Classification of ternary extremal self-dual codes of length 28

Akihiro Munemasa
(joint work with Masaaki Harada and Boris Venkov)

December 5, 2007
Self-dual codes

$p$: prime, $\mathbb{F}_p$: finite field

A linear code $C \subset \mathbb{F}_p^n$ is self-orthogonal if $C \subset C^\perp$
\[\iff \forall x, y \in C, \quad (x, y) = 0\]

$C$: self-dual
\[\iff C = C^\perp\]
\[\iff \text{self-orthogonal} \& \dim C = \frac{n}{2}\]
Lattices from codes

\[ \pi : \mathbb{Z}^n \rightarrow \mathbb{F}_p^n \]
\[ \pi^{-1}(C) \rightarrow C \]

\[ C \subset C^\perp \]
\[ \iff \forall x, y \in C, \quad (x, y) = 0 \]
\[ \iff \forall u, v \in \pi^{-1}(C), \quad (u, v) \equiv 0 \pmod{p} \]
\[ \iff \frac{1}{\sqrt{p}} \pi^{-1}(C) \text{ integral lattice (Construction A)} \]

\[ C = C^\perp \]
\[ \iff \frac{1}{\sqrt{p}} \pi^{-1}(C) \text{ and } \det \left( \frac{1}{\sqrt{p}} \pi^{-1}(C) \right) = 1 \text{ (unimodular)} \]
Minimum weight

$C \subset \mathbb{F}_3^n$: ternary self-dual code

$\min C = \min \{ \text{wt}(x) \mid x \in C, \ x \neq 0 \}$

$\text{wt}(x) = \#(\text{nonzero coordinates})$

**Theorem** (Mallows–Sloane, 1973). $\min C \leq 3 \left\lceil \frac{n}{12} \right\rceil + 3.$

Call $C$ **extremal** if $\ = \$ holds.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\min C$</th>
<th>$# \text{extremal}$</th>
<th>classified by</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>6</td>
<td>1</td>
<td>Mallows–Pless–Sloane (1976)</td>
</tr>
<tr>
<td>16</td>
<td>6</td>
<td>1</td>
<td>Conway–Pless–Sloane (1979)</td>
</tr>
<tr>
<td>24</td>
<td>9</td>
<td>2</td>
<td>Leon–Pless-Sloane (1981)</td>
</tr>
</tbody>
</table>
Minimum norm

\[ C \subset \mathbb{F}_3^{28} \text{: extremal (min } C = 9\text{) self-dual code} \]
\[ \implies \#\{x \in C \mid \text{wt}(x) = 9\} = 2184 \]
\[ L = \frac{1}{\sqrt{3}} \pi^{-1}(C) \text{: unimodular} \]
\[ \{u \in L \mid ||u||^2 = 1 \text{ or 2}\} = \frac{1}{\sqrt{3}} \{v \in \mathbb{Z}_{28}^{28} \mid ||v||^2 = 3 \text{ or 6, } v \mod 3 \in C\} = \emptyset \]
\[ \{u \in L \mid ||u||^2 = 3\} \text{ corresponds to frames} \]
\[ \{x \in C \mid \text{wt}(x) = 9\} \]
\[ \downarrow \]
\[ 2184 \]
\[ + \]
\[ \{ \pm \frac{1}{\sqrt{3}} 3e_i \mid i = 1, \ldots, 28\} \]
\[ \downarrow \]
\[ 56 = 2240 \]
R. Bacher and B. Venkov (2001) classified unimodular lattices in dimension 28 with theta series

\[ 1 + 0 \cdot q + 0 \cdot q^2 + 2240q^3 + \cdots \]

There are 36 such lattices up to isometry.

2240 norm 3 vectors in \( L = \frac{1}{\sqrt{3}}\pi^{-1}(C) \)

2184 weight 9 vectors in \( C \)

\[ 2 \times 28 \] frame vectors
Code from lattice

$L$: **unimodular** lattice, $\dim L = n$

$L \ni f_1, \ldots, f_n$: 3-frame, i.e., $(f_i, f_j) = 3\delta_{ij}$

$\implies$

$C = \{ u \mod 3 \mid u \in \mathbb{Z}^n, \frac{1}{3} \sum_{i=1}^{n} u_i f_i \in L \}$

is a **self-dual** code with $\frac{1}{\sqrt{3}} \pi^{-1}(C) = L.$

Often there are a lot of cliques (3-frames)
Equivalence

Lemma. $C_1, C_2 \subset \mathbb{F}_3^n$, $L \cong \frac{1}{\sqrt{3}} \pi^{-1}(C_1) \cong \frac{1}{\sqrt{3}} \pi^{-1}(C_2)$. Then $C_1 \cong C_2$ iff frames from $C_1$ and $C_2$ are Aut($L$)-conjugate.

Improved program

```plaintext
> AutL:=AutomorphismGroup(L);
> L3:=@ {x,-x} : x in L3 @};
> G:=actionImage(AutL,L3);
> ac:=allCliquesUpToG(Gamma,G,8);
> #ac;
1
```
Lemma. \( L \): unimodular lattice in dimension 28 with minimum norm 3.

\( u_1, u_2 \in L, \|u_1\|^2 = \|u_2\|^2 = 3, (u_1, u_2) = 0. \)

\( S \): the set of vectors of norm 3 in \( L_0^* \setminus L \), where \( L_0^* \) is the dual of the even sublattice of \( L \).

\( \exists \) 3-frame containing \( u_1 \) and \( u_2 \)

\[ \implies \exists u \in S \text{ s.t. } |(u, u_1)| = |(u, u_2)| = 3/2. \]

Modification of program: add a restriction to remove unnecessary edges
### Result

<table>
<thead>
<tr>
<th>Lattice</th>
<th>#Frames</th>
<th># Aut(L)</th>
<th>#codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4144</td>
<td>8</td>
<td>1036</td>
</tr>
<tr>
<td>2</td>
<td>4804</td>
<td>16</td>
<td>735</td>
</tr>
<tr>
<td>3</td>
<td>4218</td>
<td>16</td>
<td>589</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>28</td>
<td>0</td>
<td>7680</td>
<td>0</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>36</td>
<td>12908160</td>
<td>18341406720</td>
<td>3</td>
</tr>
<tr>
<td>total</td>
<td></td>
<td></td>
<td>6931</td>
</tr>
</tbody>
</table>

\( i = 1 \): all the 4144 frames can be enumerated.
\( i = 36 \): all the 12908160 frames could not be enumerated. But Aut(\(L\)) acts transitively on the set of three mutually orthogonal vectors of norm 3.
Remark

One of the lattices (the 36th) in the classification of Bacher–Venkov is obtained from $\text{Sp}_6(\mathbb{F}_3)$.

3-frames
$\leftrightarrow$ symplectic spreads
$\leftrightarrow$ translation planes of order 27
(classified by Dempwolff (1994))