Finite Fields and Their Applications 50 (2018) 17–34

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Some new results on the self-dual [120, 60, 24] code

Martino Borello [a,*], Javier de la Cruz [b,c]

[a] *Université Paris 13, Sorbonne Paris Cité, LAGA, CNRS, UMR 7539, Université Paris 8, F-93430, Villetaneuse, France*
[b] *Universidad del Norte, Barranquilla, Colombia*
[c] *University of Zurich, Switzerland*

ARTICLE INFO

Article history:
Received 25 June 2017
Received in revised form 4 September 2017
Accepted 3 November 2017
Available online xxxx
Communicated by L. Storme

MSC:
94B05
20B25

Keywords:
Self-dual code
Extremal code
Automorphism group

ABSTRACT

The existence of an extremal self-dual binary linear code of length 120 is a long-standing open problem. We continue the investigation of its automorphism group, proving that automorphisms of order 30 and 57 cannot occur. Supposing the involutions acting fixed point freely, we show that also automorphisms of order 8 cannot occur and the automorphism group is of order at most 120, with further restrictions. Finally, we present some necessary conditions for the existence of the code, based on shadow and design theory.

1. Introduction

In coding theory, binary self-dual codes play a central role: they are linear codes with a rich algebraic structure, good decoding properties and relations with other areas of mathematics, such as group theory, lattice theory and design theory. For example,

* Corresponding author.
E-mail addresses: martino.borello@univ-paris8.fr (M. Borello), jdelacruz@uninorte.edu.co (J. de la Cruz).

https://doi.org/10.1016/j.ffa.2017.11.004
1071-5797/

this class includes the binary extended Golay code, whose automorphism group is the sporadic simple group M_{24} and which is related to the Leech lattice.

Gleason, Pierce and Turyn showed (see [3]) that if a natural number $r > 1$ divides the weight of all codewords of a binary self-dual code, then $r = 2$ (*even* code) or $r = 4$ (*doubly-even* code). Every binary self-dual code is even. If a binary self-dual code is even but not doubly-even (*singly-even* code), then it is called a *Type I* code, while if a binary self-dual code is doubly-even, then it is called a *Type II* code. Type II codes exist only for lengths which are multiples of 8 [24] and Mallows and Sloane showed in [27] that they have minimum distance bounded by $4\lfloor n/24 \rfloor + 4$, where n is the length. A type II code attaining this bound is called *extremal* code. Among extremal codes, those of length a multiple of 24 are particularly interesting: Assmus–Mattson's theorem [2] guarantees that the supports of their codewords of a fixed nonzero weight form a 5-design. Moreover, they have relations, as mentioned above, with simple groups and extremal lattices. Zhang proved in [32] that their length is at most 3672.

Despite their theoretical importance, only two extremal codes of length a multiple of 24 are known, namely the famous binary extended Golay code, the unique up to equivalence of length 24, and the extended quadratic residue code of length 48, which is the unique up to equivalence of this length. In 1973 Sloane [30] posed explicitly the question: is there a self-dual $[72, 36, 16]$ code? Since then, multiple attempts to establish the non existence of such a code or to present a construction have been done, till now unsuccessfully. The problem is still open for all lengths from 72 to 3672 and many investigations have been also done for the cases of length 96 and 120.

This paper focuses on the last one, i.e. on the study of a self-dual $[120, 60, 24]$ code. In particular, in Section 2 we will collect, for the reader's convenience, all the definitions and the known results which will be used in the following. In Section 3 we prove new properties about the automorphism group of a self-dual $[120, 60, 24]$ code. In particular we exclude the existence of automorphisms of order 30 and 57 and we investigate the structure of the automorphism group, in the case that involutions act fixed point freely (see the introduction of Subsection 3.3 for a motivation of this choice), proving that it is either trivial or isomorphic to a group of order at most 120, with further restrictions. Finally, in Section 4 we give necessary conditions for the existence of the code, based on shadow and design theory.

2. Background

In this section we collect some classical results of coding theory which are useful in the rest of the paper.

2.1. Gleason's theorem and the shadow of a code

For the whole subsection, let C be a binary code of length n, i.e. a subspace of $\mathbb{F}_2^n$. We recall that a $[n, k, d]$ code is a code of length n, dimension k and minimum distance d.