Available online at www.sciencedirect.com
ScienceDirect
Journal of Pure and Applied Algebra 210 (2007) 113–135
JOURNAL OF PURE AND APPLIED ALGEBRA
www.elsevier.com/locate/jpaa

Some Artin–Schreier type function fields over finite fields with prescribed genus and number of rational places

Emrah Çakçak[a,1], Ferruh Özbudak[b,*]

[a] *Institute of Applied Mathematics, Middle East Technical University, İnönü Bulvarı, 06531, Ankara, Turkey*
[b] *Department of Mathematics, Middle East Technical University, İnönü Bulvarı, 06531, Ankara, Turkey*

Received 20 September 2005; received in revised form 13 June 2006
Available online 20 September 2006
Communicated by J. Walker

Abstract

We give existence and characterization results for some Artin–Schreier type function fields over finite fields with prescribed genus and number of rational places simultaneously.

MSC: 11G20; 14G05; 14G50

1. Introduction

Let $\mathbb{F}_q$ be a finite field of characteristic p with q elements. Let E be an algebraic function field and assume that $\mathbb{F}_q$ is its full constant field. Hasse–Weil inequality states that for the number of rational places $N(E)$ we have

$$q + 1 - 2g(E)q^{1/2} \leq N(E) \leq q + 1 + 2g(E)q^{1/2},$$

where $g(E)$ is the genus of E. E is called *maximal* or *minimal* if $N(E)$ is $q + 1 + 2g(E)q^{1/2}$ or $q + 1 - 2g(E)q^{1/2}$ respectively. Note that for $g(E) \geq 1$, if E is maximal or minimal, then $q^{1/2}$ is an integer. Let $n \geq 1$, $h \geq 0$ and

$$S(X) = s_0X + s_1X^q + \cdots + s_hX^{q^h} \in \mathbb{F}_{q^{2n}}[X]$$

be an $\mathbb{F}_q$-linearized polynomial of degree q^h in $\mathbb{F}_{q^{2n}}[X]$. Let F be the algebraic function field over $\mathbb{F}_{q^{2n}}$ given as

$$F = \mathbb{F}_{q^{2n}}(u, v) \quad \text{with } v^q - v = uS(u). \tag{1.1}$$

* Corresponding author.
E-mail addresses: cakcak@metu.edu.tr (E. Çakçak), ozbudak@metu.edu.tr (F. Özbudak).
[1] This paper was written while this author was visiting Institut de Mathématiques de Luminy, CNRS, Marseille, France.

0022-4049/$ - see front matter
doi:10.1016/j.jpaa.2006.08.007

For q even, we further assume that $h \geq 1$. Since the full constant field of F is $\mathbb{F}_{q^{2n}}$, throughout the paper a rational place of F means an $\mathbb{F}_{q^{2n}}$-rational place of F. Using [9, Proposition 3.7.10], we obtain that the genus $g(F)$ of F is

$$g(F) = \frac{q-1}{2}(-2 + (q^h + 2)) = \frac{(q-1)q^h}{2}.$$

Recall that the Hermitian function field H over $\mathbb{F}_{q^{2n}}$ is

$$H = \mathbb{F}_{q^{2n}}(x, y) \quad \text{with } y^{q^n} + y = x^{q^n+1}. \tag{1.2}$$

Algebraic function fields over finite fields have many applications to coding theory and related areas [7,9,10]. In this paper we systematically study the Artin–Schreier type function fields of the form (1.1). We prove the existence of a large class of function fields in this form with prescribed genus g and number N of rational places simultaneously, where the tuple (g, N) satisfies

$$(g, N) = \left(\frac{(q-1)q^{\hat{h}}}{2}, q^{2n} + 1 \mp (q-1)q^{n+\frac{\hat{k}}{2}} \right),$$

for an integer $0 \leq \hat{h}$ and an even integer $0 \leq \hat{k} \leq 2\hat{h}$. We give characterizations of all function fields in the form (1.1) whose number of rational places is distinct from $q^{2n} + 1$. In particular, we prove the existence of maximal and minimal function fields of the form (1.1) for each possible genus and show how to construct them. Moreover if F is maximal, then we prove that F is a subfield of H, the extension H/F is Galois and we determine its Galois group $\mathrm{Aut}(H/F)$ explicitly. Some of our results generalize some results of [2], which correspond the case of $q = 2$.

In Section 2, using some results from [6], we give some properties of a corresponding quadratic form (cf. (2.1)). Using the results of Section 2, we determine the number of rational places of F in Section 3. We give the existence of some special classes of function fields in Section 4. An important idea of the paper is in Section 5. Under natural conditions we prove the existence of a degree q extension of F, which is also in the form (1.1) and is of the same type as F with respect to Theorem 3.1 of Section 3. In particular if F is minimal or maximal, then we even give an algorithm for constructing such a degree q extension $F(t)$ of F, which is minimal or maximal respectively. Using these degree q extensions inductively and the special classes of function fields obtained in Section 4, we obtain our existence results and some of our characterization results. We also give concrete examples illustrating our results. In Section 6, we show that these degree q extensions and their compositions are Galois extensions of F if $N(F) > q^{2n}+1$ and we determine the Galois group of the composed extensions with respect to F. We also prove that if F is maximal, then F is a subfield of H, the extension H/F is Galois and we obtain the Galois group $\mathrm{Aut}(H/F)$ explicitly.

Throughout the paper $\mathrm{Tr}(\cdot)$ will denote the trace map from $\mathbb{F}_{q^{2n}}$ to $\mathbb{F}_q$, i.e. for $a \in \mathbb{F}_{q^{2n}}$, $\mathrm{Tr}(a) = a + a^q + \cdots + a^{q^{2n-1}}$. We begin with an observation on the number $N(F)$. We note that $N(F) = 1 + q|V_S|$, where $V_S = \{a \in \mathbb{F}_{q^{2n}} : \mathrm{Tr}(aS(a)) = 0\}$ (see the proof of Theorem 3.1). In the next section we will consider the corresponding quadratic form $a \in \mathbb{F}_{q^{2n}} \mapsto \mathrm{Tr}(aS(a)) \in \mathbb{F}_q$.

2. A quadratic form

Let B_S be a symmetric $\mathbb{F}_q$-bilinear form on $\mathbb{F}_{q^{2n}}$ given by

$$\begin{aligned} B_S : \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} &\to \mathbb{F}_q \\ (a, b) &\mapsto \mathrm{Tr}(aS(b) + bS(a)). \end{aligned}$$

B_S is alternating if q is even. Let

$$\begin{aligned} Q_S : \mathbb{F}_{q^{2n}} &\to \mathbb{F}_q \\ a &\mapsto \mathrm{Tr}(aS(a)). \end{aligned} \tag{2.1}$$

Note that Q_S is a quadratic form attached to B_S satisfying $Q_S(\lambda a) = \lambda^2 Q_S(a)$ and

$$B_S(a, b) = Q_S(a + b) - Q_S(a) - Q_S(b)$$

for each $a, b \in \mathbb{F}_{q^{2n}}$ and $\lambda \in \mathbb{F}_q$. In this section we will give some properties of the quadratic form Q_S. Let W_S be the radical of B_S:

$$W_S = \{a \in \mathbb{F}_{q^{2n}} : B_S(a, b) = 0 \text{ for each } b \in \mathbb{F}_{q^{2n}}\}.$$

W_S is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^{2n}}$ and we have:

Lemma 2.1. *W_S consists of the roots of the polynomial*

$$\sum_{i=0}^{h-1} s_{h-i}^{q^i} T^{q^i} + 2s_0^{q^h} T^{q^h} + \sum_{i=1}^{h} s_i^{q^h} T^{q^{h+i}} \in \mathbb{F}_{q^{2n}}[T]$$

in $\mathbb{F}_{q^{2n}}$ and we have $\dim W_S \leq 2h$.

Proof. From the properties of the trace function it follows that $\mathrm{Tr}(aS(b) + bS(a)) = \mathrm{Tr}\left(b\left\{\sum_{i=0}^{h}(s_i a)^{q^{-i}} + \sum_{i=0}^{h} s_i a^{q^i}\right\}\right)$, for any $a, b \in \mathbb{F}_{q^{2n}}$. Hence for any $a \in W_S$, we have $\sum_{i=0}^{h}(s_i a)^{q^{-i}} + \sum_{i=0}^{h} s_i a^{q^i} = 0$ or equivalently

$$\sum_{i=0}^{h}(s_i a)^{q^{h-i}} + \sum_{i=0}^{h}(s_i a^{q^i})^{q^h} = 0. \tag{2.2}$$

We complete the proof observing that the polynomial in (2.2) is of degree q^{2h}. □

Throughout the paper, k denotes the $\mathbb{F}_q$-dimension

$$k = \dim W_S$$

of the $\mathbb{F}_q$-linear space W_S. Recall that V_S is the subset of $\mathbb{F}_{q^{2n}}$ defined as

$$V_S = \{a \in \mathbb{F}_{q^{2n}} : Q_S(a) = 0\}.$$

Observe that when q is odd, we have $Q_S(a) = \frac{1}{2}B_S(a, a)$ for any $a \in \mathbb{F}_{q^{2n}}$ and hence $W_S \subseteq V_S$.

Definition 2.2. Let $\mathcal{V}$ be a vector space over $\mathbb{F}_q$ of dimension m. Let $\mathcal{B}$ be a symmetric $\mathbb{F}_q$-bilinear form on $\mathcal{V}$ and $\mathcal{Q}$ a quadratic form attached to $\mathcal{B}$ satisfying $\mathcal{Q}(a+b) = \mathcal{B}(a, b) + \mathcal{Q}(a) + \mathcal{Q}(b)$ and $\mathcal{Q}(\lambda a) = \lambda^2 \mathcal{Q}(a)$, for each $a, b \in \mathcal{V}$, $\lambda \in \mathbb{F}_q$. For an $\mathbb{F}_q$-basis $\mathcal{E} = \{e_1, \ldots, e_m\}$ of $\mathcal{V}$, we define *the polynomial representing the quadratic form $\mathcal{Q}$ with respect to the basis $\mathcal{E}$* as the polynomial $f_{\mathcal{E}} \in \mathbb{F}_q[X_1, \ldots, X_m]$ with quadratic terms:

$$f_{\mathcal{E}}(X_1, \ldots, X_m) = \sum_{1 \leq i \leq m} f_{i,i} X_i^2 + \sum_{1 \leq i < j \leq m} f_{i,j} X_i X_j,$$

where $f_{i,i} = \mathcal{Q}(e_i)$, $1 \leq i \leq m$ and $f_{i,j} = \mathcal{B}(e_i, e_j)$, $1 \leq i < j \leq m$. Indeed, for each $(a_1, \ldots, a_m) \in \mathbb{F}_q^m$ we have

$$f_{\mathcal{E}}(a_1, \ldots, a_m) = \mathcal{Q}(a_1 e_1 + \cdots + a_m e_m). \tag{2.3}$$

Moreover, $f_{\mathcal{E}}$ is the unique polynomial with quadratic terms satisfying (2.3) for each $(a_1, \ldots, a_m) \in \mathbb{F}_q^m$. It is easy to observe also that if $\mathcal{B}$ is nondegenerate on $\mathcal{V}$ then there is no basis $\mathcal{E}$ of $\mathcal{V}$ such that $f_{\mathcal{E}}$ is expressible in less than m variables.

Recall that k is the dimension of W_S as a vector space over $\mathbb{F}_q$.

Proposition 2.3. *Assume that q is odd. There is an $\mathbb{F}_q$-basis $\mathcal{E}$ of $\mathbb{F}_{q^{2n}}$ and $d \in \mathbb{F}_q \setminus \{0\}$ such that the polynomial f_ϵ representing Q_S with respect to $\mathcal{E}$ (cf. Definition 2.2) is*

$$\frac{1}{2}(X_1^2 + X_2^2 + \cdots + X_{2n-k-1}^2 + dX_{2n-k}^2). \tag{2.4}$$

Proof. If $k = 2n$, then $f_{\mathcal{E}}$ is the zero polynomial and the statement holds trivially. Assume that $k < 2n$. Let $\overline{W}_S$ be an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^{2n}}$ such that $W_S \cap \overline{W}_S = \{0\}$ and $\dim \overline{W}_S = 2n - k$. We have $\mathbb{F}_{q^{2n}} = W_S \oplus \overline{W}_S$ as vector spaces over $\mathbb{F}_q$. Let $\overline{B}_S$ and $\overline{Q}_S$ be the restrictions of B_S and Q_S respectively, onto $\overline{W}_S$. Then $\overline{B}_S$ is a nondegenerate symmetric bilinear form on $\overline{W}_S$ and $\overline{Q}_S$ is a quadratic form attached to $\overline{B}_S$, where $\overline{B}_S(a, b) = \overline{Q}_S(a + b) - \overline{Q}_S(a) - \overline{Q}_S(b)$ for $a, b \in \overline{W}_S$. For an $\mathbb{F}_q$-basis, $\bar{\mathcal{E}}$, of $\overline{W}_S$, let $\bar{f}_{\bar{\mathcal{E}}}$ denote the polynomial representing $\overline{Q}_S$ with respect to $\bar{\mathcal{E}}$. As $\overline{B}_S$ is nondegenerate, it follows from [3, Theorem 4.9] that there exists an $\mathbb{F}_q$-basis $\bar{\mathcal{E}} = \{e_1, \ldots, e_{2n-k}\}$ of $\overline{W}_S$ and $d \in \mathbb{F}_q \setminus \{0\}$ such that $\bar{f}_{\bar{\mathcal{E}}}$ is given by (2.4). Let $\{e_{2n-k+1}, \ldots, e_{2n}\}$ be an $\mathbb{F}_q$-basis of W_S. Then $\mathcal{E} = \{e_1, \ldots, e_{2n}\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{2n}}$ and it easily follows that the polynomial representing Q_S with respect to $\mathcal{E}$ is equal to $\bar{f}_{\bar{\mathcal{E}}}$ considered as a polynomial in $\mathbb{F}_q[X_1, \ldots, X_{2n}]$. □

Proposition 2.4. *Assume that q is even. We have that k is even. Moreover if $W_S \subseteq V_S$, then there is an $\mathbb{F}_q$-basis $\mathcal{E}$ of $\mathbb{F}_{q^{2n}}$ such that the polynomial f_ϵ representing Q_S with respect to $\mathcal{E}$ (cf. Definition 2.2) is either*

$$X_1X_2 + X_3X_4 + \cdots + X_{2n-k-1}X_{2n-k} \tag{2.5}$$

or

$$X_1X_2 + X_3X_4 + \cdots + X_{2n-k-1}X_{2n-k} + X_{2n-k-1}^2 + dX_{2n-k}^2 \tag{2.6}$$

where $d \in \mathbb{F}_q$ satisfies $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(d) = d + d^2 + d^4 + \cdots + d^{\frac{q}{2}} = 1$.

Proof. As in the proof of Proposition 2.3 we assume that $k < 2n$ without loss of generality. Moreover we define $\overline{W}_S$, $\overline{B}_S$ and $\overline{Q}_S$ similarly. Note that $\overline{B}_S$ is a nondegenerate, symmetric and alternating bilinear from on $\overline{W}_S$ and q is even. Then it follows from [3, Corollary 2.11] that $\dim \overline{W}_S$ and so k are even integers. For an $\mathbb{F}_q$-basis, $\bar{\mathcal{E}}$, of $\overline{W}_S$, let $\bar{f}_{\bar{\mathcal{E}}}$ denote the polynomial representing $\overline{Q}_S$ with respect to $\bar{\mathcal{E}}$. It follows from Definition 2.2 that there is no basis $\bar{\mathcal{E}}$ of $\overline{W}_S$ such that $\bar{f}_{\bar{\mathcal{E}}}$ is expressible in less than $2n - k$ variables. Using [6, Theorem 6.30] we obtain that there is a basis $\bar{\mathcal{E}}$ of $\overline{W}_S$ such that $\bar{f}_{\bar{\mathcal{E}}}$ is either given by (2.5) or by (2.6) where d $\in \mathbb{F}_q$ satisfies $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(d) = 1$. As in the proof of Proposition 2.3, we complete the set $\bar{\mathcal{E}}$ to a basis $\mathcal{E}$ of $\mathbb{F}_{q^{2n}}$ by elements from W_S and using $W_S \subseteq V_S$, we obtain that the polynomial representing Q_S with respect to $\mathcal{E}$ is equal to $\bar{f}_{\bar{\mathcal{E}}}$ considered as a polynomial in $\mathbb{F}_q[X_1, \ldots, X_{2n}]$. □

3. Number of rational places of F

In this section, using the results of Section 2, we determine the number of rational places of F (defined by (1.1)) in terms of the dimension of the radical W_S and the zeros of the quadratic form Q_S.

For an $\mathbb{F}_q$-basis, $\mathcal{E}$, of $\mathbb{F}_{q^{2n}}$, let $f_{\mathcal{E}}(X_1, \ldots, X_{2n})$ denote the polynomial representing Q_S with respect to $\mathcal{E}$.

Theorem 3.1. *The number of rational places of F is given as follows:*

(1) *Assume q is odd and let d be as in Proposition 2.3. We have:*
   (i) *If k is odd, then $N(F) = 1 + q^{2n}$.*
   (ii) *If k is even and $(-1)^{n-\frac{k}{2}}d$ is a square in $\mathbb{F}_q$ then $N(F) = 1 + q^{2n} + (q-1)q^{n+\frac{k}{2}}$.*
   (iii) *If k is even and $(-1)^{n-\frac{k}{2}}d$ is a nonsquare in $\mathbb{F}_q$ then $N(F) = 1 + q^{2n} - (q-1)q^{n+\frac{k}{2}}$.*

(2) *Assume q is even. We have:*
   (i) *If $W_S \not\subseteq V_S$ then $N(F) = 1 + q^{2n}$.*
   (ii) *If $W_S \subseteq V_S$ and there is an $\mathbb{F}_q$-basis, $\mathcal{E}$, of $\mathbb{F}_{q^{2n}}$ such that $f_{\mathcal{E}}$ is given by (2.5) in Proposition 2.4 then $N(F) = 1 + q^{2n} + (q-1)q^{n+\frac{k}{2}}$.*
   (iii) *If $W_S \subseteq V_S$ and there is an $\mathbb{F}_q$-basis, $\mathcal{E}$, of $\mathbb{F}_{q^{2n}}$ such that $f_{\mathcal{E}}$ is given by (2.6) in Proposition 2.4 then $N(F) = 1 + q^{2n} - (q-1)q^{n+\frac{k}{2}}$.*

Proof. There is only one rational place in F over the place at infinity of the function field $\mathbb{F}_{q^{2n}}(u)$. The other rational places of F correspond to the elements $a \in \mathbb{F}_{q^{2n}}$ satisfying $\mathrm{Tr}(a(S(a))) = 0$. Moreover for each $a \in \mathbb{F}_{q^{2n}}$ with $Q_S(a) = \mathrm{Tr}(a(S(a))) = 0$, there are q rational places in F, so that

$$N(F) = 1 + q|V_S|. \tag{3.1}$$

We first prove Case (2)(i). Assume that q is even and $W_S \not\subseteq V_S$. Let $\phi : W_S \to \mathbb{F}_q$ be the restriction of Q_S onto W_S. Then ϕ is an additive homomorphism and it follows from the assumptions that ϕ is surjective. Hence for any $\alpha \in \mathbb{F}_q$ we get

$$|\{x \in W_S : Q_S(x) = \alpha\}| = \frac{|W_S|}{q}. \tag{3.2}$$

Observe that for $a \in \mathbb{F}_{q^{2n}}$ and $x \in W_S$, $Q_S(x + a) = Q_S(x) + Q_S(a)$. Then for any coset $a + W_S$ of W_S in $\mathbb{F}_{q^{2n}}$ we have

$$|\{x \in a + W_S : Q_S(x) = 0\}| = |\{x \in W_S : Q_S(x) = Q_S(a)\}|. \tag{3.3}$$

Considering all disjoint cosets of W_S in $\mathbb{F}_{q^{2n}}$ and using (3.1)–(3.3), we complete the proof of Case (2)(i).

From here until the end of the proof we assume that if q is even, then $W_S \subseteq V_S$. Hence for the remaining cases, if $\alpha \in W_S$ then $Q_S(\alpha) = 0$.

Let $\overline{W}_S$ be an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^{2n}}$ such that $\mathbb{F}_{q^{2n}} = W_S \oplus \overline{W}_S$. For $a \in \mathbb{F}_{q^{2n}}$, let $a_1 \in W_S$ and $a_2 \in \overline{W}_S$ be the uniquely determined elements such that $a = a_1 + a_2$. As $a_1 \in W_S \subseteq V_S$ we have

$$Q_S(a) = Q_S(a_1) + B_S(a_1, a_2) + Q_S(a_2) = Q_S(a_2). \tag{3.4}$$

For q odd, let $d \in \mathbb{F}_q \setminus \{0\}$ and $\mathcal{E}$ be an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{2n}}$ such that the polynomial $f_{\mathcal{E}}(X_1, \ldots, X_{2n})$ is given by (2.4). For q even, let $\mathcal{E}$ be an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^{2n}}$ such that $f_{\mathcal{E}}(X_1, \ldots, X_{2n})$ is either given by (2.5) or by (2.6) with a corresponding $d \in \mathbb{F}_q$. Let $N(f_{\mathcal{E}}(X_1, \ldots, X_{2n-k}, 0, \ldots, 0))$ be the number of solutions of the equation

$$f_{\mathcal{E}}(X_1, \ldots, X_{2n-k}, 0, \ldots, 0) = 0$$

in $\mathbb{F}_q^{2n-k}$. Using (3.4) we obtain that

$$|V_S| = q^k N(f_{\mathcal{E}}(X_1, \ldots, X_{2n-k}, 0, \ldots, 0)). \tag{3.5}$$

If q is odd and k is odd, by [6, Theorem 6.27] we have

$$N(f_{\mathcal{E}}(X_1, \ldots, X_{2n-k}, 0, \ldots, 0)) = q^{2n-k-1}. \tag{3.6}$$

If q is odd and k is even, then by [6, Theorem 6.26] we have

$$N(f_{\mathcal{E}}(X_1, \ldots, X_{2n-k}, 0, \ldots, 0)) = \begin{cases} q^{2n-k-1} + (q-1)q^{n-k/2-1} & \text{if } (-1)^{n-k/2}d \text{ is a square in } \mathbb{F}_q, \\ q^{2n-k-1} - (q-1)q^{n-k/2-1} & \text{if } (-1)^{n-k/2}d \text{ is a nonsquare in } \mathbb{F}_q. \end{cases} \tag{3.7}$$

Using (3.1) and (3.5)–(3.7), we prove the cases in (1).

If q is even and $W_S \subseteq V_S$, then by [6, Theorem 6.32] we have

$$N(f_{\mathcal{E}}(X_1, \ldots, X_{2n-k}, 0, \ldots, 0)) = \begin{cases} q^{2n-k-1} + (q-1)q^{n-k/2-1} & \text{if (2.5) holds,} \\ q^{2n-k-1} - (q-1)q^{n-k/2-1} & \text{if (2.6) holds.} \end{cases} \tag{3.8}$$

Using (3.1), (3.5) and (3.8), we prove the remaining cases in (2). □

In the following corollaries, which are direct consequences of Theorem 3.1, we give maximality and minimality criteria for F. Recall that $k = \dim W_S$.

Corollary 3.2. *Assume that q is odd. Let $d \in \mathbb{F}_q \setminus \{0\}$ be as in Proposition 2.3. Then F is maximal if and only if $k = 2h$ and $(-1)^{n-h}d$ is a square in $\mathbb{F}_q$. Moreover F is minimal if and only if $k = 2h$ and $(-1)^{n-h}d$ is a nonsquare in $\mathbb{F}_q$. In particular if F is maximal or minimal, then $h \leq n$.*

Corollary 3.3. *Assume that q is even. Then F is maximal if and only if $W_S \subseteq V_S$, $k = 2h$ and (2.5) holds. Moreover F is minimal if and only if $W_S \subseteq V_S$, $k = 2h$ and (2.6) holds. In particular if F is maximal or minimal, then $h \leq n$.*

Lemma 3.4. *For any q, if $k = 2n$ then F cannot be of type Theorem 3.1(1)(iii) or (2)(iii). In particular, if $h = n$ there is no minimal function field F of the form (1.1).*

Proof. Otherwise $N(F) = 1 + q^{2n} - (q-1)q^{2n} = 1 - (q-2)q^{2n}$. This is already a contradiction for $q \geq 3$. If $q = 2$, this means that $N(F) = 1$, $|V_S| = 0$ and $|W_S| = q^{2n}$, which is a contradiction since $W_S \subseteq V_S$. □

4. Some examples

In this section we give existence results for some special function fields corresponding to Theorem 3.1(1)(ii), (1)(iii), (2)(ii) and (2)(iii). We begin with maximal and minimal function fields.

Lemma 4.1. *Assume that q is odd. Let $\mathcal{C}$ be the family of function fields*

$$\mathcal{C} = \{\mathbb{F}_{q^{2n}}(x, y) \text{ with } y^q - y = sx^2 : s \in \mathbb{F}_{q^{2n}} \setminus \{0\}\}.$$

Each function field in $\mathcal{C}$ is either maximal or minimal. Let M_+ and M_- denote the numbers of maximal and minimal function fields in $\mathcal{C}$ respectively. We have

$$M_+ = M_- = \frac{q^{2n} - 1}{2}.$$

Proof. For $s \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ and $S(X) = sX$ we have $W_S = \{0\}$. Using Theorem 3.1 we obtain that each function field in $\mathcal{C}$ is either maximal or minimal. Hence we have

$$M_+ + M_- = q^{2n} - 1. \tag{4.1}$$

By Hilbert's Theorem 90 we get

$$M_+ \frac{q^{2n} + (q-1)q^n}{q} + M_- \frac{q^{2n} - (q-1)q^n}{q} = M, \tag{4.2}$$

where $M = |\{(s, x) \in (\mathbb{F}_{q^{2n}} \setminus \{0\}) \times \mathbb{F}_{q^{2n}} : \mathrm{Tr}(sx^2) = 0\}|$. Indeed assume that $s \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that the function field $\mathbb{F}_{q^{2n}}(x, y)$ with $y^q - y = sx^2$ is maximal. Its genus is $\frac{q-1}{2}$ and hence its number of rational places is $1 + q^{2n} + (q-1)q^n$. Using Hilbert's Theorem 90 (cf. [9, Proposition VI.4.1]) we obtain that

$$|\{x \in \mathbb{F}_{q^{2n}} : \mathrm{Tr}(sx^2) = 0\}| = \frac{q^{2n} + (q-1)q^n}{q}.$$

Then considering all such $s \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ we have

$$|\{(s, x) \in M_+ \times \mathbb{F}_{q^{2n}} : \mathrm{Tr}(sx^2) = 0\}| = (M_+) \frac{q^{2n} + (q-1)q^n}{q}.$$

Similarly we get

$$|\{(s, x) \in M_- \times \mathbb{F}_{q^{2n}} : \mathrm{Tr}(sx^2) = 0\}| = (M_-) \frac{q^{2n} - (q-1)q^n}{q}.$$

Using (4.1) and the definition of M we obtain (4.2).

For $x = 0$ and any $s \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ we have $\mathrm{Tr}(sx^2) = 0$. For $x \in \mathbb{F}_{q^{2n}} \setminus \{0\}$, the number of $s \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that $\mathrm{Tr}(sx^2) = 0$ is $\frac{q^{2n}}{q} - 1$. Therefore we have

$$M = q^{2n} - 1 + (q^{2n} - 1)\left(\frac{q^{2n}}{q} - 1\right) = \frac{q^{2n} - 1}{q} q^{2n}. \tag{4.3}$$

Using (4.1)–(4.3) we complete the proof. □

Remark 4.2. There are only two $\mathbb{F}_{q^{2n}}$-isomorphism classes of fields in the family $\mathcal{C}$ of Lemma 4.1, each of size $(q^{2n} - 1)/2$. Indeed, let $F_1 = \mathbb{F}_{q^{2n}}(x, y)$ with $y^q - y = x^2$ and let $\mathbb{F}_\zeta = \mathbb{F}_{q^{2n}}(x, y)$ with $y^q - y = \zeta x^2$, where $\zeta \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ is a primitive element. For $s \in \mathbb{F}_{q^{2n}} \setminus \{0\}$, the function field $F_s = \mathbb{F}_{q^{2n}}(x, y)$ with $y^q - y = sx^2$ is $\mathbb{F}_{q^{2n}}$-isomorphic to F_1 or F_ζ if s is a square or not in $\mathbb{F}_{q^{2n}}$ respectively. The content of this remark is due to the anonymous referee.

For q even, there exists $s_1 \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that the polynomial $s_1^q T^{q^2} + s_1 T$ splits in $\mathbb{F}_{q^{2n}}$, for example $s_1 = 1$.

Lemma 4.3. *Assume that q is even and $s_1 \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that the polynomial $s_1^q T^{q^2} + s_1 T$ splits in $\mathbb{F}_{q^{2n}}$. Let $\mathcal{C}(s_1)$ be the family of function fields*

$$\mathcal{C}(s_1) = \{\mathbb{F}_{q^{2n}}(x, y) \text{ with } y^q - y = sx^2 + s_1 x^{q+1} : s \in \mathbb{F}_{q^{2n}}\}.$$

Each function field in $\mathcal{C}(s_1)$ is either maximal, minimal or otherwise has $q^{2n}+1$ many rational places. Let M_+, M_- and M_0 denote the numbers of the corresponding function fields in $\mathcal{C}(s_1)$ respectively. We have

$$M_+ = \frac{q^{2n-2} + q^{n-1}}{2}, \qquad M_- = \frac{q^{2n-2} - q^{n-1}}{2}, \qquad M_0 = q^{2n-2}(q^2 - 1).$$

Proof. Let $s \in \mathbb{F}_{q^{2n}}$ and $S(X) = sX + s_1 X^q$. By Lemma 2.1 we have $\dim W_S = 2$. Using Theorem 3.1 we obtain that either the corresponding function field in $\mathcal{C}(s_1)$ is maximal, minimal or otherwise has $q^{2n}+1$ many rational places. Then we have

$$M_0 + M_+ + M_- = q^{2n}, \tag{4.4}$$

and

$$\begin{aligned} &M_0 \frac{q^{2n}}{q} + M_+ \frac{q^{2n} + (q-1)q^{n+1}}{q} + M_- \frac{q^{2n} - (q-1)q^{n+1}}{q} \\ &= |\{(s, x) \in \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} : \mathrm{Tr}(sx^2 + s_1 x^{q+1}) = 0\}| \\ &= \frac{q^{2n}}{q}(q^{2n} + q - 1). \end{aligned} \tag{4.5}$$

Using (4.4) and (4.5) we obtain that $M_0 < q^{2n}$. Therefore there exists $s \in \mathbb{F}_{q^{2n}}$ such that for $S(X) = sX + s_1 X^q$ we have $W_S \subseteq V_S$. For $a \in \mathbb{F}_{q^{2n}}$, let $S_a(X) = (s+a)X + s_1 X^q$. For $a \in \mathbb{F}_{q^{2n}}$ we have $W_{S_a} = W_S$ and hence

$$W_{S_a} \subseteq V_{S_a} \iff \mathrm{Tr}(ax^2) = \left(\mathrm{Tr}(\sqrt{a}x)\right)^2 = 0 \quad \text{for each } x \in W_S.$$

The vector space $\mathrm{Hom}(W_S, \mathbb{F}_q)$ of $\mathbb{F}_q$-linear maps from W_S to $\mathbb{F}_q$ consists of the $\mathbb{F}_q$-linear maps sending $x \in W_S$ to $\mathrm{Tr}(ax)$ as a runs through $\mathbb{F}_{q^{2n}}$. Consider the $\mathbb{F}_q$-linear map

$$\begin{aligned} \mathcal{L} : \mathbb{F}_{q^{2n}} &\to \mathrm{Hom}(W_S, \mathbb{F}_q) \\ a &\mapsto L_a, \end{aligned}$$

where $L_a(x) = \mathrm{Tr}(\sqrt{a}x)$ for $x \in W_S$. Then $\mathcal{L}$ is onto and $\mathrm{Ker}\,\mathcal{L} = \{a \in \mathbb{F}_{q^{2n}} : W_{S_a} \subseteq V_{S_a}\}$. Therefore the number of elements $a \in \mathbb{F}_{q^{2n}}$ with $W_{S_a} \subseteq V_{S_a}$ is

$$\frac{|\mathbb{F}_{q^{2n}}|}{|\mathrm{Hom}(W_S, \mathbb{F}_q)|} = \frac{q^{2n}}{|W_S|} = q^{2n-2}.$$

This implies that

$$M_+ + M_- = q^{2n-2}. \tag{4.6}$$

Using (4.4)–(4.6) we complete the proof. □

We will prove the existence of maximal and minimal function fields for all possible cases of h later in Theorem 5.9 using Lemmas 4.1 and 4.3 and the results of Section 5.

Next we will show the existence of some special function fields corresponding to Theorem 3.1(1)(ii), (1)(iii), (2)(ii) and (2)(iii) with $k = 0$ and some $h \geq 1$. We begin with a technical lemma. For $h \geq 1$, let $\bar{h}$ be the integer defined as $\bar{h} = \gcd(h, n)$.

Lemma 4.4. *For $h \geq 1$ and $s \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ we consider the polynomial*

$$sT + s^{q^h} T^{q^{2h}} \in \mathbb{F}_{q^{2n}}[T]. \tag{4.7}$$

If q is odd and $h/\bar{h}$ is even, then for each $s \in \mathbb{F}_{q^{2n}} \setminus \{0\}$, the polynomial in (4.7) has no nonzero root in $\mathbb{F}_{q^{2n}}$. If q is even and $h/\bar{h}$ is odd, then there exists $s \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that the polynomial in (4.7) has no nonzero root in $\mathbb{F}_{q^{2n}}$.

Proof. Let ω be a generator of the multiplicative group of $\mathbb{F}_{q^{2n}}$ and $s = w^{\theta}$, where θ is an integer. Assume first that q is odd and $h/\bar{h}$ is even. We need to show that there is no integer l such that

$$w^{l(q^{2h}-1)} = \frac{w^{(q^{2n}-1)/2}}{w^{\theta(q^h-1)}},$$

which is equivalent to

$$l(q^{2h}-1) \equiv \frac{q^{2n}-1}{2} - \theta(q^h-1) \mod (q^{2n}-1). \tag{4.8}$$

Note that $\gcd(q^{2h}-1, q^{2n}-1) = q^{2\bar{h}}-1$. There exists a solution l of (4.8) if and only if

$$\theta(q^h-1) \equiv \frac{q^{2n}-1}{2} \mod (q^{2\bar{h}}-1). \tag{4.9}$$

As $h/\bar{h}$ is even, we have that $n/\bar{h}$ is odd and that $(q^{2\bar{h}}-1)$ divides (q^h-1). So (4.9) holds if and only if $(q^{2\bar{h}}-1)$ divides $\frac{q^{2n}-1}{2}$ which is not the case because

$$\frac{q^{2n}-1}{2} = (q^{2\bar{h}}-1)\frac{1+q^{2\bar{h}}+q^{2\bar{h}\cdot 2}+\cdots+q^{2\bar{h}\cdot(\frac{n}{\bar{h}}-1)}}{2}$$

where $n/\bar{h}$ and so the sum $1+q^{2\bar{h}}+q^{2\bar{h}\cdot 2}+\cdots+q^{2\bar{h}\cdot(\frac{n}{\bar{h}}-1)}$ is odd. This completes the proof of the first part.

Next we assume that q is even and $h/\bar{h}$ is odd. Using similar methods we reach that there exists a nonzero root of the polynomial (4.7) in $\mathbb{F}_{q^{2n}}$ if and only if

$$\theta(q^h-1) \equiv 0 \mod (q^{2\bar{h}}-1). \tag{4.10}$$

As $h/\bar{h}$ is odd, we have that $(q^{2\bar{h}}-1)$ does not divide (q^h-1). Therefore there exists an integer θ such that (4.10) does not hold. This completes the proof. □

Remark 4.5. With the notation of Lemma 4.4, using similar methods we also obtain the following related results:

If q is odd and $h/\bar{h}$ is odd, then the number of $s \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that the polynomial in (4.7) has a nonzero root in $\mathbb{F}_{q^{2n}}$ is $\frac{q^{2n}-1}{q^{2\bar{h}}-1}(q^{\bar{h}}-1)$. Moreover if θ_1 is an integer satisfying

$$\theta_1(q^h-1) \equiv \frac{q^{2n}-1}{2} \mod (q^{2\bar{h}}-1),$$

then the set of $s \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that the polynomial in (4.7) has a nonzero root is

$$\left\{\omega^{\theta_1+(q^{\bar{h}}+1)(i+j(q^{\bar{h}}-1))} : 0 \le i \le q^{\bar{h}}-2,\ 0 \le j \le \frac{q^{2n}-1}{q^{2\bar{h}}-1}-1\right\}.$$

If q is even and $h/\bar{h}$ is even, then for each $s \in \mathbb{F}_{q^{2n}} \setminus \{0\}$, the polynomial in (4.7) has a nonzero root in $\mathbb{F}_{q^{2n}}$.

For both the cases that q is odd and q is even, if the polynomial in (4.7) has a nonzero root in $\mathbb{F}_{q^{2n}}$, then its exact number of roots in $\mathbb{F}_{q^{2n}}$ is $q^{2\bar{h}}$.

We use Lemma 4.4 in the following propositions of this section.

Proposition 4.6. *For q odd and $h \ge 1$, let $\mathcal{C}$ be the family of function fields*

$$\mathcal{C} = \left\{\mathbb{F}_{q^{2n}}(x,y) \text{ with } y^q - y = sx^{q^h+1} : s \in \mathbb{F}_{q^{2n}} \setminus \{0\}\right\}.$$

Assume that $h/\bar{h}$ is even. Then for each function field in $\mathcal{C}$, its number of rational places is either

$$q^{2n}+1+(q-1)q^n, \quad \text{or} \quad q^{2n}+1-(q-1)q^n. \tag{4.11}$$

Let $M_{0,+}$ and $M_{0,-}$ denote the numbers of function fields in $\mathcal{C}$ with the corresponding numbers of rational places in (4.11) respectively. We have

$$M_{0,+}=M_{0,-}=\frac{q^{2n}-1}{2}.$$

Proof. For $S(T)=sT^{q^h}$ with $s\in\mathbb{F}_{q^{2n}}\setminus\{0\}$, it follows from Lemmas 2.1 and 4.4 that $\dim W_S=0$. Hence using Theorem 3.1 we obtain that for each function field in $\mathcal{C}$, its number of rational places is either $q^{2n}+1+(q-1)q^n$ or $q^{2n}+1-(q-1)q^n$. Then we have

$$M_{0,+}+M_{0,-}=q^{2n}-1. \tag{4.12}$$

Using Hilbert's Theorem 90 we get

$$M=M_{0,+}\frac{q^{2n}+(q-1)q^n}{q}+M_{0,-}\frac{q^{2n}-(q-1)q^n}{q}, \tag{4.13}$$

where $M=|\{(s,x)\in(\mathbb{F}_{q^{2n}}\setminus\{0\})\times\mathbb{F}_{q^{2n}}:\mathrm{Tr}(sx^{q^h+1})=0\}|=\frac{q^{2n}-1}{q}q^{2n}$. Using (4.12) and (4.13) we complete the proof. □

Remark 4.7. As in Remark 4.2, if $h/\bar{h}$ is even, there are two $\mathbb{F}_{q^{2n}}$-isomorphism classes of fields in the family $\mathcal{C}$ in Proposition 4.6, each of the same size $(q^{2n}-1)/2$. The function fields $F_1=\mathbb{F}_{q^{2n}}(x,y)$ with $y^q-y=x^{q^h+1}$ and $\mathbb{F}_\zeta=\mathbb{F}_{q^{2n}}(x,y)$ with $y^q-y=\zeta x^{q^h+1}$, where $\zeta\in\mathbb{F}_{q^{2n}}\setminus\{0\}$ is a primitive element, are two representative function fields of these isomorphism classes. Indeed it is enough to notice that $\gcd(q^{2n}-1,q^h+1)=2$ when q is odd and $h/\bar{h}$ is even.

For q even, $h\geq 1$ and $h/\bar{h}$ odd, it follows from Lemma 4.4 that there exists $s_1\in\mathbb{F}_{q^{2n}}\setminus\{0\}$ such that the polynomial $s_1T+s_1^{q^h}T^{q^{2h}}$ has no nonzero root in $\mathbb{F}_{q^{2n}}$. Using similar methods to above we prove the following proposition.

Proposition 4.8. *For q even, $h\geq 1$, and $s_1\in\mathbb{F}_{q^{2n}}\setminus\{0\}$, let $\mathcal{C}(s_1)$ be the family of function fields*

$$\mathcal{C}(s_1)=\left\{\mathbb{F}_{q^{2n}}(x,y) \text{ with } y^q-y=sx^2+s_1x^{q^h+1} : s\in\mathbb{F}_{q^{2n}}\right\}.$$

Assume that $h/\bar{h}$ is odd and the polynomial $s_1T+s_1^{q^h}T^{q^{2h}}$ has no nonzero root in $\mathbb{F}_{q^{2n}}$. Then for each function field in $\mathcal{C}(s_1)$, its number of rational places is either

$$q^{2n}+1+(q-1)q^n \quad \text{or} \quad q^{2n}+1-(q-1)q^n. \tag{4.14}$$

Let $M_{0,+}$ and $M_{0,-}$ denote the numbers of function fields in $\mathcal{C}(s_1)$ with the corresponding numbers of rational places in (4.14) respectively. We have

$$M_{0,+}=\frac{q^{2n}+q^n}{2} \quad \text{and} \quad M_{0,-}=\frac{q^{2n}-q^n}{2}.$$

Remark 4.9. For $h\geq 1$, Proposition 4.6 gives results on the case where q is odd and $h/\bar{h}$ is even, and Proposition 4.8 gives results on the case where q is even and $h/\bar{h}$ is odd. For $h\geq 1$, using Remark 4.5, now we consider the remaining cases below.

Assume that q is odd and $h/\bar{h}$ is odd. Then the number of rational places of a function field in $\mathcal{C}$ of Proposition 4.6 is either

$$\begin{aligned} &q^{2n}+1+(q-1)q^n, \qquad q^{2n}+1-(q-1)q^n,\\ &q^{2n}+1+(q-1)q^{n+\bar{h}}, \quad \text{or} \quad q^{2n}+1-(q-1)q^{n+\bar{h}}. \end{aligned} \tag{4.15}$$

Let $M_{0,+}$, $M_{0,-}$, $M_{\bar{h},+}$, and $M_{\bar{h},-}$ denote the numbers of function fields in $\mathcal{C}$ with the corresponding numbers of rational places in (4.15) respectively. We have

$$M_{0,+} = 0 \iff M_{\bar{h},-} = 0, \quad \text{and} \quad M_{0,-} = 0 \iff M_{\bar{h},+} = 0.$$

For example

$$q = 3, n = 3, h = 3 \Rightarrow M_{0,+} = 0, M_{0,-} > 0; \quad \text{and}$$
$$q = 3, n = 6, h = 3 \Rightarrow M_{0,-} = 0, M_{0,+} > 0.$$

Assume that q is even and $h/\bar{h}$ is even. Then for each $s_1 \in \mathbb{F}_{q^{2n}} \setminus \{0\}$, the number of rational places of a function field in $\mathcal{C}(s_1)$ of Proposition 4.8 is either

$$q^{2n} + 1 + (q-1)q^{n+\bar{h}}, \quad \text{or} \quad q^{2n} + 1 - (q-1)q^{n+\bar{h}}.$$

In particular for each $s_1 \in \mathbb{F}_{q^{2n}}$, the number of rational places of a function field in $\mathcal{C}(s_1)$ can be neither $q^{2n} + 1 + (q-1)q^n$ nor $q^{2n} + 1 - (q-1)q^n$.

Later in Theorem 5.13, using Propositions 4.6, 4.8 and the results of Section 5, we will prove the existence of a large class of function fields corresponding to Theorem 3.1(1)(ii), (1)(iii), (2)(ii) and (2)(iii).

5. Some degree q extensions of F

In this section we prove the existence of a degree q extension $F(t)$ of F such that $F(t)$ is also of the form (1.1) and $F(t)$ is of the same type as F with respect to Theorem 3.1. If F is minimal or maximal, then we even give an algorithm for constructing $F(t)$. Using these degree q extensions inductively and the special function fields of Section 4, we obtain the existence of a large class of function fields of the form (1.1) with prescribed genus g and number of rational places N simultaneously, where the tuple (g, N) satisfies

$$(g, N) = \left(\frac{(q-1)q^{\hat{h}}}{2}, q^{2n} + 1 \mp (q-1)q^{n+\frac{\hat{k}}{2}} \right),$$

for an integer $0 \le \hat{h}$ and an even integer $0 \le \hat{k} \le 2\hat{h}$. We also give characterizations of all function fields in the form (1.1) whose numbers of rational places are distinct from $q^{2n} + 1$.

We begin with an important technical result. We recall from Section 1 that $F = \mathbb{F}_{q^{2n}}(u, v)$ with $v^q - v = uS(u)$ where $S(X) = s_0X + \cdots + s_hX^{q^h}$ is an F_q-linearized polynomial of degree q^h.

Proposition 5.1. *Let $c \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ and consider the extension $F(t)$ of F where $t^q + ct = u$. Let $D(X) \in \mathbb{F}_{q^{2n}}[X]$ be the $\mathbb{F}_q$-linearized polynomial satisfying*

$$D(X)^q = S(X^q + cX) - s_0cX, \tag{5.1}$$

and let $R(X) \in \mathbb{F}_{q^{2n}}[X]$ be the $\mathbb{F}_q$-linearized polynomial

$$R(X) = cS(X^q + cX) + D(X) + s_0cX^q. \tag{5.2}$$

Note that $\deg R(X) = q^{h+1}$ *and using (5.1) we also have*

$$R(X) = cD(X)^q + D(X) + s_0cX^q + s_0c^2X. \tag{5.3}$$

Let $s \in F(t)$ be defined as $s = v - tD(t)$. Then we have

$$F(t) = \mathbb{F}_{q^{2n}}(t, s) \quad \text{with } s^q - s = tR(t). \tag{5.4}$$

Proof. We first consider the subfield $\mathbb{F}_{q^{2n}}(s, t)$ of $F(t)$. As $v = s + tD(t)$ and $u = t^q + ct$, we have $\mathbb{F}_{q^{2n}}(s, t) = F(t)$. Using (5.1), (5.2) and the identity $v^q - v = uS(u)$, we obtain that $s^q - s = tR(t)$. Using [9, Proposition III.7.10] and the fact that $\deg tR(t) = 1 + q^{h+1}$ is coprime to q, we get $[\mathbb{F}_{q^{2n}}(s, t) : \mathbb{F}_{q^{2n}}(t)] = q$. Hence $T^q - T - tR(t)$ is the minimal polynomial of s in $\mathbb{F}_{q^{2n}}(t, s)$ over $\mathbb{F}_{q^{2n}}(t)$, which completes the proof. □

For $c \in \mathbb{F}_{q^{2n}} \setminus \{0\}$, let $R(X) \in \mathbb{F}_{q^{2n}}[X]$ be the $\mathbb{F}_q$-linearized polynomial of degree q^{h+1} defined by (5.2). Let $B_R : \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}} \to \mathbb{F}_q$ be the bilinear form defined as

$$B_R(a, b) = \mathrm{Tr}(aR(b) + bR(a)).$$

Let $Q_R : \mathbb{F}_{q^{2n}} \to \mathbb{F}_q$ be the quadratic form attached to B_R given by $Q_R(a) = \mathrm{Tr}(aR(a))$. Moreover let W_R be the radical $W_R = \{a \in \mathbb{F}_{q^{2n}} : B_R(a, b) = 0 \text{ for each } b \in \mathbb{F}_{q^{2n}}\}$ and V_R be the subset $V_R = \{a \in \mathbb{F}_{q^{2n}} : Q_R(a) = 0\}$.

Proposition 5.2. *For $a, b \in \mathbb{F}_{q^{2n}}$ we have*

$$B_R(a, b) = B_S(a^q + ca, b^q + cb) \tag{5.5}$$

and

$$Q_R(a) = Q_S(a^q + ca). \tag{5.6}$$

Proof. For $a \in \mathbb{F}_{q^{2n}}$, using (5.1) and (5.2) we get

$$a^q R(a)^q = c^q a^q S(a^q + ca)^q + a^q S(a^q + ca) + s_0^q c^q a^q a^{q^2} - s_0 c a^q a.$$

Then using the identity $\mathrm{Tr}(aR(a)) = \mathrm{Tr}(a^q R(a)^q)$ we obtain that

$$\mathrm{Tr}(aR(a)) = \mathrm{Tr}(caS(a^q + ca)) + \mathrm{Tr}(a^q S(a^q + ca)) = \mathrm{Tr}((a^q + ca)S(a^q + ca)),$$

which proves (5.6). Now the proof of (5.5) follows from (5.6) and the identity

$$B_R(a, b) = Q_R(a + b) - Q_R(a) - Q_R(b)$$

which holds for each $a, b \in \mathbb{F}_{q^{2n}}$. □

Lemma 5.3. *The map η from the set $\{c \in \mathbb{F}_{q^{2n}} \setminus \{0\} : \text{the polynomial } T^q + cT \text{ splits in } \mathbb{F}_{q^{2n}}\}$ to the set of $\mathbb{F}_q$-linear subspaces in $\mathbb{F}_{q^{2n}}$ of codimension 1 given by*

$$\eta(c) = \{a^q + ca : a \in \mathbb{F}_{q^{2n}}\}$$

is one to one and onto. In particular for each $\mathbb{F}_q$-linear subspace $\mathcal{H}$ in $\mathbb{F}_{q^{2n}}$ of codimension 1, there exists a uniquely determined $c \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that $\mathcal{H}$ is the image of the $\mathbb{F}_q$-linear map

$$\begin{aligned} \varphi_c : \mathbb{F}_{q^{2n}} &\to \mathbb{F}_{q^{2n}} \\ a &\mapsto a^q + ca. \end{aligned}$$

Proof. Let $w_1, \ldots, w_{2n}$ form a basis of $\mathbb{F}_{q^{2n}}$. There exist $(\epsilon_1, \ldots, \epsilon_{2n}) \in \mathbb{F}_q^{2n} \setminus \{(0, \ldots, 0)\}$ such that

$$\mathcal{H} = \{\alpha_1 w_1 + \cdots + \alpha_{2n} w_{2n} : \alpha_1 \epsilon_1 + \cdots + \alpha_{2n} \epsilon_{2n} = 0 \text{ and } \alpha_1, \ldots, \alpha_{2n} \in \mathbb{F}_q\}.$$

As in the proof of [8, Theorem 3.1], let $b \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that $\mathrm{Tr}(bw_j) = \epsilon_j$ for $j = 1, \ldots, 2n$. Then $\mathcal{H} = \{\alpha \in \mathbb{F}_{q^{2n}} : \mathrm{Tr}(b\alpha) = 0\}$. Let $c = -b^{q^{2n-1}-1}$ and $\varphi_c : \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^{2n}}$ be the $\mathbb{F}_q$-linear map defined by $a \mapsto a^q + ca$. For $a \in \mathbb{F}_{q^{2n}}$ and $\bar{a} = \varphi_c(a)$, we have $\mathrm{Tr}(b\bar{a}) = 0$ since $bc + b^{q^{2n-1}} = 0$. Therefore $\mathrm{Im}\,\varphi_c \subseteq \mathcal{H}$ and $\dim \mathrm{Im}\,\varphi_c \leq 2n - 1$. As $\dim \mathrm{Ker}\,\varphi_c \leq 1$, we obtain that $\mathrm{Im}\,\varphi_c = \mathcal{H}$. It is clear that c is uniquely determined by $\mathcal{H}$. Note that the number of distinct $\mathbb{F}_q$-linear subspaces in $\mathbb{F}_{q^{2n}}$ of codimension 1 is $\frac{q^{2n}-1}{q-1}$. Moreover the polynomial $T^q + cT$ with $c \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ splits in $\mathbb{F}_{q^{2n}}$ if and only if $-c$ is a $q-1$ power in $\mathbb{F}_{q^{2n}}$. Hence the number of $c \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that $T^q + cT$ splits in $\mathbb{F}_{q^{2n}}$ is also $\frac{q^{2n}-1}{q-1}$. This completes the proof. □

Lemma 5.4. *Assume that $c \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that the polynomial $T^q + cT$ splits in $\mathbb{F}_{q^{2n}} \setminus \{0\}$ and let $\mathcal{H}_c$ be the image of the $\mathbb{F}_q$-linear map $\varphi_c : \mathbb{F}_{q^{2n}} \to \mathbb{F}_{q^{2n}}$ sending a to $a^q + ca$. Let $R(X)$ be the $\mathbb{F}_q$-linearized polynomial of degree q^{h+1} defined in (5.2) using this c. We have*

$$\dim W_R \leq \dim W_S + 2.$$

Moreover if $\mathcal{H}_c$ contains W_S, then we also have

$$\varphi_c^{-1}(W_S) \subseteq W_R,$$

and in particular

$$\dim W_S + 1 \leq \dim W_R.$$

Proof. Let U be the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^{2n}}$ defined by

$$U = \{u \in \mathbb{F}_{q^{2n}} : B_S(u, \beta^q + c\beta) = 0 \text{ for each } \beta \in \mathbb{F}_{q^{2n}}\}.$$

For $\alpha \in W_R$, since for all $\beta \in \mathbb{F}_{q^{2n}}$ we have $B_R(\alpha, \beta) = B_S(\alpha^q + c\alpha, \beta^q + c\beta) = 0$, the image $\varphi_c(W_R)$ of W_R under φ_c is contained in U. Moreover $\operatorname{Ker}\varphi_c \subseteq W_R$ and hence

$$\dim W_R - 1 = \dim \varphi_c(W_R) \leq \dim U. \tag{5.7}$$

Let $e \in \mathbb{F}_{q^{2n}} \setminus \mathcal{H}_c$ and define the $\mathbb{F}_q$-linear map

$$\begin{aligned} \psi : U &\to \mathbb{F}_q \\ u &\mapsto B_S(u, e). \end{aligned}$$

As $\operatorname{Span}\{\mathcal{H}_c, e\} = \mathbb{F}_{q^{2n}}$, we observe that $\operatorname{Ker}\psi = W_S$. Moreover $\dim \psi(U) \in \{0, 1\}$ and hence

$$\dim U \leq \dim W_S + 1. \tag{5.8}$$

Using (5.7) and (5.8) we obtain that $\dim W_R \leq \dim W_S + 2$.

Assume further that $\mathcal{H}_c$ contains W_S. Let $\alpha \in \varphi_c^{-1}(W_S)$ and $a = \alpha^q + c\alpha \in W_S$. Using (5.5) we get $B_R(\alpha, \beta) = B_S(a, \beta^q + c\beta) = 0$ for each $\beta \in \mathbb{F}_{q^{2n}}$. This proves that $\varphi_c^{-1}(W_S) \subseteq W_R$. □

Recall that k denotes the dimension of the $\mathbb{F}_q$-linear space W_S.

Proposition 5.5. *Assume that k is even, $k \leq 2n - 2$ and the number of rational places of F is*

$$1 + q^{2n} + (q - 1)q^n q^{k/2}$$

(cf. Theorem 3.1). Then there exists $c \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that the polynomial $T^q + cT$ splits in $\mathbb{F}_{q^{2n}}$, the image $\mathcal{H}_c$ of the map φ_c sending $a \in \mathbb{F}_{q^{2n}}$ to $a^q + ca \in \mathbb{F}_{q^{2n}}$ contains W_S, for the $\mathbb{F}_q$-linearized polynomial $R(X)$ of degree q^{h+1} defined in (5.2) using this c we have

$$\dim W_R = \dim W_S + 2,$$

and the number of rational places of the function field $F(t)$ defined in Proposition 5.1 using this c is

$$1 + q^{2n} + (q - 1)q^n q^{k/2+1}.$$

Proof. As $\dim W_S = k$, the number of $\mathbb{F}_q$-linear subspaces of codimension 1 in $\mathbb{F}_{q^{2n}}$ containing W_S is

$$\frac{q^{2n-k} - 1}{q - 1}. \tag{5.9}$$

Let $\mathcal{S}$ be the subset of $\mathbb{F}_{q^{2n}} \setminus \{0\}$ consisting of c such that the polynomial $T^q + cT$ splits in $\mathbb{F}_{q^{2n}}$ and the image $\mathcal{H}_C$ of the map φ_c sending $a \in \mathbb{F}_{q^{2n}}$ to $a^q + ca$ contains W_S. Using Lemma 5.3 and (5.9) we obtain that $|\mathcal{S}| = \frac{q^{2n-k}-1}{q-1}$.

For $c \in \mathcal{S}$, let $R(X) \in \mathbb{F}_{q^{2n}}[X]$ be the $\mathbb{F}_q$-linearized polynomial of degree q^{h+1} and $F(t)$ be the function field defined in Proposition 5.1 depending on c. By Lemma 5.4, we have that $\dim W_R$ is either $\dim W_S + 1$ or $\dim W_S + 2$. Then from Theorem 3.1 we get the number of rational places of $F(t)$ is either $1 + q^{2n}$, $1 + q^{2n} + (q - 1)q^n q^{k/2+1}$ or $1 + q^{2n} - (q - 1)q^n q^{k/2+1}$.

Let $\mathcal{T}$ be the subset of the cartesian product $\mathcal{S} \times \mathbb{F}_{q^{2n}}$ defined as

$$\mathcal{T} = \{(c, a) \in \mathcal{S} \times \mathbb{F}_{q^{2n}} : \operatorname{Tr}(aS(a)) = 0 \text{ and } a \in \operatorname{Im}\varphi_c\}.$$

We will determine the cardinality of $\mathcal{T}$ by first fixing $a \in \mathbb{F}_{q^{2n}}$ and varying $c \in \mathcal{S}$. If $a \in \mathbb{F}_{q^{2n}} \setminus V_S$, then there is no $c \in \mathcal{S}$ such that $(c, a) \in \mathcal{T}$. Note that $W_S \subseteq V_S$. If $a \in W_S$, then for each $c \in \mathcal{S}$ we have $a \in \operatorname{Im} \varphi_c$ by definition of $\mathcal{S}$. From Hilbert's Theorem 90 we get

$$|V_S| = \frac{1}{q}\left(q^{2n} + (q-1)q^n q^{k/2}\right).$$

For $a \in V_S \setminus W_S$, there are exactly $\frac{q^{2n-k-1}-1}{q-1}$ distinct $\mathbb{F}_q$-linear subspaces in $\mathbb{F}_{q^{2n}}$ of codimension 1 containing W_S and a. Then there are exactly $\frac{q^{2n-k-1}-1}{q-1}$ distinct $c \in \mathcal{S}$ such that $a \in \operatorname{Im} \varphi_c$. Therefore the cardinality $|\mathcal{T}|$ of $\mathcal{T}$ is given by

$$|\mathcal{T}| = q^k \frac{q^{2n-k}-1}{q-1} + \left(q^{2n-1} + (q-1)q^{n+k/2-1} - q^k\right)\frac{q^{2n-k-1}-1}{q-1}. \tag{5.10}$$

Now we estimate $|\mathcal{T}|$ by fixing $c \in \mathcal{S}$ and varying $a \in \mathbb{F}_{q^{2n}}$. Assume the contrary, that there is no $c \in \mathcal{S}$ such that the number of rational places of the corresponding function field $F(t)$ is $1 + q^{2n} + (q-1)q^n q^{k/2+1}$.

For $c \in \mathcal{S}$, as $F(t) = \mathbb{F}_{q^{2n}}(u, v, t)$ with

$$v^q - v = uS(u) \quad \text{and}$$
$$t^q + ct = u,$$

the number of rational places of $F(t)$ is $1 + q^2|\{a \in \mathbb{F}_{q^{2n}} : \operatorname{Tr}(aS(a)) = 0 \text{ and } a \in \operatorname{Im} \varphi_c\}|$. By the assumption above, for $c \in \mathcal{S}$ we have $|\{a \in \mathbb{F}_{q^{2n}} : \operatorname{Tr}(aS(a)) = 0 \text{ and } a \in \operatorname{Im} \varphi_c\}| \leq q^{2n-2}$ and hence

$$|\mathcal{T}| \leq \frac{q^{2n-k}-1}{q-1} q^{2n-2}. \tag{5.11}$$

Using (5.10), (5.11) and some straightforward calculations we obtain $(q-1)q^{3n-k/2-2} + q^{2n} + q^{2n-2} \leq (q-1)q^{n+k/2-1} + 2q^{2n-1}$, which is a contradiction since $k \leq 2n-2$. □

Note that there is no function field F of the form (1.1) with $\dim W_S = k = 2n$ and $N(F) = 1+q^{2n}-(q-1)q^n q^{k/2}$. (cf. Lemma 3.4). Now we prove an analog of Proposition 5.5.

Proposition 5.6. *Assume that k is even, $k \leq 2n-4$ and the number of rational places of F is*

$$1 + q^{2n} - (q-1)q^n q^{k/2}$$

(cf. Theorem 3.1). Then there exists $c \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that the polynomial $T^q + cT$ splits in $\mathbb{F}_{q^{2n}}$, the image $\mathcal{H}_c$ of the map φ_c sending $a \in \mathbb{F}_{q^{2n}}$ to $a^q + ca \in \mathbb{F}_{q^{2n}}$ contains W_S, for the $\mathbb{F}_q$-linearized polynomial $R(X)$ of degree q^{h+1} defined in (5.2) using this c we have

$$\dim W_R = \dim W_S + 2,$$

and the number of rational places of the function field $F(t)$ defined in Proposition 5.1 using this c is

$$1 + q^{2n} - (q-1)q^n q^{k/2+1}.$$

Proof. The proof is similar to the proof of Proposition 5.5. Let $\mathcal{S}$ and $\mathcal{T}$ be the sets defined in the same way as in the proof of Proposition 5.5. We have $|V_S| = \frac{1}{q}\left(q^{2n} - (q-1)q^n q^{k/2}\right)$ and

$$|\mathcal{T}| = q^k \frac{q^{2n-k}-1}{q-1} + \left(q^{2n-1} - (q-1)q^{n+k/2-1} - q^k\right)\frac{q^{2n-k-1}-1}{q-1}. \tag{5.12}$$

Assume the contrary, that there is no $c \in \mathcal{S}$ such that the number of rational places of the corresponding function field $F(t)$ is $1 + q^{2n} - (q-1)q^n q^{k/2+1}$. This implies that $|\{a \in \mathbb{F}_{q^{2n}} : \operatorname{Tr}(aS(a)) = 0 \text{ and } a \in \operatorname{Im} \varphi_c\}| \geq q^{2n-2}$ and hence

$$|\mathcal{T}| \geq \frac{q^{2n-k}-1}{q-1} q^{2n-2}. \tag{5.13}$$

Using (5.12) and (5.13) we obtain $(q-1)q^{n+k/2-1}+q^{2n}+q^{2n-2} \geq (q-1)q^{3n-k/2-2}+2q^{2n-1}$, which is a contradiction since $k \leq 2n-4$. □

We will use the following important theorem from [5].

Theorem 5.7. *Let E_1, E_2 be two algebraic function fields with the same finite full constant field. Assume $E_1 \subseteq E_2$. Then the L-polynomial (cf. [9, Definition V.1.14]) of E_1 divides the L-polynomial of E_2. In particular if E_2 is a maximal (resp. minimal) function field, then E_1 is also maximal (resp. minimal).*

In the next proposition, when F is maximal or minimal, we give an algorithm for constructing an extension $F(t)$ of F in the form (5.4) which is also maximal or minimal respectively. In this case, Propositions 5.5 and 5.6 give only existence results.

Recall that if F is maximal or minimal then $k=2h$ (cf. Corollary 3.2 and Corollary 3.3). We will use the following observation in the next proposition. If F is maximal with $h \leq n-1$ or F is minimal with $h \leq n-2$, then $W_S \subsetneq V_S$. Indeed otherwise $W_S = V_S$ and as $\dim W_S = 2h$ we have

$$N(F) = 1 + qq^{2h}. \tag{5.14}$$

We also have

$$N(F) = \begin{cases} 1+q^{2n}+(q-1)q^h q^n & \text{if } F \text{ is maximal,} \\ 1+q^{2n}-(q-1)q^h q^n & \text{if } F \text{ is minimal.} \end{cases} \tag{5.15}$$

Using (5.14), (5.15) and $h \leq n-1$ (resp. $h \leq n-2$) if F is maximal (resp. minimal), we obtain a contradiction.

Proposition 5.8. *Assume that F is maximal with $h \leq n-1$ or F is minimal with $h \leq n-2$. We apply the following algorithm:*

1. *Choose $e \in V_S \setminus W_S$.*
2. *Choose $f \in \mathbb{F}_{q^{2n}}$ with $B_S(e,f) \neq 0$.*
3. *If $h = n-1$, then let $\mathcal{H} = \mathrm{Span}\{W_S \cup \{e\}\}$. If $h < n-1$, let $l = n-1-h$ and choose $\{f_1, \ldots, f_{2l}\} \subseteq \mathbb{F}_{q^{2n}}$ such that $\mathrm{Span}\{ W_S \cup \{e, f\} \cup \{f_1, \ldots, f_{2l}\}\} = \mathbb{F}_{q^{2n}}$. For $1 \leq i \leq 2l$, let $\hat{f}_i \in \mathbb{F}_{q^{2n}}$ be defined by*

$$\hat{f}_i = f_i - \frac{B_S(f_i, e)}{B_S(f, e)} f.$$

Let $\mathcal{H} = \mathrm{Span}\left\{W_S \cup \{e\} \cup \{\hat{f}_1, \ldots, \hat{f}_{2l}\}\right\}$.
4. *Let c be the element of $\mathbb{F}_{q^{2n}} \setminus \{0\}$ corresponding to the $\mathbb{F}_q$-linear subspace $\mathcal{H}$ in $\mathbb{F}_{q^{2n}}$ of codimension 1 containing W_S (cf. Lemma 5.3).*
5. *Let $F(t)$ be the extension of F defined in Proposition 5.1 using this c.*

Then $F(t)$ is maximal or minimal respectively.

Proof. We can apply Step 1 by the observation above. Since $e \notin W_S$, there exists $f \in \mathbb{F}_{q^{2n}}$ with $B_S(e,f) \neq 0$. Since $e \in V_S$, we have $B_S(e,e) = 0$. Moreover $B_S(e, \hat{f}_i) = 0$ by definition of $\hat{f}_i$ for $1 \leq i \leq 2l$. Let $a = w_S + \alpha e + \alpha_1 \hat{f}_i + \cdots + \alpha_{2l}\hat{f}_{2l}$ be an element of $\mathcal{H}$ with $w_S \in W_S$ and $\alpha, \alpha_1, \ldots, \alpha_{2l} \in \mathbb{F}_q$. Then

$$B_S(e,a) = B_S(e, w_S) + \alpha B_S(e,e) + \sum_{i=1}^{2l} B_S(e, \hat{f}_i) = 0. \tag{5.16}$$

Let $W \subseteq \mathbb{F}_{q^{2n}}$ be the $\mathbb{F}_q$-linear subspace defined by using the element c of Step 4 as $W = \left\{a \in \mathbb{F}_{q^{2n}} : a^q + ca \in \mathrm{Span}\{W_S \cup \{e\}\}\right\}$. We have $\dim W = \dim \mathrm{Span}\{W_S \cup \{e\}\} + 1 = \dim W_S + 2$. Let w be an element of W. There exists $w_S \in W_S$ and $\alpha \in \mathbb{F}_q$ such that $w^q + cw = w_S + \alpha e$. For $b \in \mathbb{F}_{q^{2n}}$ we have $B_R(w,b) = B_S(w^q + cw, b^q + cb) = B_S(w_S, a) + \alpha B_S(e,a)$, where $a = b^q + cb \in H$. Then $B_R(w,b) = 0$ and hence $W \subseteq W_R$. Since $\dim W_R \leq \dim W_S + 2$ (cf. Lemma 5.4), we conclude that $W = W_R$.

Now we prove that $W_R \subseteq V_R$. If q is odd, this is obvious. We assume that q is even. Using (5.6) we obtain $Q_R(w) = Q_S(w_S + \alpha e) = Q_S(w_S) + \alpha B_S(w_S, e) + \alpha^2 Q_S(e)$. Since F is maximal or minimal, we have $Q_S(w_S) = 0$

(cf. Corollaries 3.2 and 3.3). Moreover $B_S(w_S, e) = Q_S(e) = 0$ by construction. Therefore $W_R \subseteq V_R$. We complete the proof using Theorems 3.1 and 5.7. □

Now we give our existence results of maximal and minimal function fields of the form (1.1) for all possible values of h.

Theorem 5.9. *For q odd and $0 \le h \le n$ (resp. q even and $1 \le h \le n$), there exists a maximal function field F of the form (1.1). For q odd and $0 \le h \le n-1$ (resp. q even and $1 \le h \le n-1$), there exists a minimal function field F of the form (1.1).*

Proof. Assume that q is odd. For $h = 0$ the existence of maximal and minimal function fields follows from Lemma 4.1. For $1 \le h \le n$ (resp. $1 \le h \le n-1$) using Proposition 5.8 inductively, we prove the existence of maximal (resp. minimal) function fields. In the case where q is even, we proceed similarly using Lemma 4.3 instead of Lemma 4.1. □

Remark 5.10. For $q = 2$, among other things, the existence of maximal function fields of the form (1.1) was proved in [2] using a different method.

Using the algorithm in Proposition 5.8, we obtain the following examples for Theorem 5.9.

Example 5.11. For $q = 3$ and $n = 5$, let w be a generator of the multiplicative group of $\mathbb{F}_{q^{2n}}$ such that $w^{10} + 2w^6 + 2w^5 + 2w^4 + w + 2 = 0$. Let $S_0(X), \ldots, S_5(X) \in \mathbb{F}_{q^{2n}}[X]$ be the polynomials given by

$$
\begin{aligned}
S_0(X) &= w^{50396}X,\\
S_1(X) &= w^{27864}X^3 + w^{2178}X,\\
S_2(X) &= w^{52680}X^9 + w^{49491}X^3 + w^{21290}X,\\
S_3(X) &= w^{23242}X^{27} + w^{45745}X^9 + w^{29809}X^3 + w^{29460}X,\\
S_4(X) &= w^{35464}X^{81} + w^{25366}X^{27} + w^{58844}X^9 + w^{52110}X^3 + w^{21480}X,\\
S_5(X) &= w^{13298}X^{243}.
\end{aligned}
$$

For $0 \le i \le 5$, the function field $\mathbb{F}_{q^{2n}}(u, v)$ with $v^q - v = uS_i(u)$ is maximal. Let $T_0(X), \ldots, T_4(X) \in \mathbb{F}_{q^{2n}}[X]$ be the polynomials given by

$$
\begin{aligned}
T_0(X) &= w^{19047}X,\\
T_1(X) &= w^{35989}X^3 + w^{26687}X,\\
T_2(X) &= w^{58149}X^9 + w^{16604}X^3 + w^{55544}X,\\
T_3(X) &= w^{5829}X^{27} + w^{19314}X^9 + w^{41735}X^3 + w^{9130}X,\\
T_4(X) &= w^{44553}X^{81} + w^{41470}X^{27} + w^{34505}X^9 + w^{6482}X^3 + w^{26421}X.
\end{aligned}
$$

For $0 \le i \le 4$, the function field $\mathbb{F}_{q^{2n}}(u, v)$ with $v^q - v = uT_i(u)$ is minimal.

Example 5.12. For $q = 4$ and $n = 5$, let w be a generator of the multiplicative group of $\mathbb{F}_{q^{2n}}$ such that $w^{20} + w^{10} + w^9 + w^7 + w^6 + w^5 + w^4 + w + 1 = 0$. Let $S_1(X), \ldots, S_5(X) \in \mathbb{F}_{q^{2n}}[X]$ be the polynomials given by

$$
\begin{aligned}
S_1(X) &= X^4 + w^{260760}X,\\
S_2(X) &= w^{272901}X^{16} + w^{456641}X^4 + w^{679868}X,\\
S_3(X) &= w^{137682}X^{64} + w^{497075}X^{16} + w^{259729}X^4 + w^{238458}X,\\
S_4(X) &= w^{987750}X^{256} + w^{946150}X^{64} + w^{586225}X^{16} + w^{933150}X^4 + w^{600400}X,\\
S_5(X) &= w^{375150}X^{1024}.
\end{aligned}
$$

For $1 \le i \le 5$, the function field $\mathbb{F}_{q^{2n}}(u, v)$ with $v^q - v = uS_i(u)$ is maximal. Let $T_1(X), \ldots, T_4(X) \in \mathbb{F}_{q^{2n}}[X]$ be the polynomials given by

$$
T_1(X) = X^4 + w^{186392}X,
$$

Table 1.1

k	h	$S(X)$
0	2	$w^{290}X^9$
2	3	$w^{120}X^{27} + w^{682}X^9 + w^{72}X^3$
4	4	$w^{724}X^{81} + w^{239}X^{27} + w^{633}X^9 + w^{160}X^3 + w^{628}X$
6	5	$w^{450}X^{243} + w^{193}X^{81} + w^{266}X^{27} + w^{645}X^9 + w^{258}X^3$
0	4	$w^{566}X^8 1$
2	5	$w^{156}X^{243} + w^{429}X^{81} + w^{524}X^{27}$
4	6	$w^{664}X^{729} + w^{456}X^{243} + w^{293}X^{81} + w^{381}X^{27} + w^{136}X^9$
6	7	$w^{58}X^{2187} + w^{656}X^{243} + w^{121}X^{81} + w^{686}X^{27} + w^{725}X^9 + w^{654}X^3$

$$T_2(X) = w^{780741}X^{16} + w^{541393}X^4 + w^{250945}X,$$
$$T_3(X) = w^{658821}X^{64} + w^{826124}X^{16} + w^{1028087}X^4 + w^{278641}X,$$
$$T_4(X) = w^{409317}X^{256} + w^{190565}X^{64} + w^{485402}X^{16} + w^{122205}X^4 + w^{789137}X.$$

For $1 \le i \le 4$, the function field $\mathbb{F}_{q^{2n}}(u, v)$ with $v^q - v = uT_i(u)$ is minimal.

Similarly using Propositions 4.6 and 4.8, we prove the following result for a large class of function fields corresponding to Theorem 3.1(1)(ii), (1)(iii), (2)(ii) and (2)(iii) with prescribed genus and number of rational places simultaneously.

Theorem 5.13. *We have the following existence result:*

1. *Case where q is odd: Assume that k is an even integer with $0 \le k \le 2n$ (respectively $0 \le k \le 2n-2$) and h is an integer satisfying that $h \ge k/2+1$ and $\frac{h-k/2}{\gcd(h-k/2,n)}$ is even.*
2. *Case where q is even: Assume that k is an even integer with $0 \le k \le 2n$ (respectively $0 \le k \le 2n-2$) and h is an integer satisfying that $h \ge k/2+1$ and $\frac{h-k/2}{\gcd(h-k/2,n)}$ is odd.*

Then in both cases above, there exists a function field F of the form (1.1) such that the genus $g(F)$ and the number of rational places $N(F)$ are simultaneously prescribed as

$$g(F) = \frac{(q-1)q^h}{2}, \quad \text{and}$$
$$N(F) = q^{2n} + 1 + (q-1)q^{n+k/2} \ (\text{resp. } N(F) = q^{2n} + 1 - (q-1)q^{n+k/2}).$$

Remark 5.14. Using function fields in the form (1.1) different from the ones whose existence is proved in Propositions 4.6 or 4.8, we would get further results similar to Theorem 5.13. For example using Remark 4.9 we obtain that if q is odd, k is even with $0 \le k \le 2n$ and $h \ge k/2+1$ with $\frac{h-k/2}{\gcd(h-k/2,n)}$ is odd, then there exists a function field in the form (1.1) of genus $\frac{(q-1)q^h}{2}$ such that its number of rational places is either

$$q^{2n} + 1 + (q-1)q^{n+k/2} \quad \text{or} \quad q^{2n} + 1 - (q-1)q^{n+k/2}.$$

We give some examples for Theorem 5.13.

Example 5.15. Let $q = 3$, $n = 3$ and w be the generator of the multiplicative group of $\mathbb{F}_{q^{2n}}$ satisfying $w^6 + 2w^4 + w^2 + 2w + 2 = 0$. Each line of Table 1.1 (respectively Table 1.2) corresponds to a function field $F = \mathbb{F}_{q^{2n}}(u, v)$, where $v^q - v = uS(u)$, with the corresponding k and h of the table such that the genus $g(F)$ and the number of rational places $N(F)$ are

$$g(F) = (q-1)q^h/2,$$
$$N(F) = q^{2n} + 1 + (q-1)q^{n+k/2} \ (\text{resp. } q^{2n} + 1 - (q-1)q^{n+k/2}).$$

For $q = 2$, $n = 4$ and a generator w of the multiplicative group of $\mathbb{F}_{q^{2n}}$ satisfying $w^8 + w^4 + w^3 + w^2 + 1 = 0$, Tables 2.1 and 2.2 have the same meaning respectively.

Table 1.2

k	h	$S(X)$
0	2	$w^{219}X^9$
2	3	$w^{141}X^{27} + w^{135}X^9 + w^{567}X^3$
4	4	$w^{699}X^{81} + w^{161}X^{27} + w^{251}X^9 + w^{448}X^3 + w^{19}X$
0	4	$w^{493}X^{81}$
2	5	$w^{265}X^{243} + wX^{81} + w^{75}X^{27}$
4	6	$w^{247}X^{729} + w^{667}X^{243} + w^{241}X^{81} + w^{381}X^{27} + w^{591}X^9$

Table 2.1

k	h	$S(X)$
0	2	$w^{187}X^4 + w^{74}X$
2	3	$w^{240}X^8 + w^{196}X^4 + w^{72}X^2 + w^{187}X$
4	4	$w^{146}X^{16} + w^{27}X^8 + w^{231}X^4 + w^{21}X^2 + w^{48}X$
6	5	$w^{83}X^{32} + w^{167}X^{16} + w^{228}X^8 + w^{38}X^4 + w^{171}X^2 + w^{92}X$
8	6	$w^{242}X^{64} + w^{252}X^{32} + w^{170}X^{16} + w^{231}X^8 + w^{203}X^4$
0	3	$w^{254}X^8 + w^{139}X$
2	4	$w^{149}X^{16} + w^{221}X^8 + w^{217}X^4 + w^{28}X$
4	5	$w^{27}X^{32} + w^{222}X^{16} + w^{155}X^8 + w^{26}X^4 + w^{247}X^2 + w^{15}X$
6	6	$w^{28}X^{64} + w^{188}X^{32} + w^{245}X^{16} + w^{88}X^8 + w^{88}X^4 + w^{153}X^2 + w^{35}X$
8	7	$w^{60}X^{128} + w^{15}X^{64} + w^{149}X^{32} + X^{16} + w^{172}X^8 + w^{60}X^4 + w^{120}X^2$

Table 2.2

k	h	$S(X)$
0	2	$w^{101}X^4 + w^{43}X$
2	3	$w^{11}X^8 + w^{229}X^4 + w^{253}X^2 + w^{163}X$
4	4	$w^{22}X^{16} + w^{15}X^8 + w^{66}X^4 + w^{10}X^2 + w^{89}X$
6	5	$w^3X^{32} + w^{153}X^{16} + w^{194}X^8 + w^{155}X^4 + w^8X^2 + w^{147}X$
0	3	$w^{107}X^8 + w^{63}X$
2	4	$w^{165}X^{16} + w^{209}X^8 + w^{158}X^4 + w^{201}X$
4	5	$w^{212}X^{32} + w^{150}X^{16} + w^{209}X^8 + w^6X^4 + w^{173}X^2 + w^{189}X$
6	6	$w^{56}X^{64} + w^{183}X^{32} + w^{13}X^{16} + w^{143}X^8 + w^{17}X^4 + w^{130}X^2 + w^{92}X$

Proposition 5.6 implies the following characterization of function fields corresponding to Theorem 3.1(1)(iii) and (2)(iii).

Proposition 5.16. *Let F be a function field in the form (1.1) of genus $\frac{(q-1)q^h}{2}$ and number of rational places $q^{2n} + 1 - (q-1)q^n q^{k/2}$, where k is even and $0 \le k \le 2n-2$. Let $u = h - k/2$. Then F is a subfield of a function field $\widetilde{F}$ in the form (1.1) such that its genus $g(\widetilde{F})$ is $\frac{(q-1)q^{n+u-1}}{2}$ and its number of rational places $N(\widetilde{F})$ is $q^{2n-1} + 1$ (which is $q^{2n} + 1 - (q-1)q^n q^{n-1}$).*

Our characterization corresponding to Theorem 3.1(1)(ii) and (2)(ii) is much stronger. For simplicity we assume that $h - k/2 \le n - 1$ in the next theorem.

Theorem 5.17. *Let F be a function field in the form (1.1) of genus $\frac{(q-1)q^h}{2}$ and number of rational places $q^{2n} + 1 + (q-1)q^n q^{k/2}$, where k is even, $0 \le k \le 2n$, and $h - k/2 \le n - 1$. Let $u = h - k/2$. Then F is a*

subfield of a function field $\widetilde{F}$ in the form (1.1) whose $\mathbb{F}_q$-linearized polynomial

$$\widetilde{S}(X) = \tilde{s}_0 X + \tilde{s}_1 X^q + \cdots + \tilde{s}_{n+u} X^{q^{n+u}} \in \mathbb{F}_{q^{2n}}[X] \tag{5.17}$$

is of degree q^{n+u} and satisfies that

$$\tilde{s}_0 = \tilde{s}_1 = \cdots = \tilde{s}_{n-u-1} = 0,$$
$$\tilde{s}_{n-i} + \tilde{s}_{n+i}^{q^{n-i}} = 0 \quad \textit{for each } 1 \le i \le u, \textit{ and}$$
$$\tilde{s}_n + \tilde{s}_n^{q^n} = 0.$$

In particular the genus $g(\widetilde{F})$ of $\widetilde{F}$ is $\frac{(q-1)q^{n+u}}{2}$ and the number of rational places $N(\widetilde{F})$ of $\widetilde{F}$ is $1 + q^{2n+1}$.

Proof. Using the methods of this section, we obtain a function field $\widetilde{F}$ in the form (1.1), whose $\mathbb{F}_q$-linearized polynomial $\widetilde{S}(X)$ is of degree q^{n+u} as in (5.17). Moreover the dimension $\tilde{k}$ of the radical of the corresponding bilinear form is $2n$. This implies that

$$\mathrm{Tr}\left(\alpha \widetilde{S}(\alpha)\right) = 0 \quad \text{for each } \alpha \in \mathbb{F}_{q^{2n}}. \tag{5.18}$$

Let ω be a generator of the multiplicative group of $\mathbb{F}_{q^{2n}}$. Note that for $1 \le i \le u$

$$\left(\tilde{s}_{n+i}\omega^{q^{n+i}+1}\right)^{q^{n-i}} = \tilde{s}_{n+i}^{q^{n-i}}\,\omega^{q^{n-i}+1}. \tag{5.19}$$

Using (5.18), (5.19) and [4, Theorem 2.5] we complete the proof. □

6. Some Galois extensions of F

In this section we prove that if $N(F) > q^{2n} + 1$, then the degree q extensions of Section 5 are Galois. Moreover we prove that the extension $\widetilde{F}/F$ of Theorem 5.17 is Galois and we determine its Galois group. If F is maximal, then we also prove that F is a subfield of the Hermitian function field H over $\mathbb{F}_{q^{2n}}$, the extension H/F is Galois and we obtain the Galois group $\mathrm{Aut}(H/F)$ explicitly.

Recall that $F = \mathbb{F}_{q^{2n}}(u, v)$ with $v^q - v = uS(u)$, where $S(X)$ is an $\mathbb{F}_q$-linearized polynomial of degree q^h in $\mathbb{F}_{q^{2n}}[X]$. In this section we assume that the dimension k of the radical of the corresponding bilinear form is even and the number of rational places of F is $q^{2n} + 1 + (q-1)q^{n+\frac{k}{2}}$ (cf. Theorem 3.1). For $k \le 2n-2$, let $F_1 = F(t_1)$ be the function field with $t_1^q + c_1 t_1 = u$, where c_1 is obtained using Proposition 5.5. Let $m = n - \frac{k}{2}$ and for $m \ge 2$ and $1 \le i \le m-1$, let c_{i+1} be obtained using Proposition 5.5 and $F_{i+1} = F_i(t_{i+1})$ be the function field with $t_{i+1}^q + c_{i+1}t_{i+1} = t_i$. Note that F_m corresponds to the function field $\widetilde{F}$ of Theorem 5.17. For $m \ge 1$ and $1 \le i \le m$, let φ_i be the $\mathbb{F}_q$-linear map on $\mathbb{F}_{q^{2n}}$ sending x to $x^q + c_i x$. In this section we prove that F_m/F is Galois and we compute the Galois group $\mathrm{Aut}(F_m/F)$.

Throughout this section, for $1 \le i \le m$ and a rational place Q of F_i with $v_Q(t_i) \ge 0$, we denote the evaluation of t_i at Q as $t_i(Q)$.

We begin with a technical lemma, which is not difficult but is useful. Let L be an algebraic function field such that $\mathbb{F}_{q^{2n}}$ is the full constant field of L. Let $c \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ such that the polynomial $T^q + cT$ splits in $\mathbb{F}_{q^{2n}}$. Let $a \in L$ and $L(t)$ be the extension of L with $t^q + ct = a$. Assume that the full constant field of $L(t)$ is $\mathbb{F}_{q^{2n}}$ and $[L(t) : L] = q$.

Lemma 6.1. *Under the same assumptions as above, let P be a rational place of L such that $v_P(a) \ge 0$. Let φ_c be the $\mathbb{F}_q$-linear map on $\mathbb{F}_{q^{2n}}$ sending x to $x^q + cx$. Let $a(P)$ be the evaluation of a at P. If $a(P) \notin \mathrm{Im}\,\varphi_c$, then there exists no rational place of $L(t)$ over P. If $a(P) \in \mathrm{Im}\,\varphi_c$, then there exist q rational places of $L(t)$ over P. If Q is a rational place of $L(t)$ over P and $t(Q)$ is the evaluation of t at Q, then the set of evaluations of t at all rational places of $L(t)$ over P is $\{t(Q) + \alpha : \alpha \in \mathrm{Ker}\,\varphi_c\}$.*

Proof. The proof follows from [9, Theorem III.3.7]. □

Using Lemma 6.1, we prove the following proposition.

Proposition 6.2. *Assume that $m \geq 1$. Let P be a rational place of F such that $v_P(uS(u)) \geq 0$. For $1 \leq i \leq m$, there exist either no or exactly $|\mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i)|$ rational places of F_i over P. Moreover if there exists a rational place P_i of F_i over P, then the set of evaluations of t_i at all rational places of F_i over P is $\{t_i(P_i) + \alpha_i : \alpha_i \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i)\}$.*

Proof. We prove by induction on i. For $i = 1$, the proposition follows from Lemma 6.1. Assume that it holds for some $1 \leq i \leq m-1$. Assume further that there exists a rational place P_{i+1} of F_{i+1} over P. Let P_i be the rational place of F_i under P_{i+1}. We observe that $\dim \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i \circ \varphi_{i+1})$ is either $\dim \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i) + 1$ or $\dim \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i)$. First we consider the case that $\dim \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i \circ \varphi_{i+1}) = \dim \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i) + 1$. This means that $\mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i) \subseteq \mathrm{Im}\, \varphi_{i+1}$. Since there exists a rational place of F_{i+1} over P_i, it follows from Lemma 6.1 that $t_i(P_i) \in \mathrm{Im}\, \varphi_{i+1}$. By the induction hypothesis, the set of evaluations of t_i at all rational places of F_i is $\{t_i(P_i) + \alpha_i : \alpha_i \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i)\}$. As $t_i(P_i) \in \mathrm{Im}\, \varphi_{i+1}$ and $\mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i) \subseteq \mathrm{Im}\, \varphi_{i+1}$, each rational place of F_i over P totally splits in F_{i+1}/F_i. Let Q_{i+1} be an arbitrary rational place of F_{i+1} over P and let Q_i be the rational place of F_i under F_{i+1}. Then we have

$$t_{i+1}(P_{i+1})^q + c_{i+1}t_{i+1}(P_{i+1}) = t_i(P_i), \quad \text{and}$$
$$t_{i+1}(Q_{i+1})^q + c_{i+1}t_{i+1}(Q_{i+1}) = t_i(Q_i) = t_i(P_i) + \alpha_i,$$

where $\alpha_i \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i)$. Hence for $\alpha_{i+1} = t_{i+1}(Q_{i+1}) - t_{i+1}(P_{i+1})$, we have $\varphi_{i+1}(\alpha_{i+1}) \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i)$, which means $\alpha_{i+1} \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_{i+1})$.

Next we consider the remaining case that $\dim \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i \circ \varphi_{i+1}) = \dim \mathrm{Ker}\,(\varphi_1 \circ \cdots \circ \varphi_i)$. In this case we have

$$\dim(\mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i) \cap \mathrm{Im}\, \varphi_{i+1}) = \dim \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i) - 1.$$

If Q_i is a rational place of F_i over P such that $t_i(Q_i) - t_i(P_i) \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i) \cap \mathrm{Im}\, \varphi_{i+1}$, then as in the first case Q_i totally splits in F_{i+1}/F_i and for each rational place Q_{i+1} of F_{i+1} over Q_i, there exists $\alpha_{i+1} \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i \circ \varphi_{i+1})$ such that $t_{i+1}(Q_{i+1}) - t_{i+1}(P_{i+1}) = \alpha_{i+1}$. It remains to prove that if Q_i is a rational place of F_i such that $t(Q_i) - t(P_i) \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i) \setminus \mathrm{Im}\, \varphi_{i+1}$, then there is no rational place of F_{i+1} over Q_i. Indeed, otherwise we have $t_i(P_i) \in \mathrm{Im}\, \varphi_{i+1}$ and $t_i(Q_i) \in \mathrm{Im}\, \varphi_{i+1}$. But this implies that $t_i(Q_i) - t_i(P_i) \in \mathrm{Im}\, \varphi_{i+1}$, which is a contradiction. □

Next we will show that F_m/F is Galois. We begin with a lemma.

Lemma 6.3. *For $m \geq 1$, we have $\dim \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_m) = m$.*

Proof. For $m = 1$, the lemma is obvious. For $m \geq 2$, it is enough to prove that for each $1 \leq i \leq m-1$, we have $\dim \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_{i+1}) = \dim \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i) + 1$. Assume the contrary and let i be the smallest integer such that $\dim \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_{i+1}) \neq \dim \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i) + 1$. Then $\dim \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_{i+1}) = \dim \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_i)$ and using Proposition 6.2 we obtain that $N(F_{i+1}) \leq N(F_i)$. However this is a contradiction since we have $N(F_j) = 1 + q^{2n} + (q-1)q^{n+\frac{k}{2}+j}$ for each $1 \leq j \leq m$ by construction. □

Assume that $m \geq 1$ and $a \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_m)$. Let $a^{(m)} = a$ and for $1 \leq i \leq m-1$ let $a^{(i)} = (\varphi_{i+1} \circ \cdots \circ \varphi_m)(a)$. Note that $F_m = \mathbb{F}_{q^{2n}}(u, v, t_1, \ldots, t_m)$. Let Φ_a be the map on F_m fixing F and given by

$$\Phi_a : F_m \to F_m$$
$$t_i \mapsto t_i + a^{(i)} \quad \text{for } 1 \leq i \leq m.$$

It is easy to observe that $\Phi_a(t_1^q + c_1 t_1) = u$ and $\Phi_a(t_{i+1}^q + c_{i+1}t_{i+1}) = t_i$ for $1 \leq i \leq m-1$. Therefore Φ_a is an automorphism of F_m fixing F. For $a_1, a_2 \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_m)$ and $1 \leq i \leq m$ we have $a_1^{(i)} + a_2^{(i)} = (a_1 + a_2)^{(i)}$. This implies that $\left(\Phi_{a_2} \circ \Phi_{a_1}\right)(t_i) = \Phi_{a_1+a_2}(t_i)$, for $1 \leq i \leq m$.

We have proved the following theorem. We recall that F_m corresponds to $\widetilde{F}$ of Theorem 5.17.

Theorem 6.4. *For $m \geq 1$, the extension F_m/F is Galois and its Galois group is*

$$\mathrm{Aut}(F_m/F) = \{\Phi_a : a \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_m)\} \cong \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{e \cdot m \text{ times}},$$

where $q = p^e$. Moreover if $a_1, a_2 \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_m)$, then $\Phi_{a_1+a_2} = \Phi_{a_1} \circ \Phi_{a_2}$.

From here until the end of this section we further assume that F is maximal. This means $h = \frac{k}{2} \leq n$. It follows from Proposition 5.1 that there exists a polynomial $R_m[X]$ of degree q^n in $\mathbb{F}_{q^{2n}}[X]$ such that F_m is the same as the function field $\mathbb{F}_{q^{2n}}(t_m, s_m)$, where $s_m^q - s_m = t_m R_m(t_m)$. For simplicity of notation we also denote s_m and t_m as z and x respectively. Using Theorem 5.17, we get $b \in \mathbb{F}_{q^{2n}} \setminus \{0\}$ with $b^{q^n} + b = 0$ and $R_m(X) = bX^{q^n}$. Therefore $F_m = \mathbb{F}_{q^{2n}}(x, z)$ with $z^q - z = bx^{q^n+1}$.

First we consider the case $n = 1$. Since the map $x \mapsto x^{q+1}$ is the norm map on $\mathbb{F}_{q^2}$, there exists $\beta \in \mathbb{F}_{q^2}$ such that $\beta^{q+1} = -1$. Let $z_1 = \frac{z}{b} \in F_m$ and $x_1 = \frac{x}{\beta} \in F_m$. We have

$$z^q - z = b^q z_1^q - b z_1 = b^q (z_1^q + z_1), \quad \text{and}$$
$$b x^{q+1} = -b^q (\beta x_1)^{q+1} = b^q x_1^{q+1}.$$

Therefore $F_m = \mathbb{F}_{q^2}(x_1, z_1)$ with $z_1^q + z_1 = x_1^{q+1}$, which means that F_m is the Hermitian function field over $\mathbb{F}_{q^2}$ in the case $n = 1$.

From now on we assume that $n \geq 2$. Let $U_b \subseteq \mathbb{F}_{q^{2n}}$ be the $\mathbb{F}_q$-linear space of dimension $n-1$ consisting of the roots of the additive polynomial $bX + b^q X^q + \cdots + b^{q^{n-1}} X^{q^{n-1}} \in \mathbb{F}_{q^{2n}}[X]$. For $\beta \in U_b$, we have $\beta^{q^n} + \beta = 0$. Recall that the Hermitian function field H over $\mathbb{F}_{q^{2n}}$ is $\mathbb{F}_{q^{2n}}(x, y)$ with $y^{q^n} + y = x^{q^n+1}$. For $\beta \in U_b$, let Ψ_β be the automorphism on H given by

$$\begin{aligned} \Psi_\beta : H &\to H \\ x &\mapsto x, \\ y &\mapsto y + \beta. \end{aligned}$$

For $\beta_1, \beta_2 \in U_b$ we have $\Psi_{\beta_1} \circ \Psi_{\beta_2} = \Psi_{\beta_1+\beta_2}$. Hence $\{\Psi_\beta : \beta \in U_b\}$ is a group of automorphisms of H fixing $\mathbb{F}_{q^{2n}}(x)$ and of order q^{n-1}.

Proposition 6.5. *F_m is a subfield of H, the extension H/F_m is Galois and its automorphism group is* $\mathrm{Aut}(H/F_m) = \{\Psi_\beta : \beta \in U_b\}$.

Proof. Let $z = -(by + b^q y^q + \cdots + b^{q^{n-1}} y^{q^{n-1}})$ be the element of H. For $\beta \in U_b$, as β is a root of the additive polynomial $bT + b^q T^q + \cdots + b^{q^{n-1}} T^{q^{n-1}}$, z is fixed by Ψ_β. Using $b^{q^n} = -b$ we obtain that $z^q - z = bx^{q^n+1}$. Therefore F_m is fixed by $\{\Psi_\beta : \beta \in U_b\}$. As $[H : \mathbb{F}_{q^{2n}}(x)] = q^n$ and $[F_m : \mathbb{F}_{q^{2n}}(x)] = q$, we get $[H : F_m] = q^{n-1} = |U_b|$, which completes the proof. □

When $m = 0$, Proposition 6.5 proves that F is a Galois subfield of the Hermitian function field H over $\mathbb{F}_{q^{2n}}$ and it also computes the Galois group $\mathrm{Aut}(H/F)$. From now on we assume that $m \geq 1$.

Since F_m is maximal, there exist exactly q^{2n+1} elements $(a, w) \in \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}}$ satisfying $w^w - w = ba^{q^n+1}$. For $a, w \in \mathbb{F}_{q^{2n}}$ with $w^q - w = ba^{q^n+1}$, the map

$$\begin{aligned} \Theta_{a,w} : F_m = \mathbb{F}_{q^{2n}}(x, z) &\to F_m \\ x &\mapsto x + a \\ z &\mapsto z - \left(b a^{q^n} x + b^q a^{q^{n+1}} x^q + \cdots + b^{q^{n-1}} a^{q^{2n-1}} x^{q^{n-1}} \right) + w \end{aligned}$$

defines an automorphism of F_m fixing $\mathbb{F}_{q^{2n}}$. For $a_1, a_2, w_1, w_2 \in \mathbb{F}_{q^{2n}}$ with $w_i^q - w_i = b a_i^{q^n+1}$ for $1 \leq i \leq 2$, if

$$w = w_1 + w_2 - \left(b a_2^{q^n} a_1 + b^q a_2^{q^{n+1}} a_1^q + \cdots + b^{q^{n-1}} a_2^{q^{2n-1}} a_1^{q^{n-1}} \right) \tag{6.1}$$

and $a = a_1 + a_2$, then $w^q - w = ba^{q^n+1}$. Moreover we have

$$\Theta_{a_1,w_1} \circ \Theta_{a_2,w_2} = \Theta_{a,w}. \tag{6.2}$$

We have proved the following proposition.

Proposition 6.6. *The set*

$$\{\Theta_{a,w} : a, w \in \mathbb{F}_{q^{2n}},\ w^q - w = ba^{q^n+1}\}$$

is a subgroup of order q^{2n+1} *in* $\mathrm{Aut}(F_m/\mathbb{F}_{q^{2n}})$.

Remark 6.7. For $a_1, a_2, w_1, w_2 \in \mathbb{F}_{q^{2n}}$ with $w_i^q - w_i = ba_i^{q^n+1}$ for $1 \le i \le 2$, we observe that

$$\Theta_{a_1,w_1} \circ \Theta_{a_1,w_2} = \Theta_{a_2,w_2} \circ \Theta_{a_1,w_1} \iff \mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_q}(ba_1a_2^{q^n}) = 0.$$

Note that $\{\Phi_a : a \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_m)\}$ is a subgroup of order q^{n-h} in $\mathrm{Aut}(F_m/F) \le \mathrm{Aut}(F_m/\mathbb{F}_{q^{2n}})$. In the next proposition we will prove that $\{\Phi_a : a \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_m)\}$ is even a subgroup of $\{\Theta_{a,w} : a, w \in \mathbb{F}_{q^{2n}},\ w^q - w = ba^{q^n+1}\}$.

Proposition 6.8. *For* $a \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_m)$*, there exists a uniquely determined* $w \in \mathbb{F}_{q^{2n}}$ *such that* $w^q - w = ba^{q^n+1}$ *and* $\Phi_a = \Theta_{a,w}$.

Proof. For any $w \in \mathbb{F}_{q^{2n}}$ with $w^q - w = ba^{q^n+1}$ we have

$$\begin{aligned}&\left[w - (ba^{q^n}x + b^q a^{q^{n+1}}x^q + \cdots + b^{q^{n-1}}a^{q^{2n-1}}x^{q^{n-1}})\right]^q \\ &\quad - \left[w - (ba^{q^n}x + b^q a^{q^{n+1}}x^q + \cdots + b^{q^{n-1}}a^{q^{2n-1}}x^{q^{n-1}})\right] \\ &= bax^{q^n} + ba^{q^n}x^q + ba^{q^n+1}.\end{aligned}$$

Therefore the additive polynomial

$$A(T) = T^q - T - (bax^{q^n} + ba^{q^n}x + ba^{q^n+1}) \in \mathbb{F}_{q^{2n}}(x)[T] \tag{6.3}$$

splits into linear factors as

$$A(T) = \prod_{w^q - w = ba^{q^n+1}} \left(T + (ba^{q^n}x + b^q a^{q^{n+1}}x^q + \cdots + b^{q^{n-1}}a^{q^{2n-1}}x^{q^{n-1}}) - w\right). \tag{6.4}$$

Note that $z \in F_m$, $z^q - z = bx^{q^n+1}$ and $\Phi_a(x) = x + a$. Therefore

$$(\Phi_a(z) - z)^q - (\Phi_a(z) - z) = bax^{q^n} + ba^{q^n}x + ba^{q^n+1}. \tag{6.5}$$

Using (6.3)–(6.5) we complete the proof. □

Notation 6.9. For $a \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_m)$, we denote the uniquely determined $w \in \mathbb{F}_{q^{2n}}$ such that $w^q - w = ba^{q^n+1}$ and $\Phi_a = \Theta_{a,w}$ (cf. Proposition 6.8) as w_a.

Remark 6.10. As $\{\Phi_a : a \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_m)\}$ is a commutative group, if F_m is maximal, then using Remark 6.7 and Proposition 6.8, for $a_1, a_2 \in \mathrm{Ker}(\varphi_1 \circ \cdots \circ \varphi_m)$ we get $\mathrm{Tr}_{\mathbb{F}_{q^{2n}}/\mathbb{F}_q}(ba_1a_2^{q^n}) = 0$.

Now we recall some known results on the automorphism group $\mathrm{Aut}(H/\mathbb{F}_{q^{2n}})$ of H fixing $\mathbb{F}_{q^{2n}}$. We refer the reader to [1] for the details of these facts. The automorphism group $\mathcal{A} = \mathrm{Aut}(H/\mathbb{F}_{q^{2n}})$ is isomorphic to the projective unitary group $\mathrm{PGU}(3, q^{2n})$. Let P_∞ be the unique pole of x in H. Let $\mathcal{A}(P_\infty)$ be the subgroup of $\mathcal{A}$ given by

$$\mathcal{A}(P_\infty) = \{\sigma \in \mathcal{A} : \sigma P_\infty = P_\infty\}.$$

The unique p-Sylow subgroup $\mathcal{A}_1(P_\infty)$ of $\mathcal{A}(P_\infty)$ consists of the automorphisms

$$\begin{aligned}\sigma : H &\to H \\ x &\mapsto x + \alpha \\ y &\mapsto y + \alpha^{q^n}x + \beta,\end{aligned}$$

where $\alpha \in \mathbb{F}_{q^{2n}}$, $\beta^{q^n} + \beta = \alpha^{q^n+1}$, and hence $|\mathcal{A}_1(P_\infty)| = q^{3n}$.

The elements of $\mathcal{A}_1(P_\infty)$ can be identified with the tuples $[\alpha,\beta]\in\mathbb{F}_{q^{2n}}\times\mathbb{F}_{q^{2n}}$ such that $\beta^{q^n}+\beta=\alpha^{q^n+1}$. The group law in $\mathcal{A}_1(P_\infty)$ is

$$[\alpha_1,\beta_1]\cdot[\alpha_2,\beta_2]=[\alpha_1+\alpha_2,\alpha_1\alpha_2^{q^n}+\beta_1+\beta_2].$$

For $[\alpha,\beta]\in\mathcal{A}_1(P_\infty)$, we observe that the restriction of the automorphism $[\alpha,\beta]$ of F on F_m is the automorphism $\Theta_{\alpha,w}$ of F_m, where

$$w=-(b\beta+b^q\beta^q+\cdots+b^{q^{n-1}}\beta^{q^{n-1}}).$$

Indeed $[\alpha,\beta]$ sends $z=-(by+b^q y^q+\cdots+b^{q^{n-1}}\beta^{q^{n-1}})$ to

$$\begin{aligned}&z-\left\{b(\alpha^{q^n}x+\beta)+b^q(\alpha^{q^{n+1}}x^q+\beta^q)+\cdots+b^{q^{n-1}}(\alpha^{q^{2n-1}}x^{q^{n-1}}x^{q^{n-1}}+\beta^{q^{n-1}})\right\}\\&\quad=z-\left(b\alpha^{q^n}+b^q\alpha^{q^{n+1}}+\cdots+b^{q^{n-1}}\alpha^{q^{2n-1}}x^{q^{n-1}}\right)+w,\end{aligned}$$

where $w=-\left(b\beta+b^q\beta^q+\cdots+b^{q^{n-1}}\beta^{q^{n-1}}\right)$.

Since both F and F_m are maximal, for any $\alpha\in\mathbb{F}_{q^{2n}}$, both of the polynomials

$$T^{q^n}+T-\alpha^{q^n+1}\quad\text{and}\quad T^q-T-b\alpha^{q^n+1}$$

split into linear factors in $\mathbb{F}_{q^{2n}}$. Moreover recall that the group $\{\Theta_{\alpha,w}:\alpha,w\in\mathbb{F}_{q^{2n}},w^q-w=b\alpha^{q^n+1}\}$ has order q^{2n+1} and $|\mathcal{A}_1(P_\infty)|=q^{3n}$. Therefore the restriction of the group $\mathcal{A}_1(P_\infty)$ on F_m is the group $\{\Theta_{\alpha,w}:\alpha,w\in\mathbb{F}_{q^{2n}},w^q-w=b\alpha^{q^n+1}\}$. For each $\Theta_{\alpha,w}$ with $\alpha,w\in\mathbb{F}_{q^{2n}}$ and $w^q-w=b\alpha^{q^n+1}$, there are exactly q^{n-1} distinct $\beta\in\mathbb{F}_{q^{2n}}$ such that the restriction of $[\alpha,\beta]$ on F_m is $\Theta_{\alpha,w}$ and these β's are exactly the roots of the polynomial

$$b^{q^{n-1}}T^{q^{n-1}}+\cdots+b^qT^q+bT+w. \tag{6.6}$$

Now we define a subset $\mathcal{C}$ of $\mathcal{A}_1(P_\infty)$. We will show that $\mathcal{C}$ is a subgroup of $\mathcal{A}_1(P_\infty)$ and the corresponding fixed subfield $H^{\mathcal{C}}$ will be F.

Definition 6.11. For $\alpha\in\mathrm{Ker}(\varphi_1\circ\cdots\circ\varphi_m)$, recall that w_α is the uniquely determined element of $\mathbb{F}_{q^{2n}}$ given in Proposition 6.8 (cf. Notation 6.9). Let $\mathcal{C}$ be the subset

$$\mathcal{C}=\left\{[\alpha,\beta]\in\mathcal{A}_1(P_\infty):\alpha\in\mathrm{Ker}(\varphi_1\circ\cdots\circ\varphi_m),b^{q^{n-1}}\beta^{q^{n-1}}+\cdots+b^q\beta^q+w_\alpha=0\right\}.$$

As $\dim\mathrm{Ker}(\varphi_1\circ\cdots\circ\varphi_m)=m$ and the polynomial in (6.6) splits for any w_α with $\alpha\in\mathrm{Ker}(\varphi_1\circ\cdots\circ\varphi_m)$, we have $|\mathcal{C}|=q^{n-h}\cdot q^{n-1}=q^{2n-h-1}$.

Next we show that $\mathcal{C}$ is a subgroup. For $[\alpha_1,\beta_1]$, $[\alpha_2,\beta_2]\in\mathcal{C}$, let $[\alpha,\beta]=[\alpha_1,\beta_1]\cdot[\alpha_2,\beta_2]$. Then $\alpha=\alpha_1+\alpha_2$ and $\beta=\alpha_1\alpha_2^{q^n}+\beta_1+\beta_2$. Using (6.1) and (6.2) we get

$$w_{\alpha_1+\alpha_2}=w_{\alpha_1}+w_{\alpha_2}-\left(b\alpha_2^{q^n}\alpha_1+b^q\alpha_2^{q^{n+1}}\alpha_1^q+\cdots+b^{q^{n-1}}\alpha_2^{q^{2n-1}}\alpha_1^{q^{n-1}}\right). \tag{6.7}$$

Moreover

$$\begin{aligned}&b\beta+b^q\beta^q+\cdots+b^{q^{n-1}}\beta^{q^{n-1}}=b(\alpha_1\alpha_2^{q^n}+\beta_1+\beta_2)+b^q(\alpha_1^q\alpha_2^{q^{n+1}}+\beta_1^q+\beta_2^q)\\&+\cdots+b^{q^{n-1}}(\alpha_1^{q^{n-1}}\alpha_2^{q^{2n-1}}+\beta_1^{q^{n-1}}+\beta_2^{q^{n-1}})\\&=-w_{\alpha_1}-w_{\alpha_2}+\left(b\alpha_1\alpha_2^{q^n}+b^q\alpha_1^q\alpha_2^{q^{n+1}}+\cdots+b^{q^{n-1}}\alpha_1^{q^{n-1}}\alpha_2^{q^{2n-1}}\right).\end{aligned} \tag{6.8}$$

From (6.7) and (6.8) we obtain that $[\alpha,\beta]\in\mathcal{C}$ and hence $\mathcal{C}$ is a subgroup.

It follows from Definition 6.11 and Proposition 6.8 that the restriction of $\mathcal{C}$ on F_m is the group $\{\Phi_\alpha:\alpha\in\mathrm{Ker}(\varphi_1\circ\cdots\circ\varphi_m)\}$. Therefore any $\sigma\in\mathcal{C}$ fixes F and hence F is a subfield of the fixed subfield $H^{\mathcal{C}}$ of H corresponding to $\mathcal{C}$. Moreover $[H:H^{\mathcal{C}}]=|\mathcal{C}|=q^{2n-h-1}$ and $[H:F]=[H:F_m][F_m:F]=q^{n-1}q^{n-h}=q^{2n-h-1}$. Therefore $F=H^{\mathcal{C}}$. We have proved the following theorem.

Theorem 6.12. *Assume that F is maximal. The subset $\mathcal{C}$ in Definition 6.11 is a subgroup of $\mathcal{A}_1(P_\infty)$ and F is the fixed subfield $H^{\mathcal{C}}$ of H corresponding to $\mathcal{C}$.*

Acknowledgements

The authors would like to thank Prof. Mike Zieve for some useful correspondence. The authors would also like to thank Prof. Arnaldo Garcia for his interest in this work.

The authors would like to thank the anonymous referee for useful suggestions.

The first author would like to thank the Institut de Mathématiques de Luminy, CNRS, Marseille, France, for hospitality. The first author was supported by TÜBİTAK.

The research of the second author is partially supported by the Turkish Academy of Sciences in the framework of Young Scientists Award Programme (F.Ö./TÜBA-GEBIP/2003-13).

References

[1] A. Garcia, H. Stichtenoth, C.P. Xing, On subfields of the Hermitian function field, Compos. Math. 120 (2) (2000) 137–170.
[2] G. van der Geer, M. van der Vlugt, Reed–Muller codes and supersingular curves. I, Compos. Math. 84 (3) (1992) 333–367.
[3] L.C. Grove, Classical Groups and Geometric Algebra, American Mathematical Society, Providence, 2002.
[4] C. Güneri, Artin–Schreier curves and weights of two-dimensional cyclic codes, Finite Fields Appl. 10 (4) (2004) 481–505.
[5] G. Lachaud, Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, C. R. Acad. Sci. Paris 305 (1987) 729–732.
[6] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[7] H. Niederreiter, C. Xing, Rational Points on Curves over Finite Fields: Theory and Applications, Cambridge University Press, Cambridge, 2001.
[8] F. Özbudak, H. Stichtenoth, Curves with many points and configurations of hyperplanes over finite fields, Finite Fields Appl. 5 (4) (1999) 436–449.
[9] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, Berlin, 1993.
[10] M.A. Tsfasman, S.G. Vladut, Algebraic–Geometric Codes, Kluwer, Dordrecht, 1991.