An Explicit Construction of a Class of Good Codes and Their Duals

San Ling, Ferruh Özbudak, Chaoping Xing *

San Ling and Chaoping Xing
Department of Mathematics, National University of Singapore
2 Science Drive 2, Singapore 117543, Republic of Singapore
e-mail: {matlings, matxcp}@nus.edu.sg

Ferruh Özbudak
Department of Mathematics, Middle East Technical University
İnönü Bulvarı, 06531, Ankara, Turkey
e-mail: ozbudak@math.metu.edu.tr

Abstract

We study a class of good codes and their duals explicitly. We give direct constructions of the dual codes and obtain self-orthogonal codes with good parameters.

Key words: linear codes, dual codes, self-orthogonal codes, optimal codes

1 Introduction

It is well known that subfield subcodes and propagation techniques would give codes with good parameters. Recently Xing, Ling and Niederreiter [7], [3], [4] have constructed a class of codes with very good parameters from the rational function field of $\mathbb{F}_q$ using specially chosen subcodes of Reed-Solomon codes and propagation rules. Due to their good parameters and algebraic structures, this class of linear codes has attracted further attention. For instance, a decoding algorithm of these codes is given in [5] and these codes have also been generalized to arbitrary algebraic function fields [8].

In this paper we introduce a general framework for such constructions over rational function fields and we study their dual codes. Since subcodes and propagations in the construction have nice algebraic structures, it turns out that the dual codes are also in the same class and we can easily control the dual codes so that we get self-orthogonal and self-dual codes with good parameters. As good codes, we basically mean linear codes with parameters close to the best known ones according to Brouwer's [1] table or certain known bounds. We show that all linear codes can be obtained from our construction in a unique way and dual codes as well as self-orthogonality can be obtained in a simple and explicit manner. Direct constructions of the dual codes and self-orthogonal codes are provided.

* This paper was written while the second named author was visiting the Institute for Mathematical Sciences, National University of Singapore, Republic of Singapore. He would like to thank the institute for the support. The first and third named authors are partially supported by MOE-ARF research grant number R-146-000-029-112 and DSTA research grant number R-394-000-011-422.

2 Construction

First we fix some notation. In the paper we use the usual Euclidean inner product. For $C \subseteq \mathbb{F}_q^n$ a linear code, we denote its dual by $C^\perp$. A code C is said to be self-orthogonal if $C \subseteq C^\perp$. If $C = C^\perp$, then C is said to be self-dual. For $\lambda_i \in \mathbb{F}_q \setminus \{0\}$ for $i = 1, 2, \ldots, n$, let $(\lambda_1, \ldots, \lambda_n) \cdot C$ denote the equivalent code defined as $\{(\lambda_1 c_1, \ldots, \lambda_n c_n) \mid (c_1, \ldots, c_n) \in C\}$. If $(\lambda_1, \ldots, \lambda_n) \cdot C \subseteq C^\perp$ for some $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_q \setminus \{0\}$, then C is said to be quasi self-orthogonal. Similarly, if this containment is in fact an equality, then C is quasi self-dual. Let $\mathbb{F}_q$ be a finite field and let $\overline{\mathbb{F}}_q$ be a fixed algebraic closure.

Let r be any prime and consider the set

$$\Lambda_q^r := \{(a_1, a_2, \ldots, a_r) \mid 0 \leq a_i \leq q \Leftrightarrow 1, 1 \leq i \leq r\}$$

of r-tuples of integers between 0 and $q \Leftrightarrow 1$. Let Ω_r denote the cyclic group generated by the cyclic shift ω_r on Λ_q^r, i.e.,

$$\omega_r(a_1, a_2, \ldots, a_r) := (a_2, a_3, \ldots, a_r, a_1).$$

Note that $\Omega_r = < \omega_r > \cong \mathbb{Z}/r\mathbb{Z}$. For $\mathbf{a} = (a_1, \ldots, a_r) \in \Lambda_q^r$, let $O_{\mathbf{a}}$ denote the orbit of $\mathbf{a}$ under the action of the group Ω_r on Λ_q^r

$$O_{\mathbf{a}} = \{(b_1, \ldots, b_r) = \omega_r^i(a_1, \ldots, a_r) \mid 1 \leq i \leq r\} \subset \Lambda_q^r.$$

Note that, for $\mathbf{a}' \in O_{\mathbf{a}}$, we have $O_{\mathbf{a}} = O_{\mathbf{a}'}$. We also define the associated polynomial $h_{\mathbf{a}}$ of the orbit $O_{\mathbf{a}}$ as

$$h_{\mathbf{a}} := \sum_{(b_1, \ldots, b_r) \in O_{\mathbf{a}}} x^{b_1 + b_2 q + \ldots + b_r q^{r-1}}.$$

Since r is a prime number, there are $m := (q^r \Leftrightarrow q)/r + q$ distinct orbits. Let $\mathcal{S} = \{h_1, \ldots, h_m\}$ be the set of all associated polynomials. For every $\mathbf{a} = (a_1, \ldots, a_r) \in \Lambda_q^r$, let

$$\overline{\mathbf{a}} = (q \Leftrightarrow 1 \Leftrightarrow a_1, \ldots, q \Leftrightarrow 1 \Leftrightarrow a_r).$$

Definition 2.1. For an orbit $O_{\mathbf{a}}$ of Λ_q^r under the action of Ω_r, we define $\overline{O}_{\mathbf{a}}$ as

$$\overline{O}_{\mathbf{a}} = O_{\overline{\mathbf{a}}}.$$

For $h_{\mathbf{a}} \in \mathcal{S}$, we define $\overline{h}_{\mathbf{a}} \in \mathcal{S}$ as

$$\overline{h}_{\mathbf{a}} = h_{\overline{\mathbf{a}}}.$$

Let $\mathcal{P}$ be a subset of $\mathbb{F}_{q^r}$ with the largest cardinality such that

$$\alpha \in \mathcal{P} \Rightarrow \alpha^q = \alpha \text{ or } \alpha^{q^i} \notin \mathcal{P} \text{ for } 1 \leq i \leq r \Leftrightarrow 1.$$

Then $\#\mathcal{P} = (q^r \Leftrightarrow q)/r + q = m$. Let $\mathcal{P} = \{\alpha_1, \ldots, \alpha_m\}$. It is easy to check that the $\mathbb{F}_q$-linear span of the set $\{(h_i(\alpha_1), \ldots, h_i(\alpha_m)) \mid 1 \leq i \leq m\}$ is the space $\mathbb{F}_q^m$ and $\max\{\deg h \mid h \in \mathcal{S}\} = \sum_{\alpha \in \mathcal{P}} \deg f_\alpha \Leftrightarrow \min\{\deg f_\alpha \mid \alpha \in \mathcal{P}\}$, where f_α is the minimal polynomial of α over $\mathbb{F}_q$.

Now we give our construction in a general framework. For a given positive integer n, assume that for some $m \geq n$ there exists a pair $(\hat{\mathcal{S}}, \hat{\mathcal{P}})$ such that $\hat{\mathcal{P}} = \{\alpha_1, \ldots, \alpha_m\}$ is a set

of elements of $\overline{\mathbb{F}}_q$ with distinct minimal polynomials over $\mathbb{F}_q$ and $\hat{\mathcal{S}}$ is a set of m polynomials $h_1, \ldots, h_m \in \overline{\mathbb{F}}_q$ such that the set

$$\{(h_i(\alpha_1), \ldots, h_i(\alpha_m)) \mid 1 \leq i \leq m\}$$

generates the space $\mathbb{F}_q^m$. Let f_i denote the minimal polynomial of α_i over $\mathbb{F}_q$ for $i = 1, \ldots, m$. Then it follows that $\max\{\deg h_i \mid 1 \leq i \leq m\} \geq \sum_{i=1}^{m} \deg f_i \Leftrightarrow \min\{\deg f_i \mid 1 \leq i \leq m\}$.

For example, let r be a prime number satisfying $\frac{q^r - q}{r} + q \geq n$ and let $m = (q^r \Leftrightarrow q)/r + q$. Consider the pair $(\mathcal{S}, \mathcal{P})$ as defined before. It is clear that $\hat{\mathcal{S}} = \mathcal{S}$ and $\hat{\mathcal{P}} = \mathcal{P}$ satisfies the conditions above.

We fix an order on $\hat{\mathcal{P}}$ as $\hat{\mathcal{P}} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ and let $\hat{\mathcal{P}}_n = \{\alpha_1, \ldots, \alpha_n\}$. For $k \leq n$ and an $\mathbb{F}_q$-linearly independent subset $\{g_1, \ldots, g_k\} \subseteq \mathrm{Span}_{\mathbb{F}_q}\hat{\mathcal{S}}$ with the corresponding $k \times n$ matrix $G = (g_i(\alpha_j))_{1 \leq i \leq k, 1 \leq j \leq n}$, we denote the code generated by G as $C(g_1, \ldots, g_k; \hat{\mathcal{P}}_n)$. Note that when $m = n$, we have $C(h_1, \ldots, h_n, \mathcal{P}) = \mathbb{F}_q^n$.

Remark 2.2. In [7], Xing and Ling considered the case $r = 2$ and they constructed codes with good parameters. Ling, Niederreiter and Xing [3] considered the general case that $r \geq 2$ is an integer. They constructed codes of arbitrary length and some codes with good parameters. Our construction and the constructions in [7] and [3] are identical for $r = 2$. For $r \geq 3$ a prime integer, our construction and the construction in [3] use similar subsets of $\mathbb{F}_{q^r}$ for evaluations of polynomials. For $r \geq 3$ a prime integer, the sets of polynomials used in our construction and in [3] are different. For example, it can be readily verified that, when $q = 4$ and $r = 3$, the degrees of the largest set of polynomials used in [3] is a proper subset of the one in our construction. The corresponding subset in our construction includes the set of degrees $\{33, 49, 50, 54\}$ as extra.

We observe that for $n \leq m$, any q-ary $[n, k, d]$ linear code C can be considered as $C(g_1, \ldots, g_k; \hat{\mathcal{P}}_n)$ uniquely upto an ordering of entries of $\hat{\mathcal{P}}$, for some $g_1, \ldots, g_k$.

Proposition 2.3. *Let the notation be as above. Given a q-ary $[n, k, d]$ linear code C, there exists a unique subspace $W_C =< g_1, \ldots, g_k > \subseteq \mathrm{Span}_{\mathbb{F}_q}\hat{\mathcal{S}}$ such that $C = C(g_1, \ldots, g_k; \hat{\mathcal{P}})$.*

Hence for a prime number r, fixing an order on the elements of $\mathcal{P}$, we can find all q-ary linear codes of length $n \leq m = (q^r \Leftrightarrow q)/r + q$ in a unique way. Moreover $m \to \infty$ as $r \to \infty$ for a fixed q.

For given q-ary $[n, k, d]$ code $C(g_1, \ldots, g_k; \hat{\mathcal{P}})$, this observation leads to a method of finding $g'_1, \ldots, g'_{n-k} \in \mathrm{Span}_{F_q}\hat{\mathcal{S}}$ explicitly such that $C(g_1, \ldots, g_k; \hat{\mathcal{P}})^{\perp} = C(g'_1, \ldots, g'_k; \hat{\mathcal{P}})$.

Theorem 2.4. *Let the notation be as above. Choose $g_{k+1}, \ldots, g_n \in \mathrm{Span}_{\mathbb{F}_q}\hat{\mathcal{S}}$ such that the $n \times n$ matrix $G = (g_i(\alpha_j))_{1 \leq i,j \leq n}$ is nonsingular. Consider the matrix B defined as*

$$B := (\mathbf{b}_1^t, \mathbf{b}_2^t, \ldots, \mathbf{b}_n^t) := (G^{-1})^t G^{-1},$$

where $\mathbf{b}_i = (\beta_{i,1}, \ldots, \beta_{i,n}) \in \mathbb{F}_q^n$ for $i = 1, 2, \ldots, n$. Let $g'_i \in \mathrm{Span}_{\mathbb{F}_q}\hat{\mathcal{S}}$ be defined as

$$g'_i = \beta_{k+i,1} g_1 + \beta_{k+i,2} g_2 + \ldots + \beta_{k+i,n} g_n$$

for $i = 1, 2, \ldots, n \Leftrightarrow k$. Then

$$C(g_1, \ldots, g_k; \hat{\mathcal{P}})^{\perp} = C(g'_1, \ldots, g'_{n-k}; \hat{\mathcal{P}}).$$

3 Direct Constructions of Dual Codes

Let r be a prime, $\mathbb{F}_q$ a finite field of characteristic different from r and $n = \frac{q^r - q}{r} + q$. In this section we study direct constructions of dual codes corresponding to pairs $(\mathcal{S}, \mathcal{P})$ defined in Section 2. We explicitly construct (quasi) self-orthogonal codes with good parameters. Throughout the section we order the elements of $\mathcal{S} = \{h_1, \ldots, h_n\}$ such that $\deg h_i < \deg h_{i+1}$ for $i = 1, \ldots, n \Leftrightarrow 1$. Then we have $h_1 = 1$ and $h_n = x^{(q-1)(1+q+\ldots+q^{r-1})} = x^{q^r-1}$. Moreover we also order the elements of $\mathcal{P}$ as $\mathcal{P} = (\alpha_1, \alpha_2, \ldots, \alpha_q, \alpha_{q+1}, \ldots, \alpha_n)$, where $\{\alpha_1, \ldots, \alpha_q\} = \mathbb{F}_q$.

Theorem 3.1. *Let $1 \le k \le n \Leftrightarrow 1$. For any subset $\{h_{j_1}, \ldots, h_{j_k}\} \subseteq \mathcal{S}$ with $\{h_1, h_n\} \not\subseteq \{h_{j_1}, \ldots, h_{j_k}\}$ we have*

$$C(h_{j_1}, \ldots, h_{j_k}; \mathcal{P})^{\perp} = (\underbrace{1, \ldots, 1}_{q \text{ times}}, \underbrace{r, \ldots, r}_{n-q \text{ times}}) \cdot C(h'_{j_1}, \ldots, h'_{j_{n-k}}; \mathcal{P}),$$

where $\{h'_{j_1}, \ldots, h'_{j_{n-k}}\} = \mathcal{S} \setminus \{\overline{h}_{j_1}, \ldots, \overline{h}_{j_k}\}$. Moreover if r is a square in $\mathbb{F}_q$ with $c^2 = r$ and $\overline{h}_{j_i} \notin \{h_{j_1}, \ldots, h_{j_k}\}$ for $i = 1, \ldots, k$, then

$$(\underbrace{1, \ldots, 1}_{q \text{ times}}, \underbrace{c, \ldots, c}_{n-q \text{ times}}) \cdot C(h_{j_1}, \ldots, h_{j_k}; \mathcal{P})$$

is self-orthogonal.

Proof. First note that $\sum_{\alpha \in \mathbb{F}_{q^r}} \alpha^i = 0$ for $0 \le i \le q^r \Leftrightarrow 2$. This is trivial for $i = 0$. For $1 \le i \le q^r \Leftrightarrow 2$, we can choose $c = c(i) \in \mathbb{F}_{q^r}$ such that $c^i \in \mathbb{F}_{q^r} \setminus \{0, 1\}$. Hence

$$\sum_{\alpha \in \mathbb{F}_{q^r}} \alpha^i = \sum_{\alpha \in \mathbb{F}_{q^r}} (c\alpha)^i = c^i \sum_{\alpha \in \mathbb{F}_{q^r}} \alpha^i.$$

Then

$$(1 \Leftrightarrow c^i) \sum_{\alpha \in \mathbb{F}_{q^r}} \alpha^i = 0 \text{ and } \sum_{\alpha \in \mathbb{F}_{q^r}} \alpha^i = 0 \text{ since } 1 \neq c^i.$$

Therefore if $h \in \mathbb{F}_q[x]$ and $\deg h \le q^r \Leftrightarrow 2$, then

$$\sum_{\alpha \in \mathbb{F}_{q^r}} h(\alpha) = 0. \tag{1}$$

Since $\mathrm{Span}_{\mathbb{F}_q} \mathcal{S}$ forms a ring with multiplication modulo $(x^{q^r} \Leftrightarrow x)$ and $\mathcal{S}$ is a basis, we have for any $1 \le i_1 \le k$ and $1 \le i_2 \le n \Leftrightarrow k$, a uniquely determined $a_l(i_1, i_2) \in \mathbb{F}_q$ for $l = 1, \ldots, n$ satisfying

$$h_{j_{i_1}} h'_{j_{i_2}} \equiv \sum_{l=1}^{n} a_l(i_1, i_2) h_l \mod (x^{q^r} \Leftrightarrow x). \tag{2}$$

Moreover by definition of the operation $h \mapsto \overline{h}$ on $\mathcal{S}$ and by the definition of the set $\{h'_{j_1}, \ldots, h'_{j_{n-k}}\}$, we have $a_n(i_1, i_2) = 0$ for $1 \le i_1 \le k$ and $1 \le i_2 \le n \Leftrightarrow k$. Therefore since $h(\alpha) = h(\alpha^q)$ for any $h \in \mathrm{Span}_{\mathbb{F}_q} \mathcal{S}$ and $\alpha \in \mathbb{F}_{q^r}$, we get

$$\begin{aligned} &\left(h_{j_{i_1}}(\alpha_1), \ldots, h_{j_{i_1}}(\alpha_q), h_{j_{i_1}}(\alpha_{q+1}), \ldots, h_{j_{i_1}}(\alpha_n)\right) \\ &\cdot \left(h'_{j_{i_2}}(\alpha_1), \ldots, h'_{j_{i_2}}(\alpha_q), r h'_{j_{i_2}}(\alpha_{q+1}), \ldots, r h'_{j_{i_2}}(\alpha_n)\right) = \sum_{\alpha \in \mathbb{F}_{q^r}} h_{j_{i_1}}(\alpha) h'_{j_{i_2}}(\alpha) \end{aligned}$$

for $1 \le i_1 \le k$ and $1 \le i_2 \le n \Leftrightarrow k$. Using (1) and (2) we complete the proof. □

It is possible to characterize the subsets $T \subset \mathcal{S}$ satisfying the property

$$\overline{h} \notin T \text{ for any } h \in T. \tag{3}$$

First we determine elements $\mathbf{a} \in \Lambda_q^r$ such that $\overline{O}_{\mathbf{a}} = O_{\mathbf{a}}$.

Proposition 3.2. *For $\mathbf{a} \in \Lambda_q^r$, we have the following equivalences depending on the cases.*
Case r is 2: $\overline{O}_{\mathbf{a}} = O_{\mathbf{a}} \Leftrightarrow \mathbf{a} = (a, b)$ with $a + b = q \Leftrightarrow 1$.
Case r is odd and q is even: $\overline{O}_{\mathbf{a}} \neq O_{\mathbf{a}}$ for any $\mathbf{a} \in \Lambda_q^r$.
Case r is odd and q is odd: $\overline{O}_{\mathbf{a}} = O_{\mathbf{a}} \Leftrightarrow \mathbf{a} = (a_1, \ldots, a_r)$ with $a_1 = \cdots = a_r = \frac{q-1}{2}$.

Next we define special subsets S_0, S_-, and S_+ depending on the cases.
Case r is 2 and q is odd:

$$\begin{aligned} S_0 &= \{h_{\mathbf{a}} \in \mathcal{S} \mid \mathbf{a} = (a, b) \text{ with } a + b = q \Leftrightarrow 1\}, \\ S_- &= \{h_{\mathbf{a}} \in \mathcal{S} \mid \mathbf{a} = (a, b) \text{ with } a + b < q \Leftrightarrow 1\}, \\ S_+ &= \{h_{\mathbf{a}} \in \mathcal{S} \mid \mathbf{a} = (a, b) \text{ with } a + b > q \Leftrightarrow 1\}. \end{aligned}$$

Case r is odd and q is even:

$$S_0 = \emptyset,$$

$$S_- = \left\{ h_{\mathbf{a}} \in \mathcal{S} \mid \mathbf{a} = (a_1, \ldots, a_r) \text{ and } \sum_{i=0}^{q/2-1} \#i\text{'s in } \mathbf{a} < \sum_{i=q/2}^{q-1} \#i\text{'s in } \mathbf{a} \right\},$$

$$S_+ = \left\{ h_{\mathbf{a}} \in \mathcal{S} \mid \mathbf{a} = (a_1, \ldots, a_r) \text{ and } \sum_{i=0}^{q/2-1} \#i\text{'s in } \mathbf{a} > \sum_{i=q/2}^{q-1} \#i\text{'s in } \mathbf{a} \right\}.$$

Case r is odd and q is odd: For simplicity we consider $r = 3$ and let $\mathbf{s} = ((q \Leftrightarrow 1)/2, (q \Leftrightarrow 1)/2, (q \Leftrightarrow 1)/2) \in \Lambda_q^3$.

$$S_0 = \{h_{\mathbf{s}}\},$$

$$\begin{aligned} S_- = &\left\{ h_{\mathbf{a}} \in \mathcal{S} \mid \mathbf{a} = (a_1, a_2, a_3) \text{ and } \sum_{i=0}^{(q-1)/2-1} \#i\text{'s in } \mathbf{a} < \sum_{i=(q-1)/2+1}^{q-1} \#i\text{'s in } \mathbf{a} \right\} \\ &\cup \left\{ h_{\mathbf{i}} \in \mathcal{S} \mid \mathbf{i} = (\frac{q \Leftrightarrow 1}{2}, i, q \Leftrightarrow 1 \Leftrightarrow i) \text{ and } i < \frac{q \Leftrightarrow 1}{2} \right\}, \\ S_+ = &\left\{ h_{\mathbf{a}} \in \mathcal{S} \mid \mathbf{a} = (a_1, a_2, a_3) \text{ and } \sum_{i=0}^{(q-1)/2-1} \#i\text{'s in } \mathbf{a} > \sum_{i=(q-1)/2+1}^{q-1} \#i\text{'s in } \mathbf{a} \right\} \\ &\cup \left\{ h_{\mathbf{i}} \in \mathcal{S} \mid \mathbf{i} = (\frac{q \Leftrightarrow 1}{2}, i, q \Leftrightarrow 1 \Leftrightarrow i) \text{ and } i > \frac{q \Leftrightarrow 1}{2} \right\}. \end{aligned}$$

For a subset $T \subset \mathcal{S}$, we denote by $\overline{T}$ the subset $\{\overline{h} \mid h \in T\}$.

Theorem 3.3. *Let the notation be as above. Then $\mathcal{S} = S_0 \sqcup S_- \sqcup S_+$, $\#S_- = \#S_+$ and $T \subset \mathcal{S}$ satisfies (3) if and only if*

$$\overline{(T \cap S_-)} \cap (T \cap S_+) = \emptyset \quad \textit{and} \quad T \cap S_0 = \emptyset. \tag{4}$$

Note that in the case r is odd and q is even, for $T \subset \mathcal{S}$ satisfying (4) and $\#T = n/2$ we obtain self-dual codes.

We obtain similar results for the pair $(\widetilde{\mathcal{S}}, \widetilde{\mathcal{P}})$ where

$$\widetilde{\mathcal{S}} = \mathcal{S} \setminus \{h_n\} \text{ and } \widetilde{\mathcal{P}} = (\alpha_2, \alpha_3, \ldots, \alpha_n),$$

where $\alpha_1 = 0$. Let $\tilde{n} = n \Leftrightarrow 1 = (q^r \Leftrightarrow q)/r + q \Leftrightarrow 1$ and define

$$\begin{aligned} \widetilde{\overline{h}}_i &= \overline{h}_i \quad \text{if } 2 \le i \le n \Leftrightarrow 1, \\ \widetilde{\overline{h}}_1 &= h_1. \end{aligned}$$

Theorem 3.4. *Let $1 \le k \le \tilde{n} \Leftrightarrow 1$. For any subset $\{h_{j_1}, \ldots, h_{j_k}\} \subseteq \widetilde{\mathcal{S}}$ we have*

$$C(h_{j_1}, \ldots, h_{j_k}; \widetilde{\mathcal{P}})^{\perp} = (\underbrace{1, \ldots, 1}_{q-1 \text{ times}}, \underbrace{r, \ldots, r}_{n-q \text{ times}}) \cdot C(h'_{j_1}, \ldots, h'_{j_{n-1-k}}; \widetilde{\mathcal{P}}),$$

where $\{h'_{j_1}, \ldots, h'_{j_{n-1-k}}\} = \widetilde{\mathcal{S}} \setminus \{\widetilde{\overline{h}}_{j_1}, \ldots, \widetilde{\overline{h}}_{j_k}\}$. If also r is a square in $\mathbb{F}_q$ with $c^2 = r$ and $\widetilde{\overline{h}}_{j_i} \notin \{h_{j_1}, \ldots, h_{j_k}\}$ for $i = 1, \ldots, k$, then

$$(\underbrace{1, \ldots, 1}_{q-1 \text{ times}}, \underbrace{c, \ldots, c}_{n-q \text{ times}}) \cdot C(h_{j_1}, \ldots, h_{j_k}; \widetilde{\mathcal{P}})$$

is self-orthogonal. Moreover let $T \subset \mathcal{S}$ be a subset with $h_1 \in T$ satisfying (4). If $C(T, \mathcal{P})$ is a q-ary $[n, k, d]$ code, then the code $(1, \ldots, 1, c, \ldots, c) \cdot C(T \setminus \{h_1\}; \widetilde{\mathcal{P}})$ is a (quasi) self-orthogonal q-ary $[n \Leftrightarrow 1, k \Leftrightarrow 1, d_1]$ code with $d_1 \ge d$.

Note that in the case r is odd and q is odd, $\#S_0 = 1$. Moreover let $q \equiv 1 \bmod 4$ and hence choose $e \in \mathbb{F}_q$ with $e^2 = \Leftrightarrow 1$. Then we can get (quasi) self-dual codes using $\widetilde{\mathcal{P}}$ as follows. For simplicity we assume that $r = 3$.

Theorem 3.5. *Let $\mathbb{F}_q$ be a finite field with $q \equiv 1 \bmod 4$, $e \in \mathbb{F}_q$ with $e^2 = \Leftrightarrow 1$, $r = 3$ and $\mathbf{s} = ((q \Leftrightarrow 1)/2, (q \Leftrightarrow 1)/2, (q \Leftrightarrow 1)/2) \in \Lambda_q^3$. Let $T \subset \mathcal{S}$ be a subset with $h_1, h_{\mathbf{s}} \in T$ and $T \setminus \{h_{\mathbf{s}}\}$ satisfying (4). Let $T_1 = T \cup \{eh_1 + h_{\mathbf{s}}\} \setminus \{h_1, h_{\mathbf{s}}\}$. If $C(T, \mathcal{P})$ is a q-ary $[n, k, d]$ code, then*

$$(1, \ldots, 1, c, \ldots, c) \cdot C(T_1, \widetilde{\mathcal{P}})$$

is a (quasi) self-orthogonal q-ary $[n \Leftrightarrow 1, k \Leftrightarrow 1, d_1]$ code with $d_1 \ge d$. In particular it is (quasi) self-dual when $k = (n \Leftrightarrow 1)/2 + 1$.

Example 3.6. Using Theorem 3.1 and subsets $\{h_{j_1}, \ldots, h_{j_k}\} \subset \mathcal{S}$ satisfying (4) with $\deg h_{j_1} < \deg h_{j_2}$ for $1 \le j_1 < j_2 \le n$ and $\deg h_{j_k}$ as small as possible, we obtain the following (quasi) self-orthogonal q-ary $[n, k, d]$ codes with the best known parameters as linear codes (see [1]). The minimum distances can be estimated as in [7] and using Magma [2].

$q = 2$: $[4, 2, 2], [8, 4, 4]$,
$q = 3$: $[6, 2, 4]$,
$q = 5$: $[15, 2, 12], [15, 3, 11], [45, 3, 35], [45, 4, 34], [45, 10, 24], [45, 17, 17]$,
$q = 7$: $[28, 2, 24], [28, 3, 23], [28, 5, 19], [28, 8, 15], [28, 9, 14]$,
$q = 9$: $[45, 2, 40], [45, 3, 39], [45, 6, 33], [45, 7, 30], [45, 8, 29], [45, 9, 28]$,
$[45, 10, 27], [45, 12, 24], [45, 13, 23], [45, 14, 22], [45, 16, 20]$.

Using Theorem 3.4 and similar subsets of $\mathcal{S}$ we obtain the following (quasi) self-orthogonal q-ary $[n,k,d]$ codes with the best known parameters as linear codes.

$$\begin{array}{ll} q=2: & [7,3,4], \\ q=5: & [14,2,11],[44,16,17], \\ q=7: & [27,2,23], \\ q=9: & [44,2,39],[44,15,20],[44,7,29],[44,8,28], \\ & [44,9,27],[44,12,23],[44,13,22]. \end{array}$$

We also obtain some good (quasi) self-orthogonal codes whose parameters are beyond the range of Brouwer's tables ([1]).

$$\begin{array}{ll} q=8: & [176,10,127],[176,9,127], \\ q=11: & [66,3,59],[66,6,52],[66,10,45], \\ & [65,2,59],[65,5,52],[65,9,45]. \end{array}$$

We give a generator matrix for 5-ary quasi self-orthogonal code $[45,17,17]$ in Figure I. By applying the propagation rules (see, for example, [6, Exercise 1.2.24]), we get a 5-ary code $[44,17,16]$, which is also a linear code with the best known parameters.

Remark 3.7. Example 3.6 as well as examples in [7] suggest that certain choices of r, subsets of $\mathcal{P}$ and subsets of $\mathcal{S}$ can yield good codes. It would be interesting to characterize some classes of good codes using our construction.

$$G := (I_{17} \mid P)_{17\times 45},$$

where I_{17} is the 17×17 identity matrix and P is a 17×28 matrix given as below:

$$P = \begin{pmatrix}
4&3&1&4&2&4&1&4&1&0&3&4&4&3&3&1&3&1&2&1&1&3&0&4&3&1&1&1\\
0&2&0&3&3&0&1&4&2&0&4&1&1&2&2&0&1&2&0&4&3&3&4&2&1&2&2&4\\
1&2&2&3&0&1&2&1&4&3&3&0&1&4&4&0&1&3&4&1&3&2&2&2&2&3&4&0\\
4&3&2&2&0&3&1&0&1&0&0&3&1&3&0&4&4&2&1&2&0&3&0&4&2&0&1&2\\
0&2&4&2&1&0&3&3&2&0&3&2&1&3&3&4&3&1&0&1&2&1&3&1&1&4&1&2\\
2&0&1&3&2&3&2&2&4&3&4&1&1&0&1&4&3&1&3&0&3&4&1&3&3&2&4&4\\
2&3&2&1&2&2&4&3&1&4&1&1&2&2&1&0&4&4&0&2&0&4&0&3&3&2&0&1\\
2&2&1&3&4&4&1&3&3&2&1&4&4&2&4&3&1&0&1&4&2&4&0&1&1&0&2&0\\
4&1&3&0&0&3&4&0&0&0&1&3&1&2&4&1&3&0&0&0&4&1&3&2&3&3&3&0\\
1&2&3&2&2&4&4&0&3&2&2&0&3&4&0&3&3&2&2&1&3&4&2&0&3&0&2&2\\
2&4&3&3&4&2&3&2&0&1&3&1&3&4&3&4&0&1&1&0&1&1&4&2&3&2&4&3\\
3&4&3&3&3&0&2&2&4&0&4&0&2&0&1&3&4&4&2&3&2&0&3&2&1&0&1&3\\
2&4&4&1&2&1&2&3&3&2&2&1&0&1&0&2&3&1&0&2&1&3&1&1&2&4&4&2\\
4&3&3&2&4&3&4&0&1&0&4&4&0&3&2&1&0&3&2&3&3&3&2&3&2&2&4&4\\
2&3&1&4&2&2&2&1&1&4&4&2&3&0&3&3&4&1&4&4&4&0&2&1&4&3&4&1\\
3&0&1&0&4&3&0&0&3&1&4&0&3&0&1&3&1&0&0&0&2&2&3&2&1&4&2&1\\
0&3&2&0&1&1&0&3&3&4&3&4&1&3&4&0&3&0&4&3&2&3&1&3&1&4&2&1
\end{pmatrix}.$$

Figure I: A generator matrix G for 5-ary quasi self-orthogonal [45,17,17] code

References

[1] A. Brouwer, "Bounds on minimum distance of linear codes", http://www.win.tue.nl/~aeb/voorlincod.html

[2] W. Bosma, J. Cannon, C. Playoust, "The magma algebra system I: The user language", J. Symb. Comp., vol. 24, no. 3–4, pp. 235-265, 1997.

[3] S. Ling, H. Niederreiter, C.P. Xing, "Symmetric polynomials and some good codes", Finite Fields Appl., vol. 7, no. 1, pp. 142-148, 2001.

[4] H. Niederreiter, C.P. Xing, *Rational points on curves over finite fields–theory and application,* London Mathematical Society, Lecture Note Series 285, Cambridge, 2001.

[5] R.R. Nielsen, "Decoding the Xing-Ling codes", preprint, 2001.

[6] M.A. Tsfasman, S. Vlăduţ, *Algebraic-geometric codes,* Dordrecht: Kluwer, 1991.

[7] C.P. Xing, S. Ling, "A class of linear codes with good parameters", IEEE Trans. Inform. Theory, vol. 46, no. 6, pp. 2184-2188, 2000.

[8] C.P. Xing, S. Ling, "A class of linear codes with good parameters from algebraic curves", IEEE Trans. Inform. Theory, vol. 46, no. 4, pp. 1527-1532, 2000.