Determination of the weight enumerator for optimal binary self-dual code of length 52

Nikolay Yankov

Faculty of Mathematics and Informatics, Shumen University, Shumen, Bulgaria

Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory, Pomorie, Bulgaria, 2012
Outline

1. **Introduction**
   - Previous Results
   - Some definitions

2. **Construction method**

3. **Self-dual \([52, 26, 10]\) codes with an automorphism of order 5**
Why deal with self-dual [52, 26, 10] codes?

Binary self-dual codes with an automorphism of odd prime order $p$

- All extremal binary self-dual codes up to length 48 are classified (assuming the code possesses an automorphism of odd prime order $p$)
- All possible weight enumerators for [50, 25, 10] codes are already obtained
- There was just one open case for the weight enumerator of [52, 26, 10] code
- The case of a [52, 26, 10] code with automorphism of order 5 was open
Definitions 1

- $\mathbb{F}_q$ – finite field with $q = p^r$ elements, $p$ - prime
- A linear $[n, k]$ code $C$ is a $k$-dimensional subspace of the vector space $\mathbb{F}_q^n$
- The elements of $C$ are called codewords and the (Hamming) weight of a codeword is the number of its nonzero coordinate positions
- The minimum weight $d$ of $C$ is the smallest weight among all nonzero code words of $C$, and $C$ is called a $[n, k, d]$ code
- A matrix which rows form a basis of $C$ is called a generator matrix of this code
The weight enumerator $W(y)$ of a code $C$ is given by $W(y) = \sum_{i=0}^{n} A_i y^i$ where $A_i$, is the number of codewords of weight $i$ in $C$.

Let $(u, v) : F_q^n \times F_q^n \to F_q$ be an inner product in the linear space $F_q^n$.

The dual code of $C$ is

$$C^\perp = \{ u \in F_q^n : (u, v) = 0 \text{ for all } v \in C \}.$$ 

The dual code $C^\perp$ is a linear $[n, n - k]$ code.
Definitions 3

- We call the code $C$ **self-orthogonal** if $C \subseteq C^\perp$.
- We call the code $C$ **self-dual** if $C = C^\perp$. Every binary self-dual code have even length $n = 2k$ and dimension $k = \frac{n}{2}$.

**A self-dual code $C$**

- Is **doubly-even** if $\text{wt}(v) \equiv 0 \pmod{4}$, $\forall \; v \in C$
- Is **singly-even** if $\exists \; v \in C : \text{wt}(v) \equiv 2 \pmod{4}$

We will deal with singly-even codes.
Definitions 4

Code equivalence

- Two binary codes $C, C'$ are equivalent ($C \cong C'$) if $C$ can be obtained from $C'$ using permutation of coordinates.
- Let $S_n$ denotes the symmetric group of degree $n$.
- $\sigma \in S_n$ is an automorphism of $C$, if $C = \sigma(C)$.
- All automorphisms of $C$ form a group, called the automorphism group $\text{Aut}(C)$ of $C$.
Type of automorphisms

C is a binary self-dual $[n, n/2]$ code

$\sigma$ is an automorphism of $C$ of odd prime order $p$

Let

$$\sigma = \Omega_1 \cdots \Omega_c \Omega_{c+1} \cdots \Omega_{c+t},$$

$\Omega_1, \ldots, \Omega_c$ – cycles of length $p$

$\Omega_{c+1}, \ldots, \Omega_{c+t}$ – fixed points

$\sigma$ is of type $p-(c, f)$, $n = cp + f$
The two subcodes

\[ F_\sigma(C) = \{ \mathbf{v} \in C \mid \sigma(\mathbf{v}) = \mathbf{v} \} \]

\[ E_\sigma(C) = \{ \mathbf{v} \in C \mid \text{wt}(\mathbf{v}|\Omega_i) \equiv 0 \pmod{2} \}, i = 1, 2, \ldots, c \]

\( \mathbf{v}|\Omega_i \) is the restriction of the vector \( \mathbf{v} \) on \( \Omega_i \)

**Lemma**

\[ C = F_\sigma(C) \oplus E_\sigma(C), \dim F_\sigma(C) = (p - 1)c/2. \text{ When } C \text{ is self-dual and } 2 \text{ is a primitive root modulo } p, \text{ then } c \text{ is even.} \]
The map $\pi$

$\nu \in F_\sigma(C)$ iff $\nu \in C$ and $\nu$ is constant on each cycle.

$$\pi : F_\sigma(C) \to \mathbb{F}_2^{c+f}, \quad \nu \in F_\sigma(C), \quad (\nu \pi)_i = \nu_j \text{ for some } j \in \Omega_i$$

For every vector of length $p$ we have

$$(a_0, a_1, \ldots, a_{p-1}) \mapsto a_0 + a_1 x + \cdots + a_{p-1} x^{p-1} \in \mathbb{F}_2[x]/(x^p - 1).$$
The even weight code $P$

Weight of a polynomial $f(x) = a_0 + a_1 x + \cdots + a_{p-1} x^{p-1}$

$$\text{wt}(f(x)) = \# \{i \mid a_i \neq 0\}.$$

$$P = \{ f(x) \in F_2[x]/(x^p - 1) \mid \text{wt}(f(x)) \equiv 0 \pmod{2} \}$$

is a cyclic code of length $p$ with generator polynomial $x - 1$.

**Lemma**

*Let $p$ be an odd prime such that $1 + x + x^2 + \cdots + x^{p-1}$ is irreducible over $F_2$. Then $P$ is a field with identity $x + x^2 + \cdots + x^{p-1}$.***
Let $E_\sigma(C)^*$ is the code $E_\sigma(C)$ with the last $f$ coordinates deleted.

For $v \in E_\sigma(C)$, $v|\Omega_i = (a_0, \ldots, a_{p-1})$

$$(a_0, \ldots, a_{p-1}) \xrightarrow{\varphi} a_0 + \cdots + a_{p-1} x^{p-1}, \text{ for } 1 \leq i \leq c.$$  

We have a map $\varphi : E_\sigma(C)^* \to P^c$.  

The map $\varphi$
The main theorem

Theorem

If \( 1 + x + x^2 + \cdots + x^{p-1} \) is irreducible over \( F_2 \) then a code \( C \) with automorphism \( \sigma \) of type \( p - (c, f) \) is self-dual iff:

i) \( C_\pi = \pi(F_\sigma(C)) \) is a \([c + f, \frac{c+f}{2}]\) binary self-dual code;

ii) \( C_\varphi = \varphi(E_\sigma(C)^*) \) is a self-dual \([c, \frac{c}{2}]\) code over the field \( P \) under the inner product \((u, v) = \sum_{i=0}^{c} u_i v_i^{2(\frac{p-1}{2})} \), where \( u = (u_1, \ldots, u_c) \), \( v = (v_1, \ldots, v_c) \) \( \in \mathbb{P}^c \).
A binary self-dual [52, 26, 10] code can have two possible forms of the weight enumerator:

\[ W_{52,1} = 1 + 250y^{10} + 7980y^{12} + 42,800y^{14} + \cdots , \]
\[ W_{52,2} = 1 + (442 - 16\beta)y^{10} + (6188 + 64\beta)y^{12} + \cdots , \]

where \(0 \leq \beta \leq 12, \beta \neq 11.\)

Codes exist with \(W_{52,1}\) and with \(W_{52,2}\) for all values of the parameter except \(\beta = 10.\)
Let $C$ be a binary self-dual $[52, 26, 10]$ code, possessing an automorphism $\sigma$ of order 5. There is only one possible cycle structure: $\sigma$ is of type $5 - (10, 2)$. So

$$\sigma = (1, 2, \ldots, 5)(6, 7, \ldots, 10) \ldots (46, 47, \ldots, 50).$$

Using the Main Theorem we have that the subcode $C_{\varphi}$ is a self-dual code of length 10 over the field $\mathcal{P}$ under the inner product

$$(u, v) = \sum_{i=1}^{10} u_i v_i^4.$$
The field $\mathbb{F}_{16}$

2 is a prime root modulo 5, $\mathcal{P}$ is a finite field with 16 elements isomorphic to

$$\mathcal{P} \cong \mathbb{F}_{16} = \{0, \alpha^k | k = 0, \ldots, 14\},$$

where $e = x + x^2 + x^3 + x^4$, $\alpha = x + 1$ is a primitive element of multiplicative order 15. Denote by $\delta = \alpha^5$ – an element of multiplicative order 3. We list the elements of $\mathcal{P}$ in the following Table.

<table>
<thead>
<tr>
<th>$e$</th>
<th>01111</th>
<th>$\alpha$</th>
<th>11000</th>
<th>$\alpha^2$</th>
<th>10100</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha^3$</td>
<td>11110</td>
<td>$\alpha^4$</td>
<td>10001</td>
<td>$\alpha^5$</td>
<td>01001</td>
</tr>
<tr>
<td>$\alpha^6$</td>
<td>11101</td>
<td>$\alpha^7$</td>
<td>00011</td>
<td>$\alpha^8$</td>
<td>10010</td>
</tr>
<tr>
<td>$\alpha^9$</td>
<td>11011</td>
<td>$\alpha^{10}$</td>
<td>00110</td>
<td>$\alpha^{11}$</td>
<td>00101</td>
</tr>
<tr>
<td>$\alpha^{12}$</td>
<td>10111</td>
<td>$\alpha^{13}$</td>
<td>01100</td>
<td>$\alpha^{14}$</td>
<td>01010</td>
</tr>
</tbody>
</table>
The generator matrix of $C_\varphi$

**Theorem**

Let $C_\varphi$ be a $[10, 5]$ code over $\mathcal{P}$, self-dual under the orthogonality condition such that $E_\sigma(C)$ has $d \geq 10$. Then

$$\text{gen}_{C_\varphi} = \begin{pmatrix}
e & 0 & 0 & 0 & 0 & a_{16} & a_{17} & a_{18} & a_{19} & a_{1,10} \\
0 & e & 0 & 0 & 0 & a_{26} & a_{27} & a_{28} & a_{29} & a_{2,10} \\
0 & 0 & e & 0 & 0 & a_{36} & a_{37} & a_{38} & a_{39} & a_{3,10} \\
0 & 0 & 0 & e & 0 & a_{46} & a_{47} & a_{48} & a_{49} & a_{4,10} \\
0 & 0 & 0 & 0 & e & a_{56} & a_{57} & a_{58} & a_{59} & a_{5,10} \\
\end{pmatrix},$$

$a_{1i} \in \{0, e, \delta, \delta^2\}$, $i = 6, \ldots, 10$, $a_{j6} \in \{0, e, \delta, \delta^2\}$, $j = 1, \ldots, 6$. Furthermore $(a_{16}, a_{17}, a_{18}, a_{19}, a_{1,10})$ is one of the following five vectors $(0, e, e, \delta, \delta^2)$, $(e, e, e, e, e)$, $(e, \delta, \delta, \delta, \delta)$, $(e, \delta, \delta, \delta^2, \delta^2)$, $(e, e, e, \delta, \delta)$. 
Sketch of the Proof:

Interchanging the columns of $G_\varphi$, we assume that $0 \leq a_{16} \leq a_{17} \leq a_{18} \leq a_{19} \leq a_{1,10} \leq \delta^2$.

By the orthogonal condition $v = (a_{16}, a_{17}, a_{18}, a_{19}, a_{1,10})$ is one of the vectors

<table>
<thead>
<tr>
<th>$v_1$</th>
<th>$(0,0,0,0,e)$</th>
<th>$v_2$</th>
<th>$(0,0,e,e,e)$</th>
<th>$v_3$</th>
<th>$(0,0,e,\delta,\delta)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$v_4$</td>
<td>$(0,0,e,\delta^2,\delta^2)$</td>
<td>$v_5$</td>
<td>$(0,e,e,\delta,\delta^2)$</td>
<td>$v_6$</td>
<td>$(e,e,e,e,e)$</td>
</tr>
<tr>
<td>$v_7$</td>
<td>$(e,\delta,\delta,\delta,\delta)$</td>
<td>$v_8$</td>
<td>$(e,\delta^2,\delta^2,\delta^2,\delta^2)$</td>
<td>$v_9$</td>
<td>$(e,\delta,\delta,\delta^2,\delta^2)$</td>
</tr>
<tr>
<td>$v_{10}$</td>
<td>$(e,e,e,\delta,\delta)$</td>
<td>$v_{11}$</td>
<td>$(e,e,e,\delta^2,\delta^2)$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The first three cases lead to vectors of weight 8

Using the $\mathbb{F}_{16}$-automorphism $\gamma : x \rightarrow x^{-1}$, $\delta \rightarrow \delta^2$

$$v_4 \xrightarrow{\gamma} v_3, \quad v_8 \xrightarrow{\gamma} v_7, \quad v_{11} \xrightarrow{\gamma} v_{10}$$

Weight enumerator of optimal self-dual code of length 52
A computer program for calculating all codes with generator matrix using the orthogonality condition, was created. It turns out that there are exactly 56 inequivalent \([10, 5]\) codes. Denote their generator matrices by \(H_i, i = 1, \ldots, 56\).

**Table:** Order of automorphism groups of the optimal codes over \(\mathbb{F}_{16}\)

| \(|\text{Aut}(C)|\) | 5   | 10  | 15  | 20  | 40  | 80  | 160 |
|---------------------|-----|-----|-----|-----|-----|-----|-----|
| \(\#\)              | 15  | 25  | 2   | 8   | 3   | 2   | 1   |
\( C_\pi \) is a binary self-dual [12, 6, \( \geq 2 \)] code

There are three such codes:

- \( 6i_2, B_1 = \text{gen}(6i_2) = (l_6 | l_6) \)

- \( 2i_2 + e_8, B_2 = \text{gen}(2i_2 + e_8) = \)
  \[
  \begin{pmatrix}
  100000100000 \\
  010000100000 \\
  001000001111 \\
  000100010111 \\
  000010011101 \\
  000001001110 \\
  \end{pmatrix}
  \]

- \( d_{12}, B_3 = \text{gen}(d_{12}) = \)
  \[
  \begin{pmatrix}
  100000100001 \\
  010000100011 \\
  001000010111 \\
  000100001111 \\
  000010111110 \\
  000001111101 \\
  \end{pmatrix}
  \]
We have to arrange 2 of the coordinate positions \{1, \ldots, 12\} to be the fixed points \(X_f\), such that \(F_\sigma\) have \(d \geq 10\)

There are three different generators \(G_i\):

- one from \(2i_2 + e_8\): \(G_1 = B_2\),
- two from \(d_{12}\): \(G_2 = B_3\); and \(G_3\) – the matrix \(B_3\) with columns permuted by \((10, 11)\)
The generator matrix

$S_{t_i} < S_{10}$, $i = 1, 2, 3$ consisting of all permutations on the first ten coordinates, which are induced by an automorphism of the code generated by $C_i$, $i = 1, 2, 3$

$\tau \in S_{10}$ by $C_{52, i, j}^\tau$, $i = 1, 2, 3$, $j = 1, \ldots, 56$ we denote the $[52, 26]$ self-dual code with

$$\text{gen } C_{52, i, j}^\tau = \begin{pmatrix} \varphi^{-1}(H_j) & O \\ \pi^{-1}(\tau G_i) \end{pmatrix}$$
Right transversal

Lemma

If \( \tau_1 \) and \( \tau_2 \) belong to one and the same right coset of \( S_{10} \) to \( G_i \), then the codes \( C_{i,j}^{\tau_1} \) and \( C_{i,j}^{\tau_2} \) are equivalent.

We need only to consider permutations from the right transversals \( T_i \) of \( S_{10} \) with respect to \( St_i \).
Case 1. $F_\sigma$ generated by $G_1$.

\[ St_1 = \langle (2, 8)(3, 6, 10, 5), (2, 8)(3, 4, 5)(6, 10, 9), (3, 10)(4, 9)(5, 6), (1, 2)(3, 10)(4, 9)(5, 6)(7, 8) \rangle \]

$|St_1| = 384$

$T_1$ have 9450 elements

There are 10486 codes with weight enumerator $W_{52,2}$

- 9881 with $\beta = 0$
- 604 with $\beta = 5$
- 1 code with $\beta = 10$
Case 2. $F_σ$ generated by $G_2$

$St_2 = \langle (5, 6), (4, 5)(6, 10), (3, 4)(9, 10), (2, 3)(8, 9), (1, 2)(7, 8) \rangle$

$|St_2| = 3840, |T_2| = 945$

There exist exactly 147 inequivalent codes all with weight enumerator $W_{52,1}$

Case 3. $F_σ$ generated by $G_3$

$St_3 = \langle (2, 8)(3, 6, 9, 5), (1, 2, 3, 7, 8, 9)(4, 10)(5, 6) \rangle$

$|St_3| = 384, |T_3| = 9450$

There are 8144 inequivalent codes with $W_{52,2}$

- 7624 codes for $\beta = 2$
- 520 codes for $\beta = 7$. 
Main results

**Proposition**

There are exactly 18777 inequivalent binary \([52, 26, 10]\) self-dual codes having an automorphism of type \(5 - (10, 2)\). One of these codes have weight enumerator \(W_{52,2}\) for \(\beta = 10\).

**Theorem**

There exists an optimal binary self-dual \([52, 26, 10]\) code with weight enumerator \(W\) if and only if \(W = W_{52,2}\) in with \(\beta \in [0..12], \beta \neq 11 \) or \(W = W_{52,1}\).
Introduction
Construction method
Self-dual $[52, 26, 10]$ codes with an automorphism of order 5

Automorphism groups

**Table:** Order of automorphism groups for $[52, 26, 10]$ codes

| $|\text{Aut}(C)|$ | 5  | 10 | 50 | 150 |
|-----------------|----|----|----|-----|
|                # | 18208 | 566 | 2  | 1   |

The 2 codes with $|\text{Aut}(C)| = 50$ are the 2 pure double-circulant self-dual codes.
All other codes are new.