Chapter 2
Ring Theory

In this chapter, we shall give the necessary definitions and foundational results from commutative ring theory for the study of codes over rings.

2.1 Finite Commutative Rings

Rings are one of the fundamental objects of abstract algebra. They have numerous applications in number theory, cryptography, and many other branches of mathematics. For a complete description of ring theory see [12, 14**?** , 15], and for a description of commutative algebra, see [1].

We shall assume throughout this text that a ring has a multiplicative identity and that the multiplication is commutative. We begin with some standard definitions.

Let R be a finite commutative ring. An ideal $\mathfrak{a}$ of R is an additive subgroup of R such that $r\mathfrak{a} \subseteq \mathfrak{a}$ for all $r \in R$. We note that, in terms of algebraic coding theory, an ideal of R is a code of length 1. An ideal $\mathfrak{m}$ is maximal if $\mathfrak{m}$ is not properly contained in any non-trivial ideal.

Let $\mathfrak{a}$ be an ideal of a finite commutative ring. The chain $\mathfrak{a} \supset \mathfrak{a}^2 \supset \mathfrak{a}^3 \supset \ldots$ necessarily stabilizes. We call the smallest $t \geq 1$ such that $\mathfrak{a}^t = \mathfrak{a}^{t+i}$ for $i \geq 0$ 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 $\mathfrak{a}$. In this case, it coincides with the index of stability of $\mathfrak{a}$.

Definition 2.1 A ring is a local ring if it has a unique maximal ideal.

Local rings play an important role in coding theory because we often describe rings as the product of local rings via the Chinese Remainder Theorem and reduce much of the theory of codes to the case where the ring is local.

S.T. Dougherty, *Algebraic Coding Theory Over Finite Commutative Rings*,
SpringerBriefs in Mathematics, DOI 10.1007/978-3-319-59806-2_2

Example 2.1 Let $R = \mathbb{F}_2[x, y]/\langle x^2, y^2, xy - yx\rangle$. The ring R is a local ring and has cardinality 16. The maximal ideal is $\langle x, y\rangle$. This ring has been widely studied in algebraic coding theory as the ring R_2, see [9].

Definition 2.2 A principal ideal ring is a ring in which each ideal is generated by a single element, that is every ideal $\mathfrak{a}$ can be written as $\mathfrak{a} = \langle a\rangle$ for some element a.

It is well known that $\mathbb{Z}_k$ is a principal ideal ring for all $k > 1$. This family of rings is one of the principal families of rings which are most studied in algebraic coding theory. In fact, they were the first rings which were not fields to be used as alphabets in coding theory, see [2, 3].

Definition 2.3 A chain ring is a principal ideal ring such that the ideals are linearly ordered by set theoretic containment.

It follows that if R is a finite chain ring then there is an element γ such that γ generates the unique maximal ideal and we have the following chain:

$$\{0\} \subseteq \langle \gamma^{e-1}\rangle \subseteq \langle \gamma^{e-2}\rangle \subseteq \cdots \subseteq \langle \gamma\rangle \subseteq R. \tag{2.1}$$

Example 2.2 The ring $\mathbb{Z}_{p^e}$ where p is a prime and $e > 0$ is a chain ring. Here the maximal ideal is $\langle p\rangle$. A Galois ring is a ring of the form $\mathbb{Z}_{p^e}[x]/\langle q(x)\rangle$ where $q(x)$ is irreducible over $\mathbb{Z}_{p^e}$. Galois rings are also chain rings and the maximal ideal is again $\langle p\rangle$.

Let e be the index of nilpotency of the maximal ideal $\langle \gamma\rangle$ of a finite commutative chain ring R. It is shown on page 340 of [15] that for every element a of a chain ring R, we have that there exists a unique integer i with $1 \leq i \leq e - 1$ such that $a = \mu\gamma^i$, with μ a unit.

It follows that a chain ring is necessarily a local ring, but a local ring need not be a chain ring, as in the following example.

Example 2.3 Let $R = \mathbb{Z}_4[x]/\langle x^2\rangle$. Then R is a ring of order 16 with maximal ideal $\langle 2, x\rangle = \{0, x, 2x, 3x, 2, 2 + x, 2 + 2x, 2 + 3x\}$. But the ideals $\langle 2\rangle = \{0, 2, 2x, 2 + 2x\}$ and $\langle x\rangle = \{0, x, 2x, 3x\}$ are not linearly ordered.

Let R be a commutative chain ring with maximal ideal $\langle \gamma\rangle$ with index of nilpotency e. We know that $R/\langle \gamma\rangle$ is isomorphic to a finite field $\mathbb{F}_{p^r}$. It is well known that $|\langle \gamma^j\rangle| = |\mathbb{F}_{p^r}|^{e-j}$ for $0 \leq j \leq e - 1$. It follows that

$$|R| = |\mathbb{F}_{p^r}||\langle \gamma\rangle| = |\mathbb{F}_{p^r}||\mathbb{F}_{p^r}|^{e-1} = p^{er}. \tag{2.2}$$

We give the next definition in terms of commutative rings. This definition would be slightly changed in the case of non-commutative rings. For a complete description of the Jacobson radical and socle in their general usage see [12**?**].

Definition 2.4 Let R be a commutative ring. Then the Jacobson radical $J(R)$ of a ring R can be characterized as the intersection of all maximal ideals.

In any ring, commutative or non-commutative, the Jacobson radical is a two sided ideal. In a local commutative ring, the Jacobson radical is necessarily the unique maximal ideal.

Definition 2.5 The nilradical of a commutative ring R consists of the nilpotent elements of the ring.

As we shall prove later, for finite commutative rings, the Jacobson radical and the nilpotent radical coincide. Like the definition of the Jacobson radical, the following definition of the socle of the ring would change slightly for rings in general.

Definition 2.6 Let R be a commutative ring. The socle of a ring R, $Soc(R)$, is defined as the sum of all the minimal ideals of the ring.

2.2 Frobenius Rings

For algebraic coding theory, the most important class of rings is the class of Frobenius rings. This is because both MacWilliams theorems apply for Frobenius rings, but, in general, they do not extend to larger families of rings, see Theorems 2.5 and 3.2. In essence what this means is that for codes over this class of rings we have many of the techniques and ideas that fuel classical coding theory over fields. In spaces where these two theorems do not hold, things act in a very different way than classical coding theory and we lose much of the power of the theory. Perhaps one of the most significant implications of this is that for a code C over a Frobenius ring R of length n, we have that $|C||C^{\perp}| = |R^n|$. This is not necessarily true when the ring is not Frobenius. These results were first introduced in [17, 18].

In this section, we shall give a very brief explanation of Frobenius rings. Our explanation is based on Nakayama's definition. However, we shall not discuss Frobenius rings in their broadest generality, but rather reduce definitions to their finite commutative case. For example, one would generally begin the discussion with left (right) Artinian rings, namely those that do not contain an infinite descending chain of left (right) ideals. Since we only consider finite rings, all of these rings are Artinian and we need not consider ideals as being left or right, since all ideals are two sided ideals in a commutative ring. When we want to stress that something is a module or an ideal in a ring, we shall use the notation as a left module or ideal. For a more general description of Frobenius rings as applied to coding theory, including the non-commutative case, see [5].

Recall that a module M is irreducible if it contains no non-trivial submodule and a module M is indecomposable if it has no non-trivial direct summands. We note that every irreducible module is indecomposable, but not the converse.

Any Artinian ring, as a module over itself, admits a finite direct sum decomposition, namely:

$$ {}_RR = Re_{1,1} \oplus \ldots Re_{1,\mu_1} \oplus \cdots \oplus Re_{n,1} \oplus \cdots \oplus Re_{n,\mu_n}, \tag{2.3} $$

where the $e_{i,j}$ are primitive orthogonal idempotents with $1 = \sum e_{i,j}$. This decomposition is known as the principal decomposition of the module of R over itself.

We index the $Re_{i,j}$ so that $Re_{i,j}$ is isomorphic to $Re_{k,l}$ if and only if $i = k$. Then we set $e_i = e_{i,1}$ and we write ${}_R R \cong \oplus \mu_i Re_i$.

We can extend the definition of socle and radical of a ring to a module in a natural way. That is, the socle of a module M is the sum of the simple (i.e. contains no non-zero submodules) submodules of M and the radical of a module M is the intersection of all maximal submodules of M. Then the module $Re_{i,j}$ has a unique maximal submodule $Rad(R)e_{i,j} = Re_{i,j} \cap Rad(R)$ and a unique irreducible top quotient $T(Re_{i,j}) = Re_{i,j}/Rad(R)e_{i,j}$. The socle $S(R_{e,j})$ is the submodule generated by the irreducible submodules of $Re_{i,j}$.

We can now proceed to the standard definition. Let the module of R over itself be decomposed as follows: ${}_R R = \oplus \mu_i Re_i$. Then, an Artinian ring R is quasi-Frobenius if there exists a permutation σ of $\{1, 2, \ldots, n\}$, such that

$$T(Re_i) \cong S(Re_{\sigma(i)}) \tag{2.4}$$

and

$$S(Re_i) \cong T(Re_{\sigma(i)}). \tag{2.5}$$

Then the ring is Frobenius if $\mu_{\sigma(i)} = \mu_i$ as well.

A module M over a ring R is injective if, for every pair of R-modules $B_1 \subset B_2$ and every R-linear mapping $f : B_1 \to M$, the mapping f extends to an R-linear mapping $\overline{f} : B_2 \to M$.

The proof of the following can be found in Theorem 1.2 and Remark 1.3 of [17].

Theorem 2.1 *Let R be a finite commutative ring, then the following conditions are equivalent:*

- *The ring R is Frobenius;*
- *the R-module R is injective.*
- *If R is a finite local ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbf{k}$, these conditions are equivalent with $\dim_{\mathbf{k}} \mathrm{Ann}(\mathfrak{m}) = 1$.*

Example 2.4 Consider the ring $R = \mathbb{F}_2[x, y]/\langle x^2, y^2, xy\rangle$. We have that $|R| = 8$ and R has a maximal ideal $\mathfrak{m} = \{0, x, y, x + y\}$. Notice that $\mathfrak{m} = \mathfrak{m}^{\perp}$. Then $\dim_{\mathbf{k}} \mathrm{Ann}(\mathfrak{m}) = 2$ which violates the last condition in Theorem 2.1. Hence R is not Frobenius. In this case, we have that $|\mathfrak{m}||\mathfrak{m}^{\perp}| \neq |R|$. In a Frobenius ring this is not possible.

Throughout this text, we view characters as homomorphisms $\chi : M \to \mathbb{C}^*$ rather than maps into $\mathbb{Q}/\mathbb{Z}$. For a module M, let $\widehat{M}$ denote the character module of M. One of the most important aspects of Frobenius rings in terms of algebraic coding theory is the characterization of their character module. The following theorem can be found in [17]. It characterizes Frobenius rings in terms of the character module.

Theorem 2.2 *Suppose R is a finite ring. The following are equivalent:*

- *The ring R is Frobenius.*
- *As a left module, $\widehat{R} \cong {}_R R$.*
- *As a right module $\widehat{R} \cong R_R$.*

Note that the result is more complex in terms of non-commutative rings since we must be concerned with whether the module is a left or a right module.

Let R be a Frobenius ring. Let $\phi : R \to \widehat{R}$ be the module isomorphism. Then set $\chi = \phi(1)$ so that $\phi(r) = \chi^r$ for $r \in R$. We call this character χ a generating character for $\widehat{R}$.

The following is an immediate consequence.

Theorem 2.3 *The finite commutative ring R is Frobenius if and only if $\widehat{R}$ has a generating character.*

Example 2.5 Consider the finite field $\mathbb{F}_p$ where p is a prime. Let ξ be a complex primitive p-th root of unity. Then $\chi(a) = \xi^a$ is a generating character for $\widehat{\mathbb{F}_p}$.

The generating character for a Frobenius ring R is not necessarily unique. In fact, we have the following theorem, which is Lemma 4.1 in [17], where it is stated in broader generality for the non-commutative case as well.

Theorem 2.4 *Let χ be a character of a finite commutative ring R. Then χ is a generating character if and only if $ker(\chi)$ contains no nonzero ideals of R.*

Example 2.6 Consider the finite field $\mathbb{F}_4$ where the elements are written as $a + b\omega$ for $a, b \in \mathbb{F}_2$. Then the character $\chi_1 : \mathbb{F}_4 \to \mathbb{C}$ defined by $\chi_1(a + b\omega) = (-1)^{a+b}$ is a generating character for $\widehat{\mathbb{F}_4}$. Additionally, the character $\chi_2 : \mathbb{F}_4 \to \mathbb{C}$ defined by $\chi_2(a + b\omega) = (-1)^b$ is a generating character for $\widehat{\mathbb{F}_4}$. Their respective character tables are given by the following, where the value for row α and column β is $\chi_i(\alpha\beta)$.

χ_1	0	1	ω	$1+\omega$
0	1	1	1	1
1	1	-1	-1	1
ω	1	-1	1	-1
$1+\omega$	1	1	-1	-1

χ_2	0	1	ω	$1+\omega$
0	1	1	1	1
1	1	1	-1	-1
ω	1	-1	-1	1
$1+\omega$	1	-1	1	-1

The tables described in the previous example are very important in terms of coding theory since they will be used to produce MacWilliams relations for codes over rings. See Chap. 3 for a full description.

The final characterization of Frobenius rings that we shall give is the following extension of MacWilliams' first theorem, which she had proven for finite fields. It was extended in [17] to the following theorem. In [**?**], it was shown that this theorem does not extend to quasi-Frobenius rings. We state the theorem here without proof. A detailed proof can be found in [17].

Theorem 2.5 (MacWilliams Theorem) *(A) If R is a finite Frobenius ring and C is a linear code over R, then every Hamming isometry $C \to R^n$ can be extended to a monomial transformation.*

(B) If a finite commutative ring R satisfies that all of its Hamming isometries between linear codes allow for monomial extensions, then R is a Frobenius ring.

This theorem, along with the MacWilliams relations in Chap. 3, explain why we use Frobenius rings as the alphabets for codes. Specifically, we want both of these theorems to be true in order to apply the most powerful results of algebraic coding theory to codes over rings.

2.3 Chinese Remainder Theorem

The most powerful tool for codes over commutative rings is the classical Chinese Remainder Theorem, which we now describe. For a full description of the approach to the Chinese Remainder Theorem see [14].

Definition 2.7 Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of a ring R are said to be relatively prime if $\mathfrak{a} + \mathfrak{b} = R$.

Occasionally, the term coprime is used instead of relatively prime for ideals satisfying this definition.

Lemma 2.1 *If $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime ideals of a commutative ring R, then $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.*

Proof It is immediate that $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$. If $\mathfrak{a} + \mathfrak{b} = R$, then $\mathfrak{a} \cap \mathfrak{b} = (\mathfrak{a} \cap \mathfrak{b})R = (\mathfrak{a} \cap \mathfrak{b})(\mathfrak{a} + \mathfrak{b}) \subseteq \mathfrak{ab}$. Therefore $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$. □

Lemma 2.2 *Let $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ be ideals of a commutative ring R that are relatively prime in pairs. Then $\mathfrak{a}$ is relatively prime to $\mathfrak{bc}$.*

Proof We have that $R = (\mathfrak{a} + \mathfrak{b})(\mathfrak{a} + \mathfrak{c}) \subseteq \mathfrak{a} + \mathfrak{bc}$. Therefore $\mathfrak{a} + \mathfrak{bc} = R$ and $\mathfrak{a}$ and $\mathfrak{bc}$ are relatively prime. □

Apply Lemmas 2.1 and 2.2 inductively and we have the following.

Lemma 2.3 *Let $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_s$ be ideals of a commutative ring R that are relatively prime in pairs. Then $\mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_s = \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_s$.*

Next we can use this to produce an isomorphism lemma.

Lemma 2.4 *Let $\mathfrak{a}$ and $\mathfrak{b}$ be relatively prime ideals of a commutative ring R. Then $R/\mathfrak{ab} \cong R/\mathfrak{a} \times R/\mathfrak{b}$.*

Proof Define the map $\Psi : R \to (R/\mathfrak{a} \times R/\mathfrak{b})$ by $\Psi(x) = (x \pmod{\mathfrak{a}}, x \pmod{\mathfrak{b}})$. We have $ker(\Psi) = \mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$, which gives that $R/\mathfrak{ab} \cong R/\mathfrak{a} \times R/\mathfrak{b}$. □

Computationally we have the following. Since $\mathfrak{a} + \mathfrak{b} = R$, there exists an $\alpha \in \mathfrak{a}$ and a $\beta \in \mathfrak{b}$ with $\alpha + \beta = 1$. Then $\Psi(c\alpha + d\beta) = (d, c)$. Specifically, Ψ is surjective and we can compute the preimage in a straightforward computation. Applying induction to Lemma 2.4 we have the following.

Lemma 2.5 *Let $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_s$ be ideals of a commutative ring R which are relatively prime in pairs. Then*

$$R/\mathfrak{a}_1\mathfrak{a}_2 \ldots \mathfrak{a}_s \cong R/\mathfrak{a}_1 \times R/\mathfrak{a}_2 \times \cdots \times R/\mathfrak{a}_s. \tag{2.6}$$

Let R be a finite commutative ring, with $\mathfrak{a}$ an ideal of R. Let $\Psi_\mathfrak{a}$ be the canonical homomorphism $\Psi_\mathfrak{a} : R \to R/\mathfrak{a}$, given by $\Psi_\mathfrak{a}(x) = x + \mathfrak{a}$.

Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ be the maximal ideals of a finite commutative ring R and let $e_1, \ldots, e_s$ be their respective indices of stability. The ideals $\mathfrak{m}_1^{e_1}, \ldots, \mathfrak{m}_s^{e_s}$ are relatively prime in pairs and $\prod_{i=1}^{s} \mathfrak{m}_i^{e_i} = \cap_{i=1}^{k} \mathfrak{m}_i^{e_i} = \{0\}$.

This leads us to the following well known theorem.

Theorem 2.6 (Chinese Remainder Theorem) *Let R be a finite commutative ring, with maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ where the index of stability of $\mathfrak{m}_i$ is e_i. Then the map $\Psi : R \to \prod_{i=1}^{s} R/\mathfrak{m}_i^{e_i}$, defined by $\Psi(x) = (x + \mathfrak{m}_1^{e_1}, \ldots, x + \mathfrak{m}_k^{e_k})$, is a ring isomorphism.*

Proof We have that the $\mathfrak{m}^{e_i}$ are relatively prime in pairs and $\cap_{i=1}^{s} m_i^{e_i} = \{0\}$. Then by Lemma 2.5 we have that $R \cong R/0 \cong R/\mathfrak{m}_1^{e_1} \times R/\mathfrak{m}_2^{e_2} \times \cdots \times R/\mathfrak{m}_k^{e_k}$. This gives the result. □

Let R_i denote the local ring $R/\mathfrak{m}_i^{e_i}$. The previous theorem gives that

$$R \cong R_1 \times R_2 \times \cdots \times R_s. \tag{2.7}$$

We note that R is Frobenius if and only if each R_i is Frobenius. See Remark 1.3 in [17] for an explanation.

We denote the inverse isomorphism of Ψ by CRT, so that $CRT : R_1 \times R_2 \times \cdots \times R_s \to R$.

Example 2.7 Let $\prod_{i=1}^{s} p_i^{e_i}$ be the prime factorization of a positive natural number n. Then by Theorem 2.6 we have that $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_s^{e_s}}$. This is the classical application of the Chinese Remainder Theorem and is where the name originates. Namely, it allows for the unique solution modulo $\prod n_i$ of the system of equations $x \equiv a_i \pmod{n_i}$ when the n_i are relatively prime in pairs.

By an abuse of notation, we extend both Ψ and CRT to the n fold product of their domains.

If C_i is a code over R_i, we let $C = CRT(C_1, C_2, \ldots, C_s)$ be the code over R formed by this extended isomorphism. It is immediate that any code C over R is the image of a some collection of codes $C_1, C_2, \ldots, C_s$ where C_i is a code over R_i.

The rank of a code, $rank(C)$, is the minimum number of generators of C. A code is said to be free if it is a free submodule over R. The following appears in [7].

Corollary 2.1 *Let R_i be finite commutative rings and let*

$$R = CRT(R_1, R_2, \ldots, R_s).$$

Let C_i be a code over R_i with $C = CRT(C_1, C_2, \ldots, C_s)$. Then

- $|C| = \prod_{i=1}^{s} |C_i|$;
- $rank(C) = max\{rank(C_i), i = 1, \ldots, s\}$;
- *C is free if and only if C_i is free for all i each of the same rank.*

Proof The first statement follows immediately from the fact that CRT is a bijection. To prove the second, let r_i be the rank of C_i and $\mathbf{v}_1^i, \mathbf{v}_2^i, \ldots, \mathbf{v}_{r_i}^i$ be a set of generators for C_i. Let r be the maximum value for r_i. Pad this set with zero vectors so that each generator set has r elements. Then

$$\{CRT(\mathbf{v}_1^1, \mathbf{v}_1^2, \ldots, \mathbf{v}_1^s), CRT(\mathbf{v}_2^1, \mathbf{v}_2^2, \ldots, \mathbf{v}_2^s), \ldots, CRT(\mathbf{v}_r^1, \mathbf{v}_r^2, \ldots, \mathbf{v}_r^s)\}$$

generates the code C. We need r vectors since there exists an i where $r_i = r$. It follows from this construction that the code C is free if and only if $r_i = r$ for each i and each code C_i is free. □

The following is a well known application of the Chinese Remainder Theorem.

Theorem 2.7 *Let $R = CRT(R_1, R_2, \ldots, R_s)$ be a finite commutative ring. Let $C = CRT(C_1, C_2, \ldots, C_s)$ be a code over R. Then*

$$C^{\perp} = CRT(C_1^{\perp}, C_2^{\perp}, \ldots, C_s^{\perp}). \tag{2.8}$$

Proof Consider vectors $\mathbf{v}, \mathbf{w} \in R^n$. Then $\Psi_{\mathfrak{a}}(\sum v_i w_i) = \sum \Psi_{\mathfrak{a}}(v_i) \sum \Psi_{\mathfrak{a}}(w_i)$. Hence, when $[\mathbf{v}, \mathbf{w}] = 0$, we have that $[\Psi_{\mathfrak{a}}(\mathbf{v}), \Psi_{\mathfrak{a}}(\mathbf{w})] = 0$. Then the standard cardinality argument gives equality. □

A similar proof gives the following theorem.

Theorem 2.8 *Let $R = CRT(R_1, R_2, \ldots, R_s)$ be a finite commutative ring. Let $C = CRT(C_1, C_2, \ldots, C_s)$ be a code over R. If $\overline{\mathfrak{a}} = \mathfrak{a}$ and $\Psi_{\mathfrak{a}}(\overline{\mathbf{v}}) = \overline{\Psi_{\mathfrak{a}}(\mathbf{v})}$, where the involution applies first in the ring R and then in the ring $R/\mathfrak{a}$, then $C^H = CRT(C_1^H, C_2^H, \ldots, C_s^H)$.*

We can also find the minimum weight of a code in terms of its components via the Chinese Remainder Theorem as in the following theorem.

Theorem 2.9 *Let $R = CRT(R_1, R_2, \ldots, R_s)$ be a finite commutative ring. Let $C = CRT(C_1, C_2, \ldots, C_s)$ be a code over R. Then $d(C) = min\{d(C_i)\}$.*

Proof Let d_1 be the minimum of $\{d(C_i)\}$. Then, there exists j with $d(C_j) = d_1$. Let $\mathbf{v}_j$ be a minimum weight vector in C_j, then

$$CRT(\mathbf{0}, \mathbf{0}, \ldots, \mathbf{0}, \mathbf{v}_j, \mathbf{0}, \ldots, \mathbf{0})$$

has Hamming weight d_1 which gives $d(C) \leq d_1$. Then let $\mathbf{v}$ be a minimum weight vector in C. Its projection $\Psi_{\mathfrak{a}}(\mathbf{v})$ has weight less than or equal to $d(C)$ which gives $d(C) \geq d_1$. Therefore, $d_1 = d(C)$, and we have the result. □

Recall that an ideal $\mathfrak{a}$ is prime if $ab \in \mathfrak{a}$ implies either $a \in \mathfrak{a}$ of $b \in \mathfrak{a}$. In a finite ring, prime ideals and maximal ideals coincide since finite division rings are fields. Therefore the nilradical and the Jacobson radical coincide. Moreover, since the ring is finite, the nilradical is nilpotent. This is because you can simply take the maximum nilpotency exponent of all nilpotent elements and apply this to the ideal.

Theorem 2.10 *Let R be a finite commutative ring. Then R is isomorphic, via the Chinese Remainder Theorem, to a direct product of local rings.*

Proof Let $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_s$ be the maximal ideals of R. Then the Jacobson radical $J(R) = \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_s = \mathfrak{m}_1\mathfrak{m}_2 \ldots \mathfrak{m}_s$ by Lemma 2.3. Since $J(R)$ is nilpotent we have that there exists k with $(J(R)^k) = \{0\}$. This gives that $(\mathfrak{m}_1\mathfrak{m}_2 \ldots \mathfrak{m}_s)^k = \mathfrak{m}_1^k\mathfrak{m}_2^k \ldots \mathfrak{m}_s^k = \{0\}$. We know that $\mathfrak{m}_i$ and $\mathfrak{m}_j$ are relatively prime for $i \neq j$. Then their powers are also relatively prime by Lemma 2.2. This allows us to invoke the Chinese Remainder Theorem, which gives us that R is isomorphic to $R/\mathfrak{m}_1^k \times R/\mathfrak{m}_2^k \times \cdots \times R/\mathfrak{m}_s^k$. (Notice that k is greater than or equal to the individual index of stabilities of the maximal ideals so that $\mathfrak{m}_i^k = \mathfrak{m}_i^{e_i}$.) It only remains to show that $R/\mathfrak{m}_i^k$ is local. A maximal ideal in $R/\mathfrak{m}_i^k$ corresponds to a maximal ideal $\mathfrak{a}$ of R with $\mathfrak{m}_i \subseteq \mathfrak{a}$ since $\mathfrak{a}$ is necessarily a prime ideal. Then since $\mathfrak{m}_i$ is maximal, we have that $\mathfrak{a} = \mathfrak{m}_i$. Therefore, the unique maximal ideal of $R/\mathfrak{m}_i$ is $\mathfrak{m}_i/\mathfrak{m}_i^k$. □

Theorem 2.11 *A finite commutative ring R is a principal ideal ring if and only if $R = CRT(R_1, R_2, \ldots, R_s)$ where R_i is a chain ring for all i.*

Proof Assume $R = R_1 \times R_2 \times \cdots \times R_s$ and each R_i is a chain ring. Chain rings are necessarily principal ideal rings. If $\mathfrak{a}_i$ is an ideal of R_i with $\mathfrak{a}_i = \langle a_i \rangle$ then the ideal $\mathfrak{a}_1 \times \mathfrak{a}_2 \times \cdots \times \mathfrak{a}_s$ in $R_1 \times R_2 \times \cdots \times R_s$ is principal and generated by $(a_1, a_2, \ldots, a_s)$. Hence R is principal.

Assume R is principal. Then any ideal in $R_1 \times R_2 \times \cdots \times R_s$ is principal and hence each R_i is principal. By Theorem 2.10 we have that each R_i is local. Therefore R_i is a principal ideal ring which is local and hence a chain ring. □

The standard example of this theorem is the example given in Example 2.7. Namely, $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_s^{e_s}}$. Here $\mathbb{Z}_n$ is a principal ideal ring and each $\mathbb{Z}_{p_i^{e_i}}$ is a chain ring.

Example 2.8 For integers $k \geq 1$, define the family of rings A_k to be $A_k = \mathbb{F}_2[v_1, v_2, \ldots, v_k]/\langle v_i^2 - v_i, v_i v_j - v_j v_i \rangle$. The ideal $\langle w_1, w_2, \ldots, w_k \rangle$, where $w_i \in \{v_i, 1 + v_i\}$, is a maximal ideal of cardinality 2^{2^k-1}. We denote these maximal ideals by $\mathfrak{m}_i$. We note that here are 2^k such ideals and that $\mathfrak{m}_i^e = \mathfrak{m}_i$ for all i and $e \geq 1$. It is elementary to see that the direct sum of any two of these ideals is A_k. Then, using the Chinese Remainder Theorem, we have that the ring A_k is isomorphic to $\mathbb{F}_2^{2^k}$. As such, the ring A_k is a principal ideal ring and is isomorphic to the direct product of chain rings. Codes over these rings were studied in [4].

2.4 Generators

One of the most important tools in coding theory is finding a generator matrix for a code. In general, we do not only want a matrix whose rows generate the code, but we want a matrix that generates the code with the minimum number of rows. For codes over fields, we have a simple determination of a minimal generating set. Namely, a set of vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ is linearly independent if $\sum \alpha_i \mathbf{v}_i = \mathbf{0}$ implies $\alpha_i = 0$ for all i. This standard definition and its implications from linear algebra gives that any code over a finite field is equivalent to a code that has a minimal generating matrix of the form $(I_k \mid A)$ where I_k is the k by k identity matrix. For codes over rings this is not always possible. For example, the code of length 1 over $\mathbb{Z}_4$ generated by 2 is the code $\{0, 2\}$. This code has no such matrix. Moreover, the minimality of a set of generators can also be quite different. For example, consider the code C over $\mathbb{Z}_6$ of length 2 generated by the following matrix:

$$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}.$$

Here we have that $|C| = 6$ and it may appear that this generating set is minimal, however, the vector $(2, 3)$ also generates the code which shows that the original set of generators was not minimal. In this section, we shall describe the theory for minimal generating sets for codes over rings. Much of this material was first presented in [8, 16].

Definition 2.8 Let R be a finite local commutative Frobenius ring with unique maximal ideal $\mathfrak{m}$, and let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s$ be vectors in R^n. Then $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s$ are modular independent if and only if $\sum \alpha_j \mathbf{v}_j = \mathbf{0}$ implies that $\alpha_j \in \mathfrak{m}$ for all j.

A finite field is a local ring with maximal ideal $\{0\}$, so this definition is a natural generalization of linear independence. As an example for a code over a ring, consider the generators $(2, 0)$, $(0, 4)$ over the local ring $\mathbb{Z}_8$. These vectors are modular independent since any linear combination summing to the zero vector implies that the coefficients are in the maximal ideal $\langle 2 \rangle$. The following lemma is a natural generalization for one of the primary implications of linear independence.

Lemma 2.6 *Let R be a finite local commutative Frobenius ring and let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s \in R^n$. Then $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s$ are modular dependent if and only if some $\mathbf{v}_j$ can be written as a linear combination of the other vectors.*

Proof Assume that the vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s$ are modular dependent. This implies that there exists α_i with $\sum \alpha_i \mathbf{v}_i = \mathbf{0}$ and there exists α_j such that $\alpha_j \notin \mathfrak{m}$. We have that $\mathfrak{m}$ must contain all non-units giving that α_j is a unit. Then we have that

$$\mathbf{v}_j = (-\alpha_j^{-1}\alpha_1)\mathbf{v}_1 + \cdots + (-\alpha_j^{-1}\alpha_{j-1})\mathbf{v}_{j-1} + (-\alpha_j^{-1}\alpha_{j+1})\mathbf{v}_{j+1} + \cdots + (-\alpha_j^{-1}\alpha_s)\mathbf{v}_s.$$

To prove the other direction, assume that $\mathbf{v}_j$ can be written as a linear combination of the other vectors. Then $\mathbf{v}_j = \sum_{i \neq j}^{s} \alpha_i \mathbf{v}_i$. Then we have that $\sum_{i \neq j}^{s} \alpha_i \mathbf{v}_i - \mathbf{v}_j = \mathbf{0}$. The coefficient -1 is a unit in R and this implies that $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s$ are modular dependent. □

In terms of finite local commutative Frobenius rings, this result is enough to determine minimal generating sets. Namely, we need a set of modular independent vectors. For chain rings, we can say more. Since the ideals are in a chain we can apply the previous lemma and the standard techniques of linear algebra (that is row reduction done over a chain ring) to obtain the following result.

Theorem 2.12 *Let R be a finite chain ring with maximal ideal $\langle\gamma\rangle$ and let C be a code over R. Then there exists a generator matrix for a code C over R that is permutation equivalent to the following:*

$$\begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & \cdots & A_{0,e} \\ 0 & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & \cdots & \cdots & \gamma A_{1,e} \\ 0 & 0 & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & \cdots & \cdots & \gamma^2 A_{2,e} \\ \vdots & \vdots & 0 & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \gamma^{e-1} I_{k_{e-1}} & \gamma^{e-1} A_{e-1,e} \end{pmatrix}, \tag{2.9}$$

where the $A_{i,j}$ are arbitrary matrices with elements from the ring R and I_{k_j} is the k_j by k_j identity matrix.

A code with generator matrix of this form is said to have type $\{k_0, k_1, \ldots, k_{e-1}\}$. The following is an immediate consequence of Theorem 2.12.

Corollary 2.2 *Let R be a finite chain ring with maximal ideal $\langle\gamma\rangle$. Let C be a code over R of type $\{k_0, k_1, \ldots, k_{e-1}\}$. Then,*

$$|C| = |R/\langle\gamma\rangle|^{\sum_{i=0}^{e-1}(e-i)k_i}. \tag{2.10}$$

For a code over a finite chain ring the type plays the role that the dimension plays for codes over a field. This is because two codes with the same type will have the same cardinality. This is not true for two codes with the same rank as a module over the ring.

We now expand this theory to cover any finite commutative Frobenius ring.

Definition 2.9 Let R be a finite commutative Frobenius ring with

$$R = CRT(\Psi_1(R), \Psi_2(R), \ldots, \Psi_s(R)) = (R_1, R_2, \ldots, R_s).$$

The vectors $\mathbf{v}_1, \cdots, \mathbf{v}_k$ in R^n are modular independent if $\Psi_i(\mathbf{v}_1), \cdots, \Psi_i(\mathbf{v}_k)$ are modular independent for some i, with $1 \leq i \leq s$.

Note that we are only requiring that their image under Ψ_i be modular independent over one local ring. They need not be modular independent for all i.

Theorem 2.13 *Let R be a finite commutative Frobenius ring and let $\mathbf{v}_1, \cdots, \mathbf{v}_k$ be vectors that are modular independent over R. If $\sum \alpha_j \mathbf{v}_j = \mathbf{0}$, then α_j is not a unit for all j.*

Proof Let $R = CRT(\Psi_1(R), \Psi_2(R), \ldots, \Psi_s(R))$ and let i be the index such that $\Psi_i(\mathbf{v}_1), \cdots, \Psi_i(\mathbf{v}_k)$ are modular independent over the local ring R_i. Then $\sum \alpha_j \mathbf{v}_j = \mathbf{0}$ implies that $\sum \Psi_i(\alpha_j)\Psi_i(\mathbf{v}_j) = \mathbf{0}$, and hence we have that $\Psi_i(\alpha_j) \in \mathfrak{m}_i$ where $\mathfrak{m}_i$ is the maximal ideal of R_i.

If α_j were a unit in R then there would exist a $\beta \in R$ with $\alpha_j \beta = 1$, which gives that $\Psi_i(\alpha_j)\Psi_i(\beta) = 1$. This would imply that $\Psi_i(\alpha_j)$ is a unit in R_i, which would be a contradiction. Therefore, we have that $\Psi_i(\alpha_j)$ is not a unit for all j. □

The converse of this theorem is not true. For example, consider the vectors $(5, 5)$ and $(7, 7)$ over $\mathbb{Z}_{35}$. If $\alpha_1(5, 5) + \alpha_2(7, 7) = (0, 0)$, then α_1 and α_2 must be non-units. However, these vectors are not modular independent over $\mathbb{Z}_{35}$, since their images under Ψ_1 and Ψ_2 are not modular independent over $\mathbb{Z}_5$ or $\mathbb{Z}_7$.

Because we do not have the biconditional yet, we need something else in the case when the ring is not local.

Definition 2.10 Let R be a finite commutative Frobenius ring. Let $\mathbf{v}_1, \cdots, \mathbf{v}_k$ be non-zero vectors in R^n. Then $\mathbf{v}_1, \cdots, \mathbf{v}_k$ are independent if $\sum \alpha_j \mathbf{v}_j = \mathbf{0}$ implies that $\alpha_j \mathbf{v}_j = \mathbf{0}$ for all j.

Note that we are saying something different than the coefficient is zero. We are saying that the vector $\alpha_j \mathbf{v}_j = \mathbf{0}$. Again, for a code over a field, this would imply that the coefficient is 0 since we have no zero divisors. This definition would then reduce to the standard definition for linear independence for vectors over a field.

Theorem 2.14 *Let R be a finite commutative Frobenius ring with $\mathbf{v}_1, \cdots, \mathbf{v}_k$ vectors over R. If $\mathbf{v}_1, \cdots, \mathbf{v}_k$ are independent and $\alpha \mathbf{w} \notin \langle \mathbf{v}_1, \cdots, \mathbf{v}_k \rangle$, for all $\alpha \neq 0$, then the vectors $\mathbf{v}_1, \cdots, \mathbf{v}_k, \mathbf{w}$ are independent.*

Proof If $\sum \alpha_j \mathbf{v}_j + \beta \mathbf{w} = \mathbf{0}$, then $\sum \alpha_j \mathbf{v}_j = -\beta \mathbf{w}$, which is a contradiction since then $-\beta \mathbf{w}$ would be in the span of the $\mathbf{v}_i$, unless $\beta = 0$. If $\beta = 0$ then $\sum \alpha_j \mathbf{v}_j = \mathbf{0}$, and then $\alpha_j \mathbf{v}_j = \mathbf{0}$ for all j since $\mathbf{v}_1, \cdots, \mathbf{v}_k$ are independent. Therefore, we have that the vectors $\mathbf{v}_1, \cdots, \mathbf{v}_k, \mathbf{w}$ are independent. □

Following Definition 2.10, we can easily get the following theorem.

Theorem 2.15 *Let R be a finite commutative Frobenius ring with*

$$R = CRT(\Psi_1(R), \Psi_2(R), \ldots, \Psi_s(R)) = (R_1, R_2, \ldots, R_s).$$

Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s$ be independent non-zero vectors in R^n. Then these vectors are modular independent.

Proof If $\sum \alpha_j \mathbf{v}_j = \mathbf{0}$, then $\alpha_j \mathbf{v}_j = \mathbf{0}$ for all j. Let $\mathfrak{m}$ be the maximal ideal of R. If $\alpha_j \notin \mathfrak{m}$ for some j, then α_j is a unit. This implies that $\mathbf{v}_j = \mathbf{0}$. □

We are now in a position to give the definition that we use to replace the notion of linear independence for codes over rings.

Definition 2.11 Let C be a code over a finite commutative Frobenius ring R. The codewords $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k$ are called a basis of C if they are independent, modular independent, and generate C.

We can show, by the example given in [8], that modular independence does not imply independence nor does independence imply modular independence. Let $(1, 7)$ and $(3, 9)$ be vectors over $\mathbb{Z}_{12}$. Then $(1, 7)$ and $(3, 9)$ map to $(3, 3)$ and $(3, 1)$ over $\mathbb{Z}_4$ which are modular independent. Hence the vectors $(1, 7)$ and $(3, 9)$ are modular independent. But $6(1, 7) + 2(3, 9) = (0, 0)$, and $6(1, 7) = (6, 6) = 2(3, 9) \neq (0, 0)$. Therefore they are not independent. It is easy to see that $(4, 0)$ and $(0, 3)$ are independent vectors over $\mathbb{Z}_{12}$. However, $(4, 0)$ and $(0, 3)$ map to $(0, 0)$ and $(0, 3)$ over $\mathbb{Z}_4$ and map to $(1, 0)$ and $(0, 0)$ over $\mathbb{Z}_3$. Therefore, they are not modular independent.

Returning to the example which began this section, we consider the vectors $(2, 0)$ and $(0, 3)$ over $\mathbb{Z}_6$. These vectors are independent, but they are not modular independent. Hence they do not form a basis. However, the vector $(2, 3)$ is both modular independent and independent over $\mathbb{Z}_6$. Hence this single vector is the basis for this code of length 2.

We shall now show a specific case for generating free Maximum Distance Separable codes over chain rings. These ideas can be found originally in [6] and then later in more generality in [7]. Let R be a finite chain ring with the maximal ideal $\mathfrak{m} = R\gamma$ whose nilpotency index is e. This gives that $|R/\mathfrak{m}| = q = p^s$, where p is a prime and s is a positive integer. Let $M = \{\mathbf{w} \in R^r \mid |\langle \mathbf{w} \rangle| < |R|\}$. That is, M consists of vectors in R^r that have no coordinate with a unit in it. Since we are in a chain ring, we have that each coordinate of $\mathbf{w} \in M$ is a multiple of γ. This gives that

$$M = R^r. \tag{2.11}$$

We take the standard definition of linear independence. Namely, the vectors $\mathbf{v}_1, \cdots, \mathbf{v}_n \in R^r$ are linearly independent if $\sum a_i \mathbf{v}_i = \mathbf{0}$ implies $a_i = 0$ for all i.

Lemma 2.7 *Suppose that $\mathbf{v}_1, \cdots, \mathbf{v}_{t-1} \in R^r$ are linearly independent. If $\mathbf{v}_t \notin \langle \mathbf{v}_1, \cdots, \mathbf{v}_{t-1}, M \rangle$, then $\mathbf{v}_1, \cdots, \mathbf{v}_{t-1}, \mathbf{v}_t$ are linearly independent.*

Proof Assume $\sum_{i=1}^{t} \alpha_i \mathbf{v}_i = \mathbf{0}$. If $\alpha_t = 0$, then since $\mathbf{v}_1, \cdots \mathbf{v}_{t-1} \in R^r$ are linearly independent, we have that $\alpha_i = 0$ for all i and we have the desired result.

Next assume that α_t is a unit. This gives that $\mathbf{v}_t \in \langle \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{t-1} \rangle$ which is a contradiction.

Finally, assume that $\alpha_t \neq 0$ and that α_t is not a unit. Then $\alpha_t = \beta \gamma^j$ for some unit β and positive integer j. Then we have $-\beta \gamma^j \mathbf{v}_t = \sum_{i=1}^{t-1} \alpha_i \mathbf{v}_i$. Multiply both sides by γ^{e-j}. Then we have $\mathbf{0} = \sum_{i=1}^{t-1} \gamma^{e-j} \alpha_i \mathbf{v}_i$. We know that $\mathbf{v}_1, \cdots, \mathbf{v}_{t-1}$ are linearly independent, which gives that $\gamma^{e-j} \alpha_i = 0$ for all i. This implies that $\alpha_i \in \langle \gamma^j \rangle$, which gives that $\sum_{i=1}^{t} \alpha_i \mathbf{v}_i \in M$. This contradicts the assumption. □

Lemma 2.8 *Let R be a finite commutative chain ring with $|R/\mathfrak{m}| = q = p^s$, where $\mathfrak{m} = \langle \gamma \rangle$ is the maximal ideal, p is a prime, and s is a positive integer. Let $M = \{\mathbf{w} \in R^r \mid |\langle \mathbf{w} \rangle| < |R|\}$. If $\mathbf{v}_1, \cdots, \mathbf{v}_t \in R^r$ are linearly independent, then $|\langle \mathbf{v}_1, \cdots, \mathbf{v}_t, M \rangle| = q^t (|R|/q)^r$.*

Proof We have that

$$\langle \mathbf{v}_1, \cdots, \mathbf{v}_t, M \rangle = \{\alpha_1 \mathbf{v}_1 + \cdots + \alpha_t \mathbf{v}_t + \gamma \mathbf{w} \mid \alpha_i \in R, \mathbf{w} \in R^r\}.$$

Assume

$$\alpha_1 \mathbf{v}_1 + \cdots + \alpha_t \mathbf{v}_t + \gamma \mathbf{w}_1 = \beta_1 \mathbf{v}_1 + \cdots + \beta_t \mathbf{v}_t + \gamma \mathbf{w}_2$$

for some $\mathbf{w}_1, \mathbf{w}_2 \in R^r$. Then

$$(\alpha_1 - \beta_1)\mathbf{v}_1 + \cdots + (\alpha_t - \beta_t)\mathbf{v}_t + \gamma(\mathbf{w}_1 - \mathbf{w}_2) = \mathbf{0}.$$

Multiplying both sides by γ^{e-1}, we have

$$\gamma^{e-1}(\alpha_1 - \beta_1)\mathbf{v}_1 + \cdots + \gamma^{e-1}(\alpha_t - \beta_t)\mathbf{v}_t = \mathbf{0}.$$

Since $\mathbf{v}_1, \cdots, \mathbf{v}_t$ are linearly independent, $\alpha_i - \beta_i \in \mathfrak{m}$, which gives that $\beta_i = \alpha_i + \gamma \delta_i$ for some $\delta_i \in R$ for $i = 1, \cdots, t$. Therefore, it suffices to choose representatives of $R/R\gamma$ as coefficients of the $\mathbf{v}_i$ which counts q^t elements. Then, since $|M| = |\gamma R^r| = |R\gamma|^r = (|R|/q)^r$, the lemma follows. □

We can now imitate the Gilbert-Varshamov construction found in [13, p. 33] to obtain the following theorem.

Theorem 2.16 *Let R be a finite commutative chain ring with $|R/\mathfrak{m}| = q = p^s$, where $\mathfrak{m} = \langle \gamma \rangle$ is the maximal ideal, p is a prime, and s is a positive integer. Suppose $\binom{n-1}{d-2} < \frac{q^{n-k}-1}{q^{d-2}-1}$. Then there exists a free code over R of length n and rank k with minimum distance d.*

Proof Let $M = \{\mathbf{w} \in R^r \mid |\langle \mathbf{w} \rangle| < |R|\}$. To prove the theorem, we construct an $(n - k)$ by n parity check matrix H with the property that no $d - 1$ columns are linearly dependent. Set $r = n - k$. The first column can be any $\mathbf{v}_1 \in R^r$, but not in M. 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 $\mathbf{v}_t \notin \bigcup \langle \mathbf{v}_{i_1}, \cdots, \mathbf{v}_{i_{d-2}}, M \rangle$, where the union is taken over all possible choices of $d - 2$ columns from the $t - 1$ columns. Then no $d - 1$ columns from the t columns $\mathbf{v}_1, \cdots, \mathbf{v}_t$ are linearly dependent. Such a vector would exist if $|\bigcup \langle \mathbf{v}_{i_1}, \cdots, \mathbf{v}_{i_{d-2}}, M \rangle| < |R|^r$. Then for all $t \leq n$, we have:

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

This gives the result. □

This leads to the following corollary.

Corollary 2.3 *Let R be a finite chain ring with the maximal ideal $\mathfrak{m} = R\gamma$. If $q = |R/\mathfrak{m}| > \binom{n-1}{n-k-1}$ with $n - k - 1 > 0$, then there exists a Maximum Distance Separable code over R of length n containing q^{n-k+1} elements with minimum distance $n - k + 1$.*

Proof If $d = n - k + 1$, then the inequality of Theorem 2.16 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 $n > k + 1$. This gives the desired result. □

References

1. Atiyah, M.F., Macdonald, I.G. Introduction to Commutative Algebra. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. (1969)
2. Blake, I.F.: Codes over certain rings. Inf. Control **20**, 396–404 (1972)
3. Blake, I.F.: Codes over integer residue rings. Inf. Control **29**(4), 295–300 (1975)
4. Cengellenmis, Y., Dertli, A., Dougherty, S.T.: Codes over an infinite family of rings with a Gray map. Des. Codes Cryptogr. **72**(3), 559–580 (2014)
5. Dougherty, S.T.: Foundations of algebraic coding theory. Contemp. Math. **634**, 101–136 (2015)
6. Dougherty, S.T., Gulliver, T.A., Park, Y.H., Wong, J.N.C.: Optimal linear codes over $\mathbb{Z}_m$. J. Korean Math. Soc. **44**(5), 1139–1162 (2007)
7. Dougherty, S.T., Kim, J.L., Kulosman, H.: MDS codes over finite principal ideal rings. Des. Codes Cryptogr. **50**(1), 77–92 (2009)

8. Dougherty, S.T., Liu, H.: Independence of vectors in codes over rings. Des. Codes Cryptogr. **51**(1), 55–68 (2009)
9. Dougherty, S.T., Yildiz, B., Karadeniz, S.: Codes over R_k, Gray maps and their binary images. Finite Fields Appl. **17**(3), 205–219 (2011)
10. Greferath, M., Schmidt, S.E.: Finite-ring combinatorics and MacWilliams' equivalence theorem. J. Combin. Theory Ser. A **92**(1), 17–28 (2000)
11. Lam, T.Y.: A First Course in Noncommutative Rings. Graduate Texts in Mathematics, vol. 131. Springer-Verlag, New York (1991)
12. Lam, T.Y.: Lectures on Modules and Rings. Graduate Texts in Mathematics, vol. 189. Springer-Verlag, New York (1999)
13. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. Amsterdam, North-Holland, The Netherlands (1977)
14. Matsumura, H.: Commutative Ring Theory, 2nd edn. Cambridge Studies in Advanced Mathematics, vol. 8. Cambridge University Press, Cambridge (1989). (Translated from the Japanese by M. Reid.)
15. McDonald, B.R.: Finite Rings with Identity. Marcel Dekker Inc, New York (1974)
16. Park, Y.H.: Modular independence and generator matrices for codes over $\mathbb{Z}_m$. Des. Codes Cryptogr. **50**(2), 147–162 (2009)
17. Wood, J.: Duality for modules over finite rings and applications to coding theory. Am. J. Math. **121**(3), 555–575 (1999)
18. Wood, J.: Foundations of linear codes defined over finite modules: the extension theorem and the MacWilliams identities. Lectures for the CIMPA-UNESCO-TUBITAK Summer school

http://www.springer.com/978-3-319-59805-5

Algebraic Coding Theory Over Finite Commutative Rings

Dougherty, S.T.

2017, X, 103 p., Softcover
ISBN: 978-3-319-59805-5