ARTICLE IN PRESS

Discrete Applied Mathematics ■ (■■■■) ■■■–■■■

Contents lists available at ScienceDirect

Discrete Applied Mathematics

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

Optimal binary codes from trace codes over a non-chain ring

Minjia Shi[a,b,c,*], Yan Liu[c], Patrick Solé[d]

[a] Key Laboratory of Intelligent Computing & Signal Processing, Ministry of Education, Anhui University, No. 3 Feixi Road, Hefei, Anhui Province 230039, PR China

[b] National Mobile Communications Research Laboratory, Southeast University, 210096, Nanjing, PR China

[c] School of Mathematical Sciences, Anhui University, Hefei, 230601, PR China

[d] CNRS/LAGA, University of Paris 8, 93 526 Saint-Denis, France

ARTICLE INFO

Article history:
Received 10 July 2016
Received in revised form 24 September 2016
Accepted 28 September 2016
Available online xxxx

Keywords:
Two-weight codes
Griesmer bound
Trace codes
Secret sharing schemes

ABSTRACT

We construct an infinite family of two-Lee-weight codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$. These codes are defined as trace codes and have the algebraic structure of abelian codes. Their Lee weight distribution is computed by using character sums. Then, taking Gray mapping, we obtain an infinite family of abelian binary two-weight codes which are shown to be optimal by application of the Griesmer bound. Moreover, an application to secret sharing schemes is given.

1. Introduction

Two-weight codes over fields have been studied since the seventies due to their connections to strongly regular graphs, difference sets, and finite geometry [6,7]. More recently, two-weight codes over rings have received some attention [4,5]. In [12], by using trace codes, Shi et al. constructed an infinite family of two-Lee-weight codes over the classic chain ring $\mathbb{F}_2 + u\mathbb{F}_2$ [2]. Moving to more complex rings, we consider in this paper two-Lee-weight codes over the non-chain ring $R = \mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$. Linear and constacyclic codes over that ring have been extensively studied in [13,10], respectively.

In this paper, we construct a family of two-weight codes that are provably abelian but perhaps not cyclic. This is noteworthy, as most constructions of two-weight codes in the literature are based on cyclic codes and cyclotomy [3, Section 9.8.5]. Trace codes are considered here. Their coordinate places are indexed by the group of units of an algebraic extension of R. Their weight distribution is determined by using exponential character sums. After Gray mapping, we obtain an infinite family of binary abelian two-weight codes. These are shown to be optimal for given length and dimension by application of the Griesmer bound [9]. However, they do not meet that bound with equality. An application to secret sharing schemes is sketched out.

The material is organized as follows. Section 2 sets up the basic notations and definitions. Section 3 shows that the codes and their binary images are abelian. Section 4 gives the main result in this paper, the Lee weight distribution of our codes. Section 5 proves the optimality of their binary images. Section 6 determines the minimum distance of the dual codes. Section 7 determines the support structure of binary images and describes an application to secret sharing schemes. Section 8 puts the obtained results into perspective, and makes some conjectures for future research.

[*] Corresponding author at: Key Laboratory of Intelligent Computing & Signal Processing, Ministry of Education, Anhui University, No. 3 Feixi Road, Hefei, Anhui Province 230039, PR China.

E-mail addresses: smjwcl.good@163.com (M. Shi), liuyan2612@126.com (Y. Liu), sole@enst.fr (P. Solé).

http://dx.doi.org/10.1016/j.dam.2016.09.050
0166-218X/© 2016 Elsevier B.V. All rights reserved.

2. Background material

2.1. Rings

We consider the non-chain ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, denoted by R, with $u^2 = v^2 = 0,\ uv = vu$. Given a positive integer m, we can construct the ring extension $\mathcal{R} = \mathbb{F}_{2^m} + u\mathbb{F}_{2^m} + v\mathbb{F}_{2^m} + uv\mathbb{F}_{2^m}$. There is a Frobenius operator F which maps $a + bu + cv + duv$ onto $a^2 + b^2u + c^2v + d^2uv$. The *Trace function*, denoted by Tr is then defined as

$$Tr = \sum_{j=0}^{m-1} F^j.$$

It is immediate to check that

$$Tr(a + bu + cv + duv) = tr(a) + tr(b)u + tr(c)v + tr(d)uv,$$

for $a, b, c, d \in \mathbb{F}_{2^m}$. Here $tr()$ denotes the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$.

Let $M = \{bu + cv + duv : b, c, d \in \mathbb{F}_{2^m}\}$. Obviously, for any $m' \in M$, m' is a non unit in $\mathcal{R}$. The group of units in $\mathcal{R}$, denoted by $\mathcal{R}^*$, is $\{a + bu + cv + duv : a \in \mathbb{F}^*_{2^m}, b, c, d \in \mathbb{F}_{2^m}\}$. It is obvious that $\mathcal{R}^*$ is not cyclic and $\mathcal{R} = \mathcal{R}^* \cup M$.

2.2. Codes

A *linear code* C over R of length n is an R-submodule of R^n. For any $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in R^n$, their standard inner product is defined by $\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i$, where the operation is performed in R. The *dual code* of C is denoted by $C^\perp$ and defined as $C^\perp = \{y \in R^n | \langle x, y\rangle = 0, \forall x \in C\}$.

We note that the Lee weight of an element $a + bu + cv + duv \in R$ was defined in [10] to be the Hamming weight of the binary vector $(d, c + d, b + d, a + b + c + d)$. This leads to the Gray map $\phi : R^n \to \mathbb{F}_2^{4n}$:

$$\phi(\mathbf{a} + \mathbf{b}u + \mathbf{c}v + \mathbf{d}uv) = (\mathbf{d}, \mathbf{c} + \mathbf{d}, \mathbf{b} + \mathbf{d}, \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{d}),$$

where $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in \mathbb{F}_2^n$. As was observed in [10], ϕ is a distance preserving isometry from (R^n, d_L) to $(\mathbb{F}_2^{4n}, d_H)$, where d_L and d_H denote the Lee and Hamming distance in R^n and $\mathbb{F}_2^{4n}$, respectively. This means if C is a linear code over R with parameters $(n, 2^k, d)$, then $\phi(C)$ is a binary linear code of parameters $[4n, k, d]$.

Given a finite abelian group G, a code over R is said to be *abelian* if it is an ideal of the group ring $R[G]$. In other words the coordinates of C are indexed by elements of G and G acts regularly on this set. In the special case when G is cyclic, the code is a cyclic code in the usual sense [11].

3. Symmetry

For $a \in \mathcal{R}$, define the vector $Ev(a)$ by the following evaluation map $Ev(a) = (Tr(ax))_{x\in\mathcal{R}^*}$. Define the code C_m by the formula $C_m = \{Ev(a)|a \in \mathcal{R}\}$.

Proposition 3.1. *The group of units $\mathcal{R}^*$ acts regularly on the coordinates of C_m.*

Proof. For any $v', u' \in \mathcal{R}^*$, the change of variables $x \mapsto (u'/v')x$ permutes the coordinates of C_m, and maps v' to u'. Such a permutation is unique, given v', u'.

The code C_m is thus an *abelian code* with respect to the group $\mathcal{R}^*$. In other words, it is an ideal of the group ring $R[\mathcal{R}^*]$. As observed in the previous section, $\mathcal{R}^*$ is not a cyclic group, hence C_m may be not cyclic. The next result shows that its binary image is also abelian.

Proposition 3.2. *A finite group of size $4|\mathcal{R}^*|$ acts regularly on the coordinates of $\phi(C_m)$.*

Proof. By the definition of the Gray map, $\phi(\mathbf{a} + \mathbf{b}u + \mathbf{c}v + \mathbf{d}uv) = (\mathbf{d}, \mathbf{c} + \mathbf{d}, \mathbf{b} + \mathbf{d}, \mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{d})$, where $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}$ denote binary vectors. Now if $\mathbf{a} + \mathbf{b}u + \mathbf{c}v + \mathbf{d}uv \in C_m$, by linearity $(1 + u)(\mathbf{a} + \mathbf{b}u + \mathbf{c}v + \mathbf{d}uv) = \mathbf{a} + (\mathbf{a} + \mathbf{b})u + \mathbf{c}v + (\mathbf{c} + \mathbf{d})uv \in C_m$, $(1 + v)(\mathbf{a} + \mathbf{b}u + \mathbf{c}v + \mathbf{d}uv) = \mathbf{a} + \mathbf{b}u + (\mathbf{a} + \mathbf{c})v + (\mathbf{b} + \mathbf{d})uv \in C_m$ and $(1 + u + v + uv)(\mathbf{a} + \mathbf{b}u + \mathbf{c}v + \mathbf{d}uv) = \mathbf{a} + (\mathbf{a} + \mathbf{b})u + (\mathbf{a} + \mathbf{c})v + (\mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{d})uv \in C_m$. Further $\phi(\mathbf{a}+(\mathbf{a}+\mathbf{b})u+\mathbf{c}v+(\mathbf{c}+\mathbf{d})uv) = (\mathbf{c}+\mathbf{d}, \mathbf{d}, \mathbf{a}+\mathbf{b}+\mathbf{c}+\mathbf{d}, \mathbf{b}+\mathbf{d})$, $\phi(\mathbf{a}+\mathbf{b}u+(\mathbf{a}+\mathbf{c})v+(\mathbf{b}+\mathbf{d})uv) = (\mathbf{b}+\mathbf{d}, \mathbf{a}+\mathbf{b}+\mathbf{c}+\mathbf{d}, \mathbf{d}, \mathbf{c}+\mathbf{d})$, and $\phi(\mathbf{a} + (\mathbf{a} + \mathbf{b})u + (\mathbf{a} + \mathbf{c})v + (\mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{d})uv) = (\mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{d}, \mathbf{b} + \mathbf{d}, \mathbf{c} + \mathbf{d}, \mathbf{d})$, so that $\phi(C_m)$ is invariant under an involution that permutes the four parts of a codeword. Thus, $\phi(C_m)$ is invariant under the regular action of $\mathcal{R}^*$.

4. The Lee weight enumerator of C_m

In order to determine the Lee weight of the codewords of the code C_m, we first recall the following classic lemmas.

Please cite this article in press as: M. Shi, et al., Optimal binary codes from trace codes over a non-chain ring, Discrete Applied Mathematics (2016), http://dx.doi.org/10.1016/j.dam.2016.09.050