Extremal type II $\mathbb{Z}_4$-codes of length 24 and triply even binary codes of length 48

Akihiro Munemasa

$^1$Graduate School of Information Sciences
Tohoku University

August 12, 2014
ICM 2014 Satellite Conference
on Algebraic Coding Theory
Ewha Womans University, Korea
\( L = \text{Leech lattice} \)

\[
\begin{align*}
\{\text{Virasoro frames of } V^h\} & \quad \text{most difficult} \\
\text{str} & \quad \begin{cases}
\text{triply even } D \\
\text{length } = 48, \ 1_{48} \in D \\
\text{min } D^\perp \geq 4
\end{cases} \\
\text{Dong} & \quad \text{(extended doubling)} \\
\uparrow & \quad \text{Mason} \\
\uparrow & \quad \text{Zhu} \\
\{\text{frames of } L\} & \quad \begin{cases}
\text{doubly even } C \\
\text{length } = 24, \ 1_{24} \in C \\
\text{min } C^\perp \geq 4 \\
\text{easily enumerated}
\end{cases}
\end{align*}
\]

The diagram commutes, and

\[
\text{DMZ}(\{\text{frames of } L\}) \supseteq \text{str}^{-1}(\mathcal{D}(\{\text{doubly even}\})).
\]
A binary linear code $C$ is called

- **even** $\iff \text{wt}(x) \equiv 0 \pmod{2} \quad (\forall x \in C)$
- **doubly even** $\iff \text{wt}(x) \equiv 0 \pmod{4} \quad (\forall x \in C)$
- **triply even** $\iff \text{wt}(x) \equiv 0 \pmod{8} \quad (\forall x \in C)$

If $C$ is generated by a set of vectors $r_1, \ldots, r_k$, then $C$ is **triply even** iff,

1. $\text{wt}(r_h) \equiv 0 \pmod{8}$
2. $\text{wt}(r_h \ast r_i) \equiv 0 \pmod{4}$
3. $\text{wt}(r_h \ast r_i \ast r_j) \equiv 0 \pmod{2}$

for all $h, i, j \in \{1, \ldots, k\}$. (denoting by $\ast$ the entrywise product)
Proposition

$C = \langle r_1, \ldots, r_k \rangle$ is triply even iff,

(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 $h, i, j \in \{1, \ldots, n\}$.

Proof.

Use induction on $k$. Note

$$\text{wt}(a + b + c) = \text{wt}(a) + \text{wt}(b) + \text{wt}(c)$$
$$- 2(\text{wt}(a \ast b) + \text{wt}(a \ast c) + \text{wt}(b \ast c))$$
$$+ 4 \text{wt}(a \ast b \ast c).$$
Examples of triply even codes

Let $C$ be a binary code of length $n$. Then the doubling
\(\{(x, x) \mid x \in C\}\) of $C$ is
- even
- doubly even if $C$ is even
- triply even if $C$ is doubly even

Moreover, the extended doubling

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

is
- even if $n \equiv 0 \pmod{2}$
- doubly even if $C$ is even and $n \equiv 0 \pmod{4}$
- triply even if $C$ is doubly even and $n \equiv 0 \pmod{8}$
Examples of triply even codes

\[ RM(1, 4) = D(e_8) = \begin{bmatrix} 1_8 & 0 \\ e_8 & e_8 \end{bmatrix} \]

where \( e_8 \) is the doubly even extended Hamming \([8, 4, 4]\) code.

- \( RM(1, 4) \) is the unique maximal triply even code of length 16 up to equivalence.
- If \( C \) is an indecomposable doubly even self-dual code, then \( D(C) \) is a maximal triply even code.
- Betsumiya and M. (2012) classified triply even codes of length up to 48: subcodes of direct sums of extended doublings, or the code spanned by the adjacency matrix of the triangular graph \( L(K_{10}) \) \((n = 45)\)
Virasoro frame of $V^\frac{1}{2}$

Theorem (Harada–Lam–M., 2013)

Let $C$ be doubly even, length 24, $\ni 1$. TFAE:

1. $\mathcal{D}(C)$ is the structure code of a Virasoro frame of $V^\frac{1}{2}$
2. 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

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

3. $C$ is the mod 2 residue of an extremal type II $\mathbb{Z}_4$-code of length 24

Type II $\iff$ self-dual & all Euclidean weight $\equiv 0 \pmod{8}$
Extremal $\iff$ minimum Euclidean weight 16.

We say $C$ is realizable if $C$ satisfies these conditions.
Realizable codes (Harada–Lam–M., 2013)

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>1+1+7</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>

$9 = $ Pless–Sloane (1975)
We say a doubly even code $C$ of length 24 is **realizable** if $C$ is the mod 2 residue of an extremal type II $\mathbb{Z}_4$-code of length 24.

realizable in only one way?

There may be more than one extremal type II code over $\mathbb{Z}_4$ whose residue is $C$.

**Theorem (Rains, 1999)**

If $C$ is the $[24, 12, 8]$ binary Golay code, then there are exactly **13** extremal type II code over $\mathbb{Z}_4$ whose residue is $C$. 

\[\text{Akihiro Munemasa} \quad \text{Triply even codes}\]
Classification of extremal type II codes over $\mathbb{Z}_4$

**Theorem (Betty and M.)**

The number of extremal type II code over $\mathbb{Z}_4$ with residue $C$ is

<table>
<thead>
<tr>
<th>dim $C$</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td># $C$</td>
<td>1</td>
<td>7</td>
<td>32</td>
<td>60</td>
<td>49</td>
<td>21</td>
<td>9</td>
</tr>
<tr>
<td>#</td>
<td>1</td>
<td>5</td>
<td>29</td>
<td>171</td>
<td>755</td>
<td>1880</td>
<td>1890+13</td>
</tr>
</tbody>
</table>

- Computation is easy if dim $C$ is small.
- Rains used special property of the Golay code.
- Computation for the other codes with dim $C = 12$ were hard.

For the method, visit ICM and see the Poster of Rowena Betty.
A \textit{k-frame} of a lattice $L$ of rank $n$ is $f_1, \ldots, f_n$ such that $(f_i, f_j) = k\delta_{ij}$.

For a self-dual code $C$ over $\mathbb{Z}_k$, and unimodular lattice $L$,

$$C \rightarrow \frac{1}{\sqrt{k}} A(C) \quad \text{Construction A}$$

$$C \leftarrow L \text{ together with } k\text{-frame}$$

Classification of extremal type II codes over $\mathbb{Z}_4$ is equivalent to classification of 4-frames in the Leech lattice.

- Harada–M. (2009) $\not\exists [24, 12, 10]$ code over $\mathbb{F}_5$
- $\exists ![20, 10, 9]$ code over $\mathbb{F}_7$?
Hadamard matrices

Definition
A Hadamard matrix of order $n$ is an $n \times n$ matrix $H$ with entries $\pm 1$ such that $HH^\top = nl$.

- $n$ must be 1, 2 or $\equiv 0 \pmod{4}$.
- conjectured to exist for all $n \equiv 0 \pmod{4}$
- classified up to $n = 32$
- 60 for $n = 24$
Theorem (M. and Tamura, 2012)

For a normalized Hadamard matrix $H$ of order 24, TFAE:

1. the **binary** code generated by the binary ($-1 \mapsto 0$) Hadamard matrix associated to $H$ is extremal doubly even self-dual $[24, 12, 8]$ (Golay) code

2. the **ternary** code generated by $H^\top$ is extremal $[24, 12, 9]$ code

3. “the common neighbor” of the two lattices obtained from the two codes above is the Leech lattice
Theorem (M. and Tamura, 2012)

For a normalized Hadamard matrix $H$ of order 48, TFAE:

1. the $\mathbb{Z}_4$-code generated by the binary ($-1 \mapsto 0$) Hadamard matrix associated to $H$ is extremal type II $[48, 24, 24]$ code
2. the ternary code generated by $H^\top$ is extremal self-dual $[48, 24, 15]$ code
3. “the common neighbor” of the two lattices obtained from the two codes above is an extremal even unimodular lattice (of minimum norm 6)

- Hadamard matrices of order 48: hopeless to classify
- extremal type II $[48, 24, 24]$ $\mathbb{Z}_4$-code: not well-understood
- extremal even unimodular lattice of rank 48: not classified, two well-known for a long time, Nebe found the 3rd (1998) and 4th (2013). $\exists 6$-frame in Nebe’s lattices?
Concluding Remarks

- All codes in my talks were of fixed length, 24, 48, etc. (no general theory).
- These are “testing ground” for general theory to be developed.
- The problems are computationally difficult.
- We need to develop real theory (which is very often applicable to arbitrary lengths).

Thank you very much for your attention.