ACTA ARITHMETICA
105.4 (2002)

Quadratic forms, fibre products and some plane curves with many points

by

Motoko Qiu Kawakita (Cambridge and Tokyo)
and Shinji Miura (Tokyo)

Introduction. In 1977, V. D. Goppa discovered algebraic geometric codes (see [9], [10]). In 1992, S. Miura introduced C_a^b curves for constructing algebraic geometric codes (see for example [11]–[13]). To construct good codes, we need plane curves with many rational points for fixed genus.

In the 1940s, A. Weil proved an upper bound for the number of rational points on an algebraic curve C of genus g over a finite field $\mathbb{F}_q$:

$$\sharp C(\mathbb{F}_q) \le q + 1 + 2g\sqrt{q}.$$

Hasse had proved it for elliptic curves in 1933, and therefore it is called the *Hasse–Weil upper bound.* A curve is called *maximal* over $\mathbb{F}_q$ if it attains this bound.

G. van der Geer and M. van der Vlugt [5] obtained curves with many rational points including some maximal curves using quadratic forms. In this note, we will extend their assertions from $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ to $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, where q is some power of a prime number. From our assertions we can easily determine affine equations of some maximal curves which are also C_a^b curves.

Also G. van der Geer and M. van der Vlugt [7] suggest the way to construct curves with many points by taking fibre products. We apply this method to our curves.

But curves which come from fibre products do not give codes immediately. To solve this problem we give affine defining equations for them as plane curves.

In this note, we use the following notations:

- $\mathbb{N} := \{0, 1, 2, \ldots\}$.
- p is a prime number.
- q is some power of p.
- $\mathbb{F}_q$ is a finite field of cardinality q.

2000 *Mathematics Subject Classification*: 11G20, 14G05, 14G50.

- $\mathbb{F}_q^*$ is the multiplicative group of $\mathbb{F}_q$.
- $l, m \in \mathbb{N}$, $1 \le l \le m$.
- $\mathbb{F}_q^m$ is the set of m-vectors over $\mathbb{F}_q$.
- X, Y, $Y_1, \dots, Y_m$ are variables.
- $\mathrm{Tr}(X) := X + X^q + \dots + X^{q^{m-1}} \in \mathbb{F}_q[X]$.
- For $x \in \mathbb{F}_{q^m}$, $\mathrm{Tr}(x)$ is the trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$.
- $0 \le w \le m$, $m - w \equiv 0 \bmod 2$.
- $M := (m-w)/2$.
- For $a_1, \dots, a_M, b_1, \dots, b_M \in \mathbb{F}_{q^m}$,

$$Q(X) := \sum_{i=1}^{M} \mathrm{Tr}(a_i X)\,\mathrm{Tr}(b_i X) \in \mathbb{F}_{q^m}[X].$$

- For $h > 0$, $R_h := \{\sum_{i=0}^{h} c_i X^{q^i} \in \mathbb{F}_{q^m}[X] \mid c_i \in \mathbb{F}_{q^m}\}$.
- $\mathcal{R} := \{\sum_{i=0}^{s} c_i X^{p^i} \in \mathbb{F}_{q^m}[X] \mid c_i \in \mathbb{F}_{q^m},\ s > 0\}$.

In Section 1, we will introduce C_a^b curves. In Section 2, using quadratic forms over $\mathbb{F}_{q^m}$ we will determine $\#\{x \in \mathbb{F}_{q^m} \mid Q(x) = 0\}$ in terms of m, w when $a_1, \dots, a_M, b_1, \dots, b_M$ are linearly independent over $\mathbb{F}_q$. Also we will determine the number of rational points for certain curves C_R from this assertion. In Section 3, we will find conditions on $a_1, \dots, a_M, b_1, \dots, b_M$ to lower the genus of the curve C_R. By working out a special case concretely, we obtain some maximal curves in Proposition 3.3.

In Section 4, we introduce the method of [7] to construct curves with many rational points with higher genus by taking fibre products of curves with many rational points. Also we apply this method to Proposition 3.3, and we obtain more maximal curves.

In Section 5, we give a method for writing an affine defining equation as a plane curve for some curves which are constructed by fibre product, including curves of Section 4.

1. Some C_a^b curves.

First we recall the definition and properties of C_a^b curves.

Definition 1.1 ([11]). Let F be a perfect field and a, b mutually prime integers satisfying $2 \le a < b$. A C_a^b *curve* is a projective curve with an affine equation

$$f(X,Y) := \sum_{ai+bj \le ab} \alpha_{ij} X^i Y^j = 0,$$

where $\alpha_{ij} \in F$, $\alpha_{0a} \neq 0$, $\alpha_{b0} \neq 0$.

Theorem 1.1 ([11]). *Let C_a^b be a C_a^b curve defined over a perfect field F.*

(i) *The defining equation $f(X,Y)$ of C_a^b is absolutely irreducible over F.*

(ii) *The genus g of C_a^b satisfies*

$$g \leq (a-1)(b-1)/2,$$

and equality holds if and only if the curve is smooth on the affine piece.

(iii) *The normalization of C_a^b has exactly one point P_∞ lying over the point at infinity of C_a^b. Furthermore, if C_a^b is smooth on the affine piece, then $L(mP_\infty)$ on the normalization is spanned by*

$$\{x^k y^j \mid 0 \leq j \leq a-1,\, 0 \leq k, ak+bj \leq m\}$$

over F.

Now we exhibit some C_a^b curves. Let $P(X) \in \mathbb{F}_{q^m}[X]$ where $\gcd(q,d)=1$ with $d := \deg P(X)$. We define C to be the projective curve with the affine equation

$$Y^q - Y = P(X).$$

We note that curves of this restricted type are also treated in [3], [14].

Proposition 1.1. *The genus of C is*

$$g(C) = (q-1)(d-1)/2.$$

By the next lemma and Theorem 1.1 we can easily prove this proposition.

Lemma 1.1.1. *The curve C can be singular only at infinity.*

Using Hilbert's Theorem 90, we obtain:

Proposition 1.2. *The number of rational points of C over $\mathbb{F}_{q^m}$ is*

$$\#C(\mathbb{F}_{q^m}) = \#\{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}(P(x)) = 0\} \cdot q + 1.$$

2. Quadratic forms. Our purpose in this section is to prove the following theorem.

Theorem 2.1. *There exist h and $R(X) \in R_h$ such that*

$$Q(X) \equiv \mathrm{Tr}(XR(X)) \bmod (X^{q^m} - X).$$

Using the above $R(X)$, let C_R be the projective curve with the affine equation

$$Y^q - Y = XR(X).$$

(i) *If $a_1, \ldots, a_M, b_1, \ldots, b_M$ are linearly independent over $\mathbb{F}_q$, then the number of rational points of C_R over the finite field $\mathbb{F}_{q^m}$ is*

$$\#C_R(\mathbb{F}_{q^m}) = q^m + 1 + (q-1)\sqrt{q^m q^w}.$$

(ii) *Assume one of the following*:

1. *q is even, and* $\deg R(X) \geq 2$;
2. *q is odd, and* $\deg R(X) \geq 1$.

Then the genus of C_R is given by

$$g(C_R) = (q-1)\deg R(X)/2.$$

By counting the number of rational points of certain quadratic forms over $\mathbb{F}_q$, we obtain the next proposition. This assertion is very useful to determine the number of rational points of a curve C_R. G. van der Geer and M. van der Vlugt [5] have done this for the case of $q = 2$ by using results for quadratic forms over finite fields of characteristic 2. Here we compute it for the case of a general q directly.

Proposition 2.1. *If $a_1, \dots, a_M, b_1, \dots, b_M$ are linearly independent over $\mathbb{F}_q$ then*

$$\#\{x \in \mathbb{F}_{q^m} \mid Q(x) = 0\} = \frac{q^m + (q-1)\sqrt{q^m q^w}}{q}.$$

Proof of Theorem 2.1. (i) We can deduce the statement from Propositions 1.2 and 2.1.

(ii) This immediately follows from Proposition 1.1. ∎

Now we prepare a lemma and notation for the proof of Proposition 2.1. Similar results can be found in Theorem 6.5.2 of [1] and Section 1.4, Subsection 45 of [2].

Lemma 2.1.1. *If n is even, then*

$$\#\{(X_1, \dots, X_n) \in \mathbb{F}_q^n \mid X_1X_2 + X_3X_4 + \ldots + X_{n-1}X_n = 0\} \\ = q^{n-1} + (q-1)q^{(n-2)/2}.$$

Proof. For $k \in \mathbb{N},\ t \in \mathbb{F}_q$, we set

$$\beta(k,t) := \#\{(X_1, \dots, X_{2k}) \in \mathbb{F}_q^{2k} \mid X_1X_2 + X_3X_4 + \ldots + X_{2k-1}X_{2k} = t\}.$$

We prove

$$\beta(k,0) = q^{2k-1} + (q-1)q^{(2k-2)/2}$$

by induction on k.

For $k = 1$ it is clear that $\beta(k,0) = 2q - 1$.

If the formula holds for $k-1$ then

$$\begin{aligned}\beta(k,0) &= \beta(k-1,0)\beta(1,0) + \sum_{t\in\mathbb{F}_q^*} \beta(k-1,t)\beta(1,-t) \\ &= \beta(k-1,0)(2q-1) + \sum_{t\in\mathbb{F}_q^*} \beta(k-1,t)(q-1) \\ &= \beta(k-1,0)(2q-1) + (q-1)\sum_{t\in\mathbb{F}_q^*} \beta(k-1,t) \\ &= \beta(k-1,0)(2q-1) + (q-1)(q^{2k-2} - \beta(k-1,0)) \\ &= q\beta(k-1,0) + q^{2k-2}(q-1) = q^{2k-1} + (q-1)q^{k-1}. \ ∎\end{aligned}$$

Let $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}} \in \mathbb{F}_{q^m}$ be a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. We set

$$a_i = \sum_{j=1}^{m} a_{ij}\alpha^{q^{j-1}}, \qquad b_i = \sum_{j=1}^{m} b_{ij}\alpha^{q^{j-1}}$$

where $a_{ij}, b_{ij} \in \mathbb{F}_q$ for $i, j = 1, \dots, m$. Define the $m \times m$ matrix

$$A := (\mathrm{Tr}(\alpha^{q^{i-1}} \cdot \alpha^{q^{j-1}}))_{1\le i,j\le m}$$

and the $2M \times m$ matrix

$$B := \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ b_{11} & b_{12} & \dots & b_{1m} \\ \dots & \dots & \dots & \dots \\ a_{M1} & a_{M2} & \dots & a_{Mm} \\ b_{M1} & b_{M2} & \dots & b_{Mm} \end{pmatrix}.$$

For $x \in \mathbb{F}_{q^m}$, we can write

$$x = \sum_{i=1}^{m} x_i \alpha^{q^{i-1}}$$

with $x_1, \dots, x_m \in \mathbb{F}_q$. We set $\mathbf{x} := (x_1, \dots, x_m)$.

Proof of Proposition 2.1. Since $a_1, \dots, a_M, b_1, \dots, b_M$ are linearly independent over $\mathbb{F}_q$, we have $\mathrm{rank}_{\mathbb{F}_q} B = 2M$. Define an $m \times m$ regular matrix B' over $\mathbb{F}_q$ by

$$B' := \begin{pmatrix} B \\ * \end{pmatrix}.$$

Since A is also regular over $\mathbb{F}_q$, $B' \cdot A$ is a non-singular linear transformation over $\mathbb{F}_q^m$.

We set

$${}^{\mathrm{t}}(X_1, \dots, X_m) := B' \cdot A \cdot {}^{\mathrm{t}}\mathbf{x}.$$

This means that

$$X_1 = \mathrm{Tr}\left(a_1 \sum_{j=1}^{m} \alpha^{q^{j-1}} x_j\right) = \mathrm{Tr}(a_1 x),$$

$$X_2 = \mathrm{Tr}\left(b_1 \sum_{j=1}^{m} \alpha^{q^{j-1}} x_j\right) = \mathrm{Tr}(b_1 x),$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$X_{2M-1} = \mathrm{Tr}\left(a_M \sum_{j=1}^{m} \alpha^{q^{j-1}} x_j\right) = \mathrm{Tr}(a_M x),$$

$$X_{2M} = \mathrm{Tr}\left(b_M \sum_{j=1}^{m} \alpha^{q^{j-1}} x_j\right) = \mathrm{Tr}(b_M x).$$

By this one-to-one linear transformation over $\mathbb{F}_q^m$ and Lemma 2.1.1, we obtain

$$\begin{aligned}
&\#\{x \in \mathbb{F}_{q^m} \mid Q(x) = 0\} \\
&\quad = \#\Big\{x \in \mathbb{F}_{q^m} \Bigm| \sum_{i=1}^{M} \mathrm{Tr}(a_i x)\,\mathrm{Tr}(b_i x) = 0\Big\} \\
&\quad = \#\Big\{\mathbf{x} \in \mathbb{F}_q^m \Bigm| \sum_{i=1}^{M} \mathrm{Tr}\Big(a_i \sum_{j=1}^{m} \alpha^{q^{j-1}} x_j\Big)\,\mathrm{Tr}\Big(b_i \sum_{j=1}^{m} \alpha^{q^{j-1}} x_j\Big)\Big\} \\
&\quad = \#\{(X_1, \ldots, X_m) \in \mathbb{F}_q^m \mid X_1X_2 + \ldots + X_{2M-1}X_{2M} = 0\} \\
&\quad = \#\{(X_1, \ldots, X_m) \in \mathbb{F}_q^m \mid X_1X_2 + \ldots + X_{m-w-1}X_{m-w} = 0\} \\
&\quad = \#\{(X_1, \ldots, X_{m-w}) \in \mathbb{F}_q^{m-w} \mid X_1X_2 + \ldots + X_{m-w-1}X_{m-w} = 0\}q^w \\
&\quad = (q^{m-w-1} + (q-1)q^{(m-w-2)/2})q^w \\
&\quad = \frac{q^m + (q-1)\sqrt{q^m q^w}}{q}. \ \blacksquare
\end{aligned}$$

In this section, we have determined the number of rational points of curves C_R coming from $Q(X)$. In the next section, we find the conditions on $a_1, \ldots, a_M$, $b_1, \ldots, b_M$ for determining the genus of the curve C_R. They give a method for constructing curves C_R with a smaller genus.

3. Conditions for lowering the genus. By Theorem 2.1(ii), we know that we have to find $R(X)$ with lower degree which comes from the same m and w when we want curves C_R having the same number of rational points with lower genus. This means that there is a smaller h such that $R(X) \in R_h$.

In this section, we will present conditions on $a_1, \ldots, a_M, b_1, \ldots, b_M$ depending on h. When we fix h, we can obtain $R(X) \in R_h$ with

$$Q(X) \equiv \mathrm{Tr}(XR(X)) \bmod (X^{q^m} - X)$$

under these assumptions. G. van der Geer and M. van der Vlugt [5] have done this for the case of $q = 2$.

PROPOSITION 3.1. *Let m be odd. If*

$$\sum_{i=1}^{M} (a_i^{q^j} b_i + a_i b_i^{q^j}) = 0$$

for $j = h+1, \ldots, (m-1)/2$, then

$$Q(X) \equiv \mathrm{Tr}(XR(X)) \bmod (X^{q^m} - X)$$

where

$$R(X) = \sum_{i=1}^{M} a_i b_i X + \sum_{j=1}^{h} \sum_{i=1}^{M} (a_i^{q^j} b_i + a_i b_i^{q^j}) X^{q^j} \in R_h.$$

Proof. Let $a, b, x \in \mathbb{F}_{q^m}$. We can show

$$\operatorname{Tr}(ax)\operatorname{Tr}(bx) = \operatorname{Tr}(\operatorname{Tr}(ax)bx) = \operatorname{Tr}\Big(\sum_{j=0}^{m-1} (ax)^{q^j} bx\Big) = \sum_{j=0}^{m-1} \operatorname{Tr}(a^{q^j} b x^{q^j+1}).$$

Because for any $0 \le j < m$,

$$\begin{aligned}\operatorname{Tr}(a^{q^j} b x^{q^j+1}) &= \operatorname{Tr}((a^{q^j} b x^{q^j+1})^{q^{m-j}}) = \operatorname{Tr}(a^{q^m} b^{q^{m-j}} x^{q^m+q^{m-j}}) \\ &= \operatorname{Tr}(ab^{q^{m-j}} x^{q^{m-j}+1}),\end{aligned}$$

and

$$\begin{aligned}\sum_{j=(m+1)/2}^{m-1} \operatorname{Tr}(a^{q^j} b x^{q^j+1}) &= \sum_{j=(m+1)/2}^{m-1} \operatorname{Tr}((a^{q^j} b x^{q^j+1})^{q^{m-j}}) \\ &= \sum_{j=(m+1)/2}^{m-1} \operatorname{Tr}(ab^{q^{m-j}} x^{q^{m-j}+1}) \\ &= \sum_{j=1}^{(m-1)/2} \operatorname{Tr}(ab^{q^j} x^{q^j+1}),\end{aligned}$$

we obtain

$$\begin{aligned}\operatorname{Tr}(ax)\operatorname{Tr}(bx) &= \operatorname{Tr}(abx^2) + \sum_{j=1}^{(m-1)/2} \operatorname{Tr}(a^{q^j} b x^{q^j+1}) + \sum_{j=1}^{(m-1)/2} \operatorname{Tr}(ab^{q^j} x^{q^j+1}) \\ &= \operatorname{Tr}(abx^2) + \sum_{j=1}^{(m-1)/2} \operatorname{Tr}((a^{q^j} b + ab^{q^j}) x^{q^j+1}).\end{aligned}$$

Now we can deduce

$$\begin{aligned}Q(X) &:= \sum_{i=1}^{M} \operatorname{Tr}(a_i X)\operatorname{Tr}(b_i X) \\ &\equiv \sum_{i=1}^{M} \operatorname{Tr}\Big(a_i b_i X^2 + \sum_{j=1}^{(m-1)/2} (a_i^{q^j} b + a_i b_i^{q^j}) X^{q^j+1}\Big) \bmod (X^{q^m} - X) \\ &\equiv \operatorname{Tr}\Big(X\Big(\sum_{i=1}^{M} a_i b_i X + \sum_{j=1}^{(m-1)/2} \sum_{i=1}^{M} (a_i^{q^j} b_i + a_i b_i^{q^j}) X^{q^j}\Big)\Big) \bmod (X^{q^m} - X).\end{aligned}$$

By omitting the coefficients of X^{q^j} for $j = h+1, \ldots, (m-1)/2$, we get the assertion. ■

Proposition 3.2. *Let m be even. If*

$$\sum_{i=1}^{M} (a_i^{q^j} b_i + a_i b_i^{q^j}) = 0$$

for $j = h+1, \ldots, m/2$, then

$$Q(X) \equiv \mathrm{Tr}(XR(X)) \bmod (X^{q^m} - X),$$

where for $h = m/2$,

$$R(X) = \sum_{i=1}^{M} a_i b_i X + \sum_{j=1}^{(m-2)/2} \sum_{i=1}^{M} (a_i^{q^j} b_i + a_i b_i^{q^j}) X^{q^j} + \sum_{i=1}^{M} a_i^{q^{m/2}} b_i X^{q^{m/2}} \in R_h$$

and for $h \leq (m-2)/2$,

$$R(X) = \sum_{i=1}^{M} a_i b_i X + \sum_{j=1}^{h} \sum_{i=1}^{M} (a_i^{q^j} b_i + a_i b_i^{q^j}) X^{q^j} \in R_h.$$

First we prove the next lemma.

Lemma 3.2.1. *Let m be even, $k := m/2$ and $x \in \mathbb{F}_{q^m}$. If*

$$\sum_{i=1}^{M} (a_i^{q^k} b_i + a_i b_i^{q^k}) = 0,$$

then

$$\mathrm{Tr}\Big(\sum_{i=1}^{M} a_i^{q^k} b_i x^{q^k+1}\Big) = 0.$$

Proof. We set

$$y := \sum_{i=1}^{M} a_i^{q^k} b_i x^{q^k+1}.$$

By the assumptions we have

$$y^{q^k} = \sum_{i=1}^{M} a_i^{q^{2k}} b_i^{q^k} x^{q^{2k}+q^k} = \sum_{i=1}^{M} a_i b_i^{q^k} x^{q^k+1} = -\sum_{i=1}^{M} a_i^{q^k} b_i x^{q^k+1} = -y.$$

So

$$\mathrm{Tr}(y) = \sum_{j=0}^{2k-1} y^{q^j} = \sum_{j=0}^{k-1} y^{q^j} + \sum_{j=k}^{2k-1} y^{q^j} = \sum_{j=0}^{k-1} y^{q^j} + \sum_{j=0}^{k-1} (-y^{q^j}) = 0. \ ■$$

Proof of Proposition 3.2. In the same way as in the proof of Proposition 3.1, we can show

$$Q(X) \equiv \mathrm{Tr}\Big(X\Big(\sum_{i=1}^{M} a_i b_i X + \sum_{j=1}^{m/2-1} \sum_{i=1}^{M} (a_i^{q^j} b_i + a_i b_i^{q^j}) X^{q^j} + \sum_{i=1}^{M} a_i^{q^{m/2}} b_i X^{q^{m/2}}\Big)\Big) \bmod (X^{q^m} - X).$$

For $h = m/2$ our assertion is clear.

We consider the case of $h \le (m-2)/2$. By the previous lemma, we can omit the coefficient of $X^{q^{m/2}}$. For the coefficients of X^{q^j} for $j = h+1, \ldots, (m-2)/2$, we can omit them directly. ■

We obtain some maximal curves by computing the condition in Proposition 3.2 with $w = m-2$ and $h = (m-2)/2$.

Proposition 3.3. *Let m be even. Assume one of the following*:

1. *q is even, and $m \ge 4$*;
2. *q is odd.*

Then there exists a maximal curve of genus

$$g = (q-1)q^{(m-2)/2}/2$$

over $\mathbb{F}_{q^m}$. Its affine equation is

$$Y^q - Y = XR(X),$$

where

$$R(X) := bX + \sum_{j=1}^{(m-2)/2} (b + b^{q^j}) X^{q^j} \in R_{(m-2)/2}$$

with $b^{q^{m/2}} + b = 0$ and $b^q - b \ne 0$.

Proof. Because $b^{q^{m/2}} + b = 0$ and $b^q - b \ne 0$, we can consider them in the same way as in the case of $a_1 = 1$ and $b_1 = b$ in Proposition 3.2. We obtain

$$Q(X) \equiv \mathrm{Tr}(XR(X)) \bmod (X^{q^m} - X),$$

with

$$R(X) := bX + \sum_{j=1}^{(m-2)/2} (b + b^{q^j}) X^{q^j}.$$

Let C_R be the projective curve with the affine equation

$$Y^q - Y = XR(X).$$

Because 1 and b are linearly independent over $\mathbb{F}_q$, by Theorem 2.1(i), we have

$$\#C_R(\mathbb{F}_{q^m}) = q^m + 1 + (q-1)q^{(m-2)/2}\sqrt{q^m}.$$

Since the genus of C_R satisfies

$$g(C_R) \leq (q-1)q^{(m-2)/2}/2,$$

and the Hasse–Weil upper bound for the curve of genus g over a finite field $\mathbb{F}_{q^m}$ is $q^m + 1 + 2g\sqrt{q^m}$, we can deduce that C_R is a maximal curve over $\mathbb{F}_{q^m}$ and its genus is

$$g(C_R) = (q-1)q^{(m-2)/2}/2. \ \blacksquare$$

These curves are all C_a^b curves. We have encoding and decoding algorithm for them (see [12]). In [5], the case of $q = 2$ was treated, and in [8] the case of $q = p$ maximal curves in this proposition was treated by different approach. In [4], it is proved that the function field of any curve with this type of genus is a subfield of the Hermitian function field without giving the defining equations explicitly.

4. Fibre products of Artin–Schreier curves. Using fibre products, we can obtain more curves with many points.

Let $f_1, \ldots, f_l \in \{X \cdot r(X) \in \mathbb{F}_{q^m}[X] \mid r(X) \in \mathcal{R}\}$ be independent over $\mathbb{F}_q$; C_{f_i} be projective curves with affine equations $Y_i^q - Y_i = f_i(X)$ for $i = 1, \ldots, l$; L be a linear space over $\mathbb{F}_q$ which is spanned by $f_1, \ldots, f_l$; $\phi_i : C_{f_i} \to \mathbb{P}^1$ be the map given by the inclusion $\mathbb{F}_{q^m}(x) \subset \mathbb{F}_{q^m}(x, y_i)$.

We consider the curve

$$C_D = \text{Normalization of } (C_{f_1} \times_{\mathbb{P}^1} \ldots \times_{\mathbb{P}^1} C_{f_l}),$$

the normalization of the fibre products of the C_{f_i} over $\mathbb{P}^1$ with respect to the maps ϕ_i. We remark that it is possible to define an algebraic function field $\mathbb{F}_{q^m}(x, y_1, \ldots, y_l)$ with $y_i^q - y_i = f_i(x)$ for $i = 1, \ldots, l$, because $\mathbb{F}_{q^m}(x, y_1), \ldots, \mathbb{F}_{q^m}(x, y_l)$ are linearly disjoint over $\mathbb{F}_{q^m}(x)$.

Theorem 4.1 ([7]). *Let the Frobenius trace t_C on a curve C be defined by*

$$t_C := q^m + 1 - \#C(\mathbb{F}_{q^m}).$$

The Frobenius trace t_{C_D} of C_D and the genus $g(C_D)$ satisfy

$$(q-1)t_{C_D} = \sum_{f \in L \setminus \{0\}} t_{C_f}, \qquad (q-1)g(C_D) = \sum_{f \in L \setminus \{0\}} g(C_f).$$

Applying this theorem to Proposition 3.3, we obtain:

Proposition 4.1. *Let m be even. Assume one of the following*:

1. *q is even, $m \geq 4$ and $l \leq m/2 - 1$;*
2. *q is odd, and $l \leq m/2$.*

Then there exists a maximal curve of genus

$$g = (q^l - 1)q^{(m-2)/2}/2$$

over $\mathbb{F}_{q^m}$*. It is the fibre product of the curves with the affine equations*

$$Y_i^q - Y_i = X \cdot r_i(X),$$

where

$$r_i(X) := b_i X + \sum_{j=1}^{(m-2)/2} (b_i + b_i^{q^j}) X^{q^j}$$

for $i = 1, \ldots, l$*, with* $b_i^{q^{m/2}} + b_i = 0$*,* $b_i^q - b_i \neq 0$ *for* $i = 1, \ldots, l$*, and also* $b_1, \ldots, b_l$ *linearly independent over* $\mathbb{F}_q$*.*

Proof. Let $B := \{b \in \mathbb{F}_{q^m} \mid b^{q^{m/2}} + b = 0,\ b^q - b \neq 0\} \cup \{0\}$. We have

$$\dim_{\mathbb{F}_q} B = \begin{cases} m/2 - 1 & \text{if } q \text{ is even,} \\ m/2 & \text{if } q \text{ is odd.} \end{cases}$$

For $l \leq \dim_{\mathbb{F}_q} B$ we have $b_1, \ldots, b_l \in B$ which are independent over $\mathbb{F}_q$. So $X \cdot r_1(X), \ldots, X \cdot r_l(X)$ are independent over $\mathbb{F}_q$, where

$$r_i(X) := b_i X + \sum_{j=1}^{(m-2)/2} (b_i + b_i^{q^j}) X^{q^j}.$$

For $\mu_1, \ldots, \mu_l \in \mathbb{F}_q$, let $b := \sum_{i=1}^{l} \mu_i b_i$, $r(X) := \sum_{i=1}^{l} \mu_i r_i(X)$ and C_r be the curve with the affine equation

$$Y^q - Y = X \cdot r(X).$$

Since $b \in B$ and $r(X) = bX + \sum_{j=1}^{(m-2)/2} (b + b^{q^j}) X^{q^j}$, by Proposition 3.3,

$$\#C_r(\mathbb{F}_{q^m}) = q^m + 1 + (q-1) q^{(m-2)/2} \sqrt{q^m}, \qquad g(C_r) = \frac{(q-1)q^{(m-2)/2}}{2}.$$

By Theorem 4.1, we can compute the number of rational points and the genus of the curve which is the fibre product of the curves with the affine equations

$$Y_i^q - Y_i = X \cdot r_i(X),$$

for $i = 1, \ldots, l$. It is a maximal curve of genus $g = (q^l - 1) q^{(m-2)/2}/2$. ■

In [5], the case of $q = 2$ was treated, and in [8] the case of $q = p$ maximal curves in this proposition was treated by different approach. In [4], it is proved that the function field of any curve with this type of genus is a subfield of the Hermitian function field without giving the defining equations explicitly.

5. The defining equation as a plane curve. In coding theory we need plane curves with many points. In this section, we try to give defining equations of some curves which come from fibre products of curves as plane curves. By means of them we can present our maximal curves of Section 4 as plane curves. It is well known that a finite separable extension is simple. Now we give their primitive elements exactly.

Let $r_1(X),\dots,r_l(X) \in \mathcal{R}$ be independent over $\mathbb{F}_q$, $\alpha \in \mathbb{F}_{q^m}$ where $1,\alpha,\alpha^2,\dots,\alpha^{l-1}$ are independent over $\mathbb{F}_q$, and

$$A_l(\alpha) := \Big\{(a_0,a_1,\dots,a_l) \in \mathbb{F}_{q^m}^{l+1} \;\Big|\; \sum_{i=0}^{l} a_i\alpha^{(j-1)q^i} = 0 \ (j=1,\dots,l)\Big\}.$$

For $(a_0,a_1,\dots,a_l) \in A_l(\alpha)\setminus\{0\}$, we set

$$\beta_{ij} := -\sum_{k=0}^{i} a_k\alpha^{(j-1)q^k} \qquad (i=0,1,\dots,l-1,\ j=1,\dots,l),$$

$$h(Y) := \sum_{i=0}^{l} a_iY^{q^i} \in \mathbb{F}_{q^m}[Y],$$

$$f(X) := \sum_{j=1}^{l}\sum_{i=0}^{l-1} \beta_{ij}(X\cdot r_j(X))^{q^i} \in \mathbb{F}_{q^m}[X].$$

Theorem 5.1. *We can define a function field $F := \mathbb{F}_{q^m}(x,y_1,\dots,y_l)$ with $y_j^q - y_j = x\cdot r_j(x)$ for $j=1,\dots,l$ such that:*

(i) *$h(Y)-f(x) \in \mathbb{F}_{q^m}(x)[Y]$ is irreducible over $\mathbb{F}_{q^m}(x)$.*

(ii) *$F = \mathbb{F}_{q^m}(x,y)$ with $h(y)=f(x)$.*

(iii) *For the curve with the affine defining equation $h(Y)=f(X)$, only infinity can be a singular point.*

By this theorem, we can write the maximal curves of Proposition 4.1 as plane curves.

To prove this theorem we first give a lemma.

Lemma 5.1.1. (i) $A_l(\alpha) \neq \{0\}$.
(ii) *If $(a_0,a_1,\dots,a_l) \in A_l(\alpha)\setminus\{0\}$, then $a_0 \neq 0$ and $a_l \neq 0$.*

Proof. (i) It comes from the definition of $A_l(\alpha)$ directly.
(ii) Let

$$H := \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha & \alpha^q & \dots & \alpha^{q^l} \\ \dots & \dots & \dots & \dots \\ \alpha^{l-1} & \alpha^{(l-1)q} & \dots & \alpha^{(l-1)q^l} \end{pmatrix}.$$

The set $A_l(\alpha)$ is the set of solutions of $H\cdot {}^{\mathrm{t}}(a_0,a_1,\dots,a_l)=0$.

Let $(a_0, a_1, \ldots, a_l) \in A_l(\alpha) \setminus \{0\}$. If $a_0 = 0$, then $H' \cdot {}^{\mathrm{t}}(a_1, \ldots, a_l) = 0$ where

$$H' := \begin{pmatrix} 1 & \ldots & 1 \\ \alpha^q & \ldots & \alpha^{q^l} \\ \ldots & \ldots & \ldots \\ \alpha^{(l-1)q} & \ldots & \alpha^{(l-1)q^l} \end{pmatrix}.$$

Since $\det H'$ is a Vandermonde determinant, we have

$$\det H' = \prod_{l \geq i > k \geq 1} (\alpha^{q^i} - \alpha^{q^k}) \neq 0,$$

and ${}^{\mathrm{t}}(a_1, \ldots, a_l) = 0$ gives a contradiction.

If $a_l = 0$, then $H'' \cdot {}^{\mathrm{t}}(a_0, \ldots, a_{l-1}) = 0$ where

$$H'' := \begin{pmatrix} 1 & \ldots & 1 \\ \alpha & \ldots & \alpha^{q^{l-1}} \\ \ldots & \ldots & \ldots \\ \alpha^{l-1} & \ldots & \alpha^{(l-1)q^{l-1}} \end{pmatrix}.$$

Now $\det H''$ is also a Vandermonde determinant, hence

$$\det H'' = \prod_{l-1 \geq i > k \geq 0} (\alpha^{q^i} - \alpha^{q^k}) \neq 0,$$

and ${}^{\mathrm{t}}(a_0, \ldots, a_{l-1}) = 0$ gives a contradiction. ■

Now we can prove the theorem.

Proof of Theorem 5.1. (i) and (ii). Fix i where $1 \leq i \leq l$. For $\varepsilon_i \in \mathbb{F}_q$, we define $\sigma_{\varepsilon_i} : F \to F$ as

$$\sigma_{\varepsilon_i} := \begin{cases} y_i + \varepsilon_i & \text{if } j = i, \\ y_j & \text{if } j \neq i. \end{cases}$$

Now $\sigma_{\varepsilon_i} \in \mathrm{Aut}(F/\mathbb{F}_{q^m}(x))$ and $\#\{\sigma_{\varepsilon_l} \ldots \sigma_{\varepsilon_1} \mid \varepsilon_i \in \mathbb{F}_q\} = q^l$. So

$$\# \mathrm{Aut}(F/\mathbb{F}_{q^m}(x)) \geq q^l.$$

In general, $\# \mathrm{Aut}(F/\mathbb{F}_{q^m}(x)) \leq [F : \mathbb{F}_{q^m}(x)]$. Because $[F : \mathbb{F}_{q^m}(x)] \leq q^l$, we have $[F : \mathbb{F}_{q^m}(x)] = \# \mathrm{Aut}(F/\mathbb{F}_{q^m}(x))$. Hence $F/\mathbb{F}_{q^m}(x)$ is a Galois extension.

We set $y := \sum_{j=1}^{l} \alpha^{j-1} y_j$. Now we have

$$\mathbb{F}_{q^m}(x) \subseteq \mathbb{F}_{q^m}(x)(y) \subseteq \mathbb{F}_{q^m}(x, y_1, \ldots, y_l).$$

Let

$$G' := \{\sigma \in \mathrm{Gal}(F/\mathbb{F}_{q^m}(x)) \mid \forall z \in \mathbb{F}_{q^m}(x)(y),\, \sigma(z) = z\}.$$

For $\sigma \in G'$, $\sigma = \sigma_{\varepsilon_l} \dots \sigma_{\varepsilon_1}$,

$$\sigma(y) = \sigma\Big(\sum_{j=1}^{l} \alpha^{j-1} y_j\Big) = \sum_{j=1}^{l} \alpha^{j-1}(y_j + \varepsilon_j) = y + \sum_{j=1}^{l} \alpha^{j-1} \varepsilon_j.$$

So $\sum_{j=1}^{l} \alpha^{j-1} \varepsilon_j = \sigma(y) - y = 0$. Since $1, \alpha, \dots, \alpha^{l-1}$ are independent over $\mathbb{F}_q$, $\varepsilon_l = \dots = \varepsilon_1 = 0$. Hence $\sigma = \mathrm{id}$. We can say that $G' = \{1\}$. By the fundamental theorem of Galois theory, we have $\mathbb{F}_{q^m}(x)(y) = \mathbb{F}_{q^m}(x, y_1, \dots, y_l)$.

Now we deduce that $h(y) = f(x)$.

Fix $1 \leq j \leq l$. Then

$$\begin{aligned}\sum_{i=0}^{l-1} \beta_{ij}(y_j^q - y_j)^{q^i} &= \sum_{i=0}^{l-1}\Big(-\sum_{k=0}^{i} a_k \alpha^{(j-1)q^k}\Big)(y_j^{q^{i+1}} - y_j^{q^i})\\ &= \sum_{i=0}^{l-1}\Big(-\sum_{k=0}^{i} a_k \alpha^{(j-1)q^k}\Big) y_j^{q^{i+1}} - \sum_{i=0}^{l-1}\Big(-\sum_{k=0}^{i} a_k \alpha^{(j-1)q^k}\Big) y_j^{q^i}\\ &= \sum_{i=1}^{l}\Big(-\sum_{k=0}^{i-1} a_k \alpha^{(j-1)q^k}\Big) y_j^{q^i} + \sum_{i=0}^{l-1}\Big(\sum_{k=0}^{i} a_k \alpha^{(j-1)q^k}\Big) y_j^{q^i}\\ &= -\sum_{k=0}^{l-1} a_k \alpha^{(j-1)q^k} y_j^{q^l} + \sum_{i=0}^{l-1} a_i \alpha^{(j-1)q^i} y_j^{q^i}.\end{aligned}$$

Because $\sum_{k=0}^{l} a_k \alpha^{(j-1)q^k} = 0$,

$$\sum_{i=0}^{l-1} \beta_{ij}(y_j^q - y_j)^{q^i} = \sum_{i=0}^{l} a_i \alpha^{(j-1)q^i} y_j^{q^i}.$$

So

$$h(y) = \sum_{i=0}^{l} a_i y^{q^i} = \sum_{j=1}^{l}\sum_{i=0}^{l} a_i \alpha^{(j-1)q^i} y_j^{q^i} = \sum_{j=1}^{l}\sum_{i=0}^{l-1} \beta_{ij}(y_j^q - y_j)^{q^i} = f(x).$$

By Lemma 5.1.1, we know that $a_l \neq 0$, and $h(Y) - f(x) \in \mathbb{F}_{q^m}(x)[Y] \setminus \{0\}$ where $\deg_Y(h(Y) - f(x)) = q^l$. So it is irreducible over $\mathbb{F}_{q^m}(x)$. Now we can show that $F = \mathbb{F}_{q^m}(x, y)$ with $h(y) = f(x)$.

(iii) By Lemma 5.1.1, we know that $a_0 \neq 0$. Since $\frac{\partial}{\partial Y}(h(Y) - f(X)) = a_0 \neq 0$, only infinity can be a singular point. ■

We stress that the idea of Theorem 5.1 came from the Example in [6, §2]. Using this theorem, we obtain the next corollary which is contained in the assertion of Proposition 1.1 in [3].

Corollary 5.1.2. *If l is a divisor of m then $F = \mathbb{F}_{q^m}(x,y)$ with $y^{q^l} - y = f(x)$.*

Proof. Let $\alpha \in \mathbb{F}_{q^m}$ where $\mathbb{F}^*_{q^l} = \langle\alpha\rangle$, $a_0 := -1$, $a_i := 0$ for $i = 1, \ldots, l-1$, and $a_l := 1$. Now $(a_0, \ldots, a_l) \in A_l(\alpha)$, and Theorem 5.1 yields the assertion. ∎

Thus we can use our maximal curves immediately to construct algebraic geometric codes.

Acknowledgements. The first author should like to express her gratitude to Prof. Gerard van der Geer for kindly explaining to her the ideas of [5] and suggesting that they would hold for any prime number p, and that Theorem 4.1 is a straightforward extension of [7]. She would also like to thank Prof. Toshiyuki Katsura for his useful advice, and Masayuki Kawakita and Mr. Susumu Sato for their valuable comments. Finally she would like to thank the referee for suggesting how to rewrite the second section and kindly correcting grammatical errors in the first version of this paper.

References

[1] P. J. Cameron, *Projective and Polar Spaces*, QMW Maths Notes 13, School of Math. Sciences, Queen Mary and Westfield College, London.

[2] P. Dembowski, *Finite Geometries*, reprint of the 1968 edition, Springer, Berlin, 1997.

[3] A. Garcia and H. Stichtenoth, *Elementary abelian p-extensions of algebraic function fields*, Manuscripta Math. 72 (1991), 67–79.

[4] A. Garcia, H. Stichtenoth and C. P. Xing, *On subfields of the Hermitian function field*, Compositio Math. 120 (2000), 137–170.

[5] G. van der Geer and M. van der Vlugt, *Quadratic forms, generalized Hamming weights of codes and curves with many points*, J. Number Theory 59 (1996), 20–36.

[6] —, —, *On the existence of supersingular curves of given genus*, J. Reine Angew. Math. 458 (1995), 53–61.

[7] —, —, *Fibre products of Artin–Schreier curves and generalized Hamming weights of codes*, J. Combin. Theory Ser. A 70 (1995), 337–348.

[8] —, —, *Generalized Reed–Muller codes and curves with many points*, J. Number Theory 72 (1998), 257–268.

[9] V. D. Goppa, *Codes on algebraic curves*, Soviet Math. Dokl. 24 (1981), 170–172.

[10] —, *Algebraico-geometric codes*, Math. USSR-Izv. 21 (1983), 75–91.

[11] S. Miura, *Algebraic geometric codes on certain plane curves*, IEICE Trans. Fundamentals J75-A (1992), no. 11, 1735–1745 (in Japanese).

[12] —, *The error-correcting codes based on algebraic geometry*, Ph.D. dissertation, Univ. Tokyo, 1997 (in Japanese).

[13] S. Miura and N. Kamiya, *Geometric Goppa codes on some maximal curves and their minimum distance*, in: Proc. IEEE Workshop on Information Theory (Susono-shi, 1993), 85–86.

[14] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, 1993.

Department of Pure Mathematics
and Mathematical Statistics
University of Cambridge
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WB, U.K.
E-mail: mo.kawakita@dpmms.cam.ac.uk

Graduate School of Mathematical Sciences
University of Tokyo
3-8-1 Komaba, Meguro, Tokyo 153-8914, Japan
E-mail: motoko@ms.u-tokyo.ac.jp
miura@ms.u-tokyo.ac.jp

Received on 22.6.2001
and in revised form on 11.2.2002 (4059)