WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Study on Linear Block Codes

R. Kishore, Raghotham C.G, Shreya V Dev, Sadhana M, Varsha M.S, Pruthvi Dinesh*

UG Student, Department of Computer Sc & Engineering, KSIT, Bangalore, INDIA

A B S T R A C T

The Article discusses in this paper is systematic cyclic linear block codes. A block code uses an encoder that accepts a block of message symbols, and generates a block of code word symbols at the output. This type is in contrast to a convolution code when the encoder accepts a continuous stream of symbols and similarly generates a continuous output stream. A code is linear if the addition of any two valid code words results in another valid code word. Similarly, a code is cyclic if a circular shift of any valid code word results in another valid code word.

Keywords: *block of code , Coding, Messaging*

1. Introduction

This binary information sequence is segmented intomessage block of fixed length, denoted by **u.** Each message block consists of **k** information digits. There are a total of 2^k distinct message.

1. The encoder transforms each input message **u** into a binary n-tuple **v** with n > k. This n-tuple **v** is referred to as the code word (orcodevector) of the message **u**.
2. There are distinct 2^k code words. This set of 2^k code words is called a block code.
3. For a block code to be useful, there should be a one-to-onecorrespondence between a message **u** and its code word **v.**
4. A desirable structure for a block code to possess is the linearity.
5. With this structure, the encoding complexity will be greatlyreduced.

2. Methodology

- A block code of length n and 2k code word is called a linear (n,k) code if its 2k code word from a k-dimensional subspace of the vector space of all the n-type over the field
- Since an (n,k) linear code c is a k dimensional subspace of the vector space vn of all the binary n-bites it is possible to find k linearly independent code word g_0,g_1,g_2……g_{k-1} in c

$$V=u_0g_0+u_1g_1+\ldots\ldots u_{k-1}g_{k-1}$$

Where ui=0 or 1 for 0<i<k
AA message m is a binary sequence of size k:m.e.A^K

* *Corresponding author.*
E-mail address: pruthvi.sunitha@gmail.com

- To each message m corresponding a code word which is a binary sequence c of size n:n>k.
- The code space contains 2^n point but only 2^k of them are valid code word.
- A code must be done to one relation (injection).
- n code word symbols can take $2n$ possible values. From that we select $2k$ code words to form the code.
- A block code is said to be useful when there is one to one mapping between message m and its code word c as shown above.

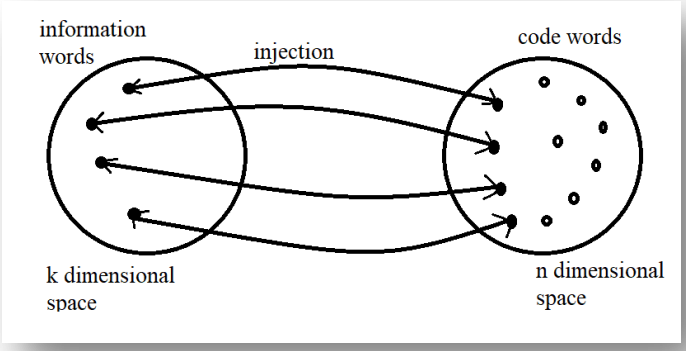


Fig 1 Mapping Between Message and its Code Word

- A code is called linear if the modulo-2 sum of two code words is also a code word.
- The encoder generates a block of n coded bits from 'k' information bits and we call this as (n, k) block codes.
- The coded bits are also called as code word symbols.

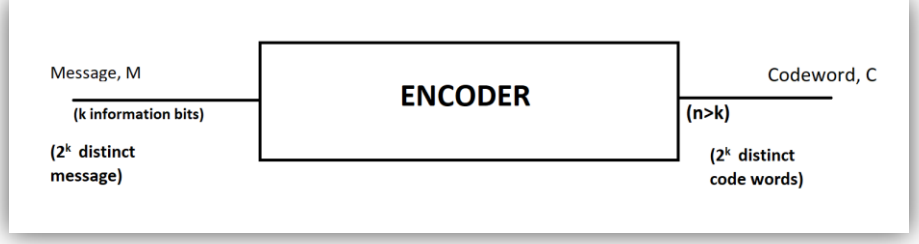


Fig 2.Encoder

- There are basically two mechanisms for addingredundancy:
    1. Block coding
    2. Convolutional coding
- A code is linear if the modulo-2 sum of two code words is also a code word.n code word symbols can take 2^n possible values.
- From that we select 2^kcode words to form the code.
- A block code is said to be useful when there is one to one mapping between message m and its code word c.

3. Generator Matrix

All code words can be obtained as linear combination of basis vectors.

- The basis vectors can be designated as $\{g_1, g_2, g_3, \ldots, g_k\}$
- For a linear code, there exists a k by n generator matrix such that $c_{1*n} = m_{1*k} . G$

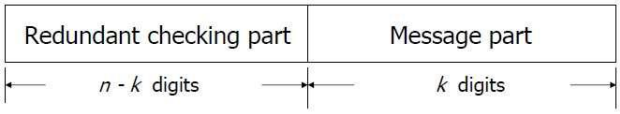
  where c=$\{c_1, c_2, \ldots, c_n\}$ and m=$\{m_1, m_2, \ldots, m_k\}$

$$G=\begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{bmatrix}=\begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & & \vdots \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}$$

Block codes in systematic form

In this form, the code word consists of (n-k) parity check bits followed by k bits of the message.

- The structure of the code word in systematic form is:



- The rate or efficiency for this code R= k/n

G = [I_k P]

C = m.G = [m mP]

m : Message part

mP: Parity part

Example: Let us consider (7, 4) linear code where k=4 and n=7

$$\text{m=(1110) and G=}\begin{bmatrix} g1 \\ g2 \\ g3 \\ g4 \end{bmatrix}=\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

c= m.G = $\boldsymbol{m_1 g_1+m_2 g_2+m_3 g_3+m_4 g_4}$=1.$\boldsymbol{g_1}$+**1**.$\boldsymbol{g_2}$+**1**.$\boldsymbol{g_3}$+**0**.$\boldsymbol{g_4}$

c = (1101000) + (0110100) + (1110010)

= (0101110)

Alternate method:

Let m=(m_1, m_2, m_3, m_4) and c= (c_1, c_2, c_3, c_4, c_5, c_6, c_7)

$$\text{c=m.G= }(m_1, m_2, m_3, m_4)\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

By matrix multiplication we obtain :

$c_1=m_1+m_3+m_4,\ c_2=m_1+m_2+m_3,\ c_3= m_2+m_3+m_4,\ c_4=m_1,\ c_5=m_2, c_6=m3,\ c_7=m_4$

The code word corresponding to the message (1110) is (0101110).

Parity check matrix:

- When G is systematic, it is easy to determine the parity check matrix H as:

$$H = [I_{n-k} P^T]$$

- The parity check matrix H of a generator matrix is an (n-k)-by-n matrix satisfying:

$$H_{(n-k)*n} G^T_{n*k} = 0$$

- Then the code words should satisfy (n-k) parity check equations

$$c_{1*n} H^T_{n*(n-k)} = m_{1*k} G_{k*n} H^T_{n*(n-k)} = 0$$

Example: Consider generator matrix of (7, 4) linear block code

$$H = [I_{n-k} P^T] \quad \text{and} \quad G = [P I_k]$$

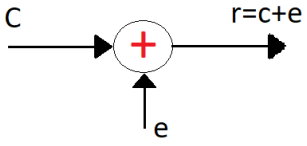
The corresponding parity check matrix is:

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$G.H^T = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = 0$$

Syndrome and error detection

For a code word c, transmitted over a noisy channel, let r be the received vector at the output of the channel with error e



$$e = \begin{cases} 1, \text{ if } r \neq c \\ 0, \text{ if } r = c \end{cases}$$

Syndrome of received vector r is given by:

$$s = r.H^T = (s_1, s_2, s_3, \ldots\ldots\ldots, s_{n-k})$$

Properties of syndrome

- The syndrome depends only on the error pattern andnot on the transmitted word.

$$s = (c+e).H^T = c.H^T + e.H^T = e.H^T$$

- All the error pattern differ by atleast a code wordhave the same syndrome s.
  Example: Let C=(0101110) be the transmitted code and r=(0001110) be the received vector.

$$s = r.H^T = (s_1, s_2, s_3)$$

$$= (r_1, r_2, r_3, r_4, r_5, r_6, r_7) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

The syndrome digits are:

$$s_1 = r_1 + r_4 + r_6 + r_7 = 0$$
$$s_2 = r_2 + r_4 + r_5 + r_6 = 1$$
$$s_3 = r_3 + r_5 + r_6 + r_7 = 0$$

The error vector, e=(e_1, e_2, e_3, e_4, e_5, e_6, e_7) =(0100000)

C= r + e
= (0001110)+(0100000)
= (0101110)
where C is the actual transmitted code word

Minimum distance of a block code:

- **Hamming weight w(c)** : It is defined as the number of non-zero components of c.

  For ex: The hamming weight of c=(11000110) is 4

- **Hamming distance d (c, x):** It is defined as the number of places where they differ.The hamming distance between c=(11000110) and x=(00100100) is 4.
- The hamming distance satisfies the triangle inequality

$$d(c, x)+d(x, y) \geq d(c, y)$$

- The hamming distance between two n-tuple c and x is equal to the hamming weight of the sum of c and x

$$d(c, x) = w(c+ x)$$

For example: The hamming distance between c=(11000110) and x=(00100100) is 4 and the weight of c + x = (11100010) is 4.

- **Minimum hamming distance (d)** :

It is defined as the smallestdistance between any pair of code vectors in the code.

For a given block code C, d is defined as:

$$d_{min}=\min\{ d(c, x):^{min} c, x€C, c x\}$$

- The Hamming distance between two code vectors in C is equal to the Hamming weight of a third code vector in C.

$$d_{min} = \min\{w(c+x):c, x €C, c\neq x\}$$

$$= \min\{w(y):y €C, y\neq 0\}$$

$$= W_{min}$$

Applications:

- Communications:
  - Satellite and deep space communications.
  - Digital audio and video transmissions.
- Storage:
  - Computer memory (RAM).
  - Single error correcting and double error detecting code.

Merits and Demerits:

- **Merits:**
  - It is the easiest and simplest technique to detect and correct errors.
  - The error probability is reduced.
- **Demerits:**
  - Transmission bandwidth requirement is more.
  - Extra bits reduces bits rate of transmitter and also reduces its power.

4. Conclusion

The field of error control coding is a fascinating subject that is of interest to both the theoretical mathematician and the practical engineer. Error control codes of some type are used in almost any digital communications system where data integrity is an issue. The literature at the end of this article will provide the interested reader with a good starting point to learn more.

REFERENCES

[1]. https://archive.org/details/channelcodesclas00ryan.
[2]. https://web.archive.org/web/20070927213247/http://jason.mchu.com/QCode/index.html
[3]. http://www.codetables.de/
[4]. http://z4codes.info/