Design and Simulation of Extended Golay Code on FPGA for Long Distance Applications – A Review

Mukta Thankachan
P. G. Scholar, Department of Electronics and Communication
RKDF-IST, Hoshangabad Road, Bhopal, India
thankachan.mukta@gmail.com

Bhagwat Kakde[2], Manish Jain[3]
[2] Assistant Professor, [3] Head of Department, Department of Electronics and Communication
RKDF-IST, Hoshangabad Road, Bhopal, India
[2]bhagwatkakde@yahoo.co.in, [3]manishj.mitece@gmail.com

Abstract— FPGA is a portable and very powerful device to efficiently implementation the logic. This paper presents a general idea to provide security when data is on channels there is a possibility that it can be affected by some malicious function. To avoid this condition some encoding schemes were used like Hamming code, block code, Turbo codes, CRC-cyclic redundancy check-based etc. This paper presents a review on number of scholars work and coding scheme introduced in those papers is binary Golay code (G_{23}) and extended binary Golay (G_{24}).These codes were used for the fulfillment of required high speed with low-latency, higher security and less complexity architecture. The main purpose of this paper is to introduce a new scheme in future that can be implemented on FPGA using both binary Golay code (G_{23}) and extended binary Golay (G_{24}).

Keywords - FPGA, syndrome, error pattern, Golay code, Extended Golay code, Encoding, Decoding, Hardware optimization.

I. INTRODUCTION (HEADING 1)

Hashing is a technique that is used in information retrieval since it requires a linear time of complexity in most cases. One of the most important characteristics of the hash searching techniques is the hash function. Several hash functions are being used widely in order to achieve the required performance, storage reduction and simplicity. Most of the functions are simple mathematical ones; such as the modulus. In this paper we suggest a new function to be used in the Hash searching techniques. The function is based on the decode operation of the famous Golay code (24, 12, 8) error detection and correction technique, which also known as extended Golay code. We aim at studying the performance characteristics along with the search capabilities of the proposed design. Hash searching techniques are widely used in information retrieval, especially when the searched key is known exactly as it is stored. However, there are situations where only partial information of the object is available. Therefore, approximate matching algorithms should be implemented.This paper presents an overview of different research work which describe different application of golay and plan to work on Extended golay code to implement it on FPGA for a new technique hash searching, in which we define a new hash function that is based on the decode operation of Golay code (24, 12, 8).

II. GOLAY CODE

GOLAY code technique based encoder and decoder using CRC methodology. This work is to increase the secure level and to optimize the circuit complexity. Golay system is used to modify the encoder and decoder data bits structure level and to add the message bit, key bit and to apply the these bits into GOLAY binary code technique. This technique is to apply the majority gate analysis process and to get the final majority output bit and to add the any location in encoder architecture output data bits. To fight this problem, a hardware module programmed to yield a Golay encoded codeword may be used. Golay decoder is used extensively in communication links for forward error correction. Therefore, a high speed and high throughput hardware for decoder could be useful in communication links for forward error correction. Literature surveys were conducted, which deal with encoding methods for Golay code, but these are not suitable for hardware implementation due to complexity the algorithms. The equations are then used to implement a data flow representation of the CRC circuit in VHDL.

Recently, parallelism in the CRC calculation becomes popular, and typically one byte or multiple bytes can be processed in parallel. A common method used to achieve parallelism is to unroll the serial implementation. Unfortunately, the algorithms used for parallelism increase the length of the worst case timing path, which falls short of ideal speedups in practice. Furthermore, the required area and power consumption increases with the

higher degree of parallelism. Therefore, we seek an alternative way to implement CRC hardware to speed up the CRC calculation while maintaining the area and power consumption requirements at a reasonable level.

One of the best possible ways to present the coder and decoder and a new approach to remove the errors is use Golay code to encrypt the data the central idea of using this code is to restrained the amount of errors as much as possible. For that addition of the redundancy bits to the messages is one of the best idea through which facilitate to find out or correct the errors that may have occurred. This paper proposed a specific type of error-correcting codes, Golay codes (23) and the extended Golay code (G24). Three steps to transfer the information, a channel transmit, and a receiver. At the time of transmission the information is changed to noise so to avoid this condition use error correction codes.

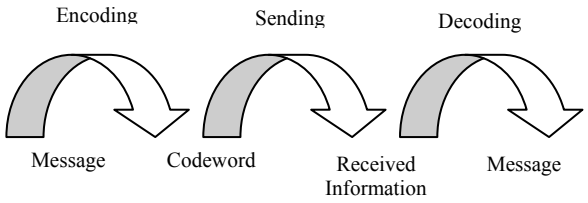

Figure. 1 message is encoded into a codeword

Fig. 1 show that a message is encoded into a codeword, it is sent to the receiver through a channel, in this channel the opportunity exists that errors occur, and the receiver tries to obtain the original message by decoding the word. The transmission of message depends on what we have received and what is send. Some important properties that give a detailed description of the extended Golay are described as follows:

1) First property shows that a message m of length k out of some finite field F generates sequence of k symbols, so m = (m1: mk) belongs to F^k. Then an n-code Cover a finite field F is a set of vectors in F^n, where $n \leq k$. Since we will be commerce with a binary code only, we will assume codes are binary from now on.
2) Second property says that the error of p probability occurs only when 0 is received when 1 was sent, or 1 is received when 0 was sent.
3) Third property says that the function F^n is a non-zero elements and hamming weight of a vector belongs to that function.
4) Fourth property says that the humming distance of two vectors belongs to a function F^n is the number of place where they differ. The idea is that an n-code C is a strict subset of F^n in which we want the Hamming distance between any two vectors to be as large as possible. Therefore, the minimum Hamming distance is an important characteristic of the code.
5) Fifth property says that the minimum Hamming distance d of a code C is defined as d = min {dist(x, y) I x, y belongs to C} where c is the code.

The first section presents an introduction about the problem occurrence at the time of transmission and the reason why this occur and how we can resolve it to achieve high performance system. The second section is the literature review that presents the work or other scholars. Third section is conclusion and forth is Acknowledgment the last section is about the reference paper.

III. LITRATURE REVIEW

Reference [1] is an IEEE Transaction paper which presents an efficient hardware implementation of encoder and decoder for both prototype binary Golay code (G23), extended binary Golay code (G24) based on CRC (Cyclic Redundancy Check) encoding scheme.Virtex-4 FPGA is used to design high speed with low latency architecture. This proposed method has various applications in the field of high speed communication links, photo spectroscopy, and ultrasonography. Reference [2] is a paper written by Mr. Golay himself. This paper proposed lossless binary coding scheme to assure the reception of the correct data. To overcome the problem of power loss which is introduced by ternary coding scheme, a 23 binary symbols is used which yields the power saving one and a half db for omitting probability of errors and this code is called Golay code. And another code is also introduced by him called extended Golay code Literature power saving up to 3 db. Reference [3] proposed a simplified soft decoding algorithm to correct up to four errors for extended binary Golay code .The results obtained by this method shows the less complex calculation were required with this method and also work on the efficiency hardware implementation on FPGA platform. And presents the detailed architecture of soft decoder and the results is also compared with the other algorithms in terms of power gain, cost, and hardware complexity. Reference [4] presents overview on Golay Complementary Sequence. These sequences are introduced by Marcel Golay in the perspective of infrared spectrometry and also give the properties and applications in different fields. Reference [5] proposed symbol –by –symbol soft in/ soft out APP decoding

algorithm for the Golay code. This decoding algorithm is suitable for convolution codes and block code with simple trellis structure.

Reference [6] this paper presents the outperformance of the extended Golay code under the hard decision decoding. And compare the performance of the binary Golay code and extended binary Golay code under the ML (maximum likelihood) conditions. Reference [7] proposed an error correction Golay code for clustering tremendous amount of Big data Streams by using error correction Golay codes and this approach is used in the field where the requirement to accumulate multidimensional data. Reference [8] presents the overview about the Golay codes and their properties. (G11) is ternary Golay code and (G23) binary cyclic code. Reference [9] proposed an efficient soft-decision decoder of the (23, 12, 7) binary Golay code up to the four errors and almost all patterns of three errors and all fewer random error can be corrected with the help of proposed algorithm. Reference [10] presents GF (2m) Galois field encoder & decoder and its verification on FPGA using the NIST chosen irreducible polynomial. Software used to do this is Xilinx Model Sim 10.0 that simulated complete verification of multiplication and implemented on FPGA. The paper presents simple circuit and performs high speed operation by increases security during communication dialogue and decreasing the number of logic gates figure 2 explains the Galois field with the help of flow chart. The flowchart of Galois field algorithm describes the encoding technique using the shift and adds method.

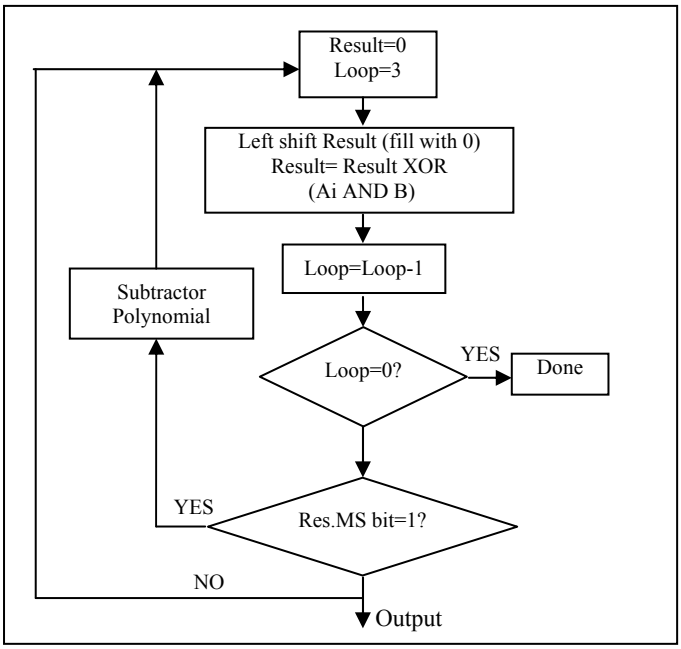

Figure.2 Algorithm for GF (2m) Multiplication

Reference [11] proposed a methodology of constructing a sequence of phase-coded waveform for which ambiguity function is free of ranges side lobes along doper shift. The problem arises with Golay code is that it has ideal ambiguity along zero Doppler-axis but are sensitive to nonzero Doppler shifts. And the application of pulse coded waveform is in the area or communication using radar. Reference [12] proposed an algorithm for the hardware implementation of (24, 12, 8) Golay code in FPGA (Field programmable gate array) based system. To remove the complexity of arithmetic operations this arises in the existing algorithm. The proposed algorithm chooses the absolute value rather than bit error probability to obtained better results as compared to the existing algorithms. Reference [13] proposed block product turbo code (BPTC) and simulated its efficiency. The proposed method used hamming (15, 11) and hamming (13,9) block channel code in combination to construct a BPSK modulation .This combination gives better results and robust against BPSK Golay code and MSK Golay. Application of the proposed algorithm is in the wireless communication system. Reference [14] proposed a method to construct the binary Golay code (24, 12, 8) by using two array codes involving four component codes. Two of them are simple linear block codes and other two are symmetric code and its extended version. Reference [15] proposes a new algorithm to fulfill the requirement of faster decoding for the Go set Lattice, Golay code and Leech Lattice. The proposed design introduced two approaches to first when charge in of length n and taking soft decoding algorithm at an arbitrary point R^n in to the nearest code word and second a decoding algorithm for a lattice A in R^n changes an arbitral point of R^n into a closest lattice point.

In Reference [16] the proposed methodology fulfill the requirement reducing the peak to average ratio (PTAR) with the help of special Fractional Fourier Transform (FRFT) followed to the low complicity Golay sequence coder in order to provide optimal de-correlation between signal and noise. To achieve the requirement

of low complexity, low bit error rate and peak to average power ratio. Reference [17] proposed a new scheme which is reversing of the conventional Golay code (24, 12, 8) which maps 24- bit vector into 12 bits message words. In this approach each object is represented by 24 bit vector at the same time we consider 1 bit probability distortion through bit modification. Consequently, this work proposed a hash table of 4096 entries that is fault-tolerant. This allows organizing a direct retrieval of a neighborhood of 24-bit vectors with two or possibly more mismatches. A retrieval capability of the proposed system and the expected hash distribution is obtained by the simulation experiments. Reference [18] proposed a new algorithm to decode the binary systematic (23, 12, 7) and (14, 21, 9) QR codes. The proposed algorithm by using lookup table directly determines the error locations without the operation of multiplication over a finite field. The reason of using the FLTD is the CPU time is half of the LTD algorithm. In terms of both speed and memory requirement in real time system FLTD algorithm is better approach as compare to the existing ones.

IV. CONCLUSION

This paper presents a review on diverse research work presented in the field of FPGA based speed optimization single and bust error reduction etc. Different encoding and decoding methods were introduced in the reference papers to control the errors and for speed optimization. Here, the main aim is to present systems which remove the complexity of system to accomplishment the requirement of low latency data and high speed application. So that a new scheme is proposed in future for FPGA using both binary Golay code (G_{23}) and extended binary Golay (G_{24}).

REFERENCES

[1] Satyabrata Sarangi and Swapna Banerjee, "Efficient Hardware Implementation of Encoder and Decoder for Golay Code", IEEE Transaction on very large scale Integration (VLSI) system, Vol.23 Issue No.9, pg.1965-1968, September 2015.

[2] Marcel J.E.Golay, "Notes on Digital Coding", Reprinted from proc. IRE, Vol.37, pg-657 June 1949.

[3] DongfuXie, "Simplified algorithm and hardware implementation for the (24,12,8) Extended Golay soft Decoder up to 4 Errors", The International Arab Journal of Information Technology, Vol.11 No.2, pg.111-115, March 2014.

[4] Matthew G. Parker, Kenneth G. Paterson and Chintha Tellambura, "Golay Complementary Sequences", January 2004.

[5] Li Ping and Kwan L. Yeung, "Symbol-by-Symbol APP Decoding of the Golay Code and Iterative Decoding of Concatenated Golay Codes", IEEE Transaction on Information theory, Vol.45, No.7, pg.2558-2562, November 1999.

[6] Jon Hamkins, "The Golay Code Outperforms the Extended Golay Code", IEEE Transactions on Information Theory, February 19, 2016.

[7] Faisal Alsaby, Kholood Alnoo waiser and Simon Berkovich, "Golay code Transformation for ensemble clustering in application of medical Diagnostics", International Journal of Advanced Computer Science and Applications (IJACSA), Vol.6 No.1, pg.49-53, 2015.

[8] Mario de Boer and Ruud Pellikaan, "The Golay codes" Springer, pg.338-347, September 1995.

[9] Wen-Ku Su, Pei-Yu Shih, Tsung-Ching Lin and Trieu-Kien Truong, "Soft-decoding of the (23, 12, 7) Binary Golay" International Multi Conference of Engineers and Computer Scientists Vol. 2, PP- 19-21 March, 2008.

[10] Dr. Ravi Shankar Mishra, Prof PuranGour and Mohd. Abdullah, "Design and Implementation of 4 bits Galois Encoder and Decoder in FPGA", International Journal of Engineering Science and Technology (IJEST), Vol.3 No.7, pg.5724-5732, July 2011.

[11] Ali Pezeshki, A. Robert Calderbank, William Moran and Stephen D. Howard, "Doppler Resilient Golay Complementary Waveforms", IEEE Transaction on Information Theory, Vol. 54, No. 9, September 2008.

[12] John H. Conway and N. J. A. Slpane, "Soft Decoding Techniques for Codes and Lattices, Including the Golay Code and the Leech Lattice, Including the Golay Codeand the Leech Lattice", IEEE Transaction on Information Theory, PP-41-51Vol.32, NO. 1, January 1986.

[13] Yihua Chen, Juehsuan Hsiao, PangFu Liu and Kunfeng Lin, "Simulation and Implementation of BPSK BPTC of MSK Golay code in DSP chip", Communications in Information Science and Management Engineering, Vol.1 No.4, pp.46-54, Nov.2011.

[14] Xiao-Hong Peng and Paddy G. Farrell, "On Construction of the (24, 12, 8) Golay Codes", December 2005.

[15] A.Iniya Mary and , N.A. Pappathi, "Simplified Algorithm and Hardware Implementation for A VLSI Implementation of Data transmission Error Detection Based Encoder And Decoder" International Conference on Current Research in Engineering Science and Technology, Vol. 11, No. 2, PP-11-13 March 2014.

[16] Eyas El-Qawasmeh, Maytham Safar and TalalKanan, "Investigation of Golay code (24, 12, 8) Structure in improving search techniques",The International Arab Journal of Information Technology, Vol.8, No.3, pg.265-271, July 2011.

[17] V.Bhushan Kumar and K.Yoga Prasad, "Reduction of PAPR and BER by Using Golay Sequences for OFDM System", International Journal of Emerging Engineering Research and Technology, Vol. 2, Issue 7, PP 191-198, October 2014.

[18] Yan-Haw Chen, Chih-Hua Chine, Chine-Hsiang Huang, Trieu-Kien Truong and Ming-Haw Jing, "Efficient Decoding of schematic (24,12,7) and (41,21,9) Quadric Residue codes", Journal of Information science And Engineering Vol.26, pg.1831-1843, December 2010.