Automorphisms of extremal codes

Gabriele Nebe

Lehrstuhl D für Mathematik

Stuttgart, June 26, 2012
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 $C^\perp := \{ x \in \mathbb{F}_2^n | (x, c) := \sum_{i=1}^{n} x_i c_i = 0 \text{ for all } c \in C \}$
- $C$ is called **self-dual** if $C = C^\perp$.
- The Hamming weight of a codeword $c \in C$ is $\text{wt}(c) := |\{i | c_i \neq 0\}|$.
- $\text{wt}(c) \equiv_2 (c, c)$, so $C \subseteq C^\perp$ implies $\text{wt}(C) \subseteq 2\mathbb{Z}$.
- $C$ is called **doubly-even** if $\text{wt}(C) \subset 4\mathbb{Z}$.
- The minimum distance $d(C) := \min\{\text{wt}(c) | 0 \neq c \in C\}$.
- The weight enumerator of $C$ is $p_C := \sum_{c \in C} x^{n-\text{wt}(c)} y^{\text{wt}(c)} \in \mathbb{C}[x, y]_n$.

The minimum distance measures the error correcting quality of a self-dual code.
Doubly-even self-dual codes

Remark

- $C = C^\perp \Rightarrow 1 = (1, \ldots, 1) \in C$, since $(c, c) = (c, 1)$.
- If $C$ is self-dual then $n = 2 \dim(C)$ is even and
  
  $1 \in C^\perp = C \subset 1^\perp = \{ c \in F_2^m \mid \wt(c) \text{ even} \}$.

- Self-dual doubly-even codes correspond to totally isotropic subspaces in the quadratic space $1^\perp/\langle 1 \rangle$.
- $C = C^\perp \leq F_2^m$ doubly-even $\Rightarrow n \in 8\mathbb{Z}$. 
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 \( \geq 8 \). \( \text{Aut}(G_{24}) = M_{24} \)

\[ p_{G_{24}} = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24} \]
Turyn’s construction of the Golay code

Construction of Golay code

Choose two copies $C$ and $D$ of $h_8$ such that

$$C \cap D = \langle 1 \rangle, \quad C + D = 1^\perp \leq \mathbb{F}_2^8$$

$$G_{24} := \{(c + d_1, c + d_2, c + d_3) \mid c \in C, d_i \in D, d_1 + d_2 + d_3 \in \langle 1 \rangle \}$$

(a) $G_{24} = G_{24}^\perp$.
(b) $G_{24}$ is doubly-even.
(c) $d(G_{24}) = 8$.

Proof: (a) unique expression if $c$ represents classes in $C/\langle 1 \rangle$, so

$$|G_{24}| = 2^3 \cdot 2^4 \cdot 2^4 \cdot 2 = 2^{12}$$

Suffices $G_{24} \subseteq G_{24}^\perp$: 

\[3(c, c') + (c, d'_1 + d'_2 + d'_3) + (d_1 + d_2 + d_3, c') + (d_1, d'_1) + (d_2, d'_2) + (d_3, d'_3) = 0\]

(b) Follows since $C$ and $D$ are doubly-even, so generators have weight divisible by 4.
Turyn’s construction of the Golay code

Construction of Golay code.

Choose two copies $C$ and $D$ of $h_8$ such that

$$C \cap D = \langle 1 \rangle, \quad C + D = 1^\perp \leq \mathbb{F}_2^8$$

$G_{24} := \{(c + d_1, c + d_2, c + d_3) \mid c \in C, d_i \in D, d_1 + d_2 + d_3 \in \langle 1 \rangle\}$

(c) $d(G_{24}) = 8$.

Proof: (c)

$\text{wt}(c + d_1, c + d_2, c + d_3) = \text{wt}(c + d_1) + \text{wt}(c + d_2) + \text{wt}(c + d_3)$.

▶ 1 non-zero component: $(d, 0, 0)$ with $d \in \langle 1 \rangle$, weight 8.

▶ 2 non-zero components: $(d_1, d_2, 0)$ with $d_1, d_2 \in D \cong h_8$, weight $\geq d(h_8) + d(h_8) = 4 + 4 = 8$.

▶ 3 non-zero components: All have even weight, so weight $\geq 2 + 2 + 2 = 6$. By (b) the weight is a multiple of 4, so $\geq 8$. 
Theorem (Gleason)

Let $C = C^\perp \leq \mathbb{F}_2^n$ be doubly even. Then

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

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

- $p_C \in \text{Inv}(G_{192}) = \mathbb{C}[p_{h8}, p_{g24}]$

- $d(C) \leq 4 + 4\lfloor \frac{n}{24} \rfloor$

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

<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>80</th>
<th>≥ 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>16</td>
<td></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>≥ 4</td>
<td>0</td>
</tr>
</tbody>
</table>
Extremal polynomials

\[ \mathbb{C}[p_{h_8}, p_{G_{24}}] = \mathbb{C}[x^8 + 14x^4y^4 + y^8, x^4y^4(x^4 - y^4)^4] = \text{Inv}(G_{192}) \]

Basis of \( \mathbb{C}[f(1,y), g(1,y)]_{8k} \)

\[
\begin{align*}
  f^k &= 1 + 14k y^4 + y^8 + \ldots \\
  f^{k-3}g &= y^4 + y^8 + \ldots \\
  f^{k-6}g^2 &= y^8 + \ldots \\
  &\vdots \\
  f^{k-3m_k}g^{m_k} &= y^{4m_k} + \ldots 
\end{align*}
\]

where \( m_k = \left\lfloor \frac{n}{24} \right\rfloor = \left\lfloor \frac{k}{3} \right\rfloor \).

**Definition**

This space contains a unique polynomial

\[
p^{(k)} := 1 + 0y^4 + 0y^8 + \ldots + 0y^{4m_k} + a_k y^{4m_k + 4} + b_k y^{4m_k + 8} + \ldots
\]

\( p^{(k)} \) is called the extremal polynomial of degree \( 8k \).

\[
\begin{align*}
p^{(1)} &= p_{h_8}, \quad p^{(2)} = p_{h_8}^2, \quad p^{(3)} = p_{G_{24}}, \quad p^{(6)} = 1 + 17296y^{12} + 535095y^{16} + \ldots \\
p^{(9)} &= 1 + 249849y^{16} + 18106704y^{20} + 462962955y^{24} + \ldots
\end{align*}
\]
Automorphism groups of extremal codes

\[ \text{Aut}(C) = \{ \sigma \in S_n \mid \sigma(C) \subseteq C \}. \]

- \( \text{Aut}(h_8) = 2^3.L_3(2) \)
- \( \text{Aut}(G_{24}) = M_{24} \)
- 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?
- Such \((72, 36, 16)\) code \(C\) has \(\text{Aut}(C)\) of order 5 or dividing 24.

<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>80</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>16</td>
<td>( )</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>( \geq 4 )</td>
<td>0</td>
</tr>
</tbody>
</table>

Turyn applied to Golay: \( C \cong G_{24} \cong D, C \cap D = \langle 1 \rangle \)

\[ X = \{(c + d_1, c + d_2, c + d_3) \mid c \in C, d_i \in D, d_1 + d_2 + d_3 \in \langle 1 \rangle \} \leq \mathbb{F}_2^{72} \]

will not define an extremal code of length 72. Such an extremal code has no automorphism of order 2 which has fixed points.
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 (Bouyuklieva).
- If $p = 5$ then $\sigma$ has 2 fixed points.
- If $p = 2$ then $C$ is a free $\mathbb{F}_2\langle\sigma\rangle$-module (N.).
- Summarize:
  - $|G| = 5$ or divides 24.
  - $G$ contains no element of order 6 (Borello).
  - Subgroups of order 8 of $G$ are $D_8$ or $C_2 \times C_2 \times C_2$ (N.)

Existence of an extremal code of length 72 is still open.
Automorphisms of doubly-even self-dual codes

Theoretical results, \( p = 2 \).

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

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

\( C \) corresponds to a maximal isotropic subspace of the quadratic space \( 1^\perp / 1 \). The stabilizer in the full orthogonal group of such a space has trivial Dickson invariant.

The restriction of the Dickson invariant to \( S_n \) is the sign.

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

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

- \( n \in 8\mathbb{N} \),
- \( G \leq \text{Alt}_n \), and
- all self-dual composition factors of the \( \mathbb{F}_2 G \)-module \( \mathbb{F}_2^n \) occur with even multiplicity.
The Type of a permutation of prime order
Theoretical results, $p$ odd.

**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. $zp + f = n$.

**Theorem (Conway, Pless)**

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

Then

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

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

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

$2^4 \not\equiv 2^{(1+3)/2} \pmod{5}$, $2^4 \not\equiv 2^{(1+5)/2} \pmod{3}$. 
A Baby Example: $n = 8$, $p = 3$

BabyTheorem

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 $\mathbb{F}_2\langle \sigma \rangle$
- $C = Ce_0 \perp Ce_1$
- $Ce_0 = \text{Fix}_C(\sigma)$ isomorphic to a self-dual code in $\mathbb{F}_4^2$, so
  
  $Ce_0 : \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$

- $Ce_1 \leq \mathbb{F}_4^2$ 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

$C : \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$
$C = C^\perp \leq \mathbb{F}_2^{72}$, doubly-even, extremal, $G := \text{Aut}(C)$.

Recall

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

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

**Corollary.** $G$ has no element of order 8.

$\sigma \in G$ 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.
Order of $\sigma = 2$

Computational results, $p = 2$.

Theorem. (N.)

Let $\sigma \in G$ of order 2. Then $C$ is a free $\mathbb{F}_2\langle \sigma \rangle$-module.

- Let $R = \mathbb{F}_2\langle \sigma \rangle$ the free $\mathbb{F}_2\langle \sigma \rangle$-module, $S = \mathbb{F}_2$ the simple one.
- Then $C = R^a \oplus S^b$ with $2a + b = 36$.
- $F := \text{Fix}_C(\sigma) = \{c \in C \mid c\sigma = c\} \cong S^{a+b}$, $C(1 - \sigma) \cong S^a$.
- $\sigma = (1, 2)(3, 4) \ldots (71, 72)$.
- $F \cong \pi(F), \pi(c) = (c_1, c_3, c_5, \ldots, c_{71}) \in \mathbb{F}_2^{36}$.
- Fact: $\pi(F) = \pi(C(1 - \sigma))^{\perp} \supseteq D = D^{\perp} \supseteq \pi(C(1 - \sigma))$.
- $d(F) \geq d(C) = 16$, 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 $\geq 8$.
- So $\pi(F) = D$ and hence $a + b = 18$, so $a = 18$, $b = 0$. 
Theorem: $C$ is a free $\mathbb{F}_2\langle \sigma \rangle$-module.

Corollary. $G$ has no element of order 8.

$g \in G$ 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. $G$ 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. $G$ has no subgroup $U \cong C_2 \times C_4$, $C_8$ or $C_{10}$.

Let $\sigma \in U$ of order 2, $F = \text{Fix}_C(\sigma) \cong \pi(F) = D = D^\perp \leq \mathbb{F}_2^{36}$. Then $D$ is one of the 41 extremal codes classified by Gaborit et al. 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.
\[ C = C^\perp \leq \mathbb{F}_2^{72} \text{ extremal}. \]

Computational results, \( p \) odd.

Assume that \( U := C_3 \times C_3 = \langle a, b \rangle \leq G = \text{Aut}(C) \).

\begin{itemize}
  \item \( a = (1, 4, 7)(2, 5, 8)(3, 6, 9) \ldots (66, 69, 72) \)
  \item \( b = (1, 2, 3)(4, 5, 6)(7, 8, 9) \ldots (70, 71, 72) \)
  \item \( R := \mathbb{F}_2 U \cong \mathbb{F}_2 \oplus \mathbb{F}_4 \oplus \mathbb{F}_4 \oplus \mathbb{F}_4 \oplus \mathbb{F}_4 \)
  \item \( \mathbb{F}_2^{72} \cong R^8 \cong \mathbb{F}_2^8 \oplus \mathbb{F}_4^8 \oplus \mathbb{F}_4^8 \oplus \mathbb{F}_4^8 \)
  \item \( C = \varphi_0(C_0) \oplus \varphi_1(C_1) \oplus \varphi_2(C_2) \oplus \varphi_3(C_3) \oplus \varphi_4(C_4) \)
  \item with \( C_0 = C_0^\perp \leq \mathbb{F}_2^8 \) doubly-even, so \( C_0 \cong h_8 \)
  \item \( C_i = C_i^\perp \leq \mathbb{F}_4^8 \) hermitian self-dual, will see \( C_i \cong \mathbb{F}_4 \otimes h_8 \)
\end{itemize}

\[ C := C_0 \otimes \langle (1, 1, 1, 1, 1, 1, 1, 1) \rangle \]
\[ \perp C_1 \otimes_{\mathbb{F}_4} \langle (1, 1, 0, 1, 1, 0, 1, 1, 0), (1, 0, 1, 1, 0, 1, 1, 0, 1) \rangle_{\mathbb{F}_2} \]
\[ \perp C_2 \otimes_{\mathbb{F}_4} \langle (1, 1, 1, 1, 1, 1, 0, 0, 1), (1, 1, 1, 0, 0, 0, 1, 1, 1) \rangle_{\mathbb{F}_2} \]
\[ \perp C_3 \otimes_{\mathbb{F}_4} \langle (1, 1, 0, 0, 1, 1, 1, 0, 1), (1, 0, 1, 1, 1, 0, 0, 1, 1) \rangle_{\mathbb{F}_2} \]
\[ \perp C_4 \otimes_{\mathbb{F}_4} \langle (1, 1, 0, 1, 0, 1, 0, 1, 1), (1, 0, 1, 0, 1, 1, 1, 1, 0) \rangle_{\mathbb{F}_2} \]

\( \varphi_0(C_0) \oplus \varphi_1(C_1) = \text{Fix}(a) = Q = S_{24} \otimes \langle (1, 1, 1) \rangle \) is an \( \mathbb{F}_2 \langle b \rangle \)-module.
No subgroup $U = C_3 \times C_3 = \langle a, b \rangle$.

Computational results, $p$ odd.

- May fix $Q := \varphi_0(C_0) \oplus \varphi_1(C_1) = G_{24} \otimes \langle (1, 1, 1) \rangle$.
- Unique conjugacy class of fixed point free automorphisms of order 3, $b' \in M_{24} = \text{Aut}(G_{24})$.
- $\mathcal{L} := \{ D \sim \mathbb{F}_4 \otimes h_8 \mid \varphi_0(C_0) \oplus \varphi_2(D) \cong Q \}$
- $|\mathcal{L}| = 17,496$.
- The centraliser of $b'$ in $M_{24}$ acts on $\mathcal{L}$ with 138 orbits.
- $\{ X := Q \perp \varphi_2(D) \mid D \in \mathcal{L}, d(X) \geq 16 \}$ contains 2 equivalence classes of $[72, 20, 16]$-codes, $X_1, X_2$.
- Both $\text{Aut}(X_i)$ contain a unique subgroup $\cong U$.
- $\mathcal{L}_j(X_i) := \{ D \in \mathcal{L} \mid d(X_i \perp \varphi_j(D)) \geq 16 \}, j = 3, 4$.
- $|\mathcal{L}_j(X_1)| = 7146, |\mathcal{L}_j(X_2)| = 2940$.
- For all $(C_3, C_4) \in \mathcal{L}_3(X_i) \times \mathcal{L}_4(X_i)$ check that $X_i \perp \varphi_3(C_3) \perp \varphi_4(C_4)$ has minimum distance $< 16$. (2 CPU days).
\( C = C^\perp \leq \mathbb{F}_2^{72} \) extremal, \( G = \text{Aut}(C) \).

Recall: Main Theorem

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

- \( |G| = 5 \) or divides 24.
- Elements of order 2 or 3 have no fixed points.
- Elements of order 5 have 2 fixed points.
- \( C \) is a free \( \mathbb{F}_2\langle \sigma \rangle \)-module, for \( \sigma \in \text{Aut}(C) \) of order 2.
- \( G \) contains no element of order 6.
- Subgroups of order 8 of \( G \) are \( D_8 \) or \( C_2 \times C_2 \times C_2 \).
- Existence of an extremal code of length 72 is still open.