Finite Fields and Their Applications **5,** 436–449 (1999)
Article ID ffta.1999.0262, available online at http://www.idealibrary.com on IDEAL®

Curves with Many Points and Configurations of Hyperplanes over Finite Fields*

Ferruh Özbudak

Department of Mathematics, Middle East Technical University, Ínönü Bulvari, 06531 Ankara, Turkey
E-mail: ozbudak@math.metu.edu.tr

and

Henning Stichtenoth

Fachbereich 6, Mathematik und Informatik, Universität Gesamthochschule Essen, 45117 Essen, Germany
E-mail: stichtenoth@uni-essen.de

Communicated by Michael Tsfasman

Received December 9, 1998

We establish a correspondence between a class of Kummer extensions of the rational function field and configurations of hyperplanes in an affine space. Using this correspondence, we obtain explicit curves over finite fields with many rational points. Some of our examples almost attain the Oesterlé bound. © 1999 Academic Press

0. INTRODUCTION

Let K be a finite field and let $\mathscr{C}$ be an absolutely irreducible nonsingular projective curve defined over K. By the Hasse–Weil theorem, the number N of K-rational points of $\mathscr{C}$ is bounded by

$$N \leq \#K + 1 + 2g(\mathscr{C}) \cdot \sqrt{\#K}, \tag{0.1}$$

* The first author was partially supported by TÜBITAK and DAAD.

1071-5797/99 $30.00

where $g(\mathscr{C})$ denotes the genus of $\mathscr{C}$. If $g(\mathscr{C})$ is large with respect to the cardinality of K, this upper bound can be improved substantially by using explicit formulas (Serre [Se 1], Oesterlé [Se 2]). In this paper our goal is to construct curves over K with "many" points , i.e., their number of rational points should be close to the Oesterlé bound.

Curves with many rational points have been studied, among others, by Serre [Se 1, Se 2], van der Geer and van der Vlugt [G–V 2, G–V 3], Niederreiter and Xing [N–X 1, N–X 2, N–X 3, N–X 4], and Auer [A]. Many applications to coding theory, cryptology, and quasi-random points have been established.

Stepanov [Ste 1, Ste 2] considered curves over the field $\mathbb{F}_{q^2}$ (in odd characteristic) of the form

$$y_i^2 = x^q + x + b_i \quad \text{for} \quad i = 1, \ldots, s \tag{0.2}$$

with pairwise distinct elements $b_i \in \mathbb{F}_q$. These curves are fibre products of s cyclic coverings of degree 2 over the rational curve. On the other hand, fibre products of Artin–Schreier coverings of the rational curve were extensively studied by van der Geer and van der Vlugt [G–V 1] who found by this method many examples of curves with many points. Our approach is a generalization and refinement of Stepanov's method. We obtain several curves whose number of rational points is fairly close to the Oesterlé bound.

We fix some notations. $K = \mathbb{F}_{q^r}$ is the finite field of cardinality q^r, with $r > 1$, and $\bar{K} \supseteq K$ is an algebraic closure of K. The trace mapping $\mathrm{Tr}: K \to \mathbb{F}_q$ is defined by $\mathrm{Tr}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{r-1}}$, for $\alpha \in K$. We extend it to a map $\mathrm{Tr}: K[x] \to K[x]$ by setting $\mathrm{Tr}(f(x)) = f(x) + f(x)^q + \cdots + f(x)^{q^{r-1}}$.

Our curves are the non-singular projective models of affine curves defined by s equations

$$y_i^m = f_i(x) \in K[x], \quad \text{with} \quad (m, q) = 1. \tag{0.3}$$

We will show that these curves are—under appropriate conditions on the polynomials $f_i(x)$—absolutely irreducible, and we will determine their genus and number of K-rational points.

1. THE GENUS

Instead of curves, we study the corresponding function fields. So we consider an algebraic function field $E = K(x, y_1, \ldots, y_s)$, where

$$y_i^m = f_i(x) \in K[x] \quad \text{for} \quad i = 1, \ldots, s \tag{1.1}$$

and $(m, q) = (m, \deg f_i(x)) = 1$ for all i. We assume that the polynomials $f_i(x)$ have only simple roots in $\bar{K}$ and set

$$S_i := \{\alpha \in \bar{K} \mid f_i(\alpha) = 0\}, \quad S := \bigcup_{i=1}^{s} S_i. \tag{1.2}$$

$\bar{E} := E \cdot \bar{K} = \bar{K}(x, y_1, \ldots, y_s)$ denotes the constant field extension of E/K with $\bar{K}$. For $\alpha \in K$ (resp. $\alpha \in \bar{K}$), P_α is the zero of $x - \alpha$ in $K(x)$ (resp. in $\bar{K}(x)$), and P_∞ is the pole of x in $K(x)$ (resp. in $\bar{K}(x)$). The genus of a function field F/K is denoted by $g(F/K)$.

THEOREM 1.1. *Notations as above. Assume moreover that*

$$[\bar{E} : \bar{K}(x)] = m^s. \tag{$*$}$$

Then K is algebraically closed in E, and the genus of E/K is

$$g(E/K) = 1 + \frac{m^{s-1}}{2}(-m - 1 + (m-1) \cdot \# S).$$

Proof. For $\alpha \in S_i \cup \{\infty\}$ the place P_α is totally ramified in the extension $\bar{K}(x, y_i)/\bar{K}(x)$, all other places are unramified. By Abhyankar's lemma [Sti, p. 125] the ramification index $e(P_\alpha)$ in the compositum $\bar{E}/\bar{K}(x)$ is then $e(P_\alpha) = m$, since ramification is tame. All places P_α with $\alpha \in \bar{K} \setminus S$ are unramified in $\bar{E}/\bar{K}(x)$. The Hurwitz genus formula for $\bar{E}/\bar{K}(x)$ yields

$$2g(\bar{E}/\bar{K}) - 2 = -2m^s + (\# S + 1) \cdot m^{s-1}(m-1).$$

Since $g(E/K) = g(\bar{E}/\bar{K})$, the result follows. ∎

2. THE RATIONAL PLACES

We specialize the situation considered in Section 1 as follows:

$$\begin{aligned} &m \geq 2 \text{ is a divisor of } (q^r - 1)/(q - 1), \quad \text{and} \\ &y_i^m = \mathrm{Tr}(a_i x) + b_i \quad \text{with} \quad a_i \in K \setminus \{0\}, \quad b_i \in \mathbb{F}_q \end{aligned} \tag{2.1}$$

for $i = 1, \ldots, s$. Observe that the sets

$$S_i = \{\alpha \in \bar{K} \mid \mathrm{Tr}(a_i \alpha) + b_i = 0\} \quad \text{and} \quad S = \bigcup_{i=1}^{s} S_i$$

are contained in K.

THEOREM 2.1. *Situation as above. We assume that*

$$[\bar{E}:\bar{K}(x)] = m^s. \tag{$*$}$$

Then the number of K-rational places of E is

$$N(E/K) = m^s(q^r - \#S) + m^{s-1} \cdot t,$$

where t is the number of elements $\alpha \in S \cup \{\infty\}$ such that P_α has a K-rational extension in E.

Proof. Let $\alpha \in K \backslash S$; then $\mathrm{Tr}(a_i\alpha) + b_i \in \mathbb{F}_q \backslash \{0\}$ for $i = 1, \ldots, s$. Since m is a divisor of $(q^r - 1)/(q - 1)$ we conclude that the equation $\beta^m = \mathrm{Tr}(a_i\alpha) + b_i$ has m distinct roots $\beta \in K$, and therefore the place P_α splits completely in the extensions $K(x, y_i)/K(x)$, for $i = 1, \ldots, s$. As E is the compositum of these extensions, P_α splits completely in $E/K(x)$. Thus we have found $m^s(q^r - \#S)$ K-rational places in E. Now let $\alpha \in S \cup \{\infty\}$. If P_α has a K-rational extension in E then all places of E above P_α are rational because $E/K(x)$ is galois. The ramification index being $e(P_\alpha) = m$ (see proof of Theorem 1.1) there are exactly m^{s-1} K-rational places of E above P_α. ∎

3. CORRESPONDENCE TO AFFINE HYPERPLANES

We maintain all previous notations. In particular we have that $K = \mathbb{F}_{q^r}$ and $E = K(x, y_1, \ldots, y_s)$ with

$$y_i^m = \mathrm{Tr}(a_i x) + b_i, \quad a_i \in K \backslash \{0\}, \quad b_i \in \mathbb{F}_q$$

for $i = 1, \ldots, s$. In order to describe the places of $K(x)$ that are ramified in $E/K(x)$, we must study the sets

$$S_{a,b} := \{\alpha \in K \mid \mathrm{Tr}(a\alpha) + b = 0\} \tag{3.1}$$

for $a \in K \backslash \{0\}$, $b \in \mathbb{F}_q$. We fix a basis $(w_1, \ldots, w_r)$ of the extension $K/\mathbb{F}_q$; then every element $\alpha \in K$ has a unique representation

$$\alpha = \sum_{j=1}^{r} \alpha_j w_j \quad \text{with} \quad \alpha_j \in \mathbb{F}_q,$$

and the mapping

$$\psi: \begin{cases} K \to \mathbb{F}_q^r \\ \alpha \mapsto (\alpha_1, \ldots, \alpha_r) \end{cases} \tag{3.2}$$

is an isomorphism of $\mathbb{F}_q$-vector spaces. Let

$$\Sigma := \{S_{a,b} | a \in K \backslash \{0\} \quad \text{and} \quad b \in \mathbb{F}_q\},$$
$$\Lambda := \{H \subseteq \mathbb{F}_q^r | H \text{ is a hyperplane}\}.$$

THEOREM 3.1. *The mapping ψ in* (3.2) *induces a bijection from Σ onto Λ, and for $a, c \in K \backslash \{0\}$ and $b, d \in \mathbb{F}_q$ the following conditions are equivalent*:

(1) *The hyperplanes $\psi(S_{a,b})$ and $\psi(S_{c,d})$ are parallel* (*or equal*).
(2) $a/c \in \mathbb{F}_q \backslash \{0\}$.

Proof. First we show that ψ maps Σ into Λ. So we consider a set $S_{a,b} \in \Sigma$ as defined in (3.1). Let $\alpha = \sum_{j=1}^r \alpha_j w_j \in K$; then

$$\begin{aligned} \alpha \in S_{a,b} &\Leftrightarrow \operatorname{Tr}(a\alpha) + b = 0 \\ &\Leftrightarrow \sum_{j=1}^{r} \alpha_j \cdot \operatorname{Tr}(a \cdot w_j) + b = 0 \\ &\Leftrightarrow \psi(\alpha) = (\alpha_1, \ldots, \alpha_r) \in H_{a,b}, \end{aligned}$$

where $H_{a,b} \subseteq \mathbb{F}_q^r$ is the hyperplane defined by the linear condition

$$H_{a,b} = \left\{(\xi_1, \ldots, \xi_r) \in \mathbb{F}_q^r \,\middle|\, \sum_{j=1}^{r} \xi_j \cdot \operatorname{Tr}(a \cdot w_j) + b = 0\right\}.$$

Observe that $H_{a,b}$ is a hyperplane because

$$(\operatorname{Tr}(a \cdot w_1), \ldots, \operatorname{Tr}(a \cdot w_r)) \neq (0, \ldots, 0).$$

Next we have to show that for any hyperplane $H \subseteq \mathbb{F}_q^r$ there are elements $a \in K \backslash \{0\}$ and $b \in \mathbb{F}_q$ such that $H = \psi(S_{a,b})$. We can describe H by a linear equation

$$H = \left\{(\xi_1, \ldots, \xi_r) \in \mathbb{F}_q^r \,\middle|\, \sum_{j=1}^{r} \xi_j \cdot \varepsilon_j + b = 0\right\}$$

with $(\varepsilon_1, \ldots, \varepsilon_r) \in \mathbb{F}_q^r \backslash \{(0, \ldots, 0)\}$ and $b \in \mathbb{F}_q$. The mapping

$$\begin{cases} K \to \mathbb{F}_q^r \\ c \mapsto (\operatorname{Tr}(cw_1), \ldots, \operatorname{Tr}(cw_r)) \end{cases}$$

is $\mathbb{F}_q$-linear and injective (since Tr: $K \to \mathbb{F}_q$ is not identically 0), hence surjective. So there is some $a \in K \backslash \{0\}$ such that $\varepsilon_j = \operatorname{Tr}(a \cdot w_j)$ for $j = 1, \ldots, r$. It is

now obvious that $H = \psi(S_{a,b})$. The equivalence of conditions (1) and (2) is clear. ■

DEFINITION 3.2. A *configuration of hyperplanes* is an s-tuple $(H_1, \ldots, H_s)$ of hyperplanes $H_i \subseteq \mathbb{F}_q^r$. We call it an *admissible* configuration if

$$H_{j+1} \not\subseteq \bigcup_{i \le j} H_i \quad \text{for} \quad j \le 1, \ldots, s-1.$$

Note that this condition may depend on the ordering of the hyperplanes H_j.

THEOREM 3.3. *Suppose that $(H_1, \ldots, H_s)$ is an admissible configuration of hyperplanes. For $j = 1, \ldots, s$ let $a_j \in K \setminus \{0\}$ and $b_j \in \mathbb{F}_q$ such that $H_j = \psi(S_{a_j, b_j})$. Consider a function field $E = K(x, y_1, \ldots, y_s)$ with $y_j^m = \mathrm{Tr}(a_j x) + b_j$ for $j = 1, \ldots, s$. Then we have*

$$[E : K(x)] = [\bar{E} : \bar{K}(x)] = m^s,$$

i.e., condition (∗) *from Theorems* 1.1 *and* 2.1 *holds.*

Proof. By induction. The case $s = 1$ is trivial, so we assume now that $s \ge 2$. For $j = 1, \ldots, s$ let

$$S_j = S_{a_j, b_j} = \{\alpha \in K \mid \mathrm{Tr}(a_j \alpha) + b_j = 0\}.$$

Since $(H_1, \ldots, H_s)$ is admissible there is an element

$$\gamma \in S_s \Big\backslash \bigcup_{j \le s-1} S_j.$$

The place P_γ of $\bar{K}(x)$ is then unramified in the extension $\bar{K}(x, y_1, \ldots, y_{s-1})/\bar{K}(x)$, and it is totally ramified in $\bar{K}(x, y_s)/\bar{K}(x)$. Hence

$$[\bar{K}(x, y_1, \ldots, y_s) : \bar{K}(x, y_1, \ldots, y_{s-1})] = m.$$

■

Finally we give a criterion for whether a place P_α of $K(x)$ which ramifies in $E/K(x)$ has K-rational extensions in E.

THEOREM 3.4. *Let $E = K(x, y_1, \ldots, y_s)$ with*

$$y_i^m = \mathrm{Tr}(a_i x) + b_i, \quad 0 \ne a_i \in K, \quad b_i \in \mathbb{F}_q$$

and m a divisor of $(q^r-1)/(q-1)$. Assume that condition $(*)$ holds, i.e., $[E:K(x)]=m^s$. Let

$$S_i=\{\alpha\in K\,|\,\mathrm{Tr}(a_i\alpha)+b_i=0\}\quad\text{and}\quad S=\bigcup_{i=1}^{s}S_i.$$

Then we have:

(i) *For $\alpha\in S$ the following conditions are equivalent*:

(1) *The place P_α of $K(x)$ has K-rational extensions in E.*

(2) *For all $i,j\in\{1,\ldots,s\}$ with $\alpha\in S_i\cap S_j$, the element a_i/a_j is an mth power of some element of K.*

(ii) *The place P_∞ has K-rational extensions in E if and only if a_i/a_j is an mth power of some element of K, for all $i,j\in\{1,\ldots,s\}$.*

Proof. We prove only (i); the proof of (ii) is similar. First we assume that condition (2) holds. We can assume that

$$\alpha\in S_i\quad\text{for}\quad i=1,\ldots,k\quad\text{and}\quad\alpha\notin S_i\quad\text{for}\quad i>k.$$

For $i\neq 2,\ldots,k$ we define $z_i:=y_i/y_1$; thus

$$E=K(x,y_1,z_2,\ldots,z_k,y_{k+1},\ldots,y_s).$$

The place P_α splits completely in the extensions $K(x,y_i)$ for $i=k+1,\ldots,s$ (see proof of Theorem 2.1). For $i=2,\ldots,k$ one has

$$\begin{aligned}z_i^m&=\frac{\mathrm{Tr}(a_ix)+b_i}{\mathrm{Tr}(a_1x)+b_1}=\frac{\mathrm{Tr}(a_ix)+b_i-(\mathrm{Tr}(a_i\alpha)+b_i)}{\mathrm{Tr}(a_1x)+b_1-(\mathrm{Tr}(a_1\alpha)+b_1)}\\&=\frac{\mathrm{Tr}(a_i(x-\alpha))}{\mathrm{Tr}(a_1(x-\alpha))}=\frac{a_i}{a_1}\cdot\frac{1+(x-\alpha)\cdot h_i(x)}{1+(x-\alpha)\cdot h_1(x)}\end{aligned}\tag{3.3}$$

with polynomials $h_i(x),h_1(x)\in K[x]$. Since a_i/a_1 is an mth power in K we see from (3.3) that P_α splits also in $K(x,z_i)/K(x)$ for $i=2,\ldots,k$. So P_α splits completely in $K(x,z_2,\ldots,z_k,y_{k+1},\ldots,y_s)/K(x)$, and P_α ramifies in $K(x,y_1)/K(x)$. We conclude that P_α has only K-rational extensions in E.

Now we assume that condition (2) does not hold; say

$$\alpha\in S_1\cap S_i\quad\text{and}\quad a_i/a_1\text{ is not an }m\text{th power in }K.$$

Since $z_i = y_i/y_1$ satisfies an equation

$$z_i^m = \frac{a_i}{a_1} \cdot \frac{1 + (x - \alpha) \cdot h_i(x)}{1 + (x - \alpha) \cdot h_1(x)},$$

the place P_α is inert in $K(x, z_i)/K(x)$ in this case. ■

COROLLARY 3.5. *Let $E = K(x, y_1, \ldots, y_s)$ and $E' = K(x, y'_1, \ldots, y'_s)$ be defined by the equations*

$$y_i^m = \mathrm{Tr}(a_i x) + b_i, \quad \textit{resp.} \quad y_i'^m = \mathrm{Tr}(a'_i x) + b'_i$$

with $a_i, a'_i \in K \backslash \{0\}$ and $b_i, b'_i \in \mathbb{F}_q$, for $i = 1, \ldots, s$. Suppose that the corresponding configurations of hyperplanes $(H_1, \ldots, H_s)$ resp. $(H'_1, \ldots, H'_s)$ are admissible and that all ratios a_i/a_j resp. a'_i/a'_j are mth powers in K. If

$$\#\left(\bigcup_{i=1}^{s} H_i\right) < \#\left(\bigcup_{i=1}^{s} H'_i\right),$$

then

$$g(E/K) < g(E'/K) \quad \text{and} \quad N(E) > N(E').$$

Proof. Clear from Theorems 1.1, 2.1, and 3.4. ■

Corollary 3.5 converts the problem of finding curves (of the type considered in this paper) with many points and small genus into finding "dense" configurations of hyperplanes.

4. EXAMPLES

In this section we give several examples of curves with many rational points. The corresponding configurations are found in Figs. 1–4.

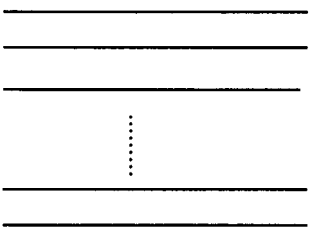

FIGURE 1

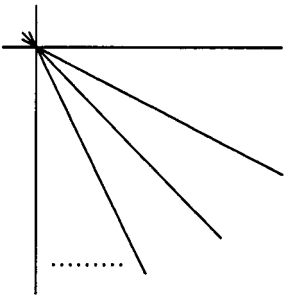

FIGURE 2

EXAMPLE 4.1 (Parallel Hyperplanes; see Fig. 1). Let $a \in \mathbb{F}_{q^r} \setminus \{0\}$ and let $b_1, \ldots, b_s \in \mathbb{F}_q$, with $b_i \neq b_j$ for $i \neq j$. Consider the configuration of hyperplanes $(H_1, \ldots, H_s)$ with

$$H_i := \psi(S_{a,b_i}), \quad i = 1, \ldots, s.$$

Since $H_i \cap H_j = \emptyset$ for $i \neq j$, this configuration is admissible, and (with notations as in Sections 2 and 3) we have

$$\# S = s \cdot q^{r-1} \quad \text{and} \quad t = 1 + s \cdot q^{r-1}.$$

The corresponding function field $E/\mathbb{F}_{q^r}$ has genus

$$g = 1 + \frac{m^{s-1}}{2}(-m - 1 + sq^{r-1}(m-1)),$$

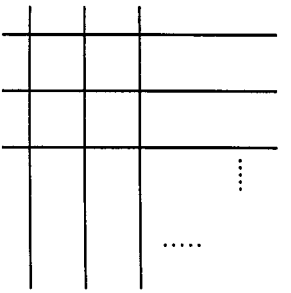

FIGURE 3

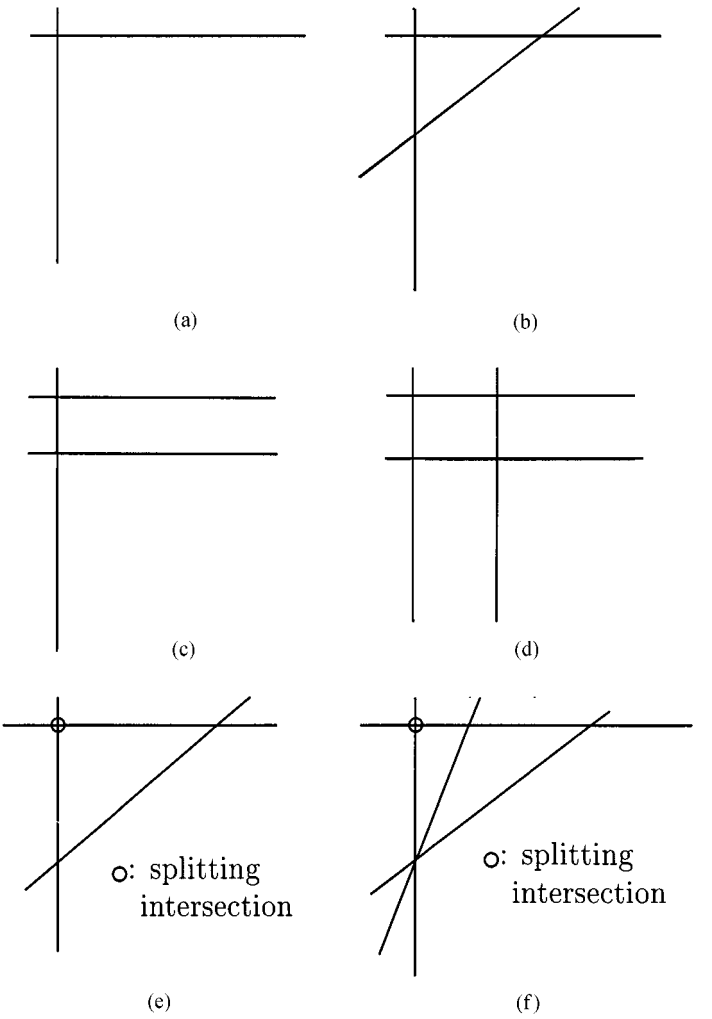

FIGURE 4

and its number of $\mathbb{F}_{q^r}$-rational places is

$$N = m^s(q^r - sq^{r-1}) + m^{s-1}(1 + sq^{r-1}).$$

Note that the case $r = 2$ (and $m = 2$) is the configuration that was used by Stepanov [Ste 1, Ste 2].

From here on we will restrict ourselves to the case $r = 2$, for simplicity. Hyperplanes are then just lines in the affine plane over $\mathbb{F}_q$.

EXAMPLE 4.2 (Lines Intersecting in One Point; see Fig. 2). Let $r = 2$ and $s \leq (q+1)/m$. Choose $a_1, \ldots a_s \in \mathbb{F}_{q^r}^{\times}$ such that all a_i are mth powers and $a_i/a_j \notin \mathbb{F}_q$ for $i \neq j$. Let

$$H_j := \psi(S_{a_j,0}) \quad \text{for} \quad j = 1, \ldots, s.$$

Then $H_i \cap H_j = \{(0,0)\}$ for $i \neq j$, and the configuration $(H_1, \ldots, H_s)$ is admissible with

$$\# S = 1 + s(q-1) \quad \text{and} \quad t = 2 + s(q-1).$$

So we have

$$g = 1 + \frac{m^{s-1}}{2}(-m - 1 + (m-1)(1 + s(q-1)))$$

and

$$N = m^s(q^2 - (1 + s(q-1))) + m^{s-1}(2 + s(q-1)).$$

EXAMPLE 4.3 (See Fig. 3). Let $r = 2$ and let m be a proper divisor of $q+1$. Choose $a_1, a_2 \in \mathbb{F}_{q^2} \setminus \{0\}$ such that a_1, a_2 are mth powers and $a_1/a_2 \notin \mathbb{F}_q$. Let $b_1, \ldots, b_u \in \mathbb{F}_q$ be pairwise distinct and consider the configuration $(H_1, \ldots, H_s)$, where $s = 2u$ and

$$H_1 = \psi(S_{a_1,b_1}), \quad H_2 = \psi(S_{a_2,b_1}), \quad H_3 = \psi(S_{a_1,b_2}), \ldots,$$
$$H_{2u-1} = \psi(S_{a_1,b_u}), \quad H_{2u} = \psi(S_{a_2,b_u}).$$

We obtain now

$$\# S = 2qu - u^2,$$
$$t = 1 + \# S = 2qu - u^2 + 1.$$

Therefore

$$g = 1 + \frac{m^{2u-1}}{2}(-m - 1 - (m-1)(2qu - u^2))$$

and

$$N = m^{2u}(q^2 - 2qu + u^2) + m^{2u-1}(2qu - u^2 + 1).$$

EXAMPLE 4.4. (1) (See Fig. 4a) $q = 2, q^r = 4, m = 3, s = 2$ and H_1, H_2 intersect in one point. We have

$$g = 4 \quad \text{and} \quad N = 15.$$

(2) (See Fig. 4a) $q = 4, q^r = 16, m = 5, s = 2, \#S = 7,$ and $t = 6$. We have

$$g = 56 \quad \text{and} \quad N = 255.$$

(3) (See Fig. 4a) $q = 8, q^r = 64, m = 3, s = 2, \#S = 15,$ and $t = 16$. We have

$$g = 40 \quad \text{and} \quad N = 489.$$

(4) (See Fig. 4a) $q = 3, q^r = 9, m = 2, s = 2, \#S = 5,$ and $t = 6$. We have

$$g = 3 \quad \text{and} \quad N = 28.$$

In the cases which correspond to Fig. 4e and 4f, the notion "splitting intersection" means that the corresponding place of $K(x)$ has rational extensions in $E/K(x)$.

(5) (See Fig. 4e) $q = 3, q^r = 9, m = 2, s = 3, \#S = 6,$ and $t = 4$. We have

$$g = 7 \quad \text{and} \quad N = 40.$$

(6) (See Fig. 4c) $q = 3, q^r = 9, m = 2, s = 3, \#S = 7,$ and $t = 8$. We have

$$g = 9 \quad \text{and} \quad N = 48.$$

(7) (See Fig. 4f) $q = 3, q^r = 9, m = 2, s = 4, \#S = 7,$ and $t = 4$. We have

$$g = 17 \quad \text{and} \quad N = 64.$$

(8) (See Fig. 4d) $q = 3, q^r = 9, m = 2, s = 4, \#S = 8,$ and $t = 9$. We have

$$g = 21 \quad \text{and} \quad N = 88.$$

(9) (See Fig. 4a) $q = 9, q^r = 81, m = 2, s = 2, \#S = 17,$ and $t = 18$. We have

$$g = 15 \quad \text{and} \quad N = 292.$$

(10) (See Fig. 4b) $q = 9$, $q^r = 81$, $m = 2$, $s = 3$, $\#S = 24$, and $t = 25$. We have

$$g = 43 \quad \text{and} \quad N = 556.$$

(11) (See Fig. 4a) $q = 5$, $q^r = 25$, $m = 2$, $s = 2$, $\#S = 9$, and $t = 10$. We have

$$g = 7 \quad \text{and} \quad N = 84.$$

One can easily generalize our method by considering distinct exponents $m_1, \ldots, m_s$; i.e.,

$$y_i^{m_i} = \mathrm{Tr}(a_i x) + b_i \quad \text{for} \quad i = 1, \ldots, s.$$

Choosing the m_i properly, one finds other examples of curves with many points. As an example, we consider

(12) (See Fig. 4a) $q = 7$, $q^r = 49$,

$$y_1^2 = x^q + x, \quad y_2^4 = a^q x^q + ax,$$

with a being a 4th power in $\mathbb{F}_{49} \backslash \mathbb{F}_7$. We have

$$g = 29 \quad \text{and} \quad N = 328.$$

Remark 4.5. The following notion is common: for q being a power of some prime number and an integer $g \geq 0$, let

$$N_q(g) = \max\{N \mid N \text{ is the number of } \mathbb{F}_q - \text{rational points on some curve of genus } g \text{ defined over } \mathbb{F}_q\}.$$

(Curve means here a non-singular, absolutely irreducible projective curve.) By the Hasse–Weil theorem,

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

Oesterlé gave an essential improvement of this upper bound, based on Serre's explicit formulas [Se 2]. Lower bounds for $N_q(g)$ are usually obtained by constructing specific curves of genus g over $\mathbb{F}_q$. The tables in [G–V 2, A] give the at present best known lower bounds for $N_q(g)$. All our examples in Example 4.4 (2), (3), (5), (6), (7), (8), (9), (10), (11), (12) provide improvements of the tables. Some of our curves are very close to the Oesterlé bound, for instance in the case $q^r = 9$ and $g = 7$ resp. 9 where the Oesterlé bound is 43 resp. 51. Examples 4.4. (1) and (4) reach the Oesterlé bound.

REFERENCES

[A] R. Auer, "Ray Class Fields of Global Function Fields with Many Rational Places," Report, University of Oldenburg, 1998, *available* http://xxx.lanl.gov, math.AG/9803065.

[G–V 1] G. van der Geer and M. van der Vlugt, Fibre products of Artin–Schreier curves and generalized Hamming weights of codes. *J. Combin. Theory A* **70** (1995), 337–348.

[G–V 2] G. van der Geer and M. van der Vlugt, Tables of the function $N_q(g)$. [Regularly updated tables, *available* http://www.uva.nl/~geer]

[G–V 3] G. van der Geer and M. van der Vlugt, How to construct curves over finite fields with many points, *in* "Arithmetic Geometry, Cortona 1994" (F. Catanese, Ed.), pp. 169–189, Cambridge Univ. Press, Cambridge, UK, 1997.

[N–X 1] H. Niederreiter and C. P. Xing, Explicit global function fields over the binary field with many rational places, *Acta Arith.* **75** (1996), 383–396.

[N–X 2] H. Niederreiter and C. P. Xing, Cyclotomic function fields, Hilbert class fields and global function fields with many rational places, *Acta Arith.* **79** (1997), 59–76.

[N–X 3] H. Niederreiter and C. P. Xing, Drinfeld modules of rank 1 and algebraic curves with many rational points, II, *Acta Arith.* **81** (1997), 81–100.

[N–X 4] H. Niederreiter and C. P. Xing, Global function fields with many rational points over the ternary field, *Acta Arith.* **83** (1998), 65–86.

[Se 1] J.-P. Serre, Sur le nombre de points rationnels d'une courbe algèbrique sur un corps fini, *C. R. Acad. Sci. Paris Ser. I* **296** (1983), 397–402.

[Se 2] J.-P. Serre, Rational points on curves over finite fields, Notes of Lectures at Harvard University, 1985.

[Ste 1] S. A. Stepanov, Codes on fibre products of hyperelliptic curves, *Discrete Math. Appl.* **7**, No. 1 (1997), 77–88.

[Ste 2] S. A. Stepanov, Character sums and coding theory, *in* "Finite Fields and Applications" (S. D. Cohen and H. Niederreiter, Eds.), pp. 355–378, Cambridge Univ. Press, Cambridge, UK, 1996.

[Sti] H. Stichtenoth, "Algebraic Function Fields and Codes," Springer-Verlag, Berlin/New York, 1993.