Available online at www.sciencedirect.com
ScienceDirect
Journal of Number Theory 128 (2008) 2053–2062
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

On some questions related to the Gauss conjecture for function fields

Yves Aubry [a], Régis Blache [b,*]

[a] *Institut de Mathématiques de Toulon, Université du Sud Toulon-Var, France*
[b] *Equipe AOC, IUFM de Guadeloupe, Guadeloupe*

Received 19 April 2007; revised 8 October 2007

Available online 28 January 2008

Communicated by D. Wan

Abstract

We show that, for any finite field $\mathbb{F}_q$, there exist infinitely many real quadratic function fields over $\mathbb{F}_q$ such that the numerator of their zeta function is a separable polynomial. As pointed out by Anglès, this is a necessary condition for the existence, for any finite field $\mathbb{F}_q$, of infinitely many real function fields over $\mathbb{F}_q$ with ideal class number one (the so-called Gauss conjecture for function fields). We also show conditionally the existence of infinitely many real quadratic function fields over $\mathbb{F}_q$ such that the numerator of their zeta function is an irreducible polynomial.

MSC: 11R29; 11R58; 11R11; 14H05

Keywords: Functions fields; Gauss conjecture; Zeta functions; Jacobian; Hyperelliptic curves; Finite fields

1. Introduction

According to a conjecture of Gauss, there exist infinitely many real quadratic number fields having a ring of integers which is a principal ideal domain, i.e. with class number one. We shall study a related conjecture for functions fields over a finite field.

Let q be a power of a prime p, and $\mathbb{F}_q$ a finite field with q elements. A *function field over* $\mathbb{F}_q$ is a finite extension K of a field of rational function $\mathbb{F}_q(x)$ (where x is transcendental over $\mathbb{F}_q$)

* Corresponding author.
E-mail addresses: yaubry@univ-tln.fr (Y. Aubry), rblache@iufm.univ-ag.fr (R. Blache).

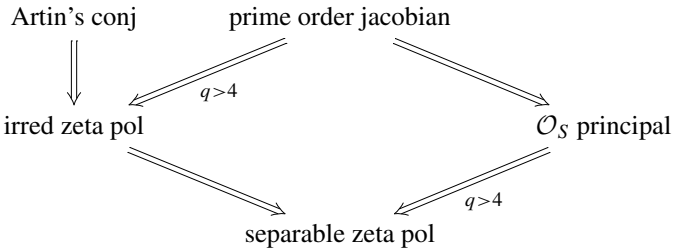
0022-314X/$ – see front matter
doi:10.1016/j.jnt.2007.10.014

with full constant field $\mathbb{F}_q$. The extension $K/\mathbb{F}_q(x)$ is said to be *quadratic* when we have $[K : \mathbb{F}_q(x)] = 2$, and *real* when the infinite prime $(\frac{1}{x})$ of $\mathbb{F}_q(x)$ splits in K. If the prime $(\frac{1}{x})$ doesn't split we say that $K/\mathbb{F}_q(x)$ is *imaginary*. By abuse of language, we will say that the quadratic function field K is *real* when one can find a transcendental element $z \in K$ such that the extension $K/\mathbb{F}_q(z)$ is quadratic and real. If S denotes the set of places in K above the place at infinity, we denote by $\mathcal{O}_S$ the ring of regular functions of K outside S. Then the *Gauss conjecture for function fields* asserts that, for any finite field $\mathbb{F}_q$, there exist infinitely many real quadratic function fields with full constant field $\mathbb{F}_q$ such that $\mathcal{O}_S$ has ideal class number one. This is the main conjecture BC discussed by Lachaud and Vladut in [6], among some weaker ones.

Using Iwasawa theory, Bruno Anglès showed in [1] that if K is a real quadratic function field over the finite field $\mathbb{F}_q$ with $q \geqslant 5$ having a principal ring of integers, then the numerator of its zeta function (called the zeta polynomial) is a polynomial with only simple roots; in other words is a separable polynomial. Thus, Anglès asks the following question which is a necessary condition for the Gauss conjecture to hold true: is there exist infinitely many real quadratic function fields over $\mathbb{F}_q$ with zeta polynomial being separable? We give a positive answer to this question considering the action of the Frobenius on the $\mathbb{F}_2$-vector space of 2-torsion points of the jacobian of certain hyperelliptic curves. Note that the separability of this polynomial is equivalent for the endomorphism ring of the jacobian to be commutative, see [8].

Then we consider if it remains true when we ask the zeta polynomial to be irreducible. This problem is stronger than the previous one, and it has been studied by various authors (see [2,5]) from a different point of view: it is known that for a family of curves of fixed genus g having large monodromy, the zeta polynomial is "generically" irreducible. More precisely, if the parameter space is d-dimensional, the number of curves having a zeta polynomial whose splitting field is not the biggest possible is $O(q^{d-\gamma} \ln q)$, where γ is a positive constant depending on g. Unfortunately, this result is of no use when q is fixed and g gets large. Thus it cannot be used to solve our question. Note that there are also unpublished results of Katz about irreducibility of the L-functions of elliptic curves over function fields, providing similar results in this case.

Here we show that assuming Artin's primitive root conjecture, then for any $q > 4$ there exist infinitely many (real, quadratic) function fields having an irreducible zeta polynomial. On the other hand, we remark that the existence of infinitely many real quadratic function fields with prime divisor class number (i.e. such that the order of the group of rational divisor classes $\mathrm{Pic}^0(K)$ of K is prime) implies the previous ones, as quoted in the following figure



The paper is organized as follows. In Section 2, we give some notations and we recall some basic facts about ideal class numbers, divisor class numbers and regulators of real quadratic function fields. Then, we recall the result of Anglès (Proposition 4.4 of [1]) which is the starting-point of the paper. Section 3 is devoted to the main result, namely the answer to the question

of Anglès. In Section 4, we give a conditional answer to the related irreducibility problem, and compare this result with previously known results in the literature.

2. Structure of rings of S-integers

In this section we recall well-known facts about rings of S-integers in function fields (see [7] for more details), and we introduce the question of Anglès.

Let $\mathbb{F}_q$ be a finite field and let us fix $\mathbb{F}_q(x)$ a one-variable rational function field over $\mathbb{F}_q$. A *real quadratic extension* K over $\mathbb{F}_q$ is a degree 2 extension of $\mathbb{F}_q(x)$ such that the infinite place ∞ of $\mathbb{F}_q(x)$ (corresponding to the pole of x) splits in K: there are two places ∞_1 and ∞_2 above ∞ in K.

Recall that for X any (smooth, projective) curve over $\mathbb{F}_q$ having K as function field, we can define for any $k \geqslant 1$ the number $N_k(X)$ of $\mathbb{F}_{q^k}$ rational points of X, and encode these numbers into the *zeta function of* K

$$Z_K(T) = \exp\left(\sum_{k\geqslant 1} N_k(X)\frac{T^k}{k}\right).$$

Weil's theorem (the Riemann hypothesis over finite fields) says that this function is actually a rational function, having denominator $(1-T)(1-qT)$, and whose numerator is a degree $2g$ polynomial in $\mathbb{Z}[T]$, where g is the *genus* of K. We shall denote this polynomial by L_K, and call it the *zeta polynomial of* K.

The *ring of S-integers* $\mathcal{O}_S$ of K (with respect to ∞) is the integral closure of the ring of polynomials $\mathbb{F}_q[x]$ in K. It is also the ring of elements of K whose poles are in $S = \{\infty_1, \infty_2\}$. It is a Dedekind domain; we denote by $\mathrm{Cl}(\mathcal{O}_S)$ the ideal class group of $\mathcal{O}_S$ and by $h_{\mathcal{O}_S}$ the order of $\mathrm{Cl}(\mathcal{O}_S)$, called the ideal class number. Then, the ring $\mathcal{O}_S$ is a principal ideal domain if and only if $h_{\mathcal{O}_S} = 1$. We will say abusively in this case that K is *principal*.

Consider the Picard group $\mathrm{Pic}^0(K)$ of rational divisors of K of degree zero modulo the principal ones. It is well-known that the Picard group is isomorphic to the group of rational points over $\mathbb{F}_q$ of the jacobian J_K of the nonsingular projective algebraic curve over $\mathbb{F}_q$ associated to the function field K:

$$\mathrm{Pic}^0(K) \simeq J_K(\mathbb{F}_q).$$

The order of this group, called the divisor class number of K, is denoted by h_K and is equal to $L_K(1)$, the evaluation at 1 of the zeta polynomial of K since it is the number of rational points of the jacobian J_K.

Consider now the group $\mathrm{Div}_S^0(K)$ of divisors of K of degree zero with support in S. Since the places of S have degree 1, the divisors of $\mathrm{Div}_S^0(K)$ are of the form $n\infty_1 - n\infty_2$ with n an integer. Thus we have an isomorphism $\mathrm{Div}_S^0(K) \simeq \mathbb{Z}$. Furthermore, since a rational function of K whose support is contained in S lies in the group of units $\mathcal{O}_S^*$, it is clear that the group $\mathcal{P}_S(K)$ of principal divisors of K with support in S is isomorphic to $\mathcal{O}_S^*/\mathbb{F}_q^*$. The units theorem of Dirichlet tell us that

$$\mathcal{O}_S^* \simeq \mathbb{F}_q^* \times \langle \varepsilon \rangle$$

where ε is a function whose divisor is of the form $r_{\mathcal{O}_S}\infty_1 - r_{\mathcal{O}_S}\infty_2$ (ε is a fundamental unit) and $r_{\mathcal{O}_S}$ is called the *regulator* of K (with respect to ∞ or S). Thus, we have

$$R_S := \mathrm{Div}_S^0(K)/\mathcal{P}_S(K) \simeq \mathbb{Z}/r_{\mathcal{O}_S}\mathbb{Z}.$$

We have the following well-known exact sequence of groups:

$$0 \longrightarrow R_S \longrightarrow J_K \longrightarrow \mathrm{Cl}(\mathcal{O}_S) \longrightarrow 0.$$

It implies in particular the *Schmidt relation* for a real quadratic function field K:

$$r_{\mathcal{O}_S} h_{\mathcal{O}_S} = h_K.$$

Moreover, if we suppose that the ring $\mathcal{O}_S$ is a principal ideal domain, then this implies that $J_K(\mathbb{F}_q)$ is a cyclic group:

Proposition 1. *Let K be a real quadratic function field. We have the following*:

(i) *K is principal if and only if we have the isomorphism*

$$J_K(\mathbb{F}_q) \simeq R_S.$$

(ii) *If K is principal, then $J_K(\mathbb{F}_q)$ is a cyclic group.*
(iii) *If the group $J_K(\mathbb{F}_q)$ has prime order then K is principal.*

Proof. Assertion (i) follows from the exact sequence above, whereas assertion (ii) comes from the cyclicity of the group R_S.

To show assertion (iii), first remark that we must have $r_{\mathcal{O}_S} > 1$. Indeed if $r_{\mathcal{O}_S} = 1$, the divisor $\infty_1 - \infty_2$ is principal: thus it is the divisor of a rational function ε and since $[K : \mathbb{F}_q(\varepsilon)] = \deg \varepsilon = 1$, K must be a rational function field. Hence the Picard group $\mathrm{Pic}^0(K)$ is trivial and $J_K(\mathbb{F}_q)$ cannot have prime order. By the previous Schmidt relation, we obtain $h_{\mathcal{O}_S} = 1$. □

Bruno Anglès proved in [1] (Proposition 4.4) the following result.

Proposition 2. *Let K be a real quadratic extension of $\mathbb{F}_q(x)$ with $q > 4$. If K has ideal class number one, then the zeta polynomial of K is separable.*

Remark. The hypothesis $q > 4$ of the previous proposition is necessary. Indeed, we can provide counter-examples for each field $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_4$.

For instance, let us consider the example of the hyperelliptic curve X of genus 5 defined by the equation

$$y^2 = x^{12} + 2x^{11} + 2x^6 + x^5 + 2$$

over $\mathbb{F}_3$. The curve X has two rational points over $\mathbb{F}_3$, corresponding to the places above infinity, thus the function field $k(X)$ of X is a real quadratic function field. Moreover, the group of rational

points over $\mathbb{F}_3$ of its jacobian is cyclic of prime order (isomorphic to $\mathbb{Z}/139\mathbb{Z}$) and thus $k(X)$ has class number one by (iii) of Proposition 1. However the zeta polynomial $L_X(T)$ of X has multiple roots since we have

$$L_X(T) = \big(T^2 - 3T + 3\big)^2\big(T^6 + 4T^5 + 12T^4 + 23T^3 + 36T^2 + 36T + 27\big).$$

3. Construction of real quadratic function fields

In this section we shall construct infinitely many hyperelliptic curves in any odd characteristic, having a separable zeta polynomial. Then we show that, up to twisting, the function field of any of these curves can be considered as a real quadratic function field.

It is well-known that the zeta polynomial $L_K(T)$ of a function field K over $\mathbb{F}_q$ can be seen as the reciprocal polynomial of the characteristic polynomial of the Frobenius endomorphism acting on any of the Tate modules of the jacobian of K. Let $q > 4$ be the power of an odd prime; the reduction modulo 2 of $L_K(T)$ can then be read by looking at the action of the Frobenius on the $\mathbb{F}_2$-vector space of 2-torsion points of the jacobian. We begin by showing that for a wide family of curves, the reduction modulo 2 of $L_K(T)$ has only simple roots in an algebraic closure $\overline{\mathbb{F}}_2$ of $\mathbb{F}_2$.

Lemma 3. *Let g be a positive integer, and $f(x)$ be an irreducible polynomial in $\mathbb{F}_q[x]$ of degree $2g+1$. Consider the quadratic extension K of $\mathbb{F}_q(x)$ defined by the equation $y^2 = f(x)$. Then the zeta polynomial of K is separable.*

Proof. Let us remark that since f is irreducible, all its roots are simple and the function field K has genus g; hence the zeta polynomial L_K of K has degree $2g$. It is well-known that if ℓ is a prime number distinct from the characteristic of K, the Tate module $T_\ell(J_f)$ of the jacobian of K is a free $\mathbb{Z}_\ell$-module of rank $2g$, on which the Frobenius endomorphism F acts. We have the following relation between the characteristic polynomial χ of this endomorphism and the zeta polynomial L_K:

$$\chi(T) = T^{2g} L_K\left(\frac{1}{T}\right).$$

In order to prove the lemma, it suffices to prove that the polynomial χ has only simple roots.

Let us fix $\ell = 2$. Then we have

$$T_2(J_f)/2T_2(J_f) \simeq J_f[2],$$

the group of 2-torsion points of J_f. If $\alpha_1, \ldots, \alpha_{2g+1}$ are the roots of f in an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, it is easy to show that a basis of the $\mathbb{F}_2$-vector space $J_f[2]$ is given by the divisor classes

$$D_1 := \big[(\alpha_1, 0) - P_\infty\big], \quad \ldots, \quad D_{2g} := \big[(\alpha_{2g}, 0) - P_\infty\big]$$

where P_∞ is the unique point over the infinite place ∞ corresponding to the prime ideal $\frac{1}{x}$ of $\mathbb{F}_q(x)$ (note that ∞ ramifies in the extension $K/\mathbb{F}_q(x)$ since $\deg f$ is odd).

But, since f is irreducible over $\mathbb{F}_q$, we can reorder its roots such that $\alpha_2 = \alpha_1^q, \ldots, \alpha_1 = \alpha_{2g+1}^q$. Hence for $1 \leqslant i \leqslant 2g-1$, we have

$$F(D_i) = \big[\big(\alpha_i^q, 0\big) - P_\infty\big] = \big[(\alpha_{i+1}, 0) - P_\infty\big] = D_{i+1}.$$

For $i = 2g$, since the principal divisor of the function y is

$$(y) = (\alpha_1, 0) + \cdots + (\alpha_{2g+1}, 0) - (2g+1)P_\infty,$$

we have

$$F(D_{2g}) = \big[\big(\alpha_{2g}^q, 0\big) - P_\infty\big] = \big[(\alpha_{2g+1}, 0) - P_\infty\big]$$

and thus

$$F(D_{2g}) = \big[(\alpha_1, 0) - P_\infty\big] + \cdots + \big[(\alpha_{2g}, 0) - P_\infty\big] = D_1 + \cdots + D_{2g}$$

in $J_f[2]$. Thus the matrix of the action of F on $J_f[2]$ in the basis $D_1, \ldots, D_{2g}$ is

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & 1 & 0 & 1 \\ 0 & \cdots & 0 & 1 & 1 \end{pmatrix}.$$

The characteristic polynomial of this matrix is $T^{2g} + \cdots + T + 1$ in $\mathbb{F}_2[T]$ and this is the reduction modulo 2 of $\chi(T)$.

Since the roots of $T^{2g} + \cdots + T + 1$ are pairwise distinct in $\overline{\mathbb{F}}_2$ (they are the $(2g+1)$th nontrivial roots of unity), the polynomial P has only simple roots, and the lemma is proved. □

Unfortunately, the function fields that appear in the previous lemma are not real extensions of $\mathbb{F}_q(x)$ since the infinite place of this last field is ramified. We have just obtained that there exist infinitely many *imaginary* quadratic function fields with separable zeta polynomial.

We now show that infinitely many of the function fields constructed above can be seen as *real* function fields.

Lemma 4. *Let X be the hyperelliptic curve over $\mathbb{F}_q$ defined by*

$$y^2 = f(x)$$

where $f(x)$ is an irreducible polynomial of $\mathbb{F}_q[x]$. If $\sharp X(\mathbb{F}_q) > 1$ then the function field of X can be viewed as a real quadratic function field, i.e. there exists a transcendental element z in K such that the extension $K/\mathbb{F}_q(z)$ is quadratic, and real.

Proof. The function field K of X can be viewed as a real quadratic extension of a rational function field $\mathbb{F}_q(z)$ if there exists a place of $\mathbb{F}_q(x)$ which splits in K; actually taking z as the

inverse of a uniformizing parameter at this place, we see that $\mathbb{F}_q(z) = \mathbb{F}_q(x)$ (and thus that $[K : \mathbb{F}_q(z)] = 2$), and that the pole of z splits in this extension.

We are reduced to show that there is a place of $\mathbb{F}_q(x)$ which splits in K; since $f(x)$ is supposed to be irreducible, the Weierstrass points are not rational except the infinite place if $f(x)$ has odd degree. Thus, there is at most one rational ramified place and then if $\sharp X(\mathbb{F}_q) > 1$ there exists at least one place which splits totally. □

In view of the previous results, it remains to show that there exist infinitely many hyperelliptic curves X defined by $y^2 = f(x)$ where $f(x)$ is an irreducible polynomial of $\mathbb{F}_q[x]$ of odd degree such that $\sharp X(\mathbb{F}_q) > 1$.

If X is the hyperelliptic curve defined by $y^2 = f(x)$ where $f(x)$ is an irreducible polynomial of $\mathbb{F}_q[x]$ of degree $2g+1$, and if v is a nonquadratic residue in $\mathbb{F}_q$, we defined the twist $\tilde{X}$ of X (with respect to v) to be the hyperelliptic curve defined by $y^2 = f_v(x)$ with $f_v(x) = vf(\frac{x}{v})$. We have the following

Lemma 5.

(i) *The polynomial $f(x)$ is irreducible if and only if $f_v(x)$ is irreducible.*
(ii) *If n is odd the numbers of $\mathbb{F}_{q^n}$-rational points of X and $\tilde{X}$ are related by*

$$\sharp X(\mathbb{F}_{q^n}) + \sharp \tilde{X}(\mathbb{F}_{q^n}) = 2q^n + 2,$$

and if n is even the relation becomes

$$\sharp X(\mathbb{F}_{q^n}) = \sharp \tilde{X}(\mathbb{F}_{q^n}).$$

Proof. The first part of the proof is trivial. We come to the second part. It is well-known that if X is a complete smooth model of the curve with affine equation $y^2 = f(x)$, with f separable, and $\mathbb{F}_{q^n}$ is any extension of $\mathbb{F}_q$, then the cardinality of $X(\mathbb{F}_{q^n})$ is given by

$$\sharp X(\mathbb{F}_{q^n}) = q^n + 1 + \sum_{x \in \mathbb{F}_{q^n}} \chi_{2,n}\big(f(x)\big),$$

where $\chi_{2,n}$ is the multiplicative character of order 2 of $\mathbb{F}_{q^n}^{\times}$ extended to $\mathbb{F}_{q^n}$ by setting $\chi_{2,n}(0) = 0$.

Applying this result to $\tilde{X}$, we get

$$\begin{aligned}
\sharp \tilde{X}(\mathbb{F}_{q^n}) &= q^n + 1 + \sum_{x \in \mathbb{F}_{q^n}} \chi_{2,n}\big(f_v(x)\big) \\
&= q^n + 1 + \chi_{2,n}(v) \sum_{x \in \mathbb{F}_{q^n}} \chi_{2,n}\left(f\left(\frac{x}{v}\right)\right) \\
&= q^n + 1 + \chi_{2,n}(v) \sum_{x \in \mathbb{F}_{q^n}} \chi_{2,n}\big(f(x)\big).
\end{aligned}$$

Now we have $\chi_{2,n} = \chi_2 \circ N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ where $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ is the norm. Since $v \in \mathbb{F}_q$, we get $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(v) = v^n$, and $\chi_{2,n}(v) = \chi_2(v)^n = (-1)^n$ since v is not a quadratic residue. This ends the proof. □

Corollary 6.

(i) *If* $\sharp X(\mathbb{F}_q) \leqslant 1$ *then* $\sharp \tilde{X}(\mathbb{F}_q) \geqslant 2q+1$.
(ii) *We have*

$$L_{\tilde{X}}(T) = L_X(-T).$$

In particular, $L_{\tilde{X}}(T)$ *has only simple roots if and only if it is the case for* $L_X(T)$ (*and* $L_{\tilde{X}}(T)$ *is irreducible if and only if* $L_X(T)$ *is*).

Proof. (i) is trivial. To show (ii), let us look at the zeta function of $\tilde{X}$:

$$Z_{\tilde{X}}(T) = \exp\Bigg(\sum_{n\geqslant 1} \sharp \tilde{X}(\mathbb{F}_{q^n}) \frac{T^n}{n}\Bigg).$$

Using the formulas in the proof of the previous lemma, and setting $A_n := \sum_{x\in\mathbb{F}_{q^n}} \chi_{2,n}(f(x))$, we get

$$Z_{\tilde{X}}(T) = \exp\Bigg(\sum_{n\geqslant 1} \big(q^n + 1 + (-1)^n A_n\big) \frac{T^n}{n}\Bigg) = \frac{\exp(\sum_{n\geqslant 1} A_n \frac{(-T)^n}{n})}{(1-T)(1-qT)}.$$

Thus $L_{\tilde{X}}(T) = \exp(\sum_{n\geqslant 1} A_n \frac{(-T)^n}{n})$. A similar calculation for X gives $L_X(T) = \exp(\sum_{n\geqslant 1} A_n \frac{T^n}{n})$, that is $L_{\tilde{X}}(T) = L_X(-T)$. □

Hence, we have proved the following theorem.

Theorem 7. *For any finite field* $\mathbb{F}_q$, *there exist infinitely many real quadratic function fields over* $\mathbb{F}_q$ *with separable zeta polynomial.*

4. Irreducibility of the zeta polynomial

We now consider the related question of the existence, for any finite field $\mathbb{F}_q$, of infinitely many real quadratic function fields over $\mathbb{F}_q$ with irreducible zeta polynomial. We prove a conditional result, and then we briefly survey the known results about this question.

Lemma 8. *Let* $q > 4$, *and* X *be a projective algebraic curve over* $\mathbb{F}_q$ *such that the group of rational points* $J_X(\mathbb{F}_q)$ *of the jacobian of* X *has prime order. Then the zeta polynomial of* X *is irreducible over* $\mathbb{Q}$ (*and thus has simple roots*).

Proof. The value $L_X(1)$, which is exactly $\sharp J_X(\mathbb{F}_q)$, is prime by hypothesis and any factor

$$Q(T) = \prod_{i\in I} (1 - \omega_i T),$$

with $I \subset \{1, \ldots, 2g\}$, of $L_X(T)$ in $\mathbb{Z}[T]$ would have a value at 1 strictly greater than 1 since

$$Q(1) = \prod_{i \in I} |1 - \omega_i| \geqslant \prod_{i \in I} (\sqrt{q} - 1) > 1$$

by the Riemann hypothesis and because $q > 4$. □

Thus we have the following conditional result.

Theorem 9. *Let $q > 4$. Assuming that there exist infinitely many real quadratic function fields over $\mathbb{F}_q$ with prime divisor class number, then there exist infinitely many real quadratic function fields over $\mathbb{F}_q$ with irreducible zeta polynomial. Furthermore in this case Gauss conjecture for function fields over $\mathbb{F}_q$ holds true.*

Proof. The first assertion follows directly from Lemma 8, and the second one from Proposition 1(iii). □

Using the previous section, we have another way to consider our problem. Indeed, assume Artin's conjecture on primitive root for the integer 2, i.e. there exist infinitely many primes ℓ such that 2 generates the multiplicative group $(\mathbb{Z}/\ell\mathbb{Z})^*$. Hence the polynomial

$$\left(x^\ell - 1\right)/(x - 1) = x^{\ell-1} + \cdots + x + 1$$

is irreducible over $\mathbb{F}_2$. From the proof of Lemma 3, this polynomial is the reduction modulo 2 of the zeta polynomial of any hyperelliptic curve of the form $y^2 = f(x)$, f irreducible of degree ℓ. Thus we obtain the following other conditional result.

Theorem 10. *Assuming Artin's primitive root conjecture, there exist infinitely many real quadratic function fields with irreducible zeta polynomial.*

Note that, in another direction, namely when the characteristic of the function field is not fixed, Koblitz in [4] found conditions under which the zeta polynomial of the curve $y^2 + y = x^d$ over $\mathbb{F}_p$, where $d = 2g + 1$ is a prime, $d \neq p$, is irreducible over $\mathbf{Q}$. As a corollary, he states the following result.

Theorem 11. *For any fixed prime $d \geqslant 3$ there are infinitely many primes p such that the zeta polynomial of $y^2 + y = x^d$ over $\mathbb{F}_p$ is irreducible over $\mathbf{Q}$.*

For a fixed characteristic, the question is still open for this class of curves, as its following conjecture states.

Conjecture 1. *For any prime p there are infinitely many primes d such that the zeta polynomial of $y^2 + y = x^d$ over $\mathbb{F}_p$ is irreducible over $\mathbf{Q}$.*

On the other hand, the question of the irreducibility of the zeta polynomial of smooth projective curves varying in a family is considered in [2,5]. Precisely, let U be a geometrically irreducible smooth affine scheme of dimension $d \geqslant 1$, and $\pi : C \to U$ be an algebraic family

of smooth projective curves of genus g over U, such that the geometric monodromy group of the integral sheaves $R^1\pi_!\mathbb{Z}_\ell$ is the full symplectic group $\mathrm{Sp}(2g)$ for any prime ℓ large enough. Then the number $N_\pi(U/\mathbb{F}_q)$ of $u \in U(\mathbb{F}_q)$ such that the curve $\pi^{-1}(\{u\})$ has its zeta polynomial reducible or having splitting field with degree strictly less than $2^g g!$ (which is the maximal degree imposed by the pairing on its roots), satisfies $N_\pi(U/\mathbb{F}_q) = O(q^{d-\gamma}\ln q)$, where γ is some constant depending on g, generally $\gamma = O(\frac{1}{g^2})$. There is an other similar estimate for families of hyperelliptic curves of the form $y^2 = f(x)(x-u)$, where the parameter space U is $\mathbf{A}^1$ with the zeroes of f removed: here Kowalski gets $N_\pi(U/\mathbb{F}_q) = O(q^{1-\gamma}\ln q)$ for some γ as above.

From Lang–Weil estimates on the number of points of varieties over finite fields, we have $\sharp U(\mathbb{F}_q) = O(q^d)$, and we see that the bound above is nontrivial only when $q^{-\gamma}\ln q = o(1)$, for instance when q is large with respect to g. Thus if we fix q and vary g, this estimate is trivial for g large enough, and cannot be used to answer our question.

More generally, we can ask for any fixed finite field $\mathbb{F}_q$, is there exist infinitely many jacobians of hyperelliptic curves with irreducible zeta polynomial. Since an *ordinary* abelian variety over $\mathbb{F}_q$ is simple if and only if its Weil polynomial is irreducible, we can look for the existence of simple ordinary jacobian varieties of every dimension. However, Howe and Zhu in [3] proved that for any finite prime fields there exist absolutely simple ordinary *abelian* varieties of every dimension. But the question of whether there exist absolutely simple *jacobians* of every dimension over a given finite field is still open (whereas the answer is yes if the field is the algebraic closure of a finite field, if it has characteristic p but is not algebraic over $\mathbb{F}_p$ or if it has characteristic zero), see [3].

Acknowledgments

The authors thank Everett Howe for the idea of Lemma 3, Christophe Ritzenthaler for the numerical example of the remark of Section 2 and Marc Perret for a lightning discussion.

References

[1] B. Anglès, On L-functions of cyclotomic function fields, J. Number Theory 116 (2) (2006) 247–269.
[2] N. Chavdarov, The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy, Duke Math. J. 87 (1) (1997) 151–180.
[3] E.W. Howe, H.J. Zhu, On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field, J. Number Theory 92 (1) (2002) 139–163.
[4] N. Koblitz, Jacobi sums, irreducible zeta-polynomials, and cryptography, Canad. Math. Bull. 34 (2) (1991) 229–235.
[5] E. Kowalski, The large sieve, monodromy, and the zeta function of curves, J. Reine Angew. Math. 601 (2006) 29–69.
[6] G. Lachaud, S. Vladut, Gauss problem for function fields, J. Number Theory 85 (2) (2000) 109–129.
[7] M. Rosen, Number Theory in Function Fields, Grad. Texts in Math., vol. 210, Springer-Verlag, New York, 2002.
[8] J. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math. 2 (1966) 134–144.