J. reine angew. Math. **458** (1995), 53—61

Journal für die reine und angewandte Mathematik

On the existence of supersingular curves of given genus

By *Gerard van der Geer* at Amsterdam and *Marcel van der Vlugt* at Leiden

---

Introduction

In this note we shall show that there exist supersingular curves for every positive genus in characteristic 2. Recall that an irreducible smooth algebraic curve C over an algebraically closed field $\mathbb{F}$ of characteristic $p > 0$ is called *supersingular* if its jacobian is isogenous to a product of supersingular elliptic curves. An elliptic curve is called supersingular if it does not have points of order p over $\mathbb{F}$. It is not clear a priori that there exist such curves for every genus. Indeed, note that in the moduli space $A_g \otimes \mathbb{F}_p$ of principally polarized abelian varieties the locus of supersingular abelian varieties has dimension $[g^2/4]$ (cf. [O], [L-O]), while the locus of jacobians has dimension $3g - 3$ for $g > 1$. Therefore, as far as dimensions are concerned there is no reason why these loci should intersect for $g \geqq 9$.

In this paper we construct for every integer $g > 0$ a supersingular curve of genus g over the field $\mathbb{F}_2$. In particular this shows that for every $g > 0$ there exists an irreducible curve of genus g whose jacobian is isogeneous to a product of elliptic curves. We refer to [E-S] for related questions in characteristic 0. We do our construction by taking a suitable fibre product of Artin-Schreier curves. This construction is inspired by coding theory, where the introduction of generalized Hamming weights led us to consider such products, cf. [G-V 2].

More generally, we are able to construct in odd characteristic p a supersingular curve over $\mathbb{F}_p$ of any genus g whose p-adic expansion consists of the digits 0 and $(p-1)/2$ only. We can also count on how many moduli the construction depends.

§ 1. Fibre products of Artin-Schreier curves

Let $\mathbb{F}$ be a fixed algebraic closure of the prime field $\mathbb{F}_2$. We consider a finite dimensional $\mathbb{F}_2$-linear subspace $\mathscr{L}$ of the function field $\mathbb{F}(x)$. Define the operator $\wp$ on $\mathbb{F}(x)$ by $\wp(f) = f^2 + f$. We shall assume that $\mathscr{L} \cap \wp(\mathbb{F}(x)) = \{0\}$.

To an element $f \in \mathscr{L} - \{0\}$ we associate the complete non-singular Artin-Schreier curve C_f with affine equation

$$y^2 + y = f.$$

Choose a basis $f_1, \ldots, f_k$ of $\mathscr{L}$ and let $\phi_i : C_{f_i} \to \mathbb{P}^1$ be the morphism given by the inclusion $\mathbb{F}(x) \subset \mathbb{F}(x, y)$. Then we define a curve $C^{\mathscr{L}}$ by

$$C^{\mathscr{L}} = \text{Normalization of } (C_{f_1} \times \cdots \times C_{f_k}),$$

where the product means the fibre product taken with respect to the morphisms ϕ_i. Up to $\mathbb{F}(x)$-isomorphism the curve $C^{\mathscr{L}}$ is independent of the chosen basis of $\mathscr{L}$.

In the following we need some properties of the curve $C^{\mathscr{L}}$; the reader can find a proof in [G-V 2].

(1.1) Proposition. (i) *The jacobian of $C^{\mathscr{L}}$ decomposes up to isogeny as*

$$\operatorname{Jac}(C^{\mathscr{L}}) \sim \prod_{f \in \mathscr{L} - \{0\}} \operatorname{Jac}(C_f)$$

and therefore the genus $g(C^{\mathscr{L}})$ can be expressed as

$$g(C^{\mathscr{L}}) = \sum_{f \in \mathscr{L} - \{0\}} g(C_f)$$

in terms of the genera of the C_f.

(1.2) Corollary. *Suppose that for all $f \in \mathscr{L} - \{0\}$ the curve C_f is supersingular or rational. Then the fibre product $C^{\mathscr{L}}$ is supersingular or rational.*

As ingredients for our fibre product we shall use special Artin-Schreier curves. We consider for $h \geqq 1$ the vector space $\mathscr{R}_h$ of 2-linearized polynomials

$$\left\{ R = \sum_{i=0}^{h} a_i x^{2^i} : a_i \in \mathbb{F} \right\}$$

and define

$$\mathscr{R}_h^* = \{ R \in \mathscr{R}_h : a_h \neq 0 \}.$$

We proved in [G-V 1] the following result.

(1.3) Proposition. *The Artin-Schreier curve C_R with affine equation $y^2 + y = xR(x)$ for $R \in \mathscr{R}_h^*$ is a (hyperelliptic) supersingular curve of genus 2^{h-1}.*

§ 2. The construction

In this section we describe how to construct a curve of a given genus in characteristic 2. Here the construction is done over a finite extension of the prime field. In Section 3 we shall show that we can find such a curve over the prime field $\mathbb{F}_2$.

(2.1) Theorem. *Let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_2$. For every positive genus g there exists a supersingular curve over $\mathbb{F}$.*

Proof. Take $g > 0$ and write g as a dyadic expansion in the form

$$(1) \qquad g = 2^{s_1}(1 + \cdots + 2^{r_1}) + 2^{s_2}(1 + \cdots + 2^{r_2}) + \cdots + 2^{s_t}(1 + \cdots + 2^{r_t}),$$

where $s_i, r_i \in \mathbb{Z}_{\geqq 0}$ and $s_i \geqq s_{i-1} + r_{i-1} + 2$ for $i = 2, \ldots, t$. We now choose for $i = 1, \ldots, t$ an $\mathbb{F}_2$-linear subspace L_i of $\mathbb{F}(x)$ contained in $\mathscr{R}^*_{u_i} \cup \{0\}$ with $u_i = (s_i + 1) - \sum_{j=1}^{i-1} (r_j + 1)$ and $\dim(L_i) = r_i + 1$. We put $\mathscr{L} = \bigoplus_{i=1}^{t} (xL_i)$. It follows directly from Propositions (1.1) and (1.3) that $C^{\mathscr{L}}$ is supersingular and that since $u_{i+1} \geqq u_i + 1$ for $1 \leqq i \leqq t-1$ the genus satisfies

$$\begin{aligned} g(C^{\mathscr{L}}) &= \sum_{f \in \mathscr{L} - \{0\}} g(C_f) \\ &= \sum_{i=1}^{t} 2^{u_i - 1} \cdot 2^{\sum_{j=1}^{i-1}(r_j+1)} (2^{r_i+1} - 1) \\ &= \sum_{i=1}^{t} 2^{s_i}(2^{r_i+1} - 1). \end{aligned}$$

This last expression yields the expression for g in (1), hence $g(C^{\mathscr{L}}) = g$. □

From the preceding proof we conclude that there exists supersingular curves of genus $g > 0$ already over the field $\mathbb{F}_{2^m}$ with $m = \max_{1 \leqq i \leqq t} (r_i + 1)$, where the t_i occur in the expansion (1).

Example. We construct a supersingular curve of genus 30. We write

$$30 = 2(1 + 2 + 2^2 + 2^3)$$

and this tells us that $t = 1$, $s_1 = 1$ and $r_1 = 3$. So our curve is defined over the finite field $\mathbb{F}_{16}$. We set $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ with $\alpha^4 + \alpha + 1 = 0$. Let $L \subset \mathscr{R}^*_{u_1} \cup \{0\} = \mathscr{R}^*_2 \cup \{0\}$ be the 4-dimensional space generated by x^4, αx^4, $\alpha^2 x^4$ and $\alpha^3 x^4$. Then $\mathscr{L} = xL$ and $C^{\mathscr{L}}$ is the desired supersingular curve of genus 30. Its function field $\mathscr{F} = \mathbb{F}_{16}(x, y_0, y_1, y_2, y_3)$ with $y_i^2 + y_i = \alpha^i x^5$ is a Galois extension of $\mathbb{F}_{16}(x)$ of degree 16. Consider the element $y = \sum_{i=0}^{3} \alpha^i y_i$. Then for all non-trivial $\sigma \in \mathrm{Gal}(\mathscr{F}/\mathbb{F}_{16}(x))$ we have $\sigma(y) \neq y$, hence $\mathscr{F} = \mathbb{F}_{16}(x, y)$. We obtain

$$\begin{aligned} y^{16} + y &= \sum_{i=0}^{3} \alpha^i (y_i^{16} + y_i) \\ &= \sum_{i=0}^{3} \alpha^i (\alpha^{8i} x^{40} + \alpha^{4i} x^{20} + \alpha^{2i} x^{10} + \alpha^i x^5) \\ &= \alpha^6 x^{40} + x^{20} + \alpha^{12} x^{10} + \alpha^9 x^5. \end{aligned}$$

Thus we have found a supersingular curve of genus 30 over the field $\mathbb{F}_{16}$ with affine equation

$$y^{16}+y=\alpha^6x^{40}+x^{20}+\alpha^{12}x^{10}+\alpha^9x^5 .$$

§ 3. Equations for fibre products

The preceding example suggests to study curves of the following type. We consider curves $C=C_{S,R}$ defined by an equation

$$S(y)=xR_1(x)+(xR_2(x))^2+\cdots+(xR_n(x))^{2^{n-1}}, \tag{2}$$

where $S\in\mathbb{F}[y]$ is a 2-linearized polynomial $S=y^{2^n}+A_{n-1}y^{2^{n-1}}+\cdots+A_0y$ with $A_0\neq 0$ and where the $R_i\in\mathbb{F}[x]$ for $i=1,\dots,n$ are also 2-linearized polynomials (not all 0). We shall assume for a moment that this equation defines an irreducible curve. Consider the $\mathbb{F}_2$-vector space

$$\Sigma=\{\sigma\in\mathbb{F}:S(\sigma)=0\} .$$

An element $\sigma\in\Sigma$ acts on C via $y\mapsto y+\sigma$. Thus the curve C is a Galois covering of $\mathbb{P}^1$ with Galois group of type $\Sigma\cong(\mathbb{Z}/2\mathbb{Z})^n$. An $\mathbb{F}_2$-linear subspace Σ' of Σ of codimension 1 defines an irreducible quotient curve C/Σ'. If $\sigma\in\Sigma-\Sigma'$ then the linear subspace Σ' corresponds to a splitting of

$$S=B(B+B(\sigma)), \tag{3}$$

where B is the 2-linearized monic polynomial of degree 2^{n-1} in $\mathbb{F}[y]$ with zero set Σ'. Note that $B(\sigma)\in\mathbb{F}^*$ is independent of the choice of $\sigma\in\Sigma-\Sigma'$. If we put

$$B=y^{2^{n-1}}+B_{n-2}y^{2^{n-2}}+\cdots+B_0y, \tag{4}$$

and $\beta=B(\sigma)$ then by comparing coefficients, (3) is equivalent to the system of equations

$$\begin{aligned}&\beta B_0+0=A_0,\\ &B_{i-1}^2+\beta B_i=A_i \quad\text{for}\quad i=1,\dots,n-2,\\ &B_{n-2}^2+\beta=A_{n-1}.\end{aligned} \tag{5}$$

The compatibility of (5) comes down to the equation

$$\sum_{j=1}^{n}\frac{A_{n-j}^{2^{j-1}}}{\beta^{2^j-1}}=1 \quad\text{or}\quad \beta^{2^n}+\sum_{j=1}^{n}A_{n-j}^{2^{j-1}}\beta^{2^n-(2^j-1)}=0 . \tag{6}$$

Observe that $\alpha=\beta^{-1}$ satisfies a *linearized* equation, namely

$$A_0^{2^{n-1}}\alpha^{2^n}+A_1^{2^{n-2}}\alpha^{2^{n-1}}+\cdots+A_{n-1}\alpha^2+\alpha=0 . \tag{7}$$

Define the $\mathbb{F}_2$-vector space

$$A = \{\alpha \in \mathbb{F} : \alpha \text{ satisfies } (7)\} .$$

The elements of $A - \{0\}$ parametrize the hyperplanes Σ' of Σ. The hyperplane corresponding to $\alpha \in A - \{0\}$ will be denoted by Σ_α. Moreover, we set

$$T = xR_1 + (xR_2)^2 + \cdots + (xR_n)^{2^{n-1}} .$$

(3.1) Lemma. *Each quotient curve $C_\alpha := C/\Sigma_\alpha$ with $\alpha \in A - \{0\}$ is of the form*

$$w^2 + w = \alpha^2 T, \tag{8}$$

where $w = \alpha B$ with B corresponding to Σ_α.

Proof. One checks that w is invariant under $y \mapsto y + \sigma$ with $\sigma \in \Sigma_\alpha$. Substitution of (3) in (2) yields (8). □

(3.2) Corollary. *The curve in* (8) *is $\mathbb{F}[x]$-isomorphic to*

$$w^2 + w = \alpha^2 xR_1 + \alpha xR_2 + \alpha^{2^{-1}} xR_3 + \cdots + \alpha^{2^{-(n-2)}} xR_n , \tag{9}$$

and therefore it is supersingular if not rational.

Proof. Consider the $\mathbb{F}[x]$-isomorphism

$$w \mapsto w + \sum_{i=2}^{n} \sum_{j=0}^{i-2} (\alpha^{2^{2-i}} xR_i)^{2^j} ,$$

and apply Proposition (1.3). □

(3.3) Proposition. *If the curve C defined by* (2) *is irreducible then it is a fibre product which is supersingular if not rational. Its jacobian is up to isogeny the product of the jacobians of the curves given in* (8) *with $\alpha \in A - \{0\}$.*

Proof. Choose an $\mathbb{F}_2$-basis of A, say $\alpha_1, \ldots, \alpha_n$. The curves $C_\alpha = C/\Sigma_\alpha$ are quotients of C, hence C admits a morphism $\phi : C \to C_{\alpha_1} \times \cdots \times C_{\alpha_n}$, the fibre product of the C_{α_i} with respect to the (canonical) maps $C_{\alpha_i} \to \mathbb{P}^1$. Since the α_i are $\mathbb{F}_2$-independent, Galois theory and Lemma (3.1) yield that the function fields of the curves $C_{\alpha_1} \times \cdots \times C_{\alpha_j}$ and $C_{\alpha_{j+1}}$ are linearly disjoint for $j = 1, \ldots, n-1$. So the fibre product $C_{\alpha_1} \times \cdots \times C_{\alpha_n}$ is a covering of degree 2^n of $\mathbb{P}^1$. Since C is also a covering of $\mathbb{P}^1$ of degree 2^n it follows that ϕ is an isomorphism. The proposition now follows from Proposition (1.1) and from Corollary (3.2). □

The condition that the curve C be irreducible is given in the following lemma.

(3.4) Lemma. *The curve defined by* (2) *is irreducible if and only if the n-dimensional $\mathbb{F}_2$-vector space $\mathscr{L}$ of functions $\alpha^2 T$ with $\alpha \in A$ satisfies $\mathscr{L} \cap \wp(\mathbb{F}(x)) = \{0\}$.*

Proof. The implication "⇒" follows from Proposition (3.3). As to the implication "⇐", we use the theory of Artin-Schreier extensions (see [B], Ch. V, § 11). According to that theory the compositum of the function fields $\mathbb{F}(x, w_\alpha)$ with $w_\alpha = \alpha B$ satisfying (8) has degree

$$\#(\mathscr{L}/\mathscr{L} \cap \wp(\mathbb{F}(x))) = 2^n$$

over $\mathbb{F}(x)$. Comparison with the degree of y in (2) shows the irreducibility. □

(3.5) Theorem. *For every integer $g > 0$ there exists a supersingular curve of genus g over the prime field $\mathbb{F}_2$.*

Proof. We construct a supersingular curve of the form (2) with prescribed genus $g > 0$. Recall the binary expansion of g given in (1)

$$g = 2^{s_1}(1 + \cdots + 2^{r_1}) + 2^{s_2}(1 + \cdots + 2^{r_2}) \cdots + 2^{s_t}(1 + \cdots + 2^{r_t})$$

where $s_i, r_i \in \mathbb{Z}_{\geqq 0}$ and $s_i \geqq s_{i-1} + r_{i-1} + 2$ for $i = 2, \ldots, t$. By w we denote the binary weight $w = \sum_{i=1}^{t} (r_i + 1)$ of g. First we determine the LHS $S(y) \in \mathbb{F}_2[y]$ of (2) and the w-dimensional $\mathbb{F}_2$-vector space A.

We start with $F_0(x) = x$ and we construct inductively a sequence of $\mathbb{F}_2$-linearized polynomials $F_i \in \mathbb{F}_2[x]$ for $i = 1, \ldots, t$ as follows. We set

$$F_i = (F_{i-1})^{2^{r_i+1}} + F_{i-1}\,.$$

Obviously, F_{i-1} divides F_i for $i = 1, \ldots, t$.

Let $S(y) = F_t(y) \in \mathbb{F}_2[y]$. It has degree 2^w. Furthermore we define $\mathbb{F}_2$-linear spaces

$$A^{(i)} = \{\alpha \in \mathbb{F} : F_i(\alpha) = 0\} \quad \text{for} \quad i = 1, \ldots, t\,.$$

We set $A = A^{(t)}$. By the divisibility property of the F_i the subspaces $A^{(i)}$ form a flag in A.

Now we consider for $1 \leqq i \leqq t-1$ the polynomials

$$F_i(\alpha, x) = F_i(\alpha)\, x^{2^{h_i}+1} \in \mathbb{F}_2[\alpha, x]\,,$$

where the $h_i = s_{i+1} - w + 1 + \sum_{j=i+1}^{t} (r_j + 1)$ form a monotonically increasing sequence. We define for $j = 0, \ldots, w-1$ polynomials $xR_{w-j}(x) \in \mathbb{F}_2[x]$ with R_{w-j} 2-linearized by writing

$$\sum_{i=1}^{t-1} F_i(\alpha, x) = \sum_{j=0}^{w-1} xR_{w-j}(x)\, \alpha^{2^j}\,.$$

Here xR_{w-j} is the sum (possibly empty) of those monomials $x^{2^{h_i}+1}$ occuring in the polynomials $F_i(\alpha, x)$ which have the monomial α^{2^j} as coefficient.

For $\alpha \in A - \{0\}$ the curves C_α with equation (9) can be written as

$$w^2 + w = F_{t-1}(\alpha)\, x^{2^{h_t}+1} + \cdots + F_0(\alpha)\, x^{2^{h_1}+1} \tag{10}$$

(after we have converted the coefficients $\alpha^2, \alpha, \ldots, \alpha^{2^{-(w-2)}}$ to $\alpha^{2^{w-1}}, \alpha^{2^{w-2}}, \ldots, \alpha$). For the $2^{w-(r_t+1)}(2^{r_t+1}-1)$ values of $\alpha \in A - A^{(t-1)}$ the irreducible Artin-Schreier curve C_α with equation (10) has genus $2^{s_t-(w-(r_t+1))}$ and these curves C_α contribute

$$2^{s_t}(1 + 2 + \cdots + 2^{r_t})$$

to the genus of the fibre product (2). The curves C_α with $\alpha \in A^{(t-1)} - A^{(t-2)}$ contribute $2^{s_{t-1}}(1 + 2 + \cdots + 2^{r_{t-1}})$ to the genus. Continuing in this way we see that the supersingular curve over $\mathbb{F}_2$ with affine equation

$$S(y) = xR_1 + (xR_2)^2 + \cdots + (xR_w)^{2^{w-1}}$$

has the prescribed genus. $\square$

Example. Take $g = 221 = 1 + 2^2(1+2+4) + 2^6(1+2)$. We have $s_1 = 0, s_2 = 2, s_3 = 6$; $r_1 = 0, r_2 = 2, r_3 = 1$ and $w = 6$. We find

$$F_0(x) = x, \quad F_1(x) = x^2 + x, \quad F_2(x) = x^{16} + x^8 + x^2 + x,$$
$$F_3(x) = x^{64} + x^{32} + x^{16} + x^4 + x^2 + x.$$

The space A equals $\{\alpha \in \mathbb{F} : F_3(\alpha) = 0\}$. For $i = 0, 1, 2$ the polynomials $F_i(\alpha, x)$ are

$$F_0(\alpha, x) = \alpha x^3, \quad F_1(\alpha, x) = (\alpha^2 + \alpha)x^5, \quad F_2(\alpha, x) = (\alpha^{16} + \alpha^8 + \alpha^2 + \alpha)x^9.$$

From the identity

$$\sum_{i=0}^{2} F_i(\alpha, x) = \sum_{j=0}^{w-1} xR_{w-j}(x)\,\alpha^{2^j}$$

we get

$$xR_6 = x^9 + x^5 + x^3, \quad xR_5 = x^9 + x^5, \quad xR_3 = x^9, \quad xR_2 = x^9, \quad xR_1 = xR_4 = 0.$$

This gives a supersingular curve of genus 221 defined by $F_3(y) = \sum_{k=1}^{6} (xR_k)^{2^{k-1}}$ i.e. by the equation

$$y^{64} + y^{32} + y^{16} + y^4 + y^2 + y = x^{288} + x^{160} + x^{144} + x^{96} + x^{80} + x^{36} + x^{18}.$$

§ 4. Number of moduli

Here we count the number of moduli for our families. In the investigation of the curves $y^2 + y = xR(x)$ for $R \in \mathscr{R}_h^*$ in [G-V 1] the polynomial

$$E_{h,R}(x) = R(x)^{2^h} + \sum_{i=0}^{h} (a_i x)^{2^{h-i}}$$

of degree 2^{2h} played an important role. We define the *radical* $\bar{W}_R$ of R as the subspace of $\mathbb{F}$ formed by the elements satisfying the equation $E_{h,R}(x) = 0$.

(4.1) Proposition. *Let $h \geqq 2$ and let $R = \sum_{i=0}^{h} a_i x^{2^i}$ and $R' = \sum_{i=0}^{h} a_i' x^{2^i}$ be elements of $\mathscr{R}_h^*$. Then the curves C_R and $C_{R'}$ are isomorphic over $\mathbb{F}$ if and only if there exists a $\varrho \in \mathbb{F}^*$ such that $a_i' = a_i \varrho^{2^i+1}$ for $i = 1, \ldots, h$.*

Proof. Since both C_R and $C_{R'}$ are hyperelliptic curves an isomorphism α induces an isomorphism $\alpha' : \mathbb{P}^1 \to \mathbb{P}^1$ which fixes the (unique) branch point ∞ and is of the form $x \mapsto \lambda x + \mu$ with $\lambda, \mu \in \mathbb{F}$, $\lambda \neq 0$. Let $\bar{W}_R$ (resp. $\bar{W}_{R'}$) be the radical of R (resp. of R'.) Then by [G-V 1] we have $\lambda^{-1} \bar{W}_R = \bar{W}_{R'}$. This implies that $E_{h,R}(\lambda X) = c_\lambda E_{h,R'}(X)$. By writing $X^{2^h} E_{h,R}(X) = \sum_i (U_i + U_i^{2^i})$ with $U_i = a_i^{2^{h-i}} X^{2^h + 2^{h-i}}$ we see that

$$\lambda^{2^h} c_\lambda a_i'^{2^{h-i}} = \lambda^{2^h + 2^{h-i}} a_i^{2^{h-i}} \quad \text{for} \quad i \geqq 1 \tag{11}$$

and

$$\lambda^{2^h} c_\lambda \in \mathbb{F}_{2^i}^* \quad \text{for all} \quad i \geqq 1 \quad \text{with} \quad a_i \neq 0 \, . \tag{12}$$

Relation (12) implies $\lambda^{2^h} c_\lambda \in \mathbb{F}_{2^d}^*$ with $d = \text{g.c.d.} \{i \geqq 1 : a_i \neq 0\}$. There exists an element $\eta \in \mathbb{F}_{2^d}^*$ such that we can write

$$\lambda^{2^h} c_\lambda = \eta^{(2^i+1)2^{h-i}} \quad \text{for} \quad i \geqq 1 \quad \text{with} \quad a_i \neq 0 \, . \tag{13}$$

Substituting (13) in (11) we find

$$a_i' = (\lambda / \eta)^{2^i+1} a_i \quad \text{for} \quad i = 1, \ldots, h \, .$$

Conversely, the relation $a_i' = \varrho^{2^i+1} a_i$ for $i = 1, \ldots, h$ shows that

$$\varrho x R(\varrho x) = x R'(x) + (\varrho^2 a_0 + a_0') x^2 \, .$$

Since for fixed $R \in \mathscr{R}^*$ and varying $a \in \mathbb{F}$ the curves C_{R+ax^2} are mutually isomorphic over $\mathbb{F}$ we conclude $C_R \cong C_{R'}$. □

Remark. The conclusion of the lemma still holds for $h = 1$ if we restrict to isomorphisms which are isomorphisms of Artin-Schreier coverings of $\mathbb{P}^1$ of degree 2.

(4.2) Corollary. *Let $n \geqq 1$. The intersection of the supersingular locus with the hyperelliptic locus in the moduli space $\mathscr{M}_{2^n} \otimes \mathbb{F}_2$ of curves of genus $g = 2^n$ has dimension $\geqq n$.*

Furthermore, consider two n-dimensional $\mathbb{F}_2$-subspaces L and L' of polynomials $R = \sum_{i=1}^{h} a_i x^{2^i} \in \mathbb{F}[x]$ with $a_1 \neq 0$ if $R \neq 0$. Let $\mathcal{L} = xL$ and $\mathcal{L}' = xL'$ and set $C = C^{\mathcal{L}}$ and $C' = C^{\mathcal{L}'}$. We then have:

(4.3) Lemma. *The curves C and C' are isomorphic as Galois covers of type $(\mathbb{Z}/2\mathbb{Z})^n$ of $\mathbb{P}^1$ if and only if there exists a $\varrho \in \mathbb{F}^*$ such that under $x \mapsto \varrho x$ the space $\mathcal{L}$ is transformed into $\mathcal{L}'$.*

Proof. If the curves C and C' are isomorphic as Galois covers of $\mathbb{P}^1$ then the corresponding quotient curves C_R and $C_{R'}$ of genus > 0 (for $R \in L$) are isomorphic as covers of $\mathbb{P}^1$. By Lemma (4.1) and the subsequent remark this happens only if there is a $\varrho \in \mathbb{F}^*$ such that the transformation $x \mapsto \varrho x$ transforms xR into xR' for $R \in L$. □

(4.4) Proposition. *Let $g \geqq 2$ be written as in* (1). *Then the supersingular locus in $\mathcal{M}_g \otimes \mathbb{F}_2$ has dimension $\geqq \sum_{i=1}^{t} (r_i + 1) u_i - 1$, where $u_i = (s_i + 1) - \sum_{j=1}^{i-1} (r_j + 1)$.*

Proof. We consider curves of the form $C^{\mathcal{L}}$ of genus $g \geqq 2$ with $\mathcal{L} = \bigoplus x L_i$ as in the proof of Theorem (2.1). Let $m = \sum_{i=1}^{t} (r_i + 1) u_i$. Then the m coefficients of the polynomials in a basis of $\mathcal{L}$ which is a union of the bases of the $(r_i + 1)$-dimensional summands xL_i in $\mathcal{R}_{u_i}^*$ define an open subset Q of affine m-space $\mathbb{A}_{\mathbb{F}}^m$. Take the $(m-1)$-dimensional quotient of Q under the action of $\mathbb{F}^*$. A given curve C of genus > 1 can be written only in finitely many ways as a Galois cover of $\mathbb{P}^1$ since $\# \mathrm{Aut}(C)(\mathbb{F}) < \infty$. Then Lemma (4.3) implies that the natural morphism $Q \to \mathcal{M}_g \otimes \mathbb{F}_2$ is quasi-finite (onto its image). This proves our result. □

References

[B] *Bourbaki*, Algèbre, Chapitres 4 à 7, Masson, Paris 1981.

[E-S] *T. Ekedahl, J.-P. Serre*, Exemples de courbes algébriques à jacobienne complètement décomposable, C.R. Acad. Sci. Paris **317** (1993), 509–513.

[G-V 1] *G. van der Geer, M. van der Vlugt*, Reed-Muller codes and supersingular curves I, Comp. Math. **84** (1992), 333–367.

[G-V 2] *G. van der Geer, M. van der Vlugt*, Fibre products of Artin-Schreier curves and generalized Hamming weights of codes, Report **93-05**, University of Amsterdam (1993), J. Comb. Th. A., to appear.

[L-O] *K.-Z. Li, F. Oort*, Moduli of supersingular abelian varieties, Preprint **824**, Universiteit Utrecht (1993).

[O] *F. Oort*, Moduli of abelian varieties and Newton polygons, C.R. Acad. Sci. Paris **312** (1991), 385–389.

Faculteit Wiskunde en Informatica, Universiteit van Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands

Mathematisch Instituut, Rijksuniversiteit te Leiden, Niels Bohrweg 1, 2300 RA Leiden, The Netherlands

Eingegangen 7. April 1994