Towards the classification of 4-frames in the Leech lattice

Akihiro Munemasa[1]

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

December 13, 2010
Kyoto, Japan

Main result

The Leech lattice has

$$1+5+29+171+755+1880+1903 \quad \text{(corrected after the talk)}$$

4-frames.

- What (Definitions)
- Where (History)
- Why (Motivations)
- How (Computation)

The Leech lattice L

A $\mathbb{Z}$-submodule L of rank 24 in $\mathbb{R}^{24}$ with basis B characterized by the following properties of its Gram matrix $G = BB^T$:

- $\det G = 1$,
- $G_{ij} \in \mathbb{Z}$,
- $G_{ii} \in 2\mathbb{Z}$
- rootless: $\forall x \in L$, $\|x\|^2 \neq 2$.

unique up to isometry in $\mathbb{R}^{24}$.

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 $H + H^T = -2I$.

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

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

$L =$ Leech lattice

$$\min L = \min\{\|x\|^2 \mid 0 \neq x \in L\} = 4 \quad \text{(rootless)}.$$

$$\#\{x \in L \mid \|x\|^2 = 4\} = 196560$$

A 4-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 4-frame.
Example:

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

There are many others, but certainly finite. Equivalence by isometry group of L.

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

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

$L/F \subset \frac{1}{4}F/F \cong \mathbb{Z}_4^{24}$.
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) $\min\{\mathrm{wt}(x) \mid x \in \mathcal{C},\ x \neq 0\} = 16$.

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

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

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

Then

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

Classification of 4-frames in $L \iff$ classification of extremal type II code over $\mathbb{Z}_4$ of length 24.

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 of length n

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

$\implies$ $8|n$.

Frame of $L \to$ Virasoro Frame of $V^\natural$

$$\{\text{Virasoro frames of } V^\natural\}$$

difficult

$$\uparrow \text{DMZ}$$

$$\{\text{frames of } L\} \quad \overset{L/F \bmod 2}{\rightarrow} \quad \left\{ \begin{array}{l} \text{doubly even } C \\ \text{len} = 24,\ \mathbf{1}_{24} \in C \\ \min C^\perp \geq 4 \\ \text{easily enumerated} \end{array} \right\}$$

DMZ = Dong–Mason–Zhu (1994)

Frame of $L \to$ Virasoro Frame of $V^\natural$

$$
\begin{array}{ccc}
\{\text{Virasoro frames of } V^\natural\} & \overset{\text{str}}{\to} & \left\{ \begin{array}{l} \text{triply even } D \\ \text{len} = 48,\ \mathbf{1}_{48} \in D \\ \min D^\perp \geq 4 \end{array} \right\} \\
\color{red}{\text{difficult}} & & \\
\uparrow \text{DMZ} & & \uparrow \mathcal{D} \text{ (doubling)} \\
\{\text{frames of } L\} & \overset{L/F \bmod 2}{\to} & \left\{ \begin{array}{l} \text{doubly even } C \\ \text{len} = 24,\ \mathbf{1}_{24} \in C \\ \min C^\perp \geq 4 \\ \color{red}{\text{easily enumerated}} \end{array} \right\}
\end{array}
$$

Lam–Yamauchi (2008): the diagram commutes, and

$$
\text{DMZ}(\{\text{frames of } L\}) \overset{(\subset)}{\color{red}{=}} \text{str}^{-1}(\mathcal{D}(\{\text{doubly even}\})).
$$

Determine {frames of L}, with the help of the map

$$\{\text{frames of } L\} \overset{L/F \bmod 2}{\rightarrow} \left\{ \begin{array}{l} \text{doubly even } C \\ \text{length} = 24,\ \mathbf{1}_{24} \in C \\ \min C^{\perp} \geq 4 \\ \text{easily enumerated} \end{array} \right\}$$

$F \subset L \subset \frac{1}{4}F \rightsquigarrow \mathcal{C} = L/F \subset \mathbb{Z}_4^{24} \rightsquigarrow C = L/F \bmod 2$.
For each $C \in$ RHS, classify F such that $\mathrm{Res}(L/F) \cong C$.

The map $F \mapsto L/F \bmod 2$ is neither injective nor surjective.
Calderbank–Sloane (with Young) (1997):
{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.

- $(x, y) = \sum_{i=1}^{n} x_i y_i$, 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 $\mathcal{C}^\perp = \{x \in \mathbb{Z}_4^n \mid (x, y) = 0\ (\forall y \in \mathcal{C})\}$,
- the residue: $\mathrm{Res}(\mathcal{C}) \subset \mathbb{F}_2^n$ (reduction $\mathbb{Z}_4 \to \mathbb{F}_2$ mod 2).
- For $u \in \mathbb{Z}_4^n$,

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

  where we regard $u_i \in \{0, 1, 2, -1\} \subset \mathbb{Z}$. A code $\mathcal{C} \subset \mathbb{Z}_4^n$ is type II if $\mathcal{C}$ is self-dual and $8 |\, \mathrm{wt}(u)$ for all $u \in \mathcal{C}$.

- Conway–Sloane (1993): 4 type II codes of length 8
- Pless–Leon–Fields (1997): 133 type II codes of length 16

The set of all type II $\mathbb{Z}_4$-codes $\mathcal{C}$ with $\mathrm{Res}(\mathcal{C}) = C$ has a structure as an affine space of dimension $(k-2)(k+1)/2$ over $\mathbb{F}_2$

Classifying such $\mathcal{C}$ amounts to enumerating $k \times n$ binary matrices M such that

$$\begin{bmatrix} A+2M \\ 2B \end{bmatrix}, \text{ where } [A] \text{ generates } C, \quad \begin{bmatrix} A \\ B \end{bmatrix} \text{ generates } C^{\perp},$$

generates a type II code.

Among the 2^{kn} matrices M, not all of them generate a self-dual code, while some matrices generate the same code as the one generated by some other matrix. This reduces the number

$$2^{kn} \text{ to } 2^{(k-2)(k+1)/2}.$$

Given $C \subset \mathbb{F}_2^n$, classify type II codes $\mathcal{C} \subset \mathbb{Z}_4^n$ with $\mathrm{Res}(\mathcal{C}) = C$.

Note: $\mathcal{C}$: type II $\mathbb{Z}_4$-code $\implies$ $\mathrm{Res}(\mathcal{C})$: doubly even, $\ni \mathbf{1}$.

Theorem (Rains, 1999)

Given a doubly even code C of length n, dimension k, $\ni \mathbf{1}$.

- the set of all type II $\mathbb{Z}_4$-codes $\mathcal{C}$ with $\mathrm{Res}(\mathcal{C}) = C$ has a structure as an affine space of dimension $(k-2)(k+1)/2$ over $\mathbb{F}_2$ (due to Gaborit, 1996),
- the group $\{\pm 1\}^n \rtimes \mathrm{Aut}(C)$ acts as an affine transformation group,
- two codes $\mathcal{C}, \mathcal{C}'$ are equivalent if and only if they are in the same orbit under this group.

Given $C \subset \mathbb{F}_2^n$, classify type II codes $\mathcal{C} \subset \mathbb{Z}_4^n$ with $\mathrm{Res}(\mathcal{C}) = C$.

Note: $\mathcal{C}$: type II $\mathbb{Z}_4$-code $\implies$ $\mathrm{Res}(\mathcal{C})$: doubly even, $\ni \mathbf{1}$.

Theorem (Rains, 1999)

Given a doubly even code C of length n, dimension k, $\ni \mathbf{1}$.

- the set of all type II $\mathbb{Z}_4$-codes C with $\mathrm{Res}(\mathcal{C}) = C$ has a structure as an affine space of dimension $(k-2)(k+1)/2$ over $\mathbb{F}_2$ (due to Gaborit, 1996),
- the group $\{\pm 1\}^n \rtimes \mathrm{Aut}(C)$ acts as an affine transformation group,
- two codes $\mathcal{C}, \mathcal{C}'$ are equivalent if and only if they are in the same orbit under this group.

Given $C \subset \mathbb{F}_2^n$, classify type II codes $\mathcal{C} \subset \mathbb{Z}_4^n$ with $\mathrm{Res}(\mathcal{C}) = C$.

Note: $\mathcal{C}$: type II $\mathbb{Z}_4$-code $\implies \mathrm{Res}(\mathcal{C})$: doubly even, $\ni \mathbf{1}$.

Theorem (Rains, 1999)

Given a doubly even code C of length n, dimension k, $\ni \mathbf{1}$.

- the set of all type II $\mathbb{Z}_4$-codes C with $\mathrm{Res}(\mathcal{C}) = C$ has a structure as an affine space of dimension $(k-2)(k+1)/2$ over $\mathbb{F}_2$ (due to Gaborit, 1996),
- the group $\{\pm 1\}^n \rtimes \mathrm{Aut}(C)$ acts as an affine transformation group,
- two codes $\mathcal{C}, \mathcal{C}'$ are equivalent if and only if they are in the same orbit under this group.

The group $\{\pm 1\}^n \rtimes \mathrm{Aut}(C)$ acts as an affine transformation group on an affine space of dimension $(k-2)(k+1)/2$

Theorem (improved version)

Given a doubly even code C of length n, dimension k, containing $\mathbf{1}_n$,

- the set of all type II $\mathbb{Z}_4$-codes $\mathcal{C}$ with $\mathrm{Res}(\mathcal{C}) = C$ has a surjection onto an affine space of dimension at most $(k-2)(k+1)/2$ over $\mathbb{F}_2$, (e.g. $65 \to 44$)
- the group $\mathrm{Aut}(C)$ acts as an affine transformation group,
- two codes $\mathcal{C}, \mathcal{C}'$ are equivalent if and only if their images are in the same orbit under this group.

Type II $\mathbb{Z}_4$-codes $\mathcal{C}$ with $\mathrm{Res}(\mathcal{C}) = C$

Given a doubly even code C of length n, dimension k, with generator matrix $[A]$, $C^\perp$ is generated by $\begin{bmatrix} A \\ B \end{bmatrix}$, set

$$\begin{aligned} \mathcal{M} &= \mathrm{Mat}_{k\times n}(\mathbb{F}_2), \\ U_0 &= \{M \in \mathcal{M} \mid MA^T + AM^T = 0, \\ &\qquad \mathrm{Diag}(AM^T) + \mathrm{Diag}(\mathbf{1}M^T) = 0\}, \\ W_0 &= \langle \{M \in \mathcal{M} \mid MA^T = 0\}, \{AE_{ii} \mid 1 \le i \le n\}\rangle, \\ U &= U_0 \oplus \mathbb{F}_2, \\ W &= W_0 \oplus \{0\}. \end{aligned}$$

$$U_0/W_0 \ni M \pmod{W_0} \mapsto \begin{array}{c}\text{eq. class of} \\ \text{code generated by}\end{array} \begin{bmatrix} \tilde{A} + 2M \\ 2B \end{bmatrix}$$

is well-defined. ($\tilde{A}$ will be chosen appropriately)

$\mathrm{Aut}(C)$ acts on U_0/W_0 as an affine transformation group, and the orbits are the preimages of equivalence classes.

$\mathrm{Aut}(C)$ acts on U_0/W_0

First, take a matrix $\tilde{A}$ over $\mathbb{Z}_4$ such that

$$\tilde{A} \bmod 2 = A \text{ and } \tilde{A}\tilde{A}^T = 0,$$
$$\text{weight of rows of } \tilde{A} \equiv 0 \pmod 8$$

$\forall P \in \mathrm{Aut}(C)$, $\exists E_1(P) \in \mathrm{GL}(k, \mathbb{F}_2)$ such that

$$AP = E_1(P)A.$$

and $\exists E_2(P) \in \mathcal{M}$ such that

$$2E_2(P) = E_1(P)^{-1}\tilde{A}P - \tilde{A}.$$

Then

$$P : M \mapsto E_1(P)^{-1}MP + E_2(P).$$

$\mathrm{Aut}(C)$ acts on U_0/W_0

Theorem

The group $\mathrm{Aut}(C)$ acts on U_0/W_0 by

$$
\begin{aligned}
P : U_0/W_0 \ni M &\pmod{W_0} \\
&\mapsto E_1(P)^{-1}MP + E_2(P) \pmod{W_0} \in U_0/W_0,
\end{aligned}
$$

where $P \in \mathrm{Aut}(C)$. Moreover, there is a bijection

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

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

Practical Implementation

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

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

$$\mathrm{Aut}(C) \to \mathrm{GL}(1 + \dim U_0/W_0).$$

A straightforward implementation works provided

$$\dim U_0/W_0 \leq 26 \text{ (depending on available memory)}$$

which is the case if $\dim C \leq 10$.

dim	6	7	8	9	10	11	12
#	1	7	32	60	49	21	9

If $\dim U_0/W_0$ is large

A straightforward computation will not work if $\dim C = 11$ or 12. For example, $C =$ extended Golay code, $\dim U_0/W_0 = 44$. So we will have a matrix representation

$$M_{24} = \mathrm{Aut}(C) \to \mathrm{GL}(45, \mathbb{F}_2).$$

As an estimate:

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

but there are only 13 extremal type II codes C with $\mathrm{Res}(\mathcal{C}) =$ Golay code.

C = Golay code

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

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

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

There are 2^{44} elements to examine for extremality.
We need to extract only extremal codes and then classify up to equivalence.
Rains (1999) avoided this, instead classified self-dual codes of lengths $22, 23$, then building up from these. (limitation to Golay case)

$\{\mathcal{C}\colon \text{type II},\ \mathrm{Res}(\mathcal{C}) = \text{Golay}\}/\{\pm 1\} \cong \mathbb{F}_2^{44}$

For each octad $x \in C$, consider the subset

$$H(x) = \{\mathcal{C} \mid \mathrm{Res}(\mathcal{C}) = C,\ \mathcal{C}\colon \text{type II},\\ \exists v \in \mathcal{C},\ \mathrm{wt}(v) = 8,\ v \bmod 2 = x\}.$$

$$\begin{aligned} x &= (111111110000\cdots 0000), && \text{octad}, \\ v &= (111111110000\cdots 0000), && \text{weight 8}, \\ v' &= (111111112200\cdots 0000), && \text{weight 16} \end{aligned}$$

$$v \in \mathcal{C} \implies \mathcal{C} \text{ is not extremal.}$$

Every member of $H(x)$ has minimum Euclidean weight 8 (non-extremal).
$H(x)$ is a subspace of codimension 4.

Another trick is to use a subgroup to classify up to equivalence using a submodule, then later classify a manageable size of representatives by M_{24}. Note that M_{24} does not have a submodule of dimension less than 44 in $M_{24} \to \mathrm{GL}(45, 2)$. We recover

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

We can modify slightly for $C \neq$ Golay code. Numbers of doubly even codes $C \subset \mathbb{F}_2^{24}$ containing $\mathbf{1}$ and $C^{\perp}$ has minimum weight ≥ 4.

$\dim$	6	7	8	9	10	11	12
$\#$	1	7	32	60	49	21	9

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

- 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 $V^\natural$).

$\dim$	6	7	8	9	10	11	12
$\#$	1	7	32	60	49	21	9
$\#\ \mathcal{C}$	1	5	29	171	755	1880	1903
	1						13

(corrected after the talk)