COMPOSITIO MATHEMATICA

GERARD VAN DER GEER
MARCEL VAN DER VLUGT

Reed-Muller codes and supersingular curves. I

Compositio Mathematica, tome 84, n° 3 (1992), p. 333-367
<http://www.numdam.org/item?id=CM_1992__84_3_333_0>

Compositio Mathematica **84**: 333–367, 1992.

Reed-Muller codes and supersingular curves. I

GERARD VAN DER GEER[1] and MARCEL VAN DER VLUGT[2]

[1]*Faculteit Wiskunde en Informatica, Universiteit van Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands and* [2]*Mathematisch Instituut, Rijksuniversiteit Leiden, Niels Bohrweg 1, 2300 RA Leiden, The Netherlands*

Received 13 May 1991; accepted 12 February 1992

1. Introduction

In this paper we study certain supersingular curves. The motivation for this comes from the theory of codes. Binary Reed-Muller codes $R(r, m)$ are one of the oldest types of codes. The words of this code $R(r, m)$ are obtained by evaluating polynomials over $\mathbb{F}_2$ in m variables whose total degree is $\leqslant r$ at the points of $(\mathbb{F}_2)^m$. In case that $r = 2$ we obtain polynomial functions of degree 2 on $(\mathbb{F}_2)^m$ by viewing the finite field $\mathbb{F}_q$ with $q = 2^m$ as a vector space over $\mathbb{F}_2$ and by considering quadratic forms $\mathrm{Tr}[xR(x)]$, where R is a so-called linearized polynomial over $\mathbb{F}_q$, i.e. one in which only powers of 2 occur as exponents. The code words then are intimately related to the curves $y^2 + y = xR(x)$; for example the weight of such a word is determined by the number of points on this curve. This leads us to the study of these curves and it turns out that they have intriguing properties. For example, their automorphism groups over an algebraic closure contain extra-special 2-groups and are very large. Moreover, our curves are supersingular in the sense that their jacobians are isogenous to products of supersingular elliptic curves (over an algebraic closure). We thus find a beautiful family of supersingular curves.

We study in detail the automorphism groups of these curves and derive consequences for the number of points on them and thus for the weights of our code words. We have also been able to determine the number of curves in families with a fixed number of rational points. In this way we can obtain in a simple manner the weight distribution of certain subcodes of the second order Reed-Muller codes, thus avoiding the tedious computations as in Berlekamp [Be]. Moreover, this can be generalized to characteristic > 2. As a corollary we find curves over $\mathbb{F}_q$ with the maximal and minimal number of points possible for any genus g equal to a power of 2 and $g \leqslant 2^{[m/2]-1}$.

The geometry of our curves over the given field $\mathbb{F}_q$ is determined to a large extent by the kernel (or radical) of the symplectic form $\mathrm{Tr}[xR(y) + yR(x)]$ and another (non-degenerate) symplectic form on this kernel. We use these forms to study the automorphism group and the decomposition of the jacobian.

The curves considered here have other applications too: curves of this type were used by Shioda and Elkies to construct lattices ("Mordell-Weil lattices") which are denser than the lattices known so far.

The organization of this paper is as follows. After giving the link between Reed-Muller codes and our curves in Section 2 we study the equation for the radical of the associated symplectic form in Section 3. In the next two sections we determine the automorphism groups of our curves and use this to get the number of rational points. Then in Section 6 we study how this number varies in families with fixed kernel and in Section 7 how the dimension of the kernel varies in general. These results are illustrated by the example of elliptic curves in Section 8. The next two sections deal with the decomposition of the jacobian both over $\bar{\mathbb{F}}_q$ and over $\mathbb{F}_q$. In Section 11 we determine the representation of the extra- special 2-groups of automorphisms on the first cohomology and in Section 12 we determine the so-called a-number of the jacobians. We conclude in Section 13 with a summary of analogs for characteristic >2.

In Part II we shall treat, among other things, questions of moduli, the behaviour of the automorphism group in families, linear relations between the frequencies of the weights and the case of characteristic $p > 2$, and we shall give more applications to coding theory.

It is our pleasure to thank N. Elkies, F. Oort and D. Zagier for their comments on an earlier version of this paper.

2. Reed-Muller codes and curves

We recall some elementary notions from coding theory. We refer to [MacW-Sl] for extensive explanations. Fix a finite field $\mathbb{F}_q$. A *linear code* C over $\mathbb{F}_q$ of length $n \in \mathbb{Z}_{>0}$ is a linear subspace of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$. An element of C is called a *word*. The *weight* $w(x)$ of $x \in C$ is defined by

$$w(x) = \#\{i : x_i \neq 0\}.$$

The *weight distribution* of a code C is the collection of non-negative integers

$$A_i = \#\{c \in C : w(c) = i\} \quad \text{for } 0 \leqslant i \leqslant n.$$

A linear code is *cyclic* if with every word $c = (a_1, \ldots, a_n) \in C$ also the word $(a_n, a_1, \ldots, a_{n-1})$ belongs to C.

We recall the definition of the *binary Reed-Muller code* $R(r, m)$ for natural numbers r and m. Let P_r be the $\mathbb{F}_2$-vector space

$$P_r = \{f \in \mathbb{F}_2[X_1, \ldots, X_m] : \text{total degree of } f \leqslant r\}.$$

Then the rth order binary Reed-Muller code $R(r,m)$ of length $n=2^m$ is obtained by evaluating the elements of P_r at the points of $(\mathbb{F}_2)^m$: it is the image of the linear map

$$\beta: P_r \to (\mathbb{F}_2)^n \quad \text{with } \beta(f) = (f(v))_{v\in(\mathbb{F}_2)^m}.$$

By deleting the component of each vector corresponding to $0\in(\mathbb{F}_2)^m$ we get a cyclic code of length 2^m-1, denoted by $R^*(r,m)$. Note that this construction works as well with 2 replaced by an arbitrary prime power q.

If we take $r=2$ and set $q=2^m$ then we can construct elements of P_2 by considering the $\mathbb{F}_2$-valued function $Q(x)$ on $\mathbb{F}_q$, considered as an m-dimensional $\mathbb{F}_2$-vector space, defined by

$$Q(x) = \mathrm{Tr}[xR(x)],$$

where Tr is the trace map from $\mathbb{F}_q$ to $\mathbb{F}_2$ and R is a so-called (2-)*linearized polynomial*

$$R = \sum_{i=0}^{h} a_i x^{2^i} \in \mathbb{F}_q[x].$$

Indeed,

$$Q(x+y)-Q(x)-Q(y) = \mathrm{Tr}[xR(y)+yR(x)]$$

is a symmetric bilinear form, hence $Q(x)$ is a quadratic form.

We set

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

and thus find that

$$C_h = \{(\mathrm{Tr}[xR(x)])_{x\in\mathbb{F}_q} : R\in R_h\}$$

is a subcode of $R(2,m)$. The punctured code

$$D_h = \{(\mathrm{Tr}[xR(x)])_{x\in\mathbb{F}_q^*} : R\in R_h\}$$

is a subcode of $R(2,m)^*$.

Consider the cyclic code C of length $q-1$ over $\mathbb{F}_q$ with generator polynomial $\Pi_{i=0}^{h}(X-\alpha^{2^i+1})$, where α generates $\mathbb{F}_q^*$. The dual $C^\perp$ of this code is cyclic with zeros

$$\{\alpha^s: 1 \leqslant s \leqslant 2^m-1,\ s \neq 2^m-1-(2^i+1) \quad \text{for } 0 \leqslant i \leqslant h\}.$$

By substituting one verifies that these are precisely the common zeros in $\mathbb{F}_q$ of the polynomials

$$\sum_{t=0}^{q-2} \alpha^t R(\alpha^t) X^t \in \mathbb{F}_q[X]/(X^{q-1}-1) \quad (R \in R_h)$$

and this means that $C^\perp = \{[xR(x)]_{x \in F_q^*}: R \in R_h\}$. Delsarte's theorem asserts that the dual of a restriction code is the trace of the dual code (cf. [MacW-S], p. 208):

$$(C|_{\mathbb{F}_2})^\perp = \mathrm{Tr}(C^\perp).$$

Hence our code $D_h = \mathrm{Tr}(C^\perp)$ is the dual of the binary cyclic code $C|\mathbb{F}_2$ with zeros $\{\alpha^{2^i+1}: 0 \leqslant i \leqslant h\}$. From this we conclude

$$\dim D_h = \begin{cases} m(h+1) & \text{for } h < \left[\frac{m}{2}\right], \\ \binom{m+1}{2} & \text{for } h = \left[\frac{m}{2}\right]. \end{cases}$$

For $h = 0, 1, 2$ the codes D_h are the duals of the 1-, 2-, 3-error correcting BCH codes.

Consider now a word $w_R = (\mathrm{Tr}[xR(x)])_{x \in \mathbb{F}_q}$ in C_h. Using the basic fact that an element of $\mathbb{F}_q$ has trace zero if and only if it is of the form y^2+y for some $y \in \mathbb{F}_q$ we see that the weight of w_R is given by

$$\#\{x \in \mathbb{F}_q: \mathrm{Tr}[xR(x)] \neq 0\}$$
$$q - \tfrac{1}{2}[\text{number of rational points on the affine curve } y^2+y = xR(x)].$$

So the weight distribution of the codes C_h (and D_h) is closely connected to the family of (affine) curves defined by the equations

$$y^2 + y = xR(x)$$

with R running through R_h. We are thus naturally led to study these curves.

3. The kernel equation of a symplectic form on $\mathbb{F}_q$

In this section we study the symplectic form associated to the quadratic form $Q(x)=\mathrm{Tr}[xR(x)]$ introduced in Section 2. View $\mathbb{F}_q$ for $q=2^m$ as an $\mathbb{F}_2$-vector space E of dimension m. Let S be the vector space of symplectic forms on E. We consider the vector space R_h of linearized polynomials introduced in the preceding section. We shall assume that $1 \leqslant h \leqslant [\frac{m}{2}]$. If $R \in R_h$ then the zeros of R form an $\mathbb{F}_2$-vector space. To an element $R \in R_h$ we associate a symplectic form on $E=\mathbb{F}_q$:

$$F_R(x, y) = \mathrm{Tr}[xR(y) + yR(x)].$$

The radical (or kernel) of the symplectic space $(\mathbb{F}_q, F_R)$ is defined by

$$W_R = \{x \in \mathbb{F}_q : F_R(x, y) = 0 \text{ for all } y \in \mathbb{F}_q\}.$$

This is an $\mathbb{F}_2$-subspace of $\mathbb{F}_q$ and if F_R is not identically zero then

$$m - \dim W_R \equiv 0 \pmod 2$$

since the rank of a non-zero symplectic form is even.

(3.1) PROPOSITION. *If* $R = \Sigma_{i=0}^{h} a_i x^{2^i} \in R_h$ *with* $a_h \neq 0$, *then*

$$W_R = \{x \in \mathbb{F}_q : E_{h,R}(x) = 0\},$$

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

Proof. As Tr is invariant under the Frobenius automorphism we have

$$\mathrm{Tr}[xR(y) + yR(x)] = \mathrm{Tr}\left[y \left\{ \sum_{i=0}^{h} (a_i x)^{2^{-i}} + R(x) \right\} \right].$$

Then $x \in W_R$ if and only if

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

which is equivalent to

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

and our proposition follows. □

This proposition implies in particular

$$0 \leqslant \dim(W_R) \leqslant 2h \quad \text{for } R \in R_h \text{ with } a_h \neq 0.$$

Note that $E_{h,R}(X)$ is also a linearized polynomial, independent of the coefficient a_0 of R. Furthermore we have

$$E_{h,R_1+R_2} = E_{h,R_1} + E_{h,R_2}.$$

We shall denote this polynomial $E_{h,R}$ simply by E_h and we shall call the equation $E_h = 0$ the *kernel equation* for (the symplectic form associated to) R.

We can describe W_R in an alternative way as follows.

(3.2) PROPOSITION. *Let $c \in \mathbb{F}_q$. Then $c \in W_R$ if and only if there exists a polynomial B in $X\mathbb{F}_q[X]$ such that*

$$B^2 + B = cR(X) + XR(c). \tag{1}$$

Proof. The if-part is obvious. By equating coefficients we see that we always can find a linearized polynomial $B \in X\mathbb{F}_q[X]$ and a scalar $d \in \mathbb{F}_q$ such that $B^2 + B = cR(X) + XR(c) + dX$ (cf. Remark (3.3) hereafter). Suppose that $c \in W_R$. Then $\mathrm{Tr}(dx)$ is zero on $\mathbb{F}_q$ and this implies $d = 0$. □

(3.3) REMARK. By equating the coefficients we find that a solution $B \in X\mathbb{F}_q[X]$ of (1) is a linearized polynomial $\Sigma_{i=0}^{h-1} b_{i+1} X^{2^i}$ whose coefficients satisfy the relations

$$\begin{aligned} b_1 &= ca_0 + R(c), \\ b_j + b_{j-1}^2 &= ca_{j-1} \quad \text{for } j = 2, \ldots, h, \\ b_h^2 &= ca_h. \end{aligned} \tag{2}$$

The compatibility of this system comes down to $E_h(c) = 0$.

Now back to the kernel equation $E_h = 0$. We want to factor the polynomial E_h. The idea is that if $c \neq 0$ is a zero of E_h and if B is the corresponding solution of (1) then because of $B(c)^2 + B(c) = cR(c) + cR(c) = 0$ we have $B(c) = 0$ or 1. Note that the polynomial B depends on c. We can thus split the polynomial E_h in a factor X, a factor $\Pi_{c \in \bar{W}_R, c \neq 0, B(c)=0}(X - c)$ and a factor $\Pi_{c \in \bar{W}_R, c \neq 0, B(c)=1}(X - c)$, where $\bar{W}_R = \{c \in \bar{\mathbb{F}}_q : E_h(c) = 0\}$. To make this explicit we introduce the auxiliary polynomials

$$F_j = \sum_{i=0}^{j-1} (a_j)^{2^i} X^{(2^j+1)(2^i-1)} \quad \text{for } j \geqslant 1.$$

(3.4) THEOREM. *Let* $R = \Sigma_{i=0}^{h} a_i X^{2^i} \in \mathbb{F}_q[X]$ *with* $a_h \neq 0$. *Then there is a factorization* $E_h = XE_h^- E_h^+$, *where*

$$E_h^- = \sum_{j=1}^{h} X^{2^{h-j}-1} F_j^{2^{h-j}} \in \mathbb{F}_q[X]$$

has degree $2^{2h-1} - 2^{h-1} - 1$ *and leading coefficient* $a_h^{2^{h-1}}$ *and*

$$E_h^+ = 1 + X^{2^h} \sum_{j=1}^{h} X^{2^{h-j}} F_j^{2^{h-j}} \in \mathbb{F}_q[X]$$

has degree $2^{2h-1} + 2^{h-1}$ *and leading coefficient* $a_h^{2^{h-1}}$.

Proof. Let $c \neq 0$ be a zero of E_h and let B be the corresponding solution of (1). From $B(c)^2 + B(c) = cR(c) + cR(c) = 0$ we see $B(c) = 0$ or $B(c) = 1$. If $B(c) = 0$ (resp. $= 1$) then c satisfies an equation

$$(b_1 c + b_2 c^2 + b_3 c^4 + \cdots + b_h c^{2^{h-1}})^{2^h} = 0 \quad \text{(resp.} = 1). \tag{3}$$

From the equations (2) we derive

$$b_i^{2^h} = \sum_{j=i}^{h} (ca_j)^{2^{h+i-j-1}} \quad \text{for } 1 \leqslant i \leqslant h.$$

Substituting this in (3) we find

$$\sum_{i=1}^{h} \left(\sum_{j=i}^{h} (ca_j)^{2^{h-j+i-1}} \right) c^{2^{h+i-1}} = 0 \quad \text{(resp.} = 1).$$

After reordering we find

$$\sum_{j=1}^{h} \left(\sum_{i=0}^{j-1} (ca_j)^{2^{h-j+i}} \right) c^{2^{h+i}} = \sum_{j=1}^{h} c^{2^h + 2^{h-j}} (F_j(c))^{2^{h-j}} = 0 \quad \text{(resp.} = 1).$$

In case $B(c) = 0$ we divide by c^{2^h+1} and obtain a polynomial equation of degree $2^{h-1}(2^h - 1) - 1$ in c:

$$\sum_{j=1}^{h} c^{2^{h-j}-1} (F_j(c))^{2^{h-j}} = 0.$$

If $B(c) = 1$ the equation

$$\sum_{j=1}^{h} c^{2^h + 2^{h-j}} (F_j(c))^{2^{h-j}} = 1$$

has degree $2^{h-1}(2^h+1)$. By replacing c by X we obtain the polynomials $E_h^{\pm}$.

A simple counting argument shows that $E_h^{\pm}$ divide E_h and that $E_h = XE_h^- E_h^+$. □

This theorem yields us polynomials $E_h^{\pm}$ or more precisely $E_{h,R}^{\pm}$. We shall always suppress the reference to R. Even if $a_h=0$ these expressions (in $a_1, \ldots, a_h, X$) make sense and we use them to define polynomials $E_h^{\pm}$ also for $R \in R_h$ with $a_h=0$. In order to compute E_h^- and E_h^+ we note that the expressions for $E_h^{\pm}$ in Theorem (3.4) imply

$$E_h^+ = 1 + X^{2^{h+1}} E_h^-$$

and

$$E_h^- = F_h + X(E_{h-1}^-)^2.$$

Here E_{h-1} corresponds to $R - a_h X^{2^h}$, though a_{h-1} may be zero. Moreover, we have

$$E_h = (a_h)^{2^h} X^{2^{2h}} + E_{h-1}^2 + a_h X.$$

(3.5) EXAMPLES. For $h=1, 2, 3$ *the polynomials* E_h, E_h^-, E_h^+ are as follows.

$$E_1 = a_1^2 X^4 + a_1 X, \qquad E_1^- = a_1, \qquad E_1^+ = a_1 X^3 + 1,$$

$$E_2 = a_2^4 X^{16} + a_1^4 X^8 + a_1^2 X^2 + a_2 X, \qquad E_2^- = a_2^2 X^5 + a_1^2 X + a_2,$$

$$E_2^+ = a_2^2 X^{10} + a_1^2 X^6 + a_2 X^5 + 1,$$

$$E_3 = a_3^8 X^{64} + a_2^8 X^{32} + a_1^8 X^{16} + a_1^4 X^4 + a_2^2 X^2 + a_3 X,$$

$$E_3^- = a_3^4 X^{27} + a_2^4 X^{11} + a_3^2 X^9 + a_1^4 X^3 + a_2^2 X + a_3,$$

$$E_3^+ = a_3^4 X^{36} + a_2^4 X^{20} + a_3^2 X^{18} + a_1^4 X^{12} + a_2^2 X^{10} + a_3 X^9 + 1.$$

(3.6) PROPOSITION. *Let* $\bar{\mathbb{F}}_q$ *be an algebraic closure of* $\mathbb{F}_q$. *The polynomials* E_h^- *and* E_h^+ *are irreducible over the purely transcendental function field* $\bar{\mathbb{F}}_q(a_1, \ldots, a_h)$.

Proof. We treat the case of E_h^-. Consider it as a polynomial in a_1. Then it is of the form

$$X^{2^{h-1}-1} a_1^{2^{h-1}} + P$$

with $P \in \mathbb{F}_q[a_2, \ldots, a_h, X]$. This is obviously irreducible as a polynomial in a_1, since either $P=0$ for $h=1$ or $(P/X^{2^{h-1}-1})$ is not a square in $\bar{\mathbb{F}}_q(a_2, \ldots, a_h, X)$.

From this we easily conclude that E_h^- is irreducible over $\bar{\mathbb{F}}_q(a_1, \ldots, a_h)$. A similar argument works for E_h^+. □

Finally we return to our $\mathbb{F}_2$-linear map defined in the beginning of this section:

$$\Phi: R_h \to S$$

given by

$$R \to F_R = \mathrm{Tr}[XR(Y) + YR(X)].$$

(3.7) PROPOSITION. *The kernel of the map* Φ *is*

$$\{a_0 X : a_0 \in \mathbb{F}_q\} \quad \text{for } h < \frac{m}{2}$$

and

$$\{a_h X^{2^h} + a_0 X : a_h \in \mathbb{F}_{\sqrt{q}}, a_0 \in \mathbb{F}_q\} \quad \text{for } m \text{ even and } h = \frac{m}{2}.$$

Proof. Suppose $R = \Sigma_{i=0}^h a_i X^{2^i}$ with $\Phi(R) = 0$. Then the kernel equation is a multiple of $X^q - X = 0$. For $h < \frac{m}{2}$ this implies that $E_h \equiv 0$, so $a_i = 0$ for $i \geqslant 1$. For $h = \frac{m}{2}$ we get $E_h = a_h^{2^h} X^q + a_h^{2^h} X$, hence $a_h^{2^h} = a_h$ and $a_i = 0$ for $1 \leqslant i \leqslant h-1$. This proves our proposition. □

Note that $\dim(S) = \binom{m}{2}$ and $\dim(R_h) = m(h+1)$. Hence $\Phi: R_{[m/2]} \to S$ is surjective.

Let us call the number $2h$ *the virtual corank* of the symplectic form $\Phi(R)$ (for $2h < m$). We can use the virtual corank to define a stratification on the space of symplectic forms. This stratification is rougher than the stratification by the usual corank. The virtual corank remains invariant if we replace our symplectic form $\mathrm{Tr}_q[xR(y) + yR(x)]$ by $\mathrm{Tr}_{q^r}[xR(y) + yR(x)]$; the usual corank will change in general.

4. The automorphism group of the curve $y^2 + y = xR(x)$

We consider the (non-singular projective) algebraic curve $C = C_R$ over $\mathbb{F}_q$ with $q = 2^m$ defined by the affine equation $y^2 + y = xR(x)$ for $R = \Sigma_{i=0}^h a_i x^{2^i} \in \mathbb{F}_q[x]$. By the Hurwitz-Zeuthen formula the genus of C_R with $\deg R = 2^h$ equals 2^{h-1}. We first determine the automorphism group over an algebraic closure $\bar{\mathbb{F}}_q$.

(4.1) THEOREM. *The subgroup* $\mathrm{Aut}^0(C)$ *of* $\mathrm{Aut}(C)$ *of* $\bar{\mathbb{F}}_q$*-automorphisms of* C

fixing the branch point of the hyperelliptic map $C \to \mathbb{P}^1$ is the semi-direct product of a normal subgroup G which is an extra-special 2-group of order 2^{2h+1} and a cyclic group of order g.c.d. $\{2^i+1 : i \geqslant 1, a_i \neq 0\}$. *This group G is the central product of $h-1$ dihedral groups of order 8 and one quaternion group of order 8 with identified centres. Moreover,* $\mathrm{Aut}^0(C) = \mathrm{Aut}(C)$ *for* $h \geqslant 2$.

Proof. Let G be the subgroup of $\mathrm{Aut}(C)$ generated by the automorphisms of C the form

$$x \to x + c$$

$$y \to y + b_0 + b_1 x + \cdots + b_m x^m = y + b_0 + B$$

with $c \in \bar{\mathbb{F}}_q$, $B \in x\bar{\mathbb{F}}_q[x]$. Comparing coefficients gives

$$B^2 + b_0^2 + B + b_0 = cR(c) + cR(x) + xR(c).$$

This implies

$$B^2 + B = xR(c) + cR(x) \tag{4}$$

$$b_0^2 + b_0 = cR(c). \tag{5}$$

As in Remark (3.3) equation (4) has a solution B in $\bar{\mathbb{F}}_q[x]$ if and only if $E_h(c) = 0$. From (5) it follows that the elements of G correspond $2-1$ to the elements of

$$\bar{W} = \{c \in \bar{\mathbb{F}}_q : E_h(c) = 0\},$$

which is an $\mathbb{F}_2$-vector space of dimension $2h$. The center Z of G consists of the two automorphisms in G with $c = 0$. Namely, if $\phi \in G$ is determined by the pair $(c, b_0 + B_\phi)$ with $c \neq 0$ then ϕ has centralizer

$$Z_\phi = \{\psi \in G \text{ determined by } (d, e_0 + B_\psi) : B_\psi(c) = B_\phi(d)\}.$$

From a simple degree consideration it follows that the equation $B_\psi(c) = B_\phi(d)$ for fixed c, can be satisfied by at most 2^{2h-1} values of d. This implies that the order of Z_ϕ is at most 2^{2h}, so $\phi \notin Z$. Furthermore the quotient group $G/Z \cong \bar{W}$ is elementary abelian. Then by Theorem 13.7 of Ch. III of [Hu] we find that G is an extra-special 2-group, that its center is Z and that the commutator $[,]$ defines a non-degenerate symplectic form on G/Z.

According to [Hu] loc. cit. there are two isomorphism types of extra-special groups of order 2^{2h+1}. They can be distinguished by the number of elements of order two. If G is the central product of h dihedral groups of order 8 with

identified centres then the number of elements of order $\leqslant 2$ equals $2^h(2^h+1)$, while for the other type the number is $2^h(2^h-1)$.

Therefore we now determine the elements of order two in G. The pair (c, b_0+B) with $c \neq 0$ determines an element of order two if and only if

$$y + B(x) + B(x+c) = y$$

i.e. $B(c) = 0$. As we saw in Section 3 this amounts to $E_h^-(c) = 0$ and we know that the degree of E_h^- equals $2^{2h-1}-2^{h-1}-1$. Including $c=0$ we have $2^{2h-1}-2^{h-1}$ values of c, each inducing 2 elements of order $\leqslant 2$ in G. This determines the isomorphism type of our group.

For $h \geqslant 2$ an arbitrary automorphism of C is of the form

$$x \to \alpha x + c_\alpha,\ y \to \delta y + b_{0,\alpha} + B_{\alpha,c_\alpha}$$

since any automorphism commutes with the hyperelliptic involution $y \to y+1$ and thus induces an automorphism of its fixed field $\mathbb{F}_q(x)$. We find $\delta^2 = \delta$, hence $\delta = 1$, and $\alpha^{2^i+1} = 1$ for $i \geqslant 1$ whenever $a_i \neq 0$. We denote the automorphism given above by $\sigma_{\alpha,c_\alpha,b_{0,\alpha}}$.

The map $\sigma_{\alpha,c_\alpha,b_{0,\alpha}} \to \alpha$ is a surjective homomorphism of $\mathrm{Aut}^0(C)$ onto a cyclic group of order g.c.d. $\{2^i+1 : i \geqslant 1, a_i \neq 0\}$ with kernel G. Since the order of G and of $\mathrm{Aut}^0(C)/G$ are coprime the extension $\mathrm{Aut}^0(C)$ splits, cf. [Hu]. This proves our theorem. □

(4.2) REMARKS. (i) Note that the automorphisms of order 4 in G come from the zeros of E_h^+ or in other words correspond to pairs (c, b_0+B) with $B(c)=1$.

(ii) The element c_α satisfies the "affine" equation

$$E_h(z) = (R(z))^{2^h} + \sum_{i=0}^{h} a_i^{2^{h-1}} z^{2^{h-1}} = (1+\alpha)a_0^{2^{h-1}}.$$

The map $\sigma_{1,c_1,b_{0,1}} \to c_1$ induces the identification of the quotient group G/Z with $\bar{W}$.

(iii) Let $c \in \bar{W}$ with $c \neq 0$. According to Proposition (3.2) there is a polynomial $B_c(X)$ associated to c. The centralizer Z_ϕ of $\phi \in G$ corresponding to c has order 2^{2h} and Z_ϕ corresponds to

$$\{d \in \bar{W} : B_d(c) = B_c(d)\}.$$

We call the equation

$$Z_h(c, X) = B_X(c) + B_c(X) = 0$$

the *centralizer equation of c*. It is a linearized polynomial of degree 2^{2h-1} in X. We have a factorization

$$E_h(X) = c^{-2^h} Z_h(c, X)(Z_h(c, X)+1).$$

Finally, using (3.4) and induction one can show the formula

$$Z_h(c, X) = (E_h^-(c)c + E_h^-(X)X)(cX)^{2^{h-1}} + a_2^{2^{h-2}}((cX)(c+X)^3)^{2^{h-2}} + P_h,$$

where $P_h \in \mathbb{F}_q[a_3, \ldots, a_h, c, X]$.

An important observation now is that the commutator defines a non-degenerate symplectic form $S(\bar{g}, \bar{h})$ on G/Z and by Remark (4.2)(ii) then also on $\bar{W}$.

One can define a quadratic form $\tilde{Q}$ on G/Z by sending $\gamma = gZ$ to 0 or 1, depending on whether the element $g^2 \in Z$ is 0 or $\neq 0$ in Z. In our case the element g is determined by (c, b_0) and c determines a polynomial B. We have

$$\tilde{Q}(\gamma) = B(c)$$

and

$$\tilde{Q}(\gamma\eta) = \tilde{Q}(\gamma) + \tilde{Q}(\eta) + S(\gamma, \eta).$$

This quadratic form defines a quadric, again denoted $\tilde{Q}$, in $\bar{W}$. We can define other quadratic forms with the same associated symplectic form S by setting

$$\tilde{Q}_c(x) = \tilde{Q}(x+c) \quad \text{for } x \in \bar{W}.$$

Note that we have: c is a zero of XE_h^- if and only if the quadric $\tilde{Q}_c$ has $2^{h-1}(2^h-1)$ points.

Of course, we also want to know the automorphism group $\mathrm{Aut}_{\mathbb{F}_q}(C)$ over $\mathbb{F}_q$. Note that the subgroup Z is defined over $\mathbb{F}_q$. Hence the automorphism group

$$G(\mathbb{F}_q) = \mathrm{Aut}^0_{\mathbb{F}_q}(C) \cap G$$

is a subgroup of G of order 2^r for some $r \leqslant 2h+1$ which contains Z. If the quadratic form $\tilde{Q}$ is non-degenerate on $G(\mathbb{F}_q)/Z$ then we find an extraspecial 2-group. But $\tilde{Q}$ can be degenerate when restricted to $G(\mathbb{F}_q)/Z$, e.g. if r is even it is degenerate.

From the proof of Theorem (4.1) we derive

(4.3) THEOREM. *Over* $\mathbb{F}_q$ *we have a bijection*

$$G(\mathbb{F}_q) \leftrightarrows \{(c, b_0) \text{ on the affine curve } y^2+y=xR(x): c \in W_R\},$$

where

$$W_R = \{x \in \mathbb{F}_q: \mathrm{Tr}[xR(y)+yR(x)] = 0 \text{ for all } y \in \mathbb{F}_q\}.$$

Moreover,

$$\# \mathrm{Aut}^0_{\mathbb{F}_q}(C)/G(\mathbb{F}_q) = \text{g.c.d. } \{q-1, 2^i+1 : i \geqslant 1,\ a_i \neq 0\}.$$

5. The number of points of the curve $y^2+y=xR(x)$

In this section we express the number of points on our curves in terms of the kernel of the associated symplectic form. In the sequel we shall denote the vector space W_R by W. Furthermore, we define the subspace

$$V = \{x \in W: \mathrm{Tr}[xR(x)] = 0\}$$

of W.

Since $x \to \mathrm{Tr}[xR(x)]$ defines a linear map $W \to \mathbb{F}_2$ we have: either $\mathrm{Tr}[xR(x)]$ is trivial on W or it vanishes on a subspace of dimension equal to $\dim W - 1$, i.e.

$$V = W \quad \text{or} \quad \dim V = \dim W - 1.$$

This demonstrates the following lemma.

(5.1) LEMMA. *We have* $\# G(\mathbb{F}_q) = 2^{\dim W}$ *or* $2^{\dim W+1}$ *depending on whether the map* $W \to \mathbb{F}_2$ *defined by* $x \to \mathrm{Tr}[xR(x)]$ *is surjective or not.*

In case $\dim V = \dim W - 1$ we find the number of points on C defined over $\mathbb{F}_q$.

(5.2) PROPOSITION. *If* $\dim V = \dim W - 1$ *then* $\# C(\mathbb{F}_q) = q+1$.

Proof. Because $V \neq W$ it follows that $\mathrm{Tr}[xR(x)]$ vanishes on half of all elements of W. For $a \in \mathbb{F}_q$ and $w \in W$ we have

$$\mathrm{Tr}[(a+w)R(a+w)] = \mathrm{Tr}[aR(a)] + \mathrm{Tr}[wR(w)]$$

so $\mathrm{Tr}[xR(x)]$ vanishes on half of each coset of W in $\mathbb{F}_q$. Hence, over half of all elements of $\mathbb{F}_q$ there lie two points of C, so over $\mathbb{F}_q$ we find $2 \cdot \frac{q}{2} = q$ points. Together with the point at infinity we find $q+1$ points. □

If $\mathrm{Tr}[xR(x)]$ is identically zero on W then $x \to \mathrm{Tr}[xR(x)]$ defines an $\mathbb{F}_2$-valued map on $\mathbb{F}_q/W$. This map is in general not additive. But we have:

(5.3) PROPOSITION. *If* $\mathrm{Tr}[xR(x)]$ *is identically zero on* W *then*

$$\left[\sum_{x\in\mathbb{F}_q}(-1)^{\mathrm{Tr}[xR(x)]}\right]^2 = q2^w,$$

where $w = \dim W$.

Proof. We have

$$\begin{aligned}
&\left[\sum_x (-1)^{\mathrm{Tr}[xR(x)]}\right]^2 \\
&\quad = \left(\sum_x (-1)^{\mathrm{Tr}[xR(x)]}\right)\left(\sum_y (-1)^{\mathrm{Tr}[yR(y)]}\right) = \sum_{x,y} (-1)^{\mathrm{Tr}[xR(x)+yR(y)]} \\
&\quad = \sum_z \left(\sum_x (-1)^{\mathrm{Tr}[xR(z)+zR(x)]}\right)(-1)^{\mathrm{Tr}[zR(z)]} \quad (\text{with } z = x+y) \\
&\quad = \sum_{z\in W} \left(\sum_x (-1)^{\mathrm{Tr}[xR(z)+zR(x)]}\right)(-1)^{\mathrm{Tr}[zR(z)]} \\
&\qquad + \sum_{z\notin W} \left(\sum_x (-1)^{\mathrm{Tr}[xR(z)+zR(x)]}\right)(-1)^{\mathrm{Tr}[zR(z)]}.
\end{aligned}$$

The contribution of the first term is $2^w q$. Moreover, the contribution of the second term is 0 since for fixed $z \notin W$ the map from $\mathbb{F}_q$ to $\mathbb{F}_2$ defined by $x \to \mathrm{Tr}[xR(z)+zR(x)]$ is a surjective linear map. This proves our proposition. □

(5.4) COROLLARY. *We have either* $\#(C(\mathbb{F}_q)) - 1 = q$ *or* $\#(C(\mathbb{F}_q)) - 1 = q \pm \sqrt{q2^w}$ *with* $w = \dim W$.

The second assertion in this corollary can also be proved by looking at the quadratic form $\mathrm{Tr}[xR(x)]$. Assuming that it vanishes on W we find a non-singular quadric in $\mathbb{F}_q/W$. It therefore has $2^{n-1}(2^n \pm 1)$ points (with $m = 2n+w$). Hence there are

$$2^w 2^{n-1}(2^n \pm 1) = \tfrac{1}{2}(q \pm \sqrt{q2^w})$$

points $x \in \mathbb{F}_q$ with $\mathrm{Tr}[xR(x)] = 0$.

6. One-dimensional families of curves $y^2+y=xR(x)$ with fixed radical

We study the family $\mathscr{F}$ of curves $y^2 + y = x(R' + a_0x)$, where $R' = \Sigma_{i=1}^{h} a_i x^{2^i} \in \mathbb{F}_q[x]$ is a fixed polynomial with $a_h \neq 0$ and where a_0 ranges over $\mathbb{F}_q$. The kernel equation $E_h = 0$ is the same for all curves in our family $\mathscr{F}$. As always, by w we denote the dimension of the $\mathbb{F}_2$-subspace W of zeros of E_h in $\mathbb{F}_q$. Note that $\mathrm{Tr}[xR'(x)]$ is a fixed quadratic form, while the expression $\mathrm{Tr}[a_0x^2] = \mathrm{Tr}[\sqrt{a_0}\,x]$ ranges over $\mathrm{Hom}(\mathbb{F}_q, \mathbb{F}_2)$.

(6.1) PROPOSITION. *Suppose that C is a curve in $\mathscr{F}$. The number of curves in $\mathscr{F}$ which are isomorphic over $\mathbb{F}_q$ to the given curve C equals at least*

$$\frac{\#C(\mathbb{F}_q)-1}{2^{w+1}}.$$

Proof. Apply to C an $\mathbb{F}_q$-transformation

$$x \to x + c,\ y \to y + b_0 + \sum_{i=0}^{h-1} b_{i+1}x^{2^i} = y + b_0 + B,$$

with

$(c, b_0) \in$ affine curve $C^0(\mathbb{F}_q)$,

$b_1 = R'(c)$,

$b_j^2 + b_{j+1} = ca_j$ for $j = 2, 3, \ldots, h-1$,

$b_h^2 = ca_h$.

The image C' of C has the equation

$$y^2 + y = xR'(x) + (a_0 + b_1^2 + b_2 + ca_1)x^2,$$

so C' is completely determined by c. The image curve is equal to the original one if and only if

$$b_1^2 + b_2 = ca_1$$

and this amounts to $E_h(c) = 0$ (see Remark (3.3)) and accordingly our transformation is an $\mathbb{F}_q$-automorphism. For that reason $\mathscr{F}$ contains at least $(\#C(\mathbb{F}_q)-1)/2 \cdot 2^w$ members which are $\mathbb{F}_q$-isomorphic to C. □

We let $t = q + 1 - \#C(\mathbb{F}_q)$, the so-called trace of Frobenius. Then we have:

(6.2) PROPOSITION. *In the family $\mathcal{F}$ the three possible values of the trace of Frobenius $t=0$, $t=+\sqrt{q2^w}$ and $t=-\sqrt{q2^w}$ occur with multiplicities*

$$n_0=\frac{2^w-1}{2^w}q, \qquad n_+=\frac{q-\sqrt{q2^w}}{2^{w+1}}$$

and

$$n_-=\frac{q+\sqrt{q2^w}}{2^{w+1}},$$

respectively.

Proof. Since W is fixed for all curves in $\mathcal{F}$ the indicated values of t follow from Corollary (5.4). Suppose that $\mathrm{Tr}[xR(x)]$ is identically zero on W for some member of $\mathcal{F}$. Then $t\neq 0$ for this curve. The kernel of the map from $\mathbb{F}_q$ onto $\mathrm{Hom}(W,\mathbb{F}_2)$ which associates to $a\in\mathbb{F}_q$ the linear map $L_a(x)=\mathrm{Tr}[ax^2]$ has dimension $m-w$. Hence there are $q/2^w$ elements in $\mathcal{F}$ with $t\neq 0$. So we find

$$n_++n_-=\frac{q}{2^w}, \tag{6}$$

$$n_0=\frac{2^w-1}{2^w}q. \tag{7}$$

From

$$\#\{(a_0,x)\in(\mathbb{F}_q)^2:\mathrm{Tr}[xR'(x)+a_0x^2]=0\}=\binom{q+1}{2} \tag{8}$$

we derive

$$\frac{q}{2}n_0+\frac{q-\sqrt{q2^w}}{2}n_++\frac{q+\sqrt{q2^w}}{2}n_-=\binom{q+1}{2}. \tag{9}$$

As a result of (6), (7) and (9) we find the claimed multiplicities. To finish the proof we have to see that not all members of $\mathcal{F}$ have $t=0$. But $t=0$ for all members contradicts (8). □

Coding theorists may notice that the weight distribution of a coset of the Reed-Muller code $R(1,m)$ in $R(2,m)$ follows at once from this theorem (cf. [MacW-S]).

The equation $y^2+y=xR(x)$ with $R\in R_h$ defines a proper curve C_h over

$\mathrm{Spec}(\mathbb{F}_q[a_0, \ldots, a_{h-1}, a_h, a_h^{-1}])$. It is easy to see that this variety is a rational variety. Using the results above we can easily calculate its number of points over $\mathbb{F}_q$.

(6.3) COROLLARY. *The number of points on the variety C_h over $\mathbb{F}_q$ equals* $q^{h+1}(q-1)$.

7. The variation of the dimension of the radical W_R

In this section we study the behaviour of $w = \dim W_R$ as R ranges over $R_h = \{R = \Sigma_{i=0}^{h} a_i x^{2^i} : a_i \in \mathbb{F}_q\}$. Since W is independent of a_0 we shall assume that $a_0 = 0$. Set $R_h^0 = \{R \in R_h : a_h \neq 0\}$. For $1 \leqslant h \leqslant m/2$ we define

$$N_w^{(h)} = \#\{R \in R_h : a_0 = 0, \dim W_R = w\}$$

and

$$n_w^{(h)} = \#\{R \in R_h^0 : a_0 = 0, \dim W_R = w\}.$$

We have

$$n_w^{(h)} = N_w^{(h)} - N_w^{(h-1)}.$$

For convenience we set

$$N_w^{(0)} = 0.$$

Note that $n_w^{(h)} = 0$ if $w \not\equiv m \pmod 2$.

(7.1) THEOREM. *The numbers $n_w^{(h)}$ satisfy the following linear relations*:

$$\sum n_w^{(h)} = q^{h-1}(q-1), \tag{10_0}$$

$$\sum_w (2^w - 1) n_w^{(h)} = 2(q-1)^2 q^{h-2} \quad \text{for } h \geqslant 2, \tag{10_1}$$

and

$$\sum_w (2^w - 1) n_w^{(1)} = q - 1, \tag{11_1}$$

or more generally, for $0 \leqslant r < h$

$$\sum_{0 \leqslant w \leqslant 2h} \prod_{0 \leqslant s < r} (2^w - 2^{2s}) n_w^{(h)} = 2^r q^{h-r-1}(q-1) \prod_{0 \leqslant s < r} (q - 2^{2s}), \tag{10_r}$$

while for $r = h$ and m even

$$\sum_{0 \leqslant w \leqslant 2h} \prod_{0 \leqslant s < h} (2^w - 2^{2s}) n_w^{(h)} = (2^h - 1) \prod_{0 \leqslant s < h} (q - 2^{2s}). \tag{11_h}$$

These identities determine the $n_w^{(h)}$ uniquely.

For a full discussion and proof of these and other identities we refer to Part II. Here we restrict ourselves to giving a proof of the first few relations. We prove (10_0), (10_1), (11_1), (10_2) and (11_2).

Proof. The equalities are shown by identifying both sides as the cardinality of the same set. Recall that for a fixed R the commutator defines a symplectic form S on $\bar{W} = \bar{W}_R$ and by restriction also on $W = W_R$. The form is non-degenerate on $\bar{W}$, but can be degenerate on W.

We first show (10_0). We have:

$$\sum_w n_w^{(h)} = \sum_{(a_1, \ldots, a_h) \in \mathbb{F}_q^h, a_h \neq 0} 1 = q^{h-1}(q-1) \quad (h \geqslant 1).$$

Next, we show (10_1). Consider the set

$$A = \{(R, c) \in R_h^0 \times \mathbb{F}_q : c \in W_R, c \neq 0\}.$$

Obviously, $\# A = \Sigma_w (2^w - 1) n_w^{(h)}$. On the other hand, A can be viewed as the set of $\mathbb{F}_q$-rational points of the algebraic set given by $E_h = 0$, $a_h X \neq 0$ in $a_1, \ldots, a_h$, X-space:

$$A = \{(a_1, \ldots, a_h, X) \in \mathbb{F}_q^{h+1} : E_h(X) = 0, a_h X \neq 0\}.$$

As we saw in Section 3 the polynomial E_h splits as $X E_h^- E_h^+$ and accordingly the algebraic set A splits into two components given by the equations $X^{2^{h+1}} E_h^-(X) = \delta$ with $\delta \in \{0, 1\}$. Since there is only one term involving a_1 in E_h^- and since it is of the form $X^{2^{h-1}} a_1^{2^{h-1}}$, each choice of $a_2, \ldots, a_h$, X uniquely determines a_1. We thus find $\# A = 2q^{h-2}(q-1)^2$. From a geometric point of view the two equations $X^{2^{h+1}} E_h^-(X) = \delta$ define purely inseparable coverings of $\mathrm{Spec}(\mathbb{F}_q[a_2, \ldots, a_{h-1}, a_h, a_h^{-1}, X, X^{-1}])$. These two coverings thus each possess $(q-1)^2 q^{h-2}$ points. We find

$$\sum_w (2^w - 1) n_w^{(h)} = 2(q-1)^2 q^{h-2}.$$

The proof of (11_1) is analogous to the proof of (10_1) except that $X^3 E_1^- = X^3 a_1 = 0$ does not contribute, while in $X^3 E_1^- = 1$ the choice of X determines a_1. We thus find $\# A = q - 1$ here.

Let now $h>2$. We shall prove (10_2) by showing the identity

$$\sum_{0\leqslant w\leqslant 2h}\prod_{0\leqslant s\leqslant 1}(2^w-2^s)n_w^{(h)}=2^3q^{h-3}(q-1)\prod_{0\leqslant s\leqslant 1}(q-2^s), \tag{$10'_2$}$$

observing that $(10'_2)=(10_2)+2\cdot(10_1)$.

Consider the set

$$B=\{(R,(c_1,c_2))\in R_h^0\times\mathbb{F}_q^2\colon (c_1,c_2)\in W_R^2,\ \dim(\langle c_1,c_2\rangle)=2\}.$$

For every $R\in R_h^0$ the radical W_R contains $(2^w-1)(2^w-2)$ $\mathbb{F}_2$-independent pairs (c_1,c_2) and hence the left-hand side of $(10'_2)$ expresses the cardinality of B.

To get the right-hand side of $(10'_2)$ we observe that B can be viewed as the set of $h+2$-tuples $(a_1,\ldots,a_h,X,Y)\in\mathbb{F}_q^{h+2}$ satisfying

$$E_h(X)=0,\qquad E_h(Y)=0,\qquad a_h\neq 0,$$
$$X\neq 0,\qquad Y\neq 0,\qquad X\neq Y. \tag{*}$$

This latter set consists of 2^3 components corresponding to the equations

$$X^{2^{h+1}}E_h^-(X)=\delta,\qquad Y^{2^{h+1}}E_h^-(Y)=\varepsilon,\qquad Z_h(X,Y)=\eta,$$

where we write $Z_h(X,Y)=B_X(Y)+B_Y(X)$ for the centralizer polynomial introduced in (4.2)(iii) and where $\delta,\varepsilon,\eta\in\{0,1\}$.

Since we can write

$$Z_h(X,Y)=(E_h^-(X)X+E_h^-(Y)Y)(XY)^{2^{h-1}}+a_2^{2^{h-2}}[XY(X+Y)^3]^{2^{h-2}}+P_h,$$

where

$$P_h\in\mathbb{F}_q[a_3,\ldots,a_h,X,Y]$$

each component has $2^3q^{h-3}(q-1)^2(q-2)$ points. This proves $(10'_2)$ and hence (10_2). In geometric terms we use the fact that each of the components is a purely inseparable covering of the affine space

$$\mathrm{Spec}(\mathbb{F}_q[a_3,\ldots,a_{h-1},a_h,a_h^{-1},X,X^{-1},Y,Y^{-1},(X+Y)^{-1}]).$$

For (11_2) we note that if $h=2$ then $P_h=0$ and we find that $\delta=\varepsilon=\eta=0$ leads to $a_2=0$, so we find one component less. Moreover, if $\delta=\varepsilon=\eta=1$ the equation

reads

$$a_2[XY(X+Y)]^3 = X^4 + X^2Y^2 + Y^4,$$

so we must exclude the solutions of $X^4 + X^2Y^2 + Y^4 = 0$. Hence we find here

$$6(q-1)(q-2)+(q-1)(q-4)$$

points satisfying the equations (*). Hence

$$\sum_{0 \leqslant w \leqslant 4} \prod_{0 \leqslant s \leqslant 1} (2^w - 2^s) n_w^{(2)} = (q-1)(7q-16).$$

Combining this with (10_1) for $h = 2$ we obtain (11_2). □

We refer to Part II for an exhaustive discussion and proofs of the remaining identities and similar relations in characteristic $p > 2$.

(7.2) REMARK. One can prove more refined identities like

$$\sum_{R \in R_h^0} (2^\rho - 1)2^w = 2^2 q^{h-2}(q-1)^2 \quad (h \geqslant 3),$$

where $\rho = \dim(\mathrm{rad}(W))$. This formula together with (10_r) with $r = 0, 1, 2$ gives finer information.

Combining the relations from (7.1) with Proposition (6.2) one gets the number of curves in the family $\{C_R : R \in R_h\}$ with a prescribed number of $\mathbb{F}_q$-rational points. Thus this theorem yields a way to derive the weight distribution of subcodes of the second-order Reed-Muller codes without making use of the MacWilliams identities, in contrast with the method of Berlekamp in [Be]. His method does not seem to generalize to characteristic $p > 2$. In Part II we shall discuss these matters in more detail.

(7.3) EXAMPLE. From (10_0) and (10_1) we deduce

$$n_3^{(2)} = (q-1)\left(\frac{q-2}{6}\right) \quad \text{and} \quad n_1^{(2)} = (q-1)\left(\frac{5q+2}{6}\right).$$

From (10_0), (10_1) and (11_2) we deduce

$$n_4^{(2)} = (q-1)\left(\frac{q-4}{60}\right), \qquad n_2^{(2)} = (q-1)\left(\frac{7q-4}{12}\right),$$

$$n_0^{(2)} = (q-1)\left(\frac{6q+6}{15}\right).$$

Combining Proposition (6.2) with these expressions for $n_w^{(2)}$ we easily obtain in a direct way the weight distribution of the dual triple error correcting BCH codes of length $n = q-1$ (cf. [MacW-S], p. 669).

Finally we give another application of Theorem (7.1). From (11_h) we derive immediately

$$N_{2h}^{(h)} = (2^h - 1) \prod_{j=1}^{h} \left(\frac{q - 2^{2j-2}}{2^{2h} - 2^{2j-2}} \right).$$

The formula for $N_{2h}^{(h)}$ reveals that we have found infinite families of *maximal* and *minimal* curves. These are curves of genus g over $\mathbb{F}_q$ with the maximum number and minimum number of points (equal to the Hasse-Weil bound $q+1 \pm 2g\sqrt{q}$), cf. [Se].

(7.4) THEOREM. *Let m be even. The curves $C = C_R$ with $R \in R_h$ such that $w = 2h$ and* $\mathrm{Tr}[xR(x)]$ *is identically zero on W are curves of genus 2^{h-1} with $q+1 \pm 2^h\sqrt{q}$ points over $\mathbb{F}_q$. They are either maximal or minimal curves. For every h there exist maximal and minimal curves.*

Proof. The Hasse-Weil bound for a curve C of genus g is

$$q+1-2g\sqrt{q} \leqslant \#C(\mathbb{F}_q) \leqslant q+1+2g\sqrt{q}.$$

For the curves indicated above either the upper or lower bound is attained. From the formula for $N_{2h}^{(h)}$ and Theorem (6.2) it follows that both signs occur for every $h < m/2$.

For $h = m/2$ we only have maximal curves. However, by replacing for a minimal curve the expression $xR(x)$ by $xR(x)+c$, where $c \in \mathbb{F}_q$ has trace equal to 1, we obtain a minimal curve. □

8. Supersingular elliptic curves

As an easy illustration we consider the family of elliptic curves $\mathscr{E}$ with equations $y^2 + y = xR(x)$, where $R(x) = ax^2 + bx$ with $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, so $h = 1$. By a coordinate change

$$x \to ax + b/a, \qquad y \to a^2 y$$

the equation of such a curve changes into

$$y^2 + a^{-2}y = x^3 + b^2 a^{-4} x.$$

This is a family of supersingular curves. For m odd we have $w = 1$ and for m even we have $w = 0$ or $w = 2$. Theorem (7.1) implies

$$n_1^{(1)} = q - 1 \quad \text{for } m \text{ odd},$$
$$n_2^{(1)} = (q-1)/3 \quad \text{for } m \text{ even}$$

and consequently

$$n_0^{(1)} = 2(q-1)/3 \quad \text{for } m \text{ even}.$$

If we combine these results with Proposition (6.2) we easily derive

(8.1) THEOREM. *In the family of supersingular elliptic curves $\mathscr{E}$ the frequency f of the value t of the trace of Frobenius is as follows*:

if $q = 2^m$ with m odd:

t	0	$-\sqrt{2q}$	$+\sqrt{2q}$
$f/(q-1)$	$q/2$	$(q+\sqrt{2q})/4$	$(q-\sqrt{2q})/4$

if $q = 2^m$ with m even:

t	0	$-\sqrt{q}$	$+\sqrt{q}$	$-2\sqrt{q}$	$+2\sqrt{q}$
$f/(q-1)$	$q/4$	$(q+\sqrt{q})/3$	$(q-\sqrt{q})/3$	$(q+2\sqrt{q})/24$	$(q-2\sqrt{q})/24$.

Note that Theorem (8.1) gives an alternative approach to computing the weight distribution of the dual of the double-error correcting BCH-code of length $q-1$ (cf. [MacW-S]).

Now we shall show that for $q > 4$ every $\mathbb{F}_q$-isomorphism class of supersingular elliptic curves occurs in the family $\mathscr{E}$. Let E be an elliptic curve over $\mathbb{F}_q$. It can be given in Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with discriminant $\Delta \neq 0$ and j-invariant $j = a_1^{12}/\Delta$. If the invariant $j = 0$ then the coordinate change $x \to x + a_2$ gives us the standard form

$$y^2 + a_3y = x^3 + a_4x + a_6,$$

where now $\Delta = a_3^4$. Such a curve has an automorphism group of order 24 over an algebraic closure of $\mathbb{F}_q$, cf. Theorem (4.1). It is well-known that the j-invariant

classifies elliptic curves up to isomorphism over an algebraically closed field. In order to classify elliptic curves over $\mathbb{F}_q$ one needs Galois cohomology. The "twists" of a given elliptic curve E, i.e. the $\mathbb{F}_q$-isomorphism classes of elliptic curves which are $\bar{\mathbb{F}}_q$-isomorphic to a given elliptic curve E over $\mathbb{F}_q$, are in $1-1$-correspondence with the elements of the cohomology set

$$H^1(\mathrm{Gal}(\bar{\mathbb{F}}_q, \mathbb{F}_q), \mathrm{Aut}(E)).$$

Note that the elliptic curves occurring in $\mathscr{E}$ are those which possess a standard form

$$y^2 + a_3 y = x^3 + a_4 x.$$

(8.2) LEMMA. *If $q > 4$ the curve E with $j = 0$ given by $y^2 + a_3 y = x^3 + a_4 x + a_6$ has at least three points over $\mathbb{F}_q$.*

Proof. By dividing the equation by a_3^2 and by applying a simple coordinate change the equation becomes

$$y^2 + y = a_3^{-2}(x^3 + a_4 x + a_6).$$

Note that

$$\#E(\mathbb{F}_q) = 1 + 2 \cdot \#\{x \in \mathbb{F}_q : \mathrm{Tr}(a_3^{-2}(x^3 + a_4 x + a_6)) = 0\}.$$

Suppose that

$$\mathrm{Tr}(a_3^{-2}(x^3 + a_4 x + a_6)) \equiv 1 \text{ on } \mathbb{F}_q.$$

Then

$$q + 1 - 2\sqrt{q} \leqslant \#E(\mathbb{F}_q) = 1,$$

which contradicts the assumption $q > 4$. □

(8.3) PROPOSITION. *Assume that $q > 4$. Any supersingular elliptic curve E over $\mathbb{F}_q$ is isomorphic to a curve from $\mathscr{E}$.*

Proof. Let E be given by $y^2 + a_3 y = x^3 + a_4 x + a_6$. According to Lemma (8.2) this curve possesses a non-zero point (c, b_0). By applying the transformation $x \to x + c$, $y \to b_0 + \sqrt{c}x$ we find an equation $y^2 + a_3 y = x^3 + a_4 x + a_6$ with $a_6 = 0$. □

By a slight modification of the method used in Proposition 6.1 we obtain:

(8.4) REMARK. The number of curves in our family $\mathscr{E}$ which are $\mathbb{F}_q$-isomorphic to a fixed curve C from the family $\mathscr{E}$ equals

$$(q-1)\frac{\#C(\mathbb{F}_q)-1}{\#\mathrm{Aut}^0_{\mathbb{F}_q}(C)},$$

where $\mathrm{Aut}^0_{\mathbb{F}_q}(C)$ is the subgroup of automorphisms fixing the origin.

We could use this to derive the frequencies in Theorem (8.1) in an alternative way.

9. Decomposing the jacobian over the algebraic closure

In this section we shall show that the jacobian of a curve $y^2+y=xR(x)$ with $R\in R_h$ of degree 2^h is isogenous to a product of supersingular elliptic curves over $\bar{\mathbb{F}}_q$. We decompose the jacobian using the non-hyperelliptic involutions in G.

If ϕ is a non-hyperelliptic involution we let

$$C_\phi = C/\phi.$$

We now show that C_ϕ is of the form $y^2+y=xS(x)$ with S a linearized polynomial of degree 2^{h-1}. In fact, we can compute an equation for C_ϕ.

(9.1) PROPOSITION. *Let ϕ be a non-hyperelliptic involution of C_R given by $x\to x+c$, $y\to y+b_0+B$. Then C/ϕ is the curve with equation*

$$v^2+v = c^{-2}uP(u),$$

where $u=x(x+c)$, $v=y+c^{-1}x(b_0c^{-1}x+B)$ and where $P(u)\in\bar{\mathbb{F}}_q[u]$ is a linearized polynomial of degree 2^{h-1}.

Proof. For an involution ϕ we have $B(c)=0$. One checks that u and v are invariant under ϕ. Furthermore, one has

$$v^2+v = y^2+y+c^{-2}x^2B^2+c^{-1}xB+c^{-4}b_0^2x^4+c^{-2}b_0x^2.$$

By (4) and (5) of Section 4 we have

$$\begin{aligned} y^2+y = xR(x) &= c^{-1}x(B^2+B+xR(c)) \\ &= c^{-1}x(B^2+B)+c^{-2}x^2(b_0^2+b_0). \end{aligned}$$

Substitution gives:

$$v^2+v = c^{-2}u(B^2+b_0^2c^{-2}x^2+b_0^2c^{-1}x).$$

The linearized polynomial

$$B^2+b_0^2c^{-2}x^2+b_0^2c^{-1}x$$

has zeros 0 and c, so can be written as a linearized polynomial P in u and our result follows. □

Let ϕ be an involution not in $Z=\langle \iota \rangle$. Then the norm map of the function fields $\mathbb{F}_q(C)\to\mathbb{F}_q(C_\phi)$ induces a morphism $Nm_\phi\colon \mathrm{Jac}(C)\to\mathrm{Jac}(C_\phi)$. On the other hand, if π_ϕ is the canonical morphism $C\to C_\phi$ we have an induced morphism

$$\pi_\phi^*\colon \mathrm{Jac}(C_\phi)\to\mathrm{Jac}(C).$$

In characteristic 2 arguments similar to those used in [Mu1, Section 1] show that π_ϕ^* and Nm_ϕ are each other's transpose. Moreover, $Nm_\phi\cdot\pi_\phi^*$ is multiplication by 2 on $\mathrm{Jac}(C_\phi)$. If ι denotes the hyperelliptic involution we have $Nm_{\phi\iota}\cdot\pi_\phi^*=0$ and $Nm_\phi\cdot\pi_{\phi\iota}^*=0$, as one sees by computing its effect on divisor classes. We thus find an isogeny

$$n=(Nm_\phi,\ Nm_{\phi\iota})\colon \mathrm{Jac}(C)\to\mathrm{Jac}(C_\phi)\times\mathrm{Jac}(C_{\phi\iota}).$$

Its transpose is $\pi^*=(\pi_\phi^*+\pi_{\phi\iota}^*)$. We thus see that

$$\deg(n)=\deg(\pi^*)$$

and

$$(\deg(n))^2=\deg[2]=2^{2h},$$

with [2] denoting multiplication by 2. Since π_ϕ is separable and ramified π_ϕ^* and similarly $\pi_{\phi\iota}^*$ are closed immersions and hence the kernel of π^* is a group scheme H of $\mathrm{Jac}(C_\phi)\times\mathrm{Jac}(C_{\phi\iota})$ which is the graph of an isomorphism

$$\mathrm{Jac}(C_\phi)[2]\to\mathrm{Jac}(C_{\phi\iota})[2]$$

such that H is maximal isotropic for the Weil-pairing, equivalently, that $(\mathrm{Jac}(C_\phi)\times\mathrm{Jac}(C_{\phi\iota}))/H$ has a principal polarization. Here [2] denotes the kernel of multiplication by 2. We summarize.

(9.2) PROPOSITION. *Let ϕ be a non-hyperelliptic involution of C. Then* Jac(C) *is isomorphic to the quotient* $[\mathrm{Jac}(C_\phi) \times \mathrm{Jac}(C_{\phi_1})]/H$, *where H is a subgroup scheme of order $2^{2^{h-1}}$ which is the graph of a symplectic isomorphism* $\mathrm{Jac}(C_\phi)[2] \to \mathrm{Jac}(C_{\phi_1})[2]$.

Let U be a maximal isotropic subspace of $\bar{W} \cong G/Z$ for the non-degenerate symplectic form induced by the commutator. Let $\rho: G \to G/Z$ be the canonical homomorphism. Then $U' = \rho^{-1}(U)$ is an abelian subgroup of G since the symplectic form comes from the commutator. It is a maximal abelian subgroup of order 2^{h+1} and of type $(4, 2, \ldots, 2)$, cf. [Hu, p. 355]. Let A be an abelian subgroup of U' of order 2^{h-1} and exponent 2 such that $A \cap Z = \{e\}$.

(9.3) LEMMA. *The quotient C/A is a supersingular elliptic curve.*

Proof. This is obvious for $h = 1$. We carry out induction on h. Note that for non-trivial $\phi \in A$ the curve C/ϕ is again of type $y^2 + y = uR'(u)$ for some linearized polynomial R' of degree 2^{h-1}. If Z_ϕ is the centralizer of ϕ then $H = Z_\phi/\langle\phi\rangle$ is an extra-special 2-group contained in the automorphism group of C/ϕ. The subgroup A determines an abelian subgroup A' of H and this is a group of order 2^{h-2} and exponent 2. By induction $C/A = (C/\phi)/A'$ is a supersingular elliptic curve. □

For each choice of a group A in $\rho^{-1}(U)$ we find a factor of the jacobian of C. For fixed U we have 2^{h-1} possibilities for A and we thus find 2^{h-1} factors E_A.

(9.4) THEOREM. *Over the algebraic closure $\bar{\mathbb{F}}_q$ the jacobian* Jac(C) *is isogenous to the product of these 2^{h-1} supersingular elliptic curves E_A. In other words, C or* Jac(C) *is geometrically supersingular.*

Proof. We use induction on h. It is true for $h = 1$. By induction we may assume that it is true for the factors $\mathrm{Jac}(C_\phi)$ and $\mathrm{Jac}(C_{\phi_1})$ of (9.2). As observed in the proof of (9.3) A induces A' in $\mathrm{Aut}(C_\phi)$ and $C/A = C_\phi/A'$. Hence the factor $E_{A'}$ of $\mathrm{Jac}(C_\phi)$ can be identified with E_A. □

(9.5) REMARK. If ϕ and ψ are two distinct commuting non-hyperelliptic involutions in Aut(C) then the intersection of $\mathrm{Jac}(C_\phi)$ and $\mathrm{Jac}(C_\psi)$ inside Jac(C) is of dimension 2^{h-3} for $h > 2$ and can up to isogeny be identified with $\mathrm{Jac}(C/\langle\phi, \psi\rangle)$. The elliptic curve E_A is contained in all factors $\mathrm{Jac}(C_\phi)$ with $\phi \in A$.

10. The decomposition of the jacobian over $\mathbb{F}_q$

The decomposition of the jacobian of $y^2 + y = xR(x)$ into isogeny factors over $\mathbb{F}_q$ is much more subtle than over $\bar{\mathbb{F}}_q$. In order to split this jacobian up to isogeny as a product of abelian varieties (or even jacobians) of dimension 2^k it *suffices* to find an abelian subgroup B in $G(\mathbb{F}_q)$ which is of order 2^{h-k} and of exponent 2 and

which contains Z. Indeed, such a subgroup B contains 2^{h-k-1} subgroups B' of order 2^{h-k-1} with $B' \cap Z = \{e\}$. Then C/B' is a curve of genus 2^k and defines a factor of Jac(C). The product of the 2^{h-k-1} factors Jac(C/B') of dimension 2^k constitutes up to isogeny the jacobian Jac(C).

We thus look for the maximal abelian subgroup B of exponent 2 (and containing Z) in $G(\mathbb{F}_q)$. Suppose that $\#B = 2^d$. Then B/Z defines an isotropic subspace U of dimension $d-1$ in G/Z. Recall

$$V = \{x \in W : \mathrm{Tr}[xR(x)] = 0\}.$$

We write

$$V = V_1 \oplus \mathrm{rad}(V),$$

with rad(V) the radical of the symplectic space $(V, S \mid V)$. Since S is non-degenerate on the $2h$-dimensional space $\bar{W}$ we have

$$r(V) \leqslant \mathrm{codim}(V \subset \bar{W})$$

with $r(V) = \dim(\mathrm{rad}(V))$. A maximal isotropic subspace U of V has dimension

$$r(V) + \dim(V_1)/2.$$

We study here the case that W is maximal.

We define for a non-singular projective curve X defined over $\mathbb{F}_q$ the polynomial $P(X/\mathbb{F}_q, T) \in \mathbb{Q}[T]$ by

$$P(X/\mathbb{F}_q, T) = (1-T)(1-qT)Z(X/\mathbb{F}_q, T),$$

with $Z(X/\mathbb{F}_q, T)$ the zeta function of X over $\mathbb{F}_q$. Furthermore, for a jacobian $A = \mathrm{Jac}(X)$ of a curve over $\mathbb{F}_q$ we put $P(A/\mathbb{F}_q, T) = P(X/\mathbb{F}_q, T)$.

(10.1) THEOREM. *Suppose that m is even and that W is maximal (i.e. $\dim(W) = 2h$). Then the jacobian of C splits up to isogeny as a power of a supersingular elliptic curve over $\mathbb{F}_q$ or as a product of a $g/2$th power of a supersingular elliptic curve with trace of Frobenius $+2\sqrt{q}$ and a $g/2$th power of a supersingular elliptic curve with trace of Frobenius $-2\sqrt{q}$.*

Proof. (a) We first prove that the jacobian is isogenous to a product of elliptic curves.

If $V = W$ then we can find an isotropic subspace of dimension h. Lifting it to $G(\mathbb{F}_q)$ we find an abelian subgroup B of order 2^{h+1} and this must be a maximal

abelian subgroup, hence of type $(4, 2, \ldots, 2)$. By the argument above $\mathrm{Jac}(C)$ is isogenous to a product of elliptic curves.

If V is of codimension 1 in W then $\mathrm{rad}(V)$ has dimension 1 and combining a maximal isotropic subspace H of V and $\mathrm{rad}(V)$ we obtain a total isotropic subspace of dimension h contained in V. By the argument above this suffices.

(b) We prove that if $V = W$ all factors are isogenous to each other. We do this by induction. It is trivially true for $h = 1$. Assume that $h \geqslant 2$. Since $\dim(W) \geqslant 4$ we have $\dim(V) \geqslant 4$. So we have at least one non-hyperelliptic involution ϕ. The curves C/ϕ and $C/\phi\iota$ have maximal kernel space. By our induction hypothesis the jacobian of each of them is a power of a supersingular elliptic curve (say E_ϕ (resp. $E_{\phi\iota}$)). But since $\dim(V) \geqslant 4$ there exists another non-hyperelliptic involution ψ different from ϕ and $\phi\iota$. Then $\mathrm{Jac}(C/\psi)$ is up to isogeny a power of an elliptic curve E_ψ and admits non-trivial maps $\mathrm{Jac}(C/\psi) \to \mathrm{Jac}(C/\phi)$ and $\mathrm{Jac}(C/\psi) \to \mathrm{Jac}(C/\phi\iota)$ using the projections on both isogeny factors. Therefore we find a non-trivial morphism of the elliptic curve E_ψ to E_ϕ and to $E_{\phi\iota}$ and this implies that they are all isogenous.

(c) If $V \neq W$ then the trace of Frobenius satisfies $t = 0$. Over $\mathbb{F}_{q^2}$ we have $V = W$ and the jacobian is (up to isogeny) a power of an elliptic curve $E/\mathbb{F}_{q^2}$ with trace of Frobenius $t_E = \pm 2q$. But then the trace of the factors of $\mathrm{Jac}(C)$ over $\mathbb{F}_q$ is zero if $t_E = -2q$ and $\pm 2\sqrt{q}$ if $t_E = +2q$. Hence the factors of $\mathrm{Jac}(C)/\mathbb{F}_q$ are elliptic curves with trace of Frobenius all equal to zero (and then they are isogenous to each other) or equal to $\pm 2\sqrt{q}$ and in the latter case there must be as many factors with a plus sign as with a minus sign since $t = 0$. □

THEOREM (10.2). *Suppose that m is odd and* $\dim(W) = 2h - 1$. *Then the following holds.*

(i) *If $V = W$ the jacobian* $\mathrm{Jac}(C)$ *splits up to isogeny as a* gth *power of a supersingular elliptic curve with* $P = 1 \pm \sqrt{2q}\,T + qT^2$.

(ii) *If $V \neq W$ and $r(V) = 2$ then* $\mathrm{Jac}(C)$ *is up to isogeny the product of the* $g/2$th *power of a supersingular elliptic curve with* $P = 1 + \sqrt{2q}\,T + qT^2$ *and the* $g/2$th *power of a supersingular elliptic curve with* $P = 1 - \sqrt{2q}\,T + qT^2$.

(iii) *If $V \neq W$, $r(V) = 0$ and over $\mathbb{F}_{q^2}$ we have $V = W$, then* $\mathrm{Jac}(C)$ *is isogenous to the* $g/2$th *power of a simple abelian surface with* $P = (1 - qT^2)^2$ *or is isogenous to the* gth *power of a supersingular elliptic curve with* $P = (1 + qT^2)$.

(iv) *If $V \neq W$, $r(V) = 0$ and over $\mathbb{F}_{q^2}$ we have $V \neq W$, then* $\mathrm{Jac}(C)$ *is up to isogeny the product of the* $g/2$th *powers of two elliptic curves E_1 and E_2 with* $P_1 = 1 + \sqrt{2q}\,T + qT^2$ *and* $P_2 = 1 - \sqrt{2q}\,T + qT^2$.

Proof. (i) A maximal isotropic subspace lifts to an abelian subgroup of G of order 2^{h+1} and type $(4, 2, \ldots, 2)$. Applying the arguments of (10.1) gives the decomposition of $\mathrm{Jac}(C)$ as a gth power of a supersingular elliptic curve with $P = 1 + \alpha T + qT^2$ with $\alpha = \pm\sqrt{2q}$ if $V = W$ by (5.4).

(ii) There is an involution $\phi \neq \iota$ with $\phi \bmod Z \in \mathrm{rad}(V)$. The quotient curves C/ϕ and $C/\phi\iota$ have $V = W$ and W is maximal. We then apply (i) to them and note that for C the trace of Frobenius equals zero.

(iii) and (iv). If $V \neq W$ and $r(V) = 0$ then we can find an abelian subgroup B of $G(\mathbb{F}_q)$ of order 2^{h-2} and exponent 2 with $B \cap Z = \{e\}$. We claim that for $h > 2$ the jacobian $\mathrm{Jac}(C)$ is a power of an abelian surface A over $\mathbb{F}_q$. Indeed, as in part b of the proof of Theorem (10.1) we find an involution ϕ and by induction the jacobian of C/ϕ (resp. $C/\phi\iota$) is a power of an abelian surface A_ϕ (resp. $A_{\phi\iota}$). Also we find another involution ψ and non-trivial maps $A_\phi \to A_\psi$ (resp. $A_{\phi\iota} \to A_\psi$) which over $\mathbb{F}_{q^2}$ have to be isogenies, hence they are isogenies over $\mathbb{F}_q$.

We first assume that $V = W$ over $\mathbb{F}_{q^2}$. Then we know that over F_{q^2} A is (up to isogeny) a power of an elliptic curve E with

$$P(E/\mathbb{F}_{q^2}, T) = 1 \pm 2qT + q^2T^2.$$

Using the relation

$$P(A/\mathbb{F}_{q^2}, T^2) = P(A/\mathbb{F}_q, T)P(A/\mathbb{F}_q, -T)$$

and

$$P(A/\mathbb{F}_{q^2}, T^2) = P(E/\mathbb{F}_{q^2}, T^2)^2$$

we find

$$P(A/\mathbb{F}_q, T) = (1 \pm qT^2)^2.$$

If $P(A/\mathbb{F}_q, T) = (1+qT^2)^2$ then A is (up to isogeny) a second power of an elliptic curve, while if $P(A/\mathbb{F}_q, T) = (1-qT^2)^2$ then by [T] the abelian surface A is simple.

Next, if over $\mathbb{F}_{q^2}$ we have $V \neq W$ then we have by Theorem (10.1)

$$P(A/\mathbb{F}_{q^2}, T) = \begin{cases} (1+q^2T^2)^2 & \text{or} \\ (1+2qT+q^2T^2)(1-2qT+q^2T^2). \end{cases}$$

In the first case we find as above

$$P(A/\mathbb{F}_q, T) = 1+q^2T^4 = (1+\sqrt{2q}\,T + qT^2)(1-\sqrt{2q}\,T + qT^2),$$

and A is isogenous over $\mathbb{F}_q$ to a product of two elliptic curves with traces of Frobenius $+\sqrt{2q}$ and $-\sqrt{2q}$. In the second case we have $P(A/\mathbb{F}_q, T) = (1-q^2T^4)$, and this is impossible. □

As a partial converse to Theorems (10.1) and (10.2) we have:

(10.3) PROPOSITION. *If the jacobian* Jac(C) *is isogenous over* $\mathbb{F}_q$ *to a power of a supersingular elliptic curve then we either have* $V \neq W$ *or* $\dim(W) \geqslant 2h-2$. *In particular, if* m *is odd then* W *is maximal.*

Proof. Let Jac(C) be isogenous to E^g. Then on the one hand we have $t(C)=0$ or $t(C)=\pm\sqrt{q2^w}$, while on the other hand $t(C)=2^{h-1}t(E)$, where $t(\ )$ denotes the trace of Frobenius. Hence either $t(E)=0$ and hence $t(C)=0$ or $t(C)=\pm 2^{h-1}\sqrt{q2^{w(E)}}$ with $0 \leqslant w(E) \leqslant 2$ and $w(E) \equiv m \pmod 2$. Thus we have $w=2h-2+w(E)$. □

From the zeta function $Z(C/\mathbb{F}_q, T)$ of the curve we can determine whether $V = W$ in extensions of $\mathbb{F}_q$.

(10.4) EXAMPLE. Let C_R be a curve over $\mathbb{F}_q$ with m odd and with $w=\dim(W)=2h-1$, $V = W$ and with trace of Frobenius $t=-\sqrt{q2^w}$. From Theorem (10.2) it follows that

$$Z(C_R/\mathbb{F}_q, T) = \frac{(1+\sqrt{2q}\,T + qT^2)^g}{(1-qT)(1-T)},$$

where $g=2^{h-1}$. If we write

$$1+\sqrt{2q}\,T + qT^2 = (1-\alpha T)(1-\bar{\alpha}T),$$

then

$$\#C(\mathbb{F}_{q^k}) = q^k+1-g(\alpha^k+\bar{\alpha}^k).$$

We easily derive that

$$\alpha^k+\bar{\alpha}^k = (\sqrt{q})^k \cdot 2\cos(\tfrac{3}{4}\pi k).$$

Note that this is an integer. The result now reads:

$$\#C(\mathbb{F}_{q^k}) = q^k - 2gq^{k/2}\cos\frac{3k\pi}{4} + 1.$$

So for C with W maximal and $\#C(\mathbb{F}_q)=q+1+\sqrt{q2^w}$ we have

$V \neq W$ over $\mathbb{F}_{q^k}$ if and only if $k \equiv 2 \pmod 4$.

Finally, as an example we consider a case where W is relatively small ($h=2, v=w=1$) and prove simpleness.

(10.5) PROPOSITION. *Let $h=2$ and m odd. Suppose that $v=w=1$. Then* Jac(C) *is simple over* $\mathbb{F}_q$.

Proof. We have $V = W$, so $t=\pm\sqrt{2q}$. If there exists a non-hyperelliptic involution ϕ then $J=\mathrm{Jac}(C)$ is isogenous to $C_\phi \times C_{\phi\iota}$, and both of the factors have $v=w=1$, hence $t=\pm\sqrt{2q}$. So $t(J)=0$ or $t(J)=\pm 2\sqrt{2q}$, in contradiction with $t=\pm\sqrt{2q}$. Therefore, $\rho^{-1}(V)\cong \mathbb{Z}/4\mathbb{Z} = \langle\psi\rangle$. Suppose that J contains an elliptic curve E defined over $\mathbb{F}_q$. If $\psi(E)=E$ we find an elliptic curve with $\#\mathrm{Aut}(E)\geqslant 4$. It is supersingular and has either $t(E)=q$ or it is of the form C_R for some $R\in R_1$ by (8.3); hence $v\geqslant 1$, $w\geqslant 1$, so $v=w$ and $t(E)=\pm\sqrt{2q}$. By Poincaré's Complete Reducibility Theorem (cf. [Mu2], p. 173) we can find another elliptic curve E' in J. If again $\psi(E')=E'$ then $t(E')=\pm\sqrt{2q}$ and $t(J)=t(E\times E')=0$ or $\pm 2\sqrt{2q}$, a contradiction. So we find a supersingular elliptic curve E such that $\psi(E)\neq E$ and J is isogenous to E^2. Again, $t(E)=q$ or $t(E)=0$ or $t(E)=\pm\sqrt{2q}$. But then $t(J)=2t(E)=2q, 0$ or $\pm 2\sqrt{2q}$, again a contradiction. So J does not contain elliptic curves. This proves our claim. □

11. The induced representation on cohomology

Here we determine the type of the representation on the first cohomology induced by the action of $G\subset \mathrm{Aut}(C)$. The representation theory of our group is well-known, cf. [Hu, p. 562]. Let $C=C_R$ with $R\in R_h$ of degree h. Then the cohomology group $H^1_{\text{ét}}(C/\bar{\mathbb{F}}_q, \bar{\mathbb{Q}}_l)$ for a prime $l\neq 2$ is a $\bar{\mathbb{Q}}_l$-vectorspace of dimension $2g=2^h$. The action of G on C induces an action of G on

$$H^1_{\text{ét}} = H^1_{\text{ét}}(C/\bar{\mathbb{F}}_q, \bar{\mathbb{Q}}_l).$$

Call this representation ψ.

(11.1) PROPOSITION. *The representation ψ of G on $H^1_{\text{ét}}$ is the unique irreducible representation of G of dimension 2^h for which the center acts by scalar multiplication.*

Proof. The hyperelliptic involution ι acts by -1 on the jacobian, hence by -1 on the l-adic cohomology. Since the group G affords only one irreducible representation on which the center Z acts non-trivially and this has dimension 2^h (see [Hu, Ch. V, Thm. 16.14]) the proposition follows. □

12. The a-number

Let A be an abelian variety over a field k of characteristic p. Let α_p be the group scheme $\mathrm{Spec}(k[X]/(X^p))$ with comultiplication given by

$$X \to 1 \otimes X + X \otimes 1.$$

Since $\mathrm{End}(\alpha_p) = k$ we can view the group $\mathrm{Hom}(\alpha_p, A)$ as a k-vector space. One defines the a-number $a(A)$ of A as the dimension of the vector space $\mathrm{Hom}(\alpha_p, A)$. One has $0 \leqslant a(A) \leqslant \dim(A)$. Moreover, one has $a(A \times B) = a(A) + a(B)$, so a product of g supersingular elliptic curves has a-number g. If A is supersingular, that is, if A is isogenous to a product of supersingular elliptic curves, we have $1 \leqslant a(A)$.

(12.1) THEOREM. *For a linearized polynomial $R \in \mathbb{F}_q[x]$ the jacobian* $\mathrm{Jac}(C_R)$ *has a-number equal to 2^{h-2} for $h \geqslant 2$ and 1 for $h = 1$.*

Proof. We compute the Hasse-Witt matrix. The space of regular differentials has a basis $\{\omega_i = x^i\,dx : 0 \leqslant i \leqslant 2^{h-1} - 1\}$. The Cartier operator acts by $C(\omega_{2i}) = 0$, $C(\omega_{2i+1}) = \omega_i$. Therefore, the rank of the Hasse-Witt matrix is zero if $h = 1$ and 2^{h-2} for $h > 1$. Since the kernel of multiplication by 2 on $\mathrm{Jac}(C_R)$ is a group scheme of type local-local the a-number is the rank of the kernel of the Hasse-Witt matrix. □

(12.2) COROLLARY. *For $h \geqslant 2$ the jacobian* $\mathrm{Jac}(C)$ *is not isomorphic to a direct product of supersingular elliptic curves.*

13. The case of characteristic $p \geqslant 3$

Most of the results for $p = 2$ have analogs for $p \geqslant 3$. We indicate a number of them.

Let $\mathbb{F}_q$ be the finite field with $q = p^m$ elements, where p is an odd prime and m is a positive integer. For $0 \leqslant h \leqslant m/2$ we consider the set of p-linearized polynomials

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

and the corresponding family of Artin-Schreier curves C_R (or C) defined for $R \in R_h$ by

$$y^p - y = xR(x).$$

By Hurwitz-Zeuthen this curve C_R has genus $\frac{1}{2}(p-1)p^h$ for R of degree p^h. To R we associate the bilinear form

$$\mathrm{Tr}[xR(y)+yR(x)]$$

on $\mathbb{F}_q$, where Tr is the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$. Now the bilinear form is symmetric, but no longer alternating. Again we have a kernel

$$W_R(=W)=\{x\in\mathbb{F}_q\colon \mathrm{Tr}[xR(y)+yR(x)]=0 \text{ for all } y\in\mathbb{F}_q\}.$$

The analog of Proposition (3.1) reads as follows.

(13.1) PROPOSITION. *If* $R(x)=\Sigma_{i=0}^{h} a_i x^{p^i}\in R_h$ *then* $W_R=\{x\in\mathbb{F}_q\colon E_{h,R}(x)=0\}$, *where*

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

As in Proposition (3.2) the condition $c\in W_R$ is equivalent to the existence of a polynomial $B\in X\mathbb{F}_q[X]$ such that $B^p-B=cR(X)+XR(c)$. For $h=0$ we have $E_0=2a_0X$, and for $h\geqslant 1$ the polynomials satisfy the recurrence relation

$$E_h=a_h^{p^h}X^{p^{2h}}+(E_{h-1})^p+a_hX,$$

where E_{h-1} is the polynomial associated to $R-a_hx^{p^h}$. Note that E_h/X, viewed as a polynomial in a_0 is of the form

$$E_h/X=2a_0^{p^h}X^{p^h-1}+P,$$

where P lies in $\mathbb{F}_q[a_1,\ldots,a_h,X]$. Then the analog of Proposition (3.6) becomes:

(13.2) PROPOSITION. *Let* $\bar{\mathbb{F}}_q$ *be an algebraic closure of* $\mathbb{F}_q$. *The polynomial* E_h/X *is irreducible over the purely transcendental function field* $\bar{\mathbb{F}}_q(a_0,a_1,\ldots,a_h)$.

The analog of Theorem (4.1) for the automorphism group of C_R is as follows.

(13.3) THEOREM. *The group* $\mathrm{Aut}^0(C)$ *of* $\bar{\mathbb{F}}_q$*-automorphisms of* C *fixing the point at infinity is the semi-direct product of a normal subgroup* G *of order* p^{2h+1}, *and a cyclic group of order*

$$e\frac{p-1}{2}\ \text{g.c.d.}\ \{p^i+1\colon i\geqslant 0,\ a_i\neq 0\},$$

where $e=2$ if the i's with $a_i \neq 0$ have the same parity, otherwise $e=1$. In case $h>0$ the subgroup G is an extra-special p-group of exponent p, while it is cyclic for $h=0$.

As for $p=2$ an important instrument is the symplectic form on G/Z (with Z the center of G) defined by the commutator in G. Moreover, we can identify G/Z with

$$\bar{W} = \{c \in \bar{\mathbb{F}}_q : E_h(c) = 0\}.$$

However, unlike the case $p=2$ the quadratic form $\mathrm{Tr}[xR(x)]$ now always vanishes on W_R, so $\mathrm{Aut}^0_{\bar{\mathbb{F}}_q}(C) \cap G$ has order $p^{\dim(W)+1}$.

By counting points on quadrics we find immediately (cf. [Jo]):

(13.4) PROPOSITION. *Let $w = \dim(W_R)$ and set $n = m - w$. Then*

$$\#C(\mathbb{F}_q) = \begin{cases} q+1 & \text{for } n \text{ odd,} \\ q+1 \pm (p-1)\sqrt{qp^w} & \text{for } n \text{ even} \end{cases}$$

with the "$\pm$" sign depending on the type of the quadric $\mathrm{Tr}[xR(x)]=0$ in $\mathbb{F}_q/W$.

The counterpart of Proposition (9.1) is:

(13.5) PROPOSITION. *Let ϕ be a non-central automorphism of C_R, $R \in R_h$ with $h \geqslant 1$, given by $x \to x + c$, $y \to y + b_0 + B$. Then C/ϕ is the curve with equation*

$$v^p - v = -c^{-p} u P(u),$$

where $u = x^p - c^{p-1}x$, $v = y + c^{-2}b_0 x^2 - c^{-1}xB$ and where $P(u) \in \bar{\mathbb{F}}_q[u]$ is a linearized polynomial of degree p^{h-1}.

We now turn to the decomposition of the jacobian. Let U be a maximal totally isotropic subspace of $\bar{W}$. Let $\rho: G \to G/Z$ be the canonical homomorphism. Then $U' = \rho^{-1}(U)$ is a maximal abelian subgroup of G of order p^{h+1}. This is an elementary abelian p-group. Let A be a subgroup of order p^h with $A \cap Z = \{e\}$. There are exactly p^h such subgroups A. The analog of Lemma (9.3) is now

(13.6) LEMMA. *The quotient C/A is a hyperelliptic curve over $\bar{\mathbb{F}}_q$ with an equation of the form $y^p - y = x^2$. This is a supersingular curve.*

Proof. By the proposition above we find that C/A is the curve with equation $y^p - y = x^2$ over a finite field extension k. This curve is obviously hyperelliptic and of genus $(p-1)/2$ by Hurwitz-Zeuthen. Curves with equations $y^p - y = x^\mu$ have been studied by Hasse and Davenport [H-D]. They assert that the eigenvalues of Frobenius on $H^1_{\text{ét}}$ are the $p-1$ ordinary Gauss sums. This implies

that over a quadratic extension of k all eigenvalues are equal. Consequently, the characteristic polynomial is a $(p-1)$th power of a linear polynomial, and hence Jac(C) is isogenous to a product of elliptic curves. □

(13.7) THEOREM. *Over* $\bar{\mathbb{F}}_q$ *the jacobian of* C_R *is isogenous to a product of supersingular elliptic curves.*

For more results we refer to Part II of this paper.

(13.8) CONCLUDING REMARK. In the same vein as the family of curves C_R with equation $y^p - y = xR(x)$ with $R \in R_h$ we can treat the curves C_R with equation $y^p - y = xR(x)$ with $R \in R_h^{(t)}$, where

$$R_h^{(t)} = \left\{ R = \sum_{i=0}^{h} a_i X^{p^{ti}} \in \mathbb{F}_q[X] \right\}.$$

Here p is a prime, t a positive divisor of m and $1 \leqslant h \leqslant [m/2t]$. The polynomials in $R_h^{(t)}$ are p^t-linearized which means that the vector spaces involved are $\mathbb{F}_{p^t}$-vector spaces. This generalization is suggested by coding theory.

Another generalization is obtained by looking at equations $y^{p^t} - y = xR(x)$ with $R \in R_h^{(t)}$. The corresponding groups of automorphisms G are special p-groups instead of extra-special ones.

References

[Be] Berlekamp, E. R.: The weight enumerators for certain subcodes of the second order Reed-Muller codes. *Info. and Control* 17 (1970), 485–500.

[H-D] Hasse, H., Davenport, H.: Die Nullstellen der Kongruenzzetafunktion in gewissen zyklischen Fällen. *Journal f.d.r.u.a. Math.* 172 (1934), 151–182.

[Hu] Huppert, B.: *Endliche Gruppen I.* Grundlehren der Math. Wiss. 134. Springer-Verlag, Berlin, 1967.

[Jo] Joly, J.-R.: Equations et variétés algébriques sur un corps fini. *Ens. Math.* 19 (1973), 1–117.

[MacW-S] MacWilliams, F. J., Sloane, N. J. A.: *The Theory of Error-correcting Codes.* North-Holland, Amsterdam, 1983.

[Mu1] Mumford, D.: *Prym Varieties I*, in *Contributions to Analysis*, pp. 325–350. Academic Press, London, New York, 1974.

[Mu2] Mumford, D.: *Abelian Varieties.* Oxford University Press 1974.

[Se] Serre, J-P.: Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. *C.R. Acad. Sci. Paris* 296, Série I (1983), 397–402.

[T] Tate, J.: Endomorphisms of abelian varieties over finite fields. *Invent. Math.* 2 (1966), 134–144.