Study of Designing of Cyclic Redundancy Check Generator

Kaluram Makwana[1], Prof. Madhvi Singh Bhanwar[2]
[1, 2] Dept of Electronics & Communication Engineering
[1, 2] SAGE University Indore

Abstract- *In an advanced transmission system, an error occurred when a bit is adjusts in the middle of transmission and gathering in a channel. A binary 1 is moved and a binary 0 is gotten or a binary 0 is moved and a binary 1 is gotten. Cyclic Redundancy Check is the most important method to detect the errors occurred during transmission of any data. Errors transpired in communication due to internal and external factors i.e. due to components, link, design, noise and interference etc. This work is focused on study of encoder and decoder of CRC.*

Keywords- CRC, Error detection, Communication, VLSI.

I. INTRODUCTION

In an advanced transmission system, an error occurred when a bit is adjusts in the middle of transmission and gathering in a channel. A binary 1 is moved and a binary 0 is gotten or a binary 0 is moved and a binary 1 is gotten. There are two kinds of errors that can happen: single-bit error and burst error [1]. A single bit error is a sequestered error that changes one bit however do not trouble neighboring bits. A burst error is an error in a bordering sequence of B bits in which the first and last bits and any number of halfway bits are gotten in error.

A single-bit error can arise in the occurrence of white noise, due to a slight arbitrary worsening of the signal-to-noise ratio, which is adequate to complicate the receiver's conclusion of a single bit. Spurt errors can be initiated by impulse noise or waning in a mobile wireless background and are more common and more problematic to contract with. The effects of rupture errors are larger at complex data rates. Bit errors occur in digital communication schemes due to inherent or extrinsic factors [2]. Intrinsic errors are due to the constituents, design and application of a link. They are produced due to internal noise causes, poor electrical influences, and sometimes receiver sampler error. In optical contacts the errors occur mainly because of the bodily components such as optical drives, optical receiver, connectors, optical fiber, etc. Errors are also caused due to optical attenuation and optical dispersion. CRCs have a long history of use for error detection in computing [3]. Error correction codes deliver a means to identify and correct errors presented by a transmission network.

Common Cyclic Redundancy Check polynomials are able to notice following types of errors:

a. Single bit error,
b. Double bit errors
c. All odd number of errors having sufficient constraint length
d. Any burst error for which the burst length is less than the polynomial length
e. Large burst errors [4].

Network models are structured into layers, with each layer representing a specific networking function. These functions are controlled by protocols, which are rules that govern end-to-end communication between devices. The Open Systems Interconnection (OSI) model was developed by the International Organization for Standardization (ISO), and formalized in 1984. It provided the first framework governing how information should be sent across a network. It gives a platform for a common technical language and has led to the standardization of communications protocols and the functions of a protocol layer. The structure and functions of the OSI architecture is given in the Figure 1 [3].

Layer	Function	Example
Application (7)	Services that are used with end user applications	SMTP,
Presentation (6)	Formats the data so that it can be viewed by the user Encrypt and decrypt	JPG, GIF, HTTPS, SSL, TLS
Session (5)	Establishes/ends connections between two hosts	NetBIOS, PPTP
Transport (4)	Responsible for the transport protocol and error handling	TCP, UDP
Network (3)	Reads the IP address form the packet.	Routers, Layer 3 Switches
Data Link (2)	Reads the MAC address from the data packet	Switches
Physical (1)	Send data on to the physical wire.	Hubs, NICS, Cable

Figure 1 OSI model & its function

II. CODING THEORY

Coding theory is a branch of mathematics and computer science dealing with the error prone process of transmitting data across noisy channels, via clever means, so that a large number of errors that occur can be corrected. It also deals with the properties of codes, and thus with their fitness for a specific application. There are two classes of codes.

1) Source coding (Data compression).
2) Channel coding (Forward error correction).

A cyclic redundancy check (CRC) is a type of hash function, which is used to produce a small, fixed-size checksum of a larger block of data, such as a packet of network traffic or a computer file. The checksum is used to detect errors after transmission or storage. A CRC is computed and appended before transmission or storage, and verified afterwards by the recipient to confirm that no changes occurred in transit. CRCs are popular because they are simple to implement in binary hardware, are easy to analyze mathematically, and are particularly good at detecting common errors caused by noise in transmission channels.

Cyclic Counter Cyclic Redundancy Check (CRC) is an error detecting technique in which a transferred message is attached with a few redundant bits from the sender and then the codeword is plaid at the receiver using modulo-2 arithmetic for errors. The message is then communicated from the encoder and is received by the receiver where a CRC check is conceded out. This procedure supports to regulate any errors in communication over the channel [4]. The assortment of producer polynomial is the most important part of implementing the CRC algorithm. The polynomial essential be chosen to maximize the error-detecting capabilities while minimizing overall collision probabilities. CRC is divided into the following types [4]:

Table 2.1: Standard CRC and their polynomials

S.No.	CRC	Polynomial	Application
1	CRC4	x^4+x^3+1	Telephone
2	CRC8	x^8+x^2+x+1	ATM header
3	CRC8 CCIT	$x^8+x^7+x^2+x+1$	1 wire bus
4	CRC10	$x^{10}+x^9+x^5+x^4+x+1$	ATM AAL
5	CRC16	$x^{16}+x^{15}+x^2+1$	HDLC/USB
6	CRC16 CCIT	$x^{16}+x^{15}+x^5+1$	X.25/Modem
7	CRC32	$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+1$	Ethernet

A CRC "checksum" is the remainder of a binary division with no bit carry (XOR used instead of subtraction), of the message bit stream, by a predefined (short) bit stream of length n + 1, which represents the coefficients of a polynomial with degree n. Before the division, n zeros are appended to the message stream. CRCs are based on division in the ring of polynomials over the finite field GF (2) (the integers modulo. In simpler terms, this is the set of polynomials where each coefficient is either zero or one (a single binary bit), and arithmetic operations wrap around.

A polynomial termed generator polynomial must be designated before the user calculates the CRC of a transferred message. The generator polynomial must have a degree greater than zero and a non-zero coefficient in the MSB and LSB positions.

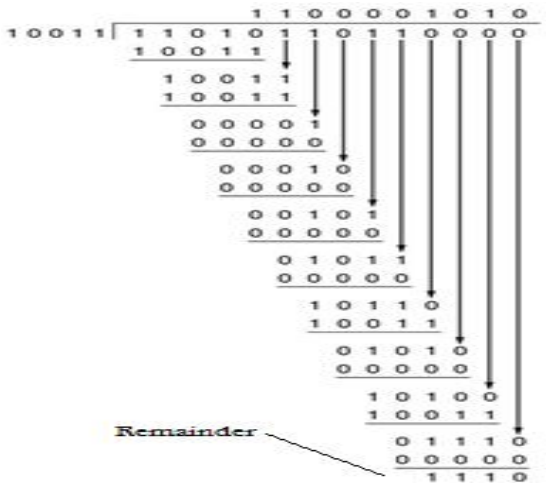

Figure 2: Division in CRC

III. LITERATURE REVIEW

Saleh et. al. [5], describes that cyclic redundancy check is the technique which is efficient error detection method is used to detect single and burst errors. It adds redundancy bits to the original data. The redundancy bit represents the remainder of division between the original message and the selected polynomial. This paper shows the implementation of CRC8 encoder and decoder.

P Aparna Anand et. al. [6], describes the design and development of modified CRC algorithm for the hardware implementation on FPGA to meet the speed constraint for Ethernet, using the reduced lookup table algorithm. This algorithm can be applied for any length of data, by processing it in a block of 16 bytes at a time. The last block may have less than 16 bytes. To process an input block of 16 bytes, the algorithm first forms an optimized table of pre-calculated CRC. Corresponding to the input data, lookup from this table

is done and the results from the table lookup are combined by XOR operations to form the final CRC of the input data.

Christopher E. Kennedy et. al. [8], said that cyclic redundancy check (CRC) is a popular error detection code (EDC) used in many digital transmission and storage protocols. Most existing digit-serial hardware CRC computation architectures are based on one of the two well known bit-serial CRC linear feedback shift register (LFSR) architectures. In this paper, we present and investigate a generalized CRC formulation that incorporates negative degree terms.

Jubin Mitra et. al. [9], describes CRC (Cyclic Redundancy Check) is a simple and an elegant method for error detection. It finds application in most of the high-speed data communication protocol. In High Energy Physics experiment often CRC is used for control and data frame communication with detectors placed at radiation zone. Reliability of CRC error detection capability alters with generator polynomial chosen. The most popular choice is to use a 32-bit checksum.

IV. PROPOSED DESIGN

The Generator Polynomial used for 8 bit CRC calculation is $x^8 + x^7 + x^6 + x^4 + x^2 + 1$ used in DVS-S2 (Digital Video Broadcasting – Satellite Second Generation). In this paper, we will be referring to the polynomial defined in DVS-S2 but results can be extended to any polynomial. For implementation, we have used VHDL (VHSIC HDL) i.e. Very High Speed Integrated Circuit Hardware Description Language which describes the method for modelling and designing of Digital Circuits and Digital logic systems.

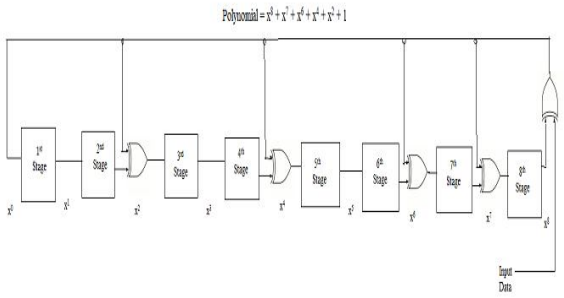

Figure 3: Hardware implementation of 8 bit CRC

Division operation of CRC is modulo-2 operation. The divider circuit of CRC consists of shift registers and mod-2 adders. Figure 3 shows the hardware implementation of 8-bit CRC using $x^8 + x^7 + x^6 + x^4 + x^2 + 1$ polynomial which consist of eight stages and five EX-OR gates.

Implementation of Encoder Algorithm

a. Read the message vector.
b. Take the generator polynomial order ‘k’.
c. Shift the message vector ‘k’ times and store it order as ‘n’. Compute (n-k).
d. Shift generator polynomial (n-k) times and store the result ‘h’.
e. XOR the generator polynomial and message vector and store the result in ‘x’.
f. Determine the highest polynomial index position of ‘x’ where 1 is occurred and take it as ‘n’.
g. If n >=k go to step 4.
h. Concatenate the check bits with the message bits.

Implementation of Checker Algorithm

a. Read the received data and take its order as ‘n’ and store it in ‘h’.
b. Take the order of generator polynomial as ‘k’. Compute (n-k).
c. Shift the generator polynomial left (n-k) times and store the result in ‘e’.
d. XOR the generator polynomial and received vector and store the results in ‘x’.
e. Determine the highest index of ‘x’ where 1 is occurred and take it as a ‘n’.
f. If n >= k go to step 3.
g. Store ‘x’ in rem.
h. If rem =0 then the received data is error free else data contains error.

V. CONCLUSION

On the basis of study of various literatures and implementation of CRC encoder and decoder, we summaries as: Reversible logics can be used in implementation which reduces delay and logic gate used. Adiabatic technique can be used.

REFERENCES

[1] T Stallings, William, "Data and computer communications", Upper Saddle River, N.J.: Pearson/Prentice Hall, 8th Edition, 2007.
[2] Palani Subbaiah, "Bit- Error Rate for High Speed Serial Data Communication", Data-communications Division, Cypress Semiconductor, November 2008.
[3] Peterson, W. & E. Weldon, "Error-Correcting Codes", Second Edition, MIT Press, 1972.
[4] Ulf Nordqvist, Thesis: "Protocol Processing in Network Terminals", Department of Electrical Engineering,

Linkopings University, SE-581 83 Linkoping, Sweden 2004.

[5] A. H. Saleh, K. M. Saleh and S. Al-Azawi, "Design and simulation of CRC encoder and decoder using VHDL," 2018 1st International Scientific Conference of Engineering Sciences - 3rd Scientific Conference of Engineering Science (ISCES), IEEE 2018, pp. 221-225.

[6] Bajarangbali P., Aparna Anand, "Design of High Speed CRC Algorithm for Ethernet on FPGA using reduced lookup table algorithm", IEEE Annual India Conference (INDICON) 2016

[7] Zavodnik, T; Kekely, L.; and Pus, V., "CRC based hashing in FPGA using DSP blocks," in Design and Diagnostics of Electronic Circuits & Systems, 17th International Symposium on , vol., no., pp.179-182, 23-25 April 2014

[8] Christopher E. Kennedy and Mehran Mozaffari-Kermani,"Generalized Parallel CRC Computation on FPGA", Proceeding of the IEEE 28th Canadian Conference on Electrical and Computer Engineering Halifax, Canada, May 3-6, 2015

[9] Jubin Mitra and Tapan K. Nayak, "Reconfigurable Concurrent VLSI (FPGA) Design Architecture of CRC-32 for high-speed data communication", 2015 IEEE International Symposium on Nanoelectronic and Information Systems