ACTA ARITHMETICA
LXXXVI.3 (1998)

Global function fields with many rational places over the quinary field. II

by

Harald Niederreiter (Wien) and Chaoping Xing (Singapore)

1. Introduction. Let q be an arbitrary prime power and K 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, so usually one has to be satisfied with bounds for $N_q(g)$. Upper bounds for $N_q(g)$ that improve on the classical Weil bound can be obtained by a method of Serre [15] (see also [16, Proposition V.3.4]).

Global function fields $K/\mathbb{F}_q$ of genus g with many rational places, that is, with $N(K)$ reasonably close to $N_q(g)$ or to a known upper bound for $N_q(g)$, have received a lot of attention in the literature. We refer to Garcia and Stichtenoth [1], Niederreiter and Xing [10], [11], and van der Geer and van der Vlugt [17] for recent surveys of this subject. 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 not only of great theoretical interest, but it is also important for applications in the theory of algebraic-geometry codes (see [13], [16]) and in recent constructions of low-discrepancy sequences (see [5], [9], [12]).

In the present paper we concentrate on the case $q = 5$ and extend the list of constructions of global function fields $K/\mathbb{F}_5$ with many rational places in [6, Section 5] and [8]. The motivation for this is that the recent tables of

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

lower and upper bounds for $N_q(g)$ in [11] and [12] cover all genera $g \le 50$, except in the case $q = 5$ where they cover only the range $g \le 22$. We now close this gap by providing constructions for $q = 5$ and $23 \le g \le 50$, and in fact for many other values of the genus. A crucial role in this is played by a general construction principle based on Hilbert class fields.

In Section 2 we review some background on Hilbert class fields and narrow ray class extensions. Section 3 presents the general construction principle mentioned above and a list of examples for $q = 5$ derived from this principle. Further examples for $q = 5$ obtained by other methods are given in Section 4.

2. Background for the constructions. First we recall some pertinent facts about Hilbert class fields. A convenient reference for this topic is Rosen [14]. Let F be a global function field with $N(F) \ge 1$ and distinguish a rational place ∞ of F. The *Hilbert class field* H_∞ of F with respect to ∞ is the maximal unramified abelian extension of F (in a fixed separable closure of F) in which ∞ splits completely. The extension H_∞/F is finite and its Galois group is isomorphic to the fractional ideal class group $\mathrm{Pic}(A)$ of the ring A of elements of F that are regular outside ∞. In the case under consideration (∞ rational), $\mathrm{Pic}(A)$ is isomorphic to the group $\mathrm{Div}^0(F)$ of divisor classes of F of degree 0. In particular, we have $[H_\infty : F] = h(F)$, the divisor class number of F. For each place P of F there is an associated Galois automorphism $\tau_P \in \mathrm{Gal}(H_\infty/F)$, and the Artin symbol of P for the extension H_∞/F is equal to τ_P. The place P corresponds to the divisor class of $P - \deg(P)\infty$ in $\mathrm{Div}^0(F)$. There is also a standard identification between places of F and prime ideals in A.

Next we collect some facts about narrow ray class extensions which can be found in [2, Section 7.5] and [4, Section 16]. Let $F = F/\mathbb{F}_q, \infty$, and A be as above and let ϕ be a sign-normalized Drinfeld A-module of rank 1. By [4, Section 15] we can assume that ϕ is defined over the Hilbert class field H_∞, i.e., that for each $z \in A$ the $\mathbb{F}_q$-endomorphism ϕ_z is a polynomial in the Frobenius with coefficients from H_∞. If $\overline{H}_\infty$ is a fixed algebraic closure of H_∞ and M a nonzero integral ideal in A, then we write Λ_M for the A-submodule of $\overline{H}_\infty$ consisting of the M-division points. Let $E_M := H_\infty(\Lambda_M)$ be the subfield of $\overline{H}_\infty$ generated over H_∞ by all elements of Λ_M. Then E_M/F is called the *narrow ray class extension* of F with modulus M. The field E_M is independent of the specific choice of the sign-normalized Drinfeld A-module ϕ of rank 1. Furthermore, E_M/F is a finite abelian extension with

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

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 $z \in F$ with $z \equiv 1 \bmod M$ and $\operatorname{sgn}(z) = 1$ (here sgn is the given sign function). We have $\operatorname{Gal}(E_M/H_\infty) \simeq (A/M)^*$, the group of units of the ring A/M. Thus, if $\Phi_q(M)$ denotes the order of the latter group, then

$$[E_M : F] = |\operatorname{Pic}_M(A)| = h(F)\Phi_q(M).$$

If $M = Q^n$ with a nonzero prime ideal Q in A and $n \geq 1$, then

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

where d is the degree of the place of F corresponding to Q. Again in this situation, E_M/F is unramified away from ∞ and Q. Furthermore, the decomposition group (and also the ramification group) D_∞ of ∞ in E_M/F is the subgroup $D_\infty = \{c + M : c \in \mathbb{F}_q^*\}$ of $(A/M)^*$, and every place of H_∞ lying over Q is totally ramified in E_M/H_∞.

In the special case where F is the rational function field $\mathbb{F}_q(x)$ over $\mathbb{F}_q$, the theory of narrow ray class extensions reduces to that of cyclotomic function fields as developed by Hayes [3]. In this case it is customary to take for ∞ the unique pole of x in $\mathbb{F}_q(x)$. We will 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.

3. Examples from Hilbert class fields.

We first establish a general construction principle for global function fields with many rational places that is based on Hilbert class fields.

THEOREM 1. *Let q be odd, let S be a subset of $\mathbb{F}_q$, and put $n = |S|$. Choose a polynomial $f \in \mathbb{F}_q[x]$ such that $\deg(f)$ is odd, f has no multiple roots, and $f(c) = 0$ for all $c \in S$. For the global function field $F = \mathbb{F}_q(x, y)$ with $y^2 = f(x)$, assume that its divisor class number $h(F)$ is divisible by $2^n m$ for some positive integer m. Then there exists a global function field $K/\mathbb{F}_q$ such that*

$$g(K) = \frac{h(F)}{2^{n+1}m}(\deg(f) - 3) + 1 \quad \textit{and} \quad N(K) \geq \frac{(n+1)h(F)}{2^n m},$$

with equality if $n = q$.

Proof. Note that F is a Kummer extension of the rational function field $\mathbb{F}_q(x)$ with

$$g(F) = \tfrac{1}{2}(\deg(f) - 1)$$

by [16, Example III.7.6]. For each $c \in S$ the place $x - c$ of $\mathbb{F}_q(x)$ is totally ramified in $F/\mathbb{F}_q(x)$, and so is the pole of x in $\mathbb{F}_q(x)$. Let ∞ denote the unique place of F lying over the pole of x in $\mathbb{F}_q(x)$. For the principal divisor $(x - c)$ of F we thus have

$$(x - c) = 2P_c - 2\infty,$$

where all P_c, $c \in S$, are rational places of F. Consequently, the divisor class of $P_c - \infty$ has order 1 or 2 in the group $\mathrm{Div}^0(F)$, and so the subgroup J of $\mathrm{Div}^0(F)$ generated by the divisor classes of all $P_c - \infty$, $c \in S$, has order dividing 2^n. It follows that there exists a subgroup of G of $\mathrm{Div}^0(F)$ with $|G| = 2^n m$ and $G \supseteq J$. Let H_∞ be the Hilbert class field of F with respect to the rational place ∞ and let K be the subfield of the extension H_∞/F fixed by G, viewed as a subgroup of $\mathrm{Gal}(H_\infty/F)$. Then

$$[K : F] = \frac{h(F)}{2^n m}.$$

By construction, the places ∞ and P_c, $c \in S$, split completely in the extension K/F, and this yields the desired lower bound for $N(K)$. Furthermore, K/F is an unramified extension, and so the formula for $g(K)$ follows immediately from the Hurwitz genus formula. ∎

Remark. It is obvious that there is an analog of Theorem 1 with base fields F that are general Kummer extensions of $\mathbb{F}_q(x)$ with arbitrary q, but Theorem 1 is of sufficient generality for our purposes.

From now on we take $q = 5$. In Table 1 we list examples of global function fields $K/\mathbb{F}_5$ with many rational places that are obtained from Theorem 1. The table contains the following data: the value of the genus $g(K)$, the value or a lower bound for the number $N(K)$ of rational places, the values of n and m, the polynomial $f(x)$, and the value of the divisor class number $h(F)$ of $F = \mathbb{F}_5(x, y)$ with $y^2 = f(x)$. In the cases where the exact value of $N(K)$ is indicated, it can be obtained from Theorem 1 or by other simple arguments. The divisor class numbers $h(F)$ have been calculated by the standard method based on the results in [16, Section V.1] and with the help of the software package Mathematica. Table 1 contains entries for $g(K) = 15, 19$, and 21 that improve on earlier examples in [8].

Table 1

$g(K)$	$N(K)$	n	m	$f(x)$	$h(F)$
15	$= 35$	4	1	$x(x+1)(x+2)(x-1)(x^3+x^2+x-2)$	112
19	≥ 45	4	1	$x(x+1)(x+2)(x-2)(x^3-2x^2+2x-2)$	144
21	$= 50$	4	1	$(x^5-x)(x^2-x+1)$	160
23	$= 55$	4	1	$x(x+1)(x+2)(x-1)(x^3+x^2-2x+1)$	176
24	$= 46$	1	1	$x(x^4+x^3+2x^2+x-2)$	46
27	$= 52$	1	1	$x(x-1)(x^3-x+2)$	52
28	$= 54$	5	2	$(x^5-x)(x^2-2x-2)(x^2-2x-1)$	576
29	≥ 56	3	1	$x(x+1)(x+2)(x-1)(x^3+x^2+x-2)$	112
30	$= 58$	1	1	$x(x^4+x^2+2)$	58
32	$= 62$	1	1	$x(x^4+2x^3-2x^2-2x+2)$	62

Table 1 (cont.)

$g(K)$	$N(K)$	n	m	$f(x)$	$h(F)$
35	≥ 68	3	1	$x(x+1)(x+2)(x^4+x^2-2x-2)$	136
37	$=72$	3	1	$x(x+1)(x+2)(x^4-2x-1)$	144
39	$=76$	3	1	$x(x+1)(x+2)(x^4+x^3-2x^2+2x+1)$	152
40	$=65$	4	3	$x(x+1)(x+2)(x-2)(x^5+2x^2-2x+1)$	624
41	$=80$	3	1	$x(x+1)(x+2)(x^4+x-1)$	160
43	$=84$	3	1	$x(x+1)(x+2)(x^4-2x^2-2)$	168
45	$=88$	3	1	$x(x+1)(x+2)(x^4+2x^2+2x+1)$	176
46	≥ 75	4	4	$x(x+1)(x+2)(x-2)(x^3-x^2-x+2)(x^2+x+2)$	960
47	$=92$	3	1	$x(x+1)(x+2)(x^4-2x^2-x-2)$	184
49	$=96$	3	1	$x(x+1)(x+2)(x^4+x^3+2x^2+2)$	192
52	$=102$	5	1	$(x^5-x)(x^4+x^2+2x+2)$	544
53	$=104$	3	1	$x(x+1)(x+2)(x^2+x+2)(x^2-x+1)$	208
55	$=108$	3	1	$x(x+1)(x+2)(x^4+x^2+2x+2)$	216
57	$=112$	3	1	$x(x+1)(x+2)(x^4-2x^2+x+1)$	224
58	≥ 95	4	3	$x(x+1)(x+2)(x-2)(x^5+2x^2+1)$	912
61	$=120$	5	1	$(x^5-x)(x^4+x^2+2)$	640
64	≥ 105	4	2	$x(x+1)(x+2)(x-2)(x^2+x+1)(x^3-x^2-2)$	672
67	$=132$	3	1	$x(x+1)(x+2)(x^4+x^3+x-2)$	264
70	≥ 115	4	2	$x(x+1)(x+2)(x-2)(x^2+2x-1)(x^3-2x^2-1)$	736
76	$=150$	5	1	$(x^5-x)(x^4+2)$	800
85	$=140$	4	1	$x(x+1)(x+2)(x-2)(x^3-x^2-1)(x^2+x+1)$	448
91	≥ 150	4	2	$x(x+1)(x+2)(x-2)(x^3-x^2-x+2)(x^2+x+2)$	960
94	$=155$	4	1	$x(x+1)(x+2)(x-2)(x^5+x^2-2x+2)$	496
97	$=160$	4	1	$x(x+1)(x+2)(x-2)(x^2+x+2)(x^3-x^2-x-1)$	512
100	$=165$	4	1	$x(x+1)(x+2)(x-2)(x^5+x^2+2x-1)$	528
103	≥ 170	4	1	$(x^5-x)(x^4+x^2+2x+2)$	544
109	≥ 180	4	1	$(x^5-x)(x^2-2x-2)(x^2-2x-1)$	576
118	$=195$	4	1	$x(x+1)(x+2)(x-2)(x^5+2x^2-2x+1)$	624
121	$=200$	4	1	$(x^5-x)(x^4+x^2+2)$	640
127	$=210$	4	1	$x(x+1)(x+2)(x-2)(x^2+x+1)(x^3-x^2-2)$	672
139	$=230$	4	1	$x(x+1)(x+2)(x-2)(x^2+2x-1)(x^3-2x^2-1)$	736
151	$=250$	4	1	$(x^5-x)(x^4+2)$	800
172	$=285$	4	1	$x(x+1)(x+2)(x-2)(x^5+2x^2+1)$	912
181	$=300$	4	1	$x(x+1)(x+2)(x-2)(x^3-x^2-x+2)(x^2+x+2)$	960
199	$=330$	4	1	$x(x+1)(x+2)(x-2)(x^5+x^2-x-2)$	1056

4. Further examples. In this section we construct examples of global function fields $K/\mathbb{F}_5$ with many rational places that are obtained by principles other than Theorem 1. In particular, we close all gaps in Table 1 in the range $23 \le g \le 50$. We summarize all our examples from [6], [8], and the present paper in Table 2. We list the value g of the genus, a lower bound N for $N_5(g)$, and a reference to either [6], [8], Table 1 of the present paper (abbreviated "Tb. 1"), or one of the following examples ("Ex.n" stands for Example n).

Table 2

g	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
N	10	12	16	18	20	21	22	22	26	27	32	30	36	39	35	40
Ref	[6]	[6]	[6]	[6]	[6]	[6]	[8]	[6]	[8]	[8]	[8]	[6]	[8]	[8]	Tb.1	[8]

g	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
N	42	32	45	30	50	51	55	46	52	45	52	54	56	58	72	62
Ref	[8]	[8]	Tb.1	[8]	Tb.1	[8]	Tb.1	Tb.1	Ex.1	Ex.2	Tb.1	Tb.1	Tb.1	Tb.1	Ex.3	Tb.1

g	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
N	64	76	68	64	72	78	76	65	80	60	84	60	88	75	92	82
Ref	Ex.4	Ex.5	Tb.1	Ex.6	Tb.1	Ex.7	Tb.1	Tb.1	Tb.1	Ex.8	Tb.1	Ex.9	Tb.1	Tb.1	Tb.1	Ex.10

g	49	50	51	52	53	55	56	57	58	61	64	67	70	76	85	91
N	96	70	104	102	104	108	101	112	95	120	105	132	115	150	140	150
Ref	Tb.1	Ex.11	Ex.12	Tb.1	Tb.1	Tb.1	Ex.13	Tb.1	Tb.1	Tb.1	Tb.1	Tb.1	Tb.1	Tb.1	Tb.1	Tb.1

g	94	97	100	103	109	118	121	127	139	151	172	181	199
N	155	160	165	170	180	195	200	210	230	250	285	300	330
Ref	Tb.1	Tb.1	Tb.1	Tb.1	Tb.1	Tb.1	Tb.1	Tb.1	Tb.1	Tb.1	Tb.1	Tb.1	Tb.1

EXAMPLE 1. $g(K) = 25$, $N(K) \ge 52$. Consider the function field $F = \mathbb{F}_5(x, y)$ with

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

Then $g(F) = 1$, $h(F) = 8$, and the place $x^2 - 2x - 2$ is inert in $F/\mathbb{F}_5(x)$. Let Q be the unique place of F lying over $x^2 - 2x - 2$. Then $\deg(Q) = 4$. We distinguish the rational place ∞ of F which is the unique pole of x, and we denote by A the ring of elements of F that are regular outside ∞. Let E_Q/F be the narrow ray class extension of F with modulus Q. Then

$$[E_Q : F] = |\mathrm{Pic}_Q(A)| = h(F)\Phi_5(Q) = 8 \cdot 624.$$

For $c = 0, 1, 2 \in \mathbb{F}_5$ we have the principal divisors $(x - c) = 2P_c - 2\infty$ in F. Let J be the subgroup of $\mathrm{Pic}_Q(A)$ generated by the residue classes of P_0, P_1, P_2 modulo $\mathcal{P}_Q(A)$. Since $P_c^2 = (x-c)A$ for $c = 0, 1, 2$ and the residue class of x modulo $x^2 - 2x - 2$ generates the group $(\mathbb{F}_5[x]/(x^2 - 2x - 2))^*$ of order 24, the order of J divides $24 \cdot 8 = 192$. Let G be a subgroup of $\mathrm{Pic}_Q(A)$ with $|G| = 384$ and $G \supseteq J$. Now let K be the subfield of E_Q/F fixed by G. Then

$$[K : F] = \frac{8 \cdot 624}{384} = 13.$$

By considering the Artin symbols, we see that P_0, P_1, P_2 split completely in K/F, and ∞ also splits completely in K/F, hence $N(K) \geq 52$. The only ramified place in K/F is Q, and it is totally and tamely ramified. Thus, the Hurwitz genus formula yields $2g(K) - 2 = (13 - 1) \cdot 4$, that is, $g(K) = 25$.

Example 2. $g(K) = 26$, $N(K) \geq 45$. Consider the function field $F = \mathbb{F}_5(x, y)$ with

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

The place $x^5 - x + 1$ is totally ramified in $F/\mathbb{F}_5(x)$. Let Q be the unique place of F lying over $x^5 - x + 1$. Then $\deg(Q) = 5$. We distinguish the rational place ∞ of F which is the unique pole of x, and we denote by A the ring of elements of F that are regular outside ∞. Let E_M/F be the narrow ray class extension of F with modulus $M = Q^2$. Then the 5-rank of the group $\mathrm{Pic}_M(A) \simeq \mathrm{Gal}(E_M/F)$ is at least 5 by the proof of [7, Theorem 3]. For $c \in \mathbb{F}_5$ we have the principal divisors $(x - c) = P_c + P_c' - 2\infty$ in F, with different rational places P_c and P_c'. The subgroup J of $\mathrm{Pic}_M(A)$ generated by the residue classes of P_0, P_1, P_2, P_3 modulo $\mathcal{P}_M(A)$ has 5-rank at most 4. Thus, there exists a subgroup G of $\mathrm{Pic}_M(A)$ with $[\mathrm{Pic}_M(A) : G] = 5$ and $G \supseteq J$.

Now let K be the subfield of E_M/F fixed by G. Then $[K : F] = 5$. Since for each $c \in \mathbb{F}_5$ we have $P_c P_c' = (x - c)A$ and

$$(x - c)^{5^5 - 1} \equiv 1 \bmod M,$$

we see that G contains also the residue classes of P_0', P_1', P_2', P_3' modulo $\mathcal{P}_M(A)$. Therefore the places $P_0, P_0', P_1, P_1', P_2, P_2', P_3, P_3'$, and ∞ split completely in K/F, hence $N(K) \geq 45$. The only ramified place in K/F is Q, and it is totally ramified. By [11, Theorem 1 and Lemma 3] the different exponent of Q in K/F is 8. Using also $g(F) = 2$, we conclude from the Hurwitz genus formula that $2g(K) - 2 = 5 \cdot (4 - 2) + 8 \cdot 5$, that is, $g(K) = 26$.

Example 3. $g(K) = 31$, $N(K) = 72$. Let $L/\mathbb{F}_5$ be the function field in [6, Example 5.4] with $g(L) = 4$ and $N(L) = 18$. Then $[L : \mathbb{F}_5(x)] = 9$ and all rational places of L lie over the zero of x or the pole of x in $\mathbb{F}_5(x)$. The only ramified places in $L/\mathbb{F}_5(x)$ are those lying over $x^2 + 2$ or $x^2 - 2$, each with ramification index 3.

Now let $K = L(y)$ with

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

Then all rational places of L split completely in the Kummer extension K/L, and so $N(K) = 72$. The only ramified places in K/L are those lying over $x^2 + 2$ or $x^2 - 2$, and $g(K) = 31$ follows from the genus formula for Kummer extensions (see [16, Corollary III.7.4]).

Example 4. $g(K) = 33$, $N(K) = 64$, $K = \mathbb{F}_5(x, y_1, y_2)$ with

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

The places $x - 1$, $x - 2$, $x + 1$, and $x + 2$ split completely in $K/\mathbb{F}_5(x)$, thus $N(K) = 64$. The field $L = \mathbb{F}_5(x, y_1)$ is as in [6, Example 5.3], so $g(L) = 3$. The only ramified places in the Kummer extension K/L are those lying over $x^4 + 2$, and $g(K) = 33$ follows from the genus formula for Kummer extensions.

Example 5. $g(K) = 34$, $N(K) = 76$. Consider the cyclotomic function field E_M with modulus $M = x^5 \in \mathbb{F}_5[x]$. With the rational places $P_1 = x+1$ and $P_2 = x - 1$ of $\mathbb{F}_5(x)$, let K be the subfield of the extension $E_M/\mathbb{F}_5(x)$ constructed in [19, Theorem 1] (see also [18, Théorème 1]). Then in the notation of [19, Theorem 1] we have

$$s = s_5(2, 5) = \lceil \log_5 5 \rceil + \left\lceil \log_5 \tfrac{5}{2} \right\rceil = 2,$$

and so $[K : \mathbb{F}_5(x)] = 25$ and $N(K) \geq 25 \cdot 3 + 1 = 76$. To calculate $g(K)$, we proceed as in [19] and consider

$$S = \{f \in \mathbb{F}_5[x] : f(x) = (x + 1)^h (x - 1)^{2j},\ h, j = 0, 1, \ldots\}$$

and

$$S_r = \{f \in S : x^r \parallel (f(x) - 1)\} \qquad \text{for } r = 1, 2, \ldots$$

We have to determine the three least values of r, called $i_1 < i_2 < i_3$, for which S_r is nonempty. It is trivial that S_1 and S_5 are nonempty. From $(x + 1)^2(x - 1)^2 = x^4 - 2x^2 + 1$ we conclude that S_2 is nonempty. Put

$$S(5) = \{\bar{f} \in (\mathbb{F}_5[x]/(x^5))^* : f \in S\},$$

where $\bar{f}$ is the residue class of f modulo x^5. Then $S(5)$ is generated by $\overline{x + 1}$ and $\overline{x^2 - 2x + 1}$, and so $|S(5)| \leq 25$. If we had $i_3 < 5$, then $|S(5)| \geq 125$ by [19, Lemma 3], a contradiction. Therefore $i_1 = 1$, $i_2 = 2$, $i_3 = 5$. In [19, Theorem 1] we thus have $j_1 = 1$ and $j_2 = 2$, and this yields

$$g(K) = 1 + \frac{1}{2} \cdot 25 \cdot 3 - \frac{1}{2}\left(1 + 1 + \frac{25 - 1}{4} + 1\right) = 34.$$

From $N_5(34) \leq 83$ it follows that $N(K) = 76$.

EXAMPLE 6. $g(K) = 36$, $N(K) = 64$, $K = \mathbb{F}_5(x, y_1, y_2, y_3)$ with

$$y_1^2 = x(x^2 - 2), \quad y_2^5 - y_2 = \frac{x^4 - 1}{y_1 - 1}, \quad y_3^2 = x^3 - 2x^2 - x - 2.$$

The field $L = \mathbb{F}_5(x, y_1, y_2)$ is as in [8, Example 4], so $g(L) = 11$ and $N(L) = 32$. All rational places of L split completely in the Kummer extension K/L, hence $N(K) = 64$. The only ramified places in K/L are those lying over $x^3 - 2x^2 - x - 2$, and $g(K) = 36$ follows from the genus formula for Kummer extensions.

EXAMPLE 7. $g(K) = 38$, $N(K) = 78$. Consider the cyclotomic function field E_Q with $Q = x^4 - 2 \in \mathbb{F}_5[x]$. Let G be the cyclic subgroup of $(\mathbb{F}_5[x]/(x^4 - 2))^* \simeq \mathrm{Gal}(E_Q/\mathbb{F}_5(x))$ generated by the residue class of x modulo $x^4 - 2$. Then $|G| = 16$. Now let K be the subfield of $E_Q/\mathbb{F}_5(x)$ fixed by G. Then $[K : \mathbb{F}_5(x)] = 39$. The zero of x and the pole of x in $\mathbb{F}_5(x)$ split completely in $K/\mathbb{F}_5(x)$, thus $N(K) \geq 78$. The only ramified place in $K/\mathbb{F}_5(x)$ is Q, and it is totally and tamely ramified. Therefore the Hurwitz genus formula yields $2g(K) - 2 = 39 \cdot (-2) + (39 - 1) \cdot 4$, that is, $g(K) = 38$. From $N_5(38) \leq 91$ it follows that $N(K) = 78$.

EXAMPLE 8. $g(K) = 42$, $N(K) = 60$, $K = \mathbb{F}_5(x, y_1, y_2)$ with

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

The field $L = \mathbb{F}_5(x, y_1)$ is as in [6, Example 5.2], so $g(L) = 2$ and $N(L) = 12$. All rational places of L split completely in the Artin–Schreier extension K/L, hence $N(K) = 60$. The only ramified places in K/L are the unique place of L of degree 2 lying over $x^2 + 2$ and the unique place of L of degree 4 lying over $x^4 - 2x^2 - 2$, thus $g(K) = 42$ follows from the genus formula for Artin–Schreier extensions (see [16, Proposition III.7.8]).

EXAMPLE 9. $g(K) = 44$, $N(K) = 60$, $K = \mathbb{F}_5(x, y_1, y_2)$ with

$$y_1^5 - y_1 = \frac{x^5 - x}{(x^2 + 2)^3}, \quad y_2^2 = (x^2 + 2)(x^8 - x^4 - x^2 - 2).$$

The field $L = \mathbb{F}_5(x, y_1)$ is as in [6, Example 5.12A], so $g(L) = 12$ and $N(L) = 30$. All rational places of L split completely in the Kummer extension K/L, hence $N(K) = 60$. The only ramified places in K/L are the unique place of L of degree 2 lying over $x^2 + 2$ and the places of L lying over $x^8 - x^4 - x^2 - 2$, thus $g(K) = 44$ follows from the genus formula for Kummer extensions.

EXAMPLE 10. $g(K) = 48$, $N(K) = 82$, $K = \mathbb{F}_5(x, y_1, y_2, y_3)$ with

$$y_1^2 = x(x^2 - 2), \quad y_2^5 - y_2 = \frac{x^4 - 1}{y_1}, \quad y_3^2 = x^3 - 2x^2 - x - 2.$$

The field $L = \mathbb{F}_5(x, y_1, y_2)$ is as in [8, Example 9], so $g(L) = 17$ and $N(L) = 42$. All rational places of L, except the unique place of L lying over x, split completely in the Kummer extension K/L, hence $N(K) = 82$. The only ramified places in K/L are those lying over $x^3 - 2x^2 - x - 2$, and $g(K) = 48$ follows from the genus formula for Kummer extensions.

Example 11. $g(K) = 50$, $N(K) = 70$. Let $L/\mathbb{F}_5$ be the function field in Table 1 with $g(L) = 15$ and $N(L) = 35$. By the construction in the proof of Theorem 1 we have $[L : \mathbb{F}_5(x)] = 14$, and the rational places of L lie over $x, x + 1, x + 2, x - 1$ or the pole of x, with each rational place of L having ramification index 2 over $\mathbb{F}_5(x)$. Now let $K = L(z)$ with

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

Then all rational places of L split completely in the Kummer extension K/L, hence $N(K) = 70$. The only ramified places in K/L are those lying over $x^3 + 2x^2 - x - 1$, and $g(K) = 50$ follows from the genus formula for Kummer extensions.

Example 12. $g(K) = 51$, $N(K) = 104$. Let E_Q/F be the same narrow ray class extension as in Example 1 and let J be the same subgroup of $\mathrm{Pic}_Q(A)$ as in Example 1. Let G be a subgroup of $\mathrm{Pic}_Q(A)$ with $|G| = 192$ and $G \supseteq J$. Now let K be the subfield of E_Q/F fixed by G. Then $[K : F] = 26$. As in Example 1 we see that the places P_0, P_1, P_2, and ∞ split completely in K/F, hence $N(K) \geq 104$. The only ramified place in K/F is Q, and it is totally and tamely ramified. Thus, the Hurwitz genus formula yields $2g(K) - 2 = (26 - 1) \cdot 4$, that is, $g(K) = 51$. From $N_5(51) \leq 115$ it follows that $N(K) = 104$.

Example 13. $g(K) = 56$, $N(K) = 101$. Consider the cyclotomic function field E_M with modulus $M = x^7 \in \mathbb{F}_5[x]$. With the rational places $P_1 = x + 1, P_2 = x - 1$, and $P_3 = x + 2$, let K be the subfield of the extension $E_M/\mathbb{F}_5(x)$ constructed in [19, Theorem 1] (see also [18, Théorème 1]). Then in the notation of [19, Theorem 1] we have

$$s = s_5(3, 7) = \lceil \log_5 7 \rceil + \left\lceil \log_5 \tfrac{7}{2} \right\rceil + \left\lceil \log_5 \tfrac{7}{3} \right\rceil = 4,$$

and so $[K : \mathbb{F}_5(x)] = 25$ and $N(K) \geq 25 \cdot 4 + 1 = 101$. To calculate $g(K)$, we proceed as in [19] and consider

$$S = \{f \in \mathbb{F}_5[x] : f(0) = 1,\ f(x) = (x+1)^h (x-1)^j (x+2)^k,\ h, j, k = 0, 1, \ldots\}$$

and

$$S_r = \{f \in S : x^r \parallel (f(x) - 1)\} \quad \text{for } r = 1, 2, \ldots$$

We have to obtain information on the five least values of r, called $i_1 < i_2 < i_3 < i_4 < i_5$, for which S_r is nonempty. It is trivial that S_1 and S_5 are nonempty. From $(x + 1)^2(x - 1)^2 = x^4 - 2x^2 + 1$ we conclude that S_2 is nonempty, and from

$$(x+1)(x-1)^8(x+2)^4 = x^{13} + \ldots + 2x^3 + 1$$

we conclude that S_3 is nonempty. Therefore $i_1 = 1$, $i_2 = 2$, $i_3 = 3$. Put

$$S(5) = \{\bar{f} \in (\mathbb{F}_5[x]/(x^5))^* : f \in S\},$$

where $\bar{f}$ is the residue class of f modulo x^5. Then $S(5)$ is generated by $\overline{1+x}$, $\overline{1-x}$, and $\overline{1-2x}$, and so $|S(5)| \le 5^3$. If we had $i_4 = 4$, then $|S(5)| = 5^4$ by [19, Lemma 3], a contradiction. Therefore $i_4 = 5$. Put

$$S(7) = \{\bar{\bar{f}} \in (\mathbb{F}_5[x]/(x^7))^* : f \in S\},$$

where $\bar{\bar{f}}$ is the residue class of f modulo x^7. Then $S(7)$ is generated by $\overline{\overline{1+x}}$, $\overline{\overline{1-x}}$, and $\overline{\overline{1-2x}}$. Since $S(7)$ is contained in the 5-Sylow subgroup of $(\mathbb{F}_5[x]/(x^7))^*$, it follows from [19, Lemma 4(ii)] that $|S(7)| \le 5^s = 5^4$. If we had $i_5 = 6$, then $|S(7)| = 5^5$ by [19, Lemma 3], a contradiction. Therefore $i_5 \ge 7$. In [19, Theorem 1] we thus have $j_1 = 1$, $j_2 = 2$, $j_3 = 3$, $j_4 = 5$, and this yields

$$g(K) = 1 + \frac{1}{2} \cdot 25 \cdot 5 - \frac{1}{2}\left(1 + 1 + 1 + 5 + \frac{25-1}{4} + 1\right) = 56.$$

From $N_5(56) \le 125$ it follows that $N(K) = 101$.

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

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

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

[8] —, —, *Global function fields with many rational places over the quinary field*, Demonstratio Math. 30 (1997), 919–930.

[9] —, —, *The algebraic-geometry approach to low-discrepancy sequences*, in: Monte Carlo and Quasi-Monte Carlo Methods 1996, H. Niederreiter *et al.* (eds.), Lecture Notes in Statist. 127, Springer, New York, 1998, 139–160.

[10] —, —, *Algebraic curves over finite fields with many rational points*, in: Number Theory, K. Győry, A. Pethő, and V. T. Sós (eds.), de Gruyter, Berlin, 1998, 423–443.

[11] H. Niederreiter and C. P. Xing, *Global function fields with many rational places and their applications*, in: Proc. Finite Fields Conf. (Waterloo, 1997), Contemp. Math., Amer. Math. Soc., Providence, to appear.
[12] —, —, *Nets*, (t, s)*-sequences, and algebraic geometry*, in: Pseudo- and Quasi-Random Point Sets, P. Hellekalek and G. Larcher (eds.), Lecture Notes in Statist., Springer, New York, to appear.
[13] O. Pretzel, *Codes and Algebraic Curves*, Oxford Univ. Press, Oxford, 1998.
[14] M. Rosen, *The Hilbert class field in function fields*, Exposition. Math. 5 (1987), 365–378.
[15] 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.
[16] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.
[17] 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.
[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] —, —, *Drinfeld modules of rank* 1 *and algebraic curves with many rational points*, Monatsh. Math., to appear.

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

Department of Information Systems
and Computer Science
The National University of Singapore
Lower Kent Ridge Road
Singapore 119260
E-mail: xingcp@comp.nus.edu.sg

Received on 22.6.1998 (3412)