Discrete Applied Mathematics 167 (2014) 188–196

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Constructing formally self-dual codes over R_k

Suat Karadeniz [a], Steven T. Dougherty [b], Bahattin Yildiz [a,*]

[a] Department of Mathematics, Fatih University, 34500 Istanbul, Turkey

[b] Department of Mathematics, University of Scranton, Scranton, PA 18510, USA

ARTICLE INFO

Article history:
Received 11 January 2013
Received in revised form 31 October 2013
Accepted 16 November 2013
Available online 6 December 2013

Keywords:
Formally self-dual codes
Codes over R_k
Extremal codes
Codes over rings

ABSTRACT

In this work, we study construction techniques of formally self-dual codes over the infinite family of rings $R_k = \mathbb{F}_2[u_1, u_2, \dots, u_k]/\langle u_i^2 = 0, u_iu_j = u_ju_i\rangle$. These codes give rise to binary formally self-dual codes. Using these constructions, we obtain a number of good formally self-dual binary codes including even formally self-dual binary codes of parameters [72, 36, 14], [56, 28, 12], [44, 22, 10] and odd formally self-dual binary codes of parameters [72, 36, 13], all of which have better minimum distances than the best known self-dual codes of the same lengths.

1. Introduction

Formally self-dual codes are an interesting type of code that have been studied quite extensively by many researchers. For some of these works we refer the reader to [5,9,10,8,7,13,14]. Formally self-dual codes can have larger minimum distances than self-dual codes, which makes them of interest in searching for good codes. Since the weight enumerators of formally self-dual codes come from the same ring of invariants as the weight enumerators of self-dual codes, the Assmus–Mattson theorem can often be used to construct many new designs.

There are a few different constructions for binary formally self-dual codes. Of particular interest is a series of constructions given as an exercise in [11]. These and variations of these were used in the literature by different researchers.

Codes over rings have been a topic of great interest in the last two decades. Certain rings have been successfully used to obtain good binary codes with different properties. The ring $\mathbb{F}_2 + u\mathbb{F}_2$ was generalized first to $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ in [17] and then to $R_k = \mathbb{F}_2[u_1, u_2, \dots, u_k]/\langle u_i^2 = 0, u_iu_j = u_ju_i\rangle$ in [2]. The rich algebraic structure of these rings have been used quite effectively to obtain good binary codes with large automorphism groups as well as some new binary self-dual codes (see [12]).

In this work, we apply the construction methods given in [11] to the ring R_k to construct formally self-dual codes over R_k. These codes result in binary formally self-dual codes with good parameters after taking the image under a weight-preserving Gray map.

The rest of the paper is organized as follows: In Section 2, we give the preliminaries about codes over the ring R_k as well as some of the definitions associated with formally self-dual codes.

In Section 3, we give constructions of formally self-dual codes from special types of matrices and prove the theoretical results. Section 4 includes the computational results about the codes constructed via the methods given in the previous section. The results are given in the form of Tables 1–5.

* Corresponding author. Tel.: +90 2128553300; fax: +90 2128663402.
E-mail addresses: skaradeniz@fatih.edu.tr (S. Karadeniz), prof.steven.dougherty@gmail.com (S.T. Dougherty), byildiz@fatih.edu.tr, bahattinyildiz@gmail.com (B. Yildiz).

0166-218X/$ – see front matter
http://dx.doi.org/10.1016/j.dam.2013.11.017

2. Preliminaries

2.1. Formally self-dual codes

We begin with the following definitions. On the binary space $\mathbb{F}_2^n$, with $\mathbf{v}, \mathbf{w} \in \mathbb{F}_2^n$, attach the usual inner-product $[\mathbf{v}, \mathbf{w}] = \sum v_i w_i$ and define $C^\perp = \{\mathbf{w} \mid [\mathbf{w}, \mathbf{v}] = 0\ \forall \mathbf{v} \in C\}$. We make the usual definition of the Hamming weight enumerator, namely $W_C(x, y) = \sum_{\mathbf{v} \in C} x^{n-wt(\mathbf{v})} y^{wt(\mathbf{v})}$ where $wt(\mathbf{v})$ is the number of non-zero coordinates of $\mathbf{v}$.

Definition 1. A binary code C is called self-dual if $C = C^\perp$. It is called isodual if C is equivalent to $C^\perp$. The code C is called formally self-dual (f.s.d.) if $W_C(x, y) = W_{C^\perp}(x, y)$, that is C and $C^\perp$ have the same weight enumerators.

A code is called *even* if all the weights are even, it is called *odd* (Type 0) otherwise. If an even code has all weights $0 \pmod 4$ then the code is said to be doubly-even (Type II), otherwise it is said to be singly-even (Type I).

From the definitions it follows immediately that self-dual and isodual codes are formally self-dual. But, there are formally self-dual codes which are not self-dual. Note however that the weight enumerator of an even formally self-dual code is held invariant by the same matrices, and hence the same Gleason theorem applies. Namely we have the following. Let C be a formally self-dual code. Then,

- $W_C(x, y) \in \mathbb{C}[x^2 + y^2, y(x - y)]$, if C is Type 0,
- $W_C(x, y) \in \mathbb{C}[x^2 + y^2, x^8 + 14x^4y^4 + y^8]$, if C is Type I,
- $W_C(x, y) \in \mathbb{C}[x^8 + 14x^4y^4 + y^8, x^4y^4(x^4 - y^4)^4]$, if C is Type II.

For the remainder we let $x = 1$ when giving the Hamming weight enumerator.

From [4], we know that if C is a binary formally self-dual code of length $2n$, and d is the minimum Hamming weight of C, then

$$d \leq 2\left\lfloor \frac{n}{4} \right\rfloor + 2.$$

Formally self-dual codes meeting this bound are called *extremal*. Formally self-dual codes for which $d = 2\left\lfloor \frac{n}{4} \right\rfloor$ are called *near-extremal*. In [14], Kim and Pless conjecture that there are no near-extremal formally self-dual even binary codes of length $n \geq 48$ with $8 \mid n$.

2.2. The ring R_k and the properties

Define the following ring for $k \geq 1$. Let

$$R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0, u_iu_j = u_ju_i \rangle. \tag{1}$$

For any subset $A \subseteq \{1, 2, \ldots, k\}$ let

$$u_A := \prod_{i \in A} u_i \tag{2}$$

with the convention that $u_\emptyset = 1$. Then any element of R_k can be represented as

$$\sum_{A \subseteq \{1,\ldots,k\}} c_A u_A, \quad c_A \in \mathbb{F}_2. \tag{3}$$

The ring R_k is a local ring with maximal ideal $\langle u_1, u_2, \ldots, u_k \rangle$ and $|R_k| = 2^{(2^k)}$. The ring is neither a principal ideal ring nor a chain ring when $k \geq 2$. The ring is however a Frobenius ring. The rings $R_0 = \mathbb{F}_2$ and $R_1 = \mathbb{F}_2 + u\mathbb{F}_2$ have been studied quite extensively in the literature of coding theory. The ring $R_2 = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ was first introduced by Yildiz and Karadeniz in [17].

In [2], it is shown that an element of R_k is a unit if and only if the coefficient of $u_\emptyset$ is 1 and that each unit is also its own inverse. We also have the following:

$$\forall a \in R_k, \quad a \cdot (u_1u_2 \ldots u_k) = \begin{cases} u_1u_2 \ldots u_k & \text{if } a \text{ is a unit} \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

$$\text{Also, } \forall a \in R_k \quad a^2 = \begin{cases} 1 & \text{if } a \text{ is a unit} \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

See [2] for proofs of these and other foundational results for the ring R_k.

A linear code of length n over R_k is defined to be an R_k-submodule of R_k^n.

We denote a vector by $\bar{a}$. We attach the usual inner product on this ambient space R_k^n, that is $\langle \bar{a}, \bar{b} \rangle_k = \sum a_ib_i$. The dual code $C^\perp$ is defined by $C^\perp = \{\bar{y} \in R_k^n \mid \langle \bar{y}, \bar{x} \rangle_k = 0 \text{ for all } \bar{x} \in C\}$. We say that a code is self-orthogonal if $C \subseteq C^\perp$ and self-dual