Construction of Doubly-even Self-dual Codes by Harada-Kimura-Tonchev operations

Akihiro Munemasa

Graduate School of Mathematics, Kyushu Univ.
and
Dept. Combinatorics & Optimization, Univ. Waterloo

based on joint work with

Masaaki Harada
Masaaki Kitazume

We consider binary codes of length $2n$.

$$u=(u_1, u_2, \cdots, u_{2n}) \in \mathbb{F}_2^{2n}$$
$$v=(v_1, v_2, \cdots, v_{2n}) \in \mathbb{F}_2^{2n}$$

$$(u,v) := \sum_{i=1}^{2n} u_i v_i \qquad \mathrm{Supp}(u)=\{i \mid u_i=1\}$$

$$\mathrm{wt}(u) := |\{i \mid u_i = 1\}| = |\mathrm{Supp}(u)|$$

$\mathbb{F}_2^{2n} \supset C$ linear code of length $2n$

$$C^\perp := \{u \in \mathbb{F}_2^{2n} \mid (u,v)=0 \ \forall v \in C\}$$

C is self-dual $\underset{\text{def}}{\Longleftrightarrow}$ $C = C^\perp$

C is doubly-even $\underset{\text{def}}{\Longleftrightarrow}$ $\mathrm{wt}(v) \equiv 0 \pmod 4$ for $\forall v \in C$

$\exists$ doubly-even self-dual code of length $2n$

$\Longleftrightarrow$ $n \equiv 0 \pmod 4$

Mimimum weight of C

$$\min(C) = \min\{\, wt(v) \mid v \in C,\ \ v \neq 0 \,\}$$

A doubly-even self-dual binary code C of length $2n$
(d.e.s.d)
is **extremal** if

$$\min(C) = 4\left[\frac{n}{12}\right] + 4$$

← largest possible

$2n$	$4\left[\frac{n}{12}\right]+4$	$\left\lvert \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \backslash O^{+}(2n-2,2)/S_{2n} \right\rvert$
8	4	1
16	4	2
24	8	8+1
32	8	80+5
40	8	too many
⋮	⋮	⋮
72	16	?

C = Row Space of

$$\begin{pmatrix} 1 & & & & 0 & 1 & 1 & 1 \\ & 1 & & & 1 & 0 & 1 & 1 \\ & & 1 & & 1 & 1 & 0 & 1 \\ & & & 1 & 1 & 1 & 1 & 0 \end{pmatrix} =$$ generator matrix of 7 extended binary Hamming $[8,4,4]$-code

$\downarrow$ switch $0 \leftrightarrow 1$

$$\begin{pmatrix} 1 & & & & 1 & 0 & 1 & 1 \\ & 1 & & & 0 & 1 & 1 & 1 \\ & & 1 & & 0 & 0 & 0 & 1 \\ & & & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

wt	
$1+3$	ok
$1+3$	ok
$1+1$	not ok
$1+1$	not ok

$\downarrow$ switch $0 \leftrightarrow 1$

$$\begin{pmatrix} 1 & & & & 1 & 0 & 1 & 1 \\ & 1 & & & 0 & 1 & 1 & 1 \\ & & 1 & & 1 & 1 & 1 & 0 \\ & & & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

again generator matrix of extended binary Hamming $[8,4,4]$-code

$$
\begin{aligned}
r &= (0\,0\,1\,0 \mid 1\,1\,0\,1) \\
+v &= (0\,0\,0\,0 \mid 1\,1\,0\,0) \\
\hline
r+v &= (0\,0\,1\,0 \mid 0\,0\,0\,1) \\
+e &= (0\,0\,0\,0 \mid 1\,1\,1\,1) \\
\hline
r+v+e &= (0\,0\,1\,0 \mid 1\,1\,1\,0)
\end{aligned}
$$

weight of latter half

$$
\begin{tikzcd}
3 \arrow[d, "\text{add } v"'] \arrow[dr] & \\
1 \arrow[d, "\text{add } e"'] & 3 \arrow[dl, "\text{do nothing}"] \\
3 &
\end{tikzcd}
$$

Suppose $\mathrm{wt}(v)=2$, first half of $v = 0$

$$
r \mapsto \begin{cases} r+v+e & \text{if } (r,v)=0 \\ r+v & \text{if } (r,v)=1 \end{cases}
$$

$$
= r+v+(1+(r,v))e
$$

Harada – Kimura (1995)

$G = (\, I \mid A \,)$: generator matrix of a doubly-even self-dual (d.e.s.d) code of length $2n$

$v = (0 \cdots 0 \mid * \cdots *)$ $\quad wt(v) \equiv 2 \pmod 4$

$e = (0 \cdots 0 \mid 1 \cdots 1)$

For each row vector r of G.

$r \mapsto r' = r + v + (1 + (r, v))e$

Then the matrix $G' = (\, r' \,;\, r : \text{row of } G \,)$ generates a d.e.s.d code.

The same result holds when

$wt(v) \equiv 0 \pmod 4$

$r \mapsto r' = r + v + (r, v)e$

Let us call this

Harada-Kimura-Tonchev (HKT) operation.

HKT operations can be used to produce new d.e.s.d. codes from a given one.

Tonchev (1989)	length 40
Harada-Kimura (1995)	length 64

$$\left.\begin{array}{l} G = (\, I \mid A \,) \\ v = (0 \cdots 0 \mid * \cdots *) \\ \quad\quad wt(v) : \text{even} \end{array}\right\} \rightarrow G'$$

Goal

Describe HKT operations as a linear transformation.

Show that ALL d.e.s.d. codes can be constructed from one d.e.s.d. code by successively applying (suitably generalized) HKT operations.

our generalization of HKT operations will not require the generator matrix to be in the standard form $(I \mid A)$

Recall HKT operation when $wt(v) \equiv 2 \pmod 4$

8/10

$$v = (0 \cdots 0 \mid * \cdots *)$$
$$e = (0 \cdots 0 \mid 1 \cdots 1)$$

For each row vector r of $G = (I \ A)$

$$r \mapsto r' = r + v + (1 + (r, v))e$$

Since $(r, e) = 1$

$$r' = r + (v + e) + (r, v)e$$
$$= r + (r, e)(v+e) + (r, v)e$$

: linear in r!

$$C \xmapsto{HKT} C' = \{x + (x, e)(v+e) + (x, v)e \mid x \in C\}$$

Rewrite the formula using

$\boxed{u} = v + e$ and $\boxed{v}$

$$x \mapsto x + (x,e)(v+e) + (x,v)e$$

$e = u + v$

$$= x + (x, u+v)u + (x,v)(u+v)$$

$v + e = u$

$$= x + (x,u)u + (x,v)v$$

Requirements

(1) $wt(v) \equiv 2 \pmod 4$

(2) $wt(u) \equiv 2 \pmod 4$

(3) $(u,v) = 0$

$u = v + e$

$wt(e) \equiv 0 \pmod 4$

$Supp(e) = Supp(u) \dot{\cup} Supp(v)$

If u, v satisfy (1)–(3) then

$$\sigma_{u,v}(x) = x + (x,u)u + (x,v)v$$

maps d.e.s.d. codes to d.e.s.d. codes.

Let us call $\sigma_{u,v}$ (generalized) HKT operation.

An easy way to check this $\rightarrow$ use quadratic form

$\mathbb{F}_2^{2n} \ni \mathbf{1}$ all one vector $= (1, 1, \dots, 1)$

$\langle \mathbf{1} \rangle^{\perp} =$ parity check code

$= \{$ vectors of even weight $\}$

$f : \langle \mathbf{1} \rangle^{\perp} \longrightarrow \mathbb{F}_2$ is a quadratic form

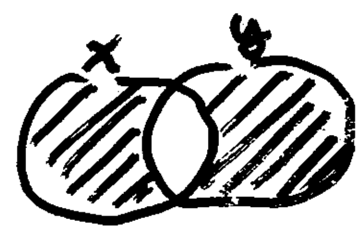
$x \longmapsto \dfrac{wt(x)}{2}$

Broué (1977) attributes this to Puig

(not in MacWilliams-Sloane-Thompson) (1972)

$f(x+y) = f(x) + f(y) + (x, y)$

follows from



$wt(x+y) = wt(x) + wt(y) - 2wt(x * y)$

Our requirements are

(1) $f(u) = 1$

(2) $f(v) = 1$

(3) $(u, v) = 0$

$\{u, v\}$ hyperbolic pair

Definitions

5A

$v \in \langle \mathbf{1} \rangle^{\perp}$ is called singular if $f(v) = 0$

nonsingular if $f(v) = 1$

$C \subset \langle \mathbf{1} \rangle^{\perp}$ is called totally singular if

$$f(v) = 0 \quad \forall v \in C$$

($\Longleftrightarrow$ doubly-even)

5B

$\forall$ d.e.s.d. code C satisfies $\langle \mathbf{1} \rangle \subset C \subset \langle \mathbf{1} \rangle^{\perp}$

Note $(\langle \mathbf{1} \rangle^{\perp})^{\perp} = \langle \mathbf{1} \rangle$, $f(\mathbf{1}) = 0$

So f induces a nondegenerate quadratic form $\bar{f}$ on $\langle \mathbf{1} \rangle^{\perp} / \langle \mathbf{1} \rangle$

$$O(f) \longrightarrow O(\bar{f}) = O^{+}(2n-2, 2)$$

$$\rho \longmapsto \bar{\rho}$$

Then, if C is a d.e.s.d. code

$$\overline{C} \subset \langle \mathbf{1} \rangle^{\perp} / \langle \mathbf{1} \rangle$$

$\overline{C}$: dim $n-1$ $\qquad$ $\langle \mathbf{1} \rangle^{\perp} / \langle \mathbf{1} \rangle$: dim $2n-2$

(maximal) totally singular subspace w.r.t. $\bar{f}$.

<u>Theorem</u> (Witt) The group $O(\bar{f})$ acts transitively on the set of maximal totally singular subspaces.

(This does not mean all d.e.s.d. codes are pairwise equivalent)

Suppose $v \in \langle 1 \rangle^{\perp}$ $f(v) = 1$

The transvection τ_v with respect to v is

$$\tau_v(x) = x + (x, v)v$$

Then $\tau_v : \langle 1 \rangle^{\perp} \to \langle 1 \rangle^{\perp}$, preserves f.

$$\tau_v \in O(f) = \left\{ \underset{\left(\substack{\text{linear} \\ \text{invertible}}\right)}{\rho : \langle 1 \rangle^{\perp} \to \langle 1 \rangle^{\perp}} \;\middle|\; \begin{array}{l} f(\rho(x)) = f(x) \\ \forall x \in \langle 1 \rangle^{\perp} \end{array} \right\}$$

orthogonal group

Suppose $f(u)=f(v)=1$, $(u,v)=0$

Then for $\forall x \in \langle \mathbb{1} \rangle^{\perp}$

$$\tau_u \tau_v (x) = \tau_v \tau_u (x)$$
$$= x + (x,u)u + (x,v)v$$
$$= \sigma_{u,v}(x)$$

(generalized) HKT operation is a nothing but the product of two commuting transvections!

$$\tau_u \in O(f) \longrightarrow \bar{\tau}_u \in O(\bar{f})$$

$$\sigma_{u,v} \in O(f) \longrightarrow \bar{\sigma}_{u,v} \in O(\bar{f})$$

Known:

$$O(\bar{f}) = O^+(2n-2,2) = \langle \bar{\tau}_u \mid u \in \langle 1 \rangle^\perp, f(u)=1 \rangle$$

$$O(\bar{f})' = \Omega^+(2n-2,2) = \left\langle \bar{\sigma}_{u,v} \;\middle|\; \begin{array}{c} u,v \in \langle 1 \rangle^\perp \\ f(u)=f(v)=1 \\ (u,v)=0 \end{array} \right\rangle$$

commutator subgroup

$$|O^+(2n-2,2) : \Omega^+(2n-2,2)| = 2$$

$\Omega^+(2n-2,2)$ is simple

Graph

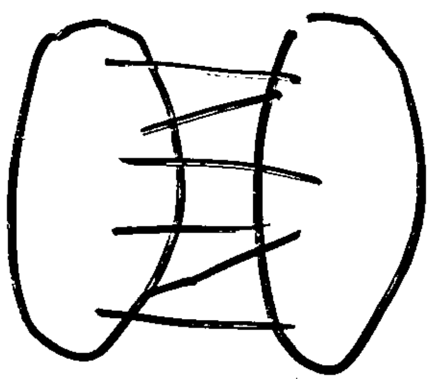
vertex set = {d.e.s.d. codes of length $2n$}

edge : (C, C') with $\dim C \cap C' = n-1$

(dual polar graph of type $D_{n-1}(2)$)

distance-transitive graph

This graph is bipartite



C, C' belong to the same half

$\Longleftrightarrow$ $n - \dim C \cap C' =$ even

$O^{+}(2n-2, 2)$: vertex-transitive

$\Omega^{+}(2n-2, 2)$: leaves the bipartition invariant

<u>Theorem</u> Let C, C' be d.e.s.d. codes of length $2n$. Then

$\exists\ u_1, v_1, \ldots, u_k, v_k \qquad 0 \le k \le \frac{n-2}{2}$

with $f(u_i) = f(v_i) = 1, \quad (u_i, v_i) = 0$

such that C is permutation equivalent to $\sigma_{u_1,v_1}\sigma_{u_2,v_2}\cdots\sigma_{u_k v_k}(C')$.

<u>Sketch of Proof</u>

Reduction: we may assume C, C' belong to the same bipartite half.

τ = transposition $(1,2)$

$\dim C \cap \tau(C) = \dim C \cap \langle v \rangle^{\perp} = n-1$

$C, \tau(C)$ belong to different halves.

If $n - \dim(C \cap C') = $ even, then

$\exists$ sequence of d.e.s.d. codes

$$C = C_0, C_1, C_2, \cdots, C_k = C'$$

$$\dim C_{i-1} \cap C_i = n-2$$

$\exists\ u_i, v_i$ with $f(u_i) = f(v_i) = 1$

$(u_i, v_i) = 0$

$$\sigma_{u_i v_i}(C_{i-1}) = C_i$$

Comments

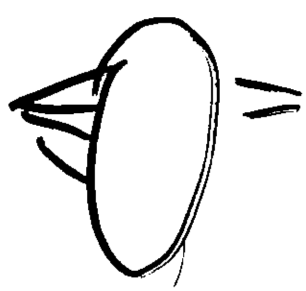
- A similar results can be obtained in the other case : $wt(v) \equiv 0 \pmod 4$

  The requirements are $f(u) = f(v) = (u,v) = 0$

  $$\sigma'_{u,v} = x + (x,u)v + (x,v)u$$
  $$= \text{product of four transvections}$$

  $$\bar{\sigma}'_{u,v} \in \Omega^+(2n-2, 2)$$

$n = 12$

Hamming  Golay doubly-even self-dual binary codes of length $2n$ $/\sim$

$$= \left\{ \left(\begin{array}{c|c} * & 0 \\ \hline * & * \end{array} \right) \right\} \backslash O^{+}(2n-2,2) / S_{2n}$$

Problem

- Enumeration done : $2n \leq 32$
- Find extremal ones as many as possible

$2n = 40$	$> 10{,}000$
$2n = 48$	only one known