Finite Fields and Their Applications 67 (2020) 101713

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Artin's primitive root conjecture for function fields revisited

Seoyoung Kim [*,1], M. Ram Murty [2]

Department of Mathematics and Statistics, Queen's University, Kingston, ON, K7L 3N6 Canada

ARTICLE INFO

Article history:
Received 14 March 2020
Received in revised form 21 June 2020
Accepted 30 June 2020
Available online xxxx
Communicated by Stephen D. Cohen

MSC:
11R58
11M41

Keywords:
Artin's conjecture
Function fields
Finite fields

ABSTRACT

Artin's primitive root conjecture for function fields was proved by Bilharz in his thesis in 1937, conditionally on the proof of the Riemann hypothesis for function fields over finite fields, which was proved later by Weil in 1948. In this paper, we provide a simple proof of Artin's primitive root conjecture for function fields which does not use the Riemann hypothesis for function fields but rather modifies the classical argument of Hadamard and de la Vallée Poussin in their 1896 proof of the prime number theorem.

1. Introduction

In a private conversation with Helmut Hasse on September 12, 1927, Emil Artin described his (now famous) conjecture regarding primitive roots. For any natural number

* Corresponding author.
E-mail addresses: sk206@queensu.ca (S. Kim), murty@mast.queensu.ca (M. Ram Murty).
[1] Research of the first author partially supported by a Coleman Postdoctoral Fellowship.
[2] Research of the second author partially supported by NSERC Discovery grant.

https://doi.org/10.1016/j.ffa.2020.101713
1071-5797/

$a > 1$, which is not a perfect square, Artin conjectured that there are infinitely many primes p for which a is a primitive root $\pmod p$. This conjecture is still open though substantial progress has been made since the time of Artin. For instance, assuming the generalized Riemann hypothesis for Dedekind zeta functions of Kummer fields, Hooley [8] established the conjecture in 1967 and even derived an asymptotic formula for the number of such primes $p \leq x$. In 1984, Gupta and Murty [6] showed the existence of a set of 13 numbers for which Artin's conjecture is true for at least one of them. More precisely, let a, b, c be three prime numbers, then at least one of the following 13 numbers

$$\{ac^2, a^3b^2, a^2b, b^3c, b^2c, a^2c^3, ab^3, a^3bc^2, bc^3, a^2b^3c, a^3c, ab^2c^3, abc\} \tag{1.1}$$

is a primitive root modulo p for infinitely many primes p. This was later refined by Heath-Brown [7] to a set of three mutually coprime numbers greater than one. A readable survey of this problem can be found in [13].

By contrast, the function field analogue of Artin's conjecture is known, but it has a curious history. Hasse assigned the classical Artin conjecture as a doctoral thesis problem to his student Bilharz in 1933. Shortly after Bilharz began working on it, Erdös announced that he had solved the problem assuming the generalized Riemann hypothesis for certain Dedekind zeta functions. Though there was no formal paper written by Erdös, this seems to have completely disillusioned Bilharz so much, that Hasse felt compelled to write to Erdös on April 5, 1935 that "in case you have already dealt with this problem, I obviously have to find as quickly as possible a new PhD subject for Mr. Bilharz, who is working on this topic for a year." This seems to be the genesis of the Artin primitive root conjecture for function fields. The details can be found in the appendix of [3, Appendix 2].

Bilharz's thesis and paper [1] were conditional and assumed the analog of the Riemann hypothesis for zeta functions of function fields over finite fields. An accurate exposition of Bilharz's paper in the English language can be found in [17, Chapter 10]. The Riemann hypothesis for congruence zeta functions was proved much later by Weil [20] in 1948, though Weil seems to have made a preliminary announcement in 1945. An excellent historical account is available in [16].

The first person, to have observed that the full strength of the Riemann hypothesis is not essential to solve the function field version of Artin's conjecture but rather that a "quasi"-generalized Riemann hypothesis is sufficient, seems to be Davenport [4]. Indeed, in [4], he shows, among other results, that if χ is a nontrivial multiplicative character of the finite field $\mathbb{F}_q$, and $f(x)$ is an irreducible polynomial of degree k, then

$$\sum_{x \in \mathbb{F}_q} \chi(f(x)) = \mathcal{O}\left(q^{1-\frac{3}{2(k+4)}}\right) \tag{1.2}$$

for $k \geq 4$. He obtains slightly better results for $k \leq 3$, and remarks that this can be used to give a proof of Artin's conjecture for function fields over finite fields (see page 102 of [4]), but he gives no further details.

Davenport's estimates like (1.2) are quite impressive since they use only the elementary theory of finite fields and Cauchy's inequality! They seem to comprise a forgotten chapter of mathematics having been superceded by Weil's theory embracing the algebraic-geometric point of view. Now, after almost a century, we have an "elementary" proof of the Riemann hypothesis for curves. Building on the works of Stepanov [19], Schmidt [18], and later Bombieri [2], we have simpler proof of the Riemann hypothesis for curves using a very minimal amount of algebraic geometry in the form of the Riemann-Roch theorem.

The purpose of this paper is to show that the Riemann hypothesis for congruence zeta functions is not needed at all (nor a "quasi" Riemann hypothesis) to resolve Artin's conjecture for function fields over finite fields. In fact, all that is needed is the analog of the zero-free region obtained by de la Vallée Poussin and Hadamard in their proof of the prime number theorem proved in 1896.

2. Preliminaries

Our strategy of proof is inspired by Jensen and Murty [10]. We will combine this with the perspective of Davenport [4]. Throughout the paper, we denote

$$\sum{}' \quad \text{and} \quad \prod{}'$$

to indicate that the sum or product is taken over monic polynomials.

Davenport [4] considers the finite field $\mathbb{F}_q$ along with distinct irreducible monic polynomials

$$f_1(x), f_2(x), \dots, f_r(x)$$

with degrees $k_1, k_2, \dots, k_r$ respectively. We set

$$K = k_1 + k_2 + \cdots + k_r.$$

If we denote by $\mathcal{X} = (\chi_1, \chi_2, \dots, \chi_r)$ an r-tuple of multiplicative characters in $\mathbb{F}_q$, and $\mathcal{F} = (f_1, f_2, \dots, f_r)$ the r-tuple of given irreducible monic polynomials, define the character sum

$$S(\mathcal{F}, \mathcal{X}) = \sum_{x \in \mathbb{F}_q} \chi_1(f_1(x)) \ \cdots \ \chi_r(f_r(x)), \tag{2.1}$$

as in [4]. With any such character sum, we can associate an L-function $L(f, X, s)$ as follows: for any polynomial $g \in \mathbb{F}_q[x]$, we define the *resultant*

$$(f, g) = \prod_{\theta} f(\theta), \tag{2.2}$$

where the product is over the zeros of g in $\overline{\mathbb{F}}_q$. Using the resultant, we define a multiplicative character X in $\mathbb{F}_q[x]$ by

$$X(g) = \chi_1((f_1, g))\chi_2((f_2, g)) \ \cdots \ \chi_r((f_r, g)), \quad g \in \mathbb{F}_q[x]. \tag{2.3}$$

Note that X is a well-defined Dirichlet character since $f_1, \ldots, f_r$ are monic. Accordingly, we define Dirichlet L-series

$$L(\mathcal{F}, X, s) = \sum_g{}' \frac{X(g)}{|g|^s}, \tag{2.4}$$

where $|g| = q^{\deg(g)}$. The sum is over all monic polynomials of $\mathbb{F}_q[x]$. Since the character X is multiplicative, $L(\mathcal{F}, X, s)$ has an Euler product

$$L(\mathcal{F}, X, s) = \prod_v{}' \left(1 - \frac{X(v)}{|v|^s}\right)^{-1}, \tag{2.5}$$

where the product is over monic irreducible polynomials v in $\mathbb{F}_q[x]$. The "zeta function" of $\mathbb{F}_q[x]$ is well-known to be

$$\zeta(s) = \frac{1}{1 - q^{1-s}} = \sum_g{}' \frac{1}{|g|^s} = \prod_v{}' \left(1 - \frac{1}{|v|^s}\right)^{-1}, \tag{2.6}$$

where the sum is over all monic g in $\mathbb{F}_q[x]$, and the last equality is valid for $\mathrm{Re}(s) > 1$. Note that $\zeta(s)$ has no zeros, but only poles at

$$s = 1 + \frac{2\pi i n}{\log q}, \quad n \in \mathbb{Z}. \tag{2.7}$$

This is in sharp contrast with the classical Riemann zeta function which only has a pole at $s = 1$ and at no other points of the complex plane.

Using elementary properties of finite fields (nowadays taught in an undergraduate course in algebra), Davenport shows that $L(\mathcal{F}, X, s)$ is a polynomial in q^{-s} of degree $K - 1$ (see Theorem 1 of [4]). That is to say, with zeros $s_1, \ldots s_{K-1}$, we have

$$L(\mathcal{F}, X, s) = (1 - q^{s_1 - s})(1 - q^{s_2 - s}) \ \cdots \ (1 - q^{s_{K-1} - s}). \tag{2.8}$$

The analogous result is known for any Dirichlet character in $\mathbb{F}_q[x]$, and a more precise account can be found in [17, Proposition 4.3]. The Euler product for $\zeta(s)$ and $L(\mathcal{F}, X, s)$ combined with the classical argument of Hadamard and de la Vallée Poussin shows that $L(\mathcal{F}, X, s) \neq 0$ for $\mathrm{Re}(s) = 1$, but more is true and we can derive a nontrivial zero free region following the classical method.

Lemma 1. *Following the notations above, we have the following inequality: for any character X, we have for $\sigma > 1$,*

$$0 \leq -Re\left\{3\frac{L'}{L}(\mathcal{F}, X_0, \sigma) + 4\frac{L'}{L}(\mathcal{F}, X, \sigma + it) + \frac{L'}{L}(\mathcal{F}, X^2, \sigma + 2it)\right\}, \tag{2.9}$$

where X_0 denotes the trivial character.

Proof. From the Euler product of $L(\mathcal{F}, X, s)$, we get

$$\log L(\mathcal{F}, X, s) = -\sum_v \log\left(1 - \frac{X(v)}{|v|^s}\right) = \sum_v \sum_{n=1}^{\infty} \frac{X(v)^n}{|v|^{sn} n}, \quad \mathrm{Re}(s) > 1. \tag{2.10}$$

Define the von Mangoldt function

$$\Lambda(g) = \begin{cases} \log|v| & \text{if } g = v^k \text{ for some irreducible } v; \\ 0 & \text{otherwise} \end{cases}$$

Logarithmic differentiation of the Euler product formula gives

$$\begin{aligned} -\frac{L'}{L}(\mathcal{F}, X, s) &= \sum_v \sum_{n=1}^{\infty} X(v)^n |v|^{-sn} \log|v| = \sum_g \Lambda(g) X(g) |g|^{-s} \\ &= \sum_g \Lambda(g) X(g) |g|^{-\sigma} e^{-it \log|g|}, \end{aligned} \tag{2.11}$$

where the sum is over all monic g in $\mathbb{F}_q[x]$ and $s = \sigma + it$. Recall the celebrated Mertens inequality

$$3 + 4\cos\theta + \cos 2\theta \geq 0. \tag{2.12}$$

As we express the real part of $X(g)e^{-it\log|g|}$ in (2.11) by $\cos\theta$ for some θ, the corresponding $\cos 2\theta$ in (2.12) can be obtained by replacing X by X^2 and t by $2t$. Hence, we get the desired inequality. □

Let us remark that (2.9) has the following consequences. We have

$$1 \leq \left|L(\mathcal{F}, X_0, \sigma)^3 L(\mathcal{F}, X, \sigma + it)^4 L(\mathcal{F}, X^2, \sigma + 2it)\right|, \tag{2.13}$$

for $\sigma > 1$. If X^2 is nontrivial, then $L(\mathcal{F}, X^2, s)$ is analytic and the classical argument now shows that $L(\mathcal{F}, X, 1 + it) \neq 0$ for all $t \in \mathbb{R}$. Indeed, if $L(\mathcal{F}, X, 1 + it) = 0$, then the above inequality introduces a zero of order 4, which cancels the pole of order 3, and we get a contradiction if $\sigma \to 1^+$. If X^2 is trivial, then the usual proof proceeds in two steps. First, one shows $L(\mathcal{F}, X, 1) \neq 0$ (see [17] for more details). Then, as $L(\mathcal{F}, X, s)$ is

periodic, with period $\frac{2\pi i}{\log q}$, we consider $L(\mathcal{F}, X, \sigma + it)$ with $t \neq 0$ and $|t| < \frac{\pi}{\log q}$. With this understanding, we now apply (2.13), and deduce that if $L(\mathcal{F}, X, 1 + it) = 0$ and X^2 is trivial, then $L(\mathcal{F}, X^2, 1 + 2it)$ is bounded, since $|t| < \frac{\pi}{\log q}$ and $L(\mathcal{F}, X^2, s)$ is analytic for $t \neq 0$, $|t| < \frac{\pi}{\log q}$. So, (2.13) gives a contradiction if we let $\sigma \to 1^+$. We record the discussion in the following lemma.

Lemma 2. *Following the notations from Lemma 1, $L(\mathcal{F}, X, s) \neq 0$ for $Re(s) = 1$.*

3. An elementary proof of Artin's conjecture over function fields

Let p be a prime and let $\mathbb{F}_q$ be a finite field with $q = p^k$ elements. Consider a polynomial $a(x) \in \mathbb{F}_q[x]$. If $a(x)$ is to be a primitive root modulo $p(x)$ for infinitely many irreducible polynomials $p(x)$, then it is clearly necessary that $a(x)$ not be a perfect dth power for any $d > 1$ such that for some $i \geq 1$, $d \mid q^i - 1$. We will show the condition is also sufficient. Artin's primitive root conjecture over function fields concerns the number of irreducible polynomials $p(x) \in \mathbb{F}_q[x]$ such that $a(x)$ generates $(\mathbb{F}_q[x]/p(x))^*$. Note that we have an isomorphism

$$\mathbb{F}_q[x]/p(x) \cong \mathbb{F}_{q^n}, \quad \text{where } n = \deg p(x)$$

which is given as follows: For $g(x) \in \mathbb{F}_q[x]$, we have

$$g(x) = p(x)q(x) + r(x), \quad \text{where } r(x) = 0 \text{ or } 0 \leq \deg r(x) < n.$$

Let $\theta \in \mathbb{F}_{q^n}$ be a root of $p(x)$. Then $\mathbb{F}_{q^n}$ is generated by $1, \theta, \theta^2, \ldots, \theta^{n-1}$ over $\mathbb{F}_q$. Since $p(x)$ has n roots, we obtain the following description of relevant sets: for a fixed $a(x) \in \mathbb{F}_q[x]$,

$$\#\left\{p(x) \in \mathbb{F}_q[x] : p(x) : \text{irreducible}, \quad \deg p(x) = n, \quad a(x) \text{ generates } (\mathbb{F}_q[x]/p(x))^*\right\} \tag{3.1}$$

$$= \frac{1}{n} \#\left\{\theta \in \mathbb{F}_{q^n} : \deg \theta = n, \quad a(\theta) \text{ generates } \mathbb{F}_{q^n}^*\right\}. \tag{3.2}$$

This suggests that it may be more convenient to count each irreducible polynomial $v(x)$ with weight $w(v) := \deg v$ whenever $a(x)$ generates $(\mathbb{F}_q[x]/p(x))^*$ and zero otherwise. This remark will be used in the next section.

3.1. Sifting function and Artin's conjecture

For estimating (3.2), we introduce the sifting function which, for instance, can be found in the works of Landau [11, Satz 496], who ascribes it to I. M. Vinogradov:

Lemma 3. *Let G be a cyclic group of order m, and let φ be the Euler phi function. Define the sifting function $\mathcal{S}$:*

$$\mathcal{S}(g) = \frac{\varphi(m)}{m}\left\{1 + \sum_{\substack{d|m \\ d>1}} \frac{\mu(d)}{\varphi(d)} \sum_{\operatorname{ord}\chi = d} \chi(g)\right\}, \tag{3.3}$$

where the rightmost sum is defined over characters χ of G which are of order d. Then, we have

$$\mathcal{S}(g) = \begin{cases} 1 & \text{if } g \text{ generates } G; \\ 0 & \text{otherwise.} \end{cases}$$

Let now $\mathcal{S}$ denote the sifting function for $\mathbb{F}_{q^n}^*$, and define $\mathcal{S}(0) = 0$. Then, by our earlier remark,

$$\sum_{v:\, \deg v | n} w(v) = \sum_{\theta \in \mathbb{F}_{q^n}^*} \mathcal{S}(a(\theta)),$$

since non-zero elements of $\mathbb{F}_{q^n}^*$ are precisely elements θ whose degree divides n.

Using the sifting function $\mathcal{S}$ in Lemma 3, to count the number of generators of $\mathbb{F}_{q^n}^*$, which is a cyclic group of order $q^n - 1$, we obtain the following:

$$\#\left\{\theta \in \mathbb{F}_{q^n} : \deg\theta \mid n, \quad a(\theta) \text{ generates } \mathbb{F}_{q^n}^*\right\} = \sum_{\theta \in \mathbb{F}_{q^n}} \mathcal{S}(a(\theta)). \tag{3.4}$$

Thus, we have

$$\sum_{\theta \in \mathbb{F}_{q^n}} \mathcal{S}(a(\theta)) = \sum_{\theta \in \mathbb{F}_{q^n}} \frac{\varphi(q^n-1)}{q^n-1}\left\{1 + \sum_{\substack{d|q^n-1 \\ d>1}} \frac{\mu(d)}{\varphi(d)} \sum_{\operatorname{ord}\chi = d} \chi(a(\theta))\right\} \tag{3.5}$$

$$= \left\{\sum_{\theta \in \mathbb{F}_{q^n}} \frac{\varphi(q^n-1)}{q^n-1}\right\} + \left\{\sum_{\theta \in \mathbb{F}_{q^n}} \frac{\varphi(q^n-1)}{q^n-1} \sum_{\substack{d|q^n-1 \\ d>1}} \frac{\mu(d)}{\varphi(d)} \sum_{\operatorname{ord}\chi = d} \chi(a(\theta))\right\} \tag{3.6}$$

$$= \frac{\varphi(q^n-1)}{(q^n-1)}\left\{(q^n-1) + \sum_{\substack{d|q^n-1 \\ d>1}} \frac{\mu(d)}{\varphi(d)} \sum_{\operatorname{ord}\chi = d} \sum_{\theta \in \mathbb{F}_{q^n}} \chi(a(\theta))\right\}. \tag{3.7}$$

From now on, we are estimating the rightmost character sum

$$\sum_{\theta \in \mathbb{F}_{q^n}} \chi(a(\theta)),$$

for a polynomial $a(x) \in \mathbb{F}_q[x]$.

These character sums were the focus of Davenport's work [4]. However, in some special cases, it is possible to use Gauss sums to estimate these sums. For instance, in the paper of Jensen and Murty [10] they established Artin's conjecture for $\mathbb{F}_q[x]$ for polynomials of the form $a(x) = x^m + c$, for any m and c using such a technique. More precisely, for these polynomials, we have

$$\left| \sum_{\theta \in \mathbb{F}_{q^n}} \chi(a(\theta)) \right| \leq m q^{\frac{n}{2}} \tag{3.8}$$

using elementary Gauss sum calculations. This shows the sum in (3.7) is an error term with contribution $\mathcal{O}(q^{\frac{n}{2}} d(q^n - 1))$. Recall that for any $\epsilon > 0$, the number of divisors of $q^n - 1$ is $\mathcal{O}(q^{n\epsilon})$, and because

$$\varphi(q^n - 1) \gg \frac{q^n}{\log \log q^n},$$

we see that the first term dominates as n tends to infinity. This gives Artin's conjecture in this special case. Hence, the first summand dominates the sum (3.7) as n tends to ∞, which gives Artin's conjecture in this special case.

In the general case, we will obtain a non-trivial estimate for the character sum which will not be a power saving. However, there is a good estimate for the divisor function due to Ramanujan that we can use. Let $d(n)$ be the number of positive divisors of n. Ramanujan showed that

$$d(n) < 2^{\frac{\log n}{\log \log n} + \mathcal{O}\left(\frac{\log n}{(\log \log n)^2}\right)}.$$

We do not need such a fine result. It suffices to know that for some constant $c > 0$,

$$d(n) < \exp\left(\frac{c \log n}{\log \log n}\right).$$

A proof of this weaker result can be found in [9, p. 345]. This implies

$$d(q^n - 1) < \exp\left(\frac{cn \log q}{\log n}\right) = q^{cn/\log n}.$$

Comparing these estimates with the main term, we see that all we need is a modest improvement over the trivial estimate on the character sum. This will be deduced following

the classical method of Hadamard and de la Vallée Poussin. In the following section, we are going to give a nontrivial estimation of the character sum (3.8) for any k and any form of polynomial in order to obtain Artin's conjecture for function fields in its full generality.

4. The main theorem

In this section, we will prove:

Theorem 4. *Let $\mathcal{F} = (f_1, f_2, \ldots, f_r)$ be an r-tuple of irreducible monic polynomials in $\mathbb{F}_q[x]$. There is an absolute constant $c > 0$ such that*

$$L(\mathcal{F}, X, s) \neq 0, \quad \text{for } Re(s) > 1 - \frac{c}{(K-1)\log q}, \tag{4.1}$$

where X is a nontrivial multiplicative character defined as in (2.3) and satisfying $X^2 \neq X_0$.

Proof of Theorem 4. Recall that $L(\mathcal{F}, X, s)$ is a polynomial in q^{-s} of degree $K-1$ with zeros $s_1, \ldots, s_{K-1}$ as in (2.8):

$$L(\mathcal{F}, X, s) = \prod_{j=1}^{K-1} (1 - q^{s_j - s}) = q^{-(K-1)s} \prod_{j=1}^{K-1} (q^s - q^{s_j}). \tag{4.2}$$

Then the logarithmic derivative gives

$$-\frac{L'}{L}(\mathcal{F}, X, s) = (K-1)\log q - \sum_{j=1}^{K-1} \frac{q^s \log q}{q^s - q^{s_j}}. \tag{4.3}$$

Now, we examine the function

$$F(s) := \frac{q^s}{q^s - q^{s_j}}. \tag{4.4}$$

The singularities of $F(s)$ are at

$$s = s_j + \frac{2\pi i n}{\log q}, \quad n \in \mathbb{Z}. \tag{4.5}$$

These are all simple poles with residue $\frac{1}{\log q}$. Thus $F(s)$ has the "partial fraction" decomposition:

$$\frac{q^s}{q^s - q^{s_j}} = \frac{1}{\log q} \sum_{n \in \mathbb{Z}} \frac{1}{s - \rho_{n,j}}, \quad \text{where } \rho_{n,j} = s_j + \frac{2\pi i n}{\log q}, \tag{4.6}$$

which combines with (4.3) to give

$$-\frac{L'}{L}(\mathcal{F}, X, s) = (K-1)\log q - \sum_{j=1}^{K-1}\sum_{n\in\mathbb{Z}} \frac{1}{s-\rho_{n,j}}. \tag{4.7}$$

Observe that

$$\mathrm{Re}\left(\frac{1}{s-\rho_{n,j}}\right) = \mathrm{Re}\left(\frac{\overline{s}-\overline{\rho}_{n,j}}{|s-\rho_{n,j}|^2}\right) > 0, \tag{4.8}$$

if $\mathrm{Re}(s) > 1$. From now on, we follow idea of the classical proof of the prime number theorem by Hadamard and de la Vallée Poussin. From (4.8), since $X^2 \neq X_0$, by omitting the summation over poles in (4.7) we have

$$\mathrm{Re}\left(-\frac{L'}{L}(\mathcal{F}, X^2, \sigma+2it)\right) \leq (K-1)\log q, \tag{4.9}$$

for any choice of σ and t. For estimating $L(\mathcal{F}, X, \sigma+it)$, we let $\beta+i\gamma$ be any zero of $L(\mathcal{F}, X, s)$. By dropping all zeros but $\beta+i\gamma$ in the equality (4.7), we obtain the following:

$$\mathrm{Re}\left(-\frac{L'}{L}(\mathcal{F}, X, \sigma+i\gamma)\right) \leq (K-1)\log q - \frac{1}{\sigma-\beta}, \tag{4.10}$$

for any $\sigma > 1$. Moreover, since $\zeta(s)$ has simple poles at

$$s = 1 + \frac{2\pi i n}{\log q}, \quad n \in \mathbb{Z}, \tag{4.11}$$

the function $f(s) = (s-1)\zeta(s)$ is a regular and nonvanishing near $s = 1$, and thus

$$\frac{f'(s)}{f(s)} = \frac{1}{s-1} + \frac{\zeta'(s)}{\zeta(s)}, \tag{4.12}$$

is also regular near $s = 1$, and bounded for $1 < \sigma \leq 2$. For any such σ, we have

$$-\frac{L'}{L}(\mathcal{F}, X_0, \sigma) = \sum_g \Lambda(g)X_0(g)|g|^{-\sigma} \leq -\frac{\zeta'}{\zeta}(\sigma) < \frac{1}{\sigma-1} + A_1, \tag{4.13}$$

for some positive absolute constant A_1. Then combining (4.9), (4.10), and inequality (2.12), we obtain

$$\frac{4}{\sigma-\beta} \leq \frac{3}{\sigma-1} + A(K-1)\log q, \tag{4.14}$$

for some positive absolute constant A. Writing $\sigma = 1 + \frac{\delta}{\log q}$, we get

$$\beta \leq 1 + \frac{\delta}{\log q} - \frac{4\delta}{(3 + \delta A(K-1)) \log q}. \tag{4.15}$$

Hence, choosing a suitable positive δ, we get the desired result that

$$\beta < 1 - \frac{c}{(K-1)\log q}. \quad \square \tag{4.16}$$

We remark that if $0 < c_1 < c$, then our theorem holds with c replaced by c_1. This remark will be used later. In the rest of the section, we are going to present the application of Theorem 4 in Artin's conjecture and character sums over function fields. Let h be any positive integer so that $\mathbb{F}_{q^h}$ is a finite extension of the field $\mathbb{F}_q$, hence any character χ in $\mathbb{F}_q$ induces a character $\chi^{(h)}$ in $\mathbb{F}_{q^h}$ satisfying

$$\chi^{(h)}(\xi) = \chi(N_{\mathbb{F}_{q^h}/\mathbb{F}_q}(\xi)), \tag{4.17}$$

where $N_{\mathbb{F}_{q^h}/\mathbb{F}_q}(\xi)$ is the norm of $\xi \in \mathbb{F}_{q^h}$ defined by its conjugates over $\mathbb{F}_q$. In connection with the character sum (2.1): Let $f_1(x), \ldots, f_r(x)$ be irreducible monic polynomials with degree $k_1, \ldots, k_r$. Let us denote by $\mathcal{X} = (\chi_1, \chi_2, \ldots, \chi_r)$ an r-tuple of multiplicative characters of $\mathbb{F}_q$, and by $\mathcal{F} = (f_1, f_2, \ldots, f_r)$ the r-tuple of irreducible monic polynomials. We define

$$S(\mathcal{F}, \mathcal{X}) = \sum_{x \in \mathbb{F}_q} \chi_1(f_1(x)) \cdots \chi_r(f_r(x)). \tag{4.18}$$

In connection with $S(\mathcal{F}, \mathcal{X})$, we define a character sum in $\mathbb{F}_{q^h}$:

$$S^{(h)}(\mathcal{F}, \mathcal{X}) = \sum_{\xi \in \mathbb{F}_{q^h}} \chi_1^{(h)}(f_1(\xi)) \cdots \chi_r^{(h)}(f_r(\xi)). \tag{4.19}$$

Denote $K = k_1 + \cdots + k_r$. We have the following result of Davenport [4] which relates the above character sums to the zeros of $L(\mathcal{F}, X, s)$:

Theorem 5. *Let $s_1, \ldots, s_{K-1}$ be distinct zeros of $L(\mathcal{F}, X, s)$, viewed as a polynomial in q^{-s} as in (2.8), ignoring the period $\frac{2\pi i}{\log q}$. Then*

$$-S^{(h)}(\mathcal{F}, \mathcal{X}) = q^{hs_1} + \cdots + q^{hs_{K-1}}. \tag{4.20}$$

In particular, when $h = 1$,

$$-S(\mathcal{F}, \mathcal{X}) = q^{s_1} + \cdots + q^{s_{K-1}}.$$

Corollary 6. *Let χ be a nontrivial character defined over $\mathbb{F}_{q^n}$, which is not quadratic, i.e., $\chi^2 \neq \chi_0$, and let f be an irreducible polynomial of degree K in $\mathbb{F}_q[x]$. Then*

$$\sum_{x\in\mathbb{F}_{q^n}} \chi(f(x)) = \mathcal{O}(q^n e^{-cn/(K-1)}), \tag{4.21}$$

where the implied constant is absolute.

Corollary 7. *Let χ be a nontrivial quadratic character defined over $\mathbb{F}_{q^n}$, and let f be an irreducible polynomial of degree K in $\mathbb{F}_q[x]$. Then*

$$\sum_{x\in\mathbb{F}_{q^n}} \chi(f(x)) = \mathcal{O}(q^{nB}), \tag{4.22}$$

where $B < 1$ is a fixed constant, and the implied constant is absolute.

Corollary 8. *Artin's conjecture over function fields holds for irreducible polynomials in $\mathbb{F}_q[x]$.*

Proof of Corollary 6. Following Theorem 5, and with notations as in (2.8), we have the equality:

$$\sum_{x\in\mathbb{F}_{q^n}} \chi(f(x)) = -q^{ns_1} - q^{ns_2} - \cdots - q^{ns_{K-1}}, \tag{4.23}$$

where $s_1, s_2, \ldots, s_{K-1}$ are zeros of (by abuse of notation) $L(f,\chi,s)$, viewed as a polynomial in q^{-s} as in (2.8), ignoring period. Hence, when $\chi^2 \neq \chi_0$, Theorem 4 implies

$$\left|\sum_{x\in\mathbb{F}_{q^n}} \chi(f(x))\right| = \mathcal{O}\left(q^n e^{-cn/(K-1)}\right). \quad \square \tag{4.24}$$

Proof of Corollary 7. When $\chi^2 = \chi_0$, since $L(f,\chi,s)$ is a polynomial in q^{-s} of degree $K-1$, we write the zeros of the polynomial as $q^{s_1}, q^{s_2}, \ldots, q^{s_{K-1}}$. Let

$$B = \max\{\mathrm{Re}(s_1), \mathrm{Re}(s_2), \ldots, \mathrm{Re}(s_{K-1})\}.$$

Note that $B < 1$ from Lemma 2. From Theorem 5, for any n,

$$\left|\sum_{x\in\mathbb{F}_{q^n}} \chi(f(x))\right| = |-q^{ns_1} - q^{ns_2} - \cdots - q^{ns_{K-1}}| = \mathcal{O}(q^{nB}). \quad \square \tag{4.25}$$

Proof of Corollary 8. From Corollary 6 and Corollary 7, we choose small enough $c > 0$ satisfying $c < (K-1)(1-B)\log q$ (recall that Theorem (4) still holds with c replaced by smaller positive constant) so that we have

$$\sum_{x\in\mathbb{F}_{q^n}} \chi(f(x)) = \mathcal{O}(q^n e^{-cn/(K-1)}), \tag{4.26}$$

for any nontrivial character χ. We use (4.26) to obtain the infinitude of the following sum in (3.7):

$$\frac{\varphi(q^n-1)}{q^n-1}\left\{(q^n-1)+\sum_{\substack{d|q^n-1\\ d>1}}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}\,\chi=d}\sum_{\theta\in\mathbb{F}_{q^n}}\chi(a(\theta))\right\}$$

to estimate the number of generators of $\mathbb{F}_{q^n}^*$. For any $\eta>0$, and denote by $d(n)$ the number of divisors of n. Then we have the following inequality by Ramanujan [12, Exercise 1.3.3]:

$$d(n)<2^{(1+\eta)\log n/\log\log n},$$

for all n sufficiently large. Therefore, along with (4.26), we have the following:

$$\sum_{\substack{d|q^n-1\\ d>1}}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}\,\chi=d}\sum_{\theta\in\mathbb{F}_{q^n}}\chi(a(\theta))=\mathcal{O}(q^ne^{-cn/(K-1)}\cdot d(q^n-1)) \tag{4.27}$$

$$=\mathcal{O}(q^ne^{-cn/(K-1)}2^{\log q(1+\eta)n/\log n}), \tag{4.28}$$

for any choice of $\eta>0$, which is dominated by q^n as n tends to ∞. Hence, we have the infinitude of the following set from (3.1):

$$\#\left\{\theta\in\mathbb{F}_{q^n}:\deg\theta\mid n,\quad a(\theta)\text{ generates }\mathbb{F}_{q^n}^*\right\}, \tag{4.29}$$

which implies that Artin's conjecture over function fields holds for irreducible polynomials in $\mathbb{F}_q[X]$. □

One can argue similarly to the proof of Corollary 6 to prove Artin's conjecture over function fields for reducible polynomials in $\mathbb{F}_q[x]$. When $f(x)\in\mathbb{F}_q[x]$ is reducible, the character sum (4.21) can be expressed using the factorization of $f(x)$ into irreducible polynomials:

$$\sum_{x\in\mathbb{F}_{q^n}}\chi(f(x))=\sum_{x\in\mathbb{F}_{q^n}}\chi(f_1(x))\chi(f_2(x))\ \cdots\ \chi(f_r(x)), \tag{4.30}$$

where $f_1(x),\dots,f_r(x)$ are all irreducible. Thus, following (4.20), we consider instead a induced character and can repeat the same procedure as in the proof of Corollary 6.

5. Concluding remarks

It is clear that the method works for relative extensions as well. Essentially, the problem is then how to find primitive roots along curves. Artin's conjecture over general

function fields was studied by Pappalardi and Shparlinski [15]. In their work, they make fundamental use of a result of Perelmuter [14] who generalized the work of Weil by considering exponential sums along curves. But what this amounts to is really the analog of the prime number theorem for relative extensions. As our method shows that in general the zeta function of any function field over a finite field does not vanish on the line $\mathrm{Re}(s) = 1$ and even provides a zero free region, the proof in this paper easily extends to provide a simple proof in the general case also.

More generally, one can study the distribution of primitive roots along varieties over finite fields. This would now require the study of zeta functions of varieties. It may be possible by a fibering technique to extend the elementary nature of this paper to the setting of varieties without appealing to the deep work of Pierre Deligne on the resolution of the Weil conjectures [5]. We relegate this to future work.

Acknowledgments

We thank Francesco Pappalardi, Michael Rosen, Joseph Silverman, and Igor Shparlinski for their comments on an earlier version of our paper. The authors would also like thank the referees for their helpful suggestions.

References

[1] Herbert Bilharz, Primdivisoren mit vorgegebener Primitivwurzel, Math. Ann. 114 (1) (1937) 476–492. MR1513151.
[2] Enrico Bombieri, Counting points on curves over finite fields (d'après S.A. Stepanov), in: Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 430, in: Lecture Notes in Math., vol. 383, 1974, pp. 234–241. MR0429903.
[3] Alina C. Cojocaru, Cyclicity of elliptic curves modulo p, ProQuest Dissertations and Theses, 2002, p. 152 (in English); Copyright - Database copyright ProQuest LLC; ProQuest does not claim copyright in the individual underlying works; Last updated - 2016-05-10.
[4] H. Davenport, On character sums in finite fields, Acta Math. 71 (1939) 99–121. MR252.
[5] Pierre Deligne, La conjecture de Weil. I, Inst. Hautes Études Sci. Publ. Math. 43 (1974) 273–307. MR340258.
[6] Rajiv Gupta, M. Ram Murty, A remark on Artin's conjecture, Invent. Math. 78 (1) (1984) 127–130. MR762358.
[7] D.R. Heath-Brown, Artin's conjecture for primitive roots, Q. J. Math. Oxf. Ser. (2) 37 (145) (1986) 27–38. MR830627.
[8] Christopher Hooley, On Artin's conjecture, J. Reine Angew. Math. 225 (1967) 209–220. MR207630.
[9] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, sixth ed., Oxford University Press, Oxford, 2008, revised by D.R. Heath-Brown and J.H. Silverman, with a foreword by Andrew Wiles. MR2445243.
[10] Erik Jensen, M. Ram Murty, Artin's conjecture for polynomials over finite fields, in: Number Theory, 2000, pp. 167–181. MR1764802.
[11] Edmund Landau, Vorlesungen über Zahlentheorie. Erster Band, zweiter Teil; zweiter Band; dritter Band, Chelsea Publishing Co., New York, 1969. MR0250844.
[12] M. Ram Murty, Problems in Analytic Number Theory, second ed., Graduate Texts in Mathematics, vol. 206, Springer, New York, 2008, Readings in Mathematics. MR2376618.
[13] M. Ram Murty, Artin's conjecture for primitive roots, Math. Intell. 10 (4) (1988) 59–67. MR966133.
[14] G.I. Perelmuter, Estimate of a sum along an algebraic curve, Mat. Zametki 5 (1969) 373–380. MR241424.
[15] Francesco Pappalardi, Igor Shparlinski, On Artin's conjecture over function fields, Finite Fields Appl. 1 (4) (1995) 399–404. MR1353988.

[16] Peter Roquette, The Riemann Hypothesis in Characteristic p in Historical Perspective, Lecture Notes in Mathematics, vol. 2222, Springer, Cham, 2018, History of Mathematics Subseries. MR3839328.
[17] Michael Rosen, Number Theory in Function Fields, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR1876657.
[18] Wolfgang M. Schmidt, Equations over Finite Fields. An Elementary Approach, Lecture Notes in Mathematics, vol. 536, Springer-Verlag, Berlin-New York, 1976. MR0429733.
[19] S.A. Stepanov, The number of points of a hyperelliptic curve over a finite prime field, Izv. Akad. Nauk SSSR, Ser. Mat. 33 (1969) 1171–1181. MR0252400.
[20] André Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg 7 (1945), Hermann et Cie., Paris, 1948. MR0027151.