IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 2, February 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 2, February 2022 ||

| DOI:10.15680/IJIRSET.2022.1102031 |

Golay Binary Codes for Error Detection and Correction: A Review

Faisal Jamal[1], Dr. Pramod Patel[2]

Research Scholar, Department of Electronics and Communication, IES College of Technology, Bhopal, India[1]

Associate Professor, Department of Electronics and Communication, IES College of Technology, Bhopal, India [2]

ABSTRACT: Golay Code is a type of Error Correction code discovered and performance very close to Shanon's limit .Good error correcting performance enables reliable communication. Since its discovery by Marcel J.E. Golay there is more research going on for its efficient construction and implementation. The binary Golay code (G23) is represented as (23, 12, 7), while the extended binary Golay code (G24) is as (24, 12, 8). High speed with low-latency architecture has been designed and implemented in Virtex-4 FPGA for Golay encoder without incorporating linear feedback shift register. This brief also presents an optimized and low-complexity decoding architecture for extended binary Golay code (24, 12, 8) based on an incomplete maximum likelihood decoding scheme.

KEYWORDS: Golay Code, Decoder, Encoder, Field Programmable Gate Array (FPGA)

I. INTRODUCTION

Communication system transmits data from source to transmitter through a channel or medium such as wired or wireless. The reliability of received data depends on the channel medium and external noise and this noise creates interference to the signal and introduces errors in transmitted data. Shannon through his coding theorem showed that reliable transmission could be achieved only if data rate is less than that of channel capacity. The theorem shows that a sequence of codes of rate less than the channel capacity have the capability as the code length goes to infinity [1]. Error detection and correction can be achieved by adding redundant symbols to the original data called as error correction and correction codes (ECCs).Without ECCs data need to retransmit if it could detect there is an error in the received data. ECC are also called as for error correction (FEC) as we can correct bits without retransmission. Retransmission adds delay, cost and wastes system throughput. ECCs is really helpful for long distance one way communications such as deep space communication or satellite communication. They also have application in wireless communication and storage devices [2].

Error detection and correction helps in transmitting data in a noisy channel to transmit data without errors. Error detection refers to detect errors if any received by the receiver and correction is to correct errors received by the receiver. Different errors correcting codes are there and can be used depending on the properties of the system and the application in which the error correcting is to be introduced. Generally error correcting codes have been classified into block codes, convolutional codes, LDPC Code and Goley Code [3, 4].

Error-Detecting codes

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if an error occurred during transmission of the message. A simple example of error-detecting code is parity check [5].

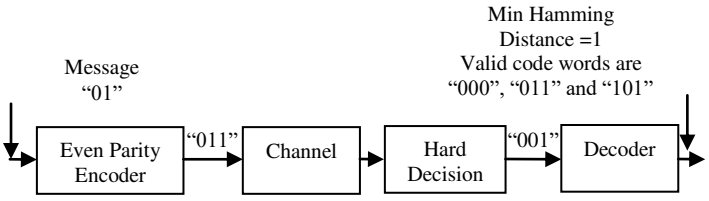

Fig. 1: Block Diagram of Error Detecting Codes

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 2, February 2022 ||

| DOI:10.15680/IJIRSET.2022.1102031 |

Error-Correcting codes:-

Along with error-detecting code, we can also pass some data to figure out the original message from the corrupt message that we received. This type of code is called an error-correcting code. Error-correcting codes also deploy the same strategy as error-detecting codes but additionally, such codes also detect the exact location of the corrupt bit [6].

In error-correcting codes, parity check has a simple way to detect errors along with a sophisticated mechanism to determine the corrupt bit location. Once the corrupt bit is located, its value is reverted (from 0 to 1 or 1 to 0) to get the original message [7].

Voltage levels of the received signal at each sampling instant are shown in the figure. The soft decision block calculates the Euclidean distance between the received signal and the all possible code words [8].

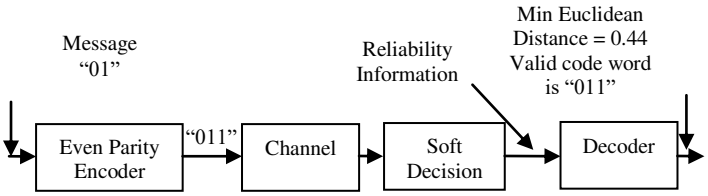

Fig. 2: Block Diagram of Error Correction Code

The minimum Euclidean distance is "0.49" corresponding to "0 1 1" code word (which is what we transmitted). The decoder selects this code word as the output. Even though the parity encoder cannot correct errors, the soft decision scheme helped in recovering the data in this case. This fact delineates the improvement that will be seen when this soft decision scheme is used in combination with forward error correcting (FEC) schemes like convolution codes, Goley Code etc.

II. LITERATURE REVIEW

Kristjane Koleci et al. [1], depicts a productive execution of the iterative decoder that is the primary piece of the unscrambling stage in the LEDAcrypt cryptosystem, as of late proposed for post-quantum cryptography in light of low-thickness equality check (LDPC) codes. The execution we present endeavors the construction of the factors to speed up the disentangling system while keeping the region limited. Specifically, our attention is on the plan of an effective multiplier, the last option being a basic part likewise taking into account considering various upsides of the cryptosystem's boundaries, as it very well may be needed in later applications. We expect to give an engineering reasonable to minimal expense execution on both Field Programmable Gate Array (FPGA) and Application Specific Integrated Circuit (ASIC) executions. Concerning the FPGA, the complete execution time is 0.6 ms on the Artix-7 200 stage, utilizing all things considered 30% of the all out accessible memory, 15% of the absolute accessible Look-up Tables and 3% of the Flip-Flops. The ASIC blend has been performed for both STM FDSOI 28 nm and UMC CMOS 65 nm advancements. After rationale blend with the STM FDSOI 28 nm, the proposed decoder accomplishes a complete inactivity of 0.15 ms and a region control of 0.09 mm 2 . The post-Place&Route execution results for the UMC 65 nm show a complete execution season of 0.3 ms, with an area control of 0.42 mm 2 and a power utilization of at most 10.5 mW.

P. Santini et al. [2], iterative decoders utilized for unraveling low-thickness equality check (LDPC) and moderate-thickness equality check (MDPC) codes are not portrayed by a deterministic deciphering range and their blunder rate execution is generally surveyed through escalated Monte Carlo recreations. In any case, a few applications, similar to code-based cryptography, need ensured low upsides of the blunder rate, which are infeasible to evaluate through recreations, accordingly requiring the advancement of hypothetical models for the mistake pace of these codes. A few models of this sort as of now exist, however become computationally unmanageable for boundaries of commonsense interest. Different methodologies inexact the code gathering conduct through presumptions, which may not remain constant for a particular code. We propose a hypothetical examination of the blunder amendment ability of LDPC and MDPC codes that permits inferring tight limits on the mistake rate at the result of equal piece flipping decoders. Unique consideration is given to the situation of codes with little bigness. Single-cycle disentangling is researched through a thorough methodology, which doesn't need any presumption and results in a dependable blunder remedy capacity for any single code. We show an illustration of use of the new bound to the setting of code-based cryptography, where ensured mistake rates are expected to accomplish solid security levels.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 2, February 2022 ||

| DOI:10.15680/IJIRSET.2022.1102031 |

J. Hu et al. [3], present a lightweight equipment plan for an as of late proposed quantum-safe key embodiment system in view of QC-LDPC codes called LEDAkem, which has been conceded as a cycle 2 contender to the NIST post-quantum normalization project. Existing executions center around fast while not many of them consider region or power productivity, which are especially unequivocal for minimal expense or power compelled IoT applications. The arrangement we propose targets augmenting the measurement of region proficiency by pivoting the QC-LDPC code portrayals among the square RAMs in digit level. In addition, upgraded parallelized processing strategies, languid gathering and square parcel are taken advantage of to work on key decapsulation as far as region and timing effectiveness. We show for example that our region streamlined execution for 128-digit security requires 6.82 x 105 cycles and 2.26 x 106 cycles to epitomize and decapsulate a common mystery, individually. The region improved plan utilizes just 39 cuts (3 percent of the accessible rationale) and 809 cuts (39 percent of the accessible rationale) for key epitome and key decapsulation individually, on a little size low-end Xilinx Spartan-6 FPGA.

D. Zoni et al. [4], considering code-based cryptography, semi cyclic low-thickness equality check (QC-LDPC) codes are predicted as one of a handful of the answers for configuration post-quantum cryptosystems. The digit flipping calculation is at the center of the unraveling system of such codes when used to plan cryptosystems. A compelling plan should represent the computational intricacy of the deciphering and the code size needed to guarantee the security edge against assaults drove by quantum PCs. To this end, it is of foremost significance to convey productive and adaptable equipment executions to help quantum-safe public-key cryptosystems, since accessible programming arrangements can't adapt to the necessary exhibition. This original copy proposes a productive and adaptable engineering for the execution of the piece flipping methodology focusing on huge QC-LDPC codes for post-quantum cryptography. To exhibit the adequacy of our answer, we utilized the nine designs of the LEDAcrypt cryptosystem as delegate use cases for QC-LDPC codes appropriate for post-quantum cryptography. For every arrangement, our format engineering can convey an exhibition enhanced decoder execution for all the FPGAs of the Xilinx Artix-7 mid-range family. The test results exhibit that our upgraded design permits the execution of enormous QC-LDPC codes even on the littlest FPGA of the Xilinx Artix-7 family. Considering the execution of our decoder on the Xilinx Artix-7 200 FPGA, the test results show a normal exhibition speedup of multiple times across all the LEDAcrypt setups, contrasted with the authority enhanced programming execution of the decoder that utilizes the Intel AVX2 augmentation.

K. Koleci et al. [5], this paper is based on cyclic redundancy check based encoding scheme. High throughput and high speed hardware for Golay code encoder and decoder could be useful in digital communication system. In this paper, a new algorithm has been proposed for CRC based encoding scheme, which devoid of any linear feedback shift registers (LFSR). In addition, efficient architectures have been proposed for both Golay encoder and decoder, which outperform the existing architectures in terms of speed and throughput. The proposed architecture implemented in virtex-4 Xilinx power estimator. Although the CRC encoder and decoder is intuitive and easy to implement, and to reduce the huge hardware complexity required. The proposed method it improve the transmission system performance level. In this architecture our work is to design a Golay
code based on encoder and decoder architecture using CRC generation technique. This technique is used to reduce the circuit complexity for data transmission and reception process.

D. Zoni et al. [6], Memories that operate in harsh environments, like for example space, suffer a significant number of errors. The error correction codes (ECCs) are routinely used to ensure that those errors do not cause data corruption. However, ECCs introduces overheads both in terms of memory bits and decoding time that limit speed. In particular, this is an issue for applications that require strong error correction capabilities. A number of recent works have proposed advanced ECCs, such as orthogonal Latin squares or difference set codes that can be decoded with relatively low delay. The price paid for the low decoding time is that in most cases, the codes are not optimal in terms of memory overhead and require more parity check bits. On the other hand, codes like the (24,12) Golay code that minimize the number of parity check bits have a more complex decoding. A compromise solution has been recently explored for Bose–Chaudhuri–Hocquenghem codes.

M. Baldi et al. [7], this brief lays out cyclic redundancy check-based encoding scheme and presents an efficient implementation of the encoding algorithm in field programmable gate array (FPGA) prototype for both the binary Golay code ($G23$) and extended binary Golay code ($G24$). High speed with low-latency architecture has been designed and implemented in Virtex-4 FPGA for Golay encoder without incorporating linear feedback shift register. This brief also presents an optimized and low-complexity decoding architecture for extended binary Golay code (24, 12, 8) based on an incomplete maximum likelihood decoding scheme. The proposed architecture for decoder occupies less area and has lower latency than some of the recent work published in this area. The encoder module runs at 238.575 MHz, while the proposed architecture for decoder has an operating clock frequency of 195.028 MHz. The proposed hardware

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 2, February 2022 ||

| DOI:10.15680/IJIRSET.2022.1102031 |

modules may be a good candidate for forward error correction in communication link, which demands a high-speed system.

III. BINARY CODES

Block codes are referred to as (n, k) codes. A block of k information bits are coded to become a block of n bits. n=k + r, where r is the number of parity bits and k is the number of information bits.

The more commonly employed Block codes are:

1. Single Parity-Check Bit Code
2. Repeated Codes
3. Hadamard Code
4. Hamming Code
5. Convolution Code Codes
6. Cyclic Codes
7. Golay Code
8. Extended Golay Codes

Marcel Golay was born in Neuchatel, Switzerland in 1902. He was a successful mathematician and information theorist who was better known for his contribution to real world applications of mathematics than any theoretical work he may have done [9, 10]. Golay's sought the perfect code. Perfect codes are considered the best codes and are of much interest to mathematicians. They play an important role in coding theory for theoretical and practical reasons. The following is a definition of a perfect code:
A code C consisting of N codewords of length N containing letters from an alphabet of length q, where the minimum distance d=2e+1 is said to be perfect if:

$$\sum_{i=0}^{e} \binom{n}{i}(q-1)^i = \frac{q^n}{N} \qquad (1)$$

There are two closely related binary Golay codes. The extended binary Golay code G24 encodes 12 bits of data in a 24-bit word in such a way that any 3-bit errors can be corrected or any 7-bit errors can be detected. The other, the perfect binary Golay code G23 has codewords of length 23 and is obtained from the extended binary Golay code by deleting one co-ordinate position. In standard code notation the codes have parameters [24, 12, 8] and [23, 12, 7] corresponding to the length of the codewords, the dimension of the code and the minimum Hamming distance between two codewords respectively. In mathematical terms, the extended binary Golay code, G24 consists of a 12-dimensional subspace W of the space V=F224 of 24-bit words such that any two distinct elements of W differ in at least eight coordinates. By linearity, the distance statement is equivalent to any non-zero element of W having at least eight non-zero coordinates. The possible sets of non-zero coordinates as w ranges over W are called code words. In the extended binary Golay code, all code words have the Hamming weights of 0, 8, 12, 16, or 24. Up to relabeling coordinates, W is unique. The perfect binary Golay code, G23 is a perfect code. That is the spheres of radius three around code words form a partition of the vector space.

Codeword Structure: A code word is formed by taking 12 information bits and appending 11 check bits which are derived from a modulo-2 division, as with the CRC. Golay [23, 12] Code word. The common notation for this structure is Golay [23, 12], indicating that the code has 23 total bits, 12 information bits, and 23- 12=11 check bits. Since each codeword is 23 bits long, there are 223, or 8,388,608 possible binary values. However, since each of the 12-bit information fields has only one corresponding set of 11 check bits, there are only 212, or 4096, valid Golay code words.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 2, February 2022 ||

| DOI:10.15680/IJIRSET.2022.1102031 |

Check bits	Information bits
××× ×××× ××××	×××× ×××× ××××

Golay [24, 12] Codeword

Parity bit	Check bits	Information bits
×	××× ×××× ××××	×××× ×××× ××××

Fig. 3: Block Diagram of Golay Code

The binary Golay code leads us to the extended Golay code. Codes can be easily extended by adding an overall parity check to the end of each code word.
This extended Golay Code can be generated by the 12 × 24 matrix G = [I_{12} | A], where I_{12} is the 12 × 12 identity matrix and A is the 12 × 12 matrix

$$A=\begin{bmatrix} 0&1&1&0&1&1&1&1&1&1&1&1\\ 1&1&1&0&1&1&1&0&0&0&1&0\\ 1&1&0&1&1&1&0&0&0&1&0&1\\ 1&0&1&1&1&0&0&0&1&0&1&1\\ 1&1&1&1&0&0&0&1&0&1&1&0\\ 1&1&1&0&0&0&1&0&1&1&0&1\\ 1&1&0&0&0&1&0&1&1&0&1&1\\ 1&0&0&0&1&0&1&1&0&1&1&1\\ 1&0&0&1&0&1&1&0&1&1&1&0\\ 1&0&1&0&1&1&0&1&1&1&0&0\\ 1&1&0&1&1&0&1&1&1&0&0&0\\ 1&0&1&1&0&1&1&1&0&0&0&1 \end{bmatrix} \quad (4)$$

The binary linear code with generator matrix G is called the extended binary Golay code and will be denoted by G24.
The extended Golay code has a minimum distance of 8. Unlike the (23, 12) code, the extended Golay code is not perfect, but simply quasi perfect.

Properties of the extended binary Golay code

- The length of G24 is 24 and its dimension is 12.
- A parity-check matrix for G24 is the 12 × 24 matrix H = [A | I_{12}].
- The code G24 is self-dual, i.e., G⊥ 24 = G24.
- Another parity-check matrix for G24 is the 12 × 24 matrix H0 = [I_{12} | A] (= G).
- Another generator matrix for G24 is the 12 × 24 matrix G0 = [A | I_{12}] (= H).
- The weight of every codeword in G24 is a multiple of 4.
- The code G24 has no codeword of weight 4, so the minimum distance of G24 is d = 8.
- The code G24 is an exactly three-error-correcting code.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 2, February 2022 ||

| DOI:10.15680/IJIRSET.2022.1102031 |

Table 1: Comparison Result of Different Types of Binary Code

Binary Code	Error Detection	Error Correction	Efficiency	Distance
Single Parity-Check Bit Code	1	1	80-85%	low
Hadamard Code	2	1	50%	Low
Hamming Code	2	1	85-90%	low
Convolution Code	2	2	85-90%	Medium
Cyclic Codes	3	2	75-80%	Medium
Golay Codes	7	3	70-75%	Large
Extended Golay Codes	8	3	80-85%	Very Large

IV. METHODOLOGY

In each step during polynomial division, simply binary XOR operation occurs for modulo-2 subtraction. The residual result obtained at each step during the division process is circularly left shifted by number of leading zeros present in the result. A 12:4 priority encoder is used to detect efficiently the number of leading zeros before first 1 bit in the residual result in each step.

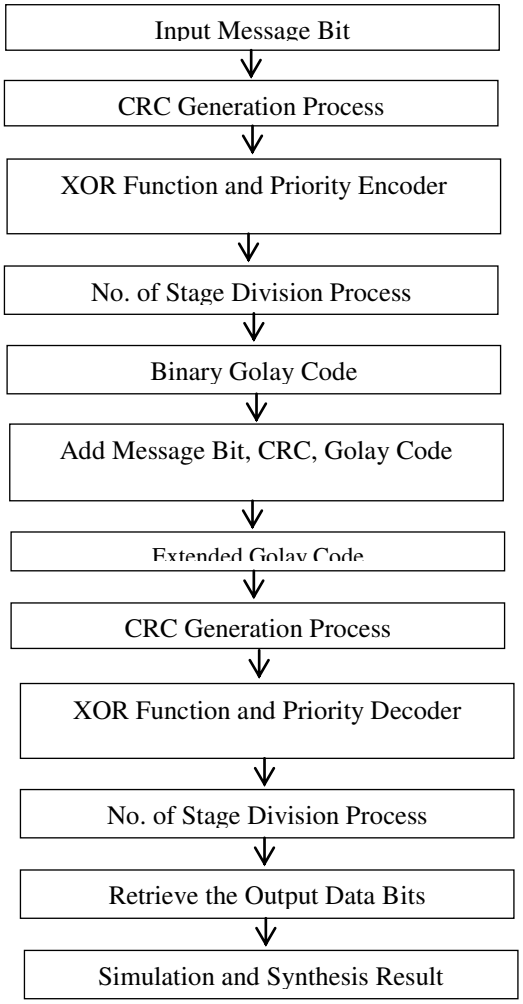

Fig. 4: Flow Chart of Golay Encoder and Decoder

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 2, February 2022 ||

| DOI:10.15680/IJIRSET.2022.1102031 |

A circular shift register is used to shift the intermediate result by the output of priority encoder. A 2:1 multiplexer is used to select the initial message or the circularly shifted intermediate result. The control signal used for the multiplexer and the controlled sub-tractor is denoted as *p*, which is bit wise OR operation of priority encoder output. A controlled sub-tractor is used for loop control mechanism. Initially, one input of sub-tractor is initialized with 11, which is the number of zeros appended in the first step of the long division process and it gets updated with the content of *R*7 register due to multiplexer selection after each iteration. The output of the priority encoder is the other input to the sub-tractor. After the final iteration, the result of sub-tractor is zero, which is stored in register *R*7. The register *R*6 is loaded when the content of register *R*7 becomes zero, which depicts the end of the division process and hence the check bits generation process.

V. CONCLUSION AND FUTURE SCOPE

In this paper, the Golay code and operation for various encoder and decoder is discussed. This encoding and decoding algorithm have been successfully applied to short block codes such as Golay code. Decoding algorithm consists of syndrome measurement unit, weight measurement unit and weight constraint.
The purpose of this study is to review the published encoding and decoding models in the literature and to critique their reliability effects. We will try to reduce the area, maximum combinational path delay (MCPD) of decoding algorithm of Golay code.

REFERENCES

[1] Kristjane Koleci, Paolo Santini, Marco Baldi, Franco Chiaraluce, Maurizio Martina And Guido Masera, “Efficient Hardware Implementation of the LEDAcrypt Decoder”, IEEE Access 2021.
[2] P. Santini, M. Battaglioni, M. Baldi, and F. Chiaraluce, “Analysis of the error correction capability of LDPC and MDPC codes under parallel bit-flipping decoding and application to cryptography,”, IEEE Trans. Communication, vol. 68, no. 8, pp. 4648_4660, Aug. 2020.
[3] J. Hu, M. Baldi, P. Santini, N. Zeng, S. Ling, and H. Wang, “Lightweight key encapsulation using LDPC codes on FPGAs”, IEEE Trans. Comput., vol. 69, no. 3, pp. 327_341, Mar. 2020.
[4] D. Zoni, A. Galimberti, andW. Fornaciari, ``Efficient and scalable FPGA oriented design of QC-LDPC bit-flipping decoders for post-quantum cryptography," *IEEE Access*, vol. 8, pp. 163419_163433, 2020.
[5] K.Koleci, M. Baldi, M. Martina, and G. Masera, ``Ahardware implementation for code-based post-quantum asymmetric cryptography," in *Proc. 3rd Italian Conf. Cybersecurity (ITASEC)*, vol. 2597, Ancona, Italy, Feb. 2020, pp. 141_152.
[6] D. Zoni, A. Galimberti, and W. Fornaciari, ``Flexible and scalable FPGA oriented design of multipliers for large binary polynomials," *IEEE Access*, vol. 8, pp. 75809_75821, 2020.
[7] M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, and P. Santini, ``LEDAcrypt: QC-LDPC code-based cryptosystems with bounded decryption failure rate," in *Code-Based Cryptography*, M. Baldi, E. Persichetti, and P. Santini, Eds. Cham, Switzerland: Springer, 2019, pp. 11_43.
[8] Shivani Tambatkar, Siddharth Narayana Menon, Sudarshan. V, M. Vinodhini and N. S. Murty, “Error Detection and Correction in Semiconductor Memories using 3D Parity Check Code with Hamming Code”, International Conference on Communication and Signal Processing, April 6-8, 2017, India.
[9] Pallavi Bhoyar, “Design of Encoder and Decoder for Golay code”, International Conference on Communication and Signal Processing, April 6-8, IEEE 2016, India.
[10] Pedro Reviriego, Shanshan Liu, Liyi Xiao, and Juan Antonio Maestro, “An Efficient Single and Double-Adjacent Error Correcting Parallel Decoder for the (24,12) Extended Golay Code”, IEEE Transactions On Very Large Scale Integration (VLSI) Systems, Vol. 34, No. 3, pp. 01-04, 2016.
[11] Satyabrata Sarangi and Swapna Banerjee, “Efficient Hardware Implementation of Encoder and Decoder for Golay Code”, IEEE Transactions on Very Large Scale Integration (VLSI) Systems 2014.
[12] P. Adde, D. G. Toro, and C. Jego, “Design of an efficient maximum likelihood soft decoder for systematic short block codes,” IEEE Trans. Signal Process. vol. 60, no. 7, pp. 3914–3919, Jul. 2012.
[13] T.-C. Lin, H.-C. Chang, H.-P. Lee, and T.-K. Truong, “On the decoding of the (24, 12, 8) Golay Code,” Inf. Sci., vol. 180, no. 23, pp. 4729–4736, Dec. 2010.
[14] M.-H. Jing, Y.-C. Su, J.-H. Chen, Z.-H. Chen, and Y. Chang,“High-speed low-complexity Golay decoder based on syndromeweight determination,” in Proc. 7th Int. Conf. Inf., Commun., Signal Process. (ICICS), Dec. 2009, pp. 1–4.
[15] Ayyoob D. Abbaszadeh and Craig K. Rushforth, Senior Member, IEEE, “VLSI Implementation of a Maximum-Likelihood Decoder for the Golay (24, 12) Code”, IEEE Journal on Selected Areas in Communications. VOL. 6, NO. 3, APRIL 1988.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details