Covering radii and shadows of binary self-dual codes

Akihiro Munemasa

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

December 15, 2015
AC2015
Tokyo Metropolitan University

We want to determine the image of the mapping

$$\{C \mid C \subset \mathbb{F}_2^n,\ C = C^\perp\} \to \mathbb{Z}[x,y]$$

defined by $C \mapsto W_C(x,y)$, where

$$W_C(x,y) = \sum_{c\in C} x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)},$$

$$\mathrm{wt}(c) = |\{i \mid c_i \neq 0\}| \quad (c \in \mathbb{F}_2^n).$$

We want to determine the image of the mapping

$$\{C \mid C \subset \mathbb{F}_2^n,\ C = C^\perp\} \to \mathbb{Z}[x, y]$$

defined by $C \mapsto W_C(x, y)$, where

$$W_C(x, y) = \sum_{c \in C} x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)},$$

$$\mathrm{wt}(c) = |\{i \mid c_i \neq 0\}| \quad (c \in \mathbb{F}_2^n).$$

If we restrict the domain to the set of doubly even codes, i.e.,

$$\mathrm{wt}(c) \equiv 0 \pmod 4 \quad (\forall c \in C),$$

then the image is contained in

$$R = \mathbb{Q}[x^8 + 14x^4y^4 + y^8, W_{\mathsf{Golay}}(x, y)]$$

Determining $W_C(x, y)$ for a given C is computationally difficult ($|C| = 2^{n/2}$).

$R = \mathbb{Q}[x^8 + 14x^4y^4 + y^8, W_{\mathsf{Golay}}(x, y)]$

$$W_{\mathsf{Golay}}(x, y) = x^{24} + y^{24} + 759(x^{16}y^8 + x^8y^{16}) + 2576x^{12}y^{12}.$$

So

$$\dim R_{(n)} = 1 + \lfloor n/24 \rfloor \quad (\text{if } 8 \mid n).$$

$R = \mathbb{Q}[x^8 + 14x^4y^4 + y^8, W_{\text{Golay}}(x, y)]$

$$W_{\text{Golay}}(x, y) = x^{24} + y^{24} + 759(x^{16}y^8 + x^8y^{16}) + 2576x^{12}y^{12}.$$

So

$$\dim R_{(n)} = 1 + \lfloor n/24 \rfloor \quad (\text{if } 8 \mid n).$$

An extremal weight enumerator is the unique homogeneous polynomial of degree n whose coefficient of x^n is 1, and those of

$$\underbrace{x^{n-4}y^4,\ x^{n-8}y^8, \ldots, x^{n-4\lfloor n/24 \rfloor}y^{4\lfloor n/24 \rfloor}}_{\lfloor n/24 \rfloor}$$

are all zero. For example, $W_{\text{Golay}}(x, y)$.
A code C is called extremal if $W_C(x, y)$ is extremal.
Equivalently, C has minimum weight $4\lfloor n/24 \rfloor + 4$, i.e.,

$$\forall c \in C,\ \mathrm{wt}(c) \neq 4, 8, \ldots, 4\lfloor n/24 \rfloor.$$

Extremal doubly even self-dual codes

$C = C^{\perp} \subset \mathbb{F}_2^n$, $8 \mid n$,
all weights$\equiv 0 \pmod 4$,
minimum weight $4\lfloor n/24 \rfloor + 4$.

k	0	1	2	3	≥ 4	
$n = 24k$	–	1	1	???	$?\cdots$	$\nexists\ k \geq 154$
$n = 24k + 8$	1	5	many?	many?	$\cdots$	$\nexists\ k \geq 159$
$n = 24k + 16$	2	16470	many?	many?	$\cdots$	$\nexists\ k \geq 164$

- $n = 72$ open since Sloane (1973).
- Nonexistence for large n by Zhang (1999).
- Uniqueness for $n = 48$ by Houghten–Lam–Thiel–Parker (2003)
- Classification for $n = 40$ by Betsumiya–Harada–M. (2012)

Covering radius

The covering radius $r(C)$ is defined as

$$r(C) = \max\{ \min\{\mathrm{wt}(u) \mid u \in v + C\} \mid v + C \in \mathbb{F}_2^n / C\}.$$

Computationally difficult.
Delsarte bound for extremal doubly even self-dual codes:

$$r(C) \leq \begin{cases} 4k & \text{if } n = 24k, \\ 4k+2 & \text{if } n = 24k+8, \\ 4k+4 & \text{if } n = 24k+16. \end{cases}$$

Covering radius

The covering radius $r(C)$ is defined as

$$r(C) = \max\{\min\{\mathrm{wt}(u) \mid u \in v + C\} \mid v + C \in \mathbb{F}_2^n/C\}.$$

Computationally difficult.
Delsarte bound for extremal doubly even self-dual codes:

$$r(C) \leq \begin{cases} 4k & \text{if } n = 24k, \\ 4k+2 & \text{if } n = 24k+8, \\ 4k+4 & \text{if } n = 24k+16. \end{cases}$$

Extremal doubly even self-dual codes

$C = C^{\perp} \subset \mathbb{F}_2^n$, $8 \mid n$,
all weights$\equiv 0 \pmod 4$,
minimum weight $4\lfloor n/24 \rfloor + 4$.
$r(C) \leq$ Delsarte bound.

k	0	1	2	3	≥ 4
$n = 24k$ $r(C)$	—	1 $4 = 4$	1 $8 = 8$	? ?	$?\cdots$
$n = 24k + 8$ $r(C)$	1	5 $6 = 6$	many $10? = 10$	many? $12, 13 < 14$	$\cdots$
$n = 24k + 16$ $r(C)$	2	16470 $7, 8 \leq 8$	many? ?	many?	$\cdots$

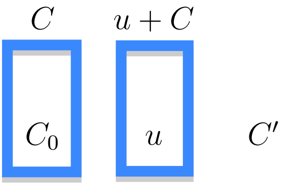
We now focus on the case $n = 24k + 8$.

$n = 24k + 8$

Delsarte: $r(C) \leq 4k + 2$.
Suppose that a coset $u + C$ has minimum weight $4k + 2$. Let

$$C_0 = C \cap \langle u \rangle^{\perp},$$
$$C' = \langle C_0, u \rangle.$$

Then $C' = C'^{\perp}$ has minimum weight $4k + 2$ (not doubly even). $S = C_0^{\perp} \setminus C'$ is called the shadow of C'.



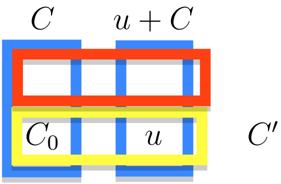
$$\min(u+C) = 4k+2 \implies \min S = 4k+4$$

$n = 24k + 8$

Delsarte: $r(C) \leq 4k + 2$.
Suppose that a coset $u + C$ has minimum weight $4k + 2$. Let

$$C_0 = C \cap \langle u \rangle^{\perp},$$
$$C' = \langle C_0, u \rangle.$$

Then $C' = C'^{\perp}$ has minimum weight $4k + 2$ (not doubly even). $S = C_0^{\perp} \setminus C'$ is called the shadow of C'.



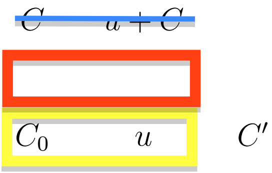
$$\min(u+C) = 4k+2 \implies \min S = 4k+4$$

$n = 24k + 8$

Delsarte: $r(C) \leq 4k + 2$.
Suppose that a coset $u + C$ has minimum weight $4k + 2$. Let

$$C_0 = C \cap \langle u \rangle^{\perp},$$
$$C' = \langle C_0, u \rangle.$$

Then $C' = C'^{\perp}$ has minimum weight $4k + 2$ (not doubly even). $S = C_0^{\perp} \setminus C'$ is called the shadow of C'.



$$\min(u+C) = 4k+2 \implies \min S = 4k+4$$

For $n = 24k + 8$, the following are equivalent:

1. $\exists$ extremal doubly even self-dual code C of length n with covering radius $4k + 2$,
2. $\exists$ self-dual code C' of length n with minimum weight $4k + 2$ and its shadow has minimum weight $4k + 4$.

Bachoc–Gaborit (2004) showed: if a (not doubly even) self-dual code C' of length n with minimum weight d and its shadow has minimum weight s, and

$$2d + s = \frac{n}{2} + 4,$$

then $W_{C'}(x, y)$ and $W_S(x, y)$ are uniquely determined.

$$2(4k + 2) + (4k + 4) = \frac{24k + 8}{2} + 4.$$

For $n = 24k + 8$, the following are equivalent:

1. $\exists$ extremal doubly even self-dual code C of length n with covering radius $4k + 2$,
2. $\exists$ self-dual code C' of length n with minimum weight $4k + 2$ and its shadow has minimum weight $4k + 4$.

$$W_{C'}(x, y) = \sum_{j=0}^{n/8} a_j (x^2 + y^2)^{n/2-4j} (x^2 y^2 (x^2 - y^2)^2)^j,$$

$$W_S(x, y) = \sum_{j=0}^{n/8} a_j (-1)^j 2^{n/2-6j} (xy)^{n/2-4j} (x^4 - y^4)^{2j},$$

the coefficients a_j are uniquely determined.

For $n = 24k + 8$, the following are equivalent:

1. $\exists$ extremal doubly even self-dual code C of length n with ~~covering radius $4k + 2$,~~ (thus $k \leq 158$ by Zhang)
2. $\exists$ self-dual code C' of length n with minimum weight $4k + 2$ and its shadow has minimum weight $4k + 4$.

$$W_{C'}(x, y) = \sum_{j=0}^{n/8} a_j (x^2 + y^2)^{n/2-4j} (x^2 y^2 (x^2 - y^2)^2)^j,$$

$$W_S(x, y) = \sum_{j=0}^{n/8} a_j (-1)^j 2^{n/2-6j} (xy)^{n/2-4j} (x^4 - y^4)^{2j},$$

the coefficients a_j are uniquely determined.

For $n = 24k + 8$, the following are equivalent:

1. $\exists$ extremal doubly even self-dual code C of length n with covering radius $4k + 2$, (thus $k \leq 158$ by Zhang)
2. $\exists$ self-dual code C' of length n with minimum weight $4k + 2$ and its shadow has minimum weight $4k + 4$.

$$W_{C'}(x,y) = \sum_{j=0}^{n/8} a_j (x^2+y^2)^{n/2-4j} (x^2y^2(x^2-y^2)^2)^j,$$

$$W_S(x,y) = \sum_{j=0}^{n/8} a_j (-1)^j 2^{n/2-6j} (xy)^{n/2-4j} (x^4-y^4)^{2j},$$

the coefficients a_j are uniquely determined.
W_S shows $k \leq 136$.

For $n = 24k + 8$, the following are equivalent:

1. $\exists$ extremal doubly even self-dual code C of length n with covering radius $4k + 2$, (thus $k \leq 158$ by Zhang)
2. $\exists$ self-dual code C' of length n with minimum weight $4k + 2$ and its shadow has minimum weight $4k + 4$.

$$W_{C'}(x, y) = \sum_{j=0}^{n/8} a_j (x^2 + y^2)^{n/2-4j} (x^2 y^2 (x^2 - y^2)^2)^j,$$

$$W_S(x, y) = \sum_{j=0}^{n/8} a_j (-1)^j 2^{n/2-6j} (xy)^{n/2-4j} (x^4 - y^4)^{2j},$$

the coefficients a_j are uniquely determined.
W_S shows $k \leq 136$.
Thank you for your attention!