Available online at www.sciencedirect.com

ScienceDirect

Journal of the Franklin Institute 350 (2013) 2837–2847

Journal of The Franklin Institute

www.elsevier.com/locate/jfranklin

Short communication

Cyclic codes over $M_2(\mathbb{F}_2)$

Adel Alahmadi[a], Houda Sboui[b], Patrick Solé[a,c,*], Olfa Yemen[d]

[a]Math Department, King Abdulaziz University, Jeddah, Saudi Arabia
[b]ENIT, El Manar, Tunis, Tunisia
[c]Telecom ParisTech, 46 rue Barrault, 75634 Paris Cedex 13, France
[d]Institut Preparatoire, El Manar, Tunis, Tunisia

Received 28 August 2012; received in revised form 14 April 2013; accepted 30 June 2013
Available online 11 July 2013

Abstract

The ring in the title is perhaps the first noncommutative ring to have been used as alphabet for block codes. The original motivation was the construction of some quaternionic modular lattices from codes. The new application is the construction of space time codes obtained by concatenation from the Golden code. In this paper, we derive structure theorems for cyclic codes over that ring, and use them to characterize the lengths where self dual cyclic codes exist. These codes in turn give rise to formally self dual $\mathbb{F}_4-$codes.

1. Introduction

Codes over rings have been a popular research topic, in particular since the paper [6], which used the arithmetic duality of codes over $\mathbb{Z}_4$ to explain the formal duality of some notoriously binary nonlinear codes. One of the main tool of that paper was a Gray map from $\mathbb{Z}_4$ to $\mathbb{F}_2^2$, which is an isometry from the Lee weight to the Hamming weight. Still, from 1994 till now there have been very few papers on codes over *noncommutative rings* [1,5,16]. The first concrete such alphabet seems to have been $A = M_2(\mathbb{F}_2)$, which appeared in algebraic constructions of modular lattices [1]. This alphabet resurfaced recently in connection with the new topic of space time codes [9]. The beautiful fact about this alphabet is the existence of a Gray map analogue of that of [6], the Bachoc map that maps isometrically this ring of order 16 with a special distance we call the Bachoc distance onto two copies of the Galois field $\mathbb{F}_4$, with the Hamming distance [1, Section 6.2].

*Corresponding author at: Telecom Paris Tech, 46 rue Barrault, 75634 Paris Cedex 13, France. Tel.: +33 650776653.
E-mail addresses: adelnife2@yahoo.com (A. Alahmadi), sboui.houda@yahoo.fr (H. Sboui), sole@telecom-paristech.fr, sole@enst.fr (P. Solé), olfa_yemen@yahoo.fr (O. Yemen).

0016-0032/$32.00
http://dx.doi.org/10.1016/j.jfranklin.2013.06.023

Table 1
Two alphabets.

$\mathbb{Z}_4$	Gray map	Lee weight	Ideal (2)	Residue field $\mathbb{F}_2$	swe_C
A	Bachoc map	Bachoc weight	Ideal $(1+i)$	Residue field $\mathbb{F}_4$	bwe_C

The idea is to introduce two matrices allusively called ω and i such that their respective characteristic polynomials are X^2+X+1 and X^2+1 and satisfying the relation $i\omega=\omega^2 i$. The ring A can be written as $A=\mathbb{F}_4+i\mathbb{F}_4$, by regarding $\mathbb{F}_4$ as $\mathbb{F}_2[\omega]$. This confers to it a quotient structure over a skew polynomial ring with coefficient ring the field $\mathbb{F}_4$, namely $\mathbb{F}_4[x;\theta]/(x^2+1)$, with θ the Frobenius operator of the field $\mathbb{F}_4$ [10]. Note, for completeness, that if M is a nonzero matrix of A then its Bachoc weight is worth 2 if M is singular nonzero, 1 if M is regular [1]. The present paper is based on the dictionary between the alphabets A and $\mathbb{Z}_4$ described in Table 1.

It seems legitimate, following a long trend in research to apply the methodology of cyclic codes over that simple and may be simplest example of noncommutative finite ring. In this paper we characterize cyclic codes by their generators. Their duals are also cyclic and their generators can be expressed simply as a function of the generators of the primal codes. We give an arithmetic criterion for a cyclic code to be self dual for the Euclidean scalar product. We show that self dual cyclic codes for the Hermitian scalar product cannot exist in odd length. We show that the Bachoc image of a self dual code for the Euclidean scalar product is formally self dual. Our new expression of the Bachoc image as a Plotkin sum of the residue and torsion codes allows us to compute the parameters of many examples of formally self dual $\mathbb{F}_4-$codes for $n\leq 31$.

2. Notation and definitions

For simplicity, we denote by $A=M_2(\mathbb{F}_2)$ the ring of matrices of order 2 over the finite field $\mathbb{F}_2$. Following [1]:

$$A=\mathbb{F}_2[\omega]\oplus i\mathbb{F}_2[\omega],$$

where ω and i are in A, and are such that their respective characteristic polynomials are X^2+X+1 and X^2+1 and satisfy the relation $i\omega=\omega^2 i$. A possible choice is

$$i=\begin{pmatrix}0&1\\1&0\end{pmatrix},\ \omega=\begin{pmatrix}0&1\\1&1\end{pmatrix}.$$

For convenience we let $u=1+i$, a nilpotent element, identify the subring $\mathbb{F}_2[\omega]$ with $\mathbb{F}_4$ and write

$$A=\mathbb{F}_4\oplus u\mathbb{F}_4.$$

Now, denote by μ the projection on the first component of that direct sum. Note that this map is $\mathbb{F}_4-$linear but not a ring morphism. This map extends coefficient wise to a map from $A[X]$ down to $\mathbb{F}_4[X]$. Define an A-**linear code** of length n, as a right A submodule of A^n. Given an A-linear code C we construct two linear $\mathbb{F}_4-$codes of the same length n, denoted by R and T, for **residue** and **torsion code** respectively, such that $R=\mu(C)$ and T is the largest $\mathbb{F}_4-$code D with the property that $uD\subseteq C$. We see by considering uC, that $R\subseteq T$, with equality if C is a free A-module.