On certain subcovers of the Hermitian curve

Arnaldo Garcia, Motoko Q. Kawakita and Shinji Miura

Abstract

We present a simple construction that gives explicit equations for certain subcovers of the Hermitian curve. We show that certain maximal curves are indeed covered by the Hermitian curve.

MSC: Primary 11G20, 14G05; Secondary 14G50.

1 Introduction

By a curve we mean a smooth geometrically irreducible projective curve. Explicit curves(i.e., curves given by explicit equations)over finite fields with many rational points with respect to their genera have attracted a lot of attention, after Goppa discovered that they can be used to construct good linear error-correcting codes (see [4]).

For the number of $\mathbb{F}_\ell$-rational points on a curve $\mathcal{C}$ of genus $g(\mathcal{C})$ over $\mathbb{F}_\ell$ the following bound

$$\#\mathcal{C}(\mathbb{F}_\ell) \leq 1 + \ell + 2\sqrt{\ell} \cdot g(\mathcal{C})$$

is well-known as the Hasse-Weil bound. This is a deep result due to Hasse for elliptic curves;i.e.,curves with $g(\mathcal{C}) = 1$, and for general curves is due to A.Weil.

When the cardinality of the finite field $\ell = q^2$ is a square, a curve $\mathcal{C}$ over $\mathbb{F}_\ell$ is called *maximal* if it attains the Hasse-Weil bound; i.e., if we have the equality

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = 1 + q^2 + 2q \cdot g(\mathcal{C}).$$

The most important example (see [7]) of a maximal curve over $\mathbb{F}_\ell$ with $\ell = q^2$ is the Hermitian curve,denoted here by $\mathcal{H}$, which the curve given by the affine equation

$$y^{q+1} = x^q + x.$$

In [3] it is determined a large number of genera of maximal curves over $\mathbb{F}_{q^2}$ by considering quotients of the Hermitian curve by subgroups of the automorphism group of $\mathcal{H}$, which is a rather large group (see [8]).

Here we present a simple construction of subcovers as in [1] and we apply this construction to get explicit equations for subcovers of the Hermitian curve over $\mathbb{F}_{q^2}$. The key point of our approach is now to get an equation $X^q + X = Q(A(X))$ and for this we apply O. Ore's results on additive polynomials. We explain our idea and method in Section 2 and construct certain maximal curves in Section 3. We also prove an interesting result saying that any maximal curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$ with equation of the form

$$y^{q+1} = A(x) \text{ with } A(X) \text{ additive and separable in } \mathbb{F}_q[X],$$

is indeed covered by the Hermitian curve $\mathcal{H}$ (see Section 4). Here the key point is that it commutes

$$Q(A(X) = A(Q(X)).$$

Finally in Section 5 we apply our method to constructions over $\mathbb{F}_{q^n}$ with $n \geq 3$.

2 Construction of subcovers

Let k be a field and $F(X)$ a polynomial in $k[X]$. If there exist polynomials $f(X)$ and $h(X)$ in $k[X]$ such that $F(X) = f(h(X))$, then we say that $F(X)$ is *left divisible* by $f(X)$.

Suppose that a curve $\mathcal{H}$ over k is given by an affine equation

$$G(y) = F(x) \tag{1}$$

where $G(Y) \in k[Y]$ and $F(X) \in k[X]$ are polynomials such that $G(Y) - F(X) \in k[X, Y]$ is absolutely irreducible.

Proposition 1. *Let $\mathcal{H}$ be a curve given as in (1) above. Suppose that G and F are left divisible by g and f, respectively. Then the curve $\mathcal{C}$ given by*

$$g(y) = f(x) \tag{2}$$

is covered by the curve $\mathcal{H}$.

Proof: By hypothesis we can find polynomials $h_1(X) \in k[X]$ and $h_2(Y) \in k[Y]$ such that

$$F(X) = f(h_1(X)) \quad \text{and} \quad G(Y) = g(h_2(Y)).$$

Just consider the following covering map

$$\mathcal{H} \longrightarrow \mathcal{C}$$
$$(\alpha, \beta) \longmapsto (h_1(\alpha), h_2(\beta)).$$

□

Algebraic curves $\mathcal{H}$ given by Equation (1) (or their subcovers as in (2) above) are specially interesting if $\deg F$ and $\deg G$ are relatively prime. Then indeed the polynomial $G(Y) - F(X)$ is absolutely irreducible and we have the genus bound (see [5]):

$$g(\mathcal{H}) \leq \frac{(\deg F - 1)(\deg G - 1)}{2}$$

with equality if and only if the curve $\mathcal{H}$ has a unique singular point (the point at infinity).

We are going to apply Proposition 1 for the construction of maximal curves over $\mathbb{F}_\ell$ with $\ell = q^2$ by taking $\mathcal{H}$ as the Hermitian curve; i.e., by taking

$$G(Y) = Y^{q+1} \quad \text{and} \quad F(X) = X^q + X.$$

Let k be a perfect field of characteristic $p > 0$ (e.g., $k = \mathbb{F}_\ell$) and let $\bar{k}$ be the algebraic closure of k. An *additive polynomial* in $k[X]$ is a polynomial of the form:

$$A(X) = \sum_{i=0}^{n} a_i X^{p^i} \in k[X].$$

The polynomial $A(X)$ is separable if and only if $a_0 \neq 0$.

For any polynomial $A(X)$ in $k[X]$ we denote by $\mathcal{Z}(A)$ its *zero-set*; i.e.,

$$\mathcal{Z}(A) = \{\alpha \in \bar{k} \ ; \ A(\alpha) = 0\}.$$

The following results are due to O. Ore (see [6]).

Theorem 2. *Let $A(X) \in k[X]$ be a separable polynomial. Then $A(X)$ is additive if and only if its zero-set $\mathcal{Z}(A)$ is an additive subgroup of $\bar{k}$.*

Note that $\mathcal{Z}(A)$ is an additive subgroup of $\bar{k}$ if and only if $\mathcal{Z}(A)$ is a finite dimensional $\mathbb{F}_p$-vector space contained in $\bar{k}$.

Theorem 3. (Division Algorithm). *Let $F(X)$ and $A(X)$ be additive polynomials in $k[X]$ with $A \neq 0$. Then there exist additive polynomials $Q(X)$ and $R(X)$ in $k[X]$ such that*

$$F(X) = Q(A(X)) + R(X) \quad \textit{with} \quad \deg R < \deg A.$$

Moreover the polynomials Q and R are uniquely determined.

The proof of Theorem 3 is similar to that of the Euclidian Algorithm.

Let $\mathcal{A}$ and $\mathcal{F}$ be finite additive subgroups of $\bar{k}$ and denote by

$$A(X) = \Pi(X - \alpha), \text{ over } \alpha \in \mathcal{A}$$

$$F(X) = \Pi(X - \alpha), \text{ over } \alpha \in \mathcal{F}.$$

From Theorem 3 it follows

$$\mathcal{A} \subseteq \mathcal{F} \quad \Leftrightarrow \quad F(X) = Q(A(X)),$$

and consequently :

Proposition 4. *Let $\mathcal{A} \subseteq \mathcal{F}$ as above. Assume that $\mathcal{F}$ is contained in k. For a polynomial $G(Y) \in k[Y]$ with $p \nmid \deg G$, the algebraic curves over k defined by*

$$G(y) = F(x) \quad \text{and} \quad G(y) = Q(x),$$

with the additive polynomial $Q(X) \in k[X]$ as above, are such that the first is a Galois cover of the second with a Galois group isomorphic to $\mathcal{A}$.

Proof: For each element $\alpha \in \mathcal{A}$, consider the automorphism of the first curve given by

$$\sigma_\alpha(x) = x + \alpha \quad \text{and} \quad \sigma_\alpha(y) = y.$$

□

3 Construction of certain maximal curves

The maximal curves that we will deal with here are the ones in Corollary 4.8 of [3]. They appeared in [1] giving several examples of nonisomorphic maximal curves with the same genus.

As before let $A(X) = \Pi(X - \alpha)$, over α in $\mathcal{A}$. We apply Proposition 4 for additive subgroups $\mathcal{A}$ of the group $\mathcal{F} = \{\alpha \in \mathbb{F}_{q^2}\ ;\ \alpha^q + \alpha = 0\}$ and with $G(Y) = Y^{q+1}$. So the curve $\mathcal{H}$ is the Hermitian curve over $\mathbb{F}_{q^2}$ and the curve $\mathcal{C}$ is a maximal curve over $\mathbb{F}_{q^2}$ with the explicit affine equation:

$$y^{q+1} = Q(x) \quad \text{where} \quad X^q + X = Q(A(X)). \tag{3}$$

Since $Q(X)$ is an additive separable polynomial in $\mathbb{F}_{q^2}[X]$, the genus of $\mathcal{C}$ is

$$g(\mathcal{C}) = q(\deg Q - 1)/2.$$

Remark: The maximal curves $\mathcal{C}$ constructed above as in (3) have just one point P at infinity and this point P is rational over $\mathbb{F}_{q^2}$. If v_P denotes the corresponding valuation, then

$$v_P(x) = -(q+1) \quad \text{and} \quad v_P(y) = -\deg Q.$$

The Weierstrass semigroup of $\mathcal{C}$ at the point P is generated by $\deg Q$ and $(q+1)$, and we have that the following set of functions on the curve $\mathcal{C}$ is a base for the Riemann-Roch space $L(rP)$, for any $r \geq 0$:

$$\{x^i \cdot y^j \ ; \ 0 \leq i \leq \deg Q - 1, \ j \geq 0 \quad \text{and} \quad i(q+1) + j \deg Q \leq r\}.$$

This makes those maximal curves $\mathcal{C}$ suitable for the construction of one-point codes; i.e., evaluation of functions in $L(rP)$ at other rational points of the curve $\mathcal{C}$.

Example: Let $\mathcal{H}$ be the Hermitian curve over $\mathbb{F}_{q^2}$ with $q = 8$. Let α be a primitive element of $\mathbb{F}_{64}$ with equation

$$\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1 = 0.$$

Take $\{1, \alpha^9, \alpha^{18}\}$ as a $\mathbb{F}_2$-basis for

$$\mathcal{F} = \{\beta \in \mathbb{F}_{64} \ ; \ \beta^8 + \beta = 0\}$$

and consider the $\mathbb{F}_2$-subspaces of $\mathcal{F}$ with basis $\{1\}$ and $\{1, \alpha^9\}$.

Corresponding to $\{1\}$ we get a genus 12 maximal curve with equation

$$y^9 = x^4 + x^2 + x.$$

Corresponding to $\{1, \alpha^9\}$ we get a genus 4 maximal curve with equation

$$y^9 = x^2 + \alpha^{27} \cdot x.$$

Remark: Other maximal curves over $\mathbb{F}_{q^2}$ are obtained as quotients of the curves $\mathcal{C}$ given by Equation (3) above. For example, for m a divisor of $(q+1)$ we obtain the maximal curves

$$y^m = Q(x) \quad \text{with} \quad Q(X) \text{ such that } X^q + X = Q(A(X)).$$

4 A special class of maximal curves

The special class we consider here are maximal curves over $\mathbb{F}_{q^2}$ of the following type

$$y^{q+1} = A(x) \quad \text{with} \quad A(X) \text{ additive and separable in } \mathbb{F}_q[X]. \tag{4}$$

One important feature for applications to Coding Theory is the easy determination of the coordinates of the rational points, as follows:

Proposition 5. *Let $\mathcal{C}$ be a maximal curve over $\mathbb{F}_{q^2}$ given by Equation (4). Then for any $\gamma \in \mathbb{F}_q$ we have that*

$$\{\alpha \in \bar{\mathbb{F}}_q \ ; \ A(\alpha) = \gamma\} \subseteq \mathbb{F}_{q^2}.$$

The rational points over $\mathbb{F}_{q^2}$ are: the unique point at infinity plus the points in the set

$$\{(\alpha, \beta) \ ; \ A(\alpha) = \gamma = \beta^{q+1} \text{ for some } \gamma \in \mathbb{F}_q\}.$$

Proof: The genus of the curve is $g(\mathcal{C}) = q \cdot (\deg A - 1)/2$. The factor q in the genus is what makes it special. This factor comes from the exponent $(q+1)$ in Equation (4).

From the maximality we have

$$1 + q^2 + 2q \cdot g(\mathcal{C}) = 1 + q^2 \cdot \deg A.$$

But we have the y-map

$$\mathcal{C} \xrightarrow{\varphi} \mathbb{P}^1$$

$$(x, y) \longmapsto y.$$

Since the number of rational points is $1 + q^2 \deg A$, where $\deg A$ is the degree of the above map φ, and the point at infinity is totally ramified, we conclude that all pre-images under φ of elements $\beta \in \mathbb{F}_{q^2}$ are rational.

This then means that $A(X) = \beta^{q+1}$ has all solutions in $\mathbb{F}_{q^2}$; and $\beta^{q+1} = \gamma$ belongs to $\mathbb{F}_q$, since $q+1$ is the exponent of the norm map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$. □

Another special feature of Equation (4) is the assumption that $A(X)$ is additive and separable with *coefficients* in $\mathbb{F}_q$. We use this special feature in the lemma below:

Lemma 6. *Let $\mathcal{C}$ be a maximal curve over $\mathbb{F}_{q^2}$ given by Equation (4). Then we have that there exists an additive and separable polynomial $Q(X) \in \mathbb{F}_q[X]$ such that*

$$X^q + X = Q(A(X)).$$

Proof: From Proposition 5 we have

$$A(X)^q - A(X) \quad \text{divides} \quad X^{q^2} - X.$$

It then follows from the discussion just before Proposition 4, that there exists an additive and separable polynomial $Q(X) \in \mathbb{F}_q[X]$ such that

$$X^{q^2} - X = Q(A(X)^q - A(X)).$$

We are sure that $Q(X)$ has coefficients in $\mathbb{F}_q$ since $A(X)$ has. We then write

$$X^{q^2} - X = Q(A(X))^q - Q(A(X)).$$

Raising to the q-th power we get

$$X^{q^3} - X^q = Q(A(X))^{q^2} - Q(A(X))^q.$$

Summing the last two equalities we obtain

$$[X^q + X - Q(A(X))]^{q^2} = X^q + X - Q(A(X)).$$

□

We can now prove the main result here:

Theorem 7. *Let $\mathcal{C}$ be a maximal curve over $\mathbb{F}_{q^2}$ given by Equation (4). Then the curve $\mathcal{C}$ is covered by the Hermitian curve over $\mathbb{F}_{q^2}$.*

Proof: It follows from Lemma 6 (see also Equation (3)) that the curve $\mathcal{C}_1$ given by

$$y^{q+1} = Q(x) \quad \text{where} \quad X^q + X = Q(A(X)),$$

is covered by the Hermitian curve, and hence $\mathcal{C}_1$ is also a maximal curve over $\mathbb{F}_{q^2}$ as in Equation (4). Lemma 6 applied to this curve $\mathcal{C}_1$ then gives the existence of some additive polynomial $B(X)$, again with coefficients in $\mathbb{F}_q$, and $X^q + X = B(Q(X))$. Substituting X by $A(X)$, we get

$$\begin{aligned} A(X)^q + A(X) &= B(Q(A(X))) \\ &= B(X^q + X) = B(X)^q + B(X), \end{aligned}$$

and hence that $A(X) = B(X)$; i.e., the polynomials $Q(X)$ and $A(X)$ commute

$$Q(A(X)) = A(Q(X)).$$

Since $X^q + X = A(Q(X))$ holds, we conclude that the curve $\mathcal{C}$ given by

$$y^{q+1} = A(x)$$

is indeed covered by the Hermitian (see Eq.(3)). □

Compare Theorem 7 with Theorem 5.11 of [1].

Remark: Consider maximal curves over $\mathbb{F}_{q^2}$ of the form

$$P(Y) = A(X), \quad \deg P = q + 1,$$

with $A(X)$ and $P(Y)$ polynomials with coefficients in $\mathbb{F}_{q^2}$, $A(X)$ additive and $P(\beta) = 0$ for some element $\beta \in \mathbb{F}_{q^2}$.

The proof of Proposition 5 gives that for each $\beta \in \mathbb{F}_{q^2}$ we have

$$\{\alpha \in \bar{\mathbb{F}}_q \ ; \ A(\alpha) = P(\beta)\} \subseteq \mathbb{F}_{q^2}.$$

Then in particular all roots of the additive polynomial $A(X)$ are in $\mathbb{F}_{q^2}$ and the map $\varphi(x, y) = y$ is Galois. Compare with Further Hypothesis 4.8 in [1].

Remark: If $y^{q+1} = A(x)$ is a maximal curve with $A(X)$ additive, then

$$\left(\frac{ay+b}{cy+d}\right)^{q+1} + (ey)^q + (ey) = A(x)$$

is also maximal, where a, b, c, d and e belong to $\mathbb{F}_{q^2}$ and $ad - bc \neq 0$.

5 Constructions over $\mathbb{F}_{q^n}$ with $n \geq 3$

We look for additive and separable polynomials $A(X) \in \mathbb{F}_q[X]$ such that there exists an additive and separable $Q(X) \in \mathbb{F}_q[X]$ satisfying

$$X^{q^{n-1}} + X^{q^{n-2}} + \cdots + X^q + X = Q(A(X)). \tag{*}$$

Proposition 8. *Let $A(X)$ and $Q(X)$ be as above. Then*

$$A(X)^q - A(X) \quad \textit{divides} \quad X^{q^n} - X.$$

Proof: We have to show that if $\alpha \in \bar{\mathbb{F}}_q$ is such that $A(\alpha) \in \mathbb{F}_q$, then α lies in $\mathbb{F}_{q^n}$. We have

$$\alpha^{q^{n-1}} + \alpha^{q^{n-2}} + \cdots + \alpha^q + \alpha = Q(A(\alpha)).$$

Taking q-th power and using that $Q(X)$ has coefficients in $\mathbb{F}_q$, we get

$$\alpha^{q^n} + \alpha^{q^{n-1}} + \cdots + \alpha^{q^2} + \alpha^q = Q(A(\alpha)^q).$$

Since $A(\alpha)^q = A(\alpha)$, we get that $\alpha^{q^n} = \alpha$. □

Polynomials (additive and separable) $A(X)$ in $\mathbb{F}_q[X]$ satisfying (*) are appropriate for the construction of good curves over $\mathbb{F}_{q^n}$, since they satisfy the above proposition; i.e., we have

$$\text{if } \alpha \in \bar{\mathbb{F}}_q \text{ and } A(\alpha) \in \mathbb{F}_q \quad \Rightarrow \quad \alpha \in \mathbb{F}_{q^n}.$$

Construction. Let $A(X) \in \mathbb{F}_q[X]$ be additive and separable satisfying Equality (*). Consider the algebraic curve $\mathcal{C}$ given by

$$S_{n,2}(y) = A(x)$$

with $S_{n,2}(Y) = S_2(Y, Y^q, \ldots, Y^{q^{n-1}})$ where $S_2(X_1, \ldots, X_n)$ is the elementary symmetric polynomial of degree 2 in n variables. Then we have

$$g(\mathcal{C}) = \frac{q^{n-1} \cdot (\deg A - 1)}{2} \quad \text{and} \quad \#\mathcal{C}(\mathbb{F}_{q^n}) = 1 + q^n \cdot \deg A.$$

Example: Suppose that $n = 3$ and

$$A(X) = X^q + aX \in \mathbb{F}_q[X].$$

From

$$X^{q^2} + X^q + X = Q(A(X))$$

we see that $Q(X) = X^q + bX$ for some $b \in \mathbb{F}_q$. Then

$$Q(A(X)) = (X^q + aX)^q + b(X^q + aX) = X^{q^2} + (a^q + b)X^q + baX.$$

Hence $b = a^{-1}$ and $a^q + b = 1$. This gives us the equation $a^{q+1} = a - 1$, and since $a \in \mathbb{F}_q$, we get $a^2 = a - 1$. In the case $p = 2$, the element a is a primitive element of $\mathbb{F}_4$. In the case $p = 3$, we can take $a = -1$. In the case $p \geq 5$ we can write $a^2 = a - 1$ as follows

$$\left(a - \frac{1}{2}\right)^2 = \frac{-3}{4}.$$

The element a can always be chosen inside $\mathbb{F}_{p^2}$ and it can be chosen inside the prime field $\mathbb{F}_p$ if and only if

$$p \equiv 1 \quad \text{or} \quad p \equiv -5 \pmod{12}.$$

Remark: If $Q(X)$ and $A(X)$ are additive and separable polynomials in $\mathbb{F}_q[X]$ such that

$$X^{q^{n-1}} + X^{q^{n-2}} + \cdots + X^q + X = Q(A(X))$$

then one can show that they commute; i.e.,

$$Q(A(X)) = A(Q(X)).$$

From this fact and from Section 2 here, one sees that the Construction above gives subcovers of the curves in Theorem 4.1 of [2].

References

[1] M. Abdón, A. Garcia, On a characterization of certain maximal curves. Finite Fields Appl. **10**(2004), no. 2, 133–158.

[2] A. Garcia, H. Stichtenoth, A class of polynomials over finite fields. Finite Fields Appl. **5**(1999), no. 4, 424–435.

[3] A. Garcia, H. Stichtenoth, C. P. Xing, On subfields of the Hermitian function field. Compositio Math. **120**(2000), no. 2, 137–170.

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

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

[6] O. Ore, On a special class of polynomials. Trans. Amer. Math. Soc. **35**(1933), no. 3, 559–584.

[7] H.-G. Rück, H. Stichtenoth, A characterization of Hermitian function fields over finite fields. J. Reine Angew. Math. **457**(1994), 185–188.

[8] H. Stichtenoth, Über die automorphismengruppe eines algebraischen functionenkörpers von primzahl-charakteristik, Teil II. Arch. Math. **24**(1973), 615–631.

Arnaldo Garcia

IMPA, Estrada Dona Castorina 110, Rio de Janeiro, 22460-320-RJ, Brazil

E-mail: garcia@impa.br

Motoko Qiu Kawakita

Department of Information Sciences, Ochanomizu University, Tokyo 112-8610, Japan

E-mail: kawakita@cc.ocha.ac.jp

Shinji Miura

Research and Development Initiative, Chuo University, Tokyo 112-8551, Japan

E-mail: smiura@tamacc.chuo-u.ac.jp