MDS Codes over Finite Principal Ideal Rings

Steven T. Dougherty
Department of Mathematics
University of Scranton
Scranton, PA 18510, USA
Email: doughertys1@scranton.edu
Jon-Lark Kim*
Department of Mathematics,
University of Louisville
Louisville, KY 40292, USA,
Email: jl.kim@louisville.edu
and
Hamid Kulosman
Department of Mathematics,
University of Louisville
Louisville, KY 40292, USA,
Email: h0kulo01@louisville.edu

(2/28/08)

*Corresponding Author, Department of Mathematics, University of Louisville, 328 Natural Sciences Building, Louisville, KY 40292, jl.kim@louisville.edu, Tel: 1-502-852-2727, Fax: 1-502-852-7132

Abstract

The purpose of this paper is to study codes over finite principal ideal rings. To do this, we begin with codes over finite chain rings as a natural generalization of codes over Galois rings $GR(p^e, l)$ (including $\mathbb{Z}_{p^e}$). We give sufficient conditions on the existence of MDS codes over finite chain rings and on the existence of self-dual codes over finite chain rings. We also construct MDS self-dual codes over Galois rings $GF(2^e, l)$ of length $n = 2^l$ for any $a \geq 1$ and $l \geq 2$. Torsion codes over residue fields of finite chain rings are introduced, and some of their properties are derived. Finally, we describe MDS codes and self-dual codes over finite principal ideal rings by examining codes over their component chain rings, via a generalized Chinese remainder theorem.

Key Words: Chain ring, Galois ring, MDS code, principal ideal ring.

1 Introduction

Codes over finite rings, especially over $\mathbb{Z}_4$, have been of great interest due to Nechaev [21] and Hammons, et. al. [13]. Some of the main results of [13] are that Kerdock and Preparata codes are linear over $\mathbb{Z}_4$ via the Gray map from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$, and that as $\mathbb{Z}_4$-codes they are duals [13]. However, 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 $\mathbb{Z}_m$ (e.g., Blake [1], [2], Spiegel [25], [26]), and codes over Galois rings $GR(p^e, l)$ (e.g., Shankar [24]).

Recently people have considered codes over finite chain rings (e.g., [16] (references therein), [14]) and codes over finite Frobenius rings (e.g., [28], [11]) with respect to homogeneous weights [6]. For codes over finite rings or Galois rings, we refer to [19] and [27]. Codes over rings have been shown to have interesting connections to lattices, modular forms [20], and Hjelmslev geometries [14] as well as to many other branches of mathematics (see [23] for a complete description). We refer to [17] for any undefined terms from coding theory.

In this work we consider codes over finite principal ideal rings by examining codes over their component chain rings. We begin with some definitions.

Let R be a finite commutative ring with identity, $n \geq 1$ an integer. A subset C of R^n is called a *linear code of length n over R* if C is an R-submodule of R^n.

For a linear code C of length n over R, we define the rank of C, denoted by $rank(C)$, to be the minimum number of generators of C. We define the free rank of C, denoted by $free\ rank(C)$, to be the maximum of the ranks of free R-submodules of C. We shall say that a linear code is free if the free rank is equal to the rank, that is, a code is a free R-submodule. A free linear code is isomorphic as a module to R^k for some k. The weight of a vector is the number of non-zero coordinates of a vector and for a code C we denote by $d_H(C)$ (or simply d) the nonzero minimum Hamming distance of the code.

It is well known (see [17] for example) that for codes C of length n over any alphabet of size m

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

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

The definition that we give for MDS codes is consistent with much of the literature, however it is distinct from the definition given in [16]. Codes which are defined to be MDS in [16] would be MDR with our definition, which we define below. We define it this way since MDS is originally defined in a combinatorial manner and there are numerous equivalent combinatorial structures to MDS codes over arbitrary alphabets. MDR codes do not, in general, meet this bound. Hence we wish to be a distinction between the combinatorial bound and the algebraic bound.

Further if C is linear, then

$$d_H(C) \leq n - rank(C) + 1. \tag{2}$$

Codes meeting this bound are called *MDR (Maximum Distance with respect to Rank) codes.*

Note that in Section 2 we introduce a new notion: indices of stability of the maximal ideals of a (finite) ring and characterize principal ideal rings in terms of this notion. We essentially use this notion throughout the paper.

We begin with codes over finite chain rings as a natural generalization of codes over Galois rings $GR(p^e, l)$ (including $\mathbb{Z}_{p^e}$). Section 2 characterizes finite principal ideal rings in terms of indices of stability. Section 3 gives sufficient conditions on the existence of MDS codes over a finite chain ring (generally over a finite local Frobenius ring) and finds the number of free subcodes of any rank of a free code over a finite chain ring. In Section 4, we give sufficient conditions on the existence of self-dual codes over finite chain rings. We also construct MDS self-dual codes over Galois rings $GR(2^e, l)$ with parameters $[2^l, 2^{l-1}, 2^{l-1}+1]$ for any $e \geq 1$ and $l \geq 2$. In Section 5, we define Torsion codes over residue fields from codes over finite chain rings. Finally, in Section 6 we describe MDS codes and self-dual codes over principal ideal rings by examining codes over their component chain rings using generalized Chinese remainder theorem, the structure of modules over product rings, and indices of stability of the maximal ideals of finite rings.

2 Finite principal ideal rings

In this section, we characterize modules over a product of rings (Proposition 2.4 and Corollary 2.5) and finite principal ideal rings as a natural extension of finite chain rings (Proposition 2.7). The characterization of finite principal ideal rings is in terms of indices of stability of maximal ideals, which is a new notion that we introduce.

We assume that all rings in this paper are commutative and with identity. For all unexplained terminology and more detailed explanations, we refer to [5], [15] and [18] (related to algebra) and to [19] and [27] (related to finite rings).

Two ideals $\mathfrak{a}, \mathfrak{b}$ of a ring R are called *relatively prime* if $\mathfrak{a} + \mathfrak{b} = R$.

The next three lemmas are the well-known versions of the *Chinese Remainder Theorem.*

Lemma 2.1 ([18], Theorem 1.3 and 1.4)**.** *Let $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ be ideals of R. The following are equivalent:*

(i) For $i \neq j$, $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are relatively prime.

(ii) The canonical homomorphism $R \to \prod_{i=1}^{n}(R/\mathfrak{a}_i)$ is surjective.

If these conditions hold, then $\cap_{i=1}^{n}\mathfrak{a}_i = \prod_{i=1}^{n}\mathfrak{a}_i$ and the canonical homomorphism $\Phi : R/\mathfrak{a} \to \prod_{i=1}^{n}(R/\mathfrak{a}_i)$, where $\mathfrak{a} = \cap_{i=1}^{n}\mathfrak{a}_i$, is bijective.

A finite family $(\mathfrak{a}_i)_{i=1}^{n}$ of ideals of R, such that the canonical homomorphism of R to $\prod_{i=1}^{n}(R/\mathfrak{a}_i)$ is an isomorphism is called a *direct decomposition of R*.

Lemma 2.2 ([3], p. 110, Proposition 10)**.** *Let $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ be ideals of R. The following are equivalent:*

(i) A family $(\mathfrak{a}_i)_{i=1}^n$ is a direct decomposition of R;

(ii) For $i \neq j$, $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are relatively prime and $\cap_{i=1}^n \mathfrak{a}_i = \{0\}$;

(iii) For $i \neq j$, $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are relatively prime and $\prod_{i=1}^n \mathfrak{a}_i = \{0\}$;

(iv) There exists a family $(e_i)_{i=1}^n$ of idempotents of R such that $e_ie_j = 0$ for $i \neq j$, $1 = \sum e_i$ and $\mathfrak{a}_i = R(1 - e_i)$ for $i = 1, \ldots, n$.

Lemma 2.3 ([5], p. 54, Proposition 6)**.** *Let $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ be ideals of R, relatively prime in pairs and let $\mathfrak{a} = \cap_{i=1}^n \mathfrak{a}_i$. For every R-module M, the canonical homomorphism $M \to \prod_{i=1}^n (M/\mathfrak{a}_i M)$ is surjective and its kernel is $\mathfrak{a}M$.*

Let $(\mathfrak{a}_i)_{i=1}^n$ be a direct decomposition of R and let M be an R-module. Let $M_i = \{x \in M : \mathfrak{a}_i x = 0\}$. This is a submodule of M. Since $\mathfrak{a}_i \subset \mathrm{Ann}(M_i)$, we have a unique $R/\mathfrak{a}_i$-module structure on M_i such that the R-module structure of M_i is induced via the homomorphism $R \to R/\mathfrak{a}_i$. Moreover, we have $M_i = e_iM$ $(i = 1, \ldots, n)$ and the R-module M is the internal direct sum of its submodules M_i ([4], page A.VII.6, Proposition 1). Here the e_i are the idempotents from Lemma 2.2. We write $M = \oplus_{i=1}^n M_i$ and for every $x \in M$ we write $x = x_1 \oplus x_2 \oplus \cdots \oplus x_n$ to denote the unique way to write x as a sum of elements $x_i \in M_i$, $i = 1, \ldots, n$. Denote by $\Psi : M \to \prod_{i=1}^n M/\mathfrak{a}_i M$ the canonical isomorphism.

Proposition 2.4. *Let R be a commutative ring, $(\mathfrak{a}_i)_{i=1}^n$ a direct decomposition of R and M an R-module. With the notation as above we have:*

(i) For each $i = 1, \ldots, n$, the submodule $M_i = e_iM$ is a complement in M of the submodule $\mathfrak{a}_iM = (1 - e_i)M$ and so the $R/\mathfrak{a}_i$-modules M_i and $M/\mathfrak{a}_iM$ are isomorphic via the map $\psi_i : M_i \to M/\mathfrak{a}_iM$, $x \mapsto x + \mathfrak{a}_iM$.

(ii) The action of R on M, $(r, x) \mapsto rx$, can be identified with the componentwise actions

$$((r_1 + \mathfrak{a}_1, \ldots, r_n + \mathfrak{a}_n), x_1 \oplus \cdots \oplus x_n) \mapsto r_1x_1 \oplus \cdots \oplus r_nx_n,$$

$$((r_1 + \mathfrak{a}_1, \ldots, r_n + \mathfrak{a}_n), (x_1 + \mathfrak{a}_1M, \ldots, x_n + \mathfrak{a}_nM)) \mapsto (r_1x_1 + \mathfrak{a}_1M, \ldots, r_nx_n + \mathfrak{a}_nM)$$

of $\prod_{i=1}^n R/\mathfrak{a}_i$ on $M = \oplus_{i=1}^n M_i$ and $\prod_{i=1}^n M/\mathfrak{a}_iM$ respectively.

(iii) Every submodule N of M is an internal direct sum of submodules $N_i = e_iN \subset M_i$, which are isomorphic via ψ_i with the submodules $N_i' = (\mathfrak{a}_iM + e_iN)/\mathfrak{a}_iM$ of $M/\mathfrak{a}_iM$ $(i = 1, \ldots, n)$. Each N_i' is isomorphic to $N/\mathfrak{a}_iN$ and so the decomposition $N \to \oplus_{i=1}^n N_i' \subset \oplus_{i=1}^n M/\mathfrak{a}_iM$ canonically corresponds to the decomposition $N \to \oplus_{i=1}^n N/\mathfrak{a}_iN$.

Conversely, if for every $i = 1, \ldots, n$, N_i' is a submodule of $M/\mathfrak{a}_iM$, then there is a unique submodule $N = \oplus_{i=1}^n N_i$ of M, such that N is isomorphic with $\oplus_{i=1}^n N_i'$ via $\Psi = \oplus_{i=1}^n \psi_i$.

Proof. (i) Since e_i and $1 - e_i$ are idempotents whose sum is 1, the submodules e_iM and $(1 - e_i)M$ of M are complements of each other. Since the map $x \mapsto x + \mathfrak{a}_iM$ maps M

onto $M/\mathfrak{a}_iM$ and its kernel is $\mathfrak{a}_iM$, M_i and $M/\mathfrak{a}_iM$ are isomorphic via the restriction of that map $\psi_i : M_i \to M/\mathfrak{a}_iM$, $x \mapsto x + \mathfrak{a}_iM$.

(ii) This follows from Lemma 2.1 and Lemma 2.3.

(iii) The composition of the canonical injection of $N = (1-e_i)N \oplus e_iN$ into $(1-e_i)M \oplus e_iN$ with the map ψ_i has the same kernel e_iN as the canonical map of N onto $N/\mathfrak{a}_iN$. Hence the canonical correspondence of the decompositions.

Conversely, we have $N = \Psi^{-1}(\oplus_{i=1}^n N'_i) = (\oplus_{i=1}^n \psi_i^{-1})(\oplus_{i=1}^n N'_i) = \oplus_{i=1}^n \psi^{-1}(N'_i) = \oplus_{i=1}^n N_i$. □

When in part (iii) of the previous proposition we fix a module M and consider its submodules N and their decompositions $\oplus_{i=1}^n N'_i \subset \oplus_{i=1}^n M/\mathfrak{a}_iM$, we say that M is an *ambient R-module* and that $\oplus_{i=1}^n M/\mathfrak{a}_iM$ is its decomposition into the *ambient $R/\mathfrak{a}_i$-modules*. If the ambient module is $M = R^n$, then $M/\mathfrak{a}_iM = R^n/\mathfrak{a}_iR^n \cong R^n \otimes (R/\mathfrak{a}_i) \cong (R/\mathfrak{a}_i)^n$ and so $\oplus_{i=1}^n (R/\mathfrak{a}_i)^n$ is its decomposition into ambient $R/\mathfrak{a}_i$-modules. More concretely, if $R = \mathbb{Z}_m$, where $m = p_1^{t_1} \dots p_k^{t_k}$, with p_i different primes and $\mathfrak{a}_i = p_i^{t_i}\mathbb{Z}_m$, then the ambient module $M = R^n = \mathbb{Z}_m^n$ is decomposed into ambient $\mathbb{Z}_{p_i{}^{t_i}}$-modules $\mathbb{Z}_{p_i{}^{t_i}}^n$.

We denote the submodule $N = \Psi^{-1}(\oplus_{i=1}^n N'_i)$ of M from the part (iii) of the previous proposition by $CRT_M(N'_1, \dots, N'_n)$ or simply by $CRT(N'_1, \dots, N'_n)$ (see [10]).

For an R-module M we call the *rank of M* the minimum number of generators of M. We denote it by $\mathrm{rank}(M)$. The following corollary is used in Section 6 in order to study the Chinese product of codes over chain rings (see Lemma 6.1).

Corollary 2.5. *With the notation as before, let N'_i be a submodule of $M/\mathfrak{a}_iM$ $(i = 1, \dots, n)$ and let $N = CRT(N'_1, \dots, N'_n)$. Then:*

(i) $|N| = \prod_{i=1}^n |N'_i|$.

(ii) $\mathrm{rank}(N) = \max\{\mathrm{rank}(N'_i) \,:\, 1 \le i \le n\}$.

(iii) N is a free R-module if and only if each N'_i is a free $R/\mathfrak{a}_i$-module of the same rank.

Proof. (i) This follows from the fact that $N = \oplus_{i=1}^n N_i$ and $N_i \cong N'_i$ for each i.

(ii) By Proposition 2.4, we can identify the R-module N with the $(\prod_{i=1}^n R/\mathfrak{a}_i)$-module $\oplus_{i=1}^n N_i$ with the action defined componentwise. Let $r_i = \mathrm{rank}(N_i)$ and let $r = \max_{1 \le i \le n} r_i$. Let $< x_1^i, x_2^i, \dots, x_{r_i}^i, 0, \dots, 0 >$ be a system of generators of N_i, consisting of r elements, where $< x_1^i, x_2^i, \dots, x_{r_i}^i >$ is a minimal system of generators of N_i and the remaining $r - r_i$ elements are arbitrary, for example zeros. Then $< x_j^1 \oplus x_j^2 \oplus \dots \oplus x_j^n \,:\, j = 1, 2, \dots, r >$ is a system of generators of the $(\prod_{i=1}^n R/\mathfrak{a}_i)$-module $\oplus_{i=1}^n N_i$. We cannot have less than r generators since $\mathrm{rank}(N_i) = r$ for some i, hence on the i^{th} coordinate we need at least r different elements from N_i.

(iii) We form a minimal system of generators like in (ii). On each coordinate $s \in \{1, 2, \dots, n\}$ we have a minimal system of generators $< x_1^s, \dots, x_r^s >$ of the free $R/\mathfrak{a}_s$-module

N_s. Hence if $\sum_{j=1}^{r}(r_j^1,\dots,r_j^n)\,x_j^1\oplus\cdots\oplus x_j^n=0\oplus\cdots\oplus 0$, then from $\sum_{j=1}^{r} r_j^s x_j^s=0$, we get $r_j^s=0$ for $j=1,\dots,r$. This holds for any s, so all $(r_j^1,\dots,r_j^n)$ are $(0,\dots,0)$ $(j=1,2,\dots,r)$ and so $N=\prod_{i=1}^{n}N_i$ is free over $R\cong\prod_{i=1}^{n}R/\mathfrak{a}_i$. $\square$

Remark. In the part (iii) of the previous corollary, all the $R/\mathfrak{a}_i$-modules N_i' have to be free of the same rank, otherwise the statement is not true. Suppose, for example, that $k=2$ and let $N_1'=M/\mathfrak{a}_1M$ be a free $R/\mathfrak{a}_1$-module of rank 2 and $N_2'=M/\mathfrak{a}_2M$ a free $R/\mathfrak{a}_2$-module of rank 1. Then $\psi^{-1}(N_1')=M_1$ is a free $R/\mathfrak{a}_1$-module of rank 2 and $\psi^{-1}(N_2')=M_2$ is a free $R/\mathfrak{a}_2$-module of rank 1. By Proposition 2.4, the R-module $M=M_1\oplus M_2$ can be considered as a module over $R/\mathfrak{a}_1\times R/\mathfrak{a}_2$ with the action defined componentwise. Any minimal system of generators of this module should have two elements. If they are $x_1\oplus y_1$ and $x_2\oplus y_2$, then there are nonzero r_2 and s_2 from R_2 such that $(0,r_2)\,x_1\oplus y_1+(0,s_2)\,x_2\oplus y_2=0\oplus 0$. Hence $M_1\oplus M_2$ is not free over $R/\mathfrak{a}_1\times R/\mathfrak{a}_2$, i.e., M is not free over R.

The next lemma is a version of the well-known *Nakayama lemma.*

Lemma 2.6 ([18], Theorem 2.2)**.** *Let M be a finitely generated module over R, $\mathfrak{a}$ an ideal of R. Then $\mathfrak{a}M=M$ if and only if there is an element $a\in\mathfrak{a}$ such that $(1+a)M=0$.*

A ring R is called a *principal ideal ring* if every ideal of R is generated by one element. If R is a local principal ideal ring, with maximal ideal $\mathfrak{m}=R\gamma$ generated by an element $\gamma\in R$, then the ideals $\mathfrak{m}^k=R\gamma^k$, $k\geq 0$, are the only ideals of R. On the other side, if the ideals of a ring R are linearly ordered by inclusion, then the ring is a local principal ideal ring. Because of these observations, local principal ideal rings are called *chain rings.*

From now on we will be mainly interested in finite rings. If R is a **finite** ring, it has finitely many ideals, in particular finitely many maximal ideals, i.e., it is *semilocal.* Moreover, all prime ideals of R are maximal and so R is *zero-dimensional.* (Indeed, since finite integral domains are fields, then if $\mathfrak{p}$ is a prime ideal of R, the quotient $R/\mathfrak{p}$ is a field and so $\mathfrak{p}$ is a maximal ideal.)

The ring $\mathbb{Z}_m$, $m\geq 1$ an integer, is a finite principal ideal ring, which is not necessarily a chain ring. The ring $\mathbb{Z}_{p^e}$, p prime, $e\geq 1$ an integer, is a chain ring. More generally, the ring $GR(p^e,l)=\mathbb{Z}_{p^e}[X]/(f)$, where p is a prime, $e,l\geq 1$ integers, and f is a monic basic irreducible polynomial of degree l, is a chain ring with maximal ideal generated by p, and its residue field $GF(p^l)$. The ring $GR(p^e,l)$ is called a *Galois ring.* Especially, we note that $GR(p^e,1)\cong\mathbb{Z}_{p^e}$ and $GR(p,l)\cong GF(p^l)$.

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

Note that if R is local, then we necessarily have $\mathfrak{m}^t = \mathfrak{m}^{t+1} = \cdots = 0$. Indeed, if $\mathfrak{m} = 0$, this is clear. Suppose that $\mathfrak{m}^t = \mathfrak{m}^{t+1} = \cdots \neq 0$. Then by Lemma 2.6 there is an element $e \in \mathfrak{m}$, $e \neq 0$, such that $(1-e)\mathfrak{m}^t = 0$. Hence $1-e$ is not invertible. Then $R(1-e)$ would be an ideal contained in $\mathfrak{m}$. But then $e + (1-e) = 1 \in \mathfrak{m}$, a contradiction.

Thus in the case of finite local rings, the index of stability of $\mathfrak{m}$ is in fact the index of nilpotency of $\mathfrak{m}$.

On the other side, if R has at least two maximal ideals, then for any maximal ideal $\mathfrak{m}$, $\mathfrak{m}^t = \mathfrak{m}^{t+1} = \cdots \neq 0$. Otherwise, if $\mathfrak{n} \neq \mathfrak{m}$ is another maximal ideal, we would have $\mathfrak{n} \supset (0) = \mathfrak{m}^t$, hence $\mathfrak{n} \supset \mathfrak{m}$, a contradiction.

We now characterize a finite principal ideal ring. Parts (i) and (*ii*) of the following proposition is well-known and can also be proved using the structure theorem for Artinian rings. We include our proof for completeness since it further shows the role of indices of stability in the decomposition.

Proposition 2.7. *Let R be a finite commutative ring. Then the following are equivalent:*

(i) R is a principal ideal ring.

(ii) R is isomorphic to a finite product of chain rings.

Moreover, the decomposition in (ii) is unique up to the order of factors. It has the form $R \cong \prod_{i=1}^k R/\mathfrak{m}_i^{t_i}$, where $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_k$ are maximal ideals of R and $t_1, t_2, \ldots, t_k$ their indices of stability respectively.

Proof. (ii)$\Rightarrow$ (i): Let $R \cong \prod_{i=1}^k R_i$, where each R_i is a chain ring, in particular a principal ideal ring. The ideals of $\prod_{i=1}^k R_i$ have the form $\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_k$, where $\mathfrak{a}_i$ is an ideal of R_i for each i. Hence all the ideals of $\prod_{i=1}^k R_i$ (hence R) are principal.

(i)$\Rightarrow$ (ii): Let R be a principal ideal ring and $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_k$ its maximal ideals. If $k = 1$ we are done. Suppose $k > 1$. The maximal ideals of R are relatively prime in pairs. Since all finite rings are zero-dimensional, the ideals $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_k$ are at the same time minimal prime ideals of R. Hence $\cap_{i=1}^k \mathfrak{m}_i$ (i.e. $\mathfrak{m}_1\mathfrak{m}_2 \ldots \mathfrak{m}_k$) is a nil-radical of R. Hence there is an integer t such that $\mathfrak{m}_1^t\mathfrak{m}_2^t \ldots \mathfrak{m}_k^t = 0$. Hence $\mathfrak{m}_1^{t_1}\mathfrak{m}_2^{t_2} \ldots \mathfrak{m}_k^{t_k} = 0$ (for if $t \geq t_i$ then $\mathfrak{m}_i^t = \mathfrak{m}_i^{t_i}$; if $t \leq t_i$ then $\mathfrak{m}_i^{t_i} \subset \mathfrak{m}_i^t$). Since $\mathfrak{m}_1^{t_1}, \mathfrak{m}_2^{t_2}, \ldots \mathfrak{m}_k^{t_k}$ are also relatively prime in pairs, we have $\mathfrak{m}_1^{t_1}\mathfrak{m}_2^{t_2} \ldots \mathfrak{m}_k^{t_k} = \cap_{i=1}^k \mathfrak{m}_i^{t_i} = 0$. Now by Lemma 2.1 we have $R \cong \prod_{i=1}^k R/\mathfrak{m}_i^{t_i}$. Each of the rings $R/\mathfrak{m}_i^{t_i}$ is a chain ring with maximal ideal $\mathfrak{m}_i/\mathfrak{m}_i^{t_i}$.

We now prove the uniqueness of the decomposition in (ii). In general, suppose that we have an isomorphism $f : \prod_{i=1}^k R_i \to \prod_{j=1}^l S_j$ of two products of local rings $(R_i, \mathfrak{m}_i)$ and $(S_j, \mathfrak{n}_j)$. Then $k = l$ (by counting the maximal ideals in each of the products). Moreover the maximal ideal $\mathfrak{M}_1 = \mathfrak{m}_1 \times R_2 \times \cdots \times R_k$ of $\prod_{i=1}^k R_i$ corresponds under f to a maximal ideal, say $\mathfrak{N}_1 = \mathfrak{n}_1 \times S_2 \times \cdots \times S_k$, of $\prod_{i=1}^k S_i$. Now the localizations $(R_1 \times \cdots \times R_k)_{\mathfrak{M}_1} \cong (R_1)_{\mathfrak{m}_1} \cong R_1$ and $(S_1 \times \cdots \times S_k)_{\mathfrak{N}_1} \cong (S_1)_{\mathfrak{n}_1} \cong S_1$ are isomorphic, so $R_1 \cong S_1$. Similarly for other factors. This proves the uniqueness of the decomposition in (ii). □

If R is a finite principal ideal ring, we say that the decomposition of R into a product of finite chain rings, as in (ii), is a *canonical decomposition of* R.

Remark. We want to generalize the procedure by which we reduce the investigation of the codes over $\mathbb{Z}_m$, where $m = p_1^{e_1} \dots p_k^{e_k}$, with p_i prime numbers and e_i positive integers, to the investigation of codes over $\mathbb{Z}_{{p_i}^{e_i}}$. The previous proposition replaces the ring $\mathbb{Z}_m$ by any principal ideal ring and the rings $\mathbb{Z}_{{p_i}^{e_i}}$ by the chain rings. The stability indices of the maximal ideals of a principal ideal ring R, which appear in the decomposition $R \cong \prod_{i=1}^{k} R/m_i^{t_i}$, are analogues of the exponents e_i in the decomposition $\mathbb{Z}_m \cong \prod_{i=1}^{k} \mathbb{Z}_{{p_i}^{e_i}}$. For example, the ring $\mathbb{Z}_{144} = \mathbb{Z}_{2^4 3^2}$ is isomorphic to $\mathbb{Z}_{2^4} \times \mathbb{Z}_{3^2}$. The stability indices of the maximal ideals $2\mathbb{Z}_{2^4 3^2}$ and $3\mathbb{Z}_{2^4 3^2}$ of the ring $\mathbb{Z}_{2^4 3^2}$ are 4 and 2 respectively. So the decomposition $\mathbb{Z}_{2^4} \times \mathbb{Z}_{3^2}$ of $\mathbb{Z}_{2^4 3^2}$ is precisely the decomposition that would be obtained from the previous proposition.

3 Bounds for MDS codes over finite chain rings

The study of codes over finite principal rings is reduced to that of codes over chain rings from the previous discussion. So this section deals with (MDS) codes over finite chain rings, more generally over finite local Frobenius rings.

We generalize results in [8] on MDS codes over $\mathbb{Z}_{p^e}$, and give a sufficient condition for the existence of such codes over finite chain rings (Corollary 3.6), which is used for the existence of MDS codes over finite principal ideal rings in Section 6.

The definitions of quasi-Frobenius and Frobenius rings can be seen for example in [28]. In this paper we deal with commutative rings and in that context quasi-Frobenius and Frobenius are equivalent notions. The following definition is convenient for our purposes: *a finite commutative ring R is Frobenius if the R-module R is injective* ([28, Theorem 1.2]).

Lemma 3.1 ([5], p. 84, Cor.1 & 2)**.** *Let $(R, \mathfrak{m})$ be a finite local ring, M a free R-module. A family (x_λ) of elements of M is a basis of a direct summand of M if and only if the family $(\overline{x_\lambda})$ is free in $M/\mathfrak{m}M$.*

Lemma 3.2. *Let R be a finite local Frobenius ring. Consider the R-module R^r, $r \geq 1$ an integer. Suppose that $\mathbf{v}_1, \cdots, \mathbf{v}_{t-1} \in R^r$ are linearly independent. If $\mathbf{v}_t \notin \langle \mathbf{v}_1, \cdots, \mathbf{v}_{t-1}, \mathfrak{m}R^r \rangle$, then $\mathbf{v}_1, \cdots, \mathbf{v}_{t-1}, \mathbf{v}_t$ are linearly independent.*

Proof. Since $\mathbf{v}_1, \cdots, \mathbf{v}_{t-1}$ are linearly independent, $\langle \mathbf{v}_1, \cdots, \mathbf{v}_{t-1} \rangle$ is isomorphic to the free module R^{t-1}, which is injective since R is injective. Since injective modules are direct summands of all modules that contain them, $\langle \mathbf{v}_1, \cdots, \mathbf{v}_{t-1} \rangle$ is a direct summand of R^r and $\mathbf{v}_1, \cdots, \mathbf{v}_{t-1}$ is its basis. Hence, by Lemma 3.1, $\overline{\mathbf{v}_1}, \cdots, \overline{\mathbf{v}_{t-1}}$ are free in $R^r/\mathfrak{m}R^r$. If $\mathbf{v}_t \notin \langle \mathbf{v}_1, \cdots, \mathbf{v}_{t-1} \rangle + \mathfrak{m}R^r$, then $\overline{\mathbf{v}_t} \notin \langle \overline{\mathbf{v}_1}, \cdots, \overline{\mathbf{v}_{t-1}} \rangle$, hence $\overline{\mathbf{v}_1}, \cdots, \overline{\mathbf{v}_t}$ are free in $R^r/\mathfrak{m}R^r$.

Consequently, by Lemma 3.1, $\mathbf{v}_1, \cdots, \mathbf{v}_t$ form a basis of a direct summand of R^r. Hence they are linearly independent. $\square$

In the above lemma it is essential that R is a local ring and also that the module is a free R-module R^r, as the next example illustrates.

Example 1. Consider the local ring $R = \mathbb{Z}_4$, $\mathfrak{m} = 2R = \{0,2\}$. Let $M = \{0,2\} \times \{0,2\} \times \mathbb{Z}_4 \subset \mathbb{Z}_4^3$. Then $\mathfrak{m}M = \{(0,0,0),(0,0,2)\}$. Let $\mathbf{v}_1 = (0,0,1)$. This vector is linearly independent. We have $< \mathbf{v}_1, \mathfrak{m}M >= \{(0,0,0),(0,0,1),(0,0,2),(0,0,3)\}$. Now let $\mathbf{v}_2 = (0,2,1) \notin < \mathbf{v}_1, \mathfrak{m}M >$. But $\mathbf{v}_1$ and $\mathbf{v}_2$ are not linearly independent since $2\mathbf{v}_1 + 2\mathbf{v}_2 = (0,0,0)$.

Lemma 3.3. *Let R be a finite local Frobenius ring. If $\mathbf{v}_1, \cdots, \mathbf{v}_t \in R^r$ are linearly independent, then*

$$|\langle \mathbf{v}_1, \cdots, \mathbf{v}_t, \mathfrak{m}R^r \rangle| = q^t (|R|/q)^r,$$

where $|R/\mathfrak{m}| = q$.

Proof. Since $\mathbf{v}_1, \cdots, \mathbf{v}_t$ are linearly independent and R is Frobenius, $\langle \mathbf{v}_1, \cdots, \mathbf{v}_t \rangle$ is a direct factor of R^r (as in Lemma 3.2). Hence, by Lemma 3.1, the family $\overline{\mathbf{v}_1}, \cdots, \overline{\mathbf{v}_t}$ is free in $R^r/\mathfrak{m}R^r$. Let $\overline{\mathbf{v}_1}, \cdots, \overline{\mathbf{v}_t}, \overline{\mathbf{v}_{t+1}}, \cdots, \overline{\mathbf{v}_r}$ be a basis of $R^r/\mathfrak{m}R^r$. (It has r elements since the canonical basis of R^r has r elements, hence, by Lemma 3.1, the images of the elements of the canonical basis form a free family in $R^r/\mathfrak{m}R^r$.) Then, by Lemma 3.1, $\mathbf{v}_1, \cdots, \mathbf{v}_t, \mathbf{v}_{t+1}, \cdots, \mathbf{v}_r$ is a basis of R^r and $\langle \mathbf{v}_1, \cdots, \mathbf{v}_t \rangle + \langle \mathbf{v}_{t+1}, \cdots, \mathbf{v}_r \rangle = R^r$ is a direct sum. Now $\langle \mathbf{v}_1, \cdots, \mathbf{v}_t, \mathfrak{m}R^r \rangle = \langle \mathbf{v}_1, \cdots, \mathbf{v}_t \rangle + \mathfrak{m}(\langle \mathbf{v}_1, \cdots, \mathbf{v}_t \rangle + \langle \mathbf{v}_{t+1}, \cdots, \mathbf{v}_r \rangle) = \langle \mathbf{v}_1, \cdots, \mathbf{v}_t \rangle + \mathfrak{m} \langle \mathbf{v}_{t+1}, \cdots, \mathbf{v}_r \rangle$. This set has $|R|^t |\mathfrak{m}|^{r-t} = q^t(|R|/q)^r$ elements. $\square$

Following the Gilbert-Varshamov construction [17, p. 33] used in the proof in [8], we obtain the following theorem.

Theorem 3.4. *Suppose $\binom{n-1}{d-2} < \frac{q^{n-k}-1}{q^{d-2}-1}$. Let $(R, \mathfrak{m})$ be any finite local Frobenius ring with $|R/\mathfrak{m}| = q$. Then there exists a free code over R of length n and rank k with minimum distance d.*

Proof. We shall construct an $(n-k)$ by n parity check matrix H such that no $d-1$ columns are linearly dependent. Let $r = n-k$. The first column can be any $\mathbf{v}_1 \in R^r$, but not in $\mathfrak{m}R^r$. Suppose that we have chosen $t-1$ columns $\mathbf{v}_1, \cdots, \mathbf{v}_{t-1} \in R^r$ so that no $d-1$ columns are linearly dependent. Suppose there is a column $\mathbf{v}_t \notin \cup \left\langle \mathbf{v}_{i_1}, \cdots, \mathbf{v}_{i_{d-2}}, \mathfrak{m}R^r \right\rangle$, where the union is taken over all possible choices of $d-2$ columns from the $t-1$ columns. Then no $d-1$ from the t columns $\mathbf{v}_1, \cdots, \mathbf{v}_t$ are linearly dependent. Such a vector would exist if $| \cup \left\langle \mathbf{v}_{i_1}, \cdots, \mathbf{v}_{i_{d-2}}, \mathfrak{m}R^r \right\rangle | < |R|^r$. Now for all $t \leq n$,

$$\begin{aligned}
|\cup \left\langle \mathbf{v}_{i_1}, \cdots, \mathbf{v}_{i_{d-2}}, \mathfrak{m}R^r \right\rangle| &\leq \binom{t-1}{d-2} |\left\langle \mathbf{v}_1, \cdots, \mathbf{v}_{d-2}, \mathfrak{m}R^r \right\rangle| - \left(\binom{t-1}{d-2} - 1 \right) |\mathfrak{m}R^r| \\
&\leq \binom{n-1}{d-2} \left\{ q^{d-2}(|R|/q)^r - (|R|/q)^r \right\} + (|R|/q)^r \\
&= (|R|/q)^r \left(\binom{n-1}{d-2}(q^{d-2}-1) + 1 \right) \\
&< (|R|/q)^r (q^{n-k}) \text{ by hypothesis} \\
&= |R|^r.
\end{aligned}$$

Thus the theorem follows. □

Theorem 3.5. *If $q > \binom{n-1}{n-k-1}$ with $n-k-1 > 0$, then there exists an MDS $[n, k, n-k+1]$ code over any finite local Frobenius ring $(R, \mathfrak{m})$ with $|R/\mathfrak{m}| = q$.*

Proof. Note that the inequality of Theorem 3.4 is independent of R. If $d = n-k+1$ then the inequality of Theorem 3.4 becomes $\binom{n-1}{n-k-1} < \frac{q^{n-k}-1}{q^{n-k-1}-1}$. Since $q < \frac{q^{n-k}-1}{q^{n-k-1}-1} \leq q+1$ for any n and k such that $n > k+1$, the theorem follows. □

Since a finite chain ring is a finite local Frobenius ring, we have the following.

Corollary 3.6. *If $q > \binom{n-1}{n-k-1}$ with $n-k-1 > 0$, then there exists an MDS $[n, k, n-k+1]$ code over any finite chain ring $(R, \mathfrak{m})$ with $|R/\mathfrak{m}| = q$.*

We can use the ideas exhibited in this section to count the number of free subcodes of a given rank. Note that if the restriction of the codes being free is removed, then the counting is not possible by simply knowing the rank. For example, given a nonzero ring R, the ring is a code of rank 1 and every nonzero ideal of R is a subcode of rank 1. Hence the number of subcodes of rank 1 is equal to the number of nonzero ideals of R. However, a minimal nonzero ideal $\mathfrak{a}$ has only itself as a subcode of rank 1.

Recall that the number of subspaces of an s-dimensional space of dimension k over a field of order p is denoted $\begin{bmatrix} s \\ k \end{bmatrix} = \frac{(p^s-1)(p^s-p)\dots(p^s-p^{k-1})}{(p^k-1)(p^k-p)\dots(p^k-p^{k-1})}$. Using the simple ideas discussed in the section, we obtain an analogous result to this over a chain ring as follows. We note that more general counting arguments using projective Hjelmslev geometries can be found in [14].

Theorem 3.7. *Let C be a free code of rank s over a chain ring R with $|R| = q = p^e$. Then the number of free subcodes of rank k is*

$$p^{(sk-k^2)(e-1)} \begin{bmatrix} s \\ k \end{bmatrix}. \qquad (3)$$

Proof. We shall construct a minimal generating set of a free subcode of rank k. Note that

$$\mathfrak{m}R^r = \{\mathbf{w} \in R^r \mid |\langle \mathbf{w} \rangle| < |R|\}.$$

Then the number of ways of picking the first vector from C is

$$(p^e)^s - (p^{e-1})^s = (p^{e-1})^s(p^s - 1),$$

since we cannot have a vector in $\mathfrak{m}R^r$. To pick the second vector there are

$$p^{es} - (p^{(e-1)s+1})$$

as was shown in Lemma 3.3. We continue in this manner choosing k vectors. We must divide this number by the number of ways of producing k linearly independent vectors that generate the space. It follows that the number of free subspaces of rank k of an s dimensional space is

$$\frac{((p^{e-1})^s)^k(p^s-1)(p^s-p)\dots(p^s-p^{k-1})}{((p^{e-1})^k)^k(p^k-1)(p^k-p)\dots(p^k-p^{k-1})}.$$

□

4 Self-dual codes over finite chain rings

In this section we show that there exist self-dual codes of any length over a finite chain ring R with even nilpotency index e of $\mathfrak{m}$. This is generalized to self-dual codes over finite principal ideal rings in Section 6. We also construct MDS self-dual codes over Galois rings.

Let R be a finite chain ring with maximal ideal $\mathfrak{m} = R\gamma$ with e its nilpotency index. The generator matrix for a code C over R can be placed in the following form:

$$\begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & \cdots & A_{0,e} \\ 0 & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & \cdots & \cdots & \gamma A_{1,e} \\ 0 & 0 & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & \cdots & \cdots & \gamma^2 A_{2,e} \\ \vdots & \vdots & 0 & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \gamma^{e-1} I_{k_{e-1}} & \gamma^{e-1} A_{e-1,e} \end{pmatrix}, \tag{4}$$

Given a code C with this generator matrix we have (see [16]) that

$$|C| = |R/\mathfrak{m}|^{\sum_{i=0}^{e-1}(e-i)k_i}. \tag{5}$$

The form of the generator matrix for a code over a ring that is not a chain ring is problematic, see [22]. As an example of the difficulty, consider the ring that has α and β

that generate relatively prime non-trivial ideals. The code generated by (α, β) is generated by a single element and has cardinality $|R|$ but does not have a generator matrix of the form $(1, \delta)$ as we would desire.

We define the following inner product on R^n: for $\mathbf{v} = (v_1, \cdots, v_n)$ and $\mathbf{w} = (w_1, \cdots, w_n)$,

$$[\mathbf{v}, \mathbf{w}] = \sum v_i w_i. \tag{6}$$

We define the orthogonal of the code $C^\perp$ by

$$C^\perp = \{\mathbf{w} \mid [\mathbf{w}, \mathbf{v}] = 0 \text{ for all } \mathbf{v} \in C\}. \tag{7}$$

By the results in [28] we know that if R is a Frobenius ring, then $C^\perp$ is linear and $|C||C^\perp| = |R|^n$. A code C is said to be self-dual if $C = C^\perp$.

We notice that the linear codes of length 1 are precisely the ideals of R.

Remark. For an ideal I of any finite commutative ring R the following are equivalent.

(a) $I^2 = 0$ and $|I| = \sqrt{|R|}$.

(b) I is a self-dual code (of length 1).

If the Jacobson radical $\mathrm{rad}(R)$ of any finite commutative ring R has an even nilpotency index e, then it produces the self-dual code $I = \mathrm{rad}(R)^{\frac{e}{2}}$ of length 1 provided I has $\sqrt{|R|}$ elements. In particular, if R is a chain ring, we have the following.

Corollary 4.1. *Let R be a chain ring with maximal ideal $\mathfrak{m} = R\gamma$ with e its nilpotency index. If e is even, then $R\gamma^{\frac{e}{2}}$ is a self-dual code of length one.*

Proof. Let $C = R\gamma^{\frac{e}{2}}$. We know $(\gamma^{\frac{e}{2}})^2 = 0$ so $C \subseteq C^\perp$. However, $C^\perp$ must be of the form $R\gamma^s$ for some s since it is an ideal in R. Then since $\gamma^{\frac{e}{2}-1} \notin C^\perp$ we have that $C = C^\perp = R\gamma^{\frac{e}{2}}$. □

We can easily see the maximal ideal $\mathfrak{m}$ is a self-dual code exactly when $e = 2$ or equivalently $|\mathfrak{m}| = \sqrt{|R|}$. If $|\mathfrak{m}| = \sqrt{|R|}$ then $|\mathfrak{m}||\mathfrak{m}^\perp| = |R|$. This gives that $|\mathfrak{m}^\perp| = \sqrt{|R|}$, and since the ideals are linearly ordered we have that $\mathfrak{m} = \mathfrak{m}^\perp$.

Lemma 4.2. *Let R be a chain ring with maximal ideal $\mathfrak{m} = R\gamma$ with odd nilpotency index e. If $R/\mathfrak{m}$ is a field of characteristic $1 \pmod 4$ or even, then there exists a self-dual code of length 2.*

Proof. Since $\mathfrak{m}$ is maximal then $R/\mathfrak{m}$ is a field. It is well known that there is a $\sqrt{-1}$ if and only if the characteristic is $1 \pmod 4$ or even. Let α be the element in $R/\mathfrak{m}$ with $\alpha^2 = -1$ then in R we have $\alpha^2 + 1$ is a multiple of γ. Consider the following generator matrix:

$$\begin{pmatrix} \gamma^{\frac{e-1}{2}} & \alpha\gamma^{\frac{e-1}{2}} \\ 0 & \gamma^{\frac{e-1}{2}+1} \end{pmatrix}. \tag{8}$$

The inner-product of the first row with itself is $(1+\alpha^2)\gamma^{e-1} = a\gamma^e = 0$ for some $a \in R$. It is easy to see that the inner-product of the first and the second and the second with itself is also 0. By Equation 5 we have that the code generated by it has order $|R/\mathfrak{m}|^e = |R|$. Hence this matrix generates a self-dual code. □

The above lemma can be stated over a finite commutative ring as follows.

Proposition 4.3. *Let R be a finite commutative ring and I an ideal of odd nilpotency index $e \geq 3$ satisfying $|I^{\frac{e-1}{2}}| \cdot |I^{\frac{e+1}{2}}| = |R|$. Let $\alpha \in R$ such that $\alpha^2 + 1 \in I$. Then*

$$\begin{pmatrix} I^{\frac{e-1}{2}} & \alpha I^{\frac{e-1}{2}} \\ 0 & I^{\frac{e+1}{2}} \end{pmatrix} \tag{9}$$

is a self-dual code of length 2 over R.

Lemma 4.4. *Let R be a chain ring with maximal ideal $\mathfrak{m} = R\gamma$ with e its odd nilpotency index. If $R/\mathfrak{m}$ is a field of characteristic $3 \pmod 4$, then there exists a self-dual code of length 4.*

Proof. We know that the field $R/\mathfrak{m}$ has α, β with $\alpha^2 + \beta^2 = -1$. Then in R we have that $\alpha^2 + \beta^2 + 1$ is a multiple of γ.

$$\begin{pmatrix} \gamma^{\frac{e-1}{2}} & 0 & \alpha\gamma^{\frac{e-1}{2}} & \beta\gamma^{\frac{e-1}{2}} \\ 0 & \gamma^{\frac{e-1}{2}} & \alpha\gamma^{\frac{e-1}{2}} & \beta\gamma^{\frac{e-1}{2}} \\ 0 & 0 & \gamma^{\frac{e-1}{2}+1} & 0 \\ 0 & 0 & 0 & \gamma^{\frac{e-1}{2}+1} \end{pmatrix} \tag{10}$$

Following the proof of the Lemma 4.2 we see that this matrix generates a self-dual code of length 4. □

This lemma can be stated over a finite commutative ring as in Proposition 4.3 if the ideal I of odd nilpotency index $e \geq 3$ satisfies $|I^{\frac{e-1}{2}}| \cdot |I^{\frac{e+1}{2}}| = |R|$ and $\alpha^2 + \beta^2 + 1 \in I$ (we replace γ in Equation (10) by I).

Theorem 4.5. *Let R be a chain ring with maximal ideal $\mathfrak{m} = R\gamma$ with its nilpotency index e. If e is even, then there exist self-dual codes of all lengths over R. If e is odd and $R/\mathfrak{m}$ has characteristic $3 \pmod 4$, then there exist self-dual codes of all lengths a multiple of 4. If e is odd and $R/\mathfrak{m}$ has characteristic $1 \pmod 4$ or even, then there exist self-dual codes of even lengths.*

Proof. The result follows from Lemma 4.1, Lemma 4.2, Lemma 4.4 and noting that if C and D are self-dual codes of length n and n' then $C \times D$ is a self-dual code of length nn'. □

In what follows, we construct MDS self-dual codes over Galois rings.

Reed-Solomon codes over Galois rings are MDS codes [16], [24]. We apply the ideas of [12] to RS codes over Galois rings to construct MDS self-dual codes over Galois rings with even size as follows. Note that the length n of the below code is largest known.

Theorem 4.6. *Let $R = GR(2^e, l)$, $n = 2^l - 1(> 2)$, and $e \geq 1$. Then there exists an MDS self-dual code over R with parameters $[2^l, 2^{l-1}, 2^{l-1} + 1]$, which is an extended RS code.*

Proof. Let $R = GR(2^e, l)$, $n = 2^l - 1$, and $\xi \in R$ a primitive nth root of unity such that $\bar{\xi}$ is a primitive nth root of unity in $K = GF(2^l)$. Then the Reed-Solomon code C_1 over R with distance $d = (n+1)/2$ is generated by $g_1(X) = (X - \xi)(X - \xi^2) \cdots (X - \xi^{d-1})$. This is a free MDS code over R with odd length n, dimension $(n + 1)/2$, and minimum distance $d = (n+1)/2$ [16]. Let $h(X) \in R[X]$ be the check polynomial of C_1, i.e., $X^n - 1 = g_1(X)h(X)$, hence $h(X) = (X - \xi^d)(X - \xi^{d+1}) \cdots (X - \xi^n)$ as $X^n - 1$ factors linearly in R. The reciprocal polynomial $h^*(X)$ is $h^*(X) = X^{\deg(h)}h(1/X) = (1 - \xi^d X)(1 - \xi^{d+1}X) \cdots (1 - \xi^n X)$.

The dual $C_2 := C_1^{\perp}$ is generated by $g_2(X) = \frac{1}{h(0)}h^*(X) = (X - 1)(X - \xi)(X - \xi^2) \cdots (X - \xi^{d-1})$, and is a free MDS code with dimension $(n - 1)/2$ and minimum distance $(n + 3)/2$ since C_1 is a free MDS code [16, Corollary 3.6, Corollary 5.5]. Since $g_1(X)$ divides $g_2(X)$, C_2 is self-orthogonal. Furthermore since the all-one vector $\mathbf{1}$ is not in C_2 but in C_1, we have $C_1 = C_2 + \mathbf{1}$. Now we extend C_1 by adding 1 at the end of $\mathbf{1}$, and zero 0 at the end of any codewords generating C_2 (and obviously by combining them). Then C_1 is also an MDS code [16]. By construction, C_1 is also self-dual. This completes the proof. □

Remark. Following the proof of the above theorem, one can see that the conclusion of the theorem will hold for any chain ring R if (i) R has the residue field $GF(2^l)$, (ii) $n = 2^l - 1(> 2)$, and (iii) R contains a primitive nth root of unity ξ such that $\bar{\xi}$ is a primitive nth root of unity in $K = GF(2^l)$.

As seen in [12], if the characteristic of the residue field K with $|K| = q$ is odd, then it is hard to construct MDS self-dual codes of length $q + 1$ over $GF(q^e, l)$ for general q, e, and l.

5 Torsion codes

In this section R is a chain ring with maximal ideal $\mathfrak{m} = R\gamma$ whose nilpotency index is e. The following definitions were originally given to study the structure of codes over $\mathbb{Z}_4$ [7] (see also [9] and [16]).

Let C be a linear code over R. Consider the codes $(C : \gamma^i) = \{\mathbf{v} \mid \gamma^i\mathbf{v} \in C\}$, $i = 0, 1, \ldots, e - 1$, over R. Let "$-$" denote the canonical map $R^n \to (R/\mathfrak{m})^n$, $(n \geq 1)$. The codes $Tor_i(C) = \overline{(C : \gamma^i)}$ over the field $R/\mathfrak{m}$ $(i = 1, 2, \ldots, e-1)$, are called the *torsion codes* associated to the code C. The code $Res(C) = Tor_0(C) = \overline{(C : \gamma^0)} = \overline{C}$ over $R/\mathfrak{m}$ is called the *residue code* associated to the code C.

Given the generator matrix from Equation (4) for the code C, the torsion code $Tor_i(C)$

has a generator matrix of the form:

$$\begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & \cdots & A_{0,e} \\ 0 & I_{k_1} & A_{1,2} & A_{1,3} & \cdots & \cdots & A_{1,e} \\ 0 & 0 & I_{k_2} & A_{2,3} & \cdots & \cdots & A_{2,e} \\ \vdots & \vdots & \vdots & \ddots & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & I_{k_i} & \cdots & A_{i,e} \end{pmatrix}. \tag{11}$$

Lemma 5.1. *If C is a code over R, then $min\{d_H(Tor_i(C))\} \geq d_H(C)$.*

Proof. Take a vector $\mathbf{v}$ in the code $Tor_i(C)$. Then $\gamma^i\mathbf{v} \in C$ and $d_H(\mathbf{v}) = d_H(\gamma^i\mathbf{v})$. Hence the minimum weight of C must be less than or equal to the minimum weight of any of the Torsion codes. □

Lemma 5.2. *If C is a code over R, then $|C| = \prod_{i=0}^{e-1} |Tor_i(C)|$.*

Proof. Let $q = |R/\mathfrak{m}|$. We have seen that

$$|C| = q^{\sum_{j=0}^{e-1}(e-j)k_j}.$$

It follows from the generator matrix that

$$|Tor_i(C)| = \prod_{j=0}^{i} q^{k_j}.$$

The result follows. □

Theorem 5.3. *Let R be a chain ring with maximal ideal $\mathfrak{m} = R\gamma$ with nilpotency index e. If there exists an MDS code of length n and rank k over R, then $Tor_i(C) = Tor_j(C)$ for all $0 \leq i, j \leq e-1$, and it is an MDS code of length n and dimension k over the field $R/\mathfrak{m}$.*

Proof. Let C be an MDS code of length n and rank k over R. The code satisfies the bound given in Equation (1) and Equation (2). This implies that the code must be a free code. We see then by examining the generator matrix of $Tor_i(C)$ that $Tor_i(C) = Tor_0(C)$ for all i, $1 \leq i \leq e-1$. The code $Tor_0(C)$ has dimension k by Lemma 5.2. By Lemma 5.1 and the bound given in Equation (1) we have that $d_H(Tor_0) = n-k+1$. Hence $Tor_i(C)$ is an MDS code of length n and dimension k. □

Theorem 5.4 ([16], Theorem 5.3)**.** *Let R be a chain ring with maximal ideal $\mathfrak{m} = R\gamma$ with nilpotency index e. If there exists an MDR code over R, then $Tor_{e-1}(C)$ is an MDS code over the field $R/\mathfrak{m}$.*

Proof. Let C be an MDR code over R of rank k with generator matrix given in Equation (4). Then $k = \sum_{i=0}^{e-1} k_i$. The code $Tor_{e-1}(C)$ has dimension k by examining its generator matrix in Equation (11). The code C has minimum weight $n-k+1$. By Lemma 5.1 the minimum weight of Tor_{e-1} is at least $n-k+1$ but by Equation (2) it cannot be higher. Hence the code is an MDS code. □

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.

Corollary 5.5. *Let R be a chain ring with maximal ideal $\mathfrak{m} = R\gamma$, with $R/\mathfrak{m}$ isomorphic to $\mathbb{F}_2$. Then there are no non-trivial MDS or MDR codes over R.*

Proof. If there were an MDR code with $k \neq 1, n$ nor $n-1$, then there would be a binary MDS code with that dimension which is well known not to exist. □

6 Codes over finite principal ideal rings

Let R be a finite ring and $(\mathfrak{a}_i)_{i=1}^n$ a direct decomposition of R . Denote $R_i = R/\mathfrak{a}_i$. Let $\Psi : R^n \to \prod_{i=1}^k R_i^n$ be the canonical R-module isomorphism.

For $i = 1, \ldots, k$ let C_i be a code over R_i of length n and let

$$C = CRT(C_1, C_2, \ldots, C_k) = \Psi^{-1}(C_1 \times \cdots \times C_k) = \{\Psi^{-1}(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k) \mid \mathbf{v}_i \in C_i\}.$$

We refer to C as the *Chinese product of codes* $C_1, C_2, \ldots, C_k$ (see [10]).

The next lemma follows from Corollary 2.5.

Lemma 6.1. *With the above notation, let $C_1, C_2, \cdots, C_k$ be codes of length n, with C_i a code over R_i and let $C = CRT(C_1, C_2, \ldots, C_k)$. Then:*

(i) $|C| = \prod_{i=1}^k |C_i|$;

(ii) $rank(C) = \max\{rank(C_i)) \mid 1 \leq i \leq k\}$;

(iii) C is a free code if and only if each C_i is a free code of the same rank.

Lemma 6.2. *With the above notation, let $C_1, C_2, \cdots, C_k$ be codes with C_i a code over R_i. Then*

$$d_H(CRT(C_1, C_2, \cdots, C_k)) = \min\{d(C_i))\}. \tag{12}$$

Proof. It follows immediately noticing that map CRT applied to a vector with the remaining vectors being all zero vectors gives a vector with the same minimum weight and the $CRT(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ projects of $\mathbf{v}_i$ over R_i so there cannot be a vector of smaller weight in $CRT(C_1, C_2, \cdots, C_k)$. □

Theorem 6.3. *With the above notation, let $C_1, C_2, \ldots, C_k$ be codes over R_i. If C_i is an MDR code for each i, then $C = CRT(C_1, C_2, \ldots, C_k)$ is an MDR code. If C_i is an MDS code of the same rank for each i, then $C = CRT(C_1, C_2, \ldots, C_k)$ is an MDS code.*

Proof. Let k_i be the rank of C_i. By Lemma 6.2 and Lemma 6.1 we have

$$\begin{aligned} d_H(CRT(C_1, C_2, \cdots, C_k)) &= \min\{d(C_i))\} = \min\{n - rank(C_i) + 1\} \\ &= n - \text{Max}\{rank(C_i)\} + 1 = n - rank(C) + 1. \end{aligned}$$

By Lemma 6.1 we have that if each is MDS, then each is free (and they have the same ranks), so $CRT(C_1, C_2, \cdots, C_k)$ is also free and hence MDS. □

Theorem 6.4. *With the above notation, let C_i be codes over R_i and $C = CRT(C_1, C_2, \ldots, C_k)$. Then $C_1, C_2, \ldots, C_k$ are self-dual codes if and only if C is a self-dual code.*

Proof. By Lemma 6.1 we have that $|C|^2 = |R|^n$ if $|C_i|^2 = |R_i|^n$. It is clear that C is self-orthogonal if and only if C_i is self-orthogonal for all i. □

Theorem 6.5. *Let R be a finite principal ideal ring all of whose residue fields satisfy $|R/\mathfrak{m}_i| > \binom{n-1}{n-k-1}$ for some integers n, k with $n - k - 1 > 0$. Then there exists an MDS $[n, k, n-k+1]$ code over R.*

Proof. Follows from Theorem 3.5 and Theorem 6.3. □

Theorem 6.6. *Let R be a principal ideal ring all of whose maximal ideals have their indices of stability equal to 1. Then any self-dual code C over R is free of rank r and length $2r$ for some r.*

Proof. Let C be a code over R of length n. Since the indices of stability of all maximal ideals $\mathfrak{m}_i$ $(1 \le i \le k)$ of R are equal to 1, then, by Lemma 2.3, C is isomorphic, as a module over R, to the product $\prod_{i=1}^k C/\mathfrak{m}_i C$. Each of $C/\mathfrak{m}_i C$ can be considered as a vector space over $\kappa_i = R/\mathfrak{m}_i$, i.e., each of the codes $C_i = C/\mathfrak{m}_i C$ over R can be considered as a code over the field κ_i. Hence each of the codes C_i is free. By Theorem 6.4, all codes C_i are self-dual. Since self-dual codes over fields have even length, n is even, say $n = 2r$.

For any $i = 1, \ldots, k$, consider the exact sequence of linear maps

$$0 \to C_i \xrightarrow{j} \kappa_i^n \xrightarrow{f} C_i \to 0,$$

where j is the canonical injection and f is defined by $f(\mathbf{v}) = \sum_{\mathbf{c} \in C} \mathbf{v} \cdot \mathbf{c}$ for $\mathbf{v} \in \kappa_i^{2r}$. This exact sequence splits, i.e., $\kappa_i^{2r} = M \oplus N$ for some $M \cong C_i$ and $N \cong C_i$. Hence $|C_i| = |\kappa|^r$ and so $\text{rank}(C_i) = r$. Since all codes C_i are free of the same rank r, C is free of rank r. □

The next example illustrates that the previous theorem is not true if R is not a principal ideal ring.

Example 2. Let $R = \mathbb{F}_2[X, Y]/(X^2, Y^3) = \mathbb{F}_2[x, y]$, where $x^2 = y^3 = 0$. This ring is a Frobenius ring which has 64 elements. The elements are of the form $a + bx + cy + dy^2 +$

$exy + fxy^2$, where $a, b, c, d, e, f \in \mathbb{F}_2$. The maximal ideal $\mathfrak{m} = (x, y)$ cannot be generated by one element and so R is not a principal ideal ring. Consider the code $C = R(x, 0) + R(0, x)$, generated by the elements $(x, 0)$ and $(0, x)$ of R^2. We have $C = \{0, x, xy, xy^2, x + xy, x + xy^2, xy + xy^2, x + xy + xy^2\} \times \{0, x, xy, xy^2, x + xy, x + xy^2, xy + xy^2, x + xy + xy^2\}$. The code $C^\perp$ consists of all $(f, g) \in R^2$ such that $(f, g)(x, 0) = 0$ and $(f, g)(0, x) = 0$. We have $C^\perp = C$, i.e., C is self-dual. But C is not free and the conclusion of the previous theorem does not hold.

Corollary 6.7 ([22], Theorem 6.4)**.** *Let m be an integer which is a product of distinct primes. Then any self-dual code C over $\mathbb{Z}_m$ is free of rank r and of length $2r$ for some r.*

Proof. If $m = p_1 p_2 \dots p_k$, where the p_i are distinct primes, then the ring $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ is a principal ideal ring whose maximal ideals $p_i\mathbb{Z}/m\mathbb{Z}$ have their indices of stability equal to 1. The statement now follows from the previous theorem. □

The next example illustrates that the previous corollary is not true if m is not a product of distinct primes.

Example 3. Let $R = \mathbb{Z}_4$ and $C = R(2, 0) + R(0, 2) = \{(0, 0), (2, 0), (0, 2), (2, 2)\} \subset \mathbb{Z}_4^2$. We have $C^\perp = C$, but C is not free and the conclusion of the previous corollary does not hold.

Theorem 6.8. *Let R be a principal ideal ring with maximal ideals $\mathfrak{m}_i$ whose indices of stability are e_i respectively $(1 \leq i \leq s)$. If e_i is even for all i then self-dual codes over R exist for all lengths. If some e_i is odd and for each i with e_i odd we have $|R/\mathfrak{m}_i| \equiv 1 \pmod 4$ then self-dual codes over R exist for all even lengths. If some e_i is odd and there is an i with $|R/\mathfrak{m}_i| \equiv 3 \pmod 4$ then self-dual codes over R exists for all lengths divisible by 4.*

Proof. The result follows from Theorem 6.4 and Theorem 4.5. □

ACKNOWLEDGMENT

The authors thank Professor Steven Seif for useful suggestions and discussions in our early work. J.-L. Kim was supported in part by a Project Completion Grant from the University of Louisville.

References

[1] Blake IF (1972) Codes over certain rings. Inform. Contr. 20:396–404.

[2] Blake IF (1975) Codes over integer residue rings. Inform. Contr. 29:295–300.

[3] Bourbaki N (1989) Algebra, Chapters 1-3, Springer-Verlag, New-York.

[4] Bourbaki N (2003) Algebra, Chapters 3-7, Springer-Verlag, New-York.

[5] Bourbaki N (1989) Commutative Algebra, Chapters 1-7, Springer-Verlag, New-York.

[6] Constantinescu I, Heise W, Honold T (1996) Monomial extensions of isometries between codes over $\mathbb{Z}_m$. in Proceedings of the 5th International Workshop on Algebraic and Combinatorial Coding Theory (ACCT '96), Unicorn Shumen:98–104.

[7] Conway JH, Sloane NJA (1993) Self-dual codes over the integers modulo 4, J. Combinat. Theory, Ser. A 62:30–45.

[8] Dougherty ST, Gulliver TA, Park YH, Wong JNC, Optimal linear codes over $\mathbb{Z}_m$, to appear in the Journal of the Korean Mathematical Society.

[9] Dougherty ST, Park YH, Kim SY (2005) Lifted codes and their weight enumerators. Discrete Math. 305:123–135.

[10] Dougherty ST and Shiromoto K (2000) MDR codes over Z_k. IEEE Trans. Inform Theory, 46:265–269.

[11] Greferath M, Schmidt SE (2000) Finite-ring combinatorics and MacWilliams' equivalence theorem. J. of Combin. Theory, Ser. A. 92:17–28.

[12] Gulliver TA, Kim J-L, Lee Y (2007) New MDS or near-MDS self-dual codes. preprint.

[13] Hammons Jr.AR, Kumar PV, Calderbank AR, Sloane NJA, Solé P (1994) The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes. IEEE Trans. Inform. Theory 40:301–319.

[14] Honold T, Landjev I (2000) Linear codes over finite chain rings. Electronic J. of Combinatorics. 7:#R11.

[15] Kunz E (1985) Introduction to Commutative Algebra and Algebraic Geometry, Birkahäuser, Boston.

[16] Norton GH, Sălăgean A (2000) On the Hamming distance of linear codes over a finite chain ring. IEEE Trans. Inform. Theory 46:1060–1067.

[17] MacWilliams FJ, Sloane NJA (1997) The Theory of Error-Correcting Codes, Amsterdam, The Netherlands: North-Holland.

[18] Matsumura H (1989) Commutative Ring Theory, Cambridge University Press, Cambridge, UK.

[19] McDonald BR (1974) Finite Rings with Identity. Marcel Dekker, Inc., New York.

[20] Nebe G, Rains EM, Sloane NJA (2006) Self-Dual Codes and Invariant Theory. Springer, Berlin, Feb.

[21] Nechaev AA (1989) The Kerdock code in a cyclic form. Diskret. Mat. 1:123–139. English translation in Discrete Math. Appl. (1991), 1:365–384.

[22] Park YH (2007) Modular Independence and generator matrices for codes over $\mathbb{Z}_m$, preprint.

[23] Pless VS, Huffman WC (1998) eds., Handbook of Coding Theory, Elsevier, Amsterdam.

[24] Shankar P (1979) On BCH codes over arbitrary integer rings. IEEE Trans. Inform. Theory 25:480–483.

[25] Spiegel E (1977) Codes over Z_m. Inform. Contr., 35:48–52.

[26] Spiegel E (1979) Codes over Z_m revisited. Inform. Contr., 37:100–104.

[27] Wan ZX (2003) Lectures on finite fields and Galois rings. World Scientific Publishing Co., Inc., River Edge, NJ.

[28] Wood J (1999) Duality for modules over finite rings and applications to coding theory. Amer. J. Math. 121:555–575.