ACTA ARITHMETICA
LXXV.4 (1996)

Explicit global function fields over the binary field with many rational places

by

HARALD NIEDERREITER (Wien) and CHAOPING XING (Hefei)

1. Introduction. In a series of papers [6], [7], [21], the authors developed methods for the construction of multidimensional low-discrepancy sequences by the use of global function fields. A survey of these methods can be found in [8]. In most cases, the construction of low-discrepancy sequences is optimized by choosing a global function field with many rational places (as usual, a rational place is meant to be a place of degree 1). It is well known that global function fields with many rational places also play an important role in algebraic coding theory, namely in the construction of good algebraic-geometry codes; see the books of Stichtenoth [16] and Tsfasman and Vlădut [17]. Global function fields with many rational places have also received a lot of attention in theoretical considerations related to global function fields and to algebraic curves over finite fields. We refer e.g. to the work of Ihara [5] and Serre [11]–[14] in the 1980s and to the more recent papers of Garcia and Stichtenoth [2], [3], Perret [9], Schoof [10], van der Geer and van der Vlugt [18], and Xing [20].

For the practical implementation of the constructions of low-discrepancy sequences and algebraic-geometry codes mentioned above, it is imperative that global function fields with many rational places are available in as explicit a form as possible, preferably in terms of generators and defining equations. In these applications the most important case is the one in which the full constant field of the global function field is the binary field $\mathbb{F}_2$, and only this case will be considered in the present paper. In this case, most examples of global function fields with many rational places have been obtained by means of class field theory (see the work of Serre quoted above), but this method rarely yields explicit forms of the global function fields.

For a global function field K with full constant field $\mathbb{F}_2$ we write $g(K)$ for its genus and $N(K)$ for the number of rational places of K. If $s \geq 1$ is a

The research of the second author was supported by the Chinese Natural Science Foundation.

given dimension and K is such that $N(K) \geq s+1$, then under some minor additional conditions the constructions in [7] and [21] yield s-dimensional low-discrepancy sequences, so-called digital (t,s)-sequences in base 2, where the quality parameter t is given by $t = g(K)$. Our main aim in this paper is to find explicitly described fields K with small $g(K)$ and relatively large $N(K)$ which allow the construction of s-dimensional low-discrepancy sequences for $1 \leq s \leq 20$. Our examples are listed in Section 3 and are obtained in most cases from Artin–Schreier extensions or cyclotomic function fields, or from subfields of the latter. We need some new results on cyclotomic function fields and certain subfields thereof, and these results are presented in Section 2.

2. Cyclotomic function fields. Let x be an indeterminate over $\mathbb{F}_2$, $R = \mathbb{F}_2[x]$ the polynomial ring, $F = \mathbb{F}_2(x)$ its quotient field, and F^{ac} an algebraic closure of F. We often use the convention that an irreducible polynomial P in R is identified with the place of F which is the zero of P, and we will denote this place also by P. For an arbitrary place Q of a global function field we write ν_Q for the normalized discrete valuation corresponding to Q.

We employ the theory of cyclotomic function fields as developed by Hayes [4]. Consider the two elements $\phi, \mu \in \mathrm{End}_{\mathbb{F}_2}(F^{\mathrm{ac}})$ given by

$$\phi(u) = u^2, \quad \mu(u) = xu \quad \text{for all } u \in F^{\mathrm{ac}}.$$

There is a ring homomorphism

$$R \to \mathrm{End}_{\mathbb{F}_2}(F^{\mathrm{ac}}), \quad f(x) \mapsto f(\phi + \mu).$$

The $\mathbb{F}_2$ vector space F^{ac} is made into an R-module by

$$u^{f(x)} = f(\phi+\mu)(u) \quad \text{for } u \in F^{\mathrm{ac}}.$$

This R-module is in fact a Carlitz module; see Carlitz [1] and Hayes [4]. For $M \in R, M \neq 0$, we define the R-module

$$\Lambda_M = \{z \in F^{\mathrm{ac}} : z^M = 0\}$$

of division points. The following facts from [4] will be needed.

Proposition 1 (Hayes [4]). (1) *Let $M \in R, M \neq 0$, have degree d. Then z^M is a separable polynomial in z of degree 2^d over R.*

(2) *Λ_M is a cyclic R-module which is naturally R-isomorphic to $R/(M)$.*

(3) *Let $F(\Lambda_M)$ be the subfield of F^{ac} generated over F by all elements of Λ_M. Then $F(\Lambda_M)/F$ is an abelian extension and $\mathrm{Gal}(F(\Lambda_M)/F)$ is isomorphic to $(R/(M))^*$, the group of units of the ring $R/(M)$. The Galois automorphism σ_A associated with the element $\overline{A} \in (R/(M))^*$ is determined by $\sigma_A(\lambda) = \lambda^A$ for $\lambda \in \Lambda_M$.*

(4) *If $P \in R$ is an irreducible polynomial not dividing M, then the Artin symbol*

$$\left[\frac{F(\Lambda_M)/F}{P}\right]$$

of P is equal to σ_P.

(5) *The infinite place of F, i.e., the pole of x, splits completely in the extension $F(\Lambda_M)/F$. In particular, $\mathbb{F}_2$ is the full constant field of $F(\Lambda_M)$.*

(6) *Suppose that $P \in R$ is an irreducible polynomial of degree d and $P^m \parallel M$ for some integer $m \geq 1$. Then the ramification index of P for the extension $F(\Lambda_M)/F$ is*

$$\Phi(P^m) = 2^{d(m-1)}(2^d - 1).$$

(7) *If $M = P^n$ for some integer $n \geq 1$ and irreducible polynomial $P \in R$ of degree d, then*:

(i) *P is the unique ramified place and it is totally ramified in the extension $F(\Lambda_M)/F$. The genus of $F(\Lambda_M)$ is given by*

$$g(F(\Lambda_M)) = \tfrac{1}{2}((dn-2)\Phi(P^n) - 2^{d(n-1)}d + 2).$$

(ii) *$f(z) = z^{P^n}/z^{P^{n-1}}$ is an Eisenstein polynomial in $R[z]$ with respect to the place P. If $\lambda \in F(\Lambda_M)$ is a root of $f(z)$ and Q is the unique place of $F(\Lambda_M)$ lying over P, then λ is a Q-prime element, i.e., $\nu_Q(\lambda) = 1$.*

Remark 1. Some parts of Proposition 1 are not stated explicitly as results in [4], but can be easily derived from them. Part (5) follows from [4, Proposition 1.4 and Theorem 3.2] and [16, Corollary III.8.4(a)]. Part (6) follows from [4, Propositions 1.4 and 2.2] and Abhyankar's lemma [16, Proposition III.8.9]. The formula $\nu_Q(\lambda) = 1$ in part (7)(ii) can be found in the proof of [4, Proposition 2.4].

The field $F(\Lambda_M)$ described in Proposition 1(3) is called a *cyclotomic function field.* We need some additional results on certain special cyclotomic function fields.

THEOREM 1. *Let $M = P_1P_2$ be the product of two distinct irreducible polynomials $P_1, P_2 \in R$. Then*:

(1) *The genus $g = g(F(\Lambda_M))$ of $F(\Lambda_M)$ is given by*

$$g = d_1(2^{d_1-1} - 1)(2^{d_2} - 1) + d_2(2^{d_1} - 1)(2^{d_2-1} - 1) - (2^{d_1} - 1)(2^{d_2} - 1) + 1,$$

where d_i is the degree of P_i for $i = 1, 2$.

(2) *$F(\Lambda_M) = F(z)$ with $z \in \Lambda_M$ satisfying the equation*

$$z\frac{z^M}{z^{P_1}z^{P_2}} = 0.$$

Proof. (1) By [4, Proposition 1.4], $F(\Lambda_M)$ is the compositum of $F(\Lambda_{P_1})$ and $F(\Lambda_{P_2})$. It follows therefore from Proposition 1(7)(i) and [16, Corollary III.8.4(b)] that P_1 and P_2 are the only ramified places in the extension $F(\Lambda_M)/F$. For $i = 1, 2$ let Q_i be a place of $F(\Lambda_M)$ lying over P_i. Then Proposition 1(6) shows that the ramification index $e(Q_i|P_i)$ is $2^{d_i} - 1$. This means that Q_1 and Q_2 are both tamely ramified. Hence it follows from the Hurwitz genus formula, in the form given in [16, Corollary III.5.6], that

$$2g - 2 = (-2)[F(\Lambda_M) : F] + d_1(2^{d_1} - 2)(2^{d_2} - 1) + d_2(2^{d_1} - 1)(2^{d_2} - 2),$$

which yields the desired result.

(2) Let z be a generator of the cyclic R-module Λ_M, then it easily follows that $F(\Lambda_M) = F(z)$; see also [4, p. 81]. By Proposition 1(3), the minimal polynomial $f(u)$ of z over F is given by

$$f(u) = \prod_A (u - z^A),$$

where A runs through a set of representatives of $(R/(M))^*$. The result follows now from the identities

$$u^M = \prod_{A \bmod M} (u - z^A), \quad u^{P_1} = \prod_{A \bmod P_1} (u - z^{AP_2}), \quad u^{P_2} = \prod_{A \bmod P_2} (u - z^{AP_1}). \blacksquare$$

We now consider certain subfields of the cyclotomic function fields $F(\Lambda_{x^n})$. The following elementary lemma is needed. Here and in the following, $\log_2$ denotes the logarithm to the base 2.

LEMMA 1. *For an integer $n \geq 2$ let H be the cyclic subgroup of $(R/(x^n))^*$ generated by the element $\overline{x+1}$. Then the order of H is*

$$|H| = 2^{\lfloor \log_2(n-1) \rfloor + 1}.$$

Proof. Since $(R/(x^n))^*$ has order 2^{n-1}, we have $|H| = 2^k$ for some integer $k \geq 1$. It remains to note that for integers $h \geq 1$ we have $(x+1)^{2^h} - 1 = x^{2^h} \equiv 0 \bmod x^n$ if and only if $2^h \geq n$, that is, if and only if $h \geq \lfloor \log_2(n-1) \rfloor + 1$. ■

According to Proposition 1(3) it is legitimate to identify $\mathrm{Gal}(F(\Lambda_{x^n})/F)$ with $(R/(x^n))^*$, and this will be done in the following.

THEOREM 2. *For $n \geq 2$ let $G = (R/(x^n))^*$ be the Galois group of the extension $F(\Lambda_{x^n})/F$ and let H be the cyclic subgroup of G generated by $\overline{x+1}$. Suppose that K is the subfield of $F(\Lambda_{x^n})$ fixed by H. Then*:

(1) *The number $N(K)$ of rational places of K is given by*

$$N(K) = 2^{n-k} + 1,$$

where $k = \lfloor \log_2(n-1) \rfloor + 1$.

(2) *The genus $g(K)$ of K is given by*

$$g(K) = 1 + (n-3)2^{n-k-2} - \sum_{j=0}^{k-1} 2^{2^j - j - 2}.$$

Proof. (1) The infinite place of F splits completely and the place x is totally ramified in the extension $F(\Lambda_{x^n})/F$, in view of parts (5) and (7)(i) of Proposition 1. Hence these two places of F contribute $[K:F]+1$ rational places to the field K. By Proposition 1(4), the Artin symbol

$$\left[\frac{F(\Lambda_{x^n})/F}{x+1}\right]$$

corresponds to the element $\overline{x+1} \in (R/(x^n))^*$, and so the place $x+1$ splits completely in the extension K/F (see [19, p. 182]). Thus

$$N(K) = 2[K:F]+1 = 2\frac{[F(\Lambda_{x^n}):F]}{|H|} + 1 = 2^{n-k}+1,$$

where we used Lemma 1 in the last step.

(2) Let P be the unique place of K lying over the place x of F and let Q be the unique place of $F(\Lambda_{x^n})$ lying over P. In order to determine $g(K)$, it suffices to compute the different exponent $d(Q|P)$. Let $\lambda \in \Lambda_{x^n}$ be a root of $f(z) = z^{x^n}/z^{x^{n-1}}$, then λ is a Q-prime element by Proposition 1(7)(ii). Furthermore, the minimal polynomial of λ over K is

$$h(z) = \prod_{\sigma \in H} (z + \sigma(\lambda)) \in K[z].$$

From Proposition 1(7)(i) we know that Q is totally ramified, hence it follows from [16, Proposition III.5.12] that

$$d(Q|P) = \nu_Q(h'(\lambda)) = \sum_{\sigma \in H \setminus \{\mathrm{id}\}} \nu_Q(\lambda + \sigma(\lambda)) = \sum_{i=1}^{r-1} \nu_Q(\lambda + \lambda^{(x+1)^i}),$$

where $r = 2^k = 2^{\lfloor \log_2(n-1) \rfloor + 1}$ (compare also with Lemma 1). For $1 \le i \le r-1$ we have

$$\lambda + \lambda^{(x+1)^i} = \lambda + \sum_{j=0}^{i} \binom{i}{j} \lambda^{x^j} = \sum_{j=1}^{\min(i,n-1)} \binom{i}{j} \lambda^{x^j}.$$

By induction on j one shows that $\nu_Q(\lambda^{x^j}) = 2^j$ for $0 \le j \le n-1$. It follows that

$$\nu_Q(\lambda + \lambda^{(x+1)^i}) = 2^e,$$

where e is the least integer with $1 \le e \le \min(i, n-1)$ and $\binom{i}{e} \equiv 1 \bmod 2$. The Lucas congruence for binomial coefficients yields $e = 2^{e_i}$, the largest power of 2 dividing i. Note also that $1 \le i \le r-1 < 2^k$, hence

$$e_i \le k-1 = \lfloor \log_2(n-1) \rfloor,$$

and so indeed $e = 2^{e_i} \le \min(i, n-1)$. Thus we have shown

$$\nu_Q(\lambda + \lambda^{(x+1)^i}) = 2^{2^{e_i}} \qquad \text{for } 1 \le i \le r-1.$$

A straightforward computation then yields

$$d(Q|P) = \sum_{j=0}^{k-1} 2^{2^j + k - j - 1}.$$

By the Hurwitz genus formula, in the form given in [16, Theorem III.4.12], we have

$$2g(F(\Lambda_{x^n})) - 2 = (2g(K) - 2)[F(\Lambda_{x^n}) : K] + d(Q|P).$$

Our formula for $g(K)$ follows from the last two identities and from Proposition 1(7)(i). ■

Next we show that the fields K in Theorem 2 can be obtained by a tower of extensions, with a known defining equation in each step of the tower. For the simplest case $n = 2$ we note that

$$z^{x^2} = z^4 + (x^2 + x)z^2 + x^2 z = z(z+x)(z^2 + xz + x),$$

thus a generator λ_2 of Λ_{x^2} satisfies $\lambda_2^2 + x\lambda_2 = x$, that is, $\lambda_2^x = x$. This explains the choice $\lambda_1 = x$ in the following theorem.

THEOREM 3. *Let E_n be the field $F(\Lambda_{x^n})$ with Galois group $G_n = (R/(x^n))^*$ over F, let H_n be the cyclic subgroup of G_n generated by $\overline{x+1}$, and let K_n be the subfield of E_n fixed by H_n. Put $\lambda_1 = x$, and for $n \ge 2$ let λ_n be a generator of Λ_{x^n} satisfying $\lambda_n^x = \lambda_{n-1}$. Put $\mu_1 = x$, and for $n \ge 2$ let μ_n be the norm*

$$\mu_n = N_{E_n/K_n}(\lambda_n) = \prod_{i=0}^{2^{k_n}-1} \lambda_n^{(x+1)^i}$$

with $k_n = \lfloor \log_2(n-1) \rfloor + 1$. Then $K_n = K_{n-1}(\mu_n)$ for $n \ge 2$, with μ_n satisfying the equation $\mu_n = \mu_{n-1}$ if $n-1$ is a power of 2 and

$$\mu_n^2 + \Big(\mu_n + \prod_{i=0}^{2^{k_n}-1} (\lambda_n^{(x+1)^i} + x)\Big)\mu_n + \mu_{n-1} = 0$$

if $n-1$ is not a power of 2.

Remark 2. We will see in the following proof that if $n-1$ is not a power of 2, then

$$\mu_n + \prod_{i=0}^{2^{k_n}-1} (\lambda_n^{(x+1)^i} + x) = \mathrm{Tr}_{K_n/K_{n-1}}(\mu_n) \in K_{n-1}.$$

Proof of Theorem 3. For $n \geq 2$ the automorphism $\sigma \in G_n$ corresponding to $\overline{x^{n-1}+1}$ leaves E_{n-1} invariant, since $E_{n-1} = F(\lambda_{n-1})$ and

$$\sigma(\lambda_{n-1}) = \lambda_{n-1}^{x^{n-1}+1} = \lambda_n^{x(x^{n-1}+1)} = \lambda_n^x = \lambda_{n-1}.$$

Together with $[E_n : E_{n-1}] = 2$ this shows that

$$\mathrm{Gal}(E_n/E_{n-1}) = \{\overline{1}, \overline{x^{n-1}+1}\} \subseteq G_n.$$

From this it follows easily that

$$\mathrm{Gal}(E_n/K_{n-1}) = \langle \overline{x+1}, \overline{x^{n-1}+1} \rangle \subseteq G_n.$$

In particular, we obtain $K_{n-1} \subseteq K_n$.

If $n-1$ is a power of 2, then $\overline{x^{n-1}+1} = \overline{(x+1)^{n-1}}$, and so $K_n = K_{n-1}$. If $n-1$ is not a power of 2, then $\mathrm{Gal}(K_n/K_{n-1}) \simeq \mathrm{Gal}(E_n/K_{n-1})/\mathrm{Gal}(E_n/K_n)$ has order 2 since $\overline{x^{n-1}+1} \notin H_n$. Therefore $[K_n : K_{n-1}] = 2$.

Next we determine the relationship between $\mu_n \in K_n$ and $\mu_{n-1} \in K_{n-1}$. First let $n = 2$. Then

$$\mu_2 = \lambda_2 \cdot \lambda_2^{x+1} = \lambda_2(x + \lambda_2) = \lambda_2^x = \lambda_1 = \mu_1.$$

For $n \geq 3$ consider again the automorphism $\sigma \in G_n$ corresponding to $\overline{x^{n-1}+1}$. Let τ be the restriction of σ to K_n. Then

$$\begin{aligned}\mu_n\tau(\mu_n) &= \mu_n \prod_{i=0}^{2^{k_n}-1} \sigma(\lambda_n^{(x+1)^i}) = \mu_n \prod_{i=0}^{2^{k_n}-1} \lambda_n^{(x^{n-1}+1)(x+1)^i} \\ &= \mu_n \prod_{i=0}^{2^{k_n}-1} \lambda_n^{(x+1)^i + x^{n-1}} = \prod_{i=0}^{2^{k_n}-1} \lambda_n^{(x+1)^i} \cdot \prod_{i=0}^{2^{k_n}-1} (\lambda_n^{(x+1)^i} + \lambda_n^{x^{n-1}}).\end{aligned}$$

Note that $\alpha_n = \lambda_n^{x^{n-1}}$ satisfies $\alpha_n^x = 0$, thus $\alpha_n^2 + x\alpha_n = 0$, hence $\alpha_n = x$. Therefore

$$\mu_n\tau(\mu_n) = \prod_{i=0}^{2^{k_n}-1} ((\lambda_n^{(x+1)^i})^2 + x\lambda_n^{(x+1)^i}) = \prod_{i=0}^{2^{k_n}-1} (\lambda_n^{(x+1)^i})^x = \prod_{i=0}^{2^{k_n}-1} \lambda_{n-1}^{(x+1)^i}.$$

If $n-1$ is a power of 2, then $\tau = \mathrm{id}$ on K_n and $k_{n-1} = k_n - 1$. Thus

$$\mu_{n-1}^2 = \Big(\prod_{i=0}^{2^{k_{n-1}}-1} \lambda_{n-1}^{(x+1)^i}\Big)^2 = \prod_{i=0}^{2^{k_{n-1}}-1} \lambda_{n-1}^{(x+1)^i} \cdot \prod_{i=2^{k_{n-1}}}^{2^{k_n}-1} \lambda_{n-1}^{(x+1)^i}$$
$$= \prod_{i=0}^{2^{k_n}-1} \lambda_{n-1}^{(x+1)^i} = \mu_n\tau(\mu_n) = \mu_n^2,$$

and so $\mu_n = \mu_{n-1}$. If $n-1$ is not a power of 2, then $\tau \neq \mathrm{id}$ on K_n and $\mathrm{Gal}(K_n/K_{n-1}) = \{\mathrm{id}, \tau\}$. Also $k_{n-1} = k_n$, therefore

$$N_{K_n/K_{n-1}}(\mu_n) = \mu_n\tau(\mu_n) = \prod_{i=0}^{2^{k_n}-1} \lambda_{n-1}^{(x+1)^i} = \mu_{n-1}.$$

The same argument shows that

$$\mathrm{Tr}_{K_n/K_{n-1}}(\mu_n) = \mu_n + \prod_{i=0}^{2^{k_n}-1} (\lambda_n^{(x+1)^i} + x),$$

and so we obtain the equation for μ_n in the theorem.

In the case where $n-1$ is not a power of 2, it remains to show that $\mu_n \notin K_{n-1}$. Let P_n be the unique place of E_n lying over x. By induction on n one shows that

$$\nu_{P_n}(\lambda_n) = 1 \quad \text{for all } n \geq 1;$$

compare also with Proposition 1(7)(ii). Now for $i \geq 0$,

$$\lambda_n^{(x+1)^i} = \sum_{j=0}^{\min(i,n-1)} \binom{i}{j} \lambda_n^{x^j} = \sum_{j=0}^{\min(i,n-1)} \binom{i}{j} \lambda_{n-j},$$

thus $\nu_{P_n}(\lambda_n^{(x+1)^i}) = 1$, and so $\nu_{P_n}(\mu_n) = 2^{k_n}$. Note that

$$[E_n : K_{n-1}] = [E_n : K_n][K_n : K_{n-1}] = 2^{k_n+1}.$$

Let Q be the unique place of K_{n-1} lying over x. If we had $\mu_n \in K_{n-1}$, then we would arrive at the contradiction

$$2^{k_n} = \nu_{P_n}(\mu_n) = 2^{k_n+1}\nu_Q(\mu_n). \ \blacksquare$$

Remark 3. From Theorem 3 we get $\mu_2 = \mu_3 = x$, and μ_4 satisfies

$$\mu_4^2 + x^2(x+1)\mu_4 + x = 0.$$

Put

$$y = \frac{\mu_4}{x^2(x+1)} + \frac{1}{x+1},$$

then

$$y^2 + y = \frac{(x+1)^2}{x^3}$$

and $K_4 = F(\mu_4) = \mathbb{F}_2(x, y)$.

3. Explicit global function fields with many rational places. In this section we list examples of global function fields K with full constant field $\mathbb{F}_2$ for which the genus $g(K)$ is small and the number $N(K)$ of rational places is relatively large. These examples are explicit in the sense that the fields K are described in terms of generators and defining equations. Furthermore, these examples allow the construction of good s-dimensional low-discrepancy sequences for $1 \le s \le 20$, and also for some larger dimensions.

Some of the examples are based on Artin–Schreier extensions. For the convenience of the reader we collect the basic facts about these extensions in Proposition 2 below, where we deal only with the case of the constant field $\mathbb{F}_2$. The stated results are special cases of [16, Proposition III.7.8].

Proposition 2. *Let K be a global function field with full constant field $\mathbb{F}_2$. For given $u \in K$ consider the extension field $E = K(y)$ with y satisfying the equation*

$$y^2 + y = u.$$

For each place P of K the well-defined integer m_P is determined as follows: $m_P = -1$ if $\nu_P(u + z^2 + z) \ge 0$ for some $z \in K$, and $m_P = m$ if there is a $z \in K$ with $\nu_P(u + z^2 + z) = -m < 0$ and m odd. Suppose that there is at least one place Q of K with $m_Q > 0$. Then $[E : K] = 2$, $\mathbb{F}_2$ is the full constant field of E, and

$$g(E) = 2g(K) - 1 + \frac{1}{2}\sum_P (m_P + 1)\deg(P),$$

where the sum runs over all places P of K. Furthermore, P is unramified in the extension E/K if and only if $m_P = -1$, and P is totally ramified in E/K if and only if $m_P > 0$.

We recall the standard notation $N_2(g) = \max N(K)$, where the maximum is extended over all global function fields K of fixed genus g and with full constant field $\mathbb{F}_2$. Values of $N_2(g)$ are tabulated in Serre [12]; see also [7, Table 2]. An example of a function field K is called *optimal* if $N(K) = N_2(g(K))$. We do not list the trivial optimal example $g(K) = 0, N(K) = 3, K = F = \mathbb{F}_2(x)$ as a numbered example.

Example 1. $g(K) = 1, N(K) = 5, K = \mathbb{F}_2(x, y)$ with

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

This example is optimal and well known (see e.g. [16, p. 191]). There are two rational places of K lying over each of x and $x+1$, and there is a totally ramified place of K lying over the infinite place of F.

Example 2. $g(K) = 2, N(K) = 6, K = \mathbb{F}_2(x, y)$ with

$$y^2 + y = \frac{x(x+1)}{x^3 + x + 1}.$$

This example is optimal and can be found also in Serre [14]. There are two rational places of K lying over each of the three rational places of F.

Example 3A. $g(K) = 3, N(K) = 7, K = F(\Lambda_{x^3+x+1}) = \mathbb{F}_2(x, y)$ with

$$y^7 + (x^4 + x^2 + x)y^3 + (x^4 + x^3 + x^2 + 1)y + x^3 + x + 1 = 0.$$

This example is optimal. All rational places of K lie over the infinite place of F; compare with Proposition 1(5).

Example 3B. Serre [11] gives the example $K = \mathbb{F}_2(x, y)$ with

$$y^3 + (x^2 + x + 1)y^2 + (x^3 + x^2)y + x^2 + x = 0,$$

which satisfies also $g(K) = 3, N(K) = 7$.

Example 4A. $g(K) = 4, N(K) = 8, K = \mathbb{F}_2(x, y_1, y_2)$ with

$$y_1^2 + y_1 = x^3 + x, \quad y_2^2 + y_2 = \frac{xy_1}{x+1}.$$

This example is optimal. There are four rational places of K lying over x and three rational places of K lying over $x+1$, and there is a totally ramified place of K lying over the infinite place of F. Note that of the two rational places of $L = \mathbb{F}_2(x, y_1)$ lying over $x+1$, one splits completely in the extension K/L and one is totally ramified in K/L.

Example 4B. Serre [14] gives the example $K = \mathbb{F}_2(x, y)$ with

$$(x^2 + x)y^3 + (x^3 + x^2 + 1)y^2 + x^3y + x^2 + 1 = 0,$$

which satisfies also $g(K) = 4, N(K) = 8$.

Example 5A. $g(K) = 5, N(K) = 9, K = \mathbb{F}_2(x, y_1, y_2)$ with

$$y_1^2 + y_1 = x^3 + x, \quad y_2^2 + y_2 = (x^2 + x)y_1.$$

This example is optimal. There are four rational places of K lying over each of x and $x + 1$, and there is a totally ramified place of K lying over the infinite place of F.

Example 5B. Let K be the subfield of $F(\Lambda_{x^6})$ fixed by the subgroup $\langle\overline{x+1}\rangle$ of $\mathrm{Gal}(F(\Lambda_{x^6})/F)$. Then $g(K) = 5$ and $N(K) = 9$ according to Theorem 2, and the rational places of K can be read off from the proof of this theorem. Note that Theorem 3 yields an explicit description of K since $K = K_6$ in the notation of this theorem.

Example 6. $g(K) = 6, N(K) = 10, K = \mathbb{F}_2(x, y_1, y_2)$ with

$$y_1^2 + y_1 = x^3 + x, \quad y_2^2 + y_2 = u := \frac{x^2(x+1)((x+1)y_1 + x^3)}{x^5 + x^4 + x^3 + x^2 + 1}.$$

This example is optimal. There are four rational places of K lying over each of x and $x+1$. The unique rational place P of $L=\mathbb{F}_2(x,y_1)$ lying over the infinite place of F splits completely in the extension K/L, thus yielding two more rational places of K. This is seen by a short calculation showing that

$$\nu_P\left(u+\left(\frac{y_1}{x}\right)^2+\frac{y_1}{x}\right)=3.$$

To calculate $g(K)$, one also has to study the splitting behavior of the place $p(x)=x^5+x^4+x^3+x^2+1$ of F. A standard application of Kummer's theorem shows that there are two different places P_1,P_2 of L lying over $p(x)$ which can be arranged in such a way that

$$y_1\equiv x^4+x \bmod P_1,\qquad y_1\equiv x^4+x+1 \bmod P_2.$$

Then $\nu_{P_1}(u)=-1$, hence $m_{P_1}=1$ in the notation of Proposition 2, and $\nu_{P_2}(u)\geq 0$, so that $m_{P_2}=-1$. Thus, P_1 is the only ramified place in the extension K/L and $\deg(P_1)=5$.

Example 7. $g(K)=7$, $N(K)=10$, $K=\mathbb{F}_2(x,y_1,y_2)$ with

$$y_1^2+y_1=x^3+x,\qquad y_2^2+y_2=\frac{x(x+1)}{x^3+x+1}.$$

This example is optimal. There are four rational places of K lying over each of x and $x+1$ and two rational places of K lying over the infinite place of F.

Example 8. $g(K)=8$, $N(K)=11$, $K=\mathbb{F}_2(x,y_1,y_2)$ with

$$y_1^2+y_1=\frac{x(x+1)}{x^3+x+1},\quad y_2^2+y_2=u:=\frac{x(x+1)(x^3+x+1)}{(x^2+x+1)^2}y_1+\frac{x(x+1)}{x^2+x+1}.$$

This example is optimal. There are four rational places of K lying over each of x and $x+1$. Of the two rational places of $L=\mathbb{F}_2(x,y_1)$ lying over the infinite place of F, one splits completely in the extension K/L and the other is totally ramified in K/L, which yields three more rational places of K. The only other ramified place in K/L is the unique place P of L with $\deg(P)=4$ lying over x^2+x+1. If we put

$$z=\frac{(x+1)y_1+1}{x^2+x+1}\in L,$$

then a straightforward calculation shows that $\nu_P(u+z^2+z)=-1$, so that $m_P=1$ in the notation of Proposition 2.

Example 9A. $g(K)=9, N(K)=12, K=\mathbb{F}_2(x,y_1,y_2)$ with

$$y_1^2+y_1=\frac{x(x+1)}{x^3+x+1},\qquad y_2^2+y_2=\frac{x(x+1)}{x^3+x^2+1}.$$

This example is optimal. There are four rational places of K lying over each of the three rational places of F.

Example 9B. Let $K = F(\Lambda_{(x^2+x+1)^2}) = \mathbb{F}_2(x, y)$ with

$$z^3 + (x^2 + x + 1)z + x^2 + x + 1 = 0,$$

where $z = y^4 + (x^2+x+1)y^2 + (x^2+x+1)y$. Then $g(K) = 9$ and $N(K) = 12$, and all rational places of K lie over the infinite place of F; compare with Proposition 1(5).

Example 10. $g(K) = 10, N(K) = 12, K = \mathbb{F}_2(x, y_1, y_2)$ with

$$y_1^2 + y_1 = \frac{x(x+1)}{x^3 + x + 1}, \qquad y_2^2 + y_2 = u := \frac{x(x+1)}{(x^3 + x + 1)(x^2 + x + 1)}.$$

According to Serre [12] we have $N_2(10) = 12$ or 13, but a recent communication by Serre [15] indicates that $N_2(10) = 13$, and so this example is not optimal. There are four rational places of K lying over each of the three rational places of F. There are exactly two ramified places in the extension K/L with $L = \mathbb{F}_2(x, y_1)$, namely the unique place of L lying over $x^2 + x + 1$ and the unique place P of L lying over x^3+x+1. To prove that P is ramified, put $z = xy_1$ and note that

$$u+z^2+z = \frac{y_1^2 + y_1}{x^2 + x + 1} + x^2y_1^2 + xy_1 = \frac{(x^3 + x + 1)(x + 1)}{x^2 + x + 1} y_1^2 + \frac{(x+1)^3}{x^2 + x + 1} y_1.$$

Since $\nu_P(y_1) = -1$, we get $\nu_P(u + z^2 + z) = -1$, and the rest follows from Proposition 2.

Example 11. $g(K) = 12, N(K) = 14, K = \mathbb{F}_2(x, y_1, y_2)$ with

$$y_1^7 + (x^4 + x^2 + x)y_1^3 + (x^4 + x^3 + x^2 + 1)y_1 + x^3 + x + 1 = 0, \qquad y_2^2 + y_2 = 1/x.$$

It is not known whether this example is optimal since $N_2(12)$ can be 14 or 15 according to Serre [12]. Note that $L = \mathbb{F}_2(x, y_1)$ is the cyclotomic function field $F(\Lambda_{x^3+x+1})$ in Example 3A. The principal divisor (x) in L is $Q - \sum_{i=1}^{7} P_i$, where Q is the place of degree 7 lying over x and the P_i, $1 \le i \le 7$, are the rational places lying over the infinite place of F. From this it follows that the P_i split completely in the extension K/L, producing all rational places of K, and that Q is the only ramified place in K/L.

Example 12. $g(K) = 13, N(K) = 15, K = \mathbb{F}_2(x, y_1, y_2, y_3)$ with

$$y_1^2 + y_1 = x^3 + x, \qquad y_2^2 + y_2 = \frac{xy_1}{x+1}, \qquad y_3^2 + y_3 = x(x + 1)y_2.$$

This example is optimal. The fact that $N_2(13) = 15$ was mentioned also in a recent communication by Serre [15]. Note that $L = \mathbb{F}_2(x, y_1, y_2)$ is the field in Example 4A. The seven rational places of L lying over x or $x + 1$ split completely in the extension K/L, whereas the rational place P of L lying over the infinite place of F is totally ramified in K/L. Furthermore, P is the only ramified place in K/L and $m_P = 11$ in the notation of Proposition 2.

EXAMPLE 13. $g(K)=14, N(K)=15, K=F(\Lambda_{x^4+x+1})=\mathbb{F}_2(x,y)$ with

$$y^{15}+(x^8+x^4+x^2+x)y^7+(x^8+x^6+x^5+x^4+x^3+x^2)y^3 \\ +(x^6+x^5+x^4+x^3+1)y+x^4+x+1=0.$$

It is not known whether this example is optimal since $N_2(14)$ can be 15 or 16 according to Serre [12]. All rational places of K lie over the infinite place of F; compare with Proposition 1(5).

EXAMPLE 14. $g(K)=15, N(K)=17, K$ is the subfield of $F(\Lambda_{x^7})$ fixed by the subgroup $\langle\overline{x+1}\rangle$ of $\mathrm{Gal}(F(\Lambda_{x^7})/F)$. This example is optimal. The rational places of K can be read off from the proof of Theorem 2. Note that Theorem 3 yields an explicit description of K since $K=K_7$ in the notation of this theorem.

EXAMPLE 15. $g(K)=17, N(K)=17, K=\mathbb{F}_2(x,y_1,y_2,y_3)$ with

$$y_1^2+y_1=x^3+x, \quad y_2^2+y_2=(x^2+x)y_1, \quad y_3^2+y_3=(x^2+x)y_2.$$

It is not known whether this example is optimal since $N_2(17)$ can be 17 or 18 according to Serre [12]. There are eight rational places of K lying over each of x and $x+1$, and there is a totally ramified place of K lying over the infinite place of F.

EXAMPLE 16. $g(K)=21, N(K)=21, K=F(\Lambda_{(x^2+x+1)(x^3+x+1)})=\mathbb{F}_2(x,y)$ with

$$y\{z^2(x+z+1)^3+z(x+z+1)^2(y^2+xy)+(x+z+1)(y^4+x^2y^2) \\ +(x^2+x+1)(x+z+1)\}+y^3+xy^2+(x+1)y+1=0$$

and $z=y^{x^2+x+1}=y^4+(x^2+x+1)y^2+(x^2+x+1)y$, where these equations are obtained from Theorem 1. This example is optimal. All rational places of K lie over the infinite place of F; compare with Proposition 1(5).

EXAMPLE 17. $g(K)=39, N(K)=33, K$ is the subfield of $F(\Lambda_{x^8})$ fixed by the subgroup $\langle\overline{x+1}\rangle$ of $\mathrm{Gal}(F(\Lambda_{x^8})/F)$. This example is optimal. The rational places of K can be read off from the proof of Theorem 2. Note that Theorem 3 yields an explicit description of K since $K=K_8$ in the notation of this theorem.

References

[1] L. Carlitz, *A class of polynomials*, Trans. Amer. Math. Soc. 43 (1938), 167–182.

[2] A. Garcia and H. Stichtenoth, *A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound*, Invent. Math. 121 (1995), 211–222.

[3] A. Garcia and H. Stichtenoth, *On the asymptotic behaviour of some towers of function fields over finite fields*, preprint, 1995.

[4] D. R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. 189 (1974), 77–91.

[5] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28 (1981), 721–724.

[6] H. Niederreiter and C. P. Xing, *Low-discrepancy sequences obtained from algebraic function fields over finite fields*, Acta Arith. 72 (1995), 281–298.

[7] —, —, *Low-discrepancy sequences and global function fields with many rational places*, Finite Fields Appl., to appear.

[8] —, —, *Quasirandom points and global function fields*, in: Finite Fields and Applications, S. D. Cohen and H. Niederreiter (eds.), Cambridge University Press, Cambridge, to appear.

[9] M. Perret, *Tours ramifiées infinies de corps de classes*, J. Number Theory 38 (1991), 300–322.

[10] R. Schoof, *Algebraic curves over $\mathbb{F}_2$ with many rational points*, ibid. 41 (1992), 6–14.

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

[12] —, *Nombres de points des courbes algébriques sur $\mathbb{F}_q$*, Sém. Théorie des Nombres 1982–1983, Exp. 22, Univ. de Bordeaux I, Talence, 1983.

[13] —, *Résumé des cours de 1983–1984*, Annuaire du Collège de France (1984), 79–83.

[14] —, *Rational Points on Curves over Finite Fields*, lecture notes, Harvard University, 1985.

[15] —, personal communication, August 1995.

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

[17] M. A. Tsfasman and S. G. Vlădut, *Algebraic-Geometric Codes*, Kluwer, Dordrecht, 1991.

[18] G. van der Geer and M. van der Vlugt, *Curves over finite fields of characteristic* 2 *with many rational points*, C. R. Acad. Sci. Paris Sér. I Math. 317 (1993), 593–597.

[19] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.

[20] C. P. Xing, *Multiple Kummer extension and the number of prime divisors of degree one in function fields*, J. Pure Applied Algebra 84 (1993), 85–93.

[21] C. P. Xing and H. Niederreiter, *A construction of low-discrepancy sequences using global function fields*, Acta Arith. 73 (1995), 87–102.

Institut für Informationsverarbeitung
Österreichische Akademie
der Wissenschaften
Sonnenfelsgasse 19
A-1010 Wien, Austria
E-mail: niederreiter@oeaw.ac.at

Department of Mathematics
University of Science and
Technology of China
Hefei, Anhui 230026, P.R. China

Received on 19.9.1995 (2868)