On the Structure of the Linear Codes with a Given Automorphism

Stefka Bouyuklieva
Faculty of Mathematics and Informatics,
St. Cyril and St. Methodius University of Veliko Tarnovo,
BULGARIA,
stefka@ts.uni-vt.bg

Abstract

The purpose of this talk is to present the structure of the linear codes over a finite field with q elements that have permutation automorphisms of prime order. Methods to construct and classify self-dual codes under the assumption that they have an automorphism of a given prime order are given by Huffman and Yorgov. These methods are extended to linear codes over larger fields. Special attention is paid to LCD and self-orthogonal codes.

1 Introduction

A linear $[n, k]$ code C is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is the finite field of q elements. Let $(u, v) : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ be an inner product in $\mathbb{F}_q^n$. If C is an $[n, k]$ linear code, then its orthogonal complement $C^\perp = \{u \in \mathbb{F}_q^n : (u, v) = 0 \ \forall v \in C\}$ is a linear $[n, n-k]$ code called the dual code of C. We consider three types of linear codes depending on the intersection with their duals:

- If $C = C^\perp$, C is termed self-dual. If the length of a self-dual code is n then its dimension must be $n/2$.
- If $C \subseteq C^\perp$, the code is self-orthogonal. A self-orthogonal code is also self-dual iff its dimension is a half of its length. Self-orthogonal codes with $k > n/2$ do not exist.
- If $C \cap C^\perp$ consists only of the zero vector, the code is called LCD (linear complementary dual). If C is an LCD code so is its dual code $C^\perp$.

The most general definition for equivalence of linear codes of length n over the finite field $\mathbb{F}_q$ is based on the action of the semilinear isometries group $\mathcal{M}_n^*(q) = \mathrm{Mon}_n(\mathbb{F}_q^*) \rtimes \mathrm{Aut}(\mathbb{F}_q) \leq \Gamma_n(\mathbb{F}_q)$ on the vector space $\mathbb{F}_q^n$, where $\Gamma_n(\mathbb{F}_q)$ is the set of all semilinear mappings, i.e. the general semilinear group, $\mathrm{Mon}_n(\mathbb{F}_q^*)$ is the group of all monomial $n \times n$ matrices over $\mathbb{F}_q$, and $\mathrm{Aut}(\mathbb{F}_q)$ is the automorphisms group of the field $\mathbb{F}_q$. Linear q-ary codes C and C' of the same length n are equivalent whenever $C' = CT$ for some

$T \in \mathcal{M}_n^*(q)$. If $CT = C$ for an element $T \in \mathcal{M}_n^*(q)$ then T is called an automorphism of the code. The set of all automorphisms of C form a group denoted by $\mathrm{Aut}(C)$.

In the next section we present some properties of a linear code having an automorphism of a given order.

2 Linear codes and their automorphisms

Any element $T \in \mathcal{M}_n^*(q)$ can be written as $T = PD\tau$ where P is a permutation matrix (permutation part), D is a diagonal matrix (diagonal part), and $\tau \in \mathrm{Aut}(\mathbb{F}_q)$. Note that in the case of prime q, $\mathcal{M}_n^*(q) = \mathrm{Mon}_n(\mathbb{F}_q^*)$, and if $q = 2$ then $\mathcal{M}_n^*(q) \cong \mathrm{Sym}(n)$ where $\mathrm{Sym}(n)$ is the symmetric group of degree n. The following lemma implies that in some cases, when considering automorphisms of prime order, we only need to examine permutation automorphisms.

Lemma 1. *[4] Let C be a linear code over $\mathbb{F}_q$ with an automorphism $T = PD\tau$ of prime order p where $p \nmid (q-1)$ and $p \nmid |\mathrm{Aut}(\mathbb{F}_q)|$. Then there exists a code C' equivalent to C where $P \in \mathrm{Aut}(C')$.*

Let C be a linear code with a permutation automorphism $\sigma \in \mathrm{Sym}(n)$ of order r (not necessarily prime) with c cycles of length r and f fixed points. In this case, we say that σ is of type r-(c, f). Without loss of generality we can assume that

$$\sigma = \Omega_1 \dots \Omega_c \Omega_{c+1} \dots \Omega_{c+f} \tag{1}$$

where $\Omega_i = ((i-1)r + 1, \dots, ir), i = 1, \dots, c$, are the cycles of length r, and $\Omega_{c+i} = (cr + i), i = 1, \dots, f$, are the fixed points. Obviously, $cr + f = n$.

We define

$$F_\sigma(C) := \{v \in C \mid v\sigma = v\}$$

and

$$E_\sigma(C) := \{v \in C : \sum_{i \in \Omega_j} v_i = 0 \text{ for all } j = 1, \dots, c + f\}.$$

The following theorem gives a very important decomposition of the linear code C.

Theorem 2. *[2] Let $C \leq \mathbb{F}_q^n$ be a linear code with a permutation automorphism $\sigma \in Sym(n)$ of order r such that $char(\mathbb{F}_q) \nmid r$. Then:*

(i) $C = F_\sigma(C) \oplus E_\sigma(C)$. Both $F_\sigma(C)$ and $E_\sigma(C)$ are σ-invariant.

(ii) If C is self-dual under the Euclidean inner product, then $\dim(F_\sigma(C)) = (c + f)/2$ and $\dim(E_\sigma(C)) = c(r-1)/2$.

Note that $v \in F_\sigma(C)$ if and only if $v \in C$ and $v|_{\Omega_j}$ is constant for $j = 1, \dots, c + f$. This allows us to define the map $\pi : F_\sigma(C) \to \mathbb{F}_q^{c+f}$ by $(\pi(v))_j = v_i$ for some $i \in \Omega_j$, $j = 1, 2, \dots, c + f$, $v \in F_\sigma(C)$. The following two theorems prove important properties of the projection code $C_\pi = \pi(F_\sigma(C))$ if C is a self-dual code or C is a binary LCD code.

Theorem 3. *[2, 6] Assume C is a self-dual $[n, n/2, d]_q$ code under the Euclidean inner product. Then C_π is a $[c+f, (c+f)/2, d_\pi]_q$ self-dual code with respect to the inner product*

$$u \cdot v = \sum_{i=1}^{c} r u_i v_i + \sum_{i=c+1}^{c+f} u_i v_i. \tag{2}$$

If either $r \equiv 1 \pmod{char(\mathbb{F}_q)}$ or $f = 0$, C_π is an Euclidean self-dual code.

Theorem 4. *[1] The binary linear code C is an LCD code if and only if $E_\sigma(C)$ and $F_\sigma(C)$ are LCD codes. The code $F_\sigma(C)$ is LCD if and only if its image C_π is also an LCD code.*

The research for the other considered types of codes is still ongoing.

Let now σ be a permutation automorphism of C of prime order $p \neq \mathrm{char}(\mathbb{F}_q)$. If $\mathrm{ord}_p(q) = p-1$, where $\mathrm{ord}_p(q)$ is the multiplicative order of q modulo p, then the polynomial $1 + x + \cdots + x^{p-1}$ is irreducible over the field $\mathbb{F}_q$. Let $\mathcal{P}$ be the principal ideal of $\mathcal{R}_p = \mathbb{F}_q[x]/(x^p - 1)$ generated by the polynomial $(1 - x)$. If we denote by $E_\sigma(C)^*$ the code $E_\sigma(C)$ without the last f coordinates, for $v \in E_\sigma(C)^*$ we identify $v \mid_{\Omega_j} = (v_0, v_1, \ldots, v_{p-1})$ with the polynomial $v_0 + v_1 x + \cdots + v_{p-1}x^{p-1}$ from $\mathcal{P} \subset \mathcal{R}_p$. Thus, we obtain the map $\varphi : E_\sigma(C)^* \longrightarrow P^c$.

Theorem 5. *[2] Assume that C is a Euclidean self-dual $[n, n/2, d]$ code and $1 + x + x^2 + \cdots + x^{p-1}$ is irreducible over $\mathbb{F}_q$. Suppose that there is a nonnegative integer t such that $q^t \equiv -1 \pmod{p}$. Then C_φ is a $[c, c/2, d']$ self-dual code over $\mathcal{P}$ under the inner product $\langle \cdot, \cdot \rangle$ given by*

$$\langle u, v \rangle = \sum_{i=1}^{c} u_i v_i^{q^t}, \tag{3}$$

where $u = (u_1, \ldots, u_c)$, $v = (v_1, \ldots, v_c) \in \mathcal{P}^c$.

On $\mathcal{P}^c$, we can use the Hermitian inner product, defined in [5], namely

$$u \cdot v = \sum_{i=1}^{c} u_i \overline{v_i} \quad \text{for } u = (u_1, \ldots, u_c),\ v = (v_1, \ldots, u_c), \tag{4}$$

where $\overline{v_i} = v_i(x^{-1}) = v_i(x^{p-1})$. Note that $v_i(x^{-1}) = v_i(x^{q^t}) = v_i(x)^{q^t}$. Therefore, the inner products (3) and (4) are equivalent. Moreover, if $\mathrm{ord}_p(q) = p - 1$ and $p \neq 2$, then $q^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Therefore we can take $t = \frac{p-1}{2}$.

In the binary case, the following theorem holds:

Theorem 6. *[1] The code $E_\sigma(C)^*$ is a binary LCD code if and only if its image C_φ is an LCD code under the inner product (4).*

The next theorem is an immediate generalization of [7, Theorem 2].

Theorem 7. *Let $C \leq \mathbb{F}_q^n$ be a linear code with an automorphism σ of prime order $p \neq char(\mathbb{F}_q)$. Suppose that $\mathrm{ord}_p(q) = p - 1$ and there is a nonnegative integer t such that $q^t \equiv -1 \pmod{p}$. Then C is an Euclidean self-dual code if and only if the following two conditions hold:*

(i) C_π *is a self-dual code of length* $c+f$ *under the inner product* (2).

(ii) $\varphi(E_\sigma(C)^*)$ *is a self-dual code of length* c *over the field* P *under the inner product* (3).

Similar theorems hold for self-orthogonal and for LCD codes. For example, for binary LCD codes we have

Theorem 8. *[1] The binary code* C *having an automorphism* σ *of odd prime order* p *is an LCD code if and only if* C_φ *and* C_π *are LCD codes.*

The structure of the code C_φ depends on the structure of $\mathcal{P}$ and $\mathcal{R}_p$. Using this structure and the presented decomposition of the code C, we can provide a method for constructing various types of codes that are invariant under an automorphism of a given order.

References

[1] S. Bouyuklieva, J. de la Cruz, On the Structure of Binary LCD Codes having an Automorphism of Odd Prime Order, *IEEE Trans. Inf. Theory 68(10)*, (2022) 6426–6433.

[2] W.C.Huffman, Decomposing and shortening codes using automorphisms, *IEEE Trans. Inform. Theory* **32** (1986), 833-836.

[3] W.C. Huffman, Automorphisms of Codes with Applications to Extremal Doubly Even Codes of Length 48, *IEEE Transactions on Information Theory*, Vol. 28, (1982) 511-521.

[4] W. C. Huffman, On extremal self-dual ternary codes of lengths 28 to 40, *IEEE Trans. Inform. Theory* **38**(4), 1395-1400 (1992)

[5] S. Ling and Patrick Sole, On the algebraic structure of quasi-cyclic codes I: Finite fields, *IEEE Trans. Inform. Theory* **47** (2001), 2751-2760.

[6] G. Nebe, On Extremal Self-Dual Ternary Codes of Length 48, *International Journal of Combinatorics*, 2012.

[7] V.Y. Yorgov, A method for Constructing Inequivalent Self-Dual Codes with Applications to Length 56, *IEEE Transactions on Information Theory*, Vol. 33, (1987) 77-82.