Classification of the Extremal Self-Dual Codes with 2-Transitive Aut Groups

Anton Malevich

3ICMCTA, Cardona, Spain
11 – 15 September 2011

joint work with W. Willems

Self-Dual Doubly-Even Codes

- Linear code is a subspace of $\mathbb{F}^n$
- The dual code

$$C^\perp = \{v \mid v \cdot u = 0 \text{ for all } u \in C\}$$

- If $C = C^\perp$ the code is self-dual
- For a self-dual code dim $= n/2$ and all codewords have even weight
- Self-dual code is Type II (doubly-even) if all weights are a multiple of 4

Extremal Doubly-Even Codes

- Length of a Type II code is a multiple of 8
- For a Type II code: $d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4$,

  If "=" then the code is extremal
- For extremal codes $n \leq 3952$
- The largest length for the known extremal code is $n = 136$

Automorphism Group

Definition

$$\mathrm{Aut}(C) = \{\sigma \in S_n \mid u\sigma \in C \text{ for all } u \in C\}$$

$G = \mathrm{Aut}(C)$

- If G is trivial, C is only a vector space
- If G is nontrivial, it may help to construct the code. C is a module for G

2-Transitive Automorphism Groups

- C is an extremal Type II code
- $\mathrm{Aut}(C)$ acts 2-transitively on coordinates

Known extremal codes with 2-tr. $\mathrm{Aut}(C)$

- Quadratic Residue codes of lengths:
  $8, 24, 32, 48, 80, 104$
- Reed-Muller code of length 32

Are there more such codes?

The Method

1. Use the structure of $G = \mathrm{Aut}(C)$
   - The socle of G is simple or el. abelian
   - Length of C = degree of G

   $\Rightarrow$ Only few possibilities for G
2. Find all G-modules of dim $^n/_2$
3. Find modules that are self-dual as codes
4. Check if the codes are extremal
   - Use subgroups of G

Simple Socle

Socle T	deg $n^\dagger$	dim $n/2$ mod.	extremal
M_{24}	24	Golay code	yes
HS	176	none	
$PSU(3,7)$	344	none	
$PSL(2,7^3)$	344	GQR code	no
$PSL(m,q)$	4 pos.	none	
$PSp(2m,2)$	6 pos.	none	
$PSL(2,p)$	$p+1$	QR codes	$n \leq 104^*$
A_n	n	none	

† $8 \mid n$, $n \leq 3952$

* Bouyuklieva, M., Willems, 2010

Elementary Abelian Socle

- $E = (\mathbb{F}_p^m, +)$, $|E| = \deg E$ (regular)
- $n = 2^m$, $m \leq 11$
- $G \leq \mathrm{AGL}(m, 2)$
- $G \cong E \rtimes H$, $H \leq \mathrm{GL}(m, 2)$ transitive
- If H has a $(n-1)$-cycle
  then C is affine invariant

Affine Invariant Codes

- $\mathrm{AGL}(1, 2^m) \leq G \leq \mathrm{AGL}(m, 2)$
- m is odd
- Charpin, Levy-dit-Vehel, 1994: A method to construct all affine invariant codes

m	n	Num of codes	extremal
5	32	1	yes
7	128	3	none
9	512	70	none
11	2048	515 617	none

Other Cases

- $G \cong E \rtimes H$, H is transitive
- $H \leq \mathrm{GL}(m, 2)$, $m \leq 10$ not prime

Possibilities for H

- $\mathrm{PSL}(k, 2^r) \leq H$, $m = kr$
- $\mathrm{PSp}(k, 2^r) \lhd H$, $m = kr$, k even
- Sporadic examples for $m = 4, 6$

- Only for $m = 9$: 3 self-dual codes for $\mathrm{PSL}(3, 2^3)$, not extremal

Summary

- Extremal codes with 2-tr. Aut(C) are known
- All self-dual codes with 2-tr. groups?
  - QR and GQR codes with PSL$(2, n-1)$
  - No codes with simple groups for large n?
  - Affine-invariant codes with AGL$(1, 2^{\text{odd}})$
  - 3 codes with $E \rtimes$ PSL$(3, 2^3)$ for $n = 2^9$
  - More codes with $E \rtimes$ PSL$(k, 2^r)$ for $n = 2^{kr}$?
  - No codes for $n = 2^{\text{even}}$?

Thank you for your attention!