

PRIMES IN SHORT INTERVALS ON CURVES OVER FINITE FIELDS

EFRAT BANK AND TYLER FOSTER

ABSTRACT. We prove an analogue of the Prime Number Theorem for short intervals on a smooth projective geometrically irreducible curve of arbitrary genus over a finite field. A short interval “of size E ” in this setting is any additive translate of the space of global sections of a sufficiently positive divisor E by a suitable rational function f . Our main theorem gives an asymptotic count of irreducible elements in short intervals on a curve in the “large q ” limit, uniformly in f and E . This result provides a function field analogue of an unresolved short interval conjecture over number fields, and extends a theorem of Bary-Soroker, Rosenzweig, and the first author, which can be understood as an instance of our result for the special case of a divisor E supported at a single rational point on the projective line.

CONTENTS

1. Introduction	1
2. Short intervals on curves	6
3. Galois group of a generic element in a short interval	8
4. Calculation of the Galois group	11
5. Proof of Theorem A	17
References	20

1. INTRODUCTION

In this paper, we give an asymptotic count of irreducible elements inside short intervals on a smooth projective geometrically irreducible curve over a finite field. Our main result (§1.3, Theorem A) provides a function field analogue of an unresolved short interval conjecture for number fields (Conjecture 1.3.1), and extends a short interval theorem of Bary-Soroker, Rosenzweig, and the first author [2, Corollary 2.4] for polynomials over finite fields.

The notion of short intervals on a curve which we use is a natural analogue of the familiar notion of short intervals over the integers. In this introduction, we review what is known about short intervals over the integers, over number fields, and over polynomials with coefficients in a finite field. The analogies that run between these different settings lead naturally to our definition of a short interval on a curve and to the statement of our main result.

1.1. The Prime Number Theorem for short intervals. The Prime Number Theorem (PNT) states that the asymptotic density of prime integers in real intervals $(0, x]$ is $1/\log x$. In other words, if we let $\pi(x)$ denote the prime counting function

$$\pi(x) = \#\{0 < p \leq x : p \text{ is a prime integer}\},$$

then

$$\pi(x) \sim \frac{x}{\log x} \quad \text{as } x \rightarrow \infty. \quad (1)$$

Date: October 15, 2018.

We get more refined statements by considering the asymptotic density of primes in families of smaller intervals. Letting $\Phi(x)$ be a real valued function with $0 < \Phi(x) < x$, we can ask for the density of primes in the intervals $I(x, \Phi) \stackrel{\text{def}}{=} [x - \Phi(x), x + \Phi(x)]$ as $x \rightarrow \infty$. Define

$$\pi(I(x, \Phi)) \stackrel{\text{def}}{=} \#\{p \in I(x, \Phi) : p \text{ is a prime integer}\},$$

Then the naive conjecture on the asymptotic density of primes in the intervals $I(x, \Phi)$ is

$$\pi(I(x, \Phi)) \sim \frac{\#(I(x, \Phi))}{\log x} \quad \text{as } x \rightarrow \infty. \quad (2)$$

For fixed $0 < c < 1$ and $\Phi(x) \sim cx$, it is a straightforward consequence of the PNT that (2) holds. Assuming the Riemann hypothesis, (2) holds for $\Phi(x) = x^{\varepsilon + \frac{1}{2}}$ for small $0 < \varepsilon < 1/2$. On the other hand, Maier [22] established what is now known as the ‘‘Maier phenomenon’’: for $\Phi(x) = (\log x)^A$, with $A > 1$, the asymptotic formula (2) fails. A classical conjecture predicts the following ‘‘short interval’’ prime number conjecture:

Conjecture 1.1.1. For $0 < \varepsilon < 1$ and $\Phi(x) = x^\varepsilon$, the asymptotic formula (2) holds.

In its full generality, Conjecture 1.1.1 is still open. Heath-Brown [15], improving on Huxley [16], proved Conjecture 1.1.1 for $\frac{7}{12} \leq \varepsilon < 1$. We refer the reader to the surveys of Granville [7, 8] for additional background.

1.2. The Prime Polynomial Theorem for short intervals over $\mathbb{F}_q[t]$. For each finite field \mathbb{F}_q , the analogy between number fields and function fields provides us with the following table of corresponding sets and quantities:

\mathbb{Z}	ring of polynomials $\mathbb{F}_q[t]$
$ x $	$ f \stackrel{\text{def}}{=} q^{\deg f}$
$(0, x]$	$M(k, q) \stackrel{\text{def}}{=} \{h \in \mathbb{F}_q[t] : h \text{ is monic and } \deg h = k\}$
$x = \#(0, x]$	$q^k = \#M(k, q)$
$\log x$	$k = \log_q q^k$

(3)

If we let $\pi_q(k)$ denote the prime polynomial counting function

$$\pi_q(k) = \#\{h \in M(k, q) : h \text{ is irreducible}\},$$

then, in accord with Table (3), the Prime Polynomial Theorem (PPT) asserts that

$$\pi_q(k) \sim \frac{q^k}{k} \quad \text{as } q^k \rightarrow \infty. \quad (4)$$

Table (3) also suggests a natural definition of short intervals in $\mathbb{F}_q[t]$:

Definition 1.2.1. Given any monic non-constant polynomial $f \in \mathbb{F}_q[t]$ and any positive real number ε , the corresponding *interval (around f)* is the set

$$I(f, \varepsilon) \stackrel{\text{def}}{=} \{h \in \mathbb{F}_q[t] : |h - f| \leq |f|^\varepsilon\}.$$

If $m \stackrel{\text{def}}{=} \lfloor \varepsilon \deg f \rfloor$ and $\mathbb{F}_q[t]^{\leq m}$ denotes the space of polynomials of degree at most m , then $I(f, \varepsilon) = f + \mathbb{F}_q[t]^{\leq m}$. We say that $I(f, \varepsilon)$ is a *short interval* if $\varepsilon < 1$, i.e., if $m < \deg f$.

Remark 1.2.2. Note that in view of Definition 1.2.1, the set $M(k, q)$ of monic polynomials of degree k is the short interval $I(t^k, k - 1)$.

Initial results on the density of prime polynomials in short intervals can be deduced from the work of Cohen [4] when $\text{char } \mathbb{F}_q > \deg f$, and from the work of Keating and Rudnick [18] in an almost everywhere sense. In [2], the first author together with Bary-Soroker and Rosenzweig prove the following analogue of Conjecture 1.1.1 in the large q limit:

Theorem 1.2.3. [2, Corollary 2.4]. For fixed $k > 0$ and a monic polynomial $f \in \mathbb{F}_q[t]$ satisfying $\deg f = k$ and $\varepsilon > 0$, define

$$\pi_q(I(f, \varepsilon)) \stackrel{\text{def}}{=} \#\{h \in I(f, \varepsilon) : h \text{ is a prime polynomial}\}.$$

Then the asymptotic formula

$$\pi_q(I(f, \varepsilon)) \sim \frac{\#I(f, \varepsilon)}{k} \quad \text{as } q \rightarrow \infty \quad (5)$$

holds uniformly for all monic $f \in \mathbb{F}_q[t]$ of degree k and all

$$\varepsilon_0 \leq \varepsilon < 1, \quad \text{where } \varepsilon_0 = \begin{cases} \frac{3}{k} & \text{if } \text{char } \mathbb{F}_q = 2 \text{ and } f' \text{ is constant;} \\ \frac{2}{k} & \text{if } \text{char } \mathbb{F}_q \neq 2 \text{ or } f' \text{ is non-constant;} \\ \frac{1}{k} & \text{if } \text{char } \mathbb{F}_q \nmid k(k-1). \end{cases} \quad (6)$$

1.3. Short interval conjectures over number fields. One can extend Conjecture 1.1.1 to arbitrary number fields. However, because the relevant notions in \mathbb{Q} have several competing generalizations to number fields larger than \mathbb{Q} , there are several competing generalizations of Conjecture 1.1.1. If we let K be an algebraic number field of degree n over \mathbb{Q} , with ring of integers \mathcal{O}_K , then each prime $\mathfrak{a} \subset \mathcal{O}_K$ comes with a norm $N_K(\mathfrak{a}) \stackrel{\text{def}}{=} \#(\mathcal{O}_K/\mathfrak{a})$. The norm of an element $a \in \mathcal{O}_K$ is by definition the norm of the ideal that a generates. We have both a prime ideal and a principal prime ideal counting function:

$$\begin{aligned} \pi_K(x) &= \#\{\text{prime ideals } \mathfrak{p} \subset \mathcal{O}_K : 2 < N_K(\mathfrak{p}) \leq x\}; \\ \pi_{K, \text{prin}}(x) &= \#\{\text{principal prime ideals } (a) \subset \mathcal{O}_K : 2 < N_K(a) \leq x\}. \end{aligned}$$

Landau's Prime Ideal Theorem (PIT) [20] states that

$$\pi_K(x) \sim \frac{x}{\log x} \quad \text{as } x \rightarrow \infty. \quad (7)$$

Letting h_K denote the class number of K , the Principal PIT [25, §7.2, Corollary 4] states that

$$\pi_{K, \text{prin}}(x) \sim \frac{1}{h_K} \cdot \frac{x}{\log x} \quad \text{as } x \rightarrow \infty. \quad (8)$$

As before, we can attempt to refine these density theorems by considering any real valued function $\Phi(x)$, with $0 < \Phi(x) < x$, the corresponding (real) intervals $I(x, \Phi) = [x - \Phi(x), x + \Phi(x)]$ and the prime ideal counting function

$$\pi_K(I(x, \Phi)) = \#\{\text{primes } \mathfrak{p} \subset \mathcal{O}_K : x - \Phi(x) \leq N_K(\mathfrak{p}) \leq x + \Phi(x)\}.$$

The naive guess about the asymptotic behavior of $\pi_K(I(x, \Phi))$ is that

$$\pi_K(I(x, \Phi)) \sim \frac{\#I(x, \Phi)}{\log x} = \frac{2\Phi(x)}{\log x} \quad \text{as } x \rightarrow \infty. \quad (9)$$

When $\Phi(x) \sim cx$ for fixed $0 < c < 1$, formula (9) follows directly from the PIT. Balog and Ono [1], using formulas for the prime ideal counting function due to Lagarias and Odlyzko [19] and zero density estimates for Dedekind zeta-functions due to Heath-Brown [14] and Mitsui [24], show that formula (9) holds for $x^{1-\frac{1}{c}+\varepsilon} \leq \Phi(x) \leq x$. Here one may take $c = 8/3$ if $[K : \mathbb{Q}] = 2$, and one can take $c = [K : \mathbb{Q}]$ if the degree of the extension is at least 3. Assuming the Riemann

Hypothesis for the Dedekind zeta function $\zeta_K(s)$, Grenié, Molteni, and Perelli [9] show that (9) holds for all $\Phi(x) = (n \log x + \log |\text{disc}(K)|) \sqrt{x}$.

In a general number field, the norm $N_K(a)$ of an element $a \in \mathcal{O}_K$ is not equal to the absolute value of a at a single infinite place of K . Likewise, given an element $b \in \mathcal{O}_K$ with $x \stackrel{\text{def}}{=} N_K(b)$, and given $0 < \varepsilon < 1$, the set of all $a \in \mathcal{O}_K$ satisfying $|N_K(a) - x| \leq x^\varepsilon$ (with $|\cdot|$ the absolute value in \mathbb{R}) is not necessarily the same as the set of all $a \in \mathcal{O}_K$ satisfying $N_K(a - b) \leq x^\varepsilon$. This ambiguity in generalizing the basic quantities in Conjecture 1.1.1 gives us at least two distinct conjectures that can be seen as extensions Conjecture 1.1.1 to an arbitrary number field K :

Conjecture 1.3.1. Let $S = \{\text{infinite places of } K\}$. There exists some constant c such that for each real vector $\varepsilon_S = (\varepsilon_{\mathfrak{p}})_{\mathfrak{p} \in S}$ in $(0, 1)^S \subset \mathbb{R}^S$, the count

$$\pi_{K, \text{prin}}(I(b, \varepsilon_S)) = \#\{a \in \mathcal{O}_K : |a - b|_{\mathfrak{p}} \leq |b|_{\mathfrak{p}}^{\varepsilon_{\mathfrak{p}}} \text{ for each } \mathfrak{p} \in S, \text{ and } (a) \subset \mathcal{O}_K \text{ is prime}\}$$

satisfies the asymptotic formula

$$\pi_{K, \text{prin}}(I(b, \varepsilon_S)) \sim c \cdot \frac{\#\{a \in \mathcal{O}_K : |a - b|_{\mathfrak{p}} \leq |b|_{\mathfrak{p}}^{\varepsilon_{\mathfrak{p}}} \text{ for all } \mathfrak{p} \in S\}}{\log N_K(b)} \quad \text{as } N_K(b) \rightarrow \infty. \quad (10)$$

Conjecture 1.3.2. There exists some constant c such that for each $0 < \varepsilon < 1$, the count

$$\pi_{K, \text{prin}}(I(x, \varepsilon)) = \#\{\text{principal prime ideals } (a) \subset \mathcal{O}_K : x - x^\varepsilon < N_K(a) \leq x + x^\varepsilon\}.$$

satisfies the asymptotic formula

$$\pi_{K, \text{prin}}(I(x, \varepsilon)) \sim c \cdot \frac{\#I(x, \varepsilon)}{\log x} = c \cdot \frac{2x^\varepsilon}{\log x} \quad \text{as } x \rightarrow \infty. \quad (11)$$

Remark 1.3.3. For $K = \mathbb{Q}$, Conjectures 1.3.1 and 1.3.2 both recover Conjecture 1.1.1 if $c = 1$.

1.4. Main result: short intervals on arbitrary curves over \mathbb{F}_q . Let C be a smooth projective geometrically irreducible curve over \mathbb{F}_q . As shown in [27, Theorem 5.12], the natural analogue of the PNT holds on C , which is to say that the counting function

$$\pi_C(k) \stackrel{\text{def}}{=} \#\{P \text{ a prime divisor of } C : \deg(P) = k\}$$

satisfies the asymptotic formula

$$\pi_C(k) \sim \frac{q^k}{k} \quad \text{as } q^k \rightarrow \infty.$$

One can formulate analogues of each of the Conjectures 1.3.1 and 1.3.2 on C . In the present paper, we focus our attention to the analogue of Conjecture 1.3.1 in the large q limit. We intend to address analogues of Conjecture 1.3.2 in a future paper.

On C , the natural analogue of the ‘‘short interval’’ implicit in Conjecture 1.3.1 is the following set:

Definition 1.4.1. Let $E = m_1 \mathfrak{p}_1 + \cdots + m_s \mathfrak{p}_s$ be an effective divisor on C , and let f be a regular function on the complement of E . The *interval (of size E around f)* is the set

$$\begin{aligned} I(f, E) &\stackrel{\text{def}}{=} \left\{ \begin{array}{l} \text{regular functions } h \text{ on } C \setminus \text{supp}(E) \text{ such} \\ \text{that } \nu_{\mathfrak{p}_i}(h - f) \geq -m_i \text{ for all } 1 \leq i \leq s \end{array} \right\} \\ &= f + H^0(C, \mathcal{O}(E)), \end{aligned} \quad (12)$$

where $H^0(C, \mathcal{O}(E))$ is the space of regular functions on $C \setminus \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ with a pole of order at most m_i at each point \mathfrak{p}_i , for $1 \leq i \leq s$.

The interval $I(f, E)$ is a *short interval* if the order of the pole of f at each \mathfrak{p}_i is strictly greater than m_i .

Remark 1.4.2. When $C = \mathbb{P}^1$ and $E = m \infty$, for $m > 0$, Definitions 1.4.1 and 1.2.1 coincide.

The value that serves as our prime count in any short interval $I(f, E)$ is

$$\pi_C(I(f, E)) \stackrel{\text{def}}{=} \# \left\{ \begin{array}{l} h \in I(f, E) \text{ such that } h \text{ generates a} \\ \text{prime ideal in the ring of regular} \\ \text{functions on } C \setminus \text{supp}(E) \end{array} \right\}. \quad (13)$$

The central result of the present paper is the following theorem, which establishes a function field analogue of Conjecture 1.1.1 and its generalization 1.3.1. In addition, this result extends Theorem 1.2.3 to curves of arbitrary genus over \mathbb{F}_q :

Theorem A. Let C be a smooth projective geometrically irreducible curve of genus g over \mathbb{F}_q . Fix a positive integer $k > 0$. Let E be an effective divisor on C , and let f be a regular function on $C \setminus \text{supp}(E)$ such that the sum of the orders of all poles of f is equal to k , and such that $I(f, E)$ is a short interval. Assume that either

- (i) $E \geq 3E_0$ for some effective divisor E_0 with $\deg E_0 \geq 2g + 1$, or
- (ii) $\text{char } \mathbb{F}_q = 2$, $E \geq 2E_0$ for some effective divisor E_0 with $\deg E_0 \geq 2g + 1$, such that the differential df vanishes on a nonempty finite subset of $C \setminus \text{supp}(E)$.

Then

$$\pi_C(I(f, E)) = \frac{\#I(f, E)}{k} \left(1 + O(q^{-1/2}) \right) \quad (14)$$

where the implied constant in the error term $O(q^{-1/2})$ depends only on k and g .

Remark 1.4.3. To establish Theorem A, we prove a result (Theorem 5.2.1) that is stronger than Theorem A. For any partition type of the set $\{1, 2, \dots, k\}$, we provide an asymptotic count of rational functions $h \in I(f, E)$ whose associated principal divisor on $C \setminus \text{supp}(E)$ has that partition type.

Remark 1.4.4. Note that since $I(f, E)$ is a short interval, all poles of f lie in $\text{supp}(E)$, and for each $\mathfrak{p} \in \text{supp}(E)$, the order $\text{ord}_{\mathfrak{p}}(f)$ of each pole of f at \mathfrak{p} is strictly greater than the order $m_{\mathfrak{p}}$ of E at \mathfrak{p} . Because k is the sum of orders of all poles of f , Definition 1.4.1 then implies that k is equal to the sum $\sum_{\mathfrak{p} \in \text{supp}(E)} \max\{m_{\mathfrak{p}}, \text{ord}_{\mathfrak{p}}(f)\}$.

1.5. Outline of the paper. In broad outline, our strategy for proving Theorem A is similar to the strategy taken in [2]; the key insight of the present paper is that specific positivity hypotheses for divisors on C allow one to adapt the steps of the original argument in [2, §3 and §4] to a curve of arbitrary genus. In more detail, the outline of the paper is as follows.

In §2 we review the divisor theory and positivity conditions we will need. We introduce a variety parameterizing the elements of a short interval, and we use this variety to describe the generic element in a short interval. In §3 we explain how to associate a Galois group to the generic element. Most of the work in this section lies in showing that the Galois group is well defined. In §4 we calculate the Galois group. Specifically, we show that it is isomorphic to a symmetric group by verifying the conditions in a particular characterization of the symmetric group. In §5 we use our knowledge of this Galois group, along with some basic facts about étale morphisms, to show that a key counting result in [2], originally stated only for the genus zero case, can be extended to a count in any genus. Finally, we use this count to prove Theorem A and its stronger form Theorem 5.2.1. Our arguments in §5 make crucial use of the Lang-Weil estimates [21] and Bary-Soroker's Chebotarev-type result [3, Proposition 2.2].

1.6. Acknowledgments. The authors would like to thank Lior Bary-Soroker and Michael Zieve for many conversations during our work on this paper that were crucial to its success. We also extend a warm thank you to Jeff Lagarias for comments on a draft of the paper and for his

assistance in formulating prime density theorems in number fields. The exposition benefited greatly from an invitation to speak at the Palmetto Number Theory Series, held at the University of South Carolina and organized by Matthew Boylan, Michael Filaseta, and Frank Thorne, and from an invitation by Jordan Ellenberg to speak in the Number Theory Seminar at the University of Wisconsin–Madison.

We are especially thankful to Brian Conrad for looking closely at an earlier version of this paper, for pointing out a gap in our uniformity argument (now filled), for pointing out that we needed to prove what is now Proposition 3.3.6, and for suggesting that we use [5, §1, Lemma 1.5] to do so.

The authors conducted the research that lead to this paper while at the University of Michigan and while the second author was a visiting researcher at L’Institut des Hautes Études Scientifiques, at L’Institut Henri Poincaré, and at the Max Planck Institute for Mathematics. We thank all four institutions for their hospitality. The first author was partially supported by Michael Zieve’s NSF grant DMS-1162181. Support for the second author came from NSF RTG grant DMS-0943832 and from Le Laboratoire d’Excellence CARMIN.

2. SHORT INTERVALS ON CURVES

Fix a finite field \mathbb{F}_q , an algebraic closure $\overline{\mathbb{F}_q}/\mathbb{F}_q$, and a smooth projective geometrically irreducible curve C over \mathbb{F}_q of arithmetic genus g .

2.1. Divisors on a curve. We make extensive use of the theory of divisors on algebraic varieties (see [13, §II.6] for instance). We briefly review the most pertinent aspects of the theory.

By a *divisor on C* , we mean a Weil divisor on C . We denote the support of a divisor D by $\text{supp}(D)$, although we drop the distinction between D and its support when it will not lead to confusion. For instance, we write $C \setminus D$ instead of $C \setminus \text{supp}(D)$. If f is a rational function on C , we denote its associated principal divisor by $\text{div}(f)$. Given a divisor $D = \sum_{\mathfrak{p} \in C} m_{\mathfrak{p}} \mathfrak{p}$ on C , its *divisor of zeros* and *divisor of poles* are, respectively, the effective divisors

$$D_+ \stackrel{\text{def}}{=} \sum_{m_{\mathfrak{p}} > 0} m_{\mathfrak{p}} \mathfrak{p} \quad \text{and} \quad D_- \stackrel{\text{def}}{=} \sum_{m_{\mathfrak{p}} < 0} -m_{\mathfrak{p}} \mathfrak{p}.$$

Note that $D = D_+ - D_-$.

Each divisor D on C determines a sheaf $\mathcal{O}(D)$ of rational functions on C whose value at each open subset $U \subset C$ is

$$\mathcal{O}(D)(U) \stackrel{\text{def}}{=} \{0\} \sqcup \{f \in \mathbb{F}_q(C)^\times : \text{div}(f)|_U \geq -D|_U\}.$$

For each $i \geq 0$, the \mathbb{F}_q -vector space $H^i(C, \mathcal{O}(D))$ is finite dimensional. We stress that according to the definition of $\mathcal{O}(D)$ that we use, the space of global sections $H^0(C, \mathcal{O}(D))$ is canonically a space of rational functions on C .

For each $m \geq 0$, fix homogeneous coordinates x_0, \dots, x_m on \mathbb{P}^m . Let $V(x_0) \subset \mathbb{P}^m$ denote the hyperplane cut out by x_0 . If $H^0(C, \mathcal{O}(D))$ admits a basis $\{f_0, \dots, f_m\}$ such that at least one of the functions f_i is non-vanishing at each $\mathfrak{p} \in C$, we say that D is *basepoint free*. If D is basepoint free, then our basis gives rise to a morphism

$$\varphi = [f_0 : \dots : f_m] : C \longrightarrow \mathbb{P}^m \tag{15}$$

into projective space of dimension

$$m = \dim H^0(C, \mathcal{O}(D)) - 1.$$

The divisor D is *very ample* if D is basepoint free and the morphism (15) is a closed embedding. Every divisor D on C satisfying $\deg D \geq 2g + 1$ is very ample.

If E is an effective very ample divisor on C , then the basis $\{f_0, \dots, f_m\}$ of $H^0(C, \mathcal{O}(E))$ can be chosen so that $f_0 = 1$, with

$$\varphi(\text{supp}(E)) = \varphi(C) \cap V(x_0) \quad \text{and} \quad C \setminus E = \varphi^{-1}(\mathbb{P}^m \setminus V(x_0)). \quad (16)$$

In particular, if E is an effective very ample divisor, then the open subscheme $C \setminus E \subset C$ is affine, and its ring of regular functions is generated by the coordinates x_1, \dots, x_m on $\mathbb{P}^m \setminus V(x_0)$. We consistently use the notation

$$R \stackrel{\text{def}}{=} \text{ring of regular functions on } C \setminus E.$$

Remark 2.1.1. Note that if D_0 and D are divisors on C satisfying $D_0 \leq D$, then we have a natural inclusion $H^0(C, \mathcal{O}(D_0)) \subset H^0(C, \mathcal{O}(D))$. Thus if D_0 is very ample and $D_0 \leq D$, then D is also very ample.

Remark 2.1.2. Given a field extension K/\mathbb{F}_q , each point \mathfrak{p} in C has a unique factorization $\mathfrak{p} = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_n^{e_n}$ locally on $C_K = \text{Spec}(K) \times_{\text{Spec}(\mathbb{F}_q)} C$. The pullback of $E = \sum m_{\mathfrak{p}} \mathfrak{p}$ to C_K is the divisor

$$E_K \stackrel{\text{def}}{=} \sum_{\mathfrak{p} \in C} \left(\sum_{i=1}^n m_{\mathfrak{p}} e_i \mathfrak{q}_i \right).$$

Note that $\deg E = \deg E_K$, and that if E is effective, then E_K is effective as well. The sheaf $\mathcal{O}(E)$ on C pulls back to a sheaf $\mathcal{O}(E)_K$ on C_K , and we have a canonical isomorphism $\mathcal{O}(E_K) \cong \mathcal{O}(E)_K$ [12, §9.4.2], thus E_K is very ample whenever E is.

2.2. Generic element in a short interval. Let E be an effective very ample divisor on C . Then following Definition 1.4.1, each regular function f on $C \setminus E$ determines an interval

$$I(f, E) = f + H^0(C, \mathcal{O}(E)).$$

The fact that $f \in R$ and $H^0(C, \mathcal{O}(E)) \subset R$ implies that $I(f, E) \subset R$.

Choose a basis $\{1, f_1, \dots, f_m\}$ of $H^0(C, \mathcal{O}(E))$ as in §16. Then we have a corresponding interpretation of

$$\mathbb{A}^{m+1} \stackrel{\text{def}}{=} \text{Spec } \mathbb{F}_q[A_0, \dots, A_m] = \text{Spec } \mathbb{F}_q[\mathbf{A}]$$

as a variety parameterizing the functions in $I(f, E)$. Let $\mathbb{F}_q(\mathbf{A})$ denote the field of rational functions $\mathbb{F}_q(A_0, \dots, A_m)$, and define

$$R[\mathbf{A}] \stackrel{\text{def}}{=} R \otimes_{\mathbb{F}_q} \mathbb{F}_q[\mathbf{A}] \quad \text{and} \quad R(\mathbf{A}) \stackrel{\text{def}}{=} R \otimes_{\mathbb{F}_q} \mathbb{F}_q(\mathbf{A}).$$

On the trivial family of curves $\mathbb{A}^{m+1} \times (C \setminus E) = \text{Spec } R[\mathbf{A}]$, we have a regular function

$$\mathcal{F}_{\mathbf{A}} \stackrel{\text{def}}{=} f + A_0 + \sum_{i=1}^m A_i f_i. \quad (17)$$

See Figure 1 for a depiction of the scheme $V(\mathcal{F}_{\mathbf{A}})$ cut out by $\mathcal{F}_{\mathbf{A}}$ inside the family $\mathbb{A}^{m+1} \times (C \setminus E)$. The restriction of $\mathcal{F}_{\mathbf{A}}$ to the generic fiber $\text{Spec } R(\mathbf{A})$ of this trivial family $\mathbb{A}^{m+1} \times (C \setminus E)$ describes the generic element of $I(f, E)$. If we denote \mathbb{F}_q -rational points in $\mathbb{A}^{m+1} = \text{Spec } \mathbb{F}_q[\mathbf{A}]$ as $(m+1)$ -tuples $\mathbf{a} = (a_0, \dots, a_m)$, then for each $\mathbf{a} \in \mathbb{A}^{m+1}(\mathbb{F}_q)$, the restriction $\mathcal{F}_{\mathbf{a}}$ of (17) to the fiber $\{\mathbf{a}\} \times (C \setminus E) \cong C \setminus E$ is an element of $I(f, E)$. The value $\pi_C(I(f, E))$ becomes the count of a particular set of \mathbb{F}_q -rational points in \mathbb{A}^{m+1} :

$$\pi_C(I(f, E)) = \#\{\mathbf{a} \in \mathbb{A}^{m+1}(\mathbb{F}_q) : \text{the ideal } (\mathcal{F}_{\mathbf{a}}) \subset R \text{ is prime}\}. \quad (18)$$

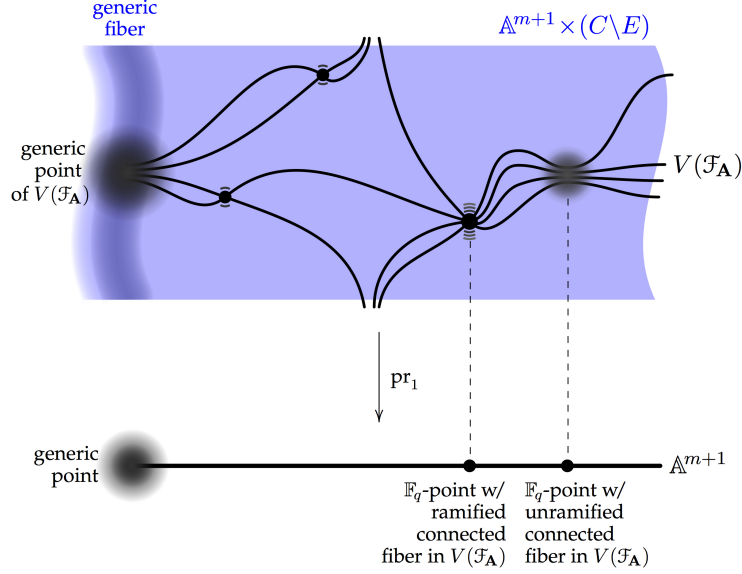


Figure 1. The scheme $V(\mathcal{F}_{\mathbf{A}})$ inside $\mathbb{A}^{m+1} \times (C \setminus E)$. By Lemmas 3.3.1 and 3.3.3, $V(\mathcal{F}_{\mathbf{A}})$ intersects the generic fiber at a single unramified point. Points $\mathbf{a} \in \mathbb{A}^{m+1}(\mathbb{F}_q)$ with unramified connected fiber in $V(\mathcal{F}_{\mathbf{A}})$ describe elements $\mathcal{F}_{\mathbf{a}} \in I(f, E)$ counted in $\pi_C(I(f, E))$.

3. GALOIS GROUP OF A GENERIC ELEMENT IN A SHORT INTERVAL

For any field K and any irreducible separable polynomial $f \in K[t]$, the residue field $\kappa(f) \stackrel{\text{def}}{=} K[t]/(f)$ admits a unique splitting field $\text{split}(f)$ inside any separable closure $\overline{K} = \overline{\kappa(f)}$. When we interpret $\kappa(f)$ as the field obtained by adjoining a single root of f to K , it becomes natural to construct $\text{split}(f)$ as the field obtained by adjoining all roots of f to K . We can also construct $\text{split}(f)$ without any explicit reference to roots of f . Indeed, $\text{split}(f)$ is the normal closure of $\kappa(f)$ inside \overline{K} [26, Theorem 2.9.5.(4)]. This latter characterization of the splitting field generalizes to the higher genus setting and, as we demonstrate in the present section, allows us to define the Galois group of the generic element in short intervals on C .

3.1. The setting of §3 and §4. The following datum is to remain fixed throughout §3 and §4: Let E be an effective very ample divisor on C , define R to be the ring of regular functions on the affine curve $C \setminus E$, and let $f \in R$ be a regular function on $C \setminus E$ satisfying

$$-\nu_{\mathfrak{p}}(f) > \nu_{\mathfrak{p}}(E) \quad \text{for all } \mathfrak{p} \in \text{supp}(E), \quad (19)$$

where $\nu_{\mathfrak{p}}(E)$ denotes the coefficient of \mathfrak{p} in E . Define

$$k \stackrel{\text{def}}{=} \deg(\text{div}(f)_-).$$

Note that the inequality (19) and the quantity k are unaffected by base change along any field extension K/\mathbb{F}_q . Let $I(f, E)$ be the short interval defined by f and E . Let $\mathcal{F}_{\mathbf{A}}$ be the generic element in $I(f, E)$ as defined in (17). Fix an algebraic closure $\overline{\mathbb{F}_q}(\mathbf{A})$ such that $\overline{\mathbb{F}_q} \subset \overline{\mathbb{F}_q}(\mathbf{A})$.

Remark 3.1.1. In the case where $g = 0$ and E is an effective divisor on \mathbb{P}^1 supported at ∞ , we have $H^0(\mathbb{P}^1, \mathcal{O}(E)) = \mathbb{F}_q[t]^{\leq m}$, where $m = \deg E$. The choice of a regular function f amounts to the choice of a polynomial $f \in \mathbb{F}_q[t]$, and $k = \deg(\text{div}(f)_-) = \deg f$. Thus the inequality (19) reduces to the requirement $m < k$ that appears in the form “ $\varepsilon_0 < 1$ ” in Theorem 1.2.3.

Remark 3.1.2. In §5, where we consider the asymptotic behavior of $I(f, E)$, we will allow E and f to vary subject to the constraint (19).

3.2. The splitting field and Galois group of a relative separable point. We can associate Galois groups to a large class of points in $C \setminus E$ as follows:

Definition 3.2.1. Let $K/\mathbb{F}_q(\mathbf{A})$ be an algebraic extension. For a prime ideal \mathfrak{P} in the ring $K \otimes_{\mathbb{F}_q(\mathbf{A})} R(\mathbf{A})$, denote by $\kappa(\mathfrak{P})$ the residue field of \mathfrak{P} . The *splitting field of \mathfrak{P} (over K)*, denoted $\text{split}(\mathfrak{P})$ or $\text{split}(\mathfrak{P}/K)$, is the normal closure of $\kappa(\mathfrak{P})$ in $\overline{\mathbb{F}_q(\mathbf{A})}$.

If the extension $\kappa(\mathfrak{P})/K$ is separable, then the *Galois group of \mathfrak{P}* is

$$\text{Gal}(\mathfrak{P}/K) \stackrel{\text{def}}{=} \text{Gal}(\text{split}(\mathfrak{P})/K).$$

Remark 3.2.2. For a prime ideal \mathfrak{P} in $K \otimes_{\mathbb{F}_q(\mathbf{A})} R(\mathbf{A})$, the fact that $\kappa(\mathfrak{P})/K$ is separable is equivalent to the statement that

$$\text{split}(\mathfrak{P}) \otimes_K \kappa(\mathfrak{P}) \cong \prod_{i=1}^{\deg \mathfrak{P}} \text{split}(\mathfrak{P}) \quad (20)$$

(see [30, Proposition 5.3.9, Definition 5.3.12 and Proposition 5.3.16.(1)]). Since $K \otimes_{\mathbb{F}_q} R(\mathbf{A})$ is a Dedekind domain, the isomorphism (20) is equivalent to the statement that in the ring $\text{split}(\mathfrak{P}) \otimes_{\mathbb{F}_q(\mathbf{A})} R(\mathbf{A})$, the ideal $\text{split}(\mathfrak{P}) \otimes_K \mathfrak{P}$ has prime factorization

$$\text{split}(\mathfrak{P}) \otimes_K \mathfrak{P} = \Omega_1 \cdots \Omega_{\deg \mathfrak{P}}, \quad (21)$$

where $\deg \Omega_i = 1$ and $\kappa(\Omega_i) \cong \text{split}(\mathfrak{P})$ for each $1 \leq i \leq \deg \mathfrak{P}$. The Galois group $\text{Gal}(\mathfrak{P}/K)$ acts faithfully and transitively on the prime factors Ω_i .

3.3. Primality and separability of the generic element. For any field extension K/\mathbb{F}_q , define

$$R_K[\mathbf{A}] \stackrel{\text{def}}{=} K \otimes_{\mathbb{F}_q} R[\mathbf{A}] \quad \text{and} \quad R_K(\mathbf{A}) \stackrel{\text{def}}{=} R \otimes_{\mathbb{F}_q} K(\mathbf{A}).$$

The canonical morphism $R[\mathbf{A}] \rightarrow R_K[\mathbf{A}]$ lets us interpret both f and $\mathcal{F}_{\mathbf{A}}$ as elements of $R_K[\mathbf{A}]$. By §2.1 and [10, Corollaire 6.9.9], we have

$$H^0(C_K, \mathcal{O}(E_K)) \cong K \otimes_{\mathbb{F}_q} H^0(C, \mathcal{O}(E)),$$

and $\mathbb{A}_K^{m+1} = \text{Spec } K[\mathbf{A}]$ becomes a variety parameterizing elements in $I(f, E_K)$.

Lemma 3.3.1. For any field extension K/\mathbb{F}_q , the ideal $(\mathcal{F}_{\mathbf{A}}) \subset R_K(\mathbf{A})$ generated by $\mathcal{F}_{\mathbf{A}}$ is prime in $R_K(\mathbf{A})$.

Proof. Let $V(\mathcal{F}_{\mathbf{A}})$ be the variety cut out by $\mathcal{F}_{\mathbf{A}}$ in $\mathbb{A}^{m+1} \times (C_K \setminus E_K)$. The projections

$$\mathbb{A}^{m+1} \xleftarrow{\text{Pr}_1} \mathbb{A}^{m+1} \times (C_K \setminus E_K) \xrightarrow{\text{Pr}_2} C_K \setminus E_K \quad (22)$$

restrict to morphisms

$$\mathbb{A}^{m+1} \xleftarrow{\text{Pr}_1|_{V(\mathcal{F}_{\mathbf{A}})}} V(\mathcal{F}_{\mathbf{A}}) \xrightarrow{\text{Pr}_2|_{V(\mathcal{F}_{\mathbf{A}})}} C_K \setminus E_K.$$

Assume that $(\mathcal{F}_{\mathbf{A}}) \subset R_K(\mathbf{A})$ is not prime. Then either the morphism $\text{pr}_1|_{V(\mathcal{F}_{\mathbf{A}})}$ has empty generic fiber, or else the subscheme $V(\mathcal{F}_{\mathbf{A}}) \subset \mathbb{A}_K^{m+1} \times (C_K \setminus E_K)$ has more than one irreducible component.

Comparing the strict inequalities (19) with the inequality defining the inclusion

$$A_0 + \sum_{i=1}^m A_i f_i \in H^0(C_{K(\mathbf{A})}, \mathcal{O}(E_{K(\mathbf{A})})),$$

we see that $\nu_{\mathfrak{p}}(\mathcal{F}_{\mathbf{A}}) < -m_{\mathfrak{p}}$ for all $\mathfrak{p} \in \text{supp } E_{K(\mathbf{A})}$. Thus

$$\text{div}(\mathcal{F}_{\mathbf{A}})_+ \neq 0 \quad \text{and} \quad \text{supp}(\text{div}(\mathcal{F}_{\mathbf{A}})_+) \subset C_K \setminus E_K. \quad (23)$$

In particular, $\mathcal{F}_{\mathbf{A}}$ is not a unit in $R_K(\mathbf{A})$, and $\text{pr}_1|_{V(\mathcal{F}_{\mathbf{A}})}$ does not have empty generic fiber.

Because $V(\mathcal{F}_{\mathbf{A}})$ is pure of codimension-1 inside $\mathbb{A}^{m+1} \times (C_K \setminus E_K)$, whereas $C_K \setminus E_K$ is 1-dimensional, an irreducible component of $V(\mathcal{F}_{\mathbf{A}})$ is either a whole fiber of the projection pr_2 in (22) over a closed point of $C_K \setminus E_K$, or else its generic point lies over the generic point of $C_K \setminus E_K$. For any point $x \in C_K \setminus E_K$, the function $\mathcal{F}_{\mathbf{A}}|_x = f(x) + A_0 + \sum A_i f_i(x) \in \kappa(x)[\mathbf{A}]$ is linear in the variables A_i , and is nonzero since A_0 has coefficient 1. For closed points $x \in C_K \setminus E_K$, this shows that closed fibers of the morphism pr_2 in (22) cannot be irreducible components of $V(\mathcal{F}_{\mathbf{A}})$. Over the generic point ξ of $C_K \setminus E_K$, linearity of the nonzero function $\mathcal{F}_{\mathbf{A}}|_{\xi}$ implies that the ideal $(\mathcal{F}_{\mathbf{A}}|_{\xi}) \subset K(C_K)[\mathbf{A}]$ is prime. Thus $V(\mathcal{F}_{\mathbf{A}})$ has a unique irreducible component. \square

Remark 3.3.2. Since C is a curve, Lemma 3.3.1 implies that the subscheme $V(\mathcal{F}_{\mathbf{A}})_K \subset C_{K(\mathbf{A})}$ consists of a single closed point \mathfrak{P}_K . The residue field $\kappa(\mathfrak{P}_K) = R_K(\mathbf{A})/(\mathcal{F}_{\mathbf{A}})$ is a finite extension of $K(\mathbf{A})$.

Lemma 3.3.3. For any field extension K/\mathbb{F}_q , the extension $\kappa(\mathfrak{P}_K)/K(\mathbf{A})$ in Remark 3.3.2 is separable.

Proof. For each homogenous function h on \mathbb{P}^m , let $D(h)$ denote the distinguished open subscheme of \mathbb{P}^m where h is nonzero. The fact that E is very ample allows us to choose a polynomial $f(\mathbf{x}) \in \mathbb{F}_q[x_1, \dots, x_m]$ such that the regular function $f \in R$ is the restriction of $f(\mathbf{x})$ to $C \setminus E = C \cap D(x_0)$. The function $\mathcal{F}_{\mathbf{A}}$ on $C_{K(\mathbf{A})}$ is then the restriction of the function

$$\mathcal{F}_{\mathbf{A}}(\mathbf{x}) \stackrel{\text{def}}{=} f(\mathbf{x}) + A_0 + \sum_{i=1}^m A_i x_i \quad \text{defined on} \quad D(x_0).$$

The curve C is smooth, therefore there exist functions $y \in \mathbb{F}_q[x_1, \dots, x_m]$ and $r_1, \dots, r_{m-1} \in \mathbb{F}_q[x_1, \dots, x_m, \frac{1}{y}]$ for which the point \mathfrak{P}_K in Remark 3.3.2 lies in the affine open neighborhood

$$C_{K(\mathbf{A})} \cap D(x_0 y)_{K(\mathbf{A})} \cong \text{Spec } K(\mathbf{A})[x_1, \dots, x_m, \frac{1}{y}] / (r_1, \dots, r_{m-1}),$$

and such that the determinant of the $(m-1) \times (m-1)$ -minor M_{mm} in the matrix

$$M \stackrel{\text{def}}{=} \begin{pmatrix} \begin{array}{cccc|c} \frac{\partial r_1}{\partial x_1} & \frac{\partial r_1}{\partial x_2} & \cdots & \frac{\partial r_1}{\partial x_{m-1}} & \frac{\partial r_1}{\partial x_m} \\ \frac{\partial r_2}{\partial x_1} & \frac{\partial r_2}{\partial x_2} & \cdots & \frac{\partial r_2}{\partial x_{m-1}} & \frac{\partial r_2}{\partial x_m} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{\partial r_{m-1}}{\partial x_1} & \frac{\partial r_{m-1}}{\partial x_2} & \cdots & \frac{\partial r_{m-1}}{\partial x_{m-1}} & \frac{\partial r_{m-1}}{\partial x_m} \end{array} \\ \hline \frac{\partial \mathcal{F}_{\mathbf{A}}(\mathbf{x})}{\partial x_1} & \frac{\partial \mathcal{F}_{\mathbf{A}}(\mathbf{x})}{\partial x_2} & \cdots & \frac{\partial \mathcal{F}_{\mathbf{A}}(\mathbf{x})}{\partial x_{m-1}} & \frac{\partial \mathcal{F}_{\mathbf{A}}(\mathbf{x})}{\partial x_m} \end{pmatrix} \quad (24)$$

is invertible on $C_{K(\mathbf{A})} \cap D(x_0 y)_{K(\mathbf{A})}$. The entries in the last row of M all have the explicit form

$$\frac{\partial \mathcal{F}_{\mathbf{A}}(\mathbf{x})}{\partial x_i} = \frac{\partial f(\mathbf{x})}{\partial x_i} + A_i.$$

Hence, the term associated to M_{mm} in the cofactor expansion of $\det(M)$ is the only cofactor term in which A_m appears. The coefficient of A_m in this term is nonzero at \mathfrak{P}_K , therefore $\det(M)$ is nonzero at \mathfrak{P}_K . The $K(\mathbf{A})$ -scheme $\text{Spec } \kappa(\mathfrak{P}_K)$ is then smooth of relative dimension

0 over $K(\mathbf{A})$, or equivalently, $\text{Spec } \kappa(\mathfrak{P}_K)$ is étale over $\text{Spec } K(\mathbf{A})$ [23, §I.3, Corollary 3.16], and the field extension $\kappa(\mathfrak{P}_K)/K(\mathbf{A})$ is separable [23, §I.3, Proposition 3.2.(a) & (e)]. \square

From Lemmas 3.3.1 and 3.3.3, we immediately have the following:

Corollary 3.3.4. For each algebraic extension K/\mathbb{F}_q , the prime ideal $\mathfrak{P}_K = (\mathcal{F}_{\mathbf{A}}) \subset R_K(\mathbf{A})$ has an associated Galois group, which we henceforth denote

$$\text{Gal}(\mathcal{F}_{\mathbf{A}}, K(\mathbf{A})) \stackrel{\text{def}}{=} \text{Gal}(\mathfrak{P}/K(\mathbf{A})). \quad \square$$

Lemma 3.3.5. For each algebraic field extension K/\mathbb{F}_q , there is an inclusion of Galois groups

$$\text{Gal}(\mathcal{F}_{\mathbf{A}}, K(\mathbf{A})) \hookrightarrow \text{Gal}(\mathcal{F}_{\mathbf{A}}, \mathbb{F}_q(\mathbf{A})). \quad (25)$$

Proof. Since $\kappa(\mathfrak{P}_K)$ is isomorphic to the compositum $K \cdot \kappa(\mathfrak{P}) \subset \overline{\mathbb{F}_q(\mathbf{A})}$, we have isomorphisms

$$\text{Gal}(\mathcal{F}_{\mathbf{A}}, K(\mathbf{A})) \xrightarrow{\sim} \text{Gal}(K \cdot \kappa(\mathfrak{P})/K(\mathbf{A})) \xrightarrow{\sim} \text{Gal}(\kappa(\mathfrak{P}_K)/K(\mathbf{A})). \quad (26)$$

Post-composing (26) with the inclusion $\text{Gal}(\kappa(\mathfrak{P}_K)/K(\mathbf{A})) \hookrightarrow \text{Gal}(\kappa(\mathfrak{P}_K)/\mathbb{F}_q(\mathbf{A}))$, we obtain the embedding (25). \square

Proposition 3.3.6. The branch locus $Z \subset \mathbb{A}_{\mathbb{F}_q}^{m+1}$ of the morphism $\text{pr}_1 : V(\mathcal{F}_{\mathbf{A}}) \rightarrow \mathbb{A}^{m+1}$ has codimension ≥ 1 in $\mathbb{A}_{\mathbb{F}_q}^{m+1}$, and its compliment $\mathbb{A}^{m+1} \setminus Z$ is the maximal open subset of $\mathbb{A}_{\mathbb{F}_q}^{m+1}$ over which $V(\mathcal{F}_{\mathbf{A}})$ is finite étale.

Proof. Lemma 3.3.3 implies that $V(\mathcal{F}_{\mathbf{A}})$ is generically unramified over $\mathbb{A}_{\mathbb{F}_q}^{m+1}$, and thus that Z has codimension ≥ 1 in $\mathbb{A}_{\mathbb{F}_q}^{m+1}$. Define

$$X \stackrel{\text{def}}{=} \mathbb{A}_{\mathbb{F}_q}^{m+1} \setminus Z \quad \text{and} \quad Y \stackrel{\text{def}}{=} V(\mathcal{F}_{\mathbf{A}})_{\mathbb{A}_{\mathbb{F}_q}^{m+1} \setminus Z} = V(\mathcal{F}_{\mathbf{A}})_X.$$

Then the resulting morphism $\text{pr}_1|_Y : Y \rightarrow X$ is finite, surjective, and unramified of degree k . The variety X is a normal, and surjectivity of $\text{pr}_1|_Y$ implies that for each $y \in Y$, the morphism of stalks $\mathcal{O}_{X, \text{pr}_1(y)} \rightarrow \mathcal{O}_{Y, y}$ is injective [29, Tag 0CC1, (1) & (6)]. Thus by [5, §1, Lemma 1.5], the morphism $\text{pr}_1|_Y$ is étale. Because $\mathbb{A}_{\mathbb{F}_q}^{m+1} \setminus X$ is the branch locus Z , this implies that X is the maximal open subset of $\mathbb{A}_{\mathbb{F}_q}^{m+1}$ over which $V(\mathcal{F}_{\mathbf{A}})$ is finite étale. \square

4. CALCULATION OF THE GALOIS GROUP

4.1. A characterization of the symmetric group. Recall from §3.1 that we fix an effective very ample divisor E on C and a function f regular on $C \setminus E$ with poles satisfying the inequalities (19), and that $k \stackrel{\text{def}}{=} \deg(\text{div}(f)_-)$. Let S_k denote the symmetric group on k letters. Our goal in the present section is to prove the following:

Theorem 4.1.1. Assume that E satisfies one of the following two conditions

- (a) There exists a very ample effective divisor E_0 on C such that $E \geq 3E_0$;
- (b) There exists a very ample effective divisor E_0 on C such that $E \geq 2E_0$, $\text{char } \mathbb{F}_q = 2$, and $df|_{C \setminus E}$ vanishes on a finite nonempty set.

Then the Galois group $\text{Gal}(\mathcal{F}_{\mathbf{A}}, \mathbb{F}_q(\mathbf{A}))$ is isomorphic to S_k .

Remark 4.1.2. To prove Theorem 4.1.1, we use the following characterization of S_k :

Lemma 4.1.3. [28, Lemma 4.4.3]. A subgroup $G \subset S_k$ is equal to S_k if and only if G satisfies the following three conditions:

- (i) G is transitive;
- (ii) G is doubly transitive;

(iii) G contains a transposition. □

Beginning of the proof of Theorem 4.1.1. Observe that for any algebraic extension K/\mathbb{F}_q the condition (19) and its consequence (23), combined with the fact that the total degree of any principal divisor is 0, imply that $\deg \mathfrak{P}_K = k$. Thus by Remark 3.2.2, the Galois group $\text{Gal}(\mathcal{F}_{\mathbf{A}}, K(\mathbf{A}))$ comes with a natural faithful action on a set of k elements, namely the prime factors in (21). In this way, we obtain an embedding

$$\text{Gal}(\mathcal{F}_{\mathbf{A}}, K(\mathbf{A})) \hookrightarrow S_k \quad (27)$$

for each algebraic extension K/\mathbb{F}_q . For the special case $K = \overline{\mathbb{F}_q}$, Lemma 3.3.5 tells us that the inclusion (27) factors as

$$\begin{array}{ccc} & \text{Gal}(\mathcal{F}_{\mathbf{A}}, \overline{\mathbb{F}_q}(\mathbf{A})) & \\ & \swarrow \quad \searrow & \\ \text{Gal}(\mathcal{F}_{\mathbf{A}}, \mathbb{F}_q(\mathbf{A})) & \hookrightarrow & S_k. \end{array}$$

It therefore suffices to check that the Galois group $\text{Gal}(\mathcal{F}_{\mathbf{A}}, \overline{\mathbb{F}_q}(\mathbf{A}))$ satisfies the three conditions in Lemma 4.1.3. We verify these conditions in §4.2 and §4.3 below.

4.2. Transitivity and double transitivity. By Remark 3.2.2, the embedding (27) realizes the group $\text{Gal}(\mathcal{F}_{\mathbf{A}}/\overline{\mathbb{F}_q}(\mathbf{A}))$ as a transitive subgroup of S_k . Verifying condition (ii) of Lemma 4.1.3 in the setting of Theorem 4.1.1 amounts to proving the following:

Proposition 4.2.1. *If E satisfies either of the conditions (a) or (b) in Theorem 4.1.1, then the subgroup $\text{Gal}(\mathcal{F}_{\mathbf{A}}/\overline{\mathbb{F}_q}(\mathbf{A})) \subset S_k$ is doubly transitive.*

Remark 4.2.2. Note that each of the conditions (a) and (b) of Theorem 4.1.1 imply the following weaker condition: for any degree-1 point \mathfrak{q} in the support of E , the divisor $E - \mathfrak{q}$ is again effective and very ample.

Proof of Proposition 4.2.1. Because $\text{Gal}(\mathcal{F}_{\mathbf{A}}/\overline{\mathbb{F}_q}(\mathbf{A}))$ is transitive, it is enough to show that there exists a factor Ω_i in (21) for which the stabilizer subgroup of Ω_i inside $\text{Gal}(\mathcal{F}_{\mathbf{A}}/\overline{\mathbb{F}_q}(\mathbf{A}))$ is transitive on the set of factors $\{\Omega_j\}_{j \neq i}$.

Fix a single $\overline{\mathbb{F}_q}$ -valued point $\mathfrak{q} \in V(f) \subset C_{\overline{\mathbb{F}_q}} \setminus E_{\overline{\mathbb{F}_q}}$. Choose a hyperplane $L \subset \mathbb{P}_{\overline{\mathbb{F}_q}}^m$ such that the only point of $V(f)$ in $C_{\overline{\mathbb{F}_q}} \cap L$ is \mathfrak{q} . Define E' to be the effective divisor associated to the weighted intersection $C_{\overline{\mathbb{F}_q}} \cap L$. Choose a linear form $\ell \in \overline{\mathbb{F}_q}[x_0, \dots, x_m]$ satisfying $E' = \text{div}(\ell) + E_{\overline{\mathbb{F}_q}}$ and let $\mathfrak{h} \in \mathbb{A}_{\overline{\mathbb{F}_q}}^{m+1}$ be the generic point of the hyperplane cut out by the equation $\sum_{i=0}^m A_i \ell_i = 0$. Let $\mathcal{F}_{\mathfrak{h}}$ denote the restriction of $\mathcal{F}_{\mathbf{A}}$ to $\text{Spec } R_{\kappa(\mathfrak{h})}$. Then $\mathcal{F}_{\mathfrak{h}}$ factors as

$$\mathcal{F}_{\mathfrak{h}} = \ell \left(f' + A'_0 + \sum_{i=1}^{m-1} A'_i f'_i \right)$$

where $\{1, f'_1, \dots, f'_{m-1}\}$ is a basis of the subspace of $H^0(C_{\overline{\mathbb{F}_q}}, \mathcal{O}(E_{\overline{\mathbb{F}_q}}))$ corresponding to the hyperplane $V(\mathfrak{h}) \subset \mathbb{A}_{\overline{\mathbb{F}_q}}^{m+1}$, and where f' is a regular function on $C_{\overline{\mathbb{F}_q}} \setminus (E' - \mathfrak{q})$ satisfying

$$\text{div}(f')_{-} > E' - \mathfrak{q}. \quad (28)$$

The linear equivalence $E' \sim E_{\overline{\mathbb{F}_q}}$ makes E' very ample, thus $\dim H^0(C_{\overline{\mathbb{F}_q}}, \mathcal{O}(E' - \mathfrak{q})) = m$ with basis $\{1, f'_1, \dots, f'_{m-1}\}$. This implies that the linear combination

$$\mathcal{F}_{\mathbf{A}'} \stackrel{\text{def}}{=} f' + A'_0 + \sum_{i=1}^{m-1} A'_i f'_i$$

is the generic element of the interval $I(f', E')$. By Remark 4.2.2, $E' - \mathfrak{q}$ is effective and very ample. Hence (28) and Lemmas 3.3.1 and 3.3.3 provide us with a Galois group $\text{Gal}(\mathcal{F}_{\mathbf{A}'}, \overline{\mathbb{F}_q}(\mathbf{A}'))$.

Let R' denote the coordinate ring of the affine curve $C_{\overline{\mathbb{F}_q}} \setminus E'$. Observe that since $\deg E' = \deg E$, the inequalities (19) imply that $\mathfrak{P}'_{\overline{\mathbb{F}_q}}$ lies in $C_{\overline{\mathbb{F}_q}(\mathbf{A})} \setminus E'_{\overline{\mathbb{F}_q}(\mathbf{A})}$. Consider the point $\mathfrak{P}' \stackrel{\text{def}}{=} (\mathcal{F}_{\mathbf{A}'}) \in \text{Spec } R'(\mathbf{A}')$ inside $V(\mathcal{F}_{\mathbf{A}}) \subset \text{Spec } R'[\mathbf{A}']$. Because Lemma 3.3.3 says that \mathfrak{P}' is separable, whereas \mathfrak{h} is a codimension-1 point in $\mathbb{A}_{\overline{\mathbb{F}_q}}^{m+1}$, the point \mathfrak{P}' corresponds to a discrete valuation on $\kappa(\mathfrak{P}'_{\overline{\mathbb{F}_q}})$. Thus the Galois group $\text{Gal}(\text{split}(\mathfrak{P}'_{\overline{\mathbb{F}_q}})/\kappa(\mathfrak{P}'_{\overline{\mathbb{F}_q}}))$ acts transitively on the roots of any monic polynomial whose roots generate the extension $\text{split}(\mathfrak{P}')/\kappa(\mathfrak{P}')$. Because $\text{Gal}(\text{split}(\mathfrak{P}'_{\overline{\mathbb{F}_q}})/\kappa(\mathfrak{P}'_{\overline{\mathbb{F}_q}}))$ is a subgroup of $\text{Gal}(\mathcal{F}_{\mathbf{A}}, \overline{\mathbb{F}_q}(\mathbf{A}))$, this completes the proof. \square

4.3. Presence of a transposition. Fix an algebraic closure $L \stackrel{\text{def}}{=} \overline{\mathbb{F}_q(\mathbf{A})}$, and define $L' \subset L$ to be the algebraic closure $L' \stackrel{\text{def}}{=} \overline{\mathbb{F}_q(A_1, \dots, A_{m-1})}$ inside L .

Consider the morphism $C_{\mathbb{F}_q(\mathbf{A})} \longrightarrow \mathbb{P}_{\mathbb{F}_q(\mathbf{A})}^1 = \text{Proj } \mathbb{F}_q(\mathbf{A})[t_0, t_1]$. It restricts to the morphism of affine schemes

$$C_{\mathbb{F}_q(\mathbf{A})} \setminus E_{\mathbb{F}_q(\mathbf{A})} \longrightarrow \text{Spec } \mathbb{F}_q(\mathbf{A})[t] = D(t_0) \quad (29)$$

dual to the morphism of $\mathbb{F}_q(\mathbf{A})$ -algebras $\mathbb{F}_q(\mathbf{A})[t] \longrightarrow R_{\mathbb{F}_q(\mathbf{A})}$ that takes $t \mapsto \mathcal{F}_{\mathbf{A}} - A_0$. Since E is effective and very ample, we can choose a lift $f(\mathbf{x}) \in \mathbb{F}_q[x_1, \dots, x_m]$ of f as in the proof of Lemma 3.3.3, and (29) becomes the restriction of the morphism

$$\Psi : \text{Spec } \mathbb{F}_q(\mathbf{A})[x_1, \dots, x_m] \longrightarrow \text{Spec } \mathbb{F}_q(\mathbf{A})[t]$$

which takes

$$\mathbf{x} \mapsto \Psi(\mathbf{x}) \stackrel{\text{def}}{=} f(\mathbf{x}) + \sum_{i=1}^m A_i x_i.$$

Proposition 4.3.1. At each point in $C_L \setminus E_L$, the ramification order of Ψ is at most 1.

Proof. Let $\Omega_{C_L \setminus E_L}^1$ denote the R_L -module of Kähler differentials on $C_L \setminus E_L = \text{Spec } R_L$, and let $d\Psi \in \Omega_{C_L \setminus E_L}^1$ denote the Kähler differential of Ψ . In $D(x_0)$, on a sufficiently small affine open neighborhood $U_{\mathbf{x}} \subset D(x_0)$ of each point $\mathbf{x} \in C_L \setminus E_L$, we have a matrix M as in equation (24), where the regular functions r_i cut out $U_{\mathbf{x}} \cup (C_L \setminus E_L)$. Since $d\Psi = d(\Psi + A_0) = d\mathcal{F}_{\mathbf{A}}$, the ramification divisor of Ψ is the effective divisor corresponding to the subscheme $V(\det(M)) \cap (C_L \setminus E_L)$ inside $U_{\mathbf{x}} \subset \text{Spec } L[x_1, \dots, x_m]$. The points of $U_{\mathbf{x}} \cap (C_L \setminus E_L)$ where Ψ has ramification order 1 are exactly the reduced points of $V(\det(M)) \cap (C_L \setminus E_L)$. Thus it suffices to prove that the L -scheme $V(\det(M)) \cap (C_L \setminus E_L)$ is smooth.

For each $1 \leq i \leq m$, let M_{mi} denote the minor of M that we obtain by removing the m^{th} -row and i^{th} -column of M , so that

$$\det(M) = \sum_{i=1}^m (-1)^{m+i} \det(M_{mi}) \left(\frac{\partial f}{\partial x_i} + A_i \right).$$

From the proof of Lemma 3.3.3, we know that $\det(M_{mm})$ is nonzero everywhere on $U_{\mathbf{x}} \cap (C_L \setminus E_L)$. Therefore $\det(M_{mm})$ is invertible on some open neighborhood of $U_{\mathbf{x}} \cap (C_L \setminus E_L)$ inside $U_{\mathbf{x}}$. In this neighborhood, the vanishing locus of $\frac{\det(M)}{\det(M_{mm})}$ coincides with $V(\det(M))$. Write

$$\frac{\det(M)}{\det(M_{mm})} = \mathfrak{G}_{\mathbf{A}} + A_m, \quad (30)$$

where $\mathcal{G}_{\mathbf{A}}$ is a regular function with no A_m dependence. Then $V(\det(M))$ is singular at precisely those points where the determinant of the $m \times m$ -matrix

$$M' \stackrel{\text{def}}{=} \begin{pmatrix} \frac{\partial r_1}{\partial x_1} & \cdots & \frac{\partial r_1}{\partial x_m} \\ \vdots & \ddots & \vdots \\ \frac{\partial r_{m-1}}{\partial x_1} & \cdots & \frac{\partial r_{m-1}}{\partial x_m} \\ \frac{\partial \mathcal{G}_{\mathbf{A}}}{\partial x_1} & \cdots & \frac{\partial \mathcal{G}_{\mathbf{A}}}{\partial x_m} \end{pmatrix}$$

vanishes. The absence of A_m from $\det(M')$ means that the zeros of $\det(M')$ are defined over the subfield $L' \subset L$, whereas the zeros of (30) are defined over the subfield $\overline{\mathbb{F}_q(A_m)} \subset L$. Because zeros of (30) are not $\overline{\mathbb{F}_q} = L' \cap \overline{\mathbb{F}_q(A_m)}$ -rational, this completes the proof. \square

Proposition 4.3.2. The morphism $\Psi : C_L \rightarrow \mathbb{P}_L^1$ is ramified at some point in $C_L \setminus E_L$ in each of the following two cases:

- (i) $g > 0$;
- (ii) $\deg E > 1$.

Proof. The rational function $\mathcal{F}_{\mathbf{A}}$ on C_L determines a morphism $\mathcal{F}_{\mathbf{A}} : C_L \rightarrow \mathbb{P}_L^1$. By definition, Ψ and $\mathcal{F}_{\mathbf{A}}$ differ by the constant A_0 , and so it suffices to show that $\mathcal{F}_{\mathbf{A}}$ is ramified at some point of $C_L \setminus E_L$.

At each point $\mathfrak{p} \in C_L$, let $\text{ram}_{\mathfrak{p}}(\mathcal{F}_{\mathbf{A}})$ denote the ramification order of $\mathcal{F}_{\mathbf{A}}$ at \mathfrak{p} (the order of vanishing of the Kähler differential $d\mathcal{F}_{\mathbf{A}} \in \Omega_{C_L}^1$ at \mathfrak{p}). Define

$$\text{ram}_{C_L \setminus E_L}(\mathcal{F}_{\mathbf{A}}) \stackrel{\text{def}}{=} \sum_{\mathfrak{p} \in C_L \setminus E_L} \text{ram}_{\mathfrak{p}}(\mathcal{F}_{\mathbf{A}}) \quad \text{and} \quad \text{ram}_{E_L}(\mathcal{F}_{\mathbf{A}}) \stackrel{\text{def}}{=} \sum_{\mathfrak{p} \in \text{supp}(E_L)} \text{ram}_{\mathfrak{p}}(\mathcal{F}_{\mathbf{A}}).$$

Then $\text{ram}_{C_L}(\mathcal{F}_{\mathbf{A}}) = \text{ram}_{C_L \setminus E_L}(\mathcal{F}_{\mathbf{A}}) + \text{ram}_{E_L}(\mathcal{F}_{\mathbf{A}})$. Recall that $k = \deg(\text{div}(f)_-)$. Lemmas 3.3.1 and 3.3.3 imply that the morphism $\mathcal{F}_{\mathbf{A}} : C_L \rightarrow \mathbb{P}_L^1$ is finite and separable, so satisfies Riemann-Hurwitz [13, §IV, Corollary 2.4]. Since k is the degree of $\mathcal{F}_{\mathbf{A}}$, this gives

$$2(g + k - 1) = \text{ram}_{C_L \setminus E_L}(\mathcal{F}_{\mathbf{A}}) + \text{ram}_{E_L}(\mathcal{F}_{\mathbf{A}}).$$

Thus it suffices to show that

$$\text{ram}_{E_L}(\mathcal{F}_{\mathbf{A}}) < 2(g + k - 1). \tag{31}$$

Fix a point $\mathfrak{p} \in \text{supp}(E_L)$, and fix a uniformizing parameter z in the stalk $\mathcal{O}_{C_L, \mathfrak{p}}$. Let $m_{\mathfrak{p}}$ denote the order of E_L at \mathfrak{p} , and recall that $k_{\mathfrak{p}}$ denotes the degree of the pole of f at \mathfrak{p} . Because E is effective, our assumption (19) implies that $k_{\mathfrak{p}} \geq m_{\mathfrak{p}} > 0$. Because E is very ample, $H^0(C_L, \mathcal{O}(E_L))$ is basepoint free, and thus there exists some nontrivial \mathbb{F}_q -linear combination \tilde{A}_0 of the variables A_0, \dots, A_m so that we can write the rational function $\sum_{i=0}^m A_i f_i$ on C_L as

$$\sum_{i=0}^m A_i f_i\left(\frac{1}{z}\right) = \tilde{A}_0 + \mathcal{G}_{\mathbf{A}}\left(\frac{1}{z}\right),$$

where the order of the pole of $\mathcal{G}_{\mathbf{A}}\left(\frac{1}{z}\right)$ at \mathfrak{p} is between 1 and $m_{\mathfrak{p}}$. Write

$$\mathcal{F}_{\mathbf{A}} = \frac{1}{z^{k_{\mathfrak{p}}}} \left(\tilde{f}(z) + \tilde{A}_0 z^{k_{\mathfrak{p}}} + \tilde{\mathcal{G}}_{\mathbf{A}}(z) \right),$$

where $\tilde{f}(z)$ is an \mathbb{F}_q -rational function that does not vanish at $z = 0$, and where the order of vanishing of $\tilde{\mathcal{G}}_{\mathbf{A}}(z)$ at $z = 0$ is between $k_{\mathfrak{p}} - 1$ and $k_{\mathfrak{p}} - m_{\mathfrak{p}}$. Thus the order of vanishing of

$d(\frac{1}{\mathcal{F}_A})$ at $z = 0$ is equal to the order of vanishing of the function

$$k_p z^{k_p-1} (\tilde{f}(z) + \tilde{A}_0 z^{k_p} + \tilde{\mathcal{G}}_A(z)) + z^{k_p} \left(\frac{d\tilde{f}}{dz} + k_p \tilde{A}_0 z^{k_p-1} + \frac{d\tilde{\mathcal{G}}_A}{dz} \right)$$

at $z = 0$. This implies that:

- If $\text{char } \mathbb{F}_q$ does not divide k_p , then $\text{ram}_p(\mathcal{F}_A) = k_p - 1$;
- If $\text{char } \mathbb{F}_q$ divides k_p , then $\text{ram}_p(\mathcal{F}_A) \leq 2k_p - 2$.

Repeating this argument at all points p in $\text{supp}(E_L)$, we see that

$$\text{ram}_{E_L}(\mathcal{F}_A) \leq 2k - 2 \# \text{supp}(E_L).$$

Thus (31) is satisfied whenever $g > 0$ or $\text{deg } E > 1$. \square

Proposition 4.3.3. Assume that one of the following two conditions holds:

- (a) There exists a very ample effective divisor E_0 on C such that $E \geq 3E_0$;
- (b) There exists a very ample effective divisor E_0 on C such that $E \geq 2E_0$, $\text{char } \mathbb{F}_q = 2$, and $df|_{C \setminus E}$ vanishes at a nonempty finite set.

Then the morphism $\Psi : C_L \rightarrow \mathbb{P}_L^1$ separates critical points in $C_L \setminus E_L$, i.e., there do not exist distinct points $x, y \in C_L \setminus E_L$ satisfying the system of equations

$$\begin{aligned} d\Psi|_x &= 0 \\ d\Psi|_y &= 0 \\ \Psi(x) &= \Psi(y). \end{aligned} \tag{32}$$

Proof. It suffices to prove that the morphism $\mathcal{F}_A : C_L \rightarrow \mathbb{P}_L^1$ separates critical points. Assume that $E \geq nE_0$, with E_0 a very ample effective divisor on C_L , and with $n = 2$ or 3 . Let $m_0 = \dim H^0(C, \mathcal{O}(E_0)) - 1$. Interpret C as a closed subvariety of \mathbb{P}^{m_0} via the closed embedding provided by E_0 . The standard proof of Bertini's Theorem [13, §II.8, proof of Theorem 8.18] implies that for any two distinct points $x, y \in C_{\overline{\mathbb{F}}_q} \setminus E_{\overline{\mathbb{F}}_q}$, we can choose a linear form t on $\mathbb{P}_{\overline{\mathbb{F}}_q}^{m_0}$ whose restriction to $C_{\overline{\mathbb{F}}_q}$ provides local uniformizing parameters $t - t(x)$ at x and $t - t(y)$ at y . We can furthermore choose t so that it satisfies the generic condition

$$t(x) \neq t(y). \tag{33}$$

Since $t \in H^0(C_{\overline{\mathbb{F}}_q}, \mathcal{O}(E_{0, \overline{\mathbb{F}}_q}))$ and $E \geq nE_0$, we have $1, t, t^2, \dots, t^n \in H^0(C_{\overline{\mathbb{F}}_q}, \mathcal{O}(E_{\overline{\mathbb{F}}_q}))$. Choose a new basis $\{1, g_1, g_2, \dots, g_m\}$ of $H^0(C_{\overline{\mathbb{F}}_q}, \mathcal{O}(E_{\overline{\mathbb{F}}_q}))$ such that $g_i = t^i$ for $0 \leq i \leq n$. Let $\{B_0, B_1, B_2, \dots\}$ denote linear generators of $\overline{\mathbb{F}}_q[\mathbf{A}]$ in this new basis, with $B_0 = A_0$. Then

$$\mathcal{F}_A = f + A_0 + B_1 t + B_2 t^2 + \dots + B_n t^n + \mathcal{G}_A, \tag{34}$$

where $\mathcal{G}_A = \sum_{i=n+1}^m B_i g_i$. Define

$$\Phi \stackrel{\text{def}}{=} \mathcal{F}_A - B_1 t - B_2 t^2.$$

Again by the dimension counts in [13, §II.8, proof of Theorem 8.18], we can fix a Zariski open neighborhood $U \subset C_{\overline{\mathbb{F}}_q} \setminus E_{\overline{\mathbb{F}}_q}$ containing both x and y , such that the restriction of t to $C_{\overline{\mathbb{F}}_q} \setminus E_{\overline{\mathbb{F}}_q}$ provides a uniformizing parameter $t - t(u)$ at every point $u \in U$. Define

$$U_{xy} \stackrel{\text{def}}{=} (U \times_{\overline{\mathbb{F}}_q} U) \setminus \{\text{diagonal in } C_{\overline{\mathbb{F}}_q} \times C_{\overline{\mathbb{F}}_q}\}.$$

At each L -valued point (u, v) in U_{xy} , the system of equations (32) holds for the function \mathcal{F}_A if and only if (u, v) satisfies the single $\overline{\mathbb{F}}_q$ -valued matrix equation

$$\begin{pmatrix} 1 & 2t(u) \\ 1 & 2t(v) \\ t(v) - t(u) & t(v)^2 - t(u)^2 \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \end{pmatrix} = \begin{pmatrix} -\frac{d\Phi}{dt}(u) \\ -\frac{d\Phi}{dt}(v) \\ \Phi(u) - \Phi(v) \end{pmatrix}, \quad (35)$$

where $\frac{d\Phi}{dt}$ denotes the regular function on U such that $d\Phi = \frac{d\Phi}{dt} dt$ as a global section of Ω_U^1 . Define functions φ on U and c on U_{xy} according to

$$\varphi \stackrel{\text{def}}{=} -\frac{d\Phi}{dt} \quad \text{and} \quad c(u, v) \stackrel{\text{def}}{=} \Phi(u) - \Phi(v).$$

By (33), the 3×2 -matrix at left in (35) has rank 2 everywhere in U_{xy} . Hence (35) holds at (u, v) if and only if (u, v) satisfies the single determinant equation

$$\det \begin{pmatrix} 1 & 2t(u) & \varphi(u) \\ 1 & 2t(v) & \varphi(v) \\ t(v) - t(u) & t(v)^2 - t(u)^2 & c(u, v) \end{pmatrix} = 0. \quad (36)$$

Interpret (36) as an equation over $\overline{\mathbb{F}}_q$ in the variables u, v, A_1, \dots, A_m . Let $T \subset \mathbb{A}_{\overline{\mathbb{F}}_q}^m \times_{\overline{\mathbb{F}}_q} U_{xy}$ denote the subscheme cut out by this equation, with projections

$$\mathbb{A}_{\overline{\mathbb{F}}_q}^m \xleftarrow{\text{Pr}_1} T \xrightarrow{\text{Pr}_2} U_{xy}.$$

Letting η denote the generic point of $\mathbb{A}_{\overline{\mathbb{F}}_q}^m$, it suffices to prove that the fiber $\text{pr}_1^{-1}(\eta) \subset T$ is empty. Because the leftmost matrix in (35) has rank 2, each fiber of pr_2 in T is at most $(m-2)$ -dimensional. The generic fiber $\text{pr}_1^{-1}(\eta)$ of T is cut out by a single equation in the 2-dimensional space $(U_{xy})_{\overline{\mathbb{F}}_q(\mathbf{A})}$. Thus if the determinant in (36) is not constantly equal to 0, we have

$$\dim T \leq 1 + m - 2 < m,$$

which implies that the image $\text{pr}_1(T) \subset \mathbb{A}_{\overline{\mathbb{F}}_q}^m$ cannot contain the generic point of $\mathbb{A}_{\overline{\mathbb{F}}_q}^m$. In order to show that (36) has no solutions in U_{xy} , it thus remains to show that the determinant appearing in (36) is not constantly equal to 0.

Let $d(u, v)$ be the determinant that appears in (36). A straightforward calculation gives

$$d(u, v) = (t(v) - t(u)) \left(2c(u, v) + (t(v) - t(u)) (\varphi(u) + \varphi(v)) \right).$$

If $n \geq 3$, then the coefficient of B_3 in $2c(u, v) + (t(v) - t(u)) (\varphi(u) + \varphi(v))$ is

$$2(t(u)^3 - t(v)^3) + 3(t(v)^2 - t(u)^2).$$

By (33), this last expression is nonzero in any characteristic. If $n = 2$ and $\text{char } \mathbb{F}_q = 2$, then

$$d(u, v) = (t(v) - t(u))^2 (\varphi(u) + \varphi(v)).$$

If df is nonconstant in this case, then $\varphi(u) + \varphi(v) = \varphi(u) - \varphi(v)$ is not constantly zero.

Because the Zariski open subsets U_{xy} cover $(C_{\overline{\mathbb{F}}_q} \times C_{\overline{\mathbb{F}}_q}) \setminus \{\text{diagonal}\}$ as (x, y) varies inside $(C_{\overline{\mathbb{F}}_q} \times C_{\overline{\mathbb{F}}_q}) \setminus \{\text{diagonal}\}$, this completes the proof. \square

Corollary 4.3.4. Assume that one of the following two conditions holds:

- (a) There exists a very ample effective divisor E_0 on C such that $E \geq 3E_0$;

- (b) There exists a very ample effective divisor E_0 on C such that $E \geq 2E_0$, $\text{char } \mathbb{F}_q = 2$, and $df|_{C \setminus E}$ vanishes on a nonempty finite set.

Then the subgroup $\text{Gal}(\mathcal{F}_{\mathbf{A}}/\overline{\mathbb{F}_q}(\mathbf{A})) \subset S_k$ contains a transposition.

Proof. If $g = 0$, then each of the conditions (a) and (b) implies condition (ii) of Proposition 4.3.2. Thus for any g , the morphism Ψ is ramified at some closed point of $C_L \setminus E_L$. Let α be such a point, which is to say that the morphism $\Psi : C_L \setminus E_L \rightarrow \mathbb{A}_L^1$ is ramified at α . Proposition 4.3.1 says that the order of ramification at any point in $C_L \setminus E_L$ is at most 1. Thus the factorization type of the fiber of Ψ containing α is $(2, 1, \dots, 1)$. As Proposition 4.3.3 says that the critical values of Ψ are distinct, this implies that $\Psi(\mathbf{x}) = \Psi(\alpha)$ has at least $k - 1$ solutions. However, since α is a ramification point, the fiber over $\Psi(\alpha)$ has exactly one double point. Hence the inertia group over $\Psi(\alpha)$ permutes two factors of $\mathcal{F}_{\mathbf{A}} = \Psi(\mathbf{x}) + A_0$ and fixes all others. Thus $\text{Gal}(\mathcal{F}_{\mathbf{A}}/\overline{\mathbb{F}_q}(\mathbf{A}))$ contains a transposition. \square

Completion of the proof of Theorem 4.1.1. By Remark 4.2.2, if either of the conditions (a) or (b) holds, then Proposition 4.2.1 holds and $\text{Gal}(\mathcal{F}_{\mathbf{A}}/\overline{\mathbb{F}_q}(\mathbf{A}))$ is doubly transitive. By Corollary 4.3.4, $\text{Gal}(\mathcal{F}_{\mathbf{A}}/\overline{\mathbb{F}_q}(\mathbf{A}))$ contains a transposition. By Lemma 4.1.3, we have $\text{Gal}(\mathcal{F}_{\mathbf{A}}/\overline{\mathbb{F}_q}(\mathbf{A})) \cong S_k$. \square

5. PROOF OF THEOREM A

We now use the Galois group calculation in §4 to prove Theorem A.

5.1. Setup for the proof of Theorem A. Let $\mathcal{F}_{\mathbf{A}} \in R[\mathbf{A}]$ be the element defined in (17), and let $\text{pr}_1 : V(\mathcal{F}_{\mathbf{A}}) \rightarrow \mathbb{A}^{m+1}$ denote the resulting projection. For each \mathbb{F}_q -rational point $\mathbf{a} \in \mathbb{A}^{m+1}$, let $\mathcal{F}_{\mathbf{a}}$ denote the restriction of $\mathcal{F}_{\mathbf{A}}$ to $R \cong \kappa(\mathbf{a}) \otimes_{\mathbb{F}_q[\mathbf{A}]} R[\mathbf{A}]$.

Proposition 5.1.1. Let E and f be as in the statement of Theorem 4.1.1, and let $Z \subset \mathbb{A}_{\mathbb{F}_q}^{m+1}$ denote the branch locus of $\text{pr}_1 : V(\mathcal{F}_{\mathbf{A}}) \rightarrow \mathbb{A}^{m+1}$. Then Z is pure of codimension 1 in \mathbb{A}^{m+1} , and it satisfies the inequality

$$\deg Z \leq g - 2 + 2k, \quad (37)$$

where g denotes the genus of C .

Proof. Define $V \stackrel{\text{def}}{=} H^0(C, \mathcal{O}(\text{div}(f)_-))^*$, the \mathbb{F}_q -vector space dual of the space of rational functions $H^0(C, \mathcal{O}(\text{div}(f)_-))$, and consider the pair of dual projective spaces

$$\mathbb{P}(V) \stackrel{\text{def}}{=} \text{Proj Sym}_{\mathbb{F}_q}^{\bullet} V^* \quad \text{and} \quad \mathbb{P}(V^*) \stackrel{\text{def}}{=} \text{Proj Sym}_{\mathbb{F}_q}^{\bullet} V,$$

where $\text{Sym}_{\mathbb{F}_q}^{\bullet} V^*$ and $\text{Sym}_{\mathbb{F}_q}^{\bullet} V$ denote the graded symmetric \mathbb{F}_q -algebras on V^* and V , respectively. Because E is a very ample effective divisor, the inequalities (19) imply that $\text{div}(f)_-$ is very ample and effective. Identify C with its image under the closed embedding

$$C \hookrightarrow \mathbb{P}(V) \quad (38)$$

induced by $\text{div}(f)_-$. Pass to the algebraic closure $\overline{\mathbb{F}_q}$ to obtain a smooth, closed, irreducible subvariety $C_{\overline{\mathbb{F}_q}} \subset \mathbb{P}(V_{\overline{\mathbb{F}_q}})$. By [17, §3.1.3 & §5.1], this subvariety determines a dual variety $C_{\overline{\mathbb{F}_q}}^{\vee} \subset \mathbb{P}(V_{\overline{\mathbb{F}_q}}^*)$.

We claim that $C_{\overline{\mathbb{F}_q}}^{\vee}$ is a hypersurface in $\mathbb{P}(V_{\overline{\mathbb{F}_q}}^*)$. To see this, let \mathcal{N} denote the conormal sheaf on $C_{\overline{\mathbb{F}_q}}$ in $\mathbb{P}(V)$, and let $\mathbb{P}(\mathcal{N})$ denote its associated projective scheme over $C_{\overline{\mathbb{F}_q}}$, which comes with a projection

$$\mathbb{P}(\mathcal{N}) \twoheadrightarrow \mathbb{P}(V_{\overline{\mathbb{F}_q}}^*) \quad (39)$$

(see [17, §3.1] for details). Note that $\dim \mathbb{P}(\mathcal{N}) = \dim \mathbb{P}(V_{\overline{\mathbb{F}_q}}) - 1$. By [17, Proposition 3.5], if the projection (39) is *not* everywhere ramified, then the projection (39) induces a birational

morphism $\mathbb{P}(\mathcal{N}) \dashrightarrow C_{\overline{\mathbb{F}}_q}^\vee$. Thus $C_{\overline{\mathbb{F}}_q}^\vee$ is a hypersurface as soon as (39) is not everywhere ramified. By [17, Proposition 3.3], exhibiting a point of $\mathbb{P}(\mathcal{N})$ where (39) is unramified reduces to exhibiting a hyperplane $H \subset \mathbb{P}(V_{\overline{\mathbb{F}}_q})$ and a point x_0 of the scheme-theoretic intersection $C_{\overline{\mathbb{F}}_q}^\vee \cap H$ such that x_0 is a *non-degenerate* (or *ordinary*) *quadratic singularity* of $C_{\overline{\mathbb{F}}_q}^\vee \cap H$ (see [17, §1.1] for details). When $C_{\overline{\mathbb{F}}_q}^\vee \cap H$ is 0-dimensional, as it is in our case, the condition that a point x_0 in $C_{\overline{\mathbb{F}}_q}^\vee \cap H$ be a non-degenerate quadratic singularity reduces to the condition that the component of $C_{\overline{\mathbb{F}}_q}^\vee \cap H$ containing x_0 is isomorphic to $\text{Spec } \overline{\mathbb{F}}_q[t]/(t^2)$. Our ability to find a hyperplane $H \subset \mathbb{P}(V_{\overline{\mathbb{F}}_q})$ and point $x_0 \in C_{\overline{\mathbb{F}}_q}^\vee \cap H$ satisfying this condition follows from the decomposition (34) of \mathcal{F}_A provided in the proof of Proposition 4.3.3. Indeed, choose values $a_0, b_1 \in \overline{\mathbb{F}}_q$, for A_0 and B_1 in (34), so that $f + a_0 + b_1 t + \mathfrak{G}_A$ vanishes to order ≥ 2 at a fixed $\overline{\mathbb{F}}_q$ -valued point x_0 in $C_{\overline{\mathbb{F}}_q}^\vee$, and then choose the value $b_2 = 1$ for B_2 .

Thus $C_{\overline{\mathbb{F}}_q}^\vee \subset \mathbb{P}(V)$ is a hypersurface, and the hypotheses of [17, §5.2] hold. By [17, Proposition 5.7.2], we then have

$$\deg C_{\overline{\mathbb{F}}_q}^\vee = g - 2 + 2k. \quad (40)$$

Our parameter space $\mathbb{A}_{\overline{\mathbb{F}}_q}^{m+1}$ admits a natural identification with a distinguished affine open chart inside a linear subspace $L \subset \mathbb{P}(V^*)$. Because the hyperplane $H_{\mathbf{a}}$ associated to a point $\mathbf{a} \in \mathbb{A}^{m+1}$ does not intersect $C_{\overline{\mathbb{F}}_q}^\vee$ at $\text{supp } E$, the morphism $V(\mathcal{F}_A)_{\overline{\mathbb{F}}_q} \dashrightarrow \mathbb{A}_{\overline{\mathbb{F}}_q}^{m+1}$ is ramified over $\mathbf{a} \in \mathbb{A}_{\overline{\mathbb{F}}_q}^{m+1}$ if and only if $\mathbf{a} \in C_{\overline{\mathbb{F}}_q}^\vee \cap L$ [17, §3.1.3] [11, §17.13.7 & Proposition 17.13.2]. By Lemma 3.3.3, $V(\mathcal{F}_A)$ is generically unramified over $\mathbb{A}_{\overline{\mathbb{F}}_q}^{m+1}$, thus the scheme-theoretic intersection $C_{\overline{\mathbb{F}}_q}^\vee \cap L$ has dimension strictly less than $\dim L$, which is to say that the intersection is proper [6, Definition 7.1]. Thus $C_{\overline{\mathbb{F}}_q}^\vee \cdot L$ is pure of codimension 1 in L , and Bézout's Theorem in $\mathbb{P}(V_{\overline{\mathbb{F}}_q}^*)$ [6, Proposition 8.4] combined with (40) implies that

$$\deg C_{\overline{\mathbb{F}}_q}^\vee \cdot L = g - 2 + 2k.$$

Because $Z_{\overline{\mathbb{F}}_q} = C_{\overline{\mathbb{F}}_q}^\vee \cap \mathbb{A}_{\overline{\mathbb{F}}_q}^{m+1} \subset C_{\overline{\mathbb{F}}_q}^\vee \cap L$, with $\deg Z = \deg Z_{\overline{\mathbb{F}}_q}$, the formula (37) follows. \square

Remark 5.1.2. Suppose that \mathbf{a} is an \mathbb{F}_q -rational point in \mathbb{A}^{m+1} such that $R/(\mathcal{F}_{\mathbf{a}})$ is a separable \mathbb{F}_q -algebra. Then since R is a Dedekind domain, the ideal $(\mathcal{F}_{\mathbf{a}})$ can be written uniquely as

$$(\mathcal{F}_{\mathbf{a}}) = \mathfrak{f}_1 \cdots \mathfrak{f}_\ell,$$

where the \mathfrak{f}_i are distinct prime ideals in R , with each $k(\mathfrak{f}_i) = R/(\mathfrak{f}_i)$ a separable extension of \mathbb{F}_q . Note that in this case, we have

$$k = \deg \mathfrak{f}_1 + \cdots + \deg \mathfrak{f}_\ell. \quad (41)$$

Definition 5.1.3. If \mathbf{a} is an \mathbb{F}_q -rational point in \mathbb{A}^{m+1} , then the *factorization type* $\lambda_{\mathbf{a}}$ is the partition of k given in (41).

The *factorization type counting function* for a fixed partition λ of k is the assignment $\pi_C(-; \lambda)$ taking the short interval $I(f, E)$ to the value

$$\pi_C(I(f, E); \lambda) \stackrel{\text{def}}{=} \#\{\mathbf{a} \in \mathbb{A}^{m+1}(\mathbb{F}_q) : R/(\mathcal{F}_{\mathbf{a}}) \text{ is separable and } \lambda_{\mathbf{a}} = \lambda\}.$$

Definition 5.1.4. Given a permutation $\sigma \in S_k$, its *partition type*, denoted λ_σ , is the partition of k determined by the cycle decomposition of σ . For an arbitrary partition λ of k , we define

$$P(\lambda) \stackrel{\text{def}}{=} \frac{\#\{\sigma \in S_k \mid \lambda_\sigma = \lambda\}}{k!}. \quad (42)$$

In other words, $P(\lambda)$ is the probability that a given permutation in S_k has partition type λ .

5.2. Proof of the main theorem. We begin by proving a general theorem that provides an estimate for the number of \mathbb{F}_q -rational substitutions in the variables A_0, \dots, A_1 for which the regular function $f + A_0 + A_1 f_1 + \dots + A_m f_m$ on $C \setminus E$ factors according to a given partition of k . The formulation of this theorem, as well as its proof, is very much in the spirit of [2, Proposition 3.1].

Theorem 5.2.1. Let C be a smooth projective geometrically irreducible curve over \mathbb{F}_q of arithmetic genus g . Fix a positive integer k . Then there exists a constant $c(k, g) > 0$, depending only on k and g , such that for any datum consisting of

- (i) a partition λ of k ;
- (ii) a prime number p and a power $q = p^e$;
- (iii) an effective divisor E on C and a regular function f on $C \setminus E$ satisfying

$$E < \operatorname{div}(f)_- \quad \text{and} \quad k \stackrel{\text{def}}{=} \deg \operatorname{div}(f)_-, \quad (43)$$

such that p , E , and f satisfy either of the following conditions:

- (a) There exists a very ample effective divisor E_0 on C with $\deg E_0 \geq 2g + 1$ such that $E \geq 3E_0$;
- (b) There exists a very ample effective divisor E_0 on C with $\deg E_0 \geq 2g + 1$ such that $E \geq 2E_0$, $p = 2$, and $df|_{C \setminus E}$ vanishes on a nonempty finite set,

we have

$$\left| \pi_C(I(f, E); \lambda) - P(\lambda) q^{m+1} \right| \leq c(m, k) q^{m+\frac{1}{2}}, \quad (44)$$

where $m \stackrel{\text{def}}{=} \deg(E) - g$.

Proof of Theorem 5.2.1. By Theorem 4.1.1, we have that $\operatorname{Gal}(\mathcal{F}_{\mathbf{A}}, \overline{\mathbb{F}}_q(\mathbf{A})) = S_k$. Note also that by the Riemann-Roch Theorem, the requirement that $\deg E_0 \geq 2g + 1$ in (a) and (b) implies that

$$\dim H^0(C, \mathcal{O}(E)) = \deg(E) - g + 1 = m + 1.$$

Let Z be the branch locus of the morphism $V(\mathcal{F}_{\mathbf{A}}) \rightarrow \mathbb{A}^{m+1}$ as in Proposition 3.3.6. By Proposition 5.1.1, we have $\deg Z \leq g - 2 + 2k$. This provides a bound on both the number of irreducible components of Z and on the degree of each of these irreducible components. Applying Lang-Weil [21, Theorem 1], we obtain a constant $c_1(k, g)$, depending only on k and g , such that

$$\#Z(\mathbb{F}_q) \leq c_1(k, g) q^m. \quad (45)$$

Consider the \mathbb{F}_q -varieties $Y \stackrel{\text{def}}{=} V(\mathcal{F}_{\mathbf{A}})_{\mathbb{A}^{m+1} \setminus Z}$ and $X \stackrel{\text{def}}{=} \mathbb{A}^{m+1} \setminus Z$. By Proposition 3.3.6, the morphism $\rho := \operatorname{pr}_1|_Y : Y \rightarrow X$ is finite étale of degree k . By the theorem of the primitive element, we can construct the normal closure of the separable extension $\kappa(\mathcal{F}_{\mathbf{A}})/\mathbb{F}_q(A_0, \dots, A_m)$ as the splitting field of some degree- k polynomial over $\mathbb{F}_q(A_0, \dots, A_m)$. The Galois closure W of Y over X (see [30, Proposition 5.3.9]) is isomorphic to the integral closure of the coordinate ring of X in this splitting field, and therefore the Galois group $\operatorname{Aut}_X W$ is degree k .

Observe that the closed embedding $C \hookrightarrow \mathbb{P}^m$ realizes $V(\mathcal{F}_{\mathbf{A}})$ as a hypersurface of degree k inside the affine open subscheme $\mathbb{A}_{\mathbb{F}_q}^{2m+1} \subset \mathbb{A}_{\mathbb{F}_q}^{m+1} \times_{\mathbb{F}_q} \mathbb{P}_{\mathbb{F}_q}^m$. Because we can construct W as a connected component of the k -fold fiber product $Y \times_X \dots \times_X Y$ [30, Proof of Proposition 5.3.9], we can realize W as a locally closed subspace of \mathbb{A}^{km+k+1} , whose closure is a hypersurface of degree $\leq k^k$. Thus we obtain a bound, depending only on k , on the degree of the closure of W inside an affine space.

The morphism $W \rightarrow X$ defines a *geometric embedding problem*, in the sense of [3, §2.1]. In [2, Proposition 3.1], Bary-Soroker, Rosenzweig, and the first author construct a *geometric embedding problem associated to a polynomial* $\mathcal{F} \in \mathbb{F}_q[\mathbf{A}, t]$, in the sense of [3, §2.1, p. 859]. However,

the last two paragraphs of [2, proof of Proposition 3.1] make no special use of the fact that the geometric embedding is associated to a polynomial. The construction depends only on the following facts:

- the degree of the Galois group of the geometric embedding problem is k ,
- W is a dense open subset of a hypersurface of degree bound by a function of k inside some affine space,
- the point count in the branch locus $Z \subset \mathbb{A}_{\mathbb{F}_q}^{m+1}$ has upper bound (45).

The proof can now proceed exactly as in the last two paragraphs of [2, proof of Proposition 3.1] upon replacing V in that proof with our variety X , and noting that (ii) above lets us replace the constant $c_2(m, B)$ appearing in [2, proof of Proposition 3.1] with a constant depending only on k , as in [2, proof of Theorem 2.3]. Thus we obtain a constant $c(k, g)$, depending only on k and g , such that

$$\left| \pi_C(I(f, E); \lambda) - P(\lambda)q^{m+1} \right| \leq c(k, g) q^{m+\frac{1}{2}}, \quad (46)$$

as desired. \square

Proof of Theorem A. Use the Young diagram $\square \cdots \square$ to denote the trivial partition of k consisting of a single set. For this partition, we have

$$P(\square \cdots \square) = \frac{1}{k}$$

and $\pi_C(I(f, E); \square \cdots \square) = \pi_C(I(f, E))$. Because the two possible conditions on E in the statement of Theorem A imply conditions (iii.a) and (iii.b) of Theorem 5.2.1, the inequality (44) in Theorem 5.2.1 becomes the inequality

$$\left| \pi_C(I(f, E)) - \frac{q^{m+1}}{k} \right| \leq c(k, g) q^{m+\frac{1}{2}} \quad (47)$$

estimating the number of elements in the short interval $I(f, E)$ with principal divisor irreducible away from E . As $I(f, E) = f + H^0(C, \mathcal{O}(E))$ with $\dim H^0(C, \mathcal{O}(E)) = m + 1$, the asymptotic formula (14) follows immediately from (47).

The statement of uniformity in Theorem A, i.e., the statement that the implied constant in the error term $O(q^{-1/2})$ depends only on k and g , follows from the fact that the constant $c(k, g)$ in Theorem 5.2.1 depends only on k and g . \square

REFERENCES

- [1] Antal Balog and Ken Ono. The Chebotarev density theorem in short intervals and some questions of Serre. *J. Number Theory*, 91(2):356–371, 2001. [1.3](#)
- [2] Efrat Bank, Lior Bary-Soroker, and Lior Rosenzweig. Prime polynomials in short intervals and in arithmetic progressions. *Duke Math. J.*, 164(2):277–295, 2015. [1](#), [1.2](#), [1.2.3](#), [1.5](#), [5.2](#), [5.2](#)
- [3] Lior Bary-Soroker. Irreducible values of polynomials. *Adv. Math.*, 229(2):854–874, 2012. [1.5](#), [5.2](#)
- [4] Stephen D. Cohen. Uniform distribution of polynomials over finite fields. *J. London Math. Soc. (2)*, 6:93–102, 1972. [1.2](#)
- [5] Eberhard Freitag and Reinhardt Kiehl. *Étale cohomology and the Weil conjecture*, volume 13 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1988. Translated from the German by Betty S. Waterhouse and William C. Waterhouse, With an historical introduction by J. A. Dieudonné. [1.6](#), [3.3](#)
- [6] William Fulton. *Intersection theory*, volume 2 of *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]*. Springer-Verlag, Berlin, second edition, 1998. [5.1](#)
- [7] Andrew Granville. Unexpected irregularities in the distribution of prime numbers. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994)*, pages 388–399. Birkhäuser, Basel, 1995. [1.1](#)
- [8] Andrew Granville. Different approaches to the distribution of primes. *Milan J. Math.*, 78(1):65–84, 2010. [1.1](#)

- [9] L. Grenié, G. Molteni, and A. Perelli. Primes and prime ideals in short intervals. *ArXiv e-prints*, February 2016. [1.3](#)
- [10] A. Grothendieck. Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. II. *Inst. Hautes Études Sci. Publ. Math.*, (17):91, 1963. [3.3](#)
- [11] A. Grothendieck. Éléments de géométrie algébrique. IV. étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math.*, (32):361, 1967. [5.1](#)
- [12] Günter Harder. *Lectures on algebraic geometry II*. Aspects of Mathematics, E39. Vieweg + Teubner, Wiesbaden, 2011. Basic concepts, coherent cohomology, curves and their Jacobians. [2.1.2](#)
- [13] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. [2.1](#), [4.3](#), [4.3](#), [4.3](#)
- [14] D. R. Heath-Brown. On the density of the zeros of the Dedekind zeta-function. *Acta Arith.*, 33(2):169–181, 1977. [1.3](#)
- [15] D. R. Heath-Brown. The number of primes in a short interval. *J. Reine Angew. Math.*, 389:22–63, 1988. [1.1](#)
- [16] M. N. Huxley. On the difference between consecutive primes. *Invent. Math.*, 15:164–170, 1972. [1.1](#)
- [17] N.M. Katz. Pinceaux de Lefschetz: Théoreme d’existence. Sem. Geom. algebrique Bois-Marie 1967-1969, SGA 7 II, Lect. Notes Math. 340, Expose XVII, 212-253 (1973), 1973. [5.1](#), [5.1](#), [5.1](#)
- [18] Jonathan P. Keating and Zeev Rudnick. The variance of the number of prime polynomials in short intervals and in residue classes. *Int. Math. Res. Not. IMRN*, (1):259–288, 2014. [1.2](#)
- [19] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977. [1.3](#)
- [20] Edmund Landau. Ueber die zu einem algebraischen Zahlkörper gehörige Zetafunktion und die Ausdehnung der Tschebyscheffschen Primzahlentheorie auf das Problem der Vertheilung der Primideale. *J. Reine Angew. Math.*, 125:64–188, 1903. [1.3](#)
- [21] Serge Lang and André Weil. Number of points of varieties in finite fields. *Amer. J. Math.*, 76:819–827, 1954. [1.5](#), [5.2](#)
- [22] Helmut Maier. Primes in short intervals. *Michigan Math. J.*, 32(2):221–225, 1985. [1.1](#)
- [23] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980. [3.3](#)
- [24] Takayoshi Mitsui. On the prime ideal theorem. *J. Math. Soc. Japan*, 20(1-2):233–247, 04 1968. [1.3](#)
- [25] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004. [1.3](#)
- [26] Steven Roman. *Field theory*, volume 158 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2006. [3](#)
- [27] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002. [1.4](#)
- [28] Jean-Pierre Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, second edition, 2008. With notes by Henri Darmon. [4.1.3](#)
- [29] The Stacks Project Authors. *Stacks Project*. <http://stacks.math.columbia.edu>, 2018. [3.3](#)
- [30] Tamás Szamuely. *Galois groups and fundamental groups*, volume 117 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2009. [3.2.2](#), [5.2](#)

Efrat Bank

UNIVERSITY OF MICHIGAN MATHEMATICS DEPARTMENT
 530 CHURCH STREET
 ANN ARBOR, MI 48109-1043
 UNITED STATES
E-mail address: ebank@umich.edu

Tyler Foster

MAX PLANCK INSTITUTE FOR MATHEMATICS
 VIVATSGASSE 7
 53111 BONN
 GERMANY
E-mail address: foster@mpim-bonn.mpg.de