An extremal [72,36,16] binary code has no automorphism group containing $Z_2 \times Z_4$, Q_8, or Z_{10}.

Gabriele Nebe[1]

ABSTRACT. Let C be an extremal self-dual binary code of length 72 and $g \in \mathrm{Aut}(C)$ be an automorphism of order 2. We show that C is a free $\mathbb{F}_2\langle g\rangle$ module and use this to exclude certain subgroups of order 8 of $\mathrm{Aut}(C)$. We also show that $\mathrm{Aut}(C)$ does not contain an element of order 10. Combining these results with the ones obtained in earlier papers we find that the order of $\mathrm{Aut}(C)$ is either 5 or divides 24. If 8 divides the order of $\mathrm{Aut}(C)$ then its Sylow 2-subgroup is either D_8 or $Z_2 \times Z_2 \times Z_2$.
Keywords: extremal self-dual code, automorphism group
MSC: primary: 94B05

1 Introduction.

Let $C = C^{\perp} \leq \mathbb{F}_2^n$ be a binary self-dual code. Then the invariance properties of the weight enumerator of C and its shadow may be used to obtain an upper bound for the minimum distance

$$d(C) := \min\{\mathrm{wt}(c) \mid 0 \neq c \in C\}, \text{ where } \mathrm{wt}(c) := |\{i \mid c_i \neq 0\}|;$$

$d(C) \leq 4\lfloor \frac{n}{24} \rfloor + 4$ unless $n \equiv_{24} 22$ where the bound is $4\lfloor \frac{n}{24} \rfloor + 6$ (see [11]). Codes achieving equality are called extremal. Of particular interest are extremal codes of length $24k$. For $n = 24$ and $n = 48$ there are unique extremal codes [9], both are extended quadratic residue codes. For $n = 72$ the extended quadratic residue code fails to be extremal and no extremal code of length 72 is known. One frequently used method to search for an extremal code is to investigate codes which are invariant under a certain subgroup of the symmetric group S_n. For $n = 72$ it has been shown in a series of papers that the automorphism group

$$\mathrm{Aut}(C) := \{\sigma \in S_n \mid \sigma(C) = C\}$$

of an extremal code is either Z_5 or Z_{10} or its order divides 24 (for more details and references see [8]). This paper introduces a new method and excludes the cases that $\mathrm{Aut}(C)$ contains a quaternion group of order 8, the cyclic group Z_{10}, or the group $Z_4 \times Z_2$. It also provides a new proof that $\mathrm{Aut}(C)$ does not contain an element of order 8.

2 Indecomposable modules for cyclic groups.

The main result from modular representation theory that we use in this note is the classification of indecomposable $\mathbb{F}G$-modules for cyclic p-groups G over a field $\mathbb{F}$ of characteristic p. By

[1]Lehrstuhl D für Mathematik, RWTH Aachen University, 52056 Aachen, Germany, nebe@math.rwth-aachen.de

the theorem of Krull Schmidt any $\mathbb{F}G$-module is up to isomorphism a unique direct sum of indecomposable modules.

Theorem 2.1. *(see for instance [2, pp 24,25]) Let $G = \langle g \rangle$ be a cyclic group of order $q := p^a$ and $\mathbb{F}$ a field of characteristic p. Then the group ring $\mathbb{F}G$ is isomorphic to $R := \mathbb{F}[X]/(X^q)$ via $g \mapsto X+1$. This ring R is a uniserial ring with ideals (X^i), $0 \le i \le q$. All indecomposable R-modules are the factor modules $V_i := R/(X^i)$ for $1 \le i \le q$. The module $V_1 \cong S$ is the simple $\mathbb{F}G$-module and $V_q = R$ is the free module of rank 1.*

Corollary 2.2. *Let G be a cyclic p-group and M an $\mathbb{F}_pG$-module. Then M is projective if and only if M is free if and only if the restriction of M to the subgroup of order p is free.*

There are not many groups where such a strong criterion holds. One other group is the quaternion group Q_8 of order 8. More precisely [6] shows the following.

Lemma 2.3. *Let $G = Q_8$ be the quaternion group of order 8 and $Z := Z(G)$ the center of G, of order 2. Let M be an $\mathbb{F}_2G$-module. Then M is free as an $\mathbb{F}_2G$-module if and only if M is free as an $\mathbb{F}_2Z$-module.*

3 The main result.

Throughout this section let $C = C^\perp \le \mathbb{F}_2^{72}$ be a self-dual code with minimum distance $d(C) = 16$ and $g \in \mathrm{Aut}(C)$ be an automorphism of order 2. By [5] the permutation g has no fixed points, so we may assume that $g = (1,2)(3,4)\dots(71,72)$. Let

$$C(g) := \{c \in C \mid g(c) = c\} = \{c = (c_1, c_1, c_2, c_2, \dots, c_{36}, c_{36}) \in C\}$$

be the fixed code of g. Define two mappings

$$\begin{array}{ll} \pi : C(g) \to \mathbb{F}_2^{36}, & (c_1, c_1, c_2, c_2, \dots, c_{36}, c_{36}) \mapsto (c_1, \dots, c_{36}) \\ \Phi : C \to \mathbb{F}_2^{36}, & (c_1, \dots, c_{72}) \mapsto (c_1 + c_2, c_3 + c_4, \dots, c_{71} + c_{72}). \end{array}$$

Then $\Phi(C) \subseteq \pi(C(g)) = \Phi(C)^\perp$ (see [4]).

Theorem 3.1. *Let g be an automorphism of order 2 of an extremal self-dual code C of length 72. Then C is a free $\mathbb{F}_2\langle g \rangle$-module and $\pi(C(g)) = \Phi(C)$ is a self-dual $[36, 18, 8]$ binary code.*

Proof. We consider C as a module for the group algebra $R := \mathbb{F}_2\langle g \rangle$. By Theorem 2.1 the ring R has up to isomorphism two indecomposable modules, the free module R and the simple module $S \cong \mathbb{F}_2$. The module C has $\mathbb{F}_2$-dimension 36 and hence is of the form $C \cong R^a \oplus S^{36-2a}$. Clearly the fixed code $C(g)$ is the socle of this module; $C(g) = \mathrm{soc}(C) \cong S^a \oplus S^{36-2a}$ of dimension $36 - a$. So $\pi(C(g)) \le \mathbb{F}_2^{36}$ has dimension $36 - a$ and the minimum distance is $d(\pi(C(g))) \ge \frac{d(C)}{2} = 8$. By the above $\pi(C(g)) = \Phi(C)^\perp \ge \Phi(C)$ is the dual of a self-orthogonal code and hence contains some self-dual code $D = D^\perp \le \mathbb{F}_2^{36}$ of minimum distance

≥ 8. By [1] there are 41 such codes. With Magma [3] one checks that no proper overcode of these 41 codes has minimum distance ≥ 8, so $\dim(C(g)) = 18$ and hence $a = 18$. Therefore $C \cong R^{18}$ is a free $\mathbb{F}_2\langle g\rangle$-module and $\pi(C(g))$ is one of these 41 extremal self-dual codes. □

The first corollary also follows from the Sloane-Thompson theorem (see [12], [10]) since any extremal code of length $24k$ is doubly even (see [11]):

Corollary 3.2. *Let $C = C^\perp$ be an extremal code of length 72. Then $\mathrm{Aut}(C)$ does not contain an element of order 8.*

Proof. Assume that there is some $\sigma \in \mathrm{Aut}(C)$ of order 8. Since C is free as a module over $\mathbb{F}_2\langle\sigma^4\rangle$ by Theorem 3.1, Corollary 2.2 says that C is a free $\mathbb{F}_2\langle\sigma\rangle$-module; so $C \cong \mathbb{F}_2\langle\sigma\rangle^a$ with $8a = \frac{72}{2} = \dim(C)$. Thus $a = 9/2$, a contradiction. □

Corollary 3.3. *Let $C = C^\perp$ be an extremal binary code of length 72. Then $\mathrm{Aut}(C)$ does not contain a quaternion group of order 8.*

Proof. Assume that there is some subgroup $G \leq \mathrm{Aut}(C)$ such that G is isomorphic to the quaternion group of order 8. Let $Z := Z(G)$ be the center of G. This is a group of order 2 and so by Theorem 3.1 the code C is a free $\mathbb{F}_2Z$-module. By Lemma 2.3 this implies that C is also a free $\mathbb{F}_2G$ module of rank $\dim(C)/8 = 9/2$, which is absurd. □

Corollary 3.4. *Let $C = C^\perp$ be an extremal binary code of length 72. Then $\mathrm{Aut}(C)$ does not contain a subgroup $Z_4 \times Z_2$.*

Proof. Assume that $U \cong Z_4 \times Z_2 = \langle h, g\rangle$ is a subgroup of $\mathrm{Aut}(C)$ such that $g^2 = h^4 = 1$. Since any element of order 2 in U acts fixed point freely on $\{1, \ldots, 72\}$, the group U acts freely on this set and $\langle h\rangle \cong Z_4$ acts freely on the set of $\langle g\rangle$-orbits. Therefore h acts as a permutation with nine 4-cycles on the the fixed code $C(g)$. A Magma computation shows that none of the 41 self-dual $[36, 18, 8]$ codes from [1] has such an automorphism. □

The following corollary summarizes these three results.

Corollary 3.5. *Let $C = C^\perp$ be an extremal binary code of length 72. If 8 divides $|\mathrm{Aut}(C)|$ then the Sylow 2-subgroup of $\mathrm{Aut}(C)$ is either $Z_2 \times Z_2 \times Z_2$ or D_8.*

Corollary 3.6. *Let $C = C^\perp$ be an extremal binary code of length 72. Then $\mathrm{Aut}(C)$ does not contain an element of order 10.*

Proof. By [7] any element of order 5 in $\mathrm{Aut}(C)$ has fourteen 5-cycles and two fixed points. If there is some $\sigma \in \mathrm{Aut}(C)$ with order 10, then σ^2 acts on the fixed code $C(\sigma^5)$ of the element of order 2 as a permutation with seven 5-cycles and one fixed point. A Magma computation shows that none of the 41 self-dual $[36, 18, 8]$ codes from [1] has such an automorphism of order 5. This is shown independently in [13]. □

Acknowledgement. All computations have been done in Magma [3].

References

[1] C. Aguilar Melchor, P. Gaborit, On the classification of extremal $[36, 18, 8]$ binary self-dual codes. IEEE Trans. Inform. Theory 54 (2008) 4743-4750.

[2] J.L. Alperin, Local representation theory. Cambridge Studies in Advanced Mathematics, 11. Cambridge University Press, Cambridge, 1986.

[3] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language. J. Symbolic Comput., 24 (1997) 235-265.

[4] S. Bouyuklieva, A method for constructing self-dual codes with an automorphism of order 2. IEEE Trans. Inform. Theory 46 (2000) 496-504.

[5] S. Bouyuklieva, On the automorphisms of order 2 with fixed points for the extremal self-dual codes of length 24m. Designs, Codes, Cryptography 25 (2002) 5-13.

[6] J.F. Carlson, Free modules over some modular group rings. J. Austral. Math. Soc. Ser. A 21 (1976) 49-55.

[7] J.H. Conway, V. Pless, On primes dividing the group order of a doubly-even (72, 36, 16) code and the group order of a quaternary (24, 12, 10) code. Discrete Math. 38 (1982) 143-156.

[8] T. Feulner, G. Nebe, The automorphism group of a self-dual binary $[72, 36, 16]$ code does not contain Z_7, $Z_3 \times Z_3$, or D_{10}. (submitted)

[9] S.K. Houghten, C.W.H. Lam, L.H. Thiel, J.A. Parker, The extended quadratic residue code is the only $(48, 24, 12)$ self-dual doubly-even code. IEEE Trans. Inform. Theory 49 (2003) 53-59.

[10] A. Günther, G. Nebe, Automorphisms of doubly even self-dual binary codes. Bull. Lond. Math. Soc. 41 (2009) 769-778.

[11] E.M. Rains, Shadow bounds for self-dual codes. IEEE Trans. Inform. Theory 44 (1998) 134-139.

[12] N.J.A. Sloane, J.G. Thompson, Cyclic self-dual codes. IEEE Trans. Inform. Theory 29 (1983) 364-366.

[13] N. Yankov, V.V. Yorgov, On the extremal binary codes of lengths 36 and 38 with an automorphism of order 5. Proc. of the 5th Int. workshop on Algebraic and Combinatorial Coding Theory (Sozopol, Bulgaria) June 1-7 1996, 307-312.