Triply even codes binary codes, lattices and framed vertex operator algebras

Akihiro Munemasa[1]

[1]Graduate School of Information Sciences
Tohoku University
(joint work with Koichi Betsumiya, Masaaki Harada and Ching-Hung Lam)

July 12, 2010
AGC2010, Gyeongju, Korea

The Hamming graph $H(n, q)$

- vertex set $= F^n$, $|F| = q$.
- $\boldsymbol{x} \sim \boldsymbol{y} \iff \boldsymbol{x}$ and $\boldsymbol{y}$ differ at one position.

$H(n, q)$ is a distance-regular graph.
When $q = 2$, we may take $F = \mathbb{F}_2$. $H(n, 2) = n$-cube.

$$\begin{aligned} \mathrm{wt}(\boldsymbol{x}) &= \text{ distance between } \boldsymbol{x} \text{ and } \mathbf{0} \\ &= \text{ number of 1's in } \boldsymbol{x} \\ \text{A binary code} &= \text{a subset of } \mathbb{F}_2^n \\ &= \text{a subset of the vertex set of } H(n,2) \\ \text{A binary linear code} &= \text{a linear subspace of } \mathbb{F}_2^n \\ \text{A codeword} &= \text{an element of a code} \end{aligned}$$

Simplex codes

The row vectors of the matrix

$$G = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

generate the $[7, 3, 4]$ simplex code $\subset \mathbb{F}_2^7$.

- Columns $=$ points of $PG(2, 2)$,
- Nonzero codewords $=$ complement of lines of $PG(2, 2)$.

$$\begin{bmatrix} 0 \cdots 0 & 1 & 1 \cdots 1 \\ G & 0 & G \end{bmatrix} \rightarrow$$

columns $=$ points
nonzero codewords
$=$ complement of planes

of $PG(3, 2)$.

generate the $[15, 4, 8]$ simplex code. 15 nonzero codewords of weight 8.

$[15, 4, 8]$ simplex code also comes from a Johnson graph $J(v, d)$

- vertex set $= \binom{V}{k}$, $|V| = v$.
- $A \sim B \iff A$ and B differ by one element.

$J(v, d)$ is a distance-regular graph.
$d = 2$: $T(m) = J(m, 2)$ (triangular graph) is a strongly regular graph.
$m = 6$: the adjacency matrix of $T(6)$ is a 15×15 matrix.
Since $T(6) = \mathrm{srg}(15, 8, 4, 4)$,

- every row has weight 8,
- every pair of rows has 1 in common 4 positions.

In fact, its row vectors are precisely the nonzero codewords of the $[15, 4, 8]$ simplex code.

Triple intersection numbers

- Γ: graph, α, β, γ: vertices of Γ
- $\Gamma(\alpha)$: the set of neighbors of a vertex α.

The triple intersection numbers of Γ are

$$|\Gamma(\alpha) \cap \Gamma(\beta) \cap \Gamma(\gamma)| \quad (\alpha, \beta, \gamma : \text{ distinct}).$$

For $\Gamma = T(6)$, the triple intersection numbers are $0, 2$ only.
Note: Γ is not "triply regular": $|\Gamma(\alpha) \cap \Gamma(\beta) \cap \Gamma(\gamma)| = 0, 2$ even for pairwise adjacent α, β, γ.

- "Double" intersection numbers $|\Gamma(\alpha) \cap \Gamma(\beta)| = \lambda, \mu = 4$.
- "Single" intersection numbers $|\Gamma(\alpha)| = k = \text{valency} = 8$.

Even, doubly even, and triply even codes

A binary linear code C is called

$$\begin{aligned} \text{even} &\iff \mathrm{wt}(\boldsymbol{x}) \equiv 0 \pmod 2 \quad (\forall \boldsymbol{x} \in C) \\ \text{doubly even} &\iff \mathrm{wt}(\boldsymbol{x}) \equiv 0 \pmod 4 \quad (\forall \boldsymbol{x} \in C) \\ \text{triply even} &\iff \mathrm{wt}(\boldsymbol{x}) \equiv 0 \pmod 8 \quad (\forall \boldsymbol{x} \in C) \end{aligned}$$

The $[15, 4, 8]$ simplex code is a triply even code.

- $\ell : \mathbb{F}_2^n \to \mathbb{F}_2$, $\ell(\boldsymbol{x}) = \mathrm{wt}(\boldsymbol{x})$ mod 2 (linear)
- $q : \mathrm{Ker}\,\ell \to \mathbb{F}_2$, $q(\boldsymbol{x}) = (\frac{\mathrm{wt}(\boldsymbol{x})}{2}$ mod 2) (quadratic)
- $c : U \to \mathbb{F}_2$, $U \subset q^{-1}(0)$, $c(\boldsymbol{x}) = (\frac{\mathrm{wt}(\boldsymbol{x})}{4}$ mod 2) (cubic)

A triply even code is a set of zeros of the cubic form c.

triply even $\iff$ $\mathrm{wt}(\boldsymbol{x}) \equiv 0 \pmod 8 \quad (\forall \boldsymbol{x} \in C)$

If C is generator by a set of vectors $r_1, \dots, r_n$, then C is triply even iff, (denoting by $*$ the entrywise product)

(i) $\mathrm{wt}(r_h) \equiv 0 \pmod 8$

(ii) $\mathrm{wt}(r_h * r_i) \equiv 0 \pmod 4$

(iii) $\mathrm{wt}(r_h * r_i * r_j) \equiv 0 \pmod 2$

for all $h, i, j \in \{1, \dots, n\}$. If C is generated by the row vectors of the adjacency matrix of a strongly regular graph Γ, then C is triply even iff

(i) $k \equiv 0 \pmod 8$

(ii) $\lambda, \mu \equiv 0 \pmod 4$

(iii) all triple intersection numbers are $\equiv 0 \pmod 2$

For $\Gamma = T(m)$, (i)–(iii) $\iff$ $m \equiv 2 \pmod 4$.

The binary code T_m of the triangular graph $T(m)$

(i) Brouwer-Van Eijl (1992): $\dim T_m = m - 2$ if $m \equiv 0 \pmod 2$.

(ii) Betsumiya-M.: T_m is a triply even code iff $m \equiv 2 \pmod 4$, maximal for its length.

(ii): $k = 2(m-2) \equiv 0 \pmod 8 \implies$ "only if." "if" part requires $\lambda = m - 2$, $\mu = 4$, and the triple intersection numbers. Proving maximality requires more work.
Let

$$\tilde{T}_m = \begin{bmatrix} \mathbf{1}_n \\ T_m; 0 \end{bmatrix}$$

where $n = 8\lceil \frac{1}{8} \frac{m(m-1)}{2} \rceil$ (for example, $m = 6 \implies n = 16$).

(iii) Betsumiya-M.: $\tilde{T}_m$ is a maximal triply even code.

From the $[15, 4, 8]$ simplex code T_6 to...

$$\tilde{T}_6 = \begin{bmatrix} \mathbf{1}_{16} \\ [15,4,8];0 \end{bmatrix} \rightsquigarrow \begin{array}{l} [16,5,8] \text{ Reed–Muller code} \\ R = RM(1,4) \end{array}$$

A triply even code appeared in the construction of the moonshine module $V^\natural$ (a vertex operator algebra with automorphism group Fischer–Griess Monster simple group), due to Dong–Griess–Höhn (1998), Miyamoto (2004).

$$\begin{bmatrix} \mathbf{1}_{16} & 0 & 0 \\ 0 & \mathbf{1}_{16} & 0 \\ 0 & 0 & \mathbf{1}_{16} \\ R & R & R \end{bmatrix} \quad (8 \times 48 \text{ matrix})$$

is a triply even $[48, 7, 16]$ code.

The extended doubling

Note

$$R = RM(1,4) = \begin{bmatrix} \mathbf{1}_8 & 0 \\ RM(1,3) & RM(1,3) \end{bmatrix}$$

and $RM(1,3)$ is doubly even. In general, we define the extended doubling of a code C of length n to be

$$\mathcal{D}(C) = \begin{bmatrix} \mathbf{1}_n & 0 \\ C & C \end{bmatrix}$$

If C is doubly even and $n \equiv 0 \pmod 8$, then $\mathcal{D}(C)$ is triply even.

If C is an indecomposable doubly even self-dual code, then $\mathcal{D}(C)$ is a maximal triply even code.

$\mathcal{D}$: doubly even length $n \longrightarrow$ triply even length $2n$, provided $8|n$.

$RM(1,4) = \mathcal{D}(RM(1,3))$ is the only maximal triply even code of length 16.
We slightly generalize the extended doubling

$$\mathcal{D}(C) = \begin{bmatrix} \mathbf{1}_n & 0 \\ C & C \end{bmatrix}$$

as

$$\tilde{\mathcal{D}}(C) = \bigoplus_{i=1}^{s} \mathcal{D}(C_i)$$

if C is the sum of indecomposable codes C_i

Every maximal triply even code of length 32 is of the form $\tilde{\mathcal{D}}(C)$ for some doubly even self-dual code of length 16.

A triply even code of length 48

Dong–Griess–Höhn (1998) and Miyamoto (2004) used (although not maximal):

$$\begin{bmatrix} \mathbf{1}_{16} & 0 & \\ 0 & \mathbf{1}_{16} & 0 \\ 0 & 0 & \mathbf{1}_{16} \\ R & R & R \end{bmatrix} = \begin{bmatrix} \mathbf{1}_8 & \mathbf{1}_8 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1}_8 & \mathbf{1}_8 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1}_8 & \mathbf{1}_8 \\ \mathbf{1}_8 & 0 & \mathbf{1}_8 & 0 & \mathbf{1}_8 & 0 \\ H & H & H & H & H & H \end{bmatrix}$$

$$\cong \begin{bmatrix} \mathbf{1}_8 & \mathbf{1}_8 & \mathbf{1}_8 & 0 & 0 & 0 \\ \mathbf{1}_8 & 0 & 0 & \mathbf{1}_8 & 0 & 0 \\ 0 & \mathbf{1}_8 & 0 & 0 & \mathbf{1}_8 & 0 \\ 0 & 0 & \mathbf{1}_8 & 0 & 0 & \mathbf{1}_8 \\ H & H & H & H & H & H \end{bmatrix} = \mathcal{D} \begin{bmatrix} \mathbf{1}_8 & 0 & 0 \\ 0 & \mathbf{1}_8 & 0 \\ 0 & 0 & \mathbf{1}_8 \\ H & H & H \end{bmatrix}$$

where $H = RM(1,3)$, so $R = \begin{bmatrix} \mathbf{1}_8 & 0 \\ H & H \end{bmatrix}$.

The triply even codes of length 48

The moonshine module $V^\natural$ is an infinite-dimensional algebra. However, it has finitely many (up to $\mathrm{Aut}\, V^\natural$) Virasoro frames $\mathcal{T}$, and $V^\natural$ is a sum of finitely many irreducible modules as a $\mathcal{T}$-module. To understand $V^\natural$: $\Longleftarrow$ classify Virasoro frames.

Virasoro frame $\mathcal{T}$ of $V^\natural \rightsquigarrow$ triply even code of length 48 (called the structure code of $\mathcal{T}$)

Theorem (Betsumiya-M.)

Every maximal triply even code of length 48 is equivalent to $\tilde{\mathfrak{D}}(C)$ for some doubly even self-dual code, or to $\tilde{T}_{10}$.

Question. Then which of the triply even codes of length 48 actually occurs as the structure code of a Virasoro frame of $V^\natural$?

Virasoro frame of $V^\natural$

$\rightsquigarrow$ triply even code D of length 48

Then

(i) $D^\perp$ has minimum weight at least 4.

(ii) $D^\perp$ is even, or equivalently, $\mathbf{1}_{48} \in D$.

(i) excludes all subcodes of $\tilde{T}_{10}$.

Theorem (Harada–Lam–M.)

If $D = \mathcal{D}(C)$ for some doubly even code C of length 24, then D is the structure code of a Virasoro frame of $V^\natural$ iff C is realizable as the binary residue code of an extremal type II $\mathbb{Z}_4$-code of length 24, i.e., there exist vectors $f_1, \dots, f_{24}$ of the Leech lattice L with $(f_i, f_j) = 4\delta_{ij}$ (called a 4-frame), and

$$C = \{\boldsymbol{x} \bmod 2 \mid \boldsymbol{x} \in \mathbb{Z}^n,\ \frac{1}{4}\sum_{i=1}^{24} x_i f_i \in L\}.$$

$L =$ Leech lattice

A doubly even code C of length 24 is realizable if there exists a 4-frame $f_1, \dots, f_{24}$ of the Leech lattice L, and

$$C = \{\boldsymbol{x} \bmod 2 \mid \boldsymbol{x} \in \mathbb{Z}^n,\ \frac{1}{4}\sum_{i=1}^{24} x_i f_i \in L\}.$$

The following lemma was useful in determining realizability.

Lemma

If C is realizable and $\boldsymbol{a} \in C^\perp \setminus C$ has weight 4, then $\langle C, \boldsymbol{a} \rangle$ is also realizable.

Using this lemma, we classified doubly even codes into realizable and non-realizable ones.

Extended doublings of doubly even codes of length 24

Numbers of inequivalent doubly even codes C of length 24 such that $\mathbf{1}_{24} \in C$ and the minimum weight of $C^\perp$ is ≥ 4.

Dimension	Total	Realizable	non-Realizable
12	9	9	0
11	21	21	0
10	49	47	2
9	60	46	14
8	32	20	12
7	7	5	2
6	1	1	0

$L =$ Leech lattice

$$\{\text{Virasoro frames of } V^\natural\} \xrightarrow{\text{str}} \left\{ \begin{array}{l} \text{triply even } D \\ \text{len} = 48,\ \mathbf{1}_{48} \in D \\ \min D^\perp \geq 4 \end{array} \right\}$$

most difficult

$\uparrow$ Dong Mason Zhu

$\uparrow \mathcal{D}$ (extended doubling)

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

easily enumerated

The diagram commutes, and

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