DEMONSTRATIO MATHEMATICA
Vol. XXX No 4 1997

Harald Niederreiter, Chaoping Xing

# GLOBAL FUNCTION FIELDS WITH MANY RATIONAL PLACES OVER THE QUINARY FIELD

## 1. Introduction

Let $q$ be an arbitrary prime power and let $K$ be a global function field with full constant field $\mathbb{F}_q$, i.e., with $\mathbb{F}_q$ algebraically closed in $K$. We use the notation $K/\mathbb{F}_q$ if we want to emphasize the fact that $\mathbb{F}_q$ is the full constant field of $K$. By a *rational place* of $K$ we mean a place of $K$ of degree 1. We write $g(K)$ for the genus of $K$ and $N(K)$ for the number of rational places of $K$. For fixed $g \geq 0$ and $q$ we put

$$N_q(g) = \max N(K),$$

where the maximum is extended over all global function fields $K/\mathbb{F}_q$ with $g(K) = g$. Equivalently, $N_q(g)$ is the maximum number of $\mathbb{F}_q$-rational points that a smooth, projective, absolutely irreducible algebraic curve over $\mathbb{F}_q$ of given genus $g$ can have. The calculation of $N_q(g)$ is a very difficult problem in algebraic geometry, so usually one has to make do with bounds for $N_q(g)$.

Global function fields $K/\mathbb{F}_q$ with many rational places, that is, with $N(K)$ reasonably close to $N_q(g(K))$ or to a known upper bound for $N_q(g(K))$, have received a lot of attention in the literature. Quite a number of papers on the subject have also been written in the language of algebraic curves over finite fields. The first systematic account of the subject was given by Serre [14], and for recent surveys we refer to Garcia and Stichtenoth [1] and Niederreiter and Xing [11]. The construction of global function fields with many rational places, or equivalently of algebraic curves over $\mathbb{F}_q$ with many $\mathbb{F}_q$-rational points, is of great theoretical interest. Moreover, it is also important for applications in the theory of algebraic-geometry codes (see [15], [16]) and in the recent constructions of low-discrepancy sequences introduced by the authors (see [5], [7], [10], [17]).

For the practical aspects of these applications it is important that the constructions of global function fields with many rational places be as explicit as possible. In the ideal case, one would like to have descriptions of the global function fields in terms of generators and defining equations. The constructions by Serre [14] use class field theory and are thus not explicit. More attention is now devoted to the desideratum of obtaining explicit constructions, see e.g. the recent papers of Niederreiter and Xing [6], [8] and the references given there.

The present paper can be viewed as a continuation of the work in [6] and [8] which led to catalogs of global function fields with many rational places for the cases $q = 2, 3, 4, 5$ and to many explicit constructions. We concentrate here on the case $q = 5$ and extend the list of constructions in [8, Section 5]. The motivation for this is the following one. For the construction of $s$-dimensional low-discrepancy sequences in a given base $q$ by means of rational places (see e.g. [5]) we need a global function field $K/\mathbb{F}_q$ with $N(K) \geq s+1$. In order to cover the standard range $1 \leq s \leq 50$ of applications of low-discrepancy sequences in an efficient manner, we need to find, for each dimension $s$ in this range, a global function field $K/\mathbb{F}_q$ of relatively small genus with $N(K) \geq s+1$. For $q = 5$ the constructions in [8, Section 5] allow us to cover only the range $1 \leq s \leq 29$, whereas the new results in the present paper cover the full range $1 \leq s \leq 50$.

In Section 2 we review some background and establish a new method of constructing global function fields with many rational places. In Section 3 we present our new examples for the case $q = 5$. Some of these examples are quite straightforward, but others require detailed arguments to validate them. The majority of the examples is based on explicit constructions.

## 2. Background for the constructions

Let $\mathbb{F}_q(x)$ be the rational function field over $\mathbb{F}_q$. We will often use the convention that a monic irreducible polynomial $P$ over $\mathbb{F}_q$ is identified with the place of $\mathbb{F}_q(x)$ which is the unique zero of $P$, and we will denote this place also by $P$. It will also be convenient to write $\infty$ for the "infinite place" of $\mathbb{F}_q(x)$, that is, for the place of $\mathbb{F}_q(x)$ which is the unique pole of $x$. For an arbitrary place $Q$ of a global function field $K$ we write $\nu_Q$ for the normalized discrete valuation corresponding to $Q$. For any $z \in K^*$ let $(z)$ denote the principal divisor of $z$.

Several examples in Section 3 are based on Artin-Schreier extensions and Kummer extensions. We will not review the theory of these extensions here since an excellent account of it is available in the book of Stichtenoth [15, Section III.7].

We recall some pertinent facts about Hilbert class fields. A convenient reference for this topic is Rosen [13]. Let $K$ be a global function field and $S$ a finite nonempty set of places of $K$. The *Hilbert class field* $H_S$ of $K$

with respect to $S$ is the maximal unramified abelian extension of $K$ (in a fixed separable closure of $K$) in which all places in $S$ split completely. The extension $H_S/K$ is finite with Galois group

$$\mathrm{Gal}(H_S/K) \simeq Cl_S,$$

where $Cl_S$ is the *S-divisor class group* of $K$, i.e., the quotient of the group of all divisors of $K$ of degree 0 with support outside $S$ by its subgroup of principal divisors. If $S = \{P\}$ is a singleton, then we also write $H_P$ instead of $H_S$. If $P$ is a rational place of $K$, then we also have

$$\mathrm{Gal}(H_P/K) \simeq \mathrm{Div}^0(K),$$

the group of divisor classes of $K$ of degree 0. In particular, we have $[H_P : K] = h(K)$, the divisor class number of $K$. The divisor class numbers appearing in Section 3 are calculated by the standard method based on the results in [15, Section V.1]. Furthermore, $\mathrm{Div}^0(K)$ is isomorphic to the fractional ideal class group $\mathrm{Pic}(A)$, where $A$ is the *P-integral ring* of $K$, i.e., $A$ consists of the elements of $K$ that are regular outside $P$. There is a standard identification between places of $K$ and prime ideals in $A$. The following new result is based on these concepts.

THEOREM 1. *Let $K/\mathbb{F}_q$ be a global function field and $L/\mathbb{F}_q$ a finite separable extension of $K$. Let $S = \{P, P_1, \ldots, P_m\}$ with $P$ a rational place of $K$ and $P_1, \ldots, P_m$ arbitrary places of $K$ different from $P$. Suppose that $S$ satisfies the following condition: either some place of $K$ not in $S$ is totally ramified in $L/K$ or some place in $S$ is inert in $L/K$. Let $T$ be the set of places of $L$ lying over those in $S$ and assume that the number $n$ of rational places in $T$ is positive. Then there exists a global function field $F/\mathbb{F}_q$ with*

$$g(F) = \frac{h(K)}{|G|}(g(L) - 1) + 1 \quad \textit{and} \quad N(F) \geq \frac{h(K)n}{|G|},$$

*where $G$ is the subgroup of* $\mathrm{Div}^0(K)$ *generated by the divisor classes of $P_1 - \deg(P_1)P, \ldots, P_m - \deg(P_m)P$.*

Proof. Let $\mathrm{Div}(K)$ be the group of divisor classes of $K$ and let $D$ be the subgroup of $\mathrm{Div}(K)$ generated by the divisor classes of $P, P_1, \ldots, P_m$. Since $S$ contains the rational place $P$, the group $\mathrm{Div}(K)$ is generated by $\mathrm{Div}^0(K)$ and $D$. Thus, from the exact sequence

$$(0) \to \mathrm{Div}^0(K)/(D \cap \mathrm{Div}^0(K)) \to Cl_S \to \mathrm{Div}(K)/\mathrm{Div}^0(K)D \to (0)$$

in the proof of [13, Lemma 1.2] we obtain

$$Cl_S \simeq \mathrm{Div}^0(K)/(D \cap \mathrm{Div}^0(K)),$$

where $Cl_S$ is the $S$-divisor class group of $K$. It follows that

$$r := |Cl_S| = \frac{h(K)}{|G|}.$$

From [13, Proposition 2.2] and the condition on $S$ we deduce that $r$ divides $|Cl_T|$, where $Cl_T$ is the $T$-divisor class group of $L$. Let $H_T$ be the Hilbert class field of $L$ with respect to $T$. Then $\mathrm{Gal}(H_T/L) \simeq Cl_T$ and $\mathbb{F}_q$ is the full constant field of $H_T$ since $n \geq 1$ (see [13, Theorem 1.3]). Let $F/\mathbb{F}_q$ be a subfield of the extension $H_T/L$ which is obtained as the fixed field of a subgroup of $Cl_T$ of order $\frac{1}{r}|Cl_T|$. Then $[F : L] = r$. Since $H_T/L$ is an unramified extension, the Hurwitz genus formula yields

$$g(F) - 1 = r(g(L) - 1) = \frac{h(K)}{|G|}(g(L) - 1).$$

Furthermore, all places in $T$ split completely in $F/L$, hence $N(F) \geq rn$. ∎

Finally, we collect some facts about Drinfeld modules and narrow ray class extensions. The book of Goss [2] and the survey article of Hayes [4] are suitable references for the theory of Drinfeld modules. Let $K/\mathbb{F}_q$ be a global function field with $N(K) \geq 1$ and distinguish a rational place $P$ of $K$. Let $H_P$ be the Hilbert class field of $K$ with respect to $P$ and let $A$ be the $P$-integral ring of $K$. Now let $\phi$ be a sign-normalized Drinfeld $A$-module of rank 1. By [4, Section 15] we can assume that $\phi$ is defined over $H_P$, i.e., that for each $y \in A$ the $\mathbb{F}_q$-endomorphism $\phi_y$ is a polynomial in the Frobenius with coefficients from $H_P$. If $\overline{H}_P$ is a fixed algebraic closure of $H_P$ and $M$ is a nonzero integral ideal in $A$, then we write $\Lambda_M$ for the $A$-submodule of $\overline{H}_P$ consisting of the $M$-division points. Let $E_M := H_P(\Lambda_M)$ be the subfield of $\overline{H}_P$ generated over $H_P$ by all elements of $\Lambda_M$. Then $E_M/K$ is called the *narrow ray class extension* of $K$ with modulus $M$.

The following facts on narrow ray class extensions can be found in [2, Section 7.5], [4, Section 16]. First of all, $\Lambda_M \simeq A/M$ as $A$-modules, so in particular $\Lambda_M$ is cyclic. The field $E_M$ is independent of the specific choice of the sign-normalized Drinfeld $A$-module $\phi$ of rank 1. Furthermore, $E_M/K$ is a finite abelian extension with

$$\mathrm{Gal}(E_M/K) \simeq \mathrm{Pic}_M(A) := \mathcal{I}_M(A)/\mathcal{P}_M(A),$$

where $\mathcal{I}_M(A)$ is the group of fractional ideals of $A$ that are prime to $M$ and $\mathcal{P}_M(A)$ is the subgroup of principal fractional ideals that are generated by elements $z \in K$ with $z \equiv 1 \bmod M$ and $\mathrm{sgn}(z) = 1$ (here sgn is the given sign function). We have $\mathrm{Gal}(E_M/H_P) \simeq (A/M)^*$, the group of units of the ring $A/M$. If $M = Q^n$ with a nonzero prime ideal $Q$ in $A$ and $n \geq 1$, then the order $\Phi_q(Q^n)$ of $(A/Q^n)^*$ is given by

$$\Phi_q(Q^n) = \left(q^d - 1\right) q^{d(n-1)},$$

where $d$ is the degree of the place of $K$ corresponding to $Q$. Again in this situation, $E_M/K$ is unramified away from $P$ and $Q$ and the decomposition group $D_P$ of $P$ in $E_M/K$ is the subgroup $D_P = \{c+M : c \in \mathbb{F}_q^*\}$ of $(A/M)^*$. Moreover, every place of $H_P$ lying over $Q$ is totally ramified in $E_M/H_P$.

In the special case where $K = \mathbb{F}_q(x)$, the theory of narrow ray class extensions reduces to that of cyclotomic function fields as developed by Hayes [3]. We note that cyclotomic function fields and narrow ray class extensions have already been used by Niederreiter and Xing [6], [8], [9], Quebbemann [12], and Xing and Niederreiter [18], [19] for the construction of global function fields with many rational places.

## 3. Constructions for the case $q = 5$

In this section we construct examples of global function fields $F$ with full constant field $\mathbb{F}_5$ and many rational places. A list of such examples for the genera $1 \le g \le 12$ was provided in [8, Section 5]. Now we consider the range $13 \le g \le 22$ and we also improve on the examples in [8] for $g = 7, 9, 10$, and 11. Note that together with the results in [8] this yields lower bounds for $N_5(g)$ for $1 \le g \le 22$. The notations and conventions introduced in Section 2 are used without further mention. We summarize the results in the following table.

**Table 1**

| $g(F)$ | 7 | 9 | 10 | 11 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $N(F)$ | 22 | 26 | 27 | 32 | 36 | 39 | 32 | 40 | 42 | 32 | 41 | 30 | 48 | 51 |

EXAMPLE 1. $g(F) = 7, N(F) = 22, F = \mathbb{F}_5(x, y)$ with

$$y^4 = (x^2 + 2)(x^4 - 2x^2 - 2).$$

The place $\infty$ splits into two rational places in the Kummer extension $F/\mathbb{F}_5(x)$, each with ramification index 2. The only other ramified places of $F$ are those lying over $x^2 + 2$ or $x^4 - 2x^2 - 2$. All rational places of $\mathbb{F}_5(x)$ different from $\infty$ split completely in $F/\mathbb{F}_5(x)$.

EXAMPLE 2. $g(F) = 9, N(F) = 26, F = \mathbb{F}_5(x, y_1, y_2)$ with

$$y_1^2 = x(x-1)(x-2), \qquad y_2^5 - y_2 = (x+2)y_1.$$

Note that $K = \mathbb{F}_5(x, y_1)$ satisfies $g(K) = 1$ and $N(K) = 8$. If $P_\infty$ is the place of $K$ lying over $\infty$, then

$$\nu_{P_\infty}\left((x+2)y_1 - \left(\frac{y_1}{x}\right)^5 + \frac{y_1}{x}\right) = \nu_{P_\infty}(y_1) = -3,$$

and so $P_\infty$ is totally ramified in the Artin-Schreier extension $F/K$. There are no other ramified places in $F/K$. Over each of $x, x-1$, and $x-2$ there is exactly one place of $K$, and each of these splits completely in $F/K$. The two places of $K$ lying over $x+2$ also split completely in $F/K$.

EXAMPLE 3. $g(F) = 10, N(F) = 27$. Consider the function field $K = \mathbb{F}_5(x,y)$ with

$$y^2 = x(x-1)(x^3-2x-2).$$

Then $g(K) = 2, N(K) = 7$, and $K$ has 13 places of degree 2, hence $h(K) = 36$. In $K$ we have $(x) = 2P_1 - 2P_\infty$ and $(x-1) = 2P_2 - 2P_\infty$. Now $F$ is obtained from Theorem 1 with $L = K$ and $S = \{P_\infty, P_1, P_2\}$. Note that $|G| = 4$ follows with the help of the Weierstrass gap theorem.

EXAMPLE 4. $g(F) = 11, N(F) = 32, F = \mathbb{F}_5(x, y_1, y_2)$ with

$$y_1^2 = x(x^2-2), \qquad y_2^5 - y_2 = \frac{x^4-1}{y_1-1}.$$

Note that $K = \mathbb{F}_5(x, y_1)$ satisfies $g(K) = 1$ and $N(K) = 10$. Let $P_\infty$ be the place of $K$ lying over $\infty$ and let $P_1 = (3,1)$ and $P_2 = (4,1)$, where $P = (a,b)$ is the rational place of $K$ determined by $(x, y_1) \equiv (a,b) \bmod P$. Since $\nu_{P_\infty}(y_1) = -3$, the principal divisor of $y_1 - 1$ in $K$ is given by

$$(y_1 - 1) = 2P_1 + P_2 - 3P_\infty.$$

Since $x-1, x-2, x+1$, and $x+2$ split completely in $K/\mathbb{F}_5(x)$, we have

$$(x^4-1) = \sum_{i=1}^{8} P_i - 8P_\infty,$$

and so

$$\left(\frac{x^4-1}{y_1-1}\right) = \sum_{i=3}^{8} P_i - P_1 - 5P_\infty.$$

Thus, $P_1$ is totally ramified in the Artin-Schreier extension $F/K$. A straightforward calculation shows that

$$\nu_{P_\infty}\left(\frac{x^4-1}{y_1-1} - \left(\frac{y_1}{x}\right)^5 + \frac{y_1}{x}\right) = -2,$$

and so $P_\infty$ is also totally ramified in $F/K$. The rational places $P_i, 3 \le i \le 8$, split completely in $F/K$.

EXAMPLE 5. $g(F) = 13, N(F) = 36$. Consider the function field $K = \mathbb{F}_5(x, y)$ with

$$y^2 = x(x-1)(x^3 + 2x + 1).$$

Then $g(K) = 2, N(K) = 9$, and $K$ has 8 places of degree 2, hence $h(K) = 48$. In $K$ we have $(x) = 2P_1 - 2P_\infty$ and $(x-1) = 2P_2 - 2P_\infty$. Now $F$ is obtained from Theorem 1 with $L = K$ and $S = \{P_\infty, P_1, P_2\}$, where we also note that $|G| = 4$.

EXAMPLE 6. $g(F) = 14, N(F) = 39$. Consider the function field $K = \mathbb{F}_5(x, y)$ with

$$y^2 = x(x-1)(x^3 - x + 2).$$

Then $g(K) = 2, N(K) = 9$, and $K$ has 12 places of degree 2, hence $h(K) = 52$. In $K$ we have $(x) = 2P_1 - 2P_\infty$ and $(x-1) = 2P_2 - 2P_\infty$. Now $F$ is obtained from Theorem 1 with $L = K$ and $S = \{P_\infty, P_1, P_2\}$, where we also note that $|G| = 4$.

EXAMPLE 7. $g(F) = 15, N(F) = 32, F = \mathbb{F}_5(x, y_1, y_2, y_3)$ with

$$y_1^2 = 3(x^4 + 2), \quad y_2^2 = x(x^2 - 2), \quad y_3^2 = (x+1)(x^2 + 2x - 1).$$

The field $K = \mathbb{F}_5(x, y_1)$ is that in [8, Example 5.1] and satisfies $g(K) = 1$ and $N(K) = 10$. The place $\infty$ is inert in $K/\mathbb{F}_5(x)$. If $L = \mathbb{F}_5(x, y_1, y_2)$, then the places of $L$ lying over $x, x^2 - 2$, or $\infty$ are the only ramified ones in the Kummer extension $L/K$ and the places of $L$ lying over $x - 1, x - 2, x + 1$, or $x + 2$ split completely in $L/K$. Thus we have $g(L) = 5$ and $N(L) = 18$. The only ramified places in the Kummer extension $F/L$ are those lying over $x + 1$ or $x^2 + 2x - 1$. The places of $L$ lying over $x, x - 1, x - 2$, or $x + 2$ split completely in $F/L$, hence $N(F) = 3 \cdot 8 + 2 \cdot 4 = 32$.

EXAMPLE 8. $g(F) = 16, N(F) = 40$. Consider the function field $K = \mathbb{F}_5(x, y_1)$ with

$$y_1^2 = x(x-1)(x+2)(x^2 + 2x - 1).$$

Then $g(K) = 2, N(K) = 8$, and $K$ has 9 places of degree 2, hence $h(K) = 40$. In $K$ we have $(x) = 2P_1 - 2P_\infty, (x-1) = 2P_2 - 2P_\infty$, and $(x+2) = 2P_3 - 2P_\infty$. Furthermore, let $L = K(y_2)$ with

$$y_2^2 = (x+1)(x^2 + 2x - 1).$$

The only ramified places in the Kummer extension $L/K$ are the two places of $K$ lying over $x + 1$, hence $g(L) = 4$. Now $F$ is obtained from Theorem 1 with $S = \{P_\infty, P_1, P_2, P_3\}$. Note that the condition on $S$ in Theorem 1 is satisfied since the two places of $K$ lying over $x + 1$ are totally ramified in $L/K$. Furthermore, we have $n = 8$ since all places in $S$ split completely in $L/K$, and also $|G| = 8$.

EXAMPLE 9. $g(F) = 17, N(F) = 42, F = \mathbb{F}_5(x, y_1, y_2)$ with

$$y_1^2 = x(x^2 - 2), \qquad y_2^5 - y_2 = \frac{x^4 - 1}{y_1}.$$

Note that $K = \mathbb{F}_5(x, y_1)$ satisfies $g(K) = 1$ and $N(K) = 10$. For the place $P_\infty$ of $K$ lying over $\infty$ we have $\nu_{P_\infty}(y_1) = -3$. The principal divisor of $y_1$ in $K$ is given by

$$(y_1) = P + Q_2 - 3P_\infty,$$

where $P$ is the rational place of $K$ lying over $x$ and $Q_2$ is the place of $K$ of degree 2 lying over $x^2 - 2$. It follows that $P$ and $Q_2$ are totally ramified in the Artin-Schreier extension $F/K$. A straightforward calculation shows that

$$\nu_{P_\infty}\left(\frac{x^4 - 1}{y_1} - \left(\frac{y_1}{x}\right)^5 + \frac{y_1}{x}\right) = -1,$$

and so $P_\infty$ is also totally ramified in $F/K$. The places $x - 1, x - 2, x + 1$, and $x + 2$ split completely in $F/\mathbb{F}_5(x)$, hence $N(F) = 4 \cdot 10 + 2 = 42$.

EXAMPLE 10. $g(F) = 18, N(F) = 32, F = \mathbb{F}_5(x, y_1, y_2)$ with

$$y_1^2 = (x^2 + 2)(x^4 - 2x^2 - 2), \qquad y_2^5 - y_2 = (y_1 - 1)x^2.$$

The field $K = \mathbb{F}_5(x, y_1)$ is that in [8, Example 5.2] and satisfies $g(K) = 2$ and $N(K) = 12$. All rational places of $\mathbb{F}_5(x)$ split completely in $K/\mathbb{F}_5(x)$. Let $Q$ and $R$ be the two places of $K$ lying over $\infty$. Then with an appropriate ordering of these two places,

$$y_1 = x^3 + O(x^{-1}) \quad \text{at } Q,$$
$$y_1 = -x^3 + O(x^{-1}) \quad \text{at } R,$$

and so

$$\nu_Q\left((y_1 - 1)x^2 - x^5 + x\right) = -2,$$
$$\nu_R\left((y_1 - 1)x^2 + x^5 - x\right) = -2.$$

It follows that $Q$ and $R$ are totally ramified in the Artin-Schreier extension $F/K$, and these are the only ramified places in $F/K$, hence $g(F) = 18$. The following rational places of $K$ split completely in $F/K$: the two places lying over $x$ and those four places $P$ lying over $x - 1, x - 2, x + 1$, or $x + 2$ with $y_1 \equiv 1 \bmod P$. Therefore $N(F) = 6 \cdot 5 + 2 = 32$.

EXAMPLE 11. $g(F) = 19, N(F) = 41, F = \mathbb{F}_5(x, y_1, y_2)$ with

$$y_1^5 - y_1 = x^4 - 1, \qquad y_2^2 = x^3 - 2x^2 - x - 2.$$

For $K = \mathbb{F}_5(x, y_1)$ we have $g(K) = 6$ and $N(K) = 21$. The place $\infty$ is totally ramified in the Artin-Schreier extension $K/\mathbb{F}_5(x)$ and $x - 1, x - 2, x + 1$, and $x + 2$ split completely in $K/\mathbb{F}_5(x)$. The places of $K$ lying over $x - 1, x - 2, x + 1$, or $x+2$ split completely in the Kummer extension $F/K$ and the place of $K$ lying over $\infty$ is totally ramified in $F/K$. The only other ramified places in $F/K$ are those places of $K$ lying over $x^3 - 2x^2 - x - 2$.

EXAMPLE 12. $g(F) = 20, N(F) = 30, F = \mathbb{F}_5(x, y_1, y_2)$ with

$$y_1^5 - y_1 = \frac{x^4 - 1}{x}, \qquad y_2^2 = 2(x^2 + x + 1).$$

The field $K = \mathbb{F}_5(x, y_1)$ is that in [8, Example 5.8] and satisfies $g(K) = 8$ and $N(K) = 22$. The places $x - 1, x - 2, x + 1$, and $x + 2$ split completely in $K/\mathbb{F}_5(x)$ and $x$ and $\infty$ are totally ramified in $K/\mathbb{F}_5(x)$. The places of $K$ lying over $x - 1, x - 2$, or $x + 2$ split completely in the Kummer extension $F/K$ and the only ramified places in $F/K$ are those lying over $x^2 + x + 1$.

EXAMPLE 13. $g(F) = 21, N(F) = 48$. Consider the function field $K = \mathbb{F}_5(x, y)$ with

$$y^2 = 2x(x^2 + 2x - 1).$$

Then $g(K) = 1$, $h(K) = 8$, and the place $x - 2$ is inert in $K/\mathbb{F}_5(x)$. In $K$ we have $(x - 2) = Q - 2P$ and $(x) = 2P_1 - 2P$, where $\deg(Q) = 2$ and $\deg(P) = \deg(P_1) = 1$. We distinguish the rational place $P$ of $K$ and denote by $A$ the $P$-integral ring of $K$. Let $E_Q/K$ be the narrow ray class extension of $K$ with modulus $Q$, then $[E_Q : K] = \Phi_5(Q)h(K) = 192$. Let $< \overline{P_1} >$ be the cyclic subgroup of $\mathrm{Pic}_Q(A) \simeq \mathrm{Gal}(E_Q/K)$ generated by the residue class $\overline{P_1}$ of $P_1$ modulo $\mathcal{P}_Q(A)$. Since $P_1^2 = xA$ and $x \equiv 2 \bmod Q$, we have $| < \overline{P_1} > | = 8$. Let $F$ be the subfield of $E_Q/K$ fixed by $< \overline{P_1} >$, then $[F : K] = 24$. Again from $x \equiv 2 \bmod Q$ we deduce that the decomposition group of $P$ in $E_Q/K$ is contained in $< \overline{P_1} >$, and so $P$ splits completely in $F/K$. By considering the Artin symbol, we see that $P_1$ also splits completely in $F/K$, hence $N(F) \geq 48$. The only ramified place in $F/K$ is $Q$. Let $R$ be a place of $F$ lying over $Q$. Then the inertia group of $R$ in $E_Q/F$ is $I \cap \mathrm{Gal}(E_Q/F)$, where $I = \mathrm{Gal}(E_Q/H_P) \simeq (A/Q)^*$. Now

$$|I \cap \mathrm{Gal}(E_Q/F)| = |(A/Q)^* \cap < \overline{P_1} > | = 4,$$

and so the ramification index of $Q$ in $F/K$ is

$$\frac{1}{4}[E_Q : H_P] = \frac{1}{4}\Phi_5(Q) = 6.$$

Consequently, $Q$ is tamely ramified in $F/K$, and so the Hurwitz genus formula yields $2g(F) - 2 = 24 \cdot (2 - 2) + (6 - 1) \cdot 8$, that is, $g(F) = 21$. Now $N_5(21) \leq 58$ by Serre's method (see [15, Proposition V.3.4]), and so we must have $N(F) = 48$.

EXAMPLE 14A. $g(F) = 22, N(F) = 51, F = \mathbb{F}_5(x, y_1, y_2)$ with

$$y_1^2 = x^5 - x + 1, \qquad y_2^5 - y_2 = (x^5 - x)y_1.$$

For $K = \mathbb{F}_5(x, y_1)$ we have $g(K) = 2$ and $N(K) = 11$. The place $\infty$ is totally ramified in the Kummer extension $K/\mathbb{F}_5(x)$ and all other rational places of $\mathbb{F}_5(x)$ split completely in $K/\mathbb{F}_5(x)$. The places of $K$ lying over the latter places split completely in the Artin-Schreier extension $F/K$. Let $P_\infty$ be the unique place of $K$ lying over $\infty$, then $\nu_{P_\infty}(y_1) = -5$. A simple calculation shows that

$$\nu_{P_\infty}\left((x^5 - x)y_1 - \left(\frac{y_1}{x}\right)^5 + \frac{y_1}{x}\right) = -7.$$

Thus, $P_\infty$ is totally ramified in $F/K$ and it is the only ramified place in $F/K$.

EXAMPLE 14B. $g(F) = 22, N(F) = 51$. Let $K = \mathbb{F}_5(x)$ and let $E_M = K(\Lambda_M)$ be the cyclotomic function field with the modulus $M$ being the principal ideal in $\mathbb{F}_5[x]$ generated by $x^4$ and with the distinguished rational place $\infty$ of $K$. Then $[E_M : K] = \Phi_5(M) = 500$. Let $D_\infty$ be the decomposition group of $\infty$ in $E_M/K$ and let $H$ be the subgroup of $\mathrm{Gal}(E_M/K) \simeq (\mathbb{F}_5[x]/M)^*$ generated by $D_\infty$ and $x + 1 + M$. Since $|D_\infty| = |\mathbb{F}_5^*| = 4$ and $x + 1 + M$ has order 5 in $(\mathbb{F}_5[x]/M)^*$, we have $|H| = 20$. Let $F$ be the subfield of $E_M/K$ fixed by $H$, then $[F : K] = 25$. The places $\infty$ and $x + 1$ split completely in $F/K$ by the construction of $F$ and the place $P = x$ is totally ramified in $F/K$, thus $N(F) = 2 \cdot 25 + 1 = 51$. Since $P$ is the only ramified place in $F/K$, it suffices to calculate its different exponent $d_P(F/K)$ to obtain $g(F)$. First of all, we have $d_P(E_M/K) = 15 \cdot 5^3$ by [3, Theorem 4.1]. We can write $H = \mathrm{Gal}(E_M/F)$ as

$$H = \{c(x+1)^j + M : c \in \mathbb{F}_5^*, 0 \le j \le 4\}.$$

Let $Q$ be the place of $F$ lying over $P$ and $R$ the place of $E_M$ lying over $P$. If $\lambda \in E_M$ is a generator of the cyclic $\mathbb{F}_5[x]$-module $\Lambda_M$, then $\nu_R(\lambda) = 1$ is shown in the proof of [3, Proposition 2.4]. Therefore, by [15, Proposition III.5.12] we obtain

$$d_Q(E_M/F) = \sum_{f \in H \setminus \{1+M\}} \nu_R(\lambda - \phi_f(\lambda)),$$

where $\phi_f$ denotes the action of the underlying Drinfeld module, which in this case of a cyclotomic function field is a Carlitz module (see [3]). From $\lambda \in \Lambda_M$ we get $\phi_M(\lambda) = 0$, and so it suffices to consider the system of representatives $c(x + 1)^j, c \in \mathbb{F}_5^*, 0 \le j \le 4$, of $H$. A simple calculation shows that

$$\nu_R(\lambda - \phi_f(\lambda)) = 5 \quad \text{if } c = 1 \text{ and } j \neq 0,$$

$$\nu_R(\lambda - \phi_f(\lambda)) = 1 \quad \text{if } c \neq 1,$$

and so $d_Q(E_M/F) = 4 \cdot 5 + 15 \cdot 1 = 35$. Now the tower formula for different exponents implies that

$$d_P(F/K) = \frac{d_P(E_M/K) - d_Q(E_M/F)}{e_Q(E_M/F)} = \frac{15 \cdot 5^3 - 35}{20} = 92,$$

where $e_Q(E_M/F)$ is the ramification index of $Q$ in $E_M/F$. Finally, the Hurwitz genus formula yields $2g(F) - 2 = -2 \cdot 25 + 92$, that is, $g(F) = 22$.

## References


[1] A. Garcia and H. Stichtenoth, *Algebraic function fields over finite fields with many rational places*, IEEE Trans. Inform. Th. 41 (1995), 1548–1563.

[2] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer, Berlin, 1996.

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

[4] D. R. Hayes, *A brief introduction to Drinfeld modules*, The Arithmetic of Function Fields (D. Goss, D.R. Hayes, and M.I. Rosen, eds.), pp. 1–32, W. de Gruyter, Berlin, 1992.

[5] H. Niederreiter and C. P. Xing, *Low-discrepancy sequences and global function fields with many rational places*, Finite Fields Appl. 2 (1996), 241–273.

[6] H. Niederreiter and C. P. Xing, *Explicit global function fields over the binary field with many rational places*, Acta Arith. 75 (1996), 383–396.

[7] H. Niederreiter and C. P. Xing, *Quasirandom points and global function fields*, Finite Fields and Applications (S. Cohen and H. Niederreiter, eds.), pp. 269–296, Cambridge University Press, Cambridge, 1996.

[8] H. Niederreiter and C. P. Xing, *Cyclotomic function fields, Hilbert class fields, and global function fields with many rational places*, Acta Arith. 79 (1997), 59–76.

[9] H. Niederreiter and C. P. Xing, *Drinfeld modules of rank 1 and algebraic curves with many rational points*. II, Acta Arith. 81 (1997), 81–100.

[10] H. Niederreiter and C. P. Xing, *The algebraic-geometry approach to low-discrepancy sequences*, Monte Carlo and Quasi-Monte Carlo Methods '96 (H. Niederreiter et al., eds.), Lecture Notes in Statistics, Vol. 127, pp. 139–160, Springer, New York, 1997.

[11] H. Niederreiter and C. P. Xing, *Algebraic curves over finite fields with many rational points*, Proc. Number Theory Conf. (Eger, 1996), W. de Gruyter, Berlin, to appear.

[12] H.-G. Quebbemann, *Cyclotomic Goppa codes*, IEEE Trans. Inform. Th. 34 (1988), 1317–1320.

[13] M. Rosen, *The Hilbert class field in function fields*, Expositiones Math. 5 (1987), 365–378.

[14] J.-P. Serre, *Rational Points on Curves over Finite Fields*, lecture notes, Harvard University, 1985.
[15] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.
[16] M. A. Tsfasman and S. G. Vlădut, *Algebraic-Geometric Codes*, Kluwer, Dordrecht, 1991.
[17] C. P. Xing and H. Niederreiter, *A construction of low-discrepancy sequences using global function fields*, Acta Arith. 73 (1995), 87–102.
[18] C. P. Xing and H. Niederreiter, *Modules de Drinfeld et courbes algébriques ayant beaucoup de points rationnels*, C.R. Acad. Sci. Paris Sér. I Math. 322 (1996), 651–654.
[19] C. P. Xing and H. Niederreiter, *Drinfeld modules of rank 1 and algebraic curves with many rational points*, preprint, 1996.

Harald Niederreiter
INSTITUT FÜR INFORMATIONSVERARBEITUNG
ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN
Sonnenfelsgasse 19
A–1010 WIEN, AUSTRIA
E-mail: niederreiter@oeaw.ac.at

Chaoping Xing
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA
HEFEI, ANHUI 230026, P.R. CHINA

*Received April 29, 1997.*