

Extremal Codes with 2-transitive Groups

Anton Malevich

joint work with Wolfgang Willems

Brussels, 4 October 2013

Self-Dual Type II Codes

- Linear code C is a subspace of Fⁿ, F = F₂,
 c ∈ C is a codeword
- The dual code

 $\mathcal{C}^{\perp} = \{ \mathbf{v} \mid \langle u, \mathbf{v}
angle = \mathbf{0} ext{ for all } u \in \mathcal{C} \}$

If $C = C^{\perp}$ the code is self-dual

- For a self-dual code dim = n/2
- Weight of c is the number of 1's
- Self-dual code is of Type II if all weights are divisible by 4

- *C* is a subspace of \mathbb{F}^8 spanned by rows
- ▶ Self-dual: $\langle u, v \rangle = 0$ for all $u, v \in C$
- Type II: all weights are divisible by 4
- Minimum distance: d = 4

$$\begin{array}{c} c_1 \\ c_2 \\ c_3 \\ c_4 \end{array} \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

- C is a subspace of \mathbb{F}^8 spanned by rows
- ▶ Self-dual: $\langle u, v \rangle = 0$ for all $u, v \in C$
 - $\langle C_1, C_2 \rangle = 0 + 0 + 1 + 0 + 0 + 0 + 0 + 1 = 0$
 - $\langle c_i, c_j \rangle = 0$ for all $i, j \in \{1, 2, 3, 4\}$
- Type II: all weights are divisible by 4
- Minimum distance: d = 4

- C is a subspace of \mathbb{F}^8 spanned by rows
- Self-dual: $\langle u, v \rangle = 0$ for all $u, v \in C$
- Type II: all weights are divisible by 4
 - ▶ wt(c_i) = # of 1's = 4
 - wt(c) = 0, 4 or 8 for c ∈ C

• Minimum distance: d = 4

- C is a subspace of \mathbb{F}^8 spanned by rows
- Self-dual: $\langle u, v \rangle = 0$ for all $u, v \in C$
- Type II: all weights are divisible by 4
- Minimum distance: d = 4
 - $d = \min\{\operatorname{wt} c \mid c \in C, \ c \neq 0\}$

Extremal Type II Codes

• Bound on $d: d \le 4 \lfloor \frac{n}{24} \rfloor + 4$,

If "=" then the code is extremal

- For extremal codes $n \le 3928$
- Length of a Type II code is a multiple of 8
- Extremal codes only constructed for n =
 8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112, 136
- ▶ Our concern: 136 < .?. ≤ 3928

• Aut(C) = { $\sigma \in S_n$ | $c\sigma \in C$ for all $c \in C$ }

Example: Extended cyclic code $\sigma = (1234567) - \text{cyclic shift, (8) is fixed}$ $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ \end{bmatrix} \xrightarrow{\sigma} \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ \end{bmatrix}$

- C is an $\mathbb{F}G$ -module of dim n/2
- $G \leq \operatorname{Aut}(C)$ helps construct a code

• Aut(C) = { $\sigma \in S_n$ | $c\sigma \in C$ for all $c \in C$ }

Example: Extended cyclic code $\sigma = (1234567) - \text{cyclic shift}, (8)$ is fixed

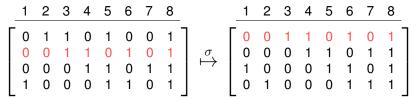
		•									•							
	1	2	3	4	5	6	7	8		1	2	3	4	5	6	7	8	
ſ	- 0	1	1	0	1	0	0	1.	$\stackrel{\sigma}{\mapsto}$	Γo	0	1	1	0	1	0	1	1
	0	0	1	1	0	1	0	1	σ_{i}	0	0	0	1	1	0	1	1	
I	0	0	0	1	1	0	1	1	$ \mapsto$	1	0	0	0	1	1	0	1	I
	1	0	0	0	1	1	0	1		0	1	0	0	0	1	1	1	
	_							-									-	

• C is an $\mathbb{F}G$ -module of dim n/2

• Aut(C) = { $\sigma \in S_n$ | $c\sigma \in C$ for all $c \in C$ }

Example: Extended cyclic code

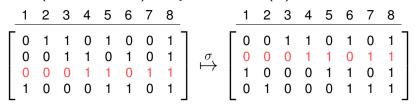
 $\sigma = (1234567) - \text{cyclic shift}, (8) \text{ is fixed}$



• C is an $\mathbb{F}G$ -module of dim n/2

• Aut(C) = { $\sigma \in S_n$ | $c\sigma \in C$ for all $c \in C$ }

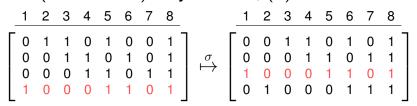
Example: Extended cyclic code $\sigma = (1234567) - \text{cyclic shift}, (8) \text{ is fixed}$



• C is an $\mathbb{F}G$ -module of dim n/2

• Aut(C) = { $\sigma \in S_n$ | $c\sigma \in C$ for all $c \in C$ }

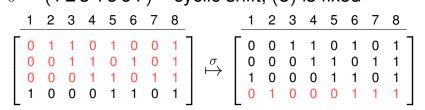
Example: Extended cyclic code $\sigma = (1234567) - \text{cyclic shift}, (8) \text{ is fixed}$



• C is an $\mathbb{F}G$ -module of dim n/2

• Aut(C) = { $\sigma \in S_n$ | $c\sigma \in C$ for all $c \in C$ }

Example: Extended cyclic code $\sigma = (1234567) - \text{cyclic shift}, (8) \text{ is fixed}$

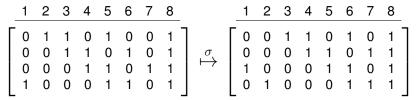


• C is an $\mathbb{F}G$ -module of dim n/2

• Aut(C) = { $\sigma \in S_n$ | $c\sigma \in C$ for all $c \in C$ }

Example: Extended cyclic code

 $\sigma = (1234567) - \text{cyclic shift}, (8) \text{ is fixed}$



• C is an **F**G-module of dim n/2

Extremal Type II Codes (cont.)

- Extremal codes only known for n =
 8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112, 136
- Common approach: one length n at a time
 - 1. Assume $G \leq Aut(C)$ for some G
 - 2. Construct extremal *C* (or prove nonexistence under the assumption)
- ► SLOANE'73: *n* = 72? Still open
 - ▶ ..., BORELLO'13: |Aut(*C*)| ≤ 5
 - Only 6 possibilities for Aut(C)
- ▶ HARADA'08: *n* = 112

Extremal Type II Codes (cont.)

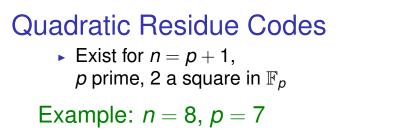
- Extremal codes only known for n =
 8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112, 136
- Common approach: one length n at a time
 - 1. Assume $G \leq Aut(C)$ for some G
 - 2. Construct extremal *C* (or prove nonexistence under the assumption)
- Our approach: all lengths $n \le 3928$
 - Families of codes: QR, QDC
 - Automorphisms of prime order $p \ge n/2$
 - ► 2-transitive Aut(*C*)

Quadratic Residue Codes

Exist for n = p + 1,
 p prime, 2 a square in F_p



Theorem (BOUYUKLIEVA, M., WILLEMS'10) The only extremal QR codes are of lengths n = 8, 24, 32, 48, 80 and 104



1, 2 and 4 are

the squares in \mathbb{F}_7^{\times}

Theorem (BOUYUKLIEVA, M., WILLEMS'10) The only extremal QR codes are of lengths n = 8, 24, 32, 48, 80 and 104

1 2 3 4 5 6 7

 0
 1
 1
 0
 1
 1
 0
 1

 0
 0
 1
 1
 0
 1
 0
 1

 0
 0
 0
 1
 1
 0
 1
 1

 1
 0
 0
 0
 1
 1
 0
 1

Quadratic Residue Codes

- Exist for n = p + 1,
 p prime, 2 a square in F_p
- Example: n = 8, p = 7

1,2 and 4 are the squares in \mathbb{F}_7^\times

Theorem (BOUYUKLIEVA, M., WILLEMS'10) The only extremal QR codes are of lengths n = 8, 24, 32, 48, 80 and 104

Quadratic Residue Codes

- Exist for n = p + 1,
 p prime, 2 a square in F_p
- Example: n = 8, p = 7

1, 2 and 4 are the squares in \mathbb{F}_7^{\times}

Theorem (BOUYUKLIEVA, M., WILLEMS'10) The only extremal QR codes are of lengths n = 8, 24, 32, 48, 80 and 104

Sketch of the Proof

- Task: find a codeword of weight < 4 [n/24] + 4 in every QR code for n ≤ 3928
- How? Search in a subcode
 C^H = {codewords fixed by all σ ∈ H},
 where H ≤ Aut(C) suitable
- How to find suitable H? (heuristic)
 - |H| large $\Leftrightarrow |C^H|$ small
 - $|C^{H}|$ depends on structure of H
 - $5 \le |H| \le 30$ works for large *n*

2-Transitive Automorphism Groups

Known extremal codes with 2-tr. Aut(C)

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

Theorem (M., WILLEMS'12 + CHIGIRA ET AL.'13) There are no other such codes.

1. Aut(*C*) is transitive =
for any *i*, *j*
$$\in$$
 {1,..., *n*} there exists
 $\tau \in$ Aut(*C*) with $\tau(i) = j$
 $i = 1, j = 8: \tau_1 = (18)(24)(37)(56) \in$ Aut(*C*)
 $\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \xrightarrow{\tau_1} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$

• $E = \{id, \tau_1, \dots, \tau_7\}$ elementary abelian $|E| = \deg E = n$, E is transitive

2. Aut(*C*) is 2-transitive = transitive and for any $i, j \in \{1, ..., n-1\}$ there exists $\sigma \in Aut(C)$ with $\sigma(i) = j$ and $\sigma(n) = n$

 $i = 1, j = 2: \sigma = (1234567) \in Aut(C)$

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \xrightarrow{\sigma} \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

• $E \rtimes \langle \sigma \rangle = \text{AGL}(1, 2^3)$ is 2-transitive

• $AGL(1, 2^m) \le Aut(C) \Rightarrow C$ affine invariant

2-Transitive Automorphism Groups

Known extremal codes with 2-tr. Aut(C)

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

Theorem (M., WILLEMS'12 + CHIGIRA ET AL.'13) There are no other such codes.

The Method

- G = Aut(C) is 2-transitive
- 1. Use the structure of G
 - ► The socle of *G* is simple or elementary abelian
 - Degree of G = length of $C \leq 3928$

 \Rightarrow Only few possibilities for G

- 2. Find all \mathbb{F} *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	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(2 <i>m</i> , 2)	6 pos.	none	
PSL(2, <i>p</i>)	<i>p</i> + 1	QR codes	<i>n</i> ≤ 104*
A _n	п	none	

† 8 | *n*, *n* ≤ 3952

* QR codes Theorem

Simple Socle: Case A_n

•
$$A_n = \{ \sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1 \}$$

Proposition

There are no extremal codes with $Aut(C) = A_n$.

$$\boldsymbol{C} \ni \boldsymbol{c} = \begin{pmatrix} i & j & k \\ \hline \ast & . & \ddots & 0 & . & 1 & . & 1 & . & \star \end{pmatrix}$$

►
$$\sigma = (i, j, k) \in A_n$$
, since sgn $(\sigma) = 1$.
 $c + c\sigma = \left(\begin{array}{cccc} i & j & k \\ \hline 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ \hline \end{array} \right)$

• wt($c + c\sigma$) = 2 \Rightarrow C not extremal

Simple Socle

Socle	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(2 <i>m</i> , 2)	6 pos.	none	
PSL(2, <i>p</i>)	<i>p</i> + 1	QR codes	<i>n</i> ≤ 104*
A _n	п	none	

† 8 | *n*, *n* ≤ 3952

* QR codes Theorem

Elementary Abelian Socle E

- ▶ $|E| = n = 2^m, m \le 11$ (since $n \le 3928$)
- $G \leq AGL(m, 2)$ 2-transitive
- \Rightarrow $G \cong E \rtimes H, H \leq GL(m, 2)$ transitive
 - Two cases:
- 1. C affine invariant
 - *H* contains cyclic shift σ of length (n-1)
- 2. C not affine invariant

Affine Invariant Codes

- $AGL(1, 2^m) \leq G \leq AGL(m, 2)$
- $n = 2^m$, *m* is odd
- CHARPIN, LEVY-DIT-VEHEL'94:
 A method to construct all aff. inv. codes

т	n	Num of codes	extremal
5	32	1	yes
7	128	3	none
9	512	70	none
11	2048	515617	none

Other Cases

- G ≅ E ⋊ H, H ≤ GL(m, 2) is transitive
 H does not contain cyclic shift σ
- $n = 2^m$, m = 4, 6, 8, 9 or 10
- Possibilities for H:
 - $\mathsf{PSL}(k, 2^r) \le H, m = kr \quad k, r \ge 2$
 - $\mathsf{PSp}(k, 2^r) \leq H, m = kr, k \text{ even}$
 - Sporadic examples for m = 4, 6

Other Cases (cont.)

- $G = E \rtimes \mathsf{PSL}(k, 2^r), m = kr$
- ▶ For *m* < 9: no self-dual codes</p>
- Only for m = 9: 3 codes, not extremal
- m = 10: Too many \mathbb{F} *G*-modules of dim n/2
 - ► CHIGIRA ET AL.'13: for m = 2sr even no self-dual codes with G ≤ E ⋊ PSL(2s, 2^r)

Summary

- ► Extremal codes with 2-tr. Aut(C) are known
 - ▶ QR codes of length 8, 24, 32, 48, 80 or 104
 - Reed-Muller code of length 32
- ⇒ If new extremal codes exist, then they have "little" structure
 - Open problems
 - Classify self-dual codes with 2-tr. Aut(C)
 - Reduce the bound $n \leq 3928$ for extremal codes

Thank you for your attention!