On the Classification of Extremal Doubly Even Self-Dual Codes with 2-Transitive Automorphism Groups

Naoki Chigira, Masaaki Harada and Masaaki Kitazume

February 21, 2013

Abstract

In this note, we complete the classification of extremal doubly even self-dual codes with 2-transitive automorphism groups.

Keywords extremal doubly even self-dual code, automorphism group, 2-transitive group

Mathematics Subject Classification 94B05, 20B25

1 Introduction

As described in [6], self-dual codes are an important class of linear codes for both theoretical and practical reasons. It is a fundamental problem to classify self-dual codes of modest lengths and determine the largest minimum weight among self-dual codes of that length (see [2, 5]). It was shown in [4] that the minimum weight $d$ of a doubly even self-dual code of length $n$ is bounded by $d \leq 4\lfloor \frac{n}{24} \rfloor + 4$. A doubly even self-dual code meeting the bound is called extremal.
extremal. A common strategy for the problem whether there is an extremal
doubly even self-dual code for a given length is to classify extremal doubly
even self-dual codes with a given nontrivial automorphism group (see [2, 5]).
Recently, Malevich and Willems [3] have shown that if C is an extremal
doubly even self-dual code with a 2-transitive automorphism group then C is
equivalent to one of the extended quadratic residue codes of lengths 8, 24, 32,
48, 80, 104, the second-order Reed–Muller code of length 32 or a putative
extremal doubly even self-dual code of length 1024 invariant under the group
T ⋊ SL(2, 2^5), where T is an elementary abelian group of order 1024.

The aim of this note is to complete the classification of extremal doubly
even self-dual codes with 2-transitive automorphism groups. This is com-
pleted by excluding the open case in the above characterization [3], using
Theorem A in [1].

Theorem 1. Let C be an extremal doubly even self-dual code with a 2-
transitive automorphism group. Then C is equivalent to one of the the ex-
tended quadratic residue codes of lengths 8, 24, 32, 48, 80, 104 or the second-
order Reed–Muller code of length 32.

2 Proof of Theorem 1

For an n-element set Ω, the power set \( P(\Omega) \) – the family of all subsets of \( \Omega \) –
is regarded as an n-dimensional binary vector space with the inner product
\((X, Y) \equiv |X \cap Y| (\text{mod} 2)\) for \( X, Y \in P(\Omega) \). The weight of \( X \) is defined to
be the integer \(|X|\). A subspace \( C \) of \( P(\Omega) \) is called a code of length n. Note
that all codes in this note are binary. The dual code \( C^\perp \) of \( C \) is the set of
all \( X \in P(\Omega) \) satisfying \((X, Y) = 0\) for all \( Y \in C \). A code \( C \) is said to be
self-orthogonal if \( C \subseteq C^\perp \), and self-dual if \( C = C^\perp \). A doubly even code is a
code whose codewords have weight a multiple of 4.

Let \( G \) be a permutation group on an n-element set \( \Omega \). We define the code
\( C(G, \Omega) \) by
\[
C(G, \Omega) = \langle \text{Fix}(\sigma) \mid \sigma \in I(G) \rangle^\perp,
\]
where \( I(G) \) denotes the set of involutions of \( G \) and \( \text{Fix}(\sigma) \) is the set of fixed
points of \( \sigma \) on \( \Omega \).

Theorem 2 (Chigira, Harada and Kitazume [1]). Let \( C \) be a binary self-
orthogonal code of length \( n \) invariant under the group \( G \). Then \( C \subseteq C(G, \Omega) \).
By using Theorem 2, some self-dual codes invariant under sporadic almost simple groups were constructed in [1]. In this note, we apply Theorem 2 to a family of 2-transitive groups containing the group $(2^{10}) \rtimes \text{SL}(2, 2^5)$.

Let $r, s$ be positive integers. We consider the following group

$$G = T \rtimes H \quad (T = (2^r)^{2s}, H = \text{SL}(2s, 2^r)),$$

where the group $T$ is regarded as the natural module $GF(2^r)^{2s}$ of $H$. Here $T$ acts regularly on $T$ itself and $H$ acts on $T$ as the stabilizer of the unit of $T$, which is regarded as the zero vector of $GF(2^r)^{2s}$. Then $G$ naturally acts 2-transitively on $T$.

**Lemma 3.** There is no self-dual code of length $2^{2rs}$ invariant under $G = T \rtimes H$.

**Proof.** By the fundamental theory of Jordan canonical forms in basic linear algebra, the dimension of the subspace of $GF(2^r)^{2s}$ spanned by the vectors fixed by an involution in $H = \text{SL}(2s, 2^r)$ is equal to or greater than $s$. Then it is easily seen that there exist two involutions $\sigma, \tau$ in $H$ such that each of them fixes some $s$-dimensional subspace of $GF(2^r)^{2s}$, and the zero vector is the only vector fixed by both of them (i.e. $T = \text{Fix}(\sigma) \oplus \text{Fix}(\tau)$). As codewords in $C(G, \Omega)^\perp$, the inner product $(\text{Fix}(\sigma), \text{Fix}(\tau))$ is equal to 1, since $|\text{Fix}(\sigma) \cap \text{Fix}(\tau)| = 1$. This yields that $C(G, T)^\perp$ is not self-orthogonal.

Suppose that $B$ is a self-dual code invariant under $G$. By Theorem 2, $B \subset C(G, T)$. Since $B^\perp \supset C(G, T)^\perp$ and $B = B^\perp$, $C(G, T)^\perp$ is self-orthogonal. This is a contradiction. \hfill \Box

The case $(r, s) = (5, 1)$ in the above lemma completes the proof of Theorem 1.

**Remark 4.** In the above proof, the cardinality of the fixed subspace of dimension $s$ is $2^{rs}$, which is smaller than the value $4\left\lfloor \frac{3^{2(s-1)r}}{24} \right\rfloor + 4$, except for the cases $(r, s) = (1, 2), (2, 1)$. This shows immediately that there is no extremal doubly self-dual code of length $2^{2rs}$ invariant under the group $G = T \rtimes \text{SL}(2s, 2^r)$ if $rs > 2$.

On the other hand, the smallest cardinality of the fixed subspace of an involution in $\text{SL}(2s - 1, 2^r)$ is $2^{rs}$. If $s > 1$ then this number is smaller than the value $4\left\lfloor \frac{3^{(2s-1)r}}{24} \right\rfloor + 4$, except for the small cases $(r, s) = (1, 2), (1, 3), (2, 2)$. When $(r, s) = (1, 2)$ or $(1, 3)$, the code $C(G, T)$, for $G = T \rtimes \text{SL}(2s - 1, 2^r)$ where $T = (2^r)^{2s-1}$, is equivalent to the extended Hamming code of length 8,
or the second-order Reed–Muller code of length 32 (see [1, Example 2.10]), respectively. For the remaining case \((r, s) = (2, 2)\) (i.e. \(G = T \times \text{SL}(3, 2^2), T = 2^6\)), the smallest cardinality of the fixed subspace of an involution is 16 (> 12), and so such an argument does not work. (Indeed the code \(C(G, T)^\perp\) is self-orthogonal with minimum weight 16.)

**Acknowledgment.** This work is supported by JSPS KAKENHI Grant Numbers 23340021, 24340002, 24540024.

**References**

[1] N. Chigira, M. Harada and M. Kitazume, Permutation groups and binary self-orthogonal codes, *J. Algebra* 309 (2007), 610–621.

[2] W.C. Huffman, On the classification and enumeration of self-dual codes, *Finite Fields Appl.* 11 (2005), 451–490.

[3] A. Malevich and W. Willems, On the classification of the extremal self-dual codes over small fields with 2-transitive automorphism groups, *Des. Codes Cryptogr.*, (to appear), DOI 10.1007/s10623-012-9655-9.

[4] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Inform. Control* 22 (1973), 188–200.

[5] E. Rains and N.J.A. Sloane, “Self-dual codes,” Handbook of Coding Theory, V.S. Pless and W.C. Huffman (Editors), Elsevier, Amsterdam 1998, pp. 177–294.