Binary codes related to the moonshine vertex operator algebra

Akihiro Munemasa[1]

[1]Graduate School of Information Sciences
Tohoku University
(in collaboration with K. Betsumiya, R. A. L. Betty, M. Harada and C. H. Lam)

May 21, 2011
MSP Annual Convention 2011
University of Santo Tomas
Manila

Group Theory

Starting from very small set of axioms

- $\cdot : G \times G \to G$, $(a, b) \mapsto a \cdot b$,
- associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- $\exists$ identity $1 \in G$, $a \cdot 1 = 1 \cdot a = a$,
- $\exists$ inverse: $\forall a \in G$, $\exists b \in G$, $a \cdot b = b \cdot a = 1$.

The goal of finite group theory is to understand the set of all finite G satisfying the axioms, in some reasonable manner.

Finite Group Theory

Finite group theory has its origin in the remarkable work of É. Galois who proved that the occurrence of a non-abelian simple group caused impossibility of solvability by radical of polynomial equations of degree ≥ 5.

- A group G is simple if $\nexists$ normal subgroup N with $\{1\} \neq N \neq G$,
- N is normal in $G \iff \forall a \in G$, $aN = Na$,
- Example: $A_5 =$ symmetry group of icosahedron

Burnside (1915) further developed finite group theory.

Finite Simple Groups

- Chevalley (1955) systematically constructed finite groups of Lie type. Steinberg, Ree, Suzuki found more families.

There are 26 sporadic ones.

- E. Mathieu (1861, 1873), E. Witt (1938): $(\mathrm{Aut}($Steiner system $S(5,8,24)) = M_{24})$, M.J.E. Golay (1949): $(\mathrm{Aut}($Golay code$) = M_{24})$
- B. Fischer, R. Griess (1982): The Monster $\mathbb{M}$, I. Frenkel, J. Lepowsky and A. Meurman (1988): $\mathrm{Aut}(V^\natural) = \mathbb{M}$. $V^\natural =$ moonshine vertex operator algebra (VOA).

The smallest among 26 is the Mathieu group M_{11} of order

$$11 \cdot 10 \cdot 9 \cdot 8 = 7920,$$

the largest is $\mathbb{M}$ of order

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

Decompositions of $V^\natural$

$$V^\natural = \bigoplus_{n=0}^{\infty} V_n$$

infinite sum of finite-dimensional subspaces.

$$\dim V_0 = 1,\ \dim V_1 = 0,$$
$$V_2 = \text{Griess algebra}, \quad \dim V_2 = 196884.$$

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots$$

This coincidence lead to Conway–Norton conjecture, proved by R. Borcherds (1992).
The smallest matrix representation of $\mathbb{M}$ has dimension 196883. R. Wilson found an explicit 196882-dimensional matrix representation of $\mathbb{M}$ over $\mathbb{F}_2 = \{0, 1\} = \mathbb{Z}/2\mathbb{Z}$.

Decompositions of $V^\natural$

Instead of

$$V^\natural = \bigoplus_{n=0}^{\infty} V_n$$

infinite sum of finite-dimensional subspaces,

$$V^\natural = \bigoplus_{\alpha \in \mathbb{F}_2^{48}} V^\alpha$$

finite sum of infinite-dimensional subspaces.
Lam–Yamauchi (2008): every Virasoro frame (certain subalgebra of $V^\natural$) gives rise to such a decomposition.

$$D = \{\alpha \in \mathbb{F}_2^{48} \mid V^\alpha \neq 0\}$$

is called the structure code of the Virasoro frame.
There are only finitely many Virasoro frames, and D is invariant under $\mathbb{M}$.

Code

Let m be an integer (actually we need only $m = 2$ (binary) and $m = 4$).

A subgroup $C \subset (\mathbb{Z}/m\mathbb{Z})^n$ is called a code of length n over $\mathbb{Z}/m\mathbb{Z}$. The dual $C^\perp$ of a code C is

$$C^\perp = \{x \in (\mathbb{Z}/m\mathbb{Z})^n \mid (x, y) = 0 \quad (\forall y \in C)\}.$$

- $m = 4$, $\mathcal{C} \subset (\mathbb{Z}/4\mathbb{Z})^n$ is type II if $\mathcal{C} = \mathcal{C}^\perp$, $\sum_{i=1}^n x_i^2 \equiv 0 \pmod 8$ for all $x \in \mathcal{C}$, and for $n = 24$, $\mathcal{C}$ is extremal if $\sum_{i=1}^n x_i^2 > 8$,
- $m = 2$, $C \subset (\mathbb{Z}/2\mathbb{Z})^n$ is doubly even if $\mathrm{wt}(x) = |\{i \mid x_i = 1\}| \equiv 0 \pmod 4$ for all $x \in C$,
- $m = 2$, $D \subset (\mathbb{Z}/2\mathbb{Z})^n$ is triply even if $\mathrm{wt}(x) = |\{i \mid x_i = 1\}| \equiv 0 \pmod 8$ for all $x \in D$.

Equivalence: permutation of coordinates, and multiplication by -1 on some coordinates $(m = 4)$.

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

An extremal type II code of length 24 over $\mathbb{Z}/4\mathbb{Z}$ is generated by the rows of:

$$\begin{bmatrix} 1 & \boxed{\quad f(X) \quad} & & \\ 1 & & \boxed{\quad f(X) \quad} & \\ 1 & & & \boxed{\quad f(X) \quad} \\ \vdots & & & \ddots \end{bmatrix}$$

23×24 matrix
Bonnecaze-Calderbank-Solé (1995)
(construction of the Leech lattice)

$\overline{f}(X) = f(X) \bmod 2$. Golay code (a doubly even code of length 24) is generated by the rows of:

$$\begin{bmatrix} 1 & \boxed{\quad \overline{f}(X) \quad} & & \\ 1 & & \boxed{\quad \overline{f}(X) \quad} & \\ 1 & & & \boxed{\quad \overline{f}(X) \quad} \\ \vdots & & & \ddots \end{bmatrix}$$

over $\mathbb{F}_2$
(mod 2 reduction)

Codes and Virasoro frames

Theorem (Dong–Mason–Zhu (1994))

$$\{\text{extremal type II code of length } 24 \text{ over } \mathbb{Z}/4\mathbb{Z}\ \}$$
$$\to \{\text{Virasoro frames } V^\natural\}$$

Theorem (Lam–Yamauchi (2008))

$$\{\text{Virasoro frames of } V^\natural\}$$
$$\xrightarrow{\text{str}} \{\text{binary triply even codes of length } 48\} \quad V^\natural = \bigoplus_{\alpha \in D} V^\alpha$$

- Actually these mapping induce mappings of equivalence classes.
- What happens if we compose these two mappings?

Composition of the two mappings gives a mapping from codes to codes

$$\begin{array}{ccc}
\begin{array}{c}\{\text{Virasoro frames of } V^\natural\} \\ \text{difficult}\end{array} & \xrightarrow{\text{str}} & \left\{\begin{array}{l}\text{binary} \\ \text{triply even codes} \\ \text{of length } 48\end{array}\right\} \\
\uparrow \text{DMZ} & & \\
\left\{\begin{array}{l}\text{extremal type II codes} \\ \text{of length } 24 \\ \text{over } \mathbb{Z}/4\mathbb{Z}\end{array}\right\} & &
\end{array}$$

There must be a easier description of the composition mapping.

Commutative Diagram

Lam–Yamauchi (2008): $\text{str} \circ \text{DMZ} = \mathcal{D} \circ \mathrm{Res}$.

$$
\begin{array}{ccc}
\{\text{Virasoro frames of } V^\natural\} & \xrightarrow{\text{str}} & \left\{ \begin{array}{l} \text{binary} \\ \text{triply even codes} \\ \text{of length } 48 \end{array} \right\} \\
\text{difficult} & & \\
\uparrow \text{DMZ} & & \uparrow \mathcal{D} \text{ (doubling)} \\
\left\{ \begin{array}{l} \text{extremal type II codes} \\ \text{of length } 24 \\ \text{over } \mathbb{Z}/4\mathbb{Z} \end{array} \right\} & \xrightarrow{\mathrm{Res}} & \left\{ \begin{array}{l} \text{binary} \\ \text{doubly even codes} \\ \text{of length } 24 \end{array} \right\}
\end{array}
$$

$\mathrm{Res}(\mathcal{C})$ and $\mathcal{D}$

If $\mathcal{C}$ is a code over $\mathbb{Z}/4\mathbb{Z}$, then its modulo 2 reduction is called the residue code and is denoted by

$$\mathrm{Res}(\mathcal{C}) \subset (\mathbb{Z}/2\mathbb{Z})^n = \mathbb{F}_2^n.$$

Let $C = \mathrm{Span}_{\mathbb{F}_2}(A)$ be the binary code of length n spanned by the row vectors of a $k \times n$ matrix A. The doubling of C is defined by

$$\mathcal{D}(C) = \mathrm{Span}_{\mathbb{F}_2} \begin{bmatrix} A & A \\ \mathbf{1}_n & 0 \\ 0 & \mathbf{1}_n \end{bmatrix},$$

where $\mathbf{1}_n = (1, 1, \ldots, 1)$.
If C is doubly even and $8|n$, then $\mathcal{D}(C)$ is a triply even code of length $2n$. In particular,

$$\{\text{doubly even code of length 24}\} \xrightarrow{\mathcal{D}} \{\text{triply even code of length 48}\}$$

Commutative Diagram

$$\begin{array}{ccc}
\{\text{Virasoro frames of } V^\natural\} & \xrightarrow{\text{str}} & \left\{\begin{array}{l}\text{binary} \\ \text{triply even codes} \\ \text{of length } 48\end{array}\right\} \\
\text{difficult} & & \\
\uparrow \text{DMZ} & & \uparrow \mathcal{D} \text{ (doubling)} \\
\left\{\begin{array}{l}\text{extremal type II codes} \\ \text{of length } 24 \\ \text{over } \mathbb{Z}/4\mathbb{Z}\end{array}\right\} & \xrightarrow{\mathrm{Res}} & \left\{\begin{array}{l}\text{binary} \\ \text{doubly even codes} \\ \text{of length } 24\end{array}\right\}
\end{array}$$

Harada–Lam–M. (2010):

$$\begin{aligned}
\text{str}^{-1}(\mathcal{D}(\{\text{doubly even}\})) &\overset{(\supset)}{=} \text{str}^{-1}(\mathcal{D} \circ \mathrm{Res}(\{\text{extremal type II}\})) \\
&\overset{(\supset)}{=} \text{DMZ}(\{\text{extremal type II}\})
\end{aligned}$$

all coincide.

$$
\begin{array}{ccc}
\begin{array}{c}\{\text{Virasoro frames of } V^\natural\} \\ \text{difficult}\end{array} & \xrightarrow{\text{str}} & \left\{\begin{array}{l}\text{binary} \\ \text{triply even codes} \\ \text{of length } 48\end{array}\right\} \\
\uparrow \text{DMZ} & & \uparrow \mathcal{D} \text{ (doubling)} \\
\left\{\begin{array}{l}\text{extremal type II codes} \\ \text{of length } 24 \\ \text{over } \mathbb{Z}/4\mathbb{Z}\end{array}\right\} & \xrightarrow{\text{Res}} & \left\{\begin{array}{l}\text{binary} \\ \text{doubly even codes} \\ \text{of length } 24\end{array}\right\}
\end{array}
$$

Pless–Sloane (1975) enumerated maximal (all have dimension 12) members of

$$\{\text{binary doubly even codes of length } 24\}.$$

$$
\begin{array}{ccc}
\begin{array}{c}\{\text{Virasoro frames of } V^\natural\}\\ \text{difficult}\end{array} & \xrightarrow{\text{str}} & \left\{\begin{array}{l}\text{binary}\\ \text{triply even codes}\\ \text{of length } 48\end{array}\right\}\\
\uparrow \text{DMZ} & & \uparrow \mathcal{D} \text{ (doubling)}\\
\left\{\begin{array}{l}\text{extremal type II codes}\\ \text{of length } 24\\ \text{over } \mathbb{Z}/4\mathbb{Z}\end{array}\right\} & \xrightarrow{\mathrm{Res}} & \left\{\begin{array}{l}\text{binary}\\ \text{doubly even codes}\\ \text{of length } 24\end{array}\right\}
\end{array}
$$

Betsumiya–M. (2010) enumerated maximal (dimension $\{9, 13, 14, 15\}$) members of

$$\{\text{binary triply even codes of length } 48\}.$$

Theorem (Betsumiya–M., 2010)

Let D be a maximal binary triply even code of length 48. Then

- $\exists$ doubly even codes C_1, C_2 of length 24,
- $\exists$ linear isomorphism $f : C_1/R_1 \to C_2/R_2$, where

$$R_i = \{\boldsymbol{x} \in (C_i * C_i)^{\perp} \mid \mathrm{wt}(\boldsymbol{x}) \equiv 0 \pmod 8 \\ \mathrm{wt}(\boldsymbol{x} * \boldsymbol{y}) \equiv 0 \pmod 4)(\forall \boldsymbol{y} \in C_i)\} \subset C_i \quad (i = 1, 2),$$

satisfying

$$\boldsymbol{x}_1 \in C_1,\ \boldsymbol{x}_2 + R_2 \in f(\boldsymbol{x}_1 + R_1) \implies \mathrm{wt}(\boldsymbol{x}_1) \equiv \mathrm{wt}(\boldsymbol{x}_2) \pmod 8,$$

such that

$$D \cong \{(\boldsymbol{x}_1\ \boldsymbol{x}_2) \mid \boldsymbol{x}_1 \in C_1,\ \boldsymbol{x}_2 + R_2 \in f(\boldsymbol{x}_1 + R_1)\}.$$

Remark Taking $C_1 = C_2$, $f =$ identity gives $\mathcal{D}(C_1)$.

Theorem (Betsumiya–M., 2010)

Every maximal member of

$$\left\{ \begin{array}{l} \text{binary triply even} \\ \text{code of length 48} \end{array} \right\}$$

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.

$$
\begin{array}{ccc}
\begin{array}{c}\{\text{Virasoro frames of } V^\natural\}\\ \text{difficult}\end{array} & \xrightarrow{\text{str}} & \left\{\begin{array}{l}\text{binary}\\ \text{triply even codes}\\ \text{of length } 48\end{array}\right\}\\
\uparrow \text{DMZ} & & \uparrow \mathcal{D}\ \text{(doubling)}\\
\left\{\begin{array}{l}\text{extremal type II codes}\\ \text{of length } 24\\ \text{over } \mathbb{Z}/4\mathbb{Z}\end{array}\right\} & \xrightarrow{\mathrm{Res}} & \left\{\begin{array}{l}\text{binary}\\ \text{doubly even codes}\\ \text{of length } 24\end{array}\right\}
\end{array}
$$

Betsumiya created database of

$$\{\text{binary triply even codes of length } 48\}.$$

http://www.st.hirosaki-u.ac.jp/~betsumi/triply-even/

$$
\begin{array}{ccc}
\begin{array}{c}\{\text{Virasoro frames of } V^{\natural}\}\\ \text{difficult}\end{array} & \xrightarrow{\text{str}} & \left\{\begin{array}{l}\text{binary}\\ \text{triply even codes}\\ \text{of length } 48\end{array}\right\} \\
\uparrow \text{DMZ} & & \uparrow \mathcal{D} \text{ (doubling)} \\
\left\{\begin{array}{l}\text{extremal type II codes}\\ \text{of length } 24\\ \text{over } \mathbb{Z}/4\mathbb{Z}\end{array}\right\} & \xrightarrow{\mathrm{Res}} & \left\{\begin{array}{l}\text{binary}\\ \text{doubly even codes}\\ \text{of length } 24\end{array}\right\}
\end{array}
$$

$$\left\{\begin{array}{l}\text{extremal type II codes}\\ \text{of length } 24\\ \text{over } \mathbb{Z}/4\mathbb{Z}\end{array}\right\} \xrightarrow{\mathrm{Res}} \left\{\begin{array}{l}\text{binary}\\ \text{doubly even codes}\\ \text{of length } 24\end{array}\right\}$$

For each binary doubly even C, classify $\mathcal{C}$ such that $\mathrm{Res}\,\mathcal{C} = C$. The map Res is neither injective nor surjective.

- Calderbank–Sloane (with Young) (1997): $\dim C = 12 \implies C \in$ image of Res.
- Rains (1999) determined the preimage for $C =$ Golay.
- Dong–Griess–Höhn (1998) found a code C of dimension 6 in the image of Res, and Harada–Lam–M. (2010) showed its preimage is unique.
- The image was determined by Harada–Lam–M. (2010), but not preimages.

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.

Enumeration by Betty–M. (2010)

The number of doubly even codes $C \subset \mathbb{F}_2^{24}$ containing $\mathbf{1}$ and $C^\perp$ has minimum weight ≥ 4, and the number of extremal type II codes $\mathcal{C} \subset (\mathbb{Z}/4\mathbb{Z})^{24}$ with $\mathrm{Res}\,\mathcal{C} = C$.

dim	6	7	8	9	10	11	12
doubly even	1	7	32	60	49	21	9
extremal type II	1	5	31	178	764	1886	1903
	1						13

$$\left\{ \begin{array}{l} \text{extremal type II codes} \\ \text{of length } 24 \\ \text{over } \mathbb{Z}/4\mathbb{Z} \end{array} \right\} \xrightarrow{\mathrm{Res}} \left\{ \begin{array}{l} \text{binary} \\ \text{doubly even codes} \\ \text{of length } 24 \end{array} \right\}$$