組合せデザインから得られる線形符号

宗政昭弘

東北大学情報科学研究科

2013 年 8 月 9 日
離散数学とその応用研究集会 2013
山形市保健センター

Contents

t-(v, k, λ) designs

Definition

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

- $\mathcal{P}$: a finite set of v "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 λ members $B \in \mathcal{B}$ such that $T \subset B$.

t-(v, k, λ) designs

Definition

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

- $\mathcal{P}$: a finite set of v "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 λ members $B \in \mathcal{B}$ such that $T \subset B$.

Examples:

- 2-$(v, 3, 1)$ design = Steiner triple system

t-(v, k, λ) designs

Definition

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

- $\mathcal{P}$: a finite set of v "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 λ members $B \in \mathcal{B}$ such that $T \subset B$.

Examples:

- 2-$(v, 3, 1)$ design = Steiner triple system

t-(v, k, λ) designs

Definition

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

- $\mathcal{P}$: a finite set of v "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 λ 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-(v, k, λ) designs

Definition

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

- $\mathcal{P}$: a finite set of v "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 λ 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-(v, k, λ) designs

Definition

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

- $\mathcal{P}$: a finite set of v "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 λ 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-(v, k, λ) designs

Definition

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

- $\mathcal{P}$: a finite set of v "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 λ 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

$$t\text{-design} \implies (t-1)\text{-design}$$

More precisely,...

Intersection numbers

$(\mathcal{P}, \mathcal{B})$: t-(v, k, λ) 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

Intersection numbers

$(\mathcal{P}, \mathcal{B})$: t-(v, k, λ) 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

Intersection numbers

$(\mathcal{P}, \mathcal{B})$: t-(v, k, λ) 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

$$\begin{aligned}
\lambda_{t-1}(k - t + 1) &= \sum_{\substack{B \in \mathcal{B} \\ T' \subset B}} |B \setminus T'| \\
&= |\{(B, x) \mid B \in \mathcal{B},\ T' \cup \{x\} \subset B,\ x \in \mathcal{P} \setminus T'\}| \\
&= \sum_{x \in \mathcal{P} \setminus T'} |\{B \in \mathcal{B} \mid T' \cup \{x\} \subset B\}| \\
&= \sum_{x \in \mathcal{P} \setminus T'} \lambda_t \\
&= \lambda_t(v - t + 1).
\end{aligned}$$

Intersection numbers

$(\mathcal{P}, \mathcal{B})$: t-(v, k, λ) 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

$$\begin{aligned}
\lambda_{t-1}(k - t + 1) &= \sum_{\substack{B \in \mathcal{B} \\ T' \subset B}} |B \setminus T'| \\
&= |\{(B, x) \mid B \in \mathcal{B},\ T' \cup \{x\} \subset B,\ x \in \mathcal{P} \setminus T'\}| \\
&= \sum_{x \in \mathcal{P} \setminus T'} |\{B \in \mathcal{B} \mid T' \cup \{x\} \subset B\}| \\
&= \sum_{x \in \mathcal{P} \setminus T'} \lambda_t \\
&= \lambda_t(v - t + 1).
\end{aligned}$$

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

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

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

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

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

$$\lambda_{t-1} = \lambda_t \frac{v-t+1}{k-t+1} = 1 \cdot \frac{24-5+1}{8-5+1} = \frac{20}{4} = 5$$

For example,

$$5\text{-}(24, 8, 1) \implies 4\text{-}(24, 8, 5)$$

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

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

$$\lambda_{t-1} = \lambda_t \frac{v-t+1}{k-t+1} = 5 \cdot \frac{24-4+1}{8-4+1} =$$

For example,

$$\begin{aligned} 5\text{-}(24, 8, 1) &\implies 4\text{-}(24, 8, 5) \\ &\implies 3\text{-}(24, 8, 21) \end{aligned}$$

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

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

$$\lambda_{t-1} = \lambda_t \frac{v-t+1}{k-t+1} = 5 \cdot \frac{24-4+1}{8-4+1} =$$

For example,

$$\begin{aligned} 5\text{-}(24, 8, 1) &\implies 4\text{-}(24, 8, 5) \\ &\implies 3\text{-}(24, 8, 21) \end{aligned}$$

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

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

$$\lambda_{t-1} = \lambda_t \frac{v-t+1}{k-t+1} = 5 \cdot \frac{24-4+1}{8-4+1} = 5 \cdot \frac{21}{5} = 21$$

For example,

$$\begin{aligned} 5\text{-}(24, 8, 1) &\implies 4\text{-}(24, 8, 5) \\ &\implies 3\text{-}(24, 8, 21) \end{aligned}$$

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

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

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

For example,

$$\begin{aligned} 5\text{-}(24,8,1) &\implies 4\text{-}(24,8,5) \\ &\implies 3\text{-}(24,8,21) \\ &\implies 2\text{-}(24,8,77) \end{aligned}$$

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

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

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

For example,

$$\begin{aligned} 5\text{-}(24,8,1) &\implies 4\text{-}(24,8,5) \\ &\implies 3\text{-}(24,8,21) \\ &\implies 2\text{-}(24,8,77) \\ &\implies 1\text{-}(24,8,253) \end{aligned}$$

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

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

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

For example,

$$\begin{aligned}5\text{-}(24,8,1) &\Longrightarrow 4\text{-}(24,8,5)\\ &\Longrightarrow 3\text{-}(24,8,21)\\ &\Longrightarrow 2\text{-}(24,8,77)\\ &\Longrightarrow 1\text{-}(24,8,253)\\ &\Longrightarrow 0\text{-}(24,8,759)\end{aligned}$$

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

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

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

For example,

$$\begin{aligned} 5\text{-}(24, 8, 1) &\Longrightarrow 4\text{-}(24, 8, 5) \\ &\Longrightarrow 3\text{-}(24, 8, 21) \\ &\Longrightarrow 2\text{-}(24, 8, 77) \\ &\Longrightarrow 1\text{-}(24, 8, 253) \\ &\Longrightarrow 0\text{-}(24, 8, 759) \\ &\Longleftrightarrow |\mathcal{B}| = 759. \end{aligned}$$

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

Let $I \subset \mathcal{P}$, $J \subset \mathcal{P}$, $|I| = i$, $|J| = j$, $I \cap J = \emptyset$, $i + j \leq t$.

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

Let $I \subset \mathcal{P}$, $J \subset \mathcal{P}$, $|I| = i$, $|J| = j$, $I \cap J = \emptyset$, $i + j \leq t$.
Define

$$\lambda_i^j = |\{B \in \mathcal{B} \mid I \subset B,\ B \cap J = \emptyset\}|.$$

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

Let $I \subset \mathcal{P}$, $J \subset \mathcal{P}$, $|I| = i$, $|J| = j$, $I \cap J = \emptyset$, $i + j \leq t$.
Define

$$\lambda_i^j = |\{B \in \mathcal{B} \mid I \subset B,\ B \cap J = \emptyset\}|.$$

In particular,

$$\lambda_i^0 = \lambda_i = |\{B \in \mathcal{B} \mid I \subset B\}|.$$

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

Let $I \subset \mathcal{P}$, $J \subset \mathcal{P}$, $|I| = i$, $|J| = j$, $I \cap J = \emptyset$, $i + j \leq t$.
Define

$$\lambda_i^j = |\{B \in \mathcal{B} \mid I \subset B,\ B \cap J = \emptyset\}|.$$

In particular,

$$\lambda_i^0 = \lambda_i = |\{B \in \mathcal{B} \mid I \subset B\}|.$$

$$\lambda_i^{j-1} = \lambda_{i+1}^{j-1} + \lambda_i^j.$$

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

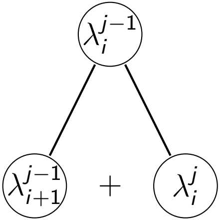
Let $I \subset \mathcal{P}$, $J \subset \mathcal{P}$, $|I| = i$, $|J| = j$, $I \cap J = \emptyset$, $i + j \le t$.
Define

$$\lambda_i^j = |\{B \in \mathcal{B} \mid I \subset B,\ B \cap J = \emptyset\}|.$$

In particular,

$$\lambda_i^0 = \lambda_i = |\{B \in \mathcal{B} \mid I \subset B\}|.$$

$$\lambda_i^{j-1} = \lambda_{i+1}^{j-1} + \lambda_i^j.$$



$$
\begin{array}{c}
\lambda_0^0 \\
\lambda_1^0\ \lambda_0^1 \\
\lambda_2^0\ \lambda_1^1\ \lambda_0^2 \\
\lambda_3^0\ \lambda_2^1\ \lambda_1^2\ \lambda_0^3 \\
\lambda_4^0\ \lambda_3^1\ \lambda_2^2\ \lambda_1^3\ \lambda_0^4 \\
\lambda_5^0\ \lambda_4^1\ \lambda_3^2\ \lambda_2^3\ \lambda_1^4\ \lambda_0^5
\end{array}
$$

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

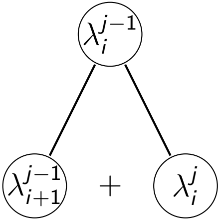
Let $I \subset \mathcal{P}$, $J \subset \mathcal{P}$, $|I| = i$, $|J| = j$, $I \cap J = \emptyset$, $i + j \leq t$.
Define

$$\lambda_i^j = |\{B \in \mathcal{B} \mid I \subset B,\ B \cap J = \emptyset\}|.$$

In particular,

$$\lambda_i^0 = \lambda_i = |\{B \in \mathcal{B} \mid I \subset B\}|.$$

$$\lambda_i^{j-1} = \lambda_{i+1}^{j-1} + \lambda_i^j.$$



$$\begin{array}{c}
\lambda_0^0 \\
\lambda_1^0\ \lambda_0^1 \\
\lambda_2^0\ \lambda_1^1\ \lambda_0^2 \\
\lambda_3^0\ \lambda_2^1\ \lambda_1^2\ \lambda_0^3 \\
\lambda_4^0\ \lambda_3^1\ \lambda_2^2\ \lambda_1^3\ \lambda_0^4 \\
\lambda_5^0\ \lambda_4^1\ \lambda_3^2\ \lambda_2^3\ \lambda_1^4\ \lambda_0^5
\end{array}$$

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

759

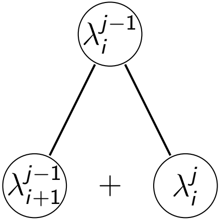
253

77

21

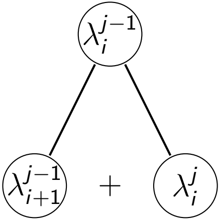
5

1



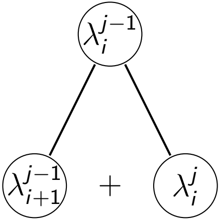
5-(24, 8, 1) design, $\lambda_i^{j-1} = \lambda_{i+1}^{j-1} + \lambda_i^j$

					759	
				253		506
			77		176	
		21		56		
	5		16			
1		4				



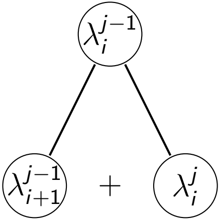
5-(24, 8, 1) design, $\lambda_i^{j-1} = \lambda_{i+1}^{j-1} + \lambda_i^j$

759
253 506
77 176 330
21 56 120
5 16 40
1 4 12



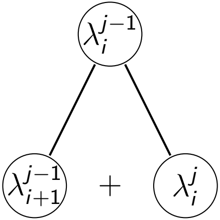
5-(24, 8, 1) design, $\lambda_i^{j-1} = \lambda_{i+1}^{j-1} + \lambda_i^j$

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



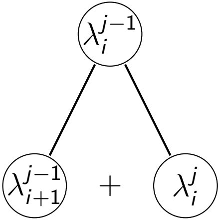
5-$(24, 8, 1)$ design, $\lambda_i^{j-1} = \lambda_{i+1}^{j-1} + \lambda_i^j$

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



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

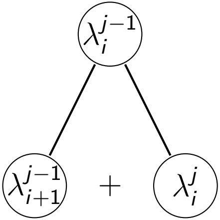
759
253 506
77 176 330
21 56 120 210
5 16 40 80 130
1 4 12 28 52 78



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

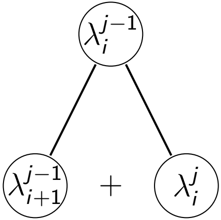
759
253 506
77 176 330
21 56 120 210
5 16 40 80 130
1 4 12 28 52 78

Next row? λ_6^0, λ_5^1, λ_4^2, ...



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

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



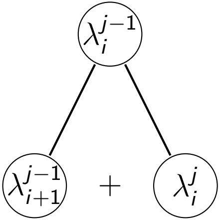
Next row? λ_6^0, λ_5^1, λ_4^2, ...

$$\lambda_6^0(I) = |\{B \in \mathcal{B} \mid I \subset B\}| = 1 \text{ or } 0$$

depending on the choice of $I \subset \mathcal{P}$ with $|I| = 6$.

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

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



Next row? λ_6^0, λ_5^1, λ_4^2, ...

$$\lambda_6^0(I) = |\{B \in \mathcal{B} \mid I \subset B\}| = 1 \text{ or } 0$$

depending on the choice of $I \subset \mathcal{P}$ with $|I| = 6$.
Choose I in such a way that $\lambda_6^0(I) = 1$.

5-(24, 8, 1) design, $I \subset \mathcal{P}$, $|I| = 6$, $I \subset \exists B \in \mathcal{B}$

$$\lambda^j_{6-j} = |\{B \in \mathcal{B} \mid I \setminus J \subset B,\ B \cap J = \emptyset\}| \quad \text{where } J \subset I,\ J = j.$$

$$\lambda^j_{5-j} = \lambda^j_{6-j} + \lambda^{j+1}_{5-j}$$

giving

759
253 506
77 176 330
21 56 120 210
5 16 40 80 130
1 4 12 28 52 78
1 0 4 8 20 32 46

Similarly, taking $I \subset \mathcal{P}$, $|I| = 7$ appropriately, we obtain λ^j_{7-j}.
Finally taking $I \in \mathcal{B}$, we obtain λ^j_{8-j}.

5-(24, 8, 1) design

759

253 506

77 176 330

21 56 120 210

5 16 40 80 130

1 4 12 28 52 78

1 0 4 8 20 32 46

1 0 0 4 4 16 16 30

1 0 0 0 4 0 16 0 30

The last row implies

$$B, B' \in \mathcal{P},\ B \neq B' \implies |B \cap B'| \in \{4, 2, 0\}.$$

Binary codes

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

Binary codes

A (linear) binary code of length v is a subspace of the vector space $\mathbb{F}_2^v$. 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

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

where

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

Binary codes

A (linear) binary code of length v is a subspace of the vector space $\mathbb{F}_2^v$. 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

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

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 $C \subset C^\perp$ and self-dual if $C = C^\perp$.

Weight

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

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

For a binary code C, its minimum weight is

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

Weight

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

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

For a binary code C, its minimum weight is

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

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

Weight

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

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

For a binary code C, its minimum weight is

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

If an $[v, k]$ code C has minimum weight d, we call C an $[v, k, d]$ code.
If $\mathrm{wt}(x) \equiv 0 \pmod 4$ for all $x \in C$, we call C doubly even.

Generator matrix of a code

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

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

is called a generator matrix of C. This means

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

Generator matrix of a code

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

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

is called a generator matrix of C. This means

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

Note

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

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

Incidence matrix of a design

If $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a t-(v, k, λ) design, the incidence matrix $M(\mathcal{D})$ of $\mathcal{D}$ is the $|\mathcal{B}| \times |\mathcal{P}|$ matrix whose rows and columns are indexed by $\mathcal{B}$ and $\mathcal{P}$, respectively, such that its (B, p) entry is 1 if $p \in B$, 0 otherwise.

Incidence matrix of a design

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

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

where $\mathcal{B} = \{B_1, \ldots, B_b\}$, and $x^{(B)} \in \mathbb{F}_2^v$ denotes the characteristic vector of B.

Incidence matrix of a design

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

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

where $\mathcal{B} = \{B_1, \ldots, B_b\}$, and $x^{(B)} \in \mathbb{F}_2^v$ denotes the characteristic vector of B.
The binary code of the design $\mathcal{D}$ is the binary code of length v having $M(\mathcal{D})$ as a generator matrix.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B_1 1 2 3 4 5 6 7 8

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

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

B_1 1 2 3 4 5 6 7 8
B_2 1 2 3 4 5 6 7 8 9

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

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

B_1 1 2 3 4 5 6 7 8
B_2 1 2 3 4 5 6 7 8 9 10 11 12

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

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

B_1	1	2	3	4	5	6	7	8				
B_2	1	2	3	4					9	10	11	12

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

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

B_1	1	2	3	4	5	6	7	8				
B_2	1	2	3	4					9	10	11	12
B_3	1	2	3		5				9			

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

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

B_1	1	2	3	4	5	6	7	8				
B_2	1	2	3	4					9	10	11	12
B_3	1	2	3	4	5	6	7	8	9	10	11	12

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

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

B_1	1	2	3	4	5	6	7	8							
B_2	1	2	3	4					9	10	11	12			
B_3	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

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

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

B_1	1	2	3	4	5	6	7	8							
B_2	1	2	3	4					9	10	11	12			
B_3	1	2	3		5				9				13	14	15

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

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

B_1	1	2	3	4	5	6	7	8							
B_2	1	2	3	4					9	10	11	12			
B_3	1	2	3		5				9				13	14	15
B_4	1	2		4	5				9						

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

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

B_1	1	2	3	4	5	6	7	8							
B_2	1	2	3	4					9	10	11	12			
B_3	1	2	3		5				9				13	14	15
B_4	1	2		4	5				9						

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

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

B_1	1	2	3	4	5	6	7	8							
B_2	1	2	3	4					9	10	11	12			
B_3	1	2	3		5				9				13	14	15
B_4	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

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

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

B_1	1	2	3	4	5	6	7	8										
B_2	1	2	3	4					9	10	11	12						
B_3	1	2	3		5				9				13	14	15			
B_4	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

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

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

B_1	1	2	3	4	5	6	7	8										
B_2	1	2	3	4					9	10	11	12						
B_3	1	2	3		5				9				13	14	15			
B_4	1	2		4	5				9							16	17	18

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

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

B_1	1	2	3	4	5	6	7	8										
B_2	1	2	3	4					9	10	11	12						
B_3	1	2	3		5				9				13	14	15			
B_4	1	2		4	5				9							16	17	18
B_5	1		3	4	5				9									

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

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

B_1	1	2	3	4	5	6	7	8													
B_2	1	2	3	4					9	10	11	12									
B_3	1	2	3		5				9				13	14	15						
B_4	1	2		4	5				9							16	17	18			
B_5	1		3	4	5				9										19	20	21

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

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

B_1	1	2	3	4	5	6	7	8													
B_2	1	2	3	4					9	10	11	12									
B_3	1	2	3		5				9				13	14	15						
B_4	1	2		4	5				9							16	17	18			
B_5	1		3	4	5				9										19	20	21
B_6		2	3	4	5				9												

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9															

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15									

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15									

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18						

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21			

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9															

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9															

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2	3	4	5	6	7	8	9	10	11	12				16	17	18	19			22		

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2	3	4	5	6	7	8	9	10	11	12				16	17	18	19			22		

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19			22		

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19			22		

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22		

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22		

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9															

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9															

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1	2	3	4	2	6	7	8	9	10	11	12	13			16			19	20	21	22	23	

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1	2	3	4	2	6	7	8	9	10	11	12	13			16			19	20	21	22	23	

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1	2	3	4	2	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9															

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2	3	4	5	6	7	8	9				13	14	15	16	17	18	19	20		22	23	

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1		3		5	6			9															

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1	2	3	4	5	6	7	8	9	10			13	14	15	16	17		19	20	21	22		24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1		3		5	6			9		11							18					23	

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1		3		5	6			9		11							18					23	
B_{12}	1	2	3						9								17							

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1		3		5	6			9		11							18					23	
B_{12}	1	2	3						9								17							

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1		3		5	6			9		11							18					23	
B_{12}	1	2	3	4	5	6			9	10	11	12	13	14	15	16	17	18	19			22		24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1		3		5	6			9		11							18					23	
B_{12}	1	2	3	4	5	6			9	10	11	12	13	14	15	16	17	18	19			22		24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1		3		5	6			9		11							18					23	
B_{12}	1	2	3	4	5	6			9	10	11	12	13	14	15	16	17	18	19		21	22	23	24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1		3		5	6			9		11							18					23	
B_{12}	1	2	3	4	5	6			9	10	11	12	13	14	15	16	17	18	19		21	22	23	24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1		3		5	6			9		11							18					23	
B_{12}	1	2	3	4	5	6			9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1		3		5	6			9		11							18					23	
B_{12}	1	2	3	4	5	6			9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1		3		5	6			9		11							18					23	
B_{12}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1		3		5	6			9		11							18					23	
B_{12}	1	2	3				7		9								17				21		23	

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

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

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1		3		5	6			9		11							18					23	
B_{12}	1	2	3				7		9								17				21		23	

The characteristic vectors of these 12 blocks generate a 12-dimensional code.

Uniqueness of the code

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1		3		5	6			9		11							18					23	
B_{12}	1	2	3				7										17				21		23	

Thus, the code generated by the design is unique. This self-dual code is known as the extended binary Golay code.

Uniqueness of the code

B_1	1	2	3	4	5	6	7	8																
B_2	1	2	3	4					9	10	11	12												
B_3	1	2	3		5				9				13	14	15									
B_4	1	2		4	5				9							16	17	18						
B_5	1		3	4	5				9										19	20	21			
B_6		2	3	4	5				9													22	23	24
B_7	1	2	3			6			9							16			19			22		
B_8	1	2		4		6			9				13							20			23	
B_9	1		3	4		6			9					14			17							24
B_{10}	1	2			5	6			9	10											21			24
B_{11}	1		3		5	6			9		11							18					23	
B_{12}	1	2	3				7										17				21		23	

Thus, the code generated by the design is unique. This self-dual code is known as the extended binary Golay code.
Next we show that the code determines the design uniquely.

Mendelsohn equations for t-(v, k, λ) design $(\mathcal{P}, \mathcal{B})$

$$\lambda_i = |\{B \in \mathcal{B} \mid I \subset B\}| \quad (|I| = i)$$

Mendelsohn equations for t-(v, k, λ) design $(\mathcal{P}, \mathcal{B})$

$$\lambda_i = |\{B \in \mathcal{B} \mid I \subset B\}| \quad (|I| = i)$$

For $S \subset \mathcal{P}$, let

$$n_i(S) = |\{B \in \mathcal{B} \mid i = |B \cap S|\}|.$$

Mendelsohn equations for t-(v, k, λ) design $(\mathcal{P}, \mathcal{B})$

$$\lambda_i = |\{B \in \mathcal{B} \mid I \subset B\}| \quad (|I| = i)$$

For $S \subset \mathcal{P}$, let

$$n_i(S) = |\{B \in \mathcal{B} \mid i = |B \cap S|\}|.$$

Then

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

Proof: Count

Mendelsohn equations for t-(v, k, λ) design $(\mathcal{P}, \mathcal{B})$

$$\lambda_i = |\{B \in \mathcal{B} \mid I \subset B\}| \quad (|I| = i)$$

For $S \subset \mathcal{P}$, let

$$n_i(S) = |\{B \in \mathcal{B} \mid i = |B \cap S|\}|.$$

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 $(\mathcal{P}, \mathcal{B})$.

$n_i(S) = |\{B \in \mathcal{B} \mid i = |B \cap S|\}|$

Let C be the binary code of the design $(\mathcal{P}, \mathcal{B})$.
Write $n_i(\mathrm{supp}(x)) = n_i(x)$ for $x \in \mathbb{F}_2^v$.

$$\sum_{i \geq 0} \binom{i}{j} n_i(x) = \lambda_j \binom{\mathrm{wt}(x)}{j} \quad (0 \leq j \leq t).$$

$n_i(S) = |\{B \in \mathcal{B} \mid i = |B \cap S|\}|$

Let C be the binary code of the design $(\mathcal{P}, \mathcal{B})$.
Write $n_i(\mathrm{supp}(x)) = n_i(x)$ for $x \in \mathbb{F}_2^v$.

$$\sum_{i \geq 0} \binom{i}{j} n_i(x) = \lambda_j \binom{\mathrm{wt}(x)}{j} \quad (0 \leq j \leq t).$$

If $x \in C^{\perp}$, then $|B \cap \mathrm{supp}(x)|$ is even, so

$$n_i(x) = |\{B \in \mathcal{B} \mid i = |B \cap \mathrm{supp}(x)|\}| = 0 \quad \text{for } i \text{ odd}.$$

$n_i(S) = |\{B \in \mathcal{B} \mid i = |B \cap S|\}|$

Let C be the binary code of the design $(\mathcal{P}, \mathcal{B})$.
Write $n_i(\mathrm{supp}(x)) = n_i(x)$ for $x \in \mathbb{F}_2^v$.

$$\sum_{i \geq 0} \binom{i}{j} n_i(x) = \lambda_j \binom{\mathrm{wt}(x)}{j} \quad (0 \leq j \leq t).$$

If $x \in C^{\perp}$, then $|B \cap \mathrm{supp}(x)|$ is even, so

$$n_i(x) = |\{B \in \mathcal{B} \mid i = |B \cap \mathrm{supp}(x)|\}| = 0 \quad \text{for } i \text{ odd}.$$

Thus

$$\sum_{\substack{0 \leq i \leq \mathrm{wt}(x) \\ i:\mathrm{even}}} \binom{i}{j} n_i(x) = \lambda_j \binom{\mathrm{wt}(x)}{j} \quad (0 \leq j \leq t).$$

$(\mathcal{P}, \mathcal{B})$: 5-(24, 8, 1) design

$$\sum_{\substack{0 \le i \le \mathrm{wt}(x) \\ i:\ \text{even}}} \binom{i}{j} n_i(x) = \lambda_j \binom{\mathrm{wt}(x)}{j} \quad (0 \le j \le 5).$$

$(\mathcal{P}, \mathcal{B})$: 5-$(24, 8, 1)$ design

$$\sum_{\substack{0 \le i \le \mathrm{wt}(x) \\ i:\ \text{even}}} \binom{i}{j} n_i(x) = \lambda_j \binom{\mathrm{wt}(x)}{j} \quad (0 \le j \le 5).$$

Taking $x \in C^{\perp}$ with $0 < \mathrm{wt}(x) < 8$ gives no solution. This means that $C^{\perp}$ has minimum weight 8.

$(\mathcal{P}, \mathcal{B})$: 5-$(24, 8, 1)$ design

$$\sum_{\substack{0 \le i \le \mathrm{wt}(x) \\ i:\ \text{even}}} \binom{i}{j} n_i(x) = \lambda_j \binom{\mathrm{wt}(x)}{j} \quad (0 \le j \le 5).$$

Taking $x \in C^\perp$ with $0 < \mathrm{wt}(x) < 8$ gives no solution. This means that $C^\perp$ has minimum weight 8.
Take $x \in C = C^\perp$ with $\mathrm{wt}(x) = 8$. Then there are six equations for five unknowns n_0, n_2, n_4, n_6, n_8. The unique solution is

$$(n_0, n_2, n_4, n_6, n_8) = (30, 448, 280, 0, 1).$$

$(\mathcal{P}, \mathcal{B})$: 5-$(24, 8, 1)$ design

$$\sum_{\substack{0 \le i \le \mathrm{wt}(x) \\ i:\ \text{even}}} \binom{i}{j} n_i(x) = \lambda_j \binom{\mathrm{wt}(x)}{j} \quad (0 \le j \le 5).$$

Taking $x \in C^{\perp}$ with $0 < \mathrm{wt}(x) < 8$ gives no solution. This means that $C^{\perp}$ has minimum weight 8.
Take $x \in C = C^{\perp}$ with $\mathrm{wt}(x) = 8$. Then there are six equations for five unknowns n_0, n_2, n_4, n_6, n_8. The unique solution is

$$(n_0, n_2, n_4, n_6, n_8) = (30, 448, 280, 0, 1).$$

This implies $\mathrm{supp}(x) \in \mathcal{B}$. Thus

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

Now the uniqueness of the design follows from that of C.

Summary

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

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

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

The Assmus–Mattson theorem

Theorem

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.

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 $\mathcal{P} = \{1, 2, \ldots, 24\}$,

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

  for some λ.

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 $\exists B, B' \in \mathcal{B},\ B \neq B'$, $|B \cap B'| \geq 5$. Then $\text{wt}(x^{(B)} + x^{(B')}) < 8$, a contradiction. Thus $\lambda = 1$.

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 $\mathcal{P} = \{1, 2, \ldots, 24\}$,

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

  for some λ.
- If $\lambda > 1$, then $\exists B, B' \in \mathcal{B},\ B \neq B'$, $|B \cap B'| \geq 5$. Then $\mathrm{wt}(x^{(B)} + x^{(B')}) < 8$, a contradiction. Thus $\lambda = 1$.
- So C is the binary code of a 5-$(24, 8, 1)$ design which was already shown to be 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.

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

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

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:

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 $\Longrightarrow$ smaller C $\Longrightarrow$ larger $C^\perp$ $\Longrightarrow$ larger S

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

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 $\Longrightarrow$ smaller C $\Longrightarrow$ larger $C^{\perp}$ $\Longrightarrow$ larger S

suppose $C = C^{\perp}$, doubly even $\Longrightarrow$ 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.

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

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.

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

- $k = 8$, $|S| = 3$, $S = \{8, 12, 16\}$, $v = 24$.

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.

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

- $k = 8$, $|S| = 3$, $S = \{8, 12, 16\}$, $v = 24$.
- $k = 12$, $|S| = 7$, $S = \{12, 16, 20, 24, 28, 32, 36\}$, $v = 48$.

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.

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

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

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, $|S| = k - 5$,

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

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

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, $|S| = k - 5$,

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

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

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 $4m + 4$.

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.

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.

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 $m \geq 1$, an extremal binary doubly even self-dual code gives a 5-$(24m, 4m + 4, \lambda)$ design by the Assmus–Mattson theorem.
- For $m \geq 3$, neither a code nor a design is known.

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 $m \geq 1$, an extremal binary doubly even self-dual code gives a 5-$(24m, 4m + 4, \lambda)$ design by the Assmus–Mattson theorem.
- 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 $m \geq 154$.