On the binary self-dual $[96, 48, 20]$ codes with an automorphism of order 9

Nikolay I. Yankov

Shumen University, Bulgaria

VII-th International Workshop on Optimal Codes and Related Topics, OC 2013, Albena, Bulgaria
10.09.2013

Outline

- Introduction
- Construction method
- Binary $[96, 48, 20]$ self-dual code
- Results

The existence of binary self-dual $[24k, 12k, 4k+4]$, $k \geq 3$ code

$k = 1$ $[24, 12, 8]$ – the Golay code G_{24} – unique (Pless, 1968), $\mathrm{Aut}(G_{24}) = M_{24}$, $|M_{24}| = 244{,}823{,}040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$

$k = 2$ a $[48, 24, 12]$ – the extended quadratic residue code QR_{48} – unique (Houghten et al. 2003), $\mathrm{Aut}(QR_{48}) = \mathrm{PSL}_2(47)$, $|PSL_2(47)| = 103{,}776 = 2^5 \cdot 3 \cdot 23 \cdot 47$

$k = 3$

N.J.A. Sloane

Is there a (72,36) $d = 16$ self-dual code?, *IEEE Trans. Inform. Theory*, vol. 19, p. 251, 1973.

Prices for this code:
S.T. Dougherty \$100 for the existence
M. Harada \$200 for the nonexistence

$k = 3$, $[72, 36, 16]$ Automorphism group of order ≤ 5:

- type 2 – $(36, 0)$
- type 3 – $(24, 0)$
- type 5 – $(14, 2)$

$k = 4$, $[96, 48, 20]$: Only 2, 3, or 5 can be primes dividing $|\mathrm{Aut}(C)|$

Bouyuklieva, Russeva, Yankov (2006) – a method for p^2 for a prime $p > 2$

Let C – $[n, k]$ binary self-dual

σ – an automorphism of C of order p^2 for a odd prime $p > 2$

$$\sigma = \underbrace{\Omega_1 \dots \Omega_c}_{\text{cycles of length } p^2} \underbrace{\Omega_{c+1} \dots \Omega_{c+t}}_{\text{cycles of length } p} \underbrace{\Omega_{c+t+1} \dots \Omega_{c+t+f}}_{\text{fixed points}},$$

$\Omega_i = ((i-1)p^2 + 1, \dots, ip^2)$, $i = 1, \dots, c$ – length p^2

$\Omega_{c+i} = (cp^2 + (i-1)p + 1, \dots, cp^2 + ip)$, $i = 1, \dots, t$, – length p

$\Omega_{c+t+i} = (cp^2 + tp + i)$, $i = 1, \dots, f$, – fixed points

σ is of type $p^2 - (c, t, f)$ and $cp^2 + tp + f = n$.

We define

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

$$E_\sigma(C) = \{v \in C : wt(v|\Omega_i) \equiv 0(\mathrm{mod}2)\},$$

$i = 1, 2, \ldots, c + t + f$, where $v|\Omega_i$ is the restriction of v on Ω_i.

Lemma

The code C is a direct sum of the subcodes $F_\sigma(C)$ and $E_\sigma(C)$

Taking a coordinate from every cycle (they are equal) we define the projective map $\pi : F_\sigma(C) \to \mathbb{F}_2^{c+t+f}$

Lemma

If C is a binary self-dual code having an automorphism σ of type $p^2 - (c, t, f)$ then $C_\pi = \pi(F_\sigma(C))$ is a binary self-dual code of length $c + t + f$.

Let $E_\sigma(C)^*$ be $E_\sigma(C)$ with the last f coordinates deleted

$E_\sigma(C)^*$ is a self-orthogonal binary code of length $cp^2 + tp$,

$$\dim E_\sigma(C)^* = \dim C - \dim F_\sigma(C) = \tfrac{1}{2}(p-1)(c(p+1)+t).$$

For $v \in E_\sigma(C)^*$ we define:

$$v|\Omega_i \xrightarrow{\varphi} \begin{cases} a_0 + a_1x + \cdots + a_{p^2-1}x^{p^2-1} \in T, & i = 1, \ldots, c \\ a_0 + a_1x + \cdots + a_{p-1}x^{p-1} \in P, & i = c+1, \ldots, c+t \end{cases}$$

T – set of even-weight polynomials in $\mathbb{F}_2[x]/(x^{p^2}-1)$

P – set of even-weight polynomials in $\mathbb{F}_2[x]/(x^{p}-1)$

The map $\varphi : E_\sigma(C)^* \to T^c \times P^t$

Definition

A linear code $C \subset T^c \times P^t$ is a subset of $T^c \times P^t$ such that $v + w \in C$ for all $v, w \in C$ and $xv \in C$ for all $v \in C$

Lemma

$C_\varphi = \varphi(E_\sigma(C)^*)$ is a linear code in $T^c \times P^t$

$a(x) \in T, P$ we define conjugation by $\overline{a(x)} = a(x^{-1})$

Hermitian inner product in T is $\langle v, w\rangle = \sum_{i=1}^{c} v_i\overline{w_i}$, $v, w \in T^c$

Similarly, $\langle v', w'\rangle = \sum_{i=1}^{t} v'_i\overline{w'_i}$, $v', w' \in P^t$

Definition

If C is a linear code in $T^c \times P^t$ we define its dual code as the set $C^\perp$ of all vectors (v, v'), $v \in T^c$, $v' \in P^t$ such that $\langle v, w\rangle = Q_{p^2}(x)\,\langle v', w'\rangle$ for all vectors $(w, w') \in C$, $w \in T^c$, $w' \in P^t$, $Q_{p^2}(x) = Q_p(x^p) = x^{p(p-1)} + x^{p(p-2)} + \cdots + x^{p+1}$ – the p^2-th cyclotomic polynomial

If $C = C^\perp$ we call it self-dual

Lemma

If C is a linear code in $T^c \times P^t$, so is its dual code $C^\perp$

Theorem

A binary code C having an automorphism σ is self-dual iff C_π is a binary self-dual code and $C_\varphi = \varphi(E_\sigma(C)^*)$ is a self-dual code in $T^c \times P^t$

Consider the factor ring

$$R = \mathbb{F}_q[x]/(x^n - 1),$$

where $(x^n - 1)$ is the principal ideal in $\mathbb{F}_q[x]$ generated by $x^n - 1$

When $n = p^2$ for a prime p, we have the following decomposition of the polynomial

$$x^{p^2} - 1 = (x - 1)Q_{p^2}(x)Q_p(x),$$

where $Q_p(x) = 1 + x + \cdots + x^{p-1}$ and $Q_{p^2}(x) = Q_p(x^p)$ are cyclotomic polynomials

$Q_p(x) = g_1(x) \ldots g_s(x)$, $Q_{p^2}(x) = h_1(x) \ldots h_m(x)$

Let

$$G_i = \left\langle \frac{x^{p^2} - 1}{g_i(x)} \right\rangle, i = 1, \ldots, s$$

$$H_i = \left\langle \frac{x^{p^2} - 1}{h_i(x)} \right\rangle, i = 1, \ldots, m$$

We have that, G_i are fields with $\frac{p-1}{s}$ elements for $i = 1, \ldots, s$

H_i are fields with $\frac{p(p-1)}{m}$ elements for $i = 1, \ldots, m$

$$R = \mathbb{F}_q[x]/(x^n - 1) = G_1 \oplus \cdots \oplus G_s \oplus H_1 \oplus \cdots \oplus H_m$$

$\forall a(x) \in T$, $a = a'_1 + \cdots + a'_s + a''_1 + \cdots + a''_m$, where $a'_i \in G_i$, $a''_j \in H_j$

A – a binary linear code of length cp^2 having an automorphism of order p^2 with c independent p^2-cycles

$$M'_j = \{u \in E_\sigma(A) : u_i \in G_j, i = 1, \ldots, c\}, j = 1, \ldots, s$$
$$M''_j = \{u \in E_\sigma(A) : u_i \in H_j, i = 1, \ldots, c\}, j = 1, \ldots, m$$

M'_j – a linear space over G_j, $j = 1, \ldots, s$, M''_j – a linear space over H_j, $j = 1, \ldots, m$

Lemma

$$M = \varphi(E_\sigma(A)) = M_1' \oplus \cdots \oplus M_s' \oplus M_1'' \oplus \cdots \oplus M_m''$$

$$(p-1)\sum_{j=1}^{s} \dim_{G_j} M_j' + (p^2 - p)\sum_{j=1}^{s} \dim_{H_j} M_j'' = \dim E_\sigma(A)$$

2 – a primitive root mod $p^2 \Rightarrow Q_p(x)$ and $Q_{p^2}(x)$ – $\mathbb{F}_2$-irreducible

$P \cong \mathbb{F}_{2^{p-1}}$

$$T = I_1 \oplus I_2,$$

I_1 and I_2 are cyclic codes with parity check $Q_p(x)$ and $Q_{p^2}(x)$

Theorem

When $t = 0$, M_1 and M_2 are Hermitian SD codes over I_1 and I_2

$$I_1 \cong \mathbb{F}_{2^{p-1}}, \qquad I_2 \cong \mathbb{F}_{2^{p^2-p}}, \qquad \varphi(E_\sigma(C)^*) = M_1 \oplus M_2$$

J. De la Cruz

Über die Automorphismengruppe extremaler Codes der Langen 96 und 120. Otto-von-Guericke-Universitat Magdeburg, PhD Thesis (2012)

For a binary self-dual $[96, 48, 20]$ code:

- only 2, 3, or 5 can be primes dividing $|\mathrm{Aut}(C)|$
- for an automorphism of order p^2 we have $p = 3$ and the following types:
    - $9-(10, 0, 6)$
    - $9-(10, 2, 0)$

$[72, 36, 16]$ code with automorphism of order 9 – nonexistent:

N. Yankov

A Putative Doubly Even $[72, 36, 16]$ Code Does Not Have an Automorphism of Order 9, *IEEE Trans. Inform. Theory*, **58(1)**, pp. 159–163 (2012)

Let C be a binary self-dual doubly even $[96, 48, 20]$ codes with an automorphism of order 9

According to the method that C has a generator matrix of the form

$$\mathcal{G} = \begin{pmatrix} \varphi^{-1}(M_2) \\ \varphi^{-1}(M_1) \\ F_\sigma \end{pmatrix}.$$

Every code satisfies the Singleton bound $d \leq n - k + 1$

A code is maximum distance separable or MDS if $d = n - k + 1$

A code is a near MDS or NMDS if $d = n - k$

M_2 is a $[10, 5]$ Hermitian self-dual code over $I_2 \cong \mathbb{F}_{64}$, $d \geq 5$

By Singleton' bound $d \leq n - k + 1 \Rightarrow d = 6$ or $d = 5$

We need to investigate both MDS and NMDS codes

C' – MDS $[10, 5, 6]$ Hermitian self-dual codes over I_2,

$\alpha = (x + 1)e_2$ – primitive element,
$\mathbb{F}_{64} \cong I_2 = \{0, \alpha^k | 0 \leq k \leq 62\}$

$\delta = \alpha^9 = x^2 + x^4 + x^5 + x^7$ of multiplicative order 7

$I_2 = \{0, x^s\delta^l | 0 \leq s \leq 8, 0 \leq l \leq 6\}$.

The minimum distance of $\varphi^{-1}(C')$ must be $d' \geq 20$. The orthogonal condition is $(u, v) = \sum_{i=1}^{n} u_i \overline{v_i} = 0$, $\overline{a} = a^8, a \in I_2$

Lemma

The generator matrix of MDS $[10, 5, 6]$ code C' is $G' = (E_5 | A')$ for

$$A' = \begin{pmatrix} \delta^{a_{11}} & \delta^{a_{12}} & \delta^{a_{13}} & \delta^{a_{14}} & \delta^{a_{15}} \\ \delta^{a_{21}} & \gamma_{22} & \gamma_{23} & \gamma_{24} & \gamma_{25} \\ \delta^{a_{31}} & \gamma_{32} & \gamma_{33} & \gamma_{34} & \gamma_{35} \\ \delta^{a_{41}} & \gamma_{42} & \gamma_{43} & \gamma_{44} & \gamma_{45} \\ \delta^{a_{51}} & \gamma_{52} & \gamma_{53} & \gamma_{54} & \gamma_{55} \end{pmatrix},$$

where $0 \leq a_{11} \leq a_{12} \leq a_{13} \leq a_{14} \leq a_{15} \leq 6$,
$0 \leq a_{21} \leq a_{31} \leq a_{41} \leq a_{51} \leq 6$, $\gamma_{ij} \in I_2^*$, $i = 2, \ldots, 5$, $j = 2, \ldots, 5$.

We have 7 cases for the first row:

- $(e, 0, 0, 0, 0, 0, e, e, e, \delta^3, \delta^3)$
- $(e, 0, 0, 0, 0, 0, e, e, \delta, \delta^2, \delta^5)$
- $(e, 0, 0, 0, 0, 0, e, e, \delta^3, \delta^5, \delta^6)$
- $(e, 0, 0, 0, 0, 0, e, \delta, \delta, \delta^2, \delta^2)$
- $(e, 0, 0, 0, 0, 0, e, \delta, \delta, \delta^3, \delta^3)$
- $(e, 0, 0, 0, 0, 0, e, \delta, \delta, \delta^5, \delta^5)$
- $(e, 0, 0, 0, 0, 0, e, \delta, \delta^2, \delta^3, \delta^6)$

A computer program constructed all 5 rows of A' in each of these 7 cases and found exactly 3144 inequivalent codes

Let C'' be a NMDS $[10, 5, 5]$ Hermitian self-dual codes over I_2 such that the minimum distance of $\varphi^{-1}(C'')$ is $d'' \geq 20$.

Lemma

The generator matrix of the code C'' is $G'' = (E_5 | A'')$ for

$$A'' = \begin{pmatrix} 0 & \delta^{a_{12}} & \delta^{a_{13}} & \delta^{a_{14}} & \delta^{a_{15}} \\ \delta^{a_{21}} & \gamma_{22} & \gamma_{23} & \gamma_{24} & \gamma_{25} \\ \delta^{a_{31}} & \gamma_{32} & \gamma_{33} & \gamma_{34} & \gamma_{35} \\ \delta^{a_{41}} & \gamma_{42} & \gamma_{43} & \gamma_{44} & \gamma_{45} \\ \delta^{a_{51}} & \gamma_{52} & \gamma_{53} & \gamma_{54} & \gamma_{55} \end{pmatrix},$$

where $0 \leq a_{12} \leq a_{13} \leq a_{14} \leq a_{15} \leq 6$,
$0 \leq a_{21} \leq a_{31} \leq a_{41} \leq a_{51} \leq 6$ *(or we have zeros in column 1),*
$\gamma_{ij} \in I_2$, $i = 2, \ldots, 5$, $j = 2, \ldots, 5$

A unique possibility for the first row

$$(e, 0, 0, 0, 0, 0, e, \delta, \delta^5, \delta^6).$$

A computer program computing all codes with generator matrix G'' turn out exactly 6703 codes

M_1 is a quaternary Hermitian self-dual $[10, 5, \geq 4]$ code

There exists two such code with generator matrices $T_k = (E_5|X_i)$, $i = 1, 2$, where

$$X_1 = \begin{pmatrix} 1 & 1 & 1 & w & w^2 \\ 1 & 1 & 1 & w^2 & w \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}, X_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & w & w^2 & w^2 & w^2 \\ 1 & w^2 & w & w & w \\ 0 & 0 & w & w^2 & 1 \\ 0 & 0 & w^2 & w & 1 \end{pmatrix}.$$

- $C_\pi = \pi(F_\sigma(C))$ – binary self-dual $[16, 8, \geq 4]$, 3 such codes: a singly-even d_8^{2+}; 2 doubly-even: d_{16}^+, and e_8^2
- Sets $X_c, X_f \subset \{1, \ldots, 16\}$, $|X_c| = 10$, $|X_f| = 6$, $X_c \cap X_f = \emptyset$
- $w \in C_\pi, \mathrm{wt}(w) = 6$, $|\mathrm{Supp}(w) \cap X_c| = l \Rightarrow$ $|\mathrm{Supp}(w) \cap X_f| = 6 - l$ and $\mathrm{wt}(\pi^{-1}(w)) = 8l + 6$ – singly-even #
- Computer check for X_c and X_f for d_{16}^+, and e_8^2 – unique possible doubly-even code from d_{16}^+

$$B = \left(\begin{array}{c|c} 1000000001 & 000101 \\ 0100000011 & 111110 \\ 0010000010 & 111111 \\ 0001000001 & 010001 \\ 0000100001 & 100001 \\ 0000010011 & 000001 \\ 0000001001 & 001001 \\ 0000000101 & 000011 \end{array}\right)$$

$$\mathcal{G} = \begin{pmatrix} \varphi^{-1}(M_2) \\ \varphi^{-1}(M_1) \\ B \end{pmatrix}$$

We fix the first block $\varphi^{-1}(H_i)$, $i = 1, \ldots, 9847$

G^τ – the matrix G with columns permuted by $\tau \in S_m$

F^τ_σ – the code with generator matrix $\pi^{-1}(B^\tau)$

$I \subseteq \{1, \ldots, 9847\}$ – the set of indices that there exists subcode C' of C, $d' \geq 20$ with generator matrix $G_{1,i,\tau} = \begin{pmatrix} \varphi^{-1}(H_i) \\ F^\tau_\sigma \end{pmatrix}$

By a computer for $G_{1,i,\tau}$, $i = 1, \ldots, 9847$, $\tau \in S_{10}$ we have $|I| = 390$

$$\mathcal{G} = \begin{pmatrix} \varphi^{-1}(M_2) \\ \varphi^{-1}(M_1) \\ B \end{pmatrix}$$

For $k = 1, 2$ we consider all images $\gamma(T_k)$ of T_k, $k = 1, 2$ using compositions of the following maps:

(i) a permutation $\tau \in S_{10}$ acting on the set of columns

(ii) a multiplication of each column by e_1, ω or $\overline{\omega}$ from I_1

(iii) a Galois automorphism γ which interchanges ω and $\overline{\omega}$

Set of indices $J \subseteq I$ such that there exists a subcode C'' of C, $d'' \geq 20$ with generator matrix

$$G_{2,j,k} = \begin{pmatrix} \varphi^{-1}(H_j) \\ \varphi^{-1}(\gamma(T_k)) \end{pmatrix}, k = 1, 2$$

For $k = 1, 2$ and $j \in I$ we have calculate all codes using only compositions of the maps (iii), (ii); and (i) for all permutations $\mu \in S_{10}$ from the right transversal R_k, of S_{10} with respect to $\mathrm{PAut}(T_k)$

$$\mathcal{G} = \begin{pmatrix} \varphi^{-1}(M_2) \\ \varphi^{-1}(M_1) \\ B \end{pmatrix}$$

all have minimum distance $d < 20$

Theorem

There does not exists a binary self-dual doubly-even $[96, 48, 20]$ *code with an automorphism of type* $9-(10, 0, 6)$

Open cases for odd composite order

Study the existence of a $[96, 48, 20]$ code with an automorphism of type:

- $9-(10, 2, 0)$
- $3.5-(6, 2, 0, 0)$