Automorphisms of extremal codes and lattices

Gabriele Nebe

Lehrstuhl D für Mathematik

Hannover 05.11.2013

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
$$\mathrm{wt}(c) := |\{i \mid c_i \neq 0\}|.$$
- $\mathrm{wt}(c) \equiv_2 (c,c)$, 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 $d(C) := \min\{\mathrm{wt}(c) \mid 0 \neq c \in C\}$.
- 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
$$p_C := \sum_{c \in C} x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)} \in \mathbb{C}[x,y]_n.$$
- $\mathrm{Aut}(C) = \{\sigma \in S_n \mid \sigma(C) \subseteq C\}$.

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

- $p_C(x,y) = p_C(x, iy)$, $p_C(x,y) = p_{C^\perp}(x,y) = p_C(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}})$
- $G_{192} := \langle \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \rangle$.
- $p_C \in \mathrm{Inv}(G_{192}) = \mathbb{C}[p_{h_8}, p_{\mathcal{G}_{24}}]$
- $d(C) \leq 4 + 4\lfloor \frac{n}{24} \rfloor$

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

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

Automorphism groups of extremal codes

$\mathrm{Aut}(C) = \{\sigma \in S_n \mid \sigma(C) \subseteq C\}$ 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.

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

Application of Burnside's orbit counting theorem

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. $zp + f = n$.

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

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

Fact: If $C = C^\perp$ and p is odd, then $\pi(\mathrm{Fix}_C(\sigma))$ 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

Remark

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

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

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

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

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

Application of quadratic forms

$\mathrm{Aut}(C) = \{\sigma \in S_n \mid \sigma(C) \subseteq C\}$ 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 $\mathrm{Aut}(C) \leq \mathrm{Alt}_n$.

- **Proof.** (sketch)
- $E_{n-2} := (\mathbf{1}^\perp/\langle\mathbf{1}\rangle, q), q(c + \langle\mathbf{1}\rangle) = \frac{1}{2}\,\mathrm{wt}(c) \pmod 2 \in \mathbb{F}_2$.
- $C/\langle\mathbf{1}\rangle$ is a maximal isotropic subspace E_{n-2}.
- The stabilizer in the orthogonal group of E_{n-2} of such a space has trivial Dickson invariant.
- 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

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

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

Theorem (Conway, Huffmann, Pless, Bouyuklieva, O'Brien, Willems, Feulner, Borello, Yankov, N., ..)

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

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

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).

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 $p = 3 \Rightarrow$ 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 $\mathbb{F}_2\langle\sigma\rangle$
- $C = Ce_0 \perp Ce_1$
- $Ce_0 = \mathrm{Fix}_C(\sigma)$ isomorphic to a self-dual code in $\mathbb{F}_2^4$, so

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

- $Ce_1 \cong E_C(\sigma) \leq \mathbb{F}_4^2$ 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 $C = C^{\perp} \leq \mathbb{F}_2^{72}$, $d(C) \geq 16$. 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 $E_C(\sigma) \leq \mathbb{F}_4^{24}$ Hermitian self-dual.
- 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.

Theoretical results, p even.

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

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

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

$\sigma \in \mathrm{Aut}(C)$ of order 8. Then

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

since σ^4 has no fixed points. So sign(σ) $= -1$, 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 $\tau \in \mathrm{Aut}(C)$ 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.

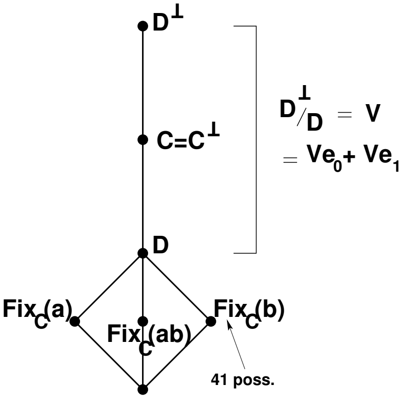
Use a theorem by J. Carlson: If M is an $\mathbb{F}_2 Q_8$-module such that the restriction of M to the center of Q_8 is free, then M is free.

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

- Let $\tau \in U$ of order 2, $F = \mathrm{Fix}_C(\tau) \cong \pi(F) = D = D^\perp \leq \mathbb{F}_2^{36}$.
- 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.

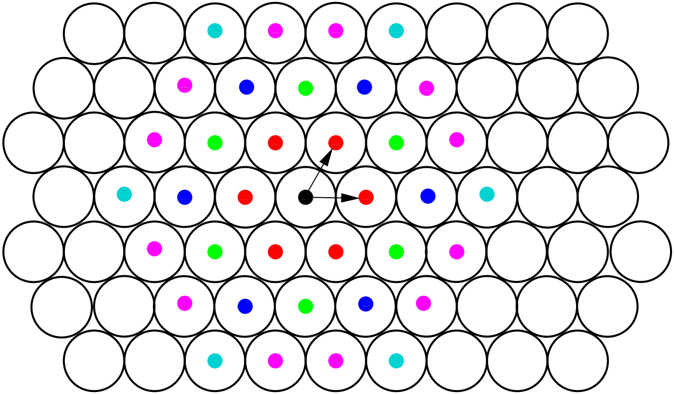
$\mathrm{Alt}_4 = \langle a, b, \sigma \rangle \trianglerighteq \langle a, b \rangle = V_4$, (Borello, N. 2013)

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.

Lattices and sphere packings



Hexagonal Circle Packing

$$\theta = 1 + 6q + 6q^3 + 6q^4 + 12q^7 + 6q^9 + \ldots.$$

Extremal even unimodular lattices

Definition

- A lattice L in Euclidean n-space $(\mathbb{R}^n, (\,,\,))$ is the $\mathbb{Z}$-span of an $\mathbb{R}$-basis $B = (b_1, \ldots, b_n)$ of $\mathbb{R}^n$

$$L = \langle b_1, \ldots, b_n \rangle_{\mathbb{Z}} = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in \mathbb{Z}\}.$$

- The dual lattice is

$$L^{\#} := \{x \in \mathbb{R}^n \mid (x, \ell) \in \mathbb{Z} \text{ for all } \ell \in L\}$$

- L is called unimodular if $L = L^{\#}$.
- L is called even if $(\ell, \ell) \in 2\mathbb{Z}$ for all $\ell \in L$.
- Then $Q : L \to \mathbb{Z}, \ell \mapsto \frac{1}{2}(\ell, \ell)$ is an integral quadratic form.
- $\min(L) := \min\{Q(\ell) \mid 0 \neq \ell \in L\}$ the minimum of L.
- L extremal if $L = L^{\#}$ and $\min(L) \geq 1 + \lfloor \frac{n}{24} \rfloor$.
- $\mathrm{Aut}(L) := \{g \in O(\mathbb{R}^n, (\,,\,)) \mid g(L) = L\}$ automorphism group of L.

Application of modular forms

The sphere packing density of a unimodular lattice is proportional to its minimum.
From the theory of modular forms one gets an upper bound for the minimum:

Extremal lattices

Let L be an n-dimensional even unimodular lattice. Then

$$n \in 8\mathbb{N} \text{ and } \min(L) \leq 1 + \lfloor \frac{n}{24} \rfloor .$$

Lattices achieving equality are called extremal.

Extremal even unimodular lattices.

n	8	16	24	32	40	48	72	80
min(L)	1	1	2	2	2	3	4	4
number of extremal lattices	1	2	1	$\geq 10^7$	$\geq 10^{51}$	≥ 4	≥ 1	≥ 4

Extremal even unimodular lattices in jump dimensions

The extremal theta series

$$f^{(3)} = 1 + 196,560q^2 + \ldots = \theta_{\Lambda_{24}}.$$
$$f^{(6)} = 1 + 52,416,000q^3 + \ldots = \theta_{P_{48p}} = \theta_{P_{48q}} = \theta_{P_{48n}} = \theta_{P_{48m}}.$$
$$f^{(9)} = 1 + 6,218,175,600q^4 + \ldots = \theta_{\Gamma_{72}}.$$

The automorphism groups

$\mathrm{Aut}(\Lambda_{24}) \cong 2.Co_1$	order $=$	8315553613086720000 $2^{22}3^9 5^4 7^2 11\ 13\ 23$
$\mathrm{Aut}(P_{48p}) \cong (\mathrm{SL}_2(23) \times S_3) : 2$	order	$72864 = 2^5 3^2 11\ 23$
$\mathrm{Aut}(P_{48q}) \cong \mathrm{SL}_2(47)$	order	$103776 = 2^5 3\ 23\ 47$
$\mathrm{Aut}(P_{48n}) \cong (\mathrm{SL}_2(13) \mathsf{Y}\, \mathrm{SL}_2(5)).2^2$	order	$524160 = 2^7 3^2 5\ 7\ 13$
$\mathrm{Aut}(P_{48m}) \geq$ soluble	order	mult. of $1200 = 2^4 3 5^2$
$\mathrm{Aut}(\Gamma_{72}) \cong (\mathrm{SL}_2(25) \times \mathrm{PSL}_2(7)) : 2$	order	$5241600 = 2^8 3^2 5^2 7\ 13$

The Type of an automorphism.

Let $L \leq \mathbb{R}^n$ be some even unimodular lattice and $\sigma \in \mathrm{Aut}(L)$ of prime order p. The fixed lattice

$$F := \mathrm{Fix}_L(\sigma) := \{v \in L \mid \sigma v = v\} \leq L$$

has dimension d, and σ acts on $M := F^{\perp}$ as a pth root of unity, so $n = d + z(p-1)$.

$$F^{\#} \perp M^{\#} \geq L = L^{\#} \geq F \perp M \geq pL$$

with $\det(F) = |F^{\#}/F| = |M^{\#}/M| = \det(M) = p^s$

Definition: p-(z,d)-s is called the Type of σ.

Proposition: $s \leq \min(d, z)$ and $z - s$ is even.

48-dimensional extremal lattices

Theorem (N. 2013)

Let L be an extremal even unimodular lattice of dimension 48 and p be a prime dividing $|\mathrm{Aut}(L)|$. Then $p = 47, 23$ or $p \leq 13$.
Let $\sigma \in \mathrm{Aut}(L)$ of order p. The fixed lattice $F := \mathrm{Fix}_L(\sigma)$ is:

p	$\dim F$	$\det(F)$	F	example
47	2	47	unique	P_{48q}
23	4	23^2	unique	P_{48q}, P_{48p}
13	0		$\{0\}$	P_{48n}
11	8	11^4	unique	P_{48p}
7	0		$\{0\}$	P_{48n}
7	6	7^5	$\sqrt{7}A_6^{\#}$	not known
5	0		$\{0\}$	P_{48n}, P_{48m}
5	8	5^8	$\sqrt{5}E_8$	P_{48m}
5	16	5^8	$[2.\mathrm{Alt}_{10}]_{16}$	P_{48m}
3	0,8,16..22	7 possibilities		
2	0		$\{0\}$	$\sigma = -1$
2	24	2^{24}	$\sqrt{2}\Lambda_{24}$	P_{48n}
2	24	2^{24}	$\sqrt{2}O_{24}$	$P_{48n}, P_{48p}, P_{48m}$

Application of number theory

Observation

The maximal dimension of the fixed lattice of some automorphism of prime order p is ≤ 22 if p is odd and ≤ 24 if $p = 2$.

Corollary

Let L be an extremal even unimodular lattice of dimension 48 and $\sigma \in \mathrm{Aut}(L)$ of order a. Then the minimal polynomial μ_σ is a multiple of the a-th cyclotomic polynomial ϕ_a.

Definition

Let $V(\sigma)$ be the maximal subspace of $\mathbb{Q}L$, on which σ acts with minimal polynomial ϕ_a. Then $V(\sigma) \cong \mathbb{Q}[\zeta_a]^z$ for some $z \geq 1$. Let $M := L \cap V(\sigma)$ and $F := L \cap V(\sigma)^\perp$. Then M is a $\mathbb{Z}[\zeta_a]$-sublattice of $V(\sigma)$ and $M \perp F$ is a sublattice of finite index in L.

The main classification result.

Theorem (N. 2013)

L even unimodular, extremal, $\dim(L) = 48$ and $\sigma \in \mathrm{Aut}(L)$ of order a such that $\varphi(a) > 24$. Then one of

- $a = 120$ and $L \cong P_{48n}$
- $a = 132$ and $L \cong P_{48p}$
- $a = 69$ and $L \cong P_{48p}$
- $a = 47$ and $L \cong P_{48q}$
- $a = 65$ and $L \cong P_{48n}$
- $a = 104$ and $L \cong P_{48n}$

The strategy of the proof is to

- first classify the candidates for M (ideal lattice)
- and F (fixed lattice of some element of prime order)
- and the possible actions of $\sigma_{|F} \in \mathrm{Aut}(F)$.
- Then compute the (σ_M, σ_F)-invariant unimodular overlattices L of $M \perp F$.
- Use reduction algorithms to prove $\min(L) \leq 2$ or
- if $\min(L) = 3$ then identify L with one of the known lattices.

Construction of the lattice P_{48m}.

Proposition (N. 2014)

Let L be an extremal even unimodular lattice of dimension 48, such that $\mathrm{Aut}(L)$ contains an automorphism σ of Type $5-(8,16)-s$. Then $s=8$, $F:=\mathrm{Fix}_L(\sigma)\cong[2.\mathrm{Alt}_{10}.2]$, $M:=\mathrm{Fix}_L(\sigma)^{\perp}$ is such that $M^{\#}$ is the unique unimodular $\mathbb{Z}[\zeta_5]$-lattice of dimension 8 with $\min(M)\geq 3$,

$$M\perp F\underbrace{\subset}_{5^8}L=L^{\#}\underbrace{\subset}_{5^8}M^{\#}\perp F^{\#}$$

Theorem (N. 2014)

$L=P_{48m}$ is the unique extremal lattice whose automorphism group contains an element of Type $5-(8,16)-8$.
(about 15 CPU years of computation)
$G:=\mathrm{Aut}(P_{48m})$ contains a soluble subgroup $S=\mathrm{Stab}_{\mathrm{Aut}(M\perp F)}(L)$ of order $2^4 3\, 5^2$. The Sylow 2-subgroup of G is $D_8 \mathrm{Y} C_4$ and the Sylow 5-subgroup of G is $C_5\times C_5$.