# An extremal problem related to binary singly even self-dual codes

Akihiro Munemasa

Graduate School of Information Sciences
Tohoku University
August 4, 2005

# A packing problem

$|\Omega_v| = v$, $\mathcal{B} \subset \binom{\Omega_v}{k}$, at most $\lambda$-intersecting:

# A packing problem

$|\Omega_v| = v$, $\mathcal{B} \subset \binom{\Omega_v}{k}$, at most $\lambda$-intersecting:

$$B \in \mathcal{B},\ B' \in \mathcal{B},\ B \neq B' \implies |B \cap B'| \leq \lambda.$$

# A packing problem

$|\Omega_v| = v$, $\mathcal{B} \subset \binom{\Omega_v}{k}$, at most $\lambda$-intersecting:

$$B \in \mathcal{B},\ B' \in \mathcal{B},\ B \neq B' \implies |B \cap B'| \leq \lambda.$$

Given $v, k, \lambda$, find the largest possible size of such a subset $\mathcal{B}$.

# Binary codes

Let $C$ be a binary linear code with minimum weight $d$.

# Binary codes

Let $C$ be a binary linear code with minimum weight $d$.
If $\boldsymbol{u}, \boldsymbol{v}$ are distinct codewords of $C$ of the same weight $w$, then

# Binary codes

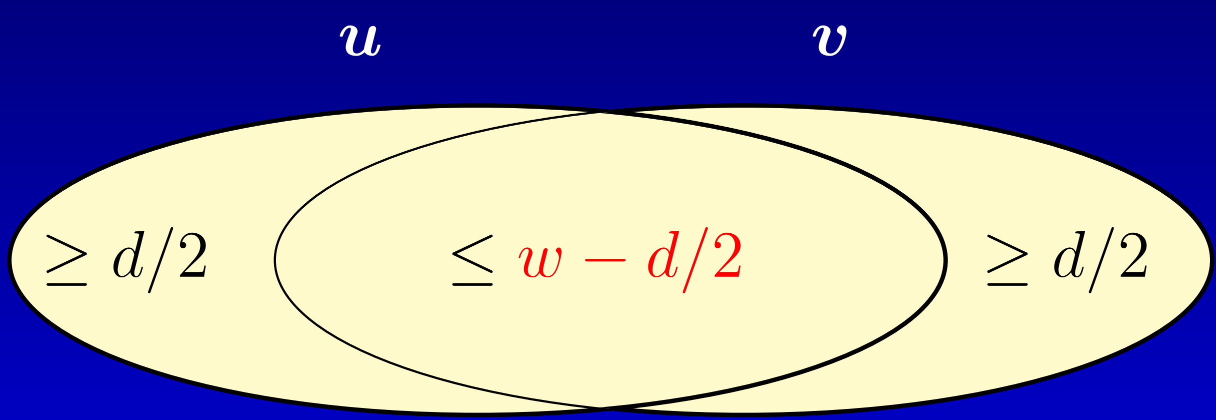
Let $C$ be a binary linear code with minimum weight $d$.
If $\boldsymbol{u}, \boldsymbol{v}$ are distinct codewords of $C$ of the same weight $w$, then

$$|\operatorname{supp}(\boldsymbol{u}) \cap \operatorname{supp}(\boldsymbol{v})| \leq w - \frac{d}{2}$$

# Binary codes

Let $C$ be a binary linear code with minimum weight $d$.
If $\boldsymbol{u}, \boldsymbol{v}$ are distinct codewords of $C$ of the same weight $w$, then

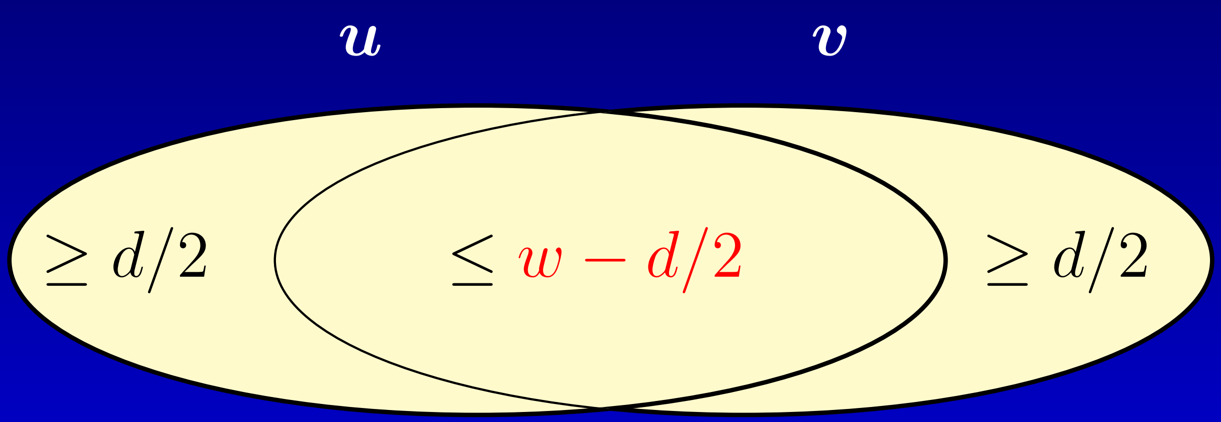
$$|\operatorname{supp}(\boldsymbol{u}) \cap \operatorname{supp}(\boldsymbol{v})| \leq w - \frac{d}{2}$$



# Binary codes

Let $C$ be a binary linear code with minimum weight $d$.
If $\boldsymbol{u}, \boldsymbol{v}$ are distinct codewords of $C$ of the same weight $w$, then

$$|\,\mathrm{supp}(\boldsymbol{u}) \cap \mathrm{supp}(\boldsymbol{v})| \leq w - \frac{d}{2}$$




(because $\boldsymbol{u} + \boldsymbol{v} \in C$)

# Linear programming bound

$\mathcal{B} \subset \binom{\Omega_v}{k}$, $2k \leq v$,    $\lambda$: a positive integer

$$B, B' \in \mathcal{B},\ B \neq B' \implies |B \cap B'| \leq \lambda$$

# Linear programming bound

$\mathcal{B} \subset \binom{\Omega_v}{k},\ 2k \leq v$, $\lambda$: a positive integer

$$B, B' \in \mathcal{B},\ B \neq B' \implies |B \cap B'| \leq \lambda$$

# Linear programming bound

$\mathcal{B} \subset \binom{\Omega_v}{k}$, $2k \leq v$, $L \subset \{0, 1, \ldots, k-1\}$

$$B, B' \in \mathcal{B},\ B \neq B' \implies |B \cap B'| \leq \lambda$$

# Linear programming bound

$\mathcal{B} \subset \binom{\Omega_v}{k}$, $2k \leq v$, $\quad L \subset \{0, 1, \ldots, k-1\}$

$$B, B' \in \mathcal{B},\ B \neq B' \implies |B \cap B'| \in L$$

# Linear programming bound

$\mathcal{B} \subset \binom{\Omega_v}{k}$, $2k \leq v$, $\quad L \subset \{0, 1, \ldots, k-1\}$

$$B, B' \in \mathcal{B},\ B \neq B' \implies |B \cap B'| \in L$$

$|\mathcal{B}|$ is bounded from the above by

# Linear programming bound

$\mathcal{B} \subset \binom{\Omega_v}{k}$, $2k \le v$, $\quad L \subset \{0, 1, \ldots, k-1\}$

$$B, B' \in \mathcal{B},\ B \neq B' \implies |B \cap B'| \in L$$

$|\mathcal{B}|$ is bounded from the above by

$\max \sum_{i=0}^{k} a_i$ subject to $(a_0, a_1, \ldots, a_k)Q \ge 0$,

$$a_0 = 1,\ a_{k-i} = 0\ (i \notin L),\ a_j \ge 0\ (\forall j)$$

# Linear programming bound

$\mathcal{B} \subset \binom{\Omega_v}{k}$, $2k \leq v$, $\quad L \subset \{0, 1, \ldots, k-1\}$

$$B, B' \in \mathcal{B},\ B \neq B' \implies |B \cap B'| \in L$$

$|\mathcal{B}|$ is bounded from the above by

$\max \sum_{i=0}^{k} a_i$ subject to $(a_0, a_1, \ldots, a_k)Q \geq 0$, (entrywise)

$$a_0 = 1,\ a_{k-i} = 0\ (i \notin L),\ a_j \geq 0\ (\forall j)$$

# Linear programming bound

$\mathcal{B} \subset \binom{\Omega_v}{k}$, $2k \leq v$, $\quad L \subset \{0, 1, \ldots, k-1\}$

$$B, B' \in \mathcal{B},\ B \neq B' \implies |B \cap B'| \in L$$

$|\mathcal{B}|$ is bounded from the above by

$\max \sum_{i=0}^{k} a_i$ subject to $(a_0, a_1, \ldots, a_k)Q \geq 0$, (entrywise)

$$a_0 = 1,\ a_{k-i} = 0\ (i \notin L),\ a_j \geq 0\ (\forall j)$$

$$Q_{ij} = \left(\binom{v}{j} - \binom{v}{j-1}\right) \sum_{r=0}^{j} (-1)^r \frac{\binom{i}{r}\binom{j}{r}\binom{v+1-j}{r}}{\binom{k}{r}\binom{v-k}{r}} \quad (0 \leq i, j \leq k).$$

# Example

$v = 62,\ k = 7,\ L = \{0, 1\}$. $|\mathcal{B}|$ is bounded from the above by

$$\max \sum_{i=0}^{7} a_i \text{ subject to } (a_0, a_1, \ldots, a_7)Q \geq 0,$$

$$a_0 = 1,\ a_{7-i} = 0\ (i \notin L),\ a_j \geq 0\ (\forall j)$$

# Example

$v = 62$, $k = 7$, $L = \{0, 1\}$. $|\mathcal{B}|$ is bounded from the above by

$$\max \sum_{i=0}^{7} a_i \text{ subject to } (a_0, a_1, \ldots, a_7)Q \geq 0,$$

$$a_0 = 1,\ a_{7-i} = 0\ (i \notin L),\ a_j \geq 0\ (\forall j)$$

$$\max \sum_{i=0}^{7} a_i \text{ subject to } (1, 0, \ldots, 0, a_6, a_7)Q \geq 0,$$

$$a_6 \geq 0,\ a_7 \geq 0$$

# Example

$v = 62, \; k = 7, \; L = \{0, 1\}$. $|\mathcal{B}|$ is bounded from the above by

$$\max \sum_{i=0}^{7} a_i \text{ subject to } (1, 0, \ldots, 0, a_6, a_7)Q \geq 0,$$
$$a_6 \geq 0, \; a_7 \geq 0$$

$$\max \; 1 + a + b \text{ subject to } (1, 0, \ldots, 0, a, b)Q \geq 0,$$
$$a \geq 0, \; b \geq 0$$

# Example

$v = 62, \; k = 7, \; L = \{0, 1\}$. $|\mathcal{B}|$ is bounded from the above by

$$\max \; 1 + a + b \text{ subject to } (1, 0, \ldots, 0, a, b)Q \geq 0,$$
$$a \geq 0, \; b \geq 0$$

# Example

$v = 62,\ k = 7,\ L = \{0,1\}$. $|\mathcal{B}|$ is bounded from the above by

$$\max\ 1 + a + b \text{ subject to } (1,0,\ldots,0,a,b)Q \geq 0,$$
$$a \geq 0,\ b \geq 0$$

$13a - 49b \geq -385,$
$-73a + 49b \geq -3465$

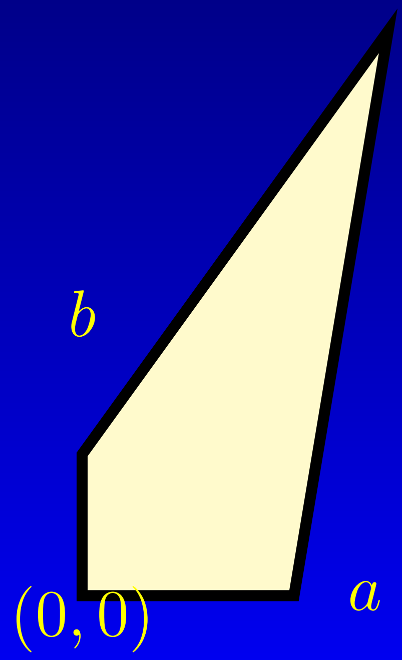
# Example

$v = 62,\ k = 7,\ L = \{0,1\}$. $|\mathcal{B}|$ is bounded from the above by

$$\max\ 1 + a + b \text{ subject to } (1,0,\ldots,0,a,b)Q \geq 0,$$
$$a \geq 0,\ b \geq 0$$

$$13a - 49b \geq -385,$$
$$-73a + 49b \geq -3465$$

maximized at $(a,b) = (\frac{385}{6}, \frac{1045}{42})$



# Example

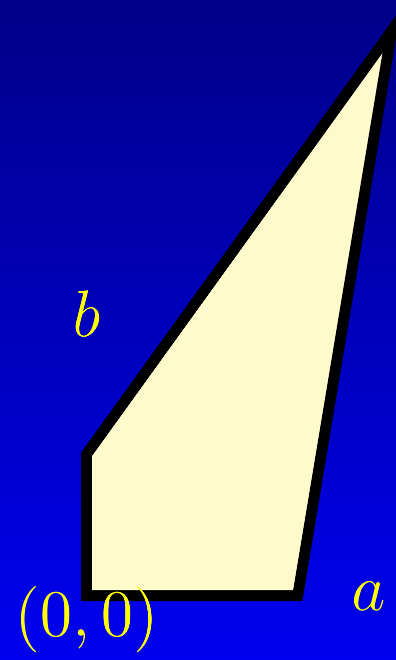
$v = 62,\ k = 7,\ L = \{0, 1\}$. $|\mathcal{B}|$ is bounded from the above by

$$\max\ 1 + a + b \text{ subject to } (1, 0, \ldots, 0, a, b)Q \geq 0,$$
$$a \geq 0,\ b \geq 0$$

$13a - 49b \geq -385,$
$-73a + 49b \geq -3465$

maximized at $(a, b) = (\frac{385}{6}, \frac{1045}{42})$

$|\mathcal{B}| \leq 1 + a + b = 1891/21$



# Example

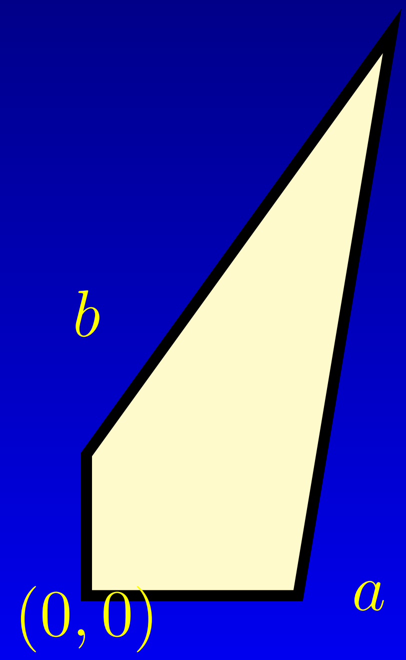
$v = 62,\ k = 7,\ L = \{0,1\}$. $|\mathcal{B}|$ is bounded from the above by

$$\max\ 1 + a + b \text{ subject to } (1,0,\ldots,0,a,b)Q \geq 0,$$
$$a \geq 0,\ b \geq 0$$

$$13a - 49b \geq -385,$$
$$-73a + 49b \geq -3465$$

maximized at $(a,b) = (\frac{385}{6}, \frac{1045}{42})$

$|\mathcal{B}| \leq 1 + a + b = 1891/21$
that is, $|\mathcal{B}| \leq 90$.



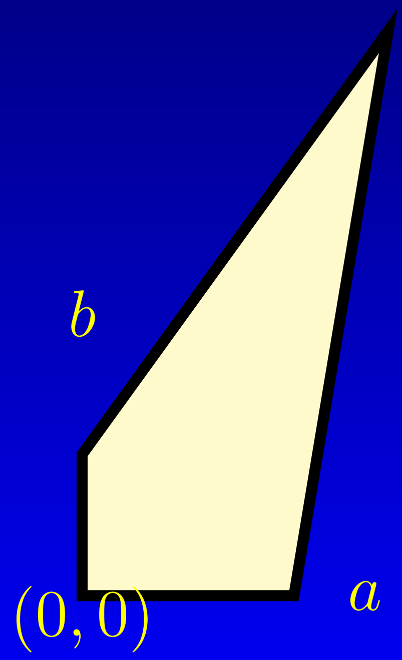
# Example

$v = 62,\ k = 7,\ L = \{0, 1\}$. $|\mathcal{B}|$ is bounded from the above by

$$\max\ 1 + a + b \text{ subject to } (1, 0, \ldots, 0, a, b)Q \geq 0,$$
$$a \geq 0,\ b \geq 0$$

$13a - 49b \geq -385,$
$-73a + 49b \geq -3465$

maximized at $(a, b) = (\frac{385}{6}, \frac{1045}{42})$




$|\mathcal{B}| \leq 1 + a + b = 1891/21$
that is, $|\mathcal{B}| \leq 90$.

# Binary codes

A binary code is a subset (often a subspace) of the vector space $\mathbb{F}_2^n$.

# Binary codes

A binary code is a subset (often a subspace) of the vector space $\mathbb{F}_2^n$.
$n$ is called the length of the code.

# Binary codes

A binary code is a subset (often a subspace) of the vector space $\mathbb{F}_2^n$. $n$ is called the length of the code. The support of a vector $\boldsymbol{u} \in \mathbb{F}_2^n$ is

$$\mathrm{supp}(\boldsymbol{u}) = \{j \mid 1 \leq j \leq n,\ u_j \neq 0\},$$

# Binary codes

A binary code is a subset (often a subspace) of the vector space $\mathbb{F}_2^n$. $n$ is called the length of the code. The support of a vector $\boldsymbol{u} \in \mathbb{F}_2^n$ is

$$\mathrm{supp}(\boldsymbol{u}) = \{j \mid 1 \leq j \leq n,\ u_j \neq 0\},$$

and the size of the support is the weight $\mathrm{wt}(\boldsymbol{u})$ of $\boldsymbol{u}$.

# Binary codes

A binary code is a subset (often a subspace) of the vector space $\mathbb{F}_2^n$.
$n$ is called the length of the code. The support of a vector $\boldsymbol{u} \in \mathbb{F}_2^n$ is

$$\mathrm{supp}(\boldsymbol{u}) = \{j \mid 1 \le j \le n,\ u_j \ne 0\},$$

and the size of the support is the weight $\mathrm{wt}(\boldsymbol{u})$ of $\boldsymbol{u}$.

An element of a code $C$ is called a codeword.

# Binary codes

A binary code is a subset (often a subspace) of the vector space $\mathbb{F}_2^n$.
$n$ is called the length of the code. The support of a vector $\boldsymbol{u} \in \mathbb{F}_2^n$ is

$$\mathrm{supp}(\boldsymbol{u}) = \{j \mid 1 \leq j \leq n,\ u_j \neq 0\},$$

and the size of the support is the weight $\mathrm{wt}(\boldsymbol{u})$ of $\boldsymbol{u}$.

An element of a code $C$ is called a codeword.
The minimum weight of $C$ is the minimum of weights of nonzero codewords.

# Binary codes

A binary code is a subset (often a subspace) of the vector space $\mathbb{F}_2^n$. $n$ is called the length of the code. The support of a vector $\boldsymbol{u} \in \mathbb{F}_2^n$ is

$$\mathrm{supp}(\boldsymbol{u}) = \{j \mid 1 \leq j \leq n,\ u_j \neq 0\},$$

and the size of the support is the weight $\mathrm{wt}(\boldsymbol{u})$ of $\boldsymbol{u}$.

An element of a code $C$ is called a codeword.
The minimum weight of $C$ is the minimum of weights of nonzero codewords.

An $[n, k, d]$ code $C$ is a linear code of length $n$, dimension $k$, and minimum weight $d$.

# Weight enumerator

Let $y$ be an indeterminate. For a binary code $C$ of length $n$, set

$$A_i = |\{\boldsymbol{u} \in C \mid \mathrm{wt}(\boldsymbol{u}) = i\}|$$

# Weight enumerator

Let $y$ be an indeterminate. For a binary code $C$ of length $n$, set

$$A_i = |\{\boldsymbol{u} \in C \mid \mathrm{wt}(\boldsymbol{u}) = i\}|$$

$$W_C = \sum_{i=0}^{n} A_i y^i$$

# Weight enumerator

Let $y$ be an indeterminate. For a binary code $C$ of length $n$, set

$$A_i = |\{\boldsymbol{u} \in C \mid \mathrm{wt}(\boldsymbol{u}) = i\}|$$

$$W_C = \sum_{i=0}^{n} A_i y^i$$

The polynomial $W_C$ is called the weight enumerator of $C$.

# Dual codes

The dual code of a linear code $C$ is

$$C^{\perp} = \{\boldsymbol{u} \in \mathbb{F}_2^n |\ (\boldsymbol{u}, \boldsymbol{v}) = 0 \text{ for all } \boldsymbol{v} \in C\}$$

# Dual codes

The dual code of a linear code $C$ is

$$C^{\perp} = \{\boldsymbol{u} \in \mathbb{F}_2^n \mid (\boldsymbol{u}, \boldsymbol{v}) = 0 \text{ for all } \boldsymbol{v} \in C\}$$

$C$: self-dual code $\iff C = C^{\perp}$.

# Dual codes

The dual code of a linear code $C$ is

$$C^{\perp} = \{\boldsymbol{u} \in \mathbb{F}_2^n \mid (\boldsymbol{u}, \boldsymbol{v}) = 0 \text{ for all } \boldsymbol{v} \in C\}$$

$C$: self-dual code $\iff C = C^{\perp}$.

For a self-dual code $C$,

# Dual codes

The dual code of a linear code $C$ is

$$C^{\perp} = \{\boldsymbol{u} \in \mathbb{F}_2^n |\ (\boldsymbol{u}, \boldsymbol{v}) = 0 \text{ for all } \boldsymbol{v} \in C\}$$

$C$: self-dual code $\iff C = C^{\perp}$.

For a self-dual code $C$,

$$C\text{: doubly even} \iff \mathrm{wt}(\boldsymbol{u}) \equiv 0 \pmod 4 \text{ for } \forall \boldsymbol{u} \in C.$$

# Dual codes

The dual code of a linear code $C$ is

$$C^{\perp} = \{\boldsymbol{u} \in \mathbb{F}_2^n \mid (\boldsymbol{u}, \boldsymbol{v}) = 0 \text{ for all } \boldsymbol{v} \in C\}$$

$C$: self-dual code $\iff C = C^{\perp}$.

For a self-dual code $C$,

$$C\text{: doubly even} \iff \mathrm{wt}(\boldsymbol{u}) \equiv 0 \pmod 4 \text{ for } \forall \boldsymbol{u} \in C.$$

Otherwise $C$ is called singly even.

# Shadows

Conway and Sloane (1990) introduced shadows of singly even self-dual codes.

# Shadows

Conway and Sloane (1990) introduced shadows of singly even self-dual codes. Let $C$ be a singly even self-dual code. Then

$$C_0 = \{\boldsymbol{u} \in C \mid \mathrm{wt}(\boldsymbol{u}) \equiv 0 \pmod 4\}$$

is a linear subspace of $C$ of codimension $1$.

# Shadows

Conway and Sloane (1990) introduced shadows of singly even self-dual codes. Let $C$ be a singly even self-dual code. Then

$$C_0 = \{\boldsymbol{u} \in C \mid \mathrm{wt}(\boldsymbol{u}) \equiv 0 \pmod 4\}$$

is a linear subspace of $C$ of codimension $1$.

There are cosets $C_1, C_2, C_3$ of $C_0$ such that
$C = C_0 \cup C_2$,
$S = C_0^{\perp} \setminus C = C_1 \cup C_3$ (shadow)

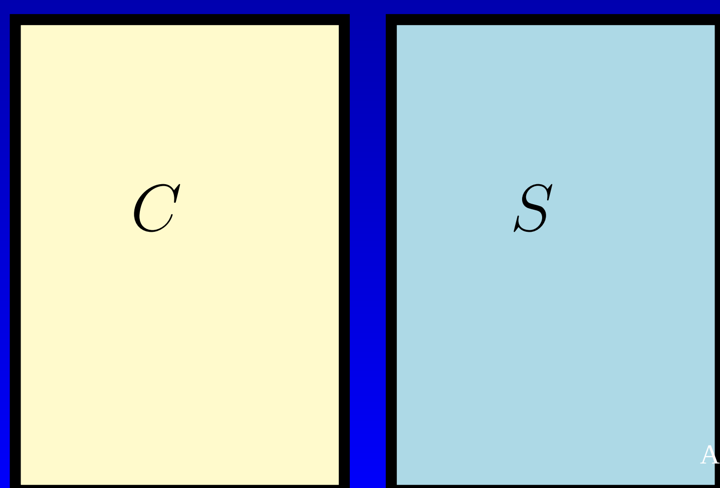
# Shadows

Conway and Sloane (1990) introduced shadows of singly even self-dual codes. Let $C$ be a singly even self-dual code. Then

$$C_0 = \{\boldsymbol{u} \in C \mid \mathrm{wt}(\boldsymbol{u}) \equiv 0 \pmod 4\}$$

is a linear subspace of $C$ of codimension $1$.

There are cosets $C_1, C_2, C_3$ of $C_0$ such that
$C = C_0 \cup C_2$,
$S = C_0^{\perp} \setminus C = C_1 \cup C_3 \quad$ (shadow)



# Weight enumerator

If $C$ is a self-dual code of length $n$, then

$$W_C = \sum_{j=0}^{[n/8]} a_j (1+y^2)^{n/2-4j} (y^2(1-y^2)^2)^j$$

# Weight enumerator

If $C$ is a self-dual code of length $n$, then

$$W_C = \sum_{j=0}^{[n/8]} a_j (1+y^2)^{n/2-4j} (y^2(1-y^2)^2)^j$$

$$W_S = \sum_{j=0}^{[n/8]} a_j (-1)^j 2^{n/2-6j} y^{n/2-4j} (1-y^4)^{2j}$$

# Weight enumerator

If $C$ is a self-dual code of length $n$, then

$$W_C = \sum_{j=0}^{[n/8]} a_j (1+y^2)^{n/2-4j} (y^2(1-y^2)^2)^j$$

$$W_S = \sum_{j=0}^{[n/8]} a_j (-1)^j 2^{n/2-6j} y^{n/2-4j} (1-y^4)^{2j}$$

In particular, $\forall \boldsymbol{u} \in S$,

$$\mathrm{wt}(\boldsymbol{u}) \equiv \frac{n}{2} \pmod 4.$$

# Extremality

The minimum weight $d$ of a self-dual code of length $n$ is bounded from the above by

$$d \leq \begin{cases} 4[n/24]+4 & n \not\equiv 22 \pmod{24}, \\ 4[n/24]+6 & n \equiv 22 \pmod{24}. \end{cases}$$

# Extremality

The minimum weight $d$ of a self-dual code of length $n$ is bounded from the above by

$$d \leq \begin{cases} 4[n/24] + 4 & n \not\equiv 22 \pmod{24}, \\ 4[n/24] + 6 & n \equiv 22 \pmod{24}. \end{cases}$$

A code achieving this bound is called extremal.

# Extremality

The minimum weight $d$ of a self-dual code of length $n$ is bounded from the above by

$$d \leq \begin{cases} 4[n/24] + 4 & n \not\equiv 22 \pmod{24}, \\ 4[n/24] + 6 & n \equiv 22 \pmod{24}. \end{cases}$$

A code achieving this bound is called extremal.
Equality imposes strong restrictions on the weight enumerator.

# Self-dual $[62, 31, 12]$ code

$$W_C = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + \cdots ,$$

$$W_S = \beta y^7 + 12(93 - \beta)y^{11} + \cdots$$

# **Self-dual** $[62, 31, 12]$ **code**

$$W_C = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + \cdots ,$$
$$W_S = \beta y^7 + 12(93 - \beta)y^{11} + \cdots$$

So $0 \le \beta \le 93$.

# **Self-dual** $[62, 31, 12]$ **code**

$$W_C = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + \cdots ,$$

$$W_S = \beta y^7 + 12(93 - \beta)y^{11} + \cdots$$

So $0 \leq \beta \leq 93$. On the other hand, there is a combinatorial bound. If $C$ has minimum distance $d$, then

# Self-dual $[62, 31, 12]$ code

$$W_C = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + \cdots ,$$

$$W_S = \beta y^7 + 12(93 - \beta)y^{11} + \cdots$$

So $0 \leq \beta \leq 93$. On the other hand, there is a combinatorial bound. If $C$ has minimum distance $d$, then

$$W_S = \sum_{r=0}^{n} B_r y^r \implies B_r \leq A(n, d, r),$$

# Self-dual $[62, 31, 12]$ code

$$W_C = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + \cdots ,$$
$$W_S = \beta y^7 + 12(93 - \beta)y^{11} + \cdots$$

So $0 \le \beta \le 93$. On the other hand, there is a combinatorial bound. If $C$ has minimum distance $d$, then

$$W_S = \sum_{r=0}^{n} B_r y^r \implies B_r \le A(n, d, r),$$

where $A(n, d, r)$ is the maximal possible number of binary vectors of length $n$, weight $r$ and Hamming distance at least $d$ apart. This is because $S$ (which is isometric to $C$) has minimum distance $d$.

# Self-dual $[62, 31, 12]$ code

$$W_C = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + \cdots ,$$

$$W_S = \beta y^7 + 12(93 - \beta)y^{11} + \cdots \qquad (0 \leq \beta \leq 93).$$

# Self-dual $[62, 31, 12]$ code

$$W_C = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + \cdots ,$$

$$W_S = \beta y^7 + 12(93 - \beta)y^{11} + \cdots \qquad (0 \le \beta \le 93).$$

$$\beta = B_7 \le A(62, 12, 7)$$

# Self-dual $[62, 31, 12]$ code

$$W_C = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + \cdots ,$$

$$W_S = \beta y^7 + 12(93 - \beta)y^{11} + \cdots \qquad (0 \le \beta \le 93).$$

$$\beta = B_7 \le A(62, 12, 7)$$

Hamming distance at least $12$ $\iff$ at most $1$-intersecting

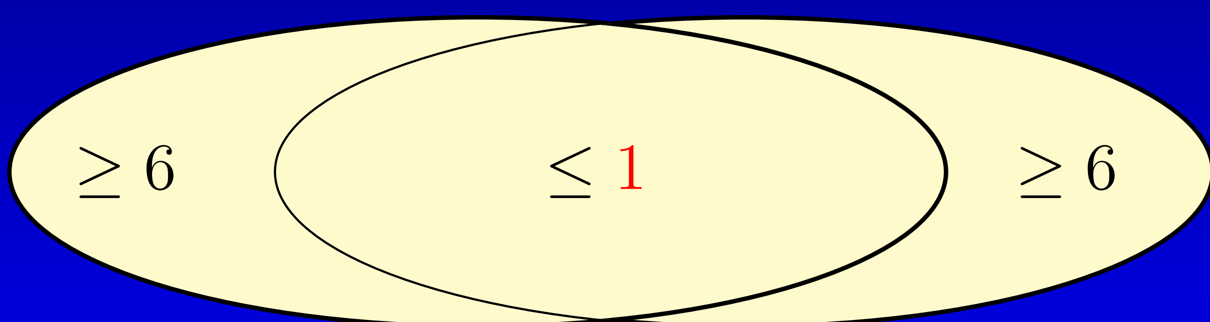
# **Self-dual** $[62, 31, 12]$ **code**

$$W_C = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + \cdots,$$

$$W_S = \beta y^7 + 12(93 - \beta)y^{11} + \cdots \qquad (0 \leq \beta \leq 93).$$

$$\beta = B_7 \leq A(62, 12, 7)$$

Hamming distance at least $12$ $\iff$ at most $1$-intersecting



# **Self-dual** $[62, 31, 12]$ **code**

$$W_C = 1 + (1860 + 32\beta)y^{12} + (28055 - 160\beta)y^{14} + \cdots ,$$
$$W_S = \beta y^7 + 12(93 - \beta)y^{11} + \cdots \qquad (0 \le \beta \le 93).$$

$$\beta = B_7 \le A(62, 12, 7)$$

Hamming distance at least $12 \iff$ at most $1$-intersecting
We have seen by the linear programming bound that

$$A(62, 12, 7) \le 90,$$

so

$$0 \le \beta \le 90.$$

# Two parts of the shadow

$C$
min. wt. 12

$S$
wt. 7

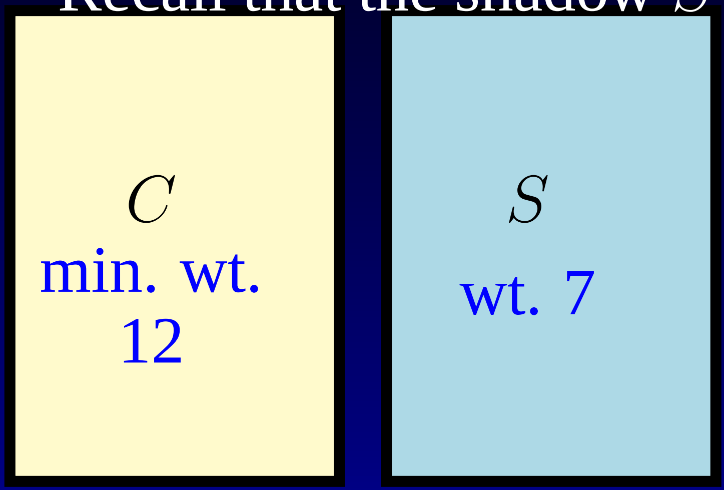
# Two parts of the shadow

| $C$ | $S$ |
| --- | --- |
| min. wt. 12 | wt. 7 |

$\Longrightarrow$ at most 1-intersecting

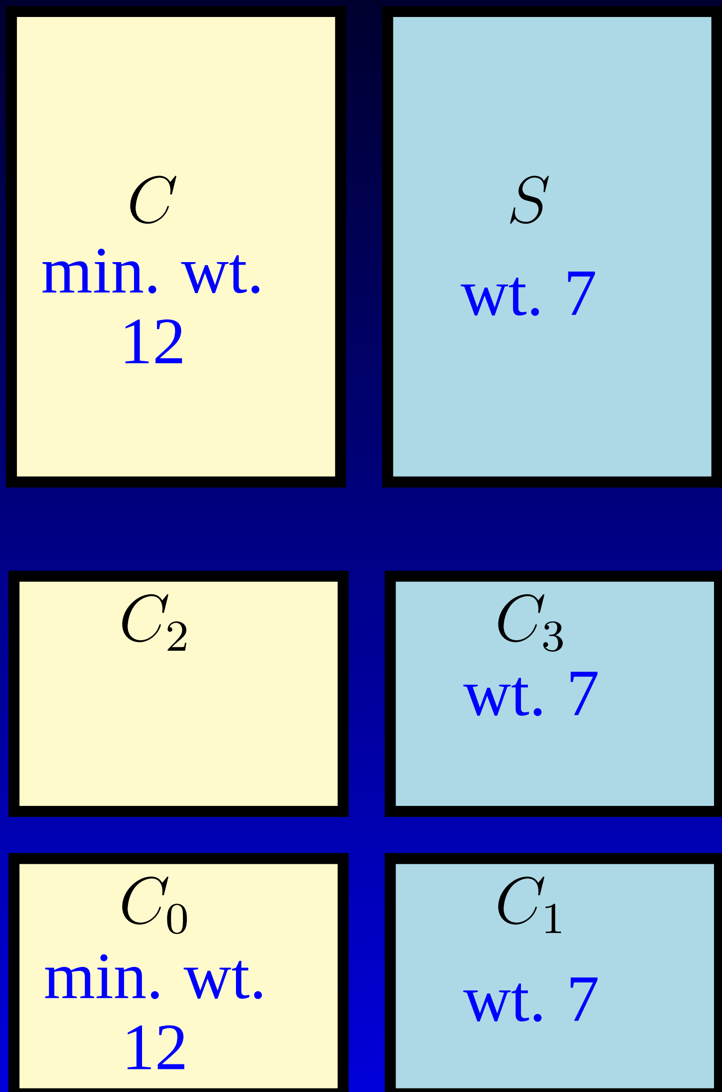
# Two parts of the shadow

Recall that the shadow $S$ consists of two cosets $C_1, C_3$ of $C_0$.



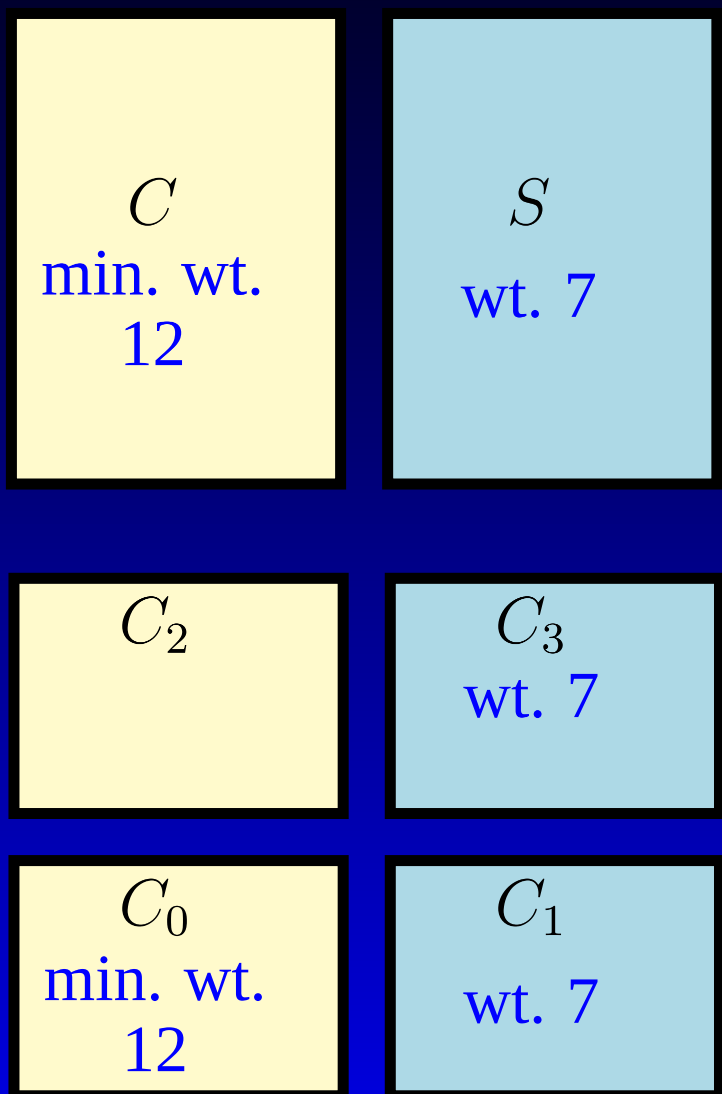

$\Longrightarrow$ at most 1-intersecting

# Two parts of the shadow




$\Longrightarrow$ at most 1-intersecting

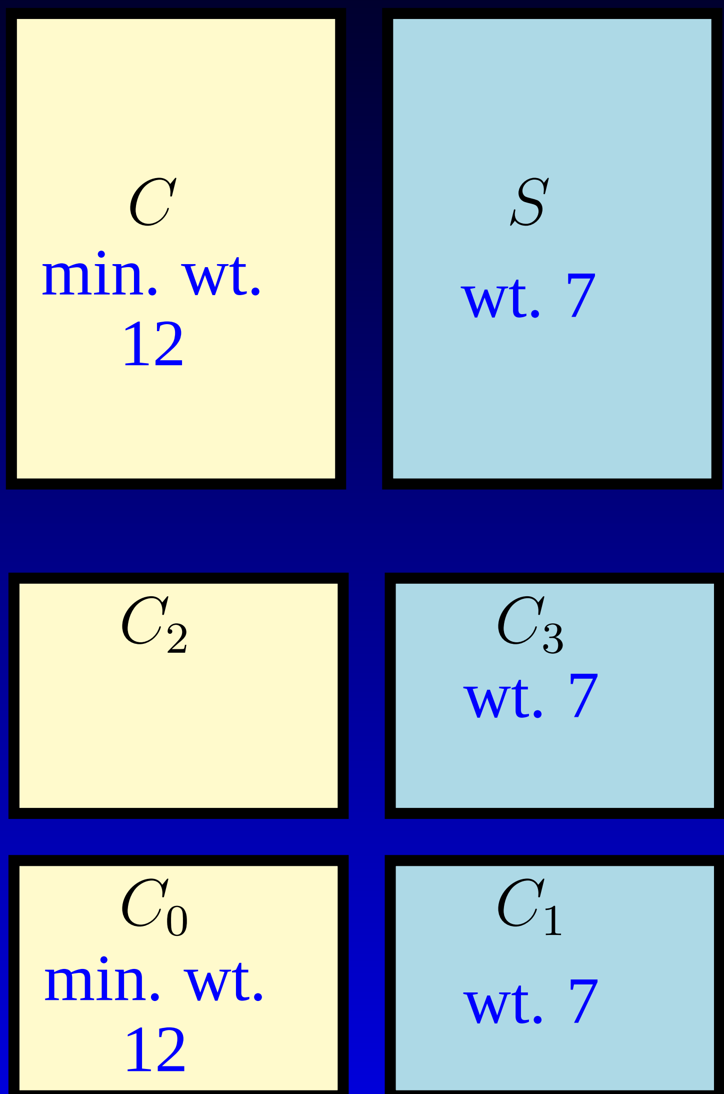
# Two parts of the shadow




$\Longrightarrow$ at most 1-intersecting

$\Longrightarrow$ Each of $C_1$ and $C_3$ is at 1-intersecting

# Two parts of the shadow

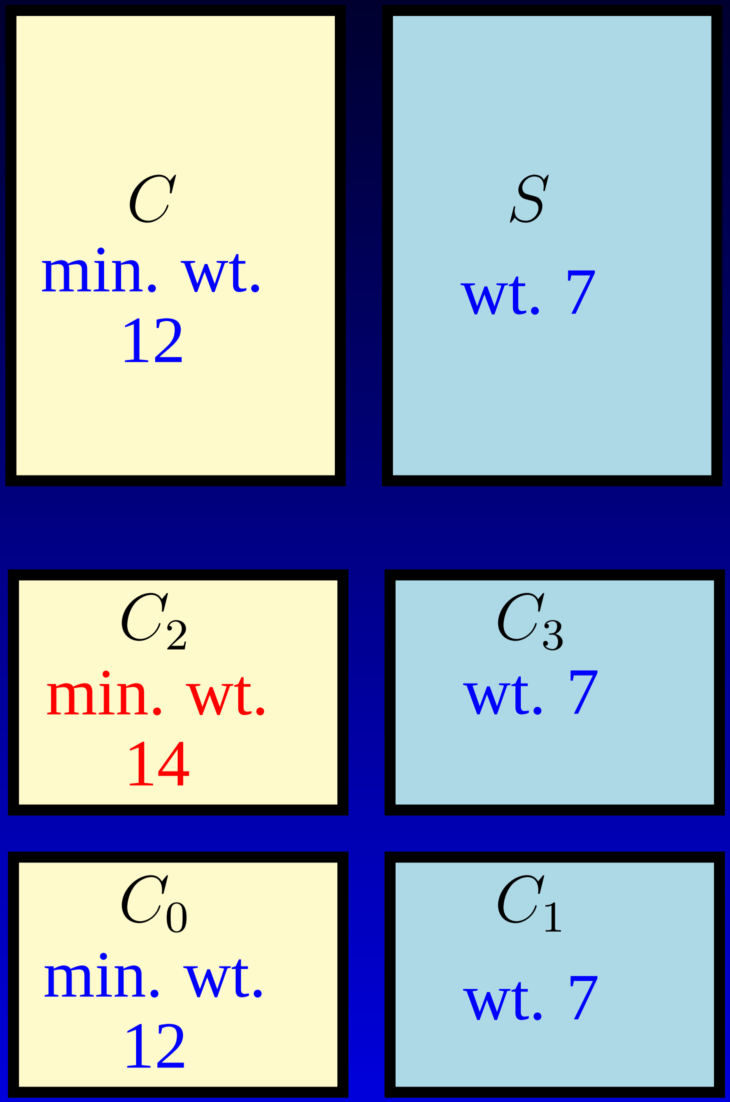



$\Longrightarrow$ at most 1-intersecting

$\Longrightarrow$ Each of $C_1$ and $C_3$ is at 1-intersecting

$$\boldsymbol{u} \in C_1, \boldsymbol{v} \in C_3 \Longrightarrow \boldsymbol{u}+\boldsymbol{v} \in C_2$$

# Two parts of the shadow




$\Longrightarrow$ at most 1-intersecting

$\Longrightarrow$ Each of $C_1$ and $C_3$ is at 1-intersecting

$$\boldsymbol{u} \in C_1, \boldsymbol{v} \in C_3 \Longrightarrow \boldsymbol{u} + \boldsymbol{v} \in C_2$$

# Two parts of the shadow

$C$
min. wt. 12

$S$
wt. 7

$\Longrightarrow$ at most 1-intersecting

$C_2$
min. wt. 14

$C_3$
wt. 7

$C_0$
min. wt. 12

$C_1$
wt. 7

$\Longrightarrow$ Each of $C_1$ and $C_3$ is at 1-intersecting

$$\boldsymbol{u} \in C_1, \boldsymbol{v} \in C_3 \Longrightarrow \boldsymbol{u} + \boldsymbol{v} \in C_2$$

$$\mathrm{supp}(\boldsymbol{u}) \cap \mathrm{supp}(\boldsymbol{v}) = \emptyset$$

# Two parts of the shadow

$$\mathcal{B}^{(i)} = \{\mathrm{supp}(\boldsymbol{u}) \mid \boldsymbol{u} \in C_i,\ \mathrm{wt}(\boldsymbol{u}) = 7\} \quad (i = 1, 3).$$

$$\mathcal{B} = \mathcal{B}^{(1)} \cup \mathcal{B}^{(3)} \subset \binom{\Omega_{62}}{7}$$

# Two parts of the shadow

$$\mathcal{B}^{(i)} = \{\mathrm{supp}(\boldsymbol{u}) \mid \boldsymbol{u} \in C_i,\ \mathrm{wt}(\boldsymbol{u}) = 7\} \quad (i = 1, 3).$$

$$\mathcal{B} = \mathcal{B}^{(1)} \cup \mathcal{B}^{(3)} \subset \binom{\Omega_{62}}{7}$$

Each of $\mathcal{B}^{(1)}, \mathcal{B}^{(3)}$ is (exactly) 1-intersecting, and

$$B \in \mathcal{B}^{(1)},\ B' \in \mathcal{B}^{(3)} \implies B \cap B' = \emptyset.$$

# Two parts of the shadow

$$\mathcal{B}^{(i)} = \{\mathrm{supp}(\boldsymbol{u}) \mid \boldsymbol{u} \in C_i,\ \mathrm{wt}(\boldsymbol{u}) = 7\} \quad (i = 1, 3).$$

$$\mathcal{B} = \mathcal{B}^{(1)} \cup \mathcal{B}^{(3)} \subset \binom{\Omega_{62}}{7}$$

Each of $\mathcal{B}^{(1)}, \mathcal{B}^{(3)}$ is (exactly) 1-intersecting, and

$$B \in \mathcal{B}^{(1)},\ B' \in \mathcal{B}^{(3)} \implies B \cap B' = \emptyset.$$

$$\Omega^{(1)} = \bigcup_{B \in \mathcal{B}^{(1)}} B, \qquad \Omega^{(3)} = \bigcup_{B' \in \mathcal{B}^{(3)}} B'.$$

# Two parts of the shadow

$$\mathcal{B}^{(i)} = \{\mathrm{supp}(\boldsymbol{u}) \mid \boldsymbol{u} \in C_i,\ \mathrm{wt}(\boldsymbol{u}) = 7\} \quad (i = 1, 3).$$

$$\mathcal{B} = \mathcal{B}^{(1)} \cup \mathcal{B}^{(3)} \subset \binom{\Omega_{62}}{7}$$

Each of $\mathcal{B}^{(1)}, \mathcal{B}^{(3)}$ is (exactly) 1-intersecting, and

$$B \in \mathcal{B}^{(1)},\ B' \in \mathcal{B}^{(3)} \implies B \cap B' = \emptyset.$$

$$\Omega^{(1)} = \bigcup_{B \in \mathcal{B}^{(1)}} B, \qquad \Omega^{(3)} = \bigcup_{B' \in \mathcal{B}^{(3)}} B'.$$

Then $\Omega^{(1)} \cap \Omega^{(3)} = \emptyset$, $\Omega^{(1)} \cup \Omega^{(3)} \subset \Omega_{62}$.

# Two parts of the shadow

$$\mathcal{B}^{(i)} = \{\mathrm{supp}(\boldsymbol{u}) \mid \boldsymbol{u} \in C_i,\ \mathrm{wt}(\boldsymbol{u}) = 7\} \quad (i = 1, 3).$$

$$\mathcal{B} = \mathcal{B}^{(1)} \cup \mathcal{B}^{(3)} \subset \binom{\Omega_{62}}{7}$$

Each of $\mathcal{B}^{(1)}, \mathcal{B}^{(3)}$ is (exactly) 1-intersecting, and

$$B \in \mathcal{B}^{(1)},\ B' \in \mathcal{B}^{(3)} \implies B \cap B' = \emptyset.$$

$$\Omega^{(1)} = \bigcup_{B \in \mathcal{B}^{(1)}} B, \qquad \Omega^{(3)} = \bigcup_{B' \in \mathcal{B}^{(3)}} B'.$$

Then $\Omega^{(1)} \cap \Omega^{(3)} = \emptyset$, $\Omega^{(1)} \cup \Omega^{(3)} \subset \Omega_{62}$.

$$\mathcal{B}^{(1)} \subset \binom{\Omega^{(1)}}{7}, \qquad \mathcal{B}^{(3)} \subset \binom{\Omega^{(3)}}{7}.$$

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta \leq 90.$$

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta \leq 90.$$

$|\mathcal{B}^{(i)}| \leq$ maximal possible size of 1-intersecting family in a $v^{(i)} = |\Omega^{(i)}|$-element set

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta \leq 90.$$

$|\mathcal{B}^{(i)}| \leq$ maximal possible size of 1-intersecting family
in a $v^{(i)} = |\Omega^{(i)}|$-element set
$\leq \max\ 1 + a$ subject to $(1, 0, 0, 0, 0, 0, a, 0)Q \geq 0,\ a \geq 0$

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta \leq 90.$$

$|\mathcal{B}^{(i)}| \leq$ maximal possible size of 1-intersecting family in a $v^{(i)} = |\Omega^{(i)}|$-element set

$\leq \max\ 1 + a$ subject to $(1, 0, 0, 0, 0, 0, a, 0)Q \geq 0,\ a \geq 0$

$=: M(v^{(i)})$.

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta \leq 90.$$

$|\mathcal{B}^{(i)}| \leq$ maximal possible size of 1-intersecting family
in a $v^{(i)} = |\Omega^{(i)}|$-element set
$\leq \max\ 1 + a$ subject to $(1, 0, 0, 0, 0, 0, a, 0)Q \geq 0,\ a \geq 0$
$=: M(v^{(i)})$.

$\beta \leq M(v^{(1)}) + M(v^{(3)})$

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta \le 90.$$

$|\mathcal{B}^{(i)}| \le$ maximal possible size of 1-intersecting family
in a $v^{(i)} = |\Omega^{(i)}|$-element set
$\le \max\ 1 + a$ subject to $(1, 0, 0, 0, 0, 0, a, 0)Q \ge 0,\ a \ge 0$
$=: M(v^{(i)})$.

$$\beta \le M(v^{(1)}) + M(v^{(3)})$$
$$\le \max\{M(v) + M(62 - v) \mid 0 \le v \le 62\}$$

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta \leq 90.$$

$|\mathcal{B}^{(i)}| \leq$ maximal possible size of 1-intersecting family in a $v^{(i)} = |\Omega^{(i)}|$-element set

$\leq \max\ 1 + a$ subject to $(1, 0, 0, 0, 0, 0, a, 0)Q \geq 0,\ a \geq 0$

$=: M(v^{(i)})$.

$$\beta \leq M(v^{(1)}) + M(v^{(3)})$$

$$\leq \max\{M(v) + M(62 - v) \mid 0 \leq v \leq 62\}$$

$$= 48.$$

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta \le 90.$$

$|\mathcal{B}^{(i)}| \le$ maximal possible size of 1-intersecting family
in a $v^{(i)} = |\Omega^{(i)}|$-element set
$\le \max\ 1 + a$ subject to $(1, 0, 0, 0, 0, 0, a, 0)Q \ge 0,\ a \ge 0$
$=: M(v^{(i)})$.

$\beta \le M(v^{(1)}) + M(v^{(3)})$
$\le \max\{M(v) + M(62 - v) \mid 0 \le v \le 62\}$
$= 48$.

Known realizable values of $\beta$:

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta \leq 90.$$

$|\mathcal{B}^{(i)}| \leq$ maximal possible size of 1-intersecting family
in a $v^{(i)} = |\Omega^{(i)}|$-element set
$\leq \max\ 1 + a$ subject to $(1, 0, 0, 0, 0, 0, a, 0)Q \geq 0,\ a \geq 0$
$=: M(v^{(i)})$.

$\beta \leq M(v^{(1)}) + M(v^{(3)})$
$\leq \max\{M(v) + M(62 - v) \mid 0 \leq v \leq 62\}$
$= 48$.

Known realizable values of $\beta$: 0,10,15.

(Dontcheva-Harada, 2002)

# Another example

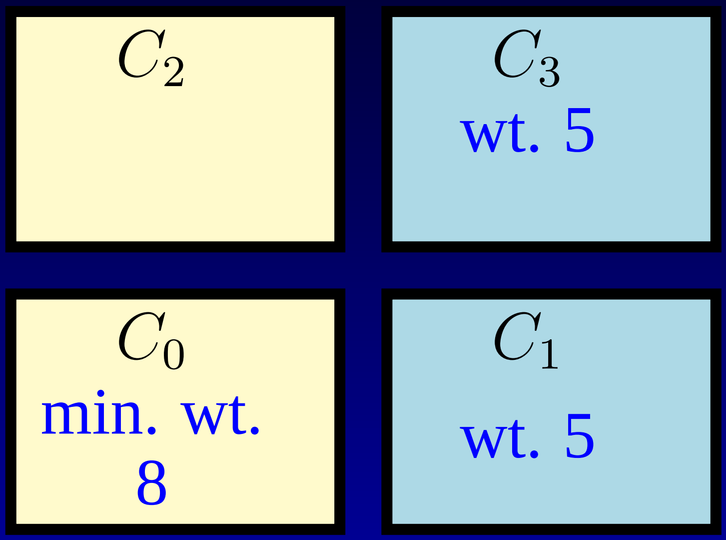
Every self-dual $[42, 21, 8]$ code $C$ whose shadow $S$ does not contain a vector of weight $1$ has weight enumerator

# Another example

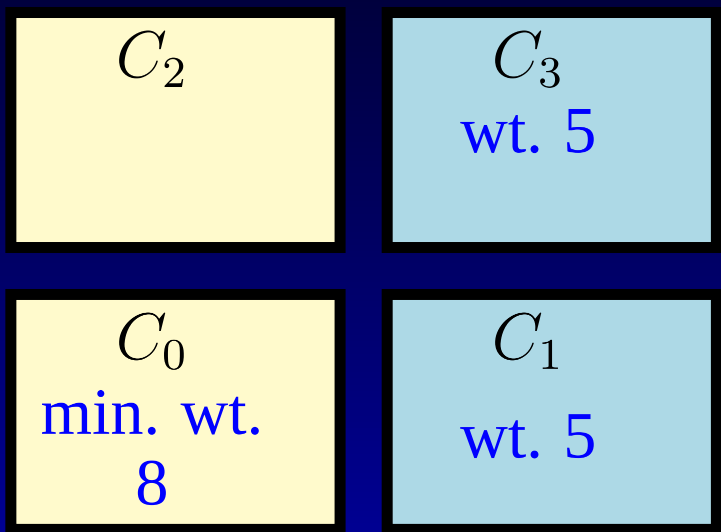
Every self-dual $[42, 21, 8]$ code $C$ whose shadow $S$ does not contain a vector of weight $1$ has weight enumerator

$$W_C = 1 + (84 + 8\beta)y^8 + (1449 - 24\beta)y^{10} + \cdots ,$$
$$W_S = \beta y^5 + (896 - 8\beta)y^9 + \cdots .$$

# Two parts of the shadow

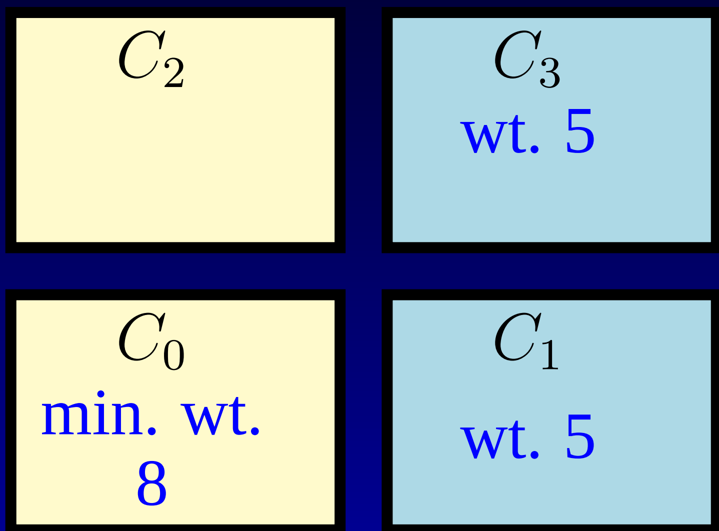


# Two parts of the shadow




$\Longrightarrow$ Each of $C_1$ and $C_3$ is at 1-intersecting

# Two parts of the shadow




$\Longrightarrow$ Each of $C_1$ and $C_3$ is at 1-intersecting

$$\boldsymbol{u} \in C_1, \boldsymbol{v} \in C_3 \Longrightarrow \boldsymbol{u} + \boldsymbol{v} \in C_2$$

# Two parts of the shadow

| | |
|---|---|
| $C_2$ min. wt. 10 | $C_3$ wt. 5 |
| $C_0$ min. wt. 8 | $C_1$ wt. 5 |

$\Longrightarrow$ Each of $C_1$ and $C_3$ is at 1-intersecting

$$\boldsymbol{u} \in C_1, \boldsymbol{v} \in C_3 \Longrightarrow \boldsymbol{u} + \boldsymbol{v} \in C_2$$

# Two parts of the shadow

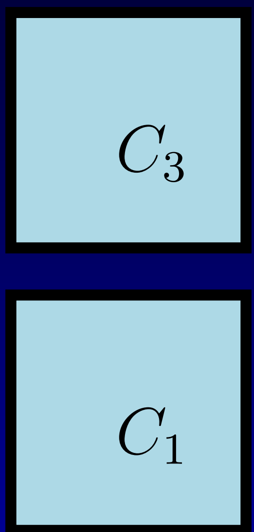
| | |
|---|---|
| $C_2$ min. wt. 10 | $C_3$ wt. 5 |
| $C_0$ min. wt. 8 | $C_1$ wt. 5 |

$\Longrightarrow$ Each of $C_1$ and $C_3$ is at 1-intersecting

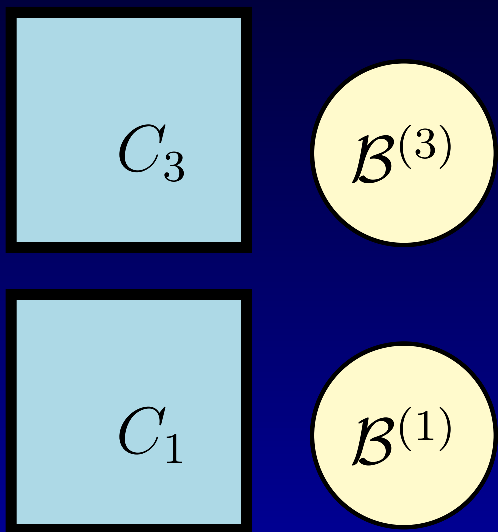
$$\boldsymbol{u} \in C_1, \boldsymbol{v} \in C_3 \implies \boldsymbol{u} + \boldsymbol{v} \in C_2$$

$$\mathrm{supp}(\boldsymbol{u}) \cap \mathrm{supp}(\boldsymbol{v}) = \emptyset$$

# Two parts of the shadow



# Two parts of the shadow




supports of
vectors of
weight $5$

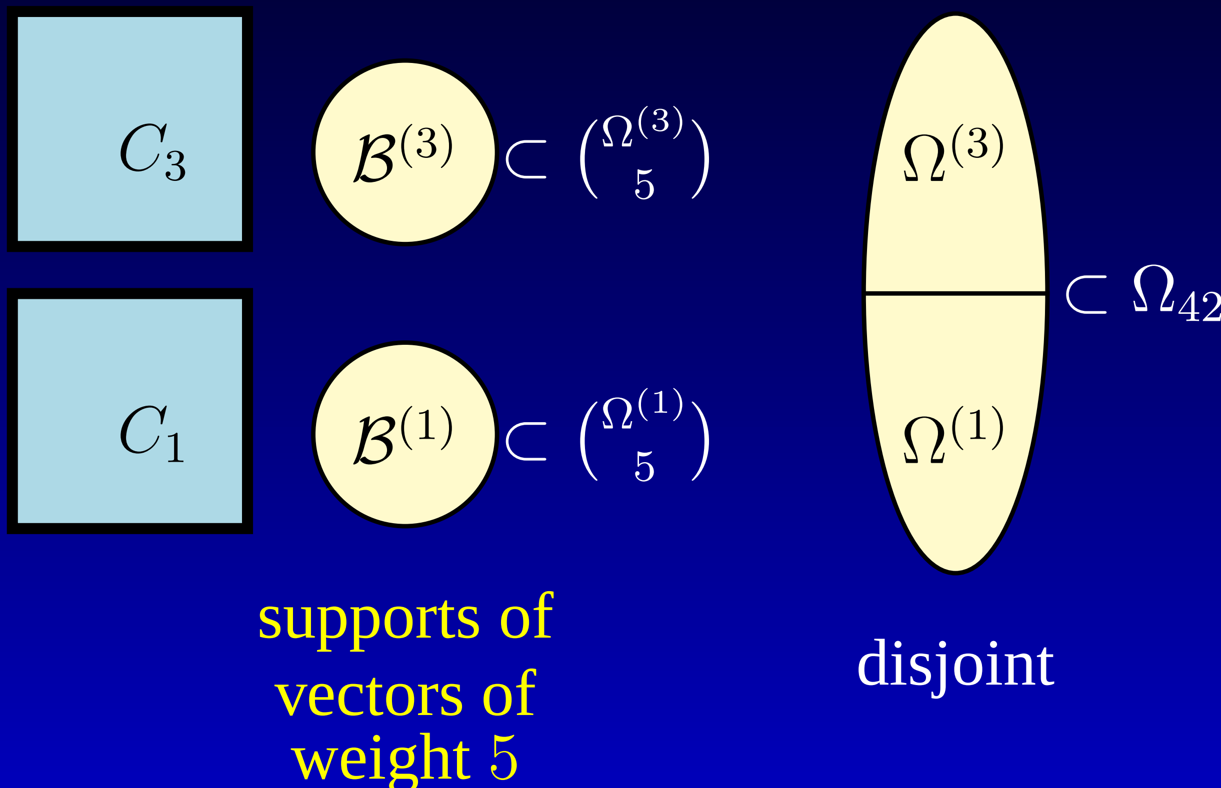
# Two parts of the shadow

$C_3$ $\mathcal{B}^{(3)} \subset \binom{\Omega^{(3)}}{5}$

$C_1$ $\mathcal{B}^{(1)} \subset \binom{\Omega^{(1)}}{5}$

supports of vectors of weight $5$

# Two parts of the shadow



# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta.$$

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta.$$

$|\mathcal{B}^{(i)}| \leq$ maximal possible size of 1-intersecting family in a $v^{(i)} = |\Omega^{(i)}|$-element set

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta.$$

$|\mathcal{B}^{(i)}| \le$ maximal possible size of 1-intersecting family
in a $v^{(i)} = |\Omega^{(i)}|$-element set
$\le \max\ 1 + a$ subject to $(1,0,0,0,0,0,a,0)Q \ge 0,\ a \ge 0$

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta.$$

$|\mathcal{B}^{(i)}| \leq$ maximal possible size of 1-intersecting family in a $v^{(i)} = |\Omega^{(i)}|$-element set

$\leq \max\ 1 + a$ subject to $(1,0,0,0,0,0,a,0)Q \geq 0,\ a \geq 0$

$=: M_5(v^{(i)}).$

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta.$$

$|\mathcal{B}^{(i)}| \leq$ maximal possible size of 1-intersecting family
in a $v^{(i)} = |\Omega^{(i)}|$-element set
$\leq \max\ 1 + a$ subject to $(1, 0, 0, 0, 0, 0, a, 0)Q \geq 0,\ a \geq 0$
$=: M_5(v^{(i)}).$

$$\beta \leq M_5(v^{(1)}) + M_5(v^{(3)})$$

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta.$$

$|\mathcal{B}^{(i)}| \leq$ maximal possible size of 1-intersecting family
in a $v^{(i)} = |\Omega^{(i)}|$-element set
$\leq \max\ 1 + a$ subject to $(1, 0, 0, 0, 0, 0, a, 0)Q \geq 0,\ a \geq 0$
$=: M_5(v^{(i)})$.

$$\beta \leq M_5(v^{(1)}) + M_5(v^{(3)})$$
$$\leq \max\{M_5(v) + M_5(42 - v) \mid 0 \leq v \leq 42\}$$

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta.$$

$|\mathcal{B}^{(i)}| \leq$ maximal possible size of 1-intersecting family
in a $v^{(i)} = |\Omega^{(i)}|$-element set
$\leq \max\ 1 + a$ subject to $(1, 0, 0, 0, 0, 0, a, 0)Q \geq 0,\ a \geq 0$
$=: M_5(v^{(i)})$.

$$\begin{aligned}\beta &\leq M_5(v^{(1)}) + M_5(v^{(3)}) \\ &\leq \max\{M_5(v) + M_5(42 - v) \mid 0 \leq v \leq 42\} \\ &= 42.\end{aligned}$$

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta.$$

$|\mathcal{B}^{(i)}| \leq$ maximal possible size of 1-intersecting family
in a $v^{(i)} = |\Omega^{(i)}|$-element set
$\leq \max\ 1 + a$ subject to $(1,0,0,0,0,0,a,0)Q \geq 0,\ a \geq 0$
$=: M_5(v^{(i)})$.

$$\beta \leq M_5(v^{(1)}) + M_5(v^{(3)})$$
$$\leq \max\{M_5(v) + M_5(42 - v) \mid 0 \leq v \leq 42\}$$
$$= 42.$$

Equality holds only if $v^{(1)} = v^{(3)} = 21$ and in this case

# Improved upper bound

$$|\mathcal{B}^{(1)}| + |\mathcal{B}^{(3)}| = |\mathcal{B}| = \beta.$$

$|\mathcal{B}^{(i)}| \le$ maximal possible size of 1-intersecting family
in a $v^{(i)} = |\Omega^{(i)}|$-element set
$\le \max\ 1 + a$ subject to $(1,0,0,0,0,0,a,0)Q \ge 0,\ a \ge 0$
$=: M_5(v^{(i)})$.

$\beta \le M_5(v^{(1)}) + M_5(v^{(3)})$
$\le \max\{M_5(v) + M_5(42 - v) \mid 0 \le v \le 42\}$
$= 42$.

Equality holds only if $v^{(1)} = v^{(3)} = 21$ and in this case

$$\mathcal{B}^{(1)} \cong \mathcal{B}^{(2)} \cong PG(2,4).$$

# Characterization

**Theorem 2.** *There exists a unique binary self-dual* $[42, 21, 8]$ *code with weight enumerator*

$$W_C = 1 + (84 + 8\beta)y^8 + (1449 - 24\beta)y^10 + \cdots\ ,$$

$$W_S = \beta y^5 + (896 - 8\beta)y^9 + \cdots\ .$$

*with* $\beta = 42$.

# Characterization

**Theorem 1.** *There exists a unique binary self-dual* $[42, 21, 8]$ *code with weight enumerator*

$$W_C = 1 + (84 + 8\beta)y^8 + (1449 - 24\beta)y^10 + \cdots \ ,$$
$$W_S = \beta y^5 + (896 - 8\beta)y^9 + \cdots \ .$$

*with* $\beta = 42$.

This theorem was obtained recently, and independently, by Stefka Buyuklieva.