Constructive enumeration of self-dual codes using tools from permutation groups

Akihiro Munemasa[1]

[1] Graduate School of Information Sciences
Tohoku University
(joint with K. Betsumiya and M. Harada)

August 25, 2011
International Conference on Coding and Cryptography
Ewha Womans University
Seoul, Korea

Binary Codes

- $\mathbb{F}_2 = \{0, 1\}$.
- $X = \mathbb{F}_2^n$ with $d =$ Hamming distance.
  - $d(x, y) =$ the number of i's with $x_i \neq y_i$, where $x, y \in X$.
  - $d(x, y) = \mathrm{wt}(x - y)$, the weight of the vector $x - y$, the number of nonzero (in this case 1) entries in $x - y$.
  - $\mathrm{supp}(x)$, the support of a vector x, the set of nonzero (in this case 1) coordinates in x.
- $C =$ linear code of length n, i.e., $C \subseteq \mathbb{F}_2^n$, closed under binary addition.
  - $\min(C) := \min\{\mathrm{wt}(x) \mid x \in C,\ x \neq 0\}$.
  - We say C is an $[n, k]$ code if $\dim C = k$.
  - We say C is an $[n, k, d]$ code if moreover $\min(C) = d$.

Equivalence and Automorphisms

Definition

If σ is a permutation on $\{1, 2, \ldots, n\}$ and $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, then $\sigma(x) := (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$. Two binary codes C, C' of length n are said to be equivalent if $\sigma(C) = C'$ for some permutation σ of $\{1, 2, \ldots, n\}$.

Definition

A permutation σ is an automorphism of a linear code $C \subseteq \mathbb{F}_2^n$ if $\sigma(C) = C$. $\mathrm{Aut}(C)$ denotes the group of all automorphisms of C.

Self-Dual Codes

- Scalar product: $(x, y) = \sum_{i=1}^{n} x_i y_i$.
- $C^\perp = \{x \in \mathbb{F}_2^n \mid (x, y) = 0\}$: dual code
- C is self-orthogonal if $C \subset C^\perp$
- C is self-dual if $C = C^\perp$
- C is doubly even if $\mathrm{wt}(c) \equiv 0 \pmod 4$ for all $c \in C$.

Proposition

$C \subset \mathbb{F}_2^n$ is self-dual $\implies$ $\dim C = \frac{n}{2}$.
doubly even $\implies$ self-orthogonal.
doubly even self-dual code exists $\iff$ $n \equiv 0 \pmod 8$.

Extremal Doubly Even Self-Dual Codes

Recall that a doubly even self-dual (d.e.s.d.) code is a linear code C with $C = C^{\perp}$, satisfying $\mathrm{wt}(x) \equiv 0 \pmod 4$ for all $x \in C$.

Proposition (Mallows–Sloane, 1973)

A doubly even self-dual code C of length n satisfies $\min(C) \leq 4[\frac{n}{24}] + 4$.

Definition

A doubly even self-dual code is said to be extremal if $\min(C) = 4[\frac{n}{24}] + 4$.

Table of Doubly Even Self-Dual Codes

length	$\min(C)$	extremal	non-extremal
n	$4[\frac{n}{24}]+4$	codes	codes
8	4	1	
16	4	2	
24	8	1	8
32	8	5	80
40	8	16470	77873
48	12	1	?
56	12	$\geq$166	?
64	12	$\geq$3270	?
72	16	?	?

Pless (1972), Pless–Sloane (1975), Conway–Pless (1980), Conway–Pless–Sloane (1992),
Betsumiya–Harada–Munemasa (2011)

Punctured and shortened codes

Let $S \subset \{1, \dots, n\}$. Let C be a binary linear code of length n.

Definition

The punctured code of C with respect to S is the code obtained from C by restricting to the coordinates $\{1, \dots, n\} \setminus S$.

(forget S)

Definition

The shortened code of C with respect to S is the subcode of C consisting of codewords whose support is disjoint from S, and then deleting the coordinates S.

(forget S only if 0)

The balance principle

Suppose

$$\{1,\dots,n\} = S_1 \cup S_2 \text{ (disjoint)}, \quad |S_1| = n_1,\ |S_2| = n_2.$$

Theorem (The balance principle (Koch 1989))

Let C be a self-dual code of length n.

$$\begin{aligned} C_1 &= \text{the shortend code of } C \text{ with respect to } S_2, \\ C_2 &= \text{the shortend code of } C \text{ with respect to } S_1, \\ k_1 &= \dim C_1,\ k_2 = \dim C_2. \end{aligned}$$

Then

$$n_1 - 2k_1 = n_2 - 2k_2.$$

The balance principle: $n_1 - 2k_1 = n_2 - 2k_2$

A generator matrix of a self-dual code of length $n = n_1 + n_2$ has the following form:

$$\begin{array}{r|c|c|l}
 & n_1 & n_2 & \\ \hline
k_1\{ & C_1 & 0 & \\ \hline
 & 0 & C_2 & \}k_2 \\ \hline
n_1 - 2k_1\{ & C_1^\perp/C_1 & C_2^\perp/C_2 & \}n_2 - 2k_2 \\ \hline
\end{array}$$

$$n_1 - 2k_1 = \dim C_1^\perp/C_1 = n_2 - 2k_2 = \dim C_2^\perp/C_2.$$

$C_1 =$ the shortend code of C with respect to S_2,

$C_2 =$ the shortend code of C with respect to S_1.

Self-dual $[10, 5, 4]$ code does not exist
$n_1 - 2k_1 = n_2 - 2k_2$

$$\begin{array}{r|c|c|l}
 & n_1 = 4 & n_2 = 6 & \\ \cline{2-3}
k_1 = 1\{ & 1\,1\,1\,1 & 0 & \\ \cline{2-3}
 & 0 & 1\,1\,1\,1\,1\,1 & \\
 & 0 & ? & \leftarrow k_2 = 2 \\ \cline{2-3}
n_1 - 2k_1 = 2\{ & * & * & \}n_2 - 2k_2 = 2 \\ \cline{2-3}
\end{array}$$

The balance principle: $n_1 - 2k_1 = n_2 - 2k_2$

Aim: Given C_1, C_2, construct self-dual codes of length $n_1 + n_2$.

$$\begin{array}{r|c|c|l}
 & n_1 & n_2 & \\ \hline
k_1\{ & C_1 & 0 & \\ \hline
 & 0 & C_2 & \}k_2 \\ \hline
n_1 - 2k_1\{ & C_1^\perp/C_1 & C_2^\perp/C_2 & \}n_2 - 2k_2 \\ \hline
\end{array}$$

Filling the last set of rows is equivalent to choosing a linear bijection

$$f : C_1^\perp/C_1 \to C_2^\perp/C_2$$

Then the resulting code is

$$C_f = \{(x|y) \mid x \in C_1^\perp,\ y \in f(x + C_1)\}$$

$$\dim C_f = k_1 + k_2 + n_1 - 2k_1 = \frac{1}{2}(n_1 + n_2).$$

The balance principle: $n_1 - 2k_1 = n_2 - 2k_2$

Proposition

$$C_1 : \text{self-orthogonal } [n_1, k_1] \text{ code}$$
$$C_2 : \text{self-orthogonal } [n_2, k_2] \text{ code}$$

For $f : C_1^\perp/C_1 \to C_2^\perp/C_2$: linear bijection, define

$$C_f = \{(x|y) \mid x \in C_1^\perp,\ y \in f(x + C_1)\}.$$

Then C_f is an $[n_1 + n_2, \frac{1}{2}(n_1 + n_2)]$ code.

When is C_f self-dual (equivalently, self-orthogonal)? This occurs precisely when

$$\forall x, \forall x' \in C_1^\perp,\ \forall y \in f(x+C_1),\ \forall y' \in f(x'+C_1),\ (x, x') = (y, y').$$

C_i: self-orthogonal $[n_i, k_i]$ code for $i = 1, 2$
$C_f = \{(x|y) \mid x \in C_1^\perp,\ y \in f(x + C_1)\}$

Induced scalar product

$$\begin{aligned}(\ , \ ) :& C_1^\perp/C_1 \times C_1^\perp/C_1 \to \mathbb{F}_2 \\ (\ , \ ) :& C_2^\perp/C_2 \times C_2^\perp/C_2 \to \mathbb{F}_2\end{aligned}$$

For a linear bijection $f : C_1^\perp/C_1 \to C_2^\perp/C_2$,

C_f is self-dual ($\iff$ self-orthogonal)

$\iff$ f is an isometry, i.e.,

$$(x + C_1, x' + C_1) = (f(x + C_1), f(x' + C_1)) \quad (\forall x, x' \in C_1^\perp).$$

Special case: $n_2 = 2$, $C_2 = 0$

C_1	0
0	C_2
$C_1^{\perp}/C_1$	$C_2^{\perp}/C_2$

becomes

$$\begin{array}{r|c|c|l} & n_1 & 2 & \\ \cline{2-3} k_1\{ & C_1 & 0 & \\ \cline{2-3} n_1 - 2k_1\{ & C_1^{\perp}/C_1 & 0^{\perp} & \}2 = 1 + 1 \\ \cline{2-3} \end{array}$$

Then $k_1 = \frac{1}{2}n_1 - 1$.
$\Longrightarrow$ C_1 is a subcode of of codimension 1 in a self-dual $[n_1, \frac{1}{2}n_1]$ code $\tilde{C}_1$.

Special case: $n_2 = 2$, $C_2 = 0$

C_1	0
x	$1\,1$
y	$0\,1$

$$C_1 \subset \langle C_1, x\rangle = \tilde{C}_1 : \text{ self-dual } [n_1, \tfrac{1}{2}n_1] \text{ code}$$

Every self-dual $[n_1 + 2, \frac{1}{2}n_1 + 1, d]$ code with $d > 2$ can be obtained from

- a self-dual $[n_1, \frac{1}{2}n_1]$ code $\tilde{C}_1$,
- an $[n_1, \frac{1}{2}n_1 - 1]$ subcode C_1 of $\tilde{C}_1$,
- $y \in C_1^{\perp}$ with $\mathrm{wt}(y)$ odd

Actually y and C_1 determine each other.

Special case: $n_2 = 2$, $C_2 = 0$

In practice one starts from a self-dual $[n_1, \frac{1}{2}n_1]$ code $\tilde{C}_1$

$\tilde{C}_1$	0 $1\,1$
y	$0\,1$

Then y determines C_1 as $\tilde{C}_1 \cap y^\perp$.
Alternatively, C_1 can be specified as a kernel of a nonzero linear mapping $\tilde{C}_1 \to \mathbb{F}_2$ (building-up method).

General case: $n_1 - 2k_1 = n_2 - 2k_2$
C_i: self-orthogonal $[n_i, k_i]$ code for $i = 1, 2$

C_1	0
0	C_2
$C_1^{\perp}/C_1$	$C_2^{\perp}/C_2$

Assume $\mathbf{1} \in C_1$, $\mathbf{1} \in C_2$ (so n_1 and n_2 are even). The induced scalar products on $C_1^{\perp}/C_1$, $C_2^{\perp}/C_2$ are symplectic. A linear bijection

$$f : C_1^{\perp}/C_1 \to C_2^{\perp}/C_2$$

corresponds to an element of $\mathrm{Sp}(2m, 2)$ $(2m = n_1 - 2k_1)$

$$|\,\mathrm{Sp}(2m, 2)| = 2^{m^2} \prod_{i=1}^{m} (2^{2i} - 1).$$

General case: $n_1 - 2k_1 = n_2 - 2k_2$ C_i: self-orthogonal $[n_i, k_i]$ code for $i = 1, 2$ $f : C_1^\perp/C_1 \to C_2^\perp/C_2$ $C_f = \{(x|y) \mid x \in C_1^\perp,\ y \in f(x + C_1)\}$

$$\sigma_i \in \operatorname{Aut} C_i \implies \sigma_i \text{ induces } C_i^\perp/C_i \to C_i^\perp/C_i$$
$$\sigma_2 \circ f \circ \sigma_1 : C_1^\perp/C_1 \to C_2^\perp/C_2$$

Then $C_f \cong C_{\sigma_2 \circ f \circ \sigma_1}$. This means that

$$\{\text{isometries } f\} \to \{\text{self-dual codes obtained from } C_1, C_2\}$$

induces

$$\begin{aligned} &\operatorname{Aut} C_2 \backslash \operatorname{Sp}(2m, 2) / \operatorname{Aut} C_1 \\ &\to \{\text{self-dual codes obtained from } C_1, C_2\}/\cong . \end{aligned}$$

General case

Theorem

Let C_i be a self-orthogonal $[n_i, k_i]$ code $\ni \mathbf{1}$ for $i = 1, 2$, and assume $n - 2k_1 = n_2 - 2k_2 = 2m$. Then there is a mapping from $\operatorname{Aut} C_2 \backslash \operatorname{Sp}(2m, 2) / \operatorname{Aut} C_1$ to the set of equivalence classes of self-dual codes with generator matrix of the form

$$\begin{array}{|c|c|l}
\hline
C_1 & 0 & \\
\hline
0 & C_2 & \\
\hline
C_1^\perp/C_1 & C_2^\perp/C_2 & \leftarrow f \\
\hline
\end{array}$$

Doubly even version

$\mathrm{O}^+(2m, 2) =$ orthogonal group.

Theorem

Let C_i be a doubly even $[n_i, k_i]$ code $\ni \mathbf{1}$ for $i = 1, 2$, and assume $n - 2k_1 = n_2 - 2k_2 = 2m$, $n_1 \equiv n_2 \equiv 0 \pmod 8$. Then there is a mapping from $\operatorname{Aut} C_2 \backslash \mathrm{O}^+(2m, 2) / \operatorname{Aut} C_1$ to the set of equivalence classes of doubly even self-dual codes with generator matrix of the form

$$\begin{array}{|c|c|l}
\hline
C_1 & 0 & \\
\hline
0 & C_2 & \\
\hline
C_1^\perp / C_1 & C_2^\perp / C_2 & \leftarrow f \\
\hline
\end{array}$$

We now apply this theorem with $n_1 = 16$, $n_2 = 24$.

Doubly even self-dual $[40, 20, 8]$ codes

C_1: doubly even $[16, k_1]$ code $\ni \mathbf{1}$
C_2: doubly even $[24, k_2]$ code $\ni \mathbf{1}$
$16 - 2k_1 = 24 - 2k_2 = 2m$.
There is a mapping from $\operatorname{Aut} C_2 \backslash \mathrm{O}^+(2m, 2) / \operatorname{Aut} C_1$ to the set of equivalence classes of doubly even self-dual codes with generator matrix of the form

C_1	0
0	C_2
$C_1^\perp / C_1$	$C_2^\perp / C_2$

Possible C_1, C_2 can easily be enumerated for all k_1, k_2.
However ...

Doubly even self-dual $[40, 20, 8]$ codes

C_1: doubly even $[16, k_1]$ code $\ni \mathbf{1}$
C_2: doubly even $[24, k_2]$ code $\ni \mathbf{1}$
$\textsc{Magma}$ could not compute $\operatorname{Aut} C_2 \backslash \mathrm{O}^+(2m, 2) / \operatorname{Aut} C_1$ when $m \geq 6$.
Thus we need:

$$16 - 2k_1 = 24 - 2k_2 = 2m \leq 10,$$

or equivalently, $k_1 \geq 3$.
We obtain a classification of doubly even self-dual $[40, 20, 8]$ codes containing a $[16, \geq 3]$ code $(\ni \mathbf{1})$ as a shortened code.
There are 16468 codes up to equivalence.

Doubly even self-dual $[40, 20, 8]$ codes

- King (2001) computed (without classifying) the total number of doubly even self-dual $[40, 20, 8]$ codes:

  $1026333556700356741507680351328762798054416384 0000000$

- We found 16468 codes up to equivalence, whose total number is

  $1026332864842368022530069356512189163921055744 0000000$

Slightly short of complete!
There is at least one doubly even self-dual $[40, 20, 8]$ code which does not contain $[16, \geq 3]$ code $(\ni \mathbf{1})$ as a shortened code.

16468+2 doubly even self-dual $[40, 20, 8]$ codes

Theorem

1. There are exactly two (up to equivalence) doubly even self-dual $[40, 20, 8]$ codes which do not contain $[16, \geq 3]$ code $(\ni \mathbf{1})$ as a shortened code.
2. There are 16470 (up to equivalence) doubly even self-dual $[40, 20, 8]$ codes.

Remark

- The two exceptional codes appeared already in the work of Yorgov (1983) and Yorgov–Zyapkov (1996).
- We have no direct proof of Part 1 of the above theorem.
- Similar consideration played an important role in the proof (by computer) of the uniqueness of doubly even self-dual $[48, 24, 12]$ code by Houghten–Lam–Thiel–Parker (2003).