An Explicit Construction of a Sequence of Codes Attaining the Tsfasman–Vlăduţ–Zink Bound The First Steps

Conny Voss and Tom Høholdt, *Member, IEEE*

***Abstract*—We present a sequence of codes attaining the Tsfasman–Vlăduţ–Zink bound. The construction is based on the tower of Artin–Schreier extensions recently described by Garcia and Stichtenoth. We also determine the dual codes. The first steps of the constructions are explicitely given as generator matrices.**

***Index Terms*—Algebraic geometric codes, asymptotically good codes.**

I. Introduction

Let $\mathbb{F}_l$ be the finite field of cardinality l and let $(F_i)_{i\geq 1}$ be a sequence of algebraic function fields over $\mathbb{F}_l$ where $F_i/\mathbb{F}_l$ has genus g_i and $N_i = N(F_i)$ places of degree one such that $g_i \to \infty$ and

$$\lim_{i\to\infty} N_i/g_i > 1. \quad (1)$$

It is well known (see [6], [8]) that in this situation one can construct asymptotically good sequences of algebraic geometric (geometric Goppa) codes over $\mathbb{F}_l$.

Let $N_l(g) := \max\{N(F)|F\cdot$ is a function field of genus g over $\mathbb{F}_l\}$ and

$$A(l) := \lim_{g\to\infty} \sup N_l(g)/g.$$

The Drinfeld–Vlăduţ bound (see [1]) tells us that

$$A(l) \leq \sqrt{l} - 1$$

and it was shown by Ihara [3] and Tsfasman, Vlăduţ, and Zink [7] that, if $l = q^2$ is a square

$$A(q^2) = q - 1.$$

For l a square, $l \geq 49$ and $\lim_{i\to\infty} N_i/g_i = A(l)$ the Tsfasman–Vlăduţ–Zink (TVZ) theorem [7] says that the parameters of the related algebraic geometric codes are better than the Gilbert–Varshamov bound in a certain range of the rate. In [4] and [9] it is shown how to reach the TVZ bound with a polynomial construction but the complexity of this algorithm is so high that the actual construction, i.e., generator or parity-check matrices of the code, is intractable. In a recent preprint by Feng and Rao [10], the authors claimed to have found asymptotically good codes in an elementary way using socalled generalized Klein curves which are defined by the equations

$$x_{i+1}^3 x_i + x_i^3 + x_{i+1} = 0, i = 1, \cdots, m-1$$

over GF (8). Pellikaan tried to figure out whether their claim was correct (the curves are asymptotically bad as recently found out by Garcia and Stichtenoth) and suggested the curves with equations

$$x_{i+1}^2 x_i + x_i^2 + x_{i+1} = 0, \quad i = 1, \cdots, m-1 \text{ over GF}(4).$$

It turned out that this gave a tower of Artin–Schreier extensions which enabled Garcia and Stichtenoth to generalize to an arbitrary square power q and to calculate the genera and the number of $\mathbb{F}_q$-rational points and therefore to prove that the curves were asymptotically good, so we have a tower of function fields $(F_i)_{i\geq 1}$ over $\mathbb{F}_{q^2}$ reaching the Drinfeld–Vlăduţ bound $A(q^2) = q - 1$. The function fields of this tower are defined in the following way:

Definition 1.1: Let $F_1 := \mathbb{F}_{q^2}(x_1)$ be the rational function field over $\mathbb{F}_{q^2}$. For $n \geq 1$ let

$$F_{n+1} := F_n(z_{n+1})$$

where z_{n+1} satisfies the equation

$$z_{n+1}^q + z_{n+1} = x_n^{q+1}$$

with

$$x_n := z_n/x_{n-1} \quad (\text{for } n \geq 2).$$

In this paper we first present sequences of asymptotically good algebraic geometric codes related to the function field tower of Garcia and Stichtenoth, and we determine their dual codes as well.

For a function field $F_i/\mathbb{F}_{q^2}$ an algebraic geometric code C_i is of the form $C_i = C_{\mathcal{L}}(D_i, G_i)$ with $D_i = P_1 + \cdots + P_n$ where the P_j's are pairwise-distinct places of degree one in $F_i/\mathbb{F}_{q^2}$, and G_i a divisor of $F_i/\mathbb{F}_{q^2}$ such that $\mathrm{supp}(G_i) \cap \mathrm{supp}(D_i) = \emptyset$. Then

$$C_i = \{(f(P_1), \cdots, f(P_n)) | f \in \mathcal{L}(G_i)\} \subseteq (\mathbb{F}_{q^2})^n.$$

For applications of such codes in practice one needs an explicit description, which means an explicit basis for the vector space $\mathcal{L}(G_i)$ or a generator matrix of the code C_i.

Manuscript received May 24, 1995; revised March 15, 1996. The material in this paper was presented in part at the AGCT-5, Luminy, France, June 1996.

The authors are with the Department of Mathematics, Technical University of Denmark, Bldg. 303, DK-2800 Lyngby, Denmark.

Publisher Item Identifier S 0018-9448(97)00158-2.

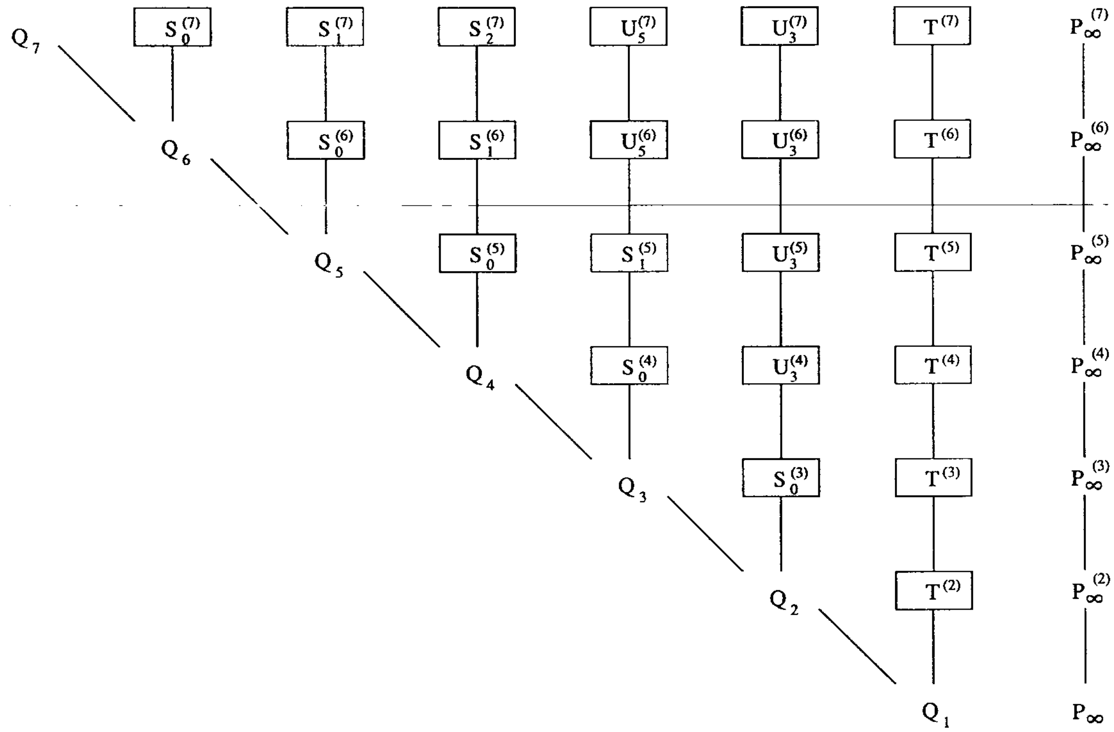

Fig. 1.

The second function field F_2 in the tower is the Hermitian function field and the related codes C_2 in our sequences are the well-known Hermitian codes (see, e.g., [6]). In the second part of this paper we will describe the codes C_3 corresponding to F_3 in detail by constructing a basis of $\mathcal{L}(G_3)$ and a generator matrix for C_3. As in the Hermitian case, it turns out that the dual codes of the codes C_3 are of the same type.

From the special case $G_3 = sP_\infty$, where $s > 0$ and P_∞ is the pole of x_1 in F_3, we get the pole numbers of P_∞. While in F_2 the pole numbers of the pole of x_1 are generated by only two numbers, namely, q and $q+1$; it turns out that in F_3 one in general needs more than three numbers to generate the whole set of pole numbers.

Our bases for the vector spaces $\mathcal{L}(G_3)$ consist of monomial expressions in x_1, x_2, and z_3 (where negative exponents are possible) which makes it easy to give a generator matrix for the codes C_3. One could maybe hope that, in a similar manner, a general description of the spaces $\mathcal{L}(G_i)$ for $i \geq 1$ would be possible, but unfortunately already for G_4 monomial expressions in x_1, x_2, x_3, and z_4 are not sufficient to generate the whole space.

II. Preliminaries

We start with some notation and definitions that are used throughout this paper. Many of them are the same as in [2].

$F_i, i \geq 1$	function fields as defined in Definition 1.1;
$g_i = g(F_i)$	genus of $F_i/\mathbb{F}_{q^2}$;
$\mathbb{P}(F)$	set of places of the function field $F/\mathbb{F}_{q^2}$;
$N_i = N(F_i)$	number of places $P \in \mathbb{P}(F_i)$ of degree one;
v_p	normalized discrete valuation associated with P;
$\mathrm{Diff}\,(F_n/F_k)$	different of the extension F_n/F_k $(k < n)$;
$\mathrm{con}_{F_n/F_k}(A)$	conorm of a divisor A of F_k in F_n $(k < n)$;
$P \cap F_k$	restriction of a place $P \in \mathbb{P}(F_n)$ to F_k $(n > k)$.

We recall some properties of the function fields $F_i/\mathbb{F}_{q^2}$ (see [2, Lemmas 2.1, 2.2]).

Lemma 2.1:

i) Suppose that a place $P \in \mathbb{P}(F_n)$ is a simple pole of x_n in F_n. Then the extension F_{n+1}/F_n has degree $[F_{n+1}: F_n] = q$ and P is totally ramified in F_{n+1}/F_n. The place $P' \in \mathbb{P}(F_{n+1})$ lying above P is a simple pole of x_{n+1}.

ii) For all $n \geq 1$ there is a unique place $Q_n \in \mathbb{P}(F_n)$ which is a common zero of the functions $x_1, z_2, z_3, \cdots, z_n$. Its degree is $\deg Q_n = 1$. For $1 \leq k \leq n$, the place Q_n is also a zero of x_k, and we have $v_{Q_n}(x_k) = q^{k-1}$. In the extension F_{n+1}/F_n the place Q_n splits into q places of F_{n+1} of degree one (one of them being Q_{n+1}).

We introduce the following sets of places and divisors:

Definition 2.2: See Fig. 1.

i) For $n \geq 3$, let

$$S_0^{(n)} := \{P \in \mathbb{P}(F_n) | P \cap F_{n-1} = Q_{n-1} \text{ and } P \neq Q_n\}$$

and

$$D_0^{(n)} := \sum_{P \in S_0^{(n)}} P.$$

ii) For $1 \leq i \leq \lfloor (n-3)/2 \rfloor$, let

$$S_i^{(n)} := \{P \in \mathbb{P}(F_n) | P \cap F_{n-1} \in S_{i-1}^{(n-1)}\}$$

and

$$D_i^{(n)} := \sum_{P \in S_i^{(n)}} P.$$

iii) Let

$$T^{(2)} := \{P \in \mathbb{P}(F_2) | P \cap F_1 = Q_1 \text{ and } P \neq Q_2\}$$

and

$$E^{(2)} := \sum_{P \in T^{(2)}} P$$

and for $n \geq 3$, let

$$T^{(n)} := \{P \in \mathbb{P}(F_n) | P \cap F_{n-1} \in T^{(n-1)}\}$$

and

$$E^{(n)} := \sum_{P \in T^{(n)}} P.$$

iv) For $n \geq 4$ and $n \equiv 0 \bmod 2$, let

$$U_{n-1}^{(n)} := \{P \in \mathbb{P}(F_n) | P \cap F_{n-1} \in S_{(n-4)/2}^{(n-1)}\}$$

and

$$M_{n-1}^{(n)} := \sum_{P \in U_{n-1}^{(n)}} P$$

and for $n \geq 5$ and $1 \leq i \leq \lfloor (n-2)/2 \rfloor$, let

$$U_{2i+1}^{(n)} := \{P \in \mathbb{P}(F_n) | P \cap F_{n-1} \in U_{2i+1}^{(n-1)}\}$$

and

$$M_{2i+1}^{(n)} := \sum_{P \in U_{2i+1}^{(n)}} P.$$

v) Let $P_\infty \in \mathbb{P}(F_1)$ denote the pole of x_1 in F_1 and for $n \geq 2$, let $P_\infty^{(n)}$ be the unique extension of P_∞ in F_n.

III. Sequences of Asymptotically Good Codes and their Duals

Definition 3.1: For $\alpha \in \mathbb{F}_{q^2}$ we denote the zero of $x_1 - \alpha$ in F_1 by P_α. We define

$$\begin{aligned}
D^{(1)} &:= \sum_{\alpha \in \mathbb{F}_{q^2}} P_\alpha \\
G^{(1)} &:= sP_\infty \\
D^{(2)} &:= Q_2 + E^{(2)} + \sum_{\alpha \in \mathbb{F}_{q^2} \setminus \{0\}} \mathrm{con}_{F_2/F_1}(P_\alpha) \\
G^{(2)} &:= sP_\infty^{(2)} \quad \text{with } 0 \leq s \leq q^3 + q^2 - q - 2
\end{aligned}$$

and for $n \geq 3$

$$\begin{aligned}
D^{(n)} &:= Q_n + D_0^{(n)} + \sum_{\alpha \in \mathbb{F}_{q^2} \setminus \{0\}} \mathrm{con}_{F_n/F_1}(P_\alpha) \\
G^{(n)} &:= \sum_{i=1}^{\lfloor (n-3)/2 \rfloor} m_i M_{2i+1}^{(n)} + rE^{(n)} + sP_\infty^{(n)}
\end{aligned}$$

where

$$\begin{aligned}
&0 \leq m_i \leq q^{n-2i-1}, \quad \text{for } 1 \leq i \leq \left\lfloor \frac{n-3}{2} \right\rfloor \\
&0 \leq r \leq q^{n-1} + q^{n-2} - q - 2 \\
&0 \leq s \leq q^{n+1} + q^n - q - 2.
\end{aligned}$$

Definition 3.2: For $i \geq 1$ we define the algebraic geometric codes

$$C_i := C_{\mathcal{L}}(D^{(i)}, G^{(i)}).$$

Observe that the codes C_1 are generalized Reed–Solomon codes and the codes C_2 are Hermitian codes (see [6]).

For $i \geq 3$ and $2g_i - 2 < \deg G^{(i)} < (q^2-1)q^{i-1} + q$ the code C_i is an $[n_i, k_i, d_i]$ code of length $n_i = (q^2-1)q^{i-1} + q$, dimension $k_i = \deg\ G^{(i)} + 1 - g_i$ and minimum distance $d_i \geq n_i - \deg G^{(i)}$, where

$$\deg\ G^{(i)} = (q-1) \sum_{j=1}^{\lfloor (i-3)/2 \rfloor} m_j q^j + (q-1)r + s$$

and (see [2, Theorem 2.10])

$$g_i = \begin{cases} q^i + q^{i-1} - q^{(i+1)/2} - 2q^{(i-1)/2} + 1, & \text{if } i \equiv 1 \bmod 2 \\ q^i + q^{i-1} - \frac{1}{2} q^{(i/2)+1} & \\ \quad - \frac{3}{2} q^{i/2} - q^{(i/2)-1} + 1, & \text{if } i \equiv 0 \bmod 2. \end{cases}$$

Thus for the codes we get

$$\frac{d_i}{n_i} + \frac{k_i}{n_i} \geq 1 + \frac{1}{n_i} - \frac{g_i}{n_i}$$

and the right-hand side is $1 - 1/q$ in the limit as $i \to \infty$, which exactly is the Tsfasman–Vlăduţ–Zink bound.

In the following, we want to determine the dual codes of the codes $C_i, i \geq 3$. From [6, Proposition II.2.10], we know that $C_i^\perp$ is again an algebraic geometric code $C_{\mathcal{L}}(D^{(i)}, H^{(i)})$ with

$$H^{(i)} = D^{(i)} - G^{(i)} + (\eta_i) \tag{2}$$

where η_i is a Weil differential of $F_i/\mathbb{F}_{q^2}$ such that

$$v_P(\eta_i) = -1 \quad \text{and} \quad \eta_{i_P}(1) = 1 \quad \text{for all } P \leq D^{(i)} \tag{3}$$

(η_{i_P} is the local component of η_i at the place P).

In order to determine the codes $C_i^\perp$ we therefore have to find a Weil differential of F_i with the property (3) and to determine its divisor. Since the divisor of such a differential depends on the different of F_i/F_1, we first compute the different.

Proposition 3.3: For $n \geq 2$ we have

$$\mathrm{Diff}\,(F_n/F_1) = (q-1)(q+2) \left(\sum_{j=1}^{\lfloor (n-3)/2 \rfloor} \sum_{l=0}^{n-2j-3} q^l M_{2j+1}^{(n)} + \sum_{i=0}^{n-3} q^i E^{(n)} + \sum_{i=0}^{n-2} q^i P_\infty^{(n)} \right).$$

Proof: For $n \geq 2$ we have for the different (see [6, Corollary III.4.11])

$$\mathrm{Diff}\,(F_n/F_1) = \mathrm{Diff}\,(F_n/F_{n-1}) + \mathrm{con}_{F_n/F_{n-1}}\,(\mathrm{Diff}\,(F_{n-1}/F_1)).$$

By [2], all places of F_{n-1} appearing in the different of F_{n-1} over F_1 are totally ramified in F_n, and $\mathrm{Diff}\,(F_2/F_1) = (q-1)(q+2)P_\infty^{(2)}$ and for $n \geq 3$

$$\mathrm{Diff}\,(F_n/F_{n-1}) = (q-1)(q+2) \cdot \left(\sum_{j=1}^{\lfloor (n-3)/2 \rfloor} M_{2j+1}^{(n)} + E^{(n)} + P_\infty^{(n)} \right).$$

The proposition now follows by induction. □

Next we determine the principal divisor $(x_1)^{(n)}$ of x_1 in F_n.

Lemma 3.4: For $n \geq 3$ we have

$$(x_1)^{(n)} = Q_n + \sum_{i=0}^{\lfloor (n-3)/2 \rfloor} D_i^{(n)} + \sum_{i=1}^{\lfloor (n-2)/2 \rfloor} q^{n-2-2i} M_{2i+1}^{(n)} + q^{n-2}E^{(n)} - q^{n-1}P_\infty^{(n)}.$$

Proof: By Lemma 2.1 and Definition 2.2 we obviously get

$$(x_1)^{(2)} = Q_2 + E^{(2)} - qP_\infty^{(2)}$$

and

$$(x_1)^{(3)} = Q_3 + D_0^{(3)} + qE^{(3)} - q^2P_\infty^{(3)}.$$

Observing that for $n \geq 4$ and $n \equiv 0 \bmod 2$ we have $U_{n-1}^{(n)} = S_{((n-4)/2)+1}^{(n)}$, the assertion follows immediately by induction. □

Lemma 3.5: Let $z := x_1^{q^2} - x_1$. Then for $n \geq 2$

i) $$(z)^{(n)} = D^{(n)} + \sum_{i=1}^{\lfloor (n-3)/2 \rfloor} D_i^{(n)} + \sum_{i=1}^{\lfloor (n-2)/2 \rfloor} q^{n-2i-2} M_{2i+1}^{(n)} + q^{n-2}E^{(n)} - q^{n+1}P_\infty^{(n)}$$

ii) $$(dz)^{(n)} = (q-1)(q+2) \cdot \left(\sum_{j=1}^{\lfloor (n-3)/2 \rfloor} \sum_{l=0}^{n-2j-3} q^l M_{2j+1}^{(n)} + \sum_{i=0}^{n-3} q^i E^{(n)} \right) + \left((q-1)(q+2) \sum_{i=0}^{n-2} q^i - 2q^{n-1} \right) P_\infty^{(n)}.$$

Proof:

i) is an immediate consequence of Lemma 3.4.

ii) For the differential dz we have

$$dz = d(x_1^{q^2} - x_1) = -dx_1$$

and therefore for its divisor in $F_n, (dz)^{(n)} = (dx_1)^{(n)}$. By [6, Remark IV.3.7.(c)]

$$(dx_1)^{(n)} = -2(x_1)_\infty^{(n)} + \mathrm{Diff}\,(F_n/F_1)$$

and we obtain the assertion from Proposition 3.3. □

Obviously $z^{-1}dz$ is a Weil differential of $F_n/\mathbb{F}_{q^2}$ with property (3), and hence we get with (2) and Lemma 3.5 the following result for the dual codes of the codes $C_i, i \geq 3$:

Theorem 3.6: For $i \geq 3$ we have

$$C_\mathcal{L}(D^{(i)}, G^{(i)})^\perp = C_\mathcal{L}(D^{(i)}, H^{(i)})$$

with

$$H^{(i)} = \sum_{j=1}^{\lfloor (i-3)/2 \rfloor} \mu_j M_{2j+1}^{(i)} + \rho E^{(i)} + \sigma P_\infty^{(i)} - \sum_{j=1}^{\lfloor (i-3)/2 \rfloor} D_j^{(i)} - \delta_i M_{i-1}^{(i)}$$

where

$$\delta_i = \begin{cases} 1, & \text{if } i \equiv 0 \bmod 2 \\ 0, & \text{if } i \equiv 1 \bmod 2. \end{cases}$$
$$\sigma = q^{i+1} + q^i - q - 2 - s$$
$$\rho = q^{i-1} + q^{i-2} - q - 2 - r$$
$$\mu_j = q^{i-2j-1} - q - 2 - \mu_j \quad \text{for } 1 \leq j \leq \left\lfloor \frac{i-3}{2} \right\rfloor.$$

Remark 3.7: It is well known that the dual code of a Hermitian code C_2 again is a Hermitian code, namely, for $0 \leq s \leq q^3 + q^2 - q - 2$ one has (see [6, Proposition VII.4.2])

$$C_\mathcal{L}(D^{(2)}, sP_\infty^{(2)})^\perp = C_\mathcal{L}(D^{(2)}, \sigma P_\infty^{(2)}) \quad \text{with } \sigma = q^3 + q^2 - q - 2 - s.$$

From Theorem 3.6 we get a similar result for the codes C_3, that is

$$C_\mathcal{L}(D^{(3)}, rE^{(3)} + sP_\infty^{(3)})^\perp = C_\mathcal{L}(D^{(3)}, \rho E^{(3)} + \sigma P_\infty^{(3)})$$

with $\rho = q^2 - 2 - r$ and $\sigma = q^4 + q^3 - q - 2 - s$.

For $i \geq 4$ it is not completely true that the dual codes are of the same type as the codes C_i, since the divisors $H^{(i)}$ prescribe in addition some zeros for the functions.

IV. The Codes Related to $F_3/\mathbb{F}_{q^2}$

Our next aim is to describe the codes corresponding to $F_3/\mathbb{F}_{q^2}$ explicitely which means that we want to determine a basis for a space $\mathcal{L}(G^{(3)})$ and a generator matrix for C_3. Since we are only dealing with the codes related to F_3, we set

$$P_\infty := P_\infty^{(3)} \qquad E := E^{(3)} \qquad D_0 := D_0^{(3)} \qquad D := D^{(3)}$$
$$G(r,s) := G^{(3)}$$

where

$$0 \leq r \leq q^2 - 2 \quad 0 \leq s \leq q^4 + q^3 - q - 2$$

and

$$2q^3 - 4q \leq (q-1)r + s < q^4 - q^2 + q.$$

Then by Definition 3.2

$$C(r,s) := C_\mathcal{L}(D, G(r,s))$$

is an $[n,k,d]$ code with

$$n = q^4 - q^2 + q, \quad k = (q-1)r + s - q^3 + 2q$$

and

$$d \geq q^4 - q^2 + q - (q-1)r - s. \tag{4}$$

We want to construct a basis of $\mathcal{L}(G(r,s))$ where all elements are of the form

$$x_1^{i_1}x_2^{i_2}z_3^{j} \quad \text{with} \quad i_1, i_2, j \in \mathbb{Z}.$$

With Lemma 2.1 we get for the principal divisors of x_1, x_2, and z_3 in F_3

$$\left.\begin{array}{l}(x_1) = Q_3 + D_0 + qE - q^2P_\infty\\ (x_2) = qQ_3 + qD_0 - qE - qP_\infty\\ (z_3) = q(q+1)Q_3 - (q+1)E - (q+1)P_\infty\end{array}\right\} \tag{5}$$

and from the valuations of x_1, x_2, and z_3 at the different places we get the conditions on the exponents i_1, i_2, j such that $x_1^{i_1}x_2^{i_2}z_3^{j} \in \mathcal{L}(G(r,s))$. The difficult part is to find enough linearly independent elements of that form.

Definition 4.1: We define the following sets:

$$\begin{aligned}I_1(r,s) := \{(i_1,i_2,j) | &0 \le i_1, 0 \le i_2, j \le q-1,\\ &i_2q + j(q+1) \le s - i_1q^2,\\ &i_2q + j(q+1) \le r + i_1q\}\\ I_2(r,s) := \{(i_1,-i_2,j) | &1 \le i_2 \le q, i_1 \ge i_2q, 0 \le j \le q-1,\\ &j(q+1) \le s + i_2q - i_1q^2,\\ &j(q+1) \le r + i_2q + i_1q,\\ &(i_1-1, -i_2+q, j) \notin I_1(r,s)\}\\ I_3(r,s) := \{(-i_1,i_2,j) | &1 \le i_1, 1 \le i_2 \le q-1,\\ &i_2q \ge i_1, 0 \le j \le q-1,\\ &i_2q + j(q+1) \le s + i_1q^2,\\ &i_2q + j(q+1) \le r - i_1q\}\\ I(r,s) := I_1(r,s) \cup &I_2(r,s) \cup I_3(r,s)\end{aligned}$$

Lemma 4.2: For $i_1, l_1 \in \mathbb{Z}$ and $0 \le i_2, l_2, j, k \le q-1$ we have

$$i_1q^2 + i_2q + j(q+1) = l_1q^2 + l_2q + k(q+1) \Leftrightarrow (i_1,i_2,j) = (l_1,l_2,k).$$

Proof: Trivial. □

Theorem 4.3: The set

$$B(r,s) := \{x_1^{i_1}x_2^{i_2}z_3^{j} | (i_1,i_2,j) \in I(r,s)\}$$

is a basis of $\mathcal{L}(G(r,s))$ over $\mathbb{F}_{q^2}$.

Proof: Using (5) and Definition 4.1 one can easily verify that

$$(x_1^{i_1}x_2^{i_2}z_3^{j}) \ge -G(r,s) \quad \text{for} \quad (i_1,i_2,j) \in I(r,s)$$

which means that $B(r,s) \subseteq \mathcal{L}(G(r,s))$.

Let $u = x_1^{i_1}x_2^{i_2}z_3^{j} \in B(r,s)$. Then

$$-v_{P_\infty}(u) = i_1q^2 + i_2q + j(q+1)$$

and from Lemma 4.2 we obtain that all elements in $B(r,s)$ have different orders at P_∞, which implies that they are linearly independent. (Observe that for $(i_1,i_2,j) \in I_2(r,s)$ we have $(i_1-1, i_2+q, j) \notin I_1(r,s)$ and $i_1q^2 + i_2q + j(q+1) = (i_1-1)q^2 + (i_2+q)q^2 + j(q+1)$.)

Since the dimension of $C(r,s)$ is $k = (q-1)r + s - q^3 + 2q$ (see (4)) it remains to prove that $\#I(r,s) = k$. In order to count the elements of $I(r,s)$ we need some preparations.

Definition 4.4: For $l \in \mathbb{Z}$ we define

i) $$h(l) := \#\{(i,j) | 0 \le i, 0 \le j \le q-1, iq + j(q+1) \le l\}$$

ii) $$\mu(l) := \begin{cases} 0, & \text{if } l \le 0\\ \left\lfloor \dfrac{l}{q+1} \right\rfloor + 1, & \text{if } 0 \le l < q^2-1\\ q, & \text{if } l \ge q^2-1.\end{cases}$$

For $l \ge q^2 - q - 1$ we have (see [6, p. 212)

$$h(l) = l + 1 - \tfrac{1}{2}q(q-1) \tag{6}$$

and it is easy to check that for $l \ge 0$

$$h(l) + \mu(l+q) = h(l+q). \tag{7}$$

Now we set (for r and s as usual)

$$a := \left\lfloor \frac{s-r}{q(q+1)} \right\rfloor \qquad d := \left\lfloor \frac{a}{q} \right\rfloor \qquad \text{and} \quad c := \left\lfloor \frac{s}{q(q^2-1)} \right\rfloor.$$

Lemma 4.5:

i) $c - 1 \le d \le c$, if $c < q$ or $r \ne 1$.

ii) $d = q-2$ if $c = q$ and $r = 1$.

iii) If $d = 0$ then

$$\begin{aligned} &a = q-1 \quad \text{and} \quad r \ge q^2 - q - 3, \quad \text{or}\\ &a = q-2 \quad \text{and} \quad r = q^2 - 2, \quad \text{or}\\ &c = q = 2 \quad \text{and} \quad a = r = 1.\end{aligned}$$

Proof: We write $s = cq(q^2-1) + \beta$ with $0 \le \beta < q^3 - q$. Recall that

$$2q^3 - 4q < (q-1)r + s < q^4 - q^2 + q.$$

From this follows that $1 \le c \le q$, and if $c = q$ then $r = 0$ and $\beta < q$, or $r = 1$ and $\beta = 0$. If $c < q$, then

$$((q-1)/q)c - 1/q \le a/q \le ((q-1)/q)(c+1)$$

thus $c - 1 \le d \le c$. i) and ii) now follow immediately.

Suppose $d = 0$. i) and ii) yield either $c = 2 = q$ and $r = 1 = a$ or $c = 1$. For $c = 1$ we have

$$a = q - 1 + \lfloor (\beta - r)/q(q+1) \rfloor$$

and

$$s = q^3 - q + \beta > 2q^3 - 4q - (q-1)r$$

that implies

$$a > q-2+(q^2-3-r)/(q+1) = 2q-3-(r+2)/(q+1) \ge q-2$$

and since $d = 0$ also $a \le q-1$. If $a = q-1$, then

$$q^2 + q > \beta - r > q^3 - 3q - qr$$

hence $r \ge q^2 - q - 3$, and if $a = q-2$, then

$$0 > \beta - r > q^3 - 3q - qr$$

hence $r = q^2 - 2$. □

Definition 4.6: We define the set

$$J(r,s) := \{(i_1,-i_2,j) | 1 \le i_2 \le q, i_1 \ge i_2 q, 0 \le j \le q-1,\\ j(q+1) \le s + i_2 q - i_1 q^2,\\ j(q+1) \le r + i_2 q + i_1 q\}.$$

The following remark is easy to check.

Remark 4.7:

i) $I_2(r,s) = J(r,s) \backslash J(r-q^2-q, s)$

ii) $r + iq \le s - iq^2 \Leftrightarrow i \le a$

iii) $h(r-q) = h\left(r - \left\lfloor \frac{r}{q} \right\rfloor q\right) + \sum_{i=1}^{\lfloor r/q \rfloor -1} \mu(r-iq)$ for $r \ge 2q$.

With Remark 4.7 ii) and Definition 4.4 i) we obtain

$$\begin{aligned}\#I_1(r,s) &= \sum_{i=0}^{a}(h(r+iq) - h(r-q^2+iq))\\ &\quad + \sum_{i=a+1}^{\lfloor s/q^2 \rfloor}(h(s-iq^2) - h(s-(i+1)q^2))\\ &= h(s-(a+1)q^2) + \sum_{i=0}^{a}(h(r+iq)\\ &\quad - h(r-q^2+iq)).\end{aligned} \tag{8}$$

(Observe that in the definition of $I_1(r,s)$ we have $i_2 \le q-1$.)

By Remark 4.7 i), ii) and Definition 4.4 ii) follows

$$\begin{aligned}\#I_2(r,s) &= \sum_{i_2=1}^{d}\left(\sum_{i_1=i_2 q}^{a}\mu(r+i_2 q+i_1 q) - \sum_{i_1=i_2 q}^{a+1}\mu(r-(q^2+q)+i_2 q+i_1 q)\right)\\ &\quad + \sum_{i_2=1}^{d}\left(\sum_{i_1=a+1}^{\lfloor (s+i_2 q)/q^2 \rfloor}\mu(s+i_2 q-i_1 q^2) - \sum_{i_1=a+2}^{\lfloor (s+i_2 q)/q^2 \rfloor}\mu(s+i_2 q-i_1 q^2)\right) + \epsilon(a)\end{aligned}$$

where

$$\epsilon(a) = \begin{cases} \mu(s-(d+1)q(q^2-1)) - \mu(r+d(q^2+q)), & \text{if } d < c \text{ and } a \equiv -1 \bmod q\\ 0, & \text{else.}\end{cases}$$

Thus by (7)

$$\begin{aligned}\#I_2(r,s) &= h(s+dq-(a+1)q^2) - h(s-(a+1)q^2)\\ &\quad + \epsilon(a) - h(r-q+d(q^2+q))\\ &\quad + h(r-q) + \sum_{i=1}^{d}(h(r+aq+iq)\\ &\quad - h(r-q^2+aq+iq)).\end{aligned} \tag{9}$$

Finally, from Remark 4.7 iii) we get

$$\#I_3(r,s) = \sum_{i=2}^{\lfloor r/q \rfloor} h(r-iq). \tag{10}$$

Lemma 4.8: For $d \ge 1$ we have

$$s + dq - (a+1)q^2 \ge q^2 - q - 1$$

and

$$r - q^2 + q + aq + dq \ge q^2 - q - 1$$

Proof: We write again $s = cq(q^2-1) + \beta$ with $0 \le \beta < q^3 - q$. As $d \ge 1$ and $(q-1)r + s > 2q^3 - 4q$ we have

$$\begin{aligned}&(q+1)(2q^2-q-1)\\ &\quad = 2q^3 + q^2 - 2q - 1 < qr + s + d(q^2+q) + q - 1\\ &\quad = (q+1)s + d(q^2+q) - q(cq(q^2-1)\\ &\qquad + \beta - r) + q - 1.\end{aligned}$$

Therefore,

$$\begin{aligned}2q^2 - q - 1 &\le s + dq - q^2\left(c(q-1) + \frac{\beta - r}{q(q+1)}\right)\\ &\le s + dq - aq^2\end{aligned}$$

and hence

$$s + dq - (a+1)q^2 \ge q^2 - q - 1.$$

Moreover,

$$\begin{aligned}&(q+1)(2q^2-2q-1)\\ &\quad = 2q^3 - 3q - 1 < qr + s + (d-1)(q^2+q) + q - 1\end{aligned}$$

thus

$$\begin{aligned}2q^2 - 2q - 1 &\le r + cq(q-1) + \frac{\beta - r}{q+1} + (d-1)q\\ &\le r + aq + dq\end{aligned}$$

which implies

$$r - q^2 + q + aq + dq \ge q^2 - q - 1. \qquad \square$$

The next proposition finishes the proof of Theorem 4.3.

Proposition 4.9:

$$\#I(r,s) = (q-1)r + s - q^3 + 2q.$$

Proof: First we consider the case $d \ge 1$. Using (8)–(10) we find

$$\begin{aligned}\#I(r,s) &= h(s+dq-(a+1)q^2) + \epsilon(a) - h(r-q+d(q^2+q))\\ &\quad + \sum_{i=0}^{d+a}(h(r+iq) - h(r-q^2+iq)) + \sum_{i=1}^{\lfloor r/q \rfloor} h(r-iq)\\ &= h(s+dq-(a+1)q^2) + \epsilon(a) - h(r-q^2+d(q^2+q))\\ &\quad + \sum_{i=1}^{q} h(r-q^2+dq+aq+iq)\end{aligned} \tag{11}$$

For $c > d$ and $a \equiv -1 \bmod q$ it is easy to verify by (7) that

$$\begin{aligned}&h(s+dq-(a+1)q^2) + \epsilon(a)\\ &\qquad = h(s+q+dq-(a+1)q^2) - q.\end{aligned}$$

The assertion for $d \geq 1$ is now an immediate consequence of (11), (6), and Lemma 4.8. Let now $d = 0$. Using (8)–(10), Lemma 4.5 iii), and (6) we obtain

$$\begin{aligned}
\#I(r,s) &= h(s-(a+1)q^2) + \epsilon(a) + \sum_{i=0}^{a} h(r+iq) \\
&\quad - \sum_{i=q-a}^{q} h(r-iq) + \sum_{i=2}^{\lfloor r/q \rfloor} h(r-iq) \\
&= \begin{cases} h(s-q^3+q) + \sum_{i=1}^{q-1} h(r+iq) \\ \qquad \text{if } a = q-1 \\ h(s-q^3+q^2) + \sum_{i=0}^{q-2} h(r+iq) \\ \qquad \text{if } a = q-2 \text{ and } c = 1 \\ h(4)+1+h(1)+h(3) \\ \qquad \text{if } c = q = 2 \end{cases} \\
&= (q-1)r + s - q^3 + 2q. \qquad \square
\end{aligned}$$

Corollary 4.10: The pole numbes of P_∞ in F_3 are of the form

$$i_1 q^2 + i_2 q + j(q+1) \quad \text{with } (i_1, i_2, j) \in \bigcup_{s \geq 0} I(0,s).$$

Example 4.11: It is well known that the pole numbers of P_∞ in the Hermitian function field are generated by q and $q+1$, which implies that the set generated by q^2 and $q(q+1)$ is a subset of the pole numbers of P_∞ in F_3. One would perhaps guess that there is just one other generator needed to get the whole set, but that is not true as the following examples show.

For $q = 2$ the generators are: $4, 6, 9, 11$.

For $q = 3$ the generators are: $9, 12, 22, 28, 32, 35$.

For $q = 4$ the generators are: $16, 20, 37, 58, 65, 70, 75, 79$.

Our next aim is to specify a generator matrix for the codes $C(r,s)$. First we introduce some new notations. We define for $\alpha \in \mathbb{F}_{q^2} \backslash \{0\}$ the set

$$M_\alpha := \{(\beta,\gamma) \in (\mathbb{F}_{q^2})^2 | \beta^q + \beta = \alpha^{q+1} \text{ and } \gamma^q + \gamma = (\alpha^{-1}\beta)^{q+1}\}.$$

For $\alpha \in \mathbb{F}_{q^2} \backslash \{0\}$ and $(\beta,\gamma) \in M_\alpha$ let $P_{\alpha\beta\gamma} \in \mathbb{P}(F_3)$ be the common zero of $x_1 - \alpha$, $z_2 - \beta$, and $z_3 - \gamma$. From the equations of the function fields F_2 and F_3 over $\mathbb{F}_{q^2}$ follows obviously that such places exist and that for $\alpha \in \mathbb{F}_{q^2} \backslash \{0\}$

$$\mathrm{con}_{F_3/F_1}(P_\alpha) = \sum_{(\beta,\gamma) \in M_\alpha} P_{\alpha\beta\gamma}.$$

We define moreover $M_0 := \{\epsilon \in \mathbb{F}_{q^2} | \epsilon^q + \epsilon = 0\}$ and $P_{00\epsilon} \in \mathbb{P}(F_3)$ the common zero of x_1, x_2, and $z_3 - \epsilon$ for $\epsilon \in M_0$. Now we can rewrite the divisor D as

$$D = \sum_{\epsilon \in M_0} P_{00\epsilon} + \sum_{\alpha \in \mathbb{F}_{q^2} \backslash \{0\}} \sum_{(\beta,\gamma) \in M_\alpha} P_{\alpha\beta\gamma}.$$

Next we fix some ordering on the set

$$M := \{(\alpha,\beta,\gamma) | P_{\alpha\beta\gamma} \leq D\}$$

and define for $m = i_1 q^2 + i_2 q + j(q+1)$ with $i_1, i_2, j \in \mathbb{Z}$ the vector

$$u_m := (u_{\alpha\beta\gamma})_{(\alpha,\beta,\gamma) \in M}$$

where

$$u_{\alpha\beta\gamma} := \begin{cases} \alpha^{i_1 - i_2} \beta^{i_2} \gamma^j, & \text{if } \alpha \neq 0 \\ 0, & \text{if } \alpha = 0 \text{ and } (i_1 \neq 0 \text{ or } i_2 \neq 0) \\ \gamma^j, & \text{if } \alpha = 0 \text{ and } i_1 = i_2 = 0. \end{cases}$$

Corollary 4.12: Let

$$\{m_l\}_{l=1}^k = \{i_1 q^2 + i_2 q + j(q+1) | (i_1, i_2, j) \in I(r,s)\}$$

with $m_l < m_{l+1}$ for $1 \leq l \leq k-1$. Then the $k \times (q^4 - q^2 + q)$ matrix whose rows are $u_{m_1}, \cdots, u_{m_k}$ is a generator matrix of $C(r,s)$.

Proof: This is an immediate consequence of Theorem 4.3 and the fact, that for $u = x_1^{i_1} x_2^{i_2} z_3^j \in B(r,s)$ we have $u(P_{\alpha\beta\gamma}) = u_{\alpha\beta\gamma}$.

The codes from F_3 considered here are better than BCH codes, and are comparable with the codes coming from the function field studied by Petersen and Sørensen in [5]. These codes over $\mathbb{F}_{q^2}$ have $n = q^4$ and

$$k + d \geq q^4 - \tfrac{1}{2}q^3 + \tfrac{1}{2}q + 1$$

where the codes we consider have $n = q^4 - q^2 + q$ and $k + d \geq q^4 - q^3 - q^2 + 3q$.

Finally, we give an example showing that one cannot find analogous bases for the spaces $\mathcal{L}(G^{(i)})$ with $i \geq 4$. By an analogous basis we mean a set of linearly independent functions of the form

$$f = \prod_{l=1}^{i-1} x_l^{i_l} z_i^j \in \mathcal{L}(G^{(i)}). \tag{12}$$

Example 4.13: We consider the function field $F_4/\mathbb{F}_4$. Its genus is $g_4 = 13$ and the pole numbers of the functions $f \in \mathcal{L}(24P_\infty^{(4)})$ that are of the form (12) are

$$0, 8, 12, 16, 18, 20, 22, 23, 24.$$

From the Weierstrass Gap Theorem (see [6, Theorem I.6.7]) we see that three pole numbers are missing.

Remark 4.14: Already in this simple example we see, that the functions of the type (12) only generate a subspace of $\mathcal{L}(G^{(i)})$ for $i \geq 4$. An idea could be to consider sequences of subcodes of the codes C_i in Definition 3.2 replacing the spaces $\mathcal{L}(G^{(i)})$ by the largest subspaces generated by functions as in (12). However, after computing many examples of such subcodes in F_4 and F_5, to us such an attempt appears not very promising, since we got the impression that those subcodes are asymptotically bad.

References

[1] V. G. Drinfeld and S. G.Vlăduţ, "Number of points of an algebraic curve" *Func. Anal.*, vol. 17, pp. 53–54, 1983.

[2] A. Garcia and H. Stichtenoth, "A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vlăduţ bound," *Inventiones Math.*, vol. 121, pp. 211–222, 1995.

[3] Y. Ihara, "Some remark on the number of rational points of algebraic curves over finite fields," *J. Fac. Sci. Tokyo*, vol. 28, pp. 721–724, 1981.

[4] G. L. Katsman, M. A. Tsfasman, and S. G. Vlăduţ," Modular curves and codes with a polynomial construction," *IEEE-Trans. Inform. Theory*, vol. IT-30, no. 2, pp. 353–355, Mar. 1984.

[5] J. P. Pedersen and A. B. Sørensen," "Codes from certain algebraic function fields with many rational places," MAT-Rep. 1990-11, Mathematical Institute, The Technical University of Denmark, Lyngby, 1990.

[6] H. Stichtenoth, *Algebraic Function Fields and Codes* (Springer Universitext). Berlin-Heidelberg-New York: Springer, 1993.

[7] M. A. Tsfasman and S. G. Vlăduţ,*Algebraic-Geometric Codes*. Dordrecht–Boston–London: Kluwer, 1991.

[8] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, "Modular curves, Shimura curves and Goppa codes, better than the Varshamov–Gilbert bound," *Math. Nachr.*, vol. 109, pp. 21–28, 1982.

[9] S. G. Vlăduţ and Y. I. Manin, "Linear codes and modular curves, *J. Sov. Math.*, vol. 30, pp. 2611–2643, 1985.

[10] G. L. Feng and T. R. N. Rao, "Improved geometric Goppa codes, part II. Generalized Klein codes," preprint.