Self-Orthogonal Codes and Hadamard Matrices

Akihiro Munemasa[1]

[1]Graduate School of Information Sciences
Tohoku University
(joint work with Masaaki Harada)

January 11, 2015
Kumamoto University

Self-Dual $\mathbb{Z}_k$-Codes

- $k \in \mathbb{Z}$, $k \geq 2$.
- $\mathbb{Z}_k$: the ring of integers modulo k.
- a submodule $C \subset \mathbb{Z}_k^n$ is called a code of length n over $\mathbb{Z}_k$, or a $\mathbb{Z}_k$-code of length n.
- $(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^n x_i y_i$, where $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_k^n$,
- C is self-dual if $C = C^\perp$, where
  $C^\perp = \{\boldsymbol{x} \in \mathbb{Z}_k^n \mid (\boldsymbol{x}, \boldsymbol{y}) = 0 \ (\forall \boldsymbol{y} \in C)\}$,

Database by M. Harada and A. M.

http://www.math.is.tohoku.ac.jp/∼munemasa/selfdualcodes.htm

k	complete	comments
3	$\leq$24	28 with min. wt. 9
5	$\leq$16	$\nexists$20 with min. wt. 10
7	$\leq$12	16 with min. wt. 7; 20 with min. wt. 9$\exists$!?

$k = 3$ length 24 by Harada–M. (2009),
length 28 by Harada–M–Venkov. (2009).

$k = 5$ length ≤ 16 by Harada–Östergård (2003),
length 20 by Harada–M. (2009),

$k = 7$ length ≤ 12 by Harada–Östergård (2002),
length 16 by Kim–Lee (2012),
length 20 by Gulliver–Harada (1999),
Gulliver–Harada–Miyabayashi (2007).

Classifying Self-Dual Codes Using Lattices

Proposed by Harada–M.–Venkov (2009) for $k = 3$, length 28.
Also used by Harada–M. (2009) for $k = 5$, length 20.

- $\pi : \mathbb{Z} \to \mathbb{Z}_k$: canonical surjection.
- $\pi : \mathbb{Z}^n \to \mathbb{Z}_k^n \supset C$. Construction A_k means:

$$L = \frac{1}{\sqrt{k}} \pi^{-1}(C) \subset \mathbb{R}^n$$

- $C = C^\perp \implies L$: unimodular.

Such lattices have been classified for $n \leq 25$.
Example: $n = 8$: $\mathbb{Z}^8$ and E_8.
A lattice obtained by Construction A_k contains a k-frame:
$\mathcal{F} = \{\pm f_1, \ldots, \pm f_n\}$ with

$$(f_i, f_j) = k\delta_{i,j}.$$

$L \subset \mathbb{R}^n$: unimodular lattice

If L contains a k-frame $\mathcal{F} = \{\pm f_1, \dots, \pm f_n\}$, i.e.,

$$(f_i, f_j) = k\delta_{i,j},$$

then $L \subset \frac{1}{k}\mathbb{Z}\mathcal{F}$, so

$$C = L/\mathbb{Z}\mathcal{F} \subset \frac{1}{k}\mathbb{Z}\mathcal{F}/\mathbb{Z}\mathcal{F} \cong \mathbb{Z}\mathcal{F}/k\mathbb{Z}\mathcal{F} \cong \mathbb{Z}_k^n$$

and C is a self-dual code.

- Knowledge of unimodular lattices can be used to classify self-dual codes.

$C \subset \mathbb{Z}_k^n$, $\mathcal{F} \subset L \subset \mathbb{R}^n$

$$C \mapsto \frac{1}{\sqrt{k}}\pi^{-1}(C) : \text{ lattice}$$

$$(L, \mathcal{F}) \mapsto L/\mathbb{Z}\mathcal{F} : \text{ code}$$

The above correspondence gives, for a fixed lattice L:

$$\{\text{codes } C \text{ with } \frac{1}{\sqrt{k}}\pi^{-1}(C) \cong L\}/(\pm 1)\text{-monomial equiv.}$$

$$\overset{1:1}{\leftrightarrow} \{k\text{-frames of } L\}/\operatorname{Aut}(L)$$

Database by M. Harada and A. M.

k	complete	comments
3	$\leq$24	28 with min. wt. 9
5	$\leq$16	$\nexists$20 with min. wt. 10
7	$\leq$12	16 with min. wt 7, 20 with min. wt. 9$\exists$!?

$k = 3$ length 24 by Harada–M. (2009),
length 28 by Harada–M–Venkov. (2009).

$k = 5$ length ≤ 16 by Harada–Östergård (2003),
length 20 by Harada–M. (2009),

$k = 7$ length ≤ 12 by Harada–Östergård (2002),
length 16 by Kim–Lee (2012),
length 20 by Gulliver–Harada (1999),
Gulliver–Harada–Miyabayashi (2007).

The only known $[20, 10, 9]$ code C over $\mathbb{Z}_7$

Length$= 20$, Self-dual $\implies$ dimension$= 10$, minimum Hamming weight$= 9$ (largest possible).
For the only known such code C, Construction A_7 gives the lattice D_{20}^+.

1. Is C the only $[20, 10, 9]$ code up to equivalence which gives D_{20}^+ by Construction A_7?
2. Is there any $[20, 10, 9]$ code which gives a lattice other than D_{20}^+ by Construction A_7? For example $D_{12}^+ \oplus E_8$?

$$D_{20} = \langle \pm e_i \pm e_j \mid 1 \leq i < j \leq 20 \rangle.$$

$$D_{20}^+ = \langle D_{20}, \ \frac{1}{2}\mathbf{1} \rangle \subset \frac{1}{2}\mathbb{Z}^{20}.$$

$$\cong \frac{1}{\sqrt{7}}\pi^{-1}(C).$$

$[20, 10, 9]$ code C over $\mathbb{Z}_7$

Construction A_7 gives the lattice D_{20}^+.

$$D_{20} = \langle \pm e_i \pm e_j \mid 1 \le i < j \le 20 \rangle.$$

$$D_{20}^+ = \langle D_{20},\ \frac{1}{2}\mathbf{1} \rangle$$

$$\cong \frac{1}{\sqrt{7}} \pi^{-1}(C) \quad \text{contains a 7-frame } \mathcal{F}$$

$\mathcal{F} = \{\pm f_1, \ldots, \pm f_{20}\}$, f_i is of the form

$$\frac{1}{2}(\pm 3, \pm 1, \ldots, \pm 1)$$

norm

$$7 = \frac{28}{4} = \frac{(\pm 3)^2 + 19 \cdot (\pm 1)^2}{4}$$

Skew Hadamard matrices of order 20

Theorem

If Construction A_7 of a self-dual $[20, 10, 9]$ code over $\mathbb{Z}_7$ gives the lattice D_{20}^{+}, then the 7-frames are of the form

$$\frac{1}{2}(H + 2I)$$

where H is a Hadamard matrix of order 20 satisfying $H + H^{\top} = 2I$.

Considering Hamming weight, we may assume the 7-frames are of the form

$$\frac{1}{2}\begin{bmatrix} 3 & & \pm 1 \\ & \ddots & \\ \pm 1 & & 3 \end{bmatrix}$$

Theorem

If Construction A_7 of a self-dual $[20, 10, 9]$ code over $\mathbb{Z}_7$ gives the lattice D_{20}^{+}, then the 7-frames are of the form

$$\frac{1}{2}(H+2I) = \frac{1}{2}\begin{bmatrix} 3 & & \pm 1 \\ & \ddots & \\ \pm 1 & & 3 \end{bmatrix}$$

where H is a Hadamard matrix of order 20 satisfying $H + H^\top = 2I$.

Proof.

If $H_{ij} = H_{ji}$, then the Hamming wt. of the codeword corresponding to $e_i + e_j \in D_{20}$ is < 9, a contradiction. So $H + H^\top = 2I$. Since $(H+2I)(H+2I)^\top = 28I$, we have $HH^\top = 20I$. $\square$

Work to be done

- Is C the only $[20, 10, 9]$ code up to equivalence which gives D_{20}^{+} by Construction A_7?
  1. Skew Hadamard matrices of order 20: classified.
  2. $\exists$ skew Hadamard matrix which gives a self-dual $[20, 10, 8]$ code.
- Is there any $[20, 10, 9]$ code which gives a lattice other than D_{20}^{+} by Construction A_7?
  1. For example $D_{12}^{+} \oplus E_8$?
  2. Given a self-dual code over $\mathbb{Z}_k$, describe a condition under which Construction A_k gives a decomposable lattice.

With Prof. Hiramine

1. A colloquium talk at University of Tsukuba 1983?
2. Hokkaido University in 1993 or 1996? Existence of an orthogonal decomposition of $\mathfrak{sl}(6, \mathbb{C})$ into 7 Cartan subalgebras, equivalently, mutually unbiased bases in dimension 6.
3. R. Craigen in 2014, mentions a conjecture which says that the existence of a $GH(n, U)$ implies that $|U|$ is a prime power.