Some self-dual codes having an automorphism of order 15

Stefka Bouyuklieva\textsuperscript{1,2}  \hspace{1cm} Nikolay Yankov\textsuperscript{3}

\textsuperscript{1}Veliko Tarnovo University,  
\textsuperscript{2}Institute of Mathematics and Informatics,  
\textsuperscript{3}Shumen University,  
Bulgaria

Algebraic and Combinatorial Coding Theory, 2014
Outline

1 Introduction
   - Self-dual codes
   - Motivation

2 On the structure of the codes
   - An automorphism of odd order $r$
   - The automorphism of order 15

3 The case $c = 6$, $t_5 = 0$

4 The Results
Self-dual codes

\textbf{\textit{C - [n,k,d] linear code}}

- \( C \) is a self-orthogonal code, if \( C \subseteq C^\perp \)
- \( C \) is a self-dual code, if \( C = C^\perp \)
- Any self-dual code has dimension \( k = n/2 \)
- All codewords in a binary self-orthogonal code have even weights
- Doubly-even code - if \( 4 \mid \text{wt}(v) \ \forall v \in C \)
- Singly-even self-dual code - if \( \exists v \in C : \text{wt}(v) \equiv 2 \pmod{4} \)
- Doubly-even self-dual codes exist iff \( n \equiv 0 \pmod{8} \)
Extremal self-dual codes

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

$$d \leq 4[n/24] + 4$$

except when $n \equiv 22 \pmod{24}$ when

$$d \leq 4[n/24] + 6$$

When $n$ is a multiple of 24, any code meeting the bound must be doubly-even.
Extremal doubly-even $[24m,12m,4m+4]$ codes

- $m \leq 153$ (Zhang);
- doubly even;
- a unique weight enumerator;
- combinatorial 5-designs (Assmus, Mattson);
- only two known codes:
  - the extended Golay code $g_{24}$;
  - the extended quadratic-residue code $q_{48}$.

- $n=72$, $d=16$ - ???
  N.J.A. Sloane, Is there a $(72,36)$, $d = 16$ self-dual code? 

- $n=96$, $d=20$ - ???

- $n=120$, $d=24$ - ???
**Optimal self-dual codes**

A self-dual code is called optimal if it has the largest minimum weight among all self-dual codes of that length.

- Any extremal self-dual code is optimal.
- For some lengths, no extremal self-dual codes exist!
- There are no extremal self-dual codes of lengths 2, 4, 6, 10, 26, 28, 30, 34, 50, 52, 54, 58, ...

**Conjecture:**

The optimal self-dual codes of lengths $24m + r$ for $r = 2, 4, 6,$ and $10$ are not extremal.
Optimal self-dual codes

Table: Largest Minimum Weights Of Self-Dual Codes

<table>
<thead>
<tr>
<th>$n$</th>
<th>96</th>
<th>98</th>
<th>100</th>
<th>102</th>
<th>104</th>
<th>106</th>
</tr>
</thead>
<tbody>
<tr>
<td>$d(n)$</td>
<td>16,20</td>
<td>16,18</td>
<td>16,18</td>
<td>18</td>
<td>18,20</td>
<td>16,18</td>
</tr>
</tbody>
</table>
An automorphism of odd order $r$

$\sigma \in \text{Aut}(C), \ |\sigma| = r$

$$\sigma = \underbrace{\Omega_1}_{l_1} \underbrace{\Omega_2}_{l_2} \ldots \underbrace{\Omega_m}_{l_m} \Rightarrow \text{lcm}(l_1, \ldots, l_m) = r \Rightarrow l_i | r$$

- $F_{\sigma}(C) = \{v \in C : \sigma(v) = v\}$ - the fixed subcode
- $E_{\sigma}(C) = \{v \in C : \text{wt}(v|\Omega_i) \equiv 0 \pmod{2}, \ i = 1, \ldots, m\}$ - the even subcode

**Theorem:**

$$C = F_{\sigma}(C) \oplus E_{\sigma}(C)$$
An automorphism of odd order $r$

The fixed subcode

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

$$\pi : F_{\sigma}(C) \rightarrow \mathbb{F}_{2}^{m}, \ C_{\pi} = \pi(F_{\sigma}(C))$$

**Theorem:**

If $C$ is a binary self-dual code then $C_{\pi} = \pi(F_{\sigma}(C))$ is a binary self-dual code of length $m$. 
An automorphism of odd order $r$

**The even subcode $E_\sigma(C)$**

If $\mathbf{v} \in E_\sigma(C)$ then $\mathbf{v} = (v_1, \ldots, v_{n-f}, 0, \ldots, 0)$

$E_\sigma(C)' = \{ \mathbf{v}' = (v_1, \ldots, v_{n-f}), \; \mathbf{v} \in E_\sigma(C) \}$

$v|\Omega_i = (v_0, v_1, \ldots, v_{s-1}) \mapsto v_0 + v_1 x + \cdots + v_{s-1} x^{s-1} = v^{(i)}(x)$

$\phi : v' \rightarrow (v^{(1)}(x), \ldots, v^{(m-f)}(x))$

**If $r = 3$**

If $r = 3$ then $\phi(E_\sigma(C)')$ is a Hermitian quaternary self-dual code over the filed $\mathcal{P}_4 = \{0, x + x^2, 1 + x^2, 1 + x \}$ of length $c = m - f$.

**If $r = 5$**

then $\phi(E_\sigma(C)')$ is a Hermitian self-dual code over the filed $\mathcal{P}_{16} = \{a_0 + a_1 x + \cdots + a_4 x^4, \ wt(a_0, \ldots, a_4) = 0, 2, 4 \}$ of length $c = m - f$. 
The automorphism of order 15

\[ \sigma \in \text{Aut}(C), \ |\sigma| = 15 \]

\[ \sigma = \Omega_1 \Omega_2 \ldots \Omega_m \]

\[ m = c + t_5 + t_3 + f, \quad n = 15c + 5t_5 + 3t_3 + f \]

c cycles of length 15, f fixed points

t_5 cycles of length 5, t_3 cycles of length 3

- \( \sigma^3 \) - type 5-(3c + t_5, 3t_3 + f);
- \( \sigma^5 \) - type 3-(5c + t_3, 5t_5 + f).

\[ d \geq 18 \Rightarrow 3c + t_5 \geq 16, 5c + t_3 \geq 28 \]

- If \( n = 96 \) then \( (c, t_5, t_3, f) = (6, 0, 0, 6) \) or \( (6, 0, 2, 0) \).
- If \( n = 98 \) then \( (c, t_5, t_3, f) = (6, 0, 0, 8) \) or \( (6, 0, 2, 2) \).
- If \( n = 100 \) then \( (c, t_5, t_3, f) = (6, 0, 0, 10), (6, 0, 2, 4), (6, 2, 0, 0) \) or \( (5, 3, 3, 1) \).
The fixed subcode, $t_3 = 0$

$$(c, t_5, t_3, f) = (6, 0, 0, f), \ f = 6, 8, 10$$

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

$$\pi : F_\sigma(C) \to \mathbb{F}_2^m, \ C_\pi = \pi(F_\sigma(C))$$

**Theorem:**

If $C$ is a binary self-dual code then $C_\pi = \pi(F_\sigma(C))$ is a binary self-dual $[f + 6, f/2 + 3, \geq 2]$ code.
The fixed subcode, \( t_3 = 0 \)

\[
G = \left( \begin{array}{cc}
[6, k_1, \geq 2] & O \\
O & [f, k_2, \geq 18] \\
E & F \\
\end{array} \right)
\]

\[
k_2 = k_1 + \frac{f - 6}{2} \quad \Rightarrow \quad k_1 = k_2 = 0, \quad f = 6
\]

If \( c = f = 6 \) then \( C_\pi \) is the self-dual \([12, 6, 4]\) code generated by the matrix \((I_6|I_6 + J_6)\).
The even subcode $E_\sigma(C)$

If $v \in E_\sigma(C)$ then $v = (v_1, \ldots, v_{n-f}, 0, \ldots, 0)$

$v|_{\Omega_i} = (v_0, v_1, \ldots, v_{s-1}) \mapsto v_0 + v_1 x + \cdots + v_{s-1} x^{s-1}$

Let $E_\sigma(C)^*$ be the shortened code of $E_\sigma(C)$ obtained by removing the last $5t_5 + 3t_3 + f$ coordinates from the codewords having 0’s there, and let $C_\phi = \phi(E_\sigma(C)^*)$.

$E_\sigma(C)^*$ - linear code of length $15c$

$x^{15} - 1 =
\begin{align*}
& (x-1) (1 + x + x^2) (1 + x + x^2 + x^3 + x^4) (1 + x + x^4) (1 + x^3 + x^4) \\
& \quad \underbrace{Q_3(x)} \quad \underbrace{Q_5(x)} \quad \underbrace{h(x)} \quad \underbrace{h^*(x)}
\end{align*}$
The even subcode \( E_\sigma(C) \)

\[
x^{15} - 1 = (x-1)(1 + x + x^2)(1 + x + x^2 + x^3 + x^4)(1 + x + x^4)(1 + x^3 + x^4) \\
\quad Q_3(x) \quad Q_5(x) \quad h(x) \quad h^*(x)
\]

\[
\Rightarrow C_\phi = M_1 \oplus M_2 \oplus M' \oplus M''
\]

- \( M_1 \) - Hermitian self-orthogonal code over the field \( G_1 \cong \mathbb{F}_4 \),
  \( G_1 = \langle (x^{15} - 1)/Q_3(x) \rangle \);
- \( M_2 \) - Hermitian self-orthogonal codes over the field \( G_2 \cong \mathbb{F}_{16} \),
  \( G_2 = \langle (x^{15} - 1)/Q_5(x) \rangle \);
- \( M' \) is a linear \([6, k', d']\) code over \( H \cong \mathbb{F}_{16} \),
  \( H = \langle (x^{15} - 1)/h(x) \rangle \);
- \( M'' \subseteq (M')^\perp \) with respect to the Euclidean inner product.
The even subcode $E_{\sigma}(C)$

\[ x^{15} - 1 = \]
\[
\begin{align*}
(x-1)(1+x+x^2)(1+x+x^2+x^3+x^4)(1+x+x^4)(1+x^3+x^4) \\
Q_3(x) \quad Q_5(x) \quad h(x) \quad h^*(x)
\end{align*}
\]

\[ \Rightarrow C_{\phi} = M_1 \oplus M_2 \oplus M' \oplus M'', \quad \dim E_{\sigma}(C)^* = 2 \dim M_1 + 4 \dim M_2 + 4( \dim M' + \dim M'' ) \leq 42. \]

\[ \leq 3 \quad \leq 3 \quad \leq 6 \]

\[ * * * t_5 = t_3 = 0 \Rightarrow \dim E_{\sigma}(C)^* = 42 * * * \]
\[ \Rightarrow \dim M_1 = 3, \quad \dim M_2 = 3, \quad \dim M' + \dim M'' = 6 \]
The even subcode $E_\sigma(C)$

\[ * * * t_5 = t_3 = 0 \Rightarrow \dim E_\sigma(C)^* = 42 * * * \]
\[ \Rightarrow \dim M_1 = 3, \ \dim M_2 = 3, \ \dim M' + \dim M'' = 6 \]

- 33 codes $M' \oplus M''$ with $\dim M' + \dim M'' = 6$ and $d(\phi^{-1}(M' \oplus M'')) \geq 20$
- $\phi^{-1}(M' \oplus M'')$ - [90, 24, $\geq 20$] doubly-even code;
- 675 inequivalent doubly-even [90, 36, 20] codes $\phi^{-1}(M' \oplus M'' \oplus M_2)$ with $\dim M_2 = 3$;
- no doubly-even [90, 42, 20] codes $E_\sigma(C)^*$
The even subcode $E_\sigma(C)$

\[ x^{15} - 1 = (x - 1)(1 + x + x^2)(1 + x + x^2 + x^3 + x^4)(1 + x + x^4)(1 + x^3 + x^4) \]

\[ \Rightarrow C_\phi = M_1 \oplus M_2 \oplus M' \oplus M'', \]

\[ \dim E_\sigma(C)^* = 2 \dim M_1 + 4 \dim M_2 + 4(\dim M' + \dim M'') \leq 42. \]

\[ \Rightarrow \dim M_1 = 2, \ \dim M_2 = 3, \ \dim M' + \dim M'' = 6 \]
The even subcode $E_\sigma(C)$

\[ \bullet \] \( t_3 = 2 \Rightarrow \dim E_\sigma(C)^* = 40 \) \[ \bullet \]

\( \Rightarrow \dim M_1 = 2, \quad \dim M_2 = 3, \quad \dim M' + \dim M'' = 6 \)

- 33 codes $M' \oplus M''$ with $\dim M' + \dim M'' = 6$ and $d(\phi^{-1}(M' \oplus M'')) \geq 20$
- $\phi^{-1}(M' \oplus M'')$ - [90, 24, \( \geq 20 \)] doubly-even code;
- 675 inequivalent doubly-even [90, 36, 20] codes $\phi^{-1}(M' \oplus M'' \oplus M_2)$ with $\dim M_2 = 3$;
- no self-orthogonal [96, 44, 20] codes $E_\sigma(C)'$
The even subcode $E_{\sigma}(C)$

\[ \ast \ast \ast t_3 = 2 \Rightarrow \dim E_{\sigma}(C)^* = 40 \ast \ast \ast \]

\[ \Rightarrow \dim M_1 = 2, \; \dim M_2 = 3, \; \dim M' + \dim M'' = 6 \]

No self-orthogonal $[96, 44, 20]$ codes $E_{\sigma}(C)'$ exist:

\[
\phi^{-1} \left( \begin{array}{ccc}
\text{gen}M' & 0 \\
\text{gen}M'' & 0 \\
\text{gen}M_2 & 0 \\
\text{gen}M_1 & 0 \\
\nu & 011011 \\
\sigma(\nu) & 101101
\end{array} \right) \begin{array}{c}
33 \text{ codes} \\
675 \text{ codes} \\
0 \text{ codes}
\end{array}
\]
Lengths 96 and 98

- If \( n = 96 \) then \((c, t_5, t_3, f) = (6, 0, 0, 6)\) or \((6,0,2,0)\).
- If \( n = 98 \) then \((c, t_5, t_3, f) = (6, 0, 0, 8)\) or \((6,0,2,2)\).

**Length 96**

An extremal binary doubly-even \([96, 48, 20]\) self-dual code with an automorphism of order 15 does not exist.

**Length 98**

An optimal binary self-dual \([98, 49, 18]\) self-dual code with an automorphism of order 15 does not exist.
Length 100

If \( n = 100 \) then \((c, t_5, t_3, f) = (6, 0, 0, 10), (6, 0, 2, 4), (6, 2, 0, 0)\) or \((5, 3, 3, 1)\).

Self-dual \([100, 50, 18]\) codes with \((c, t_5, t_3, f) = (6, 0, 0, 10), (6, 0, 2, 4), \text{ or } (5, 3, 3, 1)\) do not exist.

The case \((c, t_5, t_3, f) = (6, 2, 0, 0)\) is still running!