Extremal Configurations in Dimension 48

Akihiro Munemasa

Tohoku University

Japan

EACAC2, November 21, 2003

Kyushu University

Motivation

The binary perfect Golay code is a set of 2^{12} elements of the vector space $\mathbb{F}_2^{23}$, giving a partition of $\mathbb{F}_2^{23}$ into 2^{12} spheres of volume

$$1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11},$$

radius 3 with respect to the Hamming metric.

Motivation

The binary perfect Golay code is a set of 2^{12} elements of the vector space $\mathbb{F}_2^{23}$, giving a partition of $\mathbb{F}_2^{23}$ into 2^{12} spheres of volume

$$1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11},$$

radius 3 with respect to the Hamming metric.
The Golay code G_{23} can be made linear, and unique up to isometry.

Motivation

The binary perfect Golay code is a set of 2^{12} elements of the vector space $\mathbb{F}_2^{23}$, giving a partition of $\mathbb{F}_2^{23}$ into 2^{12} spheres of volume

$$1 + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2^{11},$$

radius 3 with respect to the Hamming metric.
The Golay code G_{23} can be made linear, and unique up to isometry.
Construction: by quadratic residues modulo 23.

Sphere Packing Bound

The Hamming distance is defined by

$$d(x,y) = \left|\{i \mid x_i \neq y_i\}\right|, \quad x, y \in \mathbb{F}_2^n.$$

Sphere Packing Bound

The Hamming distance is defined by

$$d(x,y) = |\{i \mid x_i \neq y_i\}|, \quad x,y \in \mathbb{F}_2^n.$$

$$|C| \leq \frac{2^n}{1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r}}$$

if C is a set of centers of non-overlapping spheres of radius r.

Sphere Packing Bound

The Hamming distance is defined by

$$d(x, y) = |\{i \mid x_i \neq y_i\}|, \quad x, y \in \mathbb{F}_2^n.$$

$$|C| \leq \frac{2^n}{1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r}}$$

if C is a set of centers of non-overlapping spheres of radius r.

Uniqueness: The binary perfect Golay code is the only way to partition $\mathbb{F}_2^{23}$ into spheres of radius 3

Sphere Packing Bound

The Hamming distance is defined by

$$d(x,y) = |\{i \mid x_i \neq y_i\}|, \quad x,y \in \mathbb{F}_2^n.$$

$$|C| \leq \frac{2^n}{1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r}}$$

if C is a set of centers of non-overlapping spheres of radius r.

Uniqueness: The binary perfect Golay code is the only way to partition $\mathbb{F}_2^{23}$ into spheres of radius 3

Sphere Packing Bound

The Hamming distance is defined by

$$d(x,y) = |\{i \mid x_i \neq y_i\}|, \quad x, y \in \mathbb{F}_2^n.$$

$$|C| \leq \frac{2^n}{1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r}}$$

if C is a set of centers of non-overlapping spheres of radius r.

Uniqueness: The binary perfect Golay code is the only way to partition $\mathbb{F}_2^n$ into spheres of radius $r \geq 2$.

Related Objects

The binary perfect Golay code G_{23}

Related Objects

The binary perfect Golay code G_{23}

$\longrightarrow$The extended binary Golay code

Related Objects

The binary perfect Golay code G_{23}

$\longrightarrow$The extended binary Golay code

$\longrightarrow$The Witt system W_{24}

Related Objects

The binary perfect Golay code G_{23}
$\longrightarrow$The extended binary Golay code

$\longrightarrow$The Witt system W_{24}
$\longrightarrow$The Leech lattice $\Lambda \subset \mathbb{R}^{24}$

Related Objects

The binary perfect Golay code G_{23}

$\longrightarrow$The extended binary Golay code

$\longrightarrow$The Witt system W_{24}

$\longrightarrow$The Leech lattice $\Lambda \subset \mathbb{R}^{24}$

$\longrightarrow$The Layer Λ_4

Related Objects

The binary perfect Golay code G_{23}
$\longrightarrow$The extended binary Golay code

$\longrightarrow$The Witt system W_{24}
$\longrightarrow$The Leech lattice $\Lambda \subset \mathbb{R}^{24}$

$\longrightarrow$The Layer Λ_4
$\longrightarrow$The Layer on a hyperplane $\Lambda_4 \cap \mathbb{R}^{23}$

Related Objects

The binary perfect Golay code G_{23}

$\rightarrow$The extended binary Golay code

$\rightarrow$The Mathieu group M_{24}

$\rightarrow$The Witt system W_{24}

$\rightarrow$The Leech lattice $\Lambda \subset \mathbb{R}^{24}$

$\rightarrow$The Layer Λ_4

$\rightarrow$The Layer on a hyperplane $\Lambda_4 \cap \mathbb{R}^{23}$

Related Objects

The binary perfect Golay code G_{23}

$\longrightarrow$The extended binary Golay code

$\longrightarrow$The Mathieu group M_{24}

$\longrightarrow$The Witt system W_{24}

$\longrightarrow$The Leech lattice $\Lambda \subset \mathbb{R}^{24}$

$\longrightarrow$Conway's simple groups

$\longrightarrow$The Layer Λ_4

$\longrightarrow$The Layer on a hyperplane $\Lambda_4 \cap \mathbb{R}^{23}$

Related Objects

The binary perfect Golay code G_{23}
$\longrightarrow$The extended binary Golay code
$\longrightarrow$The Mathieu group M_{24}
$\longrightarrow$The Witt system W_{24}
$\longrightarrow$The Leech lattice $\Lambda \subset \mathbb{R}^{24}$
$\longrightarrow$Conway's simple groups
$\longrightarrow$The Layer Λ_4
$\longrightarrow$The Layer on a hyperplane $\Lambda_4 \cap \mathbb{R}^{23}$

Surprisingly, Mathieu groups were discovered first.

Extremality of configurations in dimension 24

- G_{23}: sphere packing bound $\leq 2^{12}$

Extremality of configurations in dimension 24

- G_{23}: sphere packing bound $\leq 2^{12}$
- G_{24}: minimum distance bound ≤ 8

Extremality of configurations in dimension 24

- G_{23}: sphere packing bound $\leq 2^{12}$
- G_{24}: minimum distance bound ≤ 8
- Λ: minimum norm bound ≤ 4

Extremality of configurations in dimension 24

- G_{23}: sphere packing bound $\leq 2^{12}$
- G_{24}: minimum distance bound ≤ 8
- Λ: minimum norm bound ≤ 4
- $\Lambda_4 \cap \mathbb{R}^{23}$: size bound for antipodal 3-distance set ≤ 552

Extremality of configurations in dimension 24

- G_{23}: sphere packing bound $\leq 2^{12}$
- G_{24}: minimum distance bound ≤ 8
- Λ: minimum norm bound ≤ 4
- $\Lambda_4 \cap \mathbb{R}^{23}$: size bound for antipodal 3-distance set ≤ 552
- W_{24}: 5-design

Extremality of configurations in dimension 24

- G_{23}: sphere packing bound $\leq 2^{12}$
- G_{24}: minimum distance bound ≤ 8
- Λ: minimum norm bound ≤ 4
- $\Lambda_4 \cap \mathbb{R}^{23}$: size bound for antipodal 3-distance set ≤ 552
- W_{24}: 5-design
- Λ_4: spherical 11-design, bound ≥ 196560

Extremality of configurations in dimension 24

- G_{23}: sphere packing bound $\leq 2^{12}$
- G_{24}: minimum distance bound ≤ 8
- Λ: minimum norm bound ≤ 4
- $\Lambda_4 \cap \mathbb{R}^{23}$: size bound for antipodal 3-distance set ≤ 552
- W_{24}: 5-design
- Λ_4: spherical 11-design, bound ≥ 196560
- $\Lambda_4 \cap \mathbb{R}^{23}$: spherical 5-design, bound ≥ 552

General inequalities

Doubly-even self-dual code of length n

General inequalities

Doubly-even self-dual code of length n : $C \subset \mathbb{F}_2^n$,
$C = C^\perp, \forall x \in C, \mathrm{wt}(x) \equiv 0 \pmod 4$.

General inequalities

Doubly-even self-dual code of length $n : C \subset \mathbb{F}_2^n$,
$C = C^\perp, \forall x \in C, \mathrm{wt}(x) \equiv 0 \pmod 4$.

$$\mathrm{wt}(x) = d(x, 0)$$

General inequalities

Doubly-even self-dual code of length n : $C \subset \mathbb{F}_2^n$, $C = C^\perp, \forall x \in C, \mathrm{wt}(x) \equiv 0 \pmod 4$.

$$\mathrm{wt}(x) = d(x, 0)$$

$$\min \mathrm{wt}(C) = \min\{\mathrm{wt}(x) \mid x \in C,\ x \neq 0\}.$$

General inequalities

Doubly-even self-dual code of length n : $C \subset \mathbb{F}_2^n$, $C = C^\perp, \forall x \in C, \mathrm{wt}(x) \equiv 0 \pmod 4$.

$$\mathrm{wt}(x) = d(x, 0)$$

$$\min \mathrm{wt}(C) = \min\{\mathrm{wt}(x) \mid x \in C,\ x \neq 0\}.$$

length	8	16	24	32	40	48	...	n
min wt $\leq$	4	4	8	8	8	12	...	$4[n/24] + 4$

General inequalities

Doubly-even self-dual code of length n : $C \subset \mathbb{F}_2^n$, $C = C^\perp, \forall x \in C, \mathrm{wt}(x) \equiv 0 \pmod 4$.

$$\mathrm{wt}(x) = d(x, 0)$$

$$\min \mathrm{wt}(C) = \min\{\mathrm{wt}(x) \mid x \in C,\ x \neq 0\}.$$

length	8	16	24	32	40	48	...	n
min wt $\leq$	4	4	8	8	8	12	...	$4[n/24] + 4$

General inequalities

Even unimodular lattice of rank n: $\Lambda \subset \mathbb{R}^n$,

General inequalities

Even unimodular lattice of rank n: $\Lambda \subset \mathbb{R}^n$,
$\Lambda = \Lambda^* = \{x \in \mathbb{R}^n \mid \langle x, y \rangle \in \mathbb{Z}\ (\forall y in \Lambda)\}$ (or equivalently, $\operatorname{disc} \Lambda = 1$)
$\forall x \in \Lambda$, $\langle x, x \rangle \equiv 0 \pmod 2$.

General inequalities

Even unimodular lattice of rank n: $\Lambda \subset \mathbb{R}^n$, $\Lambda = \Lambda^* = \{x \in \mathbb{R}^n \mid \langle x, y\rangle \in \mathbb{Z}\ (\forall y in \Lambda)\}$ (or equivalently, $\operatorname{disc} \Lambda = 1$)
$\forall x \in \Lambda$, $\langle x, x\rangle \equiv 0 \pmod 2$.

$$\min(\Lambda) = \min\{\langle x, x\rangle \mid x \in \Lambda,\ x \neq 0\}.$$

General inequalities

Even unimodular lattice of rank n: $\Lambda \subset \mathbb{R}^n$, $\Lambda = \Lambda^* = \{x \in \mathbb{R}^n \mid \langle x, y \rangle \in \mathbb{Z} \ (\forall y in \Lambda)\}$ (or equivalently, $\operatorname{disc} \Lambda = 1$)
$\forall x \in \Lambda$, $\langle x, x \rangle \equiv 0 \pmod 2$.

$$\min(\Lambda) = \min\{\langle x, x \rangle \mid x \in \Lambda,\ x \neq 0\}.$$

rank	8	16	24	32	40	48	$\ldots$	n
min $\leq$	2	2	4	4	4	6	$\ldots$	$2[n/24]+2$

General inequalities

Even unimodular lattice of rank n: $\Lambda \subset \mathbb{R}^n$,
$\Lambda = \Lambda^* = \{x \in \mathbb{R}^n \mid \langle x, y\rangle \in \mathbb{Z}\ (\forall y in \Lambda)\}$ (or equivalently, $\operatorname{disc}\Lambda = 1$)
$\forall x \in \Lambda$, $\langle x, x\rangle \equiv 0 \pmod 2$.

$$\min(\Lambda) = \min\{\langle x, x\rangle \mid x \in \Lambda,\ x \neq 0\}.$$

rank	8	16	24	32	40	48	...	n
min $\leq$	2	2	4	4	4	6	...	$2[n/24]+2$

The Broué-Enguehard map

A doubly-even self-dual code of length n has minimum weight $\leq 4[n/24] + 4$.

The Broué-Enguehard map

A doubly-even self-dual code of length n has minimum weight $\leq 4[n/24] + 4$.
An even unimodular lattice of rank n has minimum norm $\leq 2[n/24] + 2$.

The Broué-Enguehard map

A doubly-even self-dual code of length n has minimum weight $\leq 4[n/24]+4$.
An even unimodular lattice of rank n has minimum norm $\leq 2[n/24]+2$.
This coincidence comes from Broué-Enguehard isomorphism of an invariant ring R and the ring of modular forms.

The Broué-Enguehard map

A doubly-even self-dual code of length n has minimum weight $\leq 4[n/24] + 4$.
An even unimodular lattice of rank n has minimum norm $\leq 2[n/24] + 2$.
This coincidence comes from Broué-Enguehard isomorphism of an invariant ring R and the ring of modular forms.
As a graded ring, R has Poincaré series

$$\sum_{j=0}^{\infty} \dim R_j t^j = \frac{1}{(1-t^8)(1-t^{12})}$$

The Poincaré series

The Poincaré series of the graded ring of the invariant ring containing the weight enumerator polynomials of doubly-even self-dual codes is

$$\sum_{n=0}^{\infty} \dim R_n t^n = \frac{1}{(1-t^8)(1-t^{12})}$$

$$= 1 + t^8 + t^{12} + t^{16} + t^{20}$$

$$+ 2t^{24} + t^{28} + 2t^{32} + 2t^{36} + 2t^{40} + 2t^{44}$$

$$+ 3t^{48} + 2t^{52} + 3t^{56} + \cdots$$

The Poincaré series

The Poincaré series of the graded ring of the invariant ring containing the weight enumerator polynomials of doubly-even self-dual codes is

$$\sum_{n=0}^{\infty} \dim R_n t^n = \frac{1}{(1-t^8)(1-t^{12})}$$
$$= 1 + t^8 + t^{12} + t^{16} + t^{20}$$
$$+ 2t^{24} + t^{28} + 2t^{32} + 2t^{36} + 2t^{40} + 2t^{44}$$
$$+ 3t^{48} + 2t^{52} + 3t^{56} + \cdots$$

Roughly speaking, $\dim R_n$ is the degree of freedom for minimum weight bound.

General inequality for 3-distance set

$\mathbb{R}^n \supset S^{n-1} \supset X$: finite antipodal 3-distance set. Then

$$|X| \leq n(n+1).$$

General inequality for 3-distance set

$\mathbb{R}^n \supset S^{n-1} \supset X$: finite antipodal 3-distance set. Then

$$|X| \leq n(n+1).$$

Equality holds if $n = 2$ (hexagon), $n = 3$ (icosahedron),

General inequality for 3-distance set

$\mathbb{R}^n \supset S^{n-1} \supset X$: finite antipodal 3-distance set. Then

$$|X| \leq n(n+1).$$

Equality holds if $n = 2$ (hexagon), $n = 3$ (icosahedron),

$$n = \ 23 \text{ (Leech}\cap\mathbb{R}^{23}\text{)}, \ 47 \text{ (?)}, 79\text{(?)},$$

$$\ldots, (2m+1)^2 - 2, \ldots$$

Dimension 48

A doubly-even self-dual code could have minimum weight $4[n/24] + 4$

Dimension 48

A doubly-even self-dual code could have minimum weight $4[n/24]+4 = 12.$

Dimension 48

A doubly-even self-dual code could have minimum weight $4[n/24] + 4 = 12.$
An even unimodular lattice could have minimum norm $2[n/24] + 2$

Dimension 48

A doubly-even self-dual code could have minimum weight $4[n/24] + 4 = 12.$
An even unimodular lattice could have minimum norm $2[n/24] + 2 = 6.$

Dimension 48

A doubly-even self-dual code could have minimum weight $4[n/24] + 4 = 12.$

An even unimodular lattice could have minimum norm $2[n/24] + 2 = 6.$

An antipodal 3-distance set in the unit sphere in $\mathbb{R}^{47}$ could have $n(n+1) = 47 * 48.$

Dimension 48 (Results)

A doubly-even self-dual code with minimum weight 12 is known (the extended quadratic residue code).

Dimension 48 (Results)

A doubly-even self-dual code with minimum weight 12 is known (the extended quadratic residue code).

Three even unimodular lattice with minimum norm 6 are known: $P_{48q}, P_{48p}, P_{48n}$.

Dimension 48 (Results)

A doubly-even self-dual code with minimum weight 12 is known (the extended quadratic residue code).

Three even unimodular lattice with minimum norm 6 are known: $P_{48q}, P_{48p}, P_{48n}$.

An antipodal 3-distance set in the unit sphere in $\mathbb{R}^{47}$ could have $47 * 48$,

Dimension 48 (Results)

A doubly-even self-dual code with minimum weight 12 is known (the extended quadratic residue code). Shown to be unique (by computer).
Houghten–Lam–Thiel–Parker (2003)
Three even unimodular lattice with minimum norm 6 are known: $P_{48q}, P_{48p}, P_{48n}$.

An antipodal 3-distance set in the unit sphere in $\mathbb{R}^{47}$ could have $47 * 48$,

Dimension 48 (Results)

A doubly-even self-dual code with minimum weight 12 is known (the extended quadratic residue code). Shown to be unique (by computer).
Houghten–Lam–Thiel–Parker (2003)

Three even unimodular lattice with minimum norm 6 are known: $P_{48q}, P_{48p}, P_{48n}$. Not known whether these three are the only ones.

An antipodal 3-distance set in the unit sphere in $\mathbb{R}^{47}$ could have $47 * 48$,

Dimension 48 (Results)

A doubly-even self-dual code with minimum weight 12 is known (the extended quadratic residue code). Shown to be unique (by computer).

Houghten–Lam–Thiel–Parker (2003)

Three even unimodular lattice with minimum norm 6 are known: $P_{48q}, P_{48p}, P_{48n}$. Not known whether these three are the only ones.

An antipodal 3-distance set in the unit sphere in $\mathbb{R}^{47}$ could have $47 * 48$, but it was shown recently (Bannai–M.–Venkov) that such a set does not exist.

Construction A

Let $\varphi : \mathbb{Z}^n \to (\mathbb{Z}/m\mathbb{Z})^n$ be the canonical homomorphism. If $C \subset (\mathbb{Z}/m\mathbb{Z})^n$ is a self-dual code, then the lattice

$$A_m(C) := \frac{1}{\sqrt{m}}\varphi^{-1}(C) \subset \mathbb{R}^n$$

is a unimodular lattice.

Construction A

Let $\varphi : \mathbb{Z}^n \to (\mathbb{Z}/m\mathbb{Z})^n$ be the canonical homomorphism. If $C \subset (\mathbb{Z}/m\mathbb{Z})^n$ is a self-dual code, then the lattice

$$A_m(C) := \frac{1}{\sqrt{m}} \varphi^{-1}(C) \subset \mathbb{R}^n$$

is a unimodular lattice.
The lattice $A_m(C)$ has an m-frame, i.e., $\exists f_1, \ldots, f_n \in A_m(C)$ s.t. $\langle f_i, f_j \rangle = \delta_{ij} m$.

Construction A

Let $\varphi : \mathbb{Z}^n \to (\mathbb{Z}/m\mathbb{Z})^n$ be the canonical homomorphism. If $C \subset (\mathbb{Z}/m\mathbb{Z})^n$ is a self-dual code, then the lattice

$$A_m(C) := \frac{1}{\sqrt{m}}\varphi^{-1}(C) \subset \mathbb{R}^n$$

is a unimodular lattice.

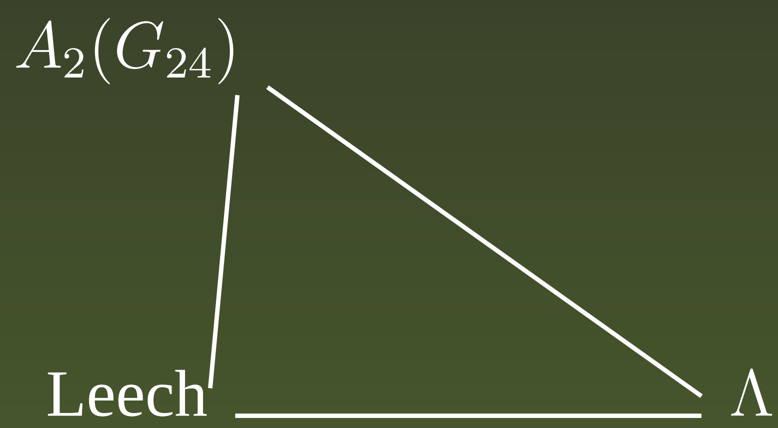
The lattice $A_m(C)$ has an m-frame, i.e., $\exists f_1, \ldots, f_n \in A_m(C)$ s.t. $\langle f_i, f_j \rangle = \delta_{ij} m$.

The lattice $A_2(G_{24})$ has a 2-frame (hence is not the Leech lattice).

Neighbor relations

Two unimodular lattices Γ, Γ' are said to be neighbors if $\Gamma \cap \Gamma'$ has index 2 in Γ (and also in Γ').

Dimension 24:



Neighbor relations

Dimension 48: (Harada–Kitazume–M.–Venkov)

$$\begin{tikzcd}
& A_4(\mathrm{QR}) \arrow[dl, dash] \arrow[dr, dash] & \\
P_{48q} \arrow[rr, dash] & & A_3(\mathrm{QR})
\end{tikzcd}$$

$$= A_6(C_q)$$

Neighbor relations

Dimension 48: (Harada–Kitazume–M.–Venkov)

$$\begin{tikzcd}
& A_4(\mathrm{QR}) \arrow[dl, dash] \arrow[dr, dash] & \\
P_{48q} \arrow[rr, dash] & & A_3(\mathrm{QR})
\end{tikzcd}$$

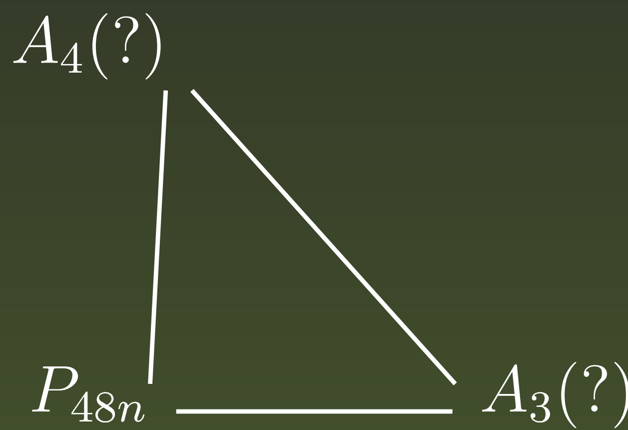
$$= A_6(C_q)$$

$$\begin{tikzcd}
& A_4(C)(\mathrm{new}) \arrow[dl, dash] \arrow[dr, dash] & \\
P_{48p} \arrow[rr, dash] & & A_3(\mathrm{Pless})
\end{tikzcd}$$

$$= A_6(C_p)$$

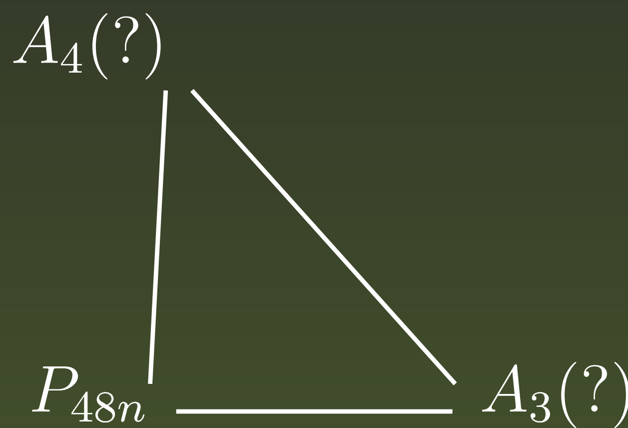
Neighbor relations

Dimension 48:



Neighbor relations

Dimension 48:



Does Nebe's lattice P_{48n} have a 6-frame?

Designs

So far we studied codes, lattices and 3-distance sets as extremal configurations.

Designs

So far we studied codes, lattices and 3-distance sets as extremal configurations. Closely related concept of a configuration is the concept of designs, defined by optimization requirement.

Designs

So far we studied codes, lattices and 3-distance sets as extremal configurations. Closely related concept of a configuration is the concept of designs, defined by optimization requirement.

Assmus–Mattson Theorem: d.e.s.d code $\longrightarrow$ (combinatorial) design.

Designs

So far we studied codes, lattices and 3-distance sets as extremal configurations. Closely related concept of a configuration is the concept of designs, defined by optimization requirement.

Assmus–Mattson Theorem: d.e.s.d code $\longrightarrow$ (combinatorial) design. Witt system W_{24} arises in this way by taking the set of supports of vectors of minimum weight in G_{24}.

Designs

So far we studied codes, lattices and 3-distance sets as extremal configurations. Closely related concept of a configuration is the concept of designs, defined by optimization requirement.

Assmus–Mattson Theorem: d.e.s.d code $\longrightarrow$ (combinatorial) design. Witt system W_{24} arises in this way by taking the set of supports of vectors of minimum weight in G_{24}.

Venkov's Theorem: lattice $\rightarrow$ spherical design.

Designs

So far we studied codes, lattices and 3-distance sets as extremal configurations. Closely related concept of a configuration is the concept of designs, defined by optimization requirement.

Assmus–Mattson Theorem: d.e.s.d code $\longrightarrow$ (combinatorial) design. Witt system W_{24} arises in this way by taking the set of supports of vectors of minimum weight in G_{24}.

Venkov's Theorem: lattice $\longrightarrow$ spherical design. The layer Λ_4 in the Leech lattice is a spherical 11-design.

Designs

So far we studied codes, lattices and 3-distance sets as extremal configurations. Closely related concept of a configuration is the concept of designs, defined by optimization requirement.

Assmus–Mattson Theorem: d.e.s.d code $\longrightarrow$ (combinatorial) design. Witt system W_{24} arises in this way by taking the set of supports of vectors of minimum weight in G_{24}.

Venkov's Theorem: lattice $\longrightarrow$ spherical design. The layer Λ_4 in the Leech lattice is a spherical 11-design.

Delsarte–Goethals–Seidel Theorem: extremal s-distance set in S^{n-1} $\longrightarrow$ spherical design

Definition of a design

A spherical t-design X is a finite subset of $S^{n-1} \subset \mathbb{R}^n$ s.t.

$$\frac{1}{\int_{S^{n-1}} 1} \int_{S^{n-1}} f(x) = \frac{1}{|X|} \sum_{x \in X} f(x)$$

holds for any polynomial $f(x)$ of degree $\leq t$.

Definition of a design

A spherical t-design X is a finite subset of $S^{n-1} \subset \mathbb{R}^n$ s.t.

$$\frac{1}{\int_{S^{n-1}} 1} \int_{S^{n-1}} f(x) = \frac{1}{|X|} \sum_{x \in X} f(x)$$

holds for any polynomial $f(x)$ of degree $\leq t$.

A (combinatorial) t-design $\mathcal{B}$ is a subset of $\binom{\Omega}{k}$ s.t.

$$\frac{1}{\binom{v}{k}} \sum_{B \in \binom{\Omega}{k}} f(B) = \frac{1}{|\mathcal{B}|} \sum_{B \in \mathcal{B}} f(B)$$

holds for any polynomial f of degree $\leq t$.

Combinatorial designs

A (combinatorial) t-design $\mathcal{B}$, or t-(v,k,λ) design is a subset of $\binom{\Omega}{k}$ such that

$$\frac{1}{\binom{v}{k}} \sum_{B \in \binom{\Omega}{k}} f(B) = \frac{1}{|\mathcal{B}|} \sum_{B \in \mathcal{B}} f(B)$$

holds for any polynomial f of degree $\leq t$, where Ω is a set of v elements, $\binom{\Omega}{k}$ is the set of all k-element subsets of Ω.

Combinatorial designs

A (combinatorial) t-design $\mathcal{B}$, or t-(v, k, λ) design is a subset of $\binom{\Omega}{k}$ such that

$$\frac{1}{\binom{v}{k}} \sum_{B \in \binom{\Omega}{k}} f(B) = \frac{1}{|\mathcal{B}|} \sum_{B \in \mathcal{B}} f(B)$$

holds for any polynomial f of degree $\leq t$, where Ω is a set of v elements, $\binom{\Omega}{k}$ is the set of all k-element subsets of Ω.

Polynomial functions are polynomial in the functions x_i $(i \in \Omega)$, with $x_i(B) = 1$ or 0 according as $i \in B$ or not.

Combinatorial designs

$$\frac{1}{\binom{v}{k}} \sum_{B \in \binom{\Omega}{k}} f(B) = \frac{1}{|\mathcal{B}|} \sum_{B \in \mathcal{B}} f(B)$$

Polynomial functions are polynomial in the functions x_i $(i \in \Omega)$, with $x_i(B) = 1$ or 0 according as $i \in B$ or not.

Combinatorial designs

$$\frac{1}{\binom{v}{k}} \sum_{B \in \binom{\Omega}{k}} f(B) = \frac{1}{|\mathcal{B}|} \sum_{B \in \mathcal{B}} f(B)$$

Polynomial functions are polynomial in the functions x_i $(i \in \Omega)$, with $x_i(B) = 1$ or 0 according as $i \in B$ or not. Taking $f = x_{i_1} x_{i_2} \cdots x_{i_t}$ with $i_1, \ldots, i_t$ distinct, we see that the number of $B \in \mathcal{B}$ containing $\{i_1, \ldots, i_t\}$ is independent of the choice of $i_1, \ldots, i_t$. This number is denoted by λ.

Designs in dimension 48

From an extremal doubly-even self-dual code of length 48, one obtains 5-$(48, 12, 8)$ design. Is such a design unique?

Designs in dimension 48

From an extremal doubly-even self-dual code of length 48, one obtains 5-$(48, 12, 8)$ design. Is such a design unique?

If $\mathcal{B}$ is a t-(v, k, λ) design, then

$$\mathcal{B} \ni B \leftrightarrow \text{vector of weight } k \text{ in } \mathbb{F}_2^v$$

and these vector generate a linear code $C \subset \mathbb{F}_2^v$.

Designs in dimension 48

From an extremal doubly-even self-dual code of length 48, one obtains 5-$(48, 12, 8)$ design. Is such a design unique?

If $\mathcal{B}$ is a t-(v, k, λ) design, then

$$\mathcal{B} \ni B \leftrightarrow \text{vector of weight } k \text{ in } \mathbb{F}_2^v$$

and these vector generate a linear code $C \subset \mathbb{F}_2^v$.

Assuming $\mathcal{B}$ is self-orthogonal, i.e.,

$$B, B' \in \mathcal{B} \implies |B \cap B'| : \text{even},$$

we aim to show that C is a (unique) extremal doubly-even self-dual code of length 48.

Characterization Method

Suppose $u \in C^{\perp}$, $A = \operatorname{supp}(u) = \{i_1, \ldots, i_m\}$. In the defining equation of a design, take f to be elementary symmetric functions of degree at most t in $\{x_{i_1}, \ldots, x_{i_m}\}$.

Characterization Method

Suppose $u \in C^{\perp}$, $A = \mathrm{supp}(u) = \{i_1, \ldots, i_m\}$. In the defining equation of a design, take f to be elementary symmetric functions of degree at most t in $\{x_{i_1}, \ldots, x_{i_m}\}$.

Then $f(B) = \binom{|A \cap B|}{s}$, and

$$\frac{1}{\binom{v}{k}} \sum_{B \in \binom{\Omega}{k}} f(B) = \frac{1}{|\mathcal{B}|} \sum_{B \in \mathcal{B}} f(B) = \frac{1}{|\mathcal{B}|} \sum_{j=0}^{\infty} \binom{j}{s} n_j$$

where $n_j = |\{B \mid B \in \mathcal{B},\ |A \cap B| = j\}|$.

Designs in dimension 48

For a self-orthogonal 5-$(48, 12, 8)$ design, if $|A| = 8$, then $n_j = 0$ unless $j \in \{0, 2, 4, 6, 8\}$. There are 5 unknowns, 6 $(s = 0, 1, 2, 3, 4, 5)$ equations, no solutions. Therefore $C^\perp$ does not contain a vector of weight 8.

Designs in dimension 48

For a self-orthogonal 5-$(48, 12, 8)$ design, if $|A| = 8$, then $n_j = 0$ unless $j \in \{0, 2, 4, 6, 8\}$. There are 5 unknowns, 6 $(s = 0, 1, 2, 3, 4, 5)$ equations, no solutions. Therefore $C^{\perp}$ does not contain a vector of weight 8.

Similar argument implies

$$\min \mathrm{wt}\, C \geq \min \mathrm{wt}\, C^{\perp} > 8$$

Designs in dimension 48

For a self-orthogonal 5-$(48, 12, 8)$ design, if $|A| = 8$, then $n_j = 0$ unless $j \in \{0, 2, 4, 6, 8\}$. There are 5 unknowns, 6 $(s = 0, 1, 2, 3, 4, 5)$ equations, no solutions. Therefore $C^\perp$ does not contain a vector of weight 8.
Similar argument implies

$$\min \mathrm{wt}\, C \geq \min \mathrm{wt}\, C^\perp > 8$$

Theorem 1 (Harada–M.–Tonchev) *A self-orthogonal* 5-$(48, 12, 8)$ *design is unique.*

Nonexistence of an extremal 3-distance set

If X is a 3-distance set of size $47 \cdot 48$ in S^{47}, then X is a spherical 5-design.

Nonexistence of an extremal 3-distance set

If X is a 3-distance set of size $47 \cdot 48$ in S^{47}, then X is a spherical 5-design.

$\sqrt{7}X$ generates an integral lattice Γ. Let $\alpha \in \Gamma^* = \{\delta \in \mathbb{R}^n \mid \langle \gamma, \delta \rangle \in \mathbb{Z}\ (\forall \gamma \in \Gamma)\}$. With $f(x) = \langle x, \alpha \rangle^s$, $0 \le s \le t = 5$,

$$\frac{1}{\int_{S^{n-1}} 1} \int_{S^{n-1}} f(x) = \frac{1}{|X|} \sum_{x \in X} f(x)$$

gives linear equations with unknowns $n_j = |\{x \in \sqrt{7}X \mid \langle x, \alpha \rangle = \pm j\}|$.

Nonexistence of an extremal 3-distance set

If X is a 3-distance set of size $47 \cdot 48$ in S^{47}, then X is a spherical 5-design.

$\sqrt{7}X$ generates an integral lattice Γ. Let $\alpha \in \Gamma^* = \{\delta \in \mathbb{R}^n \mid \langle \gamma, \delta \rangle \in \mathbb{Z}\ (\forall \gamma \in \Gamma)\}$. With $f(x) = \langle x, \alpha \rangle^s$, $0 \le s \le t = 5$,

$$\frac{1}{\int_{S^{n-1}} 1} \int_{S^{n-1}} f(x) = \frac{1}{|X|} \sum_{x \in X} f(x)$$

gives linear equations with unknowns $n_j = |\{x \in \sqrt{7}X \mid \langle x, \alpha \rangle = \pm j\}|$.

Theorem 2 (Bannai–M.–Venkov) *There is no antipodal 3-distance set of size $47 \cdot 48$ in S^{47}.*