manuscripta math. 107, 89 – 99 (2002)

Max Gebhardt

Constructing function fields with many rational places via the Carlitz module

Received: 7 September 2001/ Revised version: 19 October 2001

Abstract. We consider certain decomposition fields in extensions of $\mathbb{F}_q(Z)$ by the Carlitz module and give formulas for their genera and numbers of rational places, suitable for automatic computations. By extensive calculations we found some function fields which have more rational places than the known examples of the respective genus.

1. Introduction

In the last years the interest in the maximal number of points of a curve of genus g over the finite field $\mathbb{F}_q$ has vastly increased. One is interested in the number

$$N_q(g) := \max \left\{ \#C(\mathbb{F}_q) \mid \begin{array}{l} \text{C smooth, absolutely irreducible,} \\ \text{projective curve of genus } g \text{ over } \mathbb{F}_q \end{array} \right\}.$$

On the one hand there are different upper bounds for $N_q(g)$. The most famous one is the Weil-bound

$$N_q(g) \leq q + 1 + \lfloor 2g\sqrt{q} \rfloor.$$

On the other hand for every pair (q, g) one can get a lower bound for $N_q(g)$ by constructing a curve of genus g over $\mathbb{F}_q$ with enough rational points. An overview of the different methods is given in [GV00]. There the authors give tables for $q = 2, 4, 8, 16,\ 32, 64, 128,\ 3, 9, 27, 81$ and $g \leq 50$ of the best known results at that time. These tables are regularly updated and can be found in [GVNet]. To construct function fields with many rational places we have used methods of type II in the numbering of [GV00]. That means we used methods from class field theory based on Drinfeld modules of rank one. Thereby we followed the strategy of A.Keller in [Ke01] and used her formulas on the genus of special types of function fields. A more detailed deduction of these formulas can be found in [KeNet]. In most cases we cannot give the exact number of rational places in our function fields but we are able to give lower bounds.

M. Gebhardt: FR 6.1. Mathematik, Universität des Saarlandes, Postfach 15 11 50,
66041 Saarbrücken, Germany. e-mail: gebhardt@math.uni-sb.de

Mathematics Subject Classification (2000): 11G20, 11Y40, 11R58

2. Cyclotomic extensions of *K*

First we introduce some notations closely following [Ke01]. Let $p \in \mathbb{N}$ be a prime, $\mathbb{F}_q$ a finite field with characteristic p, $K = \mathbb{F}_q(Z)$ the rational function field in Z, and L a finite extension of K. For a finite galois extension $M|L$ and a place $\mathfrak{p}$ of L, the number of places of M over $\mathfrak{p}$ is denoted by $r(\mathfrak{p}, M|L)$, $e(\mathfrak{p}, M|L)$ denotes the ramification index, and $f(\mathfrak{p}, M|L)$ the residue class degree.

Definition 2.1. *Let $n \in \mathbb{F}_q[T]$ be a monic polynomial. Then there exists a unique factorisation of n in irreducible polynomials, namely:*

$$n = \prod_{\nu=1}^{s} p_\nu^{r_\nu},$$

with s, r_ν in $\mathbb{N}$ and $p_\nu \in \mathbb{F}_q[T]$ monic, irreducible and pairwise different polynomials of degree ≥ 1. We write for short

$$d_\nu := \deg(p_\nu)\ , \qquad q_\nu := q^{d_\nu},$$
$$n_\nu := \quad p_\nu^{r_\nu} \quad , \qquad m_\nu := \frac{n}{n_\nu} \qquad \text{and} \quad \varphi(n) := \#(\mathbb{F}_q[T]/(n))^*.$$

In the whole article we will not distinguish between an element $f \in \mathbb{F}_q[T]$ and its class $f + n \cdot \mathbb{F}_q[T]$ in $\mathbb{F}_q[T]/(n)$. The correct meaning will always be clear from the context. Note that for $\deg(n) \geq 2$ different polynomials of degree one remain different in $\mathbb{F}_q[T]/(n)$.

With every polynomial n of $\mathbb{F}_q[T]$ we associate a polynomial $\rho_n \in \mathbb{F}_q(Z)[X]$ by the following rules:

Definition 2.2. 1. $\rho_T(X) = ZX + X^q$,
2. $\rho_{T^i}(X) = \rho_T(\rho_{T^{i-1}}(X))$,
3. $\rho_{f+g}(X) = \rho_f(X) + \rho_g(X)$ *for all* $f, g \in \mathbb{F}_q[T]$,
4. $\rho_{cT}(X) = c \cdot \rho_T(X)$ *for all* $c \in \mathbb{F}_q$.

We define $K(n)$ as the splitting field of $\rho_n(X)$ over $\mathbb{F}_q(Z)$ and call n the conductor of the extension $K(n)|K$. In other words, $K(n)$ is obtained from $\mathbb{F}_q(Z)$ by adjoining the n-torsion of the Carlitz-module ρ (cf. [Go96, Chapter 3]). We denote $Gal(K(n), K)$ by $G(n)$.

Hayes proved in [Ha74] the following fundamental theorem on the structure of these extensions:

Theorem 2.3. 1. *The extension $K(n)|K$ is galois and abelian with Galois group $G(n) = (\mathbb{F}_q[T]/(n))^*$.*
2. *Let $n = p^r$ be a primary polynomial, then the extension $K(n)/K$ is totally ramified in $\mathfrak{p} = (p)$ and unramified in all other finite places $\mathfrak{q} \neq \mathfrak{p}$, $\mathfrak{q} \neq \infty$.*
3. *Let $K_+(n)$ be the fixed field of the embedding $\mathbb{F}_q^* \hookrightarrow (\mathbb{F}_q[T]/(n))^*$. Then the place ∞ of K is totally split in $K_+(n)$ and any place of $K_+(n)$ over ∞ is totally ramified in the extension $K(n)|K_+(n)$.*
4. *Let n be the product of s primary factors in $\mathbb{F}_q[T]$. Then $K(n)$ is the compositum of the fields $K(p_\nu^{r_\nu})$, $\nu = 1, \ldots, s$, and all these $K(p_\nu^{r_\nu})$ are linearly disjoint.*

5. *Let $\mathcal{O}(n)$ be the integral closure of $\mathbb{F}_q[Z]$ in $K(n)$ and λ a primitive root of ρ_n. Then*

$$\mathcal{O}(n) = (\mathbb{F}_q[Z])[\lambda] \, .$$

6. *$\mathbb{F}_q$ is the full constant field of $K(n)|K$.*

Proof. In [Ha74].

Remark 2.4. The theorem shows that the splitting fields of ρ_n have many of the properties of the cyclotomic fields over $\mathbb{Q}$. Therefore they are called *cyclotomic extensions of the rational function field*. The field $K_+(n)$ is the analogue of the maximal real extension of $\mathbb{Q}$ which is contained in the cyclotomic extension. The integral closure $\mathcal{O}(n)$ could be compared with the ring of integers $\mathbb{Z}[\zeta_m]$ for some primitive m-th root of unity ζ_m.

In the same paper Hayes also proves the following theorem:

Theorem 2.5. *Let $P(T) \in \mathbb{F}_q[T]$ be a monic irreducible polynomial, $n \in \mathbb{F}_q[T]$ monic and* $\gcd(n, P) = 1$. *Then the Artin symbol of the place $P(Z) \cdot \mathbb{F}_q[Z]$ in* $\mathrm{Gal}(K(n), K)$ *is the map given by ρ_P. So after identification of* $\mathrm{Gal}(K(n), K)$ *with* $(\mathbb{F}_q[T]/(n))^*$ *the Artin symbol of the ideal $P(Z) \cdot \mathbb{F}_q[Z]$ is the class $P(T) + n\mathbb{F}_q[T]$.*

Remark 2.6. (i) Note the use of the indeterminates T and Z in the theorem.

(ii) For every $\alpha \in \mathbb{F}_q^*$ the ideals $P(Z) \cdot \mathbb{F}_q[Z]$ and $(\alpha P(Z)) \cdot \mathbb{F}_q[Z]$ are equal. So one could wonder why in Theorem 2.5 $P(T) + n\mathbb{F}_q[T]$ and not $\alpha P(T) + n\mathbb{F}_q[T]$ corresponds to $P(Z) \cdot \mathbb{F}_q[Z]$. The answer lies in Definition 2.2. If we put there $\rho_T(X) = ZX + \beta X^q$ with some fixed $\beta \in \mathbb{F}_q^*$, Theorem 2.3 would remain valid. But in 2.5 the Artin symbol of $P(Z) \cdot \mathbb{F}_q[Z]$ would be $\gamma P(T) + n\mathbb{F}_q[T]$ with $\gamma \in \mathbb{F}_q^*$ depending on β and $P(Z)$. By choosing $\beta = 1$ we get that $\gamma = 1$ for all $P(Z)$.

3. The subfields

We will take a closer look at some subfields of $K(n)|K$. From now on we make the following assumptions:

$$n \text{ monic}\,, \quad \deg(n) \geq 2, \quad q \geq 3, \quad \gcd(T^2 - T, n) = 1.$$

The case $q = 2$ was already treated in [Ke01]. We take the following six subgroups of $\mathrm{Gal}(K(n), K)$:

$$\mathrm{Subgr} := \{\{1\}, \langle T\rangle, \langle T, T-1\rangle, \mathbb{F}_q^*, \langle \mathbb{F}_q^*, T\rangle, \langle \mathbb{F}_q^*, T, T-1\rangle\}.$$

Because of our assumptions these are actually subgroups of $G(n) = (\mathbb{F}_q[T]/(n))^*$ and $\mathbb{F}_q^* \neq \{1\}$. For every $H \in \mathrm{Subgr}$ let $K(n)^H$ be the corresponding subextension of $K(n)|K$, $S_1(n, H)$ the set of all places (finite and infinite) of $K(n)^H$ of degree one over K, and $g(n, H)$ the genus of $K(n)^H$.

4. The genus of the subextensions

For $n \in \mathbb{F}_q[T]$ and $H \in$ Subgr, A. Keller gives explicit formulas for $g(n, H)$ in [Ke01] and [KeNet]. For the convenience of the reader we will state them below. The formulas 4.3 and 4.4 are not in [Ke01] but in [KeNet].

We use the notation of Definition 2.1. Let $f \in \mathbb{F}_q[T]$ be a monic polynomial prime to T and $T-1$. We define $G(f) := (\mathbb{F}_q[T]/f)^*$ and

$$\begin{aligned} e_T(f) &:= \#\langle T \rangle_{G(f)}, & e_{T,+}(f) &:= \#\langle T, \mathbb{F}_q^* \rangle_{G(f)}, \\ \tilde{e}_{T,T-1}(f) &:= \#\langle T \rangle_{G(f)} \cap \langle T-1 \rangle_{G(f)}, & e_{T,T-1}(f) &:= \#\langle T, T-1 \rangle_{G(f)}, \\ \tilde{e}_{T,T-1,+}(f) &:= \#\langle T, T-1 \rangle_{G(f)} \cap \mathbb{F}_q^*, & e_{T,T-1,+}(f) &:= \#\langle T, T-1, \mathbb{F}_q^* \rangle_{G(f)}, \end{aligned}$$

and for $s = 1$ we put $\tilde{e}_*(m_\nu) := 1$ and $e_*(m_\nu) := 1$.

Genus Formula 4.1.

$$g(n, \{1\}) = 1 + \frac{1}{2}\,\varphi(n)\left(-2 + \frac{q-2}{q-1} + \sum_{\nu=1}^{s} d_\nu \frac{r_\nu q_\nu - r_\nu - 1}{q_\nu - 1}\right).$$

Genus Formula 4.2.

$$g(n, \mathbb{F}_q^*) = 1 + \frac{1}{q-1}\left(g(n, \{1\}) - 1 - \frac{1}{2}\left(\varphi(n)\frac{q-2}{q-1} + d_1(q-2)\right)\right)$$

for $s = 1$ and

$$g(n, \mathbb{F}_q^*) = 1 + \frac{1}{q-1}\left(g(n, \{1\}) - 1 - \frac{1}{2}\varphi(n)\frac{q-2}{q-1}\right) \quad \textit{for } s > 1.$$

Genus Formula 4.3.

$$\begin{aligned} g(n, \langle T \rangle) = 1 + \frac{1}{e_T(n)}\Bigg(g(n, \{1\}) - 1 - \frac{1}{2}\Bigg[\frac{\varphi(n)}{q-1}\left(\tilde{e}_{T,+}(n) - 1\right) \\ + \sum_{\nu=1}^{s} \varphi(m_\nu) d_\nu \cdot a_\nu(K_T(n))\Bigg]\Bigg) \end{aligned}$$

with

$$a_\nu(K_T(n)) = \frac{e_T(n)}{e_T(m_\nu)} - 1 + (q_\nu - 1)\left(\sum_{\alpha=1}^{r_\nu - 1} q_\nu^{\alpha-1} \frac{e_T(n)}{e_T(m_\nu p_\nu^\alpha)}\right) - q_\nu^{r_\nu - 1}.$$

Genus Formula 4.4.

$$\begin{aligned} g(n, \langle T, \mathbb{F}_q^* \rangle) = 1 + \frac{1}{e_{T,+}(n)}\Bigg(g(n, \{1\}) - 1 - \frac{1}{2}\Bigg[\frac{\varphi(n)}{q-1}(q-2) \\ + \sum_{\nu=1}^{s} \varphi(m_\nu) d_\nu \cdot a_\nu(K_{T,+}(n))\Bigg]\Bigg) \end{aligned}$$

with

$$a_\nu(K_{T,+}(n)) = \frac{e_{T,+}(n)}{e_{T,+}(m_\nu)} + (q_\nu - 1)\left(\sum_{\alpha=1}^{r_\nu - 1} q_\nu^{\alpha-1} \frac{e_{T,+}(n)}{e_{T,+}(m_\nu p_\nu^\alpha)}\right) - q_\nu^{r_\nu - 1}.$$

Genus Formula 4.5.

$$g(n,\langle T,T-1\rangle)=1+\frac{1}{e_{T,T-1}(n)}\left(g(n,\{1\})-1-\frac{1}{2}\left[\frac{\varphi(n)}{q-1}\left(\tilde{e}_{T,T-1,+}(n)-1\right)\right.\right.$$
$$\left.\left.+\sum_{\nu=1}^{s}\varphi(m_\nu)d_\nu\cdot a_\nu(K_{T,T-1}(n))\right]\right),$$

with

$$a_\nu(K_{T,T-1}(n))=\frac{e_{T,T-1}(n)}{e_{T,T-1}(m_\nu)}-q_\nu^{r_\nu-1}+(q_\nu-1)\sum_{\alpha=1}^{r_\nu-1}q_\nu^{\alpha-1}\frac{e_{T,T-1}(n)}{e_{T,T-1}(m_\nu p_\nu^\alpha)}.$$

Genus Formula 4.6.

$$g(n,\langle T,T-1,\mathbb{F}_q^*\rangle)=1+\frac{1}{e_{T,T-1,+}(n)}\left(g(n,\{1\})-1-\frac{1}{2}\left[\frac{\varphi(n)}{q-1}(q-2)\right.\right.$$
$$\left.\left.+\sum_{\nu=1}^{s}\varphi(m_\nu)d_\nu\cdot a_\nu(K_{T,T-1,+}(n))\right]\right),$$

with

$$a_\nu(K_{T,T-1,+}(n))=\frac{e_{T,T-1,+}(n)}{e_{T,T-1,+}(m_\nu)}-q_\nu^{r_\nu-1}+(q_\nu-1)\sum_{\alpha=1}^{r_\nu-1}\frac{q_\nu^{\alpha-1}\,e_{T,T-1,+}(n)}{e_{T,T-1,+}(m_\nu p_\nu^\alpha)}.$$

5. The number of rational places

For a place $\mathfrak{p}$ of $K(n)^H|\mathbb{F}_q(Z)$ we define the place $\tilde{\mathfrak{p}}$ of K as

$$\tilde{\mathfrak{p}}:=\begin{cases}\mathfrak{p}\cap\mathbb{F}_q[Z], & \mathfrak{p}\text{ finite}\\ \infty, & \mathfrak{p}\text{ infinite}\end{cases}$$

and

$$\begin{aligned}
N_1&:=\{\mathfrak{p}\in S_1(n,H)\mid e(\tilde{\mathfrak{p}},K(n)|K)=1,\tilde{\mathfrak{p}}\neq\infty\},\\
N_2&:=\{\mathfrak{p}\in S_1(n,H)\mid e(\tilde{\mathfrak{p}},K(n)|K)=1,\tilde{\mathfrak{p}}=\infty\},\\
N_3&:=\{\mathfrak{p}\in S_1(n,H)\mid e(\tilde{\mathfrak{p}},K(n)|K)>1,\tilde{\mathfrak{p}}\neq\infty\},\\
N_4&:=\{\mathfrak{p}\in S_1(n,H)\mid e(\tilde{\mathfrak{p}},K(n)|K)>1,\tilde{\mathfrak{p}}=\infty\}.
\end{aligned}$$

These sets are pairwise disjoint and $S_1(n,H)$ decomposes into

$$S_1(n,H)=N_1\cup N_2\cup N_3\cup N_4.$$

Now we analyse the size of the sets N_i. Since $q > 2$ we get by Theorem 2.3 that N_2 is the empty set. Furtheron we get by 2.3 and 2.5

$$\begin{aligned}\#N_1 &= \sum_{a \in \mathbb{F}_q,\, n(x)_{x=a} \neq 0, (T-a) \in H} [K(n)^H : K] \\ &= \#\{a \in \mathbb{F}_q \mid n(x)_{x=a} \neq 0,\ (T-a) \in H\} \cdot [K(n)^H : K] \\ &= \#\{a \in \mathbb{F}_q \mid (T-a) \in H\} \cdot [K(n)^H : K].\end{aligned}$$

For N_4 we have

$$\begin{aligned}\#N_4 &= \#\{\mathfrak{p} \in S_1(n, H) \mid e(\tilde{\mathfrak{p}}, K(n)|K) > 1, \tilde{\mathfrak{p}} = \infty\} \\ &\overset{q>2}{=} \#\{\mathfrak{p} \in S_1(n, H) \mid \tilde{\mathfrak{p}} = \infty\} \\ &= \frac{[K(n)^H : K]}{e(\infty, K(n)^H|K)},\end{aligned}$$

which for $\mathbb{F}_q^* \leq H$ specializes to $\#N_4 = [K(n)^H : K]$ by Theorem 2.3. So we get an explicit lower bound for $\#S_1(n, H)$.

Definition 5.1. *Let* $n \in \mathbb{F}_q[T]$ *monic,* $\gcd(T^2-T, n) = 1, \deg(n) > 1, H \in$ Subgr. *Then*

$$r(n, H) := \begin{cases} \#(N_1), & H = \{1\}, \langle T \rangle, \langle T, T-1 \rangle \\ \#(N_1 \cup N_4), & H = \mathbb{F}_q^*, \langle \mathbb{F}_q^*, T \rangle, \langle \mathbb{F}_q^*, T, T-1 \rangle \end{cases}.$$

By the previous arguments we directly get the following lemma:

Lemma 5.2. *Let* $n \in \mathbb{F}_q[T]$ *monic,* $\gcd(T^2-T, n) = 1$, $\deg(n) > 1$, $H \in$ Subgr. *Then*

$$r(n, H) = \begin{cases} [K(n)^H : \mathbb{F}_q(Z)] \cdot \#\{a \in \mathbb{F}_q \mid (T-a) \in H\}, \\ \qquad \textit{if } H = \{1\}, \langle T \rangle, \langle T, T-1 \rangle \\ \\ [K(n)^H : \mathbb{F}_q(Z)] \cdot (1 + \#\{a \in \mathbb{F}_q \mid (T-a) \in H\}), \\ \qquad \textit{if } H = \mathbb{F}_q^*, \langle \mathbb{F}_q^*, T \rangle, \langle \mathbb{F}_q^*, T, T-1 \rangle \end{cases}.$$

Proof. Clear by the preceding arguments. □

In some cases we even have equality between $r(n, H)$ and $\#S_1(n, H)$.

Lemma 5.3. *Let* $n \in \mathbb{F}_q[T]$ monic, $\deg(n) > 1$, $\gcd(T^q - T, n) = 1$, $H \in \{\mathbb{F}_q^*, \langle \mathbb{F}_q^*, T \rangle, \langle \mathbb{F}_q^*, T, T-1 \rangle\}$. *Then we have*

$$r(n, H) = \#S_1(n, H).$$

Proof. There are no zeros of n in $\mathbb{F}_q$. So by Theorem 2.3 the set N_3 is empty. □

6. Results

The above formulas have been derived and written down since they are suitable for automatic calculations. By extensive computations for $q = 4, 8, 16, 32, 64, 3, 9, 27, 5, 25$ we got the following results which beat those given in [GVNet].

There are lots of symmetries in our construction and so we got the same results for quite a lot of different conductors n. We always give the smallest one in lexicographical order.

If there is no entry in the tables [GVNet] resp. [ShNet] for a pair $(\mathbb{F}_q, g)$, we only mention results that beat the Drinfeld–Vladut bound. That means that the number of rational places is greater than $g \cdot \left(\sqrt{q} - 1\right)$. This bound seems poor for small g, and so we especially got many results for $\mathbb{F}_{25}$, because there are a lot of gaps in the corresponding table. For some values of q ($q = 4, 32, 64$) we didn't get any new result.

For every q the conductor ran through those of the lexicographically first 100 000 monic polynomials which are prime to $T^2 - T$. The bound is quite arbitrary. Except for $q = 25$ we got our results for conductors from the first 40 000 monic polynomials.

The finite field $\mathbb{F}_q$ is represented as $\mathbb{F}_p[u]/P$ with a monic, irreducible $P \in \mathbb{F}_p[u]$ of degree $[\mathbb{F}_q : \mathbb{F}_p]$. In the tables I stands for the index $[K(n)^H : \mathbb{F}_q(Z)]$, g for the genus $g(n, H)$, r for $r(n, H)$, lb gives the lower bounds and ub the upper bounds from the updated tables in [GVNet] from June 19, 2001. If the value of r meets the upper bound it is printed in bold letters. This occurs in just two cases. The value of r is framed if $H \in \{\mathbb{F}_q^*, \langle \mathbb{F}_q^*, T\rangle, \langle \mathbb{F}_q^*, T, T-1\rangle\}$ and $\gcd(n, T^q - T) = 1$. In these cases r is the exact number of rational places of the subfield $K(n)^H$ by Lemma 5.3.

Table 1.

$p = 2$								
$\mathbb{F}_q$	P	Conductor n	H	I	g	lb	r	ub
$\mathbb{F}_8$	u^3+u+1	T^5+uT^4+ $+T^3+(u^2+1)T^2+$ $+(u^2+u)T+(u^2+1)$	$\langle \mathbb{F}_q^*, T, T-1\rangle$	42	47	120	126	161
$\mathbb{F}_{16}$	u^4+u+1	$T^4+T^2+(u^2+u)T+1$	$\langle \mathbb{F}_q^*, T, T-1\rangle$	51	50	225	$\boxed{255}$	291
$\mathbb{F}_{16}$	u^4+u+1	$T^4+uT^3+u^2T^2+$ $+u^3T+(u+1)$	$\langle \mathbb{F}_q^*, T, T-1\rangle$	45	34	161	180	213

There are no tables for characteristic 5 in [GV00] and [GVNet]. So we have used the tables from [ShNet].

Remark 6.1. The most time and space consuming part of the calculations was to determine the span $\langle T, T-1\rangle < (\mathbb{F}_q[T]/(n))^*$. For the calculation of the genus we

Table 2.

$p = 3$								
$\mathbb{F}_q$	P	Conductor n	H	I	g	lb	r	ub
$\mathbb{F}_3$	–	$T^5 + 1$	$\langle \mathbb{F}_q^*, T \rangle$	16	19	28	**32**	32
$\mathbb{F}_3$	–	$T^5 + 2T^3 + 2T^2 + T + 2$	$\langle \mathbb{F}_q^*, T \rangle$	8	8	15	16	18
$\mathbb{F}_3$	–	$T^6 + T^2 + 2$	$\langle \mathbb{F}_q^*, T \rangle$	20	32	38	$\boxed{40}$	48
$\mathbb{F}_3$	–	$T^6 + T^4 + T^2 + 1$	$\langle \mathbb{F}_q^*, T \rangle$	32	49	63	$\boxed{64}$	67
$\mathbb{F}_3$	–	$T^9 + 2T + 1$	$\langle \mathbb{F}_q^*, T, T-1 \rangle$	13	42	48	$\boxed{52}$	59
$\mathbb{F}_9$	$u^2 + 1$	$T^6 + T^4 + T^2 +$ $+uT + 1$	$\langle \mathbb{F}_q^*, T, T-1 \rangle$	7	12	55	$\boxed{56}$	63
$\mathbb{F}_9$	$u^2 + 1$	$T^6 + (u+1)T^4 + 2T^3 +$ $+2uT^2 + (u+1)T +$ $+(2u^2 + 2u)$	$\langle \mathbb{F}_q^*, T, T-1 \rangle$	20	31	101	$\boxed{120}$	127
$\mathbb{F}_{27}$	$u^3 + 2u + 1$	$T^4 + T + (2u^2 + 1)$	$\langle \mathbb{F}_q^*, T \rangle$	52	50	299	312	416

Table 3.

$p = q = 5$						
Conductor n	H	I	g	lb	r	ub
$T^4 + 3T^2 + 2$	$\langle \mathbb{F}_q^*, T \rangle$	12	8	22	24	29
$T^4 + 2T^3 + 2T + 4$	$\langle \mathbb{F}_q^*, T \rangle$	16	9	26	**32**	32
$T^5 + 4T^2 + 1$	$\langle T \rangle$	12	20	–	36	–
$T^5 + T^4 + 2T^3 + T + 3$	$\langle T \rangle$	12	18	–	24	–
$T^5 + 3T^4 + 2T^3 + 2T^2 + T + 4$	$\langle \mathbb{F}_q^*, T \rangle$	32	29	56	64	73
$T^6 + 1$	$\langle \mathbb{F}_q^*, T, T-1 \rangle$	16	25	52	64	66
$T^6 + 2$	$\langle \mathbb{F}_q^*, T, T-1 \rangle$	24	45	88	$\boxed{96}$	104
$T^6 + 3T^3 + 3T^2 + T + 4$	$\langle \mathbb{F}_q^*, T, T-1 \rangle$	12	19	45	$\boxed{48}$	54
$T^6 + 4T^3 + 1$	$\langle \mathbb{F}_q^*, T, T-1 \rangle$	14	26	–	$\boxed{42}$	–
$T^6 + 3T^4 + 3T^2 + 1$	$\langle \mathbb{F}_q^*, T, T-1 \rangle$	25	44	–	75	–
$T^6 + 3T^4 + 4T^3 + 3T^2 + 1$	$\langle \mathbb{F}_q^*, T, T-1 \rangle$	18	22	51	$\boxed{54}$	60
$T^6 + T^5 + 2T^3 + 4T^2 + 2T + 4$	$\langle \mathbb{F}_q^*, T, T-1 \rangle$	12	15	35	$\boxed{36}$	45
$T^7 + T^5 + 3T^4 + 3T + 4$	$\langle \mathbb{F}_q^*, T, T-1 \rangle$	22	40	–	$\boxed{66}$	–
$T^7 + 4T^5 + 3T^4 + T^2 + 2T + 3$	$\langle \mathbb{F}_q^*, T, T-1 \rangle$	25	50	70	75	113

Table 4.

$p = 5, q = 25, P = u^2 + 2$						
Conductor n	H	I	g	lb	r	ub
$T^2 + 3T + (u + 4)$	$\langle T\rangle$	24	9	–	72	–
$T^2 + (u + 4)T + 2u$	$\langle T\rangle$	24	11	–	96	–
$T^3 + 1$	$\langle \mathbb{F}_q^*, T, T-1\rangle$	48	19	–	$\boxed{144}$	–
$T^3 + (u + 2)$	$\langle \mathbb{F}_q^*, T, T-1\rangle$	7	3	–	56	–
$T^3 + (u + 3)T + 2$	$\langle T\rangle$	42	31	–	210	–
$T^3 + T^2 + 2T + 2$	$\langle \mathbb{F}_q^*, T\rangle$	72	28	–	$\boxed{144}$	–
$T^3 + T^2 + (u + 1)T + (2u + 1)$	$\langle \mathbb{F}_q^*, T\rangle$	16	7	–	$\boxed{80}$	–
$T^3 + 4T^2 + (u + 2)T + (2u + 1)$	$\langle T, T-1\rangle$	24	15	–	96	–
$T^3 + uT^2 + T + 2u$	$\langle T, T-1\rangle$	24	14	–	96	–
$T^3 + (u + 1)T^2 + (3u + 3)T + (u + 4)$	$\langle T\rangle$	48	39	–	192	–
$T^3 + (u + 1)T^2 + (4u + 4)T + 3$	$\langle T\rangle$	18	16	–	126	–
$T^3 + (u + 2)T^2 + (2u + 4)T + (2u + 1)$	$\langle T, T-1\rangle$	48	29	–	144	–
$T^3 + (u + 3)T^2 + 1$	$\langle T, T-1\rangle$	24	20	–	120	–
$T^3 + (u + 3)T^2 + (3u + 2)T + (2u + 1)$	$\langle T, T-1\rangle$	24	21	–	144	–
$T^3 + (2u + 1)T^2 + (3u + 2)T + (3u + 3)$	$\langle T, T-1\rangle$	60	37	–	240	–
$T^4 + 3T + (u + 3)$	$\langle T, T-1\rangle$	8	5	–	56	–
$T^4 + (u + 4)T + 3u$	$\langle \mathbb{F}_q^*, T, T-1\rangle$	39	38	–	156	–
$T^4 + 4T^2 + (2u + 4)T + (u + 3)$	$\langle T, T-1\rangle$	24	26	–	120	–
$T^4 + uT^2 + 4$	$\langle \mathbb{F}_q^*, T, T-1\rangle$	13	12	101	104	140
$T^4 + (u + 1)T^2 + (2u + 4)$	$\langle T, T-1\rangle$	26	25	–	130	–
$T^4 + (u + 3)T^2 + (2u + 1)T + 4$	$\langle T, T-1\rangle$	48	47	–	192	–
$T^4 + (u + 4)T^2 + (3u + 3)$	$\langle T, T-1\rangle$	48	43	–	240	–
$T^4 + (u + 4)T^2 + (u + 2)T + (4u + 4)$	$\langle \mathbb{F}_q^*, T, T-1\rangle$	15	8	–	$\boxed{60}$	–
$T^4 + (2u + 1)T^2 + 3T + (3u + 1)$	$\langle \mathbb{F}_q^*, T, T-1\rangle$	48	33	–	$\boxed{192}$	–
$T^4 + (2u + 3)T^2 + 3u$	$\langle T, T-1\rangle$	24	27	–	120	–
$T^4 + (2u + 4)T^2 + (4u + 2)$	$\langle \mathbb{F}_q^*, T, T-1\rangle$	50	48	–	$\boxed{200}$	–
$T^4 + (2u + 4)T^2 + (2u + 1)T + (4u + 1)$	$\langle \mathbb{F}_q^*, T, T-1\rangle$	48	35	–	$\boxed{192}$	–
$T^4 + (2u + 4)T^2 + (3u + 1)T + 3u$	$\langle \mathbb{F}_q^*, T, T-1\rangle$	24	18	–	$\boxed{120}$	–
$T^4 + 2T^3 + (2u + 4)T^2 + (2u + 3)T + (3u + 1)$	$\langle T, T-1\rangle$	60	49	–	240	–
$T^4 + 3T^3 + T^2 + 2uT + (4u + 4)$	$\langle \mathbb{F}_q^*, T, T-1\rangle$	48	41	–	$\boxed{288}$	–
$T^4 + 3T^3 + 3T^2 + 2uT + (u + 1)$	$\langle \mathbb{F}_q^*, T\rangle$	48	45	–	$\boxed{192}$	–
$T^4 + 3T^3 + (2u + 2)T^2 + (3u + 4)T + 2u$	$\langle \mathbb{F}_q^*, T, T-1\rangle$	72	46	–	$\boxed{216}$	–

just need the cardinality of $\langle T, T-1\rangle$, which is easy computable by $\#\langle T, T-1\rangle = \frac{\#\langle T\rangle \cdot \#\langle T-1\rangle}{\#\{\langle T\rangle \cap \langle T-1\rangle\}}$ without knowing $\langle T, T-1\rangle$ explicitly. But since we have to know the elements in $\langle T, T-1\rangle$ to calculate $\#\{a \in \mathbb{F}_q \mid (T-a) \in \langle T, T-1\rangle\}$, we have to generate the subgroup anyway.

Remark 6.2. Especially the first example for $\mathbb{F}_3$ and the second one for $\mathbb{F}_5$ is interesting, because they realize the upper bound for genus 19 resp. 9.

7. Conclusion

By the Drinfeld–Vladut bound

$$\limsup_{g\to\infty} \frac{N_q(g)}{g} \leq \sqrt{q} - 1 \ ,$$

with equality if q is a square. But by a result in [FPS92] for every sequence of abelian extensions $(L_i|K)_{i\in\mathbb{N}}$ with $\lim_{i\to\infty}[L_i : K] = \infty$ and the same constant field $\mathbb{F}_q$,

$$\lim_{i\to\infty} \frac{\#S_1(L_i)}{g(L_i)} = 0$$

holds. Therefore, subextensions of the abelian extension $K(n)|K$ are asymptotically bad for the construction of curves with many rational places. But our calculations show that in small cases (n small) there is nevertheless a good chance to get interesting examples.

Furthermore, the choice of our six subextensions is quite arbitrary. We chose the subgroups generated by T and/or $(T - 1)$ and/or $\mathbb{F}_q^*$ to make sure that the corresponding places decompose completely in the corresponding subextensions, which yields a good chance to get many rational places therein. Since operation $Z \mapsto \alpha Z + \beta$ with $\alpha \in \mathbb{F}_q^*$, $\beta \in \mathbb{F}_q$ is 2-transitive on the finite rational places of $\mathbb{F}_q[Z]$, the choice of the two rational places T and $T - 1$ is inessential. But we could choose any other subgroup U of $(\mathbb{F}_q[T]/(n))^*$ to get interesting results, for example subgroups generated by $T, T - 1$ and some other polynomials of degree one. It is not clear which subgroups U would be good choices. For such a subgroup U we would have to calculate an explicit formula for the genus of $K(n)^U$ (in our examples this was done by A. Keller in her master thesis) and then count $\#\{a \in \mathbb{F}_q \mid (T - a) \in U\}$.

References

[FPS92] Frey, G., Perret, M., Stichtenoth, H.: On the different of abelian extensions of global fields. In: Coding theory and algebraic geometry, Proc. Int. Workshop, Luminy/Fr. 1991, Lect. Notes Math. **1518**, Berlin–Heidelberg–New York: Springer, 1992, pp. 26–32

[Go96] D. Goss: Basic Structures of Function Field Arithmetic. Berlin–Heidelberg–New York: Springer, 1996

[GV00] van der Geer, G. and van der Vlugt, M.: Tables of curves with many points. Math. Comp. **69**, no. 230, 797–810 (2000)

[GVNet] van der Geer, G. and van der Vlugt, M.: Tables of curves with many points. Available at http://www.wins.uva.nl/˜geer

[Ha74] Hayes, D.: Explicit class field theory for rational function fields. Trans. Am. Math. Soc. 77–91 (1974)

[Ke01] Keller, A.: Function Fields with Many Rational Places. In: Proceedings of the 5th International Conference on Finite Fields and Applications (Augsburg, 1999), Berlin–Heidelberg–New York: Springer, 2001, pp. 293–303

[KeNet] Keller, A.: Extremaleigenschaften von Kreisteilungserweiterungen rationaler Funktionenkörper. Master thesis, Saarbrücken 1999, available at http://www.math.uni-sb.de/˜ag-gekeler/liz/alice.html

[ShNet] Shabat, V.: Tables of curves with many points.
Available at http://www.turing.wins.uva.nl/˜shabat/tables.html