Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 40-45*

Notes on automorphisms of extremal codes

Stefka Bouyuklieva stefka@uni-vt.bg
Veliko Tarnovo University, 5000 Veliko Tarnovo, BULGARIA,

Wolfgang Willems wolfgang.willems@mathematik.uni-magdeburg.de
Otto-von-Guericke Universität, 39016 Magdeburg, GERMANY

Abstract. We prove that if a putative extremal self-dual $[24m, 12m, 4m+4]$ code has an automorphism of odd prime order p with c cycles and f fixed points then $c \geq f$. In case $p > 12m$ the results we have obtained so far give some evidence that m must be 1 or 2.

1 Introduction

Let C be an extremal (doubly-even) self-dual $[24m, 12m, 4m+4]$ binary code. By the results of Zhang [9], we know that $m \leq 153$. However, the existence of such codes is proved only for $m = 1$ and $m = 2$, and in these cases we have the extended $[24, 12, 8]$ Golay code with automorphism group M_{24} and the extended quadratic residue code $[48, 24, 12]$ with automorphism group $\mathrm{PSL}(2, 47)$. In [1] we proved that the automorphism group of a binary self-dual doubly-even $[72, 36, 16]$ code is a solvable group of order $5, 7, 10, 14, 56$, or a divisor of 72.

Here we investigate primes which may occur in the order of the automorphism group $G = \mathrm{Aut}(C)$ and the cycle structure of permutations in G. Let $\sigma \in G$ be a permutation of order p where p is an odd prime. The action of σ on the positions produces, say c cycles of length p and f fixed points and in this case we call σ of type $p-(c,f)$. In Section 2 we prove that $c \geq f$ for any automorphism of C of order p. In Section 3 we investigate the possibility $c = f = 1$.

2 The main result

First we consider the case $p = 3$. Let C be a binary self-dual code of length n with an automorphism σ of order 3 with exactly c independent 3-cycles and $f = n - 3c$ fixed points in its factorization. Let $\sigma = \Omega_1\Omega_2\ldots\Omega_c$, where $\Omega_1, \Omega_2, \ldots, \Omega_c$, are independent cycles of length 3. Two particular subcodes of C play an important role in the following investigations.

Let $F_\sigma(C) = \{v \in C : v\sigma = v\}$. Clearly, $v \in F_\sigma(C)$ iff $v \in C$ is constant on each cycle. Let $\pi : F_\sigma(C) \to \mathbb{F}_2^{c+f}$ be the projection map where if $v \in F_\sigma(C)$ then $(v\pi)_i = v_j$ for some $j \in \Omega_i, i = 1, 2, \ldots, c+f$.

We consider furthermore the vector space

$$E_\sigma(C) = \{v \in C : wt(v|\Omega_i) \equiv 0 \pmod 2, i = 1, \ldots, c, v_j = 0, j = 3c{+}1, \ldots, n\},$$

where $v|\Omega_i$ denotes the restriction of v on Ω_i. Let P be the set of even-weight polynomials in $\mathbb{F}_2[x]/(x^3+1)$, and let $v|\Omega_i = (v_0, v_1, v_2)$ correspond to the polynomial $v_0 + v_1 x + v_2 x^2$ of P for $i = 1, \ldots, c$. Thus we obtain a natural map $\phi : E_\sigma(C)^* \to P^c$. In our particular case, $P = \{0, e = x + x^2, xe, x^2 e\} \cong \mathbb{F}_4$.

Theorem 1 [2] *A binary code C with an automorphism σ is self-dual if and only if the following two conditions hold.*

(i) *$C_\pi = \pi(F_\sigma(C))$ is a self-dual binary code of length $c+f$;*

(ii) *$C_\phi = \phi(E_\sigma(C))$ is a Hermitian quaternary self-dual code of length c over the field $P \cong \mathbb{F}_4$.*

For the minimum distance of the quaternary Hermitian self-dual codes we have the following bound.

Theorem 2 [5] *If C is an $[n, n/2, d]$ Hermitian self-dual code over $\mathbb{F}_4$, then*

$$d \leq 2\lfloor n/6 \rfloor + 2.$$

Using the above theorems we obtain

Corollary 3 *If C is an extremal binary self-dual $[24m, 12m, 4m+4]$ code and σ is an automorphism of C of type $3-(c,f)$ then $c \geq f$.*

Proof: By Theorem 1, C_ϕ must be a Hermitian quaternary self-dual code of length c over the field $P \cong \mathbb{F}_4$. Since $d(C) = 4m+4$, the minimum distance of C_ϕ cannot be less than $2m+2$. By Theorem 2, $2m+2 \leq 2\lfloor c/6 \rfloor + 2 \leq 2c/6 + 2$, hence $c \geq 6m$. It follows that $f = 24m - 3c \leq 24m - 18m = 6m \leq c$. □

To restrict the possible automorphisms for particular codes we need the following theorem.

Theorem 4 [8] *Let C be a binary self-dual $[n, k, d]$ code and let $\sigma \in \mathrm{Aut}(C)$ be of type $p-(c,f)$, where p is an odd prime. If $g(s) = \sum_{i=0}^{s-1} \lceil \frac{d}{2^i} \rceil$ then*

(i) *$pc \geq g(\frac{p-1}{2}c)$ and*

(ii) *$f \geq g(\frac{f-c}{2})$ for $f > c$.*

Now let $n = 24m$ and $d = 4m + 4$. Then $g(1) = 4m + 4$, $g(2) = 6m + 6$, $g(3) = 7m + 7$, and for $s \geq 4$ we have

$$g(s) = \sum_{i=0}^{s-1} \left\lceil \frac{4m+4}{2^i} \right\rceil = 7m + 7 + \sum_{i=3}^{s-1} \left\lceil \frac{4m+4}{2^i} \right\rceil = 7m + 7 + \sum_{i=1}^{s-3} \left\lceil \frac{m+1}{2^i} \right\rceil.$$

If $2^l < m + 1 \leq 2^{l+1}$ for $l \in \mathbb{N}_0$ then

$$g(s) \geq 7m + 7 + \sum_{i=1}^{s-3} \frac{m+1}{2^i} = 7m + 7 + (m+1)\frac{2^{s-3}-1}{2^{s-3}} = (m+1)\frac{2^s - 1}{2^{s-3}}.$$

For $i > l$ we have $\frac{m+1}{2^i} < 2^{l+1-i} \leq 1$ and therefore $\lceil \frac{m+1}{2^i} \rceil = 1$. Hence for $s - 3 > l$ the following inequality holds

$$g(s) = g(l+3) + s - 3 - l \geq \left(8 - \frac{1}{2^l}\right)(m+1) - l - 3 + s = A + s$$

Using the above inequalities and Theorem 4 we prove the main result

Main Theorem 5 *If C is an extremal self-dual $[24m, 12m, 4m + 4]$ code and σ is an automorphism of C of type $p - (c, f)$, where p is an odd prime, then $c \geq f$.*

Proof: By Corollary 3, we may assume that $p \geq 5$. Suppose that $f > c$. We know that this is impossible if $m \leq 3$. Let $m \geq 4$, hence $l \geq 2$. By Theorem 4, we have the following inequalities

$$pc \geq g\Big(\frac{p-1}{2}c\Big) \quad \text{and} \quad f \geq g\Big(\frac{f-c}{2}\Big)$$

(a) We claim $\frac{p-1}{2}c > l + 3$: If $\frac{p-1}{2}c \leq l + 3$ then $c \leq \frac{2(l+3)}{p-1} \leq \frac{20}{p-1}$ since by Zhang, $m \leq 153$, hence $l \leq 7$. This inequality is possible only in the following cases: $p = 5, c \leq 5$; $p = 7$, $c \leq 3$; $p = 11$, $c \leq 2$; $p = 13, 17, 19$, $c = 1$. But for $p \geq 5$ we have $pc \geq g(\frac{p-1}{2}c) \geq g(2) = 6(m+1) \geq 30$ which does not hold in all cases.

(b) We claim $\frac{f-c}{2} > l + 3$: If $\frac{f-c}{2} \leq l + 3$ then $f - c \leq 20$ and so $f \leq 21$. But $f \geq g(\frac{f-c}{2}) \geq g(1) = 4(m+1) \geq 20$, a contradiction.

As $f = 24m - pc$ we obtain, by (a) and (b), that

$$pc \geq A + \frac{p-1}{2}c \quad \text{and} \quad 24m - pc \geq A + 12m - \frac{(p+1)c}{2},$$

hence $\frac{2A}{p+1} \leq c \leq \frac{24m-2A}{p-1}$ and therefore $A(p-1) \leq (12m-A)(p+1)$ or

$(2A - 12m)p \leq 12m$. Since

$$\begin{array}{rcl} A - 6m & = & (8 - \frac{1}{2^l})(m+1) - l - 3 - 6m \\ & \geq & (8 - \frac{1}{4})(m+1) - l - 3 - 6m = \frac{1}{4}(7m + 19 - 4l) > 0 \end{array}$$

we get $\quad p \leq \dfrac{6m}{A-6m} \leq \dfrac{24m}{7m+19-4l} \leq \dfrac{24m}{7(m-(4l-19)/7)}, \quad$ hence

$$p \leq \frac{24}{7} + \frac{24}{7}\frac{(4l-19)}{(7m-4l+19)} \leq \frac{24}{7} + \frac{24}{7}\frac{9}{(7m-9)} \leq \frac{24}{7} + \frac{24.9}{7.19} = \frac{96}{19} < 6.$$

Thus $p = 5$ and moreover by (a), we have $5c \geq g(2c) \geq A + 2c$, hence $3c \geq A$. The inequality $f = 24m - 5c > c$ implies $c < 4m$. Furthermore, $f = 24m - 5c \geq g(12m - 3c)$. Since $12m - 3c > l + 3$, by (b), we have $24m - 5c \geq A + 12m - 3c$, hence $(12 - a)m - b \geq 2c \geq \frac{2}{3}(am + b)$, where $a = 8 - \frac{1}{2^l}$, $b = a - l - 3$, $A = am + b$. Hence $(36 - 5a)m \geq 5b$ and therefore $(36 - 40 + 5/2^l)m \geq 5(5 - l) - 5/2^l$ which implies $(4.2^l - 5)m \leq 5.2^l(l - 5) + 5$, a contradiction. This proves that $c \geq f$. □

3 Automorphisms of prime order $p > 12m$

Now suppose that $p > \frac{n}{2} = 12m$. Thus, by Theorem 5, σ is of type $p - (1,1)$. Hence $n = 24m = p + 1$, and in particular $p \equiv -1 \bmod 8$. The later yields that $\frac{p-1}{2}$ is odd. As usual let $s(p)$ denote the smallest number $s \in \mathbb{N}$ such that $p \mid 2^s - 1$.

Lemma 6 *For $p > \frac{n}{2} = 12m$ we have $s(p)$ odd.*

Proof: Since $p \equiv -1 \bmod 8$ the prime 2 is a square mod p. This yields that $2^{\frac{p-1}{2}} \equiv 1 \bmod p$. As $s(p) \mid \frac{p-1}{2}$ and $\frac{p-1}{2}$ is odd the proof is complete. □

Lemma 7 *For the group algebra $\mathbb{F}_2\langle\sigma\rangle$, the trivial module is the only irreducible self-dual module.*

Proof: By Lemma 6, we know that $s(p)$ is odd. The assertion now follows directly by Theorem 2.7 of [7]. □

Using Maple we easily find all primes p of the form $2m - 1$ for $m \leq 153$. It turns out that apart from six primes, we always have $s(p) = \frac{p-1}{2}$.

Theorem 8 *Apart from the six exceptions C is an extended* QR *code.*

Proof: Let $K = \mathbb{F}_2$. The ambient space K^n of C can be written as

$$K^n = K\langle\sigma\rangle \oplus K.$$

Since $s(p) = \frac{p-1}{2}$ the non-trivial irreducible $K\langle\sigma\rangle$-modules are of dimension $\frac{p-1}{2}$. Thus by Maschke, we have the decomposition

$$(*) \qquad K\langle\sigma\rangle = K \oplus V \oplus W$$

with irreducible modules V and W both of dimension $s(p) = \frac{p-1}{2}$. By Lemma 7, we have $V \not\cong V^*$ and $W \not\cong W^*$. Since a group algebra is always selfdual we obtain $W \cong V^*$. Furthermore, the decomposition in $(*)$ is unique since the three modules are non-isomorphic. On the other hand, we know that

$$K\langle\sigma\rangle = K \oplus Q \oplus N$$

where Q is the code associated to the squares mod p and N to the non-squares. Since Q is equivalent to N we may assume that $V = Q$. Finally, if C_0 is the subspace of C with 0 in the last position then $C = \langle C_0, c\rangle$ where c is the all one word. This shows that C is an extended QR code. $\square$

Problem 9 Is an extended QR of length $p + 1 = 24m$ extremal only for $m = 1$ and $m = 2$?

By known results [4], this is true for $m \leq 21$. But we have to check up to $m = 153$. Fortunately, we do not need to compute the minimum distance in these remaining cases. Instead we only have to find a codeword of weight smaller than $4m + 4$. Apart from the largest case, i.e. $m = 153$, this is always possible if $s(p) = \frac{p-1}{2}$ splits up into a nontrivial product of primes which holds true in about half of the cases we have to consider. Here the Karlin-MacWilliams algorithm (see [3] or [6], chap. 16, section 6) is applicable and the computations have been done partly by Malevich (Minsk) and independently by O'Brien (Auckland). In the other half of cases in which $s(p) = \frac{p-1}{2}$ is a prime the Karlin-MacWilliams algorithm does not work and further theoretical investigations are needed to answer Problem 9.

Summarizing the above theoretical and computational results there is some evidence to

Conjecture 10 *If a binary extremal code C of length $24m$ has an automorphism of prime order $p > 12m$ then $m = 1$ or $m = 2$.*

References

[1] S. Bouyuklieva, E. A. O'Brien, W. Willems, The automorphism group of a binary self-dual doubly even $[72, 36, 16]$ code is solvable, *IEEE Trans. Inform. Theory* 52, 2006, 4244-4248.

[2] W. C. Huffman, Automorphisms of codes with application to extremal doubly-even codes of lenght 48, *IEEE Trans. Inform. Theory* 28, 1982, 511-521.

[3] M. Karlin, F. J. MacWilliams, On finding low weight vectors in quadratic residue codes for $p = 8m - 1$, *SIAM J. Appl. Math.* 25, 1973, 95-104.

[4] J. S. Leon, A probabilistic algorithm for computing the minimum weights of large error-correcting codes, *IEEE Trans. Inform. Theory* 34, 1988, 1354-1359.

[5] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, H. N. Ward, Self-dual codes over $GF(4)$, *J. Combin. Theory*, Series A25, 1978, 288-318.

[6] F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North Holland, Amsterdam 1977.

[7] C. Martínez-Pérez, W. Willems, Self-dual extended cyclic codes, *Appl. Algebra Eng. Comm. Computing* 17, 2006, 1-16.

[8] V. Y. Yorgov, A method for constructing inequivalent self-dual codes with applications to length 56, *IEEE Trans. Inform. Theory* 33, 1987, 77-82.

[9] S. Zhang, On the nonexistence of extremal self-dual codes, *Discr. Math.*, 91, 1999, 277-286.