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 $2n$.

$$u = (u_1, u_2, \ldots, u_{2n}) \in F_2^{2n}$$

$$v = (v_1, v_2, \ldots, v_{2n}) \in F_2^{2n}$$

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

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

$${f_2}^{2n} \supset C$$ linear code of length $2n$

$$C^\perp := \{ u \in F_2^{2n} \mid (u, v) = 0 \ \forall v \in C \}$$

$C$ is self-dual $\iff$ $C = C^\perp$

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

$\exists$ doubly-even self-dual code of length $2n$ $\iff$ $n \equiv 0 \pmod{4}$
Minimum weight of $C$

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

A doubly-even self-dual binary code $C$ (d.e.s.d) is extremal if

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

\[ \includegraphics{chart.png} \]

| $2n$   | $4\left\lceil \frac{n}{12} \right\rceil + 4$ | $| (\ast \ast \ast \ast \ast / 0^{(2n-2,2)}) / 5_{2n} |$ |
|--------|---------------------------------|----------------------------------|
| 8      | 4                               | 1                               |
| 16     | 4                               | 2                               |
| 24     | 8                               | $8+1$                           |
| 32     | 8                               | $80+5$                          |
| 40     | 8                               | too many                        |
| 72     | 16                              | ?                               |
\( C = \text{Row Space of} \)

\[
\begin{pmatrix}
1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\
\end{pmatrix}
\]

\[= \text{generator matrix of extended binary Hamming [8,4,4]-code} \]

\[
\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{pmatrix}
\]

\[\text{switch } 0 \leftrightarrow 1\]

\[
\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{pmatrix}
\]

\[\text{wt} \]

\[
\begin{array}{ccc}
1+3 & 0k \\
1+3 & 0k \\
1+1 & \text{not ok} \\
1+1 & \text{not ok} \\
\end{array}
\]

\[\text{switch } 0 \leftrightarrow 1\]

\[
\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{pmatrix}
\]

\[\text{again generator matrix of extended binary Hamming [8,4,4]-code} \]
\begin{align*}
\mathbf{r} &= (00101) \\
+ \mathbf{v} &= (00001) \\
\mathbf{r} + \mathbf{v} &= (00100) \\
\mathbf{e} &= (00001) \\
\mathbf{r} + \mathbf{v} + \mathbf{e} &= (00100)
\end{align*}

Suppose \( \text{wt}(\mathbf{v}) = 2 \), first half of \( \mathbf{v} \) = 0

\[ \mathbf{r} \rightarrow \begin{cases} 
\mathbf{r} + \mathbf{v} + \mathbf{e} & \text{if} \quad (\mathbf{r}, \mathbf{v}) = 0 \\
\mathbf{r} + \mathbf{v} & \text{if} \quad (\mathbf{r}, \mathbf{v}) = 1 
\end{cases} \]

\[ = \mathbf{r} + \mathbf{v} + (1 + (\mathbf{r}, \mathbf{v})) \mathbf{e} \]

\[ G = ( \mathbf{I} \mid \mathbf{A}) : \text{generator matrix of a} \]

doubly-even self-dual (d.e.s.d) code of length \(2n\)

\[ v = (0 \cdots 0 \mid \ast \cdots \ast) \quad \text{wt}(v) \equiv 2 \pmod{4} \]

\[ e = (0 \cdots 0 \mid 1 \cdots 1) \]

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

\[ \text{wt}(v) \equiv 0 \pmod{4} \]

\[ r \mapsto r' = r + v + (r,v)e \]

Let us call this \( \text{Harada-Kimura-Tonchev (HKT)} \) 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

\[
G = \begin{pmatrix} I & A \end{pmatrix} \begin{pmatrix} \vdots \\ \vdots \end{pmatrix} \rightarrow G'
\]

\[
u = (0 \cdots 0 | \ast \cdots \ast) \quad \text{wt}(u): \text{even}
\]
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 \((I | A)\)
Recall HKT operation when \( \text{wt}(v) \equiv 2 \pmod{4} \)

\[ \nu = (0 \cdots 0 \, | \, \ast \cdots \ast) \]
\[ \epsilon = (0 \cdots 0 \, | \, 1 \cdots 1) \]

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

\[ r \mapsto r' = r + \nu + (1 + (r, \nu)) \epsilon \]

Since \( (r, \epsilon) = 1 \)

\[ r' = r + (\nu + \epsilon) + (r, \nu) \epsilon \]

\[ = r + (r, \epsilon)(\nu + \epsilon) + (r, \nu) \epsilon \]

is linear in \( r \)!

\[ C \overset{\text{HKT}}{\longrightarrow} C' = \{ x + (x, \epsilon)(\nu + \epsilon) + (x, \nu) \epsilon \mid x \in C \} \]

Rewrite the formula using

\[ [\mu] = \nu + \epsilon \quad \text{and} \quad [\nu] \]
\[
\chi \mapsto \chi + (x, e)(v+e) + (x, v)e
\]
\[
= \chi + (x, u+v)u + (x, v)(u+v)
\]
\[
= \chi + (x, u)u + (x, v)v
\]

Requirements

1. \( \text{wt}(v) \equiv 2 \pmod{4} \)
2. \( \text{wt}(u) \equiv 2 \pmod{4} \)
3. \( (u, v) = 0 \)

If \( u, v \) satisfy (1)–(3) then

\[
\sigma_{u,v}(x) = \chi + (x, u)u + (x, v)v
\]
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
\[ F_{2}^{2n} \ni 1 \text{ all one vector } = (1,1,...,1) \]
\[ \langle 1 \rangle^\perp = \text{parity check code} = \{ \text{vectors of even weight} \} \]
\[ f : \langle 1 \rangle^\perp \to F_2 \text{ is a quadratic form} \]
\[ x \mapsto \frac{\text{wt}(x)}{2} \]

Broué attributes this to Puig (1977),

(\text{not in MacWilliams-Sloane-Thompson (1972)})

\[ f(x+y) = f(x) + f(y) + \langle x,y \rangle \]

follows from

\[ \text{wt}(x+y) = \text{wt}(x) + \text{wt}(y) - 2 \text{wt}(x \vee y) \]

Our requirements are

(1) \[ f(u) = 1 \]
(2) \[ f(v) = 1 \]
(3) \[ (u,v) = 0 \]

{\[ u, v \]} \text{ hyperbolic pair}
Definitions

\( v \in \langle 1 \rangle^+ \) is called singular if \( f(v) = 0 \)

nonsingular if \( f(v) = 1 \)

\( C \subset \langle 1 \rangle^+ \) is called totally singular if

\[ f(v) = 0 \quad \forall v \in C \]

(\( \iff \) doubly-even)

\( \forall \) d.e.s.d. code \( C \) satisfies \( \langle 1 \rangle \subset C \subset \langle 1 \rangle^+ \)

Note \( (\langle 1 \rangle^+) = \langle 1 \rangle \), \( f(1) = 0 \)

So \( f \) induces a nondegenerate quadratic form \( \bar{F} \) on \( \langle 1 \rangle^+/\langle 1 \rangle \)

\[ O(f) \rightarrow O(\bar{f}) = O^+(2n - 2, 2) \]

\( P \rightarrow \bar{P} \)
Then, if $C$ is a d.e.s.d. code
\[
\overline{C} \subset \langle 1 \rangle^\perp / \langle 1 \rangle
\]
\[
\uparrow \quad \uparrow
\]
\[
\text{dim } n-1 \quad \text{dim } 2n-2
\]
(maximal) totally singular
subspace w.r.t. $\bar{f}$.

Theorem (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 \( \nu \in \langle 1 \rangle^\perp \), \( f(\nu) = 1 \).

The transvection \( T_\nu \) with respect to \( \nu \) is

\[
T_\nu(x) = x + (x, \nu) \nu
\]

Then \( T_\nu : \langle 1 \rangle^\perp \to \langle 1 \rangle^\perp \) preserves \( f \).

\[
T_\nu \in O(f) = \{ \rho : \langle 1 \rangle^\perp \to \langle 1 \rangle^\perp \mid f(\rho(x)) = f(x) \}
\]

(\text{linear, invertible}) \quad \forall x \in \langle 1 \rangle^\perp

orthogonal group
Suppose \( f(u) = f(v) = 1 \), \((u,v) = 0\).

Then for \( \forall x \in \langle 1 \rangle^+ \):

\[
\tau_u \tau_v(x) = \tau_v \tau_u(x)
\]

\[
= x + (x, u)u + (x, v)v
\]

\[
= \sigma_{u,v}(x)
\]

(generalized) HKT operation is a nothing but the product of two commuting transvections!
\[ \tau_u \in O(f) \implies \tau_u \in O(f) \]
\[ \sigma_{u,v} \in O(f) \implies \sigma_{u,v} \in O(f) \]

**Known:**

\[ O(f) = O^+(2n-2,2) = \langle \tau_u | u \in \langle 1 \rangle^+, f(u) = 1 \rangle \]
\[ O(f)' = \Omega^+(2n-2,2) = \langle \sigma_{u,v} | u, v \in \langle 1 \rangle^+, f(u) = f(v) = 1, (u, v) = 0 \rangle \]

\[ \uparrow \text{ commutator subgroup} \]

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

\[ \Omega^+(2n-2,2) \text{ is simple} \]
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

\(\iff n - \dim C \cap C' = \text{even}\)

\(O^+(2n-2, 2):\) vertex-transitive
\(\Omega^+(2n-2, 2):\) leaves the bipartition invariant
Theorem: Let \( C, C' \) be d.e.s.d. codes of length \( 2n \). Then

\[ \exists u_i, v_i, \ldots, u_k, v_k \quad 0 \leq k \leq \frac{n-2}{2} \]

with \( f(u_i) = f(v_i) = 1 \), \( (u_i, v_i) = 0 \) such that \( C \) is permutation equivalent to \( \Sigma_{u_i, v_i} \Sigma_{u_2, v_2} \ldots \Sigma_{u_k, v_k} (C') \).

**Sketch of Proof**

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

\[ \tau = \text{transposition } (1, 2) \]

\[ \dim C \cap \tau(C) = \dim C \cap \langle v \rangle^\perp = n - 1 \]

\( C, \tau(C) \) belong to different halves.
If \( n - \dim (C \cap C') = \text{even} \), then

\[ C = C_0, C_1, C_2, \ldots, C_{n-1} = C' \]

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

\[ \exists u_i, v_i \text{ with } f(u_i) = f(v_i) = 1 \]
\[ (u_i, v_i) = 0 \]

\[ \sigma_{u_i,v_i}(C_{i-1}) = C_i \]
Comments

- A similar result can be obtained in the other case: $\text{wt}(u) \equiv 0 \pmod{4}$

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

$\sigma'_u, v = x + (x, u) v + (x, v) u$

= product of four transvections

$\overline{\sigma'}_u, v \in \Omega^+(2n-2, 2)$

$n = 12$

Hamming $\leq \bigcirc = \text{Golay}$
doubly-even self-dual binary codes of length $2n$

$$= \{ (\ast | 0) \} \setminus O^+(2n-2,2) / S_{2n}$$

Problem

• Enumeration done: $2n \leq 32$

• Find extremal ones as many as possible
  $2n = 40$ > 10,000
  $2n = 48$ only one known