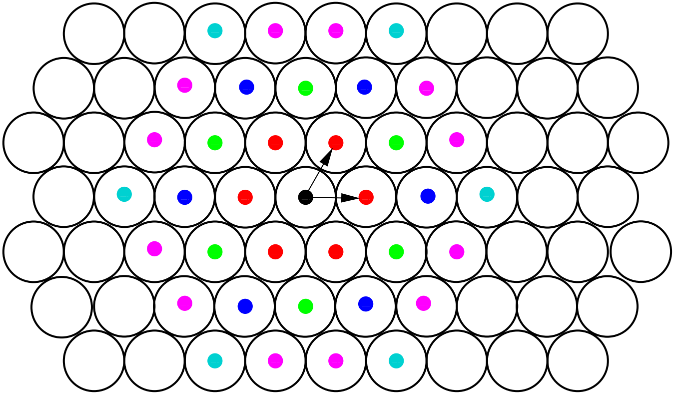
Extremal lattices and codes

Gabriele Nebe

Lehrstuhl D für Mathematik

Banff November 2011

Lattices and sphere packings



Hexagonal Circle Packing

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

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 $L = L^{\#}$.
- $Q : \mathbb{R}^n \to \mathbb{R}_{\geq 0}, Q(x) := \frac{1}{2}(x, x)$ 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 sphere packing density of an even unimodular lattice is proportional to its minimum.

Dense lattice sphere packings

- Classical problem to find densest sphere packings:
- Dimension 2: Lagrange (lattices), Fejes Tóth (general)
- Dimension 3: Kepler conjecture, proven by T.C. Hales (1998)
- Dimension ≥ 4: open
- Densest lattice sphere packings:
- Voronoi algorithm ($\sim$1900) all locally densest lattices.
- Densest lattices known in dimension 1,2,3,4,5, Korkine-Zolotareff (1872) 6,7,8 Blichfeldt (1935) and 24 Cohn, Kumar (2003).
- Density of lattice measures error correcting quality.

The densest lattices.

n	1	2	3	4	5	6	7	8	24
L	$\mathbb{A}_1$	$\mathbb{A}_2$	$\mathbb{A}_3$	$\mathbb{D}_4$	$\mathbb{D}_5$	$\mathbb{E}_6$	$\mathbb{E}_7$	$\mathbb{E}_8$	Λ_{24}

Theta-series of lattices

Let (L, Q) be an even unimodular lattice of dimension n so a regular positive definite integral quadratic form $Q : L \to \mathbb{Z}$.

- The theta series of L is

$$\theta_L = \sum_{\ell \in L} q^{Q(\ell)} = 1 + \sum_{k=\min(L)}^{\infty} a_k q^k$$

  where $a_k = |\{\ell \in L \mid Q(\ell) = k\}|$.
- θ_L defines a holomorphic function on the upper half plane by substituting $q := \exp(2\pi i z)$.
- Then θ_L is a modular form of weight $\frac{n}{2}$ for the full modular group $\mathrm{SL}_2(\mathbb{Z})$.
- n is a multiple of 8.
- $\theta_L \in \mathcal{M}_{\frac{n}{2}}(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}[E_4, \Delta]_{\frac{n}{2}}$ where $E_4 := \theta_{E_8} = 1 + 240q + \dots$ is the normalized Eisenstein series of weight 4 and

$$\Delta = q - 24q^2 + 252q^3 - 1472q^4 + \dots \text{ of weight 12}$$

Extremal modular forms

Basis of $\mathcal{M}_{4k}(\mathrm{SL}_2(\mathbb{Z}))$:

$$\begin{array}{lccccc}
E_4^k = & 1+ & 240kq+ & *q^2+ & \dots & \\
E_4^{k-3}\Delta = & & q+ & *q^2+ & \dots & \\
E_4^{k-6}\Delta^2 = & & & q^2+ & \dots & \\
\vdots & & & & & \\
E_4^{k-3m_k}\Delta^{m_k} = & & \dots & & q^{m_k}+ & \dots
\end{array}$$

where $m_k = \lfloor \frac{n}{24} \rfloor = \lfloor \frac{k}{3} \rfloor$.

Definition

This space contains a unique form

$$f^{(k)} := 1 + 0q + 0q^2 + \ldots + 0q^{m_k} + a(f^{(k)})q^{m_k+1} + b(f^{(k)})q^{m_k+2} + \ldots$$

$f^{(k)}$ is called the extremal modular form of weight $4k$.

$f^{(1)} = 1 + 240q + \ldots = \theta_{E_8}$, $f^{(2)} = 1 + 480q + \ldots = \theta_{E_8}^2$,
$f^{(3)} = 1 + 196,560q^2 + \ldots = \theta_{\Lambda_{24}}$,
$f^{(6)} = 1 + 52,416,000q^3 + \ldots = \theta_{P_{48p}} = \theta_{P_{48q}} = \theta_{P_{48n}}$,
$f^{(9)} = 1 + 6,218,175,600q^4 + \ldots = \theta_{\Gamma}$.

Extremal even unimodular lattices

Theorem (Siegel)

$a(f^{(k)}) > 0$ for all k

Corollary

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

$$\min(L) \leq 1 + \lfloor \frac{n}{24} \rfloor = 1 + m_{n/8}.$$

Lattices achieving this bound are called extremal.

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

n	8	16	24	32	40	48	72	80	$\geq 163,264$
min(L)	1	1	2	2	2	3	4	4	
number of extremal lattices	1	2	1	$\geq 10^7$	$\geq 10^{51}$	≥ 3	≥ 1	≥ 4	0

Extremal even unimodular lattices

Theorem (Siegel)

$a(f^{(k)}) > 0$ for all k

Corollary

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

$$\min(L) \leq 1 + \lfloor \frac{n}{24} \rfloor = 1 + m_{n/8}.$$

Lattices achieving this bound are called extremal.

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

n	8	16	24	32	40	48	72	80	$\geq 163,264$
min(L)	1	1	2	2	2	3	4	4	
number of extremal lattices	1	2	1	$\geq 10^7$	$\geq 10^{51}$	≥ 3	≥ 1	≥ 4	0

Extremal even unimodular lattices

Theorem (Siegel)

$a(f^{(k)}) > 0$ for all k and $b(f^{(k)}) < 0$ for large k ($k \geq 20408$).

Corollary

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

$$\min(L) \leq 1 + \lfloor \frac{n}{24} \rfloor = 1 + m_{n/8}.$$

Lattices achieving this bound are called extremal.

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

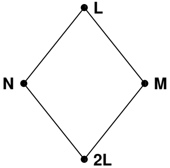
n	8	16	24	32	40	48	72	80	$\geq 163,264$
min(L)	1	1	2	2	2	3	4	4	
number of extremal lattices	1	2	1	$\geq 10^7$	$\geq 10^{51}$	≥ 3	≥ 1	≥ 4	0

Extremal even unimodular lattices in jump dimensions

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

Let L be an extremal even unimodular lattice of dimension $24m$ so $\min(L) = m + 1$

- All non-empty layers $\emptyset \neq \{\ell \in L \mid Q(\ell) = a\}$ form spherical 11-designs.
- The density of the associated sphere packing realises a local maximum of the density function on the space of all $24m$-dimensional lattices.
- If $m = 1$, then $L = \Lambda_{24}$ is unique, Λ_{24} is the Leech lattice.
- The 196560 minimal vectors of the Leech lattice form the unique tight spherical 11-design and realise the maximal kissing number in dimension 24.
- Λ_{24} is the densest 24-dimensional lattice (Cohn, Kumar).
- For $m = 2, 3$ these lattices are the densest known lattices and realise the maximal known kissing number.



Turyn's construction

- Let (L, Q) be an even unimodular lattice of dimension n.
- Choose sublattices $M, N \leq L$ such that $M + N = L$, $M \cap N = 2L$, and $(M, \frac{1}{2}Q)$, $(N, \frac{1}{2}Q)$ even unimodular.
- Such a pair (M, N) is called a polarisation of L.
- For $k \in \mathbb{N}$ let $\mathcal{L}(M, N) :=$

  $$\{(m+a, m+b, m+c) \in \perp^3 L \mid m \in M, a, b, c \in N, a+b+c \in 2L\}.$$

- Define $\tilde{Q} : \mathcal{L}(M, N) \to \mathbb{Z}$,

  $$\tilde{Q}(y_1, y_2, y_3) := \frac{1}{2}(Q(y_1) + Q(y_2) + Q(y_3)).$$

- $(\mathcal{L}(M, N), \tilde{Q})$ is an even unimodular lattice of dimension $3n$.

Turyn's construction for lattices

$$(m+a,m+b,m+c) \text{ in } \begin{cases} L \perp L \perp L \\ L(M,N) \\ 2L \perp 2L \perp 2L \end{cases}$$

m in M

a,b,c in N

a+b+c in 2L

$d := \min(L,Q) = \min(M, \frac{1}{2}Q) = \min(N, \frac{1}{2}Q)$

Then $\lceil \frac{3d}{2} \rceil \leq \min(\mathcal{L}(M,N)) \leq 2d$.

Proof:

$(a,0,0)$ $a = 2\ell \in 2L$ with $\frac{1}{2}Q(2\ell) = 2Q(\ell) \geq 2d$.

$(a,b,0)$ $a,b \in N$ with $\frac{1}{2}Q(a) + \frac{1}{2}Q(b) \geq 2d$.

(a,b,c) then $\frac{1}{2}(Q(a)+Q(b)+Q(c)) \geq \frac{3}{2}d$.

Theorem (Lepowsky, Meurman; Elkies, Gross)

Let $(L,Q) \cong E_8$ be the unique even unimodular lattice of dimension 8. Then for any polarisation (M,N) of E_8 the lattice $\mathcal{L}(M,N)$ has minimum ≥ 2.

Turyn's construction for lattices

$$(m+a,m+b,m+c) \text{ in } \begin{cases} L \perp L \perp L \\ L(M,N) \\ 2L \perp 2L \perp 2L \end{cases}$$

m in M

a,b,c in N

a+b+c in 2L

$d := \min(L,Q) = \min(M, \frac{1}{2}Q) = \min(N, \frac{1}{2}Q)$

Then $\lceil \frac{3d}{2} \rceil \leq \min(\mathcal{L}(M,N)) \leq 2d.$

Theorem (Lepowsky, Meurman; Elkies, Gross)

Let $(L,Q) \cong E_8$ be the unique even unimodular lattice of dimension 8. Then for any polarisation (M,N) of E_8 the lattice $\mathcal{L}(M,N)$ has minimum ≥ 2.

72-dimensional lattices from Leech (Griess)

If $(L,Q) \cong (M, \frac{1}{2}Q) \cong (N, \frac{1}{2}Q) \cong \Lambda_{24}$ then $3 \leq \min(\mathcal{L}(M,N)) \leq 4$.

The vectors v with $Q(v) = 3$

Assume that $(L, Q) \cong (M, \frac{1}{2}Q) \cong (N, \frac{1}{2}Q) \cong \Lambda_{24}$

- All 4095 non-zero classes of $M/2L$ are represented by vectors m with $Q(m) = 4$.
- For $m \in M$ let $N_m := \{a \in N \mid (a, m) \in 2\mathbb{Z}\}$ and $N^{(m)} := \langle N_m, m \rangle$.
- $(N^{(m)}, \frac{1}{2}Q)$ is even unimodular lattice with root system $24A_1$.
- $y := (y_1, y_2, y_3) = (m + a, m + b, m + c) \in \mathcal{L}(M, N)$ with $\tilde{Q}(y) = 3$ then $y_i \in N^{(m)}$ are roots and $m + y_1 + y_2 + y_3 \in 2L$.

Enumerate short vectors in $\mathcal{L}(M, N)$

For all 4095 nonzero classes $m + 2L \in M/2L$ and all 24^2 pairs (y_1, y_2) of roots in $N^{(m)}$ check if $\langle 2L, m + y_1 + y_2 \rangle$ has minimum ≥ 3.
Closer analysis reduces number of pairs (y_1, y_2) to $8 \cdot 16$.
$4095 \cdot 8 \cdot 16 = 524,160$
May restrict to representatives of the S-orbits on $M/2L \cong L/N$, where $S := \mathrm{Stab}_{\mathrm{Aut}(L)}(M, N)$.
E.g. 6 orbits for the extremal lattice so need to compute the minimum of $6 \cdot 8 \cdot 16 = 768$ lattices of dimension 24.

Stehlé, Watkins proof of extremality

Theorem (Stehlé, Watkins (2010))

Let L be an even unimodular lattice of dimension 72 with $\min(L) \geq 3$. Then L is extremal, if and only if it contains at least $6,218,175,600$ vectors v with $Q(v) = 4$.

Proof: L is an even unimodular lattice of minimum ≥ 3, so its theta series is

$$\theta_L = 1 + a_3 q^3 + a_4 q^4 + \ldots = f^{(9)} + a_3 \Delta^3.$$

$$\begin{array}{ccccccc} f^{(9)} & = & 1 & + & 6,218,175,600 q^4 & + \ldots \\ \Delta^3 & = & & q^3 & -72 q^4 & + \ldots \end{array}$$

So $a_4 = 6,218,175,600 - 72 a_3 \geq 6,218,175,600$ if and only if $a_3 = 0$.

Remark

A similar proof works in all jump dimensions $24k$ (extremal minimum = $k+1$) for lattices of minimum $\geq k$.
For dimensions $24k+8$ and lattices of minimum $\geq k$ one needs to count vectors v with $Q(v) = k+2$.

The history of Turyn's construction.

1967 Turyn: Constructed the Golay code $\mathcal{G}_{24}$ from the Hamming code h_8

78,82,84 Tits; Lepowsky, Meurman; Quebbemann: Construction of the Leech lattice Λ_{24} from E_8

1996 Gross, Elkies: Λ_{24} from Hermitian structure of E_8

1996 N.: Tried similar construction of extremal 72-dimensional lattices (Bordeaux).

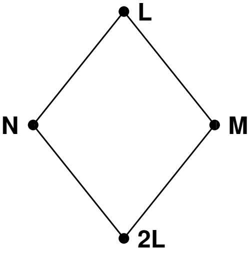
1998 Bachoc, N.: 2 extremal 80-dimensional lattices using Quebbemann's generalization and the Hermitian structure of E_8

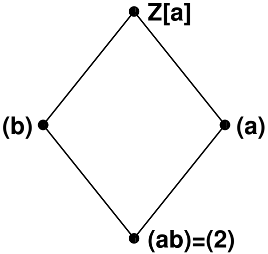
2010 Griess: Reminds Lepowsky, Meurman construction of Leech. proposes to construct 72-dimensional lattices from Λ_{24}

2010 N.: Used one of the nine $\mathbb{Z}[\alpha = \frac{1+\sqrt{-7}}{2}]$ structures of Λ_{24} to find extremal 72-dimensional lattice $\Gamma_{72} = \mathcal{L}(\alpha\Lambda_{24}, \overline{\alpha}\Lambda_{24})$

2011 Parker, N.: Check all other polarisations of Λ_{24} to show that Γ_{72} is the unique extremal lattice of the form $\mathcal{L}(M, N)$
Chance: $1 : 10^{16}$ to find extremely good polarisation.

How to find polarisations





Hermitian polarisations

- $\alpha, \beta \in \mathrm{End}(L)$ such that $(\alpha x, y) = (x, \beta y)$ and $\alpha\beta = 2$.
- $M := \alpha L$, $N := \beta L$.
- $\alpha^2 - \alpha + 2 = 0$ ($\mathbb{Z}[\alpha] =$ integers in $\mathbb{Q}[\sqrt{-7}]$).
- $(\alpha x, y) = (x, \beta y)$ where $\beta = 1 - \alpha = \overline{\alpha}$.
- Then $M := \alpha L$, $N := \beta L$ defines a polarisation of L such that $(L, Q) \cong (M, \frac{1}{2}Q) \cong (N, \frac{1}{2}Q)$.

Hermitian structures of the Leech lattice

Theorem (M. Hentschel, 2009)

There are exactly nine $\mathbb{Z}[\alpha]$-structures of the Leech lattice.

	group S	order	# S orbits on $M/2L$
1	$\mathrm{SL}_2(25)$	$2^4 3 \cdot 5^2 13$	6
2	$2.A_6 \times D_8$	$2^7 3^2 5$	12
3	$\mathrm{SL}_2(13).2$	$2^4 3 \cdot 7 \cdot 13$	9
4	$(\mathrm{SL}_2(5) \times A_5).2$	$2^6 3^2 5^2$	8
5	$(\mathrm{SL}_2(5) \times A_5).2$	$2^6 3^2 5^2$	8
6	soluble	$2^9 3^3$	11
7	$\pm\mathrm{PSL}_2(7) \times (C_7 : C_3)$	$2^4 3^2 7^2$	9
8	$\mathrm{PSL}_2(7) \times 2.A_7$	$2^7 3^3 5 \cdot 7^2$	3
9	$2.J_2.2$	$2^9 3^3 5^2 7$	2

Hermitian polarisations yield tensor products

Remark

$\mathcal{L}(\alpha L, \beta L) = L \otimes_{\mathbb{Z}[\alpha]} P_b$ where

$$P_b = \langle (\beta, \beta, 0), (0, \beta, \beta), (\alpha, \alpha, \alpha) \rangle \leq \mathbb{Z}[\alpha]^3$$

with the half the standard Hermitian form

$$h : P_b \times P_b \to \mathbb{Z}[\alpha], h((a_1, a_2, a_3), (b_1, b_2, b_3)) = \frac{1}{2} \sum_{i=1}^{3} a_i \overline{b_i}.$$

P_b is Hermitian unimodular and $\mathrm{Aut}_{\mathbb{Z}[\alpha]}(P_b) \cong \pm \mathrm{PSL}_2(7)$. So $\mathrm{Aut}(\mathcal{L}(\alpha L, \beta L)) \geq \mathrm{Aut}_{\mathbb{Z}[\alpha]}(L) \times \mathrm{PSL}_2(7)$.

In particular $\mathrm{Aut}(\Gamma) \geq \mathrm{SL}_2(25) \times \mathrm{PSL}_2(7)$.

Hermitian structures of the Leech lattice

	group	$\#\{v \in \mathcal{L}(\alpha L, \beta L) \mid Q(v) = 3\}$
1	$\mathrm{SL}_2(25)$	0
2	$2.A_6 \times D_8$	$2 \cdot 20,160$
3	$\mathrm{SL}_2(13).2$	$2 \cdot 52,416$
4	$(\mathrm{SL}_2(5) \times A_5).2$	$2 \cdot 100,800$
5	$(\mathrm{SL}_2(5) \times A_5).2$	$2 \cdot 100,800$
6	$2^9 3^3$	$2 \cdot 177,408$
7	$\pm \mathrm{PSL}_2(7) \times (C_7 : C_3)$	$2 \cdot 306,432$
8	$\mathrm{PSL}_2(7) \times 2.A_7$	$2 \cdot 504,000$
9	$2.J_2.2$	$2 \cdot 1,209,600$

The extremal 72-dimensional lattice Γ

Main result

- Γ is an extremal even unimodular lattice of dimension 72.
- $\mathrm{Aut}(\Gamma)$ contains $\mathcal{U} := (\mathrm{PSL}_2(7) \times \mathrm{SL}_2(25)) : 2$.
- $\mathcal{U}$ is an absolutely irreducible subgroup of $\mathrm{GL}_{72}(\mathbb{Q})$.
- All $\mathcal{U}$-invariant lattices are similar to Γ.
- $\mathrm{Aut}(\Gamma)$ is a maximal finite subgroup of $\mathrm{GL}_{72}(\mathbb{Q})$.
- Γ is an ideal lattice in the 91st cyclotomic number field.
- Γ realises the densest known sphere packing
- and maximal known kissing number in dimension 72.
- Structure of Γ can be used for decoding (Annika Meyer)
- Γ is a $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$-lattice. This gives $(n^2 + 5n + 5)$-modular lattices of minimum $8 + 4n$ ($n \in \mathbb{N}_0$).

Γ as $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ lattice

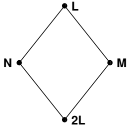
Observation

The Hermitian Leech lattice L with $\mathrm{Aut}(L) \cong SL_2(25)$ and hence also Γ has a structure over $R := \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, so $(\Gamma, Q) = (\Gamma, \mathrm{Tr}(q))$ with $q : \Gamma \to R[\frac{1}{5}]$ quadratic form.
For any totally positive $a \in R$ we obtain $N(a)$-modular lattice $(\Gamma, \mathrm{Tr}(aq))$. Let $\wp := \frac{5+\sqrt{5}}{2}$. Then $(\Gamma, \wp q)$ is unimodular R-lattice and its theta series is a Hilbert modular form of weight 36 for the full modular group.

$$\theta(\Gamma, \wp q) \in \mathbb{C}[A, B, C]$$

Theorem

Let (Λ, q) be a 36-dimensional R-lattice, such that $(\Lambda, \mathrm{Tr}(q))$ is an even unimodular lattice of minimum 4 and $\wp := (5 + \sqrt{5})/2$. For $n \in \mathbb{Z}_{\geq 0}$ put $L_n := (\Lambda, \mathrm{Tr}(\wp + n)q)$. Then L_n is an even $(n^2 + 5n + 5)$-modular lattice of minimum $8 + 4n$.



How to obtain all polarisations

A rough estimate shows that there are about 10^{10} orbits of $\mathrm{Aut}(\Lambda_{24})$ on the set of polarisations (M, N) such that $(M, \frac{1}{2}Q) \cong (N, \frac{1}{2}Q) \cong \Lambda_{24}$.

Theorem (Richard Parker, N.)

There is a unique orbit of $\mathrm{Aut}(\Lambda_{24}) \cong 2.Co_1$ for which $\mathcal{L}(M, N)$ is extremal.

Computation: Compute representatives for the 16 $\mathrm{Aut}(\Lambda_{24})$-orbits on $\{N \mid (N, \frac{1}{2}Q) \cong \Lambda_{24}\}$, and find all good complements M such that $\mathcal{L}(M, N)$ is extremal.
N defines a set of bad vectors $B(N) \subset \Lambda_{24}/2\Lambda_{24}$, so that $\mathcal{L}(M, N)$ extremal iff $M \cap B(N) = \emptyset$.
The total computation took about 2 CPU years.

Bad vectors

$\mathcal{L}(M,N) = \{(a+m, b+m, c+m) \mid a,b,c \in N, m \in M, a+c+b \in 2L\}$
Start with one of the 16 orbit representatives N. Then any nonzero class $0 \neq f+N \in \Lambda_{24}/N$ contains exactly 24 pairs $\{\pm v_1, \ldots, \pm v_{24}\}$ of minimal vectors in Λ_{24}. The set

$$B(N,f) := \{(v_i + v_j + v_k) + 2\Lambda_{24} \mid 1 \leq i,j,k \leq 24\} \subset \Lambda_{24}/2\Lambda_{24}$$

is called the set of bad vectors for N and f. Their union

$$B(N) := \bigcup_{0 \neq f+N \in \Lambda_{24}/N} B(N,f)$$

is called the set of bad vectors for N.

Remark

The lattice $\mathcal{L}(M,N)$ is extremal if and only if $M/2L \cap B(N) = \emptyset$.

Orbits on the rescaled Leech sublattices

	stabilizer	order	orbit length
1	$PSL_2(25):2$	$2^4 3 \cdot 5^2 13$	$2.7 \cdot 10^{14}$
2	$A_7 \times PSL_2(7)$	$2^6 3^3 5 \cdot 7^2$	$9.8 \cdot 10^{12}$
3	$S_3 \times PSL_2(13)$	$2^3 3^2 7 \cdot 13$	$6.3 \cdot 10^{14}$
4	$3.A_6 \times A_5$	$2^6 3^4 5^2$	$3.2 \cdot 10^{13}$
5	$PSL_2(7) \times PSL_2(7)$	$2^6 3^2 7^2$	$1.5 \cdot 10^{14}$
6	$A_5 \times$ soluble	$2^{15} 3^3 5$	$9.4 \cdot 10^{11}$
7	$G_2(4) \times A_4$	$2^{15} 3^4 5^2 7 \cdot 13$	$6.9 \cdot 10^8$
8	$PSL_2(23)$	$2^3 3 \cdot 11 \cdot 23$	$6.9 \cdot 10^{14}$
9	soluble	$2^{11} 3$	$6.8 \cdot 10^{14}$
10	soluble	$2^{12} 3^2$	$1.1 \cdot 10^{14}$
11	soluble	$2^8 3 \cdot 7$	$7.7 \cdot 10^{14}$
12	soluble	$2^{11} 3^2$	$2.3 \cdot 10^{14}$
13	$3.A_7.2$	$2^4 3^3 5 \cdot 7$	$2.7 \cdot 10^{14}$
14	soluble	$2^9 3 \cdot 5$	$5.4 \cdot 10^{14}$
15	soluble	$2^8 3 \cdot 7$	$7.7 \cdot 10^{14}$
16	soluble	$2^{14} 3^3$	$9.3 \cdot 10^{12}$

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 $\mathrm{wt}(c) := |\{i \mid c_i \neq 0\}|$.
- C is called doubly-even if $\mathrm{wt}(c) \in 4\mathbb{Z}$ for all $c \in C$.
- The minimum distance $d(C) := \min\{\mathrm{wt}(c) \mid 0 \neq c \in C\}$.
- The weight enumerator of C is $p_C := \sum_{c \in C} x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)} \in \mathbb{C}[x, y]_n$.

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

Self-dual codes

Remark

- The all-one vector $\mathbf{1}$ lies in the dual of every even code since $\mathrm{wt}(c) \equiv_2 (c,c) \equiv_2 (c,\mathbf{1})$.
- 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 $\mathbf{1}^{\perp}/\langle \mathbf{1} \rangle$.
- Annika Meyer, N. $C = C^{\perp}$ doubly-even $\Rightarrow$ $\mathrm{Aut}(C) := \mathrm{Stab}_{S_n}(C) \leq A_n$.

$$h_8 : \left[\begin{array}{cccccccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right]$$ 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 $\mathrm{Aut}(h_8) = 2^3 : \mathrm{GL}_3(2)$.

Extremal codes

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

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

Theorem (Gleason)

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

- $n \in 8\mathbb{Z}$
- $p_C \in \mathbb{C}[p_{h_8}, p_{\mathcal{G}_{24}}] = \mathrm{Inv}(G_{192})$
- $d(C) \leq 4 + 4\lfloor \frac{n}{24} \rfloor$

Doubly-even self-dual codes achieving this bound are called extremal.

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

Extremal polynomials

$$\mathbb{C}[p_{h_8}, p_{\mathcal{G}_{24}}] = \mathbb{C}[\underbrace{x^8 + 14x^4y^4 + y^8}_{f}, \underbrace{x^4y^4(x^4 - y^4)^4}_{g}] = \mathrm{Inv}(G_{192})$$

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

$$\begin{array}{llllll}
f^k = & 1+ & 14ky^4+ & *y^8+ & \dots & \\
f^{k-3}g = & & y^4+ & *y^8+ & \dots & \\
f^{k-6}g^2 = & & & y^8+ & \dots & \\
\vdots & & & & & \\
f^{k-3m_k}g^{m_k} = & & \dots & & y^{4m_k}+ & \dots
\end{array}$$

where $m_k = \lfloor \frac{n}{24} \rfloor = \lfloor \frac{k}{3} \rfloor$.

Definition

This space contains a unique polynomial

$$p^{(k)} := 1 + 0y^4 + 0y^8 + \dots + 0y^{4m_k} + a_k y^{4m_k+4} + b_k y^{4m_k+8} + \dots$$

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

$p^{(1)} = p_{h_8},\ p^{(2)} = p_{h_8}^2,\ p^{(3)} = p_{\mathcal{G}_{24}},\ p^{(6)} = p_{QR48}$

$p^{(9)} = 1 + 249849y^{16} + 18106704y^{20} + 462962955y^{24} + \dots$

Turyn's construction of the Golay code

Construction of Golay code

Choose two copies C and D of h_8 such that

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

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

(a) $\mathcal{G}_{24} = \mathcal{G}_{24}^{\perp}$.

(b) $\mathcal{G}_{24}$ is doubly-even.

(c) $d(\mathcal{G}_{24}) = 8$.

Proof: (a) unique expression if c represents classes in $h_8/\langle \mathbf{1} \rangle$, so

$$|\mathcal{G}_{24}| = 2^3 \cdot 2^4 \cdot 2^4 \cdot 2 = 2^{12}$$

Suffices $\mathcal{G}_{24} \subseteq \mathcal{G}_{24}^{\perp}$: $((c + d_1, c + d_2, c + d_3), (c' + d_1', c' + d_2', c' + d_3')) =$

$$3(c, c') + (c, d_1' + d_2' + d_3') + (d_1 + d_2 + d_3, c') + (d_1, d_1') + (d_2, d_2') + (d_3, d_3') = 0$$

(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

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

$\mathcal{G}_{24} := \{(c + d_1, c + d_2, c + d_3) \mid c \in C, d_i \in D, d_1 + d_2 + d_3 \in \langle \mathbf{1} \rangle\}$
(c) $d(\mathcal{G}_{24}) = 8$.

Proof: (c)
$\mathrm{wt}(c + d_1, c + d_2, c + d_3) = \mathrm{wt}(c + d_1) + \mathrm{wt}(c + d_2) + \mathrm{wt}(c + d_3)$.

- 1 non-zero component: $(d, 0, 0)$ with $d \in \langle \mathbf{1} \rangle$, 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 ≥ 8.

Turyn applied to Golay will not yield an extremal code of length 72. Such an extremal code has no automorphism of order 2 which has fixed points.

Automorphisms of extremal codes

Theorem (Bouyuklieva; O'Brien, Willems; N. Feulner)

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.
- $p \leq 7$.
- If $p = 2$ or $p = 3$ then σ has no fixed points.
- If $p = 5$ or $p = 7$ then σ has 2 fixed points.
- G has no element of odd order > 7.
- G is solvable.
- No subgroup $C_3 \times C_3$, C_7, D_{10}, C_{10}.
- No subgroup $C_4 \times C_2$, C_8, Q_8.
- Summarize: $|G| = 5$ or $|G|$ divides 24.

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