manuscripta math. 114, 487–501 (2004)

Irene I. Bouw · Claus Diem · Jasper Scholten

Ordinary elliptic curves of high rank over $\overline{\mathbb{F}}_p(x)$ with constant j-invariant

Received: 7 July 2003 / Revised version: 3 February 2004
Published online: 16 July 2004

Abstract. We show that under the assumption of Artin's Primitive Root Conjecture, for all primes p there exist ordinary elliptic curves over $\overline{\mathbb{F}}_p(x)$ with arbitrarily high rank and constant j-invariant. For odd primes p, this result follows from a theorem we prove which states that whenever p is a generator of $(\mathbb{Z}/\ell\mathbb{Z})^*/\langle -1\rangle$ (ℓ an odd prime) there exists a hyperelliptic curve over $\overline{\mathbb{F}}_p$ whose Jacobian is isogenous to a power of one ordinary elliptic curve.

1. Introduction

Let E be an elliptic curve over a field L. For various choices of L, it is known that $E(L)$ is a finitely generated group. This is the case if, for example,

- L is a number field (by the Mordell–Weil Theorem, see [21], [31]), or, more generally,
- L is finitely generated over its prime field ([23]), or
- L is the function field of an algebraic variety over a field k, and E is not isogenous (over L) to an elliptic curve which can be defined over k ([16]).

One might ask how large the rank of $E(L)$ can get if one fixes L and varies E. If $\mathrm{char}(L) = 0$ then it is a well known open problem whether this rank is bounded or not in any of the above cases. But if $\mathrm{char}(L)$ is positive, there are some results. In the following table we list some cases for which it is known that the rank can get arbitrarily large.

I. I. Bouw, C. Diem: Institut für Experimentelle Mathematik, Universität Duisburg–Essen, Ellernstr. 29, 45326 Essen, Germany. e-mail: {bouw, diem}@exp-math.uni-essen.de

J. Scholten: ESAT/COSIC, K.U. Leuven, Kasteelpark Arenberg 10, 3001 Leuven-Heverlee, Belgium. e-mail: jasper.scholten@esat.kuleuven.ac.be

Mathematics Subject Classification (2000): Primary: 11G05; Secondary: 11G20, 14H40, 14H52

DOI: 10.1007/s00229-004-0476-7

L	j-invariant	ord. / ss.	authors
$\overline{\mathbb{F}}_2(x)$	constant	supersingular	well known, cf. Elkies (1994), [8]
$\mathbb{F}_p(x)$ p odd	constant	supersingular	Shafarevich and Tate (1967), [25]
$\overline{\mathbb{F}}_2(x)$	constant	ordinary	follows from Gaudry, Hess and Smart (2002) et al., [10], [18], (see this paper)
$\overline{\mathbb{F}}_p(x)$ p odd	constant	ordinary	B.D.S., assuming Artin's Primitive Root Conjecture (see this paper)
$\mathbb{F}_p(x)$	non-const.	ordinary	Shioda (1986), [26], (for $\overline{\mathbb{F}}_p(x)$), Ulmer (2002), [29]

Let M be the function field of a (smooth, projective, geometrically irreducible) curve C over some field k with a k-rational divisor of degree 1. Let E be an elliptic curve over k. It is well known that there is a close relationship between $\mathrm{rank}(E(M)/E(k))$ and the number of factors of E in the Jacobian J_C of C.

Note that the group law on E induces the structure of an abelian group on $\mathrm{Mor}_k(C, E)$, and with this structure we clearly have $E(M) \simeq \mathrm{Mor}_k(C, E)$. Let us fix a k-rational divisor D of degree 1. This divisor induces an immersion $\iota : C \hookrightarrow J_C$ (given by $P \mapsto \mathcal{L}(P) \otimes \mathcal{L}(D)^{-1}$).

For $P \in E(k)$, let c_P be the constant map sending C to P. For $a \in \mathrm{Mor}_k(C, E)$, let $a^* : E^\vee \longrightarrow J_C$ be the pull-back map, and let $a_* := (a^*)^\vee \circ \lambda_C$ where $(a^*)^\vee : J_C^\vee \longrightarrow E$ is the dual of the pull-back map and $\lambda_C : J_C \longrightarrow J_C^\vee$ is the canonical principal polarization of J_C.

We have a split exact sequence

$$0 \longrightarrow E(k) \xrightarrow{P\mapsto c_P} \mathrm{Mor}_k(C, E) \overset{\alpha\mapsto\alpha\circ\iota}{\underset{a\mapsto a_*}{\rightleftarrows}} \mathrm{Hom}_k(J_C, E) \longrightarrow 0.$$

Let $r \in \mathbb{N}_0$ be such that $J_C \sim E^r \times A$ for some abelian variety A that does not have an elliptic curve isogenous to E as a factor. Then the $\mathbb{Q}$-vector space $\mathrm{Hom}_k^\circ(J_C, E) := \mathrm{Hom}_k(J_C, E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is isomorphic to $\mathrm{Hom}_k^\circ(E^r, E) \simeq \mathrm{Hom}_k^\circ(E, E)^r$. Therefore the rank of $E(M)/E(k)$ is equal to $r \cdot \mathrm{rank}(\mathrm{End}_k(E))$.

Let C be a hyperelliptic curve, let L be the quadratic subfield of M of genus 0. As $M|k$ has by assumption a k-rational divisor of degree 1, so has $L|k$. Thus $L|k$ is rational, $L = k(x)$ (cf. [27, Proposition I.6.3.]). Let us now consider the twist E^{twist} of $E_{k(x)}$ with respect to the extension $M|k(x)$. The action of the non-trivial element in $\mathrm{Gal}(M|k(x))$ on $E(M)\otimes_{\mathbb{Z}}\mathbb{Q}$ induces a decomposition into eigenspaces

$$E(M) \otimes_{\mathbb{Z}} \mathbb{Q} = E(k(x))\otimes_{\mathbb{Z}}\mathbb{Q} \oplus E^{\mathrm{twist}}(k(x))\otimes_{\mathbb{Z}}\mathbb{Q}.$$

Since $E(k(x)) = E(k)$, we have $\mathrm{rank}(E^{\mathrm{twist}}(k(x))) = \mathrm{rank}(E(M)/E(k)) = r \cdot \mathrm{rank}(\mathrm{End}_k(E))$. To construct high rank elliptic curves over $k(x)$ it suffices therefore to construct hyperelliptic curves over k with a high factor E^r in the Jacobian up to isogeny and with a k-rational divisor of degree 1. Note that if k is a finite field, the second condition is always fulfilled (cf. [27, Corollary V.1.11.]).

In [25], over all prime fields of odd characteristic, hyperelliptic curves of arbitrarily high genus with a supersingular Jacobian which decomposes completely over the prime field are given. (An abelian variety is called *completely decomposable* if it has no simple factor of dimension ≥ 2.) By the above construction (which first appeared in [25]), these curves give rise to the second line of the table. In [8], some supersingular hyperelliptic curves over $\mathbb{F}_2$ of arbitrary high genus and their Mordell–Weil groups are studied in great detail; these curves give rise to the first line of the table.

In [10] a new approach to attack the discrete-logarithm problem in the group of rational points of an elliptic curve over a non-prime finite field is given (see also [12], [18]). The interest of the authors of [10] lies within the realm of cryptology but their construction also gives rise to Theorem 1, which implies the third line of the table (see Section 2 for a proof).

Theorem 1. *For all $r \in \mathbb{N}$, there exists a hyperelliptic curve H over $\mathbb{F}_{2^r}$ such that the Jacobian variety J_H is completely decomposable into ordinary elliptic curves and $J_H \sim E^r \times A$ for some ordinary elliptic curve E and an (ordinary, completely decomposable) abelian variety A. If r is a Mersenne prime, there exists a hyperelliptic curve H over $\mathbb{F}_{2^r}$ of genus r whose Jacobian variety is isogenous to the power of one ordinary elliptic curve.*

In Section 3 of this paper, we prove the following theorem.

Theorem 2. *Let p and ℓ be odd prime numbers such that p generates $(\mathbb{Z}/\ell\mathbb{Z})^*/\langle -1 \rangle$. Then there exists a hyperelliptic curve H over $\overline{\mathbb{F}}_p$ of genus $\frac{\ell-1}{2}$ such that J_H is isogenous to the power of one ordinary elliptic curve.*

Recall that Artin's Primitive Root Conjecture states that for a given non-square integer $a \neq -1$, there exist arbitrarily large prime numbers ℓ with $\langle a \rangle = (\mathbb{Z}/\ell\mathbb{Z})^*$. This conjecture has not been proven for a single a. But it is known that there are at most 2 prime values for a for which Artin's Conjecture fails ([11]). Also, it is proven that Artin's Conjecture follows from the Generalized Riemann Hypothesis ([13]).

The fourth line of the table follows from Theorem 2 and Artin's Conjecture for prime numbers a.

To the knowledge of the authors, it was not known before whether for arbitrarily large $r \in \mathbb{N}$ there exists some hyperelliptic curve over some field of characteristic $\neq 2$ whose Jacobian variety is completely decomposable into r ordinary elliptic curves. The above Theorem 2 also gives an affirmative answer to this question. Of course, the question raised in [7] whether for all $r \in \mathbb{N}$ there exist curves over $\mathbb{C}$ of genus $\geq r$ with completely decomposable Jacobian variety remains open.

2. Proof of Theorem 1

We use the theory of function fields (in one variable) instead of the theory of curves. Let us fix the following notation: If K is a perfect field and $L|K$ is a regular function field (that is, K is algebraically closed in L), we denote the Jacobian variety of the smooth, projective model of $L|K$ by J_L.

In the following, by a *minimal subextension* of a field extension $\lambda|\kappa$ we mean some intermediate field μ of $\lambda|\kappa$ such that $\mu \supsetneq \kappa$ and $\mu|\kappa$ does not contain any non-trivial intermediate field.

We need the following lemma (see [14] and the proof of [9, Theorem 2.1]).

Lemma 1. *Let K be a perfect field, let $M|K(x)$ be a Galois extension, with Galois group an elementary abelian ℓ-group – ℓ an arbitrary prime number – such that $M|K$ is regular. Then $J_M \sim \prod_N J_N$ where N runs over all minimal subextensions of $M|K(x)$. In particular, the genus $g(M)$ of $M|K$ is equal to $\sum_N g(N)$.*

All the following extensions of $\mathbb{F}_2(x)$ should be regarded as embedded in a fixed algebraic closure $\overline{\mathbb{F}_2(x)}$. We use Artin–Schreier theory in the formulation of [15, Theorem 8.3].

Fix some algebraic extension $K|\mathbb{F}_2$ and some $\alpha \in K\backslash\{0\}$. Let $L|K(x)$ be the Artin–Schreier extension given by $y^2 - y = x^{-1} + \alpha x$, that is, L corresponds by Artin–Schreier theory to the $\mathbb{F}_2$-vector subspace $\langle x^{-1} + \alpha x\rangle$ of $K(x)/\mathcal{P}(K(x))$, where $\mathcal{P} : K(x) \longrightarrow K(x)$, $\xi \mapsto \xi^2 - \xi$ is the Artin–Schreier operator. Now $L|K$ is an ordinary elliptic function field — the ordinariness follows for example from the Deuring–Shafarevich formula ([4, Corollary 1.8.]) and the fact that $\overline{K}L|\overline{K}(x)$ has two ramified places — and J_L is an ordinary elliptic curve.

The action of the Galois group $\mathrm{Gal}(K|\mathbb{F}_2) \simeq \mathrm{Gal}(K(x)|\mathbb{F}_2(x))$ on $K(x)$ gives rise to an action on $K(x)/\mathcal{P}(K(x))$, and this action induces an action by the group ring $\mathbb{F}_2[\mathrm{Gal}(K|\mathbb{F}_2)]$. Let U be the cyclic module generated by $x^{-1} + \alpha x$, and let $M|K(x)$ be the extension corresponding to U.

We claim that $M|K$ is regular. Note that the extension $\overline{K}M|\overline{K}(x)$ is given by the image $\overline{U}$ of U in $\overline{K}(x)/\mathcal{P}(\overline{K}(x))$, and $\overline{U}$ is isomorphic to the image of U in $K(x)/\langle K \cup \mathcal{P}(K(x))\rangle$. One sees easily that $U \longrightarrow \overline{U}$ is an isomorphism. It follows that $[M : K(x)] = [\overline{K}M : \overline{K}(x)]$, and $M|K$ is regular.

The minimal subextensions N of $M|K(x)$ are given by $\mathbb{F}_2$-vector subspaces of $K(x)/\mathcal{P}(K(x))$ of the form $\langle\beta x\rangle$ for some $\beta \in K\backslash\{0\}$, or $\langle x^{-1}\rangle$, or $\langle x^{-1} + \gamma x\rangle$ for some $\gamma \in K\backslash\{0\}$. The first two kinds of fields are rational function fields; the third kind of fields are ordinary elliptic function fields. By Lemma 1, J_M is an abelian variety which is completely decomposable into ordinary elliptic curves.

For some subextension N of $M|K(x)$ and some $\sigma \in \mathrm{Gal}(K|\mathbb{F}_2) \simeq \mathrm{Gal}(K(x)|\mathbb{F}_2(x))$, let $\sigma(N)$ be the image of N in M under some extension of σ to M.

Let V be the $\mathbb{F}_2$-vector subspace of U which consists of the elements of the form βx for some $\beta \in K$. Clearly, $[U : V] = 2$. Let R be the extension of $K(x)$ corresponding to V. Then by Lemma 1, the genus of R is zero. Now, $[M : R] = [U : V] = 2$, thus M is hyperelliptic.

Now let $r \in \mathbb{N}$. Let $\alpha \in \mathbb{F}_{2^r}$, not lying in any proper subfield, let L and M be defined as above with $K = \mathbb{F}_{2^r}$ and α. Let $\sigma_{\mathbb{F}_{2^r}|\mathbb{F}_2} \in \mathrm{Gal}(\mathbb{F}_{2^r}|\mathbb{F}_2)$ be the Frobenius morphism. Then for $i = 0, \ldots, r-1$, the powers $\sigma^i_{\mathbb{F}_{2^r}|\mathbb{F}_2}(L)$ are pairwise distinct subfields of M. Now, all $J_{\sigma^i_{\mathbb{F}_{2^r}|\mathbb{F}_2}(L)}$ are isogenous to J_L (via a power of the relative Frobenius homomorphism), and again by Lemma 1,

$$J_M \sim J_L^r \times A \tag{1}$$

for some (ordinary, completely decomposable) abelian variety A over $\mathbb{F}_{2^r}$.

It remains to prove the statement on the Mersenne primes.

Let $r \in \mathbb{N}$ be an odd prime. Let β be a generator of the $\mathbb{F}_2[\mathrm{Gal}(\mathbb{F}_{2^r}|\mathbb{F}_2)]$-module $\mathbb{F}_{2^r}$ (that is, $\beta, \sigma_{\mathbb{F}_{2^r}|\mathbb{F}_2}(\beta), \ldots, \sigma^{r-1}_{\mathbb{F}_{2^r}|\mathbb{F}_2}(\beta)$ form a normal basis of $\mathbb{F}_{2^r}|\mathbb{F}_2$).

Let $\varphi_2(r)$ be the (multiplicative) order of 2 modulo r. Recall that we have canonical isomorphisms

$$\mathbb{F}_2[\mathrm{Gal}(\mathbb{F}_{2^r}|\mathbb{F}_2)] \simeq \mathbb{F}_2[\mathbb{Z}/r\mathbb{Z}] \simeq \mathbb{F}_2[x]/(X^r - 1)$$

of rings, and we have a decomposition into irreducible factors

$$X^r - 1 = (X-1) f_1 \cdots f_{\frac{r-1}{\varphi_2(r)}} \in \mathbb{F}_2[X],$$

where the f_i are pairwise distinct polynomials of degree $\varphi_2(r)$. Let

$$\alpha := (((X-1) f_2 \cdots f_{\frac{r-1}{\varphi_2(r)}})(\sigma_{\mathbb{F}_{2^r}|\mathbb{F}_2}))(\beta).$$

Then $\alpha \notin \mathbb{F}_2$ and $f_1(\sigma_{\mathbb{F}_{2^r}|\mathbb{F}_2})(\alpha) = 0$. Let U and M be defined as above. Then $x^{-1} = f_1(\sigma_{\mathbb{F}_{2^r}|\mathbb{F}_2})(x^{-1} + \alpha x) \in U$, and consequently for all $f \in \mathbb{F}_2[X]$, $x^{-1} + f(\sigma_{\mathbb{F}_{2^r}|\mathbb{F}_2})(\alpha)\, x \in U$. Now the assignment

$$f \mapsto \mathbb{F}_{2^r}(x)[\mathcal{P}^{-1}(x^{-1} + f(\sigma_{\mathbb{F}_{2^r}|\mathbb{F}_2})(\alpha)\, x)]$$

induces a bijection between the non-zero polynomials in $\mathbb{F}_2[X]$ of degree less than $\deg(f_1)$ and the minimal subextensions N of $M|\mathbb{F}_{2^r}(x)$ with genus 1. There are $2^{\varphi_2(r)} - 1$ such polynomials, and thus the genus of M is $2^{\varphi_2(r)} - 1$.

Now let r be a Mersenne prime, that is, r is a prime of the form $2^\ell - 1$. Then $\varphi_2(r) = \ell$ and the genus of M is $2^{\varphi_2(r)} - 1 = r$. By (1), we have $J_M \sim J_L^r$. $\square$

3. Proof of Theorem 2

The idea of the proof of Theorem 2 is to consider curves C over a finite field k such that, after some base extension $K|k$, J_{C_K} has an endomorphism not defined over any proper subextension of $K|k$. If additionally J_C is ordinary, this endomorphism induces a decomposition of J_{C_K} as is made precise below.

In Section 3.3, we apply this general result to hyperelliptic curves in certain algebraic families. These families have already been studied in characteristic 0 in [28]. We use techniques similar to those of [2] to show that they are generically ordinary.

3.1. Operation on abelian varieties over finite fields

In this section, we deal with the following situation:

Let $K|k$ be an extension of finite fields inside the fixed algebraic closure $\overline{k}$ of k. Let $\sigma_{K|k} \in \mathrm{Gal}(K|k)$ be the Frobenius morphism. Let A be an abelian variety over k.

Proposition 1. *Assume that we are given a* $\tau \in \mathrm{End}_K^\circ(A_K)$ *such that*

(a) the action of $\mathrm{Gal}(K|k)$ *on* $\mathrm{End}_K^\circ(A_K)$ *maps the subspace* $\mathbb{Q}[\tau] \subset \mathrm{End}_K^\circ(A_K)$ *to itself,*
(b) τ *is not defined over any intermediate field* μ *of* $K|k$ *with* $\mu \subsetneq K$,
(c) $\mathbb{Q}[\tau]$ *is a field.*

Then the characteristic polynomial of the Frobenius endomorphism of A *has the form* $f(T^{[K:k]})$ *for some polynomial* $f(T) \in \mathbb{Z}[T]$ *of degree* $2\dim(A)/[K:k]$.

Let us first draw a consequence of this proposition before we come to the proof. We make use of the so-called *Weil restriction* $\mathrm{Res}_k^K(B)$ of an abelian variety B over K with respect to $K|k$. For general facts about this object, see [1, Section 7.6], [20] and [6].

Lemma 2. *Assume that* A *is ordinary and that the characteristic polynomial of the Frobenius endomorphism of* A *has the form* $f(T^{[K:k]})$ *for some polynomial* $f(T) \in \mathbb{Z}[T]$ *of degree* $2\dim(A)/[K:k]$. *Then* A *is isogenous to the Weil restriction with respect to* $K|k$ *of an ordinary abelian variety* B *over* K *with* $\dim(B) = \dim(A)/[K:k]$.

Proof. Let χ_A be the characteristic polynomial of the Frobenius endomorphism of A. The assumption that $\chi_A = f(T^{[K:k]})$ for some polynomial $f \in \mathbb{Z}[T]$ of degree $2\dim(A)/[K:k]$ implies that $\chi_{A_K} = f(T)^{[K:k]}$.

Write $f = f_1 \cdots f_a$ with monic, irreducible polynomials f_i. Let $i \in \{1, \dots, a\}$. It is easy to see that there exists a K-simple abelian subvariety B_i of A_K such that the characteristic polynomial of B_i is a power of f_i. In particular, f_i is the minimal polynomial of the Frobenius homomorphism of B_i – let χ_i be the characteristic polynomial of B_i, then $\chi_i = f_i^e$ with some $e \in \mathbb{N}$.[1] As A_K is ordinary by assumption, so is B_i. The slopes of the Newton polygon of an ordinary abelian variety are 0 and 1. This implies with [30, Theorem 8, 4.] that $e = 1$, that is, $\chi_i = f_i$.

[1] If A is some abelian variety over some field K, ℓ a prime $\neq \mathrm{char}(K)$, and α is some endomorphism on A, then the minimal polynomial of α in its operation on $V_\ell(A)$ lies in $\mathbb{Z}[T]$, in particular, it is equal to the minimal polynomial of α in the $\mathbb{Q}$-algebra $\mathbb{Q}[\alpha]$. We refer to this polynomial as the *minimal polynomial* m_α of α.
This follows by induction on the degree of the minimal polynomial m_α of α in its operation on $V_\ell(A)$. Indeed, let h be the product of all irreducible divisors of χ_α, the characteristic polynomial of α. As $\chi_\alpha \in \mathbb{Z}[T]$ ([22, §19, Theorem 4]), h has the same property. Now, $h|m_\alpha$, and the minimal polynomial of $h(\alpha)$ in its operation on $V_\ell(A)$ is $\frac{m_\alpha}{h}$ which lies in $\mathbb{Z}[T]$ by induction assumption.

Let $B := \prod_i B_i$. Then B is an ordinary abelian variety with $\chi_B = f$. The Weil restriction of B with respect to $K|k$ has characteristic polynomial $\chi_B(T^{[K:k]}) = \chi_A$ ([20, §1 (a)]). This implies that $A \sim \mathrm{Res}_k^K(B)$ ([22, Appendix 1, Theorem 2]). □

The above proposition and lemma imply the following.

Proposition 2. *Under the assumptions of Proposition 1, assume additionally that A is ordinary. Then A is isogenous to the Weil restriction with respect to $K|k$ of an ordinary abelian variety B over K with* $\dim(B) = \dim(A)/[K:k]$. *In particular,* $A_K \sim B^{\dim(A)/[K:k]}$.

Proof of Proposition 1. By assumption, the action of the Galois group $\mathrm{Gal}(K|k)$ on $\mathbb{Q}[\tau]$ gives an injective homomorphism $\mathrm{Gal}(K|k) \longrightarrow \mathrm{Aut}(\mathbb{Q}[\tau])$. Fix some polynomial $p(T) \in \mathbb{Q}[T]$ such that $\sigma_{K|k}(\tau) = p(\tau)$. For $i \in \mathbb{N}_0$, define p_i by $p_0 := T,\ p_{i+1} := p_i(p(T))$. Then $\sigma_{K|k}^i(\tau) = p_i(\tau)$. This implies that the elements $p_i(\tau)$ for $i = 0, \ldots, [K:k]-1$ are pairwise distinct and $p_{[K:k]}(\tau) = \tau$.

Let $\ell \neq \mathrm{char}(k)$ be a prime. Let $V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, and let $\overline{V_\ell}(A) := V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$.

We show that the characteristic polynomial of the Frobenius endomorphism in its operation on $T_\ell(A)$ (or – what amounts to the same – on $\overline{V_\ell}(A)$) has the form $f(T^{[K:k]})$ for some polynomial $f(T) \in \overline{\mathbb{Q}}_\ell[T]$ of degree $2\dim(A)/[K:k]$. As $f(T^{[K:k]}) \in \mathbb{Z}[T]$, the same holds for $f(T)$.

As by assumption $\mathbb{Q}[\tau]$ is a field, the operation of τ on $\overline{V_\ell}$ is diagonalizable. For some eigenvalue λ of τ in its operation on $\overline{V_\ell}(A)$, let $\overline{V_\ell}^\lambda$ be the corresponding eigenspace.

Let π_k be the Frobenius endomorphism of A over k; π_k induces an operation on $A(\overline{k})$ which is called the *geometric Frobenius operation*. Let $\sigma_k \in \mathrm{Gal}(\overline{k}|k)$ be the Frobenius morphism. Being an element of $\mathrm{Gal}(\overline{k}|k)$, σ_k also induces an operation on $A(\overline{k})$, called the *arithmetic Frobenius operation*. These two operations are linked by the equation

$$\pi_k(P) = \sigma_k^{-1}(P) \text{ for all } P \in A(\overline{k}).$$

This equation implies $\alpha\pi_k = \pi_k\,\sigma_{K|k}(\alpha)$ for all $\alpha \in \mathrm{End}_K^\circ(A_K)$, thus

$$\tau\pi_k^i = \pi_k^i\,\sigma_{K|k}^i(\tau) = \pi_k^i\,p_i(\tau) \ \text{ for } i \in \mathbb{N}_0. \tag{2}$$

Fix some eigenvalue λ and some $i \in \mathbb{N}$. Then by (2), $\pi_k^i(\overline{V_\ell}^\lambda) \leq \overline{V_\ell}^{p_i(\lambda)}$. (In particular, $p_i(\lambda)$ is an eigenvalue of τ.) Since $\overline{V_\ell}(A)$ is the direct sum of the eigenspaces for τ and π is bijective, we have

$$\pi_k^i(\overline{V_\ell}^\lambda) = \overline{V_\ell}^{p_i(\lambda)}.$$

The equation $p_{[K:k]}(\tau) = \tau$ implies that $p_{[K:k]}(\lambda) = \lambda$. We claim that the eigenvalues $\lambda = p_0(\lambda),\ p(\lambda) = p_1(\lambda),\ \ldots,\ p_{[K:k]-1}(\lambda)$ are pairwise distinct.

To prove this, note that λ is a root of $\chi_\tau = m_\tau$, thus $\mathbb{Q}[\lambda] \simeq \mathbb{Q}[T]/(m_\tau(T)) \simeq \mathbb{Q}[\tau]$. The claim on the eigenvalues follows from the fact that the $p_i(\tau)$ are pairwise distinct for $i = 0, \ldots, [K:k]-1$.

We have a direct sum $\bigoplus_{i=0}^{[K:k]-1}(\overline{V}_\ell^{p_i(\lambda)}) \leq \overline{V}_\ell(A)$ which we denote by $\overline{V}_\ell(\lambda)$. The dimension of this space is $[K:k]\cdot\dim(\overline{V}_\ell^{\lambda})$.

The operation of π_k on $\overline{V}_\ell(A)$ restricts to $\overline{V}_\ell(\lambda)$, and on this space, π_k can be described by a block matrix of the form

$$\begin{pmatrix} O & & & M_\lambda \\ I & O & & \\ & \ddots & \ddots & \\ & & I & O \end{pmatrix},$$

where each of the blocks O, I, M_λ has size $\dim(\overline{V}_\ell^{\lambda}) \times \dim(\overline{V}_\ell^{\lambda})$.

One sees that on $\overline{V}_\ell(\lambda)$, the characteristic polynomial of the Frobenius endomorphism has the desired form. The result follows from the fact that $\overline{V}_\ell(A) = \bigoplus_\lambda \overline{V}_\ell(\lambda)$, where λ runs over a certain subset of the set of eigenvalues of τ. □

3.2. Some families of hyperelliptic curves

In this section, we want to study the p-rank of curves in certain families of hyperelliptic curves.

Let p be an odd prime. For a field k of characteristic p, a $t \in k\backslash\{\pm 2\}$ and an odd ℓ prime to p, let C_t^ℓ (or C_t if ℓ is fixed) be the hyperelliptic curve over k given by the affine equation

$$y^2 = x(x^{2\ell} + tx^\ell + 1).$$

The goal of this section is to prove the following proposition.

Proposition 3. *There exists an open subscheme $U \subset \mathbb{A}^1_{\mathbb{F}_p}\backslash\{\pm 2\}$ such that*

(a) for every ℓ as above, every field k of characteristic p and every $t \in U(k)$, the curve C_t^ℓ is ordinary,
(b) if $i \in \mathbb{N}, i > 1$, then $U(\mathbb{F}_{p^i})$ is nonempty.

Fix some ℓ, some perfect field k containing the ℓth roots of unity and $t \in k\backslash\{\pm 2\}$. Choose a primitive 2ℓth root of unity $\zeta_{2\ell} \in k$ and define an automorphism $\tau_{2\ell}$ of C_t^ℓ by $(x, y) \mapsto (\zeta_{2\ell}^2 x, \zeta_{2\ell} y)$.

Note that the genus of C_t^ℓ is ℓ. The holomorphic differentials ω_i defined by

$$\omega_i = x^{i-1}\frac{\mathrm{d}x}{y}, \qquad i = 1, \ldots, \ell$$

form a basis of $H^0(C_t^\ell, \Omega)$ ([32]). Moreover, $\tau_{2\ell}\,\omega_i = \zeta_{2\ell}^{2i-1}\omega_i$. Therefore ω_i is an eigenvector of $\tau_{2\ell}$ with eigenvalue $\zeta_{2\ell}^{2i-1}$.

Let $F : H^1(C_t^\ell, \mathcal{O}) \to H^1(C_t^\ell, \mathcal{O})$ be the absolute Frobenius; this is an $\mathbb{F}_p$-linear map which satisfies $F\alpha\xi = \alpha^p F\xi$, where $\alpha \in k$ and $\xi \in H^1(C_t^\ell, \mathcal{O})$. Let $<.,.>: H^1(C_t^\ell, \mathcal{O}) \times H^0(C_t^\ell, \Omega) \longrightarrow k$ be the perfect pairing corresponding to the Serre duality. By [24] the *Cartier operator* $\mathcal{C}$ of C_t^ℓ may be defined to be the unique $\mathbb{F}_p$-linear map $\mathcal{C} : H^0(C_t^\ell, \Omega) \to H^0(C_t^\ell, \Omega)$ which satisfies

$$< F\xi, \omega > = < \xi, \mathcal{C}\,\omega >^p, \quad \text{where } \xi \in H^1(C_t^\ell, \mathcal{O}) \text{ and } \omega \in H^0(C_t^\ell, \Omega). \tag{3}$$

It follows that the Cartier operator satisfies

$$\mathcal{C}\alpha^p\omega = \alpha\,\mathcal{C}\omega, \quad \text{where } \alpha \in k \text{ and } \omega \in H^0(C_t^\ell, \Omega). \tag{4}$$

It is a bijection if and only if C_t^ℓ is ordinary ([32, Theorem 3.1.]). We want to describe the matrix of $\mathcal{C}$ with respect to the above basis of $H^0(C_t^\ell, \Omega)$. In order to do so, we need some more notation.

For $i \in \{1, \ldots, \ell\}$, define $j(i) \in \{1, \ldots, \ell\}$ and $\alpha(i) \in \{0, \ldots, p-1\}$ by

$$2j(i) - 1 \equiv \frac{2i-1}{p} \pmod{2\ell}, \qquad \alpha(i) = \left[\frac{p(2j(i)-1)}{2\ell}\right].$$

Here $[\cdot]$ denotes the integral part, as usual.

Let $f := (x^2 + tx + 1)^{(p-1)/2} \in \mathbb{F}_p[t, x]$ and write $f = \sum_{n=0}^{p-1} c_n x^n$ with $c_n \in \mathbb{F}_p[t]$. Note that

$$c_n = \sum_{2n_1+n_2=n} \binom{(p-1)/2}{n_1}\binom{(p-1)/2-n_1}{n_2} t^{n_2}.$$

For later use we remark that if $n \le \frac{p-1}{2}$, then $\deg(c_n) = n$ (because $\binom{(p-1)/2}{n} \neq 0$).

Now let $k := \overline{\mathbb{F}_p(t)}$ and let C_t^ℓ be defined as above.

Lemma 3. *For every $i \in \{1, \ldots, \ell\}$, we have*

$$\mathcal{C}\,\omega_i = c_{\alpha(i)}^{1/p}\,\omega_{j(i)}.$$

Proof. The absolute Frobenius on C_t^ℓ commutes with $\tau_{2\ell}$, so we have $\tau_{2\ell} F = F\,\tau_{2\ell} : H^1(C_t^\ell, \mathcal{O}) \longrightarrow H^1(C_t^\ell, \mathcal{O})$, and thus by (3), we also have $\tau_{2\ell}\,\mathcal{C} = \mathcal{C}\,\tau_{2\ell} : H^0(C_t^\ell, \Omega) \longrightarrow H^0(C_t^\ell, \Omega)$. With (4) this implies that $\tau_{2\ell}\,\mathcal{C}\,\omega_i = \mathcal{C}\tau_{2\ell}\,\omega_i = \mathcal{C}\,\zeta_{2\ell}^{2i-1}\,\omega_i = \zeta_{2\ell}^{(2i-1)/p}\,\mathcal{C}\,\omega_i$, that is, $\mathcal{C}\,\omega_i$ is an eigenvector of $\tau_{2\ell}$ with eigenvalue $\zeta_{2\ell}^{(2i-1)/p}$. In particular, $\mathcal{C}\,\omega_i = \gamma_i^{1/p}\omega_{j(i)}$, for some $\gamma_i \in k$. We want to show that $\gamma_i = c_{\alpha(i)}$.

The Cartier operator extends to an $\mathbb{F}_p$-linear operator $\mathcal{C}$ on the meromorphic differentials which satisfies $\mathcal{C}h^p\omega = h\,\mathcal{C}\omega$ $(h \in k(C_t^\ell),\ \omega \in \Omega(k(C_t^\ell)))$. It is well known that $\mathcal{C}\,\frac{\mathrm{d}x}{x} = \frac{\mathrm{d}x}{x}$ and $\mathcal{C}\,x^i\mathrm{d}x = 0$ if $p \nmid (i-1)$ (see for example [32]).

We have

$$\omega_i = x^{i-1}\frac{\mathrm{d}x}{y} = \frac{x^{pj(i)}}{y^p}x^{(p-1)/2+i-j(i)p}\,f(x^\ell)\frac{\mathrm{d}x}{x}.$$

Define $g = x^{(p-1)/2+i-pj(i)}\,f(x^\ell)$ and write $g = \sum_m g_m x^m$. Then

$$\mathcal{C}\,\omega_i = \frac{x^{j(i)-1}}{y}\left(\sum_m g_{pm}^{1/p}x^m\right)\mathrm{d}x.$$

We want to find all m such that $g_{pm} \neq 0$. The definition of g implies that $g_{pm} = c_n$, where

$$pm = \frac{p-1}{2} + i - pj(i) + n\ell.$$

Recall that the degree of f is $p-1$. Therefore, we need to find all n such that $0 \leq n \leq p-1$ and

$$p - 1 + 2i - 2pj(i) + 2n\ell \equiv 0 \pmod{p}. \tag{5}$$

Because of the equality

$$p(2j(i)-1) = 2\ell\langle\frac{p(2j(i)-1)}{2\ell}\rangle + 2\ell\left[\frac{p(2j(i)-1)}{2\ell}\right] = (2i-1) + \alpha(i)2\ell,$$

(5) is equivalent to $2n\ell \equiv 2\ell\alpha(i) \pmod{p}$. The only such n is $n = \alpha(i)$. This proves the lemma. □

Proof of Proposition 3. Let $\ell, k = \overline{\mathbb{F}_p(t)}$ and C_t^ℓ be as above. Let $A^{(\ell)}$ be the matrix obtained by raising all coefficients of the matrix of the Cartier operator to the pth power. Lemma 3 shows that $A^{(\ell)}$ is the product of a permutation matrix and the diagonal matrix $(c_{\alpha(i)}\delta_{i,j})_{i,j}$, where $\delta_{i,j}$ is the Kronecker delta. (Note that the $\alpha(i)$ depend on ℓ.) Define

$$\Phi := \prod_{n=0}^{(p-1)/2} c_n.$$

Since $c_n = c_{p-1-n}$, the determinant of $A^{(\ell)}$ divides a sufficiently large power of Φ.

Now let k be an arbitrary perfect field of characteristic p, and choose some $t_0 \in k\backslash\{\pm 2\}$. Analogous to above, let $A_{t_0}^{(\ell)}$ be the matrix obtained by raising all coefficients of the matrix of the Cartier operator of $C_{t_0}^\ell$ to the pth power. Then $A_{t_0}^{(\ell)}$ is the specialization of $A_t^{(\ell)}$ induced by the homomorphism $\mathbb{F}_p[t] \longrightarrow k,\ t \mapsto t_0$.

This implies that the curve $C_{t_0}^\ell$ is ordinary if $\Phi(t_0) \neq 0$. Now define $U := \mathbb{A}^1_{\mathbb{F}_p}\backslash(\{\pm 2\} \cup \{t \mid \Phi(t) = 0\})$. Obviously U does not depend on ℓ.

We have already seen that $\deg(c_n) = n$ for $n \leq \frac{p-1}{2}$. Therefore

$$\deg(\Phi) = \sum_{n=0}^{(p-1)/2} n = \frac{p^2-1}{8} < p^2 - 2.$$

This proves (b). □

3.3. Completely decomposable Jacobians

Fix some distinct odd prime numbers p and ℓ. For a field k of characteristic p and a $t \in k$, let E_t be the elliptic curve given by the affine equation

$$y^2 = x(x^2 + tx + 1).$$

We have a cover $\pi : C_t \longrightarrow E_t$, $(x, y) \mapsto (x^\ell, y\, x^{(\ell-1)/2})$.

Let $k := \mathbb{F}_q$, where q is some power of p, and choose some $t \in k\backslash\{\pm 2\}$. Let $K := \mathbb{F}_q[\zeta_\ell]$.

Let A_t be the reduced identity component of the kernel of $\pi_* : J_{C_t} \longrightarrow J_{E_t}$ – this is an $(\ell-1)$-dimensional abelian variety. It is equal to the complement under the canonical principal polarization of J_{C_t} of $\pi^*(J_{E_t})$.

Let $\tau_\ell := \tau_{2\ell}^2$. We have $\pi^*(J_{E_t}) = \pi^*\pi_*(J_{C_t}) = (1 + \tau_\ell^* + \cdots + \tau_\ell^{*\ell-1})(J_{C_t})$, and $A_t = (1 - \frac{1+\tau_\ell^*+\cdots+\tau_\ell^{*\ell-1}}{\ell})(J_{C_t})$. (Note that $1 + \tau_\ell^* + \cdots + \tau_\ell^{*\ell-1}$ is invariant under the Galois action and thus lies in $\mathrm{End}_k^\circ(J_{C_t})$.)

This implies:

Lemma 4. *The automorphism τ_ℓ^* restricts to a K-automorphism of $(A_t)_K$, and $\mathbb{Q}[\tau_\ell] \leq \mathrm{End}_K^\circ((A_t)_K)$ is a field (isomorphic to $\mathbb{Q}[\zeta_\ell]$, where $\sigma_{K|k} \in \mathrm{Gal}(K|k)$ operates by $\zeta_\ell \mapsto \zeta_\ell^q$).*

Now let $i \in \mathbb{N}, i > 1$ and assume that p^i is a generator of $(\mathbb{Z}/\ell\mathbb{Z})^*$. By Proposition 3, there exists some $t \in \mathbb{F}_{p^i}\backslash\{\pm 2\}$ such that C_t and thus J_{C_t} is ordinary.

Again let $k := \mathbb{F}_{p^i}$ and $K := k[\zeta_\ell]$. Then $\tau_\ell^*|_{(A_t)_K}$ is not defined over any subfield μ of $K|k$ with $\mu \subsetneq K$ and $[K : k] = \ell - 1 = \dim(A_t)$. We can thus apply Proposition 2 to A_t, $K|k$ and τ_ℓ^*.

We conclude that A_t is the Weil restriction (with respect to $K|k$) of an ordinary elliptic curve over K. It follows that $J_{C_t} \sim E_t \times \mathrm{Res}_k^K(\widetilde{E}_t)$ for some elliptic curve $\widetilde{E}_t$ over K. This implies that $J_{(C_t)_K} \sim (E_t)_K \times (\widetilde{E}_t)^{\ell-1}$.

We have proven the following proposition.

Proposition 4. *Let p and ℓ be odd prime numbers and $i \in \mathbb{N}, i > 1$, such that p^i generates $(\mathbb{Z}/\ell\mathbb{Z})^*$. Then there exists a hyperelliptic curve over $\mathbb{F}_{p^i}$ of genus ℓ whose Jacobian variety becomes isogenous over $\mathbb{F}_{p^{i(\ell-1)}}$ to the product of one ordinary elliptic curve and the $(\ell-1)$th power of one ordinary elliptic curve.*

This proposition already implies the fourth line of the table in the introduction. In order to prove Theorem 2, let us study the hyperelliptic curves C_t (k arbitrary, $t \in k\backslash\{\pm 2\}$) in more detail.

In addition to the automorphism $\tau_{2\ell}$, C_t has the automorphism $\gamma : (x, y) \mapsto (\frac{1}{x}, \frac{y}{x^{\ell+1}})$ of order 2. Let D_t be the quotient of C_t by this automorphism, $c : C_t \longrightarrow D_t$ the covering morphism. The curve D_t is given by the equation

$$y^2 = D_\ell(x, 1) + t,$$

where $D_\ell(x, a) := (\frac{x+\sqrt{x^2-4a}}{2})^\ell + (\frac{x-\sqrt{x^2-4a}}{2})^\ell \in k[x]$ is the ℓ-th Dickson polynomial for $a \in k^*$ (cf. [17]). With this equation, $c : C_t \longrightarrow D_t$ is given by $(x, y) \mapsto (x + x^{-1}, \frac{y}{x^{(\ell+1)/2}})$. All this follows from the equation

$$D_\ell(x+\frac{a}{x},a)=x^\ell+\left(\frac{a}{x}\right)^\ell .$$

We see in particular that D_t has genus $\frac{\ell-1}{2}$. Note also that if C_t is ordinary so is D_t. Thus in particular, if $i>1$ there exists some $t\in\mathbb{F}_{p^i}$ such that D_t is ordinary.

The covering morphism $c:C_t\longrightarrow D_t$ induces canonical homomorphisms $c^*:J_{D_t}\longrightarrow J_{C_t}$ and $c_*:J_{C_t}\longrightarrow J_{D_t}$. The following argument shows that the kernel of $c_*:J_{C_t}\longrightarrow J_{D_t}$ contains $\pi^*(E_t)$, and the image of $c^*:J_{D_t}\longrightarrow J_{C_t}$ is contained in $\ker(\pi_*)=A_t$.

We have the identity

$$\gamma\tau_\ell=\tau_\ell^{-1}\gamma$$

in $\mathrm{Aut}(C_t)$. This identity implies

$$(\mathrm{id}+\tau^*+\cdots+\tau_\ell^{*\ell-1})\gamma^*=\gamma^*(\mathrm{id}+\tau_\ell^*+\cdots+\tau_\ell^{*\ell-1})$$

on J_{C_t}. This in turn implies that both

$$A_t=\ker(\mathrm{id}+\tau_\ell^*+\cdots+\tau_\ell^{*\ell-1})$$

and

$$\pi^*(E_t)=(\mathrm{id}+\tau_\ell^*+\cdots+\tau_\ell^{*\ell-1})(J_{C_t})$$

are invariant under γ^*. As $\pi\gamma\neq\pi$ and γ fixes a point in $C_t(\bar{k})$, we have $\gamma^*\pi^*\neq\pi^*$, that is, γ^* operates non-trivially on $\pi^*(E_t)$. Because γ^* is an involution, it operates as $-\mathrm{id}$ on $\pi^*(E_t)$. Thus $\pi^*(E_t)$ lies in the kernel of $\mathrm{id}+\gamma^*$, that is, it lies in the kernel of $c_*:J_{C_t}\longrightarrow J_{D_t}$. This implies that $c^*(J_{D_t})$ lies in $\ker(\pi_*)=A_t$, the complement of $\pi^*(E_t)$ with respect to the canonical principal polarization.

Let $\tau:=c_*\tau_\ell^*c^*\in\mathrm{End}^\circ_{k[\zeta_\ell]}((J_{D_t})_{k[\zeta_\ell]})$. We are interested in the minimal polynomial of τ and the Galois action on $\mathbb{Q}[\tau]$.

The homomorphism c^* induces an isogeny between J_{D_t} and $c^*(J_{D_t})=(\mathrm{id}+\gamma^*)(J_{C_t})$. In fact, $c_*c^*=2\,\mathrm{id}$ and $c^*c_*|_{c^*(J_{D_t})}=2\,\mathrm{id}$. This implies that we have an isomorphism of rings (with unity) and Galois modules

$$\mathrm{End}^\circ_{k[\zeta_\ell]}((J_{D_t})_{k[\zeta_\ell]})\longrightarrow\mathrm{End}^\circ_{k[\zeta_\ell]}(c^*(J_{D_t})_{k[\zeta_\ell]}),\quad \alpha\mapsto\frac{1}{2}c^*\alpha c_*|_{(J_{D_t})_{k[\zeta_\ell]}}.$$

Under this isomorphism, τ corresponds to

$$\tfrac12 c^*\tau c_*|_{c^*(J_{D_t})}=\tfrac12 c^*c_*\tau_\ell^*c^*c_*|_{c^*(J_{D_t})}=\tfrac12(\mathrm{id}+\gamma^*)\,\tau_\ell^*\,(\mathrm{id}+\gamma^*)|_{c^*(J_{D_t})}=$$
$$(\tau_\ell^*+\tau_\ell^{*-1})\,\tfrac12(\mathrm{id}+\gamma^*)|_{c^*(J_{D_t})}=(\tau_\ell^*+\tau_\ell^{*-1})|_{c^*(J_{D_t})}.$$

(In particular, $\tau_\ell^*+\tau_\ell^{*-1}$ restricts to an endomorphism of $c^*(J_{D_t})$. This also follows from the fact that $\tau_\ell^*+\tau_\ell^{*-1}$ and $\mathrm{id}+\gamma^*$ commute. The calculations in [28, 3.1] are not necessary to prove this.)

Now, $\mathbb{Q}[\tau_\ell^*]\le\mathrm{End}^\circ_{k[\zeta_\ell]}((A_t)_{k[\zeta_\ell]})$ is isomorphic to $\mathbb{Q}[\zeta_\ell]$ with $\tau\longleftrightarrow\zeta_\ell$. This implies that the minimal polynomial of $(\tau_\ell^*+\tau_\ell^{*-1})|_{A_t}$ is equal to the minimal polynomial of $\zeta_\ell+\zeta_\ell^{-1}$. It follows that the minimal polynomial of τ, that is, the minimal polynomial of $(\tau_\ell^* + \tau_\ell^{*-1})|_{c^*(J_{D_t})}$, is also equal to the minimal polynomial of $\tau_\ell + \tau_\ell^{-1}$. We conclude that $\mathbb{Q}[\tau]$ is isomorphic to $\mathbb{Q}[\zeta_\ell + \zeta_\ell^{-1}]$ with $\tau \longleftrightarrow \zeta_\ell + \zeta_\ell^{-1}$.

Let $k = \mathbb{F}_q$ for some power q of p. Then under the above isomorphism $\mathbb{Q}[\tau] \simeq \mathbb{Q}[\zeta_\ell + \zeta_\ell^{-1}]$, the operation of the Frobenius on τ corresponds to $\zeta_\ell + \zeta_\ell^{-1} \mapsto \zeta_\ell^q + \zeta_\ell^{-q}$. Thus τ is defined over $K := \mathbb{F}_q[\zeta_\ell + \zeta_\ell^{-1}]$ and over no subfield μ of $K|k$ with $\mu \subsetneq K$. Note that $\mathrm{Gal}(\mathbb{F}_q[\zeta_\ell + \zeta_\ell^{-1}]|\mathbb{F}_q) \simeq \langle q \rangle \leq (\mathbb{Z}/\ell\mathbb{Z})^*/\langle -1 \rangle$.

Let $i > 1$ such that p^i is a generator of $(\mathbb{Z}/\ell\mathbb{Z})^*/\langle -1 \rangle$. As stated above, there exists some $t \in \mathbb{F}_{p^i} \backslash \{\pm 2\}$ such that D_t is ordinary. We can apply Proposition 2 to J_{D_t}, $k = \mathbb{F}_{p^i}$, $K = \mathbb{F}_{p^{i(\ell-1)/2}}$ and τ.

We obtain that J_{D_t} is isogenous to the Weil restriction (with respect to $K|k$) of one ordinary elliptic curve over K. We have proven the following proposition which is slightly stronger than Theorem 2.

Proposition 5. *Let p and ℓ be odd prime numbers, let $i \in \mathbb{N}$, $i > 1$, such that p^i is a generator of $(\mathbb{Z}/\ell\mathbb{Z})^*/\langle -1 \rangle$. Then there exists a hyperelliptic curve over $\mathbb{F}_{p^i}$ of genus $\frac{\ell-1}{2}$ whose Jacobian variety becomes over $\mathbb{F}_{p^{i(\ell-1)/2}}$ isogenous to the power of one elliptic curve. In fact, there exists such a curve over $\mathbb{F}_{p^i}$ whose Jacobian is isogenous the the Weil restriction with respect to $\mathbb{F}_{p^{i(\ell-1)/2}}|\mathbb{F}_{p^i}$ of one ordinary elliptic curve.*

Remark 1. In [28], the curves D_t are studied in characteristic 0. There it is shown that for $\ell \neq 5$ the Jacobian of the generic curve D_t^ℓ over $\mathbb{Q}(t)$ is absolutely simple ([28, Corollary 6]). We think that the same is true for the generic curve D_t^ℓ over $\mathbb{F}_p(t)$ for any p. One could check this in some explicit cases, by specializing t, and computing the L-polynomial by counting points. We checked the case $p = 3$, $\ell = 7$. We indeed found a $t \in \mathbb{F}_{27}$ such that $J_{D_t^\ell}$ was absolutely simple. Note however that by our above results, if p is a generator of $(\mathbb{Z}/\ell\mathbb{Z})^*/\langle -1 \rangle$ then, for infinitely many $t \in \overline{\mathbb{F}}_p$, the Jacobian $J_{D_t^\ell}$ is completely decomposable.

Remark 2. As above, let p^i be a generator of $(\mathbb{Z}/\ell\mathbb{Z})^*/\langle -1 \rangle$, and let $t \in \mathbb{F}_{p^i} \backslash \{\pm 2\}$. We have used the endomorphism τ on $(J_{D_t})_{\mathbb{F}_q[\zeta_\ell + \zeta_\ell^{-1}]}$ to derive that $\chi_{J_{D_t}} = f(T^{(\ell-1)/2})$ for some polynomial $f \in \mathbb{Z}[T]$ of degree 2. But this can also be proven in an alternative way. Note that p^i being a generator of $(\mathbb{Z}/\ell\mathbb{Z})^*/\langle -1 \rangle$ is equivalent to p^{2i} generating $(\mathbb{Z}/\ell\mathbb{Z})^{*2}$. It is well known that the Dickson polynomial $D_\ell(x, a)$ is a permutation polynomial for $\mathbb{F}_q$ if $\gcd(q^2 - 1, \ell) = 1$ (cf. [17]). So $D_\ell(x, a)$ is a permutation polynomial for all $\mathbb{F}_{p^{ij}}$ with $\frac{\ell-1}{2} \nmid j$, and consequently, $\#D_t(\mathbb{F}_{p^{ij}}) = p^{ij} + 1$ for those j. It follows that the L-polynomial

$$L(D_t, T) = \exp\left(\sum_{j=1}^{\infty} (\#D_t(\mathbb{F}_{p^{ij}}) - p^{ij} - 1)\frac{T^j}{j}\right)$$

is a polynomial in $T^{(\ell-1)/2}$. Since $\chi_{J_{D_t}}$ is the reciprocal polynomial of $L(D_t, T)$, the same holds for $\chi_{J_{D_t}}$.

Remark 3. Instead of the curves C_t and D_t, it is possible to use other ordinary hyperelliptic curves whose Jacobians have suitable endomorphisms. For example, in [19], some 2-parameter algebraic families of hyperelliptic curves with real multiplication are given. In [3], we will show that these families of curves are also generically ordinary and give rise to new examples of hyperelliptic curves whose Jacobians are isogenous to a power of some ordinary elliptic curve. In this upcoming work, we will be able to use the extra parameter in a way that allows us to avoid the usage of Artin's Conjecture.

Remark 4. We already mentioned that the results in characteristic 2 of [10] were motivated by a cryptographic application. They were used to construct certain elliptic curves on which there is a relatively efficient method to compute discrete logarithms. It might be possible to do something similar for elliptic curves in characteristic > 2, by using the results of this paper.

We have constructed hyperelliptic curves D_t over finite fields $\mathbb{F}_q$ whose Jacobian is isogenous to the Weil restriction with respect to $\mathbb{F}_{q^r}|\mathbb{F}_q$ of some elliptic curve (where $r = \frac{\ell-1}{2}$ for some prime ℓ). Let us assume that $r \geq 5$. If one were able to explicitely write down a map $(D_t)_{\mathbb{F}_{q^r}} \to E$ for some elliptic curve E over $\mathbb{F}_{q^r}$, or if one could just evaluate the induced map $E(\mathbb{F}_{q^r}) \to J_{D_t}(\mathbb{F}_{q^r})$, then one would have an algorithm to evaluate discrete logarithms on $E(\mathbb{F}_{q^r})$ that is faster than generic algorithms; cf. the appendix of [5]. We have so far not succeeded in finding such maps explicitely.

Acknowledgements. The research of Jasper Scholten is funded by the AREHCC project of the European Commission (Fifth Framework Program IST - 2001).

References

[1] Bosch, S., Lütkebohmert, W., Raynaud, M.: Néron Models. Berlin, Springer-Verlag, 1980
[2] Bouw, I.: The p-rank of ramified covers of curves. Compositio Math. **126** (3), 295–322 (2001)
[3] Bouw, I., Diem, C., Scholten, J.: Ordinary elliptic curves of high rank over $\overline{\mathbb{F}}_p(x)$ with constant j-invariant II. Forthcomming
[4] Crew, R.: Etale p-covers in characteristic p. Compositio Math. **52** (1), 31–45 (1984)
[5] Diem, C.: The GHS attack in odd characteristic. J. Ramanujan Math. Soc. **18** (1), 1–32 (2003)
[6] Diem, C., Naumann, N.: On the structure of Weil restrictions of abelian varieties. J. Ramanujan Math. Soc. **18** (2), 153–174 (2003)
[7] Ekedahl T., Serre J.-P.: Exemples de courbes algébriques à Jacobienne complètement décomposable. Acad, C.R. (ed.), Sci. Paris Sér. I Math. **317** (5), 509–513 (1993)
[8] Elkies, N.: Mordell-Weil lattices in characteristic 2.I. Construction and first properties, Internat. Math. Res. Notices **8**, 343–361 (1994)
[9] García, A., Stichtenoth, H.: Elementary abelian p-extensions of algebraic function fields. Manuscripta Math. **72** (1), 67–79 (1991)
[10] Gaudry, P., Hess, F., Smart, N.: Constructive and destructive facets of Weil descent on elliptic curves. J. Cryptology **15** (1), 19–46 (2002)

[11] Heath-Brown, D.: Artin's conjecture for primitive roots. Quart. J. Math. Oxford Ser. (2) **37** (145), 27–38 (1986)
[12] Hess, F.: The GHS Attack revisited. In: Biham, E (ed.), Advances in Cryptology Eurocrypt 2003, volume 2656 of LNCS, Berlin, Springer-Verlag, 2003, pp. 374–387
[13] Hooley, C.: On Artin's conjecture. J. Reine Angew. Math. **225**, 209–220 (1967)
[14] Kani, E., Rosen, M.: Idempotent relations and factors of Jacobians. Math. Ann. **284** (2), 307–327 (1989)
[15] Lang, S.: Algebra, 3rd edn. Addison-Wesley, 1993
[16] Lang, S., Néron, A.: Rational points of abelian varieties over function fields. Am. J. Math. **81** (1), 95–118 (1959)
[17] Lidl, R., Mullen, G., Turnwald, G.: Dickson polynomials. volume 65 of Pitman Monographs and Surveys in Pure and Applied Mathematics, Longman Scientific & Technical Harlow, 1993
[18] Menezes, A., Qu, M.: Analysis of the Weil descent attack of Gaudry, Hess and Smart. Topics in cryptology—CT-RSA 2001 (San Francisco CA), volume 2020 of LNCS, Springer, Berlin, 2001, pp. 308–318
[19] Mestre, J.-F.: Familles de courbes hyperelliptiques à multiplications réelles. Arithmetic algebraic geometry (Texel 1989), volume 89 of Progr. Math., Birkhäuser Boston, Boston, MA, 1991, pp. 193–208
[20] Milne, J.: On the arithmetic of abelian varieties. Invent. Math. **17**, 177–190 (1972)
[21] Mordell, L.: On the rational solutions of the indeterminate equation of the third and fourth degrees. Proc. Cambridge Philos. Soc. **29**, 179–192 (1922)
[22] Mumford, D.: Abelian varieties. Tata Institute for Fundamental Research, Bombay, 1970
[23] Néron, A.: Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algebrique dans un corps. Bull. Soc. Math. France **80**, 101–166 (1952)
[24] Serre, J.-P.: Sur la topologie des variétés algébriques en caractéristique p. Symposium internacional de topología algebraica International symposium on algebraic topology, Universidad Nacional Autónoma de México and UNESCO Mexico City, 1958, pp. 24–53
[25] Shafarevich, I., Tate, J.: The rank of elliptic curves. Dokl. Soviet Math. Dokl. **8** (4), 917–920 (1967)
[26] Shioda, T.: An explicit algorithm for computing the Picard number of certain algebraic surfaces. Am. J. Math. **108** (2), 415–432 (1986)
[27] Stichtenoth, H.: Algebraic Function Fields and Codes. Berlin, Springer-Verlag, 1993
[28] Tautz, W., Top, J., Verberkmoes, A.: Explicit hyperelliptic curves with real multiplication and permutation polynomials. Canad. J. Math. **43** (5), 1055–1064 (1991)
[29] Ulmer, D.: Elliptic curves with large rank over function fields. Ann. Math. **155** (1), 295–315 (2002)
[30] Waterhouse, W., Milne, J.: In: Lewis, D (ed.), Abelian varieties over finite fields. Proceedings of the 1969 Summer Institute on Number Theory, volume 20 of Proc. Sympos. Pure Math. American Mathematical Society, 1971, pp. 53–64
[31] Weil, A.: L'arithmétique sur les courbes algébriques. Acta Math. **52**, 281–315 (1928)
[32] Yui, N.: On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$. J. Algebra **52** (2), 378–410 (1978)