Automorphisms of extremal codes

Gabriele Nebe

Lehrstuhl D für Mathematik

Hannover, 26.03.2014
Doubly-even self-dual codes

Definition

- A linear binary code $C$ of length $n$ is a subspace $C \leq \mathbb{F}_2^n$.
- The dual code of $C$ is
  \[ C^\perp := \{ x \in \mathbb{F}_2^n \mid (x, c) := \sum_{i=1}^n x_i c_i = 0 \text{ for all } c \in C \} \]
- $C$ is called self-dual if $C = C^\perp$.
- The Hamming weight of a codeword $c \in C$ is
  \[ \text{wt}(c) := |\{ i \mid c_i \neq 0 \}|. \]
- $\text{wt}(c) \equiv_2 (c, c)$, so $C \subseteq C^\perp$ implies $\text{wt}(C) \subseteq 2\mathbb{Z}$.
- $C$ is called doubly-even if $\text{wt}(C) \subseteq 4\mathbb{Z}$.
- The minimum distance $d(C) := \min\{ \text{wt}(c) \mid 0 \neq c \in C \}$.
- A self-dual code $C \leq \mathbb{F}_2^n$ is called extremal if $d(C) \geq 4 + 4\lfloor \frac{n}{24} \rfloor$.
- The weight enumerator of $C$ is
  \[ p_C := \sum_{c \in C} x^{n-\text{wt}(c)} y^{\text{wt}(c)} \in \mathbb{C}[x, y]_n. \]
- $\text{Aut}(C) = \{ \sigma \in S_n \mid \sigma(C) \subseteq C \}$. 
Examples for self-dual doubly-even codes

**Hamming Code**

The extended **Hamming code**, the unique doubly-even self-dual code of length 8,

\[ p_{h_8}(x, y) = x^8 + 14x^4y^4 + y^8 \]

and \( \text{Aut}(h_8) = 2^3 : L_3(2) \).

**Golay Code**

The binary **Golay code** \( G_{24} \) is the unique doubly-even self-dual code of length 24 with minimum distance \( \geq 8 \). \( \text{Aut}(G_{24}) = M_{24} \)

\[ p_{G_{24}} = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24} \]
Application of invariant theory

The weight enumerator of $C$ is $p_C := \sum_{c \in C} x^{n-wt(c)} y^{wt(c)} \in \mathbb{C}[x, y]_n$.

**Theorem (Gleason, ICM 1970)**

Let $C = C^\perp \leq \mathbb{F}_2^n$ be doubly even. Then $d(C) \leq 4 + 4 \lfloor \frac{n}{24} \rfloor$

Doubly-even self-dual codes achieving equality are called **extremal**.
The weight enumerator of $C$ is $p_C := \sum_{c \in C} x^{n - \text{wt}(c)} y^{\text{wt}(c)} \in \mathbb{C}[x, y]_n$.

**Theorem (Gleason, ICM 1970)**

Let $C = C^\perp \leq \mathbb{F}_2^n$ be doubly even. Then $d(C) \leq 4 + 4 \lfloor \frac{n}{24} \rfloor$

Doubly-even self-dual codes achieving equality are called extremal.

**Proof:**

- $p_C(x, y) = p_C(x, iy), p_C(x, y) = p_{C^\perp}(x, y) = p_C\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right)$
- $G_{192} := \langle \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \rangle$.
- $p_C \in \text{Inv}(G_{192}) = \mathbb{C}[p_{h_8}, p_{G_{24}}]$
- $\exists! f \in \mathbb{C}[p_{h_8}, p_{G_{24}}]_{8m}$ such that
  
  $f(1, y) = 1 + 0y^4 + \ldots + 0y^{4\lfloor \frac{m}{3} \rfloor} + a_m y^{4\lfloor \frac{m}{3} \rfloor} + b_m y^{4\lfloor \frac{m}{3} \rfloor} + 8 + \ldots$

- $a_m > 0$ for all $m$
Application of invariant theory

The weight enumerator of $C$ is $p_C := \sum_{c \in C} x^{n-wt(c)} y^{wt(c)} \in \mathbb{C}[x, y]_n$.

Theorem (Gleason, ICM 1970)

Let $C = C^\perp \leq \mathbb{F}_2^n$ be doubly even. Then $d(C) \leq 4 + 4 \lfloor \frac{n}{24} \rfloor$

Doubly-even self-dual codes achieving equality are called extremal.

Proof:

- $p_C(x, y) = p_C(x, iy), p_C(x, y) = p_{C^\perp}(x, y) = p_C(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}})$

- $G_{192} := \langle \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \rangle$.

- $p_C \in \text{Inv}(G_{192}) = \mathbb{C}[p_{h_8}, p_{G_{24}}]$

- $\exists! f \in \mathbb{C}[p_{h_8}, p_{G_{24}}]_{8m}$ such that

  $$f(1, y) = 1 + 0y^4 + \ldots + 0y^{4\lfloor m/3 \rfloor} + a_my^{4\lfloor m/3 \rfloor+4} + b_my^{4\lfloor m/3 \rfloor+8} + \ldots$$

- $a_m > 0$ for all $m$

Proposition

$b_m < 0$ for all $m \geq 494$ so there is no extremal code of length $\geq 3952$. 
Automorphism groups of extremal codes

<table>
<thead>
<tr>
<th>length</th>
<th>8</th>
<th>24</th>
<th>32</th>
<th>40</th>
<th>48</th>
<th>72</th>
<th>96</th>
<th>104</th>
<th>( \geq 3952 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( d(C) )</td>
<td>4</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>20</td>
<td>20</td>
<td>( \geq 1 )</td>
</tr>
<tr>
<td>extremal</td>
<td>( h_8 )</td>
<td>( G_{24} )</td>
<td>5</td>
<td>16,470</td>
<td>( QR_{48} )</td>
<td>?</td>
<td>?</td>
<td>( \geq 1 )</td>
<td>0</td>
</tr>
</tbody>
</table>

\[ \text{Aut}(C) = \{ \sigma \in S_n \mid \sigma(C) \subseteq C \} \] is the automorphism group of \( C \leq \mathbb{F}_2^n \).

- \( \text{Aut}(h_8) = 2^3.L_3(2) \)
- \( \text{Aut}(G_{24}) = M_{24} \)
- Length 40: 10,400 extremal codes with \( \text{Aut} = 1 \).
- \( \text{Aut}(QR_{48}) = L_2(47). \)
- Sloane (1973): Is there a \((72, 36, 16)\) self-dual code?
- If \( C \) is such a \((72, 36, 16)\) code then \( \text{Aut}(C) \) has order \( \leq 5 \).
Application of Burnside’s orbit counting theorem

**Definition**

Let $\sigma \in S_n$ of prime order $p$. Then $\sigma$ is of Type $(z, f)$, if $\sigma$ has $z$ $p$-cycles and $f$ fixed points. $zp + f = n$.

If $\sigma = (1, 2, .., p)(p + 1, .., 2p)...((z - 1)p + 1, .., zp) \in \text{Aut}(C)$ then $C = \text{Fix}_C(\sigma) \oplus E_C(\sigma)$, with

$$\text{Fix}_C(\sigma) = \{(c_p \cdots c_p c_{2p} \cdots c_{2p} \cdots c_{zp} \cdots c_{zp} c_{zp+1} \cdots c_n) \in C \} \cong \underbrace{\mathbb{F}_2^p}_p \underbrace{\mathbb{F}_2^p}_p \underbrace{\mathbb{F}_2^p}_p$$

$$\pi(\text{Fix}_C(\sigma)) = \{(c_p c_{2p} \cdots c_{zp} c_{zp+1} \cdots c_n) \in \mathbb{F}_2^{z+f} \mid c \in \text{Fix}_C(\sigma)\}$$

**Fact**

If $C = C^\perp$ and $p$ is odd, then $\pi(\text{Fix}_C(\sigma))$ is a self-dual code of length $z + f$. In particular

$$\dim(\text{Fix}_C(\sigma)) = \frac{z + f}{2} \text{ and } |\text{Fix}_C(\sigma)| = 2^{(z+f)/2}.$$
**Application of Burnside's orbit counting theorem**

**Theorem (Conway, Pless, 1982)**

Let $C = C^\perp \leq \mathbb{F}_2^n$, $\sigma \in \text{Aut}(C)$ of odd prime order $p$ and Type $(z, f)$. Then

$$2^{(z+f)/2} \equiv 2^{n/2} \pmod{p}.$$  

**Proof:** Apply orbit counting:

The number of $G$-orbits on a finite set $M$ is $\frac{1}{|G|} \sum_{g \in G} |\text{Fix}_M(g)|$.

Here $G = \langle \sigma \rangle$, $M = C$, $\text{Fix}_C(g) = \text{Fix}_C(\sigma)$ for all $1 \neq g \in G$, and the number of $\langle \sigma \rangle$-orbits on $C$ is $\frac{1}{p}(2^{n/2} + (p - 1)2^{(z+f)/2}) \in \mathbb{N}$.

**Corollary**

$C = C^\perp \leq \mathbb{F}_2^n$, $p > n/2$ an odd prime divisor of $|\text{Aut}(C)|$, then $p \equiv \pm 1 \pmod{8}$.

Here $z = 1$, $f = n - p$, $(z + f)/2 = (n - (p - 1))/2$, so $2^{(p-1)/2}$ is 1 mod $p$ and hence 2 must be a square modulo $p$. 
Remark

- $C = C^\perp \Rightarrow \mathbf{1} = (1, \ldots, 1) \in C$, since $(c, c) = (c, \mathbf{1})$.
- If $C$ is self-dual then $n = 2 \dim(C)$ is even and

$$\mathbf{1} \in C^\perp = C \subset \mathbf{1}^\perp = \{ c \in \mathbb{F}_2^n \mid \text{wt}(c) \text{ even} \}.$$ 

- Self-dual doubly-even codes correspond to totally isotropic subspaces in the quadratic space

$$E_{n-2} := (\mathbf{1}^\perp / \langle \mathbf{1} \rangle, q), q(c + \langle \mathbf{1} \rangle) = \frac{1}{2} \text{wt}(c) \pmod{2} \in \mathbb{F}_2.$$ 

- $C = C^\perp \leq \mathbb{F}_2^n$ doubly-even $\Rightarrow n \in 8 \mathbb{Z}$.

Theorem (A. Meyer, N. 2009)

Let $C = C^\perp \leq \mathbb{F}_2^n$ doubly-even. Then $\text{Aut}(C) \leq \text{Alt}_n$. 

Application of quadratic forms

\[ \text{Aut}(C) = \{ \sigma \in S_n \mid \sigma(C) \subseteq C \} \text{ is the automorphism group of } C \leq \mathbb{F}_2^n. \]

**Theorem (A. Meyer, N. 2009)**

Let \( C = C^\perp \leq \mathbb{F}_2^n \) doubly-even. Then \( \text{Aut}(C) \leq \text{Alt}_n \).

- **Proof.** (sketch)
  - \( E_{n-2} := (1^\perp/\langle 1 \rangle, q), q(c + \langle 1 \rangle) = \frac{1}{2} \text{wt}(c) \pmod{2} \in \mathbb{F}_2. \)
  - \( C/\langle 1 \rangle \) is a maximal isotropic subspace \( E_{n-2} \).
  - The stabilizer in the orthogonal group of \( E_{n-2} \) of such a space has trivial Dickson invariant.
  - \( S_n \leq O(E_{n-2}), \text{Aut}(C) = \text{Stab}_{S_n}(C). \)
  - The restriction of the Dickson invariant to \( S_n \) is the sign.
Application of Representation Theory

$G$ finite group, $\mathbb{F}_2G = \{\sum_{g \in G} a_g g \mid a_g \in \mathbb{F}_2\}$ group ring.
Then $G$ acts on $\mathbb{F}_2G \cong \mathbb{F}_2^{|G|}$ by permuting the basis elements.

Theorem (Sloane, Thompson, 1988)

There is a $G$-invariant self-dual doubly-even code $C \leq \mathbb{F}_2G$, if and only if $|G| \in 8\mathbb{N}$ and the Sylow 2-subgroups of $G$ are not cyclic.

Theorem (A. Meyer, N., 2009)

Given $G \leq S_n$. Then there is $C = C^\perp \leq \mathbb{F}_2^n$ doubly-even such that $G \leq \text{Aut}(C)$, if and only if

1. $n \in 8\mathbb{N}$,
2. all self-dual composition factors of the $\mathbb{F}_2G$-module $\mathbb{F}_2^n$ occur with even multiplicity, and
3. $G \leq \text{Alt}_n$. 
General theoretical results (Summary)

- Invariant Theory:
  \( C = C^\perp \leq \mathbb{F}_2^n \) extremal if \( d(C) = 4 + 4\left\lfloor \frac{n}{24} \right\rfloor \)

- Orbit Counting:
  \( C = C^\perp, \sigma \in \text{Aut}(C) \) of odd prime order \( p \) and Type \((z, f)\), then
  \( 2^{(z+f)/2} \equiv 2^{n/2} \pmod{p} \)

- Quadratic Forms:
  \( C = C^\perp \) doubly even, then \( n \in 8\mathbb{Z} \) and \( \text{Aut}(C) \leq \text{Alt}_n \).

- Equivariant Witt groups and Representation Theory:
  Characterisation of the permutation groups admitting a self-dual doubly-even invariant code.

- Modular Representation Theory and Invariant Theory (see below):
  \( n = 24m, \ d(C) = 4m + 4, \ \tau \in \text{Aut}(C) \) of Type \((12m, 0)\).
  If \( m \) is odd then \( C \) is a free \( \mathbb{F}_2\langle \tau \rangle \)-module.
C = C^⊥ \leq \mathbb{F}_2^{72} extremal, G = \text{Aut}(C).

**Theorem (Conway, Huffmann, Pless, Bouyuklieva, O’Brien, Willems, Feulner, Borello, Yorgov, N., ..)**

Let $C \leq \mathbb{F}_2^{72}$ be an extremal doubly even code, $G := \text{Aut}(C) := \{\sigma \in S_{72} \mid \sigma(C) = C\}$

- Let $p$ be a prime dividing $|G|$, $\sigma \in G$ of order $p$.
- If $p = 2$ or $p = 3$ then $\sigma$ has no fixed points. (B)
- If $p = 5$ or $p = 7$ then $\sigma$ has 2 fixed points. (CHPB)
- If $p = 2$ then $C$ is a free $\mathbb{F}_2\langle \sigma \rangle$-module. (N)
- $G$ contains no element of prime order $\geq 7$. (BYFN)
- $G$ contains no element of order 6. (Borello)
- $G$ has no subgroup $S_3$. (BN)
- $G \not\cong \text{Alt}_4$, $G \not\cong D_8$, $G \not\cong C_2 \times C_2 \times C_2$ (BN)
- and hence $|G| \leq 5$.
- $G$ contains no element of order 4. (Y)

Existence of an extremal code of length 72 is still open.
The Type of a permutation of prime order
Theoretical results, \( p \) odd.

**Definition (recall)**

Let \( \sigma \in S_n \) of prime order \( p \). Then \( \sigma \) is of Type \((z, f)\), if \( \sigma \) has \( z \) \( p \)-cycles and \( f \) fixed points. \( zp + f = n \).

**Theorem (Conway, Pless) (recall)**

Let \( C = C^\perp \leq \mathbb{F}_2^n, \sigma \in \text{Aut}(C) \) of odd prime order \( p \) and Type \((z, f)\).

Then \( 2^{(z+f)/2} \equiv 2^{n/2} \pmod{p} \).

**Corollary.** \( n = 72 \Rightarrow p \neq 37, 43, 53, 59, 61, 67. \)

**Corollary.** If \( n = 8 \) then \( p \neq 5 \) and \( p = 3 \Rightarrow \text{Type } (2, 2). \)

\( 2^4 \neq 2^{(1+3)/2} \pmod{5}, 2^4 \neq 2^{(1+5)/2} \pmod{3}. \)
Computational results, $p$ odd.

**BabyTheorem:** $n = 8, p = 3$

All doubly even self-dual codes of length 8 that have an automorphism of order 3 are equivalent to $h_8$.

- $\sigma = (1, 2, 3)(4, 5, 6)(7)(8) \in \text{Aut}(C)$
- $e_0 = 1 + \sigma + \sigma^2$, $e_1 = \sigma + \sigma^2$ idempotents in $F_2\langle \sigma \rangle$
- $C = Ce_0 \perp Ce_1 \leq F_2^8e_0 \perp F_2^8e_1 \cong F_2^4 \perp F_4^2$
- $Ce_0 = \text{Fix}_C(\sigma)$ isomorphic to a self-dual code in $F_2^4$, so

\[
Ce_0 : \begin{bmatrix}
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1
\end{bmatrix}
\]

- $Ce_1 \cong E_C(\sigma) \leq F_4^2$ Hermitian self-dual, $Ce_1 \cong [1, 1]$, so

\[
Ce_1 : \begin{bmatrix}
0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0
\end{bmatrix}
\]

and hence

\[
C : \begin{bmatrix}
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0
\end{bmatrix}
\]
Computational results, $p$ odd.

**Theorem.** (Borello, Feulner, N. 2012, 2013)

Let $C = C^\perp \leq \mathbb{F}_2^{72}$, $d(C') \geq 16$. Then $\text{Aut}(C)$ has no subgroup $C_7$, $C_3 \times C_3$, $D_{10}$, $S_3$.

▶ **Proof.** for $S_3 = \langle \sigma, \tau \mid \sigma^3, \tau^2, (\sigma\tau)^2 \rangle$

▶ $\sigma = (1, 2, 3)(4, 5, 6) \cdots (67, 68, 69)(70, 71, 72)$

▶ $\tau = (1, 4)(2, 6)(3, 5) \cdots (67, 70)(68, 72)(69, 71)$

▶ $C \cong \text{Fix}_C(\sigma) \oplus E_C(\sigma)$ with $E_C(\sigma) \leq \mathbb{F}_4^{24}$ Hermitian self-dual.

▶ $\tau$ acts on $E_C(\sigma)$ by $(\epsilon_1, \epsilon_2, \ldots, \epsilon_{23}, \epsilon_{24})^\tau = (\overline{\epsilon_2}, \overline{\epsilon_1}, \ldots, \overline{\epsilon_{24}}, \overline{\epsilon_{23}})$

▶ $\text{Fix}_{E_C(\sigma)}(\tau) = \{ \epsilon := (\overline{\epsilon_2}, \epsilon_2 \ldots, \overline{\epsilon_{24}}, \epsilon_{24}) \in E_C(\sigma) \}$

▶ $\cong \pi(\text{Fix}_{E_C(\sigma)}(\tau)) = \{ (\epsilon_2, \ldots, \epsilon_{24}) \mid \epsilon \in \text{Fix}_{E_C(\sigma)}(\tau) \} \leq \mathbb{F}_4^{12}$

▶ is trace Hermitian self-dual additive code, minimum distance $\geq 4$.

▶ There are 195,520 such codes.

▶ $\langle \text{Fix}_{E_C(\sigma)}(\tau) \rangle_{\mathbb{F}_4} = E_C(\sigma)$.

▶ No $E_C(\sigma)$ has minimum distance $\geq 8$. 
\( C = C' \perp \leq \mathbb{F}_2^{72}, \) doubly-even.

Theoretical results, \( p \) even.

**Theorem.** (A. Meyer, N.) (recall)

Let \( C = C' \perp \leq \mathbb{F}_2^n \) doubly-even. Then \( \text{Aut}(C) \leq \text{Alt}_n \).

**Corollary.** \( \text{Aut}(C') \) has no element of order 8.

\( \sigma \in \text{Aut}(C') \) of order 8. Then

\[
\sigma = (1, 2, \ldots, 8)(9, \ldots, 16) \ldots (65, \ldots, 72)
\]

since \( \sigma^4 \) has no fixed points. So \( \text{sign}(\sigma) = -1 \), a contradiction.

(This corollary was known before and is already implied by the Sloane-Thompson Theorem.)
$C = C^\perp \leq \mathbb{F}_2^{72}$, doubly even, extremal, so $d(C) = 16$

Theoretical results, $p$ even.

**Theorem. (N. 2012)**

Let $\tau \in \text{Aut}(C)$ of order 2. Then $C$ is a free $\mathbb{F}_2\langle \tau \rangle$-module.

- Let $R = \mathbb{F}_2\langle \tau \rangle$ the free $\mathbb{F}_2\langle \tau \rangle$-module, $S = \mathbb{F}_2$ the simple one.
- Then $C = R^a \oplus S^b$ with $2a + b = 36$.
- $F := \text{Fix}_C(\tau) = \{c \in C \mid c\tau = c\} \cong S^{a+b}$, $C(1 - \tau) \cong S^a$.
- $\tau = (1, 2)(3, 4) \ldots (71, 72)$.
- $F \cong \pi(F)$, $\pi(c) = (c_2, c_4, c_6, \ldots, c_{72}) \in \mathbb{F}_2^{36}$.
- **Fact:** $\pi(F) = \pi(C(1 - \tau))^\perp \supseteq D = D^\perp \supseteq \pi(C(1 - \tau))$.
- $d(F) \geq d(C) = 16$, so $d(D) \geq d(\pi(F)) \geq 8$.
- There are 41 such extremal self-dual codes $D$ (Gaborit et al).
- No code $D$ has a proper overcode with minimum distance $\geq 8$.
- This can also be seen a priori considering weight enumerators.
- So $\pi(F) = D$ and hence $a + b = 18$, so $a = 18$, $b = 0$. 
Theorem: $C$ is a free $\mathbb{F}_2\langle \tau \rangle$-module.

Corollary. $\text{Aut}(C)$ has no element of order 8.

$g \in \text{Aut}(C)$ of order 8. Then $C$ is a free $\mathbb{F}_2\langle g^4 \rangle$-module, hence also a free $\mathbb{F}_2\langle g \rangle$-module of rank $\dim(C)/8 = 36/8 = 9/2$ a contradiction.

Corollary. $\text{Aut}(C)$ has no subgroup $Q_8$.

Use a theorem by J. Carlson: If $M$ is an $\mathbb{F}_2Q_8$-module such that the restriction of $M$ to the center of $Q_8$ is free, then $M$ is free.

Corollary. $\text{Aut}(C)$ has no subgroup $U \cong C_2 \times C_4$, $C_8$ or $C_{10}$.

- Let $\tau \in U$ of order 2, $F = \text{Fix}_C(\tau) \cong \pi(F) = D = D^\perp \leq \mathbb{F}_2^{36}$.
- Then $D$ is one of the 41 extremal codes classified by Gaborit etal.
- $U/\langle \tau \rangle \cong C_4$ or $C_5$ acts on $D$.
- None of the 41 extremal codes $D$ has a fixed point free automorphism of order 4 or an automorphism of order 5 with exactly one fixed point.
\(\text{Alt}_4 = \langle a, b, \sigma \rangle \supseteq \langle a, b \rangle = V_4, \) (Borello, N. 2013)

Computational results: No \(\text{Alt}_4 \leq \text{Aut}(C)\).

3 possibilities for \(D\)
\[
\dim(D^\perp / D) = 20, 20, 22.
\]
\(C/D \leq D^\perp / D\)

maximal isotropic subspace.

\(V_4\) acts trivially on \(D^\perp / D = V\).

\(V = Ve_0 \oplus Ve_1\)
is an \(\mathbb{F}_2 \langle \sigma \rangle\)-module.

Unique possibility for \(Ce_0\).

\(Ce_1 \leq Ve_1\) Hermitian

maximal singular \(\mathbb{F}_4\)-subspace.

Compute

all these subspaces as orbit

under the unitary group of \(Ve_1\).

No extremal code is found.
Theorem. (Borello, N. 2014)

\[ C = C^\perp \leq \mathbb{F}_2^{24m}, \text{ extremal, i.e. } d(C') = 4m + 4, \quad m \geq 3, \quad \tau \in \text{Aut}(C') \text{ of order } 2. \]

- Bouyuklieva: \( \tau \sim (1, 2) \cdots (24m - 1, 24m) \) (Type \((12m, 0)\)) unless \( m = 5 \) where Type \((48, 24)\) might be possible.
- Assume \( \tau \sim (1, 2) \cdots (24m - 1, 24m) \).
- \( D' := \pi(\text{Fix}_C(\tau)) \) is the dual of some self-orthogonal code of length \( 12m \) with \( d(D') \geq 2m + 2 \).
- \( C \) is a free \( \mathbb{F}_2\langle \tau \rangle \)-module, if and only if \( D' \) is self-dual.
- If \( D' \) is not self-dual then \( d(D') \leq 4\lfloor \frac{m}{2} \rfloor + 2 \).
- If \( m \) is odd, then \( C \) is a free \( \mathbb{F}_2\langle \tau \rangle \)-module.