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 $C \subset C^\perp$
$\iff \quad \forall x, y \in C, \quad (x, y) = 0$

C: self-dual
$\iff \; C = C^\perp$
$\iff$ self-orthogonal & $\dim C = \frac{n}{2}$

Lattices from codes

$$\pi: \quad \mathbb{Z}^n \to \mathbb{F}_p^n$$
$$\pi^{-1}(C) \to C$$

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

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

Minimum weight

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

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

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

Call C extremal if $=$ holds.

n	$\min C$	# extremal	classified by
4	3	1	
8	3	1	
12	6	1	Mallows–Pless–Sloane (1976)
16	6	1	Conway–Pless–Sloane (1979)
20	6	6	Pless–Sloane–Ward (1980)
24	9	2	Leon–Pless-Sloane (1981)
28	9	$\boxed{?}$	Harada–M.–Venkov (2007)

Minimum norm

$C \subset \mathbb{F}_3^{28}$: extremal ($\min C = 9$) self-dual code

$\implies \#\{x \in C \mid \mathrm{wt}(x) = 9\} = 2184$

$L = \frac{1}{\sqrt{3}}\pi^{-1}(C)$: unimodular

$\{u \in L \mid \|u\|^2 = 1 \text{ or } 2\}$

$= \frac{1}{\sqrt{3}}\{v \in \mathbb{Z}^{28} \mid \|v\|^2 = 3 \text{ or } 6,\ v \bmod 3 \in C\} = \emptyset$

$\{u \in L \mid \|u\|^2 = 3\}$ corresponds to

$$\begin{array}{ccc} & & \text{frames} \\ \{x \in C \mid \mathrm{wt}(x) = 9\} & & \{\pm\frac{1}{\sqrt{3}}3e_i \mid i = 1, \dots, 28\} \\ \downarrow & & \downarrow \\ 2184 & + & 56 = 2240 \end{array}$$

Bacher–Venkov

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 $\quad$ 2×28 frame vectors

Code from lattice

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

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

$\Longrightarrow$

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

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

```
> C:=LinearCode<GF(3), 8 |
> [1,0,0,0,1,1,0,0],[0,1,0,0,1,2,0,0],
> [0,0,1,0,0,0,1,1],[0,0,0,1,0,0,1,2] >;
> L:=ScaledLattice(Lattice(C,"A"),1/3);
> L3:={@ x[1] : x in ShortVectors(L,3,3) @};
> orth:=func< i,j | (L3[i],L3[j]) eq 0 >;
> edges:={ {i,j} : i in {1..#L3}, j in {1..#L3} | orth(i,j) };
> Gamma:=Graph< #L3 | edges >;
> ac:=AllCliques(Gamma,8);
> #ac;
2240
```

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

```
> AutL:=AutomorphismGroup(L);
> L3:={@ {x,-x} : x in L3 @};
> G:=actionImage(AutL,L3);
> ac:=allCliquesUpToG(Gamma,G,8);
> #ac;
1
```

Sufficient condition

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

$$\Longrightarrow \nexists u \in S \text{ s.t. } |(u, u_1)| = |(u, u_2)| = 3/2.$$

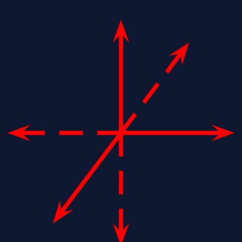
Modification of program: add a restriction to remove unnecessary edges

```
orth:=func< i,j | (L3[i],L3[j]) eq 0 >;
edges:={ {i,j} : i in {1..#L3}, j in {1..#L3} | orth(i,j) };
Gamma:=Graph< #L3 | edges >;
```

Result

Lattice	#Frames	# Aut(L)	#codes
1	4144	8	1036
2	4804	16	735
3	4218	16	589
⋮	⋮	⋮	⋮
28	0	7680	0
⋮	⋮	⋮	⋮
36	12908160	18341406720	3
total			6931

$i = 1$: 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 $Sp_6(\mathbb{F}_3)$.

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