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

by<br>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 $\mathbb{F}_{q^{-}}$

[^0]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 $\left.K / \mathbb{F}_{q}\right)$, then $N(K)=N\left(K / \mathbb{F}_{q}\right)$ 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 $N\left(F / \mathbb{F}_{q}\right) \geq 1$. We distinguish a rational place $\infty$ of $F$ and let $A$ be the $\infty$-integral ring of $F$, i.e., $A$ consists of the elements of $F$ that are regular outside $\infty$. 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 $\infty$ splits completely. The extension $H_{A} / F$ is finite and its Galois group is isomorphic to the fractional ideal class group $\operatorname{Pic}(A)$ of $A$, which in the case under consideration ( $\infty$ rational) is isomorphic to the group of divisor classes of $F$ of degree 0 . In particular, we have $\left[H_{A}: F\right]=h(F)$, the divisor class number of $F$. The value of $h(F)$ can be obtained from the $L$-polynomial

$$
L_{F}(t)=(1-t)(1-q t) Z_{F}(t)
$$

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

$$
\begin{equation*}
h\left(F_{2}\right) / h(F)=L_{F}(-1) . \tag{1}
\end{equation*}
$$

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 $\infty$ of $F$, and the $\infty$-integral ring $A$ of $F$ be as above. We fix a sgn-function and let $\phi$ be a sgn-normalized Drinfeld $A$-module of rank 1 defined over $H_{A}$. The additive group of the algebraic closure $\bar{H}_{A}$ of $H_{A}$ forms an $A$-module under the action of $\phi$. For any nonzero ideal $M$ in $A$ we consider the $M$-torsion module

$$
\Lambda(M)=\left\{u \in \bar{H}_{A}: \phi_{M}(u)=0\right\} .
$$

Then $\Lambda(M)$ is a cyclic $A$-module which is isomorphic to $A / M$ and has $\left|(A / M)^{*}\right|$ 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

$$
\operatorname{Pic}_{M}(A)=\mathcal{I}_{M}(A) / \mathcal{R}_{M}(A),
$$

where $\mathcal{R}_{M}(A)$ is the subgroup of $\mathcal{I}_{M}(A)$ consisting of all principal ideals $b A$ with $\operatorname{sgn}(b)=1$ 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 $\nu_{P}$ 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 $\phi$ 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 $\infty$ and the prime ideals in A dividing $M$.
(ii) The extension $E / F$ is abelian and there is an isomorphism $\sigma$ : $\operatorname{Pic}_{M}(A) \rightarrow \operatorname{Gal}(E / F)$, 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 $\lambda$ 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 $\sigma_{I}$.
(iii) The multiplicative group $(A / M)^{*}$ is isomorphic to $\operatorname{Gal}\left(E / H_{A}\right)$ by means of $b \mapsto \sigma_{b A}$, where $b \in A$ satisfies $\operatorname{sgn}(b)=1$ 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 $E=H_{A}\left(\Lambda\left(P^{n}\right)\right)$ be the narrow ray class field modulo $P^{n}$, where $P$ is a prime ideal in $A$ and $n \geq 1$. Then:
(i) If $\lambda$ is a generator of the cyclic $A$-module $\Lambda\left(P^{n}\right)$, then $E=H_{A}(\lambda)$ and the minimal polynomial of $\lambda$ 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 $\operatorname{deg}(P)=d$, then for the genus $g(E)$ of $E$ we have

$$
\begin{aligned}
& 2 g(E)-2 \\
& \quad=h(F) q^{d(n-1)}\left((2 g(F)-2)\left(q^{d}-1\right)+d n\left(q^{d}-1\right)-d+\frac{\left(q^{d}-1\right)(q-2)}{q-1}\right) .
\end{aligned}
$$

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

Next we observe that $\operatorname{Pic}_{P^{n}}(A)$ can also be viewed as a subgroup of $\operatorname{Pic}_{P^{n}}\left(A_{r}\right)$. 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.,

$$
D^{\psi}=D \quad \text { for all } \psi \in \operatorname{Gal}\left(\overline{\mathbb{F}}_{q} / \mathbb{F}_{q}\right) .
$$

Hence $\operatorname{Pic}_{P^{n}}(A)$ can be described as the group of all $\mathbb{F}_{q^{-}}$-rational divisors on $C / \overline{\mathbb{F}}_{q}$ prime to $P$ and $\infty$, from which we factor out the subgroup of all divisors $(c)_{0}$ with $c \in F, \operatorname{sgn}(c)=1$, and $c \equiv 1 \bmod P^{n}$, where $(c)_{0}$ is the divisor corresponding to the principal ideal $c A$. We have an analogous description for $\operatorname{Pic}_{P^{n}}\left(A_{r}\right)$, and this leads to a natural embedding of $\operatorname{Pic}_{P^{n}}(A)$ into $\operatorname{Pic}_{P^{n}}\left(A_{r}\right)$.

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

Lemma 1. We have

$$
\left(A_{r} / P^{n}\right)^{*} \cap\left(I_{\infty} \cdot \operatorname{Pic}_{P^{n}}(A)\right)=I_{\infty} \cdot\left(A / P^{n}\right)^{*},
$$

where all groups are considered as subgroups of $\operatorname{Pic}_{P^{n}}\left(A_{r}\right)$.

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

$$
(a)_{0}=(b)_{0}+D_{1}
$$

and so

$$
\left(a b^{-1}\right)_{0}-D_{1}=(c)_{0}
$$

for some $c \in F_{r}$ with $\operatorname{sgn}(c)=1$ and $c \equiv 1 \bmod P^{n}$. This means that $D_{1}=$ $\left(a b^{-1} c^{-1}\right)_{0}$. Since $D_{1}$ and $\infty$ are $\mathbb{F}_{q}$-rational, it follows that $a b^{-1} c^{-1} \in F$, hence $D_{1}$ represents an element of $\left(A / P^{n}\right)^{*}$. In view of $D=(b)_{0}+D_{1}$, we conclude that $D$ represents an element of $I_{\infty} \cdot\left(A / P^{n}\right)^{*}$.
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 $h\left(F_{r}\right)$ 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

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

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

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

Proof. (i) Let $P$ and $\infty$ 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 $\infty$-integral rings of $F$ and $F_{r}$, respectively. For fixed $n \geq 1$ let

$$
E=H_{A_{r}}\left(\Lambda\left(P^{n}\right)\right)
$$

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

$$
\begin{equation*}
\left[K: F_{r}\right]=\frac{\left[E: F_{r}\right]}{\left|I_{\infty} \cdot \operatorname{Pic}_{P^{n}}(A)\right|}=\frac{h\left(F_{r}\right)}{h(F)} q^{(r-1)(n-1)} \tag{2}
\end{equation*}
$$

By the construction of $K$, the place $\infty$ 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 $\infty$ splits completely in $K / F_{r}$ if and only if its Artin automorphism is contained in $\operatorname{Pic}_{P^{n}}(A)$, 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

$$
\begin{equation*}
\left[K: F_{r}\right](N(F)-1)=\frac{h\left(F_{r}\right)}{h(F)} q^{(r-1)(n-1)}(N(F)-1) \tag{3}
\end{equation*}
$$

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 $G(R \mid Q)$ of $R$ over $Q$ is

$$
G(R \mid Q)=\operatorname{Gal}(E / K) \cap G(R \mid P)
$$

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

$$
\begin{equation*}
e(Q \mid P)=\frac{e(R \mid P)}{e(R \mid Q)}=\frac{\left(q^{r}-1\right) q^{r(n-1)}}{\left|I_{\infty} \cdot\left(A / P^{n}\right)^{*}\right|}=q^{(r-1)(n-1)} \tag{4}
\end{equation*}
$$

where we also used the fact that $\left|I_{\infty} \cap\left(A / P^{n}\right)^{*}\right|=q-1$.
Let $T$ be the inertia field of $Q$ in the extension $K / F_{r}$. We have already noted that $\infty$ 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 $\infty$ splits completely, and so it follows from the definition of the Hilbert class field that $T \subseteq H_{A_{r}}$. We also observe that

$$
\begin{equation*}
\left[T: F_{r}\right]=\frac{\left[K: F_{r}\right]}{e(Q \mid P)}=\frac{h\left(F_{r}\right)}{h(F)} \tag{5}
\end{equation*}
$$

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 $\operatorname{Gal}(E / T)$ is the subgroup of $\operatorname{Pic}_{P^{n}}\left(A_{r}\right)$ generated by $\left(A_{r} / P^{n}\right)^{*}$ and $I_{\infty} \cdot \operatorname{Pic}_{P^{n}}(A)$. By applying Lemma 1 , we get

$$
\begin{aligned}
\operatorname{Gal}\left(H_{A_{r}} / T\right) & =\operatorname{Gal}(E / T) /\left(A_{r} / P^{n}\right)^{*} \\
& \simeq\left(I_{\infty} \cdot \operatorname{Pic}_{P^{n}}(A)\right) /\left(I_{\infty} \cdot\left(A / P^{n}\right)^{*}\right) \simeq \operatorname{Pic}_{P^{n}}(A) /\left(A / P^{n}\right)^{*}
\end{aligned}
$$

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

$$
(t)_{0}=P+D
$$

where $P \notin \operatorname{supp}(D)$ and $D$ is a positive $\mathbb{F}_{q}$-rational divisor prime to $\infty$. 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 $\operatorname{Gal}\left(H_{A_{r}} / F_{r}\right)=\operatorname{Pic}\left(A_{r}\right)$ we get $\tau_{P}=\tau_{D^{-1}}$. Since $D$ is $\mathbb{F}_{q^{-}}$ rational and prime to $P$ and $\infty$, it follows from the formula for $\operatorname{Gal}\left(H_{A_{r}} / T\right)$ above that $\tau_{P}=\tau_{D^{-1}} \in \operatorname{Gal}\left(H_{A_{r}} / T\right)$, 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 $h\left(F_{r}\right) / h(F)$ rational places of $K$. Together with (3) this yields the formula for $N(K)=N\left(K_{n, r}\right)$ in the theorem.
(ii) Let $L$ be the inertia field of $R$ in $E / K$. Then $\operatorname{Gal}(E / L)=G(R \mid Q)=$ $I_{\infty} \cdot\left(A / P^{n}\right)^{*}$ by part (i) of the proof, and $|\operatorname{Gal}(E / L)|=\left(q^{r}-1\right) q^{n-1}$. Furthermore,

$$
\operatorname{Gal}(E / L) \subseteq G(R \mid P)=\operatorname{Gal}\left(E / H_{A_{r}}\right)
$$

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 $d(R \mid S)$ of $R$ over $S$ is given by

$$
d(R \mid S)=\sum_{\gamma \in \operatorname{Gal}(E / L) \backslash\{1\}} \nu_{R}\left(\lambda-\lambda^{\gamma}\right)
$$

where $\lambda$ is a generator of $\Lambda\left(P^{n}\right)$. In accordance with Proposition 1(iii), for $\gamma \in \operatorname{Gal}(E / L)$ we have $\gamma=\sigma_{g A_{r}}$ for some $g \in A_{r}$ with $\operatorname{sgn}(g)=1$ 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 $\operatorname{Gal}(E / L)$, the $n$-tuple $\left(\alpha_{0}, \ldots, \alpha_{n-1}\right)$ of coefficients can be written in the form $\beta\left(1, b_{1}, \ldots, b_{n-1}\right)$ 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

$$
\nu_{R}\left(\lambda-\lambda^{\gamma}\right)=\nu_{R}\left(\lambda-\phi_{g}(\lambda)\right)=\nu_{R}\left((1-\beta) \lambda-\sum_{i=1}^{n-1} \beta b_{i} \phi_{t^{i}}(\lambda)\right)
$$

As in [29, Lemma 5] we see that

$$
\nu_{R}\left(\phi_{t^{i}}(\lambda)\right)=q^{r i} \quad \text { for } 0 \leq i \leq n-1
$$

Thus, if $\beta \neq 1$, then $\nu_{R}\left(\lambda-\lambda^{\gamma}\right)=1$, and if $\beta=1$ and $g \neq 1$, then

$$
\nu_{R}\left(\lambda-\lambda^{\gamma}\right)=q^{r j}
$$

where $j$ is the least positive integer with $b_{j} \neq 0$. This yields

$$
\begin{align*}
d(R \mid S) & =\left(q^{r}-2\right) q^{n-1}+\sum_{j=1}^{n-1}(q-1) q^{n-1-j} q^{r j}  \tag{6}\\
& =\left(q^{r}-2\right) q^{n-1}+(q-1) q^{n-1} \frac{q^{(r-1) n}-q^{r-1}}{q^{r-1}-1}
\end{align*}
$$

Since $\operatorname{Gal}(E / L)$ contains $I_{\infty}$, the place $\infty$ 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

$$
[L: K]=\frac{\left[E: F_{r}\right]}{[E: L]\left[K: F_{r}\right]}=h(F)
$$

Hence the Hurwitz genus formula yields

$$
\begin{equation*}
2 g(L)-2=h(F)(2 g(K)-2) \tag{7}
\end{equation*}
$$

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

$$
\begin{equation*}
2 g(E)-2=\left(q^{r}-1\right) q^{n-1}(2 g(L)-2)+\operatorname{deg}(\operatorname{Diff}(E / L)) \tag{8}
\end{equation*}
$$

Only places of $E$ lying over $P$ or $\infty$ can contribute to $\operatorname{deg}(\operatorname{Diff}(E / L))$. In part (i) of the proof we have shown that there are exactly $h\left(F_{r}\right) / h(F)$ 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 $h\left(F_{r}\right)$. Recall that $I_{\infty}$ is both the decomposition group and the inertia group of $\infty$ in $E / F_{r}$. Therefore we get

$$
\operatorname{deg}(\operatorname{Diff}(E / L))=d(R \mid S) h\left(F_{r}\right)+\left(q^{r}-2\right) h\left(F_{r}\right) q^{r(n-1)}
$$

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

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

$$
g\left(K_{r}\right)=\frac{h\left(F_{r}\right)}{h(F)}(g(F)-1)+1 \quad \text { and } \quad N\left(K_{r}\right)=\frac{h\left(F_{r}\right) N(F)}{h(F)}
$$

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 $\left\lfloor 2 q^{1 / 2}\right\rfloor$, 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

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

where $m=\left\lfloor 2 q^{1 / 2}\right\rfloor$.
Proof. Since $q$ is nonspecial, there is a function field $F / \mathbb{F}_{q}$ with $g(F)=2$ and $N(F)=q+2 m+1$ (see Serre [15], [16]). By Serre [18] we can have $g(F)=2$ and $N(F)=q+2 m+1$ only if the eigenvalues of the Frobenius are $\alpha$ and $\bar{\alpha}$ (each with multiplicity 2) with $\alpha+\bar{\alpha}=-m$ and $\alpha \bar{\alpha}=q$. Therefore

$$
L_{F}(t)=(1-\alpha t)^{2}(1-\bar{\alpha} t)^{2}=\left(q t^{2}+m t+1\right)^{2} .
$$

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

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

Proof. 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 $L_{F}(t)=\left(q t^{2}+1\right)^{2}$, 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 $L_{F}(t)=2 t^{2}+t+1$. 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 $L_{F}(t)=2 t^{2}+2 t+1$. 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

$$
\begin{array}{ll}
g\left(K_{3}\right)=5, & N\left(K_{3}\right)=17 \\
g\left(K_{4}\right)=13, & N\left(K_{4}\right)=33 \\
g\left(K_{5}\right)=33, & N\left(K_{5}\right)=65
\end{array}
$$

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

$$
L_{F}(t)=4 t^{4}+2 t^{3}+3 t^{2}+t+1
$$

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 $\operatorname{gcd}(d, r)=1$. 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

$$
N\left(K_{n}\right)=\frac{(q-1)\left(q^{d r}-1\right) h\left(F_{r}\right)}{\left(q^{d}-1\right)\left(q^{r}-1\right) h(F)} q^{d(r-1)(n-1)} N(F)
$$

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

$$
\begin{aligned}
\frac{h(F)}{h\left(F_{r}\right)}\left(2 g\left(K_{n}\right)-2\right)= & \frac{(q-1)\left(q^{d r}-1\right)}{\left(q^{d}-1\right)\left(q^{r}-1\right)} q^{d(r-1)(n-1)}(2 g(F)+d n-2) \\
& -\frac{d(q-1)\left(q^{d r}-1\right)\left(q^{d(r-1)(n-1)}-1\right)}{\left(q^{d}-1\right)\left(q^{r}-1\right)\left(q^{d(r-1)}-1\right)}-d
\end{aligned}
$$

Proof. (i) Let $\infty$ be a rational place of $F / \mathbb{F}_{q}$, and for given $r \geq 2$ let $A$ and $A_{r}$ be the $\infty$-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 $\operatorname{gcd}(d, r)=1$. For given $n \geq 1$ let

$$
E=H_{A_{r}}\left(\Lambda\left(Q^{n}\right)\right)
$$

be the narrow ray class field modulo $Q^{n}$ determined by a sgn-normalized Drinfeld $A_{r}$-module $\phi$ of rank 1 . Let $K_{n}$ be the subfield of the extension $E / F_{r}$ fixed by the subgroup $H=I_{\infty} \cdot \operatorname{Pic}_{Q^{n}}(A)$ of $\operatorname{Pic}_{Q^{n}}\left(A_{r}\right)=\operatorname{Gal}\left(E / F_{r}\right)$. Since $\left|I_{\infty} \cap \operatorname{Pic}_{Q^{n}}(A)\right|=q-1$, we have

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

and so

$$
\begin{equation*}
\left[K_{n}: F_{r}\right]=\frac{\left|\operatorname{Pic}_{Q^{n}}\left(A_{r}\right)\right|}{|H|}=\frac{(q-1)\left(q^{d r}-1\right) h\left(F_{r}\right)}{\left(q^{d}-1\right)\left(q^{r}-1\right) h(F)} q^{d(r-1)(n-1)} . \tag{9}
\end{equation*}
$$

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

$$
N\left(K_{n}\right)=\left[K_{n}: F_{r}\right] N(F),
$$

and this yields the desired formula for $N\left(K_{n}\right)$.
(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 $\operatorname{Gal}(E / L)=$ $I_{\infty} \cdot\left(A / Q^{n}\right)^{*}$ and that the place $S$ of $L$ lying under $R$ is totally ramified in $E / L$. Furthermore, the different exponent $d(R \mid S)$ of $R$ over $S$ is given by

$$
d(R \mid S)=\sum_{\gamma \in \operatorname{Gal}(E / L) \backslash\{1\}} \nu_{R}\left(\lambda-\lambda^{\gamma}\right),
$$

where $\lambda$ is a generator of $\Lambda\left(Q^{n}\right)$. 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 $\alpha_{i}$ belong to a fixed complete residue system of $A_{r}$ modulo $Q$ which includes the elements of $\mathbb{F}_{q^{r}}$ for convenience. Therefore

$$
\nu_{R}\left(\lambda-\lambda^{\gamma}\right)=\nu_{R}\left(\phi_{1-\alpha_{0}}(\lambda)-\sum_{i=1}^{n-1} \phi_{\alpha_{i}}\left(\phi_{t^{i}}(\lambda)\right)\right) .
$$

Furthermore,

$$
\nu_{R}\left(\phi_{t^{i}}(\lambda)\right)=q^{d r i} \quad \text { for } 1 \leq i \leq n-1,
$$

and $\nu_{R}\left(\phi_{b}(\lambda)\right)=1$ for $b \in A_{r}$ with $\nu_{Q}(b)=0$. Thus, if $\alpha_{0} \neq 1$, then $\nu_{R}\left(\lambda-\lambda^{\gamma}\right)=1$, and if $\alpha_{0}=1$ and $g \neq 1$, then

$$
\nu_{R}\left(\lambda-\lambda^{\gamma}\right)=q^{d r j},
$$

where $j$ is the least positive integer with $\alpha_{j} \neq 0$. Using the special form of $\operatorname{Gal}(E / L)$, we obtain
(10) $\quad d(R \mid S)$

$$
\begin{aligned}
& =\left(\frac{\left(q^{d}-1\right)\left(q^{r}-1\right)}{q-1}-1\right) q^{d(n-1)}+\sum_{j=1}^{n-1}\left(q^{d}-1\right) q^{d(n-1-j)} q^{d r j} \\
& =\left(\frac{\left(q^{d}-1\right)\left(q^{r}-1\right)}{q-1}-1+\frac{\left(q^{d}-1\right)\left(q^{d n(r-1)}-q^{d(r-1)}\right)}{q^{d(r-1)}-1}\right) q^{d(n-1)} .
\end{aligned}
$$

By the Hurwitz genus formula and $g\left(F_{r}\right)=g(F)$ we get

$$
2 g\left(K_{n}\right)-2=\left[K_{n}: F_{r}\right](2 g(F)-2)+\operatorname{deg}\left(\operatorname{Diff}\left(K_{n} / F_{r}\right)\right) .
$$

Since only the place $Q$ can be ramified in the extension $K_{n} / F_{r}$, we have

$$
\operatorname{deg}\left(\operatorname{Diff}\left(K_{n} / F_{r}\right)\right)=\frac{d\left[K_{n}: F_{r}\right] d(P \mid Q)}{e(P \mid Q)},
$$

where $d(P \mid Q)$, respectively $e(P \mid Q)$, is the different exponent, respectively ramification index, of $P$ over $Q$ and $P$ is the place of $K_{n}$ lying under $S$. Now

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

and so together with (9) this yields

$$
\operatorname{deg}\left(\operatorname{Diff}\left(K_{n} / F_{r}\right)\right)=\frac{d h\left(F_{r}\right) d(P \mid Q)}{h(F)} .
$$

Thus we obtain

$$
\begin{align*}
& \frac{h(F)}{h\left(F_{r}\right)}\left(2 g\left(K_{n}\right)-2\right)  \tag{11}\\
& \quad=\frac{(q-1)\left(q^{d r}-1\right)}{\left(q^{d}-1\right)\left(q^{r}-1\right)} q^{d(r-1)(n-1)}(2 g(F)-2)+d(P \mid Q) d
\end{align*}
$$

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

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

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

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

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

$$
d(R \mid U)=\left(n q^{d r}-n-1\right) q^{d r(n-1)} .
$$

If we combine this with (10), then we arrive at an expression for $d(P \mid Q)$, 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 $r d>m$. 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 $1 \leq l \leq r d-m$ 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 $N\left(K_{l}\right) \geq(m+1) p^{l}$ and $p^{l} \mid N\left(K_{l}\right)$. Furthermore, $N\left(K_{l}\right)=(m+1) p^{l}$ if $N(F)=m+1$.
(ii) The genus of $K_{l} / \mathbb{F}_{q}$ is given by

$$
g\left(K_{l}\right)=p^{l}(g(F)+d-1)+1-d .
$$

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

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

Then $\operatorname{dim}_{\mathbb{F}_{p}}(V)$ is equal to the $p$-rank of $\operatorname{Pic}_{Q^{2}}(A)$, which is at least the $p$-rank of $\left(A / Q^{2}\right)^{*}$. Let $t \in A$ be a uniformizer at $Q$ and let $\alpha_{1}, \ldots, \alpha_{r d}$ 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

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

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

$$
\mathbb{F}_{q^{d}}^{*} \otimes\left(\bigotimes_{i=1}^{r d}\left\langle 1+\alpha_{i} t\right\rangle\right),
$$

hence the $p$-rank of $\left(A / Q^{2}\right)^{*}$ is $r d$ since each cyclic subgroup $\left\langle 1+\alpha_{i} t\right\rangle$ 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 $1 \leq l \leq r d-m$, let $W_{l}$ be a subspace of $V$ of dimension $\operatorname{dim}_{\mathbb{F}_{p}}(V)-l$ containing all $P_{i}$. Let $G_{l}$ be the subgroup of $\operatorname{Pic}_{Q^{2}}(A)$ that
contains $\operatorname{Pic}_{Q^{2}}(A)^{p}$ and satisfies $G_{l} / \operatorname{Pic}_{Q^{2}}(A)^{p}=W_{l}$. Then $G_{l}$ contains all $P_{i}$ and $\left[\operatorname{Pic}_{Q^{2}}(A): G_{l}\right]=p^{l}$. Let

$$
E=H_{A}\left(\Lambda\left(Q^{2}\right)\right)
$$

be the narrow ray class field modulo $Q^{2}$ determined by a sgn-normalized Drinfeld $A$-module $\phi$ 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 $N\left(K_{l}\right) \geq(m+1) p^{l}$. 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 $G(S \mid R)$ of $S$ over $R$ has the order

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

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

$$
\begin{aligned}
d(S \mid T) & =\sum_{\gamma \in G(S \mid R) \backslash\{1\}} \nu_{S}\left(\lambda-\lambda^{\gamma}\right) \\
& =\sum_{\gamma \in G(S \mid R) \backslash H} \nu_{S}\left(\lambda-\lambda^{\gamma}\right)+\sum_{\gamma \in H \backslash\{1\}} \nu_{S}\left(\lambda-\lambda^{\gamma}\right),
\end{aligned}
$$

where $\lambda$ is a generator of $\Lambda\left(Q^{2}\right)$. As in the proof of Theorem 2 , we have $\nu_{S}\left(\phi_{t}(\lambda)\right)=q^{d}$ and $\nu_{S}\left(\phi_{b}(\lambda)\right)=1$ for $b \in A$ with $\nu_{Q}(b)=0$. Hence $\nu_{S}(\lambda-$ $\left.\lambda^{\gamma}\right)=1$ if $\gamma \in G(S \mid R) \backslash H$ and $\nu_{S}\left(\lambda-\lambda^{\gamma}\right)=q^{d}$ if $\gamma \in H \backslash\{1\}$. Thus we obtain

$$
d(S \mid T)=\left(q^{d}-2\right) p^{r d-l}+q^{d}\left(p^{r d-l}-1\right) .
$$

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

$$
\begin{aligned}
2 g(E)-2= & h(F)\left(q^{d}-1\right) p^{r d-l}\left(2 g\left(K_{l}\right)-2\right)+d h(F) d(S \mid T) \\
& +h(F) q^{d} \frac{\left(q^{d}-1\right)(q-2)}{q-1} .
\end{aligned}
$$

If we now use the formula for $d(S \mid T)$ above and Proposition 2(ii), then we arrive at the formula for $g\left(K_{l}\right)$.

Remark 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 $g\left(K_{1}\right)$ or $g\left(K_{1}\right)=p(g(F)-1)+1$. This holds since then $\left[K_{1}: F\right]=p$, so that either $Q$ is totally ramified in $K_{1} / F$ or the extension $K_{1} / F$ is unramified.

Remark 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 $1 \leq g \leq 51$ 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 $\infty$ of $F$ be the pole of $x$ and let $A=\mathbb{F}_{4}[x]$ be the $\infty$-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 $\left(\mathbb{F}_{2}[x] /\left(x^{3}+x+1\right)\right)^{*}$ of $\operatorname{Gal}(E / F)=(A / Q)^{*}$. Then $[K: F]=9$, and the places $x$ and $x+1$ split completely in $K / F$. The place $\infty$ 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 $2 g(K)-2=-9 \cdot 2+3 \cdot(3-1)+3 \cdot(9-1)$, 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 $Q_{2}^{\prime}$ of $F_{2} / \mathbb{F}_{4}$ of degree 2 lying over $R$, where $F_{2}=\mathbb{F}_{4} \cdot F$. Distinguish a rational place $\infty$ of $F$ and let $A$ and $A_{2}$ be the $\infty$-integral rings of $F$ and $F_{2}$, respectively. Put $E=H_{A_{2}}\left(\Lambda\left(Q_{2} Q_{2}^{\prime}\right)\right)$. We have

$$
\left|\operatorname{Pic}_{R}(A)\right|=15 \cdot h(F) \quad \text { and } \quad\left|\operatorname{Gal}\left(E / F_{2}\right)\right|=15^{2} \cdot h\left(F_{2}\right)=450 \cdot h(F)
$$

where we used (1) and $L_{F}(-1)=2$ in the last identity. Let $G$ be the subgroup of $\operatorname{Gal}\left(E / F_{2}\right)$ of order $45 \cdot h(F)$ which contains $\operatorname{Pic}_{R}(A)$, and let $K$ be the subfield of the extension $E / F_{2}$ fixed by $G$. Note that $\left[K: F_{2}\right]=10$. 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 $Q_{2}^{\prime}$, 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

$$
L_{F}(t)=4 t^{4}+6 t^{3}+5 t^{2}+3 t+1
$$

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 $Q_{2}^{\prime}$ of $F_{2} / \mathbb{F}_{4}$ of degree 2 lying over $R$, where $F_{2}=\mathbb{F}_{4} \cdot F$. Distinguish a rational place $\infty$ of $F$ and let $A$ and $A_{2}$ be the $\infty$-integral rings of $F$ and $F_{2}$, respectively. Put $E=H_{A_{2}}\left(\Lambda\left(Q_{2} Q_{2}^{\prime}\right)\right)$. We have

$$
\left|\operatorname{Pic}_{R}(A)\right|=15 \cdot h(F) \quad \text { and } \quad\left|\operatorname{Gal}\left(E / F_{2}\right)\right|=15^{2} \cdot h\left(F_{2}\right)=15^{2} \cdot h(F)
$$

where we used (1) in the last identity. Let $G$ be the subgroup of $\operatorname{Gal}\left(E / F_{2}\right)$ of order $45 \cdot h(F)$ which contains $\operatorname{Pic}_{R}(A)$, and let $K$ be the subfield of the extension $E / F_{2}$ fixed by $G$. Note that $\left[K: F_{2}\right]=5$. 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 $Q_{2}^{\prime}$, 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

$$
y^{2}+y=x^{2}(x+1)\left(x^{2}+x+1\right) .
$$

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

$$
L_{F}(t)=4 t^{4}+4 t^{3}+4 t^{2}+2 t+1 .
$$

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 $Q_{2}^{\prime}$ of $F_{2} / \mathbb{F}_{4}$ of degree 2 lying over $R$, where $F_{2}=\mathbb{F}_{4} \cdot F$. Distinguish a rational place $\infty$ of $F$ and let $A$ and $A_{2}$ be the $\infty$-integral rings of $F$ and $F_{2}$, respectively. Put $E=H_{A_{2}}\left(\Lambda\left(Q_{2} Q_{2}^{\prime}\right)\right)$ and note that $E$ is the composite field of $H_{A_{2}}\left(\Lambda\left(Q_{2}\right)\right)$ and $H_{A_{2}}\left(\Lambda\left(Q_{2}^{\prime}\right)\right)$. We have $\left|\operatorname{Pic}_{R}(A)\right|=15 \cdot h(F)$ and $\left|\operatorname{Gal}\left(E / F_{2}\right)\right|=15^{2} \cdot h\left(F_{2}\right)=675 \cdot h(F)$, where we used (1) and $L_{F}(-1)=3$ in the last identity. Furthermore, the place $\infty$ 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 $\mathbb{F}_{4}^{*} \cdot \operatorname{Pic}_{R}(A)$, then $\left[K: F_{2}\right]=15$. 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 $Q_{2}^{\prime}$, 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 $Q_{d}^{\prime}$ 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 | $Q_{2} Q_{2}^{\prime}$ | 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 | $Q_{2} Q_{2}^{\prime}$ | 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 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 | $\|G\|$ | $n$ | 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 | $Q_{2} Q_{2}^{\prime}$ | 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: $\quad y^{2}+y=\frac{x(x+1)}{x^{3}+x+1}, \quad$ F.2: $\quad y^{2}+y=x\left(x^{2}+x+1\right)^{2}$,
F.3: $\quad y^{2}+y=\frac{x}{x^{3}+x+1}, \quad$ F.4: $\quad y^{2}+y=x^{2}(x+1)\left(x^{2}+x+1\right)$,
F.5: $\quad L(\Lambda(Q))$ 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] —, 一, Algebraic function fields over finite fields with many rational places, IEEE Trans. Inform. Theory 41 (1995), 1548-1563.
[3] —, 一, 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. Vlădut, 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


[^0]:    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.

