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

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

1. Part I
   - t-designs
   - intersection numbers
   - 5-$(24, 8, 1)$ design
   - $[24, 12, 8]$ binary self-dual code
2. Part II
   - Assmus–Mattson theorem
   - extremal binary doubly even codes
3. Part III
   - Hadamard matrices
   - ternary self-dual codes

Summary of Part I

$\mathcal{D}$: 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.

The Assmus–Mattson theorem implies that every doubly even self-dual $[24, 12, 8]$ code gives rise to a 5-$(24, 8, 1)$ design, and hence such a code (the extended binary Golay code) is also unique.

Part II will cover

- proof of the Assmus–Mattson theorem
- other 5-designs obtained from doubly even self-dual codes

The Assmus–Mattson theorem (1969)

Let C be a binary code of length v, minimum weight k.

$$\begin{aligned}
\mathcal{P} &= \{1, 2, \ldots, v\}, \\
\mathcal{B} &= \{\mathrm{supp}(x) \mid x \in C,\ \mathrm{wt}(x) = k\}, \\
S &= \{\mathrm{wt}(x) \mid x \in C^\perp,\ 0 < \mathrm{wt}(x) < v\}, \\
t &= k - |S|.
\end{aligned}$$

Then $(\mathcal{P}, \mathcal{B})$ is a t-(v, k, λ) design for some λ.

In fact

$$\lambda = \frac{k(k-1)\cdots(k-t+1)}{v(v-1)\cdots(v-t+1)}|\mathcal{B}|.$$

The real vector space of dimension 2^v

From a t-(v,k,λ) design $(\mathcal{P},\mathcal{B})$,

- $p \in \mathcal{P} \to e_p$: a unit vector in $\mathbb{F}_2^v$.
- $B \in \mathcal{B} \to x^{(B)} \in \mathbb{F}_2^v$: characteristic vector
- $\mathcal{B} \to M(\mathcal{D})$: incidence matrix $\to C \subset \mathbb{F}_2^v$: binary code

From a binary code C of length v and $B \subset \{1,2,\dots,v\}$,
$V = \mathbb{R}^{2^v} = \mathbb{R}^{\mathbb{F}_2^v}$.

- $x \in \mathbb{F}_2^v \to \hat{x}$: a unit vector in V
- $B \to x^{(B)} \in \mathbb{F}_2^v \to \widehat{x^{(B)}}$: a unit vector in V
- $\mathcal{B} \to \{x^{(B)} \mid B \in \mathcal{B}\} \to$ characteristic vector in V
- $C \to \hat{C}$: the characteristic vector of C in V

Important $2^v \times 2^v$ matrices

The linear transformation of $V = \mathbb{R}^{2^v}$ which is a key to the argument below is the Hadamard matrix of Sylvester type:

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

It satisfies

$$H = H^\top, \quad H^2 = HH^\top = 2^v I.$$

We use H to investigate the metric space $\mathbb{F}_2^v$ with the Hamming distance

$$d(x,y) = \mathrm{wt}(x+y) \quad (x, y \in \mathbb{F}_2^v).$$

The i-th distance matrix A_i is defined as

$$A_i = (\delta_{d(x,y),i})_{x,y \in \mathbb{F}_2^v} \quad (0 \le i \le v).$$

A_i: the i-th distance matrix

$$
\begin{aligned}
A_0 &= I, \\
A_1 A_i &= (i+1)A_{i+1} + (v-i+1)A_{i-1} \quad (1 \le i < v).
\end{aligned}
$$

In particular, A_i is a polynomial of degree i in A_1.
Define the diagonal matrix E_i^* by

$$
\begin{aligned}
E_i^* &= (\delta_{x,y}\delta_{\mathrm{wt}(x),i})_{x,y\in\mathbb{F}_2^v} \\
&= \mathrm{diag}(A_i\hat{0}).
\end{aligned}
$$

E_i^* is "the projection onto weight-i vectors."

$$E_i^*\mathbf{1} = A_i\hat{0}, \qquad \text{where } \mathbf{1} = (1,1,\dots,1)^\top \in V.$$

$$E_i^* E_j^* = \delta_{i,j} E_i^*, \quad \sum_{i=0}^{v} E_i^* = I.$$

E_i^* is "the projection onto weight-i vectors."

Theorem (Assmus–Mattson)

Let C be a binary code of length v,

$$\hat{C} = E_0^*\hat{C} + \sum_{i\geq k} E_i^*\hat{C} \quad (\text{minimum weight} = k),$$

$$\mathcal{P} = \{1, 2, \ldots, v\},$$

$$S = \{\mathrm{wt}(x) \mid x \in C^{\perp},\ 0 < \mathrm{wt}(x) < v\},$$

$$\mathcal{B} = \{\mathrm{supp}(x) \mid x \in C,\ \mathrm{wt}(x) = k\},$$

$$t = k - |S|.$$

Then $(\mathcal{P}, \mathcal{B})$ is a t-(v, k, λ) design for some λ.

(S can also be described by E_i^* and $\widehat{C^{\perp}}$, but we first express the conclusion in terms of matrices.)

Design property expressed by matrices

- $T \subset \mathcal{P}$, $|T| = t$, $x^{(T)} \in \mathbb{F}_2^v$: the characteristic vector of T,
- $C_k = \{x \in C \mid \mathrm{wt}(x) = k\}$,
- $\mathcal{B} = \{\mathrm{supp}(x) \mid x \in C_k\}$.

$$\begin{aligned}
|\{B \in \mathcal{B} \mid T \subset B\}| &= |\{x \in C_k \mid T \subset \mathrm{supp}(x)\}| \\
&= |\{x \in C \mid d(x^{(T)}, x) = k - t\}| - \delta_{k,2t} \\
&= \sum_{x \in C} (A_{k-t})_{x^{(T)},x} - \delta_{k,2t} \\
&= (A_{k-t}\hat{C})_{x^{(T)}} - \delta_{k,2t} \\
&= (E_t^* A_{k-t}\hat{C})_{x^{(T)}} - \delta_{k,2t}.
\end{aligned}$$

So we want to show

$$E_t^* A_{k-t}\hat{C} \text{ is a constant multiple of } E_t^* \mathbf{1}.$$

$E_t^* A_{k-t} \hat{C} = \lambda E_t^* \mathbf{1}$

Theorem (Assmus–Mattson)

$$\hat{C} = E_0^* \hat{C} + \sum_{i \geq k} E_i^* \hat{C} \quad (\text{minimum weight} = k),$$

$$S = \{\text{wt}(x) \mid x \in C^\perp,\ 0 < \text{wt}(x) < v\},$$

$$t = k - |S|.$$

Then

$$E_t^* A_{k-t} \hat{C} \text{ is a constant multiple of } E_t^* \mathbf{1}.$$

(S can also be described by E_i^* and $\widehat{C^\perp}$, but then we need to express S in terms of $\hat{C}$)

C and $C^\perp$ are connected by H

$$(H\hat{C})_x = \sum_{y\in C}(-1)^{x\cdot y} = \begin{cases} |C| & \text{if } x \in C^\perp \\ 0 & \text{otherwise} \end{cases} = (|C|\widehat{C^\perp})_x,$$

so

$$\widehat{C^\perp} = \frac{1}{|C|} H\hat{C}.$$

Define

$$E_i = \frac{1}{2^v} H E_i^* H = H^{-1} E_i^* H \quad (0 \le i \le v).$$

Then $E_i E_j = \delta_{i,j} E_i$, $\sum_{i=0}^{v} E_i = I$.

$$E_i^* \widehat{C^\perp} \ne 0 \iff E_i^* H \hat{C} \ne 0 \iff H^{-1} E_i^* H \hat{C} \ne 0$$
$$\iff E_i \hat{C} \ne 0.$$

$S = \{\mathrm{wt}(x) \mid x \in C^\perp,\ 0 < \mathrm{wt}(x) < v\}$

$$S = \{i \mid 0 < i < v,\ E_i^* \widehat{C^\perp} \neq 0\}$$
$$= \{i \mid 0 < i < v,\ E_i \hat{C} \neq 0\}.$$

Since $\sum_{i=0}^{v} E_i = I$,

$$\hat{C} = (E_0 + E_v)\hat{C} + \sum_{i \in S} E_i \hat{C}.$$

Theorem (Assmus–Mattson)

$$\hat{C} = (E_0 + E_v)\hat{C} + \sum_{i \in S} E_i \hat{C} = E_0^* \hat{C} + \sum_{i \geq k} E_i^* \hat{C},$$

$$\text{and } t = k - |S| \implies E_t^* A_{k-t} \hat{C} \in \mathbb{R} E_t^* \mathbf{1}.$$

Restating further

Theorem (Assmus–Mattson)

$$\hat{C} = (E_0 + E_v)\hat{C} + \sum_{i \in S} E_i \hat{C} = E_0^* \hat{C} + \sum_{i \geq k} E_i^* \hat{C},$$

$$\text{and } t = k - |S| \implies E_t^* A_{k-t} \hat{C} \in \mathbb{R} E_t^* \mathbf{1}.$$

reduces to

Theorem (Assmus–Mattson)

$$(E_0 + E_v)\hat{C} + \sum_{i \in S} E_i \hat{C} = E_0^* \hat{C} + \sum_{i \geq k} E_i^* \hat{C} \text{ and } t = k - |S|$$

$$\implies E_t^* A_{k-t}(E_0 + E_v)\hat{C} + E_t^* A_{k-t} \sum_{i \in S} E_i \hat{C} \in \mathbb{R} E_t^* \mathbf{1}.$$

H diagonalizes A_1

For $y \in \mathbb{F}_2^v$ with $\mathrm{wt}(y) = i$,

$$\begin{aligned}(A_1 H)_{x,y} &= \sum_{z \in \mathbb{F}_2^v} (A_1)_{x,z} (-1)^{z \cdot y} = \sum_{\substack{z \in \mathbb{F}_2^v \\ d(x,z)=1}} (-1)^{z \cdot y} \\ &= \sum_{j=1}^{v} (-1)^{x \cdot y} (-1)^{y_j} = H_{x,y} \sum_{j=1}^{v} (-1)^{y_j} \\ &= H_{x,y}(v - \mathrm{wt}(y)) = (v - 2i)(HE_i^*)_{x,y} \\ &= (\sum_{j=1}^{v} (v - 2j) HE_j^*)_{x,y}.\end{aligned}$$

Thus H diagonalizes A_1:

$$A_1 H = H \sum_{j=1}^{v} (v - 2j) E_j^*.$$

$A_1 H = H \sum_{j=1}^{v} (v - 2j) E_j^*$

E_i's are projections onto eigenspaces of A_1

$$\begin{aligned} A_1 E_i &= A_1 \left(\frac{1}{2^v} H E_i^* H\right) = \frac{1}{2^v} (A_1 H) E_i^* H \\ &= \frac{1}{2^v} \left(H \sum_{j=1}^{v} (v - 2j) E_j^*\right) E_i^* H = \frac{1}{2^v} (v - 2i) H E_i^* H \\ &= (v - 2i) E_i. \end{aligned}$$

Thus A_1 has eigenvalue $v - 2i$ on $E_i V$, and

$$V = \bigoplus_{i=0}^{v} E_i V$$

is the eigenspace decomposition of A_1.

$E_i = \frac{1}{2^v} H E_i^* H$, in particular,

$$2^v (E_v)_{x,y} = (H E_v^* H)_{x,y} = \sum_{\substack{z \in \mathbb{F}_2^v \\ \mathrm{wt}(z) = v}} H_{x,z} H_{z,y}$$

$$= H_{x,\mathbf{1}} H_{\mathbf{1},y} = (-1)^{x \cdot \mathbf{1}} (-1)^{y \cdot \mathbf{1}} \quad (\mathbf{1} = (1, \dots, 1) \in \mathbb{F}_2^v)$$

$$= (-1)^{\mathrm{wt}(x)} (-1)^{\mathrm{wt}(y)} = (-1)^{\mathrm{wt}(y)} \left(\sum_{i=0}^{v} (-1)^i E_i^* \mathbf{1} \right)_x .$$

$$E_v V = \mathbb{R} \sum_{i=0}^{v} (-1)^i E_i^* \mathbf{1} \quad (\mathbf{1} = (1, \dots, 1)^\top \in V).$$

Similarly

$$E_0 V = \mathbb{R} \sum_{i=0}^{v} E_i^* \mathbf{1} = \mathbb{R} \mathbf{1}.$$

$E_v V = \mathbb{R}\sum_{i=0}^{v}(-1)^i E_i^* \mathbf{1}$, $E_0 V = \mathbb{R}\mathbf{1}$ $A_1 E_i = (v-2i)E_i$, so $A_1 E_i V \subset E_i V$

Being a polynomial in A_1, the matrices A_{k-t} and A_1^j also leave $E_i V$ invariant. Thus

$$\begin{aligned} E_t^* A_1^j (E_0 + E_v)\hat{C} &\in E_t^* A_1^j E_0 V + E_t^* A_1^j E_v V \\ &\subset E_t^* E_0 V + E_t^* E_v V \\ &= \mathbb{R} E_t^* \mathbf{1} + \mathbb{R} E_t^* \sum_{i=0}^{v} (-1)^i E_i^* \mathbf{1} \\ &= \mathbb{R} E_t^* \mathbf{1}. \end{aligned}$$

$$E_t^* A_{k-t} (E_0 + E_v)\hat{C} \in \mathbb{R} E_t^* \mathbf{1}.$$

$E_t^* A_1^j (E_0 + E_v)\hat{C},\ E_t^* A_{k-t}(E_0 + E_v)\hat{C} \in \mathbb{R}E_t^*\mathbf{1}$

Theorem (Assmus–Mattson)

$$(E_0 + E_v)\hat{C} + \sum_{i\in S} E_i\hat{C} = E_0^*\hat{C} + \sum_{i\geq k} E_i^*\hat{C} \text{ and } t = k - |S|$$

$$\implies E_t^* A_{k-t}(E_0 + E_v)\hat{C} + E_t^* A_{k-t} \sum_{i\in S} E_i\hat{C} \in \mathbb{R}E_t^*\mathbf{1}.$$

reduces to

Theorem (Assmus–Mattson)

$$E_t^* A_1^j \sum_{i\in S} E_i\hat{C} \equiv E_t^* A_1^j (E_0^*\hat{C} + \sum_{i\geq k} E_i^*\hat{C}) \pmod{\mathbb{R}E_t^*\mathbf{1}} \quad (\forall j)$$

$$\text{and } t = k - |S| \implies E_t^* A_{k-t} \sum_{i\in S} E_i\hat{C} \in \mathbb{R}E_t^*\mathbf{1}.$$

$\langle I, A_1, A_1^2, A_1^3, \dots \rangle = \langle I, A_1, A_2, A_3, \dots \rangle$

Also,

$$\begin{aligned} E_t^* A_j E_0^* \hat{C} &= E_t^* A_j \hat{0} \\ &= E_t^* E_j^* \mathbf{1} \\ &= \delta_{t,j} E_t^* \mathbf{1} \\ &\in \mathbb{R} E_t^* \mathbf{1}. \end{aligned}$$

Thus

$$E_t^* A_j E_0^* \hat{C} \in \mathbb{R} E_t^* \mathbf{1},$$

$$E_t^* A_1^j E_0^* \hat{C} \in \mathbb{R} E_t^* \mathbf{1}.$$

$E_t^* A_1^j E_0^* \hat{C} \in \mathbb{R} E_t^* \mathbf{1}$

Theorem (Assmus–Mattson)

$$E_t^* A_1^j \sum_{i \in S} E_i \hat{C} \equiv E_t^* A_1^j (E_0^* \hat{C} + \sum_{i \geq k} E_i^* \hat{C}) \pmod{\mathbb{R} E_t^* \mathbf{1}} \quad (\forall j)$$

$$\text{and } t = k - |S| \implies E_t^* A_{k-t} \sum_{i \in S} E_i \hat{C} \in \mathbb{R} E_t^* \mathbf{1}.$$

reduces to

Theorem (Assmus–Mattson)

$$E_t^* A_1^j \sum_{i \in S} E_i \hat{C} \equiv E_t^* A_1^j \sum_{i \geq k} E_i^* \hat{C} \pmod{\mathbb{R} E_t^* \mathbf{1}} \quad (\forall j)$$

$$\text{and } t = k - |S| \implies E_t^* A_{k-t} \sum_{i \in S} E_i \hat{C} \in \mathbb{R} E_t^* \mathbf{1}.$$

$V = \bigoplus_{i=0}^{v} E_i V$: eigenspace decomposition of A_1

A_1 has $|S|$ eigenvalues on

$$W = \bigoplus_{i \in S} E_i V.$$

Being a polynomial in A_1, the matrix A_{k-t} has at most $|S|$ eigenvalues on W, so $\exists a_0, \ldots, a_{|S|-1} \in \mathbb{Q}$ such that

$$A_{k-t} = \sum_{j=0}^{|S|-1} a_j A^j \quad \text{on } W.$$

So

$$A_{k-t} \sum_{i \in S} E_i \hat{C} = \sum_{j=0}^{|S|-1} a_j A^j \sum_{i \in S} E_i \hat{C}.$$

$A_{k-t}\sum_{i\in S} E_i\hat{C} = \sum_{j=0}^{|S|-1} a_j A^j \sum_{i\in S} E_i\hat{C}$

Theorem (Assmus–Mattson)

$$E_t^* A_1^j \sum_{i\in S} E_i\hat{C} \equiv E_t^* A_1^j \sum_{i\geq k} E_i^*\hat{C} \pmod{\mathbb{R}E_t^*\mathbf{1}} \quad (\forall j)$$

$$\text{and } t = k - |S| \implies E_t^* A_{k-t} \sum_{i\in S} E_i\hat{C} \in \mathbb{R}E_t^*\mathbf{1}.$$

Proof:

$$E_t^* A_{k-t} \sum_{i\in S} E_i\hat{C} = E_t^* \sum_{j=0}^{|S|-1} a_j A_1^j \sum_{i\in S} E_i\hat{C} = \sum_{j=0}^{|S|-1} a_j E_t^* A_1^j \sum_{i\in S} E_i\hat{C}$$

$$\equiv \sum_{j=0}^{|S|-1} a_j E_t^* A_1^j \sum_{i\geq k} E_i^*\hat{C} = \sum_{j=0}^{|S|-1} \sum_{i\geq k} a_j (E_t^* A_1^j E_i^*)\hat{C}.$$

End of proof.

Need to show:

$$\sum_{j=0}^{|S|-1} \sum_{i \geq k} a_j (E_t^* A_1^j E_i^*) \hat{C} = 0.$$

Since

- $t = k - |S|$,
- $0 \leq j < |S|$,
- $k \leq i$.

we have $t + j < k \leq i$, and hence $E_t^* A_1^j E_i^* = 0$ by the triangle inequality for the Hamming distance. Indeed,

$$\begin{aligned}(A_1^j)_{x,y} &= \#(\text{paths of length } j \text{ from } x \text{ to } y) \\ &= 0 \text{ if } \mathrm{wt}(x) = t \text{ and } \mathrm{wt}(y) = i.\end{aligned}$$

□

The Assmus–Mattson theorem

Theorem

Let C be a binary code of length v, minimum weight k.

$$\begin{aligned}
\mathcal{P} &= \{1, 2, \dots, v\}, \\
\mathcal{B} &= \{\mathrm{supp}(x) \mid x \in C,\ \mathrm{wt}(x) = k\}, \\
S &= \{\mathrm{wt}(x) \mid x \in C^\perp,\ 0 < \mathrm{wt}(x) < v\}, \\
t &= k - |S|.
\end{aligned}$$

Then $(\mathcal{P}, \mathcal{B})$ is a t-(v, k, λ) design for some λ.

- C: $[24, 12, 8]$ binary doubly even self-dual ($C = C^\perp$) code, so $k = 8$ and C has only weights $0, 8, 12, 16, 24$.

$$\begin{aligned}
S &= \{\mathrm{wt}(x) \mid x \in C^\perp,\ 0 < \mathrm{wt}(x) < 24\} = \{8, 12, 16\}, \\
t &= k - |S| = 8 - 3 = 5.
\end{aligned}$$

Uniqueness of the extended binary Golay code

C: $[24, 12, 8]$ binary doubly even self-dual ($C = C^\perp$) code.

- The Assmus–Mattson theorem implies $(\mathcal{P}, \mathcal{B})$ is a 5-$(24, 8, \lambda)$ design, where $\mathcal{P} = \{1, 2, \dots, 24\}$,

$$\mathcal{B} = \{\text{supp}(x) \mid x \in C,\ \text{wt}(x) = 8\},$$

  for some λ.
- If $\lambda > 1$, then there are two distinct blocks in $\mathcal{B}$ sharing at least 5 (hence 6) points. Their symmetric difference would make a vector of weight 4 in C, contradicting the fact that C has minimum weight 8. Thus $\lambda = 1$.
- So C is the binary code of a 5-$(24, 8, 1)$ design which was already shown to be unqiue.

This proves the uniqueness of the extended binary Golay code.

Applicability of the Assmus–Mattson theorem

Theorem

Let C be a binary code of length v, minimum weight k.

$$\begin{aligned} \mathcal{P} &= \{1, 2, \dots, v\}, \\ \mathcal{B} &= \{\mathrm{supp}(x) \mid x \in C,\ \mathrm{wt}(x) = k\}, \\ S &= \{\mathrm{wt}(x) \mid x \in C^\perp,\ 0 < \mathrm{wt}(x) < v\}, \\ t &= k - |S|. \end{aligned}$$

Then $(\mathcal{P}, \mathcal{B})$ is a t-(v, k, λ) design for some λ.

The conclusion is stronger if k is large and $|S|$ is small. These are conflicting requirments:

larger k $\implies$ smaller C $\implies$ larger $C^\perp$ $\implies$ larger S

suppose $C = C^\perp$, doubly even $\implies$ S not too large

Binary doubly even self-dual codes

Under what circumstance can one obtain a 5-design from a doubly even self-dual code? Let k be the minimum weight.

$$S = \{\mathrm{wt}(x) \mid x \in C,\ 0 < \mathrm{wt}(x) < v\},$$
$$5 = k - |S|.$$

- $k = 8$, $|S| = 3$, $S = \{8, 12, 16\}$, $v = 24$.
- $k = 12$, $|S| = 7$, $S = \{12, 16, 20, 24, 28, 32, 36\}$, $v = 48$.
- $k = 16$, $|S| = 11$, $S = \{16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56\}$, $v = 72$.

In general, $\forall k$: a multiple of 4, $|S| = k - 5$,

$$S = \{k, k + 4, k + 8, \dots, 5k - 24 = v - k\}$$

$v = 6k - 24 = 24m$, where $k = 4m + 4$.

Extremal binary doubly even self-dual codes

Theorem (Mallows–Sloane, 1973)

For $m \geq 1$, a binary doubly even self-dual $[24m, 12m]$ code has minimum weight at most $4m + 4$.

Definition

A binary doubly even self-dual $[24m, 12m]$ code with minimum weight $4m + 4$ is called extremal.

For $m \geq 1$, an extremal binary doubly even self-dual code gives a 5-$(24m, 4m + 4, \lambda)$ design by the Assmus–Mattson theorem.

- $m = 1$: the extended binary Golay code and the 5-$(24, 8, 1)$ design
- $m = 2$: Houghten–Lam–Thiel–Parker (2003): unique $[48, 24, 12]$ code and a 5-$(48, 12, 8)$ design which is unique under self-orthogonality.

Extremal binary doubly even self-dual codes

Definition

A binary doubly even self-dual $[24m, 12m]$ code with minimum weight $4m + 4$ is called extremal.

- For $m \geq 3$, neither a code nor a design is known.

Theorem (Zhang, 1999)

There does not exist an extremal $[24m, 12m, 4m + 4]$ binary doubly even self-dual code for $m \geq 154$.