Transitive and Self-Dual Codes Attaining the Tsfasman–Vlăduţ–Zink Bound

Henning Stichtenoth

***Abstract*—A major problem in coding theory is the question of whether the class of cyclic codes is asymptotically good. In this correspondence—as a generalization of cyclic codes—the notion of *transitive* codes is introduced (see Definition 1.4 in Section I), and it is shown that the class of transitive codes is asymptotically good. Even more, transitive codes attain the Tsfasman–Vlăduţ–Zink bound over $\mathbb{F}_q$, for all squares $q = l^2$. It is also shown that self-orthogonal and self-dual codes attain the Tsfasman–Vlăduţ–Zink bound, thus improving previous results about self-dual codes attaining the Gilbert–Varshamov bound. The main tool is a new asymptotically optimal tower $E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots$ of function fields over $\mathbb{F}_q$ (with $q = l^2$), where all extensions E_n/E_0 are Galois.**

***Index Terms*—Asymptotically good codes, cyclic codes, self-dual codes, towers of function fields, transitive codes, Tsfasman–Vlăduţ–Zink bound.**

I. Introduction and Main Results

Let $\mathbb{F}_q$ be the finite field of cardinality q. In this correspondence, we consider primarily *linear* $[n, k, d]$-codes C over $\mathbb{F}_q$; i.e., the parameters $n = n(C)$, $k = k(C)$ and $d = d(C)$ are the *length*, the *dimension* and the *minimum distance* of the code. The ratios $R = R(C) = k(C)/n(C)$ and $\delta = \delta(C) = d(C)/n(C)$ denote the *information rate* and the relative minimum distance (error detection rate), respectively, of the code.

A crucial role in asymptotic theory of codes is played by the set $U_q \subseteq [0,1] \times [0,1]$ which is defined as follows: a point $(\delta, R) \in \mathbb{R}^2$ with $0 \le \delta \le 1$ and $0 \le R \le 1$ belongs to U_q if and only if there exists a sequence $(C_i)_{i \ge 0}$ of codes over $\mathbb{F}_q$ such that

$$n(C_i) \to \infty,\ \delta(C_i) \to \delta \text{ and } R(C_i) \to R, \text{ as } i \to \infty.$$

One then defines the function $\alpha_q : [0,1] \to [0,1]$ by

$$\alpha_q(\delta) = \sup\{R; (\delta, R) \in U_q\}, \text{ for } \delta \in [0,1].$$

The following facts are well-known (and easy to prove), see [9], [20].

Proposition 1.1:

1) A point $(\delta, R) \in [0,1] \times [0,1]$ belongs to the set U_q if and only if $0 \le R \le \alpha_q(\delta)$.
2) The function α_q is continuous and nonincreasing.
3) $\alpha_q(0) = 1$, and $\alpha_q(\delta) = 0$ for $1 - q^{-1} \le \delta \le 1$.

Many *upper bounds* for $\alpha_q(\delta)$ are known, see [8], [20]. Arguably more interesting, however, are *lower bounds* for $\alpha_q(\delta)$, since any nontrivial lower bound assures the existence of arbitrarily long linear codes with good error correction parameters. The classical lower bound for $\alpha_q(\delta)$ is the asymptotic Gilbert–Varshamov bound, which says the following.

Proposition 1.2: (see [8]). For all $\delta \in (0, 1 - q^{-1})$ one has

$$\alpha_q(\delta) \ge 1 - \delta \log_q(q-1) + \delta \log_q(\delta) + (1-\delta)\log_q(1-\delta).$$

For sufficiently large nonprime q and for certain ranges of the variable δ, the Gilbert–Varshamov bound is improved by the *Tsfasman–Vlăduţ–Zink bound* as follows.

Proposition 1.3: (see [21], [14]). Let

$$A(q) = \lim\sup_{g \to \infty} N_q(g)/g$$

where $N_q(g)$ denotes the maximum number of rational places that a function field $F/\mathbb{F}_q$ of genus g can have. Then

$$\alpha_q(\delta) \ge 1 - \delta - A(q)^{-1} \text{ for } 0 \le \delta \le 1.$$

It is well known that $A(q) \le q^{1/2} - 1$ (this is the *Drinfeld–Vladut bound*), and $A(q) = q^{1/2} - 1$ if q is a square, see [7], [21], [4]. It then follows easily that the Tsfasman–Vlăduţ–Zink bound in Proposition 1.3 improves the Gilbert–Varshamov bound for all squares $q \ge 49$ and all δ in a large subinterval of $[0,1]$. For *nonlinear codes* over $\mathbb{F}_q$, the Tsfasman–Vlăduţ–Zink bound was further improved recently, see [22], [12], [13], [19], [1], [2].

In order to prove the Gilbert–Varshamov and Tsfasman–Vlăduţ–Zink bounds one constructs families of long codes with sufficiently good parameters. However, the proofs provide linear codes without any particular structure. For instance, one of the most challenging problems in coding theory is still open (see [15], [10]): Do there exist sequences $(C_i)_{i \ge 0}$ of *cyclic codes* C_i over $\mathbb{F}_q$ with

$$n(C_i) \to \infty,\ \lim_{i \to \infty} R(C_i) > 0 \text{ and } \lim_{i \to \infty} \delta(C_i) > 0\ ?$$

Cyclic codes can be understood as a special case of what we call in this correspondence *transitive codes*. Recall that a subgroup U of the symmetric group S_n is called *transitive* if for any pair (i, j) with $i, j \in \{1, \ldots, n\}$ there is a permutation $\pi \in U$ such that $\pi(i) = j$. A permutation $\pi \in S_n$ is called an *automorphism* of the code $C \subseteq \mathbb{F}_q^n$ if

$$(c_1, \ldots, c_n) \in C \Rightarrow (c_{\pi(1)}, \ldots, c_{\pi(n)}) \in C$$

holds for all codewords $(c_1, \ldots, c_n) \in C$. The *automorphism group* $\mathrm{Aut}(C) \subseteq S_n$ is the group of all automorphisms of the code C.

Definition 1.4: A code C over $\mathbb{F}_q$ of length n is said to be *transitive* if its automorphism group $\mathrm{Aut}(C)$ is a transitive subgroup of S_n.

It is obvious that any cyclic code is transitive. We can now state our first result.

Theorem 1.5: Let $q = \ell^2$ be a square. Then the class of transitive codes meets the Tsfasman–Vlăduţ–Zink bound. More precisely, let $R, \delta \ge 0$ be real numbers with $R = 1 - \delta - 1/(\ell - 1)$. Then there exists a sequence $(C_j)_{j \ge 0}$ of linear codes C_j over $\mathbb{F}_q$ with parameters $[n_j, k_j, d_j]$ with the following properties:

1) all C_j are transitive codes;
2) $n_j \to \infty$ as $j \to \infty$;
3) $\lim_{j \to \infty} k_j/n_j \ge R$ and $\lim_{j \to \infty} d_j/n_j \ge \delta$.

Other important classes of codes are the *self-orthogonal codes* and the *self-dual codes*. Recall that a linear code C is called self-orthogonal if C is contained in its dual code $C^\perp$, and C is called self-dual if $C = C^\perp$. It is clear that the information rate of self-orthogonal codes satisfies $R(C) \le 1/2$; the information rate of self-dual codes is $R(C) = 1/2$. It is well-known that self-dual codes attain the Gilbert–Varshamov bound, see [11]. In this correspondence we will prove the following.

Theorem 1.6: Let $q = \ell^2$ be a square. Then the class of self-orthogonal codes and the class of self-dual codes meet the Tsfasman–Vlăduţ–Zink bound. More precisely, we have the following holds.

1) Let $0 \le R \le 1/2$ and $\delta \ge 0$ with $R = 1 - \delta - 1/(\ell - 1)$. Then there is a sequence $(C_j)_{j \ge 0}$ of linear codes C_j over $\mathbb{F}_q$ with parameters $[n_j, k_j, d_j]$ such that the following:
   a) all C_j are self-orthogonal codes;
   b) $n_j \to \infty$ as $j \to \infty$;
   c) $\lim_{j \to \infty} k_j/n_j \ge R$ and $\lim_{j \to \infty} d_j/n_j \ge \delta$.

Manuscript received May 26, 2005; revised November 9, 2005.

The author is with Sabanci University, MDBF, Orhanli 34956 Tuzla, Istanbul, Turkey, and also with Fachbereich Mathematik, University of Duisburg-Essen, 45117 Essen, Germany (e-mail: henning@sabanciuniv.edu).

Communicated by A. Ashikhmin, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2006.872986

2) There is a sequence $(C_j)_{j\geq 0}$ of self-dual codes C_j over $\mathbb{F}_q$ with parameters $[n_j, n_j/2, d_j]$ such that $n_j \to \infty$ and

$$\lim_{j\to\infty} d_j/n_j \geq 1/2 - 1/(\ell - 1).$$

Note that the bounds given in Theorem 1.5 and Theorem 1.6 are better than the Gilbert–Varshamov bound, for all squares $q = \ell^2 \geq 49$ and all δ in a large subinterval of $[0, 1]$.

The main tool to prove Theorem 1.5 and Theorem 1.6 is a new asymptotically good tower of function fields over $\mathbb{F}_q$ which has particularly nice properties, see Theorem 1.7. Using that tower, we will construct sequences of codes over $\mathbb{F}_q$ with the desired properties, analogously to the proof of Proposition 1.3 by Tsfasman–Vlăduţ–Zink.

Before stating Theorem 1.7, we recall some notations from the theory of algebraic function fields, cf. [17].

– For a function field $F/\mathbb{F}_q$, we denote by $g(F)$ the genus and by $N(F)$ the number of rational places of F. For an element $u \in F \setminus \{0\}$, we denote by $(u)^F$, $(u)_0^F$ and $(u)_\infty^F$ the principal divisor, the zero divisor and the pole divisor, respectively, of the element u. In particular, we have $(u)^F = (u)_0^F - (u)_\infty^F$. The divisor of a differential $\mu \neq 0$ of $F/\mathbb{F}_q$ is denoted by $(\mu)^F$.
– Let $\mathbb{F}_q(x)$ be a rational function field; then we denote, for $\alpha \in \mathbb{F}_q$, by $(x = \alpha)$ the zero of the function $(x - \alpha)$ and by $(x = \infty)$ the pole of the function x in $\mathbb{F}_q(x)$.
– Let E/F be an extension of function fields over $\mathbb{F}_q$. Let P be a place of F and let Q be a place of E lying above P. Then $e(Q|P)$ and $d(Q|P)$ denote the ramification index and the different exponent, respectively, of $Q|P$. The different of E/F (which is a divisor of the function field E) is denoted by $\mathrm{Diff}(E/F)$.

Theorem 1.7: Let $q = \ell^2$ be a square. Then there exists an infinite tower $\mathcal{E} = (E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots)$ of function fields $E_i/\mathbb{F}_q$ with the following properties.

1) $\mathbb{F}_q$ is the full constant field of E_i, for all $i \geq 0$.
2) $E_0 = \mathbb{F}_q(z)$ is the rational function field.
3) There exists an element $w \in E_1$ such that $w^{\ell-1} = z$. So we have $E_0 = \mathbb{F}_q(z) \subseteq \mathbb{F}_q(w) \subseteq E_1$, and the extension $\mathbb{F}_q(w)/E_0$ is cyclic of degree $(\ell - 1)$.
4) All extensions E_n/E_0 are Galois, and the degree of E_n/E_0 is
$$[E_n : E_0] = (\ell - 1) \cdot \ell^n \cdot p^{t(n)}$$
where $p = \mathrm{char}(\mathbb{F}_q)$ is the characteristic of $\mathbb{F}_q$ and $t(n)$ is a nonnegative integer.
5) The place $(z = 1)$ of E_0 splits completely in all extensions E_n/E_0, i.e., there are $[E_n : E_0]$ distinct places of E_n above the place $(z = 1)$, and all of them are rational places of E_n. In particular, the number of rational places satisfies $N(E_n) \geq [E_n : E_0] = (\ell - 1) \cdot \ell^n \cdot p^{t(n)}$.
6) The principal divisor of the function w (as in item 3)) in the field E_n has the form
$$(w)^{E_n} = e_0^{(n)} \cdot A^{(n)} - e_\infty^{(n)} \cdot B^{(n)}$$
where $A^{(n)} > 0$ and $B^{(n)} > 0$ are positive divisors of the function field E_n. The ramification index $e_0^{(n)}$ of the place $(w = 0)$ in $E_n/\mathbb{F}_q(w)$ has the form
$$e_0^{(n)} = \ell^{n-1} \cdot p^{r(n)} \text{ with } r(n) \geq 0$$
and the ramification index $e_\infty^{(n)}$ of the place $(w = \infty)$ in the extension $E_n/\mathbb{F}_q(w)$ has the form
$$e_\infty^{(n)} = \ell^n \cdot p^{s(n)} \text{ with } s(n) \geq 0.$$
7) The different of the extension $E_n/\mathbb{F}_q(w)$ is given by
$$\mathrm{Diff}(E_n/\mathbb{F}_q(w)) = 2(e_0^{(n)} - 1)A^{(n)} + 2(e_\infty^{(n)} - 1) \cdot B^{(n)}$$
with $e_0^{(n)}$, $e_\infty^{(n)}$, $A^{(n)}$ and $B^{(n)}$ as in item 6).
8) The genus $g(E_n)$ satisfies
$$g(E_n) = [E_n : \mathbb{F}_q(w)] + 1 - (\deg A^{(n)} + \deg B^{(n)}) \leq [E_n : \mathbb{F}_q(w)]$$
with $A^{(n)}$ and $B^{(n)}$ as in item 6).
9) The tower $\mathcal{E}$ attains the Drinfeld–Vladut bound, i.e.
$$\lim_{n\to\infty} N(E_n)/g(E_n) = q^{1/2} - 1.$$

This correspondence is organized as follows. In Section II, we prove Theorem 1.7 which is the basis for our code constructions. In Section III we deal with transitive codes and give the proof of Theorem 1.5. We also explain briefly that the method of proof of Theorem 1.5 yields an improvement of the Tsfasman–Vlăduţ–Zink bound for *transitive nonlinear* codes. Finally, in Section IV we discuss self-orthogonal and self-dual codes and we prove Theorem 1.6.

II. An Asymptotically Optimal Galois Tower of Function Fields

For basic notations and facts in the theory of algebraic function fields we refer to [17] and [14]. We will in particular use the notations introduced in Section I after Theorem 1.6.

A *tower of function fields* over $\mathbb{F}_q$ is an infinite sequence $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ of function fields F_i over $\mathbb{F}_q$ with the following properties:

1) $F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots$, and all extensions F_{i+1}/F_i are separable of degree $[F_{i+1} : F_i] > 1$;
2) $\mathbb{F}_q$ is the full constant field of F_i, for all $i \geq 0$;
3) the genus $g(F_i)$ tends to infinity as $i \to \infty$.

Recall that $N(F_i)$ denotes the number of rational places of F_i over $\mathbb{F}_q$. It is well-known that the limit of the tower $\mathcal{F}$,

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} N(F_i)/g(F_i)$$

exists (see [5]). As follows from the Drinfeld–Vladut bound (see Section I),

$$0 \leq \lambda(\mathcal{F}) \leq A(q) \leq q^{1/2} - 1.$$

The tower $\mathcal{F}$ is said to be *asymptotically optimal* if $\lambda(\mathcal{F}) = A(q)$. For $q = \ell^2$ we have $A(q) = \ell - 1$, see Section I. Therefore, a tower $\mathcal{F}$ over $\mathbb{F}_q$ is asymptotically optimal if and only if $\lambda(\mathcal{F}) = \ell - 1$ (for $q = \ell^2$). The tower $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ is called a *Galois tower* if all extensions F_i/F_0 are Galois.

From here on, $q = \ell^2$ is a square. We will construct an asymptotically optimal Galois tower $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ over $\mathbb{F}_q$ with the properties stated in Theorem 1.7. The starting point is the asymptotically optimal tower $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ over $\mathbb{F}_q$ which was introduced in [5], see also [6]. It is defined as follows:

1) $F_0 = \mathbb{F}_q(x_0)$ is the rational function field;
2) for all $i \geq 0$ we have $F_{i+1} = F_i(x_{i+1})$ with
$$x_{i+1}^\ell + x_{i+1} = \frac{x_i^\ell}{x_i^{\ell-1} + 1}. \tag{2.1}$$

We will need the following properties F1)–F5) of this tower $\mathcal{F}$; see [5, Sec. 3] for the proof of F1), F2), F3), F5), and [6, Sec. 3] for the proof of F4).

F1) All extensions F_{i+1}/F_i are Galois of degree ℓ.

F2) The only places of $F_0 = \mathbb{F}_q(x_0)$ which are ramified in the tower $\mathcal{F}$, are the places $(x_0 = \alpha)$ with $\alpha^\ell + \alpha = 0$ and the place $(x_0 = \infty)$.

F3) The places $(x_0 = \infty)$ and $(x_0 = \alpha)$ with $\alpha^{\ell-1} + 1 = 0$ are totally ramified in all extensions F_n/F_0, i.e., their ramification index in F_n/F_0 is ℓ^n.

F4) One can refine the extensions F_{i+1}/F_i to Galois steps of degree $p = \mathrm{char}(\mathbb{F}_q)$ as follows:
$$F_i = H_i^{(0)} \subseteq H_i^{(1)} \subseteq \cdots \subseteq H_i^{(a)} = F_{i+1}$$
with $[H_i^{(j+1)} : H_i^{(j)}] = p$. For any place P of $H_i^{(j)}$ and Q of $H_i^{(j+1)}$ lying above P, the different exponent $d(Q|P)$ satisfies
$$d(Q|P) = 2(e(Q|P) - 1).$$

F5) All places $(x_0 = \alpha)$ of F_0 with $\alpha \in \mathbb{F}_q$ and $\alpha^\ell + \alpha \neq 0$ split completely in the tower $\mathcal{F}$, i.e., any of these places has ℓ^n extensions in $F_n|F_0$, and all of them are rational places of F_n.

We set s
$$w := x_0^\ell + x_0 \quad\text{and}\quad z := w^{\ell-1} \tag{2.2}$$
then
$$\mathbb{F}_q(z) \subseteq \mathbb{F}_q(w) \subseteq F_0 = \mathbb{F}_q(x_0) \subseteq F_1 \subseteq F_2 \subseteq \cdots .$$
The extension $\mathbb{F}_q(w)/\mathbb{F}_q(z)$ is cyclic of degree $(\ell - 1)$, and the extension $F_0/\mathbb{F}_q(w)$ is Galois of degree ℓ. In the extension $F_0/\mathbb{F}_q(z)$ we have the following ramification and splitting behavior (which is easily checked).

F6) The place $(z = \infty)$ of $\mathbb{F}_q(z)$ is totally ramified in $F_0/\mathbb{F}_q(z)$; the only place of F_0 lying above $(z = \infty)$ is the place $(x_0 = \infty)$.

F7) Exactly ℓ places of F_0 lie above the place $(z = 0)$, namely the places $(x_0 = \alpha)$ with $\alpha^\ell + \alpha = 0$. Their ramification index in $F_0/\mathbb{F}_q(z)$ is $\ell - 1$.

F8) No other places of $\mathbb{F}_q(z)$ are ramified in F_0.

F9) One can refine the extension $F_0/\mathbb{F}_q(w)$ to Galois steps of degree $p = \mathrm{char}(\mathbb{F}_q)$ as follows:
$$\mathbb{F}_q(w) = H^{(0)} \subseteq H^{(1)} \subseteq \cdots \subseteq H^{(a)} = F_0$$
with $[H^{(j+1)} : H^{(j)}] = p$. For any place P of $H^{(j)}$ and Q of $H^{(j+1)}$ lying above P, the different exponent $d(Q|P)$ satisfies
$$d(Q|P) = 2(e(Q|P) - 1).$$

F10) The place $(z = 1)$ splits completely in the extension $F_0/\mathbb{F}_q(z)$; the places of F_0 lying above $(z = 1)$ are exactly the places $(x_0 = \alpha)$ with $\alpha \in \mathbb{F}_q$ and $\alpha^\ell + \alpha \neq 0$.

After these preparations we can now prove Theorem 1.7. We start with the tower $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ as above; in particular we consider the elements $w, z \in F_0$ as defined in (2.2) above. Then we define the tower $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ as follows: $E_0 = \mathbb{F}_q(z)$ is the rational function field. For all $n \geq 1$,

E_n is the Galois closure of field extension F_{n-1}/E_0.

We have then
$$E_0 = \mathbb{F}_q(z) \subseteq \mathbb{F}_q(w) \subseteq \mathbb{F}_q(x_0) \subseteq E_1 \subseteq E_2 \subseteq \cdots$$
and items 2), 3) of Theorem 1.7 are clear. By Galois theory, the field E_n is the composite of the fields
$$F_{n-1}, \tau(F_{n-1}), \rho(F_{n-1}), \ldots$$
where $\tau, \rho, \ldots$ run through all embeddings of the field F_{n-1} over E_0 into a fixed algebraically closed field $\bar{E} \supseteq E_0$. The extension $\mathbb{F}_q(w)/E_0$ is Galois, hence the field $\mathbb{F}_q(w)$ is mapped onto itself by all such embeddings of F_{n-1}/E_0. By items F4) and F9) above, we can therefore obtain the field E_n by iterated composites of F_{n-1} with Galois extensions of degree $p = \mathrm{char}(\mathbb{F}_q)$. It follows that the degree of $E_n/F_q(w)$ is a power of p. Since $[F_{n-1} : \mathbb{F}_q(w)] = \ell^n$, item 4) of Theorem 1.7 follows.

We consider now the place $(z = 1)$ of the rational function field $E_0 = \mathbb{F}_q(z)$. By items F5) and F10), this place splits completely in the extension F_{n-1}/E_0, hence, it splits completely also in $\tau(F_{n-1})/E_0$ for all embeddings τ as above. As follows from ramification theory, the place $(z = 1)$ then splits completely in the composite field of $F_{n-1}, \tau(F_{n-1}), \ldots$ (see [17, Sec. III.8.4]). We have thus proved item 5) of Theorem 1.7. An immediate consequence is that $\mathbb{F}_q$ is the full constant field of E_n; this is item 1) of Theorem 1.7. Item 6) of Theorem 1.7 follows easily from F3) and F6).

The core of the proof of Theorem 1.7 is item 7). For its proof we need a result from [6]:

Lemma 2.1: Let $F/\mathbb{F}_q$ be a function field and let G_1/F and G_2/F be linear disjoint Galois extensions of F, both of degree $p = \mathrm{char}(\mathbb{F}_q)$. Denote by $G = G_1 \cdot G_2$ the composite field of G_1 and G_2. Let Q be a place of G and denote by Q_1, Q_2 and P its restrictions to the subfields G_1, G_2 and F. Suppose that we have
$$d(Q_i|P) = 2(e(Q_i|P) - 1), \text{ for } i = 1, 2.$$
Then $d(Q|Q_i) = 2(e(Q|Q_i) - 1)$ holds for $i = 1, 2$.

Proof: See [6, Lemma 1]. □

Now we prove item 7) of Theorem 1.7. First of all, it follows from items F2), F6), F7), F8) that the places $(w = 0)$ and $(w = \infty)$ of $\mathbb{F}_q(w)$ are the only ramified places in $F_{n-1}/\mathbb{F}_q(w)$ and hence in $E_n/\mathbb{F}_q(w)$. We consider now a place $\tilde{Q}$ of E_n which is ramified in the extension E_n/E_0. By items F2), F6), F7), F8), $\tilde{Q}$ is either a zero or a pole of the function w, i.e., $\tilde{Q}$ is in the support of the divisor $A^{(n)}$ or $B^{(n)}$ (notation as in item 6) of Theorem 1.7).

Let $Q := \tilde{Q} \cap F_{n-1}$ be the restriction of $\tilde{Q}$ to the field F_{n-1}. We refine the extension $F_{n-1}/\mathbb{F}_q(w)$ to Galois steps of degree p
$$\mathbb{F}_q(w) = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = F_{n-1} \subseteq E_n \tag{2.3}$$
with $[K_{j+1} : K_j] = p$. Let $P_j := Q \cap K_j$ for $j = 0, \ldots, m$. By items (F4), (F9), the different exponents $d(P_{j+1}|P_j)$ are given by
$$d(P_{j+1}|P_j) = 2(e(P_{j+1}|P_j) - 1), \text{ for } j = 0, \ldots, m - 1. \tag{2.4}$$
The Galois closure E_n of F_{n-1}/E_0 is obtained by iterated composites of the chain
$$K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m$$
with the chains
$$\tau(K_0) \subseteq \tau(K_1) \subseteq \cdots \subseteq \tau(K_m)$$
where τ runs through the embeddings of F_{n-1}/E_0. So we can refine the chain in (2.3) to a chain
$$\begin{aligned}\mathbb{F}_q(w) &= K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m \\ &= F_{n-1} \subseteq K_{m+1} \subseteq \cdots \subseteq K_r = E_n\end{aligned}$$
where all extensions K_{j+1}/K_j are Galois of degree p (for $j = 0, \ldots, r - 1$). We set $P_j := \tilde{Q} \cap K_j$ for $j = m + 1, \ldots, r$. It follows from the fact that the Galois closure E_n of F_{n-1}/E_0 is obtained by iterated composites of the chains $K_0 \subseteq \tau(K_1) \subseteq \cdots \subseteq \tau(K_m)$ (where τ runs over all embeddings of F_{n-1}/E_0) and from (2.4) and Lemma 2.1 that the different exponents $d(P_{j+1}/P_j)$ satisfy $d(P_{j+1}|P_j) = 2(e(P_{j+1}|P_j) - 1)$, for $j = 0, \ldots, r - 1$. Using the

transitivity of different exponents (cf. [17, Sec. III.4.11]) we obtain that

$$d(\tilde{Q}|P_0) = 2(e(\tilde{Q}|P_0) - 1).$$

This finishes the proof of item 7) of Theorem 1.7.

With notations as in items 6) and 7), the Hurwitz genus formula for the extension $E_n/\mathbb{F}_q(w)$ yields

$$\begin{aligned} 2g(E_n) - 2 =& -2[E_n : \mathbb{F}_q(w)] + 2e_0^{(n)} \deg A^{(n)} \\ &+ 2e_\infty^{(n)} \deg B^{(n)} - 2(\deg A^{(n)} + \deg B^{(n)}) \\ =& \, 2 \cdot [E_n : \mathbb{F}_q(w)] - 2(\deg A^{(n)} + \deg B^{(n)}). \end{aligned}$$

We have used here that the divisors $e_\infty^{(n)} \cdot B^{(n)}$ and $e_0^{(n)} \cdot A^{(n)}$ are the pole divisor and the zero divisor of the function w in E_n, hence their degree is equal to the degree $[E_n : \mathbb{F}_q(w)]$. We have thus proved item 8) of Theorem 1.7.

From items 5) and 8) we see that

$$N(E_n)/g(E_n) \geq \ell - 1 \text{ for all } n \geq 1 \tag{2.5}$$

Hence $\lim_{n\to\infty} N(E_n)/g(E_n) \geq \ell - 1$. By the Drinfeld–Vladut bound (see Section I) we also have that $\lim_{n\to\infty} N(E_n)/g(E_n) \leq \ell - 1$, hence equality holds. This proves item 9) and finishes the proof of Theorem 1.7.

III. Asymptotically Good Transitive Codes

The aim of this section is to prove Theorem 1.5. We use notation as in Theorem 1.5, in particular $q = \ell^2$ is a square. Let $R, \delta \geq 0$ with

$$R = 1 - \delta - \frac{1}{\ell - 1} \tag{3.1}$$

and let $\epsilon > 0$. We will construct transitive codes C over $\mathbb{F}_q$ of arbitrarily large length such that $R(C) \geq R - \epsilon$ and $\delta(C) \geq \delta$; this proves then Theorem 1.5.

Consider the tower $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ of function fields over $\mathbb{F}_q$ which was constructed in Theorem 1.7. Choose an integer $n > 0$ so large that

$$\frac{1}{\ell^n(\ell - 1)} < \epsilon. \tag{3.2}$$

Let $N := [E_n : \mathbb{F}_q(z)]$, with the function $z \in E_n$ as in Theorem 1.7, and consider the divisors D, G_0 of E_n which are given by

$$D := \sum_{P|(z=1)} P \text{ and } G_0 := \sum_{Q|(z=\infty)} Q. \tag{3.3}$$

This means: P runs over all places of E_n which are zeroes of the function $(z - 1)$, and Q runs over all poles of the function z in E_n. By Theorem 1.7 item 5) all these places P are rational, and the degree of D is $\deg D = N$. With notations as in Theorem 1.7 item 6), the divisor G_0 is just the divisor $G_0 = B^{(n)}$, since the functions w and $z = w^{\ell-1}$ have the same poles. The degree of G_0 satisfies then

$$\deg G_0 = \frac{[E_n : \mathbb{F}_q(w)]}{e_\infty^{(n)}} \leq \frac{[E_n : \mathbb{F}_q(w)]}{\ell^n} = \frac{N}{\ell^n(\ell - 1)},$$

by Theorem 1.7 item 6). Hence, we have that

$$(\deg G_0)/N < \epsilon,$$

by Inequality (3.2). We choose $r \geq 0$ such that

$$1 - \delta \geq r \cdot \frac{\deg G_0}{N} > 1 - \delta - \epsilon \tag{3.4}$$

and consider the geometric Goppa code

$$C := C_{\mathcal{L}}(D, rG_0) \subseteq \mathbb{F}_q^N$$

associated to the divisors D and rG_0. It is defined as follows (cf. [17, Sec. II.2.1] or [20]): If $\mathcal{L}(rG_0) \subseteq E_n$ denotes the Riemann–Roch space of the divisor rG_0 and the divisor D is defined as $D = P_1 + \cdots + P_N$, then

$$C_{\mathcal{L}}(D, rG_0) = \{(f(P_1), \ldots, f(P_N)) \in \mathbb{F}_q^N | f \in \mathcal{L}(rG_0)\}. \tag{3.5}$$

For the parameters $k = \dim C$ and $d = d(C)$ we have the standard estimates for geometric Goppa codes (see [17, Sec. II.2.3]):

$$k \geq r \cdot \deg G_0 + 1 - g(E_n) \text{ and } d \geq N - r \cdot \deg G_0.$$

Hence, the information rate $R(C)$ satisfies

$$R(C) = \frac{k}{N} \geq \frac{r \cdot \deg G_0}{N} + \frac{1}{N} - \frac{g(E_n)}{N} > 1 - \delta - \epsilon - \frac{g(E_n)}{N}$$

by Inequality (3.4). Now observe that

$$\frac{g(E_n)}{N} \leq \frac{1}{\ell - 1}$$

by Inequality (2.5), and we obtain using Equality (3.1) the following estimate for $R(C)$:

$$R(C) > 1 - \delta - \epsilon - \frac{1}{\ell - 1} = R - \epsilon.$$

For the relative minimum distance $\delta(C)$, we get with (3.4):

$$\delta(C) = \frac{d}{N} \geq \frac{N - r \cdot \deg G_0}{N} = 1 - \frac{r \cdot \deg G_0}{N} \geq \delta.$$

These are the desired inequalities for $R(C)$ and $\delta(C)$.

It remains to show that the code $C = C_{\mathcal{L}}(D, rG_0)$ that we constructed above is in fact a *transitive* code. To this end we consider the Galois group of the extension E_n/E_0,

$$\Gamma := \text{Gal}(E_n/E_0).$$

The places $P_1, \ldots, P_N$ in the support of the divisor D are exactly the places of E_n lying above the place $(z = 1)$; hence Γ acts transitively on the set $\{P_1, \ldots, P_N\}$, see [17, Sec. III.7.1]. The divisor rG_0 is obviously invariant under the action of Γ. Therefore Γ acts on the code $C = C_{\mathcal{L}}(D, rG_0)$ as a transitive permutation group in the following way (see [17, Sec. VII.3.3]): for $\sigma \in \Gamma$ and $f \in \mathcal{L}(rG_0)$

$$\sigma(f(P_1), \ldots, f(P_N)) = (f(\sigma P_1), \ldots, f(\sigma P_N)).$$

This completes the proof of Theorem 1.5 □

Remark 3.1: It is an obvious idea to prove the existence of asymptotically good *cyclic* codes in a similar manner. One should start with a tower $\mathcal{H} = (H_0, H_1, H_2, \ldots)$ of function fields over $\mathbb{F}_q$, where all extensions H_n/H_0 are cyclic Galois extensions; then one can do the same construction of codes as in the proof of Theorem 1.5 above. However, this method does not work: it is known that the limit $\lambda(\mathcal{H}) = \lim_{n\to\infty} N(H_n)/g(H_n)$ of such a "cyclic" tower $\mathcal{H}$ is zero, see [3].

Remark 3.2: The notion of *information rate* of a code can be defined also for *nonlinear codes* $C \subseteq \mathbb{F}_q^N$, by setting $R(C) := \log_q(|C|)/N$. Using this definition, one obtains in an obvious manner an analogue of the function $\alpha_q(\delta)$ by considering *all* codes over $\mathbb{F}_q$, not just linear codes. We denote this analoguous function again by $\alpha_q(\delta)$. It was shown in [12] and [19] (see also [1], [2], [22]) that in a large open subinterval of [0, 1], the Tsfasman–Vlăduţ–Zink bound

$$\alpha_q(\delta) \geq 1 - \delta - A(q)^{-1} \tag{3.6}$$

can be improved to

$$\alpha_q(\delta) \geq 1 - \delta - A(q)^{-1} + \log_q(1 + q^{-3}). \qquad (3.7)$$

A further slight improvement of Inequality (3.7) was very recently found in [13]. However, it seems that the codes which were constructed in [12], [13] and [19] in order to prove Inequality (3.6) do not have any algebraic or combinatoric structure. By combining the method of [19] with our proof of Theorem 1.5 we can now show that the lower bound (3.7) for $\alpha_q(\delta)$ is attained by *transitive* nonlinear codes.

Theorem 3.3: Assume that $q = \ell^2$ is a square, and set

$$\delta^* := 1 - 2/(\ell - 1) - (4q - 2)/((q - 1)(q^3 + 1)).$$

Then the bound

$$\alpha_q(\delta) \geq 1 - \delta - A(q)^{-1} + \log_q(1 + q^{-3})$$

is attained by transitive codes, for all δ in the interval $(0, \delta^*) \subseteq [0, 1]$.

Proof: (Sketch.) We recall briefly the code construction given in [19]. One considers a function field F over $\mathbb{F}_q$ of genus g and a set $\mathcal{P} = \{P_1, \dots, P_N\}$ of N distinct rational places of F. Let $H \geq 0$ be a divisor of F of degree $\deg H \geq 2g - 1$ with $\mathrm{supp}(H) \cap \mathcal{P} = \emptyset$ and consider divisors G of the form

$$G = \sum_{j=1}^{t} m_{i_j} P_{i_j} \text{ with } 1 \leq i_1 < i_2 < \cdots < i_t \leq N, m_{i_j} \geq 1 \text{ and } \deg G = s. \qquad (3.8)$$

Define the set $M_H(G)$ as follows:

$$M_H(G) := \{x \in \mathcal{L}(H + G) \mid v_{P_{i_j}}(x) = -m_{i_j} \text{ for } 1 \leq j \leq t\}.$$

Choose integers s, t with $1 \leq t \leq N$ and $s \geq t$, and set

$$S := S(H, \mathcal{P}, s, t) := \bigcup_G M_H(G)$$

where G runs over all divisors of the form (3.8). It is clear that $M_H(G_1) \cap M_H(G_2) = \emptyset$ if $G_1 \neq G_2$. Hence we can define a map $\varphi : S \to \mathbb{F}_q^N$ in the following way: for $x \in M_H(G)$ put $\varphi(x) = (x_1, \dots, x_N)$ with

$$x_i = \begin{cases} x(P_i), & \text{if } P_i \notin \mathrm{supp}(G) \\ 0, & \text{if } P_i \in \mathrm{supp}(G). \end{cases}$$

Thus we obtain a (nonlinear) code $C = C(H, \mathcal{P}, s, t)$ by setting

$$C(H, \mathcal{P}, s, t) := \varphi(S) \subseteq \mathbb{F}_q^N.$$

If the function field F runs through a sequence of function fields $(F_0, F_1, F_2, \dots)$ over $\mathbb{F}_q$ with $\lim_{n\to\infty} N(F_n)/g(F_n) = \sqrt{q} - 1$, one can choose the set $\mathcal{P}$, the divisor H and the integers s, t in such a way that the corresponding codes $C(H, \mathcal{P}, s, t)$ reach the bound (3.7), see [19, Prop. 3.3 and Th. 3.4.]

In order to obtain transitive codes with the above construction, we use again the function fields E_n of the tower $\mathcal{E} = (E_0, E_1, E_2, \dots)$ from Theorem 1.7. We choose the set $\mathcal{P}$ as in the proof of Theorem 1.5, i.e.,

$$\mathcal{P} = \{P \mid P \text{ is a zero of the function } z - 1 \text{ in } E_n\}$$

see (3.3). The divisor H is chosen as

$$H = m_0 \cdot G_0$$

with the divisor G_0 of E_n as in (3.3). Since the set $\mathcal{P}$ and the divisor G_0 are invariant under the action of the group $\Gamma = \mathrm{Gal}(E_n/E_0)$, it follows immediately that the corresponding codes $C(H, \mathcal{P}, s, t) \subseteq \mathbb{F}_q^N$ are Γ-invariant; they are therefore transitive codes. □

IV. Asymptotically Good Self-Dual and Self-Orthogonal Codes

In this section, we will prove Theorem 1.6. First, we recall some definitions and facts.

Definition 4.1: Let $C \subset \mathbb{F}_q^N$ be a linear code, and let $\underline{a} = (a_1, \dots, a_N) \in \mathbb{F}_q^N$ with nonzero components $a_1, \dots, a_N \neq 0$. We set

$$\underline{a} \cdot C := \{(a_1 \cdot c_1, \dots, a_N \cdot c_N) \in \mathbb{F}_q^N \mid (c_1, \dots, c_N) \in C\}$$

and call the codes C and $\underline{a} \cdot C$ *equivalent.*

It is clear that equivalent codes have the same parameters (length, dimension, minimum distance, information rate, relative minimum distance). Note however that the automorphism groups $\mathrm{Aut}(C)$ and $\mathrm{Aut}(\underline{a} \cdot C)$ are in general nonisomorphic.

Definition 4.2:

1) A code $C \subseteq \mathbb{F}_q^N$ is called *self-dual* if C is equal to its dual code $C^\perp$. The code C is called *self-orthogonal* if $C \subseteq C^\perp$.
2) A code C is called *iso-dual* if C is equivalent to its dual code $C^\perp$, cf. [15].
3) A code C is called *iso-orthogonal* if C is equivalent to a subcode of $C^\perp$.

Now let $F/\mathbb{F}_q$ be a function field and let $P_1, \dots, P_N$ be distinct rational places of F. Let $D = P_1 + \cdots + P_N$ and let G be a divisor with $\mathrm{supp}\, D \cap \mathrm{supp}\, G = \emptyset$. As in Section III, we consider the geometric Goppa code (cf. (3.5))

$$C_\mathcal{L}(D, G) := \{(f(P_1), \dots, f(P_N)) \in \mathbb{F}_q^N \mid f \in \mathcal{L}(G)\}. \qquad (4.1)$$

Proposition 4.3: Let D and G be divisors of the function field $F/\mathbb{F}_q$ as above and consider the code $C = C_\mathcal{L}(D, G)$ as defined in (4.1). Suppose that η is a differential of F with the property $v_{P_i}(\eta) = -1$ for $i = 1, \dots, N$. Then the dual code $C^\perp = C_\mathcal{L}(D, G)^\perp$ is given by

$$C^\perp = \underline{a} \cdot C_\mathcal{L}(D, H),$$

with $H := D - G + (\eta)$ and $\underline{a} = (\mathrm{res}_{P_1}(\eta), \dots, \mathrm{res}_{P_N}(\eta))$.

Proof: See [18, Corollary 2.7]. □

We want to apply Proposition 4.3 to geometric Goppa codes which are defined by means of the function fields E_n in the tower $\mathcal{E} = (E_0, E_1, E_2, \dots)$ of Theorem 1.7. So we must find an appropriate differential η of E_n having the properties as required in Proposition 4.3.

Proposition 4.4: We assume all notations from Theorem 1.7 and consider the differential

$$\eta := \frac{dw}{1 - z}$$

of the function field E_n (with $n \geq 2$). Then the following holds.

1) The divisor of η in E_n is given by
$$(\eta) = a_n \cdot A^{(n)} + b_n \cdot B^{(n)} - D^{(n)}$$
where the divisors $A^{(n)} > 0$ and $B^{(n)} > 0$ are as in Theorem 1.7 item 6) , the integers $a_n > 0$ and $b_n > 0$ satisfy $a_n \equiv b_n \equiv 0 \bmod 2$, and the divisor $D^{(n)}$ is the sum over all zeroes of the function $z - 1$ in E_n, i.e.,
$$D^{(n)} = \sum_{P \mid (z=1)} P.$$
2) The residue of the differential η at a place P, which is a zero of $z - 1$ in E_n, is an element of $\mathbb{F}_\ell^\times$, i.e.,
$$\mathrm{res}_P(\eta) = \alpha_P \text{ with } \alpha_P^{\ell-1} = 1.$$

Proof:

1) By Theorem 1.7 item 6), the principal divisor of the function w in E_n is
$$(w)^{E_n} = e_0^{(n)} \cdot A^{(n)} - e_\infty^{(n)} \cdot B^{(n)}$$

and by item 7) of Theorem 1.7, the different of $E_n/\mathbb{F}_q(w)$ is

$$\mathrm{Diff}(E_n/\mathbb{F}_q(w)) = 2(e_0^{(n)}-1)\cdot A^{(n)} + 2(e_\infty^{(n)}-1)\cdot B^{(n)}.$$

It follows that the divisor of the differential dw in E_n is given by (see [17, Sec. III.4.6])

$$\begin{aligned}(dw) &= -2e_0^{(n)}B^{(n)} + \mathrm{Diff}(E_n/\mathbb{F}_q(w))\\ &= 2e_0^{(n)}A^{(n)} - 2A^{(n)} - 2B^{(n)}.\end{aligned}$$

The divisor of the function $1-z$ in E_n is

$$(1-z)^{E_n} = D^{(n)} - (\ell-1)\cdot e_\infty^{(n)}\cdot B^{(n)}$$

and we obtain the divisor of the differential $\eta = dw/(1-z)$ as follows:

$$\begin{aligned}(\eta) &= 2e_0^{(n)}A^{(n)} - 2A^{(n)} - 2B^{(n)} - D^{(n)} + (\ell-1)e_\infty^{(n)}B^{(n)}\\ &= a_nA^{(n)} + b_nB^{(n)} - D^{(n)}\end{aligned}$$

with $a_n > 0, b_n > 0$ and $a_n \equiv b_n \equiv 0 \bmod 2$.

2) Let P be a place of E_n which is a zero of the function $z-1$. The element $t := z-1$ is a P-prime element. From the equation $w^{\ell-1} = z = t+1$ we obtain

$$dt = (\ell-1)w^{\ell-2}dw = -\frac{w^{\ell-1}}{w}dw = -\frac{1+t}{w}dw,$$

hence

$$\eta = \frac{dw}{1-z} = -\frac{1}{t}dw = \frac{w}{1+t}\cdot\frac{1}{t}dt.$$

Let $\alpha := w(P) \in \mathbb{F}_q$ be the residue class of w at the place P; then

$$\frac{w}{1+t} \equiv \alpha \bmod P \text{ and therefore } \mathrm{res}_P(\eta) = \alpha.$$

Since $\alpha^{\ell-1} = w^{\ell-1}(P) = z(P) = 1$, we conclude that $\alpha \in \mathbb{F}_\ell \setminus \{0\}$. □

Now we can construct certain geometric Goppa codes which are associated to the function field E_n in the tower $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ of Theorem 1.7. For the rest of this section, we fix notations as above; in particular, we will use without further explanation the divisors $A^{(n)}$, $B^{(n)}$ and $D^{(n)}$, the differential η and the integers a_n and b_n as in Proposition 4.4.

Definition 4.5: For integers a, b with $0 \le a \le a_n$ and $0 \le b \le b_n$, we define the code $C_{a,b}^{(n)}$ by

$$C_{a,b}^{(n)} := C_{\mathcal{L}}(D^{(n)}, aA^{(n)} + bB^{(n)}).$$

Remarks 4.6:

1) It is clear that the codes $C_{a,b}^{(n)}$ are transitive. This follows as in Section III from the fact that the Galois group $\Gamma = \mathrm{Gal}(E_n/E_0)$ acts transitively on the places $P \in \mathrm{supp}(D^{(n)})$ and leaves the divisors $A^{(n)}$ and $B^{(n)}$ invariant.
2) For $n \to \infty$, the codes $C_{a,b}^{(n)}$ attain the Tsfasman–Vlăduţ–Zink bound $\alpha_q(\delta) \ge 1 - \delta - 1/(\ell-1)$, for all $\delta \in (0, 1-1/(\ell-1))$. This is proved in the same manner as Theorem 1.5 (see Section III).

Proposition 4.7: We write $D^{(n)} = P_1 + \cdots + P_N$, with $N = [E_n : E_0]$, and set

$$\underline{u} := (\mathrm{res}_{P_1}\eta, \ldots, \mathrm{res}_{P_N}\eta) \in (\mathbb{F}_q^\times)^N.$$

Then the dual of the code $C_{a,b}^{(n)}$ is given by

$$(C_{a,b}^{(n)})^\perp = \underline{u}\cdot C_{a_n-a,b_n-b}^{(n)}.$$

Proof: The differential η satisfies the condition $v_{P_i}(\eta) = -1$, for $i = 1, \ldots, N$. Hence, we can apply Proposition 4.3 and obtain

$$(C_{a,b}^{(n)})^\perp = \underline{u}\cdot C_{\mathcal{L}}(D^{(n)}, H)$$

with

$$\begin{aligned}H &= D^{(n)} - (aA^{(n)} + bB^{(n)}) + (\eta)\\ &= D^{(n)} - (aA^{(n)} + bB^{(n)}) + (a_nA^{(n)} + b_nB^{(n)} - D^{(n)})\\ &= (a_n - a)A^{(n)} + (b_n - b)B^{(n)}.\end{aligned}$$

We have used here Proposition 4.4, 1). □

The following corollary is an obvious consequence from Proposition 4.7, cf. Definition 4.2.

Corollary 4.8:

1) For $0 \le a \le a_n/2$ and $0 \le b \le b_n/2$, the code $C_{a,b}^{(n)}$ is transitive and iso-orthogonal.
2) For $a = a_n/2$ and $b = b_n/2$, the code $C_{a,b}^{(n)}$ is iso-dual.

Corollary 4.9:

1) For $0 \le a \le a_n/2$ and $0 \le b \le b_n/2$, the code $C_{a,b}^{(n)}$ is equivalent to a self-orthogonal code $\tilde{C}_{a,b}^{(n)}$.
2) For $a = a_n/2$ and $b = b_n/2$, the code $C_{a,b}^{(n)}$ is equivalent to a self-dual code $\tilde{C}_{a,b}^{(n)}$.

Proof: The components of the vector $\underline{u} = (\mathrm{res}_{P_1}\eta, \ldots, \mathrm{res}_{P_N}\eta)$ in Proposition 4.7 are in $\mathbb{F}_\ell^\times$, by Proposition 4.4, 2). So we can write $\mathrm{res}_{P_i}\eta = v_i^2$ with $v_i \in \mathbb{F}_q^\times$ (note that $q = \ell^2$). We set $\underline{v} := (v_1, \ldots, v_N)$; then the code

$$\tilde{C}_{a,b}^{(n)} := \underline{v}\cdot C_{a,b}^{(n)}$$

is self-orthogonal, respectively, self-dual. □

Theorem 1.6 is now an immediate consequence of Corollary 4.9 and Remark 4.6, 2).

Remark 4.10: The existence of asymptotically good sequences $(C_j)_{j\ge0}$ of isodual geometric Goppa codes over $\mathbb{F}_q$ (with $q = \ell^2$) was already proved in [16]. However, the codes that were constructed there attain only the lower bound

$$\lim_{j\to\infty} \delta(C_j) \ge \frac{1}{2} - \frac{1}{\ell-3}. \tag{4.2}$$

The codes $\tilde{C}_n := \tilde{C}_{a,b}^{(n)}$ in Corollary 4.9 part 2) are not only iso-dual but they are self-dual. They satisfy the bound (see Theorem 1.6, 2))

$$\lim_{j\to\infty} \delta(\tilde{C}_j) \ge \frac{1}{2} - \frac{1}{\ell-1}$$

which is better than Inequality (4.2).

V. Conclusion

Let $q = \ell^2$ be a square. We have shown in this correspondence, that the following classes of linear codes over $\mathbb{F}_q$ attain the Tsfasman–Vlăduţ–Zink bound:

- *transitive* codes (Theorem 1.5);
- *transitive iso-orthogonal* codes (Corollary 4.8);
- *transitive iso-dual* codes (Corollary 4.8);
- *self-orthogonal* codes (Theorem 1.6);
- *self-dual* codes (Theorem 1.6).

In particular, the above classes of codes are better than the Gilbert–Varshamov bound, for all squares $q \ge 49$. The class of *nonlinear transitive* codes attains an even better bound than the Tsfasman–Vlăduţ–Zink bound (Theorem 3.3).

References

[1] N. Elkies, “Excellent nonlinear codes from modular curves,” in *STOC’ 01: Proc. 33rd Annu. ACM Symp. Theory Comput.*, Hersonissos, Greece, pp. 200–208.

[2] ——, “Still Better Nonlinear Codes from Modular Curves,” arXiv:math.NT/0308046, 2003.

[3] G. Frey, M. Perret, and H. Stichtenoth, “On the different of Abelian extensions of global fields,” in *Coding Theory and Algebraic Geometry*, H. Stichtenoth and M. A. Tsfasman, Eds. New York: Springer, 1992, vol. LNM 1518, Lecture Notes in Mathematics, pp. 26–32.

[4] A. Garcia and H. Stichtenoth, “A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound,” *Invent. Math.*, vol. 121, pp. 211–222, 1995.

[5] ——, “On the asymptotic behavior of some towers of function fields over finite fields,” *J. Number Theory*, vol. 61, pp. 248–273, 1996.

[6] ——, “Some Artin-Schreier towers are easy,” *Moscow Math. J.*, to be published.

[7] Y. Ihara, “Some remarks on the number of rational points of algebraic curves over finite fields,” *J. Fac. Sci. Univ. Tokyo*, vol. 28, pp. 721–724, 1981.

[8] J. H. van Lint, *Introduction to Coding Theory*. New York: Springer-Verlag, 1982.

[9] Y. I. Manin, “What is the maximal number of points on a curve over $\mathbb{F}_2$?,” *J. Fac. Sci. Univ. Tokyo*, vol. 28, pp. 715–720, 1981.

[10] C. Martinez-Perez and W. Willems, “Is the class of cyclic codes good?,” IEEE Trans. Inf. Theory, vol. 52, no. 2, pp. 696–700, Feb. 2006, to be published.

[11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[12] H. Niederreiter and F. Özbudak, “Constructive asymptotic codes with an improvement on the Tsfasman-Vlăduţ-Zink and Xing bound,” in *Coding, Cryptography and Combinatorics*, K. Q. Feng, H. Niederreiter, and C. P. Xing, Eds. Basel: Birkhäuser, 2004, vol. 23, Progress in Computer Science and Applied Logic, pp. 259–275.

[13] ——, “Further Improvements on Asymptotic Bounds for Codes using Distinguished Divisors,” preprint, 2005.

[14] H. Niederreiter and C. P. Xing, *Rational Points on Curves over Finite Fields*. Cambridge: Cambridge Univ. Press, 2001.

[15] *Handbook of Coding Theory*, vol. I and II, V. S. Pless and W. C. Huffmann, Eds., Elsevier, Amsterdam, The Netherlands, 1998.

[16] W. Scharlau, “Selbstduale Goppa-codes,” *Math. Nachr.*, vol. 143, pp. 119–122, 1989.

[17] H. Stichtenoth, *Algebraic Function Fields and Codes*. Berlin, Germany: Springer-Verlag, 1993.

[18] ——, “Self-dual Goppa codes,” *J. Pure Appl. Algebra*, vol. 55, pp. 199–211, 1988.

[19] H. Stichtenoth and C. P. Xing, “Excellent nonlinear codes from algebraic function fields,” *IEEE Trans. Inf. Theory*, vol. 51, no. 11, pp. 4044–4046, Nov. 2005.

[20] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*. Dordrecht, The Netherlands: Kluwer, 1991.

[21] 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.

[22] C. P. Xing, “Nonlinear codes from algebraic curves improving the Tsfasman-Vlăduţ-Zink bound,” *IEEE Trans. Inf. Theory*, vol. 49, pp. 1653–1657, Jul. 2003.

A Repeat Request Strategy Based on Sliding Window Decoding of Unit-Memory Convolutional Codes

Jürgen Freudenberger, *Member, IEEE,* and Sergo Shavgulidze

***Abstract*—In this correspondence, we investigate a decision feedback strategy for convolutional codes which is based on a sliding window decoding procedure and a threshold test as decision rule. For this purpose, we introduce the burst distance spectrum of a convolutional code and derive asymptotic bounds for the ensemble of periodically time-varying convolutional codes. These results are helpful for the asymptotic analysis of the decision feedback scheme. We show that unit memory codes are particularly suited for such a transmission scheme. For these codes, the decoding procedure is reduced to the decoding of block codes with lengths in the order of the overall constraint length of the convolutional code. This leads to a significantly smaller decoding complexity compared with other known decoding and decision rules. Whereas the achievable asymptotic performance is close to the best known bounds. For low rates, our results even improve these bounds.**

***Index Terms*—Error exponent, repeat request, sliding window decoding, unit-memory convolutional codes.**

I. Introduction

Convolutional coded automatic-repeat-request, so-called hybrid ARQ, is probably todays’ most common error control strategy for channels with feedback. The most popular approach is to employ Viterbi decoding to an error-correcting convolutional code and to test the reliability of the decoded message by means of a high rate error detection code, e.g., a cyclic redundancy check (CRC) code. However, very little is known about the asymptotic performance of such an ARQ scheme [1]. A remarkable result was published by Hashimoto [2], which shows that a decoding rule based on Viterbi decoding and a combination of the suboptimal likelihood-ratio test from [3] and a threshold test is capable of achieving the same reliability as Forney’s likelihood-ratio test for block codes [4] and the corresponding dual reliability function for convolutional codes.

This correspondence addresses an ARQ scheme for convolutional codes based on a sliding window decoding procedure [5], [6]. In particular, we derive an asymptotic error probability bound for the ensemble of periodically time-varying unit memory codes based on the proposed decoding strategy and discuss the asymptotic decoding complexity. We will see that the class of convolutional unit memory (UM) codes is of particular interest for decision feedback. UM codes were first introduced by Lee [7]. Later, Thommesen and Justesen [8] showed that these codes asymptotically have good distance properties and good error exponents with maximum-likelihood decoding. It was also demonstrated that in many cases of practical interest UM codes have larger free distances than ordinary (multimemory) codes with the same rate and the same number of memory elements [9]. However, usually they also have

Manuscript received March 15, 2004; revised January 30, 2006. This work was supported by the Deutsche Forschungsgemeinschaft (DFG) by Grant Bo 867/9-1. The material presented in this correspondence was presented in part at the IEEE International Sumposium on Information Theory, Chicago, IL, June/July 2004.

J. Freudenberger is with the Department of Computer Science, University of Applied Sciences, Constance, Germany (e-mail: juergen.freudenberger@alumni.uni-ulm.de).

S. Shavgulidze is with the Department of Digital Communication Theory, Georgian Technical University, Tbilisi, Republic of Georgia (e-mail: sergo_130@hotmail.com).

Communicated by K. A. S. Abdel-Ghaffar, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2006.872982