Construction of self-dual codes with an automorphism

Hyun Jin Kim

Ewha Institute of Mathematical Sciences

Coauthors,

Heisook Lee (Ewha Womans University)
June Bok Lee (Yonsei University)
Yoonjin Lee (Ewha Womans University)

November 15, 2012

Contents

1. Introduction

Best codes

- In coding theory, we have been interested in finding the “best” codes. There are notions of *optimal self-dual codes* and *extremal self-dual codes* which can be considered as the the best codes.

Methods

There are two famous methods.

- Huffman and Yorgov : Decomposition theorem
- Harada : Extension method (Kim and Lee)

Huffman and Yorgov

- Self-dual codes with an automorphism of odd prime order p.

Harada

- Construction of self-dual code of length $n+2$ from self-dual code of length n.

2. The code decomposition

Subcodes

Let $\mathcal{C}$ be a binary self-dual code of length n with an automorphism σ of odd prime order p with exactly c independent p-cycles and $f = n - cp$ fixed points in its decomposition. We may assume that

$$\sigma = (1, 2, \ldots, p)(p+1, p+2, \ldots, 2p) \cdots ((c-1)p+1, (c-1)p+2, \ldots, cp)$$

Denote the cycles of σ by $\Omega_1, \Omega_2, \ldots, \Omega_c$ and the fixed points by $\Omega_{c+1}, \Omega_{c+2}, \ldots, \Omega_{c+f}$.

- $\mathbf{F}_\sigma(\mathcal{C}) = \{\mathbf{v} \in \mathcal{C} : \mathbf{v}\sigma = \mathbf{v}\}$
- $\mathbf{E}_\sigma(\mathcal{C}) = \{\mathbf{v} \in \mathcal{C} : wt(\mathbf{v}|\Omega_i) \equiv 0(\mathrm{mod} 2), i = 1, 2, \ldots, c + f\}$,

where $\mathbf{v}|\Omega_i$ is the restriction of $\mathbf{v}$ on Ω_i

Decomposition theorem

- The code $\mathcal{C}$ is a direct sum of the subcodes $\mathbf{F}_{\sigma}(\mathcal{C})$ and $\mathbf{E}_{\sigma}(\mathcal{C})$.

$\mathbf{E}_\sigma(\mathcal{C})$

- Denote by $\mathbf{E}_\sigma(\mathcal{C})^*$ the code $\mathbf{E}_\sigma(\mathcal{C})$ with the last f coordinates deleted.
- $\mathcal{P}$ is the set of all even-weight polynomials in $\mathbb{F}_2[x]/(x^p+1)$. Defind the map $\phi : \mathbf{E}_\sigma(\mathcal{C})^* \to \mathcal{P}^c$ by $v|\Omega_i = (v_0, v_1, \cdots, v_{p-1})$ correspond to polynomial $v_0 + v_1 x + \cdots + v_{p-1}x^{p-1}$ in $\mathcal{P}$ for v in $\mathbf{E}_\sigma(\mathcal{C})^*$.

$\mathbf{F}_\sigma(\mathcal{C})$

- $v \in \mathbf{F}_\sigma(\mathcal{C})$ if and only if $v \in \mathcal{C}$ and v is a constant on each cycle.
- Let $\pi : \mathbf{F}_\sigma(\mathcal{C}) \to \mathbb{F}_2^{c+f}$ be the projection map defined by $(v\pi)_i = v_j$ for $j \in \Omega_i$, $v \in \mathbf{F}_\sigma(\mathcal{C})$.

Huffman and Yorgov

Assume that the polynomial $1 + x + x^2 + \ldots + x^{p-1}$ is irreducible in $\mathbb{F}_p[x]$. A binary $[n, n/2]$ code $\mathcal{C}$ with an automorphism σ is self-dual if and only if the following two conditions hold:

(i) $\pi(\mathbf{F}_\sigma(\mathcal{C}))$ is a self-dual binary code of length $c + f$,

(ii) $\phi(\mathbf{E}_\sigma(\mathcal{C})^*)$ is a self-dual code of length c over the field $\mathcal{P}$ under the inner product

$$(u, v) = \sum_{i=1}^{c} u_i v_i^{2^{(p-1)/2}}.$$

Extension theorem

Let G_0 be a generator matrix of a self-dual code $\mathcal{C}_0$ of length $2n$, and let

$$\mathbf{x} = (x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n})$$

be a vector in $\mathbb{F}_2^{2n}$ such that $\mathbf{x} \cdot \mathbf{x} = 1$, where $\cdot$ denotes the Euclidean inner product. Let

$$y_i := \mathbf{x} \cdot \mathbf{r}_i$$

for $1 \leq i \leq n$, where $\mathbf{r}_i$ is the i-th row vector of G_0. Then the following matrix

$$G = \left(\begin{array}{cc|ccccc} 1 & 0 & x_1 & \cdots & x_i & \cdots & x_{2n} \\ \hline y_1 & y_1 & & & & & \\ \vdots & \vdots & & & G_0 & & \\ y_n & y_n & & & & & \end{array} \right)$$

generates a self-dual code $\mathcal{C}$ of length $2n+2$.

3. Results

Result 1

- If there exists a self-dual code of length $2n$ with automorphism of type $p-(c,f)$ then there exists a self-dual code of length $2n+2$ with automorphism of type $p-(c,f+2)$.

More detail

Assume that $\mathcal{C}$ is a self-dual code of length $2n$ with an automorphism of type $p-(c,f)$, A is the generator matrix of $\mathbf{E}_\sigma(\mathcal{C})^*$ and $\left(X \mid Y\right)$ is the generator matrix of $\mathbf{F}_\sigma(\mathcal{C})$ where the number of columns of the matrix X is pc. Let the generator matrix of $\pi(\mathbf{F}_\sigma(\mathcal{C}))$ be $\left(\overline{X} \mid Y\right)$ and $(\overline{\mathbf{x}}_j \mid \mathbf{y}_j)$ the jth row vector of $(\overline{X} \mid Y)$ for $1 \leq j \leq \frac{c+f}{2}$. Let

$$\overline{G} = \left(\begin{array}{ccc|ccc|cc} x_1 & \cdots & x_c & x_{c+1} & \cdots & x_{c+f} & 0 & 1 \\ \hline & & & & & & y_1 & y_1 \\ & \overline{X} & & & Y & & \vdots & \vdots \\ & & & & & & y_{\frac{c+f}{2}} & y_{\frac{c+f}{2}} \end{array}\right),$$

where

$$y_j = (x_1, \ldots, x_c, x_{c+1}, \ldots, x_{c+f}) \cdot (\overline{\mathbf{x}}_j \mid \mathbf{y}_j)$$

for $1 \leq j \leq \frac{c+f}{2}$.

More detail

Then the matrix

$$G = \left(\begin{array}{ccc} A & \mathbf{0} & 00 \\ \hline & & \\ & \pi^{-1}(\overline{G}) & \end{array} \right)$$

generates a self-dual code of length $2n + 2$ with an automorphism of type $p - (c, f + 2)$.

Extremal condition 1

Let $\mathcal{C}$ be a code with an automorphism σ of type $p-(c, f+2)$ of length $pc+f$ and minimum weight d. In order for $\mathcal{C}$ to have $d \geq 8$ and $p=3$, $d \geq 10$ and $p=5$, or $d \geq 12$ and $p=7$, we need the following conditions: Let $\mathbf{v} \in \pi(\mathbf{F}_\sigma(\mathcal{C}))$.

C.1 : If $\mathbf{v}$ is a codeword of weight 4 then $\mathbf{v}$ has at least 2-nonzero coordinates in the first c coordinates.

C.2 : If $\mathbf{v}$ is a codeword of weight 6 then $\mathbf{v}$ has at least 1-nonzero coordinate in the first c coordinates.

Result 2

Let $\mathcal{C}$ be a binary self-dual $[c+f, (c+f)/2, \geq 4]$ code with generator matrix $(\ X \mid Y\ )$, and let c be the length of X. Assume that c is even and $\mathcal{C}$ satisfies $\mathrm{C.1}$ and $\mathrm{C.2}$. If all codewords generated by X have even weights and $rank(X) < c-1$, then there exists a vector $\mathbf{x} = (x_1, \ldots, x_{c+f})$ in $\mathbb{F}_2^{c+f}$ with $\mathbf{x} \cdot \mathbf{x} = 1$ such that the matrix

$$G = \left(\begin{array}{ccc|ccc|cc} x_1 & \cdots & x_c & x_{c+1} & \cdots & x_{c+f} & 0 & 1 \\ \hline & & & & & & y_1 & y_1 \\ & X & & & Y & & \vdots & \vdots \\ & & & & & & y_{\frac{c+f}{2}} & y_{\frac{c+f}{2}} \end{array}\right)$$

generates a binary $[c+f+2, (c+f)/2+1, \geq 4]$ self-dual code satisfying the conditions $\mathrm{C.1}$ and $\mathrm{C.2}$.

Extremal condition 2

In order for $\mathcal{C}$ to have $d = 4$ and $p = 3$, $d = 8$ and $p = 7$, or $d = 12$ and $p = 11$, we need the conditions $\mathrm{C}.3$ and $\mathrm{C}.4$: Let $\mathbf{v} \in \pi(\mathbf{F}_\sigma(\mathcal{C}))$.

C.3 : If $\mathbf{v}$ is a codeword of weight 2 then $\mathbf{v}$ has at least one nonzero coordinates in the first c coordinates.

C.4 : If $\mathbf{v}$ is a codeword of weight 4 then $\mathbf{v}$ has at least one nonzero coordinates in the first c coordinates.

Extremal condition 3

In order for $\mathcal{C}$ to have either $d = 6$ and $p = 3$, or $d \geq 10$ and $p = 7$, we need the conditions $\mathrm{C}.5$ and $\mathrm{C}.6$: Let $\mathbf{v} \in \pi(\mathbf{F}_\sigma(\mathcal{C}))$.

C.5: If $\mathbf{v}$ is a codeword of weight 2 then $\mathbf{v}$ has all nonzero coordinates in the first c coordinates.

C.6: If $\mathbf{v}$ is a codeword of weight 4 then $\mathbf{v}$ has at least one nonzero coordinates in the first c coordinates.

Extremal condition 4

Let $\mathcal{C}$ be a binary self-dual code of length $c + f$ with the generator matrix

$$G_1 = \left(\begin{array}{c|c} X & \mathbf{0} \\ & I_f \end{array} \right) \tag{1}$$

and let c be the length of X. We consider a vector $\mathbf{v} \in \mathbb{F}_2^c$ which satisfies the following conditions:

A.1 : $\mathbf{v}$ is an odd vector.

A.2 : $\mathbf{v}$ belongs to a different coset from the code which is generated by X.

Extremal condition 5

Let S_j be a subset of $\left\{\frac{c-f}{2}+1, \frac{c-f}{2}+2, \ldots, \frac{c+f}{2}\right\}$ with $|S_j| = f - j$ for $j = 0, 1, \ldots, f$. We note that the total number of such S_j is $\left(\begin{array}{c} f \\ j \end{array}\right)$. Let $S^*_{j,l} = S_j \cup T_l$ for $l = 1, 2, \ldots, 2^{(c-f)/2}$ where T_l is a subset of $\{1, 2, \ldots, \frac{c-f}{2}\}$. Let $\mathbf{r}_i$ be ith row vector of X.

B.1 : $wt(\mathbf{v} + \sum_{i \in S^*_{0,l}} \mathbf{r}_i) \geq 3.$

B.2 : $wt(\mathbf{v} + \sum_{i \in S^*_{2,l}} \mathbf{r}_i) \geq 2.$

B.3 : $wt(\mathbf{v} + \sum_{i \in S^*_{4,l}} \mathbf{r}_i) \geq 1.$

Result 3

- Let $\mathcal{C}$ be a binary self-dual $[c+f, \frac{c+f}{2}, \geq 4]$ code with the generator matrix G_1 in (1). Suppose that $\mathcal{C}$ satisfies $\mathrm{C}.1$ and $\mathrm{C}.2$, $f \geq 6$ and c is even (so f is even). Let $\mathbf{v}$ be a vector of length c satisfying the conditions $\mathrm{A}.1, \mathrm{A}.2, \mathrm{B}.1, \mathrm{B}.2$ and $\mathrm{B}.3$. Then $\mathcal{C}$ can be extended to a binary $[c+f+2, (c+f)/2+1, \geq 4]$ self-dual code satisfying $\mathrm{C}.1$ and $\mathrm{C}.2$.

Result 3

The following matrix is a generator matrix of the extended code of $\mathcal{C}$:

$$G = \left(\begin{array}{c|ccc|cc} & & \mathbf{0} & & y_1 & y_1 \\ X & & & & \vdots & \vdots \\ & & I_f & & & \\ & & & & y_{\frac{c+f}{2}} & y_{\frac{c+f}{2}} \\ \hline \mathbf{v} & 1 & \cdots & 1 & 0 & 1 \end{array}\right) \tag{2}$$

where $y_i := (\mathbf{v} \mid 1, \ldots, 1) \cdot$ ith row vector of G_1 in (1) for $i = 1, 2, \ldots, (c+f)/2$.

4. Examples

We consider vectors which belong to different cosets from the code $\mathcal{C}$. There can be several vectors of the smallest weight in each coset. We call a vector of the smallest weight in each coset *a coset leader* of the coset. If there is a coset leader of weight ≥ 3, then we can find the vector **v** which satisfies the conditions $\mathrm{A}_1, \mathrm{A}_2, \mathrm{B}_1, \mathrm{B}_2, \mathrm{B}_3$, so that we can apply Result 3.

[40,20,8] codes

- We want to construct a binary self-dual $[40, 20, 8]$ code with an automorphism of order 3 using Result 1. Suppose that σ is an automorphism of type $3-(10, 8)$ of an extremal self-dual $[38, 19, 8]$ code.

[40,20,8] codes

The following matrix generates a self-dual code $\mathcal{C}_{38}$ of length 38 with an automorphism σ.

$$
G_{38} = \begin{pmatrix}
01101101101100000000000000000000000000\\
10110110110100000000000000000000000000\\
00000001101101101100000000000000000000\\
00000010110110110100000000000000000000\\
00000000000001101101101100000000000000\\
00000000000010110110110100000000000000\\
00000000000000000001101101101100000000\\
00000000000000000010110110110100000000\\
01100001100001100001100010111000000000\\
10100010100010100010100011001100000000\\
11111100011100000011100000000000000000\\
11111111100011100000000011100010000000\\
11100011111111100000000011100001000000\\
11100011100011111111111111100000100000\\
00000011100011111100011100011100010000\\
11100011100011111111100011111100001000\\
11100011100011100011111111111100000100\\
00000011100000011100011111111100000010\\
00000000000011111100011111111100000001
\end{pmatrix}
$$

[40,20,8] codes

In this case, $\pi(\mathbf{F}_\sigma(\mathcal{C}_{38}))$ is equivalent to H_{18} [1]. A $[20, 10, 4]$ code can be constructed from $\pi(\mathbf{F}_\sigma(\mathcal{C}_{38}))$ by using Result 1 and Result 3 with the vector $\mathbf{v} = (0, 0, 0, 1, 0, \ldots, 0)$, and this code is equivalent to S_{20} [1]. From this $[20, 10, 4]$ code we find an extremal self-dual code $\mathcal{C}_{40}$ of length 40 by using Result 1 and Result 3.

[1] V. Pless, N.J.A. Sloane, H.N. Ward, *Ternary codes of minimum weight 6 and the classification of the self-dual codes of length 20*, IEEE Trans. Inform. Theory 26 (1980) 306-316.

[40,20,8] codes

The following matrix is a generator matrix of $\pi(\mathbf{F}_\sigma(\mathcal{C}_{40}))$.

$$\begin{pmatrix}
00010000001111111110\\
11010010000000000011\\
11101000101000000011\\
10111000100100000000\\
10101111100010000011\\
00101101010001000011\\
10101110110000100011\\
10101011110000010011\\
00100101110000001011\\
00001101110000000111
\end{pmatrix}$$

[54,27,10] codes

- We obtain new extremal self-dual codes of length 54 with an automorphism of order 7 using Result 1. Three inequivalent binary self-dual $[54, 27, 10]$ codes with an automorphism of order 7 are constructed from the binary self-dual code of length 52 in [2].

[2] W. C. Huffman, *The* $[52, 26, 10]$ *binary self-dual codes with an automorphism of order* 7, Finite Fields Appl.,7 (2001), 341-349.

[54,27,10] codes

$$G_{54,1} = \begin{pmatrix}
111010000000000000000000000000000001110100111010000000 \\
011101000000000000000000000000000000111010011101000000 \\
001110100000000000000000000000000000011101001110100000 \\
000000011101000000000000000000000001110100011101000000 \\
000000001110100000000000000000000000111010001110100000 \\
000000000111010000000000000000000000011101100111000000 \\
000000000000001110100000000111010011101000000000000000 \\
000000000000000111010000000011101001110100000000000000 \\
000000000000000011101000000001110100111010000000000000 \\
000000000000000000000111010011101000111010011101000000 \\
000000000000000000000011101001110100011101001110100000 \\
000000000000000000000001110100111011001110100111000000 \\
000000000000001001011100101110010110000000000000000000 \\
000000000000001100101110010111001010000000000000000000 \\
000000000000001110010111001011100100000000000000000000 \\
100101110010111001011001011100000001001011000000000000 \\
110010111001011100101100101100000001100101000000000000 \\
111001011100101110010110010100000001110010000000000000 \\
100101100101110000000001011100000000000000100101100000 \\
110010110010110000000100101100000000000000110010100000 \\
111001011001010000000110010100000000000000111001000000 \\
111111111111110000000000000000000000000000000000000011 \\
000000000000001111111111111111111110000000111111100011 \\
000000000000001111111000000000000001111111111111110000 \\
000000000000000000000111111100000001111111111111101000 \\
000000000000001111111111111100000001111111000000000111 \\
111111100000001111111000000000000000000000000000010001
\end{pmatrix},$$

[54,27,10] codes

$$G_{54,2} = \begin{pmatrix}
111010000000000000000000000000000000111010011101000000 \\
011101000000000000000000000000000000011101001110100000 \\
001110100000000000000000000000000000001110100111010000 \\
000000011101000000000000000000000000111010001110100000 \\
000000001110100000000000000000000000011101000111010000 \\
000000000111010000000000000000000000001110110011100000 \\
000000000000001110100000000111010011101000000000000000 \\
000000000000000111010000000011101001110100000000000000 \\
000000000000000011101000000001110100111010000000000000 \\
000000000000000000000111010011101000111010011101000000 \\
000000000000000000000011101001110100011101001110100000 \\
000000000000000000000001110100111011001110100111000000 \\
000000000000001001011100101110010110000000000000000000 \\
000000000000001100101110010111001010000000000000000000 \\
000000000000001110010111001011100100000000000000000000 \\
100101110010111001011001011100000001001011000000000000 \\
110010111001011100101100101100000001100101000000000000 \\
111001011100101110010110010100000001110010000000000000 \\
100101100101110000000001011100000000000000001001011000 \\
110010110010110000000100101100000000000000001100101000 \\
111001011001010000000110010100000000000000001110010000 \\
111111111111110000000000000000000000000000000000000011 \\
000000000000001111111111111111111110000000111111100011 \\
000000000000001111111000000000000001111111111111110000 \\
000000000000000000000111111100000001111111111111101011 \\
000000000000001111111111111100000001111111000000000100 \\
111111100000001111111000000000000001111111000000000001
\end{pmatrix},$$

[54,27,10] codes

$$G_{54,3} = \begin{pmatrix}
111010000000000000000000000000000001110100111010000000 \\
011101000000000000000000000000000000111010011101000000 \\
001110100000000000000000000000000000011101001110100000 \\
000000011101000000000000000000000001110100011101000000 \\
000000001110100000000000000000000000111010001110100000 \\
000000000111010000000000000000000000011101100111000000 \\
000000000000001110100000000011101001110100000000000000 \\
000000000000000111010000000001110100111010000000000000 \\
000000000000000011101000000000111010011101000000000000 \\
000000000000000000000111010011101000111010011101000000 \\
000000000000000000000011101001110100011101001110100000 \\
000000000000000000000001110100111011001110100111000000 \\
000000000000001001011100101110010110000000000000000000 \\
000000000000001100101110010111001010000000000000000000 \\
000000000000001110010111001011100100000000000000000000 \\
100101110010111001011001011100000001001011000000000000 \\
110010111001011100101100101100000001100101000000000000 \\
111001011100101110010110010100000001110010000000000000 \\
100101100101110000000001011100000000000000100101100000 \\
110010110010110000000100101100000000000000110010100000 \\
111001011001010000000110010100000000000000111001000000 \\
111111111111110000000000000000000000000000000000000011 \\
000000000000001111111111111111111110000000111111100011 \\
000000000000001111111000000000000001111111111111110011 \\
000000000000000000000111111100000001111111111111101011 \\
000000000000001111111111111100000001111111000000000111 \\
111111100000001111111000000000000000000000000000001001
\end{pmatrix}$$

[58,29,10] codes 1

- We construct extremal self-dual codes of length 58. Firstly, we construct binary self-dual codes of length 56 with an automorphism of order 3 with 18 independent cycles from a binary extremal self-dual code of length 54 with an automorphism of order 3 with 18 independent cycles using Result 1.

[58,29,10] codes 1

- We construct extremal self-dual codes of length 58. Firstly, we construct binary self-dual codes of length 56 with an automorphism of order 3 with 18 independent cycles from a binary extremal self-dual code of length 54 with an automorphism of order 3 with 18 independent cycles using Result 1.

[3] S. Bouyuklieva and P. Östergård, *New constructions of optimal self-dual binary codes of length* 54, Des. Codes Crypt., **41** (2006), 101–109.

[54,27,10] code

$$
\begin{pmatrix}
011011011011011011011000000000000000000000000000000011\\
101101101101101101101000000000000000000000000000000101\\
110101101101011011011110101000000000000000000000011000\\
011110110110101101101011110000000000000000000000101000\\
110110011000101101011110000000000000000000000011000000\\
011011101000110110101011000000000000000000000101000000\\
110110110110110101011110110000000000000000011000000000\\
011011011011011110101011011000000000000000101000000000\\
110000101000110110011011011000000000000011000000000000\\
011000110000011011101101101000000000000101000000000000\\
110000101110000110011000000000000000011000000000000000\\
011000110011000011101000000000000000101000000000000000\\
101110011110101000011101000000000011000000000000000000\\
110011101011110000101110000000000101000000000000000000\\
011101011000011110000110011000011000000000000000000000\\
101110101000101011000011101000101000000000000000000000\\
110011101000000000000011011001100000000000000000000000\\
011101110000000000000011011101000000000000000000000000\\
111111111111000000000000000000000000000000000000000000\\
000000111111111111000000000000000000000000000000000000\\
000000000000111111000111000000000000000111000000000000\\
000000000000000000000111000000111000000111000000111000\\
111000111000111000000111000000111000000000000111000000\\
000000000000000000111000111111000000000000111000000000\\
000000000000000000000000000111000111000000111000000111\\
000000000000000000111000000111000000111000000000000111\\
111111111111111111111111111111111111111111111111111111
\end{pmatrix}.
$$

[58,29,10] codes 1

We present the generator matrix of $\pi(\mathbf{F}_\sigma(\mathcal{C}_{58}))$ as follows:

$$
\begin{pmatrix}
1100000010000000000001\\
1111111111111111111111\\
0000110100000100001100\\
0000000001010010011100\\
0011110000000000001100\\
0000001011000010001111\\
1010100100100001000011\\
1000100001000000000111\\
1111000000000000001100\\
0000001001001000011100\\
0000000100100100100000
\end{pmatrix},
\begin{pmatrix}
1010000010000000000001\\
1111111111111111111111\\
0000110100000100001100\\
0000000001010010011100\\
0011110000000000001111\\
0000001011000010001111\\
1010100100100001000000\\
1000100001000000000111\\
1111000000000000001100\\
0000001001001000011100\\
0000000100100100100000
\end{pmatrix},
\begin{pmatrix}
0110000010000000000001\\
1111111111111111111111\\
0000110100000100001100\\
0000000001010010011100\\
0011110000000000001111\\
0000001011000010001111\\
1010100100100001000011\\
1000100001000000000100\\
1111000000000000001100\\
0000001001001000011100\\
0000000100100100100000
\end{pmatrix},
$$

$$
\begin{pmatrix}
1001000010000000000001\\
1111111111111111111111\\
0000110100000100001100\\
0000000001010010011100\\
0011110000000000001111\\
0000001011000010001111\\
1010100100100001000011\\
1000100001000000000111\\
1111000000000000001100\\
0000001001001000011100\\
0000000100100100100000
\end{pmatrix},
\begin{pmatrix}
0011000010000000000001\\
1111111111111111111111\\
0000110100000100001100\\
0000000001010010011100\\
0011110000000000001100\\
0000001011000010001111\\
1010100100100001000011\\
1000100001000000000100\\
1111000000000000001100\\
0000001001001000011100\\
0000000100100100100000
\end{pmatrix},
\begin{pmatrix}
1000000100100000000001\\
1111111111111111111111\\
0000110100000100001111\\
0000000001010010011100\\
0011110000000000001100\\
0000001011000010001100\\
1010100100100001000011\\
1000100001000000000111\\
1111000000000000001111\\
0000001001001000011100\\
0000000100100100100000
\end{pmatrix},
$$

[58,29,10] codes 1

$$
\begin{pmatrix}
0001010010000000000001\\
1111111111111111111111\\
0000110100000100001111\\
0000000001010010011100\\
0011110000000000001100\\
0000001011000010001111\\
1010100100100001000000\\
1000100001000000000100\\
1111000000000000001111\\
0000001001001000011100\\
0000000100100100100000
\end{pmatrix},
\begin{pmatrix}
1100000000001000000001\\
1111111111111111111111\\
0000110100000100001100\\
0000000001010010011111\\
0011110000000000001100\\
0000001011000010001100\\
1010100100100001000011\\
1000100001000000000111\\
1111000000000000001100\\
0000001001001000011100\\
0000000100100100100000
\end{pmatrix},
\begin{pmatrix}
1001000000001000000001\\
1111111111111111111111\\
0000110100000100001100\\
0000000001010010011111\\
0011110000000000001111\\
0000001011000010001100\\
1010100100100001000011\\
1000100001000000000111\\
1111000000000000001100\\
0000001001001000011100\\
0000000100100100100000
\end{pmatrix},
$$

$$
\begin{pmatrix}
0110000000000100000001\\
1111111111111111111111\\
0000110100000100001111\\
0000000001010010011100\\
0011110000000000001111\\
0000001011000010001100\\
1010100100100001000011\\
1000100001000000000100\\
1111000000000000001100\\
0000001001001000011100\\
0000000100100100100011
\end{pmatrix},
\begin{pmatrix}
0011000000001000000001\\
1111111111111111111111\\
0000110100000100001100\\
0000000001010010011111\\
0011110000000000001100\\
0000001011000010001100\\
1010100100100001000011\\
1000100001000000000100\\
1111000000000000001100\\
0000001001001000011100\\
0000000100100100100000
\end{pmatrix},
\begin{pmatrix}
1010000000000001000001\\
1111111111111111111111\\
0000110100000100001100\\
0000000001010010011100\\
0011110000000000001111\\
0000001011000010001100\\
1010100100100001000011\\
1000100001000000000111\\
1111000000000000001100\\
0000001001001000011100\\
0000000100100100100000
\end{pmatrix},
$$

[58,29,10] codes 1

$$
\begin{pmatrix}
0000001000001000100001\\
1111111111111111111111\\
0000110100000100001100\\
0000000001010010011100\\
0011110000000000001100\\
0000001011000010001111\\
1010100100100001000000\\
1000100001000000000100\\
1111000000000000001100\\
0000001001001000011100\\
0000000100100100100011
\end{pmatrix},
\begin{pmatrix}
0000000001010000100001\\
1111111111111111111111\\
0000110100000100001100\\
0000000001010010011100\\
0011110000000000001100\\
0000001011000010001111\\
1010100100100001000000\\
1000100001000000000111\\
1111000000000000001100\\
0000001001001000011111\\
0000000100100100100011
\end{pmatrix},
\begin{pmatrix}
1000000010000000100001\\
1111111111111111111111\\
0000110100000100001100\\
0000000001010010011100\\
0011110000000000001100\\
0000001011000010001111\\
1010100100100001000011\\
1000100001000000000111\\
1111000000000000001111\\
0000001001001000011100\\
0000000100100100100011
\end{pmatrix}.
$$

[58,29,10] codes 2

- We can construct four inequivalent binary self-dual $[58, 29, 10]$ codes with an automorphism of order 7 from the binary self-dual code of length 60 in [4].

[4] R. Dontcheva and M. Harada, *Some extremal self-dual codes with an automorphism of order 7*, Algebra Eng. Commun. Comput. (AAECC J.), **14** (2003), 75–79.

[58,29,10] codes 2

$$G_{58,1} = \begin{pmatrix}
1110100000000000000000000000111010011101001110100111010000 \\
0111010000000000000000000000011101001110100111010011101000 \\
0011101000000000000000000000001110100111010011101001110100 \\
0000000111010000000000000000111010000000000000000111010000 \\
0000000011101000000000000000011101000000000000000011101000 \\
0000000001110100000000000000001110100000000000000001110100 \\
0000000000000011101000000000111010000000000000000011101000 \\
0000000000000001110100000000011101000000000000000001110100 \\
0000000000000000111010000000001110100000000000000100111000 \\
0000000000000000000001110100111010000111010111010101001100 \\
0000000000000000000000111010011101010011100011101110100100 \\
0000000000000000000000011101001110101001111001110111010000 \\
1001011100101110010111001011100101100000000000000000000000 \\
1100101110010111001011100101110010100000000000000000000000 \\
1110010111001011100101110010111001000000000000000000000000 \\
1001011000000000000000010111000000001001011000000000000000 \\
1100101000000000000000001011100000001100101000000000000000 \\
1110010000000000000000100101100000001110010000000000000000 \\
1001011000000000000000010111000000000000001001011000000000 \\
1100101000000000000000100101100000000000001100101000000000 \\
1110010000000000000000110010100000000000001110010000000000 \\
1001011100101100101111110010000000000000000000001001011 00 \\
1100101110010110010110111001000000000000000000001100101 00 \\
1110010111001011001011011100000000000000000000001110010 00 \\
0000000000000000000000000000111111111111111111111111111100 \\
1111111111111111111111111111000000011111110000000111111100 \\
1111111111111111111111111111000000000000000000000000000011 \\
0000000000000011111110000000111111111111110000000000000010 \\
0000000000000000000001111111111111111111111000000000000001
\end{pmatrix},$$

[58,29,10] codes 2

$$
G_{58,2} = \begin{pmatrix}
1110100000000000000000000000111010011101001110100111010000\\
0111010000000000000000000000011101001110100111010011101000\\
0011101000000000000000000000001110100111010011101001110100\\
0000000111010000000000000000000111010000000000000011101000\\
0000000011101000000000000000000011101000000000000001110100\\
0000000001110100000000000000000001110100000000000000111010\\
0000000000000011101000000001110100000000000000000111010000\\
0000000000000001110100000000111010000000000000000011101000\\
0000000000000000111010000000011101000000000000001001110000\\
0000000000000000000001110100111010000111010111010101001100\\
0000000000000000000000111010011101010011100011101110100100\\
0000000000000000000000011101001110101001111001110111010000\\
1001011100101110010111001011100101100000000000000000000000\\
1100101110010111001011100101110010100000000000000000000000\\
1110010111001011100101110010111001000000000000000000000000\\
1001011000000000000000010111000000010010110000000000000000\\
1100101000000000000000001011100000001100101000000000000000\\
1110010000000000000000100101100000001110010000000000000000\\
1001011000000000000000001011100000000000001001011000000000\\
1100101000000000000000100101100000000000001100101000000000\\
1110010000000000000000110010100000000000001110010000000000\\
1001011100101100101111110010000000000000000000000100101100\\
1100101110010110010110111001000000000000000000000110010100\\
1110010111001011001011011100000000000000000000000111001000\\
0000000000000000000000000000111111111111111111111111111100\\
1111111111111111111111111111000000011111110000000111111100\\
1111111111111111111111111111000000000000000000000000000011\\
0000000111111100000000000000111111111111110000000000000010\\
0000000000000011111110000000111111111111110000000000000001
\end{pmatrix}.
$$

5. Conclusions

Conclusion

- We develop a construction method for finding self-dual codes with an automorphism of order p with c independent p-cycles. In more detail, we construct a self-dual code with an automorphism of type $p-(c, f+2)$ and length $n+2$ from a self dual code with an automorphism of type $p-(c, f)$ and length n
- We add simple conditions to preserve the extremality.

Conclusion

- We obtain extremal self-dual $[40, 20, 8]$ codes with an automorphism of type $3-(10, 10)$, which is constructed from an extremal self-dual $[38, 19, 8]$ code of type $3-(10, 8)$.
- We find three new inequivalent extremal self-dual $[54, 27, 10]$ codes with an automorphism of type $7-(7, 5)$.

Conclusion

- We obtain at least 482 inequivalent extremal self-dual $[58, 29, 10]$ codes with an automorphism of type $3-(18, 4)$, which is constructed from an extremal self-dual $[54, 27, 10]$ code of type $3-(18, 0)$
- We find two new inequivalent extremal self-dual $[58, 29, 10]$ codes with an automorphism of order 7 having 8 independent cycles and 2 fixed points.

Thank you.