ACTA ARITHMETICA
LXXXIII.1 (1998)

Global function fields with many rational places over the ternary field

by

Harald Niederreiter (Wien) and Chaoping Xing (Wien)

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 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 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 [15], 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 [16], [17]) and in the recent constructions of low-discrepancy sequences introduced by the authors (see [5], [7], [10], [20]).

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

1991 *Mathematics Subject Classification*: 11G09, 11G20, 11R58, 14G15, 14H05.

the global function fields in terms of generators and defining equations. The constructions by Serre [15] 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 $q = 3$ and extend the list of constructions in [8, Section 3]. The motivation for this is the following. 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 $q = 3$ the constructions in [8, Section 3] allow us to cover only the range $1 \leq s \leq 27$, whereas the new results in the present paper cover the full range $1 \leq s \leq 50$ and, in fact, a much wider range. Similar work for $q = 5$ was carried out in [12].

In Section 2 we review some background and in Section 3 we establish two general principles for the construction of global function fields with many rational places. In Section 4 we present our new examples for the case $q = 3$. Some of these examples are quite straightforward, but others require detailed arguments to validate them. Many of the examples are 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 ∞ 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 ν_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 4 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 [16, Section III.7].

We recall some pertinent facts about Hilbert class fields. A convenient reference for this topic is Rosen [14]. 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

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

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 4 are calculated by the standard method based on the results in [16, 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.

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 ϕ be a sign-normalized Drinfeld A-module of rank 1. By [4, Section 15] we can assume that ϕ is defined over H_P, i.e., that for each $y \in A$ the $\mathbb{F}_q$-endomorphism ϕ_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 Λ_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 Λ_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 Λ_M is cyclic. The field E_M is independent of the specific choice of the sign-normalized Drinfeld A-module ϕ 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

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

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 (and also the inertia group) D_P of P in E_M/K is the subgroup

$$D_P = \{c + M : c \in \mathbb{F}_q^*\} \tag{1}$$

of $(A/M)^*$, so that in particular $|D_P| = q - 1$. Moreover, every place of H_P lying over Q is totally ramified in E_M/H_P. From the facts about Galois groups noted above it follows that $(A/M)^*$ can be viewed as a subgroup of $\mathrm{Pic}_M(A)$. Concretely, if we put

$$I_M = \{\overline{zA} : z \in A,\ \mathrm{sgn}(z) = 1,\ \nu_Q(z) = 0\}, \tag{2}$$

where the bar denotes the residue class mod $\mathcal{P}_M(A)$, then I_M is a subgroup of $\mathrm{Pic}_M(A)$ isomorphic to $(A/M)^*$. The decomposition group D_P can now be described as a subgroup of $\mathrm{Pic}_M(A)$ by

$$D_P = \{\overline{(\alpha + y)A} : \alpha \in \mathbb{F}_q^*,\ y \in A,\ \mathrm{sgn}(y) = 1,\ \nu_Q(y) \geq n\} \subseteq I_M. \tag{3}$$

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], [12], Quebbemann [13], Xing [19], and Xing and Niederreiter [21], [22] for the construction of global function fields with many rational places.

3. Two general construction principles. We present two general principles for the construction of global function fields with many rational places which will be used several times in Section 4. The first construction principle is based on certain subfields of narrow ray class extensions (see Section 2 for the fundamental facts about these extensions).

Let $K/\mathbb{F}_q$ be a global function field with $N(K) \geq 1$, let P be a distinguished rational place of K, and let A be the P-integral ring of K. Let $M = Q^n$ with $n \geq 1$ and a nonzero prime ideal Q in A, or equivalently Q is a place of K different from P. For m places $P_1, \ldots, P_m$ of K that are different from P and Q we define the multiplicative semigroup

$$S(P_1, \ldots, P_m) = \{f \in A : \mathrm{sgn}(f) = 1,\ \nu_R(f) = 0 \text{ for all } R \neq P, P_1, \ldots, P_m\}$$

of A and the subgroup

$$S_M(P_1, \ldots, P_m) = \{f + M \in (A/M)^* : f \in S(P_1, \ldots, P_m)\}$$

of $(A/M)^*$. In the following we use the notation introduced in (1)–(3). Furthermore, we write $\langle P_1, \ldots, P_m \rangle$ for the subgroup of $\mathrm{Pic}(A)$ generated by the ideal classes of $P_1, \ldots, P_m$ and $\langle S_M(P_1, \ldots, P_m), D_P\rangle$ for the subgroup of $(A/M)^*$ generated by $S_M(P_1, \ldots, P_m)$ and D_P, where we think of D_P as being given in the form (1).

LEMMA 1. *With the notation above, let G be the subgroup of* $\mathrm{Pic}_M(A)$ *generated by $\overline{P}_1, \ldots, \overline{P}_m$, and D_P. Then*

$$|G| = |\langle P_1, \ldots, P_m\rangle| \cdot |\langle S_M(P_1, \ldots, P_m), D_P\rangle|.$$

Proof. If I_M is as in (2), then it suffices to prove the following:

$$G \cap I_M = \langle S_M(P_1, \ldots, P_m), D_P\rangle, \tag{4}$$

$$\langle P_1, \ldots, P_m\rangle \simeq G/(G \cap I_M). \tag{5}$$

We first note that $G \cap I_M$ consists of all $\overline{zA} \in \mathrm{Pic}_M(A)$ with $z \in A$, $\mathrm{sgn}(z) = 1$, and

$$zA = \prod_{i=1}^{m} P_i^{n_i} \cdot (\alpha + y)A \cdot wA,$$

where $\alpha \in \mathbb{F}_q^*$, $y \in A$, $\mathrm{sgn}(y) = 1$, $\nu_Q(y) \geq n$, $w \in A$, $\mathrm{sgn}(w) = 1$, $w \equiv 1 \bmod M$, and $n_1, \ldots, n_m$ are nonnegative integers. Let

$$v = \frac{z}{(\alpha + y)w}.$$

Then $vA = \prod_{i=1}^{m} P_i^{n_i}$ with $\mathrm{sgn}(v) = 1$, hence $v \in S(P_1, \ldots, P_m)$. It follows that

$$\begin{aligned} G \cap I_M &= \{\overline{vA} \cdot \overline{(\alpha + y)A} \in \mathrm{Pic}_M(A) : v \in S(P_1, \ldots, P_m),\ \overline{(\alpha + y)A} \in D_P\} \\ &= \langle S_M(P_1, \ldots, P_m), D_P\rangle, \end{aligned}$$

which is (4). To prove (5), we consider the map $\theta : G \to \mathrm{Pic}(A)$ defined by

$$\theta : G \ni \overline{(\alpha + y)A} \cdot \prod_{i=1}^{m} \overline{P}_i^{n_i} \mapsto \prod_{i=1}^{m} P_i^{n_i} \in \mathrm{Pic}(A).$$

Note that θ is a well-defined map with image $\langle P_1, \ldots, P_m\rangle$. Furthermore, θ is a group homomorphism and its kernel is easily seen to be $G \cap I_M$. Thus (5) is shown. ■

THEOREM 1. *Let $P, P_1, \ldots, P_m$ be $m + 1$ distinct rational places of the global function field $K/\mathbb{F}_q$. Let E_M/K be the narrow ray class extension of K with modulus $M = Q^n$, where $n \geq 1$ and Q is a place of K of degree d which is different from $P, P_1, \ldots, P_m$. Put*

$$r = |\langle P_1, \ldots, P_m\rangle|, \qquad t = |\langle S_M(P_1, \ldots, P_m), D_P\rangle|,$$

and assume that $\gcd(t,q)=1$. *Then there exists a subfield F of E_M/K with*

$$\begin{aligned}[F:K] &= \frac{h(K)(q^d-1)q^{d(n-1)}}{rt},\\ 2g(F)-2 &= \frac{h(K)(q^d-1)q^{d(n-1)}}{rt}(2g(K)-2)\\ &\quad+\frac{dh(K)}{rt}(n(q^d-1)q^{d(n-1)}-q^{d(n-1)}-t+1),\\ N(F) &\ge (m+1)\frac{h(K)(q^d-1)q^{d(n-1)}}{rt}.\end{aligned}$$

Furthermore, if $d=1$ and the order of the ideal class of Q in $\mathrm{Pic}(A)$ *is prime to $h(K)/r$, then*

$$N(F)\ge\frac{h(K)}{r}+(m+1)\frac{h(K)(q-1)q^{n-1}}{rt}.$$

Proof. Let G be as in Lemma 1 and let F be the subfield of E_M/K fixed by $G\subseteq \mathrm{Pic}_M(A)\simeq \mathrm{Gal}(E_M/K)$. Since

$$[E_M:K]=h(K)\Phi_q(M)=h(K)(q^d-1)q^{d(n-1)},$$

the formula for $[F:K]$ in the theorem follows from Lemma 1. Since G contains the decomposition group D_P of P and the Artin symbols of $P_1,\dots,P_m$ in E_M/K, the places $P,P_1,\dots,P_m$ split completely in F/K. This yields the lower bound for $N(F)$ in the theorem.

In order to calculate the genus $g(F)$, we first observe that the only place of K that can be ramified in F/K is Q. If R is a place of F lying over Q, then the inertia group of R in E_M/F is $\mathrm{Gal}(E_M/F)\cap I_M$, where $I_M=\mathrm{Gal}(E_M/H_P)\simeq(A/M)^*$ is the inertia group of Q in E_M/K. Hence from (4) we find that the inertia group of R in E_M/F is $\langle S_M(P_1,\dots,P_m),D_P\rangle$. In particular, the ramification index $e_R(E_M/F)$ of R in E_M/F is t. From the condition $\gcd(t,q)=1$ we see that R is tamely ramified in E_M/F, and so the different exponent $d_R(E_M/F)$ of R in E_M/F is given by

$$d_R(E_M/F)=t-1.$$

Next we note that from the proof of [22, Proposition 2] we infer that the different exponent $d_Q(E_M/K)$ of Q in E_M/K is given by

$$d_Q(E_M/K)=n(q^d-1)q^{d(n-1)}-q^{d(n-1)}.$$

Thus, the tower formula for different exponents yields

$$\begin{aligned}d_Q(F/K)&=\frac{d_Q(E_M/K)-d_R(E_M/F)}{e_R(E_M/F)}\\ &=\frac{n(q^d-1)q^{d(n-1)}-q^{d(n-1)}-t+1}{t}.\end{aligned}$$

Since the ramification index $e_Q(F/K)$ of Q in F/K is

$$e_Q(F/K)=\frac{e_Q(E_M/K)}{e_R(E_M/F)}=\frac{|(A/M)^*|}{t}=\frac{(q^d-1)q^{d(n-1)}}{t},$$

the desired identity for $g(F)$ follows from the Hurwitz genus formula.

To prove the remaining part of the theorem, we denote by f the order of the ideal class of Q in $\mathrm{Pic}(A)$ and we observe that f is the relative degree of Q in H_P/K. Now any place of H_P lying over Q is totally ramified in E_M/H_P, and so f is also the relative degree of Q in E_M/K. The relative degree $f_Q(F/K)$ of Q in F/K divides

$$\frac{[F:K]}{e_Q(F/K)}=\frac{h(K)}{r}.$$

Thus, from the condition $\gcd(f,h(K)/r)=1$ it follows that $f_Q(F/K)=1$. In the case $d=1$ this yields

$$N(F)\ge\frac{h(K)}{r}+(m+1)\frac{h(K)(q-1)q^{n-1}}{rt}. \ ■$$

The following lemma describes a set of generators of the subgroup $S_M(P_1,\ldots,P_m)$ of $(A/M)^*$ in case a certain condition on $\langle P_1,\ldots,P_m\rangle$ is met. We again use the notation introduced at the beginning of this section.

LEMMA 2. *For $1\le i\le m$ let the ideal class of P_i have order r_i in the group* $\mathrm{Pic}(A)$ *and let $f_i\in A$ be such that* $\mathrm{sgn}(f_i)=1$ *and $f_iA=P_i^{r_i}$. If $\langle P_1,\ldots,P_m\rangle$ is the direct product of $\langle P_1\rangle,\ldots,\langle P_m\rangle$, then $S_M(P_1,\ldots,P_m)$ is generated by the elements $f_1+M,\ldots,f_m+M$.*

Proof. In the language of divisors we have $(f_i)=r_iP_i-r_iP$. Let $g+M\in S_M(P_1,\ldots,P_m)$ with $g\in S(P_1,\ldots,P_m)$. Then the principal divisor of g is of the form

$$(g)=\sum_{i=1}^m t_iP_i-tP$$

with nonnegative integers $t_1,\ldots,t_m$, where $t=\sum_{i=1}^m t_i$. By the condition on $\langle P_1,\ldots,P_m\rangle$, for each $1\le i\le m$ the divisor $t_iP_i-t_iP$ is principal, hence $r_i\mid t_i$. Thus,

$$(g)=\Big(\prod_{i=1}^m f_i^{t_i/r_i}\Big).$$

Since $\mathrm{sgn}(g)=1=\mathrm{sgn}(f_i)$ for $1\le i\le m$, we obtain

$$g=\prod_{i=1}^m f_i^{t_i/r_i},$$

and the result follows. ■

A second general principle for the construction of global function fields with many rational places is based on the theory of Hilbert class fields (see Section 2). This principle was already stated in an equivalent form in [12], but for the sake of completeness we include the short proof.

THEOREM 2. *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*

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

where $r = |\langle P_1, \ldots, P_m\rangle|$.

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

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

in the proof of [14, Lemma 1.2] we obtain

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

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

$$c := |\mathrm{Cl}_S| = \frac{h(K)}{r}.$$

From [14, Proposition 2.2] and the condition on S we deduce that c divides $|\mathrm{Cl}_T|$, 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 $\mathrm{Gal}(H_T/L) \simeq \mathrm{Cl}_T$ and $\mathbb{F}_q$ is the full constant field of H_T since $n \geq 1$ (see [14, 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 $(1/c)|\mathrm{Cl}_T|$. Then $[F : L] = c$. Since H_T/L is an unramified extension, the Hurwitz genus formula yields

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

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

4. Constructions for the case $q = 3$. In this section we construct examples of global function fields F with full constant field $\mathbb{F}_3$ and many rational places. A list of such examples for the genera $1 \leq g \leq 15$ was provided in [8, Section 3]. Now we consider the range $16 \leq g \leq 51$ and also some larger values of the genus. Note that together with the results in [8] this yields lower bounds for $N_3(g)$ for $1 \le g \le 51$ and some larger values of g. The notations and conventions introduced in Sections 2 and 3 are used without further mention. We summarize the results in the following table.

Table 1

$g(F)$	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$N(F)$	27	24	26	27	30	32	28	26	28	36	36	39	37	42	34

$g(F)$	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
$N(F)$	40	38	37	44	38	36	48	36	42	54	50	39	55	42	48

$g(F)$	46	47	48	49	50	51	53	67	69	71	89	102	113	115
$N(F)$	55	47	55	54	56	60	60	72	82	84	96	104	120	120

The entries for $g = 16, 20, 46$, and 48 are taken from the table in van der Geer and van der Vlugt [18]. The entry for $g = 69$ is obtained from [22, Example 4]. The remaining entries are covered by the following examples. For some entries we list two examples, one of which provides a global function field containing additional places of relatively small degree. The latter type of example is useful in a construction of low-discrepancy sequences (see [20]). In some cases we list one explicit and one non-explicit example.

Example 1A. $g(F) = 17$, $N(F) = 24$. Consider the function field $K = \mathbb{F}_3(x, y)$ with

$$y^2 = -x(x-1)(x^5 + x^4 + x^2 + 1).$$

Then $g(K) = 3, N(K) = 3$, K has 7 places of degree 2 and 10 places of degree 3, hence $h(K) = 32$. In K we have $(x) = 2P_1 - 2P_\infty$ and $(x-1) = 2P_2 - 2P_\infty$. Now F is obtained from Theorem 2 with $L = K$ and $S = \{P_\infty, P_1, P_2\}$. It is clear that $r = |\langle P_1, P_2 \rangle| = 2$ or 4. If we had $r = 2$, then $P_1 - P_2$ would be a principal divisor of K, which is impossible by the Weierstrass gap theorem; thus $r = 4$.

Example 1B. $g(F) = 17$, $N(F) = 24$, $F = \mathbb{F}_3(x, y_1, y_2, y_3)$ with

$$y_1^2 = x^3 - x + 1, \qquad y_2^2 = -x^3 + x + 1, \qquad y_3^2 = x^5 - x + 1.$$

This is a tower of Kummer extensions and $K = \mathbb{F}_3(x, y_1, y_2)$ satisfies $g(K) = 4$. The places $x, x+1$, and $x-1$ split completely in the extension $K/\mathbb{F}_3(x)$, hence $N(K) = 12$. Since all rational places of K split completely in F/K, we get $N(F) = 24$. The only ramified places in F/K are those lying over $x^5 - x + 1$, and so $g(F) = 17$.

Example 2. $g(F) = 18$, $N(F) = 26$, $F = \mathbb{F}_3(x, y_1, y_2, y_3)$ with

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

The field $K=\mathbb{F}_3(x,y_1,y_2)$ is that in [8, Example 3.6] and satisfies $g(K)=6$ and $N(K)=14$. In K the principal divisor of u is given by

$$(u)=\sum_{i=1}^{12} Q_i-3Q-9Q_\infty,$$

where $Q_1,\dots,Q_{12},Q,Q_\infty$ are distinct rational places of K. In particular, Q is the unique place lying over the place $P_1=(0,1)$ in [8, Example 3.6] and Q_∞ is the unique place lying over ∞. It is easy to check that in K we have

$$(u+1)=P+R_1+R_2+R_3-3Q-9Q_\infty,$$

where P is the place of degree 3 lying over the place $P_2=(1,2)$ in [8, Example 3.6] and R_1,R_2,R_3 are the places of degree 3 lying over x^3-x^2-x-1 and satisfying $y_1\equiv x-x^2 \bmod R_j$ for $j=1,2,3$. The places P,R_1,R_2,R_3,Q,Q_∞ are totally ramified in the Kummer extension F/K, thus $g(F)=18$. The places $Q_1,\dots,Q_{12}$ split completely in F/K, hence $N(F)=1+1+12\cdot 2=26$.

Example 3. $g(F)=19$, $N(F)=27$. Consider the function field $K=\mathbb{F}_3(x,y)$ with

$$y^2=x(x+1)(x^5+x^4+x-1).$$

Then $g(K)=3$, $N(K)=5$, K has two places of degree 2 and six places of degree 3, 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 2 with $L=K$ and $S=\{P_\infty,P_1,P_2\}$. As in Example 1A we see that $r=4$.

Example 4. $g(F)=21$, $N(F)=32$. Let $K/\mathbb{F}_3$ be the function field in [8, Example 3.7] with $g(K)=7$ and $N(K)=16$. Recall that $[K:\mathbb{F}_3(x)]=8$ and that the places ∞ and x split completely in $K/\mathbb{F}_3(x)$. Now let $F=K(y)$ with $y^2=x^2+1$. Then all rational places of K split completely in the Kummer extension F/K, and so $N(F)=32$. The only ramified places in F/K are the places of K lying over x^2+1, and these are unramified in $K/\mathbb{F}_3(x)$. Thus we get $g(F)=1+2\cdot(7-1)+\frac{1}{2}\cdot 8\cdot 2=21$.

Example 5A. $g(F)=22$, $N(F)=28$. Consider the function field $K=\mathbb{F}_3(x,y)$ with

$$y^2=x(x^4+x^2-1).$$

Then $g(K)=2$, $N(K)=4$, and K has seven places of degree 2, hence $h(K)=14$. Let R be the place of K lying over x and Q be the place of K lying over $x+1$. Then $\deg(R)=1$ and $\deg(Q)=2$. As a distinguished rational place of K we choose the place P lying over ∞. The narrow ray class extension E_Q/K has degree $[E_Q:K]=h(K)\Phi_3(Q)=112$. It is easy to check by Lemma 2 that $S_Q(R)$ is the cyclic subgroup of $(A/Q)^*$ generated by $x+Q$, and so $|S_Q(R)|=2$. Let H be a subgroup of $(A/Q)^*$ of order 4 which contains $S_Q(R)$. Then we can find a subgroup G of $\mathrm{Pic}_Q(A)$ of order 8 which contains H and the residue class $\overline{R}$ of R mod $\mathcal{P}_Q(A)$, since $\overline{R}^2 = \overline{xA}$ and $\overline{xA} \in S_Q(R)$ when $S_Q(R)$ is viewed as a subgroup of $\mathrm{Pic}_Q(A)$. Let F be the subfield of E_Q/K fixed by G. Then $[F : K] = 14$. By construction, the places P and R split completely in F/K, and so $N(F) = 28$. The only place of K ramifying in F/K is Q and its ramification index is 2. Thus, the Hurwitz genus formula yields $2g(F) - 2 = 14(2g(K) - 2) + 7 \cdot (2 - 1) \cdot 2$, that is, $g(F) = 22$.

Example 5B. $g(F) = 22$, $N(F) = 28$, $F = \mathbb{F}_3(x, y_1, y_2, y_3)$ with

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

The field $K = \mathbb{F}_3(x, y_1, y_2)$ satisfies $g(K) = 7$. The places x and $x - 1$ split completely in $K/\mathbb{F}_3(x)$ and there are two rational places of K lying over $x + 1$, thus $N(K) = 14$. All rational places of K split completely in the Kummer extension F/K, hence $N(F) = 28$. The only ramified places in F/K are the places of K lying over $x^3 - x - 1$, and these are unramified in $K/\mathbb{F}_3(x)$. Thus we get $g(F) = 1 + 2 \cdot (7 - 1) + \frac{1}{2} \cdot 6 \cdot 3 = 22$.

Example 6. $g(F) = 23$, $N(F) = 26$, $F = \mathbb{F}_3(x, y_1, y_2, y_3)$ with

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

The field $K = \mathbb{F}_3(x, y_1, y_2)$ is that in [8, Example 3.6] and satisfies $g(K) = 6$ and $N(K) = 14$. There are 13 rational places of K lying over $x, x + 1$, or $x - 1$, and all these rational places split completely in the Kummer extension F/K, hence $N(F) = 26$. The only ramified places in F/K are the places of K lying over $x^4 - x^2 - 1$, and these are unramified in $K/\mathbb{F}_3(x)$. Thus we get $g(F) = 1 + 2 \cdot (6 - 1) + \frac{1}{2} \cdot 6 \cdot 4 = 23$. Note that the place of F lying over ∞ has degree 2.

Example 7. $g(F) = 24$, $N(F) = 28$, $F = \mathbb{F}_3(x, y_1, y_2, y_3)$ with

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

The field $K = \mathbb{F}_3(x, y_1, y_2)$ is that in [8, Example 3.8] and satisfies $g(K) = 8$ and $N(K) = 15$. There are 14 rational places of K lying over $x, x + 1$, or $x - 1$, and all these rational places split completely in the Kummer extension F/K, hence $N(F) = 28$. The only ramified places in F/K are the places of K lying over $x^3 - x - 1$, and these are unramified in $K/\mathbb{F}_3(x)$. Thus we get $g(F) = 1 + 2 \cdot (8 - 1) + \frac{1}{2} \cdot 6 \cdot 3 = 24$. Note that the place of F lying over ∞ has degree 2.

Example 8A. $g(F) = 25$, $N(F) = 36$. Consider the function field $K = \mathbb{F}_3(x,y)$ with

$$y^2 = -x(x-1)(x^5 - x + 1).$$

Then $g(K) = 3$, $N(K) = 5$, K has four places of degree 2 and eight places of degree 3, 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 2 with $L = K$ and $S = \{P_\infty, P_1, P_2\}$. As in Example 1A we see that $r = 4$.

Example 8B. $g(F) = 25$, $N(F) = 36$, and F has at least six places of degree 2. Consider the function field $K = \mathbb{F}_3(x,y)$ with

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

Then $g(K) = 1$ and $h(K) = 4$. We distinguish the rational place P of K lying over ∞. In K we have $(x) = 2P_1 - 2P$, $(x-1) = 2P_2 - 2P$, and $(x+1) = 2P_3 - 2P$, where P_1, P_2, P_3 are rational places of K. Put $M = P_2^2P_3^2$ and consider the narrow ray class extension E_M/K of degree

$$[E_M : K] = h(K)\Phi_3(P_2^2)\Phi_3(P_3^2) = 144.$$

Let H be the 2-Sylow subgroup of $(A/M)^*$. Then $|H| = 4$. Let $\overline{P}_1 \in \mathrm{Pic}_M(A)$ be the residue class of P_1 mod $\mathcal{P}_M(A)$ and G the subgroup of $\mathrm{Pic}_M(A)$ generated by $\overline{P}_1$ and H, where H is also viewed as a subgroup of $\mathrm{Pic}_M(A)$. Since $P_1^2 = xA$ and $x^2 \equiv 1 \bmod M$, we have $\overline{P}_1^2 \in H$. Furthermore, $\overline{P}_1 \notin H$ since $P_1 - P$ is not a principal divisor. Therefore $|G| = 8$.

Now let F be the subfield of E_M/K fixed by G. Then $[F:K] = 18$. The only possible ramified places in F/K are P_2 and P_3. For $i = 2,3$ let R_i be a place of F lying over P_i. Then the inertia group of R_i in E_M/F is $G \cap J_i$, where J_i is the inertia group of P_i in E_M/K. Now J_i has order 6 and it is a subgroup of $\mathrm{Gal}(E_M/H_P) \simeq (A/M)^*$ since H_P/K is an unramified extension. We recall that H is the 2-Sylow subgroup of $(A/M)^*$, and then we can conclude that the inertia group of R_i in E_M/F has order 2. Consequently, the ramification index of R_i in E_M/F is 2 and that of P_i in F/K is 3. By the proof of [22, Proposition 2], P_i has different exponent 9 in E_M/K, and then the tower formula for different exponents shows that the different exponent of P_i in F/K is 4. Therefore the Hurwitz genus formula yields

$$2g(F) - 2 = 18(2g(K) - 2) + 4 \cdot 6 + 4 \cdot 6,$$

that is, $g(F) = 25$. By the construction of F, the places P and P_1 split completely in F/K, and so $N(F) \geq 36$.

Now we consider the decomposition of P_i in F/K for $i = 2,3$. Let E_{M_i}/K be the narrow ray class extension of K with modulus $M_i = P_i^2$. Then E_M is the composite field of E_{M_2} and E_{M_3}. We have $P_3^2 = (x+1)A$ and $(x+1)^2 \equiv 1 \bmod M_2$, thus the Artin symbol of P_3 has order 4 in $\mathrm{Gal}(E_{M_2}/K) \simeq \mathrm{Pic}_{M_2}(A)$ and the relative degree of P_3 in E_M/K is 4. Since the relative degree of P_3 in F/K is a factor of that in E_M/K, it follows that the relative degree of P_3 in F/K is 2 (if this degree were 1, then $N(F) \geq 36 + 6 = 42$, a contradiction to the bound $N_3(25) \leq 40$ obtained by Serre's method described in [16, Proposition V.3.4]). In the same way one shows that the relative degree of P_2 in F/K is 2. It follows that F has at least six places of degree 2 and that $N(F)=36$.

EXAMPLE 9A. $g(F) = 26$, $N(F) = 36$, $F = \mathbb{F}_3(x, y_1, y_2, y_3)$ with

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

The field $K = \mathbb{F}_3(x, y_1, y_2)$ is that in [8, Example 3.9] and satisfies $g(K) = 9$ and $N(K) = 19$. There are 18 rational places of K lying over x or $x - 1$, and all these rational places split completely in the Kummer extension F/K, hence $N(F) = 36$. The only ramified places in F/K are the places of K lying over $x^2 - x - 1$, and these are unramified in $K/\mathbb{F}_3(x)$. Thus we get $g(F) = 1 + 2 \cdot (9 - 1) + \frac{1}{2} \cdot 9 \cdot 2 = 26$. Note that the place of F lying over ∞ has degree 2.

EXAMPLE 9B. $g(F) = 26$, $N(F) = 36$, and F has a place of degree 2. Consider the function field $K = \mathbb{F}_3(x, y)$ with

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

Then $g(K) = 2$, $N(K) = 4$, and K has one place of degree 2, hence $h(K) = 8$. We distinguish the rational place P of K lying over ∞. In K we have

$$(x - i + 1) = 2P_i - 2P \quad \text{for } i = 1, 2, 3$$

and $(x^2 + 1) = 2Q - 4P$, where P_1, P_2, P_3 are rational places of K and $\deg(Q) = 2$. Put $M = Q^2$ and consider the narrow ray class extension E_M/K of degree $[E_M : K] = h(K)\Phi_3(M) = 576$. Let G be the 2-Sylow subgroup of $\mathrm{Pic}_M(A)$ and F the subfield of E_M/K fixed by G. Then $[F : K] = 9$. For $i = 1, 2, 3$ we have

$$P_i^{16} = (x - i + 1)^8 A \quad \text{and} \quad (x - i + 1)^8 \equiv 1 \bmod M,$$

thus $\overline{P}_i^{16} = 1$ in $\mathrm{Pic}_M(A)$, and so $\overline{P}_i \in G$. It follows that the places P, P_1, P_2, P_3 split completely in F/K, hence $N(F) = 36$. Furthermore, Q is totally ramified in F/K, and so F has a place of degree 2. By the proof of [22, Proposition 2], the different exponent $d_Q(E_M/K)$ of Q in E_M/K is 135. The different exponent $d_Q(F/K)$ of Q in F/K satisfies

$$8d_Q(F/K) + 7 = d_Q(E_M/K) = 135$$

by the tower formula for different exponents, thus $d_Q(F/K) = 16$. Since Q is the only ramified place in F/K, the Hurwitz genus formula yields $2g(F) - 2 = 9(2g(K) - 2) + 16 \cdot 2$, that is, $g(F) = 26$.

Example 10. $g(F) = 27$, $N(F) = 39$. Consider the function field $K = \mathbb{F}_3(x, y)$ with

$$y^2 = -x(x-1)(x^5 + x^4 + x^2 + x + 1).$$

Then $g(K) = 3$, $N(K) = 5$, K has 4 places of degree 2 and 12 places of degree 3, 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 2 with $L = K$ and $S = \{P_\infty, P_1, P_2\}$. As in Example 1A we see that $r = 4$.

Example 11. $g(F) = 28$, $N(F) = 37$, $F = \mathbb{F}_3(x, y_1, y_2, y_3)$ with

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

The field $K = \mathbb{F}_3(x, y_1, y_2)$ is that in [8, Example 3.9] and satisfies $g(K) = 9$ and $N(K) = 19$. The 18 rational places of K lying over x or $x - 1$ split completely in the Kummer extension F/K and the unique rational place of K lying over ∞ is totally ramified in F/K, hence $N(K) = 37$. Besides the latter place, the only other places of K ramifying in F/K are those lying over $x^2 + 1$ (they are unramified in $K/\mathbb{F}_3(x)$) and the unique place of degree 3 lying over $x + 1$. Thus we get $g(F) = 1 + 2 \cdot (9-1) + \frac{1}{2}(9 \cdot 2 + 1 + 3) = 28$.

Example 12. $g(F) = 29$, $N(F) = 42$, and F has at least 14 places of degree 5. Consider the function field $K = \mathbb{F}_3(x, y)$ with

$$y^2 = -x(x-1)(x^5 + x^3 + x + 1).$$

Then $g(K) = 3$, $N(K) = 5$, K has six places of degree 2 and six places of degree 3, hence $h(K) = 56$. In K we have $(x) = 2P_1 - 2P_\infty$ and $(x-1) = 2P_2 - 2P_\infty$. Let F be obtained from Theorem 2 with $L = K$ and $S = \{P_\infty, P_1, P_2\}$, i.e., we can take F to be the subfield of H_{P_∞}/K fixed by $\langle P_1, P_2 \rangle$. As in Example 1A we see that $r = 4$. For the principal divisor of y in K we have $(y) = P_1 + P_2 + Q - 7P_\infty$, where Q is the place of K of degree 5 lying over $x^5 + x^3 + x + 1$. Thus, the ideal class of Q is contained in $\langle P_1, P_2 \rangle$, and so Q splits completely in the extension F/K of degree 14.

Example 13. $g(F) = 30$, $N(F) = 34$. Let $K/\mathbb{F}_3$ be the function field constructed in [22, Example 5] with $n = 9$. Then $g(K) = 10$, $N(K) = 19$, and $[K : \mathbb{F}_3(x)] = 6$. The places $x+1$ and $x-1$ split completely in $K/\mathbb{F}_3(x)$, there are three rational places of K lying over ∞ with ramification index 2, and over x there are three rational places of K with ramification index 1 and one rational place of K with ramification index 3. Now let $F = K(z)$ with

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

Then the places of K lying over $x + 1, x - 1$, or ∞ split completely in the Kummer extension F/K and the places of K lying over x are totally ramified in F/K, therefore $N(F) = 34$. Besides the latter places, the only other places of K ramifying in F/K are those lying over x^3+x^2-1, and they are unramified in $K/\mathbb{F}_3(x)$. Thus we get $g(F)=1+2\cdot(10-1)+\frac{1}{2}(6\cdot3+4)=30$.

Example 14. $g(F)=31$, $N(F)=40$. Consider the function field $K=\mathbb{F}_3(x,y)$ with

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

Then $g(K)=2$, $N(K)=6$, and K has two places of degree 2, hence $h(K)=20$. We distinguish the rational place P of K lying over ∞. In K we have $(x)=2P_1-2P$ and $(x^2+1)=2Q-4P$, where $\deg(P_1)=1$ and $\deg(Q)=2$. Now F is obtained from Theorem 1 with $m=1$ and $M=Q$. It is clear that $r=2$, and from $x^2\equiv-1 \bmod M$ and Lemma 2 we deduce that $t=4$.

Example 15. $g(F)=32$, $N(F)=38$, $F=\mathbb{F}_3(x,y_1,y_2,y_3)$ with

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

The field $K=\mathbb{F}_3(x,y_1,y_2)$ is that in [8, Example 3.9] and satisfies $g(K)=9$ and $N(K)=19$. All rational places of K lie over $x,x-1$, or ∞ and they split completely in the Kummer extension F/K, thus $N(F)=38$. The only places of K ramifying in F/K are those lying over x^3+x^2-x+1 (they are unramified in $K/\mathbb{F}_3(x)$) and the unique place of degree 3 lying over $x+1$. Hence we get $g(F)=1+2\cdot(9-1)+\frac{1}{2}(9\cdot3+3)=32$.

Example 16. $g(F)=33$, $N(F)=37$. Let $K/\mathbb{F}_3$ be the function field constructed in [8, Example 3.10]. Then $g(K)=10$, $N(K)=19$, and $[K:\mathbb{F}_3(x)]=9$. The places $x+1$ and ∞ split completely in $K/\mathbb{F}_3(x)$ and the place x is totally ramified in $K/\mathbb{F}_3(x)$. Now let $F=K(z)$ with

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

Then the places of K lying over $x+1$ or ∞ split completely in the Kummer extension F/K and the place of K lying over x is totally ramified in F/K, therefore $N(F)=37$. Besides the latter place, the only other places of K ramifying in F/K are those lying over x^3-x-1, and they are unramified in $K/\mathbb{F}_3(x)$. Thus we get $g(F)=1+2\cdot(10-1)+\frac{1}{2}(9\cdot3+1)=33$.

Example 17. $g(F)=34$, $N(F)=44$. Consider the function field $K=\mathbb{F}_3(x,y)$ with

$$y^2=x(x^4+x-1).$$

Then $g(K)=2$, $N(K)=6$, and K has four places of degree 2, hence $h(K)=22$. We distinguish the rational place P of K lying over ∞. In K we have $(x)=2P_1-2P$. Now F is obtained from Theorem 1 with $m=1$ and $M=Q$, where Q is a place of K of degree 2 lying over x^2+1. It is clear that $r=2$, and from $x^2\equiv-1 \bmod M$ and Lemma 2 we deduce that $t=4$.

Example 18. $g(F)=35$, $N(F)=38$, $F=\mathbb{F}_3(x,y_1,y_2,y_3)$ with

$$y_1^3-y_1=x(x-1),\qquad y_2^3-y_2=\frac{x(x-1)}{x+1},\qquad y_3^2=x^4+x^2+x+1.$$

The field $K=\mathbb{F}_3(x,y_1,y_2)$ is that in [8, Example 3.9] and satisfies $g(K)=9$ and $N(K)=19$. All rational places of K lie over $x,x-1$, or ∞ and they split completely in the Kummer extension F/K, thus $N(F)=38$. The only places of K ramifying in F/K are those lying over x^4+x^2+x+1, and they are unramified in $K/\mathbb{F}_3(x)$. Hence we get $g(F)=1+2\cdot(9-1)+\frac{1}{2}\cdot 9\cdot 4=35$.

Example 19. $g(F)=36$, $N(F)=36$. Let $K/\mathbb{F}_3$ be the function field constructed in [8, Example 3.4] with $g(K)=4$ and $N(K)=12$. Then F is obtained from [9, Theorem 3] by choosing $m=11$, $d=13$, and $l=1$.

Example 20. $g(F)=37$, $N(F)=48$. Consider the function field $K=\mathbb{F}_3(x,y_1)$ with

$$y_1^2=x(x^4-x^3+x^2-x+1).$$

Then $g(K)=2$, $N(K)=6$, and K has six places of degree 2, hence $h(K)=24$. In K we have $(x)=2P_1-2P_\infty$. Furthermore, let $L=K(y_2)$ with

$$y_2^2=x+1.$$

Then $g(L)=4$ since the only places of K ramifying in the Kummer extension L/K are those lying over $x+1$. Now F is obtained from Theorem 2 with $S=\{P_\infty,P_1\}$. Note that the condition on S in Theorem 2 is satisfied since the places of K lying over $x+1$ are totally ramified in L/K. Furthermore, we have $n=4$ since both places in S split completely in L/K, and also $r=2$. Theorem 2 yields $N(F)\geq 48$, but since $N_3(37)\leq 54$ by Serre's method, we get $N(F)=48$.

Example 21. $g(F)=38$, $N(F)=36$. Let $K/\mathbb{F}_3$ be the function field constructed in [8, Example 3.4] with $g(K)=4$ and $N(K)=12$. Then F is obtained from [9, Theorem 3] by choosing $m=11$, $d=14$, and $l=1$.

Example 22. $g(F)=39$, $N(F)=42$, $F=\mathbb{F}_3(x,y_1,y_2,y_3)$ with

$$y_1^2=(x^2+1)(x^4+x^3-x+1),\qquad y_2^3-y_2=\frac{x^3-x}{(x^2+1)^2},\qquad y_3^2=x^3-x+1.$$

The field $K=\mathbb{F}_3(x,y_1,y_2)$ is that in [8, Example 3.14] and satisfies $g(K)=14$ and $N(K)=24$. All rational places of $\mathbb{F}_3(x)$ split completely in $K/\mathbb{F}_3(x)$. All places of K lying over $x,x+1$, or $x-1$ split completely in the Kummer extension F/K and the six places of K lying over ∞ are totally ramified in F/K, hence $N(F)=42$. Besides the latter places, the only other places of K ramifying in F/K are those lying over x^3-x+1, and they are unramified in $K/\mathbb{F}_3(x)$. Thus we get $g(F)=1+2\cdot(14-1)+\frac{1}{2}(6\cdot 3+6)=39$.

EXAMPLE 23. $g(F) = 40$, $N(F) \geq 54$. Put $K = \mathbb{F}_3(x)$ and let E be the cyclotomic function field over $\mathbb{F}_3$ with modulus $M = (x+1)^3(x-1)^3$ and with the distinguished rational place ∞ of K. Then

$$[E : K] = \Phi_3((x+1)^3)\Phi_3((x-1)^3) = 324.$$

Since $x^6 \equiv 1 \bmod M$, we can find a subgroup G of $\mathrm{Gal}(E/K) \simeq (\mathbb{F}_3[x]/(M))^*$ with $|G| = 12$ such that G contains the decomposition groups of the places x and ∞ in E/K. Let F be the subfield of E/K fixed by G. Then $[F : K] = 27$. By construction, x and ∞ split completely in F/K, and so $N(F) \geq 54$. Let E_1, respectively E_2, be the cyclotomic function field over $\mathbb{F}_3$ with modulus $(x+1)^3$, respectively $(x-1)^3$, and with the distinguished rational place ∞ of K. Then

$$[E_1 : K] = [E_2 : K] = 18$$

and E is the composite field of E_1 and E_2. To calculate $g(F)$, we first determine the ramification index $e_{x+1}(F/K)$ of the place $x+1$ in F/K. From $e_{x+1}(E_1/K) = 18$, $e_{x+1}(E_2/K) = 1$, and Abhyankar's lemma (see [16, Proposition III.8.9]) we deduce that $e_{x+1}(E/K) = 18$, and so $e_{x+1}(F/K)$ divides 9.

We claim that $e_{x+1}(F/K) = 9$. If we had $e_{x+1}(F/K) = 1$ or 3, then the inertia field L of $x+1$ in F/K has degree $[L : K] = 27$ or 9. Since $x+1$ is unramified in L/K and E_2 is the inertia field of $x+1$ in E/K, we have $L \subseteq E_2$, and so $[E_2 : L] = 2$. From the fact that x splits completely in L/K it follows that the relative degree of x in E_2/K is 1 or 2. Thus, the Artin symbol of x in E_2/K has order 1 or 2, but this is impossible since $x^2 \not\equiv 1 \bmod (x-1)^3$; hence indeed $e_{x+1}(F/K) = 9$.

By [3, Theorem 4.1] the different exponent $d_{x+1}(E_1/K)$ of $x+1$ in E_1/K is given by

$$d_{x+1}(E_1/K) = 3\Phi_3((x+1)^3) - 3^2 = 45.$$

Now the tower formula for different exponents yields

$$2d_{x+1}(F/K) + 1 = d_{x+1}(E/K) = d_{x+1}(E_1/K) = 45,$$

that is, $d_{x+1}(F/K) = 22$. In the same way one shows that $e_{x-1}(F/K) = 9$ and $d_{x-1}(F/K) = 22$. Since $x+1$ and $x-1$ are the only ramified places in F/K, the Hurwitz genus formula yields $2g(F) - 2 = -2 \cdot 27 + 3 \cdot 22 + 3 \cdot 22$, that is, $g(F) = 40$.

EXAMPLE 24. $g(F) = 41$, $N(F) = 50$. Consider the function field $K = \mathbb{F}_3(x, y)$ with

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

Then $g(K)=3$, $N(K)=4$, K has 4 places of degree 2 and 16 places of degree 3, hence $h(K)=40$. We distinguish the rational place P of K lying over ∞. In K we have $(x) = 2Q - 2P$, $(x-1) = 2P_1 - 2P$, and $(x+1) = 2P_2 - 2P$, where Q, P_1, and P_2 are rational places of K. Put $M = Q^2$ and consider the narrow ray class extension E_M/K of degree $[E_M : K] = h(K)\Phi_3(M) = 240$. Let G be the 2-Sylow subgroup of $\mathrm{Pic}_M(A)$ and F the subfield of E_M/K fixed by G. Then $[F : K] = 15$. Since $P_1^4 = (x-1)^2 A$, $(x-1)^2 \equiv 1 \bmod M$, $P_2^2 = (x+1)A$, and $x+1 \equiv 1 \bmod M$, we have $\overline{P}_1, \overline{P}_2 \in G$. It follows that P, P_1, and P_2 split completely in F/K. Since $Q^2 = xA$ is a principal ideal, we see that the relative degree of Q in H_P/K is 2, and therefore the relative degree of Q in E_M/K is also 2. In view of $[F : K] = 15$, this shows that the relative degree of Q in F/K is 1. Since the ramification index of Q in F/K is 3, it follows that Q splits into five rational places in F/K. Consequently, $N(F) = 3 \cdot 15 + 5 = 50$. From the proof of [22, Proposition 2] we see that the different exponent of Q in E_M/K is 9, and so the tower formula for different exponents shows that the different exponent of Q in F/K is 4. Since Q is the only ramified place in F/K, the Hurwitz genus formula yields $2g(F) - 2 = 15(2g(K) - 2) + 4 \cdot 5$, that is, $g(F) = 41$.

Example 25. $g(F) = 42$, $N(F) \geq 39$. Let $K/\mathbb{F}_3$ be the function field constructed in [8, Example 3.6] with $g(K) = 6$ and $N(K) = 14$. Then F is obtained from [9, Theorem 3] by choosing $m = 12$, $d = 13$, and $l = 1$.

Example 26. $g(F) = 43$, $N(F) = 55$. Let $K/\mathbb{F}_3$ be the function field constructed in [8, Example 3.15] with $g(K) = 15$ and $N(K) = 28$. Then $[K : \mathbb{F}_3(x)] = 9$ and the places $x+1$, $x-1$, and ∞ split completely in $K/\mathbb{F}_3(x)$, whereas x is totally ramified in $K/\mathbb{F}_3(x)$. Now let $F = K(z)$ with

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

Then the places of K lying over $x+1, x-1$, or ∞ split completely in the Kummer extension F/K and the place of K lying over x is totally ramified in F/K, hence $N(F) = 55$. Besides the latter place, the only other places of K ramifying in F/K are those lying over x^3+x^2-1, and they are unramified in $K/\mathbb{F}_3(x)$. Thus we get $g(F) = 1 + 2 \cdot (15 - 1) + \frac{1}{2}(9 \cdot 3 + 1) = 43$.

Another example with $g(F) = 43$ and $N(F) = 55$ is given in [22, Example 5].

Example 27. $g(F) = 44$, $N(F) = 42$. Let $K/\mathbb{F}_3$ be the function field constructed in [8, Example 3.6] with $g(K) = 6$ and $N(K) = 14$. Then F is obtained from [9, Theorem 3] by choosing $m = 13$, $d = 14$, and $l = 1$.

Example 28. $g(F) = 45$, $N(F) = 48$, $F = \mathbb{F}_3(x, y_1, y_2, y_3, y_4)$ with

$$y_1^2 = x^3 - x + 1, \qquad y_2^2 = -x^4 + x^2 + 1,$$
$$y_3^2 = -x^3 + x + 1, \qquad y_4^2 = -x^4 + x^3 + x^2 - x + 1.$$

The field $K = \mathbb{F}_3(x, y_1, y_2)$ is that in [8, Example 3.5] and satisfies $g(K) = 5$ and $N(K) = 12$. The places $x, x+1$, and $x-1$ split completely in $K/\mathbb{F}_3(x)$. All rational places of K split completely in F/K, which is a tower of Kummer extensions, thus $N(F) = 48$. If $L = K(y_3)$, then the only places of K ramifying in L/K are those lying over $x^3 - x - 1$ and the only places of L ramifying in F/L are those lying over $x^4 - x^3 - x^2 + x - 1$. This yields $g(L) = 15$ and $g(F) = 45$.

EXAMPLE 29. $g(F) = 47$, $N(F) = 47$. Let the function field $K/\mathbb{F}_3$ be as in Example 26 and let $F = K(z)$ with

$$z^2 = x^3 - x + 1.$$

Then the places of K lying over $x, x + 1$, or $x - 1$ split completely in the Kummer extension F/K and the places of K lying over ∞ are totally ramified in F/K, therefore $N(F) = 2 \cdot 19 + 9 = 47$. Besides the latter places, the only other places of K ramifying in F/K are those lying over $x^3 - x + 1$, and they are unramified in $K/\mathbb{F}_3(x)$. Thus we get $g(F) = 1 + 2 \cdot (15 - 1) + \frac{1}{2}(9 \cdot 3 + 9) = 47$.

EXAMPLE 30. $g(F) = 49$, $N(F) = 54$. Consider the function field $K = \mathbb{F}_3(x, y)$ with

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

Then $g(K) = 1$ and $h(K) = 6$. We distinguish the rational place P of K lying over ∞. In K we have $(x) = 2P_1 - 2P$. Now F is obtained from Theorem 1 with $m = 1$ and $M = Q^2$, where Q is the place of K of degree 2 lying over $x^2 - x - 1$. It is clear that $r = 2$, and from $x^4 \equiv -1 \bmod M$ and Lemma 2 we deduce that $t = 8$.

EXAMPLE 31. $g(F) = 50$, $N(F) = 56$. Let the function field $K/\mathbb{F}_3$ be as in Example 5A. Then $g(K) = 2$ and $h(K) = 14$. We distinguish the rational place P of K lying over ∞. In K we have $(x) = 2P_1 - 2P$. Now F is obtained from Theorem 1 with $m = 1$ and $M = Q$, where Q is the place of K of degree 2 lying over $x + 1$. It is clear that $r = 2$, and from $x \equiv -1 \bmod M$ and Lemma 2 we deduce that $t = 2$.

EXAMPLE 32. $g(F) = 51$, $N(F) = 60$. Consider the function field $K = \mathbb{F}_3(x, y_1)$ with

$$y_1^2 = (x + 1)(x - 1)(x^2 + x - 1)(x^3 - x + 1).$$

Then $g(K) = 3$, $N(K) = 5$, K has three places of degree 2 and five places of degree 3, hence $h(K) = 40$. In K we have $(x + 1) = 2P_1 - 2P_\infty$ and $(x - 1) = 2P_2 - 2P_\infty$. Furthermore, let $L = K(y_2)$ with

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

Then $g(L) = 6$ since the only places of K ramifying in the Kummer extension L/K are those lying over x. Now F is obtained from Theorem 2 with $S = \{P_\infty, P_1, P_2\}$. Note that the condition on S in Theorem 2 is satisfied since the places of K lying over x are totally ramified in L/K. Furthermore, we have $n = 6$ since all places in S split completely in L/K, and we get $r = 4$ by the argument in Example 1A. Theorem 2 yields $N(F) \geq 60$, but since $N_3(51) \leq 69$ by Serre's method, we get $N(F) = 60$.

Example 33. $g(F) = 53$, $N(F) = 60$. Consider the function field $K = \mathbb{F}_3(x, y)$ with

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

Then $g(K) = 2$, $N(K) = 5$, and K has four places of degree 2, hence $h(K) = 16$. We distinguish the rational place P of K lying over ∞. In K we have $(x) = 2P_1 - 2P$ and $(x + 1) = 2P_2 - 2P$. We consider the narrow ray class extension E_M/K with modulus $M = Q$, where Q is the place of K of degree 4 lying over $x^2 + 1$. Then $[E_M : K] = h(K)\Phi_3(M) = 1280$. Let B be the 2-Sylow subgroup of $(A/M)^*$. Then $|B| = 16$. From $(x + 1)^4 \equiv x^2 \equiv -1 \bmod M$ and Lemma 2 we deduce that $|\langle S_M(P_1, P_2), D_P\rangle| = 8$, and so $\langle S_M(P_1, P_2), D_P\rangle \subseteq B$. Furthermore, we note that $\overline{P_1^2}, \overline{P_2^2} \in S_M(P_1, P_2)$ if $S_M(P_1, P_2)$ is viewed as a subgroup of $\mathrm{Pic}_M(A)$. Therefore, there exists a subgroup G of $\mathrm{Pic}_M(A)$ of order 64 such that G contains $\overline{P}_1, \overline{P}_2$, and B.

Now let F be the subfield of E_M/K fixed by G. Then $[F : K] = 20$. By construction, the places P, P_1, and P_2 split completely in F/K, therefore $N(F) \geq 60$. Note that the subfield L of E_M/K fixed by B is an extension of H_P of degree 5, and so the ramification index of Q in L/K is 5. From $F \subseteq L$ it follows easily that the ramification index of Q in F/K is 5. Since Q is the only ramified place in F/K, the Hurwitz genus formula yields $2g(F) - 2 = 20(2g(K) - 2) + (5 - 1) \cdot 4 \cdot 4$, that is, $g(F) = 53$. Since $N_3(53) \leq 71$ by Serre's method, we get $N(F) = 60$.

Example 34. $g(F) = 67$, $N(F) = 72$. Consider the function field $K = \mathbb{F}_3(x, y)$ with

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

Then $g(K) = 1$ and $h(K) = 4$. We distinguish the rational place P of K lying over ∞. In K we have $(x) = 2P_1 - 2P$. Now F is obtained from Theorem 1 with $m = 1$ and $M = Q^2$, where Q is the place of K of degree 2 lying over $x^2 + 1$. It is clear that $r = 2$, and from $x^2 \equiv -1 \bmod M$ and Lemma 2 we deduce that $t = 4$.

Example 35. $g(F) = 71$, $N(F) = 84$. Consider the function field $K = \mathbb{F}_3(x, y_1)$ with

$$y_1^2 = (x+1)(x-1)(x^2 + x - 1)(x^3 - x^2 + 1).$$

Then $g(K) = 3$, $N(K) = 5$, K has 5 places of degree 2 and 11 places of degree 3, hence $h(K) = 56$. In K we have $(x + 1) = 2P_1 - 2P_\infty$ and $(x - 1) = 2P_2 - 2P_\infty$. Furthermore, let $L = K(y_2)$ with

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

Now F is obtained from Theorem 2 by proceeding as in Example 32. Initially we obtain $N(F) \geq 84$, but since $N_3(71) \leq 90$ by Serre's method, we have $N(F) = 84$.

Example 36. $g(F) = 89$, $N(F) = 96$. Let the function field $K/\mathbb{F}_3$ be as in Example 1A. Then $g(K) = 3$ and $h(K) = 32$. We distinguish the rational place P_∞ of K lying over ∞. Let the rational places P_1 and P_2 of K be as in Example 1A. Now F is obtained from Theorem 1 with $m = 2$ and $M = Q$, where Q is the place of K of degree 2 lying over $x + 1$. By Example 1A we have $r = 4$, and from $x \equiv -1 \bmod M$ and Lemma 2 we deduce that $t = 2$.

Example 37. $g(F) = 102$, $N(F) = 104$. Put $K = \mathbb{F}_3(x)$ and let E be the cyclotomic function field over $\mathbb{F}_3$ with modulus $M = \sum_{i=0}^{6} x^i$ and with the distinguished rational place ∞ of K. Then $[E : K] = \Phi_3(M) = 3^6 - 1$. Since $x^7 \equiv 1 \bmod M$, the subgroup G of $\mathrm{Gal}(E/K) \simeq (\mathbb{F}_3[x]/(M))^*$ generated by the decomposition groups of the places x and ∞ in E/K satisfies $|G| = 14$. Let F be the subfield of E/K fixed by G. Then $[F : K] = 52$. By construction, x and ∞ split completely in F/K, and so $N(F) = 104$. Since M is the only ramified place in F/K, the Hurwitz genus formula yields $2g(F) - 2 = -2 \cdot 52 + (52 - 1) \cdot 6$, that is, $g(F) = 102$.

Example 38. $g(F) = 113$, $N(F) = 120$. Let the function field $K/\mathbb{F}_3$ be as in Example 33. Then $g(K) = 2$ and $h(K) = 16$. We distinguish the rational place P of K lying over ∞. Let the rational places P_1 and P_2 of K be as in Example 33. Now F is obtained from Theorem 1 with $m = 2$ and $M = Q$, where Q is as in Example 33. We have already shown in Example 33 that $t = 8$, and we obtain $r = 4$ by the argument in Example 1A.

Example 39. $g(F) = 115$, $N(F) = 120$. Let the function field $K/\mathbb{F}_3$ be as in Example 30. Then $g(K) = 1$ and $h(K) = 6$. We distinguish the rational place P of K lying over ∞ and let the rational place P_1 of K be as in Example 30. Now F is obtained from Theorem 1 with $m = 1$ and $M = R$, where R is the place of K of degree 4 lying over $x^2 + 1$. It is clear that $r = 2$, and from $x^2 \equiv -1 \bmod M$ and Lemma 2 we deduce that $t = 4$.

References

[1] A. Garcia and H. Stichtenoth, *Algebraic function fields over finite fields with many rational places*, IEEE Trans. Inform. Theory 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] —, *A brief introduction to Drinfeld modules*, in: The Arithmetic of Function Fields, D. Goss, D. R. Hayes, and M. I. Rosen (eds.), de Gruyter, Berlin, 1992, 1–32.

[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] —, —, *Explicit global function fields over the binary field with many rational places*, Acta Arith. 75 (1996), 383–396.

[7] —, —, *Quasirandom points and global function fields*, in: Finite Fields and Applications, S. Cohen and H. Niederreiter (eds.), Cambridge Univ. Press, Cambridge, 1996, 269–296.

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

[9] —, —, *Drinfeld modules of rank* 1 *and algebraic curves with many rational points. II*, ibid. 81 (1997), 81–100.

[10] —, —, *The algebraic-geometry approach to low-discrepancy sequences*, in: Monte Carlo and Quasi-Monte Carlo Methods '96, H. Niederreiter *et al.* (eds.), Lecture Notes in Statist., Springer, New York, to appear.

[11] —, —, *Algebraic curves over finite fields with many rational points*, in: Proc. Number Theory Conf. (Eger, 1996), de Gruyter, Berlin, to appear.

[12] —, —, *Global function fields with many rational places over the quinary field*, Demonstratio Math., to appear.

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

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

[15] J.-P. Serre, *Rational Points on Curves over Finite Fields*, lecture notes, Harvard University, 1985.

[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, *How to construct curves over finite fields with many points*, in: Arithmetic Geometry, F. Catanese (ed.), Cambridge Univ. Press, Cambridge, 1997, 169–189.

[19] C. P. Xing, *Maximal function fields and function fields with many rational places over finite fields of characteristic* 2, preprint, 1997.

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

[21] —, —, *Modules de Drinfeld et courbes algébriques ayant beaucoup de points rationnels*, C. R. Acad. Sci. Paris Sér. I Math. 322 (1996), 651–654.

[22] —, —, *Drinfeld modules of rank* 1 *and algebraic curves with many rational points*, preprint, 1996.

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

Received on 20.6.1997 (3206)