

THE TWO-VARIABLE ZETA FUNCTION AND THE RIEMANN HYPOTHESIS FOR FUNCTION FIELDS

MACHIEL VAN FRANKENHUIJSEN

ABSTRACT. We present Bombieri’s proof of the Riemann hypothesis for the zeta function of a curve over a finite field. We first briefly describe this zeta function and discuss the two-variable zeta function of Pellikaan. Then we give Naumann’s proof that the numerator of this function is irreducible.

Keywords: Riemann hypothesis for a curve over a finite field, zeta function of a curve over a finite field, two-variable zeta function.

1. INTRODUCTION

In his thesis [1] of 1924, Artin introduced the zeta function of a curve over a finite field, and asked if this function satisfies the Riemann hypothesis, that is, if its zeros lie on the line $\operatorname{Re} s = 1/2$. This was proved in 1933 by Hasse [3] for elliptic curves, and in full generality by Weil [9, 10] in 1942. In §2, we briefly recall the zeta function. We refer to [7, 11] for a more thorough discussion. Then we discuss the two-variable zeta function of Pellikaan [6] and we present Naumann’s proof [4] that the zeros of this function form an irreducible algebraic curve.

In §4, we reformulate the Riemann hypothesis as an estimate on the number of points on the curve. We present Bombieri’s proof [2] of the Riemann hypothesis, which was based on Stepanov’s idea for hyperelliptic curves [5]. It depends on an analysis of the action of the Frobenius automorphism on algebraic points on the curve.

2. THE ZETA FUNCTION OF \mathcal{C}

Throughout, we fix a function field K with a finite field of constants \mathbb{F}_q , and we choose a function $T \in K$ such that K is a finite separable extension of the field of rational functions $\mathbb{F}_q(T)$. Geometrically, K is the field of functions on a curve \mathcal{C} , and the choice of T corresponds to the choice of a projection of \mathcal{C} onto \mathbb{P}^1 .

The Frobenius automorphism ϕ_q acts on \mathcal{C} by raising each coordinate of a point in $\mathcal{C}(\overline{\mathbb{F}}_q)$ to the q -th power. The fixed points of this action are the points on the curve with values in \mathbb{F}_q . A valuation v of K corresponds to an orbit of points in $\mathcal{C}(\overline{\mathbb{F}}_q)$ under this action. We write $\deg v$ for its length, which is also the degree of the field of residue classes at v over \mathbb{F}_q . For a function $f \in K$, $v(f)$ equals the order of vanishing of f at any one of the point in this orbit; that is, we always normalize a valuation so that $\{v(f) : f \in K\} = \mathbb{Z}$. The restriction of v to $\mathbb{F}_q(T)$ is either a multiple of a P -adic valuation for an irreducible polynomial P , given by $v_P(P^k a/b) = k$ for polynomials a and b without factor P , or of the valuation at infinity, given by $v_\infty(a/b) = \deg b - \deg a$.

2000 *Mathematics Subject Classification*. Primary 11M26; Secondary 11M38.

For an extension L/K and a valuation w of L with restriction v , the *order of ramification* of w over v is

$$(2.1) \quad e_{w/v} = \min\{w(f) : f \in K, w(f) > 0\}.$$

Let v be a valuation of K and let v_P , for $P = \infty$ or an irreducible polynomial, be (a multiple of) its restriction to $\mathbb{F}_q(T)$. Let $\text{Tr}_{v/P}$ be the trace from the completion K_v to $\mathbb{F}_q(T)_P$. The *inverse different*

$$\{\eta \in K_v : v(\text{Tr}_{v/P}(\eta\xi)) \geq 0 \text{ for all } \xi \text{ with } v(\xi) \geq 0\}$$

is a fractional ideal, hence equal to $\{\eta \in K_v : v(\eta) \geq -d_{v/P}\}$ for some integer $d_{v/P}$. The *canonical coefficient* is defined by

$$k_v = \begin{cases} d_{v/P} & \text{if } v(T) \geq 0, v(P) > 0, \\ d_{v/\infty} - 2e_{v/\infty} & \text{if } v(T) < 0. \end{cases}$$

For every finite valuation, $k_v \geq 0$, but above infinity, the canonical coefficient may be negative. Moreover, it depends on the choice of the function T in K .

A *divisor* on \mathcal{C} is a finite formal sum $\mathcal{D} = \sum_v d_v v$ of valuations with integer coefficients. The divisor is *positive*, $\mathcal{D} \geq 0$, if $d_v \geq 0$ for every valuation. The degree of \mathcal{D} is $\deg \mathcal{D} = \sum_v d_v \deg v$. The *canonical divisor* of \mathcal{C} is $\mathcal{K} = \sum_v k_v v$. A function $f \in K^*$ gives a *principal divisor* $(f) = \sum_v v(f)v$. Given a divisor \mathcal{D} , the set of functions f such that $f = 0$ or $(f) + \mathcal{D} \geq 0$ is a vector space over \mathbb{F}_q , denoted $L(\mathcal{D})$. Its dimension over \mathbb{F}_q is denoted $l(\mathcal{D})$.

Theorem 2.1 (Riemann–Roch). *Let \mathcal{C} be a curve with canonical divisor \mathcal{K} . Then there exists a number g such that*

$$l(\mathcal{D}) = \deg \mathcal{D} + 1 - g + l(\mathcal{K} - \mathcal{D})$$

for every divisor \mathcal{D} on \mathcal{C} .

The number g is called the *genus* of \mathcal{C} . Taking $\mathcal{D} = 0$, we see that $g = l(\mathcal{K})$, so that $g \geq 0$. Taking $\mathcal{D} = \mathcal{K}$, we then see that $\deg \mathcal{K} = 2g - 2$.

For \mathbb{P}^1 , the functions $1, T, T^2, \dots, T^n$ all lie in $L(nv_\infty)$, hence $l(nv_\infty) \geq n + 1$. Taking $n > \deg \mathcal{K}$, we see that \mathbb{P}^1 has genus zero. In §3.1, we show that every curve of genus zero is isomorphic to \mathbb{P}^1 .

2.1. The Zeta Function of \mathcal{C} . For $\text{Re } s > 1$ we define

$$\zeta_{\mathcal{C}}(s) = q^{(g-1)s} \sum_{\mathcal{D} \geq 0} q^{-s \deg \mathcal{D}}.$$

In the next section, we show that $\zeta_{\mathcal{C}}(1-s) = \zeta_{\mathcal{C}}(s)$. Since divisors have a unique factorization into valuations, we obtain the Euler product

$$(2.2) \quad \zeta_{\mathcal{C}}(s) = q^{(g-1)s} \prod_v \frac{1}{1 - q^{-s \deg v}}.$$

Two divisors \mathcal{D} and \mathcal{D}' are *linearly equivalent* if there exists a function $f \in K^*$ such that $\mathcal{D}' = (f) + \mathcal{D}$. In that case, \mathcal{D} and \mathcal{D}' have the same degree. We denote by $\text{Cl}(n)$ the set of linear equivalence classes of degree n . Clearly, $\text{Cl}(0)$ is a group. This group is finite, and its order is denoted by $h_{\mathcal{C}}$, the *class number* of \mathcal{C} . Also $\text{Cl}(n)$ has $h_{\mathcal{C}}$ elements, for every integer n . For a divisor \mathcal{D} , the number of positive

divisors in its class is $q^{l(\mathcal{D})} - 1 / q - 1$. Summing over the different divisor classes of degree n , we obtain

$$\zeta_{\mathcal{C}}(s) = q^{(g-1)s} \sum_{n=-\infty}^{\infty} q^{-ns} \sum_{\mathcal{D} \in \text{Cl}(n)} \frac{q^{l(\mathcal{D})} - 1}{q - 1}.$$

For the projective line, $l(\mathcal{D}) = n + 1$ for $n = \deg \mathcal{D} \geq 0$, and we find

$$(2.3) \quad \zeta_{\mathbb{P}^1}(s) = \frac{q^{-s}}{(1 - q^{1-s})(1 - q^{-s})}.$$

The poles of this function are simple, located at $s = 2\pi i k / \log q$ (for $k \in \mathbb{Z}$), with residue $-\frac{1}{(q-1)\log q}$, and at $s = 1 + 2\pi i k / \log q$, with residue $\frac{1}{(q-1)\log q}$.

In general, we find

$$\zeta_{\mathcal{C}}(s) = q^{-gs} L_{\mathcal{C}}(q^s) \zeta_{\mathbb{P}^1}(s),$$

where $L_{\mathcal{C}}(X) = X^{2g} + l_1 X^{2g-1} + \dots + l_{2g-1} X + q^g$ is a polynomial of degree $2g$ with coefficients

$$(2.4) \quad l_n = \frac{1}{q-1} \left(\sum_{\mathcal{D} \in \text{Cl}(n)} q^{l(\mathcal{D})} - (q+1) \sum_{\mathcal{D} \in \text{Cl}(n-1)} q^{l(\mathcal{D})} + q \sum_{\mathcal{D} \in \text{Cl}(n-2)} q^{l(\mathcal{D})} \right).$$

This polynomial has a factorization,

$$(2.5) \quad L_{\mathcal{C}}(X) = \prod_{\nu=1}^{2g} (X - \omega_{\nu}).$$

In §4, we show that the zeros ω_{ν} have absolute value \sqrt{q} .

3. THE TWO-VARIABLE ZETA FUNCTION

In [6], Pellikaan defines a two-variable zeta function $\zeta_{\mathcal{C}}(s, t)$ that specializes to the zeta function $\zeta_{\mathcal{C}}(s)$ of \mathcal{C} at $t = 1$. For $\text{Re } t < \text{Re } s < 0$, this function is defined by

$$\zeta_{\mathcal{C}}(s, t) = \frac{q^{(g-1)s}}{q^t - 1} \sum_{n=-\infty}^{\infty} q^{-ns} \sum_{\mathcal{D} \in \text{Cl}(n)} q^{tl(\mathcal{D})}.$$

By Theorem 2.1, $n = \deg \mathcal{D} = g - 1 - l(\mathcal{K} - \mathcal{D}) + l(\mathcal{D})$, so that

$$\zeta_{\mathcal{C}}(s, t) = \frac{1}{q^t - 1} \sum_{n=-\infty}^{\infty} \sum_{\mathcal{D} \in \text{Cl}(n)} q^{(t-s)l(\mathcal{D}) + sl(\mathcal{K} - \mathcal{D})}.$$

From this we deduce the functional equation $\zeta_{\mathcal{C}}(t - s, t) = \zeta_{\mathcal{C}}(s, t)$.

For $\mathcal{C} = \mathbb{P}^1$, we compute as in (2.3),

$$\zeta_{\mathbb{P}^1}(s, t) = \frac{1}{(1 - q^{t-s})(q^s - 1)}.$$

Thus $\zeta_{\mathbb{P}^1}(s, t)$ is meromorphic and $\zeta_{\mathbb{P}^1}(s, 1) = \zeta_{\mathbb{P}^1}(s)$. The poles of $\zeta_{\mathbb{P}^1}$ are simple, located in (s, t) -space at the planes $s = 0 + k \frac{2\pi i}{\log q}$ and $s = t + k \frac{2\pi i}{\log q}$, for $k \in \mathbb{Z}$.

In general, we have

$$\zeta_{\mathcal{C}}(s, t) = \sum_{n=0}^{2g-2} q^{-(n+1-g)s} \sum_{\mathcal{D} \in \text{Cl}(n)} \frac{q^{tl(\mathcal{D})} - q^{t \max\{0, n+1-g\}}}{q^t - 1} + h_{\mathcal{C}} \zeta_{\mathbb{P}^1}(s, t).$$

We find that $\zeta_{\mathcal{C}}(s, t)$ also has a meromorphic continuation, with the same poles as $\zeta_{\mathbb{P}^1}(s, t)$, and $\zeta_{\mathcal{C}}(s, 1) = \zeta_{\mathcal{C}}(s)$. This shows, in particular, that $\zeta_{\mathcal{C}}(1 - s) = \zeta_{\mathcal{C}}(s)$. We obtain $\zeta_{\mathcal{C}}(s, t) = q^{-gs} L_{\mathcal{C}}(q^s, q^t) \zeta_{\mathbb{P}^1}(s, t)$, where

$$(3.1) \quad L_{\mathcal{C}}(X, Y) = \frac{h_{\mathcal{C}} X^g + (X - Y)(X - 1)}{X^{2g-2-n}} \sum_{n=0}^{2g-2} X^{2g-2-n} \sum_{\mathcal{D} \in \text{Cl}(n)} \frac{Y^{l(\mathcal{D})} - Y^{\max\{0, n+1-g\}}}{Y - 1}.$$

Thus $L_{\mathcal{C}}(X, Y)$ is a polynomial in X and Y ,

$$L_{\mathcal{C}}(X, Y) = X^{2g} + l_1(Y)X^{2g-1} + \cdots + l_{2g-1}(Y)X + Y^g,$$

where the coefficients are given by

$$(3.2) \quad l_n(Y) = \frac{1}{Y-1} \left(\sum_{\mathcal{D} \in \text{Cl}(n)} Y^{l(\mathcal{D})} - (Y+1) \sum_{\mathcal{D} \in \text{Cl}(n-1)} Y^{l(\mathcal{D})} + Y \sum_{\mathcal{D} \in \text{Cl}(n-2)} Y^{l(\mathcal{D})} \right).$$

Remark 3.1. From (2.4), we see that $L_{\mathcal{C}}(X, Y)$ is obtained from the formula for $L_{\mathcal{C}}(X)$ by replacing q by Y . However, $L_{\mathcal{C}}(X, Y)$ is not determined by $L_{\mathcal{C}}(X)$, see [6, Example 3.7]. In particular, $L_{\mathcal{C}}(X, Y)$ is in general not determined by the number of points on $\mathcal{C}(\mathbb{F}_{q^n})$ for finitely (or infinitely) many values of n .

3.1. A Criterion for Rationality.

Lemma 3.2. *Let \mathcal{D} be a divisor with $\deg \mathcal{D} \geq 1$ and $l(\mathcal{D}) \geq \deg \mathcal{D} + 1$. Then \mathcal{C} is isomorphic to \mathbb{P}^1 .*

Proof. If $\deg \mathcal{D} = 1$ and $l(\mathcal{D}) \geq 2$, then we can find two independent functions α and β such that $\mathcal{D} + (\alpha)$ and $\mathcal{D} + (\beta)$ are positive. Since these divisors have degree 1, each consists of a single point, say v and w , respectively. Then $(\alpha/\beta) = v - w$. Since α and β are independent, the function α/β is nonconstant from \mathcal{C} to \mathbb{P}^1 , and in particular, $v \neq w$. If $\alpha/\beta(a) = \infty$ then $a = w$. Moreover, if $\alpha/\beta(a) = \alpha/\beta(b) \neq \infty$, then the divisor of $\alpha/\beta - \alpha/\beta(a)$ equals $(a) - (w) = (b) - (w)$, hence $a = b$. We conclude that α/β is an isomorphism of \mathcal{C} with \mathbb{P}^1 .

Let now \mathcal{D} be a divisor of degree $d \geq 2$ with $l(\mathcal{D}) \geq d + 1$. Let $\alpha_0, \alpha_1, \dots, \alpha_d$ be $d + 1$ independent functions in $L(\mathcal{D})$ (see Theorem 2.1) and let v be a valuation where some functions α_i have a pole. Without loss of generality, assume that among the α_i 's, the function α_d has a pole of maximum order at v . Then we can find constants λ_i (in the algebraic closure $\bar{\mathbb{F}}_q$) such that $\alpha_i - \lambda_i \alpha_d$ has a pole of lower order at v , for $0 \leq i \leq d - 1$. There are d such functions, they are independent and they lie in $L(\mathcal{D} - v)$. Thus the divisor $\mathcal{D} - v$ has degree $d - 1$ and $l(\mathcal{D} - v) \geq d$. Continuing this way, we find a divisor \mathcal{D}' of degree 1 with $l(\mathcal{D}') \geq 2$. We conclude that $\mathcal{C} = \mathbb{P}^1$ be the first part of the proof. \square

Note that we may have to extend the field of constants to find an isomorphism of \mathcal{C} with \mathbb{P}^1 .

It follows that if \mathcal{C} has genus $g \geq 1$ and $\deg \mathcal{D} \geq 1$, then $l(\mathcal{D}) \leq \deg(\mathcal{D})$. By Theorem 2.1, this means that $l(\mathcal{K} - \mathcal{D}) \leq g - 1$. For \mathcal{D} instead of $\mathcal{K} - \mathcal{D}$, and using that $\deg \mathcal{K} = 2g - 2$, we conclude:

Corollary 3.3. *Let \mathcal{C} have genus $g \geq 1$. Then $l(\mathcal{D}) \leq g - 1$ for $\deg \mathcal{D} \leq 2g - 3$.*

Remark 3.4. Naumann refers for this corollary to the stronger statement [6, Prop. 3.5], and Pellikaan refers to Clifford’s theorem in [8] for a proof. As Naumann points out, Pellikaan quotes this proposition with a small mistake.

3.2. Naumann’s Theorem. We present Naumann’s argument in [4] that the numerator of $\zeta_{\mathcal{C}}(s, t)$ is an irreducible polynomial. Thus the zeros of $\zeta_{\mathcal{C}}(s)$ lie in an irreducible algebraic family $L_{\mathcal{C}}(X, Y) = 0$.

Lemma 3.5. *Let \mathcal{C} have genus $g \geq 1$. Then the top term of $L_{\mathcal{C}}(X, Y)$ as a polynomial in Y is $(1 - X)Y^g$.*

Proof. Consider $\sum_{\mathcal{D} \in \text{Cl}(n)} Y^{l(\mathcal{D})}$. For $n \geq 2g - 1$, we obtain the value $h_{\mathcal{C}}Y^{n+1-g}$ for this sum, and for $n = 2g - 2$, we obtain $h_{\mathcal{C}}Y^{g-1} + Y^{g-1}(Y - 1)$, since $l(\mathcal{D}) = g$ only for the canonical class, and otherwise, $l(\mathcal{D}) = g - 1$. By Corollary 3.3, the sum is $O(Y^{g-1})$ for $n \leq 2g - 3$. By formula (3.2), it follows that $l_{2g}(Y) = Y^g$, $l_{2g-1}(Y) = -Y^g + O(Y^{g-1})$ and $l_n(Y) = O(Y^{g-1})$ for $n \leq 2g - 2$. We conclude that $L_{\mathcal{C}}(X, Y) = (1 - X)Y^g + O(Y^{g-1})$. \square

Note that if a polynomial $F(X, Y)$ has a factorization $F(X, Y) = f(X, Y)g(X, Y)$ in polynomials in X with rational coefficients in Y , or in polynomials in Y with rational coefficients in X , then we can assume by Gauss’s lemma that f and g are polynomials in both X and Y . Hence if F is irreducible in $\mathbb{C}[X, Y]$ then it is irreducible in $\mathbb{C}(X)[Y]$ and in $\mathbb{C}(Y)[X]$.

Theorem 3.6. *The polynomial $L_{\mathcal{C}}(X, Y)$ is irreducible.*

Proof. Let $L_{\mathcal{C}} = fg$ be a factorization in polynomials in X and Y . Since the top coefficient of $L_{\mathcal{C}}(X, Y)$ as a polynomial in Y is irreducible by Lemma 3.5, we can assume that the top coefficient of f as a polynomial in Y is constant. Thus we have that $\deg_Y f(X, Y) = \deg_Y f(1, Y)$. Since $f(1, Y)g(1, Y) = h_{\mathcal{C}}$ by (3.1), we find that $\deg_Y f(X, Y) = 0$. Hence $f(X, Y) = a(X)Y^0$ for some polynomial a . Being the top coefficient of f as a polynomial in Y , we find that $a(X)$ is constant. We conclude that $L_{\mathcal{C}}(X, Y)$ is irreducible. \square

Remark 3.7. It is natural to ask about the geometry of the curve $L_{\mathcal{C}}(X, Y) = 0$. Its degree in X is $2g$, and its degree in Y is g . We do not know if this curve is nonsingular, or what its genus is. We only know that the fiber above $Y = q$ satisfies the Riemann hypothesis: $|X| = \sqrt{q}$ for each point (X, q) on the curve.

Remark 3.8. For an abelian cover \mathcal{C}' of \mathcal{C} , $L_{\mathcal{C}}(X)$ is a factor of $L_{\mathcal{C}'}(X)$. Thus we have the curious situation that the zeros of $\zeta_{\mathcal{C}'}$ lie in an irreducible family, and a subset of these zeros, the zeros of $\zeta_{\mathcal{C}}$, lie in another irreducible family.

4. THE RIEMANN HYPOTHESIS FOR \mathcal{C}

By the Euler product (2.2),

$$-\frac{1}{\log q} \frac{\zeta'_{\mathcal{C}}}{\zeta_{\mathcal{C}}}(s) = 1 - g + \sum_v \deg v \sum_{n=1}^{\infty} q^{-ns \deg v} = 1 - g + \sum_{n=1}^{\infty} N_{\mathcal{C}}(n)q^{-ns},$$

where $N_{\mathcal{C}}(n) = \sum_{\deg v|n} \deg v$ is the number of points on \mathcal{C} defined over \mathbb{F}_{q^n} . On the other hand, by (2.5), this function equals $1 - g + \sum_{n=1}^{\infty} (q^n - \omega_1^n - \dots - \omega_{2g}^n + 1)q^{-ns}$. Thus we find

$$N_{\mathcal{C}}(n) = q^n - \omega_1^n - \dots - \omega_{2g}^n + 1.$$

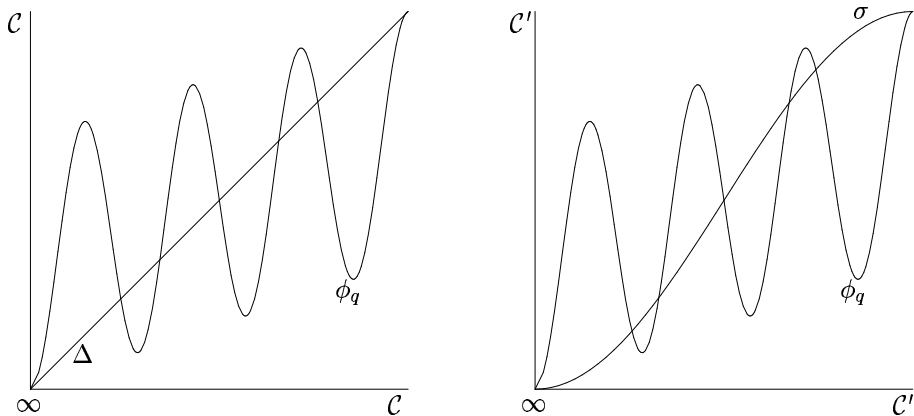


FIGURE 1. (a) The graph of Frobenius intersected with the diagonal. (b) The graph of Frobenius on C' intersected with the graph of σ .

Remark 4.1. It follows that ζ_C can be computed by counting the number of points on C over \mathbb{F}_{q^n} for $n = 1, \dots, g$.

The zeros of ζ_C are located at $s = \log_q \omega_\nu$. The Riemann hypothesis for C can be formulated as $|\omega_\nu| = \sqrt{q}$ for $\nu = 1, \dots, 2g$. It follows from the Riemann hypothesis that

$$|N_C(n) - q^n - 1| \leq 2gq^{n/2}.$$

Conversely, we have the following lemma, which states in particular that it suffices to prove (4.1) below for all even n .

Lemma 4.2. *If for every $\varepsilon > 0$ there exist a number $B > 0$ and a natural number m such that*

$$(4.1) \quad |N_C(n) - q^n - 1| \leq Bq^{n(1/2+\varepsilon)} \quad \text{for every } n = m, 2m, 3m, \dots,$$

then the Riemann hypothesis holds for C .

Proof. Let $\varepsilon > 0$. By Diophantine approximation, we can find infinitely many n such that $\operatorname{Re} \omega_\nu^{nm} \geq |\omega_\nu|^{nm}/2$ for $\nu = 1, \dots, 2g$. Then

$$|N_C(nm) - q^{nm} - 1| \geq \frac{1}{2} \max_\nu |\omega_\nu|^{nm}.$$

Letting $n \rightarrow \infty$, we find that $|\omega_\nu| \leq q^{1/2+\varepsilon}$ for every ν . Since this holds for every $\varepsilon > 0$, we obtain $|\omega_\nu| \leq q^{1/2}$. By the functional equation for ζ_C , it follows that $|\omega_\nu| = q^{1/2}$ for every ν . \square

4.1. The Graph of Frobenius. Figure 1(a) depicts the graph $Y = \phi_q(X)$. The intersection with the diagonal $\Delta: Y = X$ gives the points (x, x) in $C \times C$ with $\phi_q(x) = x$. These are the points on C defined over \mathbb{F}_q , and their number is $N_C(1)$. We assume that there is at least one point on the intersection, which we denote by (∞, ∞) . We write v_∞ for the corresponding valuation of degree 1 of K .

Remark 4.3. The Frobenius automorphism is smooth, since it is a polynomial map. Also, its derivative vanishes, so our intuition says that this map should be constant,

or at least locally constant. Being a polynomial of degree q , it seems to be a q -to-one map, but in fact, it is one-to-one. Figure 1 emphasizes the smoothness and ignores the injectivity of Frobenius.

The functions defined over \mathbb{F}_q with a pole of order at most m at ∞ and no other poles form an \mathbb{F}_q -vector space $L_m = L(mv_\infty)$. By Theorem 2.1, its dimension satisfies

$$(4.2) \quad m + 1 - g \leq l_m \leq m + 1, \quad \text{and} \quad l_m = m + 1 - g \text{ for } m > 2g - 2.$$

Clearly, L_{m+1} contains L_m as a subspace. Also, $l_{m+1} \leq l_m + 1$, since for two functions $f, g \in L_{m+1}$ for which $f \notin L_m$, we can find a constant $\lambda \in \mathbb{F}_q$ such that $g - \lambda f \in L_m$. Therefore we can find a basis s_1, \dots, s_{l_m} for L_m such that $v_\infty(s_{i+1}) < v_\infty(s_i)$, that is, the order of the pole of s_i at ∞ increases with i . Given $k \geq 0$, we choose coefficients $a_i \in L_k$ to form

$$f(X, Y) = \sum_{i=1}^{l_m} a_i(X) s_i(Y).$$

The restriction of $f(X, Y)$ to the graph of Frobenius is $f|_\phi(X) = f(X, \phi_q(X))$. The map $f \mapsto f|_\phi$ is \mathbb{F}_q -linear. Note that $s_i(\phi_q(X)) = s_i^q(X)$, since s_i is defined over \mathbb{F}_q . Hence $f|_\phi \in L_{k+qm}$. That is, $f|_\phi$ only has a pole at ∞ , of order at most $k + qm$.

Lemma 4.4. *For $k < q$, the map $f \mapsto f|_\phi$ is injective, and hence an isomorphism onto its image.*

Proof. Assume $f \mapsto 0$, that is, $f|_\phi = \sum_{i=1}^{l_m} a_i s_i^q = 0$. Consider the order of the pole of $f|_\phi$ at ∞ . If $a_i \neq 0$, then $v_\infty(a_i s_i^q) \leq qv_\infty(s_i) \leq -q + qv_\infty(s_j)$ for every $j < i$. Further, $v_\infty(a_j s_j^q) \geq -k + qv_\infty(s_j) > -q + qv_\infty(s_j)$. Hence the pole of the nonzero term of highest order in $f|_\phi$ is not cancelled by the pole of any of the other terms. It follows that the highest nonzero term vanishes. We conclude that there is no highest nonzero term, and hence $f = 0$. \square

We take the coefficients a_i to be p^μ -th powers, for $p^\mu < q$, so that $f|_\phi$ is a p^μ -th power. Hence the coefficients are of the form

$$a_i = b_i^{p^\mu}.$$

We choose $b_i \in L_n$, so that $a_i \in L_{p^\mu n}$. The space of functions $f(X, Y)$ constructed this way has dimension $l_n l_m$. To be able to apply Lemma 4.4, we assume that

$$(4.3) \quad p^\mu n < q,$$

so that also the space of functions $f|_\phi$, i.e., the image of the map of Lemma 4.4, has dimension $l_n l_m$.

We can also restrict f to the diagonal: $f|_\Delta(X) = f(X, X)$. We obtain the two restriction maps,

$$(4.4) \quad f|_\phi \longleftarrow f \longrightarrow f|_\Delta,$$

where the left arrow denotes the isomorphism of Lemma 4.4. Using the inverse $f|_\phi \mapsto f$, we obtain a linear map $f|_\phi \mapsto f|_\Delta$. Suppose that $f|_\Delta = 0$ and $f|_\phi \neq 0$. Then we have a function $f|_\phi$ on \mathcal{C} , obtained as the restriction to $Y = \phi_q(X)$ of a function on $\mathcal{C} \times \mathcal{C}$ that vanishes on the diagonal. Apart from (∞, ∞) , the diagonal intersects the graph of Frobenius in $N_{\mathcal{C}}(1) - 1$ points. Since $f|_\phi$ is a p^μ -th power, this function has at least $p^\mu(N_{\mathcal{C}}(1) - 1)$ zeros, counted with multiplicity. Comparing

with the order of the pole of $f|_\phi$, we find the inequality $N_C(1) \leq 1 + n + \frac{q}{p^\mu}m$. By (4.3), we obtain

$$(4.5) \quad N_C(1) \leq \frac{q}{p^\mu}(m+1).$$

In particular, for given μ , we find the best bound for $N_C(1)$ when m is as small as possible.

Example 4.5. For genus zero, we take $f(X, Y) = X^{p^\mu} - Y^{p^\mu}$. Then $f|_\phi(X) = X^{p^\mu} - X^{qp^\mu}$ and $f|_\Delta(X) = 0$. The function $f|_\phi$ has a pole at infinity of order qp^μ , and at least $p^\mu(N_{\mathbb{P}^1}(1) - 1)$ zeros, counted with multiplicity. Thus the number of points on the projective line over \mathbb{F}_q satisfies $N_{\mathbb{P}^1}(1) \leq q+1$. In fact, equality holds, as is well known. This is a direct verification of the Riemann hypothesis for \mathbb{P}^1 . We use it in (4.8) below to derive the Riemann hypothesis for \mathcal{C} .

For higher genus, it is much harder to explicitly find a function f such that $f|_\Delta = 0$ and $f|_\phi \neq 0$, but we can prove that it exists. Assume that $n, m \geq g$. Then $l_n l_m \geq (n+1-g)(m+1-g)$ by (4.2). The functions $f|_\Delta$ lie in $L_{p^\mu n+m}$. To assure the existence of a nontrivial function f such that $f|_\Delta = 0$, we choose n and m so that $(n+1-g)(m+1-g) > l_{p^\mu n+m}$, since then the kernel of the map $f|_\phi \mapsto f|_\Delta$ is nontrivial. Since $p^\mu n + m > 2g - 2$, this means that we want $(n+1-g)(m+1-g) > p^\mu n + m + 1 - g$, or equivalently,

$$(4.6) \quad (n-g)(m+1-g-p^\mu) > p^\mu g.$$

Since we want to choose m as small as possible, we choose n as large as possible. The largest value for n such that (4.3) is satisfied is $n = qp^{-\mu} - 1$. We thus obtain from (4.6) a lower bound for m , which we can write as

$$\frac{q}{p^\mu}(m+1) > q + g \left(\frac{q}{p^\mu} + \frac{p^\mu}{1 - (g+1)p^\mu/q} \right) > q + g \left(\frac{q}{p^\mu} + p^\mu \right).$$

We conclude that the upper bound for $N_C(1)$ that we can derive from (4.5) is best possible if $q/p^\mu = p^\mu$. Therefore, we assume that q is an even power of p , as we may by Lemma 4.2, and we choose μ such that $p^\mu = \sqrt{q}$. Then $n = \sqrt{q} - 1$ and we find

$$m+1 > \sqrt{q} + 2g + \frac{g(g+1)}{\sqrt{q} - (g+1)}.$$

For $q > (g+1)^4$, this inequality is satisfied for $m+1 = \sqrt{q} + 2g + 1$. Then clearly $n, m \geq g$. By (4.5), we obtain the following theorem:

Theorem 4.6. *For $q > (g+1)^4$, a square, we have*

$$N_C(1) \leq q + (2g+1)\sqrt{q},$$

where g is the genus of \mathcal{C} .

Note that the above argument depends on the existence of a point ∞ on $\mathcal{C}(\mathbb{F}_q)$. If such a point does not exist, then $N_C(1) = 0$ and the inequality for $N_C(1)$ is trivially satisfied.

4.2. Frobenius as Symmetries of a Cover. We also need a generalization of Theorem 4.6 to Galois covers. Let

$$(4.7) \quad \mathcal{C}' \longrightarrow \mathcal{C} \longrightarrow \mathbb{P}^1$$

be the Galois cover corresponding to the Galois closure of K over $\mathbb{F}_q(T)$. Let G be the Galois group (fundamental group) of the cover $\mathcal{C}' \rightarrow \mathbb{P}^1$.

Lemma 4.7. *Let K be the function field of a curve \mathcal{C} , and let \mathcal{C}' be a cover of \mathcal{C} with function field L such that L/K is a Galois extension. For every automorphism $\sigma \in \text{Gal}(L/K)$, we have an induced algebraic action of σ on \mathcal{C}' .*

Proof. Write L as $K[X]/(m)$ for some function $x = X + (m) \in L$ with defining polynomial m , and let $\sigma \in \text{Gal}(L/K)$. Since $\sigma(x) \in L$, we can find a polynomial f with coefficients in K such that $\sigma(x) = f(X) + (m)$. Thus the action of σ on \mathcal{C}' is algebraic, induced by $X \mapsto f(X)$. \square

For $\sigma \in G$, we define

$$N_{\mathcal{C}'}(1, \sigma) = |\{x \in \mathcal{C}'(\overline{\mathbb{F}}_q) : x \text{ projects to } \mathbb{P}^1(\mathbb{F}_q) \text{ and } \phi_q(x) = \sigma(x)\}|,$$

where ϕ_q is the Frobenius automorphism.

Lemma 4.8. *For $q > (g + 1)^4$, a square, we have*

$$N_{\mathcal{C}'}(1, \sigma) \leq q + (2g' + 1)\sqrt{q},$$

where g' is the genus of \mathcal{C}' .

Proof. Let X and Y again denote the coordinates on $\mathcal{C}' \times \mathcal{C}'$; see Figure 1(b). As in (4.4), we have the restrictions

$$f|_{\phi} \longleftarrow f \longrightarrow f|_{\sigma},$$

where $f|_{\sigma}(X) = f(X, \sigma(X))$ is the restriction of $f(X, Y)$ to the graph of σ . Clearly, if $f|_{\sigma}$ vanishes, then $f|_{\phi}$ vanishes at the points that are counted in $N_{\mathcal{C}'}(1, \sigma)$. The rest of the argument is as before, applied to \mathcal{C}' and the homomorphism $f|_{\phi} \mapsto f|_{\sigma}$. \square

Let L/K be a Galois extension of fields and let w be a valuation of L , and v (a multiple of) its restriction to K . We recall the *decomposition group*

$$Z_{w/v} = \{\sigma \in \text{Gal}(L/K) : w(\sigma x) > 0 \text{ if } w(x) > 0\}$$

of continuous automorphisms, and the *ramification group*, its subgroup

$$T_{w/v} = \{\sigma \in Z_{w/v} : w(x - \sigma x) > 0 \text{ if } w(x) \geq 0\}$$

of automorphisms that act trivially on the field of residue classes. The factor group $Z_{w/v}/T_{w/v}$ is isomorphic to the Galois group of the residue class field extension of w over v , and is generated by Frobenius. The order of $T_{w/v}$ is $e_{w/v}$ (see (2.1)), so there are $e_{w/v}$ automorphisms in $Z_{w/v}$ that induce Frobenius on the residue class field of w .

Theorem 4.9. *The curve \mathcal{C} satisfies the Riemann hypothesis. That is, $|\omega_{\nu}| = q^{1/2}$.*

Proof. In the situation of (4.7), consider the sum

$$\sum_{\sigma \in G} N_{\mathcal{C}'}(1, \sigma).$$

Above every point t of $\mathbb{P}^1(\mathbb{F}_q)$, we have $|G|/e$ points of $\mathcal{C}'(\overline{\mathbb{F}}_q)$, where e is the order of ramification of any of the associated valuations in \mathcal{C}' . Further, for a point t' of

\mathcal{C}' above t , we have e different automorphisms in G that induce Frobenius on the residue class field. Hence in the sum, each point of $\mathbb{P}^1(\mathbb{F}_q)$ is counted $|G|$ times. Since $\mathbb{P}^1(\mathbb{F}_q)$ has $q + 1$ points, we obtain

$$(4.8) \quad \sum_{\sigma \in G} N_{\mathcal{C}'}(1, \sigma) = |G|(q + 1).$$

By Lemma 4.8, we obtain for each $\tau \in G$,

$$N_{\mathcal{C}'}(1, \tau) = |G|(q + 1) - \sum_{\sigma \neq \tau} N_{\mathcal{C}'}(1, \sigma) \geq q - (|G| - 1)(2g' + 1)\sqrt{q} + |G|.$$

Let H be the subgroup of G of covering transformations that act trivially on \mathcal{C} . By the same reasoning as above for \mathbb{P}^1 , we obtain

$$\sum_{\sigma \in H} N_{\mathcal{C}'}(1, \sigma) = |H|N_{\mathcal{C}}(1).$$

It follows that $N_{\mathcal{C}}(1) \geq q - (|G| - 1)(2g' + 1)\sqrt{q} + |G|$. Combined with the upper bound of Theorem 4.6, we deduce the Riemann hypothesis for \mathcal{C} by Lemma 4.2. \square

REFERENCES

- [1] Artin, E., *Quadratische Körper im Gebiete der höheren Kongruenzen I, II*, Math. Zeitschr. **19** (1924).
- [2] Bombieri, E., *Counting points on curves over finite fields*, Seminaire Bourbaki, no. 430 (1973).
- [3] Hasse, H., *Ueber Kongruenzzetafunktionen*, S. Ber. Preuß. Ak. Wiss. 1934, p. 250.
- [4] Naumann, N., *On the irreducibility of the two variable zeta-function for curves over finite fields*, C. R. Acad. Sci. Paris Sér. I *Math.* **336** (2003), 289–292, and [arXiv:math.AG/0209092](https://arxiv.org/abs/math/0209092), 2002.
- [5] Stepanov, S. A., *On the number of points of a hyperelliptic curve over a finite prime field*, Izv. Akad. Nauk SSSR, Ser. Math. **33** (1969), pp. 1103–1114.
- [6] Pellikaan, R., On special divisors and the two variable zeta function of algebraic curves over finite fields, in: *Arithmetic, Geometry and Coding Theory*, Proceedings of the International Conference held at CIRM, Luminy, France, 1993, pp. 175–184.
- [7] Ramakrishnan, D., Valenza, R. J., *Fourier Analysis on Number Fields*, Graduate Texts in Mathematics **186**, Springer-Verlag, 1998.
- [8] Stichtenoth, H., *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.
- [9] Weil, A., *Number of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508; reprinted in [12, vol. I, pp. 399–410].
- [10] Weil, A., *Courbes algébriques et variétés abéliennes*, Hermann, Paris, 1971. (Combines in one volume *Sur les courbes algébriques et les variétés qui s'en déduisent*, Pub. Inst. Math. Strasbourg VII (1945), pp. 1–85, and *Variétés Abéliennes et courbes algébriques*, Actualités scientifiques et industrielles **1041**, Hermann, Paris, 1948.)
- [11] Weil, A., *Basic Number Theory*, Springer Classics in Mathematics, 1995.
- [12] Weil, A., *André Weil: Oeuvres Scientifiques* (Collected Papers), vols. I, II and III, 2nd ed., Springer-Verlag, Berlin and New York, 1980.

DEPARTMENT OF MATHEMATICS, UTAH VALLEY UNIVERSITY, OREM, UT 84058-5999
E-mail address: vanframa@uvsc.edu