Finite Fields and Their Applications 51 (2018) 71–92

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Constructions for self-dual codes induced from group rings

Joe Gildea [a], Abidin Kaya [b], Rhian Taylor [a], Bahattin Yildiz [c,*]

[a] *Department of Mathematics, Faculty of Science and Engineering, University of Chester, UK*
[b] *Sampoerna Academy, L'Avenue Campus, 12780, Jakarta, Indonesia*
[c] *Department of Mathematics & Statistics, Northern Arizona University, Flagstaff, AZ 86001, USA*

ARTICLE INFO

Article history:
Received 25 July 2017
Received in revised form 4 January 2018
Accepted 9 January 2018
Available online xxxx
Communicated by W. Cary Huffman

MSC:
94B05
16S34

Keywords:
Group rings
Self-dual codes
Codes over rings

ABSTRACT

In this work, we establish a strong connection between group rings and self-dual codes. We prove that a group ring element corresponds to a self-dual code if and only if it is a unitary unit. We also show that the double-circulant and four-circulant constructions come from cyclic and dihedral groups, respectively. Using groups of order 8 and 16 we find many new construction methods, in addition to the well-known methods, for self-dual codes. We establish the relevance of these new constructions by finding many extremal binary self-dual codes using them, which we list in several tables. In particular, we construct 10 new extremal binary self-dual codes of length 68.

* Corresponding author.
E-mail addresses: j.gildea@chester.ac.uk (J. Gildea), abidin.kaya@sampoernaacademy.sch.id (A. Kaya), rhian.taylor@chester.ac.uk (R. Taylor), bahattin.yildiz@nau.edu (B. Yildiz).

https://doi.org/10.1016/j.ffa.2018.01.002
1071-5797/

1. Introduction

There is a natural connection between algebraic codes and group rings. Using a map that was introduced by Hurley, to any group ring element, we can associate a matrix over the ring of coefficients, which then can be used to construct a linear code. Many of the properties of the codes can be obtained from the corresponding group ring elements. This connection has been explored in the literature to find new constructions for some well known codes such as the extended Golay code or the extended quadratic residue code. We refer the reader to [16], [15], [24], [25], [2] and the references therein for more on this connection.

Self-dual codes are a special class of codes that have connections to and applications in many fields such as Lattices, Designs, Cryptography, Invariant Theory, etc. The natural upper bound on the minimum distances of binary self-dual codes have led to the notion of extremal self-dual codes. There is a vast literature on construction and classification of extremal binary self-dual codes of certain lengths. Many different techniques have been utilized in finding extremal binary self-dual codes. A common theme in these methods of construction is the use of a computer search. In order to make this search feasible special construction methods have been used to reduce the search field. The double circulant, bordered double circulant and four circulant constructions are some of the methods by which many extremal binary self-dual codes have been obtained. While first applied over the binary field, these methods have also been applied over finite commutative rings of characteristic 2 with considerable success. For some of these constructions, we refer to [3], [17], [18], [19], [21], [22] and [27].

The motivation in this work is twofold: First, by using the strong connection between group ring elements and codes induced by Hurley's map, we find necessary and sufficient conditions on a group ring element whose corresponding code is self-dual. This brings a new motivation for studying the so-called "unitary units" in group rings. The second main result is that considering different groups in group rings lead to many new construction methods for self-dual codes. In particular we show that the double circulant, the four-circulant constructions are not some random constructions but that they come from certain groups. By considering groups of orders 8 and 16, we come up with many new construction methods for self-dual codes. We illustrate the relevance of these constructions by finding many extremal binary self-dual codes, including ten new ones of length 68, by using them over appropriate group rings. We thus establish a new-found strong connection between group rings and Algebraic Coding Theory.

The rest of the paper is organized as follows: In Section 2, we recall some of the preliminaries on self-dual codes and some finite rings that we use in the subsequent chapters. In Section 3, we establish the connection between group ring elements and the corresponding self-dual codes. In Section 4 and 5, we list all the different constructions coming from groups of order 8 and 16, respectively. We find many extremal binary self-dual codes, using these constructions, which we list in several tables. In Section 6,