Covering Radii of Extremal Binary Doubly Even Self-Dual Codes

Akihiro Munemasa\textsuperscript{1}

\begin{itemize}
  \item \textsuperscript{1}Graduate School of Information Sciences
  \item Tohoku University
  \item (joint work with Masaaki Harada)
\end{itemize}

Asian Symposium on Computer Mathematics, 2005
Definition

- $X$: a finite metric space
- $C$: a subset of $X$

The covering radius of $C$ is $\rho(C) = \max_{x \in X} \left( \min_{c \in C} d(c, x) \right)$.

$\rho(C)$ is the least nonnegative number $\rho$ such that all points of $X$ are within distance $\rho$ from some point of $C$.

Problem: Given $X$ and $|C|$, minimize $\rho(C)$. 
Definition

- \( X \): a finite metric space
- \( C \): a subset of \( X \)
- The covering radius of \( C \) is \( \rho(C) = \max_{x \in X} \left( \min_{c \in C} d(c, x) \right) \).

\( \rho(C) \) is the least nonnegative number \( \rho \) such that all points of \( X \) are within distance \( \rho \) from some point of \( C \).

Problem: Given \( X \) and \(|C|\), minimize \( \rho(C) \).
Covering Radius of a Subset of a Metric Space

**Definition**

- \( X \): a finite metric space
- \( C \): a subset of \( X \)
- The **covering radius** of \( C \) is \( \rho(C) = \max_{x \in X} \left( \min_{c \in C} d(c, x) \right) \).

\( \rho(C) \) is the least nonnegative number \( \rho \) such that all points of \( X \) are within distance \( \rho \) from some point of \( C \).

Problem: Given \( X \) and \(|C|\), minimize \( \rho(C) \).
Covering Radius of a Subset of a Metric Space

**Definition**

- **X**: a finite metric space
- **C**: a subset of **X**
- The **covering radius** of **C** is $\rho(C) = \max_{x \in X} \left( \min_{c \in C} d(c, x) \right)$.

$\rho(C)$ is the least nonnegative number $\rho$ such that all points of **X** are within distance $\rho$ from some point of **C**.

Problem: Given **X** and $|C|$, minimize $\rho(C)$. 
Binary Codes

- $\mathbb{F}_2 = \{0, 1\}$.
- $X = \mathbb{F}_2^n$ with $d = \text{Hamming distance}$.
  - $d(x, y)$ is the number of i’s with $x_i \neq y_i$, where $x, y \in X$.
  - Also $d(x, y) = \text{wt}(x - y)$, the weight of the vector $x - y$, the number of nonzero (in this case 1) entries in $x - y$.
- $C$ is a linear code of length $n$, i.e., $C \subseteq \mathbb{F}_2^n$, closed under binary addition.

Problem: Given $n, k$, minimize $\rho(C)$ among linear codes $C \subseteq \mathbb{F}_2^n$ with $\text{dim } C = k$.

- $C^\perp = \{x \in \mathbb{F}_2^n \mid \sum_{i=1}^{n} x_i y_i = 0\}$: dual code
Binary Codes

- $\mathbb{F}_2 = \{0, 1\}$.

- $X = \mathbb{F}_2^n$ with $d =$ Hamming distance.
  - $d(x, y)$ = the number of $i$’s with $x_i \neq y_i$, where $x, y \in X$.
  - also $d(x, y) = \text{wt}(x - y)$, the weight of the vector $x - y$, the number of nonzero (in this case 1) entries in $x - y$.

- $C =$ linear code of length $n$, i.e., $C \subseteq \mathbb{F}_2^n$, closed under binary addition.

Problem: Given $n, k$, minimize $\rho(C)$ among linear codes $C \subseteq \mathbb{F}_2^n$ with $\dim C = k$.

- $C^\perp = \{x \in \mathbb{F}_2^n \mid \sum_{i=1}^n x_i y_i = 0\}$ : dual code
Binary Codes

- $\mathbb{F}_2 = \{0, 1\}$.
- $X = \mathbb{F}_2^n$ with $d =$ Hamming distance.
  - $d(x, y)$ = the number of $i$’s with $x_i \neq y_i$, where $x, y \in X$.
  - Also $d(x, y) = \text{wt}(x - y)$, the weight of the vector $x - y$, the number of nonzero (in this case 1) entries in $x - y$.

- $C =$ linear code of length $n$, i.e., $C \subseteq \mathbb{F}_2^n$, closed under binary addition.

Problem: Given $n, k$, minimize $\rho(C)$ among linear codes $C \subseteq \mathbb{F}_2^n$ with $\text{dim } C = k$.

- $C^\perp = \{x \in \mathbb{F}_2^n \mid \sum_{i=1}^n x_iy_i = 0\}$ : dual code
Binary Codes

- $\mathbb{F}_2 = \{0, 1\}$.
- $X = \mathbb{F}_2^n$ with $d =$ Hamming distance.
  - $d(x, y) =$ the number of $i$’s with $x_i \neq y_i$, where $x, y \in X$.
  - Also $d(x, y) = \text{wt}(x - y)$, the weight of the vector $x - y$, the number of nonzero (in this case 1) entries in $x - y$.
- $C =$ linear code of length $n$, i.e., $C \subseteq \mathbb{F}_2^n$, closed under binary addition.

Problem: Given $n, k$, minimize $\rho(C)$ among linear codes $C \subseteq \mathbb{F}_2^n$ with $\dim C = k$.

- $C^\perp = \{x \in \mathbb{F}_2^n \mid \sum_{i=1}^{n} x_i y_i = 0\} :$ dual code
Binary Codes

- $\mathbb{F}_2 = \{0, 1\}$.
- $X = \mathbb{F}_2^n$ with $d =$ Hamming distance.
  - $d(x, y) =$ the number of $i$’s with $x_i \neq y_i$, where $x, y \in X$.
  - also $d(x, y) = \text{wt}(x - y)$, the weight of the vector $x - y$, the number of nonzero (in this case 1) entries in $x - y$.
- $C =$ linear code of length $n$, i.e., $C \subseteq \mathbb{F}_2^n$, closed under binary addition.

Problem: Given $n, k$, minimize $\rho(C)$ among linear codes $C \subseteq \mathbb{F}_2^n$ with $\text{dim } C = k$.

- $C^\perp = \{x \in \mathbb{F}_2^n \mid \sum_{i=1}^n x_i y_i = 0\}$ : dual code
Binary Codes

- $\mathbb{F}_2 = \{0, 1\}$.
- $X = \mathbb{F}_2^n$ with $d =$ Hamming distance.
  - $d(x, y)$ = the number of $i$’s with $x_i \neq y_i$, where $x, y \in X$.
  - also $d(x, y) = \text{wt}(x - y)$, the weight of the vector $x - y$, the number of nonzero (in this case 1) entries in $x - y$.
- $C =$ linear code of length $n$, i.e., $C \subseteq \mathbb{F}_2^n$, closed under binary addition.

Problem: Given $n, k$, minimize $\rho(C)$ among linear codes $C \subseteq \mathbb{F}_2^n$ with dim $C = k$.

- $C^\perp = \{x \in \mathbb{F}_2^n \mid \sum_{i=1}^n x_i y_i = 0\}$ : dual code
Binary Codes

- $\mathbb{F}_2 = \{0, 1\}$.
- $X = \mathbb{F}_2^n$ with $d =$ Hamming distance.
  - $d(x, y) =$ the number of $i$’s with $x_i \neq y_i$, where $x, y \in X$.
  - also $d(x, y) = \text{wt}(x - y)$, the weight of the vector $x - y$, the number of nonzero (in this case 1) entries in $x - y$.
- $C =$ linear code of length $n$, i.e., $C \subseteq \mathbb{F}_2^n$, closed under binary addition.

Problem: Given $n, k$, minimize $\rho(C)$ among linear codes $C \subseteq \mathbb{F}_2^n$ with dim $C = k$.

- $C^\perp = \{x \in \mathbb{F}_2^n \mid \sum_{i=1}^n x_i y_i = 0\} :$ dual code
The Delsarte Bound
An Upper Bound on the Covering Radius $\rho(C)$, due to Delsarte (1973)

- $\rho(C) \leq r(C) := |\{\text{wt}(c) \mid c \in C^\perp, c \neq 0\}|.$
- $r(C)$ is called the external distance, or the dual degree of $C$.
- For arbitrary codes $C$, hard to assert something exact on $r(C)$, since it depends on $C^\perp$.
- However, if $C = C^\perp$, $r(C)$ is directly related to $C$ itself.
The Delsarte Bound
An Upper Bound on the Covering Radius $\rho(C)$, due to Delsarte (1973)

- $\rho(C) \leq r(C) := |\{\mathrm{wt}(c) \mid c \in C^\perp, c \neq 0\}|$.
- $r(C)$ is called the external distance, or the dual degree of $C$.

- For arbitrary codes $C$, hard to assert something exact on $r(C)$, since it depends on $C^\perp$.
- However, if $C = C^\perp$, $r(C)$ is directly related to $C$ itself.
The Delsarte Bound
An Upper Bound on the Covering Radius $\rho(C)$, due to Delsarte (1973)

- $\rho(C) \leq r(C) := |\{\text{wt}(c) \mid c \in C^\perp, c \neq 0\}|$.
- $r(C)$ is called the external distance, or the dual degree of $C$.
- For arbitrary codes $C$, hard to assert something exact on $r(C)$, since it depends on $C^\perp$.
- However, if $C = C^\perp$, $r(C)$ is directly related to $C$ itself.
The Delsarte Bound
An Upper Bound on the Covering Radius $\rho(C)$, due to Delsarte (1973)

- $\rho(C) \leq r(C) := |\{\text{wt}(c) \mid c \in C^\perp, c \neq 0\}|$.
- $r(C)$ is called the external distance, or the dual degree of $C$.
- For arbitrary codes $C$, hard to assert something exact on $r(C)$, since it depends on $C^\perp$.
- However, if $C = C^\perp$, $r(C)$ is directly related to $C$ itself.
Self-Dual Codes

Definition

A linear code $C \subseteq \mathbb{F}_2^n$ satisfying $C = C^\perp$ is called self-dual.

- For a self-dual code $C$, $\rho(C) \leq r(C) = |\{\text{wt}(c) \mid c \in C, c \neq 0\}|$.
- Self-duality of $C$ implies $\text{wt}(c)$ is even for all $c \in C$.
- There are self-dual codes $C$ whose $r(C)$ is much smaller; having the property $\text{wt}(c) \equiv 0 \pmod{4}$ for all $c \in C$.

Definition

A linear code $C$ is said to be doubly even if $\text{wt}(c) \equiv 0 \pmod{4}$ for all $c \in C$. 
Definitions and Preliminaries

Self-Dual Codes

Definition

A linear code $C \subseteq \mathbb{F}_2^n$ satisfying $C = C^\perp$ is called self-dual.

- For a self-dual code $C$, $\rho(C) \leq r(C) = |\{\text{wt}(c) \mid c \in C, c \neq 0\}|$.
- Self-duality of $C$ implies $\text{wt}(c)$ is even for all $c \in C$.
- There are self-dual codes $C$ whose $r(C)$ is much smaller; having the property $\text{wt}(c) \equiv 0 \pmod{4}$ for all $c \in C$.

Definition

A linear code $C$ is said to be doubly even if $\text{wt}(c) \equiv 0 \pmod{4}$ for all $c \in C$. 
Self-Dual Codes

Definition
A linear code $C \subseteq \mathbb{F}_2^n$ satisfying $C = C^\perp$ is called self-dual.

- For a self-dual code $C$, $\rho(C) \leq r(C) = |\{\text{wt}(c) | c \in C, c \neq 0\}|$.
- Self-duality of $C$ implies wt$(c)$ is even for all $c \in C$.
- There are self-dual codes $C$ whose $r(C)$ is much smaller; having the property wt$(c) \equiv 0 \pmod{4}$ for all $c \in C$.

Definition
A linear code $C$ is said to be doubly even if wt$(c) \equiv 0 \pmod{4}$ for all $c \in C$. 
Self-Dual Codes

Definition

A linear code $C \subseteq \mathbb{F}_2^n$ satisfying $C = C^\perp$ is called **self-dual**.

- For a self-dual code $C$,  
  $$\rho(C) \leq r(C) = |\{\text{wt}(c) \mid c \in C, \ c \neq 0\}|.$$
- Self-duality of $C$ implies $\text{wt}(c)$ is even for all $c \in C$.
- There are self-dual codes $C$ whose $r(C)$ is much smaller; having the property $\text{wt}(c) \equiv 0 \pmod{4}$ for all $c \in C$.

Definition

A linear code $C$ is said to be **doubly even** if $\text{wt}(c) \equiv 0 \pmod{4}$ for all $c \in C$. 

Akihiro Munemasa

Covering Radii
Self-Dual Codes

**Definition**

A linear code $C \subseteq \mathbb{F}_2^n$ satisfying $C = C^\perp$ is called **self-dual**.

- For a self-dual code $C$, 
  $$\rho(C) \leq r(C) = |\{\text{wt}(c) \mid c \in C, \ c \neq 0\}|.$$
- Self-duality of $C$ implies $\text{wt}(c)$ is even for all $c \in C$.
- There are self-dual codes $C$ whose $r(C)$ is much smaller; having the property $\text{wt}(c) \equiv 0 \pmod{4}$ for all $c \in C$.

**Definition**

A linear code $C$ is said to be doubly even if $\text{wt}(c) \equiv 0 \pmod{4}$ for all $c \in C$. 

Akihiro Munemasa  
Covering Radii
Recall that a doubly even self-dual code is a linear code $C$ with $C = C^\perp$, satisfying $\text{wt}(c) \equiv 0 \pmod{4}$ for all $c \in C$.

**Proposition**

A doubly even self-dual code exists if and only if the length is a multiple of 8.

**Definition**

Let $\mu := \left\lfloor \frac{n}{24} \right\rfloor$. A doubly even self-dual code is said to be extremal if $\min(C) := \min \{ \text{wt}(c) \mid c \in C, c \neq 0 \} = 4\mu + 4$.

- For $n = 32$, $\{ \text{wt}(c) \mid c \in C^\perp, c \neq 0 \} = \{8, 12, 16, 20, 24, 32\}$ has size 6, i.e., $\rho(C) \leq r(C) = 6$.
- It turns out $\rho(C) = r(C)$ for all such codes $C$. 

Akihiro Munemasa

Covering Radii
Recall that a doubly even self-dual code is a linear code $C$ with $C = C^\perp$, satisfying $\text{wt}(c) \equiv 0 \pmod{4}$ for all $c \in C$.

**Proposition**

A doubly even self-dual code exists if and only if the length is a multiple of 8.

**Definition**

Let $\mu := \left\lfloor \frac{n}{24} \right\rfloor$. A doubly even self-dual code is said to be extremal if $\min(C) := \min\{\text{wt}(c) \mid c \in C, c \neq 0\} = 4\mu + 4$.

- For $n = 32$, $\{\text{wt}(c) \mid c \in C^\perp, c \neq 0\} = \{8, 12, 16, 20, 24, 32\}$ has size 6, i.e., $\rho(C) \leq r(C) = 6$.
- It turns out $\rho(C) = r(C)$ for all such codes $C$. 
Recall that a doubly even self-dual code is a linear code $C$ with $C = C^\perp$, satisfying $\text{wt}(c) \equiv 0 \pmod{4}$ for all $c \in C$.

**Proposition**

A doubly even self-dual code exists if and only if the length is a multiple of 8.

**Definition**

Let $\mu := \left\lceil \frac{n}{24} \right\rceil$. A doubly even self-dual code is said to be extremal if $\min(C) := \min\{\text{wt}(c) \mid c \in C, \ c \neq 0\} = 4\mu + 4$.

- For $n = 32$, $\{\text{wt}(c) \mid c \in C^\perp, \ c \neq 0\} = \{8, 12, 16, 20, 24, 32\}$ has size 6, i.e., $\rho(C) \leq r(C) = 6$.
- It turns out $\rho(C) = r(C)$ for all such codes $C$. 
Recall that a doubly even self-dual code is a linear code $C$ with $C = C^\perp$, satisfying $\text{wt}(c) \equiv 0 \pmod{4}$ for all $c \in C$.

**Proposition**

A doubly even self-dual code exists if and only if the length is a multiple of 8.

**Definition**

Let $\mu := \left\lfloor \frac{n}{24} \right\rfloor$. A doubly even self-dual code is said to be extremal if $\min(C) := \min\{\text{wt}(c) \mid c \in C, c \neq 0\} = 4\mu + 4$.

- For $n = 32$, $\{\text{wt}(c) \mid c \in C^\perp, c \neq 0\} = \{8, 12, 16, 20, 24, 32\}$ has size 6, i.e., $\rho(C) \leq r(C) = 6$.
- It turns out $\rho(C) = r(C)$ for all such codes $C$. 
Recall that a doubly even self-dual code is a linear code $C$ with $C = C^\perp$, satisfying $\text{wt}(c) \equiv 0 \pmod{4}$ for all $c \in C$.

**Proposition**

A doubly even self-dual code exists if and only if the length is a multiple of 8.

**Definition**

Let $\mu := \left\lfloor \frac{n}{24} \right\rfloor$. A doubly even self-dual code is said to be extremal if $\min(C) := \min\{\text{wt}(c) \mid c \in C, c \neq 0\} = 4\mu + 4$.

- For $n = 32$, $\{\text{wt}(c) \mid c \in C^\perp, c \neq 0\} = \{8, 12, 16, 20, 24, 32\}$ has size 6, i.e., $\rho(C) \leq r(C) = 6$.
- It turns out $\rho(C) = r(C)$ for all such codes $C$. 
The Sphere Covering Bound
A Lower Bound on the Covering Radius $\rho(C)$

The volume (the number of points) of a sphere of radius $\rho$ in $\mathbb{F}_2^n$ is $\sum_{i=0}^{\rho} \binom{n}{i}$.

**Proposition**

$$|C| \sum_{i=0}^{\rho(C)} \binom{n}{i} \geq 2^n$$

This gives a lower bound of $\rho(C)$.

For self-dual codes (or more generally, for even codes), slight improvement is possible:

$$|C| \sum_{i=0}^{[\rho(C)/2]} \binom{n}{2i} \geq 2^{n-1}, \quad |C| \sum_{i=0}^{[(\rho(C)-1)/2]} \binom{n}{2i+1} \geq 2^{n-1}.$$
The volume (the number of points) of a sphere of radius $\rho$ in $\mathbb{F}_2^n$ is $\sum_{i=0}^{\rho} \binom{n}{i}$.

**Proposition**

$$|C| \sum_{i=0}^{\rho(C)} \binom{n}{i} \geq 2^n$$

This gives a lower bound of $\rho(C)$.

For self-dual codes (or more generally, for even codes), slight improvement is possible:

$$|C| \sum_{i=0}^{\left\lfloor \rho(C)/2 \right\rfloor} \binom{n}{2i} \geq 2^{n-1}, \quad |C| \sum_{i=0}^{\left\lfloor (\rho(C)-1)/2 \right\rfloor} \binom{n}{2i+1} \geq 2^{n-1}.$$
The volume (the number of points) of a sphere of radius $\rho$ in $\mathbb{F}_2^n$ is $\sum_{i=0}^{\rho} \binom{n}{i}$.

**Proposition**

$$|C| \sum_{i=0}^{\rho(C)} \binom{n}{i} \geq 2^n$$

This gives a lower bound of $\rho(C)$.

For self-dual codes (or more generally, for even codes), slight improvement is possible:

$$|C| \sum_{i=0}^{\lfloor \rho(C)/2 \rfloor} \binom{n}{2i} \geq 2^{n-1},$$

$$|C| \sum_{i=0}^{\lfloor (\rho(C) - 1)/2 \rfloor} \binom{n}{2i + 1} \geq 2^{n-1}.$$
The volume (the number of points) of a sphere of radius $\rho$ in $\mathbb{F}_2^n$ is $\sum_{i=0}^{\rho} \binom{n}{i}$.

**Proposition**

$$|C| \sum_{i=0}^{\rho(C)} \binom{n}{i} \geq 2^n$$

This gives a lower bound of $\rho(C)$.

For self-dual codes (or more generally, for even codes), slight improvement is possible:

$$|C| \sum_{i=0}^{[\rho(C)/2]} \binom{n}{2i} \geq 2^{n-1}, \quad |C| \sum_{i=0}^{[(\rho(C)-1)/2]} \binom{n}{2i+1} \geq 2^{n-1}.$$
### Table of Extremal Doubly Even Self-Dual Codes

<table>
<thead>
<tr>
<th>length ( n )</th>
<th>( \min(C) )</th>
<th>( \rho(C) \leq 2\left[ \frac{n+8}{12} \right] )</th>
<th>the number of codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>4</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>24</td>
<td>8</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>32</td>
<td>8</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>40</td>
<td>8</td>
<td>6(?) , 7, 8</td>
<td>≥ 12579</td>
</tr>
<tr>
<td>48</td>
<td>12</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>56</td>
<td>12</td>
<td>8–9(?) , 10</td>
<td>≥ 166</td>
</tr>
<tr>
<td>64</td>
<td>12</td>
<td>9(?) , 10, 11, 12(?)</td>
<td>≥ 3270</td>
</tr>
<tr>
<td>72</td>
<td>16</td>
<td>10–12(?)</td>
<td>?</td>
</tr>
</tbody>
</table>

Delsarte bound = \( 2\left[ \frac{n+8}{12} \right] \)
### Table of Extremal Doubly Even Self-Dual Codes

<table>
<thead>
<tr>
<th>length $n$</th>
<th>$\min(C)$</th>
<th>$\rho(C) \leq 2\left[\frac{n+8}{12}\right]$</th>
<th>the number of codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>4</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>24</td>
<td>8</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>32</td>
<td>8</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>40</td>
<td>8</td>
<td>6(?) , 7, 8</td>
<td>$\geq 12579$</td>
</tr>
<tr>
<td>48</td>
<td>12</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>56</td>
<td>12</td>
<td>8–9(?) , 10</td>
<td>$\geq 166$</td>
</tr>
<tr>
<td>64</td>
<td>12</td>
<td>9(?) , 10, 11, 12(?)</td>
<td>$\geq 3270$</td>
</tr>
<tr>
<td>72</td>
<td>16</td>
<td>10–12(?)</td>
<td>?</td>
</tr>
</tbody>
</table>

Delsarte bound $= 2\left[\frac{n+8}{12}\right]$. 

Akihiro Munemasa

Covering Radii
### Table of Extremal Doubly Even Self-Dual Codes

<table>
<thead>
<tr>
<th>length $n$</th>
<th>$\min(C)$ $4\left[\frac{n}{24}\right] + 4$</th>
<th>$\rho(C) \leq 2\left[\frac{n+8}{12}\right]$</th>
<th>the number of codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>4</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>24</td>
<td>8</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>32</td>
<td>8</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>40</td>
<td>8</td>
<td>6(?) 7, 8</td>
<td>$\geq 12579$</td>
</tr>
<tr>
<td>48</td>
<td>12</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>56</td>
<td>12</td>
<td>8–9(?) 10</td>
<td>$\geq 166$</td>
</tr>
<tr>
<td>64</td>
<td>12</td>
<td>9(?) 10, 11, 12(?)</td>
<td>$\geq 3270$</td>
</tr>
<tr>
<td>72</td>
<td>16</td>
<td>10–12(?)</td>
<td>?</td>
</tr>
</tbody>
</table>

Delsarte bound $= 2\left[\frac{n+8}{12}\right]$
If $\sigma$ is a permutation on $\{1, 2, \ldots, n\}$ and $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, then $\sigma(x) := (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$.

**Definition**

A permutation $\sigma$ is an automorphism of a linear code $C \subseteq \mathbb{F}_2^n$ if $\sigma(x) \in C$ for all $x \in C$.

- $\text{Aut}(C)$ denotes the group of all automorphisms of $C$.
- $G := \text{Aut}(C) \subseteq S_n \subseteq GL(n, \mathbb{F}_2)$.
- $\mathbb{F}_2^n$ is an $\mathbb{F}_2G$-module, $C$ is an $\mathbb{F}_2G$-submodule.
- $\mathbb{F}_2^n/C$ is an $\mathbb{F}_2G$-module.
If $\sigma$ is a permutation on $\{1, 2, \ldots, n\}$ and $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, then $\sigma(x) := (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$.

**Definition**

A permutation $\sigma$ is an **automorphism** of a linear code $C \subseteq \mathbb{F}_2^n$ if $\sigma(x) \in C$ for all $x \in C$.

- $\text{Aut}(C)$ denotes the group of all automorphisms of $C$.
- $G := \text{Aut}(C) \subseteq S_n \subseteq GL(n, \mathbb{F}_2)$.
- $\mathbb{F}_2^n$ is an $\mathbb{F}_2G$-module, $C$ is an $\mathbb{F}_2G$-submodule.
- $\mathbb{F}_2^n/C$ is an $\mathbb{F}_2G$-module.
Automorphism Group of Linear Codes

If $\sigma$ is a permutation on $\{1, 2, \ldots, n\}$ and $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, then $\sigma(x) := (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$.

**Definition**

A permutation $\sigma$ is an **automorphism** of a linear code $C \subseteq \mathbb{F}_2^n$ if $\sigma(x) \in C$ for all $x \in C$.

- $\text{Aut}(C)$ denotes the group of all automorphisms of $C$.
- $G := \text{Aut}(C) \subseteq S_n \subseteq GL(n, \mathbb{F}_2)$.
- $\mathbb{F}_2^n$ is an $\mathbb{F}_2 G$-module, $C$ is an $\mathbb{F}_2 G$-submodule.
- $\mathbb{F}_2^n/C$ is an $\mathbb{F}_2 G$-module.
If $\sigma$ is a permutation on $\{1, 2, \ldots, n\}$ and $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, then $\sigma(x) := (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$.

**Definition**

A permutation $\sigma$ is an **automorphism** of a linear code $C \subseteq \mathbb{F}_2^n$ if $\sigma(x) \in C$ for all $x \in C$.

- $\text{Aut}(C)$ denotes the group of all automorphisms of $C$.
- $G := \text{Aut}(C) \subseteq S_n \subseteq GL(n, \mathbb{F}_2)$.
- $\mathbb{F}_2^n$ is an $\mathbb{F}_2G$-module, $C$ is an $\mathbb{F}_2G$-submodule.
- $\mathbb{F}_2^n/C$ is an $\mathbb{F}_2G$-module.
Automorphism Group of Linear Codes

If $\sigma$ is a permutation on $\{1, 2, \ldots, n\}$ and $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, then $\sigma(x) := (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$.

**Definition**

A permutation $\sigma$ is an **automorphism** of a linear code $C \subseteq \mathbb{F}_2^n$ if $\sigma(x) \in C$ for all $x \in C$.

- $\text{Aut}(C)$ denotes the group of all automorphisms of $C$.
- $G := \text{Aut}(C) \subseteq S_n \subseteq \text{GL}(n, \mathbb{F}_2)$.
- $\mathbb{F}_2^n$ is an $\mathbb{F}_2G$-module, $C$ is an $\mathbb{F}_2G$-submodule.
- $\mathbb{F}_2^n/C$ is an $\mathbb{F}_2G$-module.
If \( \sigma \) is a permutation on \( \{1, 2, \ldots, n\} \) and \( x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n \), then \( \sigma(x) := (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}) \).

**Definition**

A permutation \( \sigma \) is an **automorphism** of a linear code \( C \subseteq \mathbb{F}_2^n \) if \( \sigma(x) \in C \) for all \( x \in C \).

- \( \text{Aut}(C) \) denotes the group of all automorphisms of \( C \).
- \( G := \text{Aut}(C) \subseteq S_n \subseteq GL(n, \mathbb{F}_2) \).
- \( \mathbb{F}_2^n \) is an \( \mathbb{F}_2G \)-module, \( C \) is an \( \mathbb{F}_2G \)-submodule.
- \( \mathbb{F}_2^n / C \) is an \( \mathbb{F}_2G \)-module.
Reduction by the Action of the Automorphism Group

\[ \rho(C) = \max_{x \in \mathbb{F}_2^n} \left( \min_{c \in C} d(x, c) \right) \]
\[ = \max_{x + C \in \mathbb{F}_2^n / C} \left( \min_{y \in x + C} \text{wt}(y) \right) = \max_{T \in \mathbb{F}_2^n / C} \left( \min(T) \right). \]

\( G = \text{Aut}(C) \) acts on \( \mathbb{F}_2^n / C \), and \( \min(T) = \min(\sigma(T)) \) for \( T \in \mathbb{F}_2^n / C, \sigma \in G \).

Want to find orbit representatives for \( \mathbb{F}_2^n / C \) under the \( G \)-action.
\( |\mathbb{F}_2^{64} / C| = 2^{32} \): too large.
Definitions and Preliminaries

Results and Methods

Reduction by the Action of the Automorphism Group

\[
\rho(C) = \max_{x \in \mathbb{F}_2^n} \left( \min_{c \in C} d(x, c) \right) \\
= \max_{x + C \in \mathbb{F}_2^n/C} \left( \min_{y \in x + C} \text{wt}(y) \right) = \max_{T \in \mathbb{F}_2^n/C} \left( \min(T) \right).
\]

\(G = \text{Aut}(C)\) acts on \(\mathbb{F}_2^n/C\), and \(\min(T) = \min(\sigma(T))\) for \(T \in \mathbb{F}_2^n/C, \sigma \in G\).

Want to find orbit representatives for \(\mathbb{F}_2^n/C\) under the \(G\)-action.

\(|\mathbb{F}_2^{64}/C| = 2^{32}\): too large.
\( \rho(C) = \max_{x \in \mathbb{F}_2^n} \left( \min_{c \in C} d(x, c) \right) \)

\[ = \max_{x+C \in \mathbb{F}_2^n/C} \left( \min_{y \in x+C} \text{wt}(y) \right) = \max_{T \in \mathbb{F}_2^n/C} (\min(T)) . \]

\( G = \text{Aut}(C) \) acts on \( \mathbb{F}_2^n/C \), and \( \min(T) = \min(\sigma(T)) \) for \( T \in \mathbb{F}_2^n/C, \sigma \in G \).

Want to find orbit representatives for \( \mathbb{F}_2^n/C \) under the \( G \)-action.

\( |\mathbb{F}_2^{64}/C| = 2^{32} \): too large.
\[ \rho(C) = \max_{x \in \mathbb{F}_2^n} \left( \min_{c \in C} (d(x, c)) \right) \]

\[ = \max_{x+C \in \mathbb{F}_2^n/C} \left( \min_{y \in x+C} \text{wt}(y) \right) = \max_{T \in \mathbb{F}_2^n/C} (\min(T)). \]

\[ G = \text{Aut}(C) \text{ acts on } \mathbb{F}_2^n/C, \text{ and } \min(T) = \min(\sigma(T)) \text{ for } T \in \mathbb{F}_2^n/C, \sigma \in G. \]

Want to find orbit representatives for \( \mathbb{F}_2^n/C \) under the \( G \)-action.

\[ |\mathbb{F}_2^{64}/C| = 2^{32} : \text{ too large.} \]
Decomposition into $\mathbb{F}_2 G$-Submodules

1. $\mathbb{F}_2^n / C = M_1 \oplus M_2$ as $\mathbb{F}_2 G$-module.
   - Decompose $M_1$ into $G$-orbits, with $R$ a set of representatives.
   - Compute $\min(r + x)$, $r \in R$, $x \in M_2$, and return the maximum value.

   Improvement of a factor of $\frac{|M_1|}{|R|} \approx |G|$.

2. If $\mathbb{F}_2^n / C$ is indecomposable,
   - Find $M_1 \subseteq \mathbb{F}_2^n / C$.
   - Decompose $(\mathbb{F}_2^n / C) / M_1$ into $G$-orbits.
   - Compute $\min(x)$ for $x \in \bigcup_{r \in R} r$ and return the maximum value.
Decomposition into $\mathbb{F}_2 G$-Submodules

- $\mathbb{F}_2^n / C = M_1 \oplus M_2$ as $\mathbb{F}_2 G$-module.
  - Decompose $M_1$ into $G$-orbits, with $R$ a set of representatives.
  - Compute $\min(r + x)$, $r \in R$, $x \in M_2$, and return the maximum value.

Improvement of a factor of $\frac{|M_1|}{|R|} \approx |G|$.

- If $\mathbb{F}_2^n / C$ is indecomposable,
  - Find $M_1 \subseteq \mathbb{F}_2^n / C$.
  - Decompose $(\mathbb{F}_2^n / C) / M_1$ into $G$-orbits.
  - Compute $\min(x)$ for $x \in \bigcup_{r \in R} r$ and return the maximum value.
Decomposition into $\mathbb{F}_2 G$-Submodules

- $\mathbb{F}_2^n / C = M_1 \oplus M_2$ as $\mathbb{F}_2 G$-module.
  - Decompose $M_1$ into $G$-orbits, with $R$ a set of representatives.
  - Compute $\min(r + x)$, $r \in R$, $x \in M_2$, and return the maximum value.

Improvement of a factor of $\frac{|M_1|}{|R|} \approx |G|$.

- If $\mathbb{F}_2^n / C$ is indecomposable,
  - Find $M_1 \subseteq \mathbb{F}_2^n / C$.
  - Decompose $(\mathbb{F}_2^n / C) / M_1$ into $G$-orbits.
  - Compute $\min(x)$ for $x \in \bigcup_{r \in R} r$ and return the maximum value.
Decomposition into $\mathbb{F}_2 G$-Submodules

- $\mathbb{F}_2^n / C = M_1 \oplus M_2$ as $\mathbb{F}_2 G$-module.
  - Decompose $M_1$ into $G$-orbits, with $R$ a set of representatives.
  - Compute $\min(r + x)$, $r \in R$, $x \in M_2$, and return the maximum value.

**Improvement of a factor of** $\frac{|M_1|}{|R|} \approx |G|$.

- If $\mathbb{F}_2^n / C$ is indecomposable,
  - Find $M_1 \subseteq \mathbb{F}_2^n / C$.
  - Decompose $(\mathbb{F}_2^n / C) / M_1$ into $G$-orbits.
  - Compute $\min(x)$ for $x \in \bigcup_{r \in R} r$ and return the maximum value.
Decomposition into $\mathbb{F}_2 G$-Submodules

- $\mathbb{F}_2^n / C = M_1 \oplus M_2$ as $\mathbb{F}_2 G$-module.
  - Decompose $M_1$ into $G$-orbits, with $R$ a set of representatives.
  - Compute $\min(r + x)$, $r \in R$, $x \in M_2$, and return the maximum value.
  
  Improvement of a factor of $\frac{|M_1|}{|R|} \approx |G|$.

- If $\mathbb{F}_2^n / C$ is indecomposable,
  - Find $M_1 \subseteq \mathbb{F}_2^n / C$.
  - Decompose $(\mathbb{F}_2^n / C) / M_1$ into $G$-orbits.
  - Compute $\min(x)$ for $x \in \bigcup_{r \in R} r$ and return the maximum value.
Decomposition into $\mathbb{F}_2 G$-Submodules

- $\mathbb{F}_2^n/C = M_1 \oplus M_2$ as $\mathbb{F}_2 G$-module.
  - Decompose $M_1$ into $G$-orbits, with $R$ a set of representatives.
  - Compute $\min(r + x), r \in R, x \in M_2$, and return the maximum value.

Improvement of a factor of $\frac{|M_1|}{|R|} \approx |G|$.  

- If $\mathbb{F}_2^n/C$ is indecomposable,  
  - Find $M_1 \subseteq \mathbb{F}_2^n/C$.
  - Decompose $(\mathbb{F}_2^n/C)/M_1$ into $G$-orbits.
  - Compute $\min(x)$ for $x \in \bigcup_{r \in R} r$ and return the maximum value.
Decomposition into $\mathbb{F}_2 G$-Submodules

- $\mathbb{F}_2^n / C = M_1 \oplus M_2$ as $\mathbb{F}_2 G$-module.
  - Decompose $M_1$ into $G$-orbits, with $R$ a set of representatives.
  - Compute $\min(r + x)$, $r \in R$, $x \in M_2$, and return the maximum value.

Improvement of a factor of $\frac{|M_1|}{|R|} \approx |G|$. 

- If $\mathbb{F}_2^n / C$ is indecomposable,
  - Find $M_1 \subseteq \mathbb{F}_2^n / C$.
  - Decompose $(\mathbb{F}_2^n / C) / M_1$ into $G$-orbits.
  - Compute $\min(x)$ for $x \in \bigcup_{r \in R} r$ and return the maximum value.
Decomposition into $\mathbb{F}_2 G$-Submodules

- $\mathbb{F}_2^n/C = M_1 \oplus M_2$ as $\mathbb{F}_2 G$-module.
  - Decompose $M_1$ into $G$-orbits, with $R$ a set of representatives.
  - Compute $\min(r + x), \ r \in R, \ x \in M_2$, and return the maximum value.

  Improvement of a factor of $\frac{|M_1|}{|R|} \approx |G|$.

- If $\mathbb{F}_2^n/C$ is indecomposable,
  - Find $M_1 \subseteq \mathbb{F}_2^n/C$.
  - Decompose $(\mathbb{F}_2^n/C)/M_1$ into $G$-orbits.
  - Compute $\min(x)$ for $x \in \bigcup_{r \in R} r$ and return the maximum value.
Summary

- Length $n = 56$: computed the covering radius of 9 double-circulant ($\text{Aut}(C) \cong D_{27}$) extremal doubly even self-dual codes, → all 10, meeting the Delsarte bound.

- Length $n = 64$: computed the covering radius of 67 extremal doubly even self-dual codes ($|\text{Aut}(C)| \geq 62$), → all 10 or 11, not meeting the Delsarte bound = 12.

<table>
<thead>
<tr>
<th>length $n$</th>
<th>$\min(C)$</th>
<th>$\rho(C) \leq 2\left[\frac{n+8}{12}\right]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>56</td>
<td>12</td>
<td>8–9(?) , 10</td>
</tr>
<tr>
<td>64</td>
<td>12</td>
<td>9(?) , 10, 11, 12(?)</td>
</tr>
</tbody>
</table>