Journal of Number Theory **72**, 257–268 (1998)
Article No. NT982277

Generalized Reed–Muller Codes and Curves with Many Points

G. 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

M. van der Vlugt

E-mail: vlugt@wi.leidenuniv.nl

Communicated by D. Zagier

Received October 28, 1997; revised January 30, 1998

Words of low weight in trace codes correspond to curves with many points and the same holds for subcodes of low weight via the fibre product construction. In 1996 Heijnen and Pellikaan gave an algorithm to determine a basis of minimum weight subcodes of generalized Reed–Muller codes. We show how this algorithm can be used to produce curves with many points and also some new families of curves which reach the Hasse–Weil upper bound. © 1998 Academic Press

In the quest for curves over finite fields with many points coding theory has been a useful guide, as words of low weight in trace codes correspond to Artin–Schreier curves with many points. This correspondence can be extended to subcodes of low weight and fibre products of Artin–Schreier curves. Subcodes of minimum weight of a code $\mathscr{C}$ determine the weight hierarchy of $\mathscr{C}$ and knowledge of the weight hierarchy indicates where curves with many points are likely to be found. However, determination of weight hierarchies is a hard problem in coding theory. In 1990 Wei found the weight hierarchy of the classical binary Reed–Muller codes (see [W]). Six years later Heijnen and Pellikaan succeeded in finding the weight hierarchy of Reed–Muller codes over arbitrary finite fields, cf. [H-P]. In this paper we

0022-314X/98 $25.00

derive some results on curves with many points which are closely related to the weight hierarchy of the q-ary or generalized Reed–Muller codes. We use subcodes of generalized Reed–Muller codes to construct our curves. We also present some types of curves which attain the Hasse–Weil upper bound.

1. ON THE WEIGHT HIERARCHY OF GENERALIZED REED–MULLER CODES

Let $\mathscr{C}$ be a (linear) code of length n and dimension k over a finite field $\mathbb{F}_{q=p^t}$. An important parameter of a subcode $\mathscr{D}$ is its weight $w(\mathscr{D})$, by which we mean the number of coordinate places for which at least one word of $\mathscr{D}$ has a non-zero coordinate. Since the projection of $\mathscr{D}$ onto a coordinate place is a $\mathbb{F}_q$-linear map we have

$$w(\mathscr{D}) = \frac{1}{q^r - q^{r-1}} \sum_{d \in \mathscr{D}} w(d), \tag{1}$$

where $r = \dim(\mathscr{D})$ and $w(d)$ is the weight of the word d. The rth generalized Hamming weight $d_r(\mathscr{C})$ for $1 \leqslant r \leqslant k$ is defined by

$$d_r(\mathscr{C}) = \min\{w(\mathscr{D}): \mathscr{D} \text{ is an } r\text{-dimensional subcode of } \mathscr{C}\}.$$

The set $\{d_r(\mathscr{C}): 1 \leqslant r \leqslant k\}$ is called the *weight hierarchy* of $\mathscr{C}$.

The family of q-ary or generalized Reed–Muller codes can be defined as follows. Elements of the vector space

$$P_s = \{f \in \mathbb{F}_q[X_1, ..., X_m]: \deg(f) \leqslant s\}$$

can be evaluated at the points of the affine space $\mathbb{F}_q^m$. This defines an evaluation map

$$\beta: P_s \to \mathbb{F}_q^n$$

with $n = q^m$ given by $f \mapsto (f(v))_{v \in \mathbb{F}_q^m}$. Note that the kernel of β is the ideal generated by the polynomials $X_i^q - X_i$. A polynomial $f \in P_s$ is called *reduced* (modulo the kernel of β) if f is a $\mathbb{F}_q$-linear combination of monomials $X_1^{d_1} X_2^{d_2} \cdots X_m^{d_m}$ with $0 \leqslant d_i \leqslant q-1$ for $1 \leqslant i \leqslant m$. The image $\beta(P_s)$ is the q-ary Reed–Muller code $R_q(s, m)$ of order s in m variables. One thus obtains a large class of codes.

In the paper by Heijnen and Pellikaan [H-P] one can find the following algorithm which determines an r-dimensional subcode of $R_q(s, m)$ of minimum weight. First we fix an enumeration $\{\alpha_0, \alpha_1, ..., \alpha_{q-1}\}$ of $\mathbb{F}_q$.

(1) Let $Q = \{0, 1, ..., q-1\}$. The set Q^m is ordered lexicographically using the natural order on Q. Elements of Q^m are denoted by $\sigma = (i_1, ..., i_m)$ and have a degree defined by

$$\deg(\sigma) = \sum_{j=1}^{m} i_j.$$

(2) To an element $\sigma \in Q^m$ associate the following reduced polynomial $f = f_\sigma$:

$$f = \prod_{j=1}^{m} \prod_{t=i_j+1}^{q-1} (X_j - \alpha_t). \tag{2}$$

(3) Take the first r elements of degree $\geqslant m(q-1)-s$ in Q^m.

According to one of the main results in [H-P, Theorem 5.9] the outcome of the algorithm is:

(1.1) THEOREM. *Let $\sigma_1, ..., \sigma_r$ be the first r elements in Q^m with $\deg(\sigma_i) \geqslant m(q-1)-s$. Then the codewords induced by the polynomials $f_1, ..., f_r$ associated to $\sigma_1, ..., \sigma_r$ generate an r-dimensional subcode of minimum weight of $R_q(s, m)$.*

The same theorem in [H-P] also yields a formula for $d_r(R_q(s, m))$.

(1.2) *Formula.* If $\sigma_r = (i_1, ..., i_m)$ is the rth element in Q^m of degree $\geqslant m(q-1)-s$ then

$$d_r(R_q(s, m)) = 1 + \sum_{j=1}^{m} i_{m-j+1} q^{j-1}.$$

To illustrate this algorithm we consider an example.

(1.3) EXAMPLE. We enumerate $\mathbb{F}_p = \{\alpha_0, \alpha_1, ..., \alpha_{p-1}\} = \{p-1, p-2, ..., 0\}$ and we consider $R_p(2, 3)$ for an odd prime p. The first four elements $\sigma \in Q^m$ with degree $\geqslant 3(p-1)-2 = 3p-5$ are $(p-3, p-1, p-1)$, $(p-2, p-2, p-1)$, $(p-2, p-1, p-2)$, and $(p-2, p-1, p-1)$.

According to (2) the corresponding f_i are

$$f_1 = (X_1 - 1) X_1, \qquad f_2 = X_1 X_2, \qquad f_3 = X_1 X_3, \qquad \text{and} \qquad f_4 = X_1.$$

Now the codewords induced by $f_1 = X_1^2 - X_1$, $f_2 = X_1 X_2$, and $f_3 = X_1 X_3$ generate a 3-dimensional subcode of $R_p(2, 3)$ denoted by $\langle f_1, f_2, f_3 \rangle$ and

$$d_3(R_p(2, 3)) = 1 + (p-2) + (p-1)\, p + (p-2)\, p^2 = p^3 - p^2 - 1.$$

In the next section we relate curves to codewords in $R_q(s, m)$ and then we apply the results of this section to obtain results for curves.

2. WORDS IN $R_q(s, m)$ AND ARTIN–SCHREIER CURVES

From now on we identify reduced polynomials f in P_s and the codewords c_f which they induce by the evaluation map. A polynomial f of the form (2) is a product of independent (inhomogeneous) linear forms $(X_j - \alpha_t)$. For fixed $a \in \mathbb{F}_{q^m}$ we consider $\mathrm{Tr}(ax)$ where $\mathrm{Tr} = \mathrm{Tr}_{q^m/q}$ is the trace map from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$. When we view $\mathbb{F}_{q^m}$ as an m-dimensional vector space over $\mathbb{F}_q$ then $\mathrm{Tr}(ax)$ is a linear form in $\mathbb{F}_q[x_1, ..., x_m]$. If we choose $\mathbb{F}_q$-independent $a_1, a_2, ..., a_m$ in $\mathbb{F}_{q^m}$ we can write (2) as

$$f = \prod_{j=1}^{m} \prod_{t=i_j+1}^{q-1} (\mathrm{Tr}(a_j x) - \alpha_t).$$

Observe that for $a, b \in \mathbb{F}_{q^m}$ we have

$$\mathrm{Tr}(ax)\,\mathrm{Tr}(bx) = \mathrm{Tr}(\mathrm{Tr}(ax)\,bx) = \mathrm{Tr}\left(\sum_{j=0}^{m-1} a^{q^j} b x^{q^j+1}\right). \tag{3}$$

Repeating this process we see that the codeword corresponding to f can be written in trace form:

$$c_f = (\mathrm{Tr}(R(x)))_{x \in \mathbb{F}_{q^m}} \qquad \text{with} \quad R(x) \in \mathbb{F}_{q^m}[x].$$

An element of $\mathbb{F}_{q^m}$ has trace zero precisely if it is of the form $y^q - y$ for some $y \in \mathbb{F}_{q^m}$. Now we associate to the codeword c_f the irreducible complete smooth curve C_f over $\mathbb{F}_{q^m}$ given by the affine equation

$$y^q - y = R(x). \tag{4}$$

In the sequel we always assume that $\deg(R)$ is prime to p, the characteristic of $\mathbb{F}_{q^m}$. Then the irreducible smooth projective Artin–Schreier curve C_f given by (4) has genus

$$g(C_f) = (q-1)(\deg(R) - 1)/2. \tag{5}$$

We see immediately that there is a relation between the weigh $w(c_f)$ of c_f and the number of $\mathbb{F}_{q^m}$-rational points on C_f:

$$w(c_f) = q^m - (\#\, C_f(\mathbb{F}_{q^m}) - 1)/q. \tag{6}$$

This correspondence between codewords and curves can be extended to subcodes and fibre products of curves (see [G-V1]). If $\mathscr{D}$ is an r-dimensional subcode of $R_q(s, m)$ with basis $c_{f_1}, ..., c_{f_r}$ we consider the corresponding curves C_{f_i} defined by $y^q - y = R_i(x)$. Each of these curves admits a natural map $\varphi_i: C_{f_i} \mapsto \mathbb{P}^1$. Then we associate to $\mathscr{D}$ the curve

$$C_{\mathscr{D}} = \text{Normalization of } C_{f_1} \times_{\mathbb{P}^1} \times \cdots \times_{\mathbb{P}^1} C_{f_r}.$$

From [G-V1] we recall the following proposition.

(2.1) PROPOSITION. *The weight $w(\mathscr{D})$ satisfies*

$$w(\mathscr{D}) = q^m - (\#C_{\mathscr{D}}(\mathbb{F}_{q^m}) - 1)/q^r.$$

For f in the $\mathbb{F}_q$-vector space generated by $f_1, ..., f_r$ we denote the trace of Frobenius on C_f by τ_f (i.e., $\#C_f(\mathbb{F}_{q^m}) = q^m + 1 - \tau_f$).

According to [G-V1] the trace of Frobenius $\tau_{\mathscr{D}}$ of $C_{\mathscr{D}}$ and the genus $g(C_{\mathscr{D}})$ satisfy

$$(q-1)\,\tau_{\mathscr{D}} = \sum_{f \in \langle f_1, ..., f_r \rangle - \{0\}} \tau_f, \tag{7}$$

$$(q-1)\,g(C_{\mathscr{D}}) = \sum_{f \in \langle f_1, ..., f_r \rangle - \{0\}} g(C_f). \tag{8}$$

From (6) and Proposition (2.1) it is clear that words and subcodes of low weight correspond to curves with many rational points.

In the next section we illustrate these ideas by some examples.

3. THE CODE $R_p(2, 3)$

We consider $R_p(2, 3)$ for an odd prime p. As we saw at the end of Section 1 the first four polynomials of the form (2) are

$$f_1 = (X_1 - 1)\,X_1, \qquad f_2 = X_1 X_2, \qquad f_3 = X_1 X_3, \qquad \text{and} \qquad f_4 = X_1.$$

The number of zeros in the codeword c_{f_1} is $2p^2$, so its weight satisfies $w(c_{f_1}) = p^3 - 2p^2$. We can write $f_1 = (\mathrm{Tr}(x) - 1)\,\mathrm{Tr}(x)$, where $\mathrm{Tr} = \mathrm{Tr}_{p^3/p}$. Applying (3) we find

$$f_1 = \mathrm{Tr}(x^2 + x^{p+1} + x^{p^2+1}) - \mathrm{Tr}(x).$$

Since the trace map on $\mathbb{F}_{p^3}$ satisfies

$$\mathrm{Tr}(x^{p^2+1}) = \mathrm{Tr}(x^{p+1}) \tag{9}$$

we find for the corresponding codeword

$$c_{f_1} = \mathrm{Tr}(2x^{p+1} + x^2 - x)_{x \in \mathbb{F}_{p^3}}.$$

The curve C_{f_1} which we now associate to c_{f_1} is given by the affine equation

$$y^p - y = 2x^{p+1} + x^2 - x.$$

From the number of zeros in c_{f_1} we immediately obtain $\# C_{f_1}(\mathbb{F}_{p^3}) = 2p^3 + 1$, while according to (5) the genus satisfies $g(C_{f_1}) = (p-1)\, p/2$.

(3.1) *Result.* *For $p = 3$ we obtain a curve over $\mathbb{F}_{27}$ of genus 3 with 55 points.*

This is quite close to the upper bound 58.

(3.2) *Remark.* Note that by replacing monomials by lower degree monomials (using Frobenius as in (9)) or by neglecting the monomials or polynomials which give zero under the trace map we can reduce the genus of the curve which we associate to the codeword (see also [Wo]). This possibility of *genus reduction* makes curves much more attractive as building blocks for fibre product curves with many points.

If we change to $f_2 = \mathrm{Tr}(x)\, \mathrm{Tr}(ax)$ with $a \in \mathbb{F}_{p^3} - \mathbb{F}_p$ then along the same lines we find

$$c_{f_2} = \mathrm{Tr}((a^p + a)\, x^{p+1} + ax^2)$$

with $a^p + a \neq 0$. The word c_{f_2} has $2p^2 - p$ zeros and the corresponding curve C_{f_2} given by

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

has genus $(p-1)\, p/2$ and $\# C_{f_2}(p^3) = 2p^3 - p^2 + 1$. Now we consider the 3-dimensional subcode

$$\mathscr{D} = \langle (\mathrm{Tr}(x) - 1)\, \mathrm{Tr}(x),\ \mathrm{Tr}(x)\, \mathrm{Tr}(ax),\ \mathrm{Tr}(x)\, \mathrm{Tr}(bx) \rangle$$

with $\{1, a, b\} \subset \mathbb{F}_{p^3}$ independent over $\mathbb{F}_p$.

(3.3) Proposition. *The curve $C_{\mathscr{D}}$ defined over $\mathbb{F}_{p^3}$ corresponding to the subcode $\mathscr{D} = \langle c_{f_1}, c_{f_2}, c_{f_3} \rangle$ has genus $(p^4 - p)/2$ and $\# C_{\mathscr{D}}(\mathbb{F}_{p^3}) = p^5 + p^3 + 1$.*

Proof. The curves which occur in the fibre product induced by $\mathscr{D}$ are of the form

$$y^p - y = (2\lambda_1 + \lambda_2(a^p + a) + \lambda_3(b^p + b))\, x^{p+1} + (\lambda_1 + \lambda_2 a + \lambda_3 b)\, x^2 - \lambda_1 x \tag{10}$$

with $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{F}_p^3 - \{0\}$. The coefficient of x^{p+1} can be written as

$$(\lambda_1 + \lambda_2 a + \lambda_3 b)^p + (\lambda_1 + \lambda_2 a + \lambda_3 b).$$

If this coefficient is zero then $\lambda_1 + \lambda_2 a + \lambda_3 b \in \mathbb{F}_{p^2} \cap \mathbb{F}_{p^3} = \mathbb{F}_p$. Since $\{1, a, b\}$ are $\mathbb{F}_p$-independent we find $\lambda_2 = \lambda_3 = 0$ which implies $\lambda_1 = 0$. So the right-hand side of (10) has degree $p+1$ and the curves defined by (10) have genus $(p-1)\, p/2$. From (7) we derive

$$g(C_{\mathscr{D}}) = (p^3 - 1)\, p/2.$$

Moreover we saw at the end of Section 1 that $d_3(R_p(2, 3)) = p^3 - p^2 - 1$ and then Proposition (2.1) yields $\# C_{\mathscr{D}}(\mathbb{F}_{p^3}) = p^5 + p^3 + 1$.

(3.4) COROLLARY. *For $p = 3$ the curve $C_{\mathscr{D}}$, which is defined over $\mathbb{F}_{27}$, has genus 39 and $\# C_{\mathscr{D}}(\mathbb{F}_{27}) = 271$.*

Corollary (3.4) gives an improvement of the best value known until now for $(q, g) = (27, 39)$ which is 244 (see [G-V3]).

When we take the subcode $\mathscr{D} = \langle c_{f_1}, c_{f_2}, c_{f_3}, c_{f_4} \rangle$ we add the word corresponding to $f_4 = X_1$ to the basis of the former subcode. Note that the associated curve C_{f_4} given by $y^p - y = x$ has genus zero. Following the above procedure we find:

(3.5) PROPOSITION. *The curve $C_{\mathscr{D}}$ defined over $\mathbb{F}_{p^3}$ which corresponds to the subcode $\mathscr{D} = \langle c_{f_1}, c_{f_2}, c_{f_3}, c_{f_4} \rangle$ has genus $(p^4 - p)\, p/2$ and $\# C_{\mathscr{D}}(\mathbb{F}_{p^3}) = p^6 + 1$.*

(3.6) COROLLARY. *For $p = 3$ the curve $C_{\mathscr{D}}$ over $\mathbb{F}_{27}$ has genus 117 and $\# C_{\mathscr{D}}(\mathbb{F}_{27}) = 730$.*

This is fairly good compared to Oesterlé's upper bound which is 859 for curves of genus 117 over $\mathbb{F}_{27}$.

The next example shows that we can also use subcodes which are not of minimum weight to construct curves with many points. This is caused by the fact that the possibility of genus reduction is a very useful feature.

4. THE CODE $R_3(3, 3)$

Here we exploit the code $R_3(3, 3)$ to produce a good curve over $\mathbb{F}_{27}$. In this case the first three elements $\sigma \in Q^3$ with $\deg(\sigma) \geqslant 3$ are $(0, 1, 2)$, $(0, 2, 1)$, and $(0, 2, 2)$ with corresponding $f_1 = (X_1 - 1)\, X_1 X_2$, $f_2 = (X_1 - 1)\, X_1 X_3$, and $f_3 = (X_1 - 1)\, X_1$. We can write f_1 as

$$f_1 = (\mathrm{Tr}(x) - 1)\, \mathrm{Tr}(x)\, \mathrm{Tr}(ax) \qquad \text{with } \mathbb{F}_3\text{-independent } \{1, a\} \subset \mathbb{F}_{27}$$

and we find for the codeword

$$c_{f_1} = \mathrm{Tr}[\, 2a^9 x^{13} + (2a^3 + a)\, x^7 + (a^3 + 2a)\, x^5 - (a^3 + a)\, x^4 + ax^3 - ax^2].$$

The word c_{f_1} has 21 zeros and the related curve has genus 12, but if we could eliminate $2a^9 x^{13}$ we get a curve of genus 6 since $2a^3 + a \neq 0$. As $x^{13} \in \mathbb{F}_3$ for $x \in \mathbb{F}_{27}$ we can neglect $2a^9 x^{13}$ if we require $\mathrm{Tr}_{27/3}(a) = 0$. Unfortunately there is no $\mathbb{F}_3$-independent subspace $\langle 1, a, b \rangle$ in $\mathbb{F}_{27}$ with $\mathrm{Tr}(a) = \mathrm{Tr}(b) = 0$. However, when we take the fibre product of the curves induced by f_1 and f_3 we find:

(4.1) PROPOSITION. *For $a \in \mathbb{F}_{27} - \mathbb{F}_3$ with $\mathrm{Tr}(a) = 0$ the fibre product of the curves C_{f_1} and C_{f_3} has genus $g = 21$ and possesses 163 points over $\mathbb{F}_{27}$.*

Proof. The curve C_{f_1} is given by

$$y^3 - y = (2a^3 + a)\, x^7 + (a^3 + 2a)\, x^5 - (a^3 + a)\, x^4 + ax^3 - ax^2,$$

while C_{f_2} is defined by

$$y^3 - y = 2x^4 + x^2 - x.$$

The words in the subcode generated by c_{f_1} and c_{f_3} are

$$\lambda_1 c_{f_1} + \lambda_2 c_{f_3} = (X_1 - 1)\, X_1 (\lambda_1 X_2 + \lambda_2)$$

with $\lambda_1, \lambda_2 \in \mathbb{F}_3$. For $\lambda_1 \neq 0$ we have 21 zeros or weight 6 and for $\lambda_1 = 0$ the corresponding word has weight 9. It follows from (1) that

$$w(\mathscr{D} = \langle c_{f_1}, c_{f_3} \rangle) = (6 \cdot 6 + 2 \cdot 9)/6 = 9.$$

Then Proposition (2.1) implies $\# C_{\mathscr{D}}(\mathbb{F}_{27}) = 163$. The curves which occur in the fibre product are of the form

$$\begin{aligned} y^3 - y = {} & \lambda_1 (2a^3 + a)\, x^7 + \lambda_1 (a^3 + 2a)\, x^5 + (2\lambda_2 - \lambda_1 (a^3 + a))\, x^4 \\ & + \lambda_1 ax^3 + (\lambda_2 - \lambda_1 a)\, x^2 - \lambda_2 x \end{aligned}$$

with $(\lambda_1, \lambda_2) \in \mathbb{F}_3^2 - \{0\}$. If $\lambda_1 \neq 0$ the genus is 6, while for $\lambda_1 = 0$ the genus is 3 and we deduce from (8) that $g(C_{\mathscr{D}}) = (36+6)/2 = 21$. ∎

The curve from Proposition (4.1) satisfies the conditions of entry to the Tables [G-V3] since Oesterlé's upper bound in this case is 214.

5. CURVES THAT ATTAIN THE HASSE–WEIL UPPER BOUND

In this section we construct maximal curves, i.e., irreducible smooth curves of genus g over $\mathbb{F}_q$ for which the number of $\mathbb{F}_q$-rational points attains the Hasse–Weil upper bound $q+1+2g\sqrt{q}$. This can only happen if the genus is small compared to q, more precisely by [S-X, F-T] we know that for such curves $g \leqslant (\sqrt{q}-1)^2/4$ or $g = (q-\sqrt{q})/2$. The curves we construct here arise from the Reed–Muller codes $R_p(2, m)$ for odd primes p and even number of variables m.

According to the algorithm in Section 1 the polynomials (2) corresponding to the first m elements in Q^m with degree $\geqslant m(p-1)-2$ are

$$f_1 = (X_1 - 1)\, X_1 = (\mathrm{Tr}(x) - 1)\, \mathrm{Tr}(x),$$
$$f_i = X_1 X_i = \mathrm{Tr}(x)\, \mathrm{Tr}(a_i x) \qquad (2 \leqslant i \leqslant m),$$

where the a_i are chosen such that $\{1, a_2, ..., a_m\}$ are $\mathbb{F}_p$-independent elements of $\mathbb{F}_{p^m}$. To these polynomials f_i we can associate Artin–Schreier curves. For f_1 we find

$$C_{f_1}\colon\ y^p - y = x^{p^{m/2}+1} + 2\left(\sum_{j=1}^{(m/2)-1} x^{p^j+1}\right) + x^2 - x,$$

a curve with genus $g(C_{f_1}) = p^{m/2}(p-1)/2$ and $\#C_{f_1}(\mathbb{F}_{p^m}) = 2p^m + 1$. The elements f_i with $2 \leqslant i \leqslant m$ define curves

$$C_{f_i}\colon\ y^p - y = a_i^{p^{m/2}} x^{p^{m/2}+1} + \sum_{j=1}^{(m/2)-1} (a_i^{p^j} + a_i)\, x^{p^j+1} + a_i x^2. \qquad (11)$$

Now we observe that for all $x \in \mathbb{F}_{p^m}$ we have

$$\mathrm{Tr}_{p^m/p}(a_i^{p^{m/2}} x^{p^{m/2}+1}) = \mathrm{Tr}_{p^{m/2}/p}(a_i^{p^{m/2}} + a_i)\, x^{p^{m/2}+1},$$

so that if $a_i^{p^{m/2}} + a_i = \mathrm{Tr}_{p^m/p^{(m/2)}}(a_i) = 0$ the curve in (11) has the same number of points as the Artin–Schreier curve with the term $a_i^{p^{m/2}} x^{p^{m/2}+1}$ deleted. In this way we can reduce the genus without changing the number of points.

(5.1) PROPOSITION. *For $q = p^m$ with p odd, m even, and $1 \leqslant r \leqslant m/2$ there exists a maximal curve C over $\mathbb{F}_q$ with*

$$g(C) = p^{(m/2)-1}(p^r - 1)/2 \qquad \text{and} \qquad \#C(\mathbb{F}_q) = p^m + 1 + (p^r - 1)\, p^{m-1}.$$

Proof. Using the observation just made we consider the subspace L of elements $a_i \in \mathbb{F}_{p^m}$ with $\mathrm{Tr}_{p^m/p^{(m/2)}}(a_i) = 0$. This is a subspace of dimension $m/2$ not containing 1. Now we take a basis $\{a_2, a_3, ..., a_{(m/2)+1}\}$ of L and we consider the r-dimensional subcode $\mathscr{D} = \langle c_{f_2}, ..., c_{f_{r+1}} \rangle$ of $R_p(2, m)$ with $1 \leqslant r \leqslant m/2$. The curves involved in the fibre product defined by $\mathscr{D}$ are

$$y^p - y = \sum_{j=1}^{(m/2)-1} \left(\sum_{i=2}^{r+1} \lambda_i (a_i^{p^j} + a_i) \right) x^{p^j+1} + \left(\sum_{i=2}^{r+1} \lambda_i a_i \right) x^2 \qquad (12)$$

with $(\lambda_2, ..., \lambda_{r+1}) \in \mathbb{F}_p^r - \{0\}$. Since the elements $a_2, ..., a_{r+1}$ are independent over $\mathbb{F}_p$ and satisfy $a_i^{p^{m/2}} + a_i = 0$ the coefficient of $x^{p^{(m/2)-1}+1}$ in (12) is not zero. This implies that the genus of the curves given by (12) is $(p-1)\, p^{(m/2)-1}/2$. It follows from (8) that

$$g(C_{\mathscr{D}}) = p^{(m/2)-1}(p^r - 1)/2.$$

Furthermore, as the curves (12) are related to $X_1(\lambda_2 X_2 + \cdots + \lambda_{r+1} X_{r+1})$, which has $2p^{m-1} - p^{m-2}$ zeros, we find

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

By formula (7) we obtain $\#C_{\mathscr{D}}(\mathbb{F}_q) = p^m + 1 + (p^r - 1)\, p^{m-1}$.

(5.2) *Remark.* From the proof of Proposition (5.1) we deduce three other families of maximal curves.

- Curves of the form

$$y^p - y = \left(\sum_{j=1}^{(m/2)-1} (a^{p^j} + a)\, x^{p^j+1} \right) + ax^2 \qquad \text{with} \quad \mathrm{Tr}_{p^m/p^{(m/2)}}(a) = 0$$

are maximal curves over $\mathbb{F}_{p^m}$ of genus $p^{(m/2)-1}(p-1)/2$.

- Curves of the form

$$y^p - y = a^{p^{m/2}} x^{p^{(m/2)}+1} \qquad \text{with} \quad \mathrm{Tr}_{p^m/p^{(m/2)}}(a) = 0$$

have $p^{m+1} + 1$ rational points over $\mathbb{F}_{p^m}$ and genus $p^{m/2}(p-1)/2$, so these are maximal too.

- For $1 \leqslant r \leqslant m/2$ an r-dimensional fibre product of curves from the preceding type yields a maximal curve of genus $(p^r - 1)\, p^{m/2}/2$ with $p^{r+m} + 1$ points.

These maximal curves were mentioned in [G-V2].

As was remarked in [L], any quotient C' of a maximal curve C over $\mathbb{F}_q$ which is defined over $\mathbb{F}_q$ (i.e., the map $C \to C'$ is defined over $\mathbb{F}_q$) is automatically maximal. This enables one to obtain new maximal curves from the above ones.

(5.3) PROPOSITION. *For $q = p^m$ with m even and r a divisor of m with $1 \leqslant r \leqslant m/2$ there exists a maximal curve C' over $\mathbb{F}_q$ with*

$$g(C') = (p^{(m/2)-1} - 1)(p^r - 1)/4,$$
$$\#C'(\mathbb{F}_q) = p^m + 1 + (p^{m-1} - p^{m/2})(p^r - 1)/2.$$

Proof. Consider the maximal curve C from Proposition (5.1) which is the fibre product of the Artin–Schreier curves

$$y_i^p - y_i = \sum_{j=1}^{(m/2)-1} (a_i^{p^j} + a_i)\, x^{p^j+1} + a_i x^2 \qquad \text{for} \quad 2 \leqslant i \leqslant r+1.$$

Since each of these admits the involution $(x, y_i) \mapsto (-x, y_i)$ we have an involution on C, the fixed points of which are the p^r points lying over $x = 0$ and the point over $x = \infty$. Applying the Hurwitz–Zeuthen formula

$$2g(C) - 2 = 2(2g(C') - 2) + p^r + 1$$

we find the genus of the quotient curve

$$g(C') = (p^{(m/2)-1} - 1)(p^r - 1)/4.$$

The maximality implies that the number of points is as given. ∎

Maximal curves of the form

$$y^p - y = a^{p^{m/2}} x^{p^{(m/2)}+1} \qquad \text{with} \quad \mathrm{Tr}_{p^m/p^{m/2}}(a) = 0$$

possess an action of the dth roots of unity defined via $(x, y) \mapsto (\zeta x, y)$ provided d divides $p^{m/2} + 1$. The fixed points under these automorphisms are again the points lying over $x = 0$ and the point at infinity. The ramification is tame of order d and this gives:

(5.4) PROPOSITION. *For any positive divisor d of $p^{m/2} + 1$ there exists a maximal curve C' over $\mathbb{F}_{p^m}$ with*

$$g(C') = (p^{m/2} - d + 1)(p - 1)/2d,$$
$$\#C'(\mathbb{F}_{p^m}) = p^m + 1 + (p^m - (d-1)\, p^{m/2})(p-1)/d.$$

If we take a fibre product C as sketched in the third point of Remark (5.2) with r a divisor of m and $1 \leqslant r \leqslant m/2$ we find that C is given by an equation

$$y^{p^r} - y = F(x^{p^{(m/2)}+1}) \qquad \text{with} \quad F(t) \in \mathbb{F}_{p^m}[t].$$

The dth roots of unity act as remarked above by which we obtain the following result.

(5.5) PROPOSITION. *For any positive divisor d of $p^{m/2}+1$ and a divisor r of m with $1 \leqslant r \leqslant m/2$ there exists a maximal curve C' over $\mathbb{F}_{p^m}$ with*

$$g(C') = (p^{m/2} - d + 1)(p^r - 1)/2d,$$
$$\#C'(\mathbb{F}_{p^m}) = p^m + 1 + (p^m - (d-1)\, p^{m/2})(p^r - 1)/d.$$

REFERENCES

[F-T] R. Fuhrmann and F. Torres, The genus of curves over finite fields with many rational points, *Manuscripta Math.* **89** (1996), 103–106.

[G-V1] G. van der Geer and M. van der Vlugt, Fibre products of Artin–Schreier curves and generalized Hamming weights of codes, *J. Combin. Theory Ser. A* **70** (1995), 337–348.

[G-V2] G. van der Geer and M. van der Vlugt, How to construct curves over finite fields with many points, *in* "Arithmetic Geometry, Cortona, 1994" (F. Catanese, Ed.), pp. 169–189, Cambridge Univ. Press, Cambridge, 1997.

[G-V3] G. van der Geer and M. van der Vlugt, Tables for the function $N_q(g)$, version August 1997, regularly updated tables available at http://www.wins.uva.nl/ ~ geer.

[H-P] P. Heijnen and R. Pellikaan, Generalized Hamming weights of q-ary Reed–Muller codes, *IEEE Trans. Inform. Theory* **44** (1998), 181–196.

[L] G. Lachaud, Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, *C. R. Acad. Sci. Paris Sér. I* **305** (1987), 729–732.

[S-X] H. Stichtenoth and C. Xing, The genus of maximal function fields, *Manuscripta Math.* **86** (1995), 217–224.

[W] V. K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory* **37** (1991), 1412–1418.

[Wo] J. Wolfmann, New bounds for cyclic codes from algebraic curves, *in* "Coding Theory and Applications" (G. Cohen and J. Wolfmann, Eds.), Lecture Notes in Computer Science, Vol. 388, pp. 47–62, Springer-Verlag, Berlin, 1989.