Triply Even Binary Codes and Their Application to Framed Vertex Operator Algebras

Akihiro Munemasa[1]

[1]Graduate School of Information Sciences
Tohoku University
Sendai, 980-8579 JAPAN

October 30, 2009

Even, Doubly Even, and Triply Even Codes

- $\mathbb{F}_2 = \{0, 1\}$: field of two elements,
- $\mathrm{wt}(\boldsymbol{x}) = |\{i \mid x_i = 1\}|$, where $\boldsymbol{x} = (x_1, \dots, x_n) \in \mathbb{F}_2^n$,
- $\ell : \mathbb{F}_2^n \to \mathbb{F}_2$, $\ell(\boldsymbol{x}) = \mathrm{wt}(\boldsymbol{x}) \bmod 2$,
- $q : \mathrm{Ker}\,\ell \to \mathbb{F}_2$, $q(\boldsymbol{x}) = (\frac{\mathrm{wt}(\boldsymbol{x})}{2} \bmod 2)$,
- $c : U \to \mathbb{F}_2$, $U \subset q^{-1}(0)$, $c(\boldsymbol{x}) = (\frac{\mathrm{wt}(\boldsymbol{x})}{4} \bmod 2)$,
- a subspace $D \subset c^{-1}(0)$ is called a triply even code. In other words, $8 | \mathrm{wt}(\boldsymbol{x})$ for all $\boldsymbol{x} \in D$.

Problem Describe all maximal triply even codes.

Triangular Graph T_m

Let $m = 4k + 2$, where k is a positive integer. Define an $\binom{m}{2} \times \binom{m}{2}$ matrix A by

$$\begin{array}{cc} & \{i,j\} \in \binom{m}{2} \\ \{k,l\} \in \binom{m}{2} & \boxed{\quad 1 \text{ or } 0 \quad} \end{array} \qquad \begin{cases} 1 & |\{i,j\} \cap \{k,l\}| = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem (Betsumiya–M.)

Let C be the linear span over $\mathbb{F}_2$ of the rows of A. Then $\dim C = m - 1$ and C is a maximal triply even code.

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$(L) = Co_0$
- B. Fischer, R. Griess (1982): The Monster $\mathbb{M}$
- I. Frenkel, J. Lepowsky and A. Meurman (1988): moonshine module $V^\natural$, with Aut$(V^\natural) = \mathbb{M}$.

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

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:

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

$(23+24) \times 24$ matrix

Bonnecaze-Calderbank-Solé (1995)

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

L = Leech lattice

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

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

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

Binary Codes

A linear subspace of $\mathbb{F}_2^n$ is called a (binary) code of length n.
A code C is said to be

- even, if $2 | \operatorname{wt}(u)\ \forall u \in C$,
- doubly even, if $4 | \operatorname{wt}(u)\ \forall u \in C$,
- triply even, if $8 | \operatorname{wt}(u)\ \forall u \in C$,
- $C^\perp = \{u \in \mathbb{F}_2^n \mid (u, v) = 0\ \forall v \in C\}$.

S_n acts on $\mathbb{F}_2^n$ by permutation of coordinates.
Equivalence of codes is defined by the action of S_n.
$n = 24$: there are 9 maximal doubly even codes up to S_{24}.

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

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):
$L \rightsquigarrow D_7 \subset \mathbb{F}_2^{48} \rightsquigarrow V^\natural$.

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

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

where $D \subset \mathbb{F}_2^{48}$.
$L(1/2,0)^{\otimes 48} \cong \mathcal{T} \subset V^\natural$: not unique $\implies$ D: depends on $\mathcal{T}$ (Virasoro frame), but:

$$D\text{: triply even, } \mathbf{1}_{48} \in D.$$

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

Dong–Mason–Zhu (1994)

$$L \supset F = \bigoplus_{i=1}^{24} \mathbb{Z} f_i: \text{ 4-frame}$$

$$\to V^\natural \supset \mathcal{T} \cong L(1/2, 0)^{\otimes 48}: \text{ Virasoro frame}$$

$$V^\natural = \bigoplus_{\beta \in D} V^\beta \text{ as } \mathcal{T}\text{-modules}$$

$$D = \text{structure code of } \mathcal{T}$$

$$= \mathcal{D}(L/F \bmod 2).$$

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 $V^\natural$

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

The diagram commutes, and

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

Theorem (Betsumiya–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 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–M.)

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

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

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

Summary

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

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

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

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

Problem remains:

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