Mathematical Research Letters **9**, 639–650 (2002)

FAMILIES OF SUPERSINGULAR CURVES IN CHARACTERISTIC 2

Jasper Scholten and Hui June Zhu

Abstract. This paper determines normal forms of all hyperelliptic supersingular curves of genus g over an algebraically closed field F of characteristic 2 for $1 \leq g \leq 8$. We also show that every hyperelliptic supersingular curve of genus 9 over F has an equation $y^2 - y = x^{19} + c^8x^9 + c^3x$ for some $c \in \overline{\mathbb{F}}_2$. Consequently, the paper determines the dimensions of the open locus of hyperelliptic supersingular curves of genus $g \leq 9$ over $\overline{\mathbb{F}}_2$.

1. Introduction

In this paper, a curve is a projective, smooth and geometrically integral algebraic variety of dimension 1. A curve is *supersingular* if its Jacobian is a supersingular abelian variety, that is, its Newton polygon is a straight line segment of slope 1/2. See Introduction and Appendix of [7] for literatures on supersingular abelian varieties and related open questions on stratification in the moduli space of abelian varieties. It has been proved that there are supersingular curves of every genus over $\overline{\mathbb{F}}_2$ (see [11]), but it is not settled for which genera there are hyperelliptic supersingular curves over $\overline{\mathbb{F}}_2$, which was an initial goal of our study (see [8]). Several isolated discoveries of supersingular curves have yielded unprecedented applications in sphere packing (see [2], [3] and [4]). There are also rich literatures in coding theory upon applications of supersingular curves (see [12]). See the introduction in [8] for more recent progress regarding the hyperelliptic supersingular curves in characteristic 2. In [5, page 3216] the question is raised for which p and g there are positive dimensional families of hyperelliptic supersingular curves over $\overline{\mathbb{F}}_p$ of genus g. We give an answer to this question for $p = 2$ and $g \leq 9$ in Theorem 2.

Definition 1. A family of equations of curves such that there are only finitely many equations in the family that define the same curve upto isomorphism is called a *normal form*.

Received April 2, 2002.
Revised version received August 12, 2002.
2000 *Mathematics Subject Classification.* 11L, 14H, 14M.
Key words and phrases. supersingular curves, hyperelliptic curves, normal forms, moduli space of curves.

Let F be an algebraically closed field of characteristic 2, and X a genus-g hyperelliptic curve defined over F. A necessary condition for X to be supersingular is that its Jacobian doesn't have any 2-torsion (over F), i.e., its Jacobian has 2-rank zero. Every genus-g hyperelliptic curve F of 2-rank zero has an affine equation

$$X:\ y^2 - y \quad = \quad c_{2g+1}x^{2g+1} + c_{2g-1}x^{2g-1} + \ldots + c_1 x, \tag{1}$$

where $c_1, \ldots, c_{2g-1} \in F$ and $c_{2g+1} = 1$. (See [8, Proposition 4.1].) For $g \leq 8$ we shall find conditions on the c_ℓ such that every genus-g hyperelliptic supersingular curve has an equation (1) with the c_ℓ satisfying these conditions. Moreover, there are only finitely many such equations for each curve. This family of equations will be a normal form.

Let $\mathcal{HS}_g/F$ denote the open locus of hyperelliptic supersingular curves of genus g over F in the moduli space of principally polarized abelian varieties.

Theorem 2. *Let F be an algebraically closed field of characteristic 2. Normal forms of hyperelliptic supersingular curves over F of genus $g \leq 8$ are in the table below with all $c_\ell \in F$. The dimension of $\mathcal{HS}_g/F$ is in the right column.*

genus g	*normal form X_g*	$\dim(\mathcal{HS}_g/F)$
1	$y^2 - y = x^3$	0
2	$y^2 - y = x^5 + c_3x^3$	1
3	*none*	$-\infty$
4	$y^2 - y = x^9 + c_5x^5 + c_3x^3$	2
5	$y^2 - y = x^{11} + c_3x^3 + c_1x$	2
6	$y^2 - y = x^{13} + c_3x^3 + c_1x$	2
7	*none*	$-\infty$
8	$y^2 - y = x^{17} + c_9x^9 + c_5x^5 + c_3x^3$	3

TABLE 1. normal forms for $g \leq 8$

Remark 3. From Theorem 2 one can easily derive explicit criteria for X given by (1) to be supersingular: If $g = 1$ or 2, then all 2-rank zero curves are supersingular. If $g = 3$ or 7, then none of these curves is supersingular. If $g = 4$ then X is supersingular if and only if $c_7 = 0$. If $g = 5$ then X is supersingular if and only if $c_7 = 0$ and $c_9c_{11} = c_5^4$. If $g = 6$ then X is supersingular if and only if $c_7 = 0$, $c_{11} = 0$, and $c_5c_{13} = c_9^2$. If $g = 8$ then X is supersingular if and only if $c_{15} = c_{13} = c_{11} = c_7 = 0$.

Remark 4. We anticipate some results of a similar sort for Artin-Schreier curves in characteristic p if p is small compared to the genus. For some results for p large, see [9] and [13].

The proof of Theorem 2 splits into two parts: In Section 4 we show that all curves in Table 1 are supersingular. In Section 5 we show that every supersingular curve of genus ≤ 8 has an equation in Table 1. One main idea in the proof

of Theorem 2 is to use the key lemma of [9] to reduce the initial problem to a combinatorial problem. Then we formulate an algorithm, utilizing [8, Proposition 4.1 and Theorem 1.1], to prove our assertion. Finally we discuss our result on $g = 9$ in Section 6.

2. 2-adic box and r-tiling sequence

Set $d := 2g + 1$ for the rest of the paper.

Let $s(\cdot)$ denote the number of 1's in the binary expansion of a positive integer. Let $(\cdot)_2$ denote the binary expantion of a given integer. Let S be a finite set of positive integers. For any positive integer r, an *r-tiling sequence* (of length ν) is a sequence of integer pairs $\{[b_i, \ell_i]\}_{i=1}^{\nu}$ such that

1. $\ell_i \in S$, $0 \le b_i \le b_{i+1}$;
2. $\ell_i > \ell_{i+1}$ if $b_i = b_{i+1}$;
3. $\sum_{i=1}^{\nu} \ell_i 2^{b_i} = r$.

If no such sequence exists we set $\tilde{s}(r, S) := \infty$; otherwise, we denote by $\tilde{s}(r, S)$ the length of the shortest r-tiling sequences, i.e., the minimal ν for which there exists an r-tiling sequence. Let $\tilde{K}(r, S)$ denote the set of all shortest r-tiling sequences. For any r-tiling sequence $M = \{[b_i, \ell_i]\}_{i=1}^{\nu}$, let $\tilde{S}(M) := \{\ell_1, \ldots, \ell_\nu\}$.

Example 5. Put $r = 2^{17} - 2^2$ and $S = \{1, 3, 9, 11\}$. Observe that the binary expansion of r has 15 consecutive 1's followed by two 0's. To make the shortest r-tiling sequence, ideally one has to choose $\ell \in S$ with highest $s(\ell)$ possible and such that every 1 in $(\ell)_2$ contributes to r when added up with each other. In this example, $(9)_2 = 1001$ and $(11)_2 = 1011$ make 5 consecutive 1's if added as

$$\begin{array}{cccccc} & & & 1 & 0 & 0 & 1 \\ +) & 1 & 0 & 1 & 1 & & \\ \hline & & 1 & 1 & 1 & 1 & 1 \end{array}$$

Thus to make 15 consecutive 1's we just have to combine 3 such blocks. The shortest r-tiling sequence is demonstrated below. The only way to make a

											1	0	0	1	0	0	[2, 9]
										1	0	1	1	0	0	0	[3, 11]
						1	0	0	1	0	0	0	0	0	0	0	[7, 9]
					1	0	1	1	0	0	0	0	0	0	0	0	[8, 11]
	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	[12, 9]
+)	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	[13, 11]
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	$(2^{17} - 2^2)_2$

TABLE 2. The shortest $(2^{17} - 2^2)$-tiling sequence

shorter r-tiling sequence is to use more of the form $[*, 11]$'s in the sequence,

which is impossible since more 11 will not make consecutive 1's in its sum unless some 1's do not contribute to the sum. So $\tilde{s}(r,S) = 6$ and $\tilde{K}(r,S) = \{\{[2,9],[3,11],[7,9],[8,11],[12,9],[13,11]\}\}$. To save space, for an r-tiling such as in Table 2 we shall often adopt the following way of representation

$$2^{17} - 2^2 \quad = \quad 11 \cdot 2^{13} + 9 \cdot 2^{12} + 11 \cdot 2^8 + 9 \cdot 2^7 + 11 \cdot 2^3 + 9 \cdot 2^2.$$

If this shortest r-tiling sequence is called M, then $\tilde{S}(M) = \{9, 11\}$.

Recall the 2-adic box $\boxed{\mathbf{k}}$ and notation in [8, Section 2]. We have

$$\begin{aligned} \mathbf{K}_r &:= \{\mathbf{k} = {}^t(k_1, k_2, \ldots, k_d) \in \mathbb{Z}^d \mid k_1 \geq k_2 \geq \cdots \geq k_d \geq 0, \sum_{\ell=1}^{d} k_\ell = r\} \\ s(\mathbf{k}) &:= s(k_1 - k_2) + s(k_2 - k_3) + \ldots + s(k_{d-1} - k_d) + s(k_d). \end{aligned}$$

Lemma 6. *For any positive integer r and a finite set S of positive integers, there is a bijection between the set $\tilde{K}(r,S)$ of shortest r-tiling sequences and the set*

$$\{\mathbf{k} \in \mathbf{K}_r \mid s(\mathbf{k}) = \tilde{s}(r,S) \text{ and } k_\ell = k_{\ell+1} \text{ for all } \ell \notin S\}.$$

Proof. We shall define the map first. An r-tiling sequence $\{[b_i, \ell_i]\}_{i=1}^{\tilde{s}(r,S)} \in \tilde{K}(r,S)$ is sent to the element $\mathbf{k} \in \mathbf{K}_r$ whose *2-adic box* $\boxed{\mathbf{k}}$ has $k_{\ell,v} = \#\{i \mid v = b_i \text{ and } \ell \leq \ell_i\}$. Conversely, given $\mathbf{k} \in \mathbf{K}_r$ with $k_\ell = k_{\ell+1}$ for $\ell \notin \mathrm{supp}X$, one defines $\{[b_i, \ell_i]\}_{i=1}^{s(\mathbf{k})}$ as follows: For v such that $k_{1,v} \neq 0$ and for i such that $\sum_{j=0}^{v-1} k_{1,j} < i \leq \sum_{j=0}^{v} k_{1,j}$ let $b_i := v$. Let $m_1 > \ldots > m_{k_{1,v}} > 0$ be the sequence of positive integers such that $k_{m_1,v} > k_{m_2,v} \ldots > k_{m_{k_{1,v}},v}$ and such that $k_{m_j} > k_{m_j+1}$. Note that $m_j \in S$. Define $\ell_i := m_{i - \sum_{j=0}^{v-1} k_{j,v}}$. The detailed verification of the bijectivity of the map is routine (but tedious) so is omitted here. (We illustrate this bijection in Example 7.) □

Example 7 (see Table 3)**.** Let r and S be as in Example 5. The block above the double horizontal lines is the 2-adic box $\boxed{\mathbf{k}}$, with the i-th line equal to the binary expansions of k_i for $i = 1, \ldots, 11$. The 6 lines immediately beneath the double horizontal lines are the (nonzero) column sums of $\boxed{\mathbf{k}}$ added up in the order from right to left. Each line represents $[b_i, \ell_i]$ for $i = 1, \ldots, 6$ in the same way as in Table 2. The sum of all these column sums is equal to the binary expansion of r, as shown in the last line.

3. Supersingularity criterion

Let X be as defined with affine equation in (1). Let $\mathrm{NP}_1(X)$ be the first slope of the Newton polygon of X (see Introduction of [8]). Recall that $d := 2g + 1$. Define the set of *supports* of X by $\mathrm{supp}X := \{\ell \in \mathbb{Z} \mid c_\ell \neq 0\}$. For $r \geq 1$ let

$$\tilde{C}(r, \mathrm{supp}X) := \sum_{M \in \tilde{K}(r, \mathrm{supp}X)} \prod_{[b,\ell] \in M} c_\ell^{2^b} \in F. \tag{2}$$

	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	$(k_1)_2$
	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	$(k_2)_2$
	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	$(k_3)_2$
	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	$(k_4)_2$
	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	$(k_5)_2$
	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	$(k_6)_2$
	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	$(k_7)_2$
	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	$(k_8)_2$
	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	$(k_9)_2$
	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	$(k_{10})_2$
+)	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	$(k_{11})_2$
												1	0	0	1	0	0	$[b_1, \ell_1]$
											1	0	1	1	0	0	0	$[b_2, \ell_2]$
							1	0	0	1	0	0	0	0	0	0	0	$[b_3, \ell_3]$
						1	0	1	1	0	0	0	0	0	0	0	0	$[b_4, \ell_4]$
		1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	$[b_5, \ell_5]$
+)	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	$[b_6, \ell_6]$
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	$(r)_2$

TABLE 3. The 2-adic box and the minimal length r-tiling sequence

Lemma 8. *Let notations be as above. Let λ be a rational number with $0 \leq \lambda \leq 1/2$.*

(a) *Suppose that for all $m \geq 1$, $n \geq 1$, and $1 \leq j \leq g$ one has*

$$\tilde{s}(m2^{n+g-1} - j, \mathrm{supp}X) \quad \geq \quad \lceil n\lambda \rceil.$$

Then

$$\mathrm{NP}_1(X) \quad \geq \quad \lambda.$$

(b) *Suppose $\mathrm{NP}_1(X) \geq \lambda$. Suppose there are positive integers $1 \leq j \leq g$, $n_0 \geq 1$ such that*
(1) *for all $m \geq 1, 1 \leq n < n_0$ and for all $m \geq 2, n = n_0$ we have*

$$\tilde{s}(m2^{n+g-1} - j, \mathrm{supp}X) \quad \geq \quad \lceil n\lambda \rceil ;$$

(2) $\tilde{s}(2^{n_0+g-1} - j, \mathrm{supp}X) = \lceil n_0\lambda \rceil - 1$.
Then

$$\tilde{C}(2^{n_0+g-1} - j, \mathrm{supp}X) \quad = \quad 0.$$

Proof. Let $W(F)$ be the ring of Witt vectors of F. Let $a_\ell \in W(F)$ be a lift of $c_\ell \in F$. From the bijection discussed in Lemma 6 it follows that $\tilde{s}(r, \mathrm{supp}X) = \min\{s(\mathbf{k}) \mid \mathbf{k} \in \mathbf{K}_r, \text{ and } k_\ell = k_{\ell+1} \text{ for all } \ell \notin \mathrm{supp}X\}$. Recall the definition of

$C_r(N)$ from [8]; we know from there that

$$C_r(N) \equiv \sum_{\mathbf{k}\in\mathbf{K}_r} 2^{s(\mathbf{k})} \prod_{\ell=1}^{d-1} a_\ell^{k_\ell - k_{\ell+1}} \bmod 2^{\tilde{s}(r,\mathrm{supp}X)+1}.$$

Since $\mathrm{ord}_2(C_r(N)) \geq \tilde{s}(r,\mathrm{supp}X)$, we have

$$\frac{C_r(N)}{2^{\tilde{s}(r,\mathrm{supp}X)}} \equiv \sum_{\mathbf{k}\in\mathbf{K}_r} 2^{s(\mathbf{k})-\tilde{s}(r,\mathrm{supp}X)} \prod_{\ell=1}^{d-1} c_\ell^{k_\ell - k_{\ell+1}} \bmod 2 = \tilde{C}(r,\mathrm{supp}X). \tag{3}$$

Now apply [8, Key-Lemma 2.1], one concludes with (a) and (b). □

Corollary 9. *Let notations be as above. Let* $\sigma := \max_{\ell\in\mathrm{supp}X} s(\ell)$. *Then we have* $\mathrm{NP}_1(X) \geq 1/\sigma$.

Proof. For $r = m2^{n+g-1} - j$ consider any r-tiling sequence given by $m2^{n+g-1} - j = \sum_{i=1}^{\nu} \ell_i 2^{b_i}$. Clearly we have

$$\nu\sigma \geq \sum_{i=1}^{\nu} s(\ell_i) = \sum_{i=1}^{\nu} s(\ell_i 2^{b_1}) \geq s(m2^{n+g-1} - j) \geq n,$$

so $\nu \geq \lceil \frac{n}{\sigma} \rceil$. In particular $\tilde{s}(m2^{n+g-1} - j, \mathrm{supp}X) \geq \lceil \frac{n}{\sigma} \rceil$. By Lemma 8a we have $\mathrm{NP}_1(X) \geq 1/\sigma$. □

Corollary 10. *Any curve* X *given by an equation of the form* $y^2 - y = \sum_{i=0}^{s} c_i x^{2^i+1}$ *over* F *is supersingular.*

Proof. (This result was proved in [11] in the case $F = \overline{\mathbb{F}}_2$.) Applying Corollary 9 we get $\sigma = 2$ and so $\mathrm{NP}_1(X) \geq 1/2$. □

Corollary 11. *Suppose* X *given by equation (1) is supersingular. Let* n_0 *and* j *be positive integers satisfying the hypothesis of Lemma 8b for* $\lambda = \frac{1}{2}$. *Suppose the set* $\tilde{K}(2^{n_0+g-1} - j, \mathrm{supp}X)$ *consists of one element* M. *Then we have* $\tilde{S}(M) \neq \{2g+1\}$ *and if* $\tilde{S}(M) = \{\ell, 2g+1\}$ *with* $1 \leq \ell \leq 2g$, *then* $c_\ell = 0$.

Proof. Suppose $\tilde{S}(M) = \{2g+1\}$, then by Lemma 8b we have $\tilde{C}(2^{n_0+g-1} - j, \mathrm{supp}X) = 0$. But it is easily seen that

$$\tilde{C}(2^{n_0+g-1} - j, \mathrm{supp}X) = \prod_{[b,2g+1]\in M} c_{2g+1}^{2^b} = 1$$

because $c_{2g+1} = 1$. Contradiction. This proves the first assertion.

Now suppose $\tilde{S}(M) = \{\ell, 2g+1\}$. By Lemma 8 again, we have

$$\begin{aligned} \tilde{C}(2^{n_0+g-1} - j, \mathrm{supp}X) &= \prod_{[b,\ell]\in M} c_\ell^{2^b} \prod_{[b',2g+1]\in M} c_{2g+1}^{2^{b'}} \\ &= \prod_{[b,\ell]\in M} c_\ell^{2^b} = c_\ell^{\sum_{[b,\ell]\in M} 2^b} = 0. \end{aligned}$$

Thus $c_\ell = 0$. □

4. Curves in Table 1 are supersingular

The supersingularity of X_8 follows from Corollary 10. The supersingularity of the curve $C : y^2 - y = x^{33} + c_3x^9 + c_1x^3$ over F also follows from Corollary 10. By observing that C covers X_5, the supersingularity of X_5 follows.

Now we claim that X_6 is supersingular by a method suggested to us by Noam Elkies. We present it below: Let E be the elliptic curve defined by $y^2 - y = x^3 + t^{13} + c_3t^3 + c_1t$ over $F(t)$, which can be viewed as a quadratic twist of $E_0 : y^2 - y = x^3$ over the function field $F(X_6)$ of X_6. The curve X_6 is supersingular if and only if the rank of $E(F(t))$ is 24, the maximal possible (see [10], page 917). In the same vein as in [3, pages 3–4], one can show that the canonical height of a nonzero point in $E(F(t))$ is ≥ 8. We shall show in the next paragraph that there are 196560 nonzero points with the minimal canonical height 8. Since there are no lattices of rank ≤ 23 with that many vectors of minimal length [1, page 23], this implies that $E(F(t))$ has rank 24 and the supersingularity of X_6 follows.

If $P = (x, y)$ is a point in $E(F(t))$ with x-coordinate of the form

$$x = a^{-16}t^6 + a^{-28}t^4 + a^{-40}t^2 + a^{32}t + x_0 + a^{-64}(t - t_0)^{-2},$$

for $a \in F^*$ and $x_0, t_0 \in F$, then P has canonical height 8 (see [2, Proposition 2]). Following closely the computations presented in [3, page 6–7], one finds that P lies in $E(F(t))$ if a, x_0 and t_0 satisfy the following equations:

$$a^{4096} + c_3^{32}a^{1024} + c_1^{16}a^{256} + c_3^{16}a^{64} + c_1^4a^{16} + c_3^2a^4 + a = 0; \tag{4}$$

$$a^{36}t_0^6 + a^{24}t_0^4 + a^{12}t_0^2 + a^{84}t_0 + a^{1092} + c_3^8a^{324} + a^{312} + a^{156} + c_1^4a^{132} + c_3^2a^{120} + a^{117} + c_3a^{84} + 1 = 0; \tag{5}$$

$$a^{576} + a^{264} + {c_3}^4a^{192} + (x_0^4 + x_0)a^{160} + a^{108} + t_0^8 = 0. \tag{6}$$

(One may also check alternatively that the solutions to these 3 equations indeed yield x-coordinates of points in $E(F(t))$.) These 3 equations are separable in a, t_0 and x_0 respectively since their derivatives are nonzero constant. The number of nonzero solutions a of (4) is 4095. For each such a there are 6 solutions of t_0 satisfying (5). For each pair of (a, t_0) there are 4 solutions of x_0 satisfying (6). So there are totally $4095 \cdot 6 \cdot 4$ possible x-coordinates, each of which yields two points. This results in $2 \cdot 4 \cdot 6 \cdot 4095 = 196560$ points in $E(F(t))$.

5. Proof of Theorem 2

We complete our proof of Theorem 2 here. For the rest of the paper we shall suppress the supp$X$ from the notations $\tilde{C}(r, \text{supp}X)$, $\tilde{K}(r, \text{supp}X)$ and $\tilde{s}(r, \text{supp}X)$. For every genus we start with a curve with an equation in a box. Then we use supersingularity criteria Lemma 8 and [8, Theorem 1.1 and Proposition 4.1] to derive conditions on the coefficients, also denoted in boxes. These conditions accumulate to our desired equation declared in Table 1.

Remark 12. If there are indeed positive integers j, n_0 satisfying the hypothesis of Lemma 8b for some λ, then it is a finite problem to find them and verify. To see this, let $\tilde{T}(\nu, j)$ be the set of all sequences $\{[b_i, \ell_i]\}_{i=1}^{v}$ satisfying (b) and that

$\sum_{i=1}^{\nu} \ell_i 2^{b_i} \equiv -j \bmod 2^{b_\nu}$. Clearly, $\tilde{T}(\nu, j)$ is a finite set, and if $\nu = \tilde{s}(2^{n_0+g-1}-j)$ for some n_0, then $\tilde{T}(\nu, j)$ contains $\tilde{K}(m2^{n_0+g-1} - j)$ for every m with

$$\tilde{s}(m2^{n_0+g-1} - j) \leq \tilde{s}(2^{n_0+g-1} - j).$$

So one can verify if (b) is satisfied by computing $\tilde{T}(\nu, j)$ for $1 \leq j \leq g$ and for $\nu \geq 1$, and check for each such ν and j whether there exist n_0 with the required property.

Below we mention several times that we have checked the hypothesis of Lemma 8b in a particular case. By this we mean that we have verified it with a computer that runs the aforementioned algorithm, together with a few isolated tricks to accelerate the program. For instance, we use an observation that if two sequences $\{[b_i, \ell_i]\}_{i=1}^{\nu}$ and $\{[b'_i, \ell'_i]\}_{i=1}^{\nu'}$ satisfy $\sum_{i=1}^{\nu} \ell_i 2^{b_i} = \sum_{i=1}^{\nu'} \ell'_i 2^{b'_i}$ and $\nu' < \nu$, then one can ignore all sequences including $\{[b_i, \ell_i]\}_{i=1}^{\nu}$ as a subsequence.

5.1. $g = 5$**.** Suppose X is a hyperelliptic supersingular curve over F of genus 5. By [8, Theorem 1.1II) and Proposition 4.1] it has an equation

$$\boxed{y^2 - y = x^{11} + c_9 x^9 + c_3 x^3 + c_1 x}$$

for some $c_1, c_3, c_9 \in F$.

Let $\mathrm{supp}X = \{1, 3, 9, 11\}$. Let $g = 5$. We checked that for $n_0 = 13$, and $j = 4$ the conditions of Lemma 8b are satisfied, and $\tilde{K}(2^{n_0+g-1} - j)$ consists of a unique element M as follows

$$2^{17} - 4 = 11 \cdot 2^{13} + 9 \cdot 2^{12} + 11 \cdot 2^8 + 9 \cdot 2^7 + 11 \cdot 2^3 + 9 \cdot 2^2.$$

Note that $\tilde{S}(M) = \{9, 11\}$. (See Example 5.) Then Corollary 11 implies that $\boxed{c_9 = 0}$.

5.2. $g = 6$**.** Suppose X is a hyperelliptic supersingular curve over F of genus 6. By [8, Theorem 1.1III) and Proposition 4.1] it has an equation

$$\boxed{y^2 - y = x^{13} + c_9 x^9 + c_3 x^3 + c_1 x}$$

for some $c_1, c_3, c_9 \in F$.

Let $\mathrm{supp}X = \{1, 3, 9, 13\}$. Let $g = 6$. We checked that for $n_0 = 17$, and $j = 4$ the conditions of Lemma 8b are satisfied, and $\tilde{K}(2^{n_0+g-1} - 4)$ consists of a unique element M as follows

$$2^{22} - 4 = 9 \cdot 2^{18} + 13 \cdot 2^{17} + 9 \cdot 2^{13} + 13 \cdot 2^{12} + 9 \cdot 2^8 + 13 \cdot 2^7 + 9 \cdot 2^3 + 13 \cdot 2^2.$$

Note that $\tilde{S}(M) = \{9, 13\}$. By Corollary 11 we have $\boxed{c_9 = 0}$.

5.3. $g = 8$**.** Suppose X is a hyperelliptic supersingular curve over F of genus 8. By [8, Theorem 1.1II) and Proposition 4.1], it has an equation

$$\boxed{y^2 - y = x^{17} + c_{13} x^{13} + c_{11} x^{11} + c_9 x^9 + c_7 x^7 + c_5 x^5 + c_3 x^3}$$

for some $c_\ell \in F$.

Let $\mathrm{supp}X = \{3, 5, 7, 9, 11, 13, 17\}$. We found for $k = 0, 1, 2, 3, 4$ and 5 that $\tilde{K}(2^{21-3k} - 8)$ consists of sequences $\{[b_i, \ell_i]\}_{i=1}^{6-k}$ with either $[b_{6-k}, \ell_{6-k}] = [18 -$

$3k, 7]$ or $[b_{6-k}, \ell_{6-k}] = [17 - 3k, 13]$ and $[b_{5-k}, \ell_{5-k}] = [15 - 3k, 11]$. Hence we get

$$\begin{aligned}
\tilde{C}(2^{21}-8) &= c_7^{2^{18}}\tilde{C}(2^{18}-8) + (c_{11}c_{13}^4)^{2^{15}}\tilde{C}(2^{15}-8)\\
\tilde{C}(2^{18}-8) &= c_7^{2^{15}}\tilde{C}(2^{15}-8) + (c_{11}c_{13}^4)^{2^{15}}\tilde{C}(2^{12}-8)\\
\tilde{C}(2^{15}-8) &= c_7^{2^{12}}\tilde{C}(2^{12}-8) + (c_{11}c_{13}^4)^{2^{15}}\tilde{C}(2^{9}-8)\\
\tilde{C}(2^{12}-8) &= c_7^{2^{9}}\tilde{C}(2^{9}-8) + (c_{11}c_{13}^4)^{2^{15}}\tilde{C}(2^{6}-8)\\
\tilde{C}(2^{9}-8) &= c_7^{2^{6}}\tilde{C}(2^{6}-8) + (c_{11}c_{13}^4)^{2^{15}}\tilde{C}(2^{3}-8)\\
\tilde{C}(2^{6}-8) &= c_7^{2^{3}}\tilde{C}(2^{3}-8).
\end{aligned}$$

We checked that the conditions of Lemma 8b are satisfied for $\lambda = \frac{1}{2}$, $n_0 = 11$ and $j = 8$. Hence $\tilde{C}(2^{18}-8) = 0$. We also checked that they are satisfied for $\lambda = \frac{4}{9}$, $n_0 = 14$ and $j = 8$. Hence $\tilde{C}(2^{21}-8) = 0$. All these equations imply $\boxed{c_7 = 0}$ and $c_{11}c_{13} = 0$.

Suppose $c_{11} = 0$. Let $\mathrm{supp}X = \{3, 5, 9, 13, 17\}$. We checked that for $\lambda = \frac{1}{2}$, $j = 4$ and $n_0 = 19$ the conditions of Lemma 8b are satisfied, and $\tilde{K}(2^{n_0+g-1}-4)$ consists of a unique element M as follows

$$\begin{aligned}
2^{26}-4 &= 13\cdot 2^{22} + 17\cdot 2^{19} + 13\cdot 2^{18} + 13\cdot 2^{14} + 17\cdot 2^{11} + 13\cdot 2^{10}\\
&\quad +13\cdot 2^{6} + 17\cdot 2^{3} + 13\cdot 2^{2}.
\end{aligned}$$

Note that $\tilde{S}(M) = \{13, 17\}$. By Corollary 11 we have $\boxed{c_{13} = 0}$.

Suppose $c_{13} = 0$. Let $\mathrm{supp}X = \{3, 5, 9, 11, 17\}$. We checked that for $\lambda = \frac{1}{2}$, $j = 4$ and $n_0 = 19$ the conditions of Lemma 8b are satisfied, and $\tilde{K}(2^{n_0+g-1}-4)$ consists of a unique element M as follows

$$\begin{aligned}
2^{26}-4 = 11\cdot 2^{22} + 17\cdot 2^{20} + 11\cdot 2^{18} + 11\cdot 2^{14} + 17\cdot 2^{12} + 11\cdot 2^{10} +\\
11\cdot 2^{6} + 17\cdot 2^{4} + 11\cdot 2^{2}.
\end{aligned}$$

Note that $\tilde{S}(M) = \{11, 17\}$. By Corollary 11 we have $\boxed{c_{11} = 0}$.

6. Genus 9 and further questions

In this section we prove the following theorem.

Theorem 13. *Every supersingular curve over F of genus 9 has an equation*

$$y^2 - y = x^{19} + c^8x^9 + c^3x$$

for some $c \in \overline{\mathbb{F}}_2$. Moreover, we have $\dim(\mathcal{HS}_9/F) = 0$.

Our computation will use the following lemma (which generalizes Lemma 8).

Lemma 14. *Let notations be as above. Let λ be a rational number with $0 \leq \lambda \leq 1/2$.*

(a) *Suppose that for all* $m \geq 1$, $n \geq 1$, *and* $1 \leq j \leq g$ *one has*

$$\tilde{s}(m2^{n+g-1} - j, \mathrm{supp}X) \quad \geq \quad \lceil n\lambda \rceil.$$

Then

$$\mathrm{NP}_1(X) \quad \geq \quad \lambda.$$

(b) *Suppose* $\mathrm{NP}_1(X) \geq \lambda$. *Suppose there are positive integers* $1 \leq j \leq g$, $n_0 \geq 1$ *and* $1 \leq m_0 \leq g/2$ *such that*

(1) *for all* $m \geq 1, 1 \leq n < n_0$ *and for all* $m > g/2, n = n_0$ *we have*

$$\tilde{s}(m2^{n+g-1} - j, \mathrm{supp}X) \quad \geq \quad \lceil n\lambda \rceil ;$$

(2) $\tilde{s}(m_0 2^{n_0+g-1} - j, \mathrm{supp}X) = \lceil n_0\lambda \rceil - 1$.

Then

$$\tilde{C}(m_0 2^{n_0+g-1} - j, \mathrm{supp}X) \quad = \quad 0.$$

Proof. First one obtains a generalized version of Theorem 3.4 (ii) in [9] that states for all $m > m_0$ we have

$$V^{n_0+g-1}(\omega_{i,j}) \equiv \quad \sum_{m=1}^{m_0} C^{\sigma^{-(n_0+g-1)}}_{mp^{n_0+g-1}-j}(i, n_0+g-2)(\omega_{0,m}) \bmod p^{\lceil n_0\lambda \rceil}.$$

Its proof is an easy modification of that of Theorem 3.4 at the last several lines. The present lemma follows from this generalized version of Theorem 3.4 as Key-Lemma 3.5 does from Theorem 3.4 in [9]. □

Suppose X is a hyperelliptic supersingular curve over F of genus 9. By [8, Theorem 1.1II and Proposition 4.1] it has an equation

$$\boxed{y^2 - y = x^{19} + c_{13}x^{13} + c_{11}x^{11} + c_9x^9 + c_7x^7 + c_5x^5 + c_3x^3 + c_1x}$$

for some $c_\ell \in F$.

Let $\mathrm{supp}X = \{1, 3, 5, 7, 9, 11, 13, 19\}$. We found for $k = 0, \ldots, 7$ that $\tilde{K}(2^{27-3k} - 8)$ consists of all sequences $\{[b_i, \ell_i]\}_{i=1}^{8-k}$ possessing the following property:

$$\begin{cases} [b_{8-k}, \ell_{8-k}] = [24 - 3k, 7] \text{ or} \\ [b_{8-k}, \ell_{8-k}] = [23 - 3k, 13] \text{ and } [b_{7-k}, \ell_{7-k}] = [21 - 3k, 11] \text{ or} \\ [b_{8-k}, \ell_{8-k}] = [23 - 3k, 11] \text{ and } [b_{7-k}, \ell_{7-k}] = [21 - 3k, 19] \text{ or} \\ [b_{8-k}, \ell_{8-k}] = [23 - 3k, 13] \text{ and } [b_{7-k}, \ell_{7-k}] = [20 - 3k, 19] \text{ and} \\ \qquad\qquad\qquad\qquad\qquad\qquad [b_{6-k}, \ell_{6-k}] = [18 - 3k, 19]. \end{cases}$$

Hence

$$\begin{aligned} \tilde{C}(2^{27-3k} - 8) \quad = \quad & c_7^{2^{24-3k}} \tilde{C}(2^{24-3k} - 8) + (c_{11}c_{13}^4 + c_{11}^4)^{2^{21-3k}} \tilde{C}(2^{21-3k} - 8) \\ & + c_{13}^{2^{23-3k}} \tilde{C}(2^{18-3k} - 8). \end{aligned}$$

We checked that the conditions of Lemma 14b are satisfied for $\lambda = \frac{1}{2}$, $j = 8$ and (n_0, m_0) equal to $(17, 4)$, $(15, 2)$ and $(13, 1)$. Using the same kind of reasoning

as for genus 8, one concludes that $\boxed{c_7 = 0}$, $\boxed{c_{13} = 0}$ and $c_{11}c_{13}^4 + c_{11}^4 = 0$, which clearly implies $\boxed{c_{11} = 0}$.

So we continue with $X = \{1, 3, 5, 9, 19\}$. We checked that for $n_0 = 19$, $m_0 = 1$, $j = 8$ the conditions of Lemma 14b are satisfied, and $\tilde{K}(m_0 2^{n_0+g-1} - 8)$ consists of a unique element M as follows

$$2^{27} - 8 = 5 \cdot 2^{24} + 19 \cdot 2^{21} + 19 \cdot 2^{19} + 5 \cdot 2^{16} + 19 \cdot 2^{13} + 19 \cdot 2^{11} + 5 \cdot 2^8 + 19 \cdot 2^5 + 19 \cdot 2^3.$$

Note that $\tilde{S}(M) = \{5, 19\}$. By Corollary 11 we have $\boxed{c_5 = 0}$.

Now set $\mathrm{supp}X = \{1, 3, 9, 19\}$. We checked that for $n_0 = 25$, $m_0 = 3$, $j = 8$ the conditions of Lemma 14b are satisfied, and $\tilde{K}(m_0 2^{n_0+g-1} - 8)$ consists of a unique element M as follows

$$\begin{aligned} 3 \cdot 2^{33} - 8 \quad = \quad & 19 \cdot 2^{30} + 19 \cdot 2^{28} + 3 \cdot 2^{25} + 19 \cdot 2^{23} + 3 \cdot 2^{20} + 19 \cdot 2^{18} + 3 \cdot 2^{15} \\ & + 19 \cdot 2^{13} + 3 \cdot 2^{10} + 19 \cdot 2^8 + 3 \cdot 2^5 + 19 \cdot 2^3. \end{aligned}$$

Note that $\tilde{S}(M) = \{3, 19\}$. By Corollary 11 we have $\boxed{c_3 = 0}$.

Finally, set $\mathrm{supp}X = \{1, 9, 19\}$. We found that for $n_0 = 35$, $m_0 = 3$, $j = 8$ and $\lambda = \frac{1}{2}$ the conditions of Lemma 14b are satisfied, and that $\tilde{K}(3 \cdot 2^{43} - 8)$ consists of sequences $\{[b_i, \ell_i]\}_{i=1}^{17}$ with $[b_{17}, \ell_{17}] = [40, 19]$, $[b_{16}, \ell_{16}] = [38, 19]$ and for $k = 1, \ldots, 5$ we either have $[b_{3k}, \ell_{3k}] = [7k - 4, 19]$, $[b_{3k+1}, \ell_{3k+1}] = [7k - 2, 19]$, $[b_{3k+2}, \ell_{3k+2}] = [7k + 1, 1]$ or $[b_{3k}, \ell_{3k}] = [7k - 4, 19]$, $[b_{3k+1}, \ell_{3k+1}] = [7k - 2, 9]$, $[b_{3k+2}, \ell_{3k+2}] = [7k - 1, 9]$. So from Lemma 14 it follows that

$$0 = \tilde{C}(3 \cdot 2^{43-8} - 8) = (c_1^{32} + c_9^{12})^{2^3 + 2^{10} + 2^{17} + 2^{24} + 2^{31}}.$$

Thus $\boxed{c_9^3 = c_1^8}$, and we conclude that every hyperelliptic supersingular curve of genus 9 over F has to have an equation of the form $y^2 - y = x^{19} + c^8 x^9 + c^3 x$ for some $c \in F$.

A straightforward computation shows that the curve X with equation $y^2 - y = x^{19} + c^8 x^9 + c^3 x$ over $\overline{\mathbb{F}}_2$ is supersingular for $c \in \mathbb{F}_2$ but is *not* supersingular for $c \in \mathbb{F}_{2^2} - \mathbb{F}_2$. Therefore, this curve is supersingular for only finitely many $c \in \overline{\mathbb{F}}_2$. In other words, the open locus of hyperelliptic supersingular curves of genus 9 over $\overline{\mathbb{F}}_2$ is of dimension 0.

Let $c \in F - \overline{\mathbb{F}}_2$. Supose $X : y^2 - y = x^{19} + c^8 x^9 + c^3 x$ is supersingular. Then its specialization yields infinitely many supersingular curves over $\overline{\mathbb{F}}_2$ because the Grothendieck Specialization theorem says that the Newton polygon goes up under specialization maps (see [6]). This would contradicts the conclusion in the previous paragraph. Therefore, X has to be defined over $\overline{\mathbb{F}}_2$.

The results of this paper provide some information on the hyperelliptic supersingular curves in characteristic two. It raises the following questions:

Question 15. Are $y^2 - y = x^{19}$ and $y^2 - y = x^{19} + x^9 + x$ the only hyperelliptic supersingular curves over $\overline{\mathbb{F}}_2$?

Question 16. Could one formulate the pattern of $\dim(\mathcal{HS}_g/\overline{\mathbb{F}}_2)$ more precisely by more numerical data?

Question 17. It is clear from Theorem 2 that $\mathcal{HS}_g/F$ for $1 \leq g \leq 8$ are unirational. Is this true for all g?

Acknowledgments

We are grateful to Noam Elkies and Bjorn Poonen for their valuable suggestions in Section 4 and Remark 3, respectively. The computations in this paper used Magma and Maple packages and C-programs. The research of Hui June Zhu was partially supported by a grant of Bjorn Poonen from the David and Lucile Packard foundation. The research of Jasper Scholten was partially done while he was supported by the European project AREHCC.

References

[1] J. H. Conway, N. J. A. Sloane, *Sphere packings, lattices and groups,* Second edition. Grundlehren der Mathematischen Wissenschaften, 290. Springer-Verlag, New York, 1993.

[2] N. D. Elkies, *Mordell-Weil lattices in characteristic* 2. *I. Construction and first properties,* Int. Math. Res. Not. **8** (1994), 343–361.

[3] ———, *Mordell-Weil lattices in characteristic* 2. *II. The Leech lattice as a Mordell-Weil lattice,* Invent. Math. **128** (1997), 1–8.

[4] ———, *Mordell-Weil lattices in characteristic* 2. *III. A Mordell-Weil lattice of rank 128,* Experimental Math. **10** (2001), 467–473.

[5] J. de Jong, F. Oort, *Hyperelliptic curves in abelian varieties,* Algebraic geometry, 5. J. Math. Sci. **82** (1996), 3211–3219.

[6] N. Katz, *Slope filtration of F-crystals,* Astérisque, 63, 113–164. Soc. Math. France, Paris, 1979.

[7] K.-Z. Li, F. Oort, *Moduli of supersingular abelian varieties,* Lecture Notes in Mathematics, 1680. Springer-Verlag, Berlin, 1998.

[8] J. Scholten, H. J. Zhu, *Hyperelliptic curves in characteristic 2,* Int. Math. Res. Not. **17** (2002), 905–917.

[9] ———, *Slope estimates of Artin-Schreier curves,* to appear in Compositio Math.; `math.AG/0105005`

[10] I. R. Shafarevich, D. T. Tate, *The rank of elliptic curves,* Dokl. Akad. Nauk SSSR **175** (1967), 770–773.

[11] G. van der Geer, M. van der Vlugt, *On the existence of supersingular curves of given genus,* J. Reine Angew. Math. **458** (1995), 53–61.

[12] ———, *Reed-Muller codes and supersingular curves. I,* Compositio Math. **84** (1992), 333-367.

[13] H. J. Zhu, *p-adic variation of L functions of exponential sums. I,* `math.AG/0111194`

ESAT/COSIC, K.U. Leuven, Kasteelpark Arenberg 10, 3001 Leuven-Heverlee, Belgium.

E-mail address: `jasper.scholten@esat.kuleuven.ac.be`

Department of Mathematics, University of California, Berkeley, CA 94720-3840, U.S.A.

E-mail address: `zhu@alum.calberkeley.org`