Frames of the Leech lattice

Akihiro Munemasa[1]

[1]Graduate School of Information Sciences
Tohoku University
(joint work with Rowena A. L. Betty)

September 15, 2011
Shanghai Jiao Tong University

McKay's construction of the Leech lattice (1972)

- A Hadamard matrix of order n is a square matrix with entries ± 1 satisfying $HH^T = nI$.
- When $n = 12$, there exists a unique (up to equivalence) Hadamard matrix H, and one may take H with $H + H^T = -2I$.

The Leech lattice L is defined as

$$L = \frac{1}{2} \operatorname{Span}_{\mathbb{Z}} \begin{bmatrix} I & H - I \\ 0 & 4I \end{bmatrix} \subset \frac{1}{2}\mathbb{Z}^{24} \subset \mathbb{R}^{24}$$

L is an integral lattice.

$$L \supset \frac{1}{2} \operatorname{Span}_{\mathbb{Z}} \begin{bmatrix} 4I & 4(H - I) \\ 0 & 4I \end{bmatrix} = \operatorname{Span}_{\mathbb{Z}} 2I = 2\mathbb{Z}^{24}.$$

$L = \frac{1}{2}\mathrm{Span}_{\mathbb{Z}}\begin{bmatrix} I & H-I \\ 0 & 4I \end{bmatrix}$ = Leech lattice

$$\min L = \min\{\|x\|^2 \mid 0 \neq x \in L\} = 4.$$

$\{x \in L \mid \|x\|^2 = 4\}$ is a spherical 11-design with 196560 points, giving a unique optimal kissing configuration (Bannai–Sloane, 1981).

A frame of L is $\{\pm f_1, \pm f_2, \dots, \pm f_{24}\}$ with $(f_i, f_j) = 4\delta_{ij}$. We also call the sublattice $F = \bigoplus_{i=1}^{24} f_i$ a frame.

Example

$$L \supset \frac{1}{2}\mathrm{Span}_{\mathbb{Z}}\begin{bmatrix} 4I & 4(H-I) \\ 0 & 4I \end{bmatrix} = \mathrm{Span}_{\mathbb{Z}}\begin{bmatrix} 2I & 0 \\ 0 & 2I \end{bmatrix} = 2\mathbb{Z}^{24}.$$

There are many others. Equivalence by the isometry group of L. If F is a frame, then

$$F \subset L \subset \frac{1}{4}F.$$

$F \subset L \subset \frac{1}{4}F$, $F \cong 2\mathbb{Z}^{24}$

$L/F \subset \frac{1}{4}F/F \cong \mathbb{Z}_4^{24}$.
A code over $\mathbb{Z}_4$ of length n is a submodule of $\mathbb{Z}_4^n$.

$$F \to \mathcal{C} = L/F \subset \mathbb{Z}_4^{24}.$$

Conversely, given a code $\mathcal{C}$ over $\mathbb{Z}_4$ of length 24, there is a frame $F \subset L$ s.t. $\mathcal{C} = L/F$ if and only if

(1) $\mathcal{C}$ is self-dual,

(2) $\forall x \in \mathcal{C}$, the Euclidean weight $\mathrm{wt}(x)$ is divisible by 8,

(3) $\min\{\mathrm{wt}(x) \mid x \in \mathcal{C},\ x \neq 0\} = 16$.

Definitions

- $(x, y) = \sum_{i=1}^n x_i y_i$, where $x, y \in \mathbb{Z}_4^n$,
- a code of length n over $\mathbb{Z}_4$ is a submodule $\mathcal{C} \subset \mathbb{Z}_4^n$,
- $\mathcal{C}$ is self-dual if $\mathcal{C} = \mathcal{C}^\perp$, where
  $\mathcal{C}^\perp = \{x \in \mathbb{Z}_4^n \mid (x, y) = 0 \ (\forall y \in \mathcal{C})\}$,
- For $u \in \mathbb{Z}_4^n$, the Euclidean weight of u is

$$\mathrm{wt}(u) = \sum_{i=1}^n u_i^2,$$

where we regard $u_i \in \{0, 1, 2, -1\} \subset \mathbb{Z}$.

$F \subset L \subset \frac{1}{4}F$, $F \cong 2\mathbb{Z}^{24}$

$L/F \subset \frac{1}{4}F/F \cong \mathbb{Z}_4^{24}$.
Given a code $\mathcal{C}$ over $\mathbb{Z}_4$ of length 24, there is a frame $F \subset L$ s.t. $\mathcal{C} = L/F$ if and only if

(1) $\mathcal{C}$ is self-dual,

(2) $\forall x \in \mathcal{C}$, the Euclidean weight $\mathrm{wt}(x)$ is divisible by 8,

(3) $\min\{\mathrm{wt}(x) \mid x \in \mathcal{C},\ x \neq 0\} = 16$.

A code $\mathcal{C}$ is called type II if (1) and (2) hold.

If (1), (2) and (3) hold, then $\mathcal{C}$ is called an extremal type II code over $\mathbb{Z}_4$ of length 24.

$F \to \mathcal{C} = L/F \subset \frac{1}{4}F/F \cong \mathbb{Z}_4^{24}$: Equivalence

$\mathrm{Aut}\, L =$ the group of isometries of L.
Consider another $F' \to \mathcal{C}' = L/F' \subset \frac{1}{4}F'/F' \cong \mathbb{Z}_4^{24}$. Then

$$F \cong F' \text{ under } \mathrm{Aut}\, L$$
$$\iff \mathcal{C} \text{ and } \mathcal{C}' \text{ are monomially equivalent.}$$

frames in $L \leftrightarrow$ extremal type II code over $\mathbb{Z}_4$ of length 24.
($\leftrightarrow$ gives a correspondence of equivalence classes.)

Dong–Mason–Zhu (1994): every frame of the Leech lattice gives rise to the Virasoro frame of the moonshine vertex operator algebra.
Example of an extremal type II code over $\mathbb{Z}_4$ of length 24:
Bonnecaze–Solé–Calderbank (1995): Hensel lifted Golay code.

Residue code $= \mathcal{C} \bmod 2 = \mathrm{Res}(\mathcal{C})$

If $\mathcal{C}$ is a code over $\mathbb{Z}_4$, then its modulo 2 reduction is called the residue code and is denoted by

$$\mathrm{Res}(\mathcal{C}) \subset \mathbb{F}_2^n.$$

Example: For the Hensel lifted Golay code $\mathcal{C}$, $\mathrm{Res}(\mathcal{C})$ is the Golay code.

$\mathcal{C}$: type II code over $\mathbb{Z}_4$

$\implies$ $\mathrm{Res}(\mathcal{C})$ is a doubly even binary code containing $\mathbf{1}$

$\mathcal{C}$: extremal type II code of length 24 over $\mathbb{Z}_4$

$\implies$ $\mathrm{Res}(\mathcal{C})^\perp$ has minimum weight at least 4.

Residue code $= \mathcal{C} \bmod 2 = \mathrm{Res}(\mathcal{C})$

Determine $\{\text{frames of } L\}/\sim$, with the help of the residue map $F \mapsto \mathrm{Res}(L/F)$:

$$\{F: \text{ frame of } L\}/\sim \quad \to \quad \left\{ \begin{array}{l} \text{doubly even } C \subset \mathbb{F}_2^{24} \\ \text{length} = 24,\ \mathbf{1} \in C \\ \min C^{\perp} \geq 4 \\ \text{easily enumerated} \end{array} \right\} / \sim$$

This map is neither injective nor surjective.

- Calderbank–Sloane (with Young) (1997): $\{\text{doubly even self-dual codes}\} \subset$ image.
- The image was determined by Harada–Lam–M., but not preimages.
- Rains (1999) determined the preimage for $C =$ Golay.

$$\{F:\ \text{frame of } L\}/\sim\ \xrightarrow{\text{Res}}\ \left\{\begin{array}{l}\text{doubly even } C\subset\mathbb{F}_2^{24}\\ \text{length}=24,\ \mathbf{1}\in C\\ \min C^\perp\geq 4\\ \text{(easily enumerated)}\end{array}\right\}/\sim$$

is equivalent to

$$\left\{\mathcal{C}:\ \begin{array}{c}\text{extremal}\\ \text{type II code}\\ \text{of length } 24\\ \text{over } \mathbb{Z}_4\end{array}\right\}/\sim\ \xrightarrow{\text{Res}}\ \left\{\begin{array}{l}\text{doubly even } C\subset\mathbb{F}_2^{24}\\ \text{length}=24,\ \mathbf{1}\in C\\ \min C^\perp\geq 4\end{array}\right\}/\sim$$

but the map is more naturally considered as:

$$\left\{\mathcal{C}:\ \begin{array}{c}\text{type II code}\\ \text{of length } 24\\ \text{over } \mathbb{Z}_4\end{array}\right\}/\sim\ \xrightarrow{\text{Res}}\ \left\{\begin{array}{l}\text{doubly even } C\subset\mathbb{F}_2^{24}\\ \text{length}=24,\ \mathbf{1}\in C\end{array}\right\}/\sim$$

$$\left\{ \mathcal{C} : \begin{array}{c} \text{type II code} \\ \text{of length } 24 \\ \text{over } \mathbb{Z}_4 \end{array} \right\} / \sim \ \xrightarrow{\text{Res}} \ \left\{ \begin{array}{l} \text{doubly even } C \subset \mathbb{F}_2^{24} \\ \text{length} = 24,\ \mathbf{1} \in C \end{array} \right\} / \sim$$

This is surjective (Gaborit, 1996).
Suppose C is a doubly even code of length 24 with $\mathbf{1} \in C$.

$$[A] \text{ generates } C, \quad \begin{bmatrix} A \\ B \end{bmatrix} \text{ generates } C^{\perp}.$$

Then there exists a matrix $\tilde{A}$ with $\tilde{A} \bmod 2 = A$ such that

$$\mathcal{C} = \mathbb{Z}_4\text{-span of } \begin{bmatrix} \tilde{A} \\ 2B \end{bmatrix}$$

is a type II code over $\mathbb{Z}_4$ (i.e., $\mathrm{Res}(\mathcal{C}) = C$).

$$\mathrm{Res}^{-1}(C) \subset \{\mathbb{Z}_4\text{-span of } \begin{bmatrix} \tilde{A} + 2M \\ 2B \end{bmatrix} \mid M : (0,1) \text{ matrix}\}$$

$[A]$ generates C, $\left[\begin{smallmatrix}A\\B\end{smallmatrix}\right]$ generates $C^{\perp}$.

$$\left\{ \mathcal{C} : \begin{array}{c}\text{type II code}\\ \text{of length } 24\\ \text{over } \mathbb{Z}_4\end{array} \right\} / \sim \ \stackrel{\mathrm{Res}}{\longrightarrow} \ \left\{ \begin{array}{l}\text{doubly even } C \subset \mathbb{F}_2^{24}\\ \text{length} = 24,\ \mathbf{1} \in C\end{array} \right\} / \sim$$

$$\mathrm{Res}^{-1}(C) \subset \{\mathbb{Z}_4\text{-span of } \begin{bmatrix}\tilde{A} + 2M\\ 2B\end{bmatrix} \mid M :\ (0,1) \text{ matrix}\}$$

In fact,

$$\mathrm{Res}^{-1}(C) = \{\mathbb{Z}_4\text{-span of } \begin{bmatrix}\tilde{A} + 2M\\ 2B\end{bmatrix} \mid M \in U_0\},$$

where

$$U_0 = \{M \mid MA^T + AM^T = 0,\ \mathrm{Diag}(AM^T) + \mathrm{Diag}(\mathbf{1}M^T) = 0\}.$$

U_0 is a linear subspace of matrices.

$[A]$ generates C, $\quad \begin{bmatrix} A \\ B \end{bmatrix}$ generates $C^\perp$.

Set

$$U_0 = \{M \mid MA^T + AM^T = 0,\ \mathrm{Diag}(AM^T) + \mathrm{Diag}(\mathbf{1}M^T) = 0\}.$$

$$W_0 = \langle \{M \in U_0 \mid MA^T = 0\}, \{AE_{ii} \mid 1 \le i \le n\} \rangle,$$

Theorem

$\mathrm{Aut}(C)$ acts on U_0/W_0 as an affine transformation group. Moreover, there is a bijection

$$\mathrm{Aut}(C)\text{-orbits on } U_0/W_0 \to \left\{ \begin{array}{c} \text{eq. class} \\ \text{of type II} \\ \text{codes } \mathcal{C} \text{ with} \\ \mathrm{Res}(\mathcal{C}) = C \end{array} \right\}$$

$$M \bmod W_0 \mapsto \begin{array}{c} \text{eq. class of} \\ \text{codes generated by} \end{array} \begin{bmatrix} \tilde{A} + 2M \\ 2B \end{bmatrix}$$

Practical Implementation

Theorem

$\mathrm{Aut}(C)$ acts on U_0/W_0 as an affine transformation group. Moreover, there is a bijection

$$\mathrm{Aut}(C)\text{-orbits on } U_0/W_0 \to \left\{ \begin{array}{c} \text{eq. class} \\ \text{of type II} \\ \text{codes } \mathcal{C} \text{ with} \\ \mathrm{Res}(\mathcal{C}) = C \end{array} \right\}$$

$$\mathrm{Aut}(C) \to \mathrm{AGL}(U_0/W_0).$$

Since $\mathrm{AGL}(m, \mathbb{F}_2) \subset \mathrm{GL}(1+m, \mathbb{F}_2)$, we actually construct a linear representation:

$$\mathrm{Aut}(C) \to \mathrm{GL}(1+m, \mathbb{F}_2),$$

where $m = \dim U_0/W_0$.

C = Golay code

$\operatorname{Aut} C = M_{24}$: Mathieu group.

$$M_{24} \to \mathrm{AGL}(44,2) \to \mathrm{GL}(45,2)$$

acts on a hyperplane $\mathcal{H}$ of $\mathbb{F}_2^{45}$, and

orbits of M_{24} on $\mathcal{H}$ $\leftrightarrow$ type II codes $\mathcal{C}$ with $\mathrm{Res}(\mathcal{C}) = C$.

The 2^{44} elements of $\mathcal{H}$ are divided into orbits under M_{24}. As an estimate, there are at least

$$\frac{2^{44}}{|M_{24}|} = 71856.7\ldots$$

orbits.
We extract only those orbits which correspond to extremal codes $\to$ only 13 orbits (an independent verification of computation due to Rains (1999)).

$F \to \mathcal{C} = L/F \to \mathrm{Res}(\mathcal{C})$

Rains (1999): there are exactly 13 extremal type II codes $\mathcal{C}$ s.t. $\mathrm{Res}(\mathcal{C})$ is the binary extended Golay code.

Harada–Lam–M. there is a unique extremal type II code $\mathcal{C}$ s.t. $\dim \mathrm{Res}(\mathcal{C}) = 6$ (This is related to the code used by Miyamoto (2004) to construct $V^\natural$). $\#$ of $\mathrm{Res}(\mathcal{C})$ is also computed.

$\dim \mathrm{Res}(\mathcal{C})$	6	7	8	9	10	11	12
$\#$ of $\mathrm{Res}(\mathcal{C})$	1	7	32	60	49	21	9
$\#\ \mathcal{C}$	1	5	31	178	764	1886	1890+13

So there are $1 + 5 + 31 + 178 + 764 + 1886 + 1890 + 13 = 4768$ frames of the Leech lattice.