Groups and Codes

Anton Malevich

Otto-von-Guericke Universität Magdeburg

Hannover, 28 January 2013

1. Extremal codes: motivation

2. Extremal codes and representation theory

3. Extremal codes and 2-transitive groups

Self-Dual Type II Codes

- Linear code C is a subspace of K^n, $K = \mathbb{F}_2$,
- The dual code
$$C^{\perp} = \{v \mid (u, v) = 0 \text{ for all } u \in C\}$$
If $C = C^{\perp}$ the code is self-dual
- Self-dual code is Type II
if all weights are a multiple of 4
- Length of a Type II code is divisible by 8

Example: Hamming Code

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

- C is a subspace of K^8 spanned by rows
- Self-dual: $(u, v) = 0$ for all $u, v \in C$
- Type II: all weights are a multiple of 4
- Minimum distance: $d = 4$
  - $d = \min\{\mathrm{wt}\, c \mid c \in C,\ c \neq 0\}$

Extremal Type II Codes

- Bound on d: $d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4$,

  If "=" then the code is extremal
- For extremal codes $n \leq 3928$
- Extremal codes only constructed for $n =$

  8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112, 136
- Motivation: $136 \leq \ldots \overset{?}{\ldots} \leq 3928$

Automorphism Group

- $\mathrm{Aut}(C) = \{\sigma \in S_n \mid u\sigma \in C \text{ for all } u \in C\}$
- $u\sigma = \left(u_{\sigma^{-1}(1)}, \ldots, u_{\sigma^{-1}(n)}\right)$

Example: Extended cyclic code

$\sigma = (1\,2\,3\,4\,5\,6\,7)$ – cyclic shift, (8) is fixed

$$\begin{array}{c} \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{array} \\ \left[\begin{array}{cccccccc} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right] \end{array} \overset{\sigma}{\mapsto} \begin{array}{c} \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{array} \\ \left[\begin{array}{cccccccc} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right] \end{array}$$

- Equivalence: $C \cong C\rho$ if $\rho \notin \mathrm{Aut}(C)$

Module Structure

Let $G \leq \mathrm{Aut}(C)$

- $C \leq K^n$ as KG-modules
- $(u\sigma, v\sigma) = (u, v)$, for $u, v \in K^n$, $\sigma \in G$
- $C^\perp$ is also a KG-module
  - $\mathrm{Aut}(C) = \mathrm{Aut}(C^\perp)$
- $C^* = \mathrm{Hom}_K(C, K)$ becomes a KG-module via $(f\sigma)(c) := f(c\sigma^{-1})$

Dual Code and Dual Module

Lemma

$K^n/C^\perp \cong C^*$ as KG-modules

Proof

- $f_v : C \to K$, $f_v(c) = (v, c)$ for $v \in K^n$
- $\alpha : v \mapsto f_v$ is KG-linear with $\operatorname{Ker} \alpha = C^\perp$
- use $|C| = |C^*|$

Example: $n = 72$?

SLOANE'73:

Is there an extremal code with $n = 72$?

Examine primes $p \mid |\mathrm{Aut}(C)|$

- CONWAY, PLESS, THOMPSON'82: $p \leq 11$
- HUFFMAN, YORGOV'87: $p \neq 11$

  ...
- BORELLO'12:
  - $|\mathrm{Aut}(C)| = 2^a 3^b 5 \leq 24$
  - Only 11 possibilities for $\mathrm{Aut}(C)$

General Situation

- Extremal codes only known for $n =$
  8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112, 136
- $136 \leq \ .\overset{?}{.}\ . \ \leq 3928$

Our classifications

- All QR and QDC codes
- Codes with $\sigma \in \mathrm{Aut}(C)$, $\mathrm{ord}(\sigma) = p > n/2$
- Codes with 2-transitive $\mathrm{Aut}(C)$

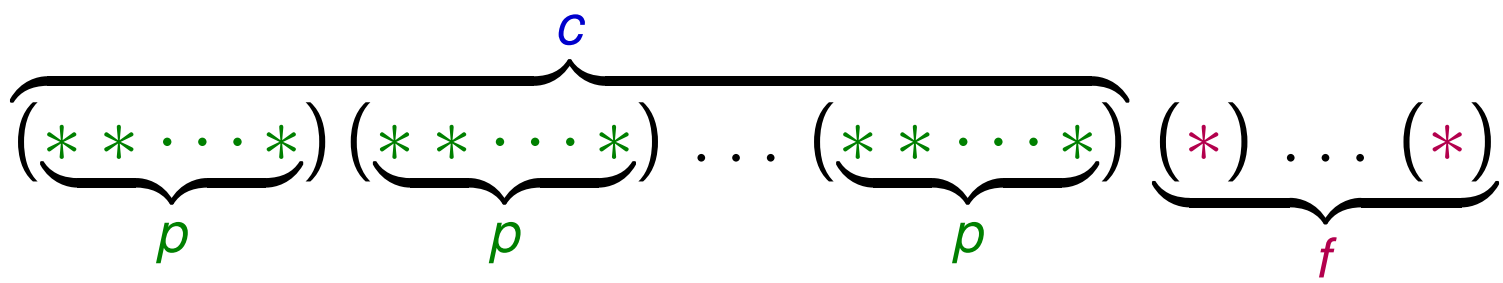
1. Extremal codes: motivation

2. Extremal codes and representation theory

3. Extremal codes and 2-transitive groups

Types of Automorphisms

$\sigma \in \mathrm{Aut}(C)$ of type p-(c, f):



Theorem (Bouyuklieva, M., Willems'10)

- C self-dual code with $n \geq 48$
- $\sigma \in \mathrm{Aut}(C)$ with $\mathrm{ord}(\sigma) = p \geq 5$.

Then $c \geq f$.

$\sigma \in \mathrm{Aut}(C)$ with $\mathrm{ord}(\sigma) = p > n/2$

Corollary

- σ of type p-$(1,1)$
- $n = p + 1 = 24m + 8i$, $i = 0, 1$.

$K\langle\sigma\rangle$ is semisimple

$$C \leq K^n = K \oplus K\langle\sigma\rangle =$$
$$K \oplus K \oplus V_1 \oplus \ldots \oplus V_{k/2} \oplus V_1^* \oplus \ldots \oplus V_{k/2}^*$$

$\dim V_i = s(p) = \min\{s : p \mid 2^s - 1\}$, $k = \frac{p-1}{s(p)}$

Case $k = 2$

Proposition

If $k = 2$ then C is an extended QR code

Proof

$$C \leq K^n = K \oplus K \langle \sigma \rangle = K \oplus K \oplus V \oplus V^*$$
$$= K \oplus Q \oplus K \oplus N$$

Example: QR code for $n = 8$, $p = 7$

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

$$\begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline \left[\begin{array}{ccccccc|c} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right] \end{array}$$

Extremal QR codes

Theorem (Bouyuklieva, M., Willems'10)

The only extremal QR codes are of lengths

$$n = 8, 24, 32, 48, 80 \text{ and } 104$$

Proof

- Task: find a codeword of weight $< 4\left\lfloor \frac{n}{24} \right\rfloor + 4$ in every QR code for $104 < n \leq 3928$
- How? Search in a subcode

$$C^H = \{\text{codewords fixed by all } \sigma \in H\},$$

where $H \leq \mathrm{Aut}(C)$ suitable

Case $k > 2$

$$K^n = K \oplus K \oplus V_1 \oplus \ldots \oplus V_{k/2} \oplus V_1^* \oplus \ldots \oplus V_{k/2}^*$$

$$\Rightarrow \quad C = K \oplus U_1 \oplus \ldots \oplus U_{k/2}, \text{ with } U_i \in \{V_i, V_i^*\},$$

since $K^n / C^\perp \cong C^*$

- $\geq \left\lceil \frac{2^{k/2}}{k} \right\rceil$ inequivalent codes
- If $s(p)$ is small and k large
  $\Rightarrow$ large number of codes
- If $s(p)$ is large prime
  $\Rightarrow$ No suitable $H \leq \mathrm{Aut}(C)$

Double Circulant codes

$$\left[\begin{array}{cccc|ccccc} 1 & & & & 0 & 1 & \cdots & 1 \\ & 1 & & & 1 & & & \\ & & \ddots & & \vdots & & Q & \\ & & & 1 & 1 & & & \end{array}\right]$$

- $n = 2m + 2$, Q is $m \times m$ circulant matrix
- $G = \langle \tau \rangle \times C_2 \leq \mathrm{Aut}(C)$, $\mathrm{ord}(\tau) = m$
- QDC code, if $m = p$ prime
  and Q corresponds to quadratic residues

Proposition (M.'12)

The only extremal QDC codes are of lengths

$$n = 8, 24, 40, 88 \text{ and } 136$$

DC codes: Decomposition

- $G = \langle \tau \rangle \times C_2$, $\mathrm{ord}(\tau) = m$
- KG is not semisimple

$$\begin{aligned} K^n &= K \oplus K \oplus KG \\ &= K \oplus K \oplus P_1 \oplus \ldots \oplus P_r \\ &= K \oplus K \oplus P(S_1) \oplus \ldots \oplus P(S_r) \end{aligned}$$

- P_i projective indecomposable
- S_i socle of P_i
- too many possibilities for C

General Situation: Arbitrary Group

- Let $C = C^{\perp}$, $G \leq \mathrm{Aut}(C)$
- Write $1 = f_1 + \ldots + f_s$ with
  - $f_i \in KG$ central orthogonal idempotents
  - $\hat{f}_i = f_i$, where $\hat{}: KG \to KG$, $\sigma \mapsto \sigma^{-1}$
- Put $V_i = K^n f_i$ and $C_i = Cf_i$
- Then we get $K^n = V_1 \perp \ldots \perp V_s$, $C = C_1 \perp \ldots \perp C_s$ and $C_i^{\perp} = C_i$

Constructing extremal codes

Algorithm (O'Brien, Willems'12)

1. Find central orthogonal idempotents $f_i = \hat{f}_i$
   - e.g., $H \trianglelefteq G$, $|H|$ odd, $f_1 = \sum_{h \in H} h$, $f_2 = 1 - f_1$
2. $L_i = \left\{ M_i^{\perp} = M_i \leq V_i \mid d(M_i) \geq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4 \right\}$
3. $L = \left\{ M = M_1 + \ldots + M_s \mid M_i \in L_i \right\}$
4. Check if any $M \in L$ is extremal

Example: $n = 72$

- Borello'12: $\pi \notin \mathrm{Aut}(C)$, $\mathrm{ord}(\pi) = 6$

1. Extremal codes: motivation

2. Extremal codes and representation theory

3. Extremal codes and 2-transitive groups

2-Transitive Automorphism Groups

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

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

Theorem (M., WILLEMS'12)

There are no other such codes,

- apart from possibly $n = 1024$

The Method

- $G = \mathrm{Aut}(C)$ is 2-transitive

1. Use the structure of G
   - The socle of G is simple or elementary abelian
   - Degree of G = length of $C \leq 3928$
2. Find submodules M of K^n with $\dim M = n/2$
3. Take such M that are self-dual as codes
4. Check if the codes are extremal
   - use subgroups of G

Simple Socle

see Table in CAMERON'81

Socle	deg $n^\dagger$	dim $M = n/2$	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	

† $8 \mid n$, $n \leq 3952$

* QR codes Theorem

Elementary Abelian Socle E

- $|E| = n = 2^m$, $m \leq 11$ (since $n \leq 3928$)
- $G \leq \mathrm{AGL}(m, 2)$ 2-transitive

$\Rightarrow$ $G \cong E \rtimes H$, $H \leq \mathrm{GL}(m, 2)$ transitive

- Two cases:

1. C affine invariant
   - H contains cyclic shift σ of length $(n-1)$
2. C not affine invariant

Affine Invariant Codes

- $C \leq KE$, $E \rtimes \langle \sigma \rangle \cong \mathrm{AGL}(1, 2^m)$
- $n = 2^m$, m is odd
- CHARPIN, LEVY-DIT-VEHEL'94:
  A method to construct all aff. inv. 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

- $G \cong E \rtimes H$, $H \leq \mathrm{GL}(m, 2)$ is transitive
  - H does not contain cyclic shift σ
- $m = 4, 6, 8, 9$ or 10
- Possibilities for H:
  - $\mathrm{PSL}(k, 2^r) \leq H$, $m = kr \quad k, r \geq 2$
  - $\mathrm{PSp}(k, 2^r) \leq H$, $m = kr$, k even
  - Sporadic examples for $m = 4, 6$
- For $m < 9$: no self-dual codes
- Only for $m = 9$: 3 codes, not extremal
- $m = 10$: case $\mathrm{PSL}(2, 2^5)$ not excluded
  - Too many KG-modules of dim $n/2$

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
  - Possibly a code of length $n = 1024$ with $E \rtimes \mathrm{PSL}(2, 2^5) \leq \mathrm{Aut}(C)$

$\Rightarrow$ If new extremal codes exist, then they have "little" structure

- Open problems
  - Finish the $n = 1024$ case
  - All self-dual codes with 2-tr. Aut(C)?
  - Reduce the bound $n \leq 3928$ for extremal codes

Thank you for your attention!