SOME MAXIMAL FUNCTION FIELDS AND ADDITIVE POLYNOMIALS

ARNALDO GARCIA AND FERRUH ÖZBUDAK

Arnaldo Garcia
IMPA, Estrada Dona Castorina, 110
Rio de Janeiro, 22460-320-RJ, Brasil
e-mail: garcia@impa.br

Ferruh Özbudak
Department of Mathematics, Middle East Technical University
İnönü Bulvarı, 06531, Ankara, Turkey
e-mail: ozbudak@metu.edu.tr

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

Abstract. We derive explicit equations for the maximal function fields F over $\mathbb{F}_{q^{2n}}$ given by $F = \mathbb{F}_{q^{2n}}(X, Y)$ with the relation $A(Y) = f(X)$, where $A(Y)$ and $f(X)$ are polynomials with coefficients in the finite field $\mathbb{F}_{q^{2n}}$, and where $A(Y)$ is q-additive and $\deg(f) = q^n + 1$. We prove in particular that such maximal function fields F are Galois subfields of the Hermitian function field H over $\mathbb{F}_{q^{2n}}$ (i.e., the extension H/F is Galois).

Keywords: Finite field, maximal curve, additive polynomial.

1. Introduction

By a curve we mean a smooth, geometrically irreducible projective curve defined over a finite field. The main result in this theory is a celebrated theorem of A. Weil bounding the number of rational points on the curve; i.e., points with all coordinates in the finite field. This theorem is equivalent to the validity of the Riemann Hypothesis in this situation of curves over finite fields. Curves with many rational points over finite fields have interesting applications in Coding

Theory, Cryptography, Finite Geometry etc. (see for example [T-V], [S], [H], [N-X]).

Let $\mathbb{F}_q$ be the finite field with q elements and $\ell \geq 1$. For the number $\#\mathcal{X}(\mathbb{F}_{q^\ell})$ of $\mathbb{F}_{q^\ell}$-rational points of a curve $\mathcal{X}$ defined over $\mathbb{F}_{q^\ell}$ of genus $g(\mathcal{X})$, the Hasse-Weil upper bound states that

$$\#\mathcal{X}(\mathbb{F}_{q^\ell}) \leq 1 + q^\ell + 2g(\mathcal{X})q^{\ell/2}.$$

This fundamental result was proved by H. Hasse for elliptic curves and, for higher genus curves, it was proved by A. Weil. A curve $\mathcal{X}$ over $\mathbb{F}_{q^\ell}$ with $\ell = 2n$ and $n \geq 1$ is called *maximal* if its number of rational points attains the Hasse-Weil upper bound above. The most important example of a maximal curve over $\mathbb{F}_{q^{2n}}$ is the Hermitian curve $\mathcal{H}$, which can be given by the plane affine equation

$$X^{q^n+1} = Z^{q^n} + Z.$$

A large class of maximal curves consists of quotients of the Hermitian curve (see [G-S-X]). It is useful for applications to have explicit equations for maximal curves. Our aim here is to describe by explicit equations certain particular maximal curves (see Equation (1.1) below) and then conclude that they are quotients of the Hermitian curve (see Section 3).

The theory of algebraic curves is essentially equivalent to the theory of function fields. From now on, we are going to use the language of function fields and our basic reference for function fields is [S]. For example the Hermitian curve $\mathcal{H}$ corresponds to the Hermitian function field H where $H = \mathbb{F}_{q^{2n}}(X, Z)$ with the relation $X^{q^n+1} = Z^{q^n} + Z$.

We call a polynomial $A(T) \in \mathbb{F}_{q^\ell}[T]$ *q-additive* if it is of the form

$$A(T) = a_0T + a_1T^q + \cdots + a_mT^{q^m}.$$

Let $f(T) \in \mathbb{F}_{q^{2n}}[T]$ be a polynomial of degree $q^n + 1$ and let $A(T) \in \mathbb{F}_{q^{2n}}[T]$ be a q-additive polynomial of degree q^m. In this paper we consider function fields F of the particular form below

$$F = \mathbb{F}_{q^{2n}}(X, Y) \text{ with } f(X) = A(Y). \tag{1.1}$$

Using some results from coding theory, we characterize in Theorem 2.3 the polynomials $f(T) \in \mathbb{F}_{q^{2n}}[T]$ of degree $q^n + 1$ and the monic q-additive polynomials $A(T) \in \mathbb{F}_{q^{2n}}[T]$ such that the function field F in (1.1) is maximal. The characterization of $A(T)$ is done in terms of its image $V = \{A(y) : y \in \mathbb{F}_{q^{2n}}\}$ (see also Corollary 2.5) and we have essentially that $f(T) = T^{q^n+1}$. Theorems 3.12 and 3.14 give an explicit description of maximal function fields F of the form

(1.1) as a fibre product of m suitable intermediate function fields F_1,...,F_m with $\mathbb{F}_{q^{2n}}(X) \subseteq F_1, \dots, F_m \subseteq F$, where $F_1, \dots, F_m$ are also maximal function fields of the form (1.1) satisfying $[F_1 : \mathbb{F}_{q^{2n}}(X)] = \cdots = [F_m : \mathbb{F}_{q^{2n}}(X)] = q$. In this way for a maximal function field F of the form (1.1), we prove that F is a Galois subfield of the Hermitian function field H and we determine the Galois group $\mathrm{Aut}(H/F)$ explicitly. Moreover in Theorem 3.17 we give a condition for maximal function fields F of the form (1.1) to be the same (see also Corollary 3.18).

This paper is closely connected with [A-G] and [G-K-M] (see Remarks 3.3 and 3.19). The emphases here is on obtaining explicit equations for maximal function fields F given as in (1.1) above. To obtain such explicit equations we consider the trace map from $\mathbb{F}_{q^{2n}}$ to the subfield $\mathbb{F}_q$ and we use it to describe $V = \{A(y) : y \in \mathbb{F}_{q^{2n}}\}$, which is an $\mathbb{F}_q$-linear space naturally attached to the additive polynomial $A(T)$ (see Corollary 2.5 and Section 3).

Throughout the paper Tr denotes the trace map from $\mathbb{F}_{q^\ell}$ or $\mathbb{F}_{q^{2n}}$ onto $\mathbb{F}_q$.

2. Characterization of polynomials

In this section using some results from coding theory we characterize the polynomials $f(T) \in \mathbb{F}_{q^{2n}}[T]$ of degree $q^n + 1$ and the monic q-additive polynomials $A(T) \in \mathbb{F}_{q^{2n}}[T]$ such that the function field in (1.1) is maximal. The results and the methods developed in this section are used in Section 3.

The following result from linear algebra will be a useful tool to get explicit polynomial equations.

Proposition 2.1. *Let $V \subseteq \mathbb{F}_{q^\ell}$ be an $\mathbb{F}_q$-linear subspace of codimension m. There exist $\gamma_1, \dots, \gamma_m \in \mathbb{F}_{q^\ell} \setminus \{0\}$ such that for $x \in \mathbb{F}_{q^\ell}$*

$$x \in V \iff \mathrm{Tr}(\gamma_1 x) = \cdots = \mathrm{Tr}(\gamma_m x) = 0. \tag{2.1}$$

Moreover for $\{\gamma_1, \dots, \gamma_m\} \subseteq \mathbb{F}_{q^\ell}$, the $\mathbb{F}_q$-linear subspace $\{x \in \mathbb{F}_{q^\ell} : \mathrm{Tr}(\gamma_1 x) = \cdots \mathrm{Tr}(\gamma_m x) = 0\}$ is of codimension m in $\mathbb{F}_{q^\ell}$ if and only if $\{\gamma_1, \cdots, \gamma_m\}$ is linearly independent over $\mathbb{F}_q$.

Proof. Let $\{\alpha_1, \dots, \alpha_{\ell-m}\}$ be a basis of V and $(\alpha_1, \dots, \alpha_{\ell-m}, \beta_1, \dots, \beta_m)$ be an ordered basis of $\mathbb{F}_{q^\ell}$. Note that Tr defines an $\mathbb{F}_q$-bilinear form on $\mathbb{F}_{q^\ell}$. Let $(\alpha_1^*, \dots, \alpha_{\ell-m}^*, \beta_1^*, \dots, \beta_m^*)$ be the corresponding dual basis using the bilinear form given by Tr (see also [L-N, Section 2.3]). Then it follows from the definition that $\gamma_1 = \beta_1^*, \dots, \gamma_m = \beta_m^*$ satisfy (2.1).

Assume that for $\{\gamma_1, \dots, \gamma_m\} \subseteq \mathbb{F}_{q^\ell}$, the $\mathbb{F}_q$-linear subspace $V = \{x \in \mathbb{F}_{q^\ell} : \mathrm{Tr}(\gamma_1 x) = \cdots = \mathrm{Tr}(\gamma_m x) = 0\}$ is of codimension m. Then the map $\Phi : \mathbb{F}_{q^\ell} \to \mathbb{F}_q^m$ given by $x \mapsto (\mathrm{Tr}(\gamma_1 x), \cdots, \mathrm{Tr}(\gamma_m x))$ is onto. If $\{\gamma_1, \dots, \gamma_m\}$ is linearly dependent over $\mathbb{F}_q$, then without loss of generality we can assume that $\gamma_m = c_1\gamma_1 + \cdots + c_{m-1}\gamma_{m-1}$ with $c_1, \ldots, c_{m-1} \in \mathbb{F}_q$. Therefore if $\mathrm{Tr}(\gamma_1 x) = \cdots = \mathrm{Tr}(\gamma_{m-1}x) = 0$, then $\mathrm{Tr}(\gamma_m x) = 0$. This implies that $(0, \cdots, 0, 1) \in \mathbb{F}_q^m$ is not in the image of Φ, which is a contradiction. Conversely assume that $\{\gamma_1, \ldots, \gamma_m\}$ is linearly independent over $\mathbb{F}_q$. Note that $V = \mathrm{Ker}\Phi$ and as the image of Φ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^m$, we have $\dim V \geq \ell - m$. Let $(\gamma_1, \ldots, \gamma_m, \beta_1, \ldots, \beta_{\ell-m})$ be an ordered basis of $\mathbb{F}_{q^\ell}$ and $(\gamma_1^*, \ldots, \gamma_m^*, \beta_1^*, \cdots, \beta_{\ell-m}^*)$ be the corresponding dual basis with respect to the bilinear form given by Tr. For $x = c_1\gamma_1^* + \cdots + c_m\gamma_m^* + d_1\beta_1^* + \cdots + d_{\ell-m}\beta_{\ell-m}^* \in V$, we have $c_1 = \cdots = c_m = 0$. Therefore $\dim V \leq \ell - m$, which implies that V is of codimension m. □

Remark 2.2. One can show that for two m-tuples $(\gamma_1, \ldots, \gamma_m)$ and $(\bar{\gamma}_1, \ldots, \bar{\gamma}_m)$ of elements from $\mathbb{F}_{q^\ell}$ satisfying (2.1), there exists an invertible $m \times m$ matrix C over $\mathbb{F}_q$ such that $\begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_m \end{bmatrix} = C \cdot \begin{bmatrix} \bar{\gamma}_1 \\ \vdots \\ \bar{\gamma}_m \end{bmatrix}$.

Now we give our characterization of the polynomials.

Theorem 2.3. *Let $f(T) \in \mathbb{F}_{q^{2n}}[T]$ be a polynomial of degree $q^n + 1$. Let $A(T) \in \mathbb{F}_{q^{2n}}[T]$ be a monic q-additive polynomial of degree q^m. Let $F = \mathbb{F}_{q^{2n}}(X, Y)$ be the algebraic function field with the relation below*

$$f(X) = A(Y).$$

Then F is maximal over $\mathbb{F}_{q^{2n}}$ if and only if the following three conditions hold:

1.) *The polynomial $A(T)$ is separable and it splits in $\mathbb{F}_{q^{2n}}$.*

Let $V = \{A(y) : y \in \mathbb{F}_{q^{2n}}\}$, then V is an $\mathbb{F}_q$-linear subspace in $\mathbb{F}_{q^{2n}}$ of codimension m. Let $(\gamma_1, \ldots, \gamma_m)$ be an m-tuple of elements from $\mathbb{F}_{q^{2n}} \setminus \{0\}$ such that for $x \in \mathbb{F}_{q^{2n}}$ (cf. Proposition 2.1)

$$x \in V \iff \mathrm{Tr}(\gamma_1 x) = \cdots = \mathrm{Tr}(\gamma_m x) = 0.$$

Denote by $\gamma = \gamma_1$ and by $a_i = \gamma_{i+1}/\gamma$ for $0 \leq i \leq m - 1$.

2.) *We have $a_1, \ldots, a_{m-1} \in \mathbb{F}_{q^n}$ and $\{1, a_1, \ldots, a_{m-1}\}$ is linearly independent over $\mathbb{F}_q$. In particular $m \leq n$.*

3.) *We have $f(T) = f_0 + uT^{q^n+1}$, where $f_0 \in \{A(y) : y \in \mathbb{F}_{q^{2n}}\}$ and*

$$u\gamma + u^{q^n}\gamma^{q^n} = 0.$$

Proof. The genus of the function field F is $q^n(q^m-1)/2$ and the field F is maximal if and only if the number of rational places of F is

$$1+q^{2n}+2\frac{q^n(q^m-1)}{2}q^n=1+q^{2n+m}.$$

Then F is maximal if and only if for each $x\in\mathbb{F}_{q^{2n}}$ the polynomial $A(T)-f(x)\in\mathbb{F}_{q^{2n}}[T]$ has q^m distinct roots in $\mathbb{F}_{q^{2n}}$. We denote the coefficients of $f(T)\in\mathbb{F}_{q^{2n}}[T]$ as below

$$f(T)=\sum_{i=0}^{q^n+1}\alpha_iT^i,\text{ and we let }\bar{f}(T)=\sum_{i=1}^{q^n+1}\alpha_iT^i.$$

Assume that F is maximal. Then $A(T)-f(0)=A(T)-\alpha_0$ has q^m distinct roots in $\mathbb{F}_{q^{2n}}$. Let $y_0\in\mathbb{F}_{q^{2n}}$ with $\alpha_0=A(y_0)$ and let $\bar{Y}=Y-y_0\in F$. We have $F=\mathbb{F}_{q^{2n}}(X,\bar{Y})$, where

$$\bar{f}(X)=A(\bar{Y}).$$

Therefore $A(T)-\bar{f}(x)\in\mathbb{F}_{q^{2n}}[T]$ has q^m distinct roots in $\mathbb{F}_{q^{2n}}$ for each $x\in\mathbb{F}_{q^{2n}}$. As $\bar{f}(0)=0$, in particular $A(T)$ is separable and it splits in $\mathbb{F}_{q^{2n}}$. Let I be the subset of $\{1,\ldots,q^n+1\}$ such that $i\in I\iff\alpha_i\neq 0$. Note that $q^n+1\in I$ and $0\notin I$. Let $I=\{i_1,\ldots,i_h\}$ with $1\le i_1<\ldots<i_h=q^n+1$ and $S(I)$ be the $\mathbb{F}_q$-linear space below

$$S(I)=\left\{\beta_1T^{i_1}+\cdots+\beta_hT^{i_h}:\beta_1,\ldots,\beta_h\in\mathbb{F}_{q^{2n}}\right\}.$$

Note that the dimension of $S(I)$ is equal to $2nh$. Let w be a generator of the multiplicative group of $\mathbb{F}_{q^{2n}}$, $t=q^{2n}-1$ and Ψ be the $\mathbb{F}_q$-linear map

$$\begin{aligned}\Psi:S(I)\to\ &\mathbb{F}_q^{mt}\\ g(T)\mapsto\ &\left(\mathrm{Tr}(\gamma_1g(w)),\ldots,\mathrm{Tr}(\gamma_1g(w^t)),\ldots\ldots,\mathrm{Tr}(\gamma_mg(w)),\ldots,\mathrm{Tr}(\gamma_mg(w^t))\right).\end{aligned}$$

As the polynomial $A(T)-\bar{f}(x)\in\mathbb{F}_{q^{2n}}[T]$ has q^m distinct roots in $\mathbb{F}_{q^{2n}}$ for each $x\in\mathbb{F}_{q^{2n}}$, we have that $\bar{f}(x)\in V=\{A(y):y\in\mathbb{F}_{q^{2n}}\}$ for each $x\in\mathbb{F}_{q^{2n}}$. By the definition of the map Ψ, this implies that $\bar{f}(T)\in\mathrm{Ker}\Psi$, and hence $\mathrm{Ker}\Psi\neq\{0\}$. Let C be the image of the map Ψ. We observe that C is the dual of the additive code over $\mathbb{F}_q$ corresponding to I and $(\gamma_1,\ldots,\gamma_m)$ (see [B, Section 5]). For $1\le i\le q^n$, we have $\left|\{iq^j\mod(q^{2n}-1):0\le j\le 2n-1\}\right|=2n$ and $\left|\{(q^n+1)q^j\mod(q^{2n}-1):0\le j\le 2n-1\}\right|=n$. Therefore using [B, Theorems 19 and 21] we obtain that

$$\dim_{\mathbb{F}_q}C=(h-1)2n+nr,$$

where r is the rank of the $m \times 2$ matrix

$$\begin{bmatrix} \gamma_1 & \gamma_1^{q^n} \\ \gamma_2 & \gamma_2^{q^n} \\ \vdots & \vdots \\ \gamma_m & \gamma_m^{q^n} \end{bmatrix}$$

over $\mathbb{F}_{q^{2n}}$. We have $r \in \{1, 2\}$ and

$$r = 1 \Longleftrightarrow m = 1 \text{ or } a_1 = \frac{\gamma_2}{\gamma_1}, \ldots, a_{m-1} = \frac{\gamma_m}{\gamma_1} \in \mathbb{F}_{q^n}.$$

If $r = 2$, then $dim_{\mathbb{F}_q} C = 2nh$ and hence $\mathrm{Ker}\Psi = \{0\}$, which is a contradiction. Since $r = 1$, we have

$$\dim_{\mathbb{F}_q} \mathrm{Ker}\Psi = 2hn - \dim_{\mathbb{F}_q} C = n.$$

For $\gamma = \gamma_1$, it is not difficult to observe that for each $u \in \mathbb{F}_{q^{2n}}$ satisfying

$$u\gamma + u^{q^n}\gamma^{q^n} = 0, \tag{2.2}$$

the polynomial $uT^{q^n+1} \in \mathrm{Ker}\Psi$. The number of $u \in \mathbb{F}_{q^{2n}}$ satisfying (2.2) is q^n and hence $\mathrm{Ker}\Psi = \{uT^{q^n+1} \in \mathbb{F}_{q^{2n}}[T] : u\gamma + u^{q^n}\gamma^{q^n} = 0\}$.This proves item 3.). Conversely, using the transitivity of traces (see Remark 3.1) it is now also clear that if the items 1.), 2.) and 3.) hold, then the function field F is maximal. This completes the proof. □

We develop further tools, which will be used in Section 3.

Lemma 2.4. *Let $A_1[T], A_2[T] \in \mathbb{F}_{q^\ell}[T]$ be monic q-additive polynomials both of degree q^m and both splitting in $\mathbb{F}_{q^\ell}$. If $\{A_1(y) : y \in \mathbb{F}_{q^\ell}\} = \{A_2(y) : y \in \mathbb{F}_{q^\ell}\}$, then $A_1(T) = A_2(T)$.*

Proof. Assume that $\{A_1(y) : y \in \mathbb{F}_{q^\ell}\} = \{A_2(y) : y \in \mathbb{F}_{q^\ell}\}$ and let $A(T) = A_1(T) - A_2(T)$. If $A_1(T) \neq A_2(T)$, then $A(T)$ is a q-polynomial of degree q^h with $h < m$. Moreover the $\mathbb{F}_q$-linear space $\{A(y) : y \in \mathbb{F}_{q^\ell}\}$ is a subspace of the $\mathbb{F}_q$-linear space $\{A_1(y) : y \in \mathbb{F}_{q^\ell}\}$, since $\{A_1(y) : y \in \mathbb{F}_{q^\ell}\} = \{A_2(y) : y \in \mathbb{F}_{q^\ell}\}$. This implies that $\{y \in \mathbb{F}_{q^\ell} : A(y) = 0\}$ is an $\mathbb{F}_q$-linear space of dimension at least m, which is a contradiction since $h < m$. □

Note that for $0 \leq m \leq \ell$, the number of m-dimensional $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_{q^\ell}$ is given by the formula below:

$$\frac{\left(q^\ell - 1\right)\left(q^\ell - q\right)\cdots\left(q^\ell - q^{m-1}\right)}{\left(q^m - 1\right)\left(q^m - q\right)\cdots\left(q^m - q^{m-1}\right)}.$$

This formula also implies that the number of $\mathbb{F}_q$-linear subspaces in $\mathbb{F}_{q^\ell}$ of dimension m is equal to the number of subspaces of codimension m. Further we note that there is a one to one correspondence between the m-dimensional $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_{q^\ell}$ and the monic q-additive polynomials in $\mathbb{F}_{q^\ell}[T]$ of degree q^m splitting in $\mathbb{F}_{q^\ell}$. Hence using also Lemma 2.4 we obtain the following corollary.

Corollary 2.5. *For each $\mathbb{F}_q$-linear subspace V in $\mathbb{F}_{q^\ell}$ of codimension m, there exists a uniquely determined monic q-additive polynomial $A(T) \in \mathbb{F}_{q^\ell}[T]$ of degree q^m (splitting in $\mathbb{F}_{q^\ell}$) such that*

$$V = \left\{A(y) : y \in \mathbb{F}_{q^\ell}\right\}.$$

Remark 2.6. Let $\gamma,\ u \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ with $u\gamma + (u\gamma)^{q^n} = 0$. Assume that $\{1, a_1, \ldots, a_{m-1}\} \subseteq \mathbb{F}_{q^n}$ is linearly independent over $\mathbb{F}_q$. Let $A(T)$ be the monic q-additive polynomial of degree q^m such that (see Corollary 2.5)

$$x \in \{A(y) : y \in \mathbb{F}_{q^{2n}}\} \Longleftrightarrow \mathrm{Tr}(\gamma x) = \mathrm{Tr}(a_1\gamma x) = \cdots = \mathrm{Tr}(a_{m-1}\gamma x) = 0,$$

and $f_0 \in \{A(y) : y \in \mathbb{F}_{q^{2n}}\}$. By Theorem 2.3, the function field $F = \mathbb{F}_{q^{2n}}(X, Y)$, where $f_0 + uX^{q^n+1} = A(Y)$ is a maximal function field. Let $\bar{X} = X$, $y_0 \in \mathbb{F}_{q^{2n}}$ such that $A(y_0) = f_0$, $\bar{Y} = u^{-1/q^m}(Y - y_0) \in F$, $\bar{\gamma} = u\gamma$ and $\bar{A}(T) = u^{-1}A\left(u^{1/q^m}T\right)$. Then F is also equal to the function field $\mathbb{F}_{q^{2n}}(\bar{X}, \bar{Y})$, where $\bar{X}^{q^n+1} = \bar{A}(\bar{Y})$, $\bar{\gamma} + \bar{\gamma}^{q^n} = 0$ and $\bar{A}(T)$ is the monic q-additive polynomial of degree q^m such that

$$x \in \{\bar{A}(y) : y \in \mathbb{F}_{q^{2n}}\} \Longleftrightarrow \mathrm{Tr}(\bar{\gamma} x) = \mathrm{Tr}(a_1\bar{\gamma} x) = \cdots = \mathrm{Tr}(a_{m-1}\bar{\gamma} x) = 0.$$

3. Galois Subcovers of the Hermitian function field

In this section using fibre products of some explicitly given maximal function fields, we represent a maximal function field F of the form (1.1) as a Galois subfield of the Hermitian function field H, explicitly.

Throughout this section we fix a root γ of $T^{q^n} + T$. Any maximal function field F of the form (1.1) corresponds to an $\mathbb{F}_q$-linearly independent set $\{c_1, \ldots, c_m\} \subseteq \mathbb{F}_{q^n}$ such that for the monic q-additive polynomial $A(T)$ satisfying

$$x \in \{A(y) : y \in \mathbb{F}_{q^{2n}}\} \Longleftrightarrow \mathrm{Tr}(c_1\gamma x) = \cdots = \mathrm{Tr}(c_m\gamma x) = 0, \tag{3.1}$$

the maximal function field F is equal to the field $F = \mathbb{F}_{q^{2n}}(X, Y)$, where we have the relation $X^{q^n+1} = A(Y)$ (cf. Remark 2.6).

Remark 3.1. The transitivity $\mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_q} = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q} \circ \mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^n}}$ of the traces implies that if (3.1) holds, then the set $\{A(y) : y \in \mathbb{F}_{q^{2n}}\}$ contains $\mathbb{F}_{q^n}$.

Proposition 3.2. *Let $\{c_1, \ldots, c_m\} \subseteq \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-linearly independent subset. Let $A(T) \in \mathbb{F}_{q^{2n}}[T]$ be the monic q-polynomial of degree q^m satisfying (3.1). We further have that $A(T) \in \mathbb{F}_{q^n}[T]$.*

Proof. Using Corollary 2.5, let $B(T) \in \mathbb{F}_{q^n}[T]$ be the monic q-additive polynomial of degree q^m such that

$$x \in \{B(z) : z \in \mathbb{F}_{q^n}\} \iff \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c_1x) = \cdots = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(c_mx) = 0.$$

Let $B(T) = T^{q^m} + b_1T^{q^{m-1}} + \cdots + b_{m-1}T^q + b_mT$ and for $1 \le i \le m$ define $a_i = b_i\gamma^{\frac{1}{q^i}-1}$. Note that $(\gamma)^{(q^n-1)(q^i-1)} = (-1)^{q^i-1} = 1$ for each $1 \le i \le m$ and hence the monic q-polynomial $A(T) = T^{q^m} + a_1T^{q^{m-1}} + \cdots + a_{m-1}T^q + a_mT \in \mathbb{F}_{q^n}[T]$. It is not difficult to observe that

$$x \in \{A(y) : y \in \mathbb{F}_{q^{2n}}\} \iff \left(\gamma x + \gamma^{q^n} x^{q^n}\right) \in \{B(z) : z \in \mathbb{F}_{q^n}\}.$$

Indeed the map sending $y \in \mathbb{F}_{q^{2n}}$ to $\gamma^{1/q^m}y + \gamma^{q^{n-m}}y^{q^n} \in \mathbb{F}_{q^n}$ is onto and for each $x,\ y \in \mathbb{F}_{q^{2n}}$ and $z = \gamma^{1/q^m}y + \gamma^{q^{n-m}}y^{q^n} \in \mathbb{F}_{q^n}$ we have

$$x = A(y) \iff \gamma x + \gamma^{q^n} x^{q^n} = B(z).$$

Therefore

$$x \in \{A(y) : y \in \mathbb{F}_{q^{2n}}\} \iff \mathrm{Tr}(c_1\gamma x) = \cdots = \mathrm{Tr}(c_m\gamma x) = 0,$$

since $\mathrm{Tr}(c_i\gamma x) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(c_i(\gamma x + \gamma^{q^n}x^{q^n})\right)$ for $1 \le i \le m$. We complete the proof using the uniqueness of $A(T)$ from Corollary 2.5. □

Remark 3.3. Proposition 3.2 shows that if $F = \mathbb{F}_{q^{2n}}(X, Y)$ with $X^{q^n+1} = A(Y)$ is a maximal function field, then the monic q-additive polynomial $A(T)$ has coefficients in $\mathbb{F}_{q^n}$. This fact was used as a hypothesis in Section 4 of [G-K-M] and we could then proceed as in [G-K-M] to show that F is a Galois subfield of the Hermitian function field H (i.e., the field extension H/F is Galois). In what follows we prove that F is a Galois subfield of H by exhibiting an explicit equation for the function field F.

Recall that the Hermitian function field H over $\mathbb{F}_{q^{2n}}$ is given by $H = \mathbb{F}_{q^{2n}}(X, Z)$, where we have the relation $X^{q^n+1} = Z^{q^n} + Z$.

Lemma 3.4. *Assume that $n = m$. For any $\mathbb{F}_q$-linearly independent set $\{c_1, \ldots, c_n\} \subseteq \mathbb{F}_{q^n}$, the corresponding monic q-additive polynomial of degree q^n is $T^{q^n} + T$, and hence the Hermitian function field is the only maximal function field of the form (1.1) in this case.*

Proof. Let $\{c_1, \ldots, c_n\} \subseteq \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$. Let V be the $\mathbb{F}_q$-linear subspace in $\mathbb{F}_{q^{2n}}$ such that

$$x \in V \iff \mathrm{Tr}(c_1\gamma x) = \mathrm{Tr}(c_2\gamma x) = \cdots = \mathrm{Tr}(c_n\gamma x) = 0.$$

By Proposition 2.1, the $\mathbb{F}_q$-dimension of V is n. Moreover for $c,\ x \in \mathbb{F}_{q^n}$ we have

$$\mathrm{Tr}(c\gamma x) = \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(\left(\gamma + \gamma^{q^n}\right) cx\right) = 0,$$

and hence $V = \mathbb{F}_{q^n}$. It is well known that $\mathbb{F}_{q^n} = \left\{y^{q^n} + y : y \in \mathbb{F}_{q^{2n}}\right\}$, and the uniqueness of $T^{q^n} + T$ follows from Corollary 2.5. □

Remark 3.5. Lemma 3.4 also follows from [R-S] since the genus of the corresponding maximal function field is $q^n(q^n - 1)/2$ in this case.

For each root α of $T^{q^n} + T$, let ψ_α be the automorphism of H over $\mathbb{F}_{q^{2n}}(X)$ given by

$$\psi_\alpha(Z) = Z + \alpha \ \ \textit{and} \ \ \psi_\alpha(X) = X.$$

For roots $\alpha_1,\ \alpha_2$ of $T^{q^n} + T$, we have $\psi_{\alpha_1} \circ \psi_{\alpha_2} = \psi_{\alpha_2} \circ \psi_{\alpha_1} = \psi_{\alpha_1+\alpha_2}$, and

$$G = \{\psi_\alpha : \alpha^{q^n} + \alpha = 0\}$$

is the group $\mathrm{Aut}(H/\mathbb{F}_{q^{2n}}(X))$ of automorphisms of H fixing $\mathbb{F}_{q^{2n}}(X)$. In particular the group G is a one dimensional $\mathbb{F}_{q^n}$-linear space generated by ψ_γ and the extension $H/\mathbb{F}_{q^{2n}}(X)$ is an abelian (Galois) extension.

For each $\mu \in \mathbb{F}_{q^n} \setminus \{0\}$, let $B_\mu(T)$ and $C_\mu(T)$ be the monic q-additive polynomials below

$$B_\mu(T) = T^q - (\mu\gamma)^{1/q-1}T, \text{ and}$$

$$C_\mu(T) = T^{q^{n-1}} + (\mu\gamma)^{1/q^2-1/q}T^{q^{n-2}} + \cdots + (\mu\gamma)^{1/q^n-1/q}T.$$

Lemma 3.6. *For each $\mu \in \mathbb{F}_{q^n} \setminus \{0\}$, we have*

$$T^{q^n} + T = B_\mu \circ C_\mu = C_\mu \circ B_\mu,$$

and hence the polynomials B_μ and C_μ split in $\mathbb{F}_{q^{2n}}$.

Proof. The proof follows from direct computations. □

Remark 3.7. For $\mu_1,\ \mu_2 \in \mathbb{F}_{q^n} \setminus \{0\}$, we have

$$C_{\mu_1}(T) = C_{\mu_2}(T) \iff \mu_1/\mu_2 \in \mathbb{F}_q.$$

Let P be a subset of $\mathbb{F}_{q^n}$ consisting of $\frac{q^n-1}{q-1}$ elements and corresponding to the projective space of dimension $n-1$ over $\mathbb{F}_q$.

For each $\mu \in \mathbb{F}_{q^n} \setminus \{0\}$, let G_μ be a subgroup of G defined by

$$G_\mu = \{\psi_\alpha : \alpha \text{ is a root of } C_\mu(T)\}.$$

Note that G_μ is an $\mathbb{F}_q$-linear subspace of G of codimension 1.

Remark 3.8. The set of all codimension one $\mathbb{F}_q$-linear subspaces of the group G is $\{G_\mu : \mu \in P\}$. For each $\mathbb{F}_q$-linear subspace $V \subseteq G$ of codimension m, there exists $\{\mu_1, \ldots, \mu_m\} \subseteq P$ such that

$$V = G_{\mu_1} \cap \cdots \cap G_{\mu_m}.$$

In general, $\{\mu_1, \ldots, \mu_m\}$ is not unique.

Lemma 3.9. *For a subset $\{\mu_1, \ldots, \mu_m\} \subseteq \mathbb{F}_{q^n} \setminus \{0\}$, if the $\mathbb{F}_q$-linear subspace $\bigcap_{i=1}^m G_{\mu_i}$ is of codimension m in G, then $\{\mu_1, \ldots, \mu_m\}$ is linearly independent over $\mathbb{F}_q$.*

Proof. For $\mu \in \mathbb{F}_{q^n} \setminus \{0\}$, let $\overline{C}_\mu = (\mu\gamma)^{1/q} C_\mu$. Note that for $\mu_1, \mu_2 \in \mathbb{F}_{q^{2n}}$ with $\mu_1 + \mu_2 \neq 0$ we have $\overline{C}_{\mu_1+\mu_2} = \overline{C}_{\mu_1} + \overline{C}_{\mu_2}$. Moreover for $\mu \in \mathbb{F}_{q^n} \setminus \{0\}$, $a \in \mathbb{F}_q \setminus \{0\}$ and $\alpha \in \mathbb{F}_{q^{2n}}$ we have

$$C_\mu(\alpha) = 0 \iff \overline{C}_\mu(\alpha) = 0 \iff \overline{C}_{a\mu}(\alpha) = 0.$$

Assume that $\{\mu_1, \ldots, \mu_m\}$ is linearly dependent over $\mathbb{F}_q$. By passing to a subset, we can assume without loss of generality that $\mu_1 = a_2\mu_2 + \cdots + a_m\mu_m$ with $a_2, \ldots, a_m \in \mathbb{F}_q \setminus \{0\}$ and that the sum of any nonempty subset of $\{a_2\mu_2, \ldots, a_m\mu_m\}$ is nonzero. For $\alpha \in \mathbb{F}_{q^{2n}}$ with $C_{\mu_2}(\alpha) = \cdots = C_{\mu_m}(\alpha) = 0$ we have $\overline{C}_{a_2\mu_2}(\alpha) = \cdots = \overline{C}_{a_m\mu_m}(\alpha) = 0$ and hence

$$C_{\mu_1}(\alpha) = \overline{C}_{\mu_1}(\alpha) = \overline{C}_{a_2\mu_2}(\alpha) + \cdots + \overline{C}_{a_m\mu_m}(\alpha) = 0.$$

Then $G_{\mu_1} \subseteq \bigcap_{i=2}^m G_{\mu_i}$ and hence $\bigcap_{i=1}^m G_{\mu_i}$ is of codimension smaller or equal to $m-1$ in G, which is a contradiction. □

Remark 3.10. In Theorem 3.14 we will prove the converse of Lemma 3.9.

Lemma 3.11. *For each $\mu \in P$, the fixed subfield of the Hermitian function field H corresponding to G_μ is $\mathbb{F}_{q^{2n}}(X, Y)$, where*

$$X^{q^n+1} = B_\mu(Y).$$

Proof. For $\psi_\alpha \in G_\mu$, we have by definition that $C_\mu(\alpha) = 0$. The function $Y = C_\mu(Z)$ of the Hermitian function field H is invariant under this subgroup G_μ of G. In fact we have

$$\psi_\alpha(Y) = \psi_\alpha\left(C_\mu(Z)\right) = C_\mu\left(Z + \alpha\right) = C_\mu(Z) + C_\mu(\alpha) = Y.$$

Now since the fixed field of G_μ has degree q over $\mathbb{F}_{q^{2n}}(X)$ and the polynomial B_μ is of degree q, we conclude the proof. □

Using Lemma 3.11 we obtain the following theorem.

Theorem 3.12. *For $m \leq n-1$, let $V \subseteq G$ be the $\mathbb{F}_q$-linear subspace of codimension m such that*

$$V = G_{\mu_1} \cap \cdots \cap G_{\mu_m},$$

where $\{\mu_1, \ldots, \mu_m\} \subseteq P$. The fixed subfield of H corresponding to the linear space V is given by $\mathbb{F}_{q^{2n}}(X, Y_1\ , \ldots, Y_m)$, where

$$\begin{aligned} X^{q^n+1} &= B_{\mu_1}(Y_1), \\ &\vdots \\ X^{q^n+1} &= B_{\mu_m}(Y_m). \end{aligned}$$

Let $W = \{\alpha : C_{\mu_1}(\alpha) = \cdots = C_{\mu_m}(\alpha) = 0\}$ and let $C_V = \prod_{\alpha \in W}(T - \alpha) \in \mathbb{F}_{q^{2n}}[T]$. There exists a uniquely determined monic q-polynomial $B_V(T) \in \mathbb{F}_{q^n}[T]$ of degree q^m such that $T^{q^n} + T = B_V \circ C_V$, and moreover we have that the function field $\mathbb{F}_{q^{2n}}(X, Y_1, \ldots, Y_m)$ is also equal to the field $\mathbb{F}_{q^{2n}}(X, Y)$, with $X^{q^n+1} = B_V(Y)$.

Proof. Let μ be any of $\mu_1, \ldots, \mu_m$. Since the polynomial C_V divides C_μ, there exists a uniquely determined monic q-additive polynomial $D \in \mathbb{F}_{q^{2n}}[T]$ such that $C_\mu = D \circ C_V$ (cf. [G-K-M, Theorem 3]). As C_V divides the polynomial $T^{q^n} + T$, similarly, we have a uniquely determined monic q-additive polynomial $B_V \in \mathbb{F}_{q^{2n}}[T]$ such that $T^{q^n} + T = B_V \circ C_V$. It then follows that $B_V = B_\mu \circ D$; in fact we have

$$B_V\left(C_V\right) = T^{q^n} + T = B_\mu \circ C_\mu = \left[B_\mu \circ D\right]\left(C_V\right).$$

The equality $B_V = B_\mu \circ D$ implies that the function field $\mathbb{F}_{q^{2n}}(X, Y)$ with the relation $X^{q^n+1} = B_V(Y)$ contains the compositum of the function fields associated to G_μ as in Lemma 3.11. Moreover using Proposition 3.2 we further have that $B_V \in \mathbb{F}_{q^n}[T]$ and this finishes the proof. □

Lemma 3.13. *For each $\mu \in \mathbb{F}_{q^n} \setminus \{0\}$ we have*

$$x \in \{B_\mu(y) : y \in \mathbb{F}_{q^{2n}}\} \iff \operatorname{Tr}(\mu\gamma x) = 0.$$

Proof. Using Hilbert's Theorem 90 we have

$$\mu\gamma x \in \{y^q - y : y \in \mathbb{F}_{q^{2n}}\} \Longleftrightarrow \mathrm{Tr}(\mu\gamma x) = 0.$$

The proof follows from the observation that

$$\left\{\frac{1}{\mu\gamma}(y^q - y) : y \in \mathbb{F}_{q^{2n}}\right\} = \{B_\mu(y) : y \in \mathbb{F}_{q^{2n}}\}.$$

□

Theorem 3.14. *For each $\{\mu_1, \ldots, \mu_m\} \subseteq \mathbb{F}_{q^n}$ such that $\{\mu_1, \ldots, \mu_m\}$ is linearly independent over $\mathbb{F}_q$, we have the following:*

1.) *For each $x \in \mathbb{F}_{q^{2n}}$ we have*

$$x \in \bigcap_{i=1}^{m} \{B_{\mu_i}(y) : y \in \mathbb{F}_{q^{2n}}\} \Longleftrightarrow \mathrm{Tr}(\mu_1\gamma x) = \cdots = \mathrm{Tr}(\mu_m\gamma x) = 0.$$

2.) *$V = G_{\mu_1} \cap \cdots \cap G_{\mu_m}$ is an $\mathbb{F}_q$-linear subspace of codimension m in G.*

3.) *For the monic q-additive polynomial $B_V \in \mathbb{F}_{q^n}[T]$ of degree q^m defined in Theorem 3.12, we have*

$$x \in \{B_V(y) : y \in \mathbb{F}_{q^{2n}}\} \Longleftrightarrow \mathrm{Tr}(\mu_1\gamma x) = \cdots = \mathrm{Tr}(\mu_m\gamma x) = 0.$$

Proof. The proof of item 1.) follows directly from Lemma 3.13. Next we consider items 2.) and 3.). Assume that the codimension of V in G is $\bar{m}$. Then the monic q-additive polynomial $B_V \in \mathbb{F}_{q^n}[T]$ defined in Theorem 3.12 is of degree $q^{\bar{m}}$. It is clear that $\bar{m} \le m$. If we have the inclusion below

$$\{B_V(y) : y \in \mathbb{F}_{q^{2n}}\} \subseteq \bigcap_{i=1}^{m} \{B_{\mu_i}(y) : y \in \mathbb{F}_{q^{2n}}\}, \tag{3.2}$$

then the codimension of $\{B_V(y) : y \in \mathbb{F}_{q^{2n}}\}$ in $\mathbb{F}_{q^{2n}}$ is greater or equal to m. As the degree of B_V is $q^{\bar{m}}$, we also have that the codimension of $\{B_V(y) : y \in \mathbb{F}_{q^{2n}}\}$ in $\mathbb{F}_{q^{2n}}$ is smaller or equal to $\bar{m}$. Therefore if (3.2) holds, then $m \le$ codimension of $\{B_V(y) : y \in \mathbb{F}_{q^{2n}}\} \le \bar{m}$ and hence $m = \bar{m}$. Moreover (3.2) also implies that $\{B_V(y) : y \in \mathbb{F}_{q^{2n}}\} = \bigcap_{i=1}^{m} \{B_{\mu_i}(y) : y \in \mathbb{F}_{q^{2n}}\}$. So we just have to prove (3.2). As in the proof of Theorem 3.12, for $1 \le i \le m$ there exists a uniquely determined monic q-additive polynomial $D_i \in \mathbb{F}_{q^{2n}}[T]$ such that $B_V = B_{\mu_i} \circ D_i$. This implies that $\{B_V(y) : y \in \mathbb{F}_{q^{2n}}\} \subseteq \{B_{\mu_i}(y) : y \in \mathbb{F}_{q^{2n}}\}$ for each $1 \le i \le m$, and this proves the inclusion in (3.2). Using Proposition 3.2 we further get that $B_V \in \mathbb{F}_{q^n}[T]$, and hence we have completed the proof. □

Remark 3.15. Using Theorem 2.3, Theorem 3.12 and Theorem 3.14, we obtain that all maximal function fields of the form (1.1) are Galois subfields of the Hermitian function field. There is a correspondence between the maximal function fields of the form (1.1) and the $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_{q^n}$. Fixing a root γ of $T^{q^n} + T$, any maximal function field of the form (1.1) determines an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^n}$ spanned by $\{c_1, \dots, c_m\} \subseteq \mathbb{F}_{q^n}$ satisfying (3.1) (cf. Theorem 2.3, Remarks 2.2 and 2.6). Again fixing a root γ of $T^{q^n} + T$ we have conversely that any $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^n}$ determines a maximal function field of the form (1.1) (cf. Lemma 3.9, Theorems 3.12 and 3.14).

Remark 3.16. Note that our results improve and complete Theorem 7 of [G-K-M]. Apart from giving explicit equations for the maximal function fields in (1.1), we do not assume here that the additive q-polynomial $A(T)$ has its coefficients in $\mathbb{F}_{q^n}$; rather, this is a result that we prove here in Proposition 3.2.

The correspondence of Remark 3.15 is not one-to-one. In the next theorem we give a sufficient condition which implies the existence of distinct $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_{q^n}$ corresponding to the same maximal function field.

For $\mu \in \mathbb{F}_{q^n} \setminus \{0\}$, we note that

$$B_\mu(T) = \prod_{c \in \mathbb{F}_q} \left(T - \frac{c}{(\mu\gamma)^{\frac{1}{q}}} \right). \tag{3.3}$$

Theorem 3.17. *Let $\{\mu_1, \dots, \mu_m\}$, $\{\nu_1, \dots, \nu_m\} \subseteq \mathbb{F}_{q^n}$ be two $\mathbb{F}_q$-linearly independent sets. If there exists a nonzero element α in $\mathbb{F}_{q^n}$ such that the $\mathbb{F}_q$-linear subspaces spanned by $\{\alpha\mu_1, \cdots, \alpha\mu_m\}$ and by $\{\nu_1, \dots, \nu_m\}$ are the same, then the corresponding maximal function fields of $\{\mu_1, \dots, \mu_m\}$ and of $\{\nu_1, \dots, \nu_m\}$ are the same. If m belongs to $\{1, n-1\}$, then for any two $\mathbb{F}_q$-linearly independent subsets of size m in $\mathbb{F}_{q^n}$, there exists such a nonzero element α in $\mathbb{F}_{q^n}$. Hence the maximal functions fields of the form (1.1) are uniquely determined when $m \in \{1, n-1\}$.*

Proof. Let $U = \bigcap_{i=1}^m G_{\mu_i}$ and $V = \bigcap_{i=1}^m G_{\nu_i}$. The subgroups U and V are $\mathbb{F}_q$-linear subspaces of codimension m in G (cf. Theorem 3.14). The fixed subfields of H corresponding to U and V are $\mathbb{F}_{q^{2n}}(X, Y_1, \dots, Y_m)$ and $\mathbb{F}_{q^{2n}}(X, Z_1, \dots, Z_m)$ respectively, where for $1 \le i \le m$

$$X^{q^n+1} = \prod_{c \in \mathbb{F}_q} \left(Y_i - \frac{c}{(\mu_i\gamma)^{1/q}} \right), \text{ and } X^{q^n+1} = \prod_{c \in \mathbb{F}_q} \left(Z_i - \frac{c}{(\nu_i\gamma)^{1/q}} \right)$$

(cf. Theorem 3.12 and (3.3)). Let W_1 and W_2 be the $\mathbb{F}_q$-linear spaces spanned by $\{\mu_1, \dots, \mu_m\}$ and $\{\nu_1, \dots, \nu_m\}$ respectively. Assume that there exists $\alpha \in \mathbb{F}_{q^n} \setminus \{0\}$

such that $W_2 = \{\alpha w : w \in W_1\}$. Let $\beta \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that $\beta^{q^n+1} = \alpha$, $\bar{X} = \dfrac{X}{\beta} \in \mathbb{F}_{q^{2n}}(X)$ and $\bar{Y}_i = \dfrac{Y_i}{\alpha^{1/q}} \in \mathbb{F}_{q^{2n}}(X, Y_1, \dots, Y_m)$ for $1 \le i \le m$. Then we have $\mathbb{F}_{q^{2n}}(X, Y_1, \dots, Y_m) = \mathbb{F}_{q^{2n}}(\bar{X}, \bar{Y}_1, \dots, \bar{Y}_m)$, where

$$\bar{X}^{q^n+1} = \prod_{c \in \mathbb{F}_q} \left(\bar{Y}_i - \frac{c}{(\alpha\mu_i\gamma)^{\frac{1}{q}}} \right) = B_{\alpha\mu_i}(\bar{Y}_i), \text{ for } 1 \le i \le m.$$

As $W_2 = \{\alpha w : w \in W_1\}$, we also have $\mathbb{F}_{q^{2n}}(\bar{X}, \bar{Y}_1, \dots, \bar{Y}_m) = \mathbb{F}_{q^{2n}}(X, Z_1, \dots, Z_m)$. It remains to prove the assertions for the case $m \in \{1, n-1\}$. For an $\mathbb{F}_q$-linear subspace W in $\mathbb{F}_{q^n}$ of dimension m with $1 \le m \le n-1$, let A be the polynomial $A = \prod_{w \in W}(T - w)$ in $\mathbb{F}_{q^n}[T]$. For $\alpha \in \mathbb{F}_{q^n} \setminus \{0\}$, the set $\overline{W} = \{\alpha w : w \in W\}$ is also an $\mathbb{F}_q$-linear subspace of dimension m in $\mathbb{F}_{q^n}$. Similarly let $\overline{A}$ be the monic q-additive polynomial $\overline{A} = \prod_{\bar{w} \in \overline{W}}(T - \bar{w})$ in $\mathbb{F}_{q^n}[T]$. Note that $W = \overline{W}$ if and only if $A = \overline{A}$. Since A is a monic q-additive polynomial we have $A = T^{q^m} + a_{m-1}T^{q^{m-1}} + \cdots + a_q T^q + a_0 T$, where $a_0, \dots, a_{m-1} \in \mathbb{F}_{q^n}$. Moreover A is separable and hence $a_0 \neq 0$. By definition of $\overline{W}$ and $\overline{A}$, we have $\overline{A}(T) = \alpha^{q^m} A\left(\frac{T}{\alpha}\right)$ and hence $\overline{A} = T^{q^m} + \alpha^{q^m - q^{m-1}} a_{m-1} T^{q^{m-1}} + \cdots + \alpha^{q^m-1} a_0 T$. If $W = \overline{W}$ then $A = \overline{A}$, hence $\alpha^{q^m-1} a_0 = a_0$ and then $\alpha \in \mathbb{F}_{q^m}$ as $a_0 \neq 0$. This implies that for $1 \le m \le n-1$ with $\gcd(m,n) = 1$, if $W = \overline{W}$ then $\alpha \in \mathbb{F}_q = \mathbb{F}_{q^n} \cap \mathbb{F}_{q^m}$. Hence for $1 \le m \le n-1$ with $\gcd(m,n) = 1$, $W = \overline{W}$ if and only if $\alpha \in \mathbb{F}_q \setminus \{0\}$. For $1 \le m \le n-1$, let S_m denote the set of all distinct $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_{q^n}$ of dimension m. The multiplicative group $\mathbb{F}_{q^n} \setminus \{0\}$ acts on S_m and the action of $\alpha \in \mathbb{F}_{q^n} \setminus \{0\}$ is

$$W \in S_m \mapsto \overline{W} = \{\alpha w : w \in W\} \in S_m. \tag{3.4}$$

It follows from the discussion above that in the cases $m = 1$ and $m = n-1$, each orbit of this action on S_m has size $\frac{q^n-1}{q-1}$. Moreover if m is 1 or $n-1$, then the size of S_m is also $\frac{q^n-1}{q-1}$. Hence this action in (3.4) is transitive if m is 1 or $n-1$, which completes the proof. □

Corollary 3.18. *The function fields $\mathbb{F}_{q^{2n}}(X,Y)$ with $X^{q^n+1} = A(Y)$, where*

$$\gamma A(Y) = \gamma Y^q - \gamma^{\frac{1}{q}} Y \ \text{ or } \ \gamma A(Y) = \gamma Y^{q^{n-1}} + \gamma^{\frac{1}{q}} Y^{q^{n-2}} + \cdots + \gamma^{\frac{1}{q^{n-2}}} Y^q + \gamma^{\frac{1}{q^{n-1}}} Y$$

are the only maximal function fields of the form (1.1) if $m = 1$ or $m = n-1$, respectively.

Proof. For $m = 1$ it is enough to observe that

$$x \in \left\{ y^q - \gamma^{\frac{1}{q}-1} y : y \in \mathbb{F}_{q^{2n}} \right\} \iff \mathrm{Tr}(\gamma x) = 0$$

(cf. Lemma 3.13). Similarly for $m = n - 1$ we have

$$x \in \left\{ y^{q^{n-1}} + \gamma^{\frac{1}{q}-1} y^{q^{n-2}} + \cdots + \gamma^{\frac{1}{q^{n-2}}-1} y^{q} + \gamma^{\frac{1}{q^{n-1}}-1} y : y \in \mathbb{F}_{q^{2n}} \right\}$$
$$\Longleftrightarrow \operatorname{Tr}(c\gamma x) = 0 \text{ for each } c \text{ satisfying } c + c^{q} + \cdots + c^{q^{n-1}} = 0,$$

which completes the proof. □

Remark 3.19. Consider the case $m = n - 1$ in Corollary 3.18 ; i.e., consider the maximal function field F over $\mathbb{F}_{q^{2n}}$ given by the equation

$$\gamma X^{1+q^{n}} = \gamma Y^{q^{n-1}} + \gamma^{1/q} Y^{q^{n-2}} + \ldots + \gamma^{1/q^{n-2}} Y^{q} + \gamma^{1/q^{n-1}} Y.$$

Setting $Y_1 = \gamma^{1/q^{n-1}} Y$ we have that $F = \mathbb{F}_{q^{2n}}(X, Y_1)$ with the relation $Y_1^{q^{n-1}} + Y_1^{q^{n-2}} + \ldots + Y_1^{q} + Y_1 = \gamma X^{1+q^{n}}$. The uniqueness result about this function field F given in Corollary 3.18 also follows from Theorem 5.11 of [A-G]. Here the proof is much simpler since we assume that the function field F is of the form (1.1), which essentially says that the extension $F/\mathbb{F}_{q^{2n}}(X)$ is a Galois extension (see also Theorem 4.10 of [A-G]).

Acknowledgments

The first author acknowledges the support from CNPq-Brazil (# 304628/2003) and from PRONEX (CNPq-FAPERJ).The second author acknowledges the partial support from the Turkish Academy of Sciences in the framework of the Young Scientists Award Programme (F.Ö./TÜBA-GEBIP/2003-13).

References

[A-G] M. Abdon and A. Garcia, "On a characterization of certain maximal curves", *Finite Fields Appl.*, vol. 10, pp. 133-158, 2004.

[B] J. Bierbrauer, "The theory of cyclic codes and a generalization to additive codes", *Des. Codes Cryptogr.*, vol. 25, pp. 189-206, 2002.

[G-K-M] A. Garcia, M. Q. Kawakita and S. Miura, "On certain subcovers of the Hermitian curve", *Comm. Algebra*, to appear.

[G-S-X] Garcia,A., Stichtenoth,H. , and Xing,C.P.: "On subfields of the Hermitian function field", *Compositio Math.*, vol. 120, pp. 137-170, 2000.

[H] J. W. P. Hirschfeld, Projective Geometries over Finite Fields, Oxford University Press, New York, 1998.

[L-N] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.

[N-X] H. Niederreiter and C. Xing, Rational Points on Curves over Finite Fields, Cambridge University Press, 2001.

[R-S] H.-G. Rück and H. Stichtenoth, "A characterization of Hermitian function fields over finite fields", *J. Reine Angew. Math.*,vol. 457, pp. 185-188, 1994.

[S] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, Berlin, 1993.

[T-V] M. Tsfasman and S. Vladuts, Algebraic-Geometric Codes, Kluwer Academic, Dordrecht, 1991.