Symmetries of discrete structures

Gabriele Nebe

Lehrstuhl D für Mathematik

ÖMG-DMV meeting 2017

RWTH AACHEN UNIVERSITY

Plan

The use of symmetry

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

Discrete structures

- strongly regular graphs
- Steiner systems
- block designs
- latin squares
- abstract projective planes
- Hadamard matrices
- codes
- lattices
- ...

Plan

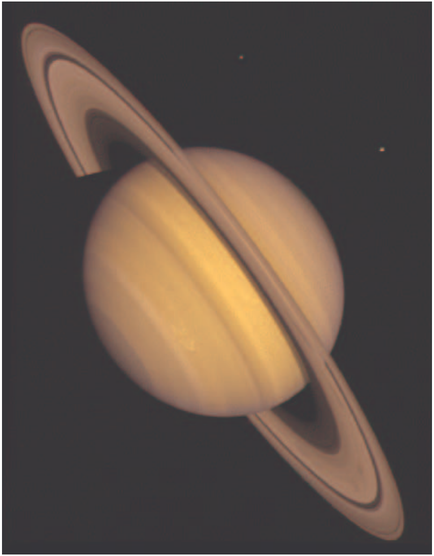
The use of symmetry

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

Discrete structures

- strongly regular graphs
- Steiner systems
- block designs
- latin squares
- abstract projective planes
- Hadamard matrices
- doubly-even self-dual codes
- even unimodular lattices
- Why ?

Voyager 1981



distance Saturn-Earth
more than
1 billion kilometers

power of transmitter:
less than 60 Watt

error correction with
Golay Code $\mathrm{QR}(23)$
of length 23

The best known codes
of small length
are self-dual
and doubly-even.

Doubly-even self-dual codes

- code $C \leq \mathbb{F}_2^n$ (linear binary code of length n)
- $C^\perp = \{x \in \mathbb{F}_2^n \mid x \cdot c := \sum_{i=1}^n x_i c_i = 0$ for all $c \in C\}$ dual code
- self-dual $C = C^\perp$
- $\mathrm{wt}(c) := |\{i \mid c_i \neq 0\}|$ weight
- $d(C) := \min\{\mathrm{wt}(c) \mid 0 \neq c \in C\}$ minimum distance
- Clear: $c \cdot c \equiv \mathrm{wt}(c) \pmod 2$
- C doubly-even if $\mathrm{wt}(C) \subseteq 4\mathbb{Z}$
- C doubly-even $\Rightarrow C \subseteq C^\perp$
- C doubly-even self-dual $\Leftrightarrow C/\langle \mathbf{1} \rangle \leq (\langle \mathbf{1} \rangle^\perp / \langle \mathbf{1} \rangle, q)$ maximal isotropic of dimension $(n-2)/2$,

$$q(c + \langle \mathbf{1} \rangle) = \frac{1}{2}\mathrm{wt}(c) + 2\mathbb{Z} \in \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2.$$

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

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

Extended Quadratic Residue Codes

Extended QR Codes, $p \equiv -1 \pmod 8$

$X^p - 1 = (X-1)g(X)h(X) \in \mathbb{F}_2[X]$, $\deg(g) = \deg(h) = \frac{p-1}{2}$.

$$\mathrm{QR}(p) := (\overline{g(X)}) \le \mathbb{F}_2[X]/(X^p - 1) \cong \mathbb{F}_2^p$$

is a code of length p and dimension $\frac{p+1}{2}$.
extended QR-Code

$$\hat{\mathrm{Q}}(p) := \{(c, \mathrm{wt}(c) + 2\mathbb{Z}) \mid c \in \mathrm{QR}(p)\} \le \mathbb{F}_2^{p+1}$$

is a self-dual doubly-even code of length $p+1$.

$\mathrm{QR}(p)$ is a cyclic code of length p ($p \mid |\mathrm{Aut}(\mathrm{QR}(p))|$).
Cyclic codes have good provable error correcting properties and fast encoding and decoding algorithms.

$\mathrm{Aut}(\hat{\mathrm{Q}}(7)) = 2^3 : \mathrm{PSL}_3(2)$, of order $8 \cdot 168 = 2^6 \cdot 3 \cdot 7$
$\mathrm{Aut}(\hat{\mathrm{Q}}(23)) = M_{24}$, of order $2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
$\mathrm{Aut}(\hat{\mathrm{Q}}(p)) = \mathrm{PSL}_2(p)$ for $p > 23$, of order $(p-1)p(p+1)/2$ (conj.).

Examples for self-dual doubly-even codes

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

$$\hat{\mathrm{Q}}(7) : \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

is the unique doubly-even self-dual code of length 8,

$$p_{\hat{\mathrm{Q}}(7)}(x,y) = x^8 + 14x^4y^4 + y^8$$

$\hat{\mathrm{Q}}(23)$ (extended Golay code) unique doubly-even self-dual code of length 24 with minimum distance ≥ 8.

$$p_{\hat{\mathrm{Q}}(23)} = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}$$

Application of invariant theory

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

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

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

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:

- $p_C(x,y) = p_C(x,iy)$, $p_C(x,y) = p_{C^\perp}(x,y) = p_C(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}})$
- $G_{192} := \langle \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \rangle$.
- $p_C \in \mathrm{Inv}(G_{192}) = \mathbb{C}[p_{\hat{Q}(7)}, p_{\hat{Q}(23)}]$
- $\exists! f \in \mathbb{C}[p_{\hat{Q}(7)}, p_{\hat{Q}(23)}]_{8m}$ 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

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

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:

- $p_C(x,y) = p_C(x,iy)$, $p_C(x,y) = p_{C^\perp}(x,y) = p_C(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}})$
- $G_{192} := \langle \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \rangle$.
- $p_C \in \mathrm{Inv}(G_{192}) = \mathbb{C}[p_{\hat{\mathrm{Q}}(7)}, p_{\hat{\mathrm{Q}}(23)}]$
- $\exists! f \in \mathbb{C}[p_{\hat{\mathrm{Q}}(7)}, p_{\hat{\mathrm{Q}}(23)}]_{8m}$ 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

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

Self-dual codes and Invariant Theory

Gleason 1970, N., Rains, Sloane 2006

Codes		Polynomials
C	$\mapsto$	p_C
properties of C (self-duality, doubly-even)	$\to$	symmetries of p_C $p_C \in \mathrm{Inv}(G)$
unstructured set		finitely generated ring
properties of C $d(C) \leq 4 + 4\lfloor \frac{n}{24} \rfloor$	$\Leftarrow$	$\mathrm{Inv}(G) = \mathbb{C}[p_1, \ldots, p_s]$
extremal code	$\to$	extremal weight enumerator

Automorphism groups of extremal codes

length	8	16	24	32	40	48	72	80	≥ 3952
$d(C)$	4	4	8	8	8	12	16	16	
extremal	$\hat{\mathrm{Q}}(7)$	2	$\hat{\mathrm{Q}}(23)$	5	$16,470$	$\hat{\mathrm{Q}}(47)$	$?$	≥ 15	0

Automorphism group $\mathrm{Aut}(C) = \{\sigma \in S_n \mid \sigma(C) = C\}$

- $\mathrm{Aut}(\hat{\mathrm{Q}}(7)) = 2^3 . \mathrm{PSL}_3(2)$
- $\mathrm{Aut}(\hat{\mathrm{Q}}(23)) = M_{24}$
- Length 32: $\mathrm{PSL}_2(31)$, $2^5 . \mathrm{PSL}_5(2)$, $2^8 . S_8$, $2^8 . \mathrm{PSL}_2(7).2$, $2^5 . S_6$.
- Length 40: 10,400 extremal codes with $\mathrm{Aut} = 1$.
- $\mathrm{Aut}(\hat{\mathrm{Q}}(47)) = \mathrm{PSL}_2(47)$.
- $d(\hat{\mathrm{Q}}(71)) = 12$, $d(\hat{\mathrm{Q}}(79)) = 16$.
- Sloane (1973): Is there a $(72, 36, 16)$ self-dual code?
- If $C = C^{\perp} \leq \mathbb{F}_2^{72}$, $d(C) = 16$ then $\mathrm{Aut}(C)$ has order ≤ 5.

Automorphism groups of extremal codes

length	8	16	24	32	40	48	72	80	≥ 3952
$d(C)$	4	4	8	8	8	12	16	16	
extremal	$\hat{\mathrm{Q}}(7)$	2	$\hat{\mathrm{Q}}(23)$	5	$16,470$	$\hat{\mathrm{Q}}(47)$	?	≥ 15	0

Automorphism group $\mathrm{Aut}(C) = \{\sigma \in S_n \mid \sigma(C) = C\}$

- $\mathrm{Aut}(\hat{\mathrm{Q}}(7)) = 2^3 . \mathrm{PSL}_3(2)$
- $\mathrm{Aut}(\hat{\mathrm{Q}}(23)) = M_{24}$
- Length 32: $\mathrm{PSL}_2(31)$, $2^5 . \mathrm{PSL}_5(2)$, $2^8 . S_8$, $2^8 . \mathrm{PSL}_2(7).2$, $2^5 . S_6$.
- Length 40: 10,400 extremal codes with $\mathrm{Aut} = 1$.
- $\mathrm{Aut}(\hat{\mathrm{Q}}(47)) = \mathrm{PSL}_2(47)$.
- $d(\hat{\mathrm{Q}}(71)) = 12$, $d(\hat{\mathrm{Q}}(79)) = 16$.
- Sloane (1973): Is there a $(72, 36, 16)$ self-dual code?
- If $C = C^{\perp} \leq \mathbb{F}_2^{72}$, $d(C) = 16$ then $\mathrm{Aut}(C)$ has order ≤ 5.
- There is no beautiful $(72, 36, 16)$ self-dual code.

The Type of an automorphism

Definition (Conway, Pless, Huffman 1982)

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, $\sigma = (1, 2, .., p)(p+1, .., 2p)...((z-1)p+1, .., zp)$.
- $\mathbb{F}_2^n = \mathrm{Fix}(\sigma) \perp E(\sigma) \cong \mathbb{F}_2^{z+f} \perp \mathbb{F}_2^{z(p-1)}$ with

$$\mathrm{Fix}(\sigma) = \left\langle \begin{array}{cccccccc} 1\dots1 & 0\dots0 & \dots & 0\dots0 & 0 & 0 & \dots & 0 \\ 0\dots0 & 1\dots1 & \dots & 0\dots0 & 0 & 0 & \dots & 0 \\ 0\dots0 & 0\dots0 & \dots & 1\dots1 & 0 & 0 & \dots & 0 \\ 0\dots0 & 0\dots0 & \dots & 0\dots0 & 1 & 0 & \dots & 0 \\ 0\dots0 & 0\dots0 & \dots & 0\dots0 & 0 & 1 & \dots & 0 \\ \underbrace{0\dots0}_{p} & \underbrace{0\dots0}_{p} & \dots & \underbrace{0\dots0}_{p} & 0 & 0 & \dots & 1 \end{array} \right\rangle$$

$$E(\sigma) = \mathrm{Fix}(\sigma)^{\perp} = \{(x_1, \dots, x_p, x_{p+1}, \dots, x_{2p}, \dots, x_{(z-1)p+1}, \dots, x_{zp}, 0, \dots, 0) \mid x_1 + \dots + x_p = x_{p+1} + \dots + x_{2p} = \dots = x_{(z-1)p+1} + \dots + x_{zp} = 0\}$$

Two self-dual codes of smaller length

- Let $C \leq \mathbb{F}_2^n$ and p an odd prime,
- $\sigma = (1, 2, .., p)(p + 1, .., 2p)...((z - 1)p + 1, .., zp) \in \mathrm{Aut}(C)$.
- Then $C = C \cap \mathrm{Fix}(\sigma) \oplus C \cap E(\sigma) =: \mathrm{Fix}_C(\sigma) \oplus E_C(\sigma)$.

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

- and $C^\perp = C^\perp \cap \mathrm{Fix}(\sigma) \oplus C^\perp \cap E(\sigma)$.

Theorem

If $C = C^\perp$ then $\pi(\mathrm{Fix}_C(\sigma)) \leq \mathbb{F}_2^{z+f}$ is self-dual and $E_C(\sigma)$ is (Hermitian) self-dual in $E(\sigma)$.

Method: Classify possibilities for $\pi(\mathrm{Fix}_C(\sigma))$ and $E_C(\sigma)$ and check if $C = \mathrm{Fix}_C(\sigma) \oplus E_C(\sigma)$ is extremal.

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

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

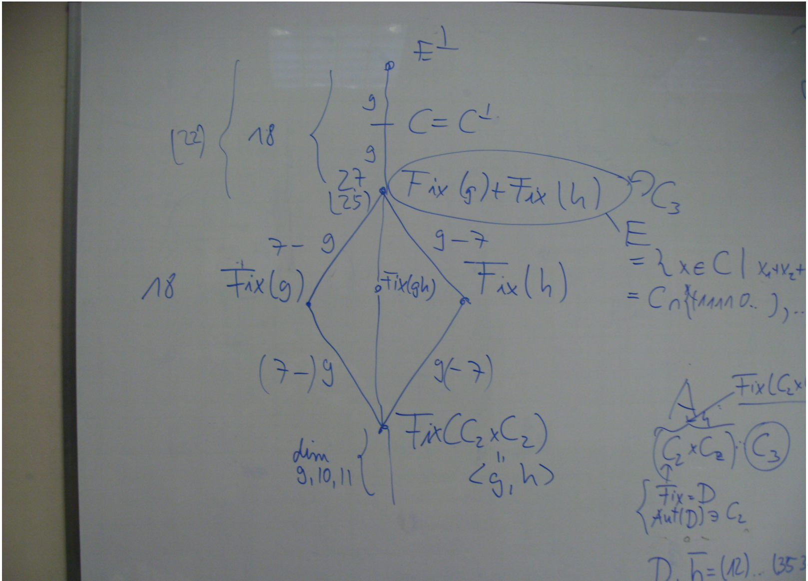
Let $C \leq \mathbb{F}_2^{72}$ be an extremal doubly even code,
$G := \mathrm{Aut}(C) := \{\sigma \in S_{72} \mid \sigma(C) = C\}$, $\sigma \in G$ of prime order p.

- 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. (N)
- $G \not\cong \mathrm{Alt}_4$, $G \not\cong D_8$, $G \not\cong C_2 \times C_2 \times C_2$ (BN)
- G contains no element of order 6. (Borello)
- and hence $|G| \leq 5$.
- G contains no element of order 4. (YY)

Existence of an extremal code of length 72 is still open.

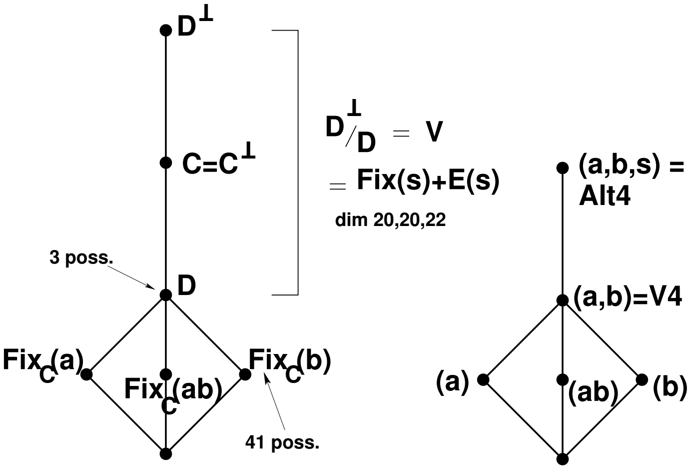
$\mathrm{Alt}_4 = \langle a,b,s \rangle \trianglerighteq \langle a,b \rangle = V_4$, (Borello, N. 2013)

Example: $C = C^\perp \leq \mathbb{F}_2^{72}$ extremal $\Rightarrow$ no $\mathrm{Alt}_4 \leq \mathrm{Aut}(C)$.



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

Example: $C = C^\perp \leq \mathbb{F}_2^{72}$ extremal $\Rightarrow$ no $\mathrm{Alt}_4 \leq \mathrm{Aut}(C)$.



Extremal binary codes: Summary

- $C = C^{\perp} \leq \mathbb{F}_2^n$ doubly-even $\Rightarrow 8 \mid n$ and $d(C) \leq 4 + 4\lfloor \frac{n}{24} \rfloor$
- all known extremal codes of length $n = 24m$:

n	C	$\mathrm{Aut}(C)$	$d(C)$
24	$\hat{\mathrm{Q}}(23)$	M_{24}	8
48	$\hat{\mathrm{Q}}(47)$	$\mathrm{PSL}_2(47)$	12
72	?	≤ 5	16

- minimum distance of extended QR-Codes:

n	72	80	104	128	152	168
d	12	16	20	20	20	24
d_{ext}	16	16	20	24	28	32

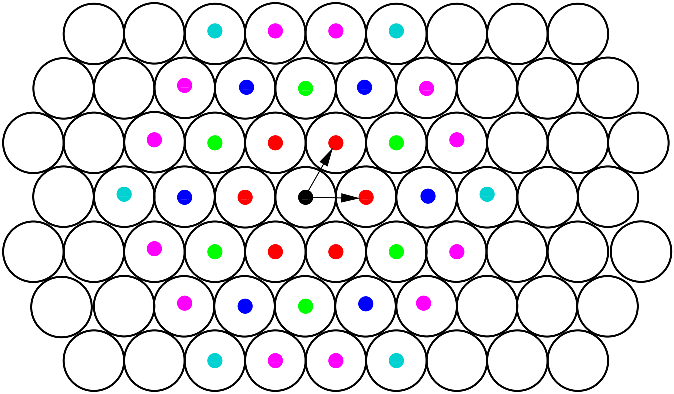
Extremal ternary codes

- $C = C^{\perp} \leq \mathbb{F}_3^n \Rightarrow 4 \mid n$ and $d(C) \leq 3 + 3\lfloor \frac{n}{12} \rfloor$
- all known extremal codes of length $n = 12m$:

n	C	$\mathrm{Aut}(C)$	$d(C)$
12	Q_{12}	$2.M_{12}$	6
24	Q_{24}	$C_2 \times \mathrm{PSL}_2(23)$	9
24	P_{24}	$(C_2 \times \mathrm{SL}_2(11)).2$	9
36	P_{36}	$(C_4 \times \mathrm{PSL}_2(17)).2$	12
48	Q_{48}	$C_2 \times \mathrm{PSL}_2(47)$	15
48	P_{48}	$(C_2 \times \mathrm{SL}_2(23)).2$	15
60	Q_{60}	$C_2 \times \mathrm{PSL}_2(59)$	18
60	P_{60}	$(C_4 \times \mathrm{PSL}_2(29)).2$	18
60	V_{60}	$\mathrm{SL}_2(29)$	18

- length 12, 24: all classified
- length 36: all other codes have $\mathrm{Aut}(C) = C_4$ or trivial
- length 48: all other codes have $|\mathrm{Aut}(C)|$ divides 48
- length 72: extremal weight enumerator has negative coefficient

Lattices and sphere packings



Hexagonal Circle Packing

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

Dense sphere packings

- Classical problem to find densest sphere packings:
- Dimension 2: Gauß (lattices), Fejes Tóth (general)
- Dimension 3: Kepler conjecture, proven by T.C. Hales
- Dimension 8 and 24: Maryna Viazovska et al. (2016):
- E_8-lattice packing and Leech lattice packing are the densest sphere packings in dimension 8 and 24
- Other dimensions: open

E_8 and Leech are even unimodular lattices

Even unimodular lattices

Definition

- A lattice L in Euclidean n-space $(\mathbb{R}^n, (,))$ is the $\mathbb{Z}$-span of an $\mathbb{R}$-basis
$$L = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in \mathbb{Z}\}.$$
- $Q : \mathbb{R}^n \to \mathbb{R}_{\geq 0}, Q(x) := \frac{1}{2}(x, x)$ associated quadratic form
- L is called even if $Q(\ell) \in \mathbb{Z}$ for all $\ell \in L$.
- $\min(L) := \min\{Q(\ell) \mid 0 \neq \ell \in L\}$ minimum of L.
- 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 $L = L^{\#}$.

Even unimodular lattices L correspond to regular positive definite integral quadratic forms $Q : L \to \mathbb{Z}$.

Even lattices and Modular forms

... Hecke, Hilbert, Siegel (1900-1970)
Quebbemann (1995)

Lattices		Holomorphic functions
L	$\mapsto$	Θ_L (Theta series)
properties of L (even, unimodular)	$\to$	symmetries of Θ_L $\Theta_L \in \mathrm{Inv}(G)$
unstructured set		finitely generated ring
properties of L $\min(L) \leq 1 + \lfloor \frac{n}{24} \rfloor$	$\Leftarrow$	$\mathrm{Inv}(G) = \mathbb{C}[p_1, \ldots, p_s]$
extremal lattices	$\to$	extremal modular forms

Extremal lattices and extremal modular forms

L extremal $\Leftrightarrow \min(L) = 1 + \lfloor \frac{n}{24} \rfloor$

$$f^{(8)} = 1 + 240q + \ldots = \theta_{E_8}.$$
$$f^{(24)} = 1 + 196,560q^2 + \ldots = \theta_{\Lambda_{24}}.$$
$$f^{(32)} = 1 + 146,880q^2 + \ldots = \theta_L.$$
$$f^{(40)} = 1 + 39,600q^2 + \ldots = \theta_L.$$
$$f^{(48)} = 1 + 52,416,000q^3 + \ldots = \theta_{P_{48pqnm}}.$$
$$f^{(72)} = 1 + 6,218,175,600q^4 + \ldots = \theta_{\Gamma_{72}}.$$
$$f^{(80)} = 1 + 1,250,172,000q^4 + \ldots = \theta_{M_{80}}.$$

Extremal even unimodular lattices L$\leq \mathbb{R}^n$

n	8	24	32	40	48	72	80	$\geq$ 163,264
min(L)	1	2	2	2	3	4	4	
number extremal lattices	1	1	$\geq 10^7$	$\geq 10^{51}$	≥ 4	≥ 1	≥ 4	0

Extremal even unimodular lattices in jump dimensions

L extremal even unimodular lattice of dimension $24m$

- All $\emptyset \neq \{\ell \in L \mid Q(\ell) = a\}$ form spherical 11-designs.
- local maximum of the density function on the space of all $24m$-dimensional lattices.

Extremal even unimodular lattices in jump dimensions

L extremal even unimodular lattice of dimension $24m$

- All $\emptyset \neq \{\ell \in L \mid Q(\ell) = a\}$ form spherical 11-designs.
- local maximum of the density function on the space of all $24m$-dimensional lattices.
- If $m = 1$, then $L = \Lambda_{24}$ is unique (Leech lattice).
- The 196.560 minimal vectors of the Leech lattice form the unique tight spherical 11-design and realise the maximal kissing number in dimension 24.
- Λ_{24} yields densest sphere packing in 24 dimensions (H.Cohn, A.Kumar, SD.Miller, D.Radchenko, M.Viazovska)

Extremal even unimodular lattices in jump dimensions

L extremal even unimodular lattice of dimension $24m$

- All $\emptyset \neq \{\ell \in L \mid Q(\ell) = a\}$ form spherical 11-designs.
- local maximum of the density function on the space of all $24m$-dimensional lattices.
- If $m = 1$, then $L = \Lambda_{24}$ is unique (Leech lattice).
- The 196.560 minimal vectors of the Leech lattice form the unique tight spherical 11-design and realise the maximal kissing number in dimension 24.
- Λ_{24} yields densest sphere packing in 24 dimensions (H.Cohn, A.Kumar, SD.Miller, D.Radchenko, M.Viazovska)
- For $m = 2, 3$ these lattices are the densest known lattices and realise the maximal known kissing number.

Notion of Equivalence

Codes	Lattices
$C \cong D \Leftrightarrow$ $\exists \sigma \in S_n, \sigma(C) = D$	$L \cong M \Leftrightarrow$ $\exists \sigma \in O_n(\mathbb{R}), \sigma(L) = M$
all transformations preserving Hamming distance	all transformations preserving inner product
$\mathrm{Aut}(C) = \mathrm{Stab}_{S_n}(C)$	$\mathrm{Aut}(L) = \mathrm{Stab}_{O_n}(L)$

Notion of Equivalence

Codes	Lattices
$C \cong D \Leftrightarrow$ $\exists \sigma \in S_n, \sigma(C) = D$ all transformations preserving Hamming distance	$L \cong M \Leftrightarrow$ $\exists \sigma \in O_n(\mathbb{R}), \sigma(L) = M$ all transformations preserving inner product
$\mathrm{Aut}(C) = \mathrm{Stab}_{S_n}(C)$	$\mathrm{Aut}(L) = \mathrm{Stab}_{O_n}(L)$

- Size of equivalence class $\sim |\,\mathrm{Aut}\,|^{-1}$
- Small equivalence class $\sim$ big stabiliser
- Interesting objects have large automorphism groups ?

Extremal even unimodular lattices in jump dimensions

The extremal theta series

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

The automorphism groups

$\mathrm{Aut}(\Lambda_{24}) \cong 2.Co_1$	order =	8315553613086720000 $2^{22}3^9 5^4 7^2 \cdot 11 \cdot 13 \cdot 23$
$\mathrm{Aut}(P_{48p}) \cong (\mathrm{SL}_2(23) \times S_3) : 2$	order	$72864 = 2^5 3^2 11 \cdot 23$
$\mathrm{Aut}(P_{48q}) \cong \mathrm{SL}_2(47)$	order	$103776 = 2^5 3 \cdot 23 \cdot 47$
$\mathrm{Aut}(P_{48n}) \cong (\mathrm{SL}_2(13) \mathsf{Y}\, \mathrm{SL}_2(5)).2^2$	order	$524160 = 2^7 3^2 5 \cdot 7 \cdot 13$
$\mathrm{Aut}(P_{48m}) \cong (C_5 \times C_{15}) : (D_8 \mathsf{Y} C_4)$	order	$1200 = 2^4 3\ 5^2$
$\mathrm{Aut}(\Gamma_{72}) \cong (\mathrm{SL}_2(25) \times \mathrm{PSL}_2(7)) : 2$	order	$5241600 = 2^8 3^2 5^2 7 \cdot 13$

The Type of an automorphism.

How many extremal lattices in dimension 48?

Use automorphisms to classify extremal even unimodular lattices of dimension 48 and 72.

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 $M := E_L(\sigma) := F^\perp$ 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 (Kirschmer, N. 2013-2017)

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 $p \leq 13$.

Type	$\mathrm{Fix}(\sigma)$	$E(\sigma)$	example	class.
47-(1,2)-1	unique	unique	P_{48q}	yes
23-(2,4)-2	unique	2	P_{48q}, P_{48p}	yes
13-(4,0)-0	$\{0\}$	at least 1	P_{48n}	
11-(4,8)-4	unique	at least 1	P_{48p}	
7-(8,0)-0	$\{0\}$	at least 1	P_{48n}	
7-(7,6)-5	$\sqrt{7}A_6^{\#}$	not known	not known	
5-(12,0)-0	$\{0\}$	at least 2	P_{48n}, P_{48m}	
5-(10,8)-8	$\sqrt{5}E_8$	at least 1	P_{48m}	
5-(8,16)-8	$[2.\mathrm{Alt}_{10}]_{16}$	Λ_{32}	P_{48m}	yes
p=3	6 possible types			
2-(24,24)-24	$\sqrt{2}\Lambda_{24}$	$\sqrt{2}\Lambda_{24}$	P_{48n}	
2-(24,24)-24	$\sqrt{2}O_{24}$	$\sqrt{2}O_{24}$	P_{48n}, P_{48p}, P_{48m}	

Large automorphisms of extremal lattices

Definition

$\sigma \in \mathrm{Aut}(L)$ is called large, if μ_σ has an irreducible factor Φ_a of degree $d = \varphi(a) > \frac{1}{2}\dim(L)$.

Remark

Let $\sigma \in \mathrm{Aut}(\Lambda_{24})$ be large. Then

a	23	33	35	39	40	52	56	60	84
d	22	20	24	24	16	24	24	16	24

Theorem (N. 2013-2014)

Let L be an extremal unimodular lattice of dimension $n = 48$ or $n = 72$, $\sigma \in \mathrm{Aut}(L)$ large.
Then $n = 48$ and

a	120	132	69	47	65	104
d	32	40	44	46	48	48
L	P_{48n}	P_{48p}	P_{48p}	P_{48q}	P_{48n}	P_{48n}

or $n = 72$, $L = \Gamma_{72}$ and either $a = 91$ ($d = 72$) or $a = 168$ ($d = 48$).

Do good objects have symmetry ?

Do good objects have symmetry ?

Do good objects have symmetry ?

- Yes, as we already assumed a certain structure.
- Yes, as we experience symmetry for small situations.

Do good objects have symmetry ?

- Yes, as we already assumed a certain structure.
- Yes, as we experience symmetry for small situations.
- No in large dimension.

Do good objects have symmetry ?

- Yes, as we already assumed a certain structure.
- Yes, as we experience symmetry for small situations.
- No in large dimension.
- Depending on definition of good:
- Measure of quality motivated by technical applications.
- These applications can make use of additional structure.
- Random even lattice $L \leq \mathbb{R}^{100}$ given by Gram matrix.
  Cannot determine its minimum, nor use it for error correction.
- Exists hardcoded decoding for the Leech lattice.
- Might be extended to Γ_{72}.