Torsion Codes over a Finite Chain Rings

M. Mehrdad

Abstract

In this paper we study codes over finite chain rings. We also give sufficient conditions on the existence of MDR codes over finite chain rings. Torsion codes over residue fields of finite chain rings are introduced, and some of their properties are derived. Finally, we show that there are no non-trivial MDR codes over $R$, when $R$ be a chain ring with maximal ideal $m = R\gamma$, with $R/m$ isomorphic to $\mathbb{F}_2$. Using generalized Chinese remainder theorems, codes over local rings will be studied.

Keywords: Finite chain rings, Linear codes, Torsion codes.

AMS Classification: 94B65

1 Introduction

The main coding problem for linear codes is to find the largest minimum weight for any linear code. The study of codes over finite rings other than finite fields goes back to early 1970’s. For example, there had been some papers on codes over $\mathbb{Z}_m$. Recently, authors have been considered codes over finite chain rings (Please see, [3]). We refer to [2] for any undefined terms from coding theory. We begin with some definitions.

In this paper, we define Torsion codes over residue fields from codes over finite chain rings.

2 Theorems and lemmas

For a linear code $C$ of length $n$ over $R$, we define the rank of $C$, denoted by $\text{rank}(C)$, to be the minimum number of generators of $C$. The weight of a
vector is the number of non-zero coordinates of a vector and for a code $C$ we denote by $d_H(C)$ the non-zero minimum Hamming distance of the code.

It is well known (see [2] for example) that for codes $C$ of length $n$ over any alphabet of size $m$

$$d_H(C) \leq n - \log_m(|C|) + 1.$$  

(1)

Codes meeting this bound are called MDS (Maximum Distance Separable) codes.

Further if $C$ is linear, then

$$d_H(C) \leq n - \text{rank}(C) + 1.$$  

(2)

Codes meeting this bound called MDR (Maximum Distance with respect to Rank) codes. We define $K(C) = \sum_{i=1}^{e-1} K_i(C)$ to be the number of rows in a generator matrix in standard form of $C$. Clearly, $K(C) = \text{rank}(C)$, when $C$ is linear code.

**Definition 1.** A finite commutative ring with identity $1 \neq 0$ is called a finite chain ring if its ideals are linearly ordered by inclusion.

**Definition 2.** Local principal ideal rings are called chain rings. If $a$ is an ideal of a finite ring, then the chain $a \supset a^2 \supset a^3 \supset \cdots$ stabilizes. The smallest $t \geq 1$ such that $a^t = a^{t+1} = \cdots$ is called the index of stability of $a$. If $a$ is nilpotent, then the smallest $t \geq 1$ such that $a^t = 0$ is called the index of nilpotency of $a$ and it is then the same as the index of stability of $a$.

**Definition 3.** Let $C$ be a linear codes over $R$. Consider the codes $(C : \gamma^i) = \{V \mid \gamma^i V \in C\}$, $i = 0, 1, \ldots, e - 1$, over $R$. Let “$\quad\mapsto$” denote the canonical map $R^n \rightarrow (R/m)^n$, $n \geq 1$. The codes $\text{Tor}_i(C) = (C : \gamma^i)$ over the field $R/m$ ($i = 1, 2, \ldots, e - 1$), are called the torsion codes associated to the code $C$. The code $\text{Res}(C) = \text{Tor}_0(C) = (C : \gamma^0) = \overline{C}$ over $R/m$ is called the residue code associated to the code $C$.

**Proposition 1.** If $C$ is a code over $R$, then $\min\{d_H(\text{Tor}_i(C))\} \geq d_H(C)$.

**Lemma 1.** Let $R$ be a chain ring with maximal ideal $m = R\gamma$ with nilpotency index $e$. If there exists an MDS code of length $n$ and rank $k$ over $R$, then $\text{Tor}_i(C) = \text{Tor}_j(C)$ for all $0 \leq i, j \leq e - 1$, and it is an MDS code of length $n$ and dimension $k$ over the field $R/m$. 
Theorem 1. Let $R$ be a chain ring with maximal ideal $m = R\gamma$ with nilpotency index $e$. If there exists an MDR code over $R$, then $\text{Tor}_{e-1}(C)$ is an MDS code over the field $R/m$.

These results give that if there are MDS and MDR codes over a finite chain ring, then there must be MDS codes of the same length and rank over the base field.

3 Results

Result 1. If $C$ is a code over $R$, then $|C| = \prod_{j=0}^{e-1} |\text{Tor}_{i}(C)|$.

proof: Let $|R/m| = q = p^e$, then given the generator matrix for the code $C$ over $R$ of the form:

$$
\begin{pmatrix}
I_{k_0} & A_{0,1} & A_{0,2} & \cdots & \cdots & A_{0,e-1} \\
0 & \gamma I_{k_1} & \gamma A_{1,2} & \cdots & \gamma A_{1,e-1} \\
0 & 0 & \gamma^2 I_{k_2} & \cdots & \gamma^2 A_{2,e-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & \gamma^{e-1} I_{k_{e-1}} \\
0 & 0 & 0 & \cdots & \gamma^{e-1} A_{i,e-1}
\end{pmatrix} \sim \begin{pmatrix}
A_{0,e-1} \\
\gamma A_{1,e-1} \\
\gamma^2 A_{2,e-1} \\
\vdots \\
\gamma^{e-1} A_{i-1,e-1}
\end{pmatrix},
$$

the code $\text{Tor}_{i}(C)$ is the code over $R/m$ generated by:

$$
\begin{pmatrix}
I_{k_0} & A_{0,1} & A_{0,2} & \cdots & \cdots & A_{0,e-1} \\
0 & I_{k_1} & A_{1,2} & \cdots & \cdots & A_{1,e-1} \\
0 & 0 & I_{k_2} & \cdots & \cdots & A_{2,e-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & I_{k_{i-1}} & A_{i,e-1}
\end{pmatrix} \sim \begin{pmatrix}
A_{0,e-1} \\
A_{1,e-1} \\
A_{2,e-1} \\
\vdots \\
A_{i,e-1}
\end{pmatrix}.
$$

We can compute the cardinality of $C$ in general by

$$
|C| = \prod_{j=0}^{e-1} (\gamma^j R)^{k_j} = |R/m|^{\sum_{j=0}^{e-1} (e-j)k_j} = (q^{\sum_{j=0}^{e-1} (e-j)k_j}).
$$

Given a code $C$ over $R$ we have that

$$
|\text{Tor}_{i}(C)| = \prod_{j=0}^{i} |q|^{k_j},
$$
and by using (3) gives

\[ |C| = (q)^{\sum_{j=0}^{e-1}(e-j)k_j} = \prod_{j=0}^{i} |q|^{\sum_{j\leq i} k_i} = \prod_{s=0}^{e-1} \prod_{j=0}^{i} |q|^{k_j} = \prod_{s=0}^{e-1} |\text{Tor}_s(C)|. \]

**Result 2.** Let \( R \) be a chain ring with maximal ideal \( m = R\gamma \), with \( R/m \) isomorphic to \( \mathbb{F}_2 \). Then, there are no non-trivial MDS or MDR codes over \( R \).

**Result 3.** Let \( R \) be a chain ring with maximal ideal \( m = R\gamma \) and \( q = \prod p_i^{e_i} \) with \( p_i \neq p_j \) when \( i \neq j \). If \( p_i > \binom{n-1}{n-k-1} \) for some integers \( n, k \) with \( n-k-1 > 0 \). Then, there exists an \([n, k, n-k+1] \) MDS code over \( R \).

**References**

