ACTA ARITHMETICA
LXXIX.1 (1997)

Cyclotomic function fields, Hilbert class fields, and global function fields with many rational places

by

Harald Niederreiter (Wien) and Chaoping Xing (Hefei)

Dedicated to Professor J. W. S. Cassels on the occasion of his 75th birthday

1. Introduction. Let K be a global function field with full constant field $\mathbb{F}_q$, where q is an arbitrary prime power. 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 K 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.

Global function fields K with many rational places, that is, with $N(K)$ close to $N_q(g(K))$, 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. We refer e.g. to the work of Ihara [7] and Serre [16]–[19] in the 1980s and to the more recent papers of Garcia and Stichtenoth [2], [3], Niederreiter and Xing [10], [11], Perret [12], Schoof [15], van der Geer and van der Vlugt [22], [23], Xing [25], and Xing and Niederreiter [27], [28]. 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 an interesting problem *per se*, but it is also important for applications in the theory of algebraic-geometry codes (see [20], [21]) and in the recent constructions of low-discrepancy sequences introduced by the authors [9], [11], [26].

The research of the second author was supported by the Austrian Academy of Sciences and the Chinese Natural Science Foundation.

For the practical aspects of these applications it is important that the constructions of global function fields with many rational places are *explicit*, in the sense that they yield descriptions in terms of generators and defining equations. The constructions by Serre [16]–[19] use class field theory and are thus not explicit. More attention is now devoted to the desideratum of obtaining explicit constructions. Typical explicit constructions use Artin–Schreier extensions (see Garcia and Stichtenoth [2] and Niederreiter and Xing [10], [11]), Kummer extensions (see Voß and Høholdt [24] and Xing [25]), and subfields of cyclotomic function fields (see Niederreiter and Xing [10] and Quebbemann [13]).

The present paper can be viewed as a continuation of the work in [10] which led to a catalog of explicitly constructed global function fields over the binary field $\mathbb{F}_2$ with many rational places. We now extend this work to other small finite fields $\mathbb{F}_q$ that are of practical interest, specifically for $q = 3, 4, 5$. We employ various methods based on Artin–Schreier extensions, Kummer extensions, cyclotomic function fields, and in some cases also Hilbert class fields. Except for the examples based on Hilbert class fields, all global function fields are explicitly constructed, but in some examples using cyclotomic function fields one may need a computer algebra system to calculate the defining equation. Some examples are quite straightforward, but others require detailed arguments to validate them. In Section 2 we recall the necessary background on cyclotomic function fields and Hilbert class fields and in Sections 3, 4, and 5 we present our examples for the cases $q = 3, 4$, and 5, respectively.

2. Background on cyclotomic function fields and Hilbert class fields. Let $B = \mathbb{F}_q[x]$ be the polynomial ring over $\mathbb{F}_q$ and $F = \mathbb{F}_q(x)$ the rational function field. We will often use the convention that a monic irreducible polynomial P in B is identified with the place of F 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 F, that is, for the place of F which is the unique pole of x. For an arbitrary place Q of a global function field we write ν_Q for the normalized discrete valuation corresponding to Q.

We briefly describe the theory of cyclotomic function fields as developed by Hayes [4]. For a fixed algebraic closure F^{ac} of F, let $\mu \in \mathrm{End}_{\mathbb{F}_q}(F^{\mathrm{ac}})$ be given by

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

There is a ring homomorphism

$$B \to \mathrm{End}_{\mathbb{F}_q}(F^{\mathrm{ac}}), \qquad f(x) \mapsto f(\mu).$$

The $\mathbb{F}_q$-vector space F^{ac} is made into a B-module by

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

This B-module is a Carlitz module, which is the simplest type of Drinfeld module; see Carlitz [1] and Hayes [4], [6]. For any monic polynomial $M \in B$ we define the B-module

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

of division points. Then Λ_M is a cyclic B-module which is B-isomorphic to $B_M := B/(M)$. The *cyclotomic function field* $F_M := F(\Lambda_M)$ is the subfield of F^{ac} generated over F by all elements of Λ_M. Then F_M/F is a finite abelian extension and $\mathrm{Gal}(F_M/F)$ is isomorphic to B_M^*, the group of units of the ring B_M. For $f \in B$ we write $\overline{f}$ for the residue class of f mod M. Then the Galois automorphism $\sigma_A \in \mathrm{Gal}(F_M/F)$ associated with the element $\overline{A} \in B_M^*$ is determined by $\sigma_A(\lambda) = \lambda^A$ for $\lambda \in \Lambda_M$. If $P \in B$ is a monic irreducible polynomial not dividing M, then the Artin symbol

$$\left[\frac{F_M/F}{P}\right]$$

of the place P is equal to σ_P. Furthermore, if M and N are two monic coprime polynomials in B, then F_{MN} is the composite field of F_M and F_N. Proofs of these results can be found in Hayes [4].

For monic polynomials $M \in B$, the Euler function Φ_q is defined by $\Phi_q(M) = |B_M^*|$, the order of the group B_M^*. If M has degree $d \geq 1$, then according to [8, Lemma 3.69] we have the formula

$$\Phi_q(M) = q^d \prod_{i=1}^{r} (1 - q^{-d_i}),$$

where $d_1, \ldots, d_r$ are the degrees of the distinct monic irreducible polynomials over $\mathbb{F}_q$ dividing M. There is a special subgroup of B_M^* consisting of all residue classes $\overline{c}$ with a nonzero $c \in \mathbb{F}_q$; we denote this subgroup by $\mathbb{F}_q^*$.

For a finite abelian extension E/K, a place P of K, and a place Q of E lying over P, the decomposition group of Q over P depends only on P and E/K, but not on Q, and so we can call it the *decomposition group of P in E/K*. This subgroup of $\mathrm{Gal}(E/K)$ fixes a subfield of E/K which we call the *decomposition field of P in E/K*. It is a well-known fact (see e.g. [20, Theorem III.8.3]) that for an intermediate field L of E/K, the place P splits completely in L/K if and only if L is contained in the decomposition field of P in E/K. For the convenience of the reader we also state the following results from Hayes [4], [5].

PROPOSITION 1. *Let $M = P^n$ for some integer $n \geq 1$ and some monic irreducible polynomial P over $\mathbb{F}_q$ of degree d. Then*:

(i) *The place ∞ of F splits into $\Phi_q(M)/(q-1)$ places in F_M/F, each with ramification index $q-1$. In particular, each place of F_M lying over ∞ is rational and the full constant field of F_M is $\mathbb{F}_q$. The decomposition group of ∞ in F_M/F is $\mathbb{F}_q^*$.*

(ii) *The only places of F that can be ramified in F_M/F are ∞ and P, and P is totally ramified. The genus of F_M is given by*

$$g(F_M) = \frac{1}{2}\left(\frac{qnd - nd - q}{q-1}\Phi_q(M) - dq^{d(n-1)} + 2\right).$$

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

Next we recall some pertinent facts about Hilbert class fields. A convenient reference for this topic is Rosen [14]. Let L be a global function field with full constant field $\mathbb{F}_q$ and assume that $N(L) \geq 1$. We distinguish a rational place P_∞ of L and let A be the P_∞-integral ring of L, i.e., A consists of the elements of L that are regular outside P_∞. Then the *Hilbert class field* H_{P_∞} of L with respect to P_∞ is the maximal unramified abelian extension of L (in a fixed separable closure of L) in which P_∞ splits completely. The extension H_{P_∞}/L is finite and its Galois group is isomorphic to the fractional ideal class group $\mathrm{Pic}(A)$ of A, which in the case under consideration (P_∞ rational) is isomorphic to the group $\mathrm{Div}^0(L)$ of divisor classes of L of degree 0. In particular, we have $[H_{P_\infty} : L] = h(L)$, the divisor class number of L. For each place P of L there is an associated Galois automorphism $\tau_P \in \mathrm{Gal}(H_{P_\infty}/L)$, and the Artin symbol of P for the extension H_{P_∞}/L is equal to τ_P. The place P corresponds to the divisor class of $P - \deg(P)P_\infty$ in $\mathrm{Div}^0(L)$. Next we prove two theorems on which several of our examples are based.

THEOREM 1. *Let $F = \mathbb{F}_q(x)$ and let L/F be an extension of degree $r \geq 2$ with $g(L) \geq 1$. Assume that there are two different rational places P and P_∞ of L which are totally ramified over F, with P_∞ lying over ∞, and suppose that $1, 2, \ldots, r-1$ are gap numbers of P. Then there exists a global function field K with full constant field $\mathbb{F}_q$ such that*

$$g(K) = \frac{h(L)}{r}(g(L) - 1) + 1 \quad \textit{and} \quad N(K) = \frac{2h(L)}{r}.$$

Proof. It follows from the conditions on P and P_∞ that $rP - rP_\infty$ is a principal divisor of L. Moreover, the condition on the gap numbers of P implies that, for each $1 \leq k \leq r-1$, the divisor $kP - kP_\infty$ of L is not principal. Consequently, the divisor class $[P - P_\infty]$ of $P - P_\infty$ in $\mathrm{Div}^0(L)$ has order r. Let G be the cyclic subgroup of $\mathrm{Div}^0(L)$ generated by $[P - P_\infty]$. Let H_{P_∞} be the Hilbert class field of L with respect to P_∞ and let K be the

subfield of H_{P_∞}/L fixed by G. Then $[K : L] = h(L)/r$. From the definition of the Hilbert class field we get that P_∞ splits completely in K/L, and by considering the Artin symbol we see that P also splits completely in K/L. Thus $N(K) \geq 2h(L)/r$. Furthermore, the extension K/L is unramified, and so the Hurwitz genus formula yields

$$2g(K) - 2 = \frac{h(L)}{r}(2g(L) - 2),$$

whence the formula for $g(K)$ in the theorem. Next we note that a rational place $Q \neq P, P_\infty$ of L splits completely in K/L if and only if the divisor class $[Q - P_\infty]$ belongs to G. This is equivalent to $[Q - P_\infty] = n[P - P_\infty]$ for some integer n with $0 \leq n \leq r - 1$, and this condition can be written as $[Q - nP + (n-1)P_\infty] = [0]$. But this identity is impossible for $n = 0$ by the Weierstrass gap theorem and for $1 \leq n \leq r - 1$ by the condition on the gap numbers of P. Therefore $N(K) = 2h(L)/r$. ∎

R e m a r k 1. If the degree r is a prime and we drop the condition on the gap numbers of P in Theorem 1, then we can still conclude that $N(K) \geq 2h(L)/r$ and that $N(K)$ is a multiple of $h(L)/r$, with $g(K)$ being given by the same formula as in Theorem 1.

R e m a r k 2. The same conclusion as in Remark 1 can be reached if we assume that L is an arbitrary global function field with full constant field $\mathbb{F}_q$, that P and P_∞ are two different rational places of L, and that r is the least positive integer such that $rP - rP_\infty$ is a principal divisor of L.

THEOREM 2. *Let the global function field L be a constant field extension of the global function field L_1 with $N(L_1) \geq 1$. Then there exists a global function field K with the same full constant field as L such that*

$$g(K) = \frac{h(L)}{h(L_1)}(g(L) - 1) + 1 \quad \textit{and} \quad N(K) = \frac{h(L)N(L_1)}{h(L_1)}.$$

P r o o f. Let P_∞ be a rational place of L lying over a rational place of L_1 and let H_{P_∞} be the Hilbert class field of L with respect to P_∞. Then $\mathrm{Gal}(H_{P_\infty}/L) = \mathrm{Div}^0(L)$. Let K be the subfield of H_{P_∞}/L fixed by $\mathrm{Div}^0(L_1)$. Then $[K : L] = h(L)/h(L_1)$. The rational places of L that are lying over a rational place of L_1 split completely in K/L. Therefore

$$N(K) = \frac{h(L)N(L_1)}{h(L_1)}.$$

Since the extension K/L is unramified, the Hurwitz genus formula yields

$$2g(K) - 2 = \frac{h(L)}{h(L_1)}(2g(L) - 2),$$

and the formula for $g(K)$ in the theorem follows. ∎

We will not review the theory of Artin–Schreier extensions and Kummer extensions since an excellent summary of it can be found in the book of Stichtenoth [20, Section III.7].

We recall from Section 1 that $N_q(g)$ is the maximum number of rational places that a global function field with full constant field $\mathbb{F}_q$ and genus g can have. Values or upper bounds for $N_q(g)$ are tabulated in Serre [16]–[19]; see also Niederreiter and Xing [11]. A global function field K with full constant field $\mathbb{F}_q$ and genus g is called *optimal* if $N(K) = N_q(g)$. The trivial optimal function field $K = F = \mathbb{F}_q(x)$ with $g(K) = 0$ and $N(K) = q + 1$ will not be listed among the following examples.

3. The case $q = 3$. In this section we list examples of global function fields K with full constant field $\mathbb{F}_3$ and many rational places. Most of these examples are obtained by an explicit construction. We summarize the results in the following table. An entry that corresponds to an optimal function field is marked with an asterisk.

Table 1

$g(K)$	1^*	2^*	3^*	4^*	5	6	7	8	9^*	10	11	12	13	14	15^*
$N(K)$	7	8	10	12	12	14	16	15	19	19	20	22	24	24	28

EXAMPLE 3.1. $g(K) = 1$, $N(K) = 7$, $K = \mathbb{F}_3(x, y)$ with

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

In the Kummer extension K/F, the places $x, x+1$, and $x-1$ split completely and the place ∞ is totally ramified. The only other ramified place of K is lying over $x^3 - x + 1$. This example is well known.

EXAMPLE 3.2. $g(K) = 2$, $N(K) = 8$, $K = \mathbb{F}_3(x, y)$ with

$$y^2 = x^6 - x^2 + 1.$$

All rational places of F split completely in the Kummer extension K/F. The only ramified place of K lies over $x^6 - x^2 + 1$.

EXAMPLE 3.3. $g(K) = 3$, $N(K) = 10$, $K = \mathbb{F}_3(x, y)$ with

$$y^3 - y = x^4 - x^2.$$

In the Artin–Schreier extension K/F, the places x, $x + 1$, and $x - 1$ split completely and the place ∞ is totally ramified. This example is listed in Serre [19].

EXAMPLE 3.4. $g(K) = 4$, $N(K) = 12$, $K = \mathbb{F}_3(x, y)$ with

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

All rational places of F split completely in the Artin–Schreier extension K/F. The only ramified place of K lies over x^2+1.

EXAMPLE 3.5. $g(K)=5$, $N(K)=12$, $K=\mathbb{F}_3(x,y_1,y_2)$ with

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

In this tower of Kummer extensions, the places x, $x+1$, and $x-1$ split completely in K/F. The first Kummer extension is the one from Example 3.1.

EXAMPLE 3.6. $g(K)=6$, $N(K)=14$, $K=\mathbb{F}_3(x,y_1,y_2)$ with

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

Note that $L=\mathbb{F}_3(x,y_1)$ is the field in Example 3.1. The rational places of L are P_∞, the unique place lying over ∞, and $P_1=(0,1)$, $P_2=(1,2)$, $P_3=(2,1)$, $P_4=(0,2)$, $P_5=(1,1)$, $P_6=(2,2)$, where $P=(a,b)$ is the rational place determined by $(x,y_1)\equiv(a,b) \bmod P$. Since $\nu_{P_\infty}(y_1)=-3$, the principal divisor of u is given by

$$(u) = \sum_{i=3}^{6} P_i - P_1 - 3P_\infty.$$

Therefore, the places P_3, P_4, P_5, and P_6 split completely in the Artin–Schreier extension K/L and P_1 is totally ramified in K/L. Furthermore, a short calculation yields

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

and so P_∞ is also totally ramified in K/L.

EXAMPLE 3.7. $g(K)=7$, $N(K)=16$. Consider the irreducible polynomial $P=x^4+x^3+x^2+x+1$ over $\mathbb{F}_3$ and the corresponding cyclotomic function field F_P. The Galois group $\mathrm{Gal}(F_P/F)=B_P^*$ has order 80. Let K be the subfield of F_P/F fixed by the subgroup $H=\mathbb{F}_3^*\cdot\langle\overline{x}\rangle$ of B_P^*, where $\langle\overline{x}\rangle$ is the cyclic subgroup generated by $\overline{x}\in B_P^*$. Then $|H|=10$ and $[K:F]=8$. From parts (i) and (ii) of Proposition 1 we know that P is the unique ramified place in K/F and that it is totally and tamely ramified. Moreover, the place ∞ splits completely in K/F. Since $\overline{x}\in H$, a consideration of the Artin symbol of the place x shows that x also splits completely in K/F. The genus of K is obtained from the Hurwitz genus formula, in the form given in [20, Theorem III.4.12], which yields $2g(K)-2=-2\cdot 8+4\cdot(8-1)$, i.e., $g(K)=7$.

EXAMPLE 3.8. $g(K)=8$, $N(K)=15$, $K=\mathbb{F}_3(x,y_1,y_2)$ with

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

This example was already given in the appendix of [9]. Note that $L = \mathbb{F}_3(x, y_1)$ is the field in Example 3.1. The places x and $x-1$ split completely in K/F and ∞ is totally ramified in K/F. The two places of L lying over $x+1$ are totally ramified in the Artin–Schreier extension K/L.

EXAMPLE 3.9. $g(K) = 9$, $N(K) = 19$, $K = \mathbb{F}_3(x, y_1, y_2)$ with

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

This example was also given in the appendix of [9]. For $L = \mathbb{F}_3(x, y_1)$ we have $g(L) = 1$ and $N(L) = 7$. The places x and $x-1$ split completely in the Artin–Schreier extension L/F and ∞ is totally ramified in L/F. The places of L lying over x or $x-1$ split completely in the Artin–Schreier extension K/L and the unique place of L lying over $x+1$ has degree 3 and is totally ramified in K/L. If P_∞ is the unique place of L lying over ∞, then $\nu_{P_\infty}(y_1) = -2$ and a straightforward calculation shows that

$$\nu_{P_\infty}\left(\frac{x(x-1)}{x+1} - \left(\frac{x+1}{y_1}\right)^3 + \frac{x+1}{y_1}\right) = -1.$$

Thus, P_∞ is totally ramified in K/L.

EXAMPLE 3.10. $g(K) = 10$, $N(K) = 19$. Consider the cyclotomic function field $E = F_M$ with $M = x^5 \in \mathbb{F}_3[x]$. The Galois group $\mathrm{Gal}(E/F) = B_M^*$ has order 162. Let K be the subfield of E/F fixed by the subgroup $H = \mathbb{F}_3^* \cdot \langle \overline{x+1} \rangle$ of B_M^*, where $\langle \overline{x+1} \rangle$ is the cyclic subgroup generated by $\overline{x+1} \in B_M^*$. Then $|H| = [E : K] = 18$ and $[K : F] = 9$. By Proposition 1(i), the place ∞ splits completely in K/F. Since $\overline{x+1} \in H$, a consideration of the Artin symbol of the place $x+1$ shows that $x+1$ also splits completely in K/F. The place x is totally ramified in K/F by Proposition 1(ii). To calculate the genus of K, we consider the extension E/K. Let Q be the unique place of K lying over the place x and R the unique place of E lying over Q. Let $\lambda \in \Lambda_{x^5}$ be a root of $f(z) = z^{x^5}/z^{x^4}$, then λ is an R-prime element by Proposition 1(iii). Furthermore, the minimal polynomial of λ over K is

$$m(z) = \prod_{\tau \in H} (z - \tau(\lambda)) \in K[z].$$

It follows then from [20, Proposition III.5.12] that the different exponent $d(R|Q)$ of R over Q is given by

$$\begin{aligned} d(R|Q) = \nu_R(m'(\lambda)) &= \sum_{\tau \in H \setminus \{\overline{1}\}} \nu_R(\lambda - \tau(\lambda)) \\ &= \sum_{i=1}^{8} \nu_R(\lambda - \lambda^{(x+1)^i}) + \sum_{i=0}^{8} \nu_R(\lambda - \lambda^{2(x+1)^i}). \end{aligned}$$

It is clear that $\nu_R(\lambda - \lambda^{2(x+1)^i}) = 1$ for $0 \le i \le 8$ since the constant term of the polynomial $2(x+1)^i$ is not equal to 1. Furthermore, we have

$$\nu_R(\lambda - \lambda^{(x+1)^i}) = \begin{cases} 27 & \text{for } i = 3, 6, \\ 3 & \text{for } i = 1, 2, 4, 5, 7, 8. \end{cases}$$

Thus, we get $d(R|Q) = 81$. The 81 places of E lying over ∞ are tamely ramified in E/K with ramification index 2 by Proposition 1(i). Altogether, the Hurwitz genus formula yields

$$18(2g(K) - 2) + 81 \cdot 1 + 81 \cdot (2 - 1) = 2g(E) - 2 = 486,$$

where the last identity is obtained from Proposition 1(ii). Hence we get $g(K) = 10$.

EXAMPLE 3.11. $g(K) = 11$, $N(K) = 20$. Let $L = \mathbb{F}_3(x, y)$ with

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

We have $g(L) = 2$ and $N(L) = 6$, with the places $x + 1$ and $x - 1$ splitting completely in the Kummer extension L/F and x and ∞ being totally ramified in L/F. Furthermore, L has exactly two places of degree 2. By the standard method (see [20, Theorem V.1.15]) we get the divisor class number $h(L) = 20$. Now it suffices to invoke Theorem 1 with $r = 2$. The condition on the gap numbers of P in Theorem 1 follows from the Weierstrass gap theorem.

EXAMPLE 3.12. $g(K) = 12$, $N(K) = 22$. Let $L = \mathbb{F}_3(x, y)$ with

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

Then $g(L) = 2$ and $N(L) = 6$, with the places $x+1$ and $x-1$ splitting completely in the Kummer extension L/F and x and ∞ being totally ramified in L/F. Furthermore, L has exactly four places of degree 2. Thus we get $h(L) = 22$. Now it suffices to invoke Theorem 1 with $r = 2$. The condition on the gap numbers of P in Theorem 1 follows from the Weierstrass gap theorem.

EXAMPLE 3.13. $g(K) = 13$, $N(K) = 24$. Let $L = \mathbb{F}_3(x, y)$ with

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

Then $g(L) = 2$ and $N(L) = 6$, with the places $x+1$ and $x-1$ splitting completely in the Kummer extension L/F and x and ∞ being totally ramified in L/F. Furthermore, L has exactly six places of degree 2. Thus we get $h(L) = 24$. Now it suffices to invoke Theorem 1 with $r = 2$. The condition on the gap numbers of P in Theorem 1 follows from the Weierstrass gap theorem.

EXAMPLE 3.14. $g(K) = 14$, $N(K) = 24$, $K = \mathbb{F}_3(x, y_1, y_2)$ with

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

For $L = \mathbb{F}_3(x, y_1)$ we have $g(L) = 2$ and $N(L) = 8$, with all rational places of F splitting completely in the Kummer extension L/F. Furthermore, all rational places of L split completely in the Artin–Schreier extension K/L, and the unique place of L lying over x^2+1 is the only ramified place in K/L.

EXAMPLE 3.15. $g(K) = 15$, $N(K) = 28$. Consider the cyclotomic function field $E = F_M$ with $M = x^6 \in \mathbb{F}_3[x]$. The Galois group $\mathrm{Gal}(E/F) = B_M^*$ has order 486. Let K be the subfield of E/F fixed by the subgroup H of B_M^* generated by $\overline{x+1}$ and $\overline{x-1}$. By noting that $(x-1)^6 \equiv (x+1)^3 \bmod x^6$, it is easily seen that $|H| = 54$. We also have $\mathbb{F}_3^* \subseteq H$ and $[K : F] = 9$. By Proposition 1(i), the place ∞ splits completely in K/F. By considering the Artin symbols, we see that the places $x+1$ and $x-1$ also split completely in K/F. Furthermore, the place x is totally ramified in K/F by Proposition 1(ii). To calculate the genus of K, we consider the extension E/K. Let Q be the unique place of K lying over the place x and R the unique place of E lying over Q. Then, as in Example 3.10, we obtain that the different exponent $d(R|Q)$ of R over Q is given by

$$d(R|Q) = \sum_{\tau \in H \setminus \{\overline{1}\}} \nu_R(\lambda - \tau(\lambda)),$$

where $\lambda \in \Lambda_{x^6}$ is a root of $f(z) = z^{x^6}/z^{x^5}$. The elements of H are the residue classes of $(-1)^i(x+1)^j(x-1)^k \bmod x^6$, where $i \in \{0,1\}$, $j \in \{0,1,2\}$, and $k \in \{0,1,\ldots,8\}$. The values of $\nu_R(\lambda - \tau(\lambda))$ are calculated by noting that $\tau(\lambda) = \lambda^{s(x)}$ for some polynomial $s(x)$ over $\mathbb{F}_3$ of degree ≤ 5, that $\nu_R(\lambda - \tau(\lambda)) = 1$ if the constant term of $s(x)$ is $\ne 1$, and that if $s(x) \ne 1$ and the constant term of $s(x)$ is 1, then $\nu_R(\lambda - \tau(\lambda)) = 3^r$ with r being the least positive integer for which the coefficient of x^r in $s(x)$ is $\ne 0$. Among the values of $\nu_R(\lambda - \tau(\lambda))$ with $\tau \in H \setminus \{\overline{1}\}$, exactly 27 values are equal to 1, exactly 18 values are equal to 3, exactly six values are equal to 9, and exactly two values are equal to 27. This leads to $d(R|Q) = 189$. The 243 places of E lying over ∞ are tamely ramified in E/K with ramification index 2 by Proposition 1(i). Altogether, the Hurwitz genus formula yields

$$54(2g(K) - 2) + 189 \cdot 1 + 243 \cdot (2-1) = 2g(E) - 2 = 1944,$$

where the last identity is obtained from Proposition 1(ii). Hence we get $g(K) = 15$.

4. The case $q = 4$. In this section we list examples of global function fields K with full constant field $\mathbb{F}_4$ and many rational places. Most of these examples are obtained by an explicit construction. We always write α for an element of $\mathbb{F}_4$ satisfying $\alpha^2 + \alpha + 1 = 0$. We summarize the results in the following table. An entry that corresponds to an optimal function field

is marked with an asterisk.

Table 2

$g(K)$	1^*	2^*	3^*	4^*	5	6^*	7	8	9	10	11	12	13	15
$N(K)$	9	10	14	15	17	20	21	21	22	27	25	28	30	33

EXAMPLE 4.1. $g(K) = 1$, $N(K) = 9$, $K = \mathbb{F}_4(x, y)$ with

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

The places $x, x+1, x+\alpha$, and $x+\alpha+1$ split completely in the Artin–Schreier extension K/F and the place ∞ is totally ramified in K/F. This example is a special case of [20, Example VI.4.2].

EXAMPLE 4.2. $g(K) = 2$, $N(K) = 10$, $K = \mathbb{F}_4(x, y)$ with

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

All rational places of F split completely in the Artin–Schreier extension K/F. The only ramified place of K lies over $x^3 + x + 1$. This example was given by Serre [19].

EXAMPLE 4.3. $g(K) = 3$, $N(K) = 14$. Consider the irreducible polynomial $P = x^3 + \alpha$ over $\mathbb{F}_4$ and the corresponding cyclotomic function field F_P. The Galois group $\mathrm{Gal}(F_P/F) = B_P^*$ has order 63. Let K be the subfield of F_P/F fixed by the subgroup of B_P^* generated by $\overline{x}$. Then $[K : F] = 7$. The place ∞ splits completely in K/F by Proposition 1(i), and a consideration of the Artin symbol shows that the place x also splits completely in K/F. By Proposition 1(ii), P is the unique ramified place in K/F and it is totally and tamely ramified. Thus, the Hurwitz genus formula yields $2g(K) - 2 = -2 \cdot 7 + 3 \cdot (7 - 1)$, i.e., $g(K) = 3$. An example obtained from a Klein curve is listed in Serre [19].

EXAMPLE 4.4A. $g(K) = 4$, $N(K) = 15$, $K = \mathbb{F}_4(x, y_1, y_2)$ with

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

Let $L = \mathbb{F}_4(x, y_1)$ be the field in Example 4.1. Then, using the notation in Example 3.6, the four places of L given by $(0, 0)$, $(0, 1)$, (α, α), and $(\alpha + 1, \alpha + 1)$ split completely in the Kummer extension K/L. The place of L lying over ∞ and the two places of L lying over $x + 1$ are totally ramified in K/L. This example is equivalent to one given by Voß and Høholdt [24].

EXAMPLE 4.4B. $g(K) = 4$, $N(K) = 15$. Consider the cyclotomic function field F_M with $M = x^4 + x + 1 \in \mathbb{F}_4[x]$. Since $x^4 + x + 1 = (x^2 + x + \alpha)(x^2 + x + \alpha^2)$ in $\mathbb{F}_4[x]$, F_M is the composite field of $F_{x^2+x+\alpha}$ and $F_{x^2+x+\alpha^2}$ by [4, Proposition 1.4] and the Galois group $\mathrm{Gal}(F_M/F) = B_M^*$ has order 225. Let K be the subfield of F_M/F fixed by the subgroup $H = \mathbb{F}_4^* \cdot (\mathbb{F}_2[x]/(M))^*$

of B_M^*. Then $|H| = 45$ and $[K : F] = 5$. Since the decomposition group of ∞ in both $F_{x^2+x+\alpha}/F$ and $F_{x^2+x+\alpha^2}/F$ has order 3 by Proposition 1(i), the decomposition group of ∞ in F_M/F has order 3 or 9. In both cases, the decomposition group of ∞ in F_M/F is contained in H, and so ∞ splits completely in K/F. Since $\overline{x}$, $\overline{x+1} \in H$, the places x and $x+1$ also split completely in K/F. The only places of K that can be ramified in K/F are those lying over $x^2+x+\alpha$ or $x^2+x+\alpha^2$, and they are tamely ramified. Hence by the Hurwitz genus formula,

$$2g(K) - 2 \le -2 \cdot 5 + 2 \cdot (5-1) + 2 \cdot (5-1),$$

i.e., $g(K) \le 4$. But $N(K) = 15 > N_4(g)$ for $g = 0, 1, 2, 3$, and so we must have $g(K) = 4$.

EXAMPLE 4.5. $g(K) = 5$, $N(K) = 17$. Consider the cyclotomic function field F_M with $M = x^4 \in \mathbb{F}_4[x]$ and Galois group $\mathrm{Gal}(F_M/F) = B_M^*$ of order 192. Let K be the subfield of F_M/F fixed by the subgroup $H = \mathbb{F}_4^* \cdot (\mathbb{F}_2[x]/(M))^*$ of B_M^*. Then $|H| = 24$ and $[K : F] = 8$. The places $x+1$ and ∞ split completely in K/F and the place x is totally ramified in K/F. This example is a member of the family of function fields constructed by Quebbemann [13].

EXAMPLE 4.6. $g(K) = 6$, $N(K) = 20$. Let $L = \mathbb{F}_4(x, y)$ with

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

and $L_1 = \mathbb{F}_2(x, y)$, so that L is a constant field extension of L_1. Note that L is the field in Example 4.2, hence $g(L) = 2$ and $N(L) = 10$. The corresponding values for L_1 are $g(L_1) = 2$ and $N(L_1) = 4$. Furthermore, L_1 has exactly three places of degree 2. Let $h(L)$ be the divisor class number of L and $h(L_1)$ the divisor class number of L_1. Then it follows from [20, Proposition V.1.10 and Theorem V.1.15] that $h(L)/h(L_1) = 5$. Now it suffices to invoke Theorem 2.

EXAMPLE 4.7. $g(K) = 7$, $N(K) = 21$. Consider the cyclotomic function field F_M with $M = (x^3+x+1)^2 \in \mathbb{F}_4[x]$ and Galois group $\mathrm{Gal}(F_M/F) = B_M^*$ of order $(4^3 - 1) \cdot 4^3$. Let $H = S_2 \cdot S_7 \subseteq B_M^*$, where S_2 is the 2-Sylow subgroup and S_7 the 7-Sylow subgroup of B_M^*. Then $|H| = 7 \cdot 4^3$. Let K be the subfield of F_M/F fixed by H, then $[K : F] = 9$. Since the order of $\overline{x}$ and $\overline{x+1}$ in B_M^* is 14, we have $\overline{x}, \overline{x+1} \in H$, and so the places x and $x+1$ split completely in K/F. Furthermore, the place ∞ splits into three rational places of K, each with ramification index 3, and the place $x^3 + x + 1$ is totally and tamely ramified in K/F. Thus, the Hurwitz genus formula yields $2g(K) - 2 = -9 \cdot 2 + 3 \cdot (3-1) + 3 \cdot (9-1)$, that is, $g(K) = 7$.

EXAMPLE 4.8. $g(K) = 8$, $N(K) = 21$. Let $L = \mathbb{F}_4(x, y)$ with

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

and $L_1 = \mathbb{F}_2(x, y)$, so that L is a constant field extension of L_1. We have $g(L) = g(L_1) = 2$, $N(L) = 9$, and $N(L_1) = 3$. Furthermore, L_1 has exactly three places of degree 2. Then $h(L)/h(L_1) = 7$ in the notation of Example 4.6. Now it suffices to invoke Theorem 2.

EXAMPLE 4.9. $g(K) = 9$, $N(K) = 22$, $K = \mathbb{F}_4(x, y_1, y_2)$ with

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

For $L = \mathbb{F}_4(x, y_1)$ we have $g(L) = 3$ and $N(L) = 13$. The places x, $x + 1$, $x + \alpha$, and $x + \alpha^2$ split completely in the Kummer extension L/F and ∞ is totally ramified in L/F. Four rational places P of L are totally ramified in the Artin–Schreier extension K/L, namely those P lying over x or $x + 1$ with $y_1 \equiv \alpha \bmod P$ or $y_1 \equiv \alpha^2 \bmod P$. The nine remaining rational places of L split completely in K/L.

EXAMPLE 4.10. $g(K) = 10$, $N(K) = 27$. Consider the cyclotomic function field $E = F_{P_1 P_2}$ with the irreducible polynomials $P_1 = x^3 + x + 1$ and $P_2 = x^3 + x^2 + 1$ in $\mathbb{F}_4[x]$ and the subfields $L_1 = F_{P_1}$ and $L_2 = F_{P_2}$ of E/F. For $i = 1, 2$ let K_i be a subfield of L_i/F such that K_i is contained in the decomposition field of ∞ in L_i/F and $[K_i : F] = 3$. Let K be the composite field of K_1 and K_2. Since L_1 and L_2 are linearly disjoint by the proof of [4, Theorem 2.3], we have $[K : F] = 9$. The place ∞ splits completely in K_1/F and K_2/F, and so ∞ splits completely in K/F by [20, Corollary III.8.4]. Note that $G = (\mathbb{F}_2[x]/(P_1 P_2))^*$ is a subgroup of $\mathrm{Gal}(E/F) = B^*_{P_1 P_2}$ of order 49 and is thus the 7-Sylow subgroup of $\mathrm{Gal}(E/F)$. Consequently, G is contained in the Galois group $\mathrm{Gal}(E/K)$ of order $9 \cdot 7^2$. By considering the Artin symbols, we see that the places x and $x + 1$ split completely in K/F, thus $N(K) = 3 \cdot 9 = 27$. In order to determine the genus of K, we observe that the place $x^3 + x + 1$ is unramified in K_2/F and the place $x^3 + x^2 + 1$ is unramified in K_1/F and we use Abhyankar's lemma [20, Proposition III.8.9]. Thus, $x^3 + x + 1$ and $x^3 + x^2 + 1$ are tamely ramified in K/F, each with ramification index 3. Together with the Hurwitz genus formula this shows that $2g(K) - 2 = -2 \cdot 9 + 9 \cdot (3 - 1) + 9 \cdot (3 - 1)$, that is, $g(K) = 10$.

EXAMPLE 4.11. $g(K) = 11$, $N(K) = 25$, $K = \mathbb{F}_4(x, y_1, y_2)$ with

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

Note that $L = \mathbb{F}_4(x, y_1)$ is as in Example 4.9, so that $g(L) = 3$ and $N(L) = 13$. The unique place of L lying over ∞ is totally ramified in the Artin–Schreier extension K/L and the other 12 rational places of L split completely in K/L.

EXAMPLE 4.12. $g(K) = 12$, $N(K) = 28$. Let L be the field in Example 4.3 with $g(L) = 3$, $N(L) = 14$, and $[L : F] = 7$. Recall that the places x and ∞ split completely in L/F. Now let $K = L(y)$ with

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

Then all rational places of L split completely in the Artin–Schreier extension K/L. The only ramified place in K/L is the unique place of L of degree 7 lying over $x + 1$.

EXAMPLE 4.13A. $g(K) = 13$, $N(K) = 30$, $K = \mathbb{F}_4(x, y_1, y_2, y_3)$ with

$$y_1^2 + y_1 = x^3, \quad y_2^2 + y_2 = \left(\frac{y_1}{x}\right)^3, \quad y_3^2 + y_3 = \left(\frac{xy_2}{y_1}\right)^3.$$

Thus, K is obtained by a tower of Artin–Schreier extensions. The places $x + 1, x + \alpha$, and $x + \alpha + 1$ split completely in K/F, the place x splits into one rational place of K with ramification index 4 and four rational unramified places of K, and the place ∞ is totally ramified in K/F. This example is a member of the family of function fields constructed by Garcia and Stichtenoth [2].

EXAMPLE 4.13B. $g(K) = 13$, $N(K) = 30$. Let L be the field in Example 4.4B with $g(L) = 4$, $N(L) = 15$, and $[L : F] = 5$. Recall that the places $x, x + 1$, and ∞ split completely in L/F and that the place $x^2 + x + \alpha$ is totally ramified in L/F. Now let $K = L(y)$ with

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

Then all rational places of L split completely in the Artin–Schreier extension K/L. The only ramified place in K/L is the unique place of L lying over $x^2 + x + \alpha$.

EXAMPLE 4.14. $g(K) = 15$, $N(K) = 33$. Consider the cyclotomic function field F_P with the irreducible polynomial $P = x^5 + x^2 + 1$ over $\mathbb{F}_4$. The Galois group $\mathrm{Gal}(F_P/F) = B_P^*$ has order 1023. Let K be the subfield of F_P/F fixed by the subgroup $H = \mathbb{F}_4^* \cdot (\mathbb{F}_2[x]/(P))^*$ of B_P^*. Then $|H| = 93$ and $[K : F] = 11$. The places x, $x + 1$, and ∞ split completely in K/F. The only ramified place in K/F is the place lying over $x^5 + x^2 + 1$ and it is totally and tamely ramified. Thus, the Hurwitz genus formula yields $2g(K) - 2 = -2 \cdot 11 + 5 \cdot (11 - 1)$, i.e., $g(K) = 15$.

5. The case $q = 5$. In this section we list examples of global function fields K with full constant field $\mathbb{F}_5$ and many rational places. All examples are obtained by an explicit construction. We summarize the results in the following table. An entry that corresponds to an optimal function field is

marked with an asterisk.

Table 3

$g(K)$	1^*	2^*	3^*	4^*	5	6	7	8	9	10	11	12
$N(K)$	10	12	16	18	20	21	20	22	24	26	26	30

EXAMPLE 5.1. $g(K) = 1$, $N(K) = 10$, $K = \mathbb{F}_5(x, y)$ with

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

All rational places of F except ∞ split completely in the Kummer extension K/F. The only ramified place of K lies over $x^4 + 2$.

EXAMPLE 5.2. $g(K) = 2$, $N(K) = 12$, $K = \mathbb{F}_5(x, y)$ with

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

All rational places of F split completely in the Kummer extension K/F. The only ramified places of K are those lying over $x^2 + 2$ or $x^4 + 3x^2 + 3$.

EXAMPLE 5.3. $g(K) = 3$, $N(K) = 16$, $K = \mathbb{F}_5(x, y)$ with

$$y^4 = 2 - x^4.$$

The places $x - 1$, $x - 2$, $x + 1$, and $x + 2$ split completely in the Kummer extension K/F. The only ramified place of K lies over $x^4 - 2$. This example was given by Serre [19].

EXAMPLE 5.4. $g(K) = 4$, $N(K) = 18$. Consider the cyclotomic function field $E = F_{P_1 P_2}$ with the irreducible polynomials $P_1 = x^2 + 2$ and $P_2 = x^2 + 3$ in $\mathbb{F}_5[x]$ and the subfields $L_1 = F_{P_1}$ and $L_2 = F_{P_2}$ of E/F. For $i = 1, 2$ let K_i be the subfield of L_i/F fixed by the cyclic subgroup $\langle \overline{x} \rangle$ of $\mathrm{Gal}(L_i/F) = B^*_{P_i}$; then $[K_i : F] = 3$. The places x and ∞ split completely in both K_1/F and K_2/F. Let K be the composite field of K_1 and K_2. Then $[K : F] = 9$ since L_1 and L_2 are linearly disjoint by the proof of [4, Theorem 2.3]. Furthermore, the places x and ∞ split completely in K/F by [20, Corollary III.8.4], and so $N(K) \geq 18$. The only ramified places in K/F are those lying over $x^2 + 2$ or $x^2 + 3$, each with ramification index 3 by Abhyankar's lemma [20, Proposition III.8.9]. Thus, the Hurwitz genus formula yields $2g(K) - 2 = -2 \cdot 9 + 3 \cdot 2 \cdot (3 - 1) + 3 \cdot 2 \cdot (3 - 1)$, that is, $g(K) = 4$. Since $N_5(4) = 18$, we must have $N(K) = 18$.

EXAMPLE 5.5. $g(K) = 5$, $N(K) = 20$, $K = \mathbb{F}_5(x, y_1, y_2)$ with

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

Note that $L = \mathbb{F}_5(x, y_1)$ is the field in Example 5.1. All rational places of L split completely in the Kummer extension K/L. The only ramified places in K/F are those lying over $x^4 + 2$ or $x^4 + 4x^3 + x^2 + 4x + 3$.

EXAMPLE 5.6. $g(K) = 6$, $N(K) = 21$, $K = \mathbb{F}_5(x, y)$ with

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

The places x, $x-1$, $x-2$, and $x-3$ split completely in the Artin–Schreier extension K/F and the place ∞ is totally ramified in K/F. This example was already given in the appendix of [9].

EXAMPLE 5.7. $g(K) = 7$, $N(K) = 20$, $K = \mathbb{F}_5(x, y_1, y_2)$ with

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

Thus, K is obtained by a tower of Kummer extensions. The places x, $x-1$, $x-2$, $x-3$, and ∞ split completely in K/F. The only ramified places of K are those lying over either x^2+2, x^4+3x^2+3, or $x^4+2x^3+2x^2+1$.

EXAMPLE 5.8. $g(K) = 8$, $N(K) = 22$, $K = \mathbb{F}_5(x, y)$ with

$$y^5 - y = \frac{x^4-1}{x}.$$

The places $x-1$, $x-2$, $x-3$, and $x-4$ split completely in the Artin–Schreier extension K/F and the places x and ∞ are totally ramified in K/F.

EXAMPLE 5.9. $g(K) = 9$, $N(K) = 24$, $K = \mathbb{F}_5(x, y_1, y_2)$ with

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

Note that $L = \mathbb{F}_5(x, y_1)$ is the field in Example 5.2. All rational places of L split completely in the Kummer extension K/L. The only ramified places in K/L are those lying over x^3+x^2+4x+1 or x^3+4x^2+4x+4.

EXAMPLE 5.10. $g(K) = 10$, $N(K) = 26$, $K = \mathbb{F}_5(x, y)$ with

$$y^5 - y = \frac{x^4-1}{x^6}.$$

The places $x-1$, $x-2$, $x-3$, $x-4$, and ∞ split completely in the Artin–Schreier extension K/F and the place x is totally ramified in K/F.

EXAMPLE 5.11. $g(K) = 11$, $N(K) = 26$, $K = \mathbb{F}_5(x, y_1, y_2)$ with

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

Note that $L = \mathbb{F}_5(x, y_1)$ satisfies $g(L) = 3$ and $N(L) = 14$. The places x, $x-1$, and $x-2$ split completely in the Kummer extension L/F and the places $x+1$ and ∞ are totally ramified in L/F. The 13 rational places of L lying over either x, $x-1$, $x-2$, or ∞ split completely in the Kummer extension K/L. The only ramified places in K/L are those lying over $x+2$ or x^2+2.

EXAMPLE 5.12A. $g(K) = 12$, $N(K) = 30$, $K = \mathbb{F}_5(x, y)$ with

$$y^5 - y = \frac{x^5-x}{(x^2+2)^3}.$$

All rational places of F split completely in the Artin–Schreier extension K/F. The only ramified place of K lies over x^2+2.

EXAMPLE 5.12B. $g(K) = 12$, $N(K) = 30$. Consider the cyclotomic function field $E = F_M$ with $M = (x^2+2)^2 \in \mathbb{F}_5[x]$ and Galois group $\mathrm{Gal}(E/F) = B_M^*$ of order 600. Let K be the subfield of E/F fixed by the cyclic subgroup $H = \langle \overline{x} \rangle$ of B_M^*. Then $|H| = 40$ and $[K : F] = 15$. The places x and ∞ split completely in K/F. To calculate the genus of K, we consider the extension E/K whose only ramified places are those lying over x^2+2 or ∞. Let Q be the unique place of K lying over x^2+2 and R the unique place of E lying over Q. Then, as in Example 3.10, we obtain that the different exponent $d(R|Q)$ of R over Q is given by

$$d(R|Q) = \sum_{\tau \in H \setminus \{\overline{1}\}} \nu_R(\lambda - \tau(\lambda)),$$

where $\lambda \in \Lambda_M$ is a root of $f(z) = z^{(x^2+2)^2}/z^{x^2+2}$. Since $x^{10} \equiv 3 \bmod M$, the elements of H are the residue classes of $cx^i \bmod M$, where c is an arbitrary nonzero element of $\mathbb{F}_5$ and $0 \le i \le 9$. The values of $\nu = \nu_R(\lambda - \tau(\lambda))$ in the sum above are as follows. For $i = 0$ and $c \ne 1$ we have $\nu = 1$; for $i = 1, 3, 5, 7, 9$ and all c we have $\nu = 1$; for each $i = 2, 4, 6, 8$ we have $\nu = 25$ for exactly one value of c and $\nu = 1$ for the other values of c. Altogether, four values of ν are equal to 25 and 35 values are equal to 1, so that $d(R|Q) = 135$. The 150 places of E lying over ∞ are tamely ramified in E/K with ramification index 4 by Proposition 1(i). Thus, the Hurwitz genus formula yields

$$40(2g(K) - 2) + 135 \cdot 2 + 150 \cdot (4 - 1) = 2g(E) - 2 = 1600,$$

where the last identity is obtained from Proposition 1(ii). Hence we get $g(K) = 12$.

References

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

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

[3] —, —, *On the asymptotic behaviour of some towers of function fields over finite fields*, J. Number Theory, to appear.

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

[5] —, *Stickelberger elements in function fields*, Compositio Math. 55 (1985), 209–239.

[6] —, *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.

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

[8] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, revised ed., Cambridge University Press, Cambridge, 1994.
[9] H. Niederreiter and C. P. Xing, *Low-discrepancy sequences and global function fields with many rational places*, Finite Fields Appl. 2 (1996), 241–273.
[10] —, —, *Explicit global function fields over the binary field with many rational places*, Acta Arith. 75 (1996), 383–396.
[11] —, —, *Quasirandom points and global function fields*, in: Finite Fields and Applications, S. D. Cohen and H. Niederreiter (eds.), Cambridge University Press, Cambridge, 1996, 269–296.
[12] M. Perret, *Tours ramifiées infinies de corps de classes*, J. Number Theory 38 (1991), 300–322.
[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] R. Schoof, *Algebraic curves over $\mathbb{F}_2$ with many rational points*, J. Number Theory 41 (1992), 6–14.
[16] 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.
[17] —, *Nombres de points des courbes algébriques sur $\mathbb{F}_q$*, Sém. Théorie des Nombres 1982-1983, Exp. 22, Univ. de Bordeaux I, Talence, 1983.
[18] —, *Résumé des cours de 1983-1984*, Annuaire du Collège de France (1984), 79–83.
[19] —, *Rational Points on Curves over Finite Fields*, lecture notes, Harvard University, 1985.
[20] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.
[21] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*, Kluwer, Dordrecht, 1991.
[22] G. van der Geer and M. van der Vlugt, *Curves over finite fields of characteristic 2 with many rational points*, C. R. Acad. Sci. Paris Sér. I Math. 317 (1993), 593–597.
[23] —, —, *How to construct curves over finite fields with many rational points*, preprint, 1995.
[24] C. Voß and T. Høholdt, *A family of Kummer extensions of the Hermitian function field*, Comm. Algebra 23 (1995), 1551–1566.
[25] C. P. Xing, *Multiple Kummer extension and the number of prime divisors of degree one in function fields*, J. Pure Appl. Algebra 84 (1993), 85–93.
[26] C. P. Xing and H. Niederreiter, *A construction of low-discrepancy sequences using global function fields*, Acta Arith. 73 (1995), 87–102.
[27] —, —, *Modules de Drinfeld et courbes algébriques ayant beaucoup de points rationnels*, C. R. Acad. Sci. Paris Sér. I Math. 322 (1996), 651–654.
[28] —, —, *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@oeaw.ac.at

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

Received on 19.4.1996 (2966)