On the classification of the extremal self-dual codes over small fields with 2-transitive automorphism groups

Anton Malevich and Wolfgang Willems

Department of Mathematics
Otto-von-Guericke University Magdeburg
39016 Magdeburg, Germany
malevich@ovgu.de, willems@ovgu.de

Abstract. There are seven binary extremal self-dual doubly-even codes which are known to have a 2-transitive automorphism group. Using representation theoretical methods we show that there are no other such codes, except possibly for length $n = 1\,024$. We also classify all extremal ternary self-dual and quaternary Hermitian self-dual codes.

Keywords: Automorphisms, Self-dual codes, Transitive groups, Simple groups

MSC: 94B05, 20B20, 20B25

1 Introduction

A binary self-dual linear code is called doubly-even if all of its weights are divisible by 4. By a result of Gleason [5], the length n of a self-dual doubly-even code is a multiple of 8. Mallows and Sloane proved in [10] that the minimum distance d of a self-dual doubly-even code is bounded by

$$d \leq 4 \left\lfloor \frac{n}{24} \right\rfloor + 4. \tag{1}$$

Codes achieving this bound are called extremal. Due to Zhang [15] extremal codes can only exist up to the length $n = 3928$.

But there is a huge gap between Zhang's bound and what actually has been constructed so far. Extremal codes are only known for the following lengths:

$$8, 16, 24, 32, 40, 48, 56, 64, 80, 88, 104, 112 \text{ and } 136.$$

A promising approach to the problem whether an extremal code C of a given length exists is to assume the invariance of C under some nontrivial automorphism and then to try either to construct such a code or to prove its nonexistence.

In this paper we assume that the automorphism group of an extremal code acts 2-transitively. Among the known codes there are exactly seven which satisfy this condition. The first six are extended quadratic residue codes of lengths $n = 8$, 24, 32, 48, 80 and 104, which are invariant under the groups $\mathrm{PSL}(2, p)$ with the action on $n = p + 1$ points of the projective line over the finite field with p elements. The seventh code is the second order Reed-Muller code of length 32. Its automorphism group is $\mathrm{AGL}(5, 2)$ with its natural 3-transitive action on 32 points.

The main result of this note is to show that there are no other extremal codes with a 2-transitive automorphism group, except possibly codes of length 1 024 invariant under the group $T \rtimes \mathrm{SL}(2, 2^5)$, where T is elementary abelian of order 2^{10}.

In order to prove this we use the structure of 2-transitive groups to establish which self-dual codes admit such a group as their automorphism group. Then we show that there are no extremal codes among them apart from the mentioned above. This is done with Magma [2] using the following.

Proposition. *Let C be a self-dual doubly-even code of length n and let H be some subgroup of the automorphism group $\mathrm{Aut}(C)$. Furthermore let C^H be the subcode of C consisting of those codewords that are fixed by H, i.e.*

$$C^H = \{c \in C \mid c\sigma = c, \forall \sigma \in H\}.$$

If C^H contains a codeword of weight less than $4\left\lfloor \frac{n}{24} \right\rfloor + 4$, then the code C is not extremal.

Remark. Finding codewords of small weights in codes of length at least 1000 is an almost impossible task even for a fast computer. The method in Proposition however works successfully if $|H|$ is chosen small (in our experience between 4 and 20).

In what follows let C be a binary extremal self-dual doubly-even code of length n. Furthermore we assume that $G = \mathrm{Aut}(C)$ acts 2-transitively on the coordinates. We shall apply the following fact about 2-transitive groups.

Lemma 1 [6]. *Every 2-transitive group has a unique minimal normal subgroup (called the socle), which is either elementary abelian or nonabelian simple.*

For the proof of this and other group theoretical facts, which we freely use in the sequel, we refer the reader to [6, Chapter I, §5 and Chapter II, §§1-3].

2 Codes invariant under extensions of elementary abelian groups

First we consider the case that the socle T of the group G is elementary abelian. Obviously, $n = 2^m$ for some m since n is a multiple of 8. Moreover, G is isomorphic to a subgroup of $\mathrm{AGL}(m, 2)$ and therefore $G = T \rtimes H$ where $H \leq \mathrm{GL}(m, 2)$. In other words, every 2-transitive group G with elementary abelian socle T which occurs as automorphism group of a self-dual doubly-even code is an extension of the group T of order 2^m by a subgroup of $\mathrm{GL}(m, 2)$, acting transitively on $2^m - 1$ points. Thus, in order to proceed with the classification we need information on transitive subgroups of general linear groups which can be found in [7, Ch. XII, 7.5].

First we consider the possibility that H contains a cycle σ of order $2^m - 1$. This is, in fact, the only possibility if m is a prime and $m \leq 11$. (Recall, that extremal codes may exist only for $n \leq 3928$, thus $m \leq 11$.) In this case the self-dual codes in question are extended cyclic codes. Moreover, the automorphism group of such a code contains the group $T \rtimes \langle \sigma \rangle \cong \mathrm{AGL}(1, 2^m)$.

Self-dual codes invariant under $\mathrm{AGL}(1, 2^m)$ are called affine-invariant and can only exist for odd values of m.

Lemma 2 [4]. *Affine-invariant codes are extended cyclic codes of length $n = 2^m$ with m odd.*

There is only one extremal code of length 8 which is affine-invariant, namely the Hamming code. Extremal codes of length 32 are classified (see [11]), and the second order Reed-Muller code is the only affine-invariant among them. By [4], there are three codes of length 128 and 70 codes of length 512 which are invariant under $\mathrm{AGL}(1, 2^m)$. Magma computations show that none of them is extremal.

Due to Zhang's bound the only length that remains to consider is $n = 2^{11} = 2\,048$. Using the method from [4] we establish with Magma that there are exactly 515 617 affine-invariant codes of this length. It turns out that all of them are not extremal.

Next we consider the case $G = T \rtimes H$ where $H \leq \mathrm{GL}(m, 2)$ acts transitively and does not contain a $(2^m - 1)$-cycle. As we mentioned already, this can only happen if m is not a prime. Since m is composite, we may write $m = kr$, for some integers k and r. Then, one of the following possibilities holds for H (see [7, Chapter XII, 7.5]):

(1) $\mathrm{SL}(k, 2^r) \leq H$ for all k and r;
(2) $\mathrm{Sp}(k, 2^r) \leq H$ for even k;

(3) $\mathrm{G}_2(2) \leq H$ for $m = 6$;
(4) $H \cong \mathrm{PSU}(3, 3^2)$ for $m = 6$;
(5) $H \cong \mathrm{A}_6$ for $m = 4$;
(6) $H \cong \mathrm{A}_7$ for $m = 4$.

In order to check whether a group $G = T \rtimes H$ for some H from the above list occurs as an automorphism group of a self-dual code C of length n, we exploit the structure of C and its ambient space $\mathbb{F}_2^n$ as a G-module (here $\mathbb{F}_2$ denotes the binary field). In particular, C is a submodule of $\mathbb{F}_2^n$ of dimension $\frac{n}{2}$. For each H from the above list we construct with Magma all G-modules of dimension $\frac{n}{2}$. Then, for every such submodule C we check whether C is self-dual as a code.

Due to the bound on the length of extremal codes, we only need to consider the cases $m \leq 11$, where $n = 2^m$. If m is even, then the only cases in which there exist $\frac{n}{2}$-dimensional $\mathbb{F}_2G$-modules are for $H \cong \mathrm{SL}(2, 2^r), r = 4, 5$. For $r = 4$ we get more than 50 000 modules, but none of them is a self-dual code. For $r = 5$ the number of modules is even larger and we are unable to find all of them with Magma. However we conjecture that in this case none of the modules is self-dual as a code.

Apart from the case $H \cong \mathrm{SL}(2, 2^5)$ for which we can not prove the desired result, the only group from the list above that admits self-dual codes is $H \cong \mathrm{SL}(3, 2^3)$ for $m = 9 = 3{\cdot}3$. In this case there are exactly three self-dual doubly-even codes of length 512 invariant under $T \rtimes \mathrm{SL}(3, 2^3)$. One of them is the Reed-Muller code which has minimum distance 32 and therefore is not extremal. Using the Proposition stated at the beginning of the paper we see that the other two codes are also not extremal.

As far as the classification of extremal codes with a 2-transitive automorphism group is concerned, we summarize the results of this section in the following

Lemma 3. *Let C be a self-dual extremal code. Then C is invariant under a 2-transitive group with elementary abelian socle if and only if C is one of the following:*

(i) the Hamming code of length 8,
(ii) the second order Reed-Muller code of length 32,
(iii) possibly a code of length 1 024 invariant under the group $T \rtimes \mathrm{SL}(2, 2^5)$, where T is elementary abelian of order 2^{10}.

Based on the results above we like to mention an interesting observation. By Lemma 2 extended cyclic self-dual codes of length $n = 2^m$ are affine-invariant only if m is odd. But even if we drop the requirement that the code is extended cyclic, there are still no self-dual codes invariant under a 2-transitive group with elementary abelian socle for even $m < 10$. Furthermore, for odd m, the only transitive subgroups of $\mathrm{GL}(m, 2)$ apart from the cyclic groups are $\mathrm{SL}(k, 2^r)$, where $m = kr$.

We want to conclude this section with an open problem.

Conjecture. *Let C be a self-dual doubly-even code of length 2^m invariant under a 2-transitive automorphism group G with elementary abelian socle T. Then m is odd and one of the following holds true*

(i) $\mathrm{AGL}(1, 2^m) \leq G$ or
(ii) $T \rtimes \mathrm{SL}(k, 2^r) \leq G$ where $m = kr$.

3 Codes invariant under simple groups

In this section we assume that the socle T of $G = \mathrm{Aut}(C)$ is a simple nonabelian group.

Lemma 4 [3]. *All 2-transitive groups with a simple nonabelian minimal normal subgroup are known.*

Table 1. Simple groups that can occur as a socle of a 2-transitive group with even degree n

T	n	Remarks
A_n	n	
$\mathrm{PSL}(2,q)$	$q+1$	$q>3$ an odd prime power
$\mathrm{PSL}(d,q)$, $d>2$	$(q^d-1)/(q-1)$	
$\mathrm{PSU}(3,q)$	$q+1$	$q>2$
${}^2\mathrm{G}_2(q)$ (Ree)	q^3+1	$q=3^{2a+1}>3$
$\mathrm{PSp}(2d,2)$	$2^{2d-1}+2^{d-1}$	
$\mathrm{PSp}(2d,2)$	$2^{2d-1}-2^{d-1}$	
M_{11} (Mathieu)	12	
M_{12} (Mathieu)	12	
M_{22} (Mathieu)	22	
M_{24} (Mathieu)	24	
$\mathrm{PSL}(2,8)$	28	
HS (Higman-Sims)	176	
Co_3 (Conway)	276	

Cameron lists all simple nonabelian groups T that can occur as a socle of a 2-transitive group in [3]. For reader's convenience we list in Table 1 those which have even degree n.

As in the previous section, we use the structure of C as a T-module for any T in Table 1 where $8 \mid n$ and $n \leq 3928$. Recall that C is a T-module of dimension $\frac{n}{2}$ since it is a self-dual code.

Once again, in order to find all extremal codes which are invariant under a given group T, we search for all $\frac{n}{2}$-dimensional T-invariant submodules of the ambient space $\mathbb{F}_2^n$, which are self-dual as codes, and check the minimum distance.

First note that $T = \mathrm{A}_n$ can not occur since the only A_n-invariant subspaces of $\mathbb{F}_2^n$ are the trivial submodule and the submodule of all even weight vectors.

In case $T = \mathrm{PSL}(2,q)$ where q is a prime the code C must be an extended quadratic residue code by the following result of Knapp and Schmid.

Lemma 5 [9]. *Let q be a prime of the form $q \equiv -1 \bmod 8$. Then the extended quadratic residue codes are the only self-dual codes of length $n = q+1$ which are invariant under the group* $\mathrm{PSL}(2,q)$.

All extremal extended quadratic residue codes are classified.

Lemma 6 [1]. *The only extremal extended quadratic residue codes are those of length* $8, 24, 32, 48, 80$ *or* 104.

Next we consider $T = \mathrm{PSL}(2,q)$ with q a prime power. Since $n \leq 3928$ the only possibility is $\mathrm{PSL}(2,7^3)$. In this case MAGMA shows that there are exactly two T-invariant submodules of dimension $\frac{n}{2}$ in the ambient space, and as codes they are not extremal. Actually both codes are extended generalized quadratic residue codes of length 344 in the sense of [13].

In case $T = \mathrm{M}_{24}$ we know that C is the Golay code which is an extended quadratic residue code. One way to see that the Golay code is the only self-dual code invariant under M_{24} is to apply Lemma 5, since $\mathrm{PSL}(2,23) \leq \mathrm{M}_{24}$.

For $T = \mathrm{PSL}(d,q)$ with $d > 2$ the permutation representation of degree n in Table 1 is given by its natural action on the projective space, and for $T = \mathrm{PSU}(3,q)$ by the action on the cosets of the Borel subgroup. Because of the restriction on the degree n we have to consider only the cases $(d,q) = (4,3), (4,7), (4,11), (8,3)$ for $\mathrm{PSL}(d,q)$ and $q = 7$ for $\mathrm{PSU}(3,q)$. It turns out that in all cases the only T-invariant subspaces of $\mathbb{F}_2^n$ are of

dimension 1 and $n-1$.

In case $T = \mathrm{HS}$ the 2-transitive representation of degree $n = 176$ can be taken from the Atlas of Finite Group Representations [14]. With Magma we see that there are no HS-modules of dimension $\frac{n}{2}$.

Finally, let $T = \mathrm{PSp}(2d, 2)$ with $d = 4, 5, 6$. In this case we use the fact that every permutation representation of T is given by the action of T on the cosets of its maximal subgroups. Using [8] we see that the maximal subgroups of T that yield the representations of degree $n = 2^{2d-1} \pm 2^{d-1}$ are the orthogonal groups $\mathrm{O}^+(2d, 2)$ and $\mathrm{O}^-(2d, 2)$. Computations with Magma prove that in all cases there are no T-invariant submodules of dimension $\frac{n}{2}$. Thus we have

Theorem 7. *Let C be an extremal self-dual doubly-even code with a 2-transitive automorphism group. Then C is either the extended quadratic residue code of length 8, 24, 32, 48, 80 or 104 or the second order Reed-Muller code of length 32 or C is possibly a code of length 1 024 invariant under the group $T \rtimes \mathrm{SL}(2, 2^5)$, where T is elementary abelian of order 2^{10}.*

4 Extremal codes over larger fields

In this section we classify extremal self-dual ternary and quaternary codes with 2-transitive permutation automorphism groups. In order to do so we use the same methods as before.

Doubly-even self-dual binary codes can be considered in a framework of so-called divisible codes for which the weights of all codewords are divisible by some integer $\Delta > 1$. All such self-dual codes are classified in the famous Gleason–Pierce theorem (see [11, Section 4]). Apart from doubly-even binary codes, these include singly-even binary codes, ternary codes with $\Delta = 3$ and quaternary Hermitian self-dual codes with $\Delta = 2$. For singly-even binary codes there is a bound on minimum distance, similar to (1) (see [10]), but only a theoretical bound on the length of extremal codes (see [12]). Since there is no explicit bound we do not see how to classify these codes.

Let C be a self-dual code over $\mathbb{F}_3$. Then all weights of C are divisible by 3, the length n of C is a multiple of 4 (see [5]) and the minimum distance d of C satisfies (see [10])

$$d \leq 3 \left\lfloor \frac{n}{12} \right\rfloor + 3. \tag{2}$$

If $d = 3 \left\lfloor \frac{n}{12} \right\rfloor + 3$ then the code is called extremal. Extremal self-dual ternary codes do not exist if $n = 72, 96, 120$ or $n \geq 144$ (see [15] and [11]). In the following theorem we classify all extremal ternary codes having a 2-transitive permutation automorphism group (i.e. we only allow permutations of coordinates, but not multiplication by scalars from the field).

Theorem 8. *Let C be an extremal self-dual code over the field $\mathbb{F}_3$ with a 2-transitive permutation automorphism group. Then C is the ternary Golay code.*

Proof. Let G denote the permutation automorphism group of C. Since G is 2-transitive, the socle T of G is either elementary abelian or simple by Lemma 1.

Consider the case that T is elementary abelian. Since $4 \mid n$ we have $n = 2^m$ and $m \leq 7$ since $n < 144$. As in Section 2 we write $G = T \rtimes H$ where $H \leq \mathrm{GL}(m, 2)$ acts transitively on $2^m - 1$ points (the possibilities for H are given in Section 2). With Magma we find that for $m \leq 7$ and all groups H there are no $\frac{n}{2}$-dimensional $\mathbb{F}_3 G$-modules and thus no self-dual ternary codes.

Let now T be simple. Then T is one of the groups from Table 1 with $4 \mid n \neq 72, 96, 120$ and $n < 144$. With Magma we see that the only possible group which has an $\frac{n}{2}$-dimensional $\mathbb{F}_3 T$-module is M_{11} of degree 12. This module is in fact the famous $[12, 6, 6]_3$ Golay code. Note that the full (monomial) automorphism group of this code is a non split extension of $\mathbb{Z}_2$ by M_{12}.

Now let C be a Hermitian self-dual code over $\mathbb{F}_4 = \{0, 1, w, w^2\}$ where $w^2 + w + 1 = 0$. The duality in this case is considered with respect to the Hermitian inner product

$$(u, v) = \sum_{i=1}^{n} u_i v_i^2,$$

where $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n) \in \mathbb{F}_4^n$. The weights and the length of a Hermitian self-dual code are always even (see [11]), and for the minimum distance d we have the following bound

$$d \leq 2 \left\lfloor \frac{n}{6} \right\rfloor + 2. \tag{3}$$

Once again we call C extremal if it achieves the bound. Furthermore the length n of an extremal quaternary Hermitian self-dual code satisfies

$$\begin{array}{l} n \leq 96, \text{ if } n = 6m, \\ n \leq 116, \text{ if } n = 6m + 2, \\ n \leq 130, \text{ if } n = 6m + 4, \end{array} \tag{4}$$

by [15].

As in the case of ternary codes, we classify the quaternary extremal Hermitian self-dual codes with 2-transitive permutation groups.

Theorem 9. *Let C be an extremal Hermitian self-dual code over the field $\mathbb{F}_4$ with a 2-transitive permutation automorphism group. Then C is either the extended quadratic residue code of length $n = 6, 8, 14$ or 30 or a unique code of length 22.*

Proof. As before let G denote the permutation automorphism group of C and let T denote the socle of G.

If T is elementary abelian, then $n = 2^m$ and by (4) $m \leq 6$. We check with MAGMA that for even m there are no Hermitian self-dual codes for all possible groups G. If $m = 3$ or 5 then we find with MAGMA that the only Hermitian self-dual code invariant under G is the generalized Reed-Muller code. It is extremal only for length $n = 8$, in which case it is also equivalent to the extended quadratic residue code. For $m = 2, 4$ or 6 MAGMA computations show that there are no Hermitian self-dual codes for all possibilities of G.

Now let T be simple. Then T is one of the groups in Table 1 with n even and satisfying (4). With MAGMA we find that the only groups which have $\frac{n}{2}$-dimensional $\mathbb{F}_4 T$-modules are M_{22}, M_{24}, or $\mathrm{PSL}(2, p)$ for p a prime.

If $T = \mathrm{M}_{22}$ there are two Hermitian self-dual codes, but only one is extremal.

For M_{24} we get only one Hermitian self-dual code, namely the $\mathbb{F}_4$ extension of the binary Golay code, which is also an extended quadratic residue code. Its minimum distance is 8 and therefore the code is not extremal.

By [9], we know that extended quadratic residue codes are the only codes over $\mathbb{F}_4$ of length $n = p + 1$ which are invariant under the group $\mathrm{PSL}(2, p)$. Note that the extended quadratic residue codes over $\mathbb{F}_4$ are not always Hermitian self-dual. To our knowledge no easy to handle criterion is known which characterizes self-duality with respect to Hermitian inner products. By [13] the extended quadratic residue codes are self-dual with respect to Euclidean inner products exactly when -1 is a nonsquare in $\mathbb{F}_p$.

Among quaternary Hermitian self-dual extended quadratic residue codes only those of length $n = 6, 8, 14$ and 30 are extremal. □

References

1. S. Bouyuklieva, A. Malevich and W. Willems. Automorphisms of extremal self-dual codes. IEEE Trans. Inform. Theory, 56(5), 2091–2096 (2010)
2. W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language. J. Symbolic Comput., 24, 235-265 (1997)
3. P.J. Cameron. Finite permutation groups and finite simple groups. Bull. London Math. Soc., 13(1), 1–22 (1981)
4. P. Charpin and F. Levy-dit-Vehel. On self-dual affine-invariant codes. J. Combin. Theory Ser. A, 67(2), 223–244 (1994)
5. A.M. Gleason. Weight polynomials of self-dual codes and the MacWilliams identities. In Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 3, 211–215, Gauthier-Villars, Paris (1971)
6. B. Huppert. Endliche Gruppen I. Springer-Verlag, Berlin (1967)
7. B. Huppert, N. Blackburn. Finite Groups III. Springer-Verlag, Berlin (1982)
8. M.W. Liebeck. On the orders of maximal subgroups of the finite classical groups. Proc. London Math. Soc., (3), 50(3), 426–446 (1985)
9. W. Knapp and P. Schmid. Codes with prescribed permutation group. J. Algebra, 67, 415–435 (1980)
10. C.L. Mallows and N.J.A. Sloane. An upper bound for self-dual codes. Information and Control, 22, 188–200 (1973)
11. E.M. Rains and N.J.A. Sloane. Self-dual codes. In Handbook of coding theory, Vol. I, II, pages 177–294. North-Holland, Amsterdam (1998)
12. E.M. Rains. New asymptotic bounds for self-dual codes and lattices. IEEE Trans. Inform. Theory, 49(5), 1261–1274 (2003)
13. J.H. van Lint and F.J. MacWilliams. Generalized quadratic residue codes. IEEE Trans. Inform. Theory, 24(6), 730–737 (1978)
14. R. Wilson, P. Walsh, J. Tripp and I. Suleiman. Atlas of finite group representations. Available at `http://brauer.maths.qmul.ac.uk/Atlas/v3/`
15. S. Zhang. On the nonexistence of extremal self-dual codes. Discrete Appl. Math., 91(1-3), 277–286 (1999)