1. $t$-designs
2. Intersection numbers
3. $5$-$(24, 8, 1)$ design
4. Binary codes
5. $[24, 12, 8]$ binary self-dual code
6. Assmus–Mattson theorem
7. Extremal binary doubly even codes

**t-(v, k, \lambda) designs**

**Definition**

A $t$-$(v, k, \lambda)$ design is a pair $(\mathcal{P}, \mathcal{B})$, where

- $\mathcal{P}$: a finite set of “points”,
- $\mathcal{B}$: a collection of $k$-subsets of $\mathcal{P}$, a member of which is called a “block,”
- $\forall T \subset \mathcal{P}$ with $|T| = t$, there are exactly $\lambda$ members $B \in \mathcal{B}$ such that $T \subset B$.

Examples:

- $2$-$(v, 3, 1)$ design = Steiner triple system
- $2$-$(q^2, q, 1)$ design = affine plane of order $q$

$t$-design $\implies$ $(t - 1)$-design

More precisely,...

**Intersection numbers**

$(\mathcal{P}, \mathcal{B})$: $t$-$(v, k, \lambda)$ design. Write $\lambda = \lambda_t$, 

$$\lambda_{t-1} = |\{B \in \mathcal{B} \mid T' \subset B\}|,$$

where $T' \subset \mathcal{P}$, $|T'| = t - 1$. Then

$$\lambda_{t-1}(k - t + 1) = \sum_{\substack{B \in \mathcal{B} \mid T' \subset B}} |B \setminus T'|$$

$$= |\{(B, x) \in \mathcal{B} \mid T' \cup \{x\} \subset B, x \in \mathcal{P} \setminus T'\}|$$

$$= \sum_{x \in \mathcal{P} \setminus T'} |\{B \in \mathcal{B} \mid T' \cup \{x\} \subset B\}|$$

$$= \sum_{x \in \mathcal{P} \setminus T'} \lambda_t$$

$$= \lambda_t (v - t + 1).$$
(P, B): t-(v, k, \lambda) design

Then (P, B): (t - 1)-(v, k, \lambda_{t-1}) design, where

\lambda_{t-1} = \frac{\lambda_t v - t + 1}{k - t + 1}.

For example,

5-(24, 8, 1) \implies 4-(24, 8, 5)
\implies 3-(24, 8, 21)
\implies 2-(24, 8, 77)
\implies 1-(24, 8, 253)
\implies 0-(24, 8, 759)
\iff |B| = 759.

5-(24, 8, 1) design, \lambda_{i-1} = \lambda_{i+1}^j + \lambda_i^j.

759
253 506
77 176 330
21 56 120 210
5 16 40 80 130
1 4 12 28 52 78

Next row?

\lambda_0^0, \lambda_0^1, \lambda_0^2, \ldots

\lambda_0^0(l) = |\{B \in B \mid l \subset B\}| = 1 or 0

depending on the choice of \(l \subset P\) with \(|l| = 6\).

Choose \(l\) in such a way that \(\lambda_0^0(l) = 1\).
5-(24, 8, 1) design

Let $(P, B)$ be a 5-(24, 8, 1) design. Then

$$B, B' \in P, B \neq B' \implies \|B \cap B'\| = 4 \implies B \triangle B' \in B.$$ 

Proof by contradiction:

Here "****" must be odd and even simultaneously.

Binary codes

A (linear) binary code of length $v$ is a subspace of the vector space $\mathbb{F}_2^n$. If $C$ is a binary code and $\dim C = k$, we say $C$ is an binary $[v, k]$ code.

The dual code of a binary code $C$ is defined as

$$C^\perp = \{ x \in \mathbb{F}_2^v | x \cdot y = 0 \ (\forall y \in C) \}.$$ 

where

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

Then

$$\dim C^\perp = v - \dim C.$$ 

The code $C$ is said to be self-orthogonal if $C \subseteq C^\perp$ and self-dual if $C = C^\perp$.

Weight

For $x \in \mathbb{F}_2^n$, we write

$$\supp(x) = \{ i \ | \ 1 \leq i \leq v, \ x_i \neq 0 \},$$

$$\wt(x) = |\supp(x)|.$$ 

For a binary code $C$, its minimum weight is

$$\min\{\wt(x) \ | \ 0 \neq x \in C\}.$$ 

If an $[v, k]$ code $C$ has minimum weight $d$, we call $C$ an $[v, k, d]$ code. $C$ is doubly even if $\wt(x) \equiv 0 \ (\text{mod} \ 4) \ (\forall x \in C)$. Note

$$C \subseteq C^\perp \iff |\supp(x) \cap \supp(y)| \equiv 0 \ (\text{mod} \ 2) \ (\forall x, y \in C).$$
Generator matrix of a code

If a binary code $C$ is generated by row vectors $x^{(1)}, \ldots, x^{(b)}$, then the matrix

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

is called a generator matrix of $C$. This means

$$
C = \{ \sum_{i=1}^{b} \epsilon_i x^{(i)} \mid \epsilon_1, \ldots, \epsilon_b \in \mathbb{F}_2 \} \subset \mathbb{F}_2^r.
$$

Note

$$
C \subset C^\perp \iff |\text{supp}(x^{(i)}) \cap \text{supp}(x^{(j)})| \equiv 0 \pmod{2} \quad (\forall i,j).
$$

$C : \text{doubly even} \iff C \subset C^\perp \text{ and } \text{wt}(x^{(i)}) \equiv 0 \pmod{4} \quad (\forall i)$.

**dim $C \leq 12$ for 5-(24, 8, 1) design**

Recall that in a 5-(24, 8, 1) design $(P, B)$,

$$
|B \cap B'| \in \{8, 4, 2, 0\} \quad (\forall B, B' \in B).
$$

The binary code $C$ of a 5-(24, 8, 1) design is self-orthogonal. Indeed, the incidence matrix has row vectors $x^{(B)}$ ($B \in B$), the characteristic vector of the block $B$. Then

$$
x^{(B)} \cdot x^{(B')} = |B \cap B'| \mod 2 = (8 \text{ or } 4 \text{ or } 2 \text{ or } 0) \mod 2 = 0.
$$

Thus $C \subset C^\perp$, hence

$$
\dim C \leq \frac{1}{2}(\dim C + \dim C^\perp) \leq \frac{24}{2} = 12.
$$

Incidence matrix of a design

If $D = (P, B)$ is a $t$-$(\nu, k, \lambda)$ design, the incidence matrix $M(D)$ of $D$ is $|B| \times |P|$ matrix whose rows and columns are indexed by $B$ and $P$, respectively, such that its $(B, p)$ entry is 1 if $p \in B$, 0 otherwise. In other words, the row vectors of $M(D)$ are the characteristic vectors of blocks:

$$
M(D) = \begin{bmatrix}
x^{(B_1)} \\
\vdots \\
x^{(B_b)}
\end{bmatrix} : b \times \nu \text{ matrix},
$$

where $B = \{B_1, \ldots, B_b\}$, and $x^{(B)} \in \mathbb{F}_2^\nu$ denotes the characteristic vector of $B$, i.e., $\text{supp}(x^{(B)}) = B$.

The binary code of the design $D$ is the binary code of length $\nu$ having $M(D)$ as a generator matrix.

The 5-(24, 8, 1) design, $|B \cap B'| \in \{4, 2, 0\}$

$P = \{1, 2, \ldots, 24\}$. We may take $B$ as:

$$
\begin{array}{cccccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
1 & 2 & 3 & 4 & 9 & 10 & 11 & 12 \\
1 & 2 & 3 & 5 & 9 & 13 & 14 & 15 \\
1 & 2 & 4 & 5 & 9 & 16 & 17 & 18 \\
1 & 3 & 4 & 5 & 9 & 19 & 20 & 21 \\
2 & 3 & 4 & 5 & 9 & 22 & 23 & 24 \\
1 & 2 & 3 & 6 & 9 & 16 & 19 & 22 \\
1 & 2 & 4 & 6 & 9 & 13 & 20 & 23 \\
1 & 3 & 4 & 6 & 9 & 14 & 17 & 24 \\
1 & 2 & 5 & 6 & 9 & 10 & 21 & 24 \\
1 & 3 & 5 & 6 & 9 & 11 & 18 & 23 \\
\end{array}
$$

Do we have to find 759 blocks one by one? No, 12 blocks are sufficient (so one more needed).
Consequence of Todd’s lemma

\[ (B_1 \triangle B_4) \triangle (B_5 \triangle B_6) = \{7, 8, 17, 18, 20, 21, 23, 24\} \in B. \]

By Todd’s lemma

\[ B_0 = ((B_1 \triangle B_4) \triangle B_7) \triangle (B_5 \triangle B_6) = \{7, 8, 17, 18, 20, 21, 23, 24\} \in B. \]

One more block for 5-(24, 8, 1) design

We know

\[ B_0 = \{7, 8, 17, 18, 20, 21, 23, 24\} \in B, \quad x(B_0) \in C_0 = C_0^{(7, 8)}. \]

We have either

\[ B = \{1, 2, 3, 8, 9, 17, 21, 23\} \in B \text{ or} \]
\[ B' = \{1, 2, 3, 8, 9, 18, 20, 24\} \in B. \]

But \[ B^{(7, 8)} = B \triangle B_0, \] so

\[ \langle C_0, x(B')^{(7, 8)} \rangle = \langle C_0, x(B) + x(B_0) \rangle = \langle C_0, x(B) \rangle. \]

Therefore, the code generated by the design is unique up to isomorphism. This self-dual \( C = C^\perp \) code is known as the extended binary Golya code. Next we show that the code determines the design uniquely.

Mendelsohn equations for \( t-(v, k, \lambda) \) design \( (P, B) \)

For \( S \subset P \), let

\[ n_i(S) = |\{B \in B \mid i = |B \cap S|\}|. \]

Then

\[ \sum_{i \geq 0} \binom{i}{j} n_i(S) = \lambda_j \binom{|S|}{j} \quad (0 \leq j \leq t). \]

Proof: Count

\[ \{(J, B) \mid J \subset S \cap B, \ |J| = j\} \]

in two ways.
\[ n_i(S) = |\{ B \in \mathcal{B} \mid i = |B \cap S|\}| \]

Let \( C \) be the binary code of the design \((\mathcal{P}, \mathcal{B})\).
Write \( n_i(\text{supp}(v)) = n_i(v) \) for \( v \in \mathbb{F}_2^n \).
\[
\sum_{i \geq 0} \binom{i}{j} n_i(v) = \lambda_j \left( \text{wt}(v) \right) \quad (0 \leq j \leq t).
\]

If \( v \in \mathbb{F}_2^n \), then \( |B \cap \text{supp}(v)| \) is even, so
\[
n_i(v) = |\{ B \in \mathcal{B} \mid i = |B \cap \text{supp}(v)|\}| = 0 \quad \text{for } i \text{ odd}.
\]

Thus
\[
\sum_{0 \leq j \leq \text{wt}(v)} \binom{j}{i} n_i(v) = \lambda_j \left( \text{wt}(v) \right) \quad (0 \leq j \leq t).
\]

The Assmus–Mattson theorem

**Theorem**

Let \( C \) be a binary code of length \( n \), minimum weight \( k \).
\[
\mathcal{P} = \{1, 2, \ldots, v\},
\]
\[
\mathcal{B} = \{\text{supp}(x) \mid x \in C, \text{wt}(x) = k\},
\]
\[
S = \{\text{wt}(x) \mid x \in C, 0 < \text{wt}(x) < v\},
\]
\[
t = k - |S|.
\]

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

- \( C \): \([24, 12, 8]\) binary doubly even self-dual \((C = C^\perp)\) code, so \( k = 8 \) and \( C \) has only weights \( 0, 8, 12, 16, 24 \).
\[
S = \{\text{wt}(x) \mid x \in C, 0 < \text{wt}(x) < 24\} = \{8, 12, 16\},
\]
\[
t = k - |S| = 8 - 3 = 5.
\]
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 ($P, B$) is a 5-(24, 8, $\lambda$) design, where $P = \{1, 2, \ldots, 24\}$,
  \[ B = \{\text{supp}(x) \mid x \in C, \ \text{wt}(x) = 8\}, \]
  for some $\lambda$.
- If $\lambda > 1$, then $\exists B, B' \in B$, $B \neq B'$, $|B \cap B'| \geq 5$. Then $\text{wt}(x(B) + x(B')) < 8$, a contradiction. Thus $\lambda = 1$.
- So $C$ is the binary code of a 5-(24, 8, 1) design which was already shown to be unique.

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

Then $(P, B)$ is a $t$-($v, k, \lambda$) design for some $\lambda$.

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

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

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

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

\[ S = \{k, k + 4, k + 8, \ldots, 5k - 24 = v - k\} \]
\[ v = 6k - 24 = 24m, \text{ where } k = 4m + 4. \]

Extremal binary doubly even self-dual codes

**Theorem (Mallows–Sloane, 1973)**

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

**Definition**

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

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

- $m = 1$: the extended binary Golay code and the 5-(24, 8, 1) design
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 \(m \geq 154\).