On Extremal Codes With Automorphisms

S. Bouyuklieva A. Malevich W. Willems

Optimal Codes and Related Topics,
16.6 – 22.6.2009

- C is a binary, self-dual, doubly-even $[n, n/2, d]$–code
- n is a multiple of 8
- $d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4$, if "$=$" C is extremal
- Zhang: extremal codes do not exist for $n > 3952$

Lengths of known extremal codes:

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

For red lengths extended QR codes are extremal.

Lengths of known extremal codes:

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

For red lengths extended QR codes are extremal.

Why Is The Automorphism Group Of Interest?

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

- 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 $pc + f = n$.

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

Proposition

- *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 (for $n \geq 48$)

- $c = f = 1$ *since* $n = pc + f$
- σ *is of type* $p - (1, 1)$
- $n = p + 1 = 24m + 8i, \; i = 0, 1$
- $i \neq 2$ *since* $3 \mid 24m + 16 - 1$ *not a prime*

Assumptions

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

Corollary (for $n \geq 48$)

- $c = f = 1$ *since* $n = pc + f$
- σ *is of type* $p - (1, 1)$
- $n = p + 1 = 24m + 8i,\ \ i = 0, 1$
- $i \neq 2$ *since* $3 \mid 24m + 16 - 1$ *not a prime*

Definition

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

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

$s(p) = \dfrac{p-1}{k}$, $k \geq 2$ 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

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

$$s(p) = \frac{p-1}{k},\ k \geq 2 \text{ even}$$

Proposition

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

Main Result

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 $C' < C$.

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

$$C' = C^H = \{c \in C \mid ch = c \quad \forall h \in H\}$$

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
- $H = \mathrm{Syl}_2(G)$

Conjecture

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

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

List Of Open Cases

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

Summary

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

- For $s(p) = \frac{p-1}{2}$ we now all codes due to main result on extended QR codes
- For $s(p) < \frac{p-1}{2}$ some cases still remain open