On Extremal Codes With Automorphisms

Anton Malevich

Magdeburg, 20 April 2010

joint work with S. Bouyuklieva and W. Willems

1. Linear codes

2. Self-dual and extremal codes

3. Quadratic residue codes

4. Automorphisms of extremal codes

1. Linear codes

2. Self-dual and extremal codes

3. Quadratic residue codes

4. Automorphisms of extremal codes

Introduction

- Linear code C is a k-dim subspace of an n-dim vector space
- Generator matrix G consists of basis vectors of C

$$G = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{pmatrix}$$

- Parity check matrix H (size $n \times (n-k)$):

$$Hx = 0 \quad \text{for all } x \in C$$

Introduction

- Weight of a codeword is the number of its nonzero coordinates
- Weight enumerator:

$$W_C(x, y) = \sum_{u \in C} x^{n-\mathrm{wt}(u)} y^{\mathrm{wt}(u)} = \sum_{i=0}^{n} A_i x^{n-i} y^i$$

- Parameters $[n, k, d]$ stand for length, dimension and minimum distance.

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

Types of Automorphisms

Definition

$\sigma \in \mathrm{Aut}(C)$ is called of type p-(c, f) if it has exactly c cycles of length p and f fixed points. If n is the length of C then $pc + f = n$.

$$\overbrace{(\underbrace{* * \cdots *}_{p})(\underbrace{* * \cdots *}_{p}) \ldots (\underbrace{* * \cdots *}_{p})}^{c}\ \underbrace{(*) \ldots (*)}_{f}$$

- The dual code

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

- The dual weight enumerator

$$W_{C^{\perp}}(x, y) = \frac{1}{|C|} W_C(x + y, x - y)$$

- If $C = C^{\perp}$ the code is self-dual
- For a self-dual code $k = n/2$ and all codewords have even weight

Self-Dual Codes

- Two types of self-dual codes:
  Type I (SE): all weights are even
  Type II (DE): all weights are a multiple of 4

Theorem (Gleason)

Weight enumerator of a self-dual code is a polynomial in f and g of degrees respectively

- *for Type I codes:* 2 *and* 8*,*
- *for Type II codes:* 8 *and* 24*.*

Self-Dual Codes

- Two types of self-dual codes:
  Type I (SE): all weights are even
  Type II (DE): all weights are a multiple of 4

Corollary

Length of a Type II code is a multiple of 8

$$n = 24m + 8i, \quad i = 0, 1 \text{ or } 2$$

Extremality

Corollary (Mallows, Sloane)

- $d \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 4$ *Type II (tight)*
- $d \leq 2\left\lfloor \frac{n}{8} \right\rfloor + 2$ *Type I (NOT tight)*

Theorem (Rains, using shadow)

New bounds for Type I codes are:

- $d \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 4$ $n \not\equiv 22 \pmod{24}$
- $d \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 6$ $n \equiv 22 \pmod{24}$

- Zhang: no extremal DE codes for $n > 3952$

Lengths of known extremal codes:

$8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112, 136$

For red lengths extended quadratic residue codes are extremal.

For blue lengths quadratic double circulant codes are extremal.

Existing Codes

$[24, 12, 8]$ Golay code

- $\mathrm{Aut}(C) = \mathrm{M}_{24}$ (5-transitive)
- Order of $\mathrm{Aut}(C)$: $2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
- Unique

$[48, 24, 12]$ QR-code

- $\mathrm{Aut}(C) = \mathrm{PSL}_2(47)$ (2-transitive)
- Order of $\mathrm{Aut}(C)$: $2^4 \cdot 3 \cdot 23 \cdot 47$
- Unique (computer search)

Putative Codes

$[72, 36, 16]$-code

- $\mathrm{Aut}(C)$ is solvable
- Possible primes in $|\mathrm{Aut}(C)|$: $2, 3, 5, 7$
- Possible order: $|\mathrm{Aut}(C)| \leq 36$

$[96, 48, 20]$-code

- Possible primes in $|\mathrm{Aut}(C)|$: $2, 3, 5$

Cyclic Codes

$$G = \begin{pmatrix} a_0 & a_1 & \cdots & a_p \\ a_p & a_0 & \cdots & a_{p-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}$$

- C is an ideal in $\mathbb{F}_2[x]/_{\langle x^p-1\rangle}$
- $C = \langle e(x)\rangle$ with $e(x) = e^2(x)$
- Automorphisms of C:
    - cyclic shift σ of order p
    - $\mu\colon x \mapsto x^2$ of order $s(p)$

Definition of QR Codes

- $p \equiv \pm 1 \bmod 8$
- Quadratic residues Q and nonresidues N
- QR codes are cyclic codes with
$$e(x) = \sum_{n \in N} x^n \quad \text{or} \quad e(x) = \sum_{r \in Q} x^r$$

Extended QR Codes

If $p \equiv -1 \bmod 8$:

- Extended QR code C is self-dual of Type II
- $\mathrm{Aut}(C) = \mathrm{PSL}_2(p), \quad p \neq 7$ or 23
- $\mathrm{Aut}(C)$ is 2-transitive
- $|\mathrm{Aut}(C)| = p^{\frac{(p-1)(p+1)}{2}}$

Importance of QR Codes

- Hamming and Golay codes are QR
- Large minimum distance: $d^2 - d + 1 \geq p$
  (if $p \equiv \pm 1 \bmod 8$)
- Asymptotically good?
- Different decoding techniques

Quadratic Double Circulant Codes

- $n = 2q + 2$, $q \equiv 3 \bmod 8$ is a prime

$$G = \begin{pmatrix} 1 & & & & 0 & 1 & \dots & 1 \\ & 1 & & & 1 & & & \\ & & \ddots & & \vdots & & Q & \\ & & & 1 & 1 & & & \end{pmatrix}$$

- Q – cyclic matrix, corr. to residues
- C is self-dual of Type II
- $\mathrm{Aut}(C) = \mathrm{PSL}_2(q) \times \mathbb{Z}_2$

1. Linear codes

2. Self-dual and extremal codes

3. Quadratic residue codes

4. Automorphisms of extremal codes

Motivation

n	d	$p \mid \lvert \mathrm{Aut}(C) \rvert$	comment
8	4	$2, 3, 7$	*xQR*, *QDC*
24	8	$2, 3, 5, 7, 11, 23$	*xQR*, *QDC*
32	8	$2, 3, 5, 7, 31$	*xQR*
40	8	$2, 3, 5, 7, 19$	*QDC*
48	12	$2, 3, 23, 47$	*xQR*
80	16	$2, 5, 19, 79$	*xQR*
88	16	$2, 3, 7, 11, 43$	*QDC*
104	16	$2, 3, 13, 17, 103$	*xQR*
112	16	$2, 7$	*Harada*, 2008
136	20	$2, 3, 11, 67$	*QDC*

Possible Automorphisms

Theorem

- *C is an extremal self-dual code*
- *C is of length $n \geq 48$*
- *$\sigma \in \mathrm{Aut}(C)$ is of type $p-(c,f)$ where $p \geq 5$ is a prime.*

Then $c \geq f$.

Assumptions

- C is self-dual, doubly-even, extremal
- $\sigma \in \mathrm{Aut}(C)$ of prime order $p > n/2$

Corollary

- $c = f = 1$ *since* $n = pc + f$
- σ *is of type* $p - (1, 1)$
- $n = p + 1 = 24m + 8i,\ i = 0, 1$
- $i \neq 2$ *since* $24m + 16 - 1$ *is not a prime*

Definition

$s(p)$ denotes the smallest number $s \in \mathbb{N}$, such that

$$p \mid 2^s - 1.$$

In our case: $s(p) = \dfrac{p-1}{k}$, $k \geq 2$ even

Proposition

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

Definition

$s(p)$ denotes the smallest number $s \in \mathbb{N}$, such that

$$p \mid 2^s - 1.$$

In our case: $s(p) = \dfrac{p-1}{k}$, $k \geq 2$ even

Proposition

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

Classification of QR Codes

Theorem

Let C be a self-dual doubly-even extended QR code. Then C is extremal exactly for the lengths

$$8, 24, 32, 48, 80 \textit{ and } 104$$

Sketch of the proof

- Task: find a codeword of weight $< 4\left\lfloor \frac{n}{24} \right\rfloor + 4$ in a large code C.
- Way out: search in a suitable subcode $C' < C$.

$H < \mathrm{Aut}(C)$

$$C' = C^H = \{\text{codewords fixed by } H\}$$

Sketch of the proof

- C extended QR of length $n = p + 1$
- $G = \mathrm{Aut}(C) = \mathrm{PSL}(2, p)$

$H < G$

- $H =$ cyclic of order 4 or 6
- $H = \mathrm{Syl}_2(G)$

Cases depending on k

$$n = 24m \quad \text{or} \quad n = 24m + 8$$

$$p = n - 1$$

$$s(p) = \frac{p-1}{k}$$

- $k = 2$ (one code) solved
- $k > 2$ $\left(\geq \left\lceil \frac{2^{k/2}}{k} \right\rceil \text{ codes}\right)$ open
  - similar method may be applied

Case $k > 2$

- Possibly large number of codes
- C is an extended cyclic code
  - automorphisms of order p and $s(p)$
- $\mathrm{Aut}(C)$ is not transitive!
- if $s(p)$ prime $\Rightarrow$ difficulties

List of Open Cases

p	$s(p)$	k	codes	d
1399	233	6	2	236
2351	47	50	$\geq 671\,089$	396
2383	397	6	2	400
2687	79	34	$\geq 3\,856$	452
2767	461	6	2	464
3191	55	58	$\geq 9\,256\,396$	536
3343	557	6	2	560
3391	113	30	$\geq 1\,093$	568
3463	577	6	2	580
3601	601	6	2	604

Conjecture

There are no extremal self-dual doubly-even codes having an automorphism of prime order $p > n/2$ apart from the cases

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

Summary

- C is self-dual, doubly-even, extremal
- $\sigma \in \mathrm{Aut}(C)$ of prime order $p > n/2$

- We give full classification of extremal extended QR codes that solves the case $s(p) = \frac{p-1}{2}$
- For $s(p) < \frac{p-1}{2}$ some cases still remain open