ECEN 604 - Channel Coding for Communication
Lectures by Graduate Students

Narayanan Rengaswamy
Department of Electrical and Computer Engineering
Texas A&M University, College Station, TX 77843

October 2015

Lecture 5

1 Rings and Cyclic Codes

We have understood the motivation behind coding theory, fundamentals of groups and fields, construction of block codes, their generator and parity-check matrices as a result of imposing linearity on them, decoding methods leveraging the concepts of coset tables of subgroups, and simple bounds on linear block codes. Next, we will explore and impose an additional structure on block codes: the *cyclic* property. In addition to being linear, cyclic codes should satisfy the property that the cyclic shift of any codeword results in another codeword of the same code. Therefore, for a cyclic code $\mathcal{C}$, if $\underline{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ is a codeword, then there should be another codeword in $\mathcal{C}$ such that $\underline{c'} = (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$.

Definition 1. An (n, k) block code $\mathcal{C}$ is said to be **cyclic** if it is *linear* and if for every codeword $\underline{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, its right cyclic shift $\underline{c'} = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is also in $\mathcal{C}$.

It is common to deal with polynomials in the realm of cyclic codes. A vector $\underline{c} = (c_0, c_1, c_2, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ can be written as the polynomial $c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1}$. Given this notation, a cyclic shift would be written as $c'(x) = c_{n-1} + c_0 x + c_1 x^2 + c_2 x^3 + \cdots + c_{n-2} x^{n-1}$. A non-cyclic shift can be represented as $xc(x) = c_0 x + c_1 x^2 + c_2 x^3 + \cdots + c_{n-1} x^n$ so that

$$(0, c_0, c_1, c_2, \ldots, c_{n-1}) \leftrightarrow c_0 x + c_1 x^2 + c_2 x^3 + \cdots + c_{n-1} x^n.$$

To make this cyclic, we need to perform a polynomial division by $(x^n - 1)$ and take the remainder. To see this, consider $c^{(1)}(x) = c_{n-1} + c_0 x + c_1 x^2 + c_2 x^3 + \cdots + c_{n-2} x^{n-1}$, which

is the cyclic shifted polynomial of $c(x)$ that we intend to obtain. It is clear that

$$\begin{aligned} & xc(x) + c_{n-1} - c_{n-1}x^n = c^{(1)}(x) \\ \Rightarrow\ & xc(x) - c_{n-1}(x^n - 1) = c^{(1)}(x) \\ \Rightarrow\ & xc(x) = c_{n-1}(x^n - 1) + c^{(1)}(x) \\ \therefore\ & xc(x)/(x^n - 1) = c^{(1)}(x), \end{aligned}$$

which implies that the cyclic shifted polynomial $c^{(1)}(x)$ is obtained as the non-cyclic shifted polynomial $c'(x)$ modulo $(x^n - 1)$.

We will need to understand rings to appreciate and work with cyclic codes. A good reference for the material of this lecture is [1, Chapter 4].

1.1 Rings

Definition 2. A **ring $(R, +, \times)$** is a set R with two binary operations + (addition) and $\times$ (multiplication) defined on it such that

(i) $(R, +)$ is a Abelian group (identity is 0).

(ii) $(R, \times)$ is closed.

(iii) $(R, \times)$ is associative.

(iv) Multiplication distributes over addition, i.e. $\forall\ a, b, c \in R$,

$$\begin{aligned} &\text{(left)} \quad a \times (b + c) = (a \times b) + (a \times c), \\ &\text{(right)}\ (a + b) \times c = (a \times c) + (b \times c). \end{aligned}$$

Note from the definition that the multiplication operation of a ring neither need to be commutative nor need to have an identity, necessarily.

Definition 3. A ring is said to be a **commutative ring** if the multiplication operation is commutative on the set R, i.e. $a \times b = b \times a\ \forall\ a, b \in R$.

We will be dealing with commutative rings extensively in this course.

Definition 4. A ring is said to be a **ring with an identity** if the multiplication operation $\times$ has an identity element 1, i.e. $a \times 1 = 1 \times a = a\ \forall\ a \in R$.

Note that a field is a commutative ring with an identity where all non-zero elements have a multiplicative inverse.

Example. The set of all $n \times n$ matrices over $\mathbb{R}$, $\mathbb{R}^{n \times n}$, with matrix addition and multiplication operations is a non-commutative ring with identity.

Definition 5. For any ring R, its **polynomial ring** $R[x]$ is given by

$$R[x] = \{p(x) = \sum_i a_i x^i \mid a_i \in R\}.$$

Example. Since $(\mathbb{R}^{n\times n}, +, \times)$ is a ring of all real $n \times n$ matrices, $\mathbb{R}^{n\times n}[x]$ is its ring of polynomials with coefficients from $\mathbb{R}^{n\times n}$. For example,

$$p(x) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 3.3 \\ -0.15 & 2 \end{bmatrix} x + \begin{bmatrix} 1.375 & 2 \\ 3 & -9 \end{bmatrix} x^2 \ \in \ \mathbb{R}^{n\times n}[x].$$

Definition 6. An **ideal *I*** of a ring R is a subset I such that

(*i*) $(I, +)$ is a subgroup of $(R, +)$.

(*ii*) $a \times r \in I \ \forall \ a \in I, r \in R$.

Example. Since $(\mathbb{Z}, +, \times)$ is a ring of all integers, then $3\mathbb{Z} = \{3x \mid x \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$. But, note that $3\mathbb{Z} \ \cup \ 2\mathbb{Z}$ is *not* an ideal of $\mathbb{Z}$.

Example. $\mathbb{Z}[x]$ is the ring of polynomials with integer coefficients. Then, $(x^2+1)\mathbb{Z}[x]$ is an ideal of $\mathbb{Z}[x]$.

Definition 7. An ideal I in a ring R is said to be a **principal ideal** if there exists some $g \in I$ such that every element $a \in I$ can be expressed as a product $a = mg$ for some $m \in R$. Such an element g is called a **generator** element and the principal ideal is represented as $\langle g \rangle$ so that

$$\langle g \rangle = \{mg \mid m \in R\}.$$

Definition 8. The **quotient ring**, or **factor ring**, $\boldsymbol{R/I}$ of a *commutative* ring R generated by the ideal I is a commutative ring whose elements are the *residue classes* $R/I = \{a + I \mid a \in R\}$, i.e. the cosets of the additive subgroup I.

The addition and multiplication operations for the factor ring are defined as

$$\begin{aligned} &\text{(Addition)} && (a + I) \oplus (b + I) = (a + b) + I, \\ &\text{(Multiplication)} && (a + I) \otimes (b + I) = (a \times b) + I, \ \forall \ a, b, \in R. \end{aligned}$$

Example. For the ideal $3\mathbb{Z}$ of the ring $\mathbb{Z}$, the quotient ring is $R/I = \{3\mathbb{Z}, 3\mathbb{Z} + 1, 3\mathbb{Z} + 2\}$.

Now, let us extend the concept of factor rings to rings of polynomials. Consider the ring $\mathbb{F}_2[x]$ and its ideal $(x^3 - 1)\mathbb{F}_2[x]$. The factor ring formed by this ideal is denoted as $\mathbb{F}_2[x]/(x^3-1)$, which is the set of all polynomials of degree at most 2 with binary coefficients.

Theorem 9. *Let I be an ideal in $\mathbb{F}_q[x]/(x^n - 1)$. Then,*

(*i*) *There is a unique* monic *polynomial $g(x) \in I$ of minimal degree.*

(*ii*) *I is principal with generator $g(x)$.*

(*iii*) *$g(x)$ divides $(x^n - 1)$ in $\mathbb{F}_q[x]$.*

1.2 Cyclic Codes

Definition 10. An (n, k) linear block code $\mathcal{C}$ over a field $\mathbb{F}_q$ is **cyclic** if it is a **principal ideal** in the (quotient) ring of polynomials $\mathbb{F}_q[x]/(x^n - 1)$.

Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_q$. Recollect that a codeword can be represented as

$$\underline{c} = (c_0, c_1, \ldots, c_{n-1}) \;\leftrightarrow\; c(x) = \sum_{i=0}^{n-1} c_i x^i \in \mathcal{C},$$

where $c_i \in \mathbb{F}_q[x]$. Since $\mathcal{C}$ is an ideal in $\mathbb{F}_q[x]/(x^n - 1)$, it has a **generator polynomial $\boldsymbol{g(x)}$** such that any codeword $c(x)$ can be obtained as

$$c(x) = m(x)g(x), \tag{1}$$

for some **message polynomial** $m(x) = \sum_{i=0}^{k-1} m_i x^i \in \mathbb{F}_q^k$. Equation (1) represents the **non-systematic encoding** for the cyclic code $\mathcal{C}$.

A **systematic encoder** for $\mathcal{C}$ is given by

$$c(x) = x^{n-k} m(x) - R_{g(x)}[x^{n-k} m(x)], \tag{2}$$

where $R_{g(x)}[\cdot]$ represents the remainder of the argument after dividing by $g(x)$.

From Theorem 9 we know that $g(x) \mid (x^n - 1)$. The quotient obtained by dividing $(x^n - 1)$ by $g(x)$ is the **parity-check polynomial $\boldsymbol{h(x)}$** of the code $\mathcal{C}$.

$$x^n - 1 = g(x)\; h(x), \tag{3}$$

where $g(x)$ has degree $r = n - k$ and $h(x)$ has degree k.

The non-systematic generator and parity-check matrices can be obtained as

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_r & & & & \\ & g_0 & g_1 & g_2 & \cdots & g_r & & & \\ & & g_0 & g_1 & g_2 & \cdots & g_r & & \\ & & & \ddots & \ddots & \cdots & & \ddots & \\ & & & & g_0 & g_1 & g_2 & \cdots & g_r \end{bmatrix} \tag{4}$$

$$H = \begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & & & & \\ & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & & & \\ & & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & & \\ & & & \ddots & \ddots & \cdots & & \ddots & \\ & & & & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 \end{bmatrix} \tag{5}$$

Example: (7,4) Binary Hamming Code

We have $n = 7, k = 4$ over $\mathbb{F}_2$. In $\mathbb{F}_2[x]$, $(x^7 - 1)$ can be factorized as

$$x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Note that $-1 = 1$ in $\mathbb{F}_2$. The $(7, 4)$ binary Hamming code can be constructed by setting the generator polynomials as $g(x) = x^3 + x + 1$. Hence, the parity-check polynomial is $h(x) = (x + 1)(x^3 + x^2 + 1) = x^4 + x^2 + x + 1$.

1.3 Decoding

Let $c(x) = m(x)g(x)$ be the transmitted codeword and $r(x) = c(x) + e(x)$ be the received word, where $e(x)$ is the **error polynomial**. Syndrome decoding can be implemented using the syndrome polynomial

$$s(x) = R_{g(x)}[r(x)] = R_{g(x)}[e(x)], \tag{6}$$

since $R_{g(x)}[c(x)] = 0$. For each error polynomial $e(x)$ that we intend to correct, we can compute and store $s(x)$. Given a received vector, we can find the syndrome and correct it using the lookup table consisting of error polynomials and syndrome polynomials.

Burst Errors

A burst error of length ℓ is defined by an error vector having two 1s marking the beginning and ending of the burst and $\ell - 2$ entries between them, which are not necessarily 1s.

Theorem 11. *Given an (n, k) cyclic code $\mathcal{C}$, all error bursts of length ℓ can be* detected *if $\ell \leq deg[g(x)] = n - k$.*

Proof. Suppose the burst occurs at the beginning of a codeword. Then $e(x) = 1 + x + x^2 + \cdot + x^{\ell-1}$. So, clearly, if $\deg[e(x)] < \deg[g(x)]$, $e(x)$ is not divisible by $g(x)$ and the error will be detected.

If the error burst is shifted, then $e(x) = x^i(1 + x + x^2 + \cdots + x^{\ell-1})$. But, $g(x)$ has at least two non-zero terms since it is monic and does not have x as a factor. Hence, x^i cannot be divided by $g(x)$ and hence $e(x) \bmod g(x) \neq 0$. □

This concept is used to construct *cyclic redundancy check (CRC)* codes for error detection purposes.

References

[1] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms.* John Wiley & Sons, Inc., 2005.