Finite Fields and Their Applications 33 (2015) 80–89

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On involutions in extremal self-dual codes and the dual distance of semi self-dual codes

Martino Borello [a,*,1], Gabriele Nebe [b]

[a] *Dipartimento di Matematica e Applicazioni, Università degli Studi di Milano Bicocca, 20125 Milan, Italy*
[b] *Lehrstuhl D für Mathematik, RWTH Aachen University, 52056 Aachen, Germany*

ARTICLE INFO

Article history:
Received 11 June 2014
Accepted 14 November 2014
Available online 4 December 2014
Communicated by Xiang-dong Hou

MSC:
94B05
20B25

Keywords:
Semi self-dual codes
Bounds on minimum distance
Automorphism group
Free modules
Extremal codes

ABSTRACT

A classical result of Conway and Pless is that a natural projection of the fixed code of an automorphism of odd prime order of a self-dual binary linear code is self-dual [13]. In this paper we prove that the same holds for involutions under some (quite strong) conditions on the codes.

In order to prove it, we introduce a new family of binary codes: the semi self-dual codes. A binary self-orthogonal code is called semi self-dual if it contains the all-ones vector and is of codimension 2 in its dual code. We prove upper bounds on the dual distance of semi self-dual codes.

As an application we get the following: let $\mathcal{C}$ be an extremal self-dual binary linear code of length $24m$ and $\sigma \in \mathrm{Aut}(\mathcal{C})$ be a fixed point free automorphism of order 2. If m is odd or if $m = 2k$ with $\binom{5k-1}{k-1}$ odd then $\mathcal{C}$ is a free $\mathbb{F}_2\langle\sigma\rangle$-module. This result has quite strong consequences on the structure of the automorphism group of such codes.

* Corresponding author.
E-mail addresses: martino.borello@unimib.it (M. Borello), nebe@math.rwth-aachen.de (G. Nebe).
[1] Member INdAM-GNSAGA (Italy).

http://dx.doi.org/10.1016/j.ffa.2014.11.008
1071-5797/

1. Introduction

The research in this paper is motivated by the study of involutions of extremal self-dual codes, which plays a fundamental role in [17,6,5,8,7,21]. A classical result of Conway and Pless is that a natural projection of the fixed code of an automorphism of odd prime order of a self-dual binary linear code is self-dual [13]. We will prove that the same holds for involutions under some (quite strong) conditions on the codes

Let $m \in \mathbb{N}$ and $\mathcal{C} = \mathcal{C}^\perp \leq \mathbb{F}_2^{24m}$ be an extremal binary self-dual code, so $d(\mathcal{C}) = 4m+4$ [15]. Then $\mathcal{C}$ is doubly even [19]. There are unique extremal self-dual codes of length 24 and 48 and these are the only known extremal codes of length $24m$. It is an intensively studied open question raised in [20], whether an extremal code of length 72 exists. A series of many papers has shown that if such a code exists, then its automorphism group $\mathrm{Aut}(\mathcal{C}) = \{\sigma \in S_{24m} \mid \sigma(\mathcal{C}) = \mathcal{C}\}$ has order ≤ 5 (see [4] for an exposition of this result). Stefka Bouyuklieva [9] studies automorphisms of order 2 of such codes. She shows that if $\mathcal{C}$ is an extremal code of length $24m$, $m \geq 2$ and $\sigma \in \mathrm{Aut}(\mathcal{C})$ has order 2, then the permutation σ has no fixed points, with one exception, $m = 5$, where there might be 24 fixed points. If $\sigma = (1,2),\ldots,(24m-1,24m)$ is a fixed point free automorphism of a doubly even self dual code $\mathcal{C}$, then its *fixed code*

$$\mathcal{C}(\sigma) := \{c \in \mathcal{C} \mid \sigma(c) = c\}$$

is isomorphic to

$$\pi\big(\mathcal{C}(\sigma)\big) = \{(c_1,\ldots,c_{12m}) \in \mathbb{F}_2^{12m} \mid (c_1,c_1,c_2,c_2,\ldots,c_{12m},c_{12m}) \in \mathcal{C}\}$$

such that

$$\pi\big(\{c+\sigma(c) \mid c \in \mathcal{C}\}\big) = \pi\big(\mathcal{C}(\sigma)\big)^\perp \subseteq \pi\big(\mathcal{C}(\sigma)\big).$$

As $\mathcal{C}$ is doubly-even, all words in $\pi(\mathcal{C}(\sigma))$ have even weight. It is shown in [17] and [5] that the code $\mathcal{C}$ is a free $\mathbb{F}_2\langle\sigma\rangle$-module, if and only if $\pi(\mathcal{C}(\sigma))$ is self-dual. If $\pi(\mathcal{C}(\sigma))$ is not self-dual then it contains the dual $\mathcal{D}^\perp$ of some code $\mathcal{D}$ of length $12m$ with

$$\mathbf{1} := (1,\ldots,1) \in \pi\big(\mathcal{C}(\sigma)\big)^\perp \subseteq \mathcal{D} \subseteq \mathcal{D}^\perp \subseteq \pi\big(\mathcal{C}(\sigma)\big).$$

In particular $\mathrm{d}(\mathcal{D}^\perp) \geq \mathrm{d}(\pi(\mathcal{C}(\sigma))) = \frac{1}{2}\mathrm{d}(\mathcal{C}(\sigma)) \geq \frac{1}{2}\mathrm{d}(\mathcal{C})$.

Definition 1.1. A binary self-orthogonal code $\mathcal{D} \subseteq \mathcal{D}^\perp \leq \mathbb{F}_2^n$ of length n is called *semi self-dual*, if $\mathbf{1} := (1,\ldots,1) \in \mathcal{D}$ and $\dim(\mathcal{D}^\perp/\mathcal{D}) = 2$.

Self-orthogonal codes always consist of words of even weight, so $\mathrm{wt}(c) := |\{i \mid c_i = 1\}| \in 2\mathbb{Z}$ for all $c \in \mathcal{D}$. Hence already the condition that $\mathbf{1} \in \mathcal{D}$ implies that the length $n = 12m$ of $\mathcal{D}$ is even. Note that $\mathcal{D}^\perp \subseteq \mathbf{1}^\perp = \{c \in \mathbb{F}_2^n \mid \mathrm{wt}(c) \in 2\mathbb{Z}\}$ implies that also