Extremal Lattices and Spherical Designs

Akihiro Munemasa

Graduate School of Information Sciences
Tohoku University
Japan

(joint work with Boris Venkov)

July 21, 2004
Pusan National University

Venkov's Theorem (1984)

Let $\Lambda \subset \mathbb{R}^{24n}$ be an extremal even unimodular lattice.

$$X = \{x \in \Lambda \mid (x, x) = 2n + 2\}.$$

Then X is a spherical 11-design (after rescaling).

Example: in $\mathbb{R}^{24}$, the Leech lattice has 196,560 shortest vectors, which form a tight 11-design after scaling.

Theorem 1 (Bannai–Sloane, 1981). *Every tight spherical 11-design in $\mathbb{R}^{24}$ is equivalent to the example above.*

Definition of a Spherical Design

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

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

holds for any polynomial $f(x)$ of degree $\leq t$.
If X is a spherical $(2s+1)$-design in $\mathbb{R}^n$ with $X = -X$, then

$$|X| \geq 2 \binom{n-1+s}{s}.$$

X is said to be tight if equality holds.

Strategy

X: tight spherical 11-design in the unit sphere in $\mathbb{R}^{24}$
$\Longrightarrow$

$$|X| = 2\binom{24-1+5}{5} = 196,560.$$

$\Longrightarrow$ $(x, y) \in \{\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, 0\}$.
How can one use the fact that X is a spherical design?

$$\frac{1}{|X|}\sum_{x\in X} f(x) = \frac{\int_{S^{23}} f d\mu}{\int_{S^{23}} 1 d\mu}$$

holds for any polynomial $f(x)$ of degree at most 11.
Take $f(x) = (\alpha, x)^2$, with $\alpha \in \mathbb{R}^{24}$, $\alpha \neq 0$.

$$\frac{1}{|X|}\sum_{x\in X}(\alpha, x)^2 = \frac{(\alpha, \alpha)}{24}.$$

Lattice

- A lattice is a $\mathbb{Z}$-submodule of $\mathbb{R}^n$ of rank n containing a basis of $\mathbb{R}^n$.
- A lattice Λ is called integral if $\forall x, y \in \Lambda$, $(x, y) \in \mathbb{Z}$.
- The dual lattice Λ^* of an integral lattice Λ is

$$\Lambda^* = \{x \in \mathbb{R}^n \mid (x, y) \in \mathbb{Z} \; \forall y \in \Lambda\} \supset \Lambda.$$

  and $|\Lambda^* : \Lambda| < \infty$.
- An integral lattice Λ is called even if $(x, x) \in 2\mathbb{Z} \; \forall x \in \Lambda$.
- An integral lattice Λ is called unimodular if $\Lambda = \Lambda^*$.

Strategy

X: spherical 11-design, $X = -X$,
$(x, y) \in \{\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, 0\}$.
The lattice $\Lambda = 2\mathbb{Z}X$ is even, since it is integral and is generated by vectors of even norm.

Theorem 2 (Conway). *The Leech lattice is the unique even unimodular lattice of dimension 24 with minimum norm* 4.

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

We wish to prove $\Lambda = 2\mathbb{Z}X$ is unimodular and Λ has minimum norm 4.

Strategy

X: spherical 11-design, $X=-X$,
$2X \ni \forall x, y$, $(x,x)=4$, $(x,y)\in\mathbb{Z}$.

$$\frac{1}{|X|}\sum_{x\in X} f(x) = \frac{\int_{S^{23}} f\,d\mu}{\int_{S^{23}} 1 d\mu}$$

holds for any polynomial $f(x)$ of degree at most 11.
Take $f(x)=(\alpha,x)^{2j}$, with $\alpha\in\mathbb{R}^{24}$, $j=1,2,3,4,5$.

$$\sum_{x\in X}(\alpha,x)^{2j} = |X|\frac{(2j-1)!!(\alpha,\alpha)^j}{24\cdot 26\cdots(24+2j-2)}$$

holds for $j=1,2,3,4,5$.

Strategy

$$\sum_{x \in 2X} (\alpha, x)^{2j} = |X| \frac{4^j (2j-1)!!(\alpha,\alpha)^j}{24 \cdot 26 \cdots (24+2j-2)}$$

holds for $j = 1, 2, 3, 4, 5.$
Take $\alpha \in \Lambda^* = (2\mathbb{Z}X)^*$. Then $(\alpha, x) \in \mathbb{Z}$ for all $x \in 2X$,

$$\sum_{k=1}^{\infty} n_k k^{2j} = |X| \frac{(2j-1)!! 4^j (\alpha,\alpha)^j}{24 \cdot 26 \cdots (24+2j-2)}$$

holds for $j = 1, 2, 3, 4, 5$, where

$$n_k = |\{x \in 2X \mid (\alpha, x) = \pm k\}| \quad (k = 1, 2, \ldots).$$

System of Linear Equations

X: spherical 11-design, $X = -X$,
$2X \ni \forall x, y$, $(x, x) = 4$, $(x, y) \in \mathbb{Z}$.

$$\begin{pmatrix} 1 & 2^2 & 3^2 & \cdots \\ 1 & 2^4 & 3^4 & \cdots \\ 1 & 2^6 & 3^6 & \cdots \\ 1 & 2^8 & 3^8 & \cdots \\ 1 & 2^{10} & 3^{10} & \cdots \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \\ n_3 \\ \vdots \end{pmatrix} = \begin{pmatrix} c_1(m) \\ c_2(m) \\ c_3(m) \\ c_4(m) \\ c_5(m) \end{pmatrix}$$

where

$$c_j(m) = |X| \frac{(2j-1)!! 4^j m^j}{24 \cdot 26 \cdots (24 + 2j - 2)},$$

$$m = (\alpha, \alpha),$$

$$n_k = |\{x \in 2X \mid (\alpha, x) = \pm k\}|$$

Trick

X: spherical 11-design, $X = -X$,
$2X \ni \forall x, y$, $(x, x) = 4$, $(x, y) \in \mathbb{Z}$. $\Lambda = 2\mathbb{Z}X$.
Take $\alpha \in \Lambda^*$ in such a way that

$$m = (\alpha, \alpha) = \min\{(\beta, \beta) \mid 0 \neq \beta \in \alpha + \Lambda\}.$$

Then $|(\alpha, x)| \leq 2 \quad \forall x \in 2X$, unless $\alpha \in 2X$.
Indeed, since $(x, x) = 4$,
$(\alpha, x) \geq 3$ $(\exists x \in 2X \subset \Lambda) \implies \alpha - x \in \alpha + \Lambda$ and

$$(\alpha - x, \alpha - x) = (\alpha, \alpha) - 2(\alpha, x) + (x, x)$$

$$\leq (\alpha, \alpha) - 2 \cdot 3 + 4$$

$$< (\alpha, \alpha).$$

Trick

X: spherical 11-design, $X = -X$,
$2X \ni \forall x, y$, $(x,x) = 4$, $(x,y) \in \mathbb{Z}$. $\Lambda = 2\mathbb{Z}X$.
Take $\alpha \in \Lambda^*$ in such a way that

$$m = (\alpha, \alpha) = \min\{(\beta, \beta) \mid 0 \neq \beta \in \alpha + \Lambda\}.$$

Then $|(\alpha, x)| \leq 2 \quad \forall x \in 2X$, unless $\alpha \in 2X$.

$$\begin{pmatrix} 1 & 2^2 \\ 1 & 2^4 \\ 1 & 2^6 \\ 1 & 2^8 \\ 1 & 2^{10} \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{pmatrix} c_1(m) \\ c_2(m) \\ c_3(m) \\ c_4(m) \\ c_5(m) \end{pmatrix}$$

Conclusion

$$\begin{pmatrix} 1 & 2^2 \\ 1 & 2^4 \\ 1 & 2^6 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = |X| m \begin{pmatrix} \frac{1}{6} \\ \frac{m}{13} \\ \frac{5m^2}{91} \end{pmatrix}$$

$m^2 - 7m + \frac{182}{15} = 0 \implies m \notin \mathbb{Q}$.
But $m = (\alpha, \alpha)$, $\alpha \in \Lambda^*$, $k = |\Lambda^* : \Lambda| < \infty$
$\implies k\alpha \in \Lambda \implies (k\alpha, k\alpha) \in \mathbb{Z} \implies m = (\alpha, \alpha) \in \mathbb{Q}$.
Conclusion:

$$\alpha \in \Lambda^* : \text{minimal in } \alpha + \Lambda, \alpha \notin 2X \implies \text{contradiction}$$

This implies $\Lambda^* = \Lambda$
$X =$ shortest vectors of Λ

$\implies \Lambda =$ Leech lattice.

Observation

$$\begin{pmatrix} 1 & 2^2 \\ 1 & 2^4 \\ 1 & 2^6 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = |X| m \begin{pmatrix} \frac{1}{6} \\ \frac{m}{13} \\ \frac{5m^2}{91} \end{pmatrix}$$

- $|X|$ is not important.
- Suffices to assume X is a spherical 6-design (equivalently, 7-design, since $X = -X$).

Theorem 3. *Let X be a spherical 7-design in $\mathbb{R}^{24}$ with $X = -X$, $4(x, y) \in \mathbb{Z}\ \forall x, y \in X$. Then $2X$ coincides with the $196,560$ shortest vectors of the Leech lattice.*

Corollary 1 (Bannai–Sloane, 1981). *A tight spherical 11-design in $\mathbb{R}^{24}$ is unique.*

Extremal Lattices

An even unimodular lattice $\Lambda \subset \mathbb{R}^{24n}$ is called extremal if $\min \Lambda = 2n + 2$.

Examples:

- $24n = 24$, $\min \Lambda = 4$: the Leech lattice.
- $24n = 48$, $\min \Lambda = 6$: three lattices known.
- $24n = 72$, $\min \Lambda = 8$: no lattices known.
- $24n \geq 96$, $\min \Lambda = 2n + 2$: no lattices known.

Venkov's theorem implies that we always have a spherical 11-design.

Dimension 48

Theorem 4. $\mathbb{R}^{48} \supset X$: *spherical* 9*-design,* $X \ni \forall x, y$, $6(x,y) \in \mathbb{Z}$, $\implies \Lambda = \sqrt{6}\mathbb{Z}X =$ *an extremal lattice,* $\sqrt{6}X =$ *the set of shortest vectors of* Λ.

Proof. $\alpha \in \Lambda^*$: minimal in $\alpha + \Lambda$, $m = (\alpha, \alpha)$.

$$\begin{pmatrix} 1 & 2^2 & 3^2 \\ 1 & 2^4 & 3^4 \\ 1 & 2^6 & 3^6 \\ 1 & 2^8 & 3^8 \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \\ n_3 \end{pmatrix} = |X| m \begin{pmatrix} c_1 \\ c_2(m) \\ c_3(m) \\ c_4(m) \end{pmatrix}$$

$\implies$ an irreducible cubic equation in m. $\square$

Remark 1. Such a design is necessarily a spherical 11-design by Venkov's theorem. There are three extremal lattices of dimension 48 known.

Dimension 72

Theorem 5. $\mathbb{R}^{72} \supset X$: *spherical* 11-*design*, $X \ni \forall x, y$, $8(x,y) \in \mathbb{Z}$, $\implies$ $\Lambda = \sqrt{8}\mathbb{Z}X$ = *an extremal lattice*, $\sqrt{8}X$ = *the set of shortest vectors of* Λ.

Proof. $\alpha \in \Lambda^*$: minimal in $\alpha + \Lambda$, $m = (\alpha, \alpha)$.

$$\begin{pmatrix} 1 & 2^2 & 3^2 & 4^2 \\ 1 & 2^4 & 3^4 & 4^4 \\ 1 & 2^6 & 3^6 & 4^6 \\ 1 & 2^8 & 3^8 & 4^8 \\ 1 & 2^{10} & 3^{10} & 4^{10} \end{pmatrix} \begin{pmatrix} n_1 \\ n_2 \\ n_3 \\ n_4 \end{pmatrix} = |X|m \begin{pmatrix} c_1 \\ c_2(m) \\ c_3(m) \\ c_4(m) \\ c_5(m) \end{pmatrix}$$

$\implies$ an irreducible quartic equation in m. $\square$

Problem 1. *Does there exist an extremal even unimodular lattice of dimension 72?*

Binary Code Analogues

spherical $(2t+1)$-design	t-design
integral lattice	binary self-orthogonal code
unimodular lattice	binary self-dual code
Venkov's theorem	Assmus–Mattson theorem
Leech lattice	extended binary Golay code
tight 11-design in $\mathbb{R}^{24}$	$S(5,8,24)$
extremal lattice in $\mathbb{R}^{48}$	extended binary quadratic residue code of length 48
spherical 11-design in $\mathbb{R}^{48}$	self-orthogonal 5-$(48,12,8)$ design
spherical 11-design in $\mathbb{R}^{72}$	self-orthogonal 5-$(72,16,78)$ design

Binary Code Analogues

Let X be (the set of blocks of) a 5-design which is likely to be derived from a putative extremal doubly even self-dual $[72, 36, 16]$ code.

- $\forall x \in X$, $\mathrm{wt}(x) = 16$.
- $\forall x, y \in X$, $(x, y) = 0$ (self-orthogonal).
- $|X| = 249849$.

Theorem 6 (Harada–Kitazume–Munemasa, 2004). *The set X coincides with the set of vectors of weight 16 in an extremal doubly even self-dual $[72, 36, 16]$ code.*

An analogous result for length 48 was obtained by Harada–Munemasa–Tonchev (preprint, 2004).