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

Akihiro Munemasa\textsuperscript{1}

\textsuperscript{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 $= F^n$, $|F| = q$.
- $x \sim y \iff x$ and $y$ 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.

$$\text{wt}(x) = \text{distance between } x \text{ and } 0$$
$$= \text{number of 1's in } x$$

A binary code $= \text{a subset of } \mathbb{F}_2^n$
$$= \text{a subset of the vertex set of } H(n, 2)$$

A binary linear code $= \text{a linear subspace of } \mathbb{F}_2^n$
A codeword $= \text{an element of a code}$
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 \(PG(2, 2)\).

\[
\begin{bmatrix}
0 \ldots 0 & 1 & 1 \ldots 1 \\
G & 0 & G \\
\end{bmatrix}
\]

\(\rightarrow\) columns = points
nonzero codewords = complement of planes

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 \( = \binom{V}{k}, |V| = v. \)
- \( A \sim B \iff A \text{ and } B \text{ differ by one element.} \)

\( J(v, d) \) 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 \( 15 \times 15 \) matrix.

Since \( T(6) = \text{srg}(15, 8, 4, 4), \)

- 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

- $\Gamma$: graph, $\alpha, \beta, \gamma$: vertices of $\Gamma$
- $\Gamma(\alpha)$: the set of neighbors of a vertex $\alpha$

The triple intersection numbers of $\Gamma$ 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: $\Gamma$ is not “triply regular”: $|\Gamma(\alpha) \cap \Gamma(\beta) \cap \Gamma(\gamma)| = 0, 2$ even for pairwise adjacent $\alpha, \beta, \gamma$.

- “Double” intersection numbers $|\Gamma(\alpha) \cap \Gamma(\beta)| = \lambda, \mu = 4$.
- “Single” intersection numbers $|\Gamma(\alpha)| = k = \text{valency} = 8$. 
A binary linear code $C$ is called

\[
\text{even } \iff \text{wt}(x) \equiv 0 \pmod{2} \quad (\forall x \in C)
\]

\[
\text{doubly even } \iff \text{wt}(x) \equiv 0 \pmod{4} \quad (\forall x \in C)
\]

\[
\text{triply even } \iff \text{wt}(x) \equiv 0 \pmod{8} \quad (\forall x \in C)
\]

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

- $\ell : F_2^n \to F_2$, $\ell(x) = \text{wt}(x) \mod 2$ (linear)
- $q : \text{Ker} \ell \to F_2$, $q(x) = (\frac{\text{wt}(x)}{2} \mod 2)$ (quadratic)
- $c : U \to F_2$, $U \subset q^{-1}(0)$, $c(x) = (\frac{\text{wt}(x)}{4} \mod 2)$ (cubic)

A triply even code is a set of zeros of the cubic form $c$. 
triply even $\iff \text{wt}(x) \equiv 0 \pmod{8} \quad (\forall x \in C)$

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

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

(ii) $\text{wt}(r_h \ast r_i) \equiv 0 \pmod{4}$

(iii) $\text{wt}(r_h \ast r_i \ast r_j) \equiv 0 \pmod{2}$

for all $h, i, j \in \{1, \ldots, n\}$. If $C$ is generated by the row vectors of the adjacency matrix of a strongly regular graph $\Gamma$, 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): $k = 2(m - 2) \equiv 0 \pmod{8} \implies \text{“only if.” “if” part requires } \lambda = m - 2, \mu = 4, \text{ and the triple intersection numbers. Proving maximality requires more work.}$

Let

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

where $n = 8\left\lceil \frac{1}{8} \frac{m(m-1)}{2} \right\rceil$ (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...

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

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

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

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

Note

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

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

\[ D(C) = \begin{bmatrix} 1^n & 0 \\ C & C \end{bmatrix} \]

If \( C \) is doubly even and \( n \equiv 0 \pmod{8} \), then \( D(C) \) is triply even.
If \( C \) is an indecomposable doubly even self-dual code, then \( D(C) \) is a maximal triply even code.
\( \mathcal{D} \): doubly even length \( n \rightarrow \) triply even length \( 2n \), provided \( 8 \mid n \).

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

We slightly generalize the extended doubling

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

as

\[
\tilde{\mathcal{D}}(C') = \bigoplus_{i=1}^s \mathcal{D}(C_i) \quad \text{if} \ C \text{ is the sum of indecomposable codes } C_i
\]

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


\[
\begin{bmatrix}
1_{16} & 0 \\
0 & 1_{16} \\
0 & 0 & 1_{16} \\
R & R & R
\end{bmatrix}
= \begin{bmatrix}
1_8 & 1_8 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1_8 & 1_8 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1_8 & 1_8 & 1_8 \\
H & H & H & H & H & H & H
\end{bmatrix}
\]

\[
\Rightarrow \begin{bmatrix}
1_8 & 1_8 & 1_8 & 0 & 0 & 0 \\
1_8 & 0 & 0 & 1_8 & 0 & 0 \\
0 & 1_8 & 0 & 0 & 1_8 & 0 \\
0 & 0 & 1_8 & 0 & 0 & 1_8 \\
H & H & H & H & H & H
\end{bmatrix}
= \mathcal{D} \begin{bmatrix}
1_8 & 0 & 0 \\
0 & 1_8 & 0 \\
0 & 0 & 1_8 \\
H & H & H
\end{bmatrix}
\]

where \( H = RM(1, 3) \), so \( R = \begin{bmatrix}
1_8 & 0 \\
H & H
\end{bmatrix} \).
The triply even codes of length 48

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

Virasoro frame $\mathcal{T}$ of $V^\mathbb{Z}$ \(\rightsquigarrow\) 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 $\tilde{\mathcal{D}}(C')$ 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 $V^\mathbb{Z}$?
Virasoro frame of $V^h$

$\leadsto$ triply even code $D$ of length 48

Then

(i) $D^\perp$ has minimum weight at least 4.
(ii) $D^\perp$ is even, or equivalently, $1_{48} \in D$.

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

Theorem (Harada–Lam–M.)

If $D = D(C)$ for some doubly even code $C$ of length 24, then $D$ is the structure code of a Virasoro frame of $V^h$ 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 $f_1, \ldots, f_{24}$ of the Leech lattice $L$ with $(f_i, f_j) = 4\delta_{ij}$ (called a 4-frame), and

$$ C = \{ x \mod 2 \mid x \in \mathbb{Z}^n, \frac{1}{4} \sum_{i=1}^{24} x_if_i \in L \}. $$
$L = \text{Leech lattice}$

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

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

The following lemma was useful in determining realizability.

**Lemma**

If $C$ is realizable and $a \in C^\perp \setminus C$ has weight 4, then $\langle C, a \rangle$ 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 $1_{24} \in C$ and the minimum weight of $C^\perp$ is $\geq 4.$

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Total</th>
<th>Realizable</th>
<th>non-Realizable</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>9</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>21</td>
<td>21</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>49</td>
<td>47</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>60</td>
<td>46</td>
<td>14</td>
</tr>
<tr>
<td>8</td>
<td>32</td>
<td>20</td>
<td>12</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
\( L = \text{Leech lattice} \)

\{\text{Virasoro frames of } V^\oplus\} \quad \text{most difficult}

\rightarrow

\{ \text{triply even } D \}

\text{len} = 48, \quad 1_{48} \in D

\min D^\perp \geq 4

\uparrow \quad \text{(extended doubling)}

\uparrow \mathcal{D}

\{ \text{doubly even } C \}

\text{len} = 24, \quad 1_{24} \in C

\min C^\perp \geq 4

\text{easily enumerated}

The diagram commutes, and

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