On the Classification of Self-Dual $\mathbb{Z}_k$-Codes

Akihiro Munemasa[1]

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

December 15, 2009
12th IMA Conference on Cryptography and Coding

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

- $k \in \mathbb{Z}$, $k \geq 2$.
- $\mathbb{Z}_k$: the ring of integers modulo k.
- $(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^{n} x_i y_i$, where $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_k^n$,
- Euclidean weight: $\mathrm{wt}(\boldsymbol{x}) = \sum_{i=1}^{n} x_i^2 \in \mathbb{Z}$, where $\mathbb{Z}_k = \{0, \pm 1, \pm 2, \dots\}$ is considered as $\subset \mathbb{Z}$
- 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.
- C is self-dual if $C = C^{\perp}$, where $C^{\perp} = \{\boldsymbol{x} \in \mathbb{Z}_k^n \mid (\boldsymbol{x}, \boldsymbol{y}) = 0 \ (\forall \boldsymbol{y} \in C)\}$,
- For k even, C is Type II $\iff$ $C = C^{\perp}$ and $2k \mid \mathrm{wt}(\boldsymbol{x})$ for all $\boldsymbol{x} \in C$.

For k even, C is Type II $\iff$ $C = C^\perp$ and $\mathrm{wt}(\boldsymbol{x}) \equiv 0 \pmod{2k}$.

A Type II code of length n exists if and only if $8|n$.
For $n = 8$:

- $k = 2$: Binary Extended Hamming Code (unique).
- $k = 4$: Four Codes (Conway–Sloane, 1993).
- $k = 6$: Two Codes (Kitazume–Ooi, 2004).
- $k = 8$: (Dougherty–Gulliver–Wong, 2006, incomplete).

Mass formula (which gives the total number of Type II codes of given length and k) is known for $k = 2, 4, 6$ but not known for $k = 8$ until 2009 (previous talk).

New Method of Classifying Self-Dual and Type II Codes Using Lattices

Proposed by Harada–Munemasa–Venkov (2009).

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

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

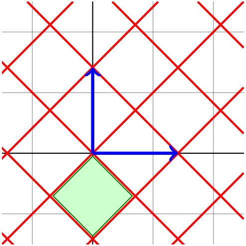
- $C = C^\perp \implies L$: unimodular.
- C: Type II $\implies L$: even unimodular

Such lattices have been classified for $n \leq 24$.
Example: $n = 8$: $\mathbb{Z}^8$ and E_8.

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

Example: $n = 2$, $k = 2$, $C = \langle (1,1) \rangle \subset \mathbb{Z}_2^2$.

$$L = \frac{1}{\sqrt{2}}\{(x,y) \in \mathbb{Z}^2 \mid x \equiv y \pmod{2}\}.$$



L unimodular
$\iff$ det(Gram matrix) $= 1$
$\iff$ vol(fundamental domain) $= 1$

$f_1 = (\sqrt{2}, 0)$, $f_2 = (0, \sqrt{2})$.

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

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

and C is a self-dual code.
(If, moreover, L is even, then C is Type II).

- Knowledge of unimodular lattices can be used to classify self-dual codes or Type II codes.
- The method does not require k to be a prime.

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

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

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

The above correspondence gives, for a fixed lattice L:

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

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

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

Define a graph Γ

- vertices $V(\Gamma) = \{\{\pm f\} \mid f \in L,\ (f, f) = k\}$
- edges: $\{\pm f\} \sim \{\pm f'\} \iff (f, f') = 0$

Then k-frames of $L \leftrightarrow n$-cliques (complete subgraph) in Γ, and $\exists \varphi : \mathrm{Aut}(L) \to \mathrm{Aut}(\Gamma)$.

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

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

$$\overset{1:1}{\leftrightarrow} \{n\text{-cliques of } \Gamma\}/\varphi(\mathrm{Aut}(L))$$

$$V(\Gamma) = \{\{\pm f\} \mid f \in L,\ (f,f) = k\}$$

How large is $|V(\Gamma)|$?

For example, for any n, there is a standard unimodular lattice $\mathbb{Z}^n$, and it has a k-frame when $n \geq 4$.

n	16	17	18	19	20
$k=4$	14576	19057	24498	31027	38780

n	8	9	10	11	12	13	14
$k=6$	1568	*	*	*	32208	*	*
$k=8$	4664	*	26010	*	126852	*	544726
$k=9$	6056	17401	44330	104775	236380	515957	
$k=10$	7056	*	64532	*	412632	*	

Remark: For prime k:

$k=2$: $n \leq 34$ by Bilous (2006),

$k=3$: $n \leq 24$ by Harada–Munemasa (2009),

$k=5$: $n \leq 16$ by Harada–Östergård (2003),

$k=7$: $n \leq 12$ by Harada–Östergård (2002).

Table

$k = 4$	$1, 2, \ldots, 15$ Conway–Sloane (1993) Fields–Gaborit–Leon–Pless (1998)	$16, 17, 18, 19$
$k = 6$	4 Dougherty–Harada–Solé (1999)	8 $4\|n$
$k = 8$	$2, 4$ Dougherty–Gulliver–Wong (2004)	$6, 8, 10, 12$ $2\|n$
$k = 9$	$1, 2, \ldots, 8$ Bealmaceda–Betty–Nemenzo (2009)	$9, 10, 11, 12$
$k = 10$		$2, 4, 6, 8, 10$ $2\|n$