Maximal hyperelliptic curves of genus three

Kodama, Tetsuo; Top, Jaap; Washio, Tadashi

Published in:
Finite fields and their applications

DOI:
10.1016/j.ffa.2009.02.002

Publication date:
2009

Finite Fields and Their Applications 15 (2009) 392–403

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Maximal hyperelliptic curves of genus three

Tetsuo Kodama [a,1], Jaap Top [b,*], Tadashi Washio [c]

[a] Kyushu University, Fukuoka 810-8560, Japan
[b] IWI-RuG, University of Groningen, Mathematics Department, Nijenborgh 9, 9747 AG Groningen, The Netherlands
[c] Department of Mathematics, Faculty of Education, Nagasaki University, 1-14, Bunkyo-machi, Nagasaki 852-8521, Japan

ARTICLE INFO

Article history:
Received 24 June 2008
Revised 29 January 2009
Available online 27 February 2009
Communicated by H. Stichtenoth

ABSTRACT

This note contains general remarks concerning finite fields over which a so-called maximal, hyperelliptic curve of genus 3 exists. Moreover, the geometry of some specific hyperelliptic curves of genus 3 arising as quotients of Fermat curves, is studied. In particular, this results in a description of the finite fields over which a curve as studied here, is maximal.

1. Introduction

The Hasse–Weil–Serre bound for the number of rational points on a smooth, geometrically irreducible curve C of genus g over the finite field $\mathbb{F}_q$ states that $\#C(\mathbb{F}_q) \leqslant q+1+gm$, where $m := \lfloor \sqrt{4q} \rfloor$ denotes the largest integer $\leqslant 2\sqrt{q}$.

Moreover, if a curve over $\mathbb{F}_q$ attains this bound, then the numerator of its zeta function over $\mathbb{F}_q$ equals $(1+mT+qT^2)^g$. A curve with this property is called a maximal curve over $\mathbb{F}_q$.

Deuring [2] in case $g=1$ and Serre [11] in case $g=2$ proved simple necessary and sufficient conditions on q under which a maximal curve of genus 1 or 2 exists over $\mathbb{F}_q$.

The case of genus $\geqslant 3$ seems to be much more complicated. From Deuring's result and the definition, it follows that if maximal curves over $\mathbb{F}_q$ of genus one do not exist, then for no positive $g>0$, a maximal curve over $\mathbb{F}_q$ of genus g exists. So, for example, maximal curves of positive genus do not exist over $\mathbb{F}_{2^7}$ and over $\mathbb{F}_{2^{11}}$, $\mathbb{F}_{3^7}$, $\mathbb{F}_{5^9}$, $\mathbb{F}_{7^5}$, ...

Ibukiyama in [6] showed that if $q=p^n$ for an odd prime p and an exponent $n \equiv 2 \bmod 4$, then a maximal curve of genus 3 over $\mathbb{F}_q$ exists. However, his proof does not give an equation for such a curve. Using results of Howe, Lauter and Serre, our paper [15] shows that a maximal curve of genus 3 exists over $\mathbb{F}_q$ with $q \leqslant 100$, if and only if

* Corresponding author.
E-mail addresses: j.top@rug.nl (J. Top), washio@nagasaki-u.ac.jp (T. Washio).
[1] Current address: 1-26-12, Higasiirube, Sawaraku, Fukuoka 811-1102, Japan.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2009.02.002

$$q \in \{8, 9, 19, 25, 29, 41, 47, 49, 53, 61, 64, 67, 71, 79, 81, 89, 97\}.$$

Moreover, in each of these cases an explicit example is given.

Other explicit examples are known by reducing well-known curves of genus 3 defined over $\mathbb{Q}$. A famous example is the Klein curve, defined by the equation

$$x^3y + y^3z + z^3x = 0.$$

This turns out to be a maximal curve over $\mathbb{F}_{q^2}$, if and only if the prime power $q \equiv 6 \bmod 7$. The beautiful survey by Elkies [3] does not mention this result which is probably well known; a recent reference is the PhD thesis [10]. A second well-known example is given by the Fermat curve with equation

$$x^4 + y^4 + z^4 = 0.$$

This defines a maximal curve over $\mathbb{F}_{q^2}$, for every prime power $q \equiv 3 \bmod 4$.

The literature also contains some maximal hyperelliptic curves of genus 3. In the present note we describe the geometry of some of these examples, and add some new ones. The new ones are obtained by taking quotients of certain hyperelliptic curves of higher genus, following a construction given in [14, §2]. The idea of constructing explicit maximal curves as quotients of known ones is well known; for instance, it has been used in the case of so-called Hermitian curves [1,4].

A hyperelliptic curve C over $\mathbb{F}_q$ has a unique quadratic twist by the hyperelliptic involution, which is denoted C^{tw}. If $\#C(\mathbb{F}_q) = q + 1 - t$, then $\#C^{\mathrm{tw}}(\mathbb{F}_q) = q + 1 + t$. In particular, a maximal hyperelliptic curve over $\mathbb{F}_q$ exists if and only if a minimal hyperelliptic curve over $\mathbb{F}_q$ exists. Here minimal means that the number of rational points equals $q + 1 - gm$, with notations as before.

Since $q + 1 - 3m < 0$ for all prime powers $q \leqslant 27$ (and also for $q = 31$), a maximal hyperelliptic curve of genus 3 does not exist over a field of cardinality $\leqslant 27$ or equal to 31. For $q \in \{29, 32\}$ one finds $q + 1 - 3m = 0$, and [5, Thm. 1.3] yields that a hyperelliptic curve of genus 3 without rational points does not exist over $\mathbb{F}_q$ for these q. The list given earlier shows that for $q = 37$ a maximal curve of genus 3 does not exist. Moreover, the curve corresponding to $y^2 = x^8 + 1$ is maximal over $\mathbb{F}_{49}$, as follows from Proposition 2 below. We now consider all prime powers q between 37 and 49.

For $q = 47$ one finds $m = \lfloor \sqrt{4q} \rfloor = 13$ and $m^2 - 4q = -19$. In this case, a unique maximal curve of genus 3 over $\mathbb{F}_{47}$ exists, as is explained in, e.g., [17]. The resulting curve is, however, not hyperelliptic.

For $q = 43$ it follows from [9, Thm. 1] that a maximal curve of genus 3 does not exist.

The case $q = 41$ we treated by explicit calculation: inspecting all hyperelliptic curves of genus 3 over $\mathbb{F}_{41}$, one finds that none of them is maximal.

Hence we showed:

Proposition 1. *$q = 49$ is the smallest prime power for which a maximal hyperelliptic curve of genus 3 over $\mathbb{F}_q$ exists.*

In the remainder of this note, proofs are presented for the following results.

Proposition 2. *The equation $y^2 = x^8 + 1$ corresponds to a smooth, complete, hyperelliptic curve of genus 3 in every characteristic $\neq 2$. For an odd prime number p, this curve is maximal over $\mathbb{F}_q$ with $q = p^n$, if and only if $p \equiv 7 \bmod 8$ and $n \equiv 2 \bmod 4$.*

This is shown in Section 2.

Proposition 3. *The equations $y^2 = x^7 + 1$ and $y^2 = x^8 + x$ correspond, in every characteristic $\neq 2, \neq 7$, to the same smooth, complete, hyperelliptic curve of genus 3. For an odd prime power q not divisible by 7, this*

curve is maximal over $\mathbb{F}_{q^2}$, if and only if $q \equiv 6 \bmod 7$. For the curve to be maximal over $\mathbb{F}_q$ with q not a square, a necessary but not sufficient condition is that $q \equiv 1 \bmod 14$ and $\lfloor \sqrt{4q} \rfloor \equiv -2 \bmod 14$.

A proof for this is found in Section 3.

Proposition 4. *In every characteristic $\neq 2$ and $\neq 3$, the equation $y^2 = x^7 + x$ corresponds to a smooth, complete, hyperelliptic curve of genus 3. For an odd prime power q not divisible by 3, this curve is maximal over $\mathbb{F}_{q^2}$, if and only if $q \equiv 3 \bmod 4$.*

For the curve to be maximal over $\mathbb{F}_q$ with q not a square, a necessary but not sufficient condition is that $q \equiv 1 \bmod 12$ and $\lfloor \sqrt{4q} \rfloor \equiv 2 \bmod 4$ and moreover the splitting behaviour of the two polynomials $X^4 - 4 = (X^2 - 2)(X^2 + 2)$ and $X^4 + 12$ in $\mathbb{F}_q[X]$ is the same.

A necessary and sufficient condition for maximality of this curve over $\mathbb{F}_q$ is that the three elliptic curves

$$E_1\colon\ y^2 = x^3 - 3x$$

and

$$E_2\colon\ y^2 = x^3 + x$$

and

$$E_3\colon\ y^2 = x^3 + 108x$$

are all maximal over $\mathbb{F}_q$.

This is proven in Section 4. In Section 5, a proof of the following result is presented.

Proposition 5. *Suppose p is a prime number $\neq 2$ and $\neq 3$ and let n be a positive integer and write $q = p^n$. Then the equation*

$$y^2 = \left(x^2 - 4\right)\left(x^2 - 2\right)\left(x^4 - 4x^2 + 1\right)$$

corresponds to a smooth, complete, hyperelliptic curve C of genus 3 over $\mathbb{F}_q$. The following conditions are equivalent:

(1) *C is maximal over $\mathbb{F}_q$.*
(2) *$p \equiv 11 \bmod 12$ and $n \equiv 2 \bmod 4$.*
(3) *The smooth, complete genus 5 curve corresponding to*

$$y^2 = x^{12} + 1$$

is maximal over $\mathbb{F}_q$.

Finally, we describe two more examples in Section 6:

Proposition 6. *In any characteristic $\neq 2$ and $\neq 3$, the equations*

$$y^2 = (x - 2)\left(x^2 - 2\right)\left(x^4 - 4x^2 + 1\right)$$

and

$$y^2 = (x+2)\big(x^2-2\big)\big(x^4-4x^2+1\big)$$

correspond to smooth, complete, hyperelliptic curves C_1 *resp.* C_2 *of genus* 3.

For a prime number $p \neq 3, \neq 2$ *and a positive exponent* n*, the next four conditions are equivalent*:

(1) $p \equiv 13 \bmod 24$ *or* $p \equiv 23 \bmod 24$*, and* $n \equiv 2 \bmod 4$.
(2) C_1 *is maximal over* $\mathbb{F}_{p^n}$.
(3) C_2 *is maximal over* $\mathbb{F}_{p^n}$.
(4) *The genus* 6 *curve corresponding to*

$$y^2 = x^{13} + x$$

is maximal over $\mathbb{F}_{p^n}$.

2. $y^2 = x^8 + 1$

The hyperelliptic curve C corresponding to the equation $y^2 = x^8 + 1$ has automorphisms $\sigma : (x, y) \mapsto (1/x, y/x^4)$ and $\rho : (x, y) \mapsto (\zeta x, y)$ (for a primitive 8th root of unity ζ) and the hyperelliptic involution $\iota : (x, y) \mapsto (x, -y)$. The quotient by ρ^4 yields an elliptic curve isogenous to E_1: $y^2 = x^3 + x$. An explicit map $C \to E_1$ is given by $(x, y) \mapsto (x^4, x^2 y)$. The pull-back of the invariant differential dx/y on E_1 via this map, is the differential $4x\,dx/y$ on C (which is, by construction, invariant under the action of ρ^4).

The quotient of C by the group generated by σ and $\iota\rho^4$ is the elliptic curve E_2 given by $y^2 = x^3 - 4x^2 + 2x$. An explicit quotient map $C \to E_2$ is given by

$$(x, y) \mapsto \big((x + 1/x)^2, y(x + 1/x)/x^2\big).$$

In this case, the pull-back of dx/y on E_2 is $(2x^2 - 2)\,dx/y$ on C.

The quotient of C by the group generated by $\iota\sigma$ and $\iota\rho^4$ is the elliptic curve E_3 given by $y^2 = (x^2 - 2)(x - 2)$. A pull-back of an invariant differential in this case is $(1 + x^2)\,dx/y$. An explicit quotient map is

$$(x, y) \mapsto \big(x^2 + x^{-2}, y(x - 1/x)/x^2\big).$$

Since the three differentials on C given above generate the space of regular differentials, it follows that the Jacobian variety of C is isogenous over $\mathbb{Q}$ to the product $E_1 \times E_2 \times E_3$. Now observe that E_1 has complex multiplication by $\mathbb{Z}[\sqrt{-1}]$ and E_2, E_3 have complex multiplication by $\mathbb{Z}[\sqrt{-2}]$. Hence every prime number p which is inert in both these rings, which means every $p \equiv 7 \bmod 8$, is a supersingular prime for each of the curves E_1, E_2, E_3. It follows that the numerator of the zeta function of C over $\mathbb{F}_p$, which is the product of the numerators of the zeta functions of the E_j over $\mathbb{F}_p$, equals $(1 + pT^2)^3$ in case $p \equiv 7 \bmod 8$. This implies that for every prime power q satisfying $q \equiv 7 \bmod 8$, the curve C is maximal over $\mathbb{F}_{q^2}$.

In fact, this is well known. For example, it is an immediate consequence of a result of Shafarevich and Tate [12, Thm. 1], which in turn follows from work of Weil [16].

One observes that a converse is also true: if for an odd prime power q the curve C is maximal over $\mathbb{F}_q$, then $q = p^n$ for a prime number $p \equiv 7 \bmod 8$ and an exponent $n \equiv 2 \bmod 4$. This is seen as follows. The endomorphism algebra of E_1 is $\mathbb{Q}(\sqrt{-1})$ in characteristic $p \equiv 1 \bmod 4$, and is a quaternion algebra in characteristic $p \equiv 3 \bmod 4$. Similarly for $j = 2, 3$ the endomorphism algebra of E_j in characteristic p is $\mathbb{Q}(\sqrt{-2})$ if $p \equiv 1, 3 \bmod 8$ and is a quaternion algebra in characteristic $p \equiv 5, 7 \bmod 8$. For C to be maximal over a finite field of characteristic p, a necessary condition is that E_1, E_2 and E_3 are isogenous over that finite field, which would imply that the endomorphism algebras of the three elliptic curves have to be the same. This can only happen in characteristic $p \equiv 7 \bmod 8$.

In characteristic $p \equiv 7 \bmod 8$, the p-power Frobenius endomorphism π_j on E_j satisfies $\pi_j^2 = -p$. It follows that for odd $n > 0$ one has

$$\#C(\mathbb{F}_{p^n}) = p^n + 1$$

and for even $n = 2m > 0$ one finds

$$\#C(\mathbb{F}_{p^n}) = p^n + 1 - (-1)^m 6p^m.$$

Hence only for a prime power $q \equiv 7 \bmod 8$ is the curve C maximal over $\mathbb{F}_{q^2}$.

Remark. Note that the proof presented here is purely geometrical: it does not use any Jacobi sum calculation as in work of Weil [16] and of Kodama and Washio [8].

Although the argument above is rather simple, in general it seems out of reach to determine all finite fields over which a given curve is maximal.

A weaker necessary condition for maximality of C over $\mathbb{F}_q$, namely that $q \equiv 1 \bmod 8$, can alternatively be obtained as follows. Note that for $q \not\equiv 1 \bmod 8$, every fourth power in $\mathbb{F}_q$ is also an eighth power. Hence in this case $\#C(\mathbb{F}_q)$ equals the number of $\mathbb{F}_q$-points on the genus one curve corresponding to $y^2 = x^4 + 1$. By the Hasse–Weil bound for genus one, it follows that C is not maximal over $\mathbb{F}_q$.

3. $y^2 = x^7 + 1$

In this section we denote by C the (smooth, complete) curve corresponding to the equation $y^2 = x^7 + 1$. Using the coordinates $\xi = 1/x$ and $\eta = y/x^4$, an alternative equation for the same curve is $\eta^2 = \xi^8 + \xi$.

Applying [8, Thm. 1 and its corollary], one concludes that for this curve to be maximal over $\mathbb{F}_{p^{2n}}$, a necessary condition is that $p \equiv 3, 5, 6 \bmod 7$. Assuming p satisfies this condition, one may apply [12, Thm. 1] to determine the numerator of the zeta function of C over $\mathbb{F}_p$. The result is that this numerator equals

$$1 + p^3 T^6 \quad \text{in case } p \equiv 3, 5 \mod 7;$$
$$\left(1 + pT^2\right)^3 \quad \text{in case } p \equiv 6 \mod 7.$$

It follows that for a prime power q the curve C is maximal over $\mathbb{F}_{q^2}$ if and only if $q \equiv 6 \bmod 7$.

For this particular curve, one may use elementary methods to deal with some of the non-square prime powers. Namely, when $q \not\equiv 1 \bmod 7$, then the map $x \mapsto x^7$ and hence also $x \mapsto x^7 + 1$ defines a bijection on $\mathbb{F}_q$. So in this case (provided q is odd) $\#C(\mathbb{F}_q) = q + 1$ and hence C is not maximal over $\mathbb{F}_q$.

Now assume the prime power q to be $\equiv 1 \bmod 14$. This implies that $\mathbb{F}_q$ contains a primitive 7th root of unity ζ. The cyclic group G of automorphisms of C, generated by $(x, y) \mapsto (\zeta x, -y)$ partitions $C(\mathbb{F}_q)$ in one orbit of length 1 coming from the point at infinity, one orbit $G \cdot (0, 1)$ of length 2, one orbit $G \cdot (-1, 0)$ of length 7, and all other orbits have length 14. So for $q \equiv 1 \bmod 14$ one concludes

$$\#C(\mathbb{F}_q) \equiv 10 \mod 14.$$

If moreover C would be maximal over $\mathbb{F}_q$, this implies $q + 1 + 3\lfloor\sqrt{4q}\rfloor \equiv 10 \bmod 14$ and hence $\lfloor\sqrt{4q}\rfloor \equiv -2 \bmod 14$. This proves the necessary condition stated in Proposition 3.

To see that this condition is not sufficient, consider the example $p = 743$. Then indeed $p \equiv 1 \bmod 7$ and $\lfloor\sqrt{4p}\rfloor = 54 \equiv -2 \bmod 14$. In this case $\#C(\mathbb{F}_p) = 808$ so C is not maximal over $\mathbb{F}_{743}$.

Observe that this argument proving the necessary condition, also yields an alternative and elementary proof of the statement, that when p is odd and $q = p^n \neq 6 \bmod 7$, then C is not maximal over $\mathbb{F}_{q^2}$.

Concerning the geometry of C, as observed above, the 7th roots of unity act as automorphisms on C, and hence on the Jacobian J of C. This defines a CM-type (as defined by Shimura and Taniyama [13, pp. 42–44]) on the field $\mathbb{Q}(\zeta_7)$. The CM-type may be described as the partition

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_7)/\mathbb{Q}\big) \cong (\mathbb{Z}/7\mathbb{Z})^* = \{1, 2, 3\} \cup \{4, 5, 6\}.$$

Since this CM-type is primitive, [13, p. 69] implies that in characteristic 0, the Jacobian J is an absolutely simple abelian threefold.

4. $y^2 = x^7 + x$

In this section C denotes the smooth, complete curve corresponding to the equation $y^2 = x^7 + x$. This curve C has the automorphisms $\sigma(x, y) := (1/x, y/x^4)$ and $\rho(x, y) := (\zeta^2 x, \zeta y)$ where ζ is a primitive 12th root of unity. Clearly, ρ has order 12 and σ has order 2, and we have $\sigma\rho = \rho^5\sigma$.

The quotient of C by σ is the elliptic curve E_1 with equation

$$E_1\colon\ y^2 = x^3 - 3x$$

and an explicit quotient map is given by

$$(x, y) \mapsto \big(x + 1/x, y/x^2\big).$$

A regular differential on C invariant under σ is $(x^2 - 1)\,dx/y$.

The quotient of C by the group generated by ρ^4 is the elliptic curve E_2 given by

$$E_2\colon\ y^2 = x^3 + x$$

and an explicit quotient map is given by

$$(x, y) \mapsto \big(x^3, xy\big).$$

A regular differential on C invariant under ρ^4 is $x\,dx/y$.

Since the two elliptic curves given here correspond to linearly independent differentials on C, one concludes that over the prime field the Jacobian J of C is isogenous to a product $E_1 \times E_2 \times E_3$, in which E_3 is another elliptic curve. In fact,

$$E_3 = (1 - \sigma)\big(1 - \rho^4\big)\big(1 - \rho^8\big)J.$$

This follows since $(1 - \sigma)(1 - \rho^4)(1 - \rho^8)$ acts as multiplication by 3 on the differential $(x^2 + 1)\,dx/y$ and sends the two differentials $(x^2 - 1)\,dx/y$ and $x\,dx/y$ to 0. Moreover, as an endomorphism of J, the map $(1 - \sigma)(1 - \rho^4)(1 - \rho^8)$ is Galois-invariant, hence indeed its image is an abelian subvariety of dimension 1 defined over the prime field. Now observe that ρ^3 commutes with σ and with ρ, hence it defines an automorphism on E_3 which has order 4 (since ρ^6 is the hyperelliptic involution on C, hence the -1-map on J). It follows that E_3, as well as E_1 and E_2, has complex multiplication by $\mathbb{Z}[\sqrt{-1}]$. Finally, note that since J has good reduction at all primes > 3, the same holds for E_3.

The above discussion implies that C is a maximal curve over $\mathbb{F}_q$ if, and only if, each of the curves E_j is maximal over $\mathbb{F}_q$. For q a square, this can only happen when the E_j are supersingular, which happens if and only if the characteristic is 3 mod 4. Vice versa, if $q = p^{2m}$ for a prime $p \equiv 3 \bmod 4$ and $p \neq 3$, then

$$\#C(\mathbb{F}_q) = q + 1 - (-1)^m \cdot 6 \cdot p^m.$$

So for a prime power q not a power of 2 or 3, the conclusion is that C is maximal over $\mathbb{F}_{q^2}$ if and only if $q \equiv 3 \bmod 4$.

In characteristics 3 mod 4 and q not a square, the curves E_j and hence also C, have $q+1$ rational points over $\mathbb{F}_q$. Hence we found all cases, in these characteristics, where C is maximal.

The remaining possibilities are $q = p^n$ for a prime $p \equiv 1 \bmod 4$ and an odd exponent n, which we will assume in what follows. A necessary condition on q such that C is maximal over $\mathbb{F}_q$ is that E_1, E_2, and E_3 are isogenous. In characteristic $p \equiv 1 \bmod 4$, the curves E_j are ordinary, hence the q-power Frobenius endomorphism π_j on E_j can be written as $\pi_j = a_j + b_j\iota$ for integers a_j, b_j and ι the endomorphism $\iota(x, y) = (-x, \sqrt{-1}y)$. The degree of π_j equals $q = a_j^2 + b_j^2$, which implies that one of a_j, b_j is odd and the other one is even. Moreover,

$$\#E_j(\mathbb{F}_q) = \deg(1 - \pi_j) = q + 1 - 2a_j.$$

On E_2 the rational point $T := (\sqrt{-1}, 0)$ satisfies $\iota(T) = T + (0, 0)$, hence

$$T = \pi_2(T) = a_2T + b_2T + b_2(0, 0);$$

hence b_2 is even and a_2 is odd. If $p \equiv 5 \bmod 12$, then $\sqrt{3} \notin \mathbb{F}_q$ hence the point $S := (\sqrt{3}, 0)$ on E_1 satisfies $\pi_1(S) = S + (0, 0) = \iota(S)$. Reasoning as before, this shows that a_1 is odd when $p \equiv 5 \bmod 12$. In particular, $\#E_1(\mathbb{F}_q) \neq \#E_2(\mathbb{F}_q)$ and hence E_1 and E_2 are not isogenous over $\mathbb{F}_q$.

The remaining case is that $q \equiv 1 \bmod 12$ is not a square. In this case, one calculates that the action of π_j on the $2 + 2\iota$-torsion of E_j is multiplication by -1 if (for $j = 1$) the polynomial $X^4 + 12$ is a product of two irreducible quadratic factors in $\mathbb{F}_q[X]$, resp. (for $j = 2$) the polynomial $X^4 - 4$ is a product of two irreducible quadratic factors in $\mathbb{F}_q[X]$. And π_j acts as multiplication by 1 if the polynomial mentioned here splits completely.

So for $q \equiv 1 \bmod 12$ not a square, one concludes that E_1 and E_2 are isogenous over $\mathbb{F}_q$ if and only if the splitting behaviour of the two polynomials $X^4 - 4$ and $X^4 + 12$ is the same in $\mathbb{F}_q[X]$. Moreover, since a primitive 12th root of unity exists in $\mathbb{F}_q$ in this case, the cyclic group G of automorphisms of C generated by ρ splits the set $C(\mathbb{F}_q)$ in the orbits of length one $G \cdot (0, 0)$ and G times the point at infinity, the orbit $G \cdot (\zeta, 0)$ of length six, and all other orbits of length twelve. Hence $\#C(\mathbb{F}_q) \equiv 8 \bmod 12$, which implies the necessary condition for maximality $\lfloor\sqrt{4q}\rfloor \equiv 2 \bmod 4$ when $q \equiv 1 \bmod 12$. The given necessary condition for C to be maximal over $\mathbb{F}_q$ is not a sufficient one. Indeed, take $p = 373$, then $p \equiv 1 \bmod 12$ and $m = \lfloor\sqrt{4p}\rfloor = 38 \equiv 2 \bmod 4$. The polynomials $X^4 - 4$ and $X^4 + 12$ both have two irreducible factors of degree 2. And C is not maximal over $\mathbb{F}_p$, since $\#C(\mathbb{F}_p) = 416 < 488 = p + 1 + 3m$.

To be able to say a little more, we first give an equation for E_3. Over $\mathbb{Q}$, we know that E_3 is a curve with j-invariant 1728 and with good reduction away from 2 and 3. Hence an equation for E_3 is of the form $y^2 = x^3 + ax$, in which $a = \pm 2^k 3^l$ for integers k, l with $0 \leqslant k, l \leqslant 3$. Since the curve with a is 2-isogenous to the one with $-4a$, we may assume $a > 0$. The exact value of a is then found using

$$\#C(\mathbb{F}_p) = \#E_1(\mathbb{F}_p) + \#E_2(\mathbb{F}_p) + \#E_3(\mathbb{F}_p) - 2(p + 1).$$

Evaluating this for $p = 5$ shows $a \in \{3, 8, 18, 108\}$. The case $p = 13$ shows $a \neq 3$ and $a \neq 8$ and $a \neq 18$. So one concludes

$$E_3\colon\ y^2 = x^3 + 108x.$$

Now observe that for $p \equiv 1 \bmod 12$, the field $\mathbb{F}_p$ contains a square root of 3 and of -1, and therefore -36 is a fourth power in $\mathbb{F}_p$. This implies that in this case E_1 and E_3 are isomorphic. In other words, having an equation for E_3 does not give us a stronger condition on q such that C is maximal over $\mathbb{F}_q$.

5. A quotient of $y^2 = x^{12} + 1$

The (smooth, complete) curve corresponding to the equation $y^2 = x^{12} + 1$ is denoted D. This is a hyperelliptic curve of genus 5. The curve D admits an involution σ defined by $\sigma(x, y) = (1/x, -y/x^6)$. The quotient of D by σ is a hyperelliptic genus 3 curve C, defined as

$$C\colon\ y^2 = \bigl(x^2 - 4\bigr)\bigl(x^2 - 2\bigr)\bigl(x^4 - 4x^2 + 1\bigr).$$

This curve C is maximal over $\mathbb{F}_q$ whenever D is maximal over $\mathbb{F}_q$.

Using [12, Thm. 1] it follows that D is maximal over $\mathbb{F}_{p^n}$ for every prime $p \equiv 11 \bmod 12$ and exponent $n \equiv 2 \bmod 4$. So under the same conditions, C is maximal as well. We will now give an alternative, more geometrical proof of the same result, from which we can also deduce that the above prime powers are the only ones for which C is maximal over $\mathbb{F}_q$.

A basis for the regular differentials on D is $\{e_1, e_2, e_3, e_4, e_5\}$, with $e_j := x^{j-1}\,dx/y$. The automorphism μ on D, defined by $\mu(x, y) := (-x, y)$, acts on this basis as $e_j \mapsto (-1)^j e_j$. Hence the invariant differentials are spanned by e_2 and e_4. The quotient of D by μ is the genus 2 curve C_1 corresponding to the equation $y^2 = x^6 + 1$. The Jacobian of C_1 is isogenous to the product $E \times E$, in which E denotes the elliptic curve with equation $y^2 = x^3 + 1$. Two morphisms $C_1 \to E$ with independent pull-backs of the regular differential dx/y on E, are $(x, y) \mapsto (x^2, y)$ and $(x, y) \mapsto (1/x^2, y/x^3)$.

Similarly, the automorphism λ on D defined as $\lambda(x, y) := (-x, -y)$ acts on the e_j as $e_j \mapsto (-1)^{j+1} e_j$. Hence in this case the invariant regular differentials are spanned by e_1, e_3 and e_5. The quotient of D by λ is the genus 3 curve C_2 corresponding to the equation $y^2 = x^7 + x$, which was studied in Section 4. An explicit quotient map $D \to C_2$ is given by $(x, y) \mapsto (x^2, xy)$.

Recall from Section 4 that the Jacobian of C_2 is isogenous to a product $E_1 \times E_2 \times E_3$ of three elliptic curves, each with j-invariant 1728. It follows that the Jacobian of D is isogenous (over the prime field) to the product $E \times E \times E_1 \times E_2 \times E_3$.

The Jacobian of C, corresponding to the three differentials $e_1 + e_5, e_2 + e_4$ and e_3 which are invariant under σ, is therefore (over the prime field) isogenous to $E \times E' \times E''$ in which E', E'' are two of the curves E_1, E_2, E_3. Since (in characteristic zero) E has endomorphism algebra $\mathbb{Q}(\sqrt{-3})$ and E' has endomorphism algebra $\mathbb{Q}(\sqrt{-1})$, an argument completely analogous to what is done in Section 2 shows that for C to be maximal, it is necessary that both E and E' are supersingular, which implies that the characteristic is $\equiv 11 \bmod 12$. Under the latter condition, the numerator of the zeta function of C over $\mathbb{F}_p$ equals $(1 + pT^2)^3$, which implies that C is maximal over $\mathbb{F}_{p^n}$ precisely when $n \equiv 2 \bmod 4$.

The same argument shows that C is maximal over $\mathbb{F}_q$, if and only if D is maximal over $\mathbb{F}_q$.

Similar to the arguments presented at the end of Sections 2 and 3, one can show parts of the above results in a more elementary way.

It is not possible to use the curve given by $y^2 = x^{12} + x$ (or $\eta^2 = \xi^{11} + 1$, which via $x = 1/\xi$, $y = \eta/\xi^6$ defines the same curve) in a similar way to obtain genus 3 curves. The reason is that the action of the 11th roots of unity ζ_{11}^a as automorphisms on this curve, defines a primitive CM-type on the field $\mathbb{Q}(\zeta_{11})$. Hence in this case the Jacobian of the genus 5 curve is absolutely simple in characteristic 0.

6. Quotients of $y^2 = x^{13} + x$

We consider the smooth, projective curve D of genus 6, corresponding to the equation

$$D\colon\ y^2 = x^{13} + x.$$

Let ζ be a primitive 24th root of unity. Define the automorphism ρ on D, by $\rho(x, y) = (\zeta^2 x, \zeta y)$. Then ρ has order 24 and ρ^{12} is the hyperelliptic involution on D. Another automorphism on D is σ, given by $\sigma(x, y) = (1/x, y/x^7)$. The order of σ is 2, and $\sigma\rho = \rho^{11}\sigma$.

Using [8, Thm. 2 and corollary], one finds that for every prime power q which is congruent to 13 or to 23 modulo 24, the curve D (and hence also any quotient of it) is maximal over $\mathbb{F}_{q^2}$. We will study the geometry of D and of some of its quotients.

The quotient of D by σ is the genus 3 curve C_2, with equation

$$C_2\colon\ y^2 = (x+2)\big(x^2-2\big)\big(x^4-4x^2+1\big).$$

A quotient map is given by

$$(x, y) \mapsto \big(x + 1/x,\, y(x+1)/x^4\big).$$

With the basis $e_j := x^{j-1}\,dx/y$ (for $0 \leqslant j \leqslant 5$) for the regular differentials on D, one checks that a basis for the differentials invariant under σ is $\{e_1 - e_6, e_2 - e_5, e_3 - e_4\}$ which also generate the pull-backs of the regular differentials on C_2.

The quotient of D by $\sigma\rho^{12}$ is the genus 3 curve C_1, with equation

$$C_1\colon\ y^2 = (x-2)\big(x^2-2\big)\big(x^4-4x^2+1\big).$$

A quotient map is given by

$$(x, y) \mapsto \big(x + 1/x,\, y(x-1)/x^4\big).$$

One checks that a basis for the differentials invariant under $\sigma\rho^{12}$ is $\{e_1 + e_6, e_2 + e_5, e_3 + e_4\}$ which also generate the pull-backs of the regular differentials on C_1.

Observe that $(x, y) \mapsto (-x, \zeta^6 y)$ defines an isomorphism $C_1 \cong C_2$. This isomorphism is defined over every field containing a primitive 4th root of unity. In particular, for $q \equiv 3 \bmod 4$ a prime power (but not divisible by 3), one has $\#C_1(\mathbb{F}_q) + \#C_2(\mathbb{F}_q) = 2q + 2$. This implies that over such a field at least one of C_1, C_2 is not maximal, hence also D is not maximal.

In what follows, the main idea is to describe abelian subvarieties of the Jacobian $J(D)$, and endomorphisms of these subvarieties. This is analogous to the construction of the elliptic curve called E_3 in Section 4. Namely, the group G of automorphisms of D, generated by ρ and σ gives the group ring $\mathbb{Z}[G]$. Consider this as a subring of the endomorphism ring $\mathrm{End}(J(D))$. Any $\varphi \in \mathbb{Z}[G]$ such that $\varphi^2 = n\varphi$ for some nonzero $n \in \mathbb{Z}$, yields an isogeny

$$(\varphi, n-\varphi)\colon\ J(D) \to \varphi J(D) \times (n-\varphi)J(D).$$

Moreover, if $\psi \in \mathrm{End}(J(D))$ commutes with φ, then ψ defines an endomorphism of the abelian subvarieties $\varphi J(D)$ and $(n-\varphi)J(D)$. This idea is well known; for instance, it is the basis of the paper [7] by Kani and Rosen. In the present case, we will exploit this to obtain isogenies (defined over the prime field $\mathbb{F}_p$)

$$J(D) \sim A_1 \times E_1 \times A_2 \times E_2$$

where the E_j are elliptic curves and the A_j are abelian surfaces. Moreover,

$$J(C_j) \sim A_j \times E_j$$

for $j = 1, 2$. The curves E_j have complex multiplication by $\sqrt{-2}$ and the surfaces A_j have CM by $\sqrt{-6}, \sqrt{-2}$. From this, it is relatively easy to deduce necessary and sufficient conditions for maximality of D and C_1, C_2 over a given field $\mathbb{F}_q$, similar to the previous sections of this paper. We now start with the details of the argument.

Up to isogeny, the Jacobians $J(C_j)$ of C_j are abelian subvarieties of $J(D)$, namely the subvarieties $(1-\sigma)J(D)$ and $(1+\sigma)J(D)$, respectively. This is seen by considering the action of $1 \pm \sigma$ on the differentials e_j; for $1+\sigma$ the image is spanned by $e_1 - e_6, e_2 - e_5, e_3 - e_4$ while for $1-\sigma$ the image is the span of $e_1 + e_6, e_2 + e_5, e_3 + e_4$. Note that the endomorphisms $1 \pm \sigma \in \mathrm{End}(J(D))$ are defined over the prime field, and hence the same is true for their image.

The quotient of D by the order three group with generator ρ^8 is a genus 2 curve C_3 corresponding to $y^2 = x^5 + x$. An explicit quotient map is

$$(x, y) \mapsto \left(x^3, xy\right)$$

and the regular differentials on D invariant under ρ^8 (hence the pull-backs of the given quotient map) are spanned by e_2 and e_5.

The endomorphism $1 + \rho^8 + \rho^{16} = 1 - \rho^4 + \rho^8$ on $J(D)$ acts as multiplication by 3 on e_2 and e_5 and sends all other e_j to zero. Moreover, this endomorphism is defined over the prime field. So $(1 - \rho^4 + \rho^8)J(D)$ is an abelian subvariety of $J(D)$ defined over the prime field and isogenous to $J(C_3)$.

The group generated by ρ is fixed under conjugation by σ and hence σ descends to an automorphism (which we will also denote by σ) on C_3. The quotient of C_3 by σ equals the quotient of D by the group generated by ρ^8 and σ. It is the elliptic curve E_2, given as

$$E_2\colon\ y^2 = (x+2)\left(x^2 - 2\right).$$

The quotient map $C_3 \to E_2$ is given by $(x, y) \mapsto (x + 1/x, y(1+x)/x^2)$, and the quotient map $D \to E_2$ by $(x, y) \mapsto (x^3 + 1/x^3, y(1+x^3)/x^5)$. The regular differentials on E_2 pull back to the regular differentials on D which are invariant under σ and ρ^8. Clearly, this is the space spanned by $e_2 - e_5$. The endomorphism $(1 - \rho^4 + \rho^8)(1+\sigma)$ is defined over the prime field and acts as multiplication by 3 on $e_2 - e_5$ and as 0 on $e_1 \pm e_6, e_3 \pm e_4, e_2 + e_5$. Hence the abelian subvariety $(1 - \rho^4 + \rho^8)(1+\sigma)J(D)$ of $J(D)$ is isogenous over the prime field to E_2.

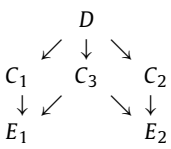
By construction, since σ is in the group generated by σ and ρ^8, the quotient map $D \to E_2$ factors as $D \to C_2 \to E_2$. The map $C_2 \to E_2$ here, is given by $(x, y) \mapsto (x^3 - 3x, xy - y)$.

Similarly, one may consider the group generated by ρ^8 and $\rho^{12}\sigma$. This results in quotient maps $D \to C_3 \to E_1$, for the elliptic curve

$$E_1\colon\ y^2 = (x-2)\left(x^2 - 2\right).$$

The quotient map $C_3 \to E_1$ is given by $(x, y) \mapsto (x + 1/x, y(x-1)/x^2)$, and the quotient map $D \to E_2$ by $(x, y) \mapsto (x^3 + 1/x^3, y(x^3-1)/x^5)$. The regular differentials on E_2 pull back to the regular differentials on D which are invariant under $\rho^{12}\sigma$ and ρ^8. Clearly, this is the space spanned by $e_2 + e_5$. Analogous to the assertions concerning E_2 one finds that E_1 is isogenous over the prime field to the abelian subvariety $(1 - \rho^4 + \rho^8)(1-\sigma)J(D)$ of $J(D)$.

The quotient map $D \to E_1$ factors as $D \to C_1 \to E_1$. The map $C_1 \to E_1$ here, is given by $(x, y) \mapsto (x^3 - 3x, xy + y)$. All maps described here are given in the following diagram.



In End($J(D)$), write $\lambda := \rho^3 + \rho^9$ and $\mu := \rho + \rho^5 + \rho^7 + \rho^{11} = (\rho^3 - \rho^9)(\rho^4 + \rho^8)$. Then $\rho\lambda = \lambda\rho$ and $\rho\sigma = \sigma\rho$ and $\lambda^2 = -2$. It follows that $\mathbb{Q}(\sqrt{-2})$ is in the endomorphism algebra of any abelian variety isogenous to an abelian subvariety of $J(D)$ which is obtained as image of an endomorphism from the subring of End($J(D)$) generated by ρ and σ. In particular, this is the case for the elliptic curves E_1 and E_2 (which in fact have $\mathbb{Z}[\sqrt{-2}]$ in their endomorphism ring). The endomorphism μ also commutes with both ρ and σ. It satisfies $\mu^2 = 2(\rho^8 - 2 - \rho^4)$.

So on the part of $J(D)$ where ρ^8 acts as identity (which is the subvariety defined over the prime field $(1 - \rho^4 + \rho^8)J(D)$ of dimension 2), one has that $\mu^2 = 0$. And on the part of $J(D)$ where ρ^8 acts as an automorphism of order 3 (which is the subvariety defined over the prime field $(2 + \rho^4 - \rho^8)J(D) = (1 - \rho^8)(1 - \rho^{16})J(D)$ of dimension 4), one has that $\mu^2 = -6$.

The discussion above shows that, with $\sim$ denoting isogeny defined over the prime field,

$$J(D) \sim (1 - \sigma)J(D) \times (1 + \sigma)J(D) \sim J(C_1) \times J(C_2)$$

and

$$J(C_1) \sim \big(1 - \rho^8\big)\big(1 - \rho^{16}\big)(1 - \sigma)J(D) \times \big(1 + \rho^8 + \rho^{16}\big)(1 - \sigma)J(D) \sim A_1 \times E_1$$

and

$$J(C_2) \sim \big(1 - \rho^8\big)\big(1 - \rho^{16}\big)(1 + \sigma)J(D) \times \big(1 + \rho^8 + \rho^{16}\big)(1 + \sigma)J(D) \sim A_2 \times E_2.$$

Here A_1, A_2 are abelian surfaces defined over the prime field, given by $A_1 := (1 - \rho^8)(1 - \rho^{16}) \times (1 - \sigma)J(D)$ and $A_2 := (1 - \rho^8)(1 - \rho^{16})(1 + \sigma)J(D)$. The endomorphism algebra of A_j contains the field $\mathbb{Q}(\sqrt{-2}, \sqrt{-6})$.

In characteristic zero, the CM-type defined using this (i.e., corresponding to the action of λ, μ on the differentials $e_1 + e_6, e_3 + e_4$ resp. $e_1 - e_6, e_3 - e_4$) is not primitive. Hence over some extension of $\mathbb{Q}$, A_j is isogenous to a product $E \times E'$ of elliptic curves. Since the endomorphism algebra of this product contains a field of degree 4, the curves E, E' are isogenous and have an endomorphism algebra containing an imaginary quadratic subfield of $\mathbb{Q}(\sqrt{-2}, \sqrt{-6})$. By reduction, the same is true in every characteristic > 3.

Now $\lambda e_j = (\zeta^3 + \zeta^9)e_j$ for $j = 1, 6$ and $\lambda e_j = -(\zeta^3 + \zeta^9)e_j$ for $j = 3, 4$ whereas $\mu e_j = (\zeta + \zeta^5 + \zeta^7 + \zeta^{11})e_j$ for each of $j = 1, 3, 4, 6$. This implies that the curve E has CM by $\sqrt{-6}$ and not by $\sqrt{-2}$.

Similar to the argument presented in Section 2, it follows that the curves C_j can only be maximal over a finite field of characteristic $p > 3$, if p is inert in both $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-6})$ (so that all elliptic curves involved, are supersingular).

Although we have not used this above, note that in characteristic zero, the endomorphism ring of E does not contain a square root of -2, so E is not an image of $J(D)$ under an endomorphism in the ring generated by ρ and σ. In fact, in characteristic zero (and hence by reduction in any characteristic > 3), the two abelian surfaces A_j are isogenous to Weil restrictions of an elliptic curve defined over $\mathbb{Q}(\sqrt{2})$ with CM by $\mathbb{Z}[\sqrt{-6}]$. An explicit equation of such an elliptic curve is

$$y^2 = x^3 + 6\sqrt{2}(1 + \sqrt{2})x^2 + 3x.$$

Acknowledgments

It is a pleasure to thank Christiaan van de Woestijne for his comments concerning an earlier version of this work, and Henning Stichtenoth for starting the contact between the Dutch and the two Japanese authors of this paper. We are grateful for the referee's comments, which not only led to the correction of several typos but also to some improvements of our original results.

References

[1] A. Cossidente, G. Korchmáros, F. Torres, On curves covered by the Hermitian curve, J. Algebra 216 (1999) 56–76.
[2] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hansische 14 (1941) 197–272.
[3] N.D. Elkies, The Klein quartic in number theory, in: The Eightfold Way, in: Math. Sci. Res. Inst. Publ., vol. 35, Cambridge Univ. Press, Cambridge, 1999, pp. 51–101.
[4] A. Garcia, H. Stichtenoth, C.-P. Xing, On subfields of the Hermitian function field, Compos. Math. 120 (2000) 137–170.
[5] E.W. Howe, K.E. Lauter, J. Top, Pointless curves of genus three and four, in: Arithmetic, geometry and coding theory, AGCT, 2003, in: Semin. Congr., vol. 11, Soc. Math. France, Paris, 2005, pp. 125–141.
[6] T. Ibukiyama, On rational points of curves of genus 3 over finite fields, Tôhoku Math. J. 45 (1993) 311–329.
[7] E. Kani, M. Rosen, Idempotent relations and factors of Jacobians, Math. Ann. 284 (1989) 307–327.
[8] T. Kodama, T. Washio, A family of hyperelliptic function fields with Hasse–Witt-invariant zero, J. Number Theory 36 (1990) 187–200.
[9] K. Lauter, The maximum or minimum number of rational points on genus three curves over finite fields, with an appendix by J.-P. Serre, Compos. Math. 134 (2002) 87–111.
[10] S. Meagher, Twists of genus three curves and their Jacobians, PhD thesis, University of Groningen, 2008.
[11] J.-P. Serre, Nombres de points des courbes algébriques sur $\mathbb{F}_q$, Sém. de Théorie des Nombres de Bordeaux, 1982/1983, Exp. No. 22 (Oeuvres III, No. 129, 664–668).
[12] I.R. Shafarevich, J.T. Tate, The rank of elliptic curves, Soviet Math. Dokl. 8 (1967) 917–920.
[13] G. Shimura, Y. Taniyama, Complex multiplication of abelian varieties and its application to number theory, Publ. Math. Soc. Japan 6 (1961).
[14] W. Tautz, J. Top, A. Verberkmoes, Explicit hyperelliptic curves with real multiplication and permutation polynomials, Canad. J. Math. 43 (1991) 1055–1064.
[15] J. Top, Curves of genus 3 over small finite fields, Indag. Math. (N.S.) 14 (2003) 275–283.
[16] A. Weil, Jacobi sums as "Grössencharactere", Trans. Amer. Math. Soc. 73 (1952) 487–495.
[17] A. Zaytsev, Optimal curves of low genus over finite fields, http://arxiv.org/abs/0706.4203 (also printed as Chapter 3 in the PhD thesis, Optimality properties of curves over finite fields, by A. Zaytsev, University of Amsterdam, 2008).