On the Structure of the Linear Codes with a Given Automorphism

Stefka Bouyuklieva

St. Cyril and St. Methodius University of Veliko Tarnovo, BULGARIA

ALCOCRYPT

Outline

Linear codes

- $\mathbb{F}_q$ - finite field with q elements;
- $\mathbb{F}_q^n$ - n-dimensional vector space over $\mathbb{F}_q$;
- (Hamming) weight of a vector $x \in \mathbb{F}_q^n$: $\mathrm{wt}(x) = |\{i | x_i \neq 0\}|$;

Linear $[n, k, d]_q$ code: k-dimensional subspace of $\mathbb{F}_q^n$ with $d(C) = \min\{\mathrm{wt}(x) | x \in C,\ x \neq \mathbf{0}\}$

- n - length, k - dimension, d - minimum weight (distance)
- Generator matrix G of C - a $k \times n$ matrix whose rows form a basis of C as a linear subspace of $\mathbb{F}_q^n$.

Self-orthogonal and LCD codes

- $(u, v) : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ be an inner product in the linear space $\mathbb{F}_q^n$;
- $C^\perp = \{u \in \mathbb{F}_q^n : (u, v) = 0 \text{ for all } v \in C\}$;
- $C^\perp$ is a linear $[n, n-k]$ code;
- C is a **self-orthogonal code**, if $C \subseteq C^\perp \Rightarrow C \cap C^\perp = C$;
- C is an **LCD code**, if $C \cap C^\perp = \{\mathbf{0}\}$;
- C is a **self-dual code**, if $C = C^\perp$.

Equivalence of codes - Definition 1

Two linear codes of the same length and dimension are equivalent if one can be obtained from the other by a sequence of the following transformations:

(1) a permutation of the coordinate positions of all codewords;

(2) a multiplication of a coordinate of all codewords with a nonzero element from $\mathbb{F}_q$;

(3) a field automorphism.

A sequence of the transformations given above that maps a code C to itself is called an automorphism of C. The set of all automorphisms of C forms a group, called the automophism group of the code and denoted by $\mathrm{Aut}(C)$.

Equivalence of codes

Definition 2:

We say that two codes C_1 and C_2 of the same length over $\mathbb{F}_q$ are equivalent provided there is a monomial matrix M and an automorphism γ of the field such that $C_2 = C_1 M\gamma$.

- $M = PD$ - a monomial matrix
- P - a permutation matrix
- D - a diagonal matrix
- $\gamma \in \mathrm{Gal}(\mathbb{F}_q)$

Automorphisms of codes

Let C be a code of length n over $\mathbb{F}_q$.

1. The set of coordinate permutations that map the code C to itself forms a group, called the permutation automorphism group of C and denoted by $PAut(C)$, $PAut(C) < S_n$.
2. The set of monomial matrices that map C to itself forms the group $MAut(C)$ called the monomial automorphism group of C.
3. The set of maps of the form $M\gamma$, where M is a monomial matrix and γ is a field automorphism, that map C to itself forms the group $\Gamma\mathrm{Aut}(C)$, called automorphism group of C.
4. If q is a prime then $MAut(C) = \Gamma\mathrm{Aut}(C)$.
5. If $q = 2$ then $PAut(C) = MAut(C) = \Gamma\mathrm{Aut}(C)$.

The permutation automorphisms

We focus on the permutation automorphisms!

$$P \leftrightarrow \sigma \in \mathrm{Sym}(n) \quad \Rightarrow \sigma = \Omega_1 \Omega_2 \dots \Omega_s,$$

where $\Omega_1, \dots, \Omega_s$ are independent cycles.

If l_i is the length of Ω_i, $1 \leq i \leq s$, then

$$\mathrm{ord}\sigma = |\sigma| = \mathrm{lcm}\{l_1, \dots, l_s\} = m.$$

- $F_\sigma(C) = \{v \in C : \sigma(v) = v\}$ - the fixed subcode
- $E_\sigma(C) = \{v \in C : \sum_{i \in \Omega_j} v_i = 0 \text{ in } \mathbb{F}_q,\ i = 1, \dots, s\}$

Theorem:

If $\gcd(m, q) = 1$ then $C = F_\sigma(C) \oplus E_\sigma(C)$, $F_\sigma(C) \perp E_\sigma(C)$.

The fixed subcode $F_\sigma(C) = \{v \in C : \sigma(v) = v\}$, $p = \mathrm{char}\mathbb{F}_q$

$$\sigma = \underbrace{\Omega_1}_{l_1}\underbrace{\Omega_2}_{l_2}\ldots\underbrace{\Omega_s}_{l_s}, \quad \pi : F_\sigma(C) \to \mathbb{F}_q^s,$$

$(\pi(v))_j = v_i$ for some $i \in \Omega_j$, $j = 1, 2, \ldots, s$, $v \in F_\sigma(C)$

Theorem:

Let $l_i \equiv 1 \pmod{p}$ for all $i = 1, \ldots, s$. Then:

(1) if C is self-orthogonal so is $\pi(F_\sigma(C))$;

(2) if C is self-dual so is $\pi(F_\sigma(C))$;

(3) if C is LCD so is $\pi(F_\sigma(C))$.

Theorem:

Let $l_i \equiv 0 \pmod{p}$ for all $i = 1, \ldots, s$. Then $F_\sigma(C)$ is a self-orthogonal code and it is a subcode of $E_\sigma(C)$.

The even subcode $E_\sigma(C)$

$$\sigma = \underbrace{\Omega_1}_{l_1}\underbrace{\Omega_2}_{l_2}\cdots\underbrace{\Omega_s}_{l_s}$$

$$E_\sigma(C) = \{v \in C : \sum_{i\in\Omega_j} v_i = 0 \text{ in } \mathbb{F}_q, i = 1,\ldots,s\}, \quad \psi : \mathbb{F}_q^n \to \mathbb{F}_q^s,$$

$$\psi(v) = (\sum_{i\in\Omega_1} v_i, \ldots, \sum_{i\in\Omega_s} v_i), \ v \in \mathbb{F}_q^n$$

Proposition

ψ is a linear map and $\ker(\psi|_C) = E_\sigma(C)$. Moreover, if C is self-orthogonal, $\gcd(m, q) = 1$, and $l_i \equiv m \pmod p$ for all $i = 1,\ldots,s$, then $\psi(C)$ is also a self-orthogonal code.

The permutation automorphism $\sigma = \Omega_1\Omega_2\ldots\Omega_s$

$$\phi : \mathbb{F}_q^n \to \mathcal{R}_{l_1} \times \mathcal{R}_{l_2} \times \cdots \times \mathcal{R}_{l_s}, \quad \mathcal{R}_\ell = \mathbb{F}_q[x]/(x^\ell - 1)$$

$$\phi(c) = (c_1(x), \ldots, c_s(x)) = (\sum_{i=0}^{l_1-1} c_{1i}x^i, \ldots, \sum_{i=0}^{l_s-1} c_{si}x^i)$$

for $c = (c_{10}, c_{11}, \ldots, c_{1,l_1-1}, \ldots, c_{s0}, c_{s1}, \ldots, c_{s,l_s-1}) \in \mathbb{F}_q^n$

Definition

The subset $\mathcal{A} \subset \mathcal{R}_{l_1} \times \mathcal{R}_{l_2} \times \cdots \times \mathcal{R}_{l_s}$ is a linear code if $v + w \in \mathcal{A}$ for all $v, w \in \mathcal{A}$ and $xv \in \mathcal{A}$ for all $v \in \mathcal{A}$.

Lemma

If C is a linear code over the field $\mathbb{F}_q$ having an automorphism σ, then $\phi(C)$ is a linear code in $\mathcal{R}_{l_1} \times \mathcal{R}_{l_2} \times \cdots \times \mathcal{R}_{l_s}$.

If $l_1 = \cdots = l_s = m$, C is a quasi-cyclic code of length $n = ms$

$$\sigma = \underbrace{\Omega_1}_{m}\underbrace{\Omega_2}_{m}\ldots\underbrace{\Omega_s}_{m} \in \mathrm{Aut}(C)$$

Quasi-cyclic codes are extensively studied!

San Ling and P. Sole, On the algebraic structure of quasi-cyclic codes

- I: Finite fields, 2001;
- II: Chain Rings, 2003;
- III: Generator Theory, 2005;
- IV: Repeated Roots, 2006.

If $l_1 = \cdots = l_s = m$, C is a quasi-cyclic code of length $n = ms$

$$\sigma = \Omega_1 \Omega_2 \dots \Omega_s \in \mathrm{Aut}(C)$$

$$\phi : \mathbb{F}_q^{ms} \to \mathcal{R}_m^s, \quad \mathcal{R}_m = \mathbb{F}_q[x]/(x^m - 1)$$

$$c = (c_{01}, c_{02}, \dots, c_{0s}, c_{11}, \dots, c_{1,s}, \dots, c_{m-1,1}, \dots, c_{m-1,s})$$

$$\downarrow$$

$$c = (\underbrace{c_{01}, c_{11}, \dots, c_{m-1,1}}_{\Omega_1}, \underbrace{c_{02}, \dots, c_{m-1,2}}_{\Omega_2}, \dots, \underbrace{c_{0,s}, \dots, c_{m-1,s}}_{\Omega_s})$$

$$\downarrow$$

$$\phi(c) = (c_1(x), \dots, c_s(x)), \quad c_i(x) = c_{0i} + c_{1i}x + \cdots + c_{m-1,i}x^{m-1}$$

If $l_1 = \cdots = l_s = m$, C is a quasi-cyclic code of length $n = ms$

$$\sigma = \Omega_1\Omega_2\ldots\Omega_s \in \mathrm{Aut}(C), \quad \gcd(m, q) = 1$$

$$\phi : \mathbb{F}_q^{ms} \to \mathcal{R}_m^s, \quad \mathcal{R}_m = \mathbb{F}_q[x]/(x^m - 1)$$

$$x^m - 1 = \delta \underbrace{g_0(x)g_1(x)\cdots g_r(x)h_1(x)h_1^*(x)\cdots h_t(x)h_t^*(x)}_{\text{irreducible factors}},$$

where $h_j^*(x) \neq h_j(x)$ is the reciprocal polynomial of $h_j(x)$, $g_i^*(x) = g_i(x)$, $i = 0, 1, \ldots, r$, $g_0(x) = x - 1$.

$$\Rightarrow \mathcal{R}_m = G_0 \oplus \cdots \oplus G_r \oplus H_1' \oplus H_1'' \oplus \cdots \oplus H_t' \oplus H_t'',$$

$$G_i = \langle \tfrac{x^m-1}{g_i(x)} \rangle \lhd \mathcal{R}_m,\ G_i \cong \mathbb{F}_q[x]/(g_i(x)),\ i = 0, 1, \ldots, r,$$
$$H_j' = \langle \tfrac{x^m-1}{h_j(x)} \rangle \lhd \mathcal{R}_m,\ H_j' \cong \mathbb{F}_q[x]/(h_j(x)),\ j = 1, \ldots, t,$$
$$H_j'' = \langle \tfrac{x^m-1}{h_j^*(x)} \rangle \lhd \mathcal{R}_m,\ H_j'' \cong \mathbb{F}_q[x]/(h_j^*(x)),\ j = 1, \ldots, t$$

If $l_1 = \cdots = l_s = m$, C is a quasi-cyclic code of length $n = ms$

$$\mathcal{R}_m = \mathbb{F}_q[x]/(x^m - 1) = G_0 \oplus \cdots \oplus G_r \oplus H'_1 \oplus H''_1 \oplus \cdots \oplus H'_t \oplus H''_t,$$

$\mathcal{A}$ - a linear code of length s over $\mathcal{R}_m$

$$\mathcal{A} = \mathcal{A}_0 \oplus \cdots \oplus \mathcal{A}_r \oplus \mathcal{A}'_1 \oplus \mathcal{A}''_1 \oplus \cdots \oplus \mathcal{A}'_t \oplus \mathcal{A}''_t,$$

$\mathcal{A}_i$ - a linear code over G_i of length s, $0 \leq i \leq r$
$\mathcal{A}'_i$ - a linear code over H'_i of length s, $1 \leq i \leq t$
$\mathcal{A}''_i$ - a linear code over H''_i of length s, $1 \leq i \leq t$

$$G_0 = \langle 1 + x + \cdots + x^{m-1} \rangle = \{\alpha(1 + x + \cdots + x^{m-1}) \mid \alpha \in \mathbb{F}_q\} \cong \mathbb{F}_q$$

If $l_1 = \cdots = l_s = m$, C is a quasi-cyclic code of length $n = ms$

$$\mathcal{R}_m = \mathbb{F}_q[x]/(x^m - 1) = G_0 \oplus \cdots \oplus G_r \oplus H'_1 \oplus H''_1 \oplus \cdots \oplus H'_t \oplus H''_t,$$

Conjugate elements:

- if $c \in G_0 \cong \mathbb{F}_q$ then $\overline{c} = c$;
- if $c \in G_i$, $1 \leq i \leq r$, then $\overline{c} = c(x^{-1}) = c(x^{m-1}) \in G_i$;
- if $c \in H'_i$, $1 \leq i \leq t$, then $\overline{c} = c(x^{-1}) = c(x^{m-1}) \in H''_i$

$c = (c_0, \ldots, c_r, c'_1, c''_1, \ldots, c'_t, c''_t) \rightarrow \overline{c} = (\overline{c}_0, \ldots, \overline{c}_r, c''_1, c'_1, \ldots, c''_t, c'_t)$

Hermitian inner product

If $a, b \in \mathcal{R}_m^s$ then $\langle a, b \rangle = \sum_{i=1}^{s} a_i \overline{b}_i =$

$$(\sum_i a_{i0}\overline{b}_{i0}, \ldots, \sum_i a_{ir}\overline{b}_{ir}, \sum_i a'_{i1}b''_{i1}, a''_{i1}b'_{i1}, \ldots, a'_{it}b''_{it}, a''_{it}b'_{it})$$

If $l_1 = \cdots = l_s = m$, C is a quasi-cyclic code of length $n = ms$

$$\sigma = \Omega_1\Omega_2 \ldots \Omega_s \in PAut(C), \quad \gcd(m, q) = 1$$

$$\mathcal{R}_m = \mathbb{F}_q[x]/(x^m - 1) = G_0 \oplus \cdots \oplus G_r \oplus H_1' \oplus H_1'' \oplus \cdots \oplus H_t' \oplus H_t'',$$

$$C \longleftrightarrow \phi(C) = C_0 \oplus \cdots \oplus C_r \oplus C_1' \oplus C_1'' \oplus \cdots \oplus C_t' \oplus C_t''$$

Theorem:

C is a self-dual code with respect to the Euclidean inner product $\iff$ C_i are self-dual codes over G_i, $i = 0, 1, \ldots, r$ with respect to the defined Hermitian inner product, and $C_j'' = (C_j')^{\perp}$, $j = 1, \ldots, t$, with respect to the Euclidean inner product.

$\phi^{-1}(C_0) = \{c \in C \ : \ \sigma(c) = c\}$ - the fixed subcode of C

If $l_1 = \cdots = l_s = m$, C is a quasi-cyclic code of length $n = ms$

$$\sigma = \Omega_1\Omega_2 \ldots \Omega_s \in PAut(C), \quad \gcd(m, q) = 1$$

$$\mathcal{R}_m = \mathbb{F}_q[x]/(x^m - 1) = G_0 \oplus \cdots \oplus G_r \oplus H'_1 \oplus H''_1 \oplus \cdots \oplus H'_t \oplus H''_t,$$

$$C \longleftrightarrow \phi(C) = C_0 \oplus \cdots \oplus C_r \oplus C'_1 \oplus C''_1 \oplus \cdots \oplus C'_t \oplus C''_t$$

Theorem:

C is an Euclidean LCD code $\iff$ C_i are LCD codes over G_i, $i = 0, 1, \ldots, r$ with respect to the defined Hermitian inner product, $C''_j \cap (C'_j)^\perp = \{0\}$ and $C'_j \cap (C''_j)^\perp = \{0\}$, $j = 1, \ldots, t$, with respect to the Euclidean inner product.

If $l_1 = \cdots = l_s = m$, C is a quasi-cyclic code of length $n = ms$

$$\sigma = \Omega_1\Omega_2 \ldots \Omega_s \in \mathrm{Aut}(C), \quad m = p^a m', \gcd(m', q) = 1$$

$$\phi : \mathbb{F}_q^{ms} \to \mathcal{R}_m^s, \quad \mathcal{R}_m = \mathbb{F}_q[x]/(x^m - 1)$$

$$x^m - 1 = (\delta g_0 g_1 \cdots g_r h_1 h_1^* \cdots h_t h_t^*)^{p^a},$$

where $h_j^*(x) \neq h_j(x)$ is the reciprocal polynomial of $h_j(x)$, $g_i^*(x) = g_i(x)$, $i = 0, 1, \ldots, r$, $g_0(x) = x - 1$.

$$\Rightarrow \mathcal{R}_m = (\bigoplus_{i=0}^{r} \mathbb{F}_q[x]/(g_i^{p^a})) \oplus (\bigoplus_{i=1}^{t} (\mathbb{F}_q[x]/(h_i^{p^a}) \oplus \mathbb{F}_q[x]/((h_i^*)^{p^a}))$$

If f is a monic irreducible factor of $x^{m'} - 1$ then the factor ring $\mathbb{F}_q[x]/(f^{p^a})$ can be identified with the finite chain ring $\mathbb{F}_{q^k} + u\mathbb{F}_{q^k} + \cdots + u^{p^a-1}\mathbb{F}_{q^k}$, where $u^{p^a} = 0$.

If $l_1 = \cdots = l_s = m$, C is a quasi-cyclic code of length $n = ms$

$$\sigma = \Omega_1\Omega_2 \ldots \Omega_s \in \mathrm{Aut}(C), \quad m = p^a m', \gcd(m', q) = 1$$

$$\phi : \mathbb{F}_q^{ms} \to \mathcal{R}_m^s, \quad \mathcal{R}_m = \mathbb{F}_q[x]/(x^m - 1)$$

Lemma

Let C be a quasi-cyclic code over $\mathbb{F}_q$ of length sm and of index s. Then $\phi(C)^\perp = \phi(C^\perp)$, where the dual in $\mathbb{F}_q^{ms}$ is taken with respect to the Euclidean inner product, while the dual in $\mathcal{R}_m^s$ is taken with respect to the Hermitian inner product. In particular, a quasi-cyclic code C over $\mathbb{F}_q$ is self-dual with respect to the Euclidean inner product if and only if $\phi(C)$ is self-dual over $\mathcal{R}_m$ with respect to the Hermitian inner product.

$\sigma = \Omega_1\Omega_2\ldots\Omega_s \in PAut(C)$, $m = p^a m'$, $\gcd(m', q) = 1$

$$x^m - 1 = (\delta g_0 g_1 \cdots g_r h_1 h_1^* \cdots h_t h_t^*)^{p^a}$$

$$\Rightarrow \mathcal{R}_m = (\bigoplus_{i=0}^{r} \mathbb{F}_q[x]/(g_i^{p^a})) \oplus (\bigoplus_{i=1}^{t} (\mathbb{F}_q[x]/(h_i^{p^a}) \oplus \mathbb{F}_q[x]/((h_i^*)^{p^a}))$$

Theorem

A linear code $\mathcal{A}$ over $\mathcal{R}_m$ of length s is self-dual with respect to the Hermitian inner product if and only if $\mathcal{A} = (\bigoplus_{i=0}^{r} \mathcal{A}_i) \oplus (\bigoplus_{i=1}^{t} (\mathcal{A}'_j \oplus (\mathcal{A}'_j)^{\perp}))$, where, for $0 \leq i \leq r$, $\mathcal{A}_i$ is a self-dual code over R_i of length s (with respect to the Hermitian inner product) and, for $1 \leq j \leq t$, $\mathcal{A}'_j$ is a linear code of length s over R'_j and $(\mathcal{A}'_j)^{\perp}$ is its dual with respect to the Euclidean inner product.

If $l_1 = \cdots = l_s = m$, C is a quasi-cyclic code of length $n = ms$

$$\sigma = \Omega_1\Omega_2 \ldots \Omega_s \in \mathrm{Aut}(C), \quad m = p^a m', \gcd(m', q) = 1$$

$$F_\sigma(C) := \{v \in C \mid v\sigma = v\}, \quad \pi : F_\sigma(C) \to \mathbb{F}_q^{c+f},$$

Theorem

Let $\psi : C \to \mathbb{F}_q^s$ be the map defined by

$$\psi(c) = (\sum_{i\in\Omega_1} c_i, \ldots, \sum_{i\in\Omega_s} c_i).$$

If C is a self-orthogonal code then $C_\psi = \psi(C)$ is also self-orthogonal, and $C_\pi = \pi(F_\sigma(C)) \subset C_\psi^\perp$. If C is self-dual then $C_\pi = C_\psi^\perp$.

The permutation automorphisms - some restrictions

C - almost quasi-cyclic code of length $n = mc + f$

$$\sigma = \underbrace{\Omega_1 \dots \Omega_c}_{\text{order } m} \underbrace{\Omega_{c+1} \dots \Omega_{c+f}}_{\text{fixed points}} \in PAut(C)$$

A question for colleagues:

Which is better - almost quasi-cyclic, near quasi-cyclic or something else?

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

$E_\sigma(C)$ has f zero coordinates
$E_\sigma(C)^*$ - $E_\sigma(C)$ without the last f coordinates
$E_\sigma(C)^*$ - a quasi-cyclic code of length cm

The permutation automorphisms - some restrictions

$$\sigma = \underbrace{\Omega_1 \dots \Omega_c}_{\text{order } m} \underbrace{\Omega_{c+1} \dots \Omega_{c+f}}_{\text{fixed points}} \in PAut(C)$$

$$F_\sigma(C) := \{v \in C \mid v\sigma = v\}, \quad \pi : F_\sigma(C) \to \mathbb{F}_q^{c+f},$$

$(\pi(v))_j = v_i$ for some $i \in \Omega_j$, $j = 1, 2, \dots, c+f$, $v \in F_\sigma(C)$

Corollary

Let $m \equiv 1 \pmod{p}$. Then:

(1) if C is self-orthogonal so is $\pi(F_\sigma(C))$;

(2) if C is self-dual so is $\pi(F_\sigma(C))$;

(3) if C is LCD so is $\pi(F_\sigma(C))$.

The permutation automorphisms - some restrictions

Why focus on quasi-cyclic and almost quasi-cyclic codes?

Cauchy's theorem (a corollary to Sylow's first theorem)

Given a finite group G and a prime number r dividing the order of G, then there exists an element (and thus a cyclic subgroup generated by this element) of order r in G.

Lemma (W. Cary Huffman)

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

Automorphisms of prime order

- W.C.Huffman, Decomposing and shortening codes using automorphisms, *IEEE Trans. Inform. Theory*, 1986.
- W.C. Huffman, Automorphisms of Codes with Applications to Extremal Doubly Even Codes of Length 48, *IEEE Transactions on Information Theory*, 1982.
- W.C. Huffman, On extremal self-dual quaternary codes of lengths 18 to 28, I and II, *IEEE Trans. Inform. Theory*, 1990 and 1991.
- W. C. Huffman, On extremal self-dual ternary codes of lengths 28 to 40, *IEEE Trans. Inform. Theory* 1992.
- W. C. Huffman, Self-dual $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes with an automorphism of prime order, *Advances in Mathematics of Communications*, 2013.

Self-dual and LCD codes

- V. Yorgov, A method for Constructing Inequivalent Self-Dual Codes with Applications to Length 56, *IEEE Trans. Inform. Theory*, 1987.
- G. Nebe, On Extremal Self-Dual Ternary Codes of Length 48, *International Journal of Combinatorics*, 2012.
- M. Borello and W. Willems, Automorphisms of Order $2p$ in Binary Self-Dual Extremal Codes of Length a Multiple of 24, *IEEE Trans. Inform. Theory*, 2013.
- S.Buyuklieva, A method for constructing self-dual codes with an automorphism of order 2, *IEEE Trans. Inf. Theory*, 2000.
- S. Bouyuklieva, J. de la Cruz, On the Structure of Binary LCD Codes having an Automorphism of Odd Prime Order, *IEEE Trans. Inf. Theory*, 2022.

The automorphism group of a putative self-dual $[72, 36, 16]$ code

Suppose that C is a self-dual $[72, 36, 16]$ binary code. If the prime p divides $|Aut(C)|$ then:

- $p \leq 17$ and $p \neq 13$ (Conway and Pless, 1982)
- $p \neq 17$ (Pless and Thompson, 1982)
- $p \neq 11$ (Huffman and Yorgov, 1987)
- if $\sigma \in Aut(C)$ is of order 2 or 3 then σ does not fixed points (Bouyuklieva, 2002, 2004)
- V. Yorgov, On the automorphism group of a putative code, *IEEE Trans. Inf. Theory*, 2006.

The automorphism group of a putative self-dual $[72, 36, 16]$ code

The automorphism group of a binary self-dual doubly even $[72, 36, 16]$ code

- is a solvable group of order 5, 7, 10, 14, 56, or a divisor of 72 (Bouyuklieva, O'Brien, Willems, 2006).
- has order 5, 7, 10, 14, or d where d divides 18 or 24, or it is $A_4 \times C_3$ (O'Brien, Willems, 2011):.
- has order 5 or d where d divides 24 (Yankov, Gabriele Nebe, Thomas Feulner).
- is either cyclic of order 1, 2, 3, 4, 5 or elementary abelian of order 4 (M. Borello, F. Dalla Volta and G. Nebe. 2013; M. Borello, 2014).
- does not have an element of order 4 (V. Yorgov and D. Yorgov, 2014).

The putative self-dual $[72, 36, 16]$ code

Gerald Janusz, Solution of the $[72, 36, 16]$ Problem, arXiv:2210.02551v2, 9 Nov 2022.

This is the Mathematica file (or as close to the Mathematica file as TeX would allow) that computed the covering polynomials reported in the paper [2], No Type II Code Has Parameters $[72, 36, 16]$ submitted to Designs, Codes and Cryptography on Sept. 22, 2022. We compute enough covering polynomials to show that no Type II binary code has parameters $[72, 36, 16]$ or $[96, 48, 20]$. See [1] for definitions and the recursion formula.

1 Janusz, Gerald J. Covering polynomials and projections of self-dual codes. Des. Codes Cryptogr. (2022).

2 Janusz, Gerald J. No Type II Code Has Parameters [72, 36, 16], submitted.