A binary extremal doubly even self-dual code of length 72 –Length 72 problem–

Masaaki Harada

Yamagata University/JST–PRESTO

RIMS Camp-style Seminar “On analysis of combinatorial structures and its applications for information theory”
In 1973, N.J.A. Sloane proposed the following problem

Is there an extremal Type II code
(doubly even self-dual code) of length 72?

(N.J.A. Sloane, Is there a \((72,36)\) \(d = 16\) self-dual code? \(IEEE\ Trans.\ Information\ Theory\ 19\) (1973), p. 251.)

This is a long-standing problem!

In this talk, I describe how this problem was produced. Also I present what is known on this problem currently.
Contents

- What are Type II codes?
- How are extremal Type II codes defined?
- Known extremal Type II codes
- Length 72 problem
- Another length 72 problem (lattices)
1. What are Type II codes?

- $\mathbb{F}_q$: finite field of order $q$ ($q$: prime power)
- $C$: $[n,k]$ code over $\mathbb{F}_q \leftrightarrow k$-dimensional subspace of $\mathbb{F}_q^n$
  
  $n$: length of $C$, $k$: dimension of $C$
- weight of $x = (x_1, \ldots, x_n) \in C$: $\text{wt}(x) = \# \{ i \mid x_i \neq 0 \}$
- minimum weight $d(C)$ of $C$: $\min \{ \text{wt}(x) \mid 0 \neq x \in C \}$
- $[n,k,d]$ code $\leftrightarrow [n,k]$ code with minimum weight $d$
- dual code $C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot y = 0 \ (\forall y \in C)\}$
  
  \begin{equation}
  (x \cdot y \text{ is the standard inner product})
  \end{equation}

- $C$: **self-dual** $\iff C = C^\perp$

- $C$: binary code $\iff C$: code over $\mathbb{F}_2$

- $C$: binary code
  - $C$: **doubly even** $\iff \text{wt}(x) \equiv 0 \pmod{4} \ (\forall x \in C)$

  \begin{equation}
  C: \textbf{Type II} \iff C: \text{doubly even and self-dual}
  \end{equation}

Main target of this talk: **Type II codes** (What is motivation?)
• weight enumerator of $C$: $W_C(x, y) = \sum_{c \in C} x^{n - \text{wt}(c)} y^{\text{wt}(c)}$

• $C$: formally self-dual $\iff W_C(x, y) = W_{C^\perp}(x, y)$

---

**Theorem (Gleason–Pierce (1969))**

$C$: formally self-dual code over $\mathbb{F}_q$.
All weights are divisible by an integer $\alpha \geq 2$
Then one of the following holds:
(1) $q = 2$, $\alpha = 2$
(2) $q = 2$, $\alpha = 4$ and $C$ is self-dual $\iff$ Type II code
(3) $q = 3$, $\alpha = 3$ and $C$ is self-dual
(4) $q = 4$, $\alpha = 2$
(5) (trivial case) $q$: any, $\alpha = 2$ and $W_C(x, y) = (x^2 + (q-1)y^2)^{n/2}$
Example  (two examples of Type II codes)

- **extended Hamming [8, 4, 4] code** $e_8$
  extended cyclic code with generator polynomial $x^3 + x^2 + 1$

- **extended Golay [24, 12, 8] code** $G_{24}$
  extended cyclic code with generator polynomial
  
  $$x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$$

($e_8, G_{24}$: extended quadratic residue codes of lengths 8, 24)

- **weight enumerators**
  
  $W_{e_8}(x, y) = x^8 + 14x^4y^4 + y^8$
  
  $W_{G_{24}}(x, y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^{8}y^{16} + y^{24}$

2. Definition of extremal Type II codes

N.J.A. Sloane, Error-correcting codes and invariant theory: 
new applications of a nineteenth-century technique, 

Lemma. (1) $C$: formally self-dual code
\[ W_C(x, y) = W_C\left(\frac{x + y}{\sqrt{2}}, \frac{x - y}{\sqrt{2}}\right) \]

(2) $C$: doubly even code
\[ W_C(x, y) = W_C(x, iy) \text{ where } i = \sqrt{-1}. \]
Proof. $n$: length of $C$

(1) By the MacWilliams identity:

\[ W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + y, x - y), \]

\[ W_C(x, y) = W_{C^\perp}(x, y) = \frac{1}{2^{n/2}} W_C(x + y, x - y) = W_C\left(\frac{x + y}{\sqrt{2}}, \frac{x - y}{\sqrt{2}}\right) \]

(2) $\text{wt}(c) \equiv 0 \pmod{4}$ ($\forall c \in C$) \Rightarrow $(iy)^{\text{wt}(c)} = i^{\text{wt}(c)}y^{\text{wt}(c)}$

\[ \Rightarrow \]

\[ W_C(x, iy) = \sum_{c \in C} x^{n-\text{wt}(c)}(iy)^{\text{wt}(c)} = \sum_{c \in C} x^{n-\text{wt}(c)}y^{\text{wt}(c)} = W_C(x, y). \]
For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, \mathbb{C})$ and $f(x, y) \in \mathbb{C}[x, y]$, 

$$A \circ f(x, y) = f(ax + by, cx + dy)$$

$C$: Type II code (by the lemma)

$$\Rightarrow W_C\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) = W_C(x, y), W_C(x, iy) = W_C(x, y)$$

$$\Rightarrow \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \circ W_C(x, y) = W_C(x, y), \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \circ W_C(x, y) = W_C(x, y)$$
• Define the group: \( G = \langle \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \rangle \) (\( \subset GL(2, \mathbb{C}) \)).

\[ A \circ W_G(x, y) = W_G(x, y) \ (\forall A \in G) \]
\( (G \text{ is a unitary reflection group of order } 192) \)

• \( \mathbb{C}[x, y]^G = \{ f(x, y) \in \mathbb{C}[x, y] \mid A \circ f(x, y) = f(x, y) \ (\forall A \in G) \} \)

\[ W_G(x, y) \in \mathbb{C}[x, y]^G \]

• \( a_i \): \# linearly independent polynomials \( \in \mathbb{C}[x, y]^G \) of degree \( i \)

Molien series:
\[ \Phi(\lambda) = \sum_i a_i \lambda^i = (1 + \lambda^8 + \lambda^{16} + \lambda^{24} + \cdots)(1 + \lambda^{24} + \lambda^{48} + \cdots) \]
\[ = 1 + \lambda^8 + \lambda^{16} + 2\lambda^{24} + 2\lambda^{32} + 2\lambda^{40} + 3\lambda^{48} + \cdots \]
**Theorem (Gleason (1970))**

Let $C$ be a Type II code. Then

$$W_C(x, y) \in \mathbb{C}[x, y]^G = \mathbb{C}[\phi_8, \phi_{24}]$$

where $\phi_8 = W_{\epsilon_8}(x, y)$, $\phi_{24} = W_{G_{24}}(x, y)$.

**Corollary**

\[ \exists \text{ Type II code of length } n \implies n \equiv 0 \pmod{8}. \]
**Theorem (Mallows–Sloane (1973))**

Let $C$ be a Type II code of length $n$. Then

$$d(C) \leq 4\left(\left\lceil \frac{n}{24} \right\rceil + 1\right).$$

**Proof.** ($n = 72$)

Suppose that $d(C) \geq 16$. By the Gleason theorem,

$$W_C(x, y) = a_0 \phi_8^9 + a_1 \phi_8^6 \phi_{24} + a_2 \phi_8^3 \phi_{24}^2 + a_3 \phi_{24}^3 \quad (a_0, \ldots, a_3 \in \mathbb{C})$$

$$= (a_0 + a_1 + a_2 + a_3)x^{72} + (126a_0 + 84a_1 + 42a_2)x^{68}y^4$$

$$+ (7065a_0 + 3705a_1 + 2109a_2 + 2277a_3)x^{64}y^8$$

$$+ (231504a_0 + 121632a_1 + 71736a_2 + 7728a_3)x^{60}y^{12}$$

$$+ (4889844a_0 + 3041172a_1 + 1691712a_2 + 1730520a_3)x^{56}y^{16} + \cdots.$$
\[ A_i = \#\{x \in C \mid \text{wt}(x) = i\} \]
\[ A_0 = 1 \Rightarrow a_0 + a_1 + a_2 + a_3 = 1. \]
\[ A_4 = A_8 = A_{12} = 0 \Rightarrow \]
\[ 126a_0 + 84a_1 + 42a_2 = 0 \]
\[ 7065a_0 + 3705a_1 + 2109a_2 + 2277a_3 = 0 \]
\[ 231504a_0 + 121632a_1 + 71736a_2 + 7728a_3 = 0 \]

\[ \Rightarrow a_0 = -\frac{1081}{3087}, \quad a_1 = -\frac{989}{4116}, \quad a_2 = \frac{3151}{2058}, \quad a_3 = \frac{733}{12348} \]

Then we have
\[ W_C(1, y) = 1 + 249849y^{16} + 18106704y^{20} + 462962955y^{24} \]
\[ + 4397342400y^{28} + 16602715899y^{32} \]
\[ + 25756721120y^{36} + \cdots + y^{72}. \]
\[ A_{16} \neq 0 \Rightarrow d(C) \leq 16. \]
Definition. \( C \): extremal \iff d(C) = 4\left\lfloor \frac{n}{24} \right\rfloor + 4.

Fundamental Problem (existence)
Determine whether an extremal Type II code exists for \( n \equiv 0 \pmod{8} \).

(classification)
Determine the number \( N_n \) of inequivalent extremal Type II codes for \( n \equiv 0 \pmod{8} \).

- \( C, C' \): equivalent \( (C \cong C') \) \iff 
  \exists \text{ a permutation matrix } P \text{ with } C' = C \cdot P = \{xP \mid x \in C\}. 
3. Known extremal Type II codes

<table>
<thead>
<tr>
<th>Length $n$</th>
<th>$d(C)$</th>
<th>$N_n$</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>4</td>
<td>1</td>
<td>Pless (1972)</td>
</tr>
<tr>
<td>16</td>
<td>4</td>
<td>2</td>
<td>Pless (1972)</td>
</tr>
<tr>
<td>24</td>
<td>8</td>
<td>1</td>
<td>Pless (1969)</td>
</tr>
<tr>
<td>32</td>
<td>8</td>
<td>5</td>
<td>Conway–Pless–Sloane (1992)</td>
</tr>
<tr>
<td>40</td>
<td>8</td>
<td>$\geq 12579$</td>
<td>King (2001)</td>
</tr>
<tr>
<td>48</td>
<td>12</td>
<td>1</td>
<td>[HLTP]</td>
</tr>
<tr>
<td>56</td>
<td>12</td>
<td>$\geq 1151$</td>
<td>H (2005)</td>
</tr>
<tr>
<td>64</td>
<td>12</td>
<td>$\geq 3270$</td>
<td>H–Kimura (1995)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Length</th>
<th>$n$</th>
<th>$d(C)$</th>
<th>$N_n$</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>88</td>
<td>16</td>
<td>≥ 470</td>
<td></td>
<td></td>
</tr>
<tr>
<td>96</td>
<td>20</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>104</td>
<td>20</td>
<td>≥ 1</td>
<td></td>
<td>MacWilliams–Sloane (1977)</td>
</tr>
<tr>
<td>112</td>
<td>20</td>
<td>≥ 1</td>
<td></td>
<td>H (2008)</td>
</tr>
<tr>
<td>120</td>
<td>24</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>128</td>
<td>24</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>136</td>
<td>24</td>
<td>≥ 1</td>
<td></td>
<td>Moore (1976)</td>
</tr>
<tr>
<td>144</td>
<td>28</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3688</td>
<td>616</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3696</td>
<td>620</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. Length 72 Problem

**Problem (Sloane (1973))**
Is there an extremal Type II code of length 72?

Some known results on the existence $\cdots$

The Gleason theorem determines:

\[
\begin{align*}
x^{72} &+ 249849x^{56}y^{16} + 18106704x^{52}y^{20} + 462962955x^{48}y^{24} \\
&+ 4397342400x^{44}y^{28} + 16602715899x^{40}y^{32} \\
&+ 25756721120x^{36}y^{36} + \cdots + y^{72}. 
\end{align*}
\]
Proposition (Dougherty–Harada (1999))

\exists \text{ an extremal Type II code of length 72 }

\iff \exists \text{ a self-dual } [70, 35, 14] \text{ code }

Proof. \( \Rightarrow \) \( C' \): extremal Type II code of length 72

\[ C' = \{ (x_3, \ldots, x_{72}) \mid (x_1, \ldots, x_{72}) \in C, x_1 + x_2 = 0 \} \]

\( \Rightarrow \) \( C' \): self-dual [70, 35, 14] code

\begin{itemize}
  \item \( C \): a self-dual code which is not Type II
    \[ C_0 = \{ x \in C \mid \text{wt}(x) \equiv 0 \pmod{4} \} \Rightarrow |C : C_0| = 2 \]
  \item shadow \( S \) of \( C \) \iff \( C_0^\perp \setminus C \)
    \begin{itemize}
      \item basic properties of shadow (Conway–Sloane (1990))
    \end{itemize}
\end{itemize}
(⇐) \( C \): self-dual \([70,35,14]\) code with shadow \( S \)

Put \( C_0^\perp = C_0 \cup C_2 \cup C_1 \cup C_3 \) \((C = C_0 \cup C_2, \ S = C_1 \cup C_3)\)

\[
C^* = (0,0,C_0) \cup (1,1,C_2) \cup (1,0,C_1) \cup (0,1,C_3) \quad (\subset \mathbb{F}_2^{72})
\]

\(((x,y,C_i) = \{(x,y,c) \mid c \in C_i\}\))

\(\Rightarrow C^*\): self-dual code of length 72

\[
\text{wt}(x) \equiv 3 \pmod{4} \quad (\forall x \in S) \quad \text{(Conway–Sloane (1990))}
\]

\(\Rightarrow C^*\): Type II code of length 72

\[
d(S) = 15 \Rightarrow C^*\): extremal Type II code of length 72
\]

Remark. \(\exists\) formally self-dual \([70,35,14]\) code (Gulliver–H (1998))
Related combinatorial structure

\[ D = (X, \mathcal{B}): \ t-(v, k, \lambda) \ design \ \iff \]
\[ X = \{1, 2, \ldots, v\} \text{ (points)} \]
\[ \mathcal{B}: \text{ collection of } k\text{-subsets of } X \text{ (blocks)} \]
\[ \text{such that every } t\text{-subset of } X \text{ is contained in exactly } \lambda \text{ blocks.} \]

**Assmus–Mattson (1969):**

\( C: \text{ extremal Type II code of length 72} \)
\[ \supp(x) = \{i \mid x_i \neq 0\} \ (\subset X = \{1, 2, \ldots, 72\}) \]
\[ \mathcal{B} = \{\supp(x) \mid x \in C, \text{wt}(x) = 16\} \]
\[ \Rightarrow D = (X, \mathcal{B}): \ 5-(72, 16, 78) \text{ design } (\#\mathcal{B} = 249849 = A_{16}) \]

block intersection number of \( D \): \( \#(B_i \cap B_j) \) \( (B_i \neq B_j \in \mathcal{B}) \)
\( C: \text{ self-dual } \& \ d(C) = 16 \Rightarrow \text{block intersection numbers } 0, 2, 4, 6, 8. \)
Theorem (Harada–Kitazume–Munemasa (2004))

∃ an extremal Type II code of length 72 \iff
∃ a 5-(72, 16, 78) design with even block intersection numbers

Proof. (⇒) From the Assmus–Mattson theorem

(⇐) \( D = (X, B) \): 5-(72, 16, 78) design
with even block intersection numbers
\[
X = \{1, 2, \ldots, 72\}, \quad B = \{B_1, B_2, \ldots, B_b\}, \quad b = 249849
\]
\[
A = (a_{ij}) : b \times 72 \text{ incidence matrix of } D
\]
\[
(a_{ij} = 1 \text{ if } j \in B_i \text{ and } a_{ij} = 0 \text{ otherwise})
\]

\( C \): the binary code generated by rows of \( A \)

\( =_{\text{(nontrivial)}} \Rightarrow \quad C: \text{ extremal Type II code of length } 72 \) \( \square \)
Results on the automorphism group

\[ \sigma \in S_n \text{ (symmetric group of degree } n) \]
\[ \sigma(x) = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) \text{ for } x = (x_1, \ldots, x_n) \in C \]

**automorphism group** \( \text{Aut}(C) \) of \( C \): \{\( \sigma \in S_n \mid \sigma(x) \in C \ (\forall x \in C) \} \)
\( \sigma \): **automorphism** of \( C \) \( \iff \sigma \in \text{Aut}(C) \)

\( C_{72} \): extremal Type II code of length 72

Results on automorphisms of \( C_{72} \) and \( \text{Aut}(C_{72}) \) \( \cdots \)
• automorphism $\sigma$ of $C_{72}$

$\sigma \in \text{Aut}(C_{72})$ has prime order $p \Rightarrow p = 2, 3, 5, 7$

\[
\begin{align*}
\text{(Conway–Pless (1982), Pless (1982),} \\
\text{Pless–Thompson (1982), Huffman–Yorgov (1987)})
\end{align*}
\]

$p = 5, 7 \Rightarrow \sigma$ has two fixed points

\[
\text{(Dontcheva–Zanten–Dodunekov (2004))}
\]

$p = 2, 3 \Rightarrow \sigma$ is fixed-point-free

\[
\text{(Bouyuklieva (2002), (2004))}
\]

• $\text{Aut}(C_{72})$: solvable group of order $56, 14, 10, 7, 5$ or a divisor of $72$

\[
\text{(Bouyuklieva–O’Brien–Willems (2006))}
\]
5. Another length 72 problem (lattices)

- $\mathbb{R}^n$: Euclidean space equipped with standard inner product $(x, y)$
- $L (\subset \mathbb{R}^n)$: $n$-dimensional (Euclidean) lattice $\iff$
  $\exists$ basis $v_1, \ldots, v_n$ of $\mathbb{R}^n$ such that $L = \{k_1v_1 + \cdots + k_nv_n | k_i \in \mathbb{Z}\}$
- dual lattice $L^* = \{x \in \mathbb{R}^n | (x, y) \in \mathbb{Z} (\forall y \in L)\}$
- $L$: unimodular $\iff L = L^*$.
- $L$: unimodular lattice
  $L$: even $\iff$ norm $(x, x) \in 2\mathbb{Z} (\forall x \in L)$
- **$L$: Type II $\iff L$:** even unimodular

- **minimum norm** $\min(L)$ of $L \iff \min\{(x, x) \mid 0 \neq x \in L\}$

- **theta series of $L$:** $\theta_L(q) = \sum_{x \in L} q^{(x,x)}$

- (Hecke) **$L$:** Type II lattice $\Rightarrow \theta_L(q) \in \mathbb{C}[E_4(q), \Delta_{24}(q)]$
  
  \[ E_4(q) = 1 + 240 \sum_{m=1}^{\infty} \sigma_3(m)q^{2m} \quad (\sigma_3(m) = \sum_{0<d|m} d^3) \]
  
  \[ \Delta_{24}(q) = q^2 \prod_{m=1}^{\infty} (1 - q^{2m})^{24} \]

- **$L$:** Type II lattice $\Rightarrow n \equiv 0 \pmod{8}$
  
  $\Rightarrow \min(L) \leq 2\lfloor n/24 \rfloor + 2$

- **$L$:** **extremal** $\iff \min(L) = 2\lfloor n/24 \rfloor + 2$
Parallelism between codes and lattices

<table>
<thead>
<tr>
<th>codes</th>
<th>lattices</th>
</tr>
</thead>
<tbody>
<tr>
<td>(minimum) weight</td>
<td>(minimum) norm</td>
</tr>
<tr>
<td>weight enumerator</td>
<td>theta series</td>
</tr>
<tr>
<td>self-dual</td>
<td>unimodular</td>
</tr>
<tr>
<td>doubly even</td>
<td>even</td>
</tr>
<tr>
<td>Type II</td>
<td>Type II</td>
</tr>
<tr>
<td>Gleason theorem</td>
<td>Hecke theorem</td>
</tr>
<tr>
<td>$n \equiv 0 \pmod{8}$</td>
<td>$n \equiv 0 \pmod{8}$</td>
</tr>
<tr>
<td>$d(C) \leq 4[n/24] + 4$</td>
<td>$\min(L) \leq 2[n/24] + 2$</td>
</tr>
<tr>
<td>extremal</td>
<td>extremal</td>
</tr>
</tbody>
</table>
∃ extremal Type II code or lattice:

<table>
<thead>
<tr>
<th>$n$</th>
<th>8</th>
<th>16</th>
<th>24</th>
<th>32</th>
<th>40</th>
<th>48</th>
<th>56</th>
<th>64</th>
<th>72</th>
<th>80</th>
<th>88</th>
</tr>
</thead>
<tbody>
<tr>
<td>codes</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>lattices</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>?</td>
<td>0</td>
<td>?</td>
</tr>
</tbody>
</table>

“another length 72 problem”

**Problem**
Is there a 72-dimensional extremal Type II lattice?
Conclusion

- What are extremal Type II codes?
- Known results on the existence of extremal Type II codes
- Length 72 problem:
  - Is there an extremal Type II code of length 72?
- Another length 72 problem:
  - Is there a 72-dimensional extremal Type II lattice?

Thank you for your attention!