Notes on automorphisms of extremal codes

Stefka Bouyuklieva and Wolfgang Willems

ACCT, Pamporovo, Bulgaria, 16.6.-22.6.2008

Problem

What are the binary extremal self-dual doubly-even codes?

extremal: $d = 4\lfloor \frac{n}{24} \rfloor + 4$

stick to the case: **n=24m**

Zhang: $n \leq 3672$ or $m \leq 153$

known examples

$m = 1$	$[24, 12, 8]$	Golay code,	M_{24}
$m = 2$	$[48, 24, 12]$	quadratic residue code,	$\mathrm{PSL}(2, 47)$
$m = 3$	$[72, 36, 16]$	?????	
$m = 4$	$[96, 48, 20]$	?????	

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

- if $\mathrm{Aut}(C)$ is nontrivial, it may help to construct the code

- if $\mathrm{Aut}(C)$ is trivial, C has no structure, it's only a combinatorial object

Theorem (Bouyuklieva, O'Brien, Willems)

The automorphism group of a putative self-dual doubly-even $[72, 36, 16]$ code has order

5, 7, 10, 14, $d \mid 24$ or $d \mid 36$.

(the group is solvable, primes involved are: $2, 3, 5, 7$)

Theorem (Dontcheva, Yorgov)

If the prime p divides the order of the automorphism group of a putative self-dual doubly-even $[96, 48, 20]$ code then

$p = 2, 3$ or 5.

Conjecture

Let C be a self-dual doubly-even $[24m, 12m, 4m+4]$ code. If p is a prime with $p \geq \frac{n}{2} = 12m$ then

$$p \not| \, |\mathrm{Aut}(C)| \qquad \text{for } m > 2$$

Warning: This is wrong for $m = 1$ and $m = 2$.

Definition

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: $\quad n = cp + f$

Proposition

If $m > 2$ and $\sigma \in \mathrm{Aut}(C)$ of type $p - (c, f)$ then $c \geq f$.

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

Corollary

If $p \geq \frac{n}{2} = 12m$ then $p = n - 1 = 24m - 1$

Proof σ is of type $p - (1, 1)$

Example

- $[24, 12, 8]$ Golay code σ of order 23
- $[48, 24, 12]$ QR code σ of order 47
- $[72, 36, 16]$???? no σ of prime order > 7
- $[96, 48, 20]$???? no σ of prime order > 5

In order to prove the **Conjecture** we have to show:

if $n-1 = 24m-1 = p$ is a prime and $\sigma \in \mathrm{Aut}(C)$ of order p then C is not extremal

where $m = 3, 4, \ldots, 153$

Remark

For $m = 4, 5, 6, 9, 12, 14, ..., 148, 149, 150, 152$

$24m-1$ is not a prime, and we are done

Definition

For an odd prime p let $s(p)$ denote the smallest natural number s.t. $p \mid 2^{s(p)} - 1$.

Clearly, $s(p) \mid p - 1$ by the little Fermat

Lemma

If there exists $\sigma \in \mathrm{Aut}(C)$ of odd prime order $p \geq \frac{n}{2} = 12m$ then $s(p)$ is odd.

Proof

- $\left(\frac{2}{p}\right) = 1$ since $p = 24m - 1 \equiv -1 \bmod 8$
- $2^{\frac{p-1}{2}} \equiv 1 \bmod p$, hence $s(p) \mid \frac{p-1}{2}$
- $8 \mid 24m = p + 1$, hence $\frac{p-1}{2}$ odd

Proposition

If $\sigma \in \mathrm{Aut}(C)$ of prime order $p = n - 1 = 24m - 1$ and $s(p) = \frac{p-1}{2}$ 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 $s(P) = \frac{p-1}{2}$

$V \ncong V^{*} = W$ since $s(p)$ odd

Looking at the list

$m = 3, 4, 5, \ldots, 153$

$p = 24m - 1$ is a prime only in 64 cases of m

$s(p)$ always odd

$s(p) = \frac{p-1}{2}$ unless $m = 18, 36, 46, 98, 112, 133$

Warning. There is no way to compute the minimum distance for a QR code of length larger than 600.

But there is an algorithm of MacWilliams-Karlin to find codewords of small weight if $s(p) = \frac{p-1}{2}$ splits

Computations have been done independently by O'Brien (Auckland) and partly by Malevich (Minsk).

m	$p = 24m - 1$	$s(p)$	$4m + 4$	wt found	Ref	ifactor (p-1)/2
1	23	$*$	8	8		11
2	47	$*$	12	12		23
3	71	$*$	16	12		$5 \cdot 7$
7	167	$*$	32	24	Leon	83
8	191	$*$	36	28	Leon	$5 \cdot 19$
10	239	$*$	44	32	Leon	$7 \cdot 17$
11	263	$*$	48	36	Leon	131
13	311	$*$	56	36	Leon	$5 \cdot 31$
15	359	$*$	64	40	Leon	179
16	383	$*$	68	48	Leon	191
18	431	43	76	48	Leon	$5 \cdot 43$
20	479	$*$	84	56	Leon	239
21	503	$*$	88	56	Leon	251
25	599	$*$	104	80	KMW	$13 \cdot 23$
27	647	$*$	112	104	KMW	$17 \cdot 19$
30	719	$*$	124	?	Leon*	359

m	$p=24m-1$	$s(p)$	$4m+4$	wt found	Ref	ifactor (p-1)/2
31	743	$*$	128	108	KMW	$7 \cdot 53$
35	839	$*$	144		Leon*	419
36	863	$*$	148			431
37	887	$*$	152			443
38	911	91	156			$5 \cdot 7 \cdot 13$
41	983	$*$	168			491
43	1031	$*$	176		KMW	$5 \cdot 103$
46	1103	29	188			$19 \cdot 29$
48	1151	$*$	196	184	KMW	$5 \cdot 5 \cdot 23$
51	1223	$*$	208	96	KMW	$13 \cdot 47$
55	1319	$*$	224			659
57	1367	$*$	232			683
60	1439	$*$	244			719
62	1487	$*$	252			743

m	$p = 24m - 1$	$s(p)$	$4m + 4$	wt found	Ref	ifactor (p-1)/2
63	1511	$*$	256		KMW	$5 \cdot 151$
65	1559	$*$	264	228	KMW	$19 \cdot 41$
66	1583	$*$	268		KMW	$7 \cdot 113$
67	1607	$*$	272	244	KMW	$11 \cdot 73$
76	1823	$*$	308			911
77	1847	$*$	312	300	KMW	$13 \cdot 71$
78	1871	$*$	316	308	KMW	$5 \cdot 11 \cdot 17$
85	2039	$*$	344			1019
86	2063	$*$	348			1031
87	2087	$*$	352	300	KMW	$7 \cdot 149$
88	2111	$*$	356		KMW	$5 \cdot 211$
92	2207	$*$	372			1103
98	2351	47	396			$5 \cdot 5 \cdot 47$

m	$p = 24m - 1$	$s(p)$	$4m + 4$	wt found	Ref	ifactor(p-1)/2
100	2399	$*$	404		KMW	$11 \cdot 109$
101	2423	$*$	408	348	KMW	$7 \cdot 173$
102	2447	$*$	412			1223
106	2543	$*$	428	412	KMW	$31 \cdot 41$
108	2591	$*$	436	372	KMW	$5 \cdot 7 \cdot 37$
111	2663	$*$	448		KMW	$11 \cdot 11 \cdot 11$
112	2687	79	452			$17 \cdot 79$
113	2711	$*$	456		KMW	$5 \cdot 271$
120	2879	$*$	484			1439
121	2903	$*$	488			1451
122	2927	$*$	492	420	KMW	$7 \cdot 11 \cdot 19$
125	2999	$*$	504			1499
126	3023	$*$	508			1511
130	3119	$*$	524			1559

m	$p = 24m - 1$	$s(p)$	$4m + 4$	wt found	Ref	ifactor(p-1)/2
132	3167	$*$	532			1583
133	3191	55	536			$5 \cdot 11 \cdot 29$
140	3359	$*$	564	508	KMW	$23 \cdot 73$
142	3407	$*$	572		KMW	$13 \cdot 131$
147	3527	$*$	592	560	KMW	$41 \cdot 43$
151	3623	$*$	608			1811
153	3671	$*$	616			$5 \cdot 367$

State of art for primes $p \geq \frac{n}{2}$

There are 21 out of 153 dimensions left open

Others methods have to come in now.