ACTA ARITHMETICA
LXXXI.1 (1997)

Drinfeld modules of rank 1 and algebraic curves with many rational points. II

by

Harald Niederreiter (Wien) and Chaoping Xing (Hefei)

1. Introduction. We continue the presentation of new constructions of algebraic curves over a finite field $\mathbb{F}_q$ with many $\mathbb{F}_q$-rational points by a method based on Drinfeld modules of rank 1 which was initiated in our earlier papers [28], [29]. By an algebraic curve over $\mathbb{F}_q$ we always mean a projective, smooth, absolutely irreducible algebraic curve defined over $\mathbb{F}_q$. Let $N(C)$ denote the number of $\mathbb{F}_q$-rational points of C. For given $g \geq 0$ and q we put

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

where the maximum is extended over all algebraic curves C of fixed genus g over $\mathbb{F}_q$.

An algebraic curve C over $\mathbb{F}_q$ of genus g is called *optimal* if $N(C) = N_q(g)$. Optimal curves, and more generally algebraic curves C over $\mathbb{F}_q$ of genus g with many $\mathbb{F}_q$-rational points, i.e., with $N(C)$ close to $N_q(g)$, have received a lot of attention in the literature. We refer e.g. to the work of Ihara [6] and Serre [15]–[18] in the 1980s and to the more recent papers of Garcia and Stichtenoth [1], [3], Niederreiter and Xing [8]–[10], Perret [11], Schoof [14], van der Geer and van der Vlugt [23], [24], Xing [26], and Xing and Niederreiter [28], [29]. The construction 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 [21], [22]) and in the recent constructions of low-discrepancy sequences introduced by the authors [7], [8], [27].

It will be convenient to use the correspondence between an algebraic curve C over $\mathbb{F}_q$ and its function field K, which is a global function field with full constant field $\mathbb{F}_q$, i.e., with $\mathbb{F}_q$ algebraically closed in K. An $\mathbb{F}_q$-

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

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

rational point of C corresponds to a rational place (i.e., a place of degree 1) of K, and vice versa, and the genus of C is the same as the genus of K. If K is an arbitrary global function field which has $\mathbb{F}_q$ as its full constant field (if we want to stress this property, it will be expressed by the notation $K/\mathbb{F}_q$), then $N(K) = N(K/\mathbb{F}_q)$ denotes the number of rational places of K and $g(K)$ the genus of K. By analogy with the case of algebraic curves, we call K *optimal* if $N(K) = N_q(g(K))$. Throughout this paper we will use the language of algebraic curves over finite fields and that of global function fields interchangeably.

The constructions of algebraic curves over $\mathbb{F}_q$ with many $\mathbb{F}_q$-rational points presented in our earlier papers [28], [29] were restricted to the case where q is a prime. The present paper is devoted to general prime powers q, with a stress on the case where q is composite which requires new ideas. In Section 2 we review the necessary background on Hilbert class fields and Drinfeld modules, in particular the theory of narrow ray class fields obtained from sgn-normalized Drinfeld modules of rank 1. Three different constructions of algebraic curves over $\mathbb{F}_q$ with many $\mathbb{F}_q$-rational points, or equivalently of global function fields with many rational places, are described in Sections 3 and 4. In Section 5 we present various specific examples of algebraic curves over $\mathbb{F}_4$ with many $\mathbb{F}_4$-rational points as well as a table of the intervals in which $N_4(g)$ lies for many values of g.

2. Background on Hilbert class fields and Drinfeld modules. We recall some pertinent facts about Hilbert class fields. A convenient reference for this topic is Rosen [12]. Let $F/\mathbb{F}_q$ be a global function field with $N(F/\mathbb{F}_q) \geq 1$. We distinguish a rational place ∞ of F and let A be the ∞-integral ring of F, i.e., A consists of the elements of F that are regular outside ∞. Then the *Hilbert class field* H_A of F with respect to A is the maximal unramified abelian extension of F (in a fixed separable closure of F) in which ∞ splits completely. The extension H_A/F 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 (∞ rational) is isomorphic to the group of divisor classes of F of degree 0. In particular, we have $[H_A : F] = h(F)$, the divisor class number of F. The value of $h(F)$ can be obtained from the L-polynomial

$$L_F(t) = (1-t)(1-qt)Z_F(t)$$

of F, where $Z_F(t)$ is the zeta-function of F, by the formula $h(F) = L_F(1)$. For $r \geq 2$ the constant field extension $F_r = \mathbb{F}_{q^r} \cdot F$ is viewed as a global function field with full constant field $\mathbb{F}_{q^r}$. In the case $r = 2$ we have

$$h(F_2)/h(F) = L_F(-1). \tag{1}$$

This follows from [21, Theorem V.1.15].

For the basic facts on Drinfeld modules we refer to the survey article of Hayes [5]. Let the global function field $F/\mathbb{F}_q$, the rational place ∞ of F, and the ∞-integral ring A of F be as above. We fix a sgn-function and let ϕ be a sgn-normalized Drinfeld A-module of rank 1 defined over H_A. The additive group of the algebraic closure $\overline{H}_A$ of H_A forms an A-module under the action of ϕ. For any nonzero ideal M in A we consider the M-torsion module

$$\Lambda(M) = \{u \in \overline{H}_A : \phi_M(u) = 0\}.$$

Then $\Lambda(M)$ is a cyclic A-module which is isomorphic to A/M and has $|(A/M)^*|$ generators, where $(A/M)^*$ is the group of units of the ring A/M.

Let $\mathcal{I}(A)$ be the fractional ideal group of A and let $\mathcal{I}_M(A)$ be the subgroup of all fractional ideals in $\mathcal{I}(A)$ which are prime to M. We define the quotient group

$$\mathrm{Pic}_M(A) = \mathcal{I}_M(A)/\mathcal{R}_M(A),$$

where $\mathcal{R}_M(A)$ is the subgroup of $\mathcal{I}_M(A)$ consisting of all principal ideals bA with $\mathrm{sgn}(b) = 1$ and $b \equiv 1 \bmod M$. We will often identify places and prime ideals in the obvious manner. Furthermore, for an arbitrary place P of a global function field we write ν_P for the corresponding normalized discrete valuation.

The field $H_A(\Lambda(M))$ generated by the elements of $\Lambda(M)$ over H_A is called the *narrow ray class field modulo* M. This field is independent of the specific choice of the sgn-normalized Drinfeld A-module ϕ of rank 1. The following facts from [5] are needed.

PROPOSITION 1. *Let $E = H_A(\Lambda(M))$ be the narrow ray class field modulo M. Then*:

(i) *The extension E/F is unramified away from ∞ and the prime ideals in A dividing M.*

(ii) *The extension E/F is abelian and there is an isomorphism $\sigma : \mathrm{Pic}_M(A) \to \mathrm{Gal}(E/F)$, determined by $\sigma_I\phi = I * \phi$ for any ideal I in A prime to M, and $\lambda^{\sigma_I} = \phi_I(\lambda)$ for any generator λ of the cyclic A-module $\Lambda(M)$. Moreover, for any ideal I in A that is prime to M, the corresponding Artin automorphism of E/F is exactly σ_I.*

(iii) *The multiplicative group $(A/M)^*$ is isomorphic to $\mathrm{Gal}(E/H_A)$ by means of $b \mapsto \sigma_{bA}$, where $b \in A$ satisfies $\mathrm{sgn}(b) = 1$ and is prime to M.*

We now consider the special case where M is a power of a prime ideal. The results in part (i) of the following proposition can be found in [5], and the genus formula in part (ii) was shown in [29].

PROPOSITION 2. *Let $E = H_A(\Lambda(P^n))$ be the narrow ray class field modulo P^n, where P is a prime ideal in A and $n \geq 1$. Then*:

(i) *If λ is a generator of the cyclic A-module $\Lambda(P^n)$, then $E = H_A(\lambda)$ and the minimal polynomial of λ over H_A is*

$$f(z) := \phi_{P^n}(z)/\phi_{P^{n-1}}(z).$$

Moreover, $f(z)$ is Eisenstein at any place Q of H_A lying over P. Thus, Q is totally ramified in E/H_A and $\nu_R(\lambda) = 1$ for the place R of E lying over Q.

(ii) *If $\deg(P) = d$, then for the genus $g(E)$ of E we have*

$$2g(E) - 2$$
$$= h(F)q^{d(n-1)}\left((2g(F) - 2)(q^d - 1) + dn(q^d - 1) - d + \frac{(q^d - 1)(q - 2)}{q - 1}\right).$$

Let $F/\mathbb{F}_q$ again be a global function field, let ∞ be a rational place of F and A the ∞-integral ring of F. For $r \geq 2$ we consider the constant field extension $F_r = \mathbb{F}_{q^r} \cdot F$. Then ∞ can be viewed as a rational place of $F_r/\mathbb{F}_{q^r}$ with ∞-integral ring A_r of F_r. Let $P \neq \infty$ be a place of F of degree d with $\gcd(d, r) = 1$. Then similarly, P is a place of $F_r/\mathbb{F}_{q^r}$ of the same degree d. We now consider the group $\mathrm{Pic}_{P^n}(A_r)$ for a given $n \geq 1$. Note that $(A_r/P^n)^*$ can be viewed as a subgroup of $\mathrm{Pic}_{P^n}(A_r)$ in the following way: for every $a \in A_r$ there is a $b \in F_r$ satisfying $\mathrm{sgn}(b) = 1$ and $b \equiv a \bmod P^n$; then we have the embedding $(A_r/P^n)^* \ni \overline{a} \mapsto \overline{bA} \in \mathrm{Pic}_{P^n}(A_r)$.

Next we observe that $\mathrm{Pic}_{P^n}(A)$ can also be viewed as a subgroup of $\mathrm{Pic}_{P^n}(A_r)$. One way to see this is to use the language of algebraic curves. Let C be an algebraic curve over $\mathbb{F}_q$ with function field F. If we view C as a curve over $\overline{\mathbb{F}}_q$, then a divisor D on $C/\overline{\mathbb{F}}_q$ is a divisor of F if and only if D is $\mathbb{F}_q$-rational, i.e.,

$$D^\psi = D \quad \text{for all } \psi \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q).$$

Hence $\mathrm{Pic}_{P^n}(A)$ can be described as the group of all $\mathbb{F}_q$-rational divisors on $C/\overline{\mathbb{F}}_q$ prime to P and ∞, from which we factor out the subgroup of all divisors $(c)_0$ with $c \in F$, $\mathrm{sgn}(c) = 1$, and $c \equiv 1 \bmod P^n$, where $(c)_0$ is the divisor corresponding to the principal ideal cA. We have an analogous description for $\mathrm{Pic}_{P^n}(A_r)$, and this leads to a natural embedding of $\mathrm{Pic}_{P^n}(A)$ into $\mathrm{Pic}_{P^n}(A_r)$.

Let I_∞ be the subgroup of $(A_r/P^n)^*$ formed by the residue classes mod P^n of the elements of $\mathbb{F}_{q^r}^*$, so that in particular $|I_\infty| = q^r - 1$. According to Hayes [4], [5], I_∞ is both the decomposition group and the inertia group of ∞ in the extension $H_{A_r}(\Lambda(P^n))/F_r$.

Lemma 1. *We have*

$$(A_r/P^n)^* \cap (I_\infty \cdot \mathrm{Pic}_{P^n}(A)) = I_\infty \cdot (A/P^n)^*,$$

where all groups are considered as subgroups of $\mathrm{Pic}_{P^n}(A_r)$.

P r o o f. It is trivial that $I_\infty \cdot (A/P^n)^* \subseteq (A_r/P^n)^* \cap (I_\infty \cdot \mathrm{Pic}_{P^n}(A))$. Conversely, consider an element of $(A_r/P^n)^* \cap (I_\infty \cdot \mathrm{Pic}_{P^n}(A))$. This element is a residue class mod $\mathcal{R}_{P^n}(A_r)$ determined by an $\mathbb{F}_{q^r}$-rational divisor D prime to P and ∞. Since D represents an element of $(A_r/P^n)^*$, we can write $D = (a)_0$ with $a \in F_r$, $\mathrm{sgn}(a) = 1$, and $a \not\equiv 0 \bmod P$, where $(a)_0$ is the divisor corresponding to the principal ideal aA_r. Now D also represents an element of $I_\infty \cdot \mathrm{Pic}_{P^n}(A)$, hence mod $\mathcal{R}_{P^n}(A_r)$ we can write $D = (b)_0 + D_1$, where $b \in F_r$, $\mathrm{sgn}(b) = 1$, $b \equiv \alpha \bmod P^n$ for some $\alpha \in \mathbb{F}_{q^r}^*$, and D_1 is an $\mathbb{F}_q$-rational divisor prime to P and ∞. Thus, mod $\mathcal{R}_{P^n}(A_r)$ we have

$$(a)_0 = (b)_0 + D_1,$$

and so

$$(ab^{-1})_0 - D_1 = (c)_0$$

for some $c \in F_r$ with $\mathrm{sgn}(c) = 1$ and $c \equiv 1 \bmod P^n$. This means that $D_1 = (ab^{-1}c^{-1})_0$. Since D_1 and ∞ are $\mathbb{F}_q$-rational, it follows that $ab^{-1}c^{-1} \in F$, hence D_1 represents an element of $(A/P^n)^*$. In view of $D = (b)_0 + D_1$, we conclude that D represents an element of $I_\infty \cdot (A/P^n)^*$. ∎

3. The first construction. We show how to use narrow ray class fields to construct global function fields over $\mathbb{F}_{q^r}$ with many rational places from global function fields over $\mathbb{F}_q$ with many rational places. The notations from the previous sections will remain operative. In particular, we recall that $F_r = \mathbb{F}_{q^r} \cdot F$, viewed as a global function field with full constant field $\mathbb{F}_{q^r}$, denotes a constant field extension of the global function field $F/\mathbb{F}_q$, and that $h(F)$ and $h(F_r)$ denote the divisor class numbers of F and F_r, respectively.

Theorem 1. *Let $F/\mathbb{F}_q$ be a global function field of genus $g(F)$ with $N(F) \geq 2$. Then for all integers $n \geq 1$ and $r \geq 2$ there exists a global function field $K_{n,r}/\mathbb{F}_{q^r}$ such that*:

(i) *The number of rational places of $K_{n,r}/\mathbb{F}_{q^r}$ is given by*

$$N(K_{n,r}) = \frac{h(F_r)}{h(F)}(1 + q^{(r-1)(n-1)}(N(F) - 1)).$$

(ii) *The genus of $K_{n,r}/\mathbb{F}_{q^r}$ satisfies*

$$\frac{h(F)}{h(F_r)}(2g(K_{n,r}) - 2) = q^{(r-1)(n-1)}(2g(F) + n - 2) - \frac{q^{(r-1)(n-1)} - 1}{q^{r-1} - 1} - 1.$$

P r o o f. (i) Let P and ∞ be two different rational places of $F/\mathbb{F}_q$. For given $r \geq 2$ consider the constant field extension $F_r = \mathbb{F}_{q^r} \cdot F$, and let A and A_r be the ∞-integral rings of F and F_r, respectively. For fixed $n \geq 1$ let

$$E = H_{A_r}(\Lambda(P^n))$$

be the narrow ray class field modulo P^n determined by a sgn-normalized Drinfeld A_r-module ϕ of rank 1. Let $K = K_{n,r}$ be the subfield of the extension E/F_r fixed by the subgroup $I_\infty \cdot \mathrm{Pic}_{P^n}(A)$ of $\mathrm{Pic}_{P^n}(A_r) = \mathrm{Gal}(E/F_r)$. Since $|I_\infty \cap \mathrm{Pic}_{P^n}(A)| = q-1$, we have

$$[K : F_r] = \frac{[E : F_r]}{|I_\infty \cdot \mathrm{Pic}_{P^n}(A)|} = \frac{h(F_r)}{h(F)} q^{(r-1)(n-1)}. \tag{2}$$

By the construction of K, the place ∞ of F_r splits completely in the extension K/F_r. A rational place of $F_r/\mathbb{F}_{q^r}$ different from P and ∞ splits completely in K/F_r if and only if its Artin automorphism is contained in $\mathrm{Pic}_{P^n}(A)$, and this holds if and only if the restriction of this rational place to $F/\mathbb{F}_q$ is rational. In this way we get

$$[K : F_r](N(F) - 1) = \frac{h(F_r)}{h(F)} q^{(r-1)(n-1)}(N(F) - 1) \tag{3}$$

rational places of $K/\mathbb{F}_{q^r}$. In order to determine $N(K)$, it remains to study the decomposition of P in the extension K/F_r.

Let Q be a place of K lying over P and R a place of E lying over Q. Then the inertia group $G(R|Q)$ of R over Q is

$$G(R|Q) = \mathrm{Gal}(E/K) \cap G(R|P),$$

where $G(R|P)$ is the inertia group of R over P, which is equal to $(A_r/P^n)^*$ (recall that the extension H_{A_r}/F_r is unramified). By Lemma 1 we conclude that $G(R|Q) = I_\infty \cdot (A/P^n)^*$, and so for the ramification indices we get

$$e(Q|P) = \frac{e(R|P)}{e(R|Q)} = \frac{(q^r - 1)q^{r(n-1)}}{|I_\infty \cdot (A/P^n)^*|} = q^{(r-1)(n-1)}, \tag{4}$$

where we also used the fact that $|I_\infty \cap (A/P^n)^*| = q - 1$.

Let T be the inertia field of Q in the extension K/F_r. We have already noted that ∞ splits completely in K/F_r, and so by Proposition 1(i) the only ramified place in K/F_r can be P. Consequently, T/F_r is an unramified abelian extension in which ∞ splits completely, and so it follows from the definition of the Hilbert class field that $T \subseteq H_{A_r}$. We also observe that

$$[T : F_r] = \frac{[K : F_r]}{e(Q|P)} = \frac{h(F_r)}{h(F)} \tag{5}$$

in view of (2) and (4). Let $J = H_{A_r} \cap K$, then $F_r \subseteq T \subseteq J$. On the one hand, the extension J/T is unramified, and on the other hand, any place of T lying over P is totally ramified in J/T. Thus, we must have $J = H_{A_r} \cap K = T$. It follows that $\mathrm{Gal}(E/T)$ is the subgroup of $\mathrm{Pic}_{P^n}(A_r)$ generated by $(A_r/P^n)^*$ and $I_\infty \cdot \mathrm{Pic}_{P^n}(A)$. By applying Lemma 1, we get

$$\begin{aligned} \mathrm{Gal}(H_{A_r}/T) &= \mathrm{Gal}(E/T)/(A_r/P^n)^* \\ &\simeq (I_\infty \cdot \mathrm{Pic}_{P^n}(A))/(I_\infty \cdot (A/P^n)^*) \simeq \mathrm{Pic}_{P^n}(A)/(A/P^n)^*. \end{aligned}$$

Let $t \in A$ be a uniformizer at P. Then

$$(t)_0 = P + D,$$

where $P \notin \mathrm{supp}(D)$ and D is a positive $\mathbb{F}_q$-rational divisor prime to ∞. For the corresponding fractional ideals (denoted by the same symbols) we have $P = D^{-1}$ modulo principal ideals, and so for the corresponding Galois automorphisms in $\mathrm{Gal}(H_{A_r}/F_r) = \mathrm{Pic}(A_r)$ we get $\tau_P = \tau_{D^{-1}}$. Since D is $\mathbb{F}_q$-rational and prime to P and ∞, it follows from the formula for $\mathrm{Gal}(H_{A_r}/T)$ above that $\tau_P = \tau_{D^{-1}} \in \mathrm{Gal}(H_{A_r}/T)$, and so the theory of Hilbert class fields shows that P splits completely in T/F_r. By taking into account (5), we see that P splits into $h(F_r)/h(F)$ rational places of K. Together with (3) this yields the formula for $N(K) = N(K_{n,r})$ in the theorem.

(ii) Let L be the inertia field of R in E/K. Then $\mathrm{Gal}(E/L) = G(R|Q) = I_\infty \cdot (A/P^n)^*$ by part (i) of the proof, and $|\mathrm{Gal}(E/L)| = (q^r - 1)q^{n-1}$. Furthermore,

$$\mathrm{Gal}(E/L) \subseteq G(R|P) = \mathrm{Gal}(E/H_{A_r}),$$

hence $H_{A_r} \subseteq L$. Thus, the place S of L lying under R is totally ramified in E/L. Then by [21, Proposition III.5.12] the different exponent $d(R|S)$ of R over S is given by

$$d(R|S) = \sum_{\gamma \in \mathrm{Gal}(E/L)\setminus\{1\}} \nu_R(\lambda - \lambda^\gamma),$$

where λ is a generator of $\Lambda(P^n)$. In accordance with Proposition 1(iii), for $\gamma \in \mathrm{Gal}(E/L)$ we have $\gamma = \sigma_{gA_r}$ for some $g \in A_r$ with $\mathrm{sgn}(g) = 1$ and $g = \sum_{i=0}^{n-1} \alpha_i t^i$, where all $\alpha_i \in \mathbb{F}_{q^r}$ and $t \in A_r$ is a uniformizer at P. Using the special form of $\mathrm{Gal}(E/L)$, the n-tuple $(\alpha_0, \ldots, \alpha_{n-1})$ of coefficients can be written in the form $\beta(1, b_1, \ldots, b_{n-1})$ with $\beta \in \mathbb{F}_{q^r}^*$ and $b_1, \ldots, b_{n-1} \in \mathbb{F}_q$. By Proposition 1(ii) and [5, Lemma 4.4] we have

$$\nu_R(\lambda - \lambda^\gamma) = \nu_R(\lambda - \phi_g(\lambda)) = \nu_R\Big((1-\beta)\lambda - \sum_{i=1}^{n-1} \beta b_i \phi_{t^i}(\lambda)\Big).$$

As in [29, Lemma 5] we see that

$$\nu_R(\phi_{t^i}(\lambda)) = q^{ri} \quad \text{for } 0 \le i \le n-1.$$

Thus, if $\beta \neq 1$, then $\nu_R(\lambda - \lambda^\gamma) = 1$, and if $\beta = 1$ and $g \neq 1$, then

$$\nu_R(\lambda - \lambda^\gamma) = q^{rj},$$

where j is the least positive integer with $b_j \neq 0$. This yields

$$d(R|S) = (q^r - 2)q^{n-1} + \sum_{j=1}^{n-1}(q-1)q^{n-1-j}q^{rj} \tag{6}$$

$$= (q^r - 2)q^{n-1} + (q-1)q^{n-1}\frac{q^{(r-1)n} - q^{r-1}}{q^{r-1} - 1}.$$

Since $\mathrm{Gal}(E/L)$ contains I_∞, the place ∞ splits completely in L/F_r. By the definition of L, the place Q is unramified in L/K, and this holds for any place of K lying over P. Thus, L/K is an unramified extension. Furthermore, we have

$$[L:K] = \frac{[E:F_r]}{[E:L][K:F_r]} = h(F).$$

Hence the Hurwitz genus formula yields

$$2g(L) - 2 = h(F)(2g(K) - 2). \tag{7}$$

For the extension E/L the Hurwitz genus formula shows that

$$2g(E) - 2 = (q^r - 1)q^{n-1}(2g(L) - 2) + \deg(\mathrm{Diff}(E/L)). \tag{8}$$

Only places of E lying over P or ∞ can contribute to $\deg(\mathrm{Diff}(E/L))$. In part (i) of the proof we have shown that there are exactly $h(F_r)/h(F)$ rational places of K lying over P. If we also use the facts that the extension L/K of degree $h(F)$ is unramified and that the places of L lying over P are totally ramified in E/L, then we can conclude that the sum of the degrees of the places of E lying over P is equal to $h(F_r)$. Recall that I_∞ is both the decomposition group and the inertia group of ∞ in E/F_r. Therefore we get

$$\deg(\mathrm{Diff}(E/L)) = d(R|S)h(F_r) + (q^r - 2)h(F_r)q^{r(n-1)}.$$

If we now combine this formula with Proposition 2(ii) (of course with q replaced by q^r), (6), (7), and (8), and if we note that $g(F_r) = g(F)$, then we arrive at the desired formula for $g(K) = g(K_{n,r})$. ∎

Corollary 1. *Let $F/\mathbb{F}_q$ be a global function field of genus $g(F)$ with $N(F) \geq 2$. Then for every integer $r \geq 2$ there exists a global function field $K_r/\mathbb{F}_{q^r}$ with*

$$g(K_r) = \frac{h(F_r)}{h(F)}(g(F) - 1) + 1 \quad \text{and} \quad N(K_r) = \frac{h(F_r)N(F)}{h(F)}.$$

Proof. Apply Theorem 1 with $n = 1$. ∎

In the theory of algebraic curves over $\mathbb{F}_q$ of genus 2 (see Serre [15], [16], [18]), the prime power $q = p^e$, p prime, $e \geq 1$, is called *nonspecial* if either (i) e is even and $q \neq 4, 9$; or (ii) e is odd, p does not divide $\lfloor 2q^{1/2} \rfloor$, and q is not of the form $k^2 + 1, k^2 + k + 1$, or $k^2 + k + 2$ for some integer k.

COROLLARY 2. *If the prime power q is nonspecial, then there exists a global function field $K/\mathbb{F}_{q^2}$ with*

$$g(K) = (q-m+1)^2 + 1 \quad \textit{and} \quad N(K) = (q+2m+1)(q-m+1)^2,$$

where $m = \lfloor 2q^{1/2} \rfloor$.

P r o o f. Since q is nonspecial, there is a function field $F/\mathbb{F}_q$ with $g(F) = 2$ and $N(F) = q + 2m + 1$ (see Serre [15], [16]). By Serre [18] we can have $g(F) = 2$ and $N(F) = q+2m+1$ only if the eigenvalues of the Frobenius are α and $\overline{\alpha}$ (each with multiplicity 2) with $\alpha+\overline{\alpha} = -m$ and $\alpha\overline{\alpha} = q$. Therefore

$$L_F(t) = (1-\alpha t)^2(1-\overline{\alpha}t)^2 = (qt^2 + mt + 1)^2.$$

By Corollary 1 and (1) we get a function field $K/\mathbb{F}_{q^2}$ with the desired values of $g(K)$ and $N(K)$. ∎

COROLLARY 3. *Let q be a nonsquare and let the characteristic p of $\mathbb{F}_q$ satisfy $p \equiv 1 \bmod 4$. Then there exists a global function field $K/\mathbb{F}_{q^2}$ with*

$$g(K) = q^2 + 2q + 2 \quad \textit{and} \quad N(K) = (q+1)^3.$$

P r o o f. It is well known that under our conditions on q there exists an elliptic curve E over $\mathbb{F}_q$ with $N(E) = q + 1$ (see e.g. Schoof [13] and Waterhouse [25]). Then E is a supersingular elliptic curve with a cyclic group of $\mathbb{F}_q$-rational points (see [13, Lemma 4.8]). Furthermore, the order of the Frobenius acting on the group of 2-division points of E is at most 2. Thus according to Serre [18], E can be glued to itself if the j-invariant of E is not equal to 1728. By [20, p. 144, Example 4.5] an elliptic curve with the j-invariant 1728 is not supersingular if $p \equiv 1 \bmod 4$. Hence under our assumptions, E can be glued to itself. If C is the algebraic curve over $\mathbb{F}_q$ with Jacobian isogenous to $E \times E$, then for its function field $F/\mathbb{F}_q$ we have $g(F) = 2$, $N(F) = q+1$, and $h(F) = (q+1)^2$. This yields $L_F(t) = (qt^2+1)^2$, and so the desired result follows from Corollary 1 and (1). ∎

EXAMPLE 1. Let F be the rational function field $\mathbb{F}_2(x)$. Then with $n = 4$ and $r = 2$ in Theorem 1 we get a function field $K/\mathbb{F}_4$ with $g(K) = 5$ and $N(K) = 17$.

EXAMPLE 2. Let $F = \mathbb{F}_2(x, y)$ be the function field defined by

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

Then $g(F) = 1$, $N(F) = 4$, and $L_F(t) = 2t^2 + t + 1$. Thus, by using (1) and Theorem 1 with $n = 3$ and $r = 2$, we get a function field $K/\mathbb{F}_4$ with $g(K) = 9$ and $N(K) = 26$. The function field K is optimal.

EXAMPLE 3. Let $F = \mathbb{F}_2(x, y)$ be the function field defined by

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

Then $g(F) = 1$, $N(F) = 5$, and $L_F(t) = 2t^2 + 2t + 1$. Thus, by using (1) and Theorem 1 with $n = 3, 4, 5$ and $r = 2$, we get three function fields $K_n/\mathbb{F}_4, n = 3, 4, 5$, with

$$\begin{aligned} g(K_3) &= 5, \quad & N(K_3) &= 17; \\ g(K_4) &= 13, \quad & N(K_4) &= 33; \\ g(K_5) &= 33, \quad & N(K_5) &= 65. \end{aligned}$$

The function field K_4 is optimal.

EXAMPLE 4. Let $F = \mathbb{F}_2(x, y)$ be the function field defined by

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

Then $g(F) = 2$ and $N(F) = 4$. Since F has exactly three places of degree 2, we obtain

$$L_F(t) = 4t^4 + 2t^3 + 3t^2 + t + 1.$$

Thus, by using (1) and Theorem 1 with $n = 1$ and $r = 2$, we get a function field $K/\mathbb{F}_4$ with $g(K) = 6$ and $N(K) = 20$. The function field K is optimal.

EXAMPLE 5. Let F be the rational function field $\mathbb{F}_q(x)$, where q is an arbitrary prime power. Then with $n = 3$ and $r = 2$ in Theorem 1 we get a function field $K/\mathbb{F}_{q^2}$ with $g(K) = q(q-1)/2$ and $N(K) = q^3 + 1$. The field K is the well-known Hermitian function field (see [2, Section V]), it is optimal and meets the Weil bound.

4. The second and third constructions. In the first construction the only ramification occurred at rational places of the base field F. In this section we present constructions in which places of F of higher degree can be ramified.

THEOREM 2. *Let $F/\mathbb{F}_q$ be a global function field of genus $g(F)$ with $N(F) \geq 1$ and let $r \geq 2$ be an integer. Suppose that F has at least one place of degree $d > 1$ with $\gcd(d, r) = 1$. Then for every integer $n \geq 1$ there exists a global function field $K_n/\mathbb{F}_{q^r}$ such that*:

(i) *The number of rational places of $K_n/\mathbb{F}_{q^r}$ is given by*

$$N(K_n) = \frac{(q-1)(q^{dr}-1)h(F_r)}{(q^d-1)(q^r-1)h(F)} q^{d(r-1)(n-1)} N(F).$$

(ii) *The genus of $K_n/\mathbb{F}_{q^r}$ satisfies*

$$\begin{aligned} \frac{h(F)}{h(F_r)}(2g(K_n) - 2) = {} & \frac{(q-1)(q^{dr}-1)}{(q^d-1)(q^r-1)} q^{d(r-1)(n-1)}(2g(F) + dn - 2) \\ & - \frac{d(q-1)(q^{dr}-1)(q^{d(r-1)(n-1)}-1)}{(q^d-1)(q^r-1)(q^{d(r-1)}-1)} - d. \end{aligned}$$

P r o o f. (i) Let ∞ be a rational place of $F/\mathbb{F}_q$, and for given $r \geq 2$ let A and A_r be the ∞-integral rings of F and $F_r = \mathbb{F}_{q^r} \cdot F$, respectively. Let Q be a place of $F/\mathbb{F}_q$ of degree d. Then Q is still a place of degree d of $F_r/\mathbb{F}_{q^r}$ since $\gcd(d, r) = 1$. For given $n \geq 1$ let

$$E = H_{A_r}(\Lambda(Q^n))$$

be the narrow ray class field modulo Q^n determined by a sgn-normalized Drinfeld A_r-module ϕ of rank 1. Let K_n be the subfield of the extension E/F_r fixed by the subgroup $H = I_\infty \cdot \mathrm{Pic}_{Q^n}(A)$ of $\mathrm{Pic}_{Q^n}(A_r) = \mathrm{Gal}(E/F_r)$. Since $|I_\infty \cap \mathrm{Pic}_{Q^n}(A)| = q - 1$, we have

$$|H| = \frac{q^r - 1}{q - 1}(q^d - 1)q^{d(n-1)}h(F),$$

and so

$$[K_n : F_r] = \frac{|\mathrm{Pic}_{Q^n}(A_r)|}{|H|} = \frac{(q-1)(q^{dr}-1)h(F_r)}{(q^d-1)(q^r-1)h(F)}q^{d(r-1)(n-1)}. \tag{9}$$

By arguments in the proof of Theorem 1 it is clear that

$$N(K_n) = [K_n : F_r]N(F),$$

and this yields the desired formula for $N(K_n)$.

(ii) Let R be a place of E lying over Q and let L be the inertia field of R in E/K_n. As in the proof of Theorem 1(ii) we see that $\mathrm{Gal}(E/L) = I_\infty \cdot (A/Q^n)^*$ and that the place S of L lying under R is totally ramified in E/L. Furthermore, the different exponent $d(R|S)$ of R over S is given by

$$d(R|S) = \sum_{\gamma \in \mathrm{Gal}(E/L)\setminus\{1\}} \nu_R(\lambda - \lambda^\gamma),$$

where λ is a generator of $\Lambda(Q^n)$. We continue to proceed as in the proof of Theorem 1(ii), but now $g = \sum_{i=0}^{n-1} \alpha_i t^i$, where $t \in A_r$ is a uniformizer at Q and the α_i belong to a fixed complete residue system of A_r modulo Q which includes the elements of $\mathbb{F}_{q^r}$ for convenience. Therefore

$$\nu_R(\lambda - \lambda^\gamma) = \nu_R\Big(\phi_{1-\alpha_0}(\lambda) - \sum_{i=1}^{n-1} \phi_{\alpha_i}(\phi_{t^i}(\lambda))\Big).$$

Furthermore,

$$\nu_R(\phi_{t^i}(\lambda)) = q^{dri} \quad \text{for } 1 \leq i \leq n-1,$$

and $\nu_R(\phi_b(\lambda)) = 1$ for $b \in A_r$ with $\nu_Q(b) = 0$. Thus, if $\alpha_0 \neq 1$, then $\nu_R(\lambda - \lambda^\gamma) = 1$, and if $\alpha_0 = 1$ and $g \neq 1$, then

$$\nu_R(\lambda - \lambda^\gamma) = q^{drj},$$

where j is the least positive integer with $\alpha_j \neq 0$. Using the special form of $\mathrm{Gal}(E/L)$, we obtain

$$(10)\quad d(R|S)$$
$$= \left(\frac{(q^d-1)(q^r-1)}{q-1} - 1\right) q^{d(n-1)} + \sum_{j=1}^{n-1} (q^d-1) q^{d(n-1-j)} q^{drj}$$
$$= \left(\frac{(q^d-1)(q^r-1)}{q-1} - 1 + \frac{(q^d-1)(q^{dn(r-1)} - q^{d(r-1)})}{q^{d(r-1)}-1}\right) q^{d(n-1)}.$$

By the Hurwitz genus formula and $g(F_r) = g(F)$ we get

$$2g(K_n) - 2 = [K_n : F_r](2g(F) - 2) + \deg(\mathrm{Diff}(K_n/F_r)).$$

Since only the place Q can be ramified in the extension K_n/F_r, we have

$$\deg(\mathrm{Diff}(K_n/F_r)) = \frac{d[K_n : F_r] d(P|Q)}{e(P|Q)},$$

where $d(P|Q)$, respectively $e(P|Q)$, is the different exponent, respectively ramification index, of P over Q and P is the place of K_n lying under S. Now

$$e(P|Q) = \frac{|(A_r/Q^n)^*|}{[E:L]} = \frac{(q-1)(q^{dr}-1)}{(q^d-1)(q^r-1)} q^{d(r-1)(n-1)},$$

and so together with (9) this yields

$$\deg(\mathrm{Diff}(K_n/F_r)) = \frac{dh(F_r) d(P|Q)}{h(F)}.$$

Thus we obtain

$$(11)\quad \frac{h(F)}{h(F_r)}(2g(K_n) - 2)$$
$$= \frac{(q-1)(q^{dr}-1)}{(q^d-1)(q^r-1)} q^{d(r-1)(n-1)}(2g(F) - 2) + d(P|Q)d.$$

It remains to calculate $d(P|Q)$. By the tower formula for different exponents we have $d(R|P) = d(R|S)$ and

$$d(R|Q) = [E:L] d(P|Q) + d(R|P),$$

and also $d(R|Q) = d(R|U)$, where U is the place of H_{A_r} lying under R. This yields

$$d(P|Q) = \frac{(q-1)(d(R|U) - d(R|S))}{(q^d-1)(q^r-1) q^{d(n-1)}}.$$

Now $d(R|U)$ was calculated in the proof of [29, Proposition 2], and accordingly we get

$$d(R|U) = (nq^{dr} - n - 1) q^{dr(n-1)}.$$

If we combine this with (10), then we arrive at an expression for $d(P|Q)$, and by substituting this into (11) we obtain the desired identity. ∎

EXAMPLE 6. Let the function field $F/\mathbb{F}_2$ be as in Example 3. Then F has a place of degree 5. Thus, by using (1) and Theorem 2 with $r = 2, d = 5$, and $n = 1$, we get a function field $K/\mathbb{F}_4$ with $g(K) = 26$ and $N(K) = 55$. The function field K is optimal.

EXAMPLE 7. Let F be the rational function field $\mathbb{F}_q(x)$, where q is an arbitrary prime power. Then with $r = 2, d = 3$, and $n = 1$ in Theorem 2 we get a function field $K/\mathbb{F}_{q^2}$ with $g(K) = q(q-1)/2$ and $N(K) = q^3 + 1$. This is again the Hermitian function field (compare with Example 5).

THEOREM 3. *Let $q = p^r$ with a prime p and $r \geq 1$, and for a given integer $m \geq 1$ let $F/\mathbb{F}_q$ be a global function field of genus $g(F)$ with $N(F) \geq m+1$. Suppose that F has at least one place of degree $d > 1$ with $rd > m$. Assume also that $N_q(1 + p(g(F) - 1)) < (m+1)p$ in case $g(F) \geq 1$. Then for every integer l with $1 \leq l \leq rd - m$ there exists a global function field $K_l/\mathbb{F}_q$ such that*:

(i) *The number of rational places of $K_l/\mathbb{F}_q$ satisfies $N(K_l) \geq (m+1)p^l$ and $p^l \mid N(K_l)$. Furthermore, $N(K_l) = (m+1)p^l$ if $N(F) = m+1$.*

(ii) *The genus of $K_l/\mathbb{F}_q$ is given by*

$$g(K_l) = p^l(g(F) + d - 1) + 1 - d.$$

Proof. (i) Let $\infty, P_1, \ldots, P_m$ be $m+1$ distinct rational places of F and let A be the ∞-integral ring of F. Let Q be a place of F of degree d. Consider the $\mathbb{F}_p$-vector space

$$V := \mathrm{Pic}_{Q^2}(A)/\,\mathrm{Pic}_{Q^2}(A)^p.$$

Then $\dim_{\mathbb{F}_p}(V)$ is equal to the p-rank of $\mathrm{Pic}_{Q^2}(A)$, which is at least the p-rank of $(A/Q^2)^*$. Let $t \in A$ be a uniformizer at Q and let $\alpha_1, \ldots, \alpha_{rd}$ be a basis of the residue field of Q over $\mathbb{F}_p$. We identify the residue field of Q with $\mathbb{F}_{q^d}$. Then

$$(A/Q^2)^* \simeq (\mathbb{F}_{q^d}[t]/(t^2))^*.$$

The group $(\mathbb{F}_{q^d}[t]/(t^2))^*$ has a direct decomposition

$$\mathbb{F}_{q^d}^* \otimes \Big(\bigotimes_{i=1}^{rd} \langle 1 + \alpha_i t \rangle \Big),$$

hence the p-rank of $(A/Q^2)^*$ is rd since each cyclic subgroup $\langle 1 + \alpha_i t \rangle$ has order p. If we view $P_1, \ldots, P_m$ as elements of the vector space V in an obvious sense, then they generate a subspace of V of dimension at most m. For a given l with $1 \leq l \leq rd - m$, let W_l be a subspace of V of dimension $\dim_{\mathbb{F}_p}(V) - l$ containing all P_i. Let G_l be the subgroup of $\mathrm{Pic}_{Q^2}(A)$ that

contains $\mathrm{Pic}_{Q^2}(A)^p$ and satisfies $G_l/\mathrm{Pic}_{Q^2}(A)^p = W_l$. Then G_l contains all P_i and $[\mathrm{Pic}_{Q^2}(A) : G_l] = p^l$. Let

$$E = H_A(\Lambda(Q^2))$$

be the narrow ray class field modulo Q^2 determined by a sgn-normalized Drinfeld A-module ϕ of rank 1. Let K_l be the subfield of the extension E/F fixed by G_l. Then K_l/F is an extension of degree p^l and $\infty, P_1, \ldots, P_m$ split completely in K_l/F, hence $N(K_l) \geq (m+1)p^l$. The remaining assertions in part (i) of the theorem follow from the fact that Q is the only possible ramified place in K_l/F.

(ii) We first show that Q is totally ramified in K_l/F. Otherwise, one could find a subfield J of K_l/F such that J/F is an unramified extension of degree p. This is impossible if $g(F) = 0$. If $g(F) \geq 1$, then the genus of J is $1 + p(g(F) - 1)$ and the number of rational places of J is at least $(m+1)p$. This yields the contradiction $(m+1)p \leq N(J) \leq N_q(g(J)) < (m+1)p$.

Now let R be the place of K_l lying over Q and S a place of E lying over R. Then the inertia group $G(S|R)$ of S over R has the order

$$\frac{|(A/Q^2)^*|}{[K_l : F]} = (q^d - 1)p^{rd-l}$$

and it is a subgroup of $G(S|Q) = \mathrm{Gal}(E/H_A) = (A/Q^2)^*$. Hence $G(S|R)$ has a direct decomposition $\mathbb{F}_{q^d}^* \otimes H$, where H is a subgroup of $\bigotimes_{i=1}^{rd} \langle 1 + \alpha_i t \rangle$ of order p^{rd-l}. Let T be the place lying under S in the inertia field of S in E/K_l. Then the different exponent $d(S|T)$ of S over T is given by

$$\begin{aligned} d(S|T) &= \sum_{\gamma \in G(S|R)\setminus\{1\}} \nu_S(\lambda - \lambda^\gamma) \\ &= \sum_{\gamma \in G(S|R)\setminus H} \nu_S(\lambda - \lambda^\gamma) + \sum_{\gamma \in H\setminus\{1\}} \nu_S(\lambda - \lambda^\gamma), \end{aligned}$$

where λ is a generator of $\Lambda(Q^2)$. As in the proof of Theorem 2, we have $\nu_S(\phi_t(\lambda)) = q^d$ and $\nu_S(\phi_b(\lambda)) = 1$ for $b \in A$ with $\nu_Q(b) = 0$. Hence $\nu_S(\lambda - \lambda^\gamma) = 1$ if $\gamma \in G(S|R)\setminus H$ and $\nu_S(\lambda - \lambda^\gamma) = q^d$ if $\gamma \in H\setminus\{1\}$. Thus we obtain

$$d(S|T) = (q^d - 2)p^{rd-l} + q^d(p^{rd-l} - 1).$$

Places of E lying over ∞ are tamely ramified. Thus, the Hurwitz genus formula yields

$$\begin{aligned} 2g(E) - 2 = {} & h(F)(q^d - 1)p^{rd-l}(2g(K_l) - 2) + dh(F)d(S|T) \\ & + h(F)q^d \frac{(q^d - 1)(q - 2)}{q - 1}. \end{aligned}$$

If we now use the formula for $d(S|T)$ above and Proposition 2(ii), then we arrive at the formula for $g(K_l)$. ∎

R e m a r k 1. If $l = 1$ and we drop the condition on $N_q(1 + p(g(F) - 1))$ in Theorem 3, then in Theorem 3(ii) we either have the stated formula for $g(K_1)$ or $g(K_1) = p(g(F)-1)+1$. This holds since then $[K_1 : F] = p$, so that either Q is totally ramified in K_1/F or the extension K_1/F is unramified.

R e m a r k 2. Theorem 3 improves values in the table of bounds for $N_2(g)$ in [29] or equalizes values in [24] for $q = 2$. In the following Table 1 we list the values of $g(K)$ and $N(K)$ obtained from Theorem 3, the value of the genus $g(F)$ of the base field F in Theorem 3, and the values of l, m, and d in Theorem 3. In all cases we take, of course, $p = 2$ and $r = 1$ in Theorem 3.

Table 1

$g(K)$	24	27	38	41	48	60	63	70	74	78	85	87	89	91
$N(K)$	20	22	28	30	34	40	42	44	48	48	52	56	56	54
$g(F)$	6	8	12	13	15	6	21	23	25	9	10	3	11	31
l	1	1	1	1	1	2	1	1	1	2	2	3	2	1
m	9	10	13	14	16	9	20	21	23	11	12	6	13	26
d	13	12	15	16	19	13	22	25	25	15	16	10	16	30

Example 8. Let $F = \mathbb{F}_4(x, y)$ be the function field defined by

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

Then $g(F) = 1$ and $N(F) = N_4(1) = 9$. Furthermore, $F/\mathbb{F}_4$ has a place of degree 5, for instance by [29, Lemma 8]. Thus, we can apply Theorem 3 with $m = 8$, $d = 5$, and $l = 2$, and this yields a function field $K/\mathbb{F}_4$ with $g(K) = 16$ and $N(K) = 36$.

Example 9. Since $N_8(1) = 14$, there exists a function field $F/\mathbb{F}_8$ with $g(F) = 1$ and $N(F) = 14$. By [29, Lemma 8], $F/\mathbb{F}_8$ has a place of degree 5. Thus, we can apply Theorem 3 with $m = 13$, $d = 5$, and $l = 2$, and this yields a function field $K/\mathbb{F}_8$ with $g(K) = 16$ and $N(K) = 56$.

5. Curves over $\mathbb{F}_4$ with many rational points. In this section, by applying the three theorems in Sections 3 and 4, we give a table of intervals $[a, b]$ in which $N_4(g)$ lies for $1 \le g \le 51$ and some selected larger values. This table extends and improves the corresponding table in [24]. But first we present some examples which cannot be derived from our previous theorems. In these examples, it will be convenient to identify an irreducible polynomial over $\mathbb{F}_q$ with the place of $\mathbb{F}_q(x)$ of which it is a zero.

Example 10. Let F be the rational function field $\mathbb{F}_4(x)$. Let the place ∞ of F be the pole of x and let $A = \mathbb{F}_4[x]$ be the ∞-integral ring of F.

Put $E = H_A(\Lambda(Q))$, where Q is the place $x^3 + x + 1$ of F. Let K be the subfield of the extension E/F fixed by the subgroup $(\mathbb{F}_2[x]/(x^3 + x + 1))^*$ of $\mathrm{Gal}(E/F) = (A/Q)^*$. Then $[K : F] = 9$, and the places x and $x + 1$ split completely in K/F. The place ∞ splits into three rational places in K/F, each with ramification index 3. Thus we get $N(K) = 21$. The place Q is totally and tamely ramified in K/F. Hence 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 11. Let the function field $F/\mathbb{F}_2$ be as in Example 2. Let R be one of the two places of F of degree 4 lying over the place $x^4+x^3+x^2+x+1$ of $\mathbb{F}_2(x)$. Then there are two places Q_2 and Q_2' of $F_2/\mathbb{F}_4$ of degree 2 lying over R, where $F_2 = \mathbb{F}_4 \cdot F$. Distinguish a rational place ∞ of F and let A and A_2 be the ∞-integral rings of F and F_2, respectively. Put $E = H_{A_2}(\Lambda(Q_2Q_2'))$. We have

$$|\mathrm{Pic}_R(A)| = 15 \cdot h(F) \quad \text{and} \quad |\mathrm{Gal}(E/F_2)| = 15^2 \cdot h(F_2) = 450 \cdot h(F),$$

where we used (1) and $L_F(-1) = 2$ in the last identity. Let G be the subgroup of $\mathrm{Gal}(E/F_2)$ of order $45 \cdot h(F)$ which contains $\mathrm{Pic}_R(A)$, and let K be the subfield of the extension E/F_2 fixed by G. Note that $[K : F_2] = 10$. Clearly, all rational places of $F/\mathbb{F}_2$ split completely in the extension K/F_2, and so for the function field $K/\mathbb{F}_4$ we have $N(K) \geq 40$. The only ramified places in the extension K/F_2 are Q_2 and Q_2', each with ramification index 5. Hence the Hurwitz genus formula yields $g(K) = 17$. Since $N_4(17) \leq 40$, the function field K is optimal and $N(K) = 40$.

EXAMPLE 12. Let $F = \mathbb{F}_2(x, y)$ be the function field defined by

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

Then $g(F) = 2$, $N(F) = 6$, and

$$L_F(t) = 4t^4 + 6t^3 + 5t^2 + 3t + 1.$$

The place $x^2 + x + 1$ of $\mathbb{F}_2(x)$ is inert in $F/\mathbb{F}_2(x)$, hence it yields a place R of F of degree 4. Furthermore, there are two places Q_2 and Q_2' of $F_2/\mathbb{F}_4$ of degree 2 lying over R, where $F_2 = \mathbb{F}_4 \cdot F$. Distinguish a rational place ∞ of F and let A and A_2 be the ∞-integral rings of F and F_2, respectively. Put $E = H_{A_2}(\Lambda(Q_2Q_2'))$. We have

$$|\mathrm{Pic}_R(A)| = 15 \cdot h(F) \quad \text{and} \quad |\mathrm{Gal}(E/F_2)| = 15^2 \cdot h(F_2) = 15^2 \cdot h(F),$$

where we used (1) in the last identity. Let G be the subgroup of $\mathrm{Gal}(E/F_2)$ of order $45 \cdot h(F)$ which contains $\mathrm{Pic}_R(A)$, and let K be the subfield of the extension E/F_2 fixed by G. Note that $[K : F_2] = 5$. All rational places of $F/\mathbb{F}_2$ split completely in the extension K/F_2, and so for the function field $K/\mathbb{F}_4$ we have $N(K) \geq 30$. Since $F/\mathbb{F}_2$ has no places of degree 2, all rational places of $F_2/\mathbb{F}_4$ are lying over rational places of $F/\mathbb{F}_2$, and so $N(K) = 30$.

The only ramified places in the extension K/F_2 are Q_2 and Q_2', and they are totally and tamely ramified. Hence the Hurwitz genus formula yields $g(K) = 14$.

EXAMPLE 13. Let $F = \mathbb{F}_2(x, y)$ be the function field defined by

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

Then $g(F) = 2$, $N(F) = 5$, and

$$L_F(t) = 4t^4 + 4t^3 + 4t^2 + 2t + 1.$$

Let R be one of the two places of F of degree 4 lying over the place x^4+x+1 of $\mathbb{F}_2(x)$. Then there are two places Q_2 and Q_2' of $F_2/\mathbb{F}_4$ of degree 2 lying over R, where $F_2 = \mathbb{F}_4 \cdot F$. Distinguish a rational place ∞ of F and let A and A_2 be the ∞-integral rings of F and F_2, respectively. Put $E = H_{A_2}(\Lambda(Q_2Q_2'))$ and note that E is the composite field of $H_{A_2}(\Lambda(Q_2))$ and $H_{A_2}(\Lambda(Q_2'))$. We have $|\mathrm{Pic}_R(A)| = 15 \cdot h(F)$ and $|\mathrm{Gal}(E/F_2)| = 15^2 \cdot h(F_2) = 675 \cdot h(F)$, where we used (1) and $L_F(-1) = 3$ in the last identity. Furthermore, the place ∞ has ramification index 3 in the extension E/F_2, and so its inertia group in E/F_2 has order 3 and can be identified with $\mathbb{F}_4^*$. Now let K be the subfield of the extension E/F_2 fixed by $\mathbb{F}_4^* \cdot \mathrm{Pic}_R(A)$, then $[K : F_2] = 15$. All rational places of $F/\mathbb{F}_2$ split completely in the extension K/F_2, and so for the function field $K/\mathbb{F}_4$ we have $N(K) \geq 75$. The only ramified places in the extension K/F_2 are Q_2 and Q_2', and as in the proof of Theorem 1(i) it is seen that each has ramification index 5. Hence the Hurwitz genus formula yields $g(K) = 40$. From $N_4(40) \leq 77$ it follows that $N(K) = 75$.

We need to explain the symbols appearing in Table 2 below. In all three theorems and in the examples of our paper, the field K is a subfield of a narrow ray class extension E/F with a base field F of lower genus.

- $g = g(K)$ — the genus of $K/\mathbb{F}_4$.

In the column labeled $N_4(g)$, the first number is the lower bound for $N(K)$, and thus for $N_4(g)$, and the second is the upper bound for $N_4(g)$ obtained by Weil's explicit formulas and the trigonometric polynomials of Oesterlé (see [15], [18]). A program for calculating upper bounds for $N_q(g)$ was kindly supplied to us by Jean-Pierre Serre. If only one number is given under $N_4(g)$, then this is the exact value.

- $g(F)$ — the genus of the base field F.
- M — the ideal yielding the narrow ray class field. In the column labeled M, the ideal P always corresponds to a rational place of F and the ideals Q_d and Q_d' correspond to places of F of degree d.
- G — the Galois group of K/F.

• n — the number of rational places of F that split completely in K/F.

• Ref — the theorem, example, or reference from which the resulting field K is obtained. Where necessary, a reference to the base field F is also given, and the various base fields are listed after the table.

Table 2

g	$N_4(g)$	$g(F)$	M	$\|G\|$	n	Ref
1	9					[25]
2	10					[17]
3	14					[17]
4	15					[17]
5	17-18	0	P^4	8	2	Ex. 1 (see also Ex. 3)
6	20	2	P	5	4	Ex. 4
7	21-22	0	Q_3	9	2	Ex. 10
8	21-24	2	P	7	3	Th. 1, F.2
9	26	1	P^3	8	3	Ex. 2
10	27-28	2	P^2	6	4	Th. 1, F.4
11	25-30					[10]
12	28-31	3	Q_7^2	2	14	Th. 3, $l=1, m=13, d=7, r=2$
13	33	1	P^4	8	4	Ex. 3
14	30-35	2	Q_2Q_2'	5	6	Ex. 12
15	33-37	0	Q_5	11	3	Th. 2
16	36-38	1	Q_5^2	4	9	Ex. 8
17	40	1	Q_2Q_2'	10	4	Ex. 11
18	34-42	5	Q_9^2	2	17	Th. 3, $l=1,\ m=16,\ d=9,\ r=2$
19	36-43	1	Q_6^2	4	9	Th. 3, $l=2,\ m=8,\ d=6,\ r=2$
20	36-45	2	Q_5^2	4	9	Th. 3, $l=2,\ m=8,\ d=5,\ r=2$
21	41-47	2	P^4	8	5	Th. 1, F.1
22	40-48	6	Q_{11}^2	2	20	Th. 3, $l=1,\ m=19,\ d=11,\ r=2$
23	40-50	2	Q_6^2	4	10	Th. 3, $l=2,\ m=9,\ d=6,\ r=2$
24	42-52	7	Q_{11}^2	2	21	Th. 3, $l=1,\ m=20,\ d=11,\ r=2$
25	51-53	2	P^3	12	4	Th. 1, F.4
26	55	1	Q_5	11	5	Ex. 6
27	49-56					[24]
28	44-58	9	Q_{11}^2	2	22	Th. 3, $l=1,\ m=21,\ d=11,\ r=2$
29	49-60	3	P^4	8	6	Th. 1, F.5
30	52-61	3	Q_7^2	4	13	Th. 3, $l=2,\ m=12,\ d=7,\ r=2$
31	60-63	2	Q_3	15	4	Th. 2, F.3
32	52-65	10	Q_{13}^2	2	26	Th. 3, $l=1,\ m=25,\ d=13,\ r=2$
33	65-66	1	P^5	16	4	Ex. 3
34	57-68					[24]
35	54-69	10	Q_{16}^2	2	27	Th. 3, $l=1,\ m=26,\ d=16,\ r=2$
36	64-71	1	Q_5^2	8	8	Th. 3, $l=3,\ m=7,\ d=5,\ r=2$

Table 2 (cont.)

g	$N_4(g)$	$g(F)$	M	$\lvert G\rvert$	n	Ref
37	66-72	2	Q_5	11	6	Th. 2, F.1
38	56-74	12	Q_{15}^2	2	28	Th. 3, $l=1,\ m=27,\ d=15,\ r=2$
39	56-75	13	Q_{14}^2	2	28	Th. 3, $l=1,\ m=27,\ d=14,\ r=2$
40	75-77	2	Q_2Q_2'	15	5	Ex. 13
41	65-78	2	P^3	20	3	Th. 1, F.3
42	66-80	13	Q_{17}^2	2	33	Th. 3, $l=1,\ m=32,\ d=17,\ r=2$
43	72-81	1	Q_6^2	8	9	Th. 3, $l=3,\ m=8,\ d=6,\ r=2$
44	68-83	5	Q_9^2	4	17	Th. 3, $l=2,\ m=16,\ d=9,\ r=2$
45	80-84	0	Q_4^2	16	5	Th. 3, $l=4,\ m=4,\ d=4,\ r=2$
46	66-86	13	Q_{21}^2	2	33	Th. 3, $l=1,\ m=32,\ d=21,\ r=2$
47	68-87	5	Q_{10}^2	4	17	Th. 3, $l=2,\ m=16,\ d=10,\ r=2$
48	77-89	3	Q_5	11	7	Th. 2, F.5
49	81-90	2	P^5	16	5	Th. 1, F.1
50	91-92					[19]
51	80-93	2	Q_6^2	8	10	Th. 3, $l=3,\ m=9,\ d=6,\ r=2$
53	80-96	17	Q_{20}^2	2	40	Th. 3, $l=1,\ m=39,\ d=20,\ r=2$
54	80-98	6	Q_{11}^2	4	20	Th. 3, $l=2,\ m=19,\ d=11,\ r=2$
61	99-108	2	P^4	24	4	Th. 1, F.4
73	112-125	3	Q_8^2	8	14	Th. 3, $l=3,\ m=13,\ d=8,\ r=2$
133	204-209					[19]

F.1: $y^2+y=\dfrac{x(x+1)}{x^3+x+1}$, F.2: $y^2+y=x(x^2+x+1)^2$,

F.3: $y^2+y=\dfrac{x}{x^3+x+1}$, F.4: $y^2+y=x^2(x+1)(x^2+x+1)$,

F.5: $L(\Lambda(Q))$ with $L=\mathbb{F}_2(x)$ and $Q=x^3+x+1$ (see [9, Example 3A]).

References

[1] 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.

[2] —, —, *Algebraic function fields over finite fields with many rational places*, IEEE Trans. Inform. Theory 41 (1995), 1548–1563.

[3] —, —, *On the asymptotic behaviour of some towers of function fields over finite fields*, J. Number Theory 61 (1996), 248–273.

[4] D. R. Hayes, *Stickelberger elements in function fields*, Compositio Math. 55 (1985), 209–239.

[5] —, *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.

[6] 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.

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

[8] H. Niederreiter and C. P. Xing, *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.
[9] —, —, *Explicit global function fields over the binary field with many rational places*, Acta Arith. 75 (1996), 383–396.
[10] —, —, *Cyclotomic function fields, Hilbert class fields, and global function fields with many rational places*, ibid. 79 (1997), 59–76.
[11] M. Perret, *Tours ramifiées infinies de corps de classes*, J. Number Theory 38 (1991), 300–322.
[12] M. Rosen, *The Hilbert class field in function fields*, Exposition. Math. 5 (1987), 365–378.
[13] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A 46 (1987), 183–211.
[14] —, *Algebraic curves over $\mathbb{F}_2$ with many rational points*, J. Number Theory 41 (1992), 6–14.
[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] —, *Nombres de points des courbes algébriques sur $\mathbb{F}_q$*, in: Sém. Théorie des Nombres 1982-1983, Exp. 22, Univ. de Bordeaux I, Talence, 1983.
[17] —, *Résumé des cours de* 1983-1984, Annuaire du Collège de France (1984), 79–83.
[18] —, *Rational Points on Curves over Finite Fields*, lecture notes, Harvard University, 1985.
[19] —, Personal communication, September 1995.
[20] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.
[21] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.
[22] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*, Kluwer, Dordrecht, 1991.
[23] 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.
[24] —, —, *How to construct curves over finite fields with many rational points*, in: Proc. Conf. Algebraic Geometry (Cortona, 1995), to appear.
[25] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. Ecole Norm. Sup. (4) 2 (1969), 521–560.
[26] 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.
[27] C. P. Xing and H. Niederreiter, *A construction of low-discrepancy sequences using global function fields*, Acta Arith. 73 (1995), 87–102.
[28] —, —, *Modules de Drinfeld et courbes algébriques ayant beaucoup de points rationnels*, C. R. Acad. Sci. Paris Sér. I Math. 322 (1996), 651–654.
[29] —, —, *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 7.2.1997 (3132)