Codes Generated by Designs, and Designs Supported by Codes Part III

Akihiro Munemasa[1]

[1]Graduate School of Information Sciences
Tohoku University

May, 2013
CIMPA-UNESCO-MESR-MINECO-THAILAND
research school
Graphs, Codes, and Designs
Ramkhamhaeng University

Contents

Summary of Part I and II

$\mathcal{D}$: 5-$(24, 8, 1)$ design (Witt system).

- The binary code C of $\mathcal{D}$ is a doubly even self-dual $[24, 12, 8]$ code.
- $\{\mathrm{supp}(x) \mid x \in C,\ \mathrm{wt}(x) = 8\} = \mathcal{B}$.
- There is a unique 5-$(24, 8, 1)$ design up to isomorphism.
- There is a unique doubly even self-dual $[24, 12, 8]$ code (up to isomorphism), by the Assmus–Mattson theorem.

Part III will cover

- Hadamard matrices
- Characterization of Hadamard matrices contained in the doubly even self-dual $[24, 12, 8]$ code, and their relationships to ternary self-dual codes

Hadamard matrices

Definition

A Hadamard matrix of order n is an $n \times n$ matrix with entries ± 1, such that rows are pairwise orthogonal:

- H: $n \times n$ matrix,
- $H_{i,j} \in \{\pm 1\}$ for all $i, j \in \{1, \dots, n\}$,
- $HH^\top = nI$.

Example

The Hadamard matrix of Sylvester type, where $n = 2^v$:

$$H = ((-1)^{x \cdot y})_{x,y \in \mathbb{F}_2^v}.$$

$$v = 1 \implies H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Hadamard matrices of Sylvester type, $n = 2^v$

$$v = 2 \implies H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

$$v = 3 \implies H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \end{bmatrix}$$

Existence of Hadamard matrices

A Hadamard matrix of order n exists for

$$n = 1, 2, 4, 8, 12, 16, \ldots \text{(multiples of 4)}, \ldots, 664, \ldots$$

Except $n = 1, 2$, the existence of a Hadamard matrix of order n implies $n \equiv 0 \pmod 4$:

$$\begin{array}{cccc}
1 \cdots 1 & 1 \cdots 1 & 1 \cdots 1 & 1 \cdots 1 \\
1 \cdots 1 & 1 \cdots 1 & -1 \cdots -1 & -1 \cdots -1 \\
1 \cdots 1 & -1 \cdots -1 & 1 \cdots 1 & -1 \cdots -1
\end{array}$$

But it is not known whether a Hadamard matrix of order 668 exists.

Conjecture

A Hadamard matrix of order n exists for any $n \equiv 0 \pmod 4$.

Sylvester type: $n = 2^v = 1, 2, 4, 8, 16, \ldots$.

Classification of Hadamard matrices

If H is a Hadamard matrix, then so is $H^\top$.
Two Hadamard matrices are said to be equivalent if one is obtained from the other by row or column permutations or negations:

$$H_1 \cong H_2 \iff \exists P, Q,\ PH_1Q = H_2,$$

where P and Q are matrices in which only 1 or -1 appear exactly once in every row and once in every column, all other entries are 0.
The numbers of equivalence classes of Hadamard matrices are known for orders up to 32.

order	1	2	4	8	12	16	20	24	28	32
number	1	1	1	1	1	5	3	60	487	13,710,027

16, 20: Hall; 24: Ito–Leon–Longyear, Kimura; 28: Kimura, Spence; 32: Kharaghani and Tayfeh-Rezaie (2012).

Normalized and binary Hadamard matrices

Every Hadamard matrix is equivalent to the one with 1 everywhere in the first row:

$$H = \begin{bmatrix} 1 & 1 \cdots 1 \\ & \cdots \\ & \pm 1 \\ & \cdots \end{bmatrix}$$

Such a Hadamard matrix H is said to be normalized. The binary Hadamard matrix associated to H is

$$B = \frac{1}{2}(H + J) = \begin{bmatrix} 1 & 1 \cdots 1 \\ & \cdots \\ & 1 \text{ or } 0 \\ & \cdots \end{bmatrix} = \begin{bmatrix} \mathbf{1} \\ b^{(1)} \\ \vdots \\ b^{(n-1)} \end{bmatrix}$$

Hadamard 3-design

- H: a normalized Hadamard matrix of order n.
- $B = \frac{1}{2}(H + J)$: the associated binary Hadamard matrix. B has row vectors $b^{(0)} = \mathbf{1}$, $b^{(1)}, \dots, b^{(n-1)}$.

$$\mathcal{P} = \{1, \dots, n\},$$
$$\mathcal{B} = \bigcup_{i=1}^{n-1} \{\mathrm{supp}(b^{(i)}), \mathrm{supp}(\mathbf{1} + b^{(i)})\}.$$

Then $(\mathcal{P}, \mathcal{B})$ is a 3-$(n, \frac{n}{2}, \frac{n}{4} - 1)$ design. Indeed, consider the transpose of

$$\begin{matrix} 1\cdots 1 & 1\cdots 1 & 1\cdots 1 & 1\cdots 1 \\ 1\cdots 1 & 1\cdots 1 & -1\cdots -1 & -1\cdots -1 \\ 1\cdots 1 & -1\cdots -1 & 1\cdots 1 & -1\cdots -1 \\ \mathbf{1}^\top \end{matrix} \quad \text{in} \begin{bmatrix} H \\ -H \end{bmatrix}$$

The isomorphism class of Hadamard 3-design

Definition

Two designs $(\mathcal{P}, \mathcal{B})$ and $(\mathcal{P}', \mathcal{B}')$ are said to be isomorphic if there is a bijection from $\mathcal{P}$ to $\mathcal{P}'$ which maps $\mathcal{B}$ to $\mathcal{B}'$.

$$\begin{array}{rl} & H \xrightarrow{\text{normalize}} B \to (\mathcal{P}, \mathcal{B}) \\ \text{swap rows} & \downarrow \\ & H' \xrightarrow{\text{normalize}} B' \to (\mathcal{P}, \mathcal{B}') \end{array}$$

In general, $(\mathcal{P}, \mathcal{B}) \not\cong (\mathcal{P}, \mathcal{B}')$

Definition

The binary code of a Hadamard matrix H is defined as that of the Hadamard 3-design $(\mathcal{P}, \mathcal{B})$ obtained from the binary Hadamard matrix associated to any normalized Hadamard matrix equivalent to H.

Is it well defined?

The isomorphism class of the binary code

$$H = \begin{bmatrix} \mathbf{1} \\ h^{(1)} \\ \vdots \\ h^{(n-1)} \end{bmatrix} \longrightarrow B = \frac{1}{2}(H+J) = \begin{bmatrix} \mathbf{1} \\ b^{(1)} \\ \vdots \\ b^{(n-1)} \end{bmatrix}$$

$$\begin{bmatrix} h^{(1)} \\ \mathbf{1} \\ \vdots \\ h^{(n-1)} \end{bmatrix} \to H' = \begin{bmatrix} \mathbf{1} \\ h^{(1)} \\ h^{(2)} * h^{(1)} \\ \vdots \\ h^{(n-1)} * h^{(1)} \end{bmatrix} \to B' = \frac{1}{2}(H'+J) = \begin{bmatrix} \mathbf{1} \\ b^{(1)} \\ b^{(2)} + b^{(1)} + \mathbf{1} \\ \vdots \\ b^{(n-1)} + b^{(1)} + \mathbf{1} \end{bmatrix}$$

$h^{(1)}$	$h^{(2)}$	$h^{(1)} * h^{(2)}$	$b^{(1)}$	$b^{(2)}$	$b^{(1)} + b^{(2)} + \mathbf{1}$
1	1	1	1	1	1
1	−1	−1	1	0	0
−1	1	−1	0	1	0
−1	−1	1	0	0	1

B and B' generate the same binary code

Normalized and binary Hadamard matrices

$$H = \begin{bmatrix} \mathbf{1} \\ h^{(1)} \\ \vdots \\ h^{(n-1)} \end{bmatrix} \longrightarrow B = \frac{1}{2}(H + J) = \begin{bmatrix} \mathbf{1} \\ b^{(1)} \\ \vdots \\ b^{(n-1)} \end{bmatrix}$$

Then

- B has first row $\mathbf{1}$, the vector with weight n.
- All the other rows have weight $\frac{n}{2}$.
- Two distinct rows of weight $\frac{n}{2}$ have $\frac{n}{4}$ coordinates in common in their supports.
- $n \equiv 0 \pmod 8 \implies$ the binary code of H is self-orthogonal.

The binary code of a Hadamard matrix

Lemma

Let C be the binary code of a Hadamard matrix of order n.

- If $n \equiv 0 \pmod 8$, then C is doubly even self-orthogonal.
- If $n \equiv 8 \pmod{16}$, then C is doubly even self-dual.

In particular, for $n = 24$, C is doubly even self-dual.

- One can ask: which of the 60 Hadamard matrices of order 24 give the extended binary Golay code?
- Among the 60 Hadamard matrices of order 24, only two give the extended binary Golay code.

Ternary codes

A (linear) ternary code of length n is a subspace of the vector space $\mathbb{F}_3^n$. If C is a ternary code and $\dim C = k$, we say C is an ternary $[n, k]$ code. The dual code of a ternary code C is defined as

$$C^\perp = \{x \in \mathbb{F}_3^n \mid x \cdot y = 0 \ (\forall y \in C)\}.$$

where

$$x \cdot y = \sum_{i=1}^{n} x_i y_i.$$

Then $\dim C^\perp = n - \dim C$. The code C is said to be self-orthogonal if $C \subset C^\perp$ and self-dual if $C = C^\perp$.
Two ternary codes are said to be isomorphic if one is obtained from the other by permutation and negation of coordinates.

Generator matrix of a ternary code

If a ternary code C of length n is generated by row vectors $x^{(1)}, \dots, x^{(m)}$, then the matrix

$$\begin{bmatrix} x^{(1)} \\ \vdots \\ x^{(m)} \end{bmatrix}$$

is called a generator matrix of C. This means

$$C = \{\sum_{i=1}^{m} \epsilon_i x^{(i)} \mid \epsilon_1, \dots, \epsilon_m \in \mathbb{F}_3\} \subset \mathbb{F}_3^n.$$

Definition

The ternary code of a Hadamard matrix H is the ternary code with generator matrix H.

Weight

For $x \in \mathbb{F}_3^v$, we write

$$\begin{aligned} \operatorname{supp}(x) &= \{i \mid 1 \le i \le v,\ x_i \ne 0\}, \\ \operatorname{wt}(x) &= |\operatorname{supp}(x)|. \end{aligned}$$

For a ternary code C, its minimum weight is

$$\min\{\operatorname{wt}(x) \mid 0 \ne x \in C\}.$$

If an $[v, k]$ ternary code C has minimum weight d, we call C an $[v, k, d]$ code.

Ternary self-dual codes of length 24

Lemma

Let n be an integer divisible by 4. If $3|n$ and $9 \nmid n$, then the ternary code of a Hadamard matrix of order n is self-dual.

In particular, the ternary code of a Hadamard matrix of order 24 is self-dual.

- Leon–Pless–Sloane (1981): there are two self-dual codes of length 24 with minimum weight 9 (largest possible), up to isomorphism.
- One can ask: which of the 60 Hadamard matrices of order 24 give the codes with minimum weight 9?
- Among the 60 Hadamard matrices of order 24, only two give codes with minimum weight 9.

Verification using MAGMA

Assmus and Key in their 1992 book observed:

```
DB:=HadamardDatabase();
NumberOfMatrices(DB,24) eq 60;
H24s:=[Matrix(DB,24,i):i in [1..60]];
normalize:=func<H|H*DiagonalMatrix(Eltseq(H[1]))>;
J:=Matrix(Integers(),24,24,[1:i in [1..24^2]]);
bH:=func<H|Parent(H)![x div 2:x in Eltseq(normalize(H)+J)]>;
bC:=func<H|LinearCode(ChangeRing(bH(H),GF(2)))>;
tCT:=func<H|LinearCode(ChangeRing(Transpose(H),GF(3)))>;
[i:i in [1..60]|MinimumWeight(bC(H24s[i])) eq 8] eq [3,9];
[i:i in [1..60]|MinimumWeight(tCT(H24s[i])) eq 9] eq [3,9];
```

Assmus and Key, 1992

Fact

Let H be a Hadamard matrix of order 24. The following are equivalent.

- The binary code of H has minimum weight 8 (largest).
- The ternary code of $H^\top$ has minimum weight 9 (largest).

- The binary code of H is doubly even self-dual, and the minimum weight is 4 or 8.
- The ternary code of $H^\top$ is self-dual, and the minimum weight is 6 or 9. (A ternary self-dual code may have minimum weight 3, but no ternary code of a Hadamard matrix has minimum weight 3).
- There are two (up to equivalence) Hadamard matrices H satisfying the above equivalent conditions.

H: a normalized Hadamard matrix of order 24

- C_2: the binary code of $H =$ the binary code with generator matrix $B = \frac{1}{2}(H + J)$.
- C_3: the ternary code of $H^\top$.
- C_2 is doubly even self-dual, and C_3 is self-dual.
- C_2 has only weights divisible by 4, C_3 has only weights divisible by 3.

Fact

The following are equivalent:

- C_2 has minimum weight 8 (largest).
- C_3 has minimum weight 9 (largest).

We first show: $C_3 = C_3^\perp$ has no vectors of weight 3.

C_3: the ternary code of $H^\top$ (n is arbitrary)

Suppose

$$\begin{aligned} C_3^\perp &= \{v \in \mathbb{F}_3^n \mid H^\top v^\top = 0\} \\ &= \{v \bmod 3 \mid v \in \mathbb{Z}^n,\ vH \equiv 0 \pmod 3\} \end{aligned}$$

contains a vector v of weight 3:

$$v = (0, \dots, 0, \epsilon_i, 0, \dots, 0, \epsilon_j, 0, \dots, 0, \epsilon_k, 0, \dots, 0)$$

where $\epsilon_i, \epsilon_j, \epsilon_k \in \{\pm 1\}$.

$$\begin{aligned} & vH \equiv 0 \pmod 3 \\ \implies & \epsilon_i H_{i,\ell} + \epsilon_j H_{j,\ell} + \epsilon_k H_{k,\ell} \equiv 0 \pmod 3 \quad (\forall \ell \in \{1, \dots, n\}) \\ \implies & \epsilon_i H_{i,\ell} = \epsilon_j H_{j,\ell} = \epsilon_k H_{k,\ell} \quad (\forall \ell \in \{1, \dots, n\}) \\ \implies & \epsilon_j \epsilon_i H_{i,\ell} = H_{j,\ell} \quad (\forall \ell \in \{1, \dots, n\}) \\ \implies & \text{row } i \text{ of } H = \text{row } j \text{ of } H, \text{ up to sign} \end{aligned}$$

This is impossible for a Hadamard matrix H.

$C_3^\perp$ does not have weight 3

- H: a normalized Hadamard matrix of order 24
- C_2: the binary code of $H =$ the binary code with generator matrix $B = \frac{1}{2}(H + J)$.
- C_3: the ternary code of $H^\top$.
- C_2 is doubly even self-dual, and C_3 is self-dual.
- C_2 has only weights divisible by 4, C_3 has only weights divisible by 3.
- $C_3 = C_3^\perp$ does not have weight 3

Fact

The following are equivalent:

- C_2 has minimum weight 8 (i.e., C_2 doesn't have weight 4)
- C_3 has minimum weight 9 (i.e., C_2 doesn't have weight 6)

H: a normalized Hadamard matrix of order 24

- C_2: the binary code of $H =$ the binary code with generator matrix $B = \frac{1}{2}(H + J)$.
- C_3: the ternary code of $H^\top$.

Theorem

The following are equivalent.

- C_2 has weight 4.
- C_3 has weight 6.

H: a normalized Hadamard matrix of order 24

- $C_2 = \{vB \bmod 2 \mid v \in \mathbb{Z}^{24}\}$: the binary code of H, $B = \frac{1}{2}(H + J)$.
- $C_3 = \{v \bmod 3 \mid v \in \mathbb{Z}^{24},\ vH \equiv 0 \pmod 3\}$: the ternary code of $H^\top$.

Theorem

The following are equivalent.

1. C_2 has weight 4.
2. C_3 has weight 6.

Proof of ($2 \implies 1$). $v \in \{0, \pm 1\}^{24} \subset \mathbb{Z}^{24}$, $\mathrm{wt}(v) = 6$, $vH \equiv 0 \pmod 3$. Set

$$u = \frac{1}{6} vH.$$

Then $u \in \mathbb{Z}^{24}$, $u \bmod 2 \in C_2$, $\mathrm{wt}(u \bmod 2) = 4$.

Hadamard matrices and norms

Lemma

Let H be a Hadamard matrix of order n, v a vector in $\mathbb{Z}^n$. Then

- $vH \equiv \|v\|^2\mathbf{1} \pmod 2$,
- $\|vH\|^2 = n\|v\|^2$.

Proof.

$$vH \equiv vJ = (\sum_{i=1}^{n} v_i)\mathbf{1} \equiv (\sum_{i=1}^{n} v_i^2)\mathbf{1} = \|v\|^2\mathbf{1} \pmod 2.$$

$$\|vH\|^2 = vHH^\top v^\top = v(nI)v^\top = n\|v\|^2.$$

□

H: a normalized Hadamard matrix of order 24

- $C_2 = \{vB \bmod 2 \mid v \in \mathbb{Z}^{24}\}$: the binary code of H, $B = \frac{1}{2}(H + J)$.
- $v \in \{0, \pm 1\}^{24} \subset \mathbb{Z}^{24}$, $\mathrm{wt}(v) = 6$, $vH \equiv 0 \pmod 3$.

$$u = \frac{1}{6} vH \implies u \in \mathbb{Z}^{24},\ \mathrm{wt}(u \bmod 2) = 4,\ u \bmod 2 \in C_2.$$

Lemma

- $vH \equiv \|v\|^2 \mathbf{1} \pmod 2$,
- $\|vH\|^2 = n\|v\|^2 = 24\|v\|^2$.

Since $\|v\|^2 = \mathrm{wt}(v) = 6$, $vH \equiv \|v\|^2 \mathbf{1} \equiv 0 \pmod 2$. Thus $vH \equiv 0 \pmod 6$, and $u \in \mathbb{Z}^{24}$.

$$\|u\|^2 = \frac{1}{6^2} 24 \|v\|^2 = \frac{24 \cdot 6}{6^2} = 4 \implies \mathrm{wt}(u \bmod 2) = 4.$$

H: a normalized Hadamard matrix of order 24

- $C_2 = \{vB \bmod 2 \mid v \in \mathbb{Z}^{24}\}$: the binary code of H, $B = \frac{1}{2}(H + J)$.
- $v \in \{0, \pm 1\}^{24} \subset \mathbb{Z}^{24}$, $\mathrm{wt}(v) = 6$, $vH \equiv 0 \pmod 3$.

$$u = \frac{1}{6}vH \implies u \in \mathbb{Z}^{24},\ \mathrm{wt}(u \bmod 2) = 4,\ u \bmod 2 \in C_2.$$

$$\begin{aligned}
u &\equiv \frac{3}{6}vH \pmod 2 \\
&= \frac{1}{2}v(2B - J) = vB - \frac{1}{2}vJ \\
&\equiv vB + \epsilon\mathbf{1} \pmod 2 \quad (\epsilon \in \{0, 1\}) \\
&= (v + \epsilon e_1)B \in C_2 \quad \text{(after reducing mod 2).}
\end{aligned}$$

H: a normalized Hadamard matrix of order 24

- C_2: the binary code of H = the binary code with generator matrix $B = \frac{1}{2}(H + J)$.
- C_3: the ternary code of $H^\top$.

Then C_2 is doubly even self-dual, and C_3 is self-dual.

Theorem (Munemasa–Tamura, 2012)

The following are equivalent:

1. C_2 has minimum weight 8 (largest).
2. C_3 has minimum weight 9 (largest).

We have proved $1 \implies 2$ by showing its contrapositive assertion. The other implication can be proved similarly.

H: a normalized Hadamard matrix of order 48

Similarly, one can consider a code over $\mathbb{Z}/4\mathbb{Z}$, the ring of integers modulo 4. The Euclidean weight of a vector $v \in (\mathbb{Z}/4\mathbb{Z})^n$ is

$$\mathrm{wt}(v) = \sum_{i=1}^{n} v_i^2,$$

where we regard $v_i \in \{0, \pm 1, 2\} \subset \mathbb{Z}$.

Theorem

- C_4: the code over $\mathbb{Z}/4\mathbb{Z}$ with generator matrix $B = \frac{1}{2}(H + J)$.
- C_3: the ternary code of $H^\top$.

Then both C_4 and C_3 are self-dual. Moreover, the following are equivalent:

- C_4 has minimum Euclidean weight 24 (largest).
- C_3 has minimum weight 15 (largest).

Hadamard matrices of order 48 and ternary codes

Theorem

If C is a ternary self-dual code of length 48 and minimum weight 15, then C is generated by a Hadamard matrix.

Unlike the case $n = 24$, the following problem is still open.

Problem

Classify ternary self-dual codes of length 48 with minimum weight 15, or classify Hadamard matrices of order 48 which generate such a code.

Extremal ternary self-dual codes

Theorem (Mallows–Sloane, 1973)

For $m \geq 1$, a ternary self-dual $[12m, 6m]$ code has minimum weight at most $3m + 3$.

Definition

A ternary self-dual $[12m, 6m]$ code with minimum weight $3m + 3$ is called extremal.

- $m = 1$: the extended ternary Golay code and the 5-$(12, 6, 1)$ design,
- $m = 2$: exactly two codes,
- $m = 3$: at least one code,
- $m = 4$: at least two codes,
- $m = 5$: at least two codes.

All these codes are generated by a Hadamard matrix.

Extremal ternary self-dual codes

Definition

A ternary self-dual $[12m, 6m]$ code with minimum weight $3m + 3$ is called extremal.

For $m \geq 6$, no code is known. In fact, for m even and $m \geq 6$, an extremal ternary self-dual $[12m, 6m, 3m + 3]$ code does not exist.

Theorem (Zhang, 1999)

There does not exist an extremal $[12m, 6m, 3m + 3]$ ternary self-dual code for $m \geq 70$.