = b(\lambda_{f;E/\mathbb{F}_q(T)}) \quad \text{and} \quad r_{E/\mathbb{F}_q(T)}(f) = r(\lambda_{f;E/\mathbb{F}_q(T)}). \tag{14}$$

Indeed, by (11) and (12), it suffices to note that $w = \left(\frac{E/\mathbb{F}_q(T)}{P}\right)$, then $e_w = e(P;E)$, $f_w = f(P;E)$, and $g_w = g(P;E)$.

Proof of Theorem 5.1. By Theorem 4.3, it suffices to compute the average of the G-factorization arithmetic functions b and r given in (14) on the group $G \wr S_n$. For brevity we compute them together by computing the average of r^s for any $s \in \mathbb{C}$ (and noting that $r = r^1$ and $b = r^0$). Put $N = |G|$ and let $s \in \mathbb{C}$. We show that

$$\left\langle r^s_{G\wr S_n}(\xi,\sigma)\right\rangle_{(\xi,\sigma)\in G\wr S_n} = \binom{n + N^{s-1} - 1}{n}.$$

Let $\sigma = \sigma_1 \cdots \sigma_r$ be the factorization of $\sigma \in S_n$ to disjoint cycles and let $\xi \in G^n$. Recall that if we write $\sigma_i = (j_1 \ \cdots \ j_\ell)$, then $C_{(\xi,\sigma),\sigma_i}$ is defined to be the conjugacy class of the element

$$\xi(j_\ell)\cdots\xi(j_1).$$

Let $d, a \geq 1$ and $\omega \in \Omega_G$ with $\lambda_{(\xi,\sigma)}(d,a,\omega) > 0$. Then $a = 1$ and $\omega = C_{(\xi,\sigma),\sigma_i}$ for some i. In particular, $e_\omega = 1$, and thus $f_\omega = 1$ if and only if $C_{(\xi,\sigma),\sigma_i} = 1$, where e_ω and f_ω are as defined in Example 5.3.

By (13), we have that $r^s_{G\wr S_n}(\xi,\sigma) \neq 0$ if and only if $f_\omega \mid a$ for all (d,a,ω) with $\lambda_{(\xi,\sigma)}(d,a,\omega) > 0$. So if $r^s_{G\wr S_n}(\xi,\sigma) \neq 0$, then $a = 1$, hence $f_\omega = 1$, and so $C_{(\xi,\sigma),\sigma_i} = 1$, for all i. As $g_\omega = \frac{N}{e_\omega f_\omega} = N$, and so $\binom{a/e+g-1}{g-1} = N$, we deduce from (13) that

$$r^s_{G\wr S_n}(\xi,\sigma) = \begin{cases} \prod_{(d,a,\omega):\lambda_{(\xi,\sigma)}(d,a,\omega)>0} N^{s\lambda_{(\xi,\sigma)}(d,a,\omega)}, & \text{if } C_{(\xi,\sigma),\sigma_i} = 1 \text{ for all } i,\\ 0, & \text{otherwise.}\end{cases}$$

Put

$$X_n = \{(\xi,\sigma) \in G \wr S_n : C_{(\xi,\sigma),\sigma_i} = 1, \forall i\},$$

so that

$$\left\langle r^s_{G\wr S_n}(\xi,\sigma)\right\rangle_{(\xi,\sigma)\in G\wr S_n} = \frac{\sum_{(\xi,\sigma)\in X_n}(N^s)^{r(\sigma)}}{\# G \wr S_n}, \tag{15}$$

where $r(\sigma)$ is the number of cycles in σ. For a fixed $\sigma \in S_n$ with a factorization $\sigma = \sigma_1 \ldots \sigma_r$ to disjoint cycles, we have

$$\sum_{\xi\in G^n:(\xi,\sigma)\in X_n} (N^s)^{r(\sigma)} = (N^s)^r N^{n-r} = N^n \cdot (N^{s-1})^r, \tag{16}$$

since if $\sigma_i = (j_1 \ \ldots \ j_d)$, then $\xi(j_1), \ldots, \xi(j_{d-1})$ can be chosen arbitrarily and $\xi(j_d)$ must be equal to $\prod_{k=1}^{d-1}\xi(j_k)^{-1}$, so we lose one power of N for each orbit. Plugging

(16) in (15), we find that

$$\left\langle r^s_{G\wr S_n}(\xi,\sigma)\right\rangle_{(\xi,\sigma)\in G\wr S_n}=\frac{\sum_{\sigma\in S_n}(N^{s-1})^{r(\sigma)}}{\#S_n}. \tag{17}$$

We apply the exponential formula for permutations [37, Cor. 5.1.9] with $f(i)=N^{s-1}$ the constant function and h defined by $h(0)=1$ and

$$h(i)=\sum_{\sigma\in S_i}(N^{s-1})^{r(\sigma)}.$$

Then the formula gives that

$$E(x):=\sum_{i=0}^{\infty}h(i)\frac{x^i}{i!}=\exp(\sum_{i\geq 1}N^{s-1}\frac{x^i}{i}).$$

As $\sum_{i\geq 1}x^i/i=-\ln(1-x)$, we can simplify the right hand side using the binomial series to get that

$$E(x)=(1-x)^{-N^{s-1}}=\sum_{i\geq 0}(-1)^i\binom{-N^{s-1}}{i}x^i.$$

In particular, by (17) we have

$$\left\langle r^s_{G\wr S_n}(\xi,\sigma)\right\rangle_{(\xi,\sigma)\in G\wr S_n}=\frac{h(n)}{n!}=(-1)^n\binom{-N^{s-1}}{n}=\binom{n+N^{s-1}-1}{n},$$

as needed. □

6. Galois Theory

6.1. *G*-factorization arithmetic functions and the Frobenius automorphism.

Let ψ be a G-factorization arithmetic function and $E/\mathbb{F}_q(T)$ a G-Galois geometric extension. The goal of this section is, for a given $a=(a_0,\dots,a_{n-1})\in\mathbb{F}_q^n$, to naturally construct an element $\phi_a\in G\wr S_n$ such that

$$\psi_{E/\mathbb{F}_q(T)}(T^n+a_{n-1}T^{n-1}+\cdots+a_0)=\psi_{G\wr S_n}(\phi_a). \tag{18}$$

We start with a general construction which we later specialize to our setting. Let F be a field and $\pi\colon C\to\mathbb{A}^1_F$ a branched covering of smooth geometrically connected F-curves with function field extension $E/F(T)$. Assume that $E/F(T)$ is Galois with Galois group G.

This gives rise to the following cover of varieties with corresponding function fields

$$\begin{tikzcd}
C^n \arrow[d, "\pi^n"] & & E_1\cdots E_n \arrow[d, dash] \\
\mathbb{A}^n_F \arrow[d, "s"] & & F(Y_1,\dots,Y_n) \arrow[d, dash] \\
\mathbb{A}^n_F = \mathbb{A}^n/S_n & & F(A_0,\dots,A_n).
\end{tikzcd} \tag{19}$$

Here S_n acts on $\mathbb{A}^n$ by permuting the coordinates: if $(Y_1,\dots,Y_n)$ are the coordinates of $\mathbb{A}^n$ and $(A_0,\dots,A_{n-1})$ of $\mathbb{A}^n = \mathbb{A}^n/S_n$, then the map s is given by

$$A_0 = (-1)^n Y_1\cdots Y_n \quad , \quad \dots \quad , \quad A_{n-1} = -(Y_1+\dots+Y_n).$$

Also, E_i is the function field of the i-th copy of C in C^n, in particular, for every i there exists an isomorphism

$$\varphi_i\colon E_i \to E \tag{20}$$

with $\varphi_i(Y_i) = T$ that fixes F. Put $\varphi_{i,j}\colon E_i \to E_j$ to be $\varphi_j^{-1}\circ\varphi_i$. Let $D_1(T)\mathbb{F}_q[T]$ be the discriminant ideal of π and $D_2(A_0,\dots,A_{n-1}) = \mathrm{disc}_T(T^n+A_{n-1}T^{n-1}+\dots+A_0)$ and put

$$D(A_0,\dots,A_{n-1}) = D_2(A_0,\dots,A_{n-1})\prod_i D_1(Y_i) \in F[A_0,\dots,A_{n-1}] \tag{21}$$

which is a non-zero polynomial in the A_i-s. Then, for a point $a\in\mathbb{A}^n(F)$ we have

$$D(a)\neq 0 \Longrightarrow \ a \text{ is unramified in } C^n. \tag{22}$$

If we write $f(T) = T^n + a_{n-1}T^{n-1}+\dots+a_0$, then the condition $D(a)\neq 0$ is equivalent to f being a separable polynomial that does not vanish on the branch points of π which are exactly the roots of D_1. The Riemann-Hurwitz formula (see e.g. [13, Thm. 3.6.1]) gives that $\deg D_1 \ll \mathrm{genus}(C) + |G|$. On the other hand, $\deg D_2 \ll n$. So, if $B \geq \max\{\mathrm{genus}(C), |G|, n\}$ then $\deg D$ is bounded in terms of B.

The extension $E_1\cdots E_n/F(A_1,\dots,A_n)$ is a Galois extension with Galois group isomorphic to $G\wr S_n$. More explicitly, the action of an element $(\xi,\sigma)\in G\wr S_n$ on $E_1\cdots E_n$ is given by

$$(\xi,\sigma).e_i = \xi(\sigma(i))(\varphi_{i,\sigma(i)}(e_i)), \qquad e_i\in E_i. \tag{23}$$

This is compatible with the imprimitive action (7).

If $F=\mathbb{F}_q$ is a finite field, then any point $a\in\mathbb{A}^n(F)$ with $D(a)\neq 0$ induces a Frobenius conjugacy class $\phi_a\subseteq G\wr S_n$, which is the higher dimensional version of (4) and is defined similarly. Now we can prove (18):

Proposition 6.1. *Let $F = \mathbb{F}_q$, let $f(X) = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in \mathbb{F}_q[T]$ such that the point $a = (a_0, \dots, a_{n-1})$ is unramified in C^n and let $\phi_a \subseteq G \wr S_n$ be the Frobenius conjugacy class. Then (18) holds for every $\psi \in \Lambda^*$.*

Proof. To ease notation we identify each of the E_i with E via the map ϕ_i. Let $f = P_1 \cdots P_r$ be the prime factorization of f with P_i monic irreducible of degree d_i. For each $i = 1, \dots, r$, let $\alpha_{i,1} \in \mathbb{A}^1(\overline{\mathbb{F}}_q)$ be a root of P_i and $\beta_{i,1} \in C(\overline{\mathbb{F}}_q)$ with $\alpha_{i,1} = \pi(\beta_{i,1})$ and let $\alpha_{i,j} = \alpha_{i,1}^{q^{j-1}}$ be the other roots, and respectively $\beta_{i,j} = \beta_{i,j}^{q^{j-1}}$, $j = 1, \dots, d_i - 1$. We replace the indices of C^n and of the middle $\mathbb{A}^n$ in (19) to be $I = \{(i, j) : i = 1, \dots, r,\ j = 1, \dots, d_i\}$.

So $(\beta_{i,j})_{(i,j)\in I} \in C^n(\overline{\mathbb{F}}_q)$ maps under π^n to $(\alpha_{i,j})_{(i,j)\in I} \in \mathbb{A}^n(\overline{\mathbb{F}}_q)$ which maps under s to $a = (a_0, \dots, a_{n-1}) \in \mathbb{A}^n(\mathbb{F}_q)$.

To this end, let ϕ_a be the corresponding Frobenius element of $(\beta_{i,j})_{(i,j)\in I}$ and let $h \in E_{i,1}$ be a rational function that is regular at all $\beta_{i,j}$. Then, by definition,

$$(\phi_a^{d_i} h)(\beta_{i,1}) = (h(\beta_{i,1}))^{q^{d_i}}.$$

Write $\phi_a = (\xi, \sigma)$; then $\phi_a^{d_i} = (\prod_{k=1}^{d_i} \xi^{\sigma^{k-1}}, \sigma^{d_i})$. The coordinate $\sigma \in S_n$ is induced from the action of the Frobenius automorphism on the roots of f, so since $\alpha_{i,j} = \alpha_{i,1}^{q^{j-1}}$, we have that $Y_{i,j} = \sigma^j(Y_{i,1})$, $j = 0, \dots, d_i - 1$ and $Y_{i,1} = \sigma^{d_i}(Y_{i,1})$. The latter also implies that $E_{i,1}$ maps to itself under σ^{d_i}, hence

$$(\phi_a^{d_i} h)(\beta_{i,1}) = (\prod_{k=1}^{d_i} \xi^{\sigma^{k-1}}(i, 1)h)(\beta_{i,1}) = (\prod_{j=1}^{d_i} \xi(i, j)h)(\beta_{i,1}).$$

To conclude, we obtained

$$(\prod_{j=1}^{d_i} \xi(i, j)h)(\beta_{i,1}) = (h(\beta_{i,1}))^{q^{d_i}},$$

but the Frobenius at P_i in E is the unique element of G satisfying this, so $\mathrm{Frob}_{P_i} = \prod_{j=1}^{d_i} \xi(i, j)$. Thus, $\lambda_{\phi_a} = \lambda_{f;E/\mathbb{F}_q(T)}$, which completes the proof. □

6.2. **Computation of a Galois group.** We keep the notation as in §6.1, in particular F is a field and $\pi : C \to \mathbb{A}^1_F$ is a branched covering of geometrically irreducible F-curves that is generically Galois with Galois group G. For $a = (a_0, \dots, a_{n-1}) \in \mathbb{A}^n$ and for $0 \le m < n$, we consider the following subspace of $\mathbb{A}^n$

$$W = W_{a,m} = \{(w_0, \dots, w_{n-1}) \in \mathbb{A}^n : w_i = a_i,\ i = m+1, \dots, n-1\} \cong \mathbb{A}^{m+1}. \tag{24}$$

So if $\mathbb{A}^n$ is the space of coefficients of polynomials, then W is the short interval $I(T^n + a_{n-1}T^{n-1} + \cdots + a_0, m)$. Let U and V be irreducible components of $(s \circ \pi^n)^{-1}(W)$ and $s^{-1}(W)$, respectively. Let M, L, and K be the function fields of U, V, and W, where $A_0, \dots, A_m$ are independent variables and the y_i-s satisfy

$$\begin{tikzcd}
C^n \arrow[d, "\pi^n"] & U \arrow[l] \arrow[d, "\pi^n"] \\
\mathbb{A}^n_F \arrow[d, "s"] & V \arrow[l] \arrow[d, "s"] \\
\mathbb{A}^n_F & W \arrow[l]
\end{tikzcd}
\qquad
\begin{tikzcd}
M \arrow[d, dash] \\
L = K(y_1, \ldots, y_n) \arrow[d, dash] \\
K = F(A_0, \ldots, A_m)
\end{tikzcd}$$

Figure 1. Variety and field diagrams

$$f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_{m+1}T^{m+1} + A_mT^m + \cdots + A_0 = \prod_{i=1}^{n}(T - y_i).$$

Then, M/K is a Galois extension and if $D(a_{n-1}, \ldots, a_{m+1}, A_m, \ldots, A_0) \neq 0$, then by (22), it is unramified, hence its Galois group is canonically isomorphic to the subgroup the generic Galois group $G \wr S_n$ given in (23); namely all elements that generically map U to itself. We identify $\mathrm{Gal}(M/K)$ with this subgroup, in particular

$$H = \mathrm{Gal}(M/L) \leq G^n.$$

We have that $\mathrm{Gal}(M/K)$ equals $G \wr S_n$ if and only if $(s \circ \pi^n)^{-1}(W)$ is irreducible, i.e. equals to U.

We prove that this is indeed the case if the ramification at infinity is tame.

Proposition 6.2. *Under the notation above, assume that $m \geq 2$ if q is odd and $m \geq 3$ if q is even. Further assume that the infinite prime is tamely ramified in the fixed field E^{ab} in E of the commutator of G. Then*

$$\mathrm{Gal}(M/K) = G \wr S_n.$$

Remark 6.3. Proposition 4.6 in [3] coincides with the special case of Proposition 6.2 where $G = \mathbb{Z}/2\mathbb{Z}$, $C = \mathbb{A}^1$ and $\pi(x) = x^2$. Cyclic extensions with genus 0 were partly treated by Cohen [9, Thm. 12].

6.2.1. *Reduction steps.* Since by [4, Proposition 3.6], $\mathrm{Gal}(L/K) = S_n$ and since $\mathrm{Gal}(M/K) \leq G \wr S_n$, in order to prove that $\mathrm{Gal}(M/K) = G \wr S_n$ it suffices to show that $H = G^n$.

The proof of Proposition 6.2 is reduced, by elementary finite group theory, to the following statements:

Lemma 6.4. *Proposition 6.2 holds true if G is abelian.*

Lemma 6.5. *For each $i \neq j$ the projection on the i, j-th coordinates $H \to G^n \to G^2$ is surjective.*

Proof that Lemmas 6.4 and 6.5 imply Proposition 6.2. From Lemma 6.4 applied to the abelianization G^{ab} of G, we get that H surjects onto $(G^{\text{ab}})^n$. This in particular means that H is contained in no proper normal subgroup with abelian quotient. By Lemma 6.5, H surjects onto any projection to two coordinates. To finish the proof we need that these two group theoretical properties suffice to imply that $H = G^n$ and this is indeed the case, as the lemma below shows. □

Lemma 6.6. *Let H be a subgroup of G^n. Suppose that H maps surjectively onto G^2 under each possible projection onto two copies. If H is a proper subgroup of G^n, then it is contained in a proper normal subgroup with abelian quotient.*

Proof. The case $n = 2$ is trivial, and by induction, we may assume this is true for $n-1$ and that $n \geq 3$. If any map from H to the product of $n-1$ copies of G is not surjective, then the image of H is contained in a normal subgroup with abelian quotient, so H is as well. So we may assume that the projections from H to any product of $n-1$ copies of G are surjective. Now apply Goursat's lemma to G^{n-1} and G. We get that there is a group G', surjections $a\colon G^{n-1} \to G'$ and $b\colon G \to G'$, such that H consists of tuples $(g_1, \dots, g_n)$ in G^n with $a(g_1, ..., g_{n-1}) = b(g_n)$. Moreover since H is a proper subgroup, G' is non-trivial.

Now because the map $H \to G^{n-1}$ obtained by dropping the i-th coordinate is surjective, for any g_n there exists some g_i such that $(e, \dots, e, g_i, e, \dots, g_n) \in H$, and so $a(e, \dots, e, g_i, \dots, e) = b(g_n)$. Putting $G_1 = \{(g_1, e, \dots, e) : g_1 \in G\}$ and $G_2 = \{(e, g_2, e, \dots, e) : g_2 \in G\}$, we conclude that a maps both G_1 and G_2 onto G'. Thus as G_1 and G_2 commute, we get that G' must be abelian. Thus the pre-image of G' is the desired normal subgroup with abelian quotient. □

To finish the proof of Proposition 6.2, it remains to prove Lemmas 6.4 and 6.5. Since the former lemma is technical, we start by proving the latter assuming the former.

6.2.2. *Proof of Lemma 6.5 using Lemma 6.4.* We look at the covering Υ of W defined by adjoining two roots y_i, y_j of the polynomial; i.e., Υ is the quotient space of V under the action of S_{n-2}, so $\mathrm{Gal}(V/\Upsilon) \cong S_{n-2}$, the group of all permutations fixing i, j. Let Γ be the Galois group of U/Υ. So, the restriction-of-automorphisms map induces a surjection $\Gamma \to \mathrm{Gal}(V/\Upsilon) = S_{n-2}$.

The covering Υ maps to $\mathbb{A}^2$ by sending to the two roots. The fibers are connected because we just add two congruence conditions. We have the covering $C^2 \to \mathbb{A}^2$ with Galois group G^2, and its fiber product $\Upsilon \times_{\mathbb{A}^2} (C^2)$ is geometrically connected, since the fiber of $\Upsilon \to \mathbb{A}^2$ is geometrically connected. This implies that Γ surjects onto G^2.

We apply Goursat's lemma to these two maps. They are jointly surjective unless some quotient of G^2 matches some quotient of S_{n-2}. But all normal subgroups of S_{n-2} are contained in A_{n-2}, so this can only happen if there is some non-trivial relation with order two quotients of G. This is not possible by the abelian case, hence the proof is done. □

The proof of Lemma 6.4 is more technical and requires some preparation.

6.2.3. *Some more group theory.* This section contains well known facts that we summarize for the convenience of the reader. We start by stating two well known facts on the symmetric group. The first is on normal subgroups:

Lemma 6.7. *Let $n \geq 1$. The group S_n does not have any normal subgroups of odd prime index.*

The second is about the invariant subspaces of the standard representation of S_n on $\mathbb{F}_p^n$ acting by permuting the coordinates.

Lemma 6.8. *The invariant subspaces of $\mathbb{F}_p^n$ under S_n ($n \geq 3$) are:*

(1) $V_0 = \{(0, \ldots, 0)\}$,
(2) $V_1 = \mathrm{sp}_{\mathbb{F}_p}\{(1, \ldots, 1)\}$,
(3) $V_{n-1} = \{(x_1, \ldots, x_n) \in \mathbb{F}_p^n : \sum_{i=1}^n x_i = 0\}$, *and*
(4) $V_n = \mathbb{F}_p^n$.

Recall that the Frattini subgroup $\Phi(G)$ of a group G is defined by $\Phi(G) = \bigcap_{U \leq_m G} U$, where the intersection is over the maximal subgroups of G. It has the property that for every $H \leq G$, if $H/H \cap \Phi(G) = G/\Phi(G)$, then $H = G$. If G is finite and $p \mid |G|$, then the subgroup $\Phi_p(G) = [G, G]G^p$ generated by commutators and p-th power of elements is normal and $G/\Phi_p(G) \cong (\mathbb{Z}/p\mathbb{Z})^r$. Thus,

$$\Phi_p(G) = U_1 \cap \cdots \cap U_r, \tag{25}$$

with U_i the kernel of the projection on the i-th coordinate, so U_i is normal in G of index p.

Lemma 6.9. *Let G be a finite abelian group and $H \leq G$. Assume that $H/(H \cap \Phi_p(G)) \cong G/\Phi_p(G)$ for every $p \mid |G|$. Then $H = G$.*

Proof. Since G is abelian, $\Phi(G) = \bigcap_{p||G|} \Phi_p(G)$ and $G/\Phi(G) \cong \prod_{p||G|} G/\Phi_p(G)$. So the assumption gives that $H/(H \cap \Phi(G)) = G/\Phi(G)$ and so $H = G$. □

Let L be a field and p a prime. If $p \nmid \mathrm{char}(L)$ let $\wp(x) = x^p$ and $L^\circ = L^\times$, otherwise let $\wp(x) = x^p - x$ and $L^\circ = L$. We say that elements in L° are p-independent if they are linearly independent in $L^\circ/\wp(L^\circ)$, considered as a $\mathbb{F}_p$-vector space.

Lemma 6.10. *Let G be a finite abelian group and $H \leq G$. Let L be a field such that for every $p \mid |G|$, either L contains a primitive p-th root of unity or L is of characteristic p. Let M/L be an H-Galois extension. For a prime divisor p of $|G|$, put $U_1, \ldots, U_{r(p)}$ as in (25). Then, for every $1 \leq i \leq r$ there exists $\alpha_{i,p} \in L$ such that*

$$M^{H \cap U_i} = L(\beta_{i,p}), \qquad \wp(\beta_{i,p}) = \alpha_{i,p}.$$

Moreover, if $\alpha_{1,p}, \ldots, \alpha_{r(p),p}$ are p-independent for all $p \mid |G|$, then $H = G$.

Proof. First we note that $H/(H\cap U_i) \leq G/U_i = \mathbb{Z}/p\mathbb{Z}$ so $\mathrm{Gal}(M^{H\cap U)i}/L) \leq \mathbb{Z}/p\mathbb{Z}$, and Kummer theory (if $\mathrm{char}(L) \neq p$) or Artin-Schreier theory (otherwise) give us the required elements $\alpha_{i,p}$. Now, if the $\alpha_{i,p}$-s are p-independent, then by (25), Kummer theory and Artin-Schreier theory, we find that

$$(\mathbb{Z}/p\mathbb{Z})^{r(p)} \cong \mathrm{Gal}(M^{H\cap\Phi_p(G)}/L) \cong H/(H\cap\Phi_p(G)).$$

So by Lemma 6.9, $H = G$. □

6.2.4. *Rational functions.* We borrow the following from [3, Lem. 4.5].

Lemma 6.11. *Let $\tilde{f}(T) \in K[T]$ be a separable polynomial and let $f(T) = \tilde{f}(T) + A \in K(A)[T]$ where A is transcendental over $K(T)$. Then $\mathrm{disc}(f) \in K[A]$ is not divisible by A.*

Lemma 6.12. *Let F be a field and let $\mathbf{A} = (A_1, \dots, A_m)$ be an m-tuple of variables ($m \geq 2$). Let $\alpha = (\alpha_1, \dots, \alpha_m)$ be an m-tuple of scalars from F. Let $f_0(T) \in F[T]$ be a polynomial of degree $> m$. Then $\mathcal{F}(\mathbf{A}, T) = f_0(T) + \sum_{i=1}^m A_i T^i + \sum_{i=1}^m A_i\alpha_i$ is separable in T.*

Proof. It suffices to show that $\mathcal{F}$ is irreducible in T, because $\mathcal{F}'$ is linear in A_1 and in particular non-zero. Since $\mathcal{F}$ is primitive in T, it is irreducible in T if and only if it is irreducible in $R = F(A_2, \dots, A_m)[A_1, T]$ by Gauss's lemma. Since

$$\mathcal{F} = (T + \alpha_1)A_1 + \mathcal{G},$$

with $\mathcal{G} = f_0(T) + \sum_{i>1} A_i(T^i + \alpha_i)$, either $\mathcal{F}$ is primitive in A_1, then again by Gauss it is irreducible in A_1 and thus in T, or $T + \alpha_1$ divides $\mathcal{G}$ in R. In the latter case, $\mathcal{H} = A_1 + \frac{\mathcal{G}}{T+\alpha_1}$ is irreducible in T (again primitivity and linearity) and $\deg_{A_2} \frac{\partial\mathcal{H}}{\partial T} = 1$ hence it is non-zero, so $\mathcal{H}$ is separable in T. Moreover, $\mathcal{H}|_{T=-\alpha_1} \neq 0$, so we get that $\mathcal{F} = (T + \alpha_1)\mathcal{H}$ is separable, as needed. □

Lemma 6.13. *Let F be an algebraically closed field of characteristic p. Let $\mathbf{A} = (A_0, \dots, A_m)$ be an $(m+1)$-tuple of variables, $m \geq 1$. Let $f_0(T) \in F[T]$ be a monic polynomial of degree $n > m$. Let $f(T) = f_0(T) + \sum_{i=0}^m A_i T^i$ be a polynomial with coefficients in $K = F(\mathbf{A})$. Let L be the splitting field of $f(T) = \prod_{i=1}^n (T - y_i)$.*

Let $D(T) = \frac{r_1(T)}{r_2(T)} \in F(T)^\times$ be a reduced rational function with $\deg r_2 \geq \deg r_1$, and $r_2(T) = c\prod_{j=1}^d (T - \alpha_j)$ ($c \in F^\times, \alpha_j \in F$). We have

$$\sum_{i=1}^n D(y_i) = \frac{h(\mathbf{A})}{\prod_{j=1}^d f(\alpha_j)} \tag{26}$$

where $h \in F[\mathbf{A}]$ is coprime to $\prod_{j=1}^d f(\alpha_j)$ as a polynomial in A_0.

Proof. We first prove (26) in the special case $D(T) = 1/(T - \alpha)^k$. Let

$$g(T) := \frac{f(\frac{1}{T} + \alpha)T^n}{f(\alpha)} = \frac{f_0(\frac{1}{T} + \alpha)T^n + \sum_{i=0}^m A_i(1 + \alpha T)^i T^{n-i}}{f(\alpha)}. \tag{27}$$

We have

$$g(T) = \prod_{i=1}^{n} (T - \frac{1}{y_i - \alpha}). \tag{28}$$

By Newton's identities, if $p_k := \sum_{i=1}^{n} \frac{1}{(y_i - \alpha)^k}$ and $e_i := \sum_{1 \le a_1 < a_2 < \ldots < a_i \le n} \prod_{j=1}^{i} \frac{1}{y_{a_j} - \alpha}$, then

$$p_k = \sum_{\substack{\nu_1 + 2\nu_2 + \ldots + k\nu_k = k \\ \nu_1 \ge 0, \ldots, \nu_k \ge 0}} (-1)^k \frac{k(\nu_1 + \ldots + \nu_k - 1)!}{\nu_1! \nu_2! \ldots \nu_k!} \prod_{i=1}^{k} (-e_i)^{\nu_i}, \tag{29}$$

and the coefficients are in fact integers. By (27) and (28), e_j has denominator $f(\alpha)$ and numerator independent of $A_0, \ldots, A_{j-1}$. Thus all the summands in (29), except e_1^k, are of the form $\frac{s(\mathbf{A})}{f(\alpha)^j}$ for some $j < k$ and $s \in F[A_1, \ldots, A_m]$. Moreover, e_1^k has denominator $f(\alpha)^k$ and non-zero numerator (it is $(-(f_0'(\alpha) + \sum_{i=1}^{m} iA_i\alpha^{i-1}))^k$, which depends on A_1). From (29) we establish (26) with $D = \frac{1}{(T-\alpha)^k}$.

To prove (26) for general D, we write r_2 as $c\prod_{i=1}^{e}(T - \beta_i)^{k_i}$, where $\beta_i \in F$ are distinct. The partial fraction decomposition of D is given by

$$D(T) = c_0 + \sum_{i=1}^{e} \sum_{j=1}^{k_i} \frac{c_{i,j}}{(T - \beta_i)^j}, \qquad (c_0, c_{i,j} \in F, c_{i,k_i} \neq 0). \tag{30}$$

Applying (26) to each summand in (30) and summing, we obtain (26) in its generality. □

Lemma 6.14. *Let F be a field of characteristic p, $K = F(A_0)$ a field of rational functions and $\wp(x) = x^p - x$. Suppose that*

$$\frac{a}{b} \equiv \frac{c}{d} \bmod \wp(K) \tag{31}$$

where both fractions are in reduced form, and that b, d coprime. Then b, d are p-th powers.

Proof. From (31), $\frac{ad-cb}{bd} = z^p - z$ for $z \in K$. Writing $z = \frac{z_1}{z_2}$ in reduced form, it follows that the denominator of $z^p - z$ is a perfect p-th power, and so bd is a perfect p-th power, and the conclusion follows since b, d are coprime. □

6.2.5. *Proof of Lemma 6.4.* Let $\bar{F}$ be an algebraic closure of F. Since

$$\mathrm{Gal}(M\bar{F}/K\bar{F}) \le \mathrm{Gal}(M/K) \le G \wr S_n,$$

it suffices to prove that $\mathrm{Gal}(M\bar{F}/K\bar{F}) \cong G \wr S_n$. Therefore we may assume w.l.o.g. that $F = \bar{F}$. In particular, if $p \mid |G|$ and $p \neq \mathrm{char}(F)$, the field F contains a primitive p-th root of unity.

As explained before Lemma 6.4 it suffices to prove that $\mathrm{Gal}(M/L) = G^n$. To do this we apply Lemma 6.10 to M/L with the group G^n instead of G.

For a prime $p \mid |G|$ with $p \nmid \mathrm{char}(F)$, let $D_1(T), \dots, D_r(T) \in F[T]$ be p-powerfree polynomials that are p-independent such that

$$E^{\Phi_p(G)} = L(\sqrt[p]{D_1(T)}, \dots, \sqrt[p]{D_r(T)}).$$

If $p \mid \mathrm{char}(F), |G|$, let $D_1(T), \dots, D_r(T) \in F(T)$ be rational functions that are p-independent such that

$$E^{\Phi_p(G)} = L(\beta_1, \dots, \beta_r), \qquad \beta_i^p - \beta_i = D_i(T). \tag{32}$$

So the $\alpha_{i,p}$-s of Lemma 6.10 can be taken to be $D_i(y_j)$ with $i = 1, \dots, r$ and $j = 1, \dots, n$. Then, it suffices to prove that the $D_i(y_j)$ are p-independent to finish the proof. We separate this part into two cases depending on whether $\mathrm{char}(F) = p$ or not.

Case A: $\mathrm{char}(F) \neq p$

Step 1: $r = 1$.

Put $D = D_1$ and $w_j = D(y_j)$. Let V be the space of linear dependencies of the w_j-s:

$$V = \{(v_1, \dots, v_n) \in \mathbb{F}_p^n : w_1^{v_1} \cdots w_n^{v_n} \equiv 1 \mod (L^\times)^p\}. \tag{33}$$

We need to prove that $V = 0$. Since V is an invariant subspace of $\mathbb{F}_p^n$ under the action of $S_n = \mathrm{Gal}(L/K)$, by Lemma 6.8 it suffices to prove that $V \neq V_1, V_{n-1}, V_n$.

Sub-step 1a: $(1, \dots, 1) \notin V$; hence $V \neq V_1, V_n$.

We assume in contradiction that $(1, \dots, 1) \in V$. In other words, there exists $z \in L$ such that

$$D(y_1) \cdots D(y_n) = z^p. \tag{34}$$

We factor D over F (recall that we reduced to the case $F = \bar{F}$):

$$D(T) = c \prod_{j=1}^{d} (T - \alpha_j), \qquad \alpha_j \in F, c \in F^\times. \tag{35}$$

Since

$$(-1)^n f(\alpha_j) = \prod_{i=1}^{n} (y_i - \alpha_j),$$

and using (34) and (35) we obtain

$$z^p = D(y_1) \cdots D(y_n) = c^n \prod_{j=1}^{d} \prod_{i=1}^{n} (y_i - \alpha_j) = (-1)^{nd} c^n \prod_{j=1}^{d} f(\alpha_j). \tag{36}$$

In particular, $K(z)/K$ is a Galois subextension of the S_n-extension L/K of degree p or 1. Put $H = \mathrm{Gal}(L/K(z))$ so that by Lemma 6.7, either $H = 1$, $H = S_n$ or $H = A_n$, where the latter is possible only if $p = 2$.

If $H = 1$, then $K(z) = L$, so $n! = 1$ or $n! = p$, which contradicts $n > 2$. Thus, $H \neq 1$.

Now we show that $H \neq S_n$. If $H = S_n$, then $[K(z) : K] = 1$. Therefore $z \in K$, as such z is a rational function in the A_i-s. From (36), it follows that $\prod_{j=1}^{d} f(\alpha_j)$ is a p-th power in K. Each $f(\alpha_j)$, as a polynomial in A_0, is linear with leading coefficient 1, so it must appear a multiple of p times. On the other hand, by comparing the coefficient of A_1, the equality $f(\alpha_j) = f(\alpha_k)$ implies that $\alpha_j = \alpha_k$. As D is p-th powerfree in $F[T]$ by assumption, we arrive to contradiction.

So $H = A_n$ and $p = 2$ and in particular the characteristic is $\neq 2$. There is a unique field K' such that $K \subseteq K' \subseteq L$ with $\mathrm{Gal}(L/K') = A_n$, namely $K' = K(\sqrt{\mathrm{disc}(f)})$. Thus, $K(z) = K(\sqrt{\mathrm{disc}(f)})$, and so by (36)

$$(-1)^{nd} c^n \prod_{j=1}^{d} f(\alpha_j) \cdot \mathrm{disc}(f) \in (K^\times)^2. \tag{37}$$

The linear-in-A_0 polynomial $f(\alpha_j)$ is coprime to $\mathrm{disc}(f)$. Indeed, put $A = f(\alpha_j)$ and apply Lemma 6.12 to $\tilde{f}(T) = f(T) - A$, to obtain that $\tilde{f}(T)$ is separable in T and thus by Lemma 6.11, $\mathrm{disc}(f)$ is not divisible by $A = f(\alpha_1)$, hence coprime to it, as needed. But then $\mathrm{disc}(f)$ is a square by (37), which contradicts the fact that $\mathrm{Gal}(L/K) = S_n$.

Sub-step 1b: $(1, -1, 0, \ldots, 0) \notin V$; hence $V \neq V_{n-1}$ and $V \neq V_n$.

Assume in contradiction that $(1, -1, 0, ..., 0) \in V$. So, there exists $z \in L$ such that

$$D(y_1) = D(y_2) z^p. \tag{38}$$

Consider the following diagram of fields

$$\begin{tikzcd}
L \arrow[d, no head] \arrow[dd, dashed, no head, bend left=60, "S_{n-2}"] \arrow[dddd, dashed, no head, bend right=60, "S_n"'] \\
K(y_1, y_2)(z) \arrow[d, no head, "1 \text{ or } p"] \\
K(y_1, y_2) \arrow[d, no head, "n-1"] \\
K(y_1) \arrow[d, no head] \\
K
\end{tikzcd}$$

with $\mathrm{Gal}(L/K(y_1, y_2)) = S_{n-2}$ and $K(y_1, y_2)(z)/K(y_1, y_2)$ Galois of degree 1 or p.

Assume in contradiction that $[K(y_1, y_2)(z) : K(y_1, y_2)] = 1$, then $z \in K(y_1, y_2)$. Applying the norm map

$$N\colon K(y_1, y_2) \to K(y_1) \tag{39}$$

on (38), multiplying by $D(y_1)$, and considering (36), we obtain

$$D(y_1)^n = D(y_1)D(y_2)\cdots D(y_n)N(z)^p = (-1)^{dn}c^n \prod_{j=1}^{d} f(\alpha_j)N(z)^p. \tag{40}$$

The field $K(y_1)$ is the field of rational functions in $A_0, A_2, \ldots, A_m, y_1$ over F since $A_1 = -\frac{A_0+A_2y_1^2+\cdots}{y_1}$.

This implies that $f(\alpha_j)$ and $f(\alpha_k)$, as elements in $F(A_2, \cdots, A_m, y_1)[A_0]$ are associate if and only if $\alpha_j = \alpha_k$. Since D is p-th powerfree, for every j the multiplicity of $f(\alpha_j)$ in the right hand side product in (40) is $\not\equiv 0 \mod p$. On the other hand, on the left hand side of (40) the multiplicity of $f(\alpha_j)$ is 0 since A_0 does not appear. This contradicts (40), therefore $[K(y_1, y_2)(z) : K(y_1, y_1)] = p$.

By Lemma 6.7, $p = 2$ and thus the characteristic is $\neq 2$. As $L/K(y_1, y_2)$ is an S_{n-2}-extension, it has a unique subextension of degree 2 which is the fixed field of $A_{n-2} = A_n \cap S_{n-2}$ hence is generated by $\sqrt{\mathrm{disc}(f)}$. But z also generates a quadratic subextension, hence

$$\frac{D(y_1)}{D(y_2)}\mathrm{disc}(f) = z^2\mathrm{disc}(f) \in (K(y_1, y_2)^\times)^2. \tag{41}$$

Apply the norm map (39) to obtain

$$\frac{D(y_1)^n}{D(y_1)\cdots D(y_n)} \cdot \mathrm{disc}^{n-1}(f) \in (K(y_1)^\times)^2. \tag{42}$$

If n is even, then $(1, \ldots, 1) \in V_{n-1}$ (as $p = 2$). Therefore, by Sub-step 1a, $V \neq V_1, V_{n-1}, V_n$, that is, $V = 0$, in contradiction to the assumption that $(1, -1, 0, \ldots, 0) \in V$. Thus, n is odd. By (42) and (36)

$$D(y_1) \equiv \prod_{j=1}^{d} f(\alpha_j) \mod (F(y_1, A_0, A_2, \cdots, A_m)^\times)^2. \tag{43}$$

As D is not a square and each of the $f(\alpha_j)$ is linear in A_0, and by the fact that $f(\alpha_j)$ and $f(\alpha_k)$ are associate only if $\alpha_j = \alpha_k$, we must have that A_0 appears in the left hand side, which is a contradiction.

Step 2: General r.

Put $w_{i,j} = D_i(y_j)$ and as before let V be the space of linear dependencies:

$$V = \{(v_{i,j})_{1\le i\le r, 1\le j\le n} \in \mathbb{F}_p^{nr} : \prod_{i=1}^{r}\prod_{j=1}^{n} D_i^{v_{i,j}}(y_j) \in (L^\times)^p\} \tag{44}$$

and we want to prove that $V = 0$.

Here the action of $S_n = \mathrm{Gal}(L/K)$ on the $w_{i,j}$ is by permuting the j-th index, so V is an S_n-invariant space with respect of the action of S_n given by permuting the columns.

Assume in contradiction that $V \neq 0$. We begin by constructing a matrix B in V of rank 1. Let $A \in V$ be a non-zero matrix. Denote its columns by $v_1, \cdots, v_n$. If $\mathrm{rk}(A) = 1$ we take $B = A$. Otherwise, assume without loss of generality that v_1 and v_2 are linearly independent. Then the matrix

$$B = A - (v_2 \mid v_1 \mid v_3 \mid v_4 \mid \cdots) = (v_1 - v_2 \mid v_2 - v_1 \mid 0 \mid \cdots) \in V.$$

has rank 1, as needed.

There are non-zero vectors $\mathbf{a} = (a_1, \ldots, a_r) \in \mathbb{F}_p^r$, $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_p^n$ such that

$$B_{i,j} = a_i \cdot b_j.$$

The relation $B \in V$ is equivalent to

$$\prod_{i=1}^{r} \prod_{j=1}^{n} D_i^{a_i \cdot b_j}(y_j) \in (L^\times)^p. \tag{45}$$

Let $D(T) := \prod_{i=1}^r D_i^{a_i}(T)$. We have $\prod_{j=1}^n D^{b_j}(y_j) \in (L^\times)^p$, which by Step 1 implies that $b_j = 0$ for all j, contradicting the fact that $\mathbf{b} \neq 0$. This concludes the proof of Case A.

Case B: $\mathrm{char}(F) = p$

From now on, $\wp(x) = x^p - x$. Let v be the discrete valuation at the infinite prime; that is to say, $v(h(T)/g(T)) = \deg h - \deg g$. Since $E/\mathbb{F}_q(T)$ is tamely ramified at v, the extension generated by a root of $X^p - X = D_i(T)$ is unramified at v. This implies that there exists some $g_i(T)$ with $v(D_i + g_i^p - g_i) \geq 0$. We may replace D_i by $D_i + g_i^p - g$, to assume without loss of generality that $v(D_i(T)) \geq 0$. We may further assume that the roots in the denominators of $D_i(T)$ have multiplicity indivisible by p [23, §2]. The proof goes analogously to Case A:

Step 1: $r = 1$.

Put $D = D_1$ and $w_j = D(y_j)$. Let V be the space of linear dependencies of the w_j-s:

$$V = \{(v_1, \ldots, v_n) \in \mathbb{F}_p^n : \sum_{i=1}^{n} w_i v_i \equiv 0 \mod \wp(L)\} \tag{46}$$

We need to prove that $V = 0$. Since V is an invariant subspace of $\mathbb{F}_p^n$ under the action of $S_n = \mathrm{Gal}(L/K)$, by Lemma 6.8 it suffices to prove that $V \neq V_1, V_{n-1}, V_n$.

Sub-step 1a: $(1, \ldots, 1) \notin V$; hence $V \neq V_1, V_n$.

We assume in contradiction that $(1, \ldots, 1) \in V$. In other words, there exists $z \in L$ such that

$$D(y_1) + \ldots + D(y_n) = z^p - z. \tag{47}$$

Write $D = \frac{r_1(T)}{r_2(T)}$ where r_1, r_2 are coprime, and $r_2(T) = c\prod_{j=1}^{d}(T-\alpha_j)$ ($c \in F^\times, \alpha_j \in F$). By Lemma 6.13,

$$z^p - z = \sum_{i=1}^{n} D(y_i) = \frac{h(\mathbf{A})}{\prod_{j=1}^{d} f(\alpha_j)}, \tag{48}$$

where $h(\mathbf{A}) \in F[\mathbf{A}]$ is coprime to the denominator as polynomials in A_0. In particular, $K(z)/K$ is a Galois subextension of the S_n-extension L/K of degree p or 1. Put $H = \mathrm{Gal}(L/K(z))$ so that by Lemma 6.7, either $H = 1$, $H = S_n$ or $H = A_n$, where the latter is possible only if $p = 2$.

If $H = 1$, then $K(z) = L$, so $n! = 1$ or $n! = p$, which contradicts $n > 2$. Thus, $H \neq 1$.

Now we show that $H \neq S_n$. If $H = S_n$, then $[K(z) : K] = 1$. Therefore $z \in K$. The denominator of $z^p - z$ is a (possibly trivial) p-th power in K, so that by (48) it follows $\prod_{j=1}^{d} f(\alpha_j)$ is a p-th power in K. Each $f(\alpha_j)$, as a polynomial in A_0, is linear with leading coefficient 1, so it must appear a multiple of p times. On the other hand, by comparing the coefficient of A_1, the equality $f(\alpha_j) = f(\alpha_k)$ implies that $\alpha_j = \alpha_k$. As α_i have multiplicity indivisible by p by our assumption on $r_2(T)$, we arrive to contradiction.

So $H = A_n$ and $p = 2$. In characteristic 2, we must use the Berlekamp discriminant $\mathrm{Berl}(f)$[1] in place of the usual $\mathrm{disc}(f)$. There is a unique field K' such that $K \subseteq K' \subseteq L$ with $\mathrm{Gal}(L/K') = A_n$, namely $K' = K(\delta)$ for δ which satisfies $\delta^2 - \delta = \mathrm{Berl}(f)$. Thus, $K(z) = K(\delta)$, or equivalently

$$\wp(z) \equiv \wp(\delta) \bmod \wp(K), \tag{49}$$

which by (48) becomes

$$\mathrm{Berl}(f) \equiv \frac{h(\mathbf{A})}{\prod_{j=1}^{d} f(\alpha_j)} \bmod \wp(K). \tag{50}$$

As in Sub-step 1a in the Kummer case, the linear-in-A_0 polynomial $f(\alpha_j)$ is coprime to $\mathrm{disc}(f)$. The Berlekamp discriminant is of the form $N(f)/\mathrm{disc}(f)$ for some polynomial N in the coefficients of f. Thus, the denominators of the two fractions in (50) are coprime as polynomials in A_0. By Lemma 6.14, this implies that the denominator $\prod_{j=1}^{d} f(\alpha_j)$ is a square, contradicting the fact that the α_j have odd multiplicity by our assumption on $r_2(T)$.

Sub-step 1b: $(1, -1, 0, \dots, 0) \notin V$; hence $V \neq V_{n-1}$ and $V \neq V_n$.

Assume in contradiction that $(1, -1, 0, ..., 0) \in V$. So, there exists $z \in L$ such that

$$D(y_1) = D(y_2) + z^p - z. \tag{51}$$

[1] See [6] or [8] for a recent use in a similar setting.

We have $\mathrm{Gal}(L/K(y_1,y_2)) = S_{n-2}$ and $K(y_1,y_2)(z)/K(y_1,y_2)$ Galois of degree 1 or p. Assume in contradiction that $[K(y_1,y_2)(z) : K(y_1,y_2)] = 1$, then $z \in K(y_1,y_2)$. Applying the trace map

$$T\colon K(y_1,y_2) \to K(y_1). \tag{52}$$

on (51), adding by $D(y_1)$, and considering (48), we obtain

$$nD(y_1) = \frac{h(\mathbf{A})}{\prod_{j=1}^{d} f(\alpha_j)} + T(z)^p - T(z) \equiv \frac{h(\mathbf{A})}{\prod_{j=1}^{d} f(\alpha_j)} \mod \wp(K(y_1)). \tag{53}$$

The field $K(y_1)$ is the field of rational functions in $A_0, A_2, \dots, A_m, y_1$ over F since $A_1 = -\frac{A_0+A_2y_1^2+\cdots}{y_1}$.

This implies that $f(\alpha_j)$ and $f(\alpha_k)$, as elements in $F(A_2,\cdots,A_m,y_1)[A_0]$ are associate if and only if $\alpha_j = \alpha_k$. The denominator in the left hand side of (53) does not involve A_0 and so it is coprime to the denominator in the right hand side. By Lemma 6.14, this means that the denominator in the right hand side is a p-th power, contradicting the fact that for every j, the multiplicity of $f(\alpha_j)$ is $\not\equiv 0 \mod p$. Therefore $[K(y_1,y_2)(z) : K(y_1,y_1)] = p$, and by Lemma 6.7, $p = 2$.

As $L/K(y_1,y_2)$ is an S_{n-2}-extension, it has a unique subextension of degree 2 which is the fixed field of $A_{n-2} = A_n \cap S_{n-2}$ hence is generated by $\delta \in L$ which satisfies $\delta^2 - \delta = \mathrm{Berl}(f)$. But z also generates a quadratic subextension, hence

$$D(y_1) - D(y_2) + \mathrm{Berl}(f) = z^2 - z + \mathrm{Berl}(f) \in \wp(K(y_1,y_2)). \tag{54}$$

Apply the trace map (52) to obtain

$$nD(y_1) - (D(y_1) + \ldots + D(y_n)) + (n-1)\mathrm{Berl}(f) \in \wp(K(y_1)). \tag{55}$$

If n is even, then $(1,\dots,1) \in V_{n-1}$ (as $p=2$). Therefore, by Sub-step 1a, $V \neq V_1, V_{n-1}, V_n$, that is, $V = 0$, in contradiction to the assumption that $(1,-1,0,\dots,0) \in V$. Thus, n is odd. By (55) and (48)

$$\frac{r_1(y_1)}{r_2(y_1)} \equiv \frac{h(\mathbf{A})}{\prod_{j=1}^{d} f(\alpha_j)} \mod \wp(F(y_1,A_0,A_2,\cdots,A_m)). \tag{56}$$

The denominator in the left hand side does not involve A_0 and so it is coprime to the denominator in the right hand side as a polynomial in A_0. By Lemma 6.14, this means that the denominator in the right hand side is a square. This contradicts the fact that for every j, the multiplicity of $f(\alpha_j)$ is odd, and that $f(\alpha_j)$ and $f(\alpha_k)$ are associate if and only if $\alpha_j = \alpha_k$.

Step 2: General r.

Put $w_{i,j} = D_i(y_j)$ and let V be the space of linear dependencies:

$$V = \{(v_{i,j})_{1\le i\le r, 1\le j\le n} \in \mathbb{F}_p^{nr} : \sum_{i=1}^{r}\sum_{j=1}^{n} v_{i,j}D_i(y_j) \in \wp(L)\} \tag{57}$$

and we want to prove that $V = 0$. Assume in contradiction that $V \neq 0$. As in Step 2 of the Kummer case, there exists B in V of rank 1. There are non-zero vectors $\mathbf{a} = (a_1, \dots, a_r) \in \mathbb{F}_p^r$, $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_p^n$ such that

$$B_{i,j} = a_i \cdot b_j.$$

The relation $B \in V$ is equivalent to

$$\sum_{i=1}^{r} \sum_{j=1}^{n} a_i b_j D_i(y_j) \in \wp(L). \tag{58}$$

Let $D(T) := \sum_{i=1}^{r} a_i D_i(T)$. We have $\sum_{j=1}^{n} b_j D(y_j) \in \wp(L)$, which by Step 1 implies that $b_j = 0$ for all j, contradicting the fact that $\mathbf{b} \neq 0$. This concludes the proof of Case B. □

7. Proof of Theorem 4.3

First we prove the assertion for $\psi = \delta_\lambda$, where λ is a G-factorization type supported on $e = 1$ with $\deg \lambda = n$ and $\delta_\lambda \in \Lambda^*$ is given by

$$\delta_\lambda(\lambda') = \begin{cases} 1, & \text{if } \lambda' = \lambda, \\ 0, & \text{otherwise.} \end{cases}$$

Let $C = \{h \in G \wr S_n : \lambda_h = \lambda\} \subseteq G \wr S_n$. Since λ is supported on $e = 1$ and $\deg \lambda = n$, by Lemma 4.2, C is a conjugacy class.

Write $f_0 = T^n + \sum_{i=0}^{n-1} a_i T^i$ and put $W = W_{a,m}$ as in (24). Every $(w_0, \dots, w_{n-1}) \in W(\mathbb{F}_q)$ corresponds in a bijective way to $f = T^n + \sum_{i=0}^{n-1} w_i T^i$ with $\deg(f - f_0) \leq m$.

By the explicit Chebotarev theorem[2] and by Proposition 6.2,

$$\frac{\#\{w \in W(\mathbb{F}_q) : w \text{ is unramified in } U \text{ and } \phi_w \in C\}}{q^{m+1}} = \frac{|C|}{|G \wr S_n|} + O(q^{-1/2}),$$

where the implied constant is bounded in terms of the complexity of U, which is bounded in terms of $|G|$, genus(C), and n and hence in terms of B. This finishes the proof of this case since $\frac{|C|}{|G \wr S_n|} = \left\langle \delta_\lambda(\lambda_{(\xi,\sigma)}) \right\rangle_{(\xi,\sigma) \in C}$, for unramified w we have $\delta_\lambda(f) = \delta_\lambda(\phi_w)$ by Lemma 6.1, there are $O_B(q^m)$ ramified w (the zeros of D given in (21)), and so

$$\langle \delta_\lambda(f) \rangle_{\deg(f-f_0) \leq m} = \frac{\#\{w \in W(\mathbb{F}_q) : w \text{ is unramified in } U \text{ and } \phi_w \in C\}}{q^{m+1}} + O_B(q^{-1}).$$

[2] For a version which is sufficiently uniform in the parameters see either [1, Appendix] or [12, Thm. 3]. In the former there is a mistake in the formulation of the theorem, in the notation of loc. cit. the error term should be dependent on the complexity of S and not on the complexity of R and $\deg \mathcal{F}$ as written. In the setting where R is a polynomial ring in several variables and S is the ring generated by adding roots of a polynomial $\mathcal{F} \in R[X]$, then the complexity of S is bounded in terms of the complexity of R and the total degree of $\mathcal{F}$.

For general ψ, we partition $\Lambda = \Lambda_1 \cup \Lambda_2 \cup \Lambda_3$, where Λ_1 consists of λ-s of degree n supported on $e = 1$, Λ_2 consists of the other λ-s of degree n, and Λ_3 consists of λ-s of degree $\neq n$. This decomposes $\psi = \psi_1 + \psi_2 + \psi_3$ with ψ_i supported on Λ_i. Now, as $\deg(f - f_0) \leq m$ implies that $\deg f = n$, we have

$$\langle \psi_3(f) \rangle_{\deg(f-f_0)\leq m} = 0.$$

Since $\psi_2(f) = 0$ if f is squarefree and there are $O_B(q^m)$ non-squarefrees satisfying $\deg(f - f_0) \leq m$ [17, Thm. 1.3], we get that

$$\langle \psi_2(f) \rangle_{\deg(f-f_0)\leq m} = O_B(q^{-1}).$$

The function ψ_1 decomposes as $\psi_1 = \sum_{\lambda\in\Lambda_1} \psi_1(\lambda)\delta_{\lambda_1}$, so by the special case proved above

$$\begin{aligned}
\langle \psi_1(f) \rangle_{\deg(f-f_0)\leq m} &= \sum_{\lambda\in\Lambda_1} \psi_1(\lambda) \, \langle \delta_\lambda(f) \rangle_{\deg(f-f_0)\leq m} \\
&= \sum_{\lambda\in\Lambda_1} \psi_1(\lambda) \, \langle \delta_\lambda(\xi,\sigma) \rangle_{(\xi,\sigma)\in G\wr S_n} + O_B(q^{-1/2}) \\
&= \langle \psi_1(\xi,\sigma) \rangle_{(\xi,\sigma)\in G\wr S_n} + O_B(q^{-1/2}).
\end{aligned}$$

This completes the proof as $\psi_1(\xi,\sigma) = \psi(\xi,\sigma)$. □

8. Non-geometric extensions

Here we explain how the results for non-geometric extensions may be reduced to geometric extensions over a field extension: Let G be a finite group, let $E/\mathbb{F}_q(T)$ be a G-extension and let E^{ab} be the fixed field of the commutator of G in E. Assume that E^{ab} is tamely ramified at infinity and that E (or equivalently E^{ab}) is not geometric. Let $\mathbb{F}_{q^\nu}$ be the algebraic closure of $\mathbb{F}_q$ in E, $C_\nu = \mathrm{Gal}(\mathbb{F}_{q^\nu}/\mathbb{F}_q)$, and $H = \mathrm{Gal}(E/\mathbb{F}_{q^\nu}(T))$. By replacing E with $E\mathbb{F}_{q^\mu}$ for some large μ, we may assume without loss of generality that $G = H \rtimes C_\nu$. Now we apply the construction of §6 to the extension $E/\mathbb{F}_{q^\nu}(T)$ to get that the corresponding Galois group is $\mathrm{Gal}(M/K) = H \wr S_n$ and we have a diagram of fields whose right column is as in Figure 6.2

$$\begin{tikzcd}
 & M \arrow[d, dash] \\
L_0 = K_0(y_1,\dots,y_n) \arrow[r, dash] \arrow[d, dash] & L = K(y_1,\dots,y_n) \arrow[d, dash] \\
K_0 = \mathbb{F}_q(A_0,\dots,A_m) \arrow[r, dash] & K = \mathbb{F}_{q^\nu}(A_0,\dots,A_m)
\end{tikzcd}$$

Now, $\mathrm{Gal}(L_0/K_0) = S_n$ for the same reason that $\mathrm{Gal}(L/K) = S_n$, and $\mathrm{Gal}(K/K_0) \cong \mathrm{Gal}(\mathbb{F}_{q^\nu}/\mathbb{F}_q) = C_\nu$. Thus, $\mathrm{Gal}(L/K_0) = S_n \times C_\nu$. With a little more effort, one can verify that in fact M/K_0 is Galois, and that $\mathrm{Gal}(M/K_0) = (H \wr S_n) \rtimes C_\nu$ with C_ν

acting trivially on S_n and acting diagonally on H^n. Now we can apply the higher dimensional Chebotarev theorem, to get a Chebotarev theorem in short intervals for this extension.

Appendix A. Norms in full intervals

We use the notation of §5. The goal of this appendix is to compute the mean value of $b_{E/\mathbb{F}_q(T)}$ and of $r_{E/\mathbb{F}_q(T)}$ in the most general setting of the limit $q^n \to \infty$.

Theorem A.1. *Let $E/\mathbb{F}_q(T)$ be a non-trivial geometric G-extension. Then*

$$\left\langle b_{E/\mathbb{F}_q(T)}(f) \right\rangle_{f \in M_{n,q}} = K_E \binom{n + \frac{1}{|G|} - 1}{n} \left(1 + O_{\mathrm{genus}(E),|G|}\left(\frac{1}{\sqrt{q}n}\right)\right), \tag{59}$$

where K_E is a positive constant that satisfies

$$K_E = 1 + O_{\mathrm{genus}(E),|G|}\left(\frac{1}{\sqrt{q}}\right). \tag{60}$$

The mean value of $r_{E/\mathbb{F}_q(T)}$ depends on the following zeta function

$$\zeta_{\mathcal{O}_E}(s) = \sum_{0 \neq I \text{ ideal in } \mathcal{O}_E} \frac{1}{(\#\mathcal{O}_E/I)^s}.$$

Proposition A.2. *Let $E/\mathbb{F}_q(T)$ be a non-trivial geometric extension of degree d. If $n \gg_{\mathrm{genus}(E),d} 1$ then*

$$\left\langle r_{E/\mathbb{F}_q(T)}(f) \right\rangle_{f \in M_{n,q}} = \lambda_E \log q, \tag{61}$$

where $\lambda_E > 0$ is the residue of $\zeta_{\mathcal{O}_E}(s)$ at $s = 1$, and it satisfies

$$\lambda_E \log q = 1 + O_{\mathrm{genus}(E),d}\left(\frac{1}{\sqrt{q}}\right). \tag{62}$$

Unlike the rest of the paper, here the methods are analytic.

A.1. Bounds on prime counting functions.

We use the notation $\mathcal{P}_{n,q}$ introduced in §1.2, with one modification – we do not include the infinite prime in $\mathcal{P}_{1,q}$. For any positive integer f, define

$$\pi_{E;f}(n) = \sum_{\substack{P \in \mathcal{P}_{n,q}, \\ f(P;E) = f}} 1$$

and set

$$\psi_E(n) = \sum_{df \mid n} df \pi_{E;f}(d).$$

Lemma A.3. *We have*

$$|\pi_{E;1}(n) - \frac{q^n}{n|G|}| \ll \frac{\max\{\mathrm{genus}(E), |G|\}}{n} q^{n/2}.$$

Proof. Let e be the identity element of G. The number $\pi_{C;q}(n;E)$ with $C=\{e\}$ is equal to $\pi_{E;1}(n)$, up to a contribution of ramified primes:

$$|\pi_{\{e\};q}(n;E)-\pi_{E;1}(n)| \leq \sum_{P\in\mathcal{P}_{n,q},\text{ ramified in }E} 1. \tag{63}$$

The Riemann-Hurwitz formula [32, Thm. 7.16] shows that

$$\sum_{P\in\mathcal{P}_{n,q},\text{ ramified in }E} 1 \ll \frac{\max\{\text{genus}(E),|G|\}}{n}. \tag{64}$$

By (5) with $C=\{e\}$, we have

$$|\pi_{\{e\};q}(n;E)-\frac{q^n}{n|G|}| \ll \frac{\max\{\text{genus}(E),|G|\}}{|G|}\frac{q^{n/2}}{n}. \tag{65}$$

From (63)–(65) and the triangle inequality, the proof follows. □

Proposition A.4. *We have*

$$\left|\psi_E(n)-\frac{q^n}{|G|}\right| \ll \max\{\text{genus}(E),|G|\}q^{\frac{n}{2}}.$$

Proof. We separate the summands in $\psi_E(n)$ according to whether $d=n$ (a case which contributes $n\pi_{E;1}(n)$) or not:

$$\psi_E(n)=n\pi_{E;1}(n)+T(n).$$

The triangle inequality gives us

$$\left|\psi_E(n)-\frac{q^n}{|G|}\right| \leq \left|n\pi_{E;1}(n)-\frac{q^n}{|G|}\right|+T(n). \tag{66}$$

We may bound $T(n)$ from above as follows, using the fact that $|\mathcal{P}_{n,q}|\leq\frac{q^n}{n}$:

$$T(n)\leq\sum_{d=1}^{\lfloor\frac{n}{2}\rfloor}\sum_{f=1}^{\lfloor\frac{n}{d}\rfloor}df\pi_{E;f}(d)\leq n\sum_{d=1}^{\lfloor\frac{n}{2}\rfloor}\sum_{f=1}^{\lfloor\frac{n}{d}\rfloor}\pi_{E;f}(d)\leq n\sum_{d=1}^{\lfloor\frac{n}{2}\rfloor}\frac{q^d}{d}.$$

One can show by induction that

$$\sum_{i=1}^{m}\frac{q^i}{i}\leq 4\frac{q^m}{m}$$

for all $m\geq 1$, which implies that

$$T(n)\ll q^{n/2}. \tag{67}$$

From (66), (67) and Lemma A.3, we conclude the proof of the proposition. □

A.2. **Proof of Theorem A.1.** Consider the power series

$$D_E(u) = \sum_{f\in\mathbb{F}_q[T],\text{ monic}} b_{E/\mathbb{F}_q(T)}(f)u^{\deg f} = \sum_{n\geq 0}\langle b_{E/\mathbb{F}_q(T)}(f)\rangle_{f\in M_{n,q}}(qu)^n. \tag{68}$$

Lemma 5.2 shows that D_E admits the following Euler product:

$$\begin{aligned} D_E(u) &= \prod_{P\in\mathcal{P}_q}\left(1+u^{\deg(P^{f(P;E)})}+u^{\deg(P^{2\cdot f(P;E)})}+\dots\right) \\ &= \prod_{P\in\mathcal{P}_q}\left(1-u^{f(P;E)\deg P}\right)^{-1} = \exp\left(\sum_{P\in\mathcal{P}_q}\sum_{k\geq 1}\frac{u^{f(P;E)\deg P\cdot k}}{k}\right). \end{aligned}$$

From the definition of $\pi_{E;f}(n)$ and $\psi_E(n)$, we may write the above expression as

$$D_E(u) = \exp\left(\sum_{n\geq 1}\frac{u^n}{n}\sum_{df\mid n} df\,\pi_{E;f}(d)\right) = \exp\left(\sum_{n\geq 1}\frac{u^n}{n}\psi_E(n)\right). \tag{69}$$

For any positive integer n, define

$$e_n = \psi_E(n) - \frac{q^n}{|G|}.$$

Let

$$a(u) = \exp\left(\sum_{n\geq 1}\frac{e_n u^n}{n}\right), \quad b(u) = (1-qu)^{-\frac{1}{|G|}}.$$

By (69), we have $D_E(u) = \exp\left(\sum_{n\geq 1}\frac{q^n u^n}{n|G|}\right)\exp\left(\sum_{n\geq 1}\frac{e_n u^n}{n}\right) = a(u)b(u)$, and so

$$\langle b_{E/\mathbb{F}_q(T)}(f)\rangle_{f\in M_{n,q}} = q^{-n}[u^n]D_E(u) = q^{-n}[u^n]a(u)b(u),$$

where $[u^n]F(u)$ is a notation for the coefficient of u^n in a power series F. From Proposition A.4 we have

$$|e_n| \ll \max\{\text{genus}(E), |G|\}q^{n/2}.$$

Hence we may apply [14, Thm. 3.3] with $a(u), b(u)$ and obtain

$$\langle b_{E/\mathbb{F}_q(T)}(f)\rangle_{f\in M_{n,q}} = \binom{n+\frac{1}{|G|}-1}{n}\left(a(q^{-1})+E\right),$$

where

$$|E| \ll_{\text{genus}(E),|G|} \frac{1}{\sqrt{q}n}.$$

which establishes (59) with $K_E = a(q^{-1})$. By [14, Rem. 3.6] we have (60). □

A.3. **Proof of Proposition A.2.** Let

$$\mathcal{Z}_E(u) = \prod_{\mathcal{P} \text{ a prime in } E} (1-u^{\deg \mathcal{P}})^{-1},$$
$$\mathcal{Z}_{\mathcal{O}_E}(u) = \prod_{\mathcal{P} \text{ a prime in } \mathcal{O}_E} (1-u^{\deg \mathcal{P}})^{-1},$$

be the Dedekind zeta function of E and of $\mathcal{O}_E$; in particular, $\mathcal{Z}_{\mathcal{O}_E}(q^{-s}) = \zeta_{\mathcal{O}_E}(s)$. They are related by

$$\mathcal{Z}_{\mathcal{O}_E}(u) = \mathcal{Z}_E(u) \prod_{\mathcal{P}|P_\infty} (1-u^{\deg \mathcal{P}}), \tag{70}$$

where P_∞ denotes the infinite prime of $\mathbb{F}_q(T)$. Suppose that $P_\infty = \mathcal{P}_1^{e_1}\cdots\mathcal{P}_m^{e_m}$ with $\mathcal{P}_i$ distinct primes of E and put $f_i = f(\mathcal{P}_i; E)$. Then we have

$$\prod_{\mathcal{P}|P_\infty} (1-u^{\deg \mathcal{P}}) = \prod_{i=1}^m (1-u^{f_i}). \tag{71}$$

As $E/\mathbb{F}_q(T)$ is geometric, the Riemann Hypothesis for Function Fields (RH) implies that $\mathcal{Z}_E$ is a rational function of the form

$$\mathcal{Z}_E(u) = \frac{P_E(u)}{(1-qu)(1-u)}, \tag{72}$$

where $\deg P_E = 2\mathrm{genus}(E)$, $P_E(0)=1$ and the inverse absolute value of the roots of P_E is $\sqrt{q}$. From (70)–(72),

$$\mathcal{Z}_{\mathcal{O}_E}(u) = \frac{P_E(u)}{(1-qu)} \cdot \frac{\prod_{i=1}^m (1-u^{f_i})}{1-u} = \frac{\tilde{P}_E(u)}{(1-qu)}, \tag{73}$$

with $\tilde{P}_E(u) = P_E(u)\cdot\frac{\prod_{i=1}^m(1-u^{f_i})}{1-u}$. The function $\mathcal{Z}_{\mathcal{O}_E}(u)$ is a generating function for the mean value of $r_{E/\mathbb{F}_q(T)}$:

$$\mathcal{Z}_{\mathcal{O}_E}(u) = \sum_{n\geq 0} \langle r_{E/\mathbb{F}_q(T)}(f)\rangle_{f\in M_{n,q}} (qu)^n. \tag{74}$$

From (73), (74), it follows that if $n \geq \deg \tilde{P}_E$, we have

$$\langle r_{E/\mathbb{F}_q(T)}(f)\rangle_{f\in M_{n,q}} = \tilde{P}_E(\frac{1}{q}).$$

As $\mathcal{Z}_{\mathcal{O}_E}(q^{-s}) = \zeta_{\mathcal{O}_E}(s)$, we have $\tilde{P}_E(\frac{1}{q}) = \lambda_E \log q$. As $f_i, m \leq d$, we have $\deg \tilde{P}_E = 2\mathrm{genus}(E) + \sum_{i=1}^m f_i - 1 \ll_{\mathrm{genus}(E),d} 1$. Finally, RH implies that

$$\lambda_E \log q = (1+O(\frac{1}{\sqrt{q}}))^{2\mathrm{genus}(E)}(1+O(\frac{1}{q}))^{O(d^2)} = 1 + O_{\mathrm{genus}(E),d}(\frac{1}{\sqrt{q}}),$$

as needed. □

Acknowledgment

We wish to thank to Kumar Murty for helpful discussion on Chebotarev theorem.

References

1. J. C. Andrade, L. Bary-Soroker, and Z. Rudnick, *Shifted convolution and the Titchmarsh divisor problem over $\mathbb{F}_q[t]$*, Philos. Trans. Roy. Soc. A **373** (2015), no. 2040, 20140308, 18. MR 3338116 2
2. Antal Balog and Ken Ono, *The Chebotarev density theorem in short intervals and some questions of Serre*, J. Number Theory **91** (2001), no. 2, 356–371. MR 1876282 1.1
3. Efrat Bank, Lior Bary-Soroker, and Arno Fehm, *Sums of two squares in short intervals in polynomial rings over finite fields*, Amer. J. Math. **140** (2018), no. 4, 1113–1131. MR 3828042 2, 6.3, 6.2.4
4. Efrat Bank, Lior Bary-Soroker, and Lior Rosenzweig, *Prime polynomials in short intervals and in arithmetic progressions*, Duke Math. J. **164** (2015), no. 2, 277–295. MR 3306556 2, 6.2.1
5. Lior Bary-Soroker and Arno Fehm, *Correlations of sums of two squares and other arithmetic functions in function fields*, International Mathematics Research Notices (2017), rnx250. 3
6. E. R. Berlekamp, *An analog to the discriminant over fields of characteristic two*, J. Algebra **38** (1976), no. 2, 315–317. MR 0404197 1
7. Jean Bourgain and Nigel Watt, *Mean square of zeta function, circle problem and divisor problem revisited*, arXiv preprint arXiv:1709.04340 (2017). 5.2
8. Dan 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** (2015), no. 2040, 20140311, 14. MR 3338117 1
9. S. D. Cohen, *The Galois group of a polynomial with two indeterminate coefficients*, Pacific J. Math. **90** (1980), no. 1, 63–76. MR 599320 2, 6.3
10. S. D. Cohen and R. W. K. Odoni, *The Farey density of norm subgroups of global fields. II*, Glasgow Math. J. **18** (1977), no. 1, 57–67. MR 0432597 1.2
11. Mark D. Coleman, *The Hooley-Huxley contour method for problems in number fields. III. Frobenian functions*, J. Théor. Nombres Bordeaux **13** (2001), no. 1, 65–76, 21st Journées Arithmétiques (Rome, 2001). MR 1838070 2
12. Alexei Entin, *Monodromy of hyperplane sections of curves and decomposition statistics over finite fields*, arXiv preprint arXiv:1805.05454 (2018). 2
13. Michael D. Fried and Moshe Jarden, *Field arithmetic*, second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2005. MR 2102046 1.2, 6.1
14. Ofir Gorodetsky, *A polynomial analogue of Landau's theorem and related problems*, Mathematika **63** (2017), no. 2, 622–665. MR 3706601 A.2
15. Loïc Grenié and Giuseppe Molteni, *An explicit Chebotarev density theorem under GRH.*, J. Number Theory **200** (2019), 441–485 (English). 1.1
16. Franz Halter-Koch, *Der Čebotarev'sche Dichtigkeitssatz und ein Analogon zum Dirichlet'schen Primzahlsatz für Algebraische Funktionenkörper*, Manuscripta Math. **72** (1991), no. 2, 205–211. MR 1114006 1.2

17. Jonathan Keating and Zeev Rudnick, *Squarefree polynomials and Möbius values in short intervals and arithmetic progressions*, Algebra Number Theory **10** (2016), no. 2, 375–420. MR 3477745 7
18. Jonathan P. Keating and Zeév Rudnick, *The variance of the number of prime polynomials in short intervals and in residue classes*, Int. Math. Res. Not. IMRN (2014), no. 1, 259–288. MR 3158533 1.2
19. Vijaya Kumar Murty and John Scherk, *Effective versions of the Chebotarev density theorem for function fields*, C. R. Acad. Sci. Paris Sér. I Math. **319** (1994), no. 6, 523–528. MR 1298275 1.2
20. J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 409–464. MR 0447191 1.1
21. Serge Lang, *Sur les séries L d'une variété algébrique*, Bull. Soc. Math. France **84** (1956), 385–407. MR 0088777 1.2
22. Huixue Lao, *On the distribution of integral ideals and Hecke Grössencharacters*, Chin. Ann. Math. Ser. B **31** (2010), no. 3, 385–392. MR 2652933 5.2
23. Daniel J. Madden, *Arithmetic in generalized Artin-Schreier extensions of $k(x)$*, J. Number Theory **10** (1978), no. 3, 303–323. MR 506641 6.2.5
24. Helmut Maier, *Primes in short intervals*, Michigan Math. J. **32** (1985), no. 2, 221–225. MR 783576 1.1
25. M. Ram Murty, V. Kumar Murty, and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. **110** (1988), no. 2, 253–281. MR 935007 1.1
26. R. W. K. Odoni, *On the norms of algebraic integers*, Mathematika **22** (1975), no. 1, 71–80. MR 0424757 5.2
27. ———, *Solution of some problems of Serre on modular forms: The method of Frobenian functions.*, Recent progress in analytic number theory, Symp. Durham 1979, Vol. 2, London ; New York : Academic Press, 1981, pp. 159–169. 2
28. ———, *Notes on the method of Frobenian functions with applications to Fourier coefficients of modular forms*, Elementary and analytic theory of numbers (Warsaw, 1982), Banach Center Publ., vol. 17, PWN, Warsaw, 1985, pp. 371–403. MR 840484 2
29. K. Ramachandra, *Some problems of analytic number theory*, Acta Arith. **31** (1976), no. 4, 313–324. MR 0424723 5.2
30. Hans Reichardt, *Der Primdivisorsatz für algebraische Funktionenkörper über einem endlichen Konstantenkörper*, Math. Z. **40** (1936), no. 1, 713–719. MR 1545595 1.2
31. Brad Rodgers, *Arithmetic functions in short intervals and the symmetric group*, Algebra Number Theory **12** (2018), no. 5, 1243–1279. MR 3840876 3
32. Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR 1876657 1.2, A.1
33. Jean-Pierre Serre, *Divisibilité de certaines fonctions arithmétiques*, (1975), 28. MR 0392831 2
34. ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401. MR 644559 1.1
35. ———, *Abelian l-adic representations and elliptic curves*, Research Notes in Mathematics, vol. 7, A K Peters, Ltd., Wellesley, MA, 1998, With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original. MR 1484415 1.1
36. K. Soundararajan, *The distribution of prime numbers*, Equidistribution in number theory, an introduction, NATO Sci. Ser. II Math. Phys. Chem., vol. 237, Springer, Dordrecht, 2007, pp. 59–83. MR 2290494 1.1

37. Richard P. Stanley, *Enumerative combinatorics. Vol. 2*, Cambridge Studies in Advanced Mathematics, vol. 62, Cambridge University Press, Cambridge, 1999, With a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin. MR 1676282 5.2

38. Jesse Thorner, *A variant of the Bombieri-Vinogradov theorem in short intervals and some questions of Serre*, Math. Proc. Cambridge Philos. Soc. **161** (2016), no. 1, 53–63. MR 3505669 1.1

39. H. Weber, *Lehrbuch der Algebra. In zwei Bänden. 2. Band.*, Braunschweig : Friedrich Vieweg und Sohn, 1896. 5.2

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

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel
E-mail address: ofir.goro@gmail.com

Department of Mathematics, Caltech, Pasadena, CA 91125, USA
E-mail address: tkaridi@caltech.edu

Department of Mathematics, Columbia University, New York, NY 10027, USA
E-mail address: sawin@math.columbia.edu