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

Akihiro Munemasa[1]

[1]Graduate School of Information Sciences
Tohoku University

August 12, 2014
ICM 2014 Satellite Conference
on Algebraic Coding Theory
Ewha Womans University, Korea

L = Leech lattice

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

most difficult

$\uparrow$ Dong Mason Zhu $\qquad\qquad$ $\uparrow \mathcal{D}$ (extended doubling)

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

easily enumerated

The diagram commutes, and

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

Even, doubly even, and triply even codes

A binary linear code C is called

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

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

(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 $h, i, j \in \{1, \dots, k\}$. (denoting by $*$ the entrywise product)

Proposition

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

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

Proof.

Use induction on k. Note

$$\begin{aligned}\mathrm{wt}(a+b+c) = {} & \mathrm{wt}(a) + \mathrm{wt}(b) + \mathrm{wt}(c) \\ & - 2(\mathrm{wt}(a*b) + \mathrm{wt}(a*c) + \mathrm{wt}(b*c)) \\ & + 4\,\mathrm{wt}(a*b*c).\end{aligned}$$

□

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

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

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

$$RM(1,4) = \mathcal{D}(e_8) = \begin{bmatrix} \mathbf{1}_8 & 0 \\ e_8 & e_8 \end{bmatrix}$$

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 $\mathcal{D}(C)$ 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 $V^\natural$

Theorem (Harada–Lam–M., 2013)

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

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

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

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 $\mathbf{1}_{24} \in C$ and the minimum weight of $C^\perp$ is ≥ 4.

Dimension	Total	Realizable	non-Realizable
12	9	1+1+7	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

9 = Pless–Sloane (1975)
$1 + 1 + 7$ = Bonnecaze–Solé–Calderbank (1995), Calderbank–Sloane (1997), Young–Sloane (unpublished)

Realizable codes

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.

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

dim C	6	7	8	9	10	11	12
$\#C$	1	7	32	60	49	21	9
$\#$	1	5	29	171	755	1880	1890+13

- 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.

Definition

A k-frame of a lattice L of rank n is $f_1, \dots, f_n$ such that $(f_i, f_j) = k\delta_{ij}$.

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

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

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

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

- Harada–M. (2009) $\nexists$ $[24, 12, 10]$ 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 ± 1 such that $HH^\top = nI$.

- 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 $n = 24$

Assmus–Key 1992

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 ternary self-dual $[48, 24, 15]$ code: not classified
- 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.