Automorphisms of extremal codes

Gabriele Nebe

Lehrstuhl D für Mathematik

Princeton, November 2015

Plan

The use of symmetry

- Beautiful objects have symmetries.
- Symmetries help to reduce the search space for nice objects
- and hence make huge problems accessible to computations.

The use of challenge problems

- Applications for classical theories and theorems such as
- Burnside orbit counting
- Invariant theory of finite groups
- Theory of quadratic forms
- Representation theory of finite groups
- Provide a practical introduction to abstract theory.

Self-dual codes

- 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
$$\mathrm{wt}(c) := |\{i \mid c_i \neq 0\}|.$$
- $\mathrm{wt}(c) \equiv_2 (c,c)$, so $C \subseteq C^\perp$ implies $\mathrm{wt}(C) \subset 2\mathbb{Z}$.
- C is called doubly-even if $\mathrm{wt}(C) \subset 4\mathbb{Z}$.
- The minimum distance $d(C) := \min\{\mathrm{wt}(c) \mid 0 \neq c \in C\}$.
- $\mathrm{Aut}(C) = \{\sigma \in S_n \mid \sigma(C) = C\}$.
- The weight enumerator of C is
$$p_C := \sum_{c \in C} x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)} \in \mathbb{C}[x,y]_n.$$

Facts

- $\dim(C) + \dim(C^\perp) = n$ so $C = C^\perp \Rightarrow \dim(C) = \frac{n}{2}$.
- Let $\mathbf{1} = (1,\ldots,1)$. Then $(c,c) = (c,\mathbf{1})$.
- So if $C = C^\perp$ then $\mathbf{1} \in C$.

Examples for self-dual doubly-even codes

Hamming Code

$$h_8 : \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

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 $\mathrm{Aut}(h_8) = 2^3 : L_3(2)$.

Golay Code

The binary Golay code $\mathcal{G}_{24}$ is the unique doubly-even self-dual code of length 24 with minimum distance ≥ 8. $\mathrm{Aut}(\mathcal{G}_{24}) = M_{24}$

$$p_{\mathcal{G}_{24}} = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}$$

Application of invariant theory

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

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.

Application of invariant theory

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

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:

- $p_C(x,y) = p_C(x,iy)$, $p_C(x,y) = p_{C^\perp}(x,y) = p_C(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}})$
- $G_{192} := \langle \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \rangle$.
- $p_C \in \mathrm{Inv}(G_{192}) = \mathbb{C}[p_{h_8}, p_{\mathcal{G}_{24}}]$
- $\exists! f \in \mathbb{C}[p_{h_8}, p_{\mathcal{G}_{24}}]_{8m}$ such that

$$f(1,y) = 1 + 0y^4 + \ldots + 0y^{4\lfloor \frac{m}{3} \rfloor} + a_m y^{4\lfloor \frac{m}{3} \rfloor + 4} + b_m y^{4\lfloor \frac{m}{3} \rfloor + 8} + \ldots$$

- $a_m > 0$ for all m

Application of invariant theory

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

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:

- $p_C(x,y) = p_C(x,iy)$, $p_C(x,y) = p_{C^\perp}(x,y) = p_C(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}})$
- $G_{192} := \langle \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \rangle$.
- $p_C \in \mathrm{Inv}(G_{192}) = \mathbb{C}[p_{h_8}, p_{\mathcal{G}_{24}}]$
- $\exists ! f \in \mathbb{C}[p_{h_8}, p_{\mathcal{G}_{24}}]_{8m}$ such that

$$f(1,y) = 1 + 0y^4 + \ldots + 0y^{4\lfloor \frac{m}{3} \rfloor} + a_m y^{4\lfloor \frac{m}{3} \rfloor + 4} + b_m y^{4\lfloor \frac{m}{3} \rfloor + 8} + \ldots$$

- $a_m > 0$ for all m

Proposition (Mallows, Sloane)

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

Classification of extremal codes

length	8	24	32	40	48	72	80	96	104	≥ 3952
$d(C)$	4	8	8	8	12	16	16	20	20	
extremal	h_8	$\mathcal{G}_{24}$	5	$16,470$	QR_{48}	?	≥ 15	?	≥ 1	0

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

- $\mathrm{Aut}(h_8) = 2^3.L_3(2)$
- $\mathrm{Aut}(\mathcal{G}_{24}) = M_{24}$
- Length 32: $L_2(31)$, $2^5.L_5(2)$, $2^8.S_8$, $2^8.L_2(7).2$, $2^5.S_6$.
- Length 40: 10,400 extremal codes with $\mathrm{Aut} = 1$.
- $\mathrm{Aut}(QR_{48}) = L_2(47)$.
- Sloane (1973): Is there a $(72, 36, 16)$ self-dual code?
- If C is such a $(72, 36, 16)$ code then $\mathrm{Aut}(C)$ has order ≤ 5.

Classification of extremal codes

length	8	24	32	40	48	72	80	96	104	≥ 3952
$d(C)$	4	8	8	8	12	16	16	20	20	
extremal	h_8	$\mathcal{G}_{24}$	5	$16,470$	QR_{48}	?	≥ 15	?	≥ 1	0

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

- $\mathrm{Aut}(h_8) = 2^3.L_3(2)$
- $\mathrm{Aut}(\mathcal{G}_{24}) = M_{24}$
- Length 32: $L_2(31)$, $2^5.L_5(2)$, $2^8.S_8$, $2^8.L_2(7).2$, $2^5.S_6$.
- Length 40: 10,400 extremal codes with $\mathrm{Aut} = 1$.
- $\mathrm{Aut}(QR_{48}) = L_2(47)$.
- Sloane (1973): Is there a $(72, 36, 16)$ self-dual code?
- If C is such a $(72, 36, 16)$ code then $\mathrm{Aut}(C)$ has order ≤ 5.
- There is no beautiful $(72, 36, 16)$ self-dual code.

Extremal even unimodular lattices

n	8	24	32	48	72	80	$\geq 163, 264$
min(L)	2	4	4	6	8	8	
extremal	1	1	$\geq 10^7$	≥ 4	≥ 1	≥ 4	0

The automorphism groups

$$\mathrm{Aut}(\Lambda_{24}) \cong 2.Co_1 \qquad 8315553613086720000 = 2^{22}3^9 5^4 7^2 \cdot 11 \cdot 13 \cdot 23$$

$$\mathrm{Aut}(P_{48p}) \cong (\mathrm{SL}_2(23) \times S_3) : 2 \qquad 72864 = 2^5 3^2 11 \cdot 23$$

$$\mathrm{Aut}(P_{48q}) \cong \mathrm{SL}_2(47) \qquad 103776 = 2^5 3 \cdot 23 \cdot 47$$

$$\mathrm{Aut}(P_{48n}) \cong (\mathrm{SL}_2(13) \mathsf{Y}\, \mathrm{SL}_2(5)).2^2 \qquad 524160 = 2^7 3^2 5 \cdot 7 \cdot 13$$

$$\mathrm{Aut}(P_{48m}) \cong (C_5 \times C_5 \times C_3) : (D_8 \mathsf{Y} C_4) \qquad 1200 = 2^4 3\, 5^2$$

$$\mathrm{Aut}(\Gamma_{72}) \cong (\mathrm{SL}_2(25) \times \mathrm{PSL}_2(7)) : 2 \qquad 5241600 = 2^8 3^2 5^2 7 \cdot 13$$

The Type of an automorphism

Definition

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

- Let p be odd, $\sigma = (1, 2, .., p)(p+1, .., 2p)...((z-1)p+1, .., zp)$
- $\mathbb{F}_2^n = \mathrm{Fix}(\sigma) \perp E(\sigma) = \mathbb{F}_2^n e_0 \perp \mathbb{F}_2^n e_1$ with
- $e_0 = 1 + \sigma + \ldots + \sigma^{p-1}$, $e_1 = 1 - e_0$.
- $C = C^{\perp}$, $\sigma \in \mathrm{Aut}(C)$
- get two self-dual codes Ce_0 and Ce_1 of smaller length

$$\begin{aligned}
Ce_0 = \mathrm{Fix}_C(\sigma) \quad &= \{(\underbrace{c_p \ldots c_p}_{p}\, \underbrace{c_{2p} \ldots c_{2p}}_{p} \ldots \underbrace{c_{zp} \ldots c_{zp}}_{p}\, c_{zp+1} \ldots c_n) \in C\} \\
\pi(\mathrm{Fix}_C(\sigma)) \quad &= \{(c_p c_{2p} \ldots c_{zp} c_{zp+1} \ldots c_n) \in \mathbb{F}_2^{z+f} \mid c \in \mathrm{Fix}_C(\sigma)\}
\end{aligned}$$

Fact

$\pi(\mathrm{Fix}_C(\sigma))$ is a self-dual code of length $z + f$, in particular

$$\dim(\mathrm{Fix}_C(\sigma)) = \frac{z+f}{2} \text{ and } |\mathrm{Fix}_C(\sigma)| = 2^{(z+f)/2}.$$

Application of Burnside's orbit counting theorem

Theorem (Conway, Pless, 1982)

Let $C = C^{\perp} \leq \mathbb{F}_2^n$, $\sigma \in \mathrm{Aut}(C)$ 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 $\frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}_M(g)|$.
Here $G = \langle \sigma \rangle$, $M = C$, $\mathrm{Fix}_C(g) = \mathrm{Fix}_C(\sigma)$ 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 $|\,\mathrm{Aut}(C)|$, 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.

Application of quadratic forms

Theorem (A. Meyer, N. 2009)

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

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

Application of Representation Theory

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

Theorem (Sloane, Thompson, 1988)

There is a G-invariant self-dual doubly-even code $C \leq \mathbb{F}_2 G$, 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 $G \leq \mathrm{Aut}(C)$, if and only if

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

General theoretical results (Summary)

- Invariant Theory:
  $C = C^\perp \leq \mathbb{F}_2^n$ extremal if $d(C) = 4 + 4\lfloor \frac{n}{24} \rfloor$
- Orbit Counting:
  $C = C^\perp$, $\sigma \in \mathrm{Aut}(C)$ 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 $\mathrm{Aut}(C) \leq \mathrm{Alt}_n$.
- Equivariant Witt groups and Representation Theory:
  Characterisation of the permutation groups admitting a self-dual doubly-even invariant code.

$C = C^{\perp} \leq \mathbb{F}_2^{72}$ extremal, $G = \mathrm{Aut}(C)$.

Theorem (Conway, Huffman, Pless, Bouyuklieva, O'Brien, Willems, Feulner, Borello, Yorgov, N., ..)

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

- If $p = 2$ or $p = 3$ then σ has no fixed points. (B)
- If $p = 5$ or $p = 7$ then σ has 2 fixed points. (CHPB)
- G contains no element of prime order ≥ 7. (BYFN)
- G has no subgroup S_3, D_{10}, $C_3 \times C_3$. (BFN)
- If $p = 2$ then C is a free $\mathbb{F}_2\langle\sigma\rangle$-module. (N)
- G has no subgroup C_{10}, $C_4 \times C_2$, Q_8.
- $G \not\cong \mathrm{Alt}_4$, $G \not\cong D_8$, $G \not\cong C_2 \times C_2 \times C_2$ (BN)
- G contains no element of order 6. (Borello)
- 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 σ is of Type (z, f), if σ has z p-cycles and f fixed points. $zp + f = n$.

Theorem (Conway, Pless) (recall)

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

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

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

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

$2^4 \not\equiv 2^{(1+3)/2} \pmod{5}$, $2^4 \not\equiv 2^{(1+5)/2} \pmod{3}$.

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.

- $\sigma = (1,2,3)(4,5,6)(7)(8) \in \mathrm{Aut}(C)$
- $e_0 = 1 + \sigma + \sigma^2$, $e_1 = \sigma + \sigma^2$ idempotents in $\mathbb{F}_2\langle\sigma\rangle$
- $C = Ce_0 \perp Ce_1 \leq \mathbb{F}_2^8 e_0 \perp \mathbb{F}_2^8 e_1 \cong \mathbb{F}_2^4 \perp \mathbb{F}_4^2$
- $Ce_0 = \mathrm{Fix}_C(\sigma)$ isomorphic to a self-dual code in $\mathbb{F}_2^4$, so

$$Ce_0 : \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

- $Ce_1 = E_C(\sigma) \leq \mathbb{F}_4^2$ 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

$$C \quad : \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Computational results, p odd.

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

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

- **Proof.** for $S_3 = \langle \sigma, \tau \mid \sigma^3, \tau^2, (\sigma\tau)^2 \rangle$
- $\sigma = (1,2,3)(4,5,6)\cdots(67,68,69)(70,71,72)$
- $\tau = (1,4)(2,6)(3,5)\cdots(67,70)(68,72)(69,71)$
- $C \cong \mathrm{Fix}_C(\sigma) \oplus E_C(\sigma)$ with $\mathrm{Fix}_C(\sigma) \cong (1,1,1) \otimes \mathcal{G}_{24}$ and
- $E_C(\sigma) \leq \mathbb{F}_4^{24}$ Hermitian self-dual, minimum distance ≥ 8.
- τ acts on $E_C(\sigma)$ by $(\epsilon_1, \epsilon_2, \ldots, \epsilon_{23}, \epsilon_{24})^{\tau} = (\overline{\epsilon_2}, \overline{\epsilon_1}, \ldots, \overline{\epsilon_{24}}, \overline{\epsilon_{23}})$
- $\mathrm{Fix}_{E_C(\sigma)}(\tau) = \{\epsilon := (\overline{\epsilon_2}, \epsilon_2 \ldots, \overline{\epsilon_{24}}, \epsilon_{24}) \in E_C(\sigma)\}$
- $\cong \pi(\mathrm{Fix}_{E_C(\sigma)}(\tau)) = \{(\epsilon_2, \ldots, \epsilon_{24}) \mid \epsilon \in \mathrm{Fix}_{E_C(\sigma)}(\tau)\} \leq \mathbb{F}_4^{12}$
- is trace Hermitian self-dual additive code, minimum distance ≥ 4.
- There are 195,520 such codes.
- $\langle \mathrm{Fix}_{E_C(\sigma)}(\tau) \rangle_{\mathbb{F}_4} = E_C(\sigma)$.
- No $E_C(\sigma)$ has minimum distance ≥ 8.

$C = C^{\perp} \leq \mathbb{F}_2^{72}$, doubly even, extremal, so $d(C) = 16$

Theorem. (N. 2012)

Let $\tau \in \mathrm{Aut}(C)$ 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 $2a + b = 36$.
- $F := \mathrm{Fix}_C(\tau) = \{c \in C \mid c\tau = c\} \cong S^{a+b}$, $C(1-\tau) \cong S^a$.
- $\tau = (1,2)(3,4)\ldots(71,72)$.
- $F \cong \pi(F), \pi(c) = (c_2, c_4, c_6, \ldots, c_{72}) \in \mathbb{F}_2^{36}$.
- **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 etal).
- No code D has a proper overcode with minimum distance ≥ 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. $\mathrm{Aut}(C)$ has no element of order 8.

$g \in \mathrm{Aut}(C)$ 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. $\mathrm{Aut}(C)$ has no subgroup Q_8.

Use a theorem by J. Carlson: If M is an $\mathbb{F}_2 Q_8$-module such that the restriction of M to the center of Q_8 is free, then M is free.

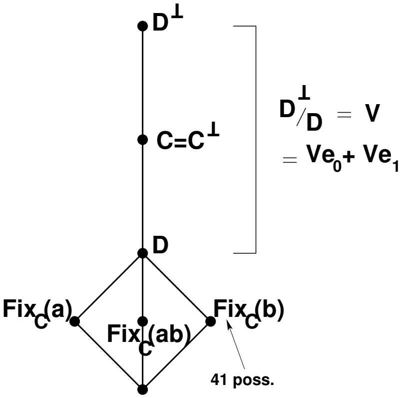
Corollary.

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

(needs inspection of automorphism group of the 41 possibile fixed codes)

$\mathrm{Alt}_4 = \langle a, b, \sigma \rangle \trianglerighteq \langle a, b \rangle = V_4$, (Borello, N. 2013)

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



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.

Theoretical results, $p = 2$.

Theorem. (N. 2012)

$C = C^{\perp} \leq \mathbb{F}_2^{72}$ extremal, $\tau \in \mathrm{Aut}(C)$ of order 2. Then C is a free $\mathbb{F}_2\langle\tau\rangle$-module.

Theorem (Borello, N. 2015)

Let $m \geq 3$ be odd and $C = C^{\perp}$ an extremal doubly-even binary code of length $24m$.

- If $\tau \in \mathrm{Aut}(C)$ is of order 2 and fixed point free then C is a free $\mathbb{F}_2\langle\tau\rangle$-module.
- If 8 divides $|\mathrm{Aut}(C)|$, then the Sylow 2-subgroups of $\mathrm{Aut}(C)$ are isomorphic to $C_2 \times C_2 \times C_2$, $C_2 \times C_4$, or D_8.

Conclusion

Search for extremal codes with automorphisms provides a nice application for classical theories in particular

- Quadratic Forms:
  $C = C^{\perp}$ doubly even, then $n \in 8\mathbb{Z}$ and $\mathrm{Aut}(C) \leq \mathrm{Alt}_n$.
- Obtain characterisation of the permutation groups admitting a self-dual doubly-even invariant code.
- Modular Representation Theory and Invariant Theory
  $n = 24m$, $d(C) = 4m + 4$, $\tau \in \mathrm{Aut}(C)$ of Type $(12m, 0)$.
  If m is odd then C is a free $\mathbb{F}_2\langle\tau\rangle$-module.

Motivation for explicit computations with a practical and detailed use of the structure of the automorphism group.