Frames of the Leech lattice and their applications

Akihiro Munemasa[1]

[1]Graduate School of Information Sciences
Tohoku University

August 6, 2009

The Leech lattice

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

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

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

cf. E_8-lattice is a unique even unimodular lattice of rank 8.

Factorization of the polynomial $X^{23} - 1$

$$(X-1)(X^{22}+X^{21}+\cdots+X+1) \qquad \text{over } \mathbb{Z}$$

$$\begin{aligned} &= (X-1)(X^{11}+X^{10}+\cdots+1) \\ &\qquad \times (X^{11}+X^{9}+\cdots+1) \qquad \text{over } \mathbb{F}_2 \end{aligned}$$

$$\begin{aligned} &= (X-1)(X^{11}-X^{10}+\cdots-1) \\ &\qquad \times (X^{11}+2X^{10}-X^{9}+\cdots-1) \qquad \text{over } \mathbb{Z}/4\mathbb{Z} \end{aligned}$$

(by Hensel's lemma).

$X^{23} - 1 = (X-1)f(X)g(X)$ over $\mathbb{Z}/4\mathbb{Z}$

L is generated by the rows of:

$$\left[\begin{array}{llll}
\frac{1}{2} & \boxed{\tfrac{1}{2}f(X)} & & \\
\frac{1}{2} & & \boxed{\tfrac{1}{2}f(X)} & \\
\frac{1}{2} & & & \boxed{\tfrac{1}{2}f(X)} \\
\vdots & & & \ddots \\
\hline
\multicolumn{4}{c}{2I_{24}}
\end{array}\right]$$

$(23+24) \times 24$ matrix

Bonnecaze-Calderbank-Solé (1995)

cf. $\overline{f}(X) = f(X)$ mod 2. Golay code is

row sp. of
$$\left[\begin{array}{llll}
1 & \boxed{\overline{f}(X)} & & \\
1 & & \boxed{\overline{f}(X)} & \\
1 & & & \boxed{\overline{f}(X)} \\
\vdots & & & \ddots
\end{array}\right]$$
over $\mathbb{F}_2$ (mod 2 reduction of L).

L = Leech lattice

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

A frame of L is $\{\pm f_1, \pm f_2, \ldots, \pm f_{24}\}$ with $(f_i, f_j) = 4\delta_{ij}$.

$$\left[\begin{array}{llll}
\frac{1}{2} & \boxed{\tfrac{1}{2} f(X)} & & \\
\frac{1}{2} & & \boxed{\tfrac{1}{2} f(X)} & \\
\frac{1}{2} & & & \boxed{\tfrac{1}{2} f(X)} \\
\vdots & & & \ddots \\
\hline
\multicolumn{4}{c}{2I_{24}}
\end{array}\right] \leftarrow \text{here}$$

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

cf. E_8 has 240 roots and a unique frame (of norm 2) up to $W(E_8)$.

Contents

History

- E. Mathieu (1861, 1873): Mathieu groups
- E. Witt (1938): (Aut(Steiner system $S(5, 8, 24)) = M_{24}$)
- M.J.E. Golay (1949): (Aut(Golay code) $= M_{24}$)
- J. Leech (1965): lattice L
- J.H. Conway (1968): Aut$(L) = Co_0$
- E. Bannai and N.J.A. Sloane (1981): 196560 vectors
- B. Fischer, R. Griess (1982): The Monster $\mathbb{M}$
- I. Frenkel, J. Lepowsky and A. Meurman (1988): Aut$(V^\natural) = \mathbb{M}$.

Total of 26 sporadic finite simple groups.
The most remarkable of all $\mathbb{M}$: moonshine
$1 + 196883 = 196884 \to V^\natural$ (vertex operator algebra).
Ultimate Goal: Want to understand $V^\natural$ or $\mathbb{M}$ better.

Quadratic Forms

$L =$ even unimodular, rank 24, without roots
B: basis of L
$\to G = BB^T$: Gram matrix
$\to Q(x) = x^T Gx$ is a pos. def. quadratic form $\mathbb{Z}^{24} \to 2\mathbb{Z}$.
$\to L$.

Golay code is also related to a quadratic form in a different sense.

Example. For $x, y, z \in \mathbb{F}_2$,

$$x^2 + y^2 + z^2 + xy + yz + zx = \frac{1}{2}\,\mathrm{wt}((x, y, z, x + y + z)) \bmod 2,$$

where $\mathrm{wt}((x_1, \ldots, x_n)) = \#i$ with $x_i = 1$.

A quadratic form over $\mathbb{F}_2$

More generally,

$$\mathbb{F}_2^n \supset \mathbf{E}_n = \{u \in \mathbb{F}_2^n \mid \mathrm{wt}(u) \text{ even}\} : \quad \dim = n - 1.$$

$$Q : \mathbf{E}_n \to \mathbb{F}_2, \quad Q(u) = \frac{\mathrm{wt}(u)}{2} \bmod 2$$

Then

$$Q(u + v) = Q(u) + Q(v) + \sum_{i=1}^{n} u_i v_i.$$

Witt's theorem $\implies$ $\exists!$ maximal subspace U of $\mathbf{E}_n$ such that $Q|_U = 0$, up to the action of $\mathrm{O}(\mathbf{E}_n, Q)$.
Note, however, that $\mathrm{O}(\mathbf{E}_n, Q)$ does not preserve $\mathrm{wt}(u)$.
The subgroup S_n preserves $\mathrm{wt}(u)$.

$$Q(u) = \frac{\mathrm{wt}(u)}{2} \bmod 2$$

A linear subspace of $\mathbb{F}_2^n$ is called a (binary) code of length n.
A code $C \subset \mathbf{E}_n$ is said to be doubly even if $Q|_C = 0$, i.e., $4 | \mathrm{wt}(u)\ \forall u \in C$.

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

$$C^\perp = \{u \in \mathbb{F}_2^n \mid (u, v) = 0\ \forall v \in C\}.$$

Witt's theorem $\implies$ $\exists!$ maximal doubly even code of length n up to the action of $\mathrm{O}(\mathbf{E}_n, Q)$.
$S_n \subset \mathrm{O}(\mathbf{E}_n, Q)$ acts on the set of maximal doubly even code of length n. Equivalence of codes is defined by the action of S_n.
$n = 24$: there are 9 maximal doubly even codes up to S_{24}, Golay code is one of them.

Quadratic $\leftrightarrow$ doubly even
Cubic $\leftrightarrow$ triply even

- $\mathbb{F}_2^n \to \mathbb{F}_2$, $u \mapsto \mathrm{wt}(u)$ mod 2: linear
- $\mathbf{E}_n \to \mathbb{F}_2$, $Q : u \mapsto \frac{\mathrm{wt}(u)}{2}$ mod 2: quadratic
- for a doubly even code C, $C \to \mathbb{F}_2$, $T : u \mapsto \frac{\mathrm{wt}(u)}{4}$ mod 2: cubic

There is no analogue of Witt's theorem for cubic forms $\Longrightarrow$ it is nontrivial to classify maximal codes C with $T|_C = 0$, i.e.,

$$\forall u \in C,\ 8 | \mathrm{wt}(u).$$

Call such C triply even.

$\mathrm{Aut}\, V^\natural = \mathbb{M}$

C is triply even iff $\forall u \in C,\ 8 \mid \mathrm{wt}(u)$

A triply even code appeared in the construction of $V^\natural$ due to Dong–Griess–Höhn (1998), Miyamoto (2004).
Leech lattice $\rightsquigarrow D_7 \subset \mathbb{F}_2^{48} \rightsquigarrow V^\natural$.

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \qquad H_3 = \begin{bmatrix} H & H & H \\ \mathbf{1}_8 & 0 & 0 \\ 0 & \mathbf{1}_8 & 0 \\ 0 & 0 & \mathbf{1}_8 \end{bmatrix}$$

$$D_7 = \mathbb{F}_2\text{-span of } \begin{bmatrix} H_3 & H_3 \\ \mathbf{1}_{24} & 0 \\ 0 & \mathbf{1}_{24} \end{bmatrix} \ : \text{ triply even}$$

where $\mathbf{1}_n = (1, 1, \ldots, 1) \in \mathbb{F}_2^n$.

$\mathbb{F}_2$-span of

$$H_3 = \begin{bmatrix} H & H & H \\ \mathbf{1}_8 & 0 & 0 \\ 0 & \mathbf{1}_8 & 0 \\ 0 & 0 & \mathbf{1}_8 \end{bmatrix}$$

is doubly even $\implies$ $\mathbb{F}_2$-span of

$$D_7 = \mathcal{D}(H_3) = \begin{bmatrix} H_3 & H_3 \\ \mathbf{1}_{24} & 0 \\ 0 & \mathbf{1}_{24} \end{bmatrix}$$

is triply even.
More generally, if A spans a doubly even code C of length $n \equiv 0 \pmod 8$, then

$$\mathcal{D}(C) = \mathbb{F}_2\text{-span of } \begin{bmatrix} A & A \\ \mathbf{1}_n & 0 \\ 0 & \mathbf{1}_n \end{bmatrix}$$

is a triply even code of length $2n$. $\mathcal{D}$ = doubling.

Framed Vertex Operator Algebra

Dong–Griess–Höhn (1998), Miyamoto (2004):
$L \rightsquigarrow D_7 \subset \mathbb{F}_2^{48} \rightsquigarrow V^\natural$.

$$V^\natural \supset L(1/2,0)^{\otimes 48}, \text{ where } L(1/2,0) : \text{ Virasoro VOA}$$

$$L \supset F = \bigoplus_{i=1}^{24} \mathbb{Z} f_i, \text{ where } (f_i, f_j) = 4\delta_{ij} : \text{ frame}$$

$$L = \bigcup_{x \in L/F} (x + F) \quad \text{coset decomposition}$$

$$V^\natural = \bigoplus_{\beta \in D} V^\beta \quad \text{as } L(1/2,0)^{\otimes 48}\text{-modules}$$

$F \subset L$: not unique.
$L(1/2,0)^{\otimes 48} \cong \mathcal{T} \subset V^\natural$: not unique $\implies$ D: depends on $\mathcal{T}$ (Virasoro frame), but:

$$D \subset \mathbb{F}_2^{48}, \ D: \text{ triply even}, \ \mathbf{1}_{48} \in D.$$

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

Dong–Mason–Zhu (1994)

$$
\begin{aligned}
L \supset F = \bigoplus_{i=1}^{24} \mathbb{Z} f_i &: \text{ frame} \\
\to V^\natural \supset \mathcal{T} \cong L(1/2,0)^{\otimes 48} &: \text{ Virasoro frame} \\
V^\natural = \bigoplus_{\beta \in D} V^\beta & \text{ as } \mathcal{T}\text{-modules} \\
D = \text{structure code} & \text{ of } \mathcal{T} \\
= \mathcal{D}(L/F & \bmod 2).
\end{aligned}
$$

Note $L/F \subset (\mathbb{Z}/4\mathbb{Z})^{24}$ since $F \subset L \subset \frac{1}{4}F$, so $L/F \bmod 2 \subset \mathbb{F}_2^{24}$

Classification of $F \subset L \implies$ classification of $\mathcal{T} \subset V^\natural$?

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

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

The diagram commutes, and

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

Theorem (Betsumiya–Harada–Shimakura–M.)

Every maximal member of

$$\left\{ \begin{array}{l} \text{triply even } D \\ \text{length} = 48,\ \mathbf{1}_{48} \in D \end{array} \right\}$$

is

- $\mathcal{D}(C)$ for some doubly even code C of length 24, or
- decomposable (only two such codes, one of the form $\mathcal{D}(C_1) \oplus \mathcal{D}(C_2) \oplus \mathcal{D}(C_3)$, another of the form $\mathcal{D}(C_1) \oplus \mathcal{D}(C_2)$), or
- a code of dimension 9 obtained from the triangular graph T_{10} on $45 = |S_{10} : S_2 \times S_8|$ vertices.

The last case does not occur if we assume min $D^{\perp} \geq 4$. According to Lam–Yamauchi, it must be a structure code of some framed VOA, not $V^{\natural}$.

Corollary (Betsumiya–Harada–Shimakura–M.)

$$\left\{ \begin{array}{l} \text{triply even } D \\ \text{len} = 48,\ \mathbf{1}_{48} \in D \\ \text{min}\, D^{\perp} \geq 4 \end{array} \right\}$$

$$= \mathcal{D}\left(\left\{ \begin{array}{l} \text{doubly even } C \\ \text{len} = 24,\ \mathbf{1}_{24} \in C \\ \text{min}\, C^{\perp} \geq 4 \end{array} \right\} \right)$$

$$\cup \{\text{subcodes of decomposable } \mathcal{D}(C_1) \oplus \mathcal{D}(C_2), \ldots\}$$

$$\{\mathcal{T} \subset V^\natural\} \quad \overset{\text{str}}{\longrightarrow} \quad \mathcal{D}\left(\left\{\begin{array}{l} \text{doubly even } C \\ \text{length} = 24 \\ \mathbf{1}_{24} \in C \\ \min C^\perp \geq 4 \end{array}\right\}\right) \cup \{\mathcal{D}(C_1) \oplus \mathcal{D}(C_2), \dots\}$$

$$\uparrow \text{DMZ} \qquad\qquad \uparrow \mathcal{D} \text{ (doubling)}$$

$$\{F \subset L\} \quad \overset{\text{mod } 2}{\longrightarrow} \quad \left\{\begin{array}{l} \text{doubly even } C \\ \text{length} = 24 \\ \mathbf{1}_{24} \in C \\ \min C^\perp \geq 4 \end{array}\right\}$$

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

Problem remains:

- $\{\mathcal{T} \subset V^\natural\} \to \{\mathcal{D}(C_1) \oplus \mathcal{D}(C_2), \dots\}$?
- $\{F \subset L\}$?

Determine $\{F \subset L\}$, i.e., classify all frames of the Leech lattice L, with the help of the map

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

$$F \subset L \subset \tfrac{1}{4}F \rightsquigarrow \mathcal{C}_F = L/F \subset (\mathbb{Z}/4\mathbb{Z})^{24} \rightsquigarrow C = L/F \bmod 2.$$

For each $C \in$ RHS, classify F such that $\mathcal{C}_F \bmod 2 \cong C$.
The map $F \mapsto L/F \bmod 2$ is neither injective nor surjective.

Codes over $\mathbb{Z}/4\mathbb{Z}$

A code over $\mathbb{Z}/4\mathbb{Z}$ of length n is a submodule of $(\mathbb{Z}/4\mathbb{Z})^n$.
Equivalence is by $\{\pm 1\}^n \rtimes S_n$.
For $u \in (\mathbb{Z}/4\mathbb{Z})^n$,

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

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

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

A code $\mathcal{C} \subset (\mathbb{Z}/4\mathbb{Z})^n$ is Type II if $8 | \mathrm{wt}(u)$ for all $u \in \mathcal{C}$. Then

$$\{\text{frames of } L\} \overset{1:1}{\leftrightarrow} \left\{ \begin{array}{c} \mathcal{C} \subset (\mathbb{Z}/4\mathbb{Z})^{24} \\ \mathcal{C} : \text{ Type II} \\ \min \mathcal{C} = 16 \end{array} \right\} \overset{\text{mod } 2}{\longrightarrow} \left\{ \begin{array}{l} \text{doubly even } C \\ \text{length} = 24 \\ \mathbf{1}_{24} \in C \\ \min C^\perp \geq 4 \end{array} \right\}$$

$$\left\{\begin{array}{c}\mathcal{C} \subset (\mathbb{Z}/4\mathbb{Z})^{24}, \\ \mathcal{C} : \text{ Type II}, \\ \min \mathcal{C} = 16\end{array}\right\} \overset{\text{mod } 2}{\longrightarrow} \left\{\begin{array}{l}\text{doubly even } C \\ \text{length } = 24 \\ \mathbf{1}_{24} \in C \\ \min C^{\perp} \geq 4\end{array}\right\}$$

Let C be a doubly even code of length n spanned by the rows of a matrix $A \in \mathrm{Mat}_{k\times n}(\mathbb{F}_2)$.

$$V = \{M \in \mathrm{Mat}_{k\times n}(\mathbb{F}_2) \mid MA^T + AM^T = 0\},$$

$$W = \langle \{M \in \mathrm{Mat}_{k\times n}(\mathbb{F}_2) \mid MA^T = 0\}, \{AE_{ii} \mid 1 \leq i \leq n\}\rangle.$$

Theorem (Rains (1999))

$\exists\, \mathrm{Aut}(C) \to \mathrm{AGL}(V/W)$ and

$$\{\mathcal{C} \subset (\mathbb{Z}/4\mathbb{Z})^n \mid \mathcal{C} = \mathcal{C}^{\perp},\ \mathcal{C} \text{ mod } 2 = C\}/\sim$$
$$\overset{1:1}{\longleftrightarrow} \{\text{orbits of } \mathrm{Aut}(C) \text{ on } V/W\}$$

Hopefully leads to the classification of $F \subset L$.