Linear Block Codes

Kwame Ackah Bohulu

April 18, 2018

1 Linear Block Codes

Focus is on the study of channel coding schemes, especially block codes which can be constructed using the idea of groups, rings and fields.

1.1 Basic Definitions

In block codes we choose an **information sequence** m of length k which is a member of a set of possible information sequences of size $M = 2^k$. This information sequence is then mapped to a binary sequence (**codeword**)of length n and transmitted over the channel using a suitable modulation scheme. Block codes are memoryless since the codeword depends only on the current information sequence m .

The **code rate** R_c of the block code is given by

$$R_c = \frac{k}{n} \tag{1}$$

and represents the number of information bits sent in the transmission of the codeword over the channel.

If the symbol duration is given by T_s then the transmission time for k bits is given by $T = LT_s$ and the transmission rate is given by

$$R = \frac{k}{LT_s} \tag{2}$$

We set $L = \frac{n}{\log_2 M}$ Where L is an integer representing the number of M-ary symbols transmitted per codeword and M is the constellation size of the modulation scheme used. (2) becomes

$$R = R_c \frac{\log_2 M}{T_s} \tag{3}$$

and the minimum required transmission bandwidth is given by

$$W = \frac{N}{T_s} = \frac{RN}{2R_c \log_2 M} \tag{4}$$

From (3) and (4) we can see that compared to systems without channel coding that use the same modulation scheme there is a decrease in channel rate and and increase in bandwidth respectively.

1.1.1 Structure of Finite Fields

We begin by defining an Abelian group is a set with a binary operation that has the basic properties of addition. It is denoted by $\{G, +, 0\}$ and the set G and $+$ constitute and Abelian group if the operation $+$ is commutative, associative and has an identity element and the set G has an inverse element.

A finite field or Galois field is a finite set F with 2 binary operations + and $\cdot$(representing mutliplication) and is denoted by $\{F, +, \cdot\}$. F is a finite field if it satisfies the properties that

- $\{F, +, 0\}$ is an Abelian group
- $\{F - \{0\}, \cdot, 1\}$ is an Abellian group
- Multiplication is distributive with respect to addition, i.e. $a \cdot (b + c) = (b + c) \cdot a = a \cdot b + a \cdot c$

The set $F = \{0, 1\}$ with modulo-2 addition and multiplication is an example of a Galois field and is known as the binary field and is denoted by $GF(2)$

Characteristic of a Field and a Ground Field A fundamental theory of algebra states that that a Gaolois field with q elements ($GF(q)$) exist if and only if $q = p^m$, where p is a prime and m is a positive integer. The Galois field $GF(q)$ is known as the **extension field** of the **ground field** $GF(p)$ and p is called the **characteristic** of $GF(p^m)$

Polynomial over Finite Fields A polynomial of degree m over $GF(p)$ is a polynomial

$$g(X) = g_0 + g_1 X + g_2 X^2 + \cdots + g_m X^m \tag{5}$$

It should be noted that $g_i, 0 \leq i \leq m$, are all elements of $GF(p)$, $g_m \neq 0$ and all addition and multiplication of coefficients are done modulo-p. If $g_m = 1$, the polynomial is **monic** and if the polynomial cannot be written as a product of 2 polynomial of lower degree over the same Galois Field the polynomial is irreducible. A prime polynomial is both irreducible and and monic. A polynomial of degree m has m roots but a which in general are in some extension field of $GF(p)$

Structure of Extension Fields It should be noted that $GF(p^m)$ contains p^m polynomials and of degree less than m, with two special polynomials $g(X) = 0$ and $g(X) = 1$. Assuming $g(X)$ is a primitive polynomial and and considering the set of polynomials of degree less that m over $GF(p)$, we can show that the set of these polynomials with addition and multiplication operations form a Galois field with p^m elements.

Example construction of $GF(2^2)$ from $GF(2)$ with $g(X) = X^2 + X + 1$.

+	0	1	X	$X+1$
0	0	1	X	$X+1$
1	1	0	$X+1$	X
X	X	$X+1$	0	1
$X+1$	$X+1$	X	1	0

Table 1: Addition for $GF(4)$

·	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	X+1	1
$X+1$	0	$X+1$	1	X

Table 2: Multiplication for $GF(4)$

The elements of $GF(4)$ may be written as powers of X, i.e. $X = X^1$, $X+1 = X^2$, $1 = X^3$. They can also be written in binary notation , i.e. $X = 10$, $X + 1 = 11$, $1 = 01$.

For any nonzero element $\beta \in GF(q)$ the smallest value of i such that $\beta^i = 1$ is called the order of β. A nonzero element of $GF(q)$ is called a primitive element if its order is $q-1$. If $GF(p^m)$ generated by $g(X)$ is such that in this field X is a primitive element, then $g(X)$ is a primitive polynomial. A second definition of a primitive polynomial is that if $g(X)$ does not divide X^i+1 for any $i < p^m - 1$

Let β be a non zero element of $GF(2^m)$. Then the minimal polynomial of β, denoted by ϕ_β is a monic polynomial of lowest degree with coefficients in $GF(2)$ such that $\phi_\beta(\beta) = 0$

To find the minimal polynomial of a field element we note that since $\beta \in GF(2^m)$ and $\beta \neq 0$, $\beta^{2^m-1} = 1$. However, it is possible that for some integer $l < m$ we have $\beta^{2^l-1} = 1$.

It can be shown that for any $\beta \in GF(2^m)$ the minimal polynomial ϕ_β is given by

$$\phi_\beta = \prod_{i=0}^{l-1} \left(X + \beta^{2^i} \right) \tag{6}$$

Elements of the form $\beta^{2^i}, 1 < i \leq l-1$, are called conjugates of β. All elements of the finite field that are conjugates of each other are said to belong to the same conjugacy class.

We use the following steps to find the minimal polynomial of $\beta \in GF(q)$

- find l such that $\beta^{2^l} = \beta$
- find the conjugacy class of β
- find $\phi_\beta(X)$ using 6

This is demonstrated by going through Example 7.1-5

We conclude our discussion by stating that all nonzero elements of $GF(p^m)$ are roots of $X^{p^m-1} - 1 = 0$ This means that $X^{2^m-1} - 1$ can be factorized over $GF(2)$ as the product of all prime polynomials over GF(2) whose degree divides m

1.2 General Properties of Linear Block Codes

A $q-$ary block code C consists of a set of M vectors of length n denoted by $\mathbf{c}_m = (c_{m1}, c_{m2}, ..., c_{mn}), 1 \leq m \leq M$ called codewords which are selected from an alphabet of q symbols. Binary codes are selected from an alphabet with 1 and 1 as the only elements.

There are 2^n possible codewords in a binary block code of length n from which we may select $M = 2^k$ codewords $(n > k)$ to form a code. The resulting block code is reffered to as an (n, k) codeword with rate $R_c = k/n$. Another important parameter of a codeword is it's weight, which is the number of nonzero elements present in the codeword and the set of all weights in a code is known as the weight distribution of the code. Constant-weight codes have codewords of the same weight.

A linear block codes C, which is a subset of block codes which have been widely studied to to their relatively easy implementation. Binary linear block codes have the property such that the addition of any of the 2^k codewords produces another codeword.

1.2.1 Generator and Parity Check Matrices

The generator matrix $\mathbf{G}$ is a $(k \times n)$ which shows the mapping from the set of $M = 2^k$ information sequences of length k to the corresponding 2^k codewords of length n and

$$\mathbf{c}_m = \mathbf{u}_m \mathbf{G}, 1 \leq m \leq 2^k \tag{7}$$

where $\mathbf{u}_m$ is the binary vector of length k denoting theinformation sequence. c_m may also be witten as

$$\mathbf{c}_m = \sum_{i=1}^{k} u_{mi} \mathbf{g}_i, 1 \leq i \leq k \tag{8}$$

where $\mathbf{g}_i$ denotes the ith row of $\mathbf{G}$

if the $\mathbf{G}$ is in the form $\mathbf{G} = [\mathbf{I}_k | \mathbf{P}]$, the resulting linear block code is called systematic. $\mathbf{I}_k$ is a $k \times k$ identity matrix and $\mathbf{P}$ is a $k \times (n-k)$ matrix. In a

systematic code, the first k element are the same as the information sequence and the remaining $n-k$ elements called the parity check bits provide redundancy for protection against errors. The dual code of C is an $(n, n-k)$ dimensional code and has an $(n-k \times n)$ generator matrix whose rows are otrhogonal to $\mathbf{G}$ and is known as the parity check matrix $\mathbf{H}$ of the original code. It is worth noting that

$$\mathbf{cH}^t = \mathbf{0}$$

In the special case of systematic binary codes, if $\mathbf{G}$ is in systematic form , we can write

$$\mathbf{H} = [\mathbf{P}^t | \mathbf{I_{n-k}}] \tag{9}$$

for further explanation we consider Example 7.2-1 .

1.2.2 Weight and Distance for Linear Block Codes

The weight of a codeword $w(\mathbf{c})$ is the number of nonzero components of that codeword. The Hamming distance between two codewords $\mathbf{c}_1, \mathbf{c}_2$ denoted by $d(\mathbf{c}_1, \mathbf{c}_2)$ is the number of components at which $\mathbf{c}_1$ and $\mathbf{c}_2$ differ. It can easily be seen that for linear block codes, $d(\mathbf{c}_1, \mathbf{c}_2) = w(\mathbf{c}_1 + \mathbf{c}_2)$

The minimum distance of a code is the minimum of all possible of all possible distances between distince codewords of the code, ie

$$d_{min} = \min_{\mathbf{c}_1, \mathbf{c}_2 \in C, \mathbf{c}_1 \neq \mathbf{c}_2} d(\mathbf{c}_1, \mathbf{c}_2) \tag{10}$$

The minimum weight of a code is the minimum of all the weights of all nonzero codewords, and for the case of linear block codes this is equal to the minimum distance.

$$w_{min} = \min_{\mathbf{c} \in C, c \neq 0} w(c) \tag{11}$$

It should be noted that in $\mathbf{H}$, d_{min} represents the minimum number of columns that can be linearly dependent.

2 Cyclic Codes

Cyclic codes are a subset of linear block codes which satisfy the cyclic shift property : if $\mathbf{c} = (c_{n-1}, c_{n-2}, ..., c_1, c_0)$ then any cyclic shift of the elements in $\mathbf{c}$ is also a codeword.

For convenience $\mathbf{c}$ is usually represented by a polynomial $c(X)$ of degree at most $n-1$

$$c(X) = c_{n-1}X^{n-1} + c_{n-2}X^{n-1} + ... + c_1X + c_0 \tag{12}$$

We can generate a cyclic code by using a generator polynomial $g(X)$ of degree $n-k$. This generator polynomial is a factor of $X^n + 1$ and has the general form

$$g(X) = X^{n-k} + g_{n-k-1}X^{n-k-1} + ... + g_1X + 1 \tag{13}$$

The message polynomial $u(X)$ is defined by

$$u(X) = u_{k-1}X^{k-1} + u_{k-2}X^{k-2} + ... + u_1X + u_0 \tag{14}$$

For further explanation do Example 7.9-1
In general, the polynomial $X^n + 1$ may be factored as

$$X^n + 1 = g(X)h(X) \tag{15}$$

where $h(X)$ denotes the parity check polynomial that has degree k and this can be used to generate the dual code. To do this, we define the reciprocal polynomial of $h(X)$ as

$$X^k h(X-1) = 1 + h_{k-1}X + hk - 2X^2 + \cdots + h_1X^{k-1} + X^k \tag{16}$$

$X^k h(X-1)$ is the generator polynomial of an $(n, n-k)$ cyclic code. do Example 7.9-3

We show how the generator matrix can be generated from the generator polynomial $g(X)$ To do this we use a set of k linearly independent codewords which corresponds to the set of linearly independent polynomials $X^{k-1}g(X), x^{k-2}g(X), Xg(X), g(X)$

Explain with example 7.9-4

2.1 Systematic Cyclic Codes

We may generate a systematic cyclic code by either using the generator polynomial or directly from the message polynomial. Using the generator polynomial we observe that the lth row of $\mathbf{G}$ corresponds to a polynomial of the form $X^{n-l} + R_l(X), l = 1, 2, ..., k$ where $R_l(X)$ is a polynomial of degree less than $n - k$. This can be obtained by dividing X^{n-1} by $g(X)$ and the desired polynomial to generate the systematic form of $\mathbf{G}$ is $X^{n-l} + R_l(X)$.
Do Example 7.9-5
To obtain the systematic code directly from the message polynomial $u(X)$ we first multiply $u(X)$ by X^{n-k}. We then divide the product by $g(X)$ to obtain the remainder $r(X)$. Finally, we add $r(X)$ to $X^{n-k}u(X)$