Chapter 2

Basics of Algebraic Coding Theory

2.1 Basics of Coding Theory

We will provide the required concepts and basic findings from commutative ring theory for the study of codes over rings in this chapter. One of the most fundamental concepts in abstract algebra is rings. They are useful in number theory, cryptography, and a variety of other fields of mathematics.

Definition 2.1.1. [12] Consider a code alphabet $W = \{w_0, w_1, ..., w_{k-1}\}$.

1. Elements of W are called code symbols.

2. A sequence $a = a_0a_1...a_{n-1}$ with each $a_i \in W$ for all i is called a word of length n over W.

3. Alternatively, a may be viewed as an n-tuple $(a_0, a_1, ..., a_{n-1})$.

ISBN: 978-81-989164-0-2
Thesis DOI: 10.21467/thesis.183

Series: AIJR Thesis

4. A nonempty set C of words having the same length n is called a code of length n over W.

5. A codeword c of the code C is an element of C.

6. The number of codewords in C is called the size of C and is denoted by $|C|$.

7. A code C of length n with a distance d can be denoted as an $[n, M, d]$-code, where M is the size of C.

The family of finite commutative rings has been widely used as alphabets to study a variety of algebraic codes. For a complete description of ring theory, readers can refer to [7, 8, 11], and also they can see [1, 13] for a description of commutative algebra.

2.1.1 Rings

Definition 2.1.2. [7, 8] Let G be a nonempty set. A **binary operation** on G is a function that assigns each ordered pair of elements of G to an element of G.

Definition 2.1.3. [8] Let G be a nonempty set together with a binary operation $\star$ that assigns to each ordered pair (x, y) of elements of G an element in G denoted by $x \star y$. We say G is a **group** under this operation if the following conditions are satisfied.

1. (Associativity) $x \star (y \star z) = (x \star y) \star z$ for all $x, y, z \in G$.

2. (Existence of Identity) There is an element $e \in G$ (called the identity) such that $x \star e = e \star x = x$ for all $x \in G$.

3. (Existence of Inverse) For each element $x \in G$, there is an element $x' \in G$ (called an inverse of x) such that $x \star x' = x' \star x = e$.

Definition 2.1.4. [7, 8] If a group G has the property that $x \star y = y \star x$ for every pair of elements (x, y), then the group is called an **abelian group**.

Definition 2.1.5. [8] If a subset H of a group G is itself a group under the operation of G, then H is called a subgroup of G.

Definition 2.1.6. [7, 8, 11] A **ring** is a non empty set $\mathcal{R}$ equipped with two binary operations, namely addition and multiplication, that satisfy the following conditions for all $x, y, z \in \mathcal{R}$:

1. $\mathcal{R}$ is an abelian group under addition i.e.,
   (a) $x + y \in \mathcal{R}$.
   (b) $(x + y) + z = x + (y + z)$.
   (c) There is an element $0 \in R$ with the property $0 + x = x + 0 = x$.
   (d) For each $x \in \mathcal{R}$, there is an element of $\mathcal{R}$, called $-x$, such that $x + (-x) = (-x) + x = 0$.
   (e) $x + y = y + x$
2. $xy \in \mathcal{R}$
3. $(xy)z = x(yz)$.
4. $(x + y)z = xz + yz$.
5. $x(y + z) = xy + xz$.

Definition 2.1.7. [7, 8] A **commutative ring** is a ring $\mathcal{R}$ such that

$$x \cdot y = y \cdot x, \text{ for all } x, y \in \mathcal{R}$$

Definition 2.1.8. [8] A unity (or identity) in a ring is a nonzero element that is an identity under multiplication. A **ring with unity** is a ring $\mathcal{R}$ that contains an element $1 \in \mathcal{R}$ such that

$$x \cdot 1 = 1 \cdot x = x, \text{ for all } x \in \mathcal{R}$$

Definition 2.1.9. [8] A ring $\mathcal{R}$ is said to be a **finite ring** if $\mathcal{R}$ has a finite number of elements.

Definition 2.1.10. [7] A subset S of a ring $\mathcal{R}$ is a **subring** of $\mathcal{R}$ if S is itself a ring with the operations of $\mathcal{R}$.

Definition 2.1.11. [8] A subring A of a ring $\mathcal{R}$ is called a (two-sided) **ideal** of $\mathcal{R}$ if for every $r \in \mathcal{R}$ and every $a \in A$ both ra and ar are in A.
An ideal A of $\mathcal{R}$ is called a proper ideal of $\mathcal{R}$ if A is a proper subset of $\mathcal{R}$.

Definition 2.1.12. [7] Let $\mathcal{R}$ be a commutative ring with unity and let $a \in \mathcal{R}$. The set $\langle a \rangle = \{ra | r \in \mathcal{R}\}$ is an ideal of $\mathcal{R}$ called the **principal ideal** generated by a.

Definition 2.1.13. [8] A **maximal ideal** A of a commutative ring $\mathcal{R}$ is a proper ideal of $\mathcal{R}$ such that, whenever B is an ideal of $\mathcal{R}$ and $A \subseteq B \subseteq \mathcal{R}$, then $B = A$ or $B = \mathcal{R}$.

Definition 2.1.14. [8] If all of the ideals of a commutative ring with unity form a chain under set theoretic inclusion, it is called a **chain ring**.

Definition 2.1.15. [7] Let $\mathcal{R}$ be a ring and let A be an ideal of $\mathcal{R}$. A **quotient or factor ring** is denoted by $\frac{\mathcal{R}}{A}$ and it is the set of additive cosets $\{r + A | r \in \mathcal{R}\}$, with addition and multiplication defined as $(r + A) + (s + A) = r + s + A$ and $(r + a)(s + A) = rs + A$.

Definition 2.1.16. [7, 8, 11] A nonzero element of a commutative ring with unity need not have a multiplicative inverse. When it exists, then it is a **unit** of the ring. Thus, x is a unit if x^{-1} exists.

Definition 2.1.17. [8] A **field** is a commutative ring with unity in which every nonzero element is a unit.

2.1.2 Vector Spaces

Definition 2.1.18. [8, 12] A nonempty set V, together with some (vector) addition denoted $+$ and scalar multiplication by elements of any finite field $\mathbb{F}_q$, is a **vector space** over $\mathbb{F}_q$ if it satisfies the following conditions. For all $x, y, z \in V$ and for all $a, b \in \mathbb{F}_q$, the following conditions hold:

1. $x + y \in V$.
2. $(x + y) + z = x + (y + z)$.
3. There is an element $0 \in V$ such that $0 + x = x + 0 = x$ for all $x \in V$.
4. For each $x \in V$, there is an element $-x$ of V such that $x+(-x) = (-x)+x = 0$.
5. $x + y = y + x$
6. $ax \in V$
7. $a(x + y) = ax + ay, (a + b)x = ax + bx$.

8. $(ab)x = a(bx)$.

9. If 1 is the multiplicative identity of $\mathbb{F}_q$, then $1x = x$.

Definition 2.1.19. [9, 12] If V is a vector space over a field $\mathbb{F}_q$ and U is a subset of V, then U is a **linear subspace** of V if U is a vector space over $\mathbb{F}_q$ under the operations of V.

Definition 2.1.20. [10, 11] Let $\mathcal{R}$ be a commutative ring with unity. An **$\mathcal{R}$-module** N is an abelian group $(N, +)$ together with a map $\cdot : R \times N \to N$ defined by $(r, m) \mapsto rm$ that satisfies the following conditions for all $r, s \in \mathcal{R}, m, n \in N$:

1. $r(m + n) = rm + rn$

2. $(r + s)m = rm + sm$

3. $(rs)m = r(sm)$

4. $1m = m$

Definition 2.1.21. [10, 11] Consider an $\mathcal{R}$-module N and a subgroup P of N. Then P is an **$\mathcal{R}$-submodule** of N if for any $n \in P$ and any $r \in \mathcal{R}$, the product $rn \in P$.

2.1.3 Linear Codes over Finite Rings

Now, from here we shall assume throughout this text that the ring $\mathcal{R}$ has a multiplicative identity and that the multiplication is commutative.

Definition 2.1.22. [6, 15, 16] Let $\mathcal{R}$ be a finite commutative ring. A **linear code** C over the alphabet $\mathcal{R}$ of length n is a submodule of $\mathcal{R}^n$.

Remark 2.1.23. [6, 15] If $\mathcal{R}$ is a finite field, then the linear codes are subspaces of $\mathcal{R}^n$.

Remark 2.1.24. [6] For codes over finite fields, we often denote a code C as an $[n, k, d]$-code when it is linear where n is the length, k is the dimension, and d is the minimum distance. For codes over rings, this notation is not as useful since we do not have dimension for all rings. So, we use the notation $[n, M, d]$ to indicate the same except that $|C| = M$.

Definition 2.1.25. [9, 12, 15] Consider a code C of length n over R and let $\pi = (\pi_0, \pi_1, \pi_2, ..., \pi_{n-1}) \in C$ be a codeword, then its polynomial representation is $\pi(x) = \pi_0 + \pi_1 x + \pi_2 x^2 + ... + \pi_{n-1} x^{n-1} \in R[x]$.

Definition 2.1.26. [12, 16] Consider a code C of length n over $\mathcal{R}$ and let $\pi \in C$ be a codeword.

- The **Hamming weight** of π is denoted by $wt_H(\pi)$ and is given by the total number of nonzero components of π i.e, $wt_H(\pi) = |\{j : \pi_j \neq 0\}|$.
- The smallest weight among all its nonzero codewords is the minimum weight of the code C and is denoted by $wt_H(C)$.
- The **Hamming distance** of the code C is denoted by $d_H(C)$ and is defined as $d_H(C) = \min\{wt_H(\pi) |\ \pi \neq 0, \pi \in C\}$.

2.1.4 Cyclic, Negacyclic and Constacyclic Codes

Definition 2.1.27. [6]

Let $\mathcal{R}$ be a finite commutative chain ring and let $\pi = (\pi_0, \pi_1, \pi_2, ..., \pi_{n-1}) \in C$ be any codeword. A code C of length n over $\mathcal{R}$ is said to be

- a **cyclic code**, if C satisfies the following:

$$(\pi_0, \pi_1, \pi_2, ..., \pi_{n-1}) \in C \Rightarrow (\pi_{n-1}, \pi_0, \pi_1, \pi_2, ..., \pi_{n-2}) \in C$$

- a **negacyclic code**, if C satisfies the following:

$$(\pi_0, \pi_1, \pi_2, ..., \pi_{n-1}) \in C \Rightarrow (-\pi_{n-1}, \pi_0, \pi_1, \pi_2, ..., \pi_{n-2}) \in C$$

- a **constacyclic code**, if C satisfies the following:

$$(\pi_0, \pi_1, \pi_2, ..., \pi_{n-1}) \in C \Rightarrow (\mu\pi_{n-1}, \pi_0, \pi_1, \pi_2, ..., \pi_{n-2}) \in C$$

where μ is a unit in $\mathcal{R}$.

The following conditions on the codewords follows immediately from the definition of cyclic, negacyclic and constacyclic codes.

Theorem 2.1.28. *[6] Consider a linear code C of length n over $\mathcal{R}$. Then*

- *C is a cyclic code over $\mathcal{R}$ if and only if it is an ideal of $\frac{\mathcal{R}[x]}{\langle x^n-1\rangle}$.*
- *C is a negacyclic code over $\mathcal{R}$ if and only if it is an ideal of $\frac{\mathcal{R}[x]}{\langle x^n+1\rangle}$.*
- *C is a constacyclic code over $\mathcal{R}$ if and only if it is an ideal of $\frac{\mathcal{R}[x]}{\langle x^n-\mu\rangle}$, where μ is a unit in $\mathcal{R}$.*

2.2 Symbol-pair Codes

A standard method of analysing noisy channels in information theory is to divide the message into information units called symbols. Individual symbols are frequently assumed to be studied in research on the writing and reading processes. The symbols, however, can only be written and read in possibly overlapping groups due to the use of high-density data storage technology. Cassuto and Blaum [2, 3] investigated a novel coding scheme for symbol-pair read channels in 2010. The outputs of the read process are pairs of successive symbols.

Consider an alphabet Γ of size q, and $\theta = (\theta_0, \theta_1, \ldots, \theta_{n-1}) \in \Gamma^n$. Then the symbol-pair read n-tuple of θ is $\Pi_{sp}(\theta) = ((\theta_0, \theta_1), (\theta_1, \theta_2), \ldots, (\theta_{n-1}, \theta_0)) \in (\Gamma^2)^n$.

Definition 2.2.1. [2, 3] The symbol-pair distance between two codewords θ and ϕ in Γ^n is defined as

$$d_{sp}(\theta, \phi) = |\{0 \leq j \leq n-1 : (\theta_j, \theta_{j+1}) \neq (\phi_j, \phi_{j+1})\}|,$$

where the subscripts are reduced modulo n.

Theorem 2.2.2. *[2, 3] For the symbol-pair distance between two codewords θ and ϕ in Γ^n, we have $d_{sp}(\theta, \phi) = d_H(\Pi_{sp}(\theta), \Pi_{sp}(\phi))$.*

Definition 2.2.3. [2, 3] The symbol-pair weight of a codeword θ in Γ^n is defined as

$$wt_{sp}(\theta) = |\{0 \leq j \leq n-1 : (\theta_j, \theta_{j+1}) \neq \mathbf{0}\}|,$$

where the subscripts are reduced module n and $\mathbf{0}$ denotes the all-zero n-tuple.

Definition 2.2.4. [2, 3] The symbol-pair distance of a code C is defined to be $d_{sp}(C) = \min\{wt_{sp}(\theta) |\ \theta \neq 0, \theta \in C\}$.

2.3 b-symbol Codes

Yaakobi et al. [18] expand the results of [2, 3] to b-symbol read channels, where the read operation is executed as a successive sequence of $b > 2$. Consider an alphabet Γ of size q, and $\theta = (\theta_0, \theta_1, \ldots, \theta_{n-1}) \in \Gamma^n$. Then the b-symbol read θ as $\Pi_b(\theta) = ((\theta_0, \theta_1, ..., \theta_{b-1}), \ldots, (\theta_{n-1}, \theta_0, ..., \theta_{b-2})) \in (\Gamma^b)^n$.

Definition 2.3.1. [18] The b-symbol distance between two codewords θ and ϕ in Γ^n is defined as

$$d_b(\theta, \phi) = |\{0 \leq j \leq n-1 : (\theta_j, ..., \theta_{j+b-1}) \neq (\phi_j, ..., \phi_{j+b-1})\}|,$$

where the subscripts are reduced modulo n.

Theorem 2.3.2. *[18] For the b-symbol distance between two codewords θ and ϕ in Γ^n, we have $d_b(\theta, \phi) = d_H(\Pi_b(\theta), \Pi_b(\phi))$.*

Definition 2.3.3. [18] The b-symbol weight of a codeword θ in Γ^n is defined as

$$wt_b(\theta) = |\{0 \leq j \leq n-1 : (\theta_j, \theta_{j+b-1}) \neq \mathbf{0}\}|,$$

where the subscripts are reduced modulo n and $\mathbf{0}$ denotes the all-zero n-tuple.

Definition 2.3.4. [18] The b-symbol distance of a code C is defined to be $d_b(C) = \min\{wt_b(\theta)|\ \theta \neq 0, \theta \in C\}$.

Remark 2.3.5. In view of this definition, b-symbol distance is the Hamming distance if $b = 1$, and the symbol-pair distance if $b = 2$.

2.4 Singleton Bounds and MDS Codes

We provide Singleton bounds for the Hamming, symbol-pair, and b-symbol distances in the following theorem.

Theorem 2.4.1. *[4, 5, 14, 17, 18] Let C be an n-length code over $\mathcal{R}$.*

1. *With respect to the Hamming distance, the Singleton bound is as follows:*

$$|C| \leq |\mathcal{R}|^{(n-d_H(C)+1)}.$$

2. *With respect to the symbol-pair distance, the Singleton bound is as follows:*

$$|C| \leq |\mathcal{R}|^{(n-d_{sp}(C)+2)}.$$

3. *With respect to the b-symbol distance, the Singleton bound is as follows:*

$$|C| \leq |\mathcal{R}|^{(n-d_b(C)+b)}.$$

Definition 2.4.2. [4, 5, 14, 17, 18] Let C be a code of length n over $\mathcal{R}$.

1. If $|C| = |\mathcal{R}|^{(n-d_H(C)+1)}$, then C is known as a maximum distance separable (MDS) code with respect to the Hamming distance.

2. If $|C| = |\mathcal{R}|^{(n-d_{sp}(C)+2)}$, then C is known as an MDS symbol-pair code.

3. If $|C| = |\mathcal{R}|^{(n-d_b(C)+1)}$, then C is known as an MDS b-symbol code.

2.5 The Ring $\Re$

Let p be an odd prime and m be any positive integer. Consider a finite field $\mathbb{F}_{p^m}$ of order p^m, then $\Re = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ with $u^2 = 0$ is a finite commutative chain ring with unity.

- The ring, $\Re = \mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ with $u^2 = 0$ is isomorphically, $\frac{\mathbb{F}_{p^m}[u]}{\langle u^2 \rangle}$, where p is a prime.
- It is a finite chain ring having $\langle u \rangle$ as a unique maximal ideal.
- The set containing all elements of $\Re$ is given as $\{h_0 + uh_1 | h_0, h_1 \in \mathbb{F}_{p^m}$ and $u^2 = 0\}$.
- There are two types of units in the ring $\Re$, first is of Ω type and second is of $(\Phi + u\Psi)$ type, where $\Omega, \Phi, \Psi \in \mathbb{F}_{p^m}^*$.

References

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass-London-Don, Ont., 1969.

[2] Y. Cassuto and M. Blaum, "Codes for symbol-pair read channels," *IEEE Trans. Inform. Theory*, vol. 57, pp. 988–992, 2010.

[3] Y. Cassuto and M. Blaum, "Codes for symbol-pair read channels," *Proceedings of IEEE International Symposium on Information Theory*, vol. 57, no. 12, pp. 8011–8020, 2011.

[4] Y. M. Chee, L. Ji, H. M. Kiah, C. Wang, and J. Yin, "Maximum distance separable codes for symbol-pair read channels," *IEEE Trans. Inform. Theory*, vol. 59, no. 11, pp. 7259–7267, 2013.

[5] B. Ding, T. Zhang, and G. Ge, "Maximum distance separable codes for b-symbol read channels," *Finite Fields Appl.*, vol. 49, pp. 180–197, 2018.

[6] S. T. Dougherty, *Algebraic coding theory over finite commutative rings*. Springer, 2017.

[7] D. S. Dummit and R. M. Foote, *Abstract algebra*. Wiley Hoboken, 2004, vol. Third Edition.

[8] J. A. Gallian, *Contemporary abstract algebra*. Chapman and Hall/CRC, 2021.

[9] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*. Cambridge University Press, 2010.

[10] M. E. Keating, *A first course in module theory*. World Scientific, 1998.

[11] T.-Y. Lam, *Lectures on modules and rings*. Springer Science & Business Media, 2012, vol. 189.

[12] S. Ling and C. Xing, *Coding theory: A first course*. Cambridge University Press, 2004.

[13] H. Matsumura, *Commutative ring theory*. Cambridge University Press, 1989.

[14] G. H. Norton and A. Sălăgean, "On the Hamming distance of linear codes over a finite chain ring," *IEEE Trans. Inform. Theory*, vol. 46, no. 3, pp. 1060–1067, 2000.

[15] V. Pless, *Introduction to the theory of error-correcting codes*. John Wiley & Sons, 1998, vol. 48.

[16] R. Roth, *Introduction to coding theory*. Cambridge University Press, 2006.

[17] R. Singleton, "Maximum distance q-nary codes," *IEEE Trans. Inform. Theory*, vol. 10, no. 2, pp. 116–118, 1964.

[18] E. Yaakobi, J. Bruck, and P. H. Siegel, "Constructions and decoding of cyclic codes over b-symbol read channels," *IEEE Trans. Inform. Theory*, vol. 62, no. 4, pp. 1541–1551, 2016.

*****