International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 1 ǁ 2022 ǁ PP. 69-73

Verilog Implementation of Hamming Code for Error Control Coding

M A Muneeb[1]; Namratha S[2]
*[*1]Pre-Final Year Undergraduate Student, Dept. of Electronics and Communication Engineering,*
Guru Nanak Dev Engineering College, Bidar, Karnataka, India.
*[*2]Assistant Professor, Dept. of Electronics and Communication Engineering,*
Guru Nanak Dev Engineering College, Bidar, Karnataka, India.
Corresponding Author: M A Muneeb

Abstract

This paper generally introduces to the method that is used for error control coding and particularly about Hamming Codes. Theoretical generation of codes is done using the formula and hardware implementation is done in Verilog (Hardware Description Language) using Xilinx Vivado Design Suite. Waveforms are given in which the code generation can be seen.

Keywords: *Error Control Coding, Hamming Code, VLSI, Encryption, Verilog.*

Date of Submission: 28-12-2021 Date of acceptance: 07-01-2022

I. INTRODUCTION

As we all are moving towards globalization of technology where dependency of human beings on technology keeps increasing day by day. The advancements in the technology brings all of us on a single platform i.e., Internet. Communication is made easy with the help of Internet and multimedia. The information can be shared by anyone and can be accessed from different parts of the world immediately and easily, one of the most important thing to be kept in mind is the proper transmission of information. Cyber theft is increasing and different ways to hack and crack the digital systems are made, so there is a need for encryption and decryption techniques to properly transmit data from transmitter to receiver. In digital Communication, Error Control Coding is the most effective way for encrypting the data for proper transmission.

II. ERROR CONTROL CODING

In the world of computing and communication, an error correction code (ECC) is employed for controlling errors in data over unreliable or noisy communication channels. The main idea is that the sender encodes the message with redundant information within the sort of an ECC. The added codewords allows the receiver to detect a limited number of errors which will occur within the message, and sometimes to correct these errors without the need of retransmission. The American mathematician R. Hamming explored this field within the 1940s and invented the error-correcting code in 1950: the Hamming (7,4) code.

ECC contrasts with error detection there in errors that are encountered are often corrected, not simply detected. The advantage is that a system using ECC doesn't require a reverse channel to request retransmission of data when a mistake occurs. ECC is designed in such a way that it adds redundancy to the transmitted information using an algorithm. A redundant bit could also be a mixed function of the many original information bits.

ECC is generally classified into two categories: Block codes and Convolutional codes.

Block codes work on fixed-size blocks (packets) of bits or symbols of predetermined size. Practical block codes can generally be hard-decoded in polynomial time to their block length.

Convolutional codes work on bit or symbol streams of arbitrary length. They are most frequently soft decoded with the Viterbi algorithm, though other algorithms are sometimes used.

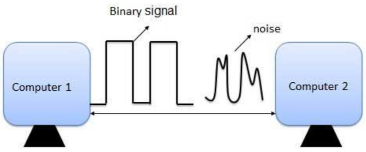


Fig.: Introduction of noise during transmission

III. LINEAR BLOCK CODING

Linear block code is a type of error-correcting code in which the actual information bits are linearly combined with the parity check bits so as to generate a linear codeword that is transmitted through the channel.

Each block of k-message bits is encoded into a block of n-bits (n>k) as shown. The check bits are derived from the message bits and are added to them.

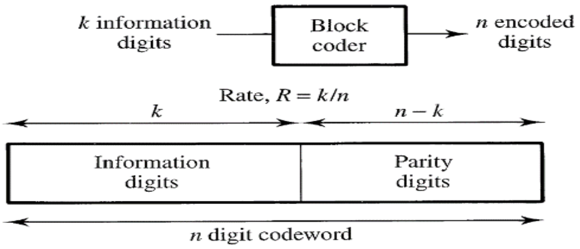


Fig.: Linear Block Coding Technique

IV. HAMMING CODE

Hamming codes comes under linear error-correcting codes. Hamming codes can detect one-bit and two-bit errors, or correct one-bit errors without detection of uncorrected errors. Hamming codes are perfect codes, that is, they achieve the highest possible rate for codes with their block length and minimum distance of three. Richard W. Hamming invented Hamming codes in 1950 as a way of automatically correcting errors introduced by punched card readers. In his original paper, Hamming elaborated his general idea, but specifically focused on the Hamming (7,4) code which adds three parity bits to four bits of data.

4.1 Encoding procedure:

In linear block code, the first k bits of the codeword are the message bits i.e.

$$C_{k+1} = P_{1,1}.d_1 \oplus P_{2,1}d_2 \quad ... \oplus P_{k,1}.d_k$$

$$C_{k+2} = P_{1,2}.d_1 \oplus P_{2,2}d_2 \quad ... \oplus P_{k,2}.d_k$$

$$Cn = P_{1,n\text{-}k}.d_1 \oplus P_{2,n\text{-}k}d_2 \quad ... \oplus P_{k,n\text{-}k}.d_k$$

Fig. Formula for codewords generation

Let the Generator Matrix be ‘G’. It has two sub matrices namely, Identity Matrix (I_k) & Parity matrix (P_k). When some data is multiplied with the identity matrix then same data is obtained, hence the name given is Identity Matrix. Parity matrix is used to derive the parity bits in the codeword.

$$G = \left[\; \underbrace{\begin{matrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{matrix}}_{\substack{\text{Identity matrix}\\(\mathrm{I_k})}} \;\vdots\; \underbrace{\begin{matrix}1&1&0\\0&1&1\\1&0&1\\1&1&1\end{matrix}}_{\substack{\text{Parity Matrix}\\(\mathrm{P})}} \;\right]$$

Fig. Generator Matrix in Terms of Identity Matrix and Parity Matrix

Therefore, Codeword C can be calculated by,

$$C = D * G$$

Where C – Codeword
D - Data word
& G - Generator matrix

Let’s take D= [0101]

then

$$C = [0101] * G$$

taking in terms of matrix,

$$C= [\ 0\ 1\ 0\ 1] * \left[\begin{array}{cccc:ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

Solving, we get

$$C = 0\ 1\ 0\ 1\ 1\ 0\ 0$$

Similarly, we can generate for other possible data words.

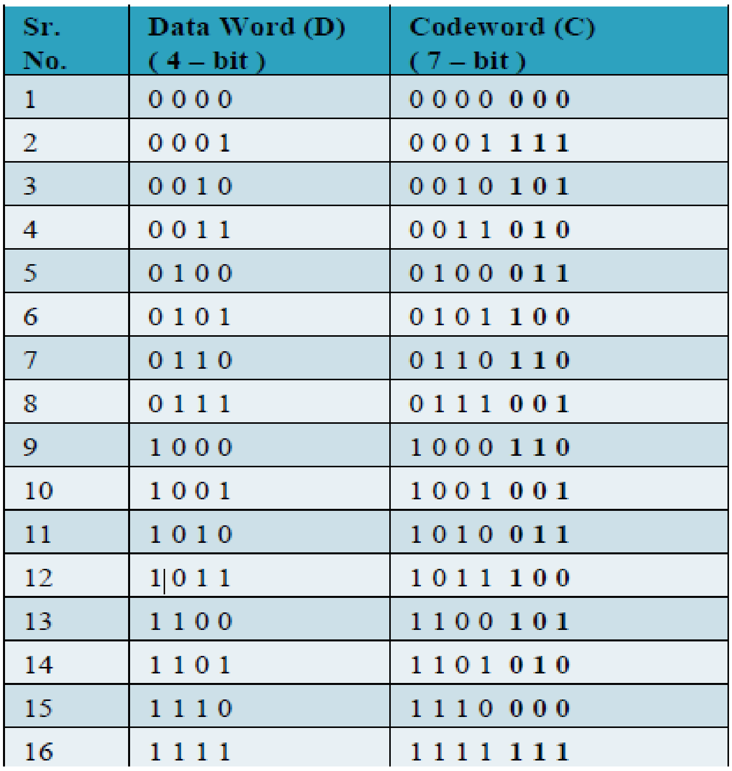
Possible data words given by the formula

$$\text{Possible data words} = 2^k$$

Where k = No. of bits

As we are taking 4 bits,

$$\text{Possible data words} = 2^k = 2^4 = 16$$



Sr. No.	Data Word (D) (4 – bit)	Codeword (C) (7 – bit)
1	0 0 0 0	0 0 0 0 **0 0 0**
2	0 0 0 1	0 0 0 1 **1 1 1**
3	0 0 1 0	0 0 1 0 **1 0 1**
4	0 0 1 1	0 0 1 1 **0 1 0**
5	0 1 0 0	0 1 0 0 **0 1 1**
6	0 1 0 1	0 1 0 1 **1 0 0**
7	0 1 1 0	0 1 1 0 **1 1 0**
8	0 1 1 1	0 1 1 1 **0 0 1**
9	1 0 0 0	1 0 0 0 **1 1 0**
10	1 0 0 1	1 0 0 1 **0 0 1**
11	1 0 1 0	1 0 1 0 **0 1 1**
12	1|0 1 1	1 0 1 1 **1 0 0**
13	1 1 0 0	1 1 0 0 **1 0 1**
14	1 1 0 1	1 1 0 1 **0 1 0**
15	1 1 1 0	1 1 1 0 **0 0 0**
16	1 1 1 1	1 1 1 1 **1 1 1**

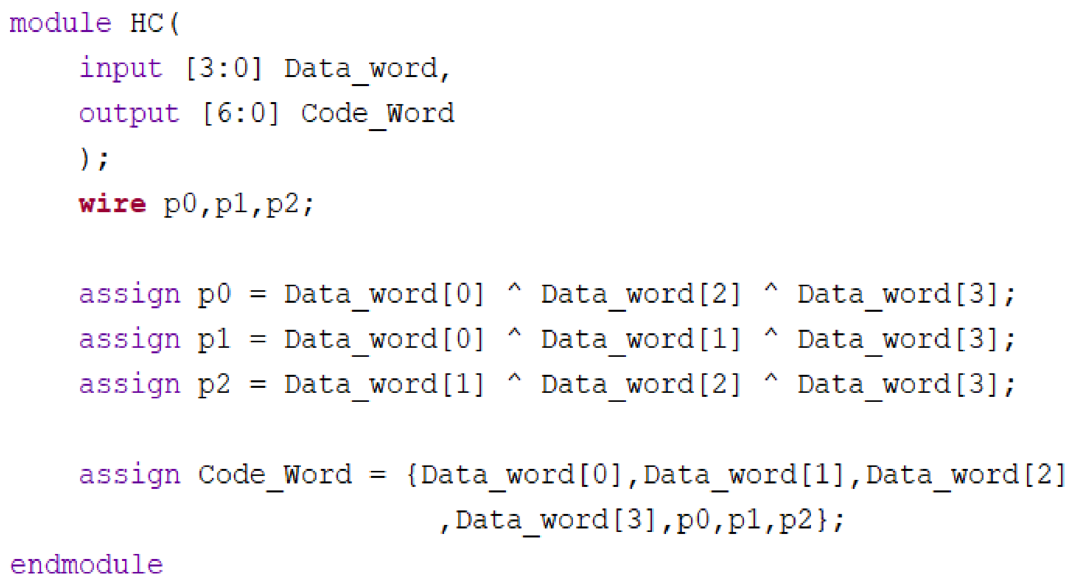
Fig. Possible data words and Codewords for the given parity

V. HARDWARE IMPLEMENTATION

Modelling the circuit to generate codewords in Verilog HDL.
Tool Used – Xilinx Vivado Design Suite (2021.2 Edition)

5.1 Verilog Code

The circuit is designed using Hardware Description Language – Verilog.



```
module HC(
    input [3:0] Data_word,
    output [6:0] Code_Word
    );
    wire p0,p1,p2;

    assign p0 = Data_word[0] ^ Data_word[2] ^ Data_word[3];
    assign p1 = Data_word[0] ^ Data_word[1] ^ Data_word[3];
    assign p2 = Data_word[1] ^ Data_word[2] ^ Data_word[3];

    assign Code_Word = {Data_word[0],Data_word[1],Data_word[2]
                         ,Data_word[3],p0,p1,p2};
endmodule
```

Fig. Verilog Code

5.2 Circuit Diagram (RTL Schematic)

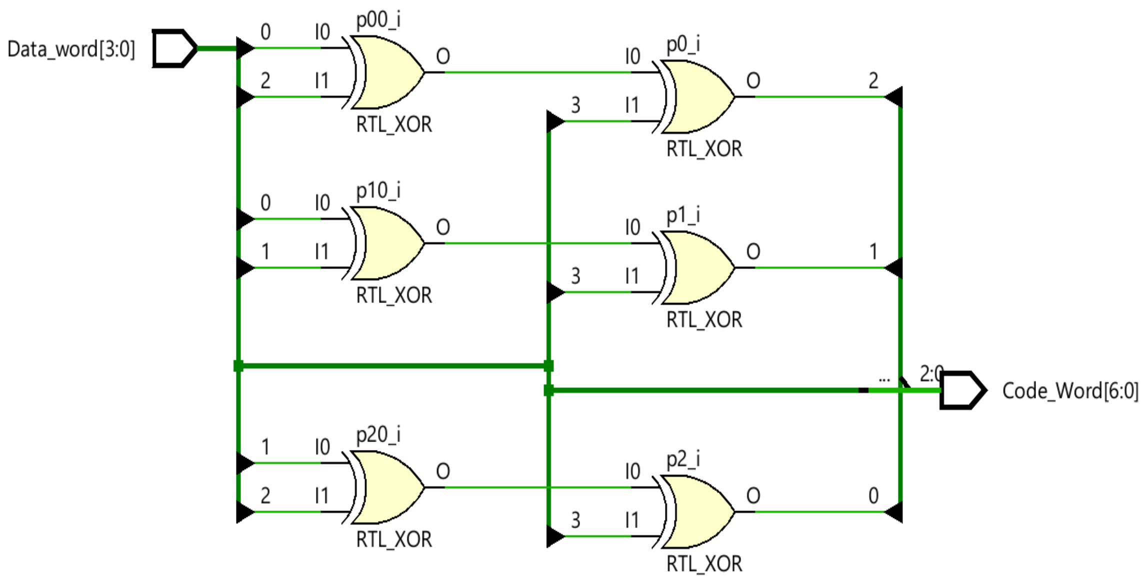


Fig. Circuit Diagram

5.3 Waveform

The codewords that are generated by simulating the Verilog code can be seen in the waveform below.

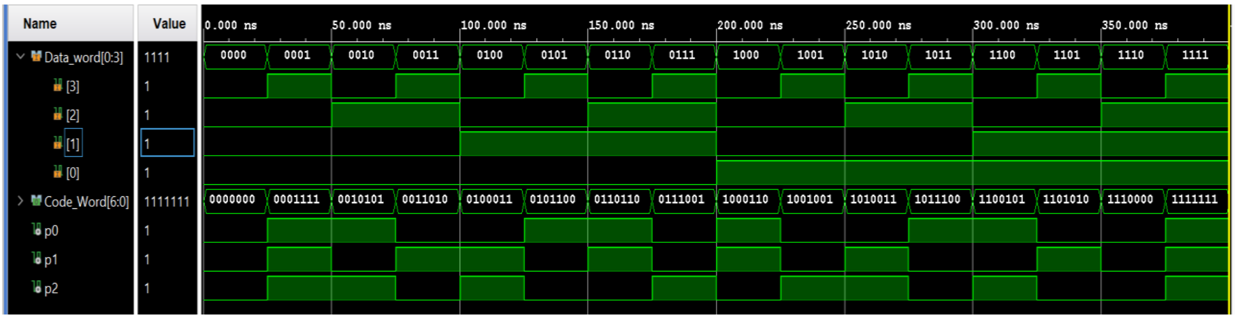


Fig. Waveform representing codeword generation

VI. CONCLUSION

Thus, codewords can be generated using the linear block code method which is then transmitted so that the encrypted information is safe and can be decoded at the receiver side. The main advantage of this method is that we do not need to retransmit the information if error is detected. This method will automatically correct the error. The future-work should provide insights into design of complete Circuit used for detecting and correcting errors.

REFERENCES

[1]. Ambadas balu shinde, "Implementation of linear block code for Digital Communication System using Configurable FPGA" Conference paper–January 2010. PVP Institute of Technology India.

[2]. R. W. Hamming. "Error detecting and error correcting codes" Bell System technical journal, vol. 29, no. 2, pp. 147–160, 1950.

[3]. A. Mazumdar and A. S. Rawat On "Adversarial Joint Source Channel Coding". Information Theory Proceedings (ISIT), 2015 IEEE International Symposium on. IEEE, 2015.

[4]. Arash Ahmadpour and A. Ahadpour Shal (2009) "A Novel formulation of hamming code" Conference Paper. Conference ID: ECTI-CON 2009.