Binary extremal self-dual codes of type II and their automorphisms

Wolfgang Willems

Otto-von-Guericke-Universität Magdeburg

ALCOMA 2010, Schloss Thurnau, 11.4.-18.4.2010

joint work with S. Bouyuklieva and A. Malevich

set up / notations

- $K = \mathbb{F}_2$, $V = K^n$

- $< v, w > = \sum_{i=1}^{n} v_i w_i$ for $v, w \in V$

- $C = C^{\perp} \leq V$ (self-dual code)

- $\mathrm{wt}(v) = |\{i \mid v_i = 1\}|$ (weight of v)

- C is called of type II if $4 \mid \mathrm{wt}(c)$ for all $c \in C$

- $\mathsf{d}(v, w) = |\{i \mid v_i \neq w_i\}|$ (distance)

- $\mathsf{d}(C) = \min_{c \neq c' \in C} \mathsf{d}(c, c')$ (minimum distance of C)

- $[n, \frac{n}{2}, d]$ (parameters of C)

[length of C, dimension of C, minimum distance of C]

What do we know about self-dual codes of type II ?

Gleason (1970): $8 \mid n$

Mallows, Sloane (1973): $d \leq 4\lfloor \frac{n}{24} \rfloor + 4$

C is called extremal if $d = 4\lfloor \frac{n}{24} \rfloor + 4$

Zhang (1999), Duursma (2003): $n \leq 3672, 3800, 3928$

What extremal codes of type II are known?

n	no of codes	$p \mid \lvert\mathrm{Aut}(C)\rvert$		$\mathrm{Aut}(C) = 1$
8	1	$2, 3, 7$	ext. QR, QDC	
16	2	$2, 3, 5, 7$		
24	1	$2, 3, 5, 7, 11, 23$	ext. QR, QDC	
32	5	$2, 3, 5, 7, 31$	ext. QR	
40	≥ 1000	$2, 3, 5, 7, 19$	QDC	yes
48	≥ 1	$2, 3, 23, 47$	ext. QR	
56	≥ 166	$..., 13$		yes
64	≥ 3270	$..., 31$		
80	≥ 15	$2, 5, 19, 79$	ext. QR	
88	≥ 470	$2, 3, 7, 11, 43$	QDC	
104	≥ 1	$2, 3, 13, 17, 103$	ext. QR	
112	≥ 1	$2, 7,$	Harada, 2008	
136	≥ 1	$2, 3, 11, 67$	QDC	

Definition quadratic double circulant code (QDC)

$n = 2q + 2$ where $q \equiv 3 \bmod 8$ is prime.

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

where Q is the generator matrix of a QR code of length q.

Observations

1. Open (up to 136) are n = 72, 96, 120 and 128.

2. There is a big gap between the bound n=3928 and what we can construct.

3. $G = \mathrm{Aut}(C)$ (in known examples)

   - In some cases $G = 1$.

   - If p is a large prime with $p \mid |G|$ then $p = n - 1$ or $p = \frac{n-2}{2}$.

stick to the case: $n = 24m \leq 3672$

What is known?

code		$G = \mathrm{Aut}(C)$	primes in $\lvert G \rvert$	
[24,12,8]	Golay	M_{24}	2,3,5,7,11,<u>23</u>	
[48,24,12]	ext. QR	PSL(2,47)	2,3,23,<u>47</u>	
[72,36,16]	?	$\lvert G \rvert \leq 36$	2,3,5,7	
[96,48,20]	?	?	2,3,5	
[120,60,24]	?	?	2,3,5,7,19,29	de la Cruz

Why is $G = \mathrm{Aut}(C)$ of interest?

- If G is nontrivial, it may help to construct the code.
- If G is trivial, C has no structure, it's only a combinatorial object; hard to find if it is large and exists.

Definition

Let p be a prime.

We say that $\sigma \in \mathrm{Aut}(C)$ is of type p-(c, f) if σ has c p-cycles and f fixed points.

In particular: $n = cp + f$

Theorem

Let C be an extremal self-dual code (not necessarily of type II) of length $n \geq 48$. If σ is an automorphism of C of type p-(c, f), where $p \geq 5$ is a prime, then $c \geq f$.

Proof If $f > c$ then $f > \sum_{i=0}^{\frac{f-c}{2}-1} \lceil \frac{d}{2^i} \rceil$, by Yorgov.

Remark

- need $n \geq 48$:

  n=44: 5-$(4, 24)$ automorphism

- need $p \geq 5$:

  n=60: 3-$(14, 18)$ is open

Corollary

If $p > \frac{n}{2} \geq 24$ and $p \mid |\mathrm{Aut}(C)|$ for $C = C^{\perp}$ then $p = n - 1$.

Proof

$\frac{n}{2} < p < n$ implies $c = 1$.

σ is of type p-$(1,1)$ implies $n = p + 1$.

- We are not able to classify all extremal self-dual codes of type II which have an automorphism of prime order $p \geq \frac{n}{2}$, i.e. $p = n - 1$.

- An automorphism of order $p = n - 1$ exists for extended QR codes.

Definition Let p be an odd prime. The $s(p)$ is the smallest number $n \in \mathbb{N}$ such that $p \mid 2^n - 1$.

Lemma

Suppose that σ has odd prime order. If $s(p)$ is odd then

$$V \ncong V^* = \mathrm{Hom}_K(V, K)$$

for $1 \neq V$ a simple $K[\sigma]$-module.

Proof

Suppose $1 \neq V \cong V^*$ simple.

$\dim_K V$ is even, by Fong's Lemma.

$\dim_K V = s(p)$ is odd.

Proposition Let $C = C^{\perp}$. If $\sigma \in \mathrm{Aut}(C)$ is of prime order $p = n - 1$ and $s(p) = \frac{p-1}{2}$ is odd then C is an extended QR code.

Proof: $C = C^{\perp} \subseteq K[\sigma] \oplus K$

Maschke $K[\sigma] = K \oplus V \oplus W = K \oplus Q \oplus N$

V and W are irreducible since $s(p) = \frac{p-1}{2}$

$V \not\cong V^* = W$, by the above lemma.

Theorem

If C is an extremal self-dual extended QR-code of type II and of length n then $n = 8, 24, 32, 48, 80$ and 104.

Proof $n = p+1 \leq 3928$ where $n \neq 8, 24, 32, 48, 80, 104$

- $G = \mathrm{PSL}(2, p)$

- Choose $H \leq G$ carefully; cyclic of order 4 or 6; Sylow-2-subgroup

- Find in $C^H = \{c \in C \mid ch = c \text{ for all } h \in H\}$ a codeword c with $\mathrm{wt}(c) < 4\lfloor \frac{n}{24} \rfloor + 4$.

Observation

If there is an automorphism of prime order $p = n - 1$ we needed $s(p) = \frac{p-1}{2}$ to get that C is an extended QR code.

# of cases in which $s(p) \neq \frac{p-1}{2}$:

- 6 if $24 \mid n$
- 27 if $n \equiv 8 \bmod 24$
- $n \equiv 16 \bmod 24$ does not occur

  since $3 \mid 24m + 16 - 1 = p$

Problem If $s(p) \neq \frac{p-1}{2}$ then, with $k = \frac{p-1}{s(p)}$, we have

- $C = C^{\perp} \leq K^n = K[\sigma] \oplus K = K \oplus V_1 \oplus \ldots \oplus V_k \oplus K$

- $V_i \ncong V_i^*$

- $K^n/C = K^n/C^{\perp} \cong C^* = \mathrm{Hom}_K(C, K)$

- $\#$ of possible C: $2^{k/2}$

- C is invariant under $\alpha : x \to x^2$ of order $s(p)$.

- Try to find a codeword of small order in the fixed point space C^H where $H \leq \langle \alpha \rangle$.

Examples

p	$s(p)$	k	Num of Codes	d	
1103	29	38	$2^{19} = 524288$	188	not extremal
2687	79	34	$2^{17} = 131072$	452	open
3191	$55 = 5 \cdot 11$	58	$2^{29} = 536870912$	536	open
3823	$637 = 7^2 \cdot 13$	6	2	640	not extremal

List of open cases

p	$s(p)$	$k = \frac{p-1}{s(p)}$	Num of Codes	d
1399	233	6	2	236
2351	47	50	2^{25}	396
2383	397	6	2	400
2687	79	34	2^{17}	452
2767	461	6	2	464
3191	$55 = 5 \cdot 11$	58	2^{29}	536
3343	557	6	2	560
3391	113	30	2^{15}	568
3463	577	6	2	580
3601	601	6	2	604

Conjecture

Extremal self-dual codes of type II which have an automorphism of prime order $p \geq \frac{n}{2}$ are extended QR codes except the $[32, 16, 8]$ Reed-Muller code.

$\mathrm{Aut}([32, 16, 8]\ \text{Reed-Muller}) = \mathrm{AGL}(5, 2)$

Remark

Let $n = 2q + 2$ with q an odd prime.

For $n = 16, 40, 64, 88$ there are extremal self-dual codes of type II with an automorphism of order q which are not equivalent to QDC codes.

Theorem

If C is an extremal self-dual QDC code of type II and of length n then $n = 8, 24, 40, 88$ and 136.

Proof $\quad n = 2q + 2 = 2(q + 1)$

- $\mathrm{Aut}(C) = \mathrm{diag}(\mathrm{PSL}(2, q) \times \mathrm{PSL}(2, q)) \times C_2$

- Argument similar to the QR case

Methods for smaller primes

Proposition

Suppose that $C = C^{\perp}$ and $\sigma \in \mathrm{Aut}(C)$ of prime order $p \neq 2$. If $s(p)$ is even, then c is even.

Proof: $K^n = \underbrace{K[\sigma] \oplus \ldots \oplus K[\sigma]}_{c} \oplus \underbrace{k \oplus \ldots \oplus K}_{f}$

- There is an irreducible $K[\sigma]$-module $V \cong V^* \neq 1$.
- The multiplicity of V in $K[\sigma]$ is equal to c.
- $K^n/C \cong C^*$

Example (Javier de la Cruz)

Possible primes p in the automorphism group of a putative self-dual $[120, 60, 24]$ code are:

2, 3, 5, 7, 19, 29

13 and 17 are excluded by the proposition above:

$s(13) = 12$ even, $c = 8$ (9 not allowed, 10 too big), thus $f = n - cp = 16 > 8$, a contradiction.