Journal of Number Theory 156 (2015) 414–431

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Decomposing Jacobians of curves over finite fields in the absence of algebraic structure

Omran Ahmadi[a,*,1], Gary McGuire[b,2], Antonio Rojas-León[c,3]

[a] *School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran*
[b] *School of Mathematical Sciences, University College, Dublin, Ireland*
[c] *Department of Algebra, University of Seville, Spain*

ARTICLE INFO

Article history:
Received 17 November 2014
Accepted 18 April 2015
Available online 9 June 2015
Communicated by D. Wan

MSC:
14H45
11M38

Keywords:
Curve
Jacobian
Supersingular
Finite field
L-polynomial

ABSTRACT

We consider the issue of when the L-polynomial of one curve over $\mathbb{F}_q$ divides the L-polynomial of another curve. We prove a theorem which shows that divisibility follows from a hypothesis that two curves have the same number of points over infinitely many extensions of a certain type, and one other assumption. We also present an application to a family of curves arising from a conjecture about exponential sums. We make our own conjecture about L-polynomials, and prove that this is equivalent to the exponential sums conjecture.

* Corresponding author.
E-mail addresses: oahmadid@ipm.ir (O. Ahmadi), gary.mcguire@ucd.ie (G. McGuire), arojas@us.es (A. Rojas-León).

[1] Research supported by IPM.
[2] Research supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.
[3] Partially supported by MTM2010-19298 (Min. Ciencia e Innovación) and FEDER.

http://dx.doi.org/10.1016/j.jnt.2015.04.014
0022-314X/© 2015 Elsevier Inc. All rights reserved.

1. Introduction

Let $q = p^a$ where p is a prime, and let $\mathbb{F}_q$ denote the finite field with q elements. Let $C = C(\mathbb{F}_q)$ be a projective smooth absolutely irreducible curve of genus g defined over $\mathbb{F}_q$. For any $n \geq 1$ let $C(\mathbb{F}_{q^n}) = C(\mathbb{F}_q) \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$ be the set of $\mathbb{F}_{q^n}$-rational points of C, and let $\#C(\mathbb{F}_{q^n})$ be the cardinality of $C(\mathbb{F}_{q^n})$. Similarly, if $\overline{\mathbb{F}_q}$ denotes a fixed algebraic closure of $\mathbb{F}_q$, let $C(\overline{\mathbb{F}_q}) = C(\mathbb{F}_q) \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$.

The divisor group of C is the free abelian group generated by the points of $C(\overline{\mathbb{F}_q})$. Thus, a divisor is a formal sum $\sum n_P P$ over all $P \in C(\overline{\mathbb{F}_q})$, where all but finitely many n_P are 0. The degree of a divisor is $\sum n_P$. The divisor of a function in the function field $\overline{\mathbb{F}_q}(C)$ must have degree 0, and is called a principal divisor. The quotient of the subgroup of degree 0 divisors by the principal divisors is denoted $Pic^0(C(\overline{\mathbb{F}_q}))$, and is canonically isomorphic to the Jacobian of C, $Jac(C)(\overline{\mathbb{F}_q})$, after a point at infinity is chosen. The Galois group $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ acts on divisors and divisor classes, and we define $Jac(C) = Jac(C)(\mathbb{F}_q) = Pic^0(C) = Pic^0(C(\mathbb{F}_q))$ to be the divisor classes that are fixed by every element of $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. The Jacobian $Jac(C)$ is an abelian variety of dimension g defined over $\mathbb{F}_q$.

The Frobenius map $\pi : x \mapsto x^q$ on $\overline{\mathbb{F}_q}$ induces a Frobenius map on $C(\overline{\mathbb{F}_q})$. The elements of $C(\mathbb{F}_{q^n})$ are the fixed points of π^n. The Frobenius morphism π induces a map on divisor classes, and hence on the Jacobian, and hence a Frobenius endomorphism on the ℓ-adic Tate module $V_\ell(Jac(C))$. Let $P_C(t)$ denote the characteristic polynomial of the Frobenius endomorphism, which is known to have integer coefficients. An abelian variety defined over $\mathbb{F}_q$ is called $\mathbb{F}_q$-simple if it is not isogenous over $\mathbb{F}_q$ to a product of abelian varieties of lower dimensions. An abelian variety is absolutely simple if it is $\overline{\mathbb{F}_q}$-simple. If $Jac(C)$ is $\mathbb{F}_q$-simple then it can be shown that $P_C(X) = h(X)^e$ where $h(X) \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Z}$ and $e \geq 1$. We refer the reader to Waterhouse [17] for these and further details about abelian varieties.

Given an abelian variety A of dimension g defined over $\mathbb{F}_q$, for a prime $\ell \neq p$ one defines $A[\ell]$ as the group of points on A (with values in an algebraic closure $\bar{k}$) of order dividing ℓ. Like in the classical case over $\mathbb{C}$ it can be shown that $A[\ell]$ is a $2g$-dimensional $\mathbb{Z}/\ell\mathbb{Z}$-vector space. Things are different when $\ell = p$. The *p-rank* of A is defined by

$$r_p(A) = \dim_{\mathbb{F}_p} A[p](\bar{k}),$$

where $A[p](\bar{k})$ is the subgroup of p-torsion points over the algebraic closure. The p-rank can take any value between 0 and $g = \dim(A)$. When $r_p(A) = g$ we say that A is ordinary. The number $r_p(A)$ is invariant under isogenies over k, and satisfies $r_p(A_1 \times A_2) = r_p(A_1) + r_p(A_2)$.

The zeta function of C is defined by

$$Z_C(t) = exp\left(\sum_{n\geq 1} \#C(\mathbb{F}_{q^n})\frac{t^n}{n}\right) = exp\left(\sum_{n\geq 1} \#Fix(\pi^n)\frac{t^n}{n}\right).$$

It was shown by Artin and Schmidt (see Roquette [13]) that $Z_C(t)$ can be written in the form

$$\frac{L_C(t)}{(1-t)(1-qt)}$$

where $L_C(t) \in \mathbb{Z}[t]$ (called the L-polynomial of C) is of degree $2g$. Weil showed that $L_C(t) = t^{2g}P_C(1/t)$, and therefore factorizations of $P_C(t)$ are equivalent to factorizations of $L_C(t)$.

The characteristic polynomial of Frobenius carries a lot of information about an abelian variety. In fact, the isogeny classes of abelian varieties are completely classified by their characteristic polynomials, as the following theorem of Tate shows.

Theorem 1 *(Tate). Let A and B be abelian varieties defined over $\mathbb{F}_q$. Then an abelian variety A is $\mathbb{F}_q$-isogenous to an abelian subvariety of B if and only if $P_A(t)$ divides $P_B(t)$ over $\mathbb{Q}[t]$. In particular, $P_A(t) = P_B(t)$ if and only if A and B are $\mathbb{F}_q$-isogenous.*

When $Jac(C)$ is not $\mathbb{F}_q$-simple it decomposes up to isogeny (by Poincare's theorem) into a product of abelian varieties of smaller dimensions, and Tate's theorem shows that the characteristic polynomial $P_C(t)$ is divisible by the characteristic polynomials of the subvarieties. In this paper we are interested in this phenomenon of the decomposition of $Jac(C)$.

It follows from this discussion that decomposing the Jacobian up to isogeny, factorizing the characteristic polynomial, and factorizing the L-polynomial, are all equivalent.

The decomposition of $Jac(C)$ has been studied in many papers before now, see Aubry–Perret [2], Paulhus [11] or Bauer–Teske–Weng [3] for example, and there are two well-known approaches. The first approach is to use the Kani–Rosen decomposition theorem [7], applicable for many groups $G = Aut(C)$.

Theorem 2 *(Kani–Rosen). Given a curve C, let $G \leq Aut(C)$ be a finite group such that $G = H_1 \cup \cdots \cup H_t$ where the H_i are subgroups of G such that $H_i \cap H_j = \{1\}$ if $i \neq j$. Then we have the following isogeny relation*

$$\mathrm{Jac}(C)^{t-1} \times \mathrm{Jac}(C/G)^{|G|} \sim \mathrm{Jac}(C/H_1)^{|H_1|} \times \cdots \times \mathrm{Jac}(C/H_t)^{|H_t|}.$$

This usually yields a decomposition of the Jacobian and a factorization of $L_C(t)$. For example, in the special case where G is the Klein 4-group with subgroups H_1, H_2, H_3, the Kani–Rosen theorem implies an isogeny

$$\mathrm{Jac}(C)^2 \times \mathrm{Jac}(C/G)^4 \sim \mathrm{Jac}(C/H_1)^2 \times \mathrm{Jac}(C/H_2)^2 \times \mathrm{Jac}(C/H_3)^2$$

which implies the following L-polynomial relation

$$L_C(t)\ L_{C/G}(t)^2 = L_{C/H_1}(t)\ L_{C/H_2}(t)\ L_{C/H_3}(t).$$

An example of a paper applying the theorem in the case of the Klein-4-group is [10]. However, as pointed out in [11], the Kani–Rosen theorem will not apply when $Aut(C)$ is cyclic. Also, most curves have trivial automorphism group, so the theorem does not apply to them.

Related to this method is the fact that the L-polynomial of a fibre product $C \times D$ is divisible by the L-polynomials of C and D.

The second well-known approach is to use a theorem of Kleiman [8], also sometimes attributed to Serre, which implies a decomposition of $Jac(C)$ whenever there is a covering map $C \longrightarrow C'$.

Theorem 3 *(Kleiman–Serre). If there is a morphism of curves $C \longrightarrow C'$ that is defined over $\mathbb{F}_q$ then $L_{C'}(t)$ divides $L_C(t)$.*

These two approaches show that $L_C(t)$ is divisible by the L-polynomial of a curve that is a quotient of C or a morphic image of C. In this article we will add a third approach, which may apply to curves with no nontrivial automorphisms, and in situations where there are no nontrivial covering maps. We replace the hypotheses of algebraic structure with a hypothesis about the number of rational points, and show that the Jacobians of such curves can exhibit similar decomposition behaviour. Specifically, we will prove the following theorem.

Theorem 4. *Let C and D be two smooth projective curves over $\mathbb{F}_q$. Assume there exists a positive integer k such that*

1. *$\#C(\mathbb{F}_{q^m}) = \#D(\mathbb{F}_{q^m})$ for every m that is not divisible by k, and*
2. *the k-th powers of the roots of $L_C(t)$ are all distinct.*

Then $L_D(t) = q(t^k)L_C(t)$ for some polynomial $q(t)$ in $\mathbb{Z}[t]$.

The theorem of Tate (Theorem 1) when applied to two elliptic curves E_1 and E_2 defined over $\mathbb{F}_q$ says that when E_1 and E_2 have the same number of $\mathbb{F}_q$-rational points, there must be an isogeny between the curves. Thus, two curves having the same number of points cannot be a combinatorial accident; it must happen because of an isogeny. Theorem 4 may be seen as a generalization of this result when curves C_1 and C_2 are of different genera. Theorem 4 says that if the two curves have the same number of points over all the prescribed extension fields, then this is not a combinatorial accident but is coming from a geometric relationship between their Jacobians. There may not be a relationship between the curves, such as a morphism, but there must be a relationship between their Jacobians.

In Section 2 we will recall some background that we need for the article. In Section 3 we will prove Theorem 4. In Section 4 we will apply our results to a family of curves, and state our own conjectures about this family. In Section 5 we give our motivation for this work, which was a conjecture on exponential sums. Finally in Section 6 we prove equivalence of the conjectures.

2. Background

2.1. L-polynomials

It is traditional to write

$$L_C(t) = \prod_{i=1}^{2g}(1-\alpha_i t), \text{ and } P_C(t) = \prod_{i=1}^{2g}(t-\alpha_i).$$

The α_i are called the Frobenius eigenvalues of C (or of $Jac(C)$), because they are the eigenvalues of the $\mathbb{F}_q$-Frobenius endomorphism action on the ℓ-adic Tate module $V_\ell(Jac(C))$. We briefly recall some further well-known facts about L-polynomials (see [16] for example). If $L^{(n)}(t)$ denotes the L-polynomial of $C(\mathbb{F}_{q^n})$ then

$$L^{(n)}(t) = \prod_{i=1}^{2g}(1-\alpha_i^n t).$$

The number of rational points for all $n \geq 1$ is given by

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n.$$

This means that the coefficient of t in $L^{(n)}(t)$ is equal to $\#C(\mathbb{F}_{q^n}) - (q^n + 1)$.

The algebraic integers α_i can be labelled so that $\overline{\alpha_i} = \alpha_{i+g}$ and $\alpha_i\alpha_{i+g} = q$, so $|\alpha_i| = \sqrt{q}$.

2.2. Morphisms

In this section first we recall some theorems which will be used later.

Theorem 5. *(See [15, Theorem 2.3].) Let $\phi : C_1 \longrightarrow C_2$ be a morphism of curves. Then ϕ is either constant or surjective.*

Now let K be a field of characteristic $p > 0$ and let $q = p^r$. If C is a curve defined by a single equation $f = 0$ over K, then we can define a new curve $C^{(q)}$ which is the zero set of the equation $f^{(q)} = 0$ where $f^{(q)}$ is the polynomial obtained from f by raising its coefficients to the power q. It follows that there is a natural morphism between C and $C^{(q)}$ called the Frobenius morphism.

Theorem 6. *(See [15, Corollary 2.12].) Every map $\psi : C_1 \longrightarrow C_2$ of smooth curves over a field of characteristic $p > 0$ factors as*

$$C_1 \xrightarrow{\phi} C_1^{(q)} \xrightarrow{\lambda} C_2$$

for some q where the map ϕ is the Frobenius map, and the map λ is separable.

The following is an immediate corollary of the above theorem as with the assumptions of the following corollary, $C_1^{(q)} = C_1$.

Corollary 7. *Let p be a prime number, $\mathbb{F}_p$ the finite field with p elements, and let C_1, C_2 be smooth curves defined over $\mathbb{F}_p$. Furthermore suppose that there is a map $\psi : C_1 \longrightarrow C_2$. Then there is a map $\lambda : C_1 \longrightarrow C_2$ which is separable.*

3. Divisibility of L-polynomials

In this section we prove our result on the divisibility relation between L-polynomials. Again $q = p^a$ where p is a prime. After proving the theorem we will then prove a partial converse.

3.1. Divisibility theorem

We begin with one preliminary lemma.

Lemma 8. *Suppose that $f(x), g_1(x)$ and $g_2(x)$ are polynomials in $\mathbb{Z}[x]$ where $f(0) \neq 0$ and $f(x)^n = g_1(x^k)/g_2(x^k)$ for positive integers k and n. Then there exists a polynomial $h(x)$ in $\mathbb{Z}[x]$ so that $f(x) = h(x^k)$.*

Proof. Let ζ_k be a primitive k-th root of unity. Then

$$f(\zeta_k x)^n = g_1((\zeta_k x)^k)/g_2((\zeta_k x)^k) = g_1(x^k)/g_2(x^k) = f(x)^n.$$

Thus $f(\zeta_k x) = \zeta_n f(x)$ for some n-th root of unity ζ_n. Since $f(0) \neq 0$ we have $\zeta_n = 1$ and $f(\zeta_k x) = f(x)$. Now the claim follows. □

We restate Theorem 4 and give the proof.

Theorem 9. *Let C and D be two smooth projective curves over $\mathbb{F}_q$. Assume there exists a positive integer k such that*

1. *$\#C(\mathbb{F}_{q^m}) = \#D(\mathbb{F}_{q^m})$ for every m that is not divisible by k, and*
2. *the k-th powers of the roots of $L_C(t)$ are all distinct.*

Then $L_D(t) = q(t^k)L_C(t)$ for some polynomial $q(t)$ in $\mathbb{Z}[t]$.

Proof. Let $L_C(t) = \prod_{i=1}^{2g(C)}(1-\alpha_i t)$ and $L_D(t) = \prod_{j=1}^{2g(d)}(1-\beta_j t)$, then

$$\#C(\mathbb{F}_{q^m}) = 1 + q^m - \sum_{i=1}^{2g(C)} \alpha_i^m$$

and

$$\#D(\mathbb{F}_{q^m}) = 1 + q^m - \sum_{j=1}^{2g(D)} \beta_j^m.$$

So, by hypothesis, there exists a positive integer k such that

$$\sum_{i=1}^{2g(C)} \alpha_i^m = \sum_{j=1}^{2g(D)} \beta_j^m$$

for every m with $k \nmid m$. This gives an equality of certain zeta functions, namely

$$\exp\left(\sum_{m:k\nmid m}\sum_{i=1}^{2g(C)} \alpha_i^m \frac{t^m}{m}\right) = \exp\left(\sum_{m:k\nmid m}\sum_{j=1}^{2g(D)} \beta_j^m \frac{t^m}{m}\right)$$

Now

$$\begin{aligned}\exp\left(\sum_{m:k\nmid m}\sum_{i=1}^{2g(C)} \alpha_i^m \frac{t^m}{m}\right) &= \exp\left(\sum_{m}\sum_{i=1}^{2g(C)} \alpha_i^m \frac{t^m}{m} - \sum_{m:k\mid m}\sum_{i=1}^{2g(C)} \alpha_i^m \frac{t^m}{m}\right)\\ &= \exp\left(\sum_{m}\sum_{i=1}^{2g(C)} \alpha_i^m \frac{t^m}{m} - \sum_{m}\sum_{i=1}^{2g(C)} \alpha_i^{km} \frac{t^{km}}{km}\right)\\ &= \frac{\prod_{i=1}^{2g(C)}(1-\alpha_i^k t^k)^{1/k}}{\prod_{i=1}^{2g(C)}(1-\alpha_i t)}\\ &= \frac{L_C^{(k)}(t^k)^{1/k}}{L_C(t)}\end{aligned}$$

Therefore,

$$\frac{L_C^{(k)}(t^k)^{1/k}}{L_C(t)} = \frac{L_D^{(k)}(t^k)^{1/k}}{L_D(t)}$$

and, raising to the k-th power, we get a polynomial equality

$$L_C(t)^k L_D^{(k)}(t^k) = L_D(t)^k L_C^{(k)}(t^k) \tag{1}$$

In particular, $L_C(t)^k$ divides $L_D(t)^k L_C^{(k)}(t^k)$. But

$$L_C^{(k)}(t^k) = \prod_{i=1}^{2g(C)}(1-(\alpha_i t)^k) = \prod_{i=1}^{2g(C)}\prod_{\zeta^k=1}(1-\zeta\alpha_i t)$$

$$= L_C(t) \prod_{i=1}^{2g(C)} \prod_{\zeta^k=1,\zeta\neq 1} (1-\zeta\alpha_i t)$$

so $L_C(t)^{k-1}$ divides $L_D(t)^k \prod_{i=1}^{2g(C)} \prod_{\zeta^k=1,\zeta\neq 1}(1-\zeta\alpha_i t)$. Since $L_C(t)$ and this last product are relatively prime by assumption, we conclude that $L_C(t)^{k-1}$ divides $L_D(t)^k$. Since $L_C(t)$ is square free, it must divide $L_D(t)$.

Having proved the divisibility of $L_D(t)$ by $L_C(t)$ we need to prove their quotient is of desired form. Using (1) and writing $L_D(t) = p(t)L_C(t)$, we have

$$p(t)^k = L_D^{(k)}(t^k)/L_C^{(k)}(t^k).$$

Now the claim follows from Lemma 8 and there exists $q(t)$ in $\mathbb{Z}[t]$ so that $L_D(t) = q(t^k)L_C(t)$. □

We remark that the theorem becomes false when we replace the first hypothesis "for every m that is not divisible by k" with "for every m with $\gcd(m,k) = 1$." A counterexample is given by the curves (defined over $\mathbb{F}_3$) $D : y^2+(x^2+x+1)y = x^5+x^4+x^2+x+1$ which has L-polynomial $9t^4+3t^3-2t^2+t+1$ and the curve $C : y^2+(2x+1)y = x^3+2x^2+2$ which has L-polynomial $3t^2+t+1$. The curve C is an ordinary curve and it follows from Lemma 8 of [1] that $L_C^{(n)}(t)$ is an irreducible polynomial for every n and hence it has distinct roots. Furthermore, the curves C and D have the same number of rational points over $\mathbb{F}_{3^m}$ when $\gcd(m,6) = 1$ but there is no divisibility of L-polynomials. More generally, for a suitable a a curve with L-polynomial $L_1 : qt^2 - at + 1$ and a curve with L-polynomial $L_2 : q^2t^4 - aqt^3 + (a^2 - q)t^2 - at + 1$ have the same number of rational points over $\mathbb{F}_{q^m}$ when $\gcd(m,6) = 1$ but there is no divisibility of L-polynomials. The existence of curves of genus one with L-polynomial equal to L_1 for some a and curves of genus two with L-polynomial equal to L_2 is guaranteed by the results on the classification of Weil polynomials of degree two and four [5,14].

3.2. A converse

We have the following theorem which is a partial converse of the theorem above.

Theorem 10. *Let C and D be two smooth projective curves over $\mathbb{F}_q$. Assume that there exists a positive integer $k > 1$ such that $L_D(t) = q(t^k)L_C(t)$ for some polynomial $q(t)$ in $\mathbb{Z}[t]$. Then $\#C(\mathbb{F}_{q^m}) = \#D(\mathbb{F}_{q^m})$ for every m that is not divisible by k.*

Proof. Since

$$\frac{L_C(t)}{(1-t)(1-qt)} = Z_C(t) = exp\left(\sum_{m\geq 1} \#C(\mathbb{F}_{q^m})\frac{t^m}{m}\right),$$

it follows that

$$\log L_C(t) = \sum_{m\geq 1} (\#C(\mathbb{F}_{q^m}) - 1 - q^m)\frac{t^m}{m}$$

in $\mathbb{Q}[[t]]$. Similarly, we have

$$\log L_D(t) = \sum_{m\geq 1} (\#D(\mathbb{F}_{q^m}) - 1 - q^m)\frac{t^m}{m}.$$

Now from $L_D(t) = q(t^k)L_C(t)$ we have $\log L_D(t) = \log q(t^k) + \log L_C(t)$ in $\mathbb{Q}[[t]]$, and since $\log q(t^k)$ is a power series in t^k, the coefficients of t^m in $\log L_C(t)$ and $\log L_D(t)$ are equal for m not a multiple of k, and so are $\#C(F_{q^m})$ and $\#D(F_{q^m})$ whenever m is not a multiple of k. □

4. Application to curves

We present a simple family of curves where our theorem (Theorem 4) applies, modulo a conjecture, and yet the Kani–Rosen and Kleiman–Serre theorems do not apply. Our family is a subfamily of a family considered by Poonen [12].

We let D_k be the hyperelliptic curve defined by the affine equation

$$D_k : y^2 + y = x^{2^k+1} + x^{-1}$$

over $\mathbb{F}_2$. We make the following conjecture, where the L-polynomials stated are over $\mathbb{F}_2$.

Conjecture 11. *The L-polynomial of D_k is divisible by the L-polynomial of D_1.*

In fact we will also make a more refined conjecture.

Conjecture 12. *Let $k = p_1^{a_1} \cdots p_m^{a_m}$ be the prime factorization of k, where $p_1, \ldots, p_m$ are distinct primes. Then*

$$L_{D_k}(t) = q_1(t^{p_1}) \cdots q_m(t^{p_m}) L_{D_1}(t)$$

for some polynomials $q_i(t)$ in $\mathbb{Z}[t]$.

We verified the conjectures for $k \leq 5$ using MAGMA [4]. The first five L-polynomials are

$D_1 : 4t^4 + 2t^3 + t + 1$
$D_2 : (4t^4 + 2t^3 + t + 1)(2t^2 + 1)$
$D_3 : (4t^4 + 2t^3 + t + 1)(8t^6 - 4t^3 + 1)$
$D_4 : (4t^4 + 2t^3 + t + 1)(128t^{14} + 64t^{12} + 2t^2 + 1)$

$D_5 : (4t^4 + 2t^3 + t + 1)(32768t^{30} + 4096t^{25} + 4t^5 + 1)$

Multiplying the curve equation by x^2 and replacing xy by y shows that the curve D_k is birational to

$$E_k : y^2 + xy = x^{2^k+3} + x.$$

Thus it follows that D_k is of genus $2^{k-1} + 1$. Now considering the degree 2 map $\psi : D_k \longrightarrow \mathbb{P}^1$ which maps the point (x, y) to x, the ramification points are P_0 and P_∞, where P_0 is the point with x-coordinate 0 and P_∞ is the point at infinity. It follows that the ramification divisor is $2g_{D_k}P_0 + 2P_\infty$. Using the Hurwitz genus formula this fact also shows that the genus of D_k is $2^{k-1} + 1$. Notice that the curve D_k has one singularity at P_∞.

Lemma 13. *The* 2*-rank of* D_k *is* 1*.*

Proof. By the Deuring–Shafarevitch formula, for an Artin–Schreier curve $y^p - y = f(x)$ the p-rank is $m(p - 1)$ where $m + 1$ is the number of poles of $f(x)$. Our curves D_k have two poles, at 0 and ∞. □

Poonen [12] studied the following family of curves

$$L_g : y^2 + y = x^{2g-1} + x^{-1}$$

and showed that their automorphism group consists of the identity and the hyperelliptic involution. Notice that L_g is of genus g, and the family of curves L_g includes D_k. Computer experiments show that the analogue of Conjecture 11 is false for the larger family of L_g curves. As we need the theorem of Poonen in the rest of this section we include its proof for the sake of completeness.

Theorem 14. *(See [12].) The automorphism group of L_g consists of the identity and the hyperelliptic involution.*

Proof. The ramification points of degree 2 map $\psi : L_g \longrightarrow \mathbb{P}^1$ which maps the point (x, y) to x are P_0 and P_∞. It is well known that the Weierstrass points of hyperelliptic curves are exactly the ramification points of the hyperelliptic involution and any automorphism fixes the set of Weierstrass points. It is also well known that the automorphism of the hyperelliptic curves are lifts of the automorphisms of $\mathbb{P}^1$. Thus it follows that automorphisms of L_g are lifts of the maps taking x to λx for some nonzero λ in the algebraic closure of $\mathbb{F}_2$. But according to Artin–Schreier theory the following two curves

$$y_1^2 + y_1 = x^{2g-1} + x^{-1}$$

and

$$y_2^2 + y_2 = (\lambda x)^{2g-1} + (\lambda x)^{-1}$$

are distinct. □

A consequence of Theorem 14 is that the Kani–Rosen method (Theorem 2) will not work if we want to use it to prove Conjecture 11.

The second approach mentioned in the introduction that one might use to prove Conjecture 11 is the Kleiman–Serre theorem, Theorem 3. To apply this theorem one would have to show that there is a map $D_k \longrightarrow D_1$ for any $k > 1$. If there were such a map, there would in particular be a map $D_2 \longrightarrow D_1$. However, the following theorem shows that there is no morphism from D_2 to D_1, and hence the Kleiman–Serre theorem does not apply to our case.

Theorem 15. *There is no non-constant morphism from the curve D_{k+1} to D_k, for any $k \geq 1$.*

Proof. Suppose there is a morphism

$$\phi : D_{k+1} \longrightarrow D_k.$$

Using Corollary 7, we can assume that ϕ is a separable map. Applying the Riemann–Hurwitz genus formula [15, Theorem 5.9] we have

$$2g_{D_{k+1}} - 2 \geq \deg(\phi)(2g_{D_k} - 2) + \sum_{P \in D_{k+1}} (e(P) - 1).$$

Since $g_{D_{k+1}} = 2^k + 1$ and $g_{D_k} = 2^{k-1} + 1$, it follows that $\deg(\phi) = 2$ and $\sum_{P \in D_{k+1}} (e(P) - 1) = 0$. So D_{k+1} is an unramified double cover of D_k. Now ϕ is a separable map of degree 2. Thus D_{k+1} is a Galois cover of D_k. This would imply that there is an involution other than the hyperelliptic involution in the automorphism group of D_{k+1} which contradicts Theorem 14. Notice that here we need the separability of ϕ as our curves are defined over a field of characteristic two. □

Corollary 16. *There is no non-constant morphism from the curve D_2 to D_1.*

We have shown that the Kani–Rosen and Kleiman–Serre approaches will not apply to prove Conjectures 11 and 12.

5. Motivation

In this section we will give our motivation for studying the curves D_k, which comes from a problem on certain exponential sums.

In [6], while studying the cross-correlation of m-sequences, Johansen, Helleseth and Kholosha considered the following exponential sums

$$G_m^{(k)} = \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{Tr_m(x^{2^k+1}+x^{-1})}$$

where $Tr_m(.)$ denotes the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. In particular, $G_m^{(1)} = \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{Tr_m(x^3+x^{-1})}$. They made the following conjecture.

Conjecture 17. *If* $\gcd(k,m) = 1$ *then* $G_m^{(k)} = G_m^{(1)}$.

They also made a more general conjecture, that $G_m^{(k)} = G_m^{(\gcd(k,m))}$, i.e., that $G_m^{(k)}$ depends only on $\gcd(k,m)$.

Now if $Tr_m(u^3 + u^{-1}) = 0$ for $u \in \mathbb{F}_{2^m}$, then there are two points on the following curve considered over $\mathbb{F}_{2^m}$

$$D_k : y^2 + y = x^{2^k+1} + x^{-1}$$

with x-coordinate equal to u, and if $Tr_m(u^3 + u^{-1}) = 1$ then there is no point on D_k with x-coordinate equal to u. Thus we have

$$\#D_k(\mathbb{F}_{2^m}) = 2^m + 1 - G_m^{(k)}.$$

Hence we may restate Conjecture 17 as follows.

Conjecture 18. *When* $\gcd(k,m) = 1$ *the curves* D_1 *and* D_k *have the same number of rational points over* $\mathbb{F}_{2^m}$.

While investigating Conjecture 17, we looked at the zeta function of D_k and we observed empirically using MAGMA [4] that the L-polynomial of D_1 over $\mathbb{F}_2$ divides the L-polynomial of D_k over $\mathbb{F}_2$, and we made Conjecture 11. In the next section we will prove that Conjecture 17 is equivalent to Conjecture 12.

6. Equivalence of conjectures

In this section we consider the relationship between Conjectures 11 and 12 and Conjecture 17.

6.1. Conjecture 12 implies Conjecture 17

Theorem 19. *For any $k \geq 1$, Conjecture 12 implies Conjecture 17.*

Proof. This follows from an argument similar to the proof of Theorem 10. Let $k = p_1^{a_1} \cdots p_m^{a_m}$ be the prime factorization of k, and suppose

$$L_{D_k}(t) = q_1(t^{p_1}) \cdots q_m(t^{p_m}) L_{D_1}(t)$$

for some polynomials $q_i(t)$ in $\mathbb{Z}[t]$. Taking the log on both sides leads to an equality of formal power series. Each of the terms $\log q_i(t^{p_i})$ is a polynomial in t^{p_i}, so for any m that is relatively prime to k the coefficient of t^m in all these terms is 0. Therefore $L_{D_k}(t)$ and $L_{D_1}(t)$ have the same coefficient of t^m for any m with $\gcd(m, k) = 1$, and Conjecture 17 is true. □

Corollary 20. *Conjecture 17 is true for $k \leq 5$.*

Proof. Using Magma we computed the following L-polynomials:

$D_1 : 4t^4 + 2t^3 + t + 1$
$D_2 : (4t^4 + 2t^3 + t + 1)(2t^2 + 1)$
$D_3 : (4t^4 + 2t^3 + t + 1)(8t^6 - 4t^3 + 1)$
$D_4 : (4t^4 + 2t^3 + t + 1)(128t^{14} + 64t^{12} + 2t^2 + 1)$
$D_5 : (4t^4 + 2t^3 + t + 1)(32768t^{30} + 4096t^{25} + 4t^5 + 1)$.

Since Conjecture 12 is then clearly true for $k \leq 5$, the result follows from Theorem 19. □

6.2. Conjecture 17 implies Conjecture 11

We shall prove that Conjecture 17 implies Conjecture 11 for general k, and Conjecture 12 if k has at most 2 prime powers. First we consider the case where k is a prime power.

Theorem 21. *Let $k = p^a$ be a prime power. Then Conjecture 17 implies Conjecture 12.*

Proof. This follows from Theorem 4 (applied to $k = p$) with $C = D_1$ and $D = D_k$. The first condition in Theorem 4 holds by the hypotheses, since being relatively prime to p^a is equivalent to not being divisible by p. To show the second condition in Theorem 4 it suffices to show that the L-polynomial of $D_1(\mathbb{F}_{2^r})$ for each r is irreducible. Since D_1 has genus 2, its L-polynomial has degree 4 and the L-polynomial for $\mathbb{F}_2$ is easily calculated to be $4t^4 + 2t^3 + t + 1$ which is irreducible. This implies that the Jacobian of $D_1(\mathbb{F}_2)$ is simple. By [9] any simple abelian surface of 2-rank 1 is absolutely simple, so the Jacobian is absolutely simple. By Lemma 2.12 of [9] the L-polynomial of $D_1(\mathbb{F}_{2^r})$ for each r is therefore irreducible. □

For general k we will first prove that Conjecture 17 implies Conjecture 11, after a small lemma.

Lemma 22. *Let $P \in 1+t\mathbb{Z}[t]$ be the L-polynomial of a curve with p-rank 0. Let $Q \in 1+t\mathbb{Z}[t]$ be the L-polynomial of a curve with p-rank > 0. Then $Q(t)$ does not divide $P(t)$.*

Proof. A theorem of Manin states that the p-rank is equal to the degree of the mod p reduction of the L-polynomial. Therefore the mod p reduction of $P(t)$, denoted $\overline{P(t)}$, is 1.

Let $d(t) = \gcd(P(t), Q(t))$. Then $\overline{d(t)} = 1$, and $\overline{Q(t)} \neq 1$, so $d(t) \neq Q(t)$. □

Theorem 23. *Conjecture 17 implies Conjecture 11.*

Proof. We proceed by induction on the number of prime divisors of k. If $k = p^a$ for some prime p, then this follows from Theorem 21. Let $k = p_1^{a_1} \cdots p_m^{a_m}$ where $p_1, \ldots, p_m$ are distinct primes, and let $k' = k/p_m^{a_m}$.

Conjecture 17 implies that $\#D_k(\mathbb{F}_{2^r}) = \#D_{k'}(\mathbb{F}_{2^r})$ for every r which is not divisible by p_m. An argument similar to the proof of Theorem 4 shows that

$$L_{D_k}(t)^{p_m} L_{D_{k'}}^{(p_m)}(t^{p_m}) = L_{D_{k'}}(t)^{p_m} L_{D_k}^{(p_m)}(t^{p_m}).$$

By induction hypothesis, $L_{D_{k'}}(t) = L_{D_1}(t) \cdot P(t)$ for some $P \in 1 + t\mathbb{Z}[t]$. Note that, since both $L_{D_{k'}}$ and L_{D_1} have p-rank 1, P must have p-rank 0. Then we have

$$L_{D_k}(t)^{p_m} L_{D_1}^{(p_m)}(t^{p_m}) P^{(p_m)}(t^{p_m}) = L_{D_1}(t)^{p_m} P(t)^{p_m} L_{D_k}^{(p_m)}(t^{p_m}).$$

Since the p_m-th powers of the roots of L_{D_1} are distinct, we can deduce as in the proof of Theorem 4 that $L_{D_1}(t)^{p_m-1}$ divides $L_{D_k}(t)^{p_m} P^{(p_m)}(t^{p_m})$. However $L_{D_1}(t)$ cannot divide $P(t^{p_m})$, as the latter has p-rank 0, by Lemma 22. Therefore, since $L_{D_1}(t)$ is irreducible it must divide $L_{D_k}(t)$. □

Before extending the argument to show that Conjecture 17 implies Conjecture 12 when k has at most 2 prime factors, we prove two lemmas.

Lemma 24. *Suppose that $f_1(x)$, $f_2(x)$, $g_1(x)$ and $g_2(x)$ are polynomials in $\mathbb{Z}[x]$ where $f_i(0) \neq 0$ for $i = 1, 2$ and $(f_1(x)/f_2(x))^n = g_1(x^k)/g_2(x^k)$ for positive integers k and n. Then there are polynomials $h_1(x)$ and $h_2(x)$ in $\mathbb{Z}[x]$ so that $f_1(x)/f_2(x) = h_1(x^k)/h_2(x^k)$.*

Proof. Without loss of generality we may assume that f_1 and f_2 are coprime. Let ζ_k be a primitive k-th root of unity. Then

$$\begin{aligned}(f_1(\zeta_k x)/f_1(\zeta_k x))^n &= g_1((\zeta_k x)^k)/g_2((\zeta_k x)^k) \\ &= g_1(x^k)/g_2(x^k) \\ &= (f_1(x)/f_2(x))^n.\end{aligned}$$

Thus

$$\frac{f_1(x)}{f_2(x)} = \zeta_n \frac{f_1(\zeta_k x)}{f_2(\zeta_k x)}$$

for some n-th root of unity ζ_n. If we let $x = 0$, from the fact that $f_i(0) \neq 0$ for $i = 1, 2$ we derive that $\zeta_n = 1$, and hence

$$\frac{f_1(x)}{f_2(x)} = \frac{f_1(\zeta_k x)}{f_2(\zeta_k x)}$$

which is equivalent to

$$f_1(x) f_2(\zeta_k x) = f_2(x) f_1(\zeta_k x).$$

Now we know that f_1 and f_2 have no common root, so from the equation above it follows that a is a root of f_1 with multiplicity l if and only if $\zeta_k a$ is a root of f_1 with multiplicity l. Thus $f_1(x) = h_1(x^k)$ for some h_1. Similarly, $f_2(x) = h_2(x^k)$ for some h_2. □

Lemma 25. *Let $f \in 1 + T \cdot \mathbb{Z}[T]$ and let p, q be relatively prime integers such that there exist polynomials $g_1, g_2, h_1, h_2 \in 1 + T \cdot \mathbb{Z}[T]$ with*

$$f(t) = \frac{g_1(t^p) g_2(t^q)}{h_1(t^p) h_2(t^q)}.$$

Then there exist polynomials $f_1, f_2 \in 1 + T \cdot \mathbb{Z}[T]$ such that $f(t) = f_1(t^p) f_2(t^q)$.

Proof. We may assume without loss of generality that g_1, h_1 are relatively prime (if they have a common factor, then they have a common factor of the form $P(t^p)$). Similarly with g_2, h_2.

We proceed by induction on $n = \deg(f) + \deg(h_1) + \deg(h_2)$, the case $n = 0$ being obvious. Let α be a (reciprocal) root of $f(t)$. Then α is a root of either $g_1(t^p)$ or of $g_2(t^q)$. Without loss of generality, let us assume that it is a root of the former. Then $\zeta_p^i \alpha$ is also a root for every $i = 0, \ldots, p-1$, where ζ_p is a primitive p-th root of unity. We now distinguish two cases:

If $\zeta_p^i \alpha$ is a root of $f(t)$ for every $i = 0, \ldots, p-1$, then $f(t)$ and $g_1(t^p)$ are divisible by $\prod_i (1 - \zeta_p^i \alpha T) = 1 - \alpha^p T^p$. Let $a(t^p) \in 1 + T^p \mathbb{Z}[T^p]$ be the product of all Galois conjugates of $1 - \alpha^p t^p$. Then $f(t)$ and $g_1(t^p)$ are divisible by $a(t^p)$, and we have

$$\frac{f(t)}{a(t^p)} = \frac{\frac{g_1(t^p)}{a(t^p)} g_2(t^q)}{h_1(t^p) h_2(t^q)}.$$

By induction hypothesis there exist $\hat{f}_1, \hat{f}_2 \in 1 + T \cdot \mathbb{Z}[T]$ such that $\frac{f(t)}{a(t^p)} = \hat{f}_1(t^p) \hat{f}_2(t^q)$, and we take $f_1(t) = a(t) \hat{f}_1(t)$, $f_2(t) = \hat{f}_2(t)$.

Now suppose that there exists some i_0 such that $\zeta_p^{i_0} \alpha$ is not a root of $f(t)$. Then from $f(t) h_1(t^p) h_2(t^q) = g_1(t^p) g_2(t^q)$ we get that $\zeta_p^{i_0} \alpha$ is a root of $h_2(t^q)$, and then so is $\zeta_q^j \zeta_p^{i_0} \alpha$

for every $j = 0, \dots, q-1$, where ζ_q is a primitive q-th root of unity. Since g_2 and h_2 are relatively prime, $\zeta_q^j \zeta_p^{i_0} \alpha$ is a root of $g_1(t^p)$ for every $j = 0, \dots, q-1$. Then $\zeta_q^j \zeta_p^i \alpha$ is a root of $g_1(t^p)$ for every i, j, so $g_1(t^p)$ is divisible by $1 - \alpha^{pq} t^{pq}$. Let $b(t^{pq})$ be the product of all Galois conjugates of $1 - \alpha^{pq} t^{pq}$, then $g_1(t^p)$ is divisible by $b(t^{pq})$, let $g_1(t^p) = g_1'(t^p) b(t^{pq})$. We have

$$f(t) h_1(t^p) h_2(t^q) = g_1'(t^p)(b(t^{pq}) g_2(t^q)).$$

If $b(t^{pq})$ and $h_2(t^q)$ are not relatively prime, then they have a common factor of the form $p(t^q)$. Dividing both of them by that factor we get $f(t) h_1(t^p) h_2'(t^q) = g_1'(t^p) g_2'(t^q)$, and we conclude by induction hypothesis since $\deg(h_2') < \deg(h_2)$. Otherwise, $b(t^{pq})$ must divide $f(t)$. Writing $f(t) = f'(t) b(t^{pq})$ we get

$$f'(t) h_1(t^p) h_2(t^q) = g_1'(t^p) g_2(t^q)$$

and again we conclude by induction. □

Finally we prove the main result of this section.

Theorem 26. *If k has at most 2 prime factors, Conjecture 17 implies Conjecture 12.*

Proof. The prime power case is Theorem 21, so suppose that $k = p_1^{a_1} p_2^{a_2}$.

Following the proof of Theorem 23, and assuming that

$$L_{D_{k'}}(t) = P(t) L_{D_1}(t)$$

and

$$L_{D_k}(t) = Q(t) L_{D_1}(t)$$

from the main equation in Theorem 23 we get that

$$Q(t)^{p_2} P(t)^{(p_2)}(t^{p_2}) = P(t)^{p_2} Q(t)^{(p_2)}(t^{p_2}).$$

This is equivalent to

$$\left(\frac{Q(t)}{P(t)}\right)^{p_2} = \frac{Q^{(p_2)}(t^{p_2})}{P^{(p_2)}(t^{p_2})}.$$

Applying Lemma 8, we have that

$$\frac{Q(t)}{P(t)} = \frac{h_1(t^{p_2})}{h_2(t^{p_2})}.$$

From this and Theorem 21 we have

$$L_{D_k}(t) = Q(t) L_{D_1}(t) = \frac{h_1(t^{p_2})}{h_2(t^{p_2})} P(t) L_{D_1}(t) = \frac{h_1(t^{p_2})}{h_2(t^{p_2})} q_1(t^{p_1}) L_{D_1}(t)$$

for some $q_1(t) \in \mathbb{Z}[t]$. By Lemma 25 the proof is complete. □

When k has more than 2 prime factors, it is not hard to see that the proofs of the theorem above and Theorem 23 along with an induction can be used to prove that Conjecture 17 implies a weaker version of Conjecture 12 where the polynomials in Conjecture 12 are replaced with ratios of polynomials. More precisely, we have the following theorem. Notice that the proof of the converse claim in the following is similar to the proof of Theorem 10.

Theorem 27. *Let $k = p_1^{a_1} \cdots p_m^{a_m}$ be the prime factorization of k, where $p_1, \ldots, p_m$ are distinct primes. Then Conjecture 17 implies that*

$$L_{D_k}(t) = \frac{q_{m,1}(t^{p_m})}{q_{m,2}(t^{p_m})} \frac{q_{m-1,1}(t^{p_{m-1}})}{q_{m-1,2}(t^{p_{m-1}})} \cdots \frac{q_{2,1}(t^{p_2})}{q_{2,2}(t^{p_2})} q_1(t^{p_1}) L_{D_1}(t)$$

for some polynomials $q_{i,1}(t), q_{i,2}(t)$ and $q_1(t)$ in $\mathbb{Z}[t]$. Conversely, if $L_{D_k}(t)$ is in the above form, then Conjecture 17 is true.

Acknowledgments

We would like to thank Robert Granger and Alexey Zaytsev for many insightful discussions during the preparation of this paper.

References

[1] Omran Ahmadi, Igor E. Shparlinski, On the distribution of the number of points on algebraic curves in extensions of finite fields, Math. Res. Lett. 17 (4) (2010) 689–699.

[2] Y. Aubry, M. Perret, Divisibility of zeta functions of curves in a covering, Arch. Math. 82 (2004) 205–213.

[3] Mark Bauer, Edlyn Teske, Annegret Weng, Point counting on Picard curves in large characteristic, Math. Comp. 74 (252) (2005) 1983–2005.

[4] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, in: London, 1993, J. Symbolic Comput.: Computational Algebra and Number Theory 24 (3–4) (1997) 235–265.

[5] Max Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Semin. Hans. Univ. 14 (1941) 197–272.

[6] Aina Johansen, Tor Helleseth, Alexander Kholosha, Further results on m-sequences with five-valued cross correlation, IEEE Trans. Inform. Theory 55 (12) (2009) 5792–5802.

[7] E. Kani, M. Rosen, Idempotent relations and factors of Jacobians, Math. Ann. 284 (1989) 307–327.

[8] S.L. Kleiman, Algebraic cycles and the Weil conjectures, in: Dix esposés sur la cohomologie des schémas, North-Holland, Amsterdam, 1968, pp. 359–386.

[9] D. Maisner, E. Nart, Abelian surfaces over finite fields as Jacobians, Exp. Math. 11 (3) (2002) 321–337, with an appendix by Everett W. Howe.

[10] Gary McGuire, Alexey Zaytsev, On the zeta functions of an optimal tower of function fields over $\mathbb{F}_4$, in: Finite Fields: Theory and Applications, in: Contemp. Math., vol. 518, Amer. Math. Soc., Providence, RI, 2010, pp. 327–338.

[11] Jennifer Paulhus, Decomposing jacobians of curves with extra automorphisms, Acta Arith. 132 (2008) 231–244.

[12] Bjorn Poonen, Varieties without extra automorphisms. II. Hyperelliptic curves, Math. Res. Lett. 7 (1) (2000) 77–82.

[13] P. Roquette, The Riemann hypothesis in characteristic p, its origin and development. Part 1. The formation of the zeta-functions of Artin and of F.K. Schmidt, http://www.rzuser.uni-heidelberg.de/~ci3/rv.pdf.

[14] Hans-Georg Rück, Abelian surfaces and Jacobian varieties over finite fields, Compos. Math. 76 (3) (1990) 351–366.

[15] Joseph H. Silverman, The Arithmetic of Elliptic Curves, second edition, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[16] Henning Stichtenoth, Algebraic Function Fields and Codes, Universitext, Springer, 1993.

[17] W.C. Waterhouse, Abelian varieties over finite fields, Ann. Sci. Éc. Norm. Supér. (4) 2 (1969) 521–560.