Finite Fields and Their Applications **6,** 327–341 (2000)
doi.10.1006/ffta.2000.0286, available online at http://www.idealibrary.com on IDEAL®

Kummer Covers with Many Points

Gerard van der Geer

Faculteit Wiskunde en Informatica, Universiteit van Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands
E-mail: geer@wins.uva.nl

and

Marcel van der Vlugt

Mathematisch Instituut, Rijksuniversiteit te Leiden, Niels Bohrweg 1, 2333 CA Leiden, The Netherlands
E-mail: vlugt@math.leidenuniv.nl

Communicated by Harald Niederreiter

Received October 4, 1999; published online August 19, 2000

INTRODUCTION

Let p be a prime, let $\mathbf{F}_q$ be a finite field with $q = p^m$ elements, and let $\bar{\mathbf{F}}_q$ be an algebraic closure of $\mathbf{F}_q$. In this paper we present a method for constructing curves over finite fields with many points which are Kummer covers of $\mathbf{P}^1$ or of other suitable base curves. For this we look at rational functions $f \in \mathbf{F}_q(x)$ such that f assumes a fixed value $a \in \mathbf{F}_q$ on a (preferably large) set $\mathscr{P} \subseteq \mathbf{P}^1(\mathbf{F}_q)$. To take a concrete example we set $a = 1$. Then the algebraic curve which is the Kummer covering of $\mathbf{P}^1$ given by the equation

$$y^{q-1} = f(x)$$

has fibres with many rational points and judicious choices of f lead to improvements and extensions of the tables [2] of curves with many points. The methods we employed in the past were mostly based on Artin–Schreier covers of the projective line.

In Section 1 we sketch the method and describe a way to obtain good rational functions as above. This is based on an appropriate splitting

1071-5797/00 $35.00

$f = f_1 + f_2$ of a linearized polynomial f having as zero set a linear subspace L of $\mathbf{F}_q$. In the following section we treat the case where the linear space L is the full space $\mathbf{F}_q$. We find curves C_m defined over $\mathbf{F}_q$ for which the ratio $\#C_m(\mathbf{F}_q)/g(C_m)$ of the number of rational points by the genus exceeds $\sqrt{q}$ for m even and $2\sqrt{pq}/(p+1)$ for m odd. For g large compared to q the only way known so far to prove the existence of curves with a comparable ratio is by class field theory, which is less explicit (cf. [1]). Note that the result of Drinfeld–Vladut, that $\lim\sup_{g\to\infty} \#C(\mathbf{F}_q)/g(C) \leq \sqrt{q} - 1$, shows that for given q there are only finitely many isomorphism classes of curves C over $\mathbf{F}_q$ whose ratio $\#C(\mathbf{F}_q)/g(C)$ exceeds $\sqrt{q}$ for m even.

In Section 3 we consider the case where the linear subspace is of codimension 1 in $\mathbf{F}_q$ and we complement this note with a section with variations. We illustrate the sections with numerous examples and thus obtain a number of improvements of the existing tables. In many cases the methods also give a relatively easy way to construct for certain pairs (q, g) a curve realizing the lower entry of the interval in the tables [2]. We conclude the article with a table summarizing the new results from the examples.

1. THE METHOD

We consider the non-singular complete irreducible Kummer curve C over $\mathbf{F}_q$ defined by the affine equation

$$y^{q-1} = f(x),$$

where the rational function $f(x) \in F_q(x)$ satisfies the following conditions.

(1.1) *Conditions.*

(i) *f is not the dth power of an element $g \in \bar{\mathbf{F}}_q(x)$ for any divisor $d > 1$ of $q - 1$;*

(ii) *$f(x) = 1$ on a substantial subset $\mathscr{P}$ of $\mathbf{P}^1(\mathbf{F}_q)$;*

(iii) *$f(x)$ has many multiple zeros and poles.*

By (i) the curve C is a cyclic cover of $\mathbf{P}^1$ of degree $q - 1$, by (ii) the curve C has at least $(q-1)\#\mathscr{P}$ rational points, and condition (iii) keeps the genus of C within bounds.

The Hurwitz-Zeuthen formula gives the genus of C (cf., e.g., [3]):

(1.2) PROPOSITION. *If the divisor of f is $(f) = \sum_{i=1}^{\ell} d_i P_i$ with distinct $P_i \in \mathbf{P}^1(\bar{\mathbf{F}}_q)$ then the genus $g(C)$ of C is given by*

$$2g(C) - 2 = (\ell - 2)(q-1) - \sum_{i=1}^{\ell} \gcd(q-1, |d_i|). \tag{1}$$

Note that a small value of ℓ and the greatest common divisors influence the genus in a favourable way for our game.

Rational functions which satisfy Conditions (1.1) arise for instance in the following way.

Let L be an r-dimensional subspace of the $\mathbf{F}_p$-vector space $\mathbf{F}_{q=p^m}$ with $r \geq 2$. Then the polynomial

$$R = \prod_{c \in L} (x - c)$$

is a p-linearized polynomial, i.e., is of the form

$$R(x) = \sum_{i=0}^{r} a_i x^{p^i} \in \mathbf{F}_q[x],$$

and moreover satisfies $a_0 a_r \neq 0$.

Now we split R as

$$R(x) = R_1(x) + R_2(x) \tag{2}$$

so that $R_1(x) = \sum_{i=s}^{r} b_i x^{p^i} \in \mathbf{F}_q[x]$ and $R_2(x) = \sum_{i=0}^{t} c_i x^{p^i}$ with $0 < s < r$, $t \leq s$, $b_s b_r \neq 0$, and $c_0 c_t \neq 0$. We denote the zero sets of R_1 (resp. R_2) by L_1 (resp. L_2) with $\# L_1 = p^{r-s}$ (resp. $\# L_2 = p^t$). Furthermore, in connection with Condition (1.1) (i) we require that $L_1 \neq L_2$.

It is obvious that

$$f(x) = -\frac{R_1(x)}{R_2(x)} = -\frac{(\sum_{i=s}^{r} b_i^{1/p^s} x^{p^{i-s}})^{p^s}}{\sum_{i=0}^{t} c_i x^{p^i}} \tag{3}$$

satisfies $f(x) = 1$ for $x \in L - (L_1 \cup L_2)$. From (2) it follows that $L \cap (L_1 \cup L_2) = L_1 \cap L_2$, which means that $L - (L_1 \cup L_2) = L - (L_1 \cap L_2)$. Moreover, the zeros of R_1 and the pole ∞ have multiplicities > 1. Hence f satisifies Conditions (1.1).

(1.3) PROPOSITION. *The Kummer cover C of $\mathbf{P}^1$ defined by the equation $y^{q-1} = f(x)$ with $f(x) = -R_1/R_2$ as in* (3) *has genus*

$$g = \{(p^{r-s} + p^t - \delta - 1)(q-2) - \delta p^{\gcd(m,s)} - p^{\gcd(m,r-t)} + 2\delta + 2\}/2 \tag{4}$$

and the number of $\mathbf{F}_q$-rational points on C satisfies

$$\# C(\mathbf{F}_q) \geq (p^r - \delta)(q-1), \tag{5}$$

where $\delta = \# (L_1 \cap L_2)$.

Proof. By the assumption $L_1 \neq L_2$ it follows that the function f satisfies (1.1) (i). The divisor of f is

$$(f) = \sum_{P \in L_1 \cap L_2} (p^s - 1)P + \sum_{P \in L_1 - (L_1 \cap L_2)} p^s P - \sum_{P \in L_2 - (L_1 \cap L_2)} P - (p^r - p^t) P_\infty.$$

The number ℓ of distinct zeros and poles of f is

$$\# L_1 + \# L_2 - \# (L_1 \cap L_2) + 1 = p^{r-s} + p^t - \delta + 1.$$

According to Proposition (1.2) the genus satisfies

$$2g(C) - 2 = (p^{r-s} + p^t - \delta - 1)(q - 1) - \delta(p^{\gcd(m,s)} - 1)$$

$$- (p^{r-s} - \delta) - (p^{\gcd(m,r-t)} - 1)$$

and we obtain (4). For $x \in L - (L_1 \cap L_2)$ we have $f(x) = 1$ and thus over each $y \in \mathbf{F}_q^*$ we find $p^r - \delta$ rational points on C. Other rational points could come from the branch points of C. The set of branch points is $L_1 \cup L_2 \cup \infty$ and they contribute rational points if the ramification points over such branch points happen to be rational. This yields the required estimate (5). ■

(1.4) EXAMPLE. Take $\mathbf{F}_{16}$ with $L = \mathbf{F}_{16}$. Then $R = x^{16} + x$ and we split R as $R = R_1 + R_2$ with $R_1 = x^{16} + x^2$ and $R_2 = x^2 + x$. In this case $r = 4$, $s = t = 1$, $L_1 = \mathbf{F}_8$, $L_2 = \mathbf{F}_2$ and $\delta = 2$. From Proposition (1.3) we see that the curve C defined over $\mathbf{F}_{16}$ by

$$y^{15} = (x^{16} + x^2)/(x^2 + x) = x^{14} + x^{13} + \cdots + x$$

has genus $g(C) = 49$ and $\# C(\mathbf{F}_{16}) = 14 \times 15 + 3 = 213$ since the ramification points over the branch points in $\mathbf{F}_2 \cup \infty$ are rational. This provides a new entry for the tables in [2].

We remark that the ratio $\# C(\mathbf{F}_q)/g(\mathbf{F}_q)$ for the curves that appear in Proposition (1.3) exceeds $2p^r/(p^{r-s} + p^t)$, which is optimal for $s = t = [r/2]$. For that choice

$$\# C(\mathbf{F}_q)/g(C) > \begin{cases} \sqrt{p^r} & \text{for } r \text{ even}, \\ 2\sqrt{p^{r+1}}/(p+1) & \text{for } r \text{ odd}. \end{cases} \tag{6}$$

From (6) it follows that the case $L = \mathbf{F}_{p^m}$ with $R = x^{p^m} - x$ is of special interest.

2. THE CASE $L = \mathbf{F}_q$

In this section we consider the case where L equals the full vector space $\mathbf{F}_q$. For odd m we write

$$x^{p^m} - x = R_1 + R_2 = (x^{p^m} - ax^{p^{(m-1)/2}}) + (ax^{p^{(m-1)/2}} - x),$$

with $a \in \mathbf{F}_q^*$; i.e., we look at the case $s = t = [m/2]$. Since

$$\gcd(x^{p^m} - ax^{p^{(m-1)/2}},\ ax^{p^{(m-1)/2}} - x) = \gcd(x^{p^m} - x,\ ax^{p^{(m-1)/2}} - x)$$

we have for $u \in \mathbf{F}_q^*$

$$u \in L_1 \cap L_2 \Leftrightarrow u^{p^{(m-1)/2}-1} = 1/a.$$

This equation has no solutions in $\mathbf{F}_q^*$ if a is not a $(p^{(m-1)/2} - 1)$th power in $\mathbf{F}_q^*$ and the number of solutions in $\mathbf{F}_q^*$ is $\gcd(p^{(m-1)/2} - 1, p^m - 1) = p - 1$ if a is a $(p^{(m-1)/2} - 1)$th power in $\mathbf{F}_q^*$. The latter holds always if $p = 2$.

First we consider the case that a is a $(p^{(m-1)/2} - 1)$th power in $\mathbf{F}_q^*$. Often we shall write $a \in (\mathbf{F}_q^*)^d$ to indicate that a is a dth power in $\mathbf{F}_q^*$.

(2.1) PROPOSITION. *For odd $m \geq 3$ the curve C_m defined over $\mathbf{F}_{q=p^m}$ by the equation*

$$y^{q-1} = -\frac{(x^{p^{(m+1)/2}} - a^{p^{(m+1)/2}}\, x)^{p^{(m-1)/2}}}{ax^{p^{(m-1)/2}} - x}$$

with $a \in (\mathbf{F}_q^*)^{p^{(m-1)/2}-1}$ has genus

$$g(C_m) = \{(p^{(m+1)/2} + p^{(m-1)/2} - p - 1)(q-2) - p^2 + p + 2\}/2$$

and has the following number of rational points:

$$\#C_m(\mathbf{F}_q) = \begin{cases} (q-1)(q-p) & \text{for odd } p, \\ (q-1)(q-p) + 3 & \text{for } p = 2. \end{cases}$$

Proof. The degree of $\gcd(R_1, R_2) = \gcd(x^{p^{(m+1)/2}} - a^{p^{(m+1)/2}}\, x,\ ax^{p^{(m-1)/2}} - x)$ is the cardinality of the $\mathbf{F}_p$-vector space $L_1 \cap L_2$. The condition that a is a $(p^{(m-1)/2} - 1)$th power implies $\delta = p$. We have $s = t = (m-1)/2$ and the expression for the genus now follows directly by substitution in Proposition (1.3). Over each $y \in \mathbf{F}_q^*$ we have $p^m - \delta = p^m - p$ rational points on C_m. The only branch points which possibly contribute rational points to C_m are the branch points in $\mathbf{F}_p \cup \infty$. Over each point of $\mathbf{F}_p \cup \infty$ there lie $p - 1$

ramification points on C_m. These are rational if and only if $-a$ is a $(p-1)$th power in $\mathbf{F}_q$. This holds for pairs (p, m) with pm even, which implies our formula for $\#C_m(\mathbf{F}_q)$. ■

(2.2) EXAMPLE. As an illustration of Proposition (2.1) we take $p = 3$, $m = 3$ and get the curve C over $\mathbf{F}_{27}$ given by

$$-y^{26} = x^{24} + x^{22} + \cdots + x^2$$

with $g(C) = 98$ and $\#C(\mathbf{F}_{27}) = 624$. In this case the Oesterlé upper bound is $b = 745$, so C satisfies our qualification criterion $\#C(\mathbf{F}_{27}) \geq [b/\sqrt{2}]$ for the tables in [2].

For another example we take $\mathbf{F}_{32}$. Then the curve C with affine equation

$$y^{31} = (x^8 + x)^4/(x^4 + x)$$

has genus $g(C) = 135$ and $\#C(\mathbf{F}_{32}) = 31 \times 30 + 3 = 933$. The Oesterlé upper bound in this case is 1098.

For $q = 3^5$ we obtain from Proposition (2.1) a curve C of genus $g(C) = 3854$ and $\#C(\mathbf{F}_{243}) = 58{,}080$. The Oesterlé upper bound is 81,835.

For a not a $(p^{(m-1)/2} - 1)$th power in $\mathbf{F}_q^*$ we have a similar proposition.

(2.3) PROPOSITION. *For odd $m \geq 3$ the curve C_m over $\mathbf{F}_{q=p^m}$ defined by*

$$y^{q-1} = -\frac{(x^{p^{(m+1)/2}} - a^{p^{(m+1)/2}} x)^{p^{(m-1)/2}}}{a x^{p^{(m-1)/2}} - x}$$

with $a \notin (\mathbf{F}_q^*)^{p^{(m-1)/2}-1}$ has genus

$$g(C_m) = \{(p^{(m+1)/2} + p^{(m-1)/2} - 2)(q-2) - 2p + 4\}/2$$

and has the following number of rational points:

$$\#C_m(\mathbf{F}_q) = \begin{cases} (q-1)^2 & \text{if } -a \notin (\mathbf{F}_q^*)^{p-1}, \\ (q-1)^2 + 2(p-1) & \text{if } -a \in (\mathbf{F}_q^*)^{p-1}. \end{cases}$$

Proof. The proof is similar to that of Proposition (2.1) with the following modifications. In this case $\gcd(R_1, R_2)$ has degree 1 which means that $\delta = \#(L_1 \cap L_2) = 1$ and over each $y \in \mathbf{F}_q^*$ we have $p^m - \delta = p^m - 1$ rational points on C_m. The branch points which possibly contribute rational points on C_m are 0 and ∞. Over these points there are $p-1$ ramification points on C_m which are rational points if and only if $-a$ is a $(p-1)$th power in $\mathbf{F}_q$. This gives the formula for the number of rational points. ■

(2.4) EXAMPLES. For p odd we take $a = -1$ since -1 is not a $(p^{(m-1)/2} - 1)$th power in $\mathbf{F}_q^*$. Over $\mathbf{F}_{27}$ the curve C_m has genus $g(C_m) = 124$ and $\#C_m(\mathbf{F}_{27}) = 680$ while the Oesterlé upper bound is 901. Over $\mathbf{F}_{3^5}$ we find $g(C_m) = 4096$ and $\#C_m(\mathbf{F}_{3^5}) = 58{,}568$. The Oesterlé upper bound is here 86,441.

For $q = p^m$ with m even the splitting

$$x^q - x = (x^q - ax^{\sqrt{q}}) + (ax^{\sqrt{q}} - x),$$

where $a \in \mathbf{F}_q^*$ is such that $a \notin (\mathbf{F}_q^*)^{\sqrt{q}-1}$ yields very good curves.

(2.5) PROPOSITION. *If $q = p^m$ with m even then the curve C_m defined over $\mathbf{F}_{q=p^m}$ by the equation*

$$y^{q-1} = -\frac{x^q - ax^{\sqrt{q}}}{ax^{\sqrt{q}} - x} \quad \text{with} \quad a \in \mathbf{F}_q^*,\ a \notin (\mathbf{F}_q^*)^{\sqrt{q}-1}$$

has genus $g(C_m) = (\sqrt{q} - 1)(q - 2) - \sqrt{q} + 2$ and $\#C_m(\mathbf{F}_q) = (q-1)^2$.

Proof. In this situation we have $s = t = m/2$ and the condition $a^{\sqrt{q}+1} \neq 1$ implies $L_1 \cap L_2 = \{0\}$, so $\delta = 1$. The formula for $g(C_m)$ follows from Proposition (1.3). Over each $y \in \mathbf{F}_q^*$ there are $p^m - \delta$ rational points on C_m. The only branch points which possibly give rise to rational points on C_m are 0 and ∞. The ramification points over 0 (resp. ∞) on C_m are rational iff the equation $w^{\sqrt{q}-1} = -a$ (resp. $w^{\sqrt{q}-1} = (-1/a)$) is solvable in $\mathbf{F}_q$. Since $a^{\sqrt{q}+1} \neq 1$ these equations have no solutions in $\mathbf{F}_q$ and consequently we have $\#C_m(\mathbf{F}_q) = (q-1)^2$. ∎

Note that in this case

$$\#C_m(\mathbf{F}_q)/g(C_m) > \sqrt{q} + 1.$$

(2.6) EXAMPLES. For $q = 9$ we find $g(C_m) = 13$ and $\#C_m(\mathbf{F}_9) = 64$. This is very close to the Oesterlé upper bound 66 and might well be optimal (i.e., equal to the actual maximum number $N_q(g)$, cf. [2]). For $q = 16$ we find $g(C_m) = 40$, $\#C_m(\mathbf{F}_{16}) = 225$; the Oesterlé upper bound is 244. For $q = 64$ we find $g(C_m) = 428$ and $\#C_m(\mathbf{F}_{64}) = 3969$ with Oesterlé upper bound 4786. For $q = 81$ we find $g(C_m) = 625$ and $\#C_m(\mathbf{F}_{81}) = 6400$, still reasonable compared with the Oesterlé upper bound 7824.

3. SUBSPACES OF CODIMENSION 1

We take as a subspace of $\mathbf{F}_q$ the $(m-1)$-dimensional subspace

$$L = \{x \in \mathbf{F}_q : \mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(x) = 0\}, \quad \text{where} \quad \mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_p}(x) = x^{p^{m-1}} + \cdots + x^p + x,$$

and put $R(x) = \sum_{i=0}^{m-1} x^{p^i}$. Note that by a transformation $x \mapsto ax$ on $\mathbf{F}_q$ with $a \in \mathbf{F}_q^*$ we can transform any codimension 1 space into this subspace L. We split the polynomial R as $R_1 + R_2$ with $R_1 = \sum_{i=s}^{m-1} x^{p^i}$ and $R_2 = \sum_{i=0}^{s-1} x^{p^i}$. The corresponding curve C_m over $\mathbf{F}_q$ is defined by

$$y^{q-1} = -(x^{p^{m-1-s}} + \cdots + x)^{p^s}/(x^{p^{s-1}} + \cdots + x). \tag{7}$$

Applying Proposition (1.3) to this situation gives the following result.

(3.1) PROPOSITION. *For $m \geq 3$ and $0 < s < m-1$ such that* $\gcd(m, s) = 1$ *the curve C_m given by* (7) *has genus*

$$g(C_m) = \{(p^{m-1-s} + p^{s-1} - 2)(q-2) - 2p + 4\}/2$$

and

$$\#C_m(\mathbf{F}_q) = \begin{cases} (p^{m-1}-1)(q-1) & \text{if } pm \text{ odd and } p \nmid s(m-s), \\ (p^{m-1}-1)(q-1) + (p-1) & \text{if } pm \text{ odd and } p \mid s(m-s), \\ (p^{m-1}-1)(q-1) + 2(p-1) & \text{if } pm \text{ even and } p \nmid s(m-s), \\ (p^{m-1}-1)(q-1) + 3(p-1) & \text{if } pm \text{ even and } p \mid s(m-s). \end{cases}$$

Proof. In the notation used in Section 1 we find

$$L_1 = \{x \in \mathbf{F}_{p^{m-s}} : \mathrm{Tr}_{\mathbf{F}_{p^{m-s}}/\mathbf{F}_p}(x) = 0\}$$

and

$$L_2 = \{x \in \mathbf{F}_{p^s} : \mathrm{Tr}_{\mathbf{F}_{p^s}/\mathbf{F}_p}(x) = 0\}.$$

Then $L_1 \cap L_2 \subset \mathbf{F}_{p^{m-s}} \cap \mathbf{F}_{p^s} = \mathbf{F}_{p^{\gcd(m,s)}} = \mathbf{F}_p$. Combining $\gcd(m, s) = 1$ with the condition on the traces gives $L_1 \cap L_2 = \{0\}$, hence $\delta = 1$. If $p \nmid s(m-s)$ the ramification points over $L_1 - \{0\}$ and $L_2 - \{0\}$ are not rational. On the other hand, if $p \mid s(m-s)$ then $\mathbf{F}_q^* \cap (L_1 \cup L_2) = \mathbf{F}_p^*$ and the ramification points over $\mathbf{F}_p^*$ are rational. Over the branch point 0 (resp. ∞) which has multiplicity $p^s - 1$ (resp. $p^{m-1} - p^{s-1}$) there lie $p-1$ ramification points on C_m. These are rational if and only if -1 is a $(p-1)$th power in $\mathbf{F}_q$ which holds if and only if pm is even. The formulas now follow from Proposition (1.3). ■

(3.2) EXAMPLES. Take $\mathbf{F}_{27}$; then $L = \{x \in \mathbf{F}_{27} : \mathrm{Tr}_{\mathbf{F}_{27}/\mathbf{F}_3}(x) = 0\}$ is given by $R(x) = x^9 + x^3 + x$ and we can consider the curve

$$C : y^{26} = -(x^8 + x^2).$$

It follows from Proposition (3.1) that $g(C) = 24$ and $\#C(\mathbf{F}_{27}) = 208$ which improves [2].

For $\mathbf{F}_{32}$ with (7) of the form $y^{31} = (x^4 + x^2 + x)^4/(x^2 + x)$ we obtain according to Proposition (3.1) a curve C of genus 60 and $\#C(\mathbf{F}_{32}) = 468$. The Oesterlé upper bound is 542.

(3.3) EXAMPLE. Finally we consider an example where $\gcd(m, s) \neq 1$. Take $\mathbf{F}_{64}$ and

$$f(x) = \frac{x^{32} + x^{16}}{x^8 + x^4 + x^2 + x} = \frac{(x^2 + x)^{15}}{(x^4 + x + 1)(x^2 + x + 1)}.$$

For the curve C given by $y^{63} = f(x)$ Proposition (1.2) implies that $2g - 2 = 7 \times 63 - 3 \times 3 - 6 \times 1$, hence $g(C) = 214$. Each of the branch points 0, 1, and ∞ induces three rational ramification points on C and the zeros of $x^2 + x + 1$ induce one ramification point each, while the ramification points from the zeros of $x^4 + x + 1$ are not rational. The number of rational points on C is thus $\#C(\mathbf{F}_{64}) = (32 - 2) \times 63 + 11 = 1901$. The Oesterlé upper bound is 2553.

(3.4) *Remark*. For even m and $L = \{x \in \mathbf{F}_{q=p^m} : \mathrm{Tr}_{\mathbf{F}_{p^m}/\mathbf{F}_p}(x) = 0\}$ the splitting

$$\sum_{i=0}^{m-1} x^{p^i} = R_1 + R_2 = \sum_{i=m/2}^{m-1} x^{p^i} + \sum_{i=0}^{(m/2)-1} x^{p^i}$$

does not satisfy condition (i). The corresponding equation $y^{q-1} = -R_1/R_2 = -R_2^{\sqrt{q}-1}$ leads to the curve

$$C : y^{\sqrt{q}+1} = aR_2 = a(x^{p^{(m/2)}-1} + x^{p^{(m/2)}-2} + \cdots + x), \tag{8}$$

where $a \in \mathbf{F}_q^*$ is such that $a^{\sqrt{q}} + a = 0$.

To determine $g(C)$ and $\#C(\mathbf{F}_q)$ we consider the $\mathbf{F}_p$-linear map ϕ on L defined by $\phi(x) = aR_2(x)$. The kernel of ϕ is

$$\ker(\phi) = \{x \in \mathbf{F}_{\sqrt{q}} : \mathrm{Tr}_{\mathbf{F}_{\sqrt{q}}/\mathbf{F}_p}(x) = 0\} \quad \text{and} \quad \phi(L) = \mathbf{F}_{\sqrt{q}}.$$

For $y \in \mathbf{F}_q^*$ we have $y^{\sqrt{q}+1} \in \mathbf{F}_{\sqrt{q}}^*$, so over each $y \in \mathbf{F}_q^*$ there are $\#\ker(\phi) = \sqrt{q}/p$ rational points on C. The set of branch points is $\ker(\phi) \cup \infty$ and each branch point induces one rational point on C. Hence

$$\#C(\mathbf{F}_q) = (q - 1)\sqrt{q}/p + \sqrt{q}/p + 1 = (q\sqrt{q}/p) + 1.$$

From Proposition (1.2) we find $g(C) = (q - p\sqrt{q})/2p$. We thus get explicit maximal curves:

(3.5) PROPOSITION. *The curve C over $\mathbf{F}_q$ given by* (8) *with* $g(C) = (q - p\sqrt{q})/2p$ *and* $\#C(\mathbf{F}_q) = (q\sqrt{q}/p) + 1$ *is a maximal curve; i.e., it attains the Hasse-Weil upper bound.*

By the substitution $x \mapsto z^p - z$ in (8) we obtain the equation for the Hermitian curve $y^{\sqrt{q}+1} = a(z^{\sqrt{q}} - z)$. So the curve C figuring in Proposition (3.5) is a quotient of the Hermitian curve.

4. VARIATIONS

To find curves with many points with this method it is not necessary to depart from a linearized polynomial. This is illustrated by the following example, where we take a curve of the form

$$y^{q-1} = xf(x)^p$$

with $f(x) \in \mathbf{F}_q[x]$.

(4.1) EXAMPLE. Take $\mathbf{F}_{16}$ and consider the irreducible complete non-singular curve C given by the affine equation

$$y^{15} = x(x^2 + x + 1)^2.$$

Remark that $x(x^2 + x + 1)^2 = x^5 + x^3 + x$ satisfies Conditions (1.1). According to (1) the curve C has genus $g(C) = 12$ and the number of points is $\#C(\mathbf{F}_{16}) = 15 \times 5 + 8 = 83$, where the branch point ∞ contributes 5 rational points and the branch points in $\mathbf{F}_4 - \{1\}$ each contribute 1 rational point. This example provides a new entry for the tables [2], where the interval [68–97] is given.

An advantage of our method is that we can also find good curves C such that only a few fibres over $\mathbf{P}^1(\mathbf{F}_q)$ contribute to the rational points on C, but these then do so substantially, as in the preceding example. We can use this for instance to construct Artin-Schreier covers of C given by

$$z^p - z = h(x),$$

where in order to obtain good curves one has to impose the condition $\mathrm{Tr}(h(x)) = 0$ for a few values x only.

(4.2) EXAMPLE. Take the field $\mathbf{F}_{32}$ and consider the curve C defined by

$$y^{31} = x^5 + x^3.$$

The polynomial $x^5 + x^3 + 1$ is irreducible over $\mathbf{F}_2$, so it has five zeros in $\mathbf{F}_{32}$. There are three ramification points, P_0, P_1, and P_∞, lying over 0, 1, and ∞.

$$g(C) = 15, \quad \#C(\mathbf{F}_{32}) = 158,$$

which comes up to the best value known for $(q, g) = (32, 15)$ in [2].

We immediately see that the zeros $x \in \mathbf{F}_{32}$ of $x^5 + x^3 + 1$ satisfy $\mathrm{Tr}(x) = 0$. The divisor of x is

$$(x) = 31P_0 - 31P_\infty.$$

The Artin-Schreier cover $\tilde{C}$ of C given by

$$z^2 + z = x$$

has 2 rational points over each of the 155 points (x, y) of $C(\mathbf{F}_{32})$ with $y \in \mathbf{F}_{32}^*$. We thus find

$$\#\tilde{C}(\mathbf{F}_{32}) = 2 \times 155 + 1 + 2 = 313,$$

and $g(\tilde{C}) = 45$. (See [3] for formulas for the genus.) This improves [2], where the interval is [302–428].

As a variation on this theme we take $\mathbf{F}_{16}$ with the curve C given by

$$y^{15} = x^4 + x^3.$$

This has genus $g(C) = 6$ with 65 rational points. The Artin-Schreier cover $\tilde{C}$ of C defined by $z^2 + z = 1/x$ yields a curve of genus $g(\tilde{C}) = 20$ with $\#\tilde{C}(\mathbf{F}_{16}) = 127$.

If one has a curve C with many points then often a curve C' obtained as the image under a $\mathbf{F}_q$-morphism $C \to C'$ is also a good curve because the set of eigenvalues of Frobenius for C' is a subset of those for C. In the cases dealt with in the preceding sections where the curve is of the form

$$y^{q-1} = f(x^{p-1}),$$

we can consider the curves $y^s = f(x^t)$ for any divisor s of $q - 1$ and t of $p - 1$.

(4.3) EXAMPLE. From the curve C over $\mathbf{F}_{27}$ given in Example (2.2) we obtain the curve C'

$$-y^{13} = x^{24} + x^{22} + \cdots + x^2 \text{ with } g(C') = 48 \quad \text{and} \quad \#C'(\mathbf{F}_{27}) = 316,$$

where the tables give [325–402], and

$$-y^{26} = x^{12} + x^{11} + \cdots + x \text{ with } g(C') = 49 \quad \text{and} \quad \#C'(\mathbf{F}_{27}) = 314,$$

a new entry in the tables.

Of course, the methods can be varied in several ways. For example, one can replace y^{q-1} by y^t for t a divisor of $q-1$ and take a function f which assumes for many x a tth power in F_q. We now give an example of this.

(4.4) EXAMPLE. Take $\mathbf{F}_{81}$ and consider the curve given by the equation

$$y^{10} = x^2 + x.$$

For $y \in \mathbf{F}_{81}$ we have $y^{10} \in \mathbf{F}_9$, so the equation $x^2 + x = y^{10}$ always has solutions $x \in \mathbf{F}_{81}$. The curve C has genus $g(C) = 4$ and $\#C(\mathbf{F}_{81}) = 154$. Consider the double cover $\tilde{C}$ of C given by

$$z^2 = x^2 + x + 2.$$

Over each $(x, y) \in C(\mathbf{F}_{81})$ with $y \in \mathbf{F}_{81}^*$ the curve $\tilde{C}$ has rational points since $x^2 + x + 2 \in \mathbf{F}_9$. A computation of the genus and the number of points yields

$$g(\tilde{C}) = 17, \quad \#\tilde{C}(\mathbf{F}_{81}) = 288.$$

This is a new entry for the tables [2].

We can also apply the methods to a base curve different from $\mathbf{P}^1$ as the following examples show.

(4.5) EXAMPLE. Take $\mathbf{F}_8$ and consider the curve C of genus 1 defined by

$$y^2 + y = x + \frac{1}{x} + 1.$$

It has 14 rational points, namely the two ramification points P_0 and P_∞, and six pairs of points P_ζ, P'_ζ, one over each 7th root $\zeta \neq 1$ of 1. Consider now the cover $\tilde{C}$ of C defined by

$$z^7 = x(x^6 + 1)/(x + 1);$$

cf. Proposition (2.1). It has branch points P_0 and P_∞ and P_x, P'_x for x a third root of unity. Then the genus $g(\tilde{C})$ satisfies $2g(\tilde{C}) - 2 = 7 \times 0 + 8 \times 6 = 48$, hence $g(\tilde{C}) = 25$. The rational points come from 12 fibres of order 7 over P_ζ and P'_ζ, and from the two ramification points over P_0 and P_∞, giving $\#\tilde{C}(\mathbf{F}_8) = 86$, which improves the entry [84–97] of the tables.

(4.6) EXAMPLE. Take $\mathbf{F}_8$ and consider the Klein curve C of genus 3 defined by $y^3 + x^3y + x = 0$. It has 24 rational points. Consider then the cover $\tilde{C}$ given by $z^7 = x(x^6 + 1)/(x + 1)$. The branch points on C are the points lying over $x = 0$, $x =$ a third root of unity and $x = \infty$. We find $g(\tilde{C}) = 51$ and $\#\tilde{C}(\mathbf{F}_8) = 132$. The Oesterlé upper bound is 173.

(4.7) EXAMPLE. Take $\mathbf{F}_9 = \mathbf{F}_3[i]$ with $i^2 = -1$ and consider the curve C of genus 1 defined by

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

It has 16 rational points over $\mathbf{F}_9$, the 4 ramification points P_0, P_∞, P_i and P_{-i}, and 6 pairs P_x, P'_x for $x \in \mathbf{F}_9 - \{0, \pm i\}$. Take the function $f = x/y$ with divisor $(f) = P_0 + P_\infty - P_i - P_{-i}$ and consider the cover $\tilde{C}$ of C defined by

$$z^4 = f^3 + f.$$

Observe that for $u \in \mathbf{F}_9^*$ the expression $u^3 + u$ is a 4th power in $\mathbf{F}_9^*$. One has $(f(f^2 + 1)) = P_0 + P_\infty + 2P_1 + 2P'_1 - 3P_i - 3P_{-i}$. The curve $\tilde{C}$ has genus $g(\tilde{C}) = 9$ and has $10 \times 4 + 4 + 4 = 48$ rational points. Here the points P_0, P_∞, P_i, P_{-i} are branch points with total ramification, while the branch points P_1 and P'_1 each contribute 2 rational points. This comes up to the best known curve and is very close to the Oesterlé upper bound 51.

(4.8) EXAMPLE. Take $\mathbf{F}_9 = \mathbf{F}_3[i]$ with $i^2 = -1$ and consider the curve C of genus 2 defined by

$$z^2 = x(x^4 + x^2 + 2).$$

It has 18 rational points over $\mathbf{F}_9$. We denote them by P_0, P_∞ and by P_x, P'_x in the fibre over x for each $x \in \mathbf{F}_9^*$. According to Proposition (2.5) the Kummer cover D of $\mathbf{P}^1$ defined by

$$y^8 = -\frac{(x^9 - ax^3)}{(ax^3 - x)} = -\frac{x^2(x^2 - a^3)^3}{ax^2 - 1} \qquad \text{with } a \text{ such that } a^2 + a + 2 = 0 \tag{9}$$

has fibres consisting of 8 rational points over each $x \in \mathbf{F}_9^*$. We consider the curve $\tilde{C}$ which is the cover of C defined by (9). The branch points on C are the four points P_0, P_∞, P_ξ, P'_ξ with $\xi^2 = a^3$ and the four points P_η, P'_η with $\eta' = 1/a$. The divisor of the function f given by the right hand side of (9) is

$$(f) = 4P_0 + 6P_\xi + 6P_{-\xi} - P_\eta - P'_\eta - P_{-\eta} - P'_{-\eta} - 12P_\infty.$$

By Hurwitz-Zeuthen the genus is 33. Over each $x \in \mathbf{F}_9^*$ we find 16 rational points on $\tilde{C}$ giving $\#\tilde{C}(\mathbf{F}_9) = 128$, a significant improvement of the entry [109–133] in the tables [2].

If we take here instead of the base curve C the curve C' of genus 2 with 18 rational points defined by

$$z^2 = x(x^4 + x^3 + x^2 + x + 1)$$

then (9) defines a Kummer cover $\tilde{C}'$ of C' of genus 41 with 128 rational points.

By employing the methods in a systematic way we expect more improvements and supplements to the tables in [2].

5. SUMMARY

For a summary of the new results from our examples for tables of curves with many points, see Table 1.

TABLE 1

q	$g(C)$	New entry	Old entry
		$\langle p = 2 \rangle$	
8	25	[86–97]	[84–97]
8	51	[132–173]	
16	12	[83–97]	[68–97]
16	20	[127–140]	[121–140]
16	40	[225–244]	[197–244]
16	49	[213–286]	
32	45	[313–428]	[304–428]
32	60	[468–542]	
32	135	[933–1098]	
64	214	[1901–2553]	
64	428	[3969–4786]	
		$\langle p = 3 \rangle$	
9	13	[64–66]	[60–66]
9	33	[128–133]	[109–133]
9	41	[128–158]	[119–158]
27	24	[208–235]	[190–235]
27	49	[314–409]	
27	98	[624–745]	
27	124	[680–901]	
81	17	[288–387]	
81	625	[6400–7824]	
243	3854	[58080–81835]	
243	4096	[58568–86441]	

REFERENCES

1. R. Auer, Ray class fields of global function fields with many rational places, preprint, University of Oldenburg, 1998.
2. G. van der Geer and M. van der Vlugt, Tables of curves with many points, *Math. Comput.* **69** (2000), 797–810.
3. H. Stichtenoth, "Algebraic Function Fields and Codes," Springer-Verlag, Berlin, 1993.