Volume 6, Issue 5, May 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

VLSI Implementation of Golay Code using Encoder and Decoder

Ashima Dubey
Student, Department of ECE,
Lakshmi Narain College of Tech.,
Bhopal, India

Dr. Rita Jain
Head of Department of ECE,
Lakshmi Narain College of Tech.,
Bhopal, India

Prof. Soheb Munir
Professor, Department of ECE,
Lakshmi Narain College of Tech.,
Bhopal, India

Abstract— This brief lays out cyclic redundancy check-based encoding scheme and presents an efficient implementation of the encoding algorithm in Field Programmable Gate Array prototype for both theGolay Codes. Golay Code is a type of Error Correction Code and its performance is very close to Shanon's limit.Good error correcting performance enables reliable communication. The binary Golay Code (G_{23}) is represented as (23, 12, 7) while the extended binary Golay Code (G_{24}) 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 G_{24} (24, 12, 8) based on an incomplete maximum likelihood decoding scheme.

Index Terms— GolayCode, Decoder, Encoder, Field Programmable Gate Array

I. INTRODUCTION

Communication system transmits data from source to destination 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 in 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. Error detection and correction can be achieved by adding redundant symbols in the original data called as Error Correction Codes (ECCs). 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.

Error detection and correction helps in transmitting errorless data in a noisy channel. 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, Low Density Parity Check Code (LDPC) and Golay Code.

The detailed description of Golay Code is presented in 3rd section of this paper to address error correcting phenomena. In addition, Golay Code plays a vital role in different applications like coded excitation for a laser and ultrasound imaging due to the complete sidelobe nullification property of complementary Golay pair. All these applications need generation of Golay sequence, which is fed as trigger to the laser modules. However, for generating Golay Code, an automatic pattern generator is used, which is of very high cost. To combat this problem, a hardware module programmed to yield a Golay encoded codeword may beused. 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 forforward error correction.

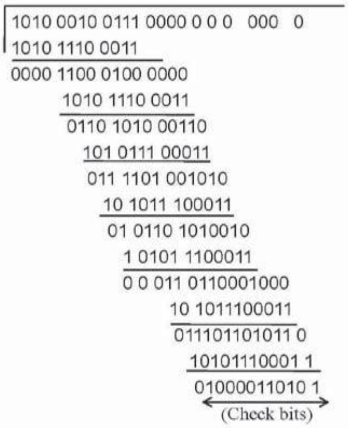
II. LITERATURE REVIEW

SatyabrataSarangi and Swapna Banerjee [1], 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. Their designed encoder module runs at 238.575 MHz. In addition, this architecture utilizes 187 Look Up Tables (LUTs) and 103 slices out of 135 168 each. The proposed architecture for decoder has an operating clock frequency of 195.028 MHz. In addition, this architecture utilizes 785 Look Up Tables (LUTs) and 230 slices out of 135 168 each. The proposed hardware modules may be a good candidate for forward error correction in communication link, which demands a high-speed system.

The steps required to accomplish the encoding procedure are enlisted as follows-

1) A characteristic polynomial $G(x)$ is chosen for check bits generation.
2) 11 zeros are appended to the right of message $M(x)$, such that resultant polynomial $P(x)$ participates in long division process with $G(x)$.
3) The remainder bits except the most significant bit (MSB) resulted at the end of the division operation are the check bits for G_{23}. Appending check bits with the message gives us the encoded Golay (23, 12, 7) Codeword.

4) A parity bit is added to convert the binary Golay Code into extended binary Golay Code (24, 12, 8). If the weight of binary Golay Code is even, then parity bit 0 is appended, otherwise 1 is appended.



```
1010 0010 0111 0000 0 0 0   000   0
1010 1110 0011
0000 1100 0100 0000
      1010 1110 0011
       0110 1010 00110
         101 0111 00011
          011 1101 001010
             10 1011 100011
              01 0110 1010010
                1 0101 1100011
                0 0 011 0110001000
                     10 1011100011
                      011101101011 0
                        10101110001 1
                         01000011010 1
                         (Check bits)
```

Fig 1- Example of check bits generation.

An example of Golay Codeword generation based on the encoding algorithm is shown in Fig. 1. Let us say, the message to be encoded is A27h. Hence, $M(x)$ = A27h and $P(x)$ in binary format is represented as 1010 0010 0111 0000 0000 000. Finally, the generated check bits in hexadecimal format are 435h. Hence, the encoded codeword for the message bits (A27h) is A27435h. This is a binary Golay Codeword. To convert it into an extended Golay Code, a parity bit 1 is appended, as weight of A27435h is 11 (odd). Finally, the generated Golay (24, 12, 8) Codeword is (1010 0010 0111 1000 0110 101 1). The validity of the generated Golay Code can be tested by measuring the weight of the code.

Xiao-Hong Peng[2] have studied thattwo product array codes are used to construct the(24, 12, 8) Binary GolayCode through the direct sum operation.This construction provides a systematic way to find proper (8, 4,4) Linear Block Component Codes for generating the Golay Code,and it generates and extends previously existing methods that usea similar construction framework. The code constructed is simpleto decode.

The two array codes concerned are both two-dimensional product codes. A product code C is formed by a direct product of two component code $C_1 = (n_1, k_1, d_1)$ and $C_2 = (n_2, k_2, d_2)$. The generator matrix G, of C is represented in the form of a Kronecker product denoted by $\otimes$.

$$G = G_1 \otimes G_2 \qquad (1)$$

G is of size $(k_1k_2) \times (n_1n_2)$.

The first array code C is the (24, 8, 8) product code constituted by $C = C_1 \times C_2$, where C_1 and C_2denote an (8, 4,4) linear systematic block code and a (3, 2, 2) single-parity check code, respectively. The generator matrix of C_2 is,

$$G_2 = \begin{bmatrix} 101 \\ 011 \end{bmatrix} \qquad (2)$$

Therefore, according to (1), the generator matrix of C is given by,

$$G = G_1 \otimes G_2 = \begin{bmatrix} G_1 & 0 & G_1 \\ 0 & G_1 & G_1 \end{bmatrix} \qquad (3)$$

Where G_1 is the 4× 8 generator matrix of C_1, and '0'represents a 4× 8 null matrix.W. Cao [3] in 1996 presented an efficient algorithm and the VLSI-architecture for fast soft-decision permutation decoding of the (24,12) extended Golay Code. The technique consists of an optimized permutation decoding with look-ahead error-correction and a modified parity check soft-decision decoding with reduced test pattern based on Chase's algorithm-2. He has also proposed a Parallel VLSI architecture which will allow for data rates reaching in the hundreds of Mbit/s.

The Chase's algorithm-2 (Chase-2) is an approximate maximum-likelihood decoding algorithm, which performs $2^{d/2}$test pattern operations for decoding one received word, where 'd'is the minimum distance. Based on Chase-2 algorithm, a more efficient decoding technique for (24,12,8) extended Golay Code is presented by making use of the parity-check information and investigating the error patterns. The new algorithm achieves the same decoding performance as Chase-2 algorithm by performing half as many test patterns (Chase-2 algorithm needs 16 test patterns). It becomes only slightly inferior to the Chase-2 algorithm when it performs only 4test patterns. With an additional parity check, the decoding algorithm can be described as follows:

Algorithm

IF parity-check = even, *THEN*

test patterns $\in$ *{0001, 0010, 0100,1000}*

IF parity-check = odd, *THEN*

testpattems $\in$ *{0000, 0011, 0101, 0110)*

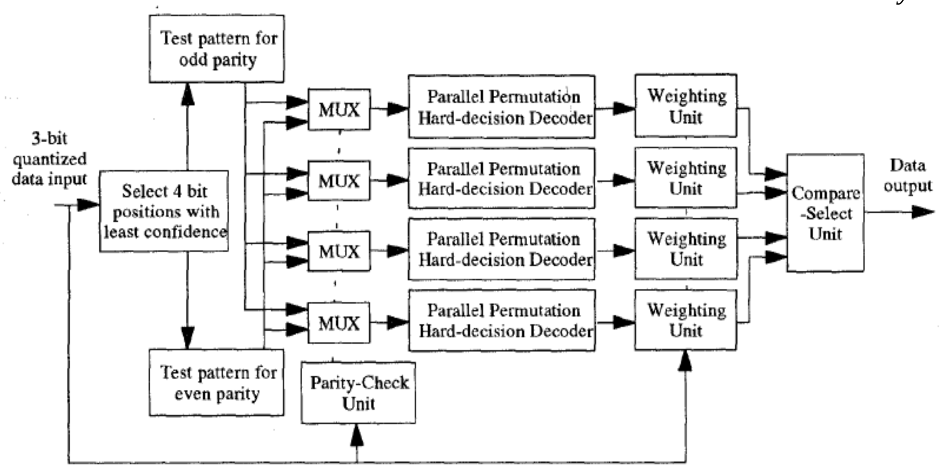

Test pattern for odd parity
3-bit quantized data input
Select 4 bit positions with least confidence
MUX
MUX
MUX
MUX
Parallel Permutation Hard-decision Decoder
Parallel Permutation Hard-decision Decoder
Parallel Permutation Hard-decision Decoder
Parallel Permutation Hard-decision Decoder
Weighting Unit
Weighting Unit
Weighting Unit
Weighting Unit
Compare -Select Unit
Data output
Test pattern for even parity
Parity-Check Unit

Figure 3. Block diagram of parallel soft-decision decoder for (24,12) extended Golay code with 4 test patterns

Fig 2- Block diagram of parallel soft decision decoder for extended Golay Code

The VLSI-architecture for soft-decision decoding of the (24,12,8) Golay code with parity-check operation is shown in Fig. 2. This high-speed soft-decision decoder processes simultaneously four parallel hard-decision operations in parallel structure. Thus, a high data rate canbe achieved in the range of hundreds of M bits/s.

Table 1: Comparison of the Decoder architecture considering Latency and Area

Reference	Latency	Area (Number of Gates)
[1]	576 clock cycles	-
[2]	23 gate level delay	6000
[3]	-	3500
[4]	48 clock cycles	4000
[5]	27 clock cycles	3013
proposed	24 clock cycles	2543

Table 2: Comparison of the Encoder Architecture considering Latency and LUT's

Reference	LUT Utilization (%)	Latency
[7]	1.33	12
[8]	1.72	12
[5]	0.14	12
proposed	0.12	12

Ayyoob D. Abbaszadeh and Craig K. Rushforth [4], described an efficient bit-serial Very Large Scale Integrated (VLSI) implementation of the exact maximum-likelihood decoding of the Golay (24, 12) Code in the additive white Gaussian noise channel. The design consists of two chips developed using Path Programmable Logic (PPL) and an associated system of automated design tools for 3μm NMOS technology. They have estimated that their decoder will produce an information bit every 1.6-2.4μs. Higher speeds can be achieved by using a faster technology or by replicating the chips to perform more operations in parallel.

III. BINARY GOLAY CODE

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. Extended Codes
6. Cyclic Codes
7. The Golay Code
8. BCH 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. Golay 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:

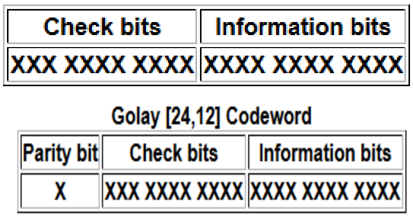
A code C consisting of N Codewords of length N containing letters from an alphabet of length q, where the minimum distance d=2e+1 is said to be perfect if:

$$\sum_{i=0}^{e}\binom{n}{i}(q-1)^{i}=\frac{q^{n}}{N} \qquad (4)$$

There are two closely related binary Golay Codes. The extended binary Golay Code G_{24}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 G_{23} has codewords of length 23 and is obtained from the extended binary GolayCode 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, G_{24} 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. 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, G_{23} is a perfect code. That is the spheres of radius three around Code words form a partition of the vector space.

Codeword Structure:

A codeword is formed by taking 12 information bits and appending 11 check bits which are derived from a modulo-2 division, as with the Cyclic Redundancy Check (CRC)Golay [23,12] Codeword as shown in Fig 3. 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 Codewords.



Check bits	Information bits
XXX XXXX XXXX	XXXX XXXX XXXX

Golay [24,12] Codeword

Parity bit	Check bits	Information bits
X	XXX XXXX XXXX	XXXX XXXX XXXX

Fig 3 – Notation of Check Bits and Information bits for Golay Code word

The generator matrix for the (23, 12, 7) code is:

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

.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.

The binary linear code with generator matrix G is called the extended binary Golay Code and will be denoted by G_{24}.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 G_{24} is 24 and its dimension is 12.
- A parity-check matrix for G_{24} is the 12 × 24 matrix H = [A | I_{12}].
- The code G_{24} is self-dual, i.e., G⊥ 24 = G_{24}.
- Another parity-check matrix for G_{24} is the 12 × 24 matrix H = [I_{12} | A] (= G).
- Another generator matrix for G_{24} is the 12 × 24 matrix G0 = [A | I_{12}] (= H).
- The weight of every Code word in G_{24} is a multiple of 4.

- The code G_{24} has no Code word of weight 4, so the minimum distance of G_{24} is d = 8.
- The code G_{24} is an exactly three-error-correcting code.

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

IV. METHODOLOGY

In each step during polynomial division, simple 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. 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 subtractor is denoted as *p*, which is bit wise OR operation of priority encoder output. A controlled subtractor is used for loop control mechanism.

Initially, one input of subtractor 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 subtractor. After the final iteration, the result of subtractor 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.

Architecture for decoding extended Golay Code consist of syndrome measurement, weight measurement, priority encoder and multiplexer to select the register. SatyabrataSarangi and Swapna Banerjee [1] proposed the structure of weight measurement unit that consists of 2-bit and 3-bit ripple carry adder. Ripple Carry Adder consumes large area and induces more delay as compared to Common Boolean Logic (CBL) adder and Kogge-Stone Logic (KSL) adder. Thus to overcome the mentioned problems we will use CBL and KSL in our model.

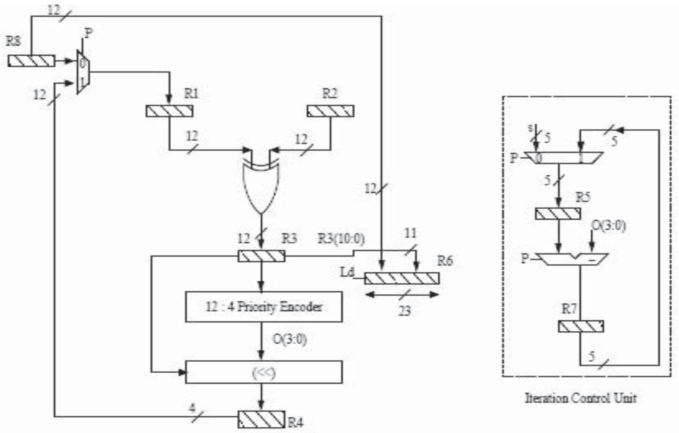


Fig 3- Architecture for generating binary Golay Code.

V. STEPS OF DESIGN

1. Use of Common Boolean Logic (CBL) adder and Kogge-stone adder reduce area and delay of decoding algorithm.
2. Design 13:1 mux using 2:1 mux and 4:1 mux to reduce the delay.
3. Use of different binary Golay Code is (23, 12, 7) and (24, 12, 8).
4. All the modules design to different device family i.e. Spartan-3, Virtex-4 and Virtex-7.

VI. CONCLUSION, RESULTS 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. Table 1 gives our approximated count of reduction in the number of gates resulting in minimising the area and improved latency of 24 clock cycles in the

Decoder Architecture. Also, Table 2 gives the approximated percentage (0.12%) of LUT utilization and improved Latency of the Encoder Architecture.The purpose of this thesis 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] SatyabrataSarangi and Swapna Banerjee, "Efficient Hardware Implementation of Encoderand Decoder for Golay Code", IEEE Transactions On Very Large Scale Integration (VLSI) Systems 2014.

[2] Xiao-Hong Peng, *Member, IEEE,* and Paddy G. Farrell, *Life Fellow, IEEE, "*On Construction of the (24, 12, 8) Golay Codes*", IEEE* Manuscript received January 19, 2005; revised July 7, 2005 and December15, 2005, respectively.

[3] W. Cao, "High-speed parallel hard and soft-decision Golay decoder: Algorithm and VLSI-architecture," in *Proc. IEEE Int. Conf. Acoust.,Speech, Signal Process. (ICASSP).*, vol. 6. May 1996, pp. 3295–3297.

[4] 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.

[5] W. Cao, "High-speed parallel VLSI-architecture for the (24, 12) Golay decoder with optimized permutation decoding," in *Proc. IEEE Int. Symp.Circuits Syst. (ISCAS), Connecting World*, vol. 4. May 1996, pp. 61–64.

[6] 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.

[7] B. Honary and G. Markarian, "New simple encoder and trellis decoder for Golay Codes", ELECTRONICS LETTERS 9th December 1993 Vol. 29 No. 25.

[8] Michael Sprachmann, "Automatic Generation of Parallel CRC Circuits", 0740-7475/01/$10.00 © 2001 IEEE.

[9] Giuseppe Campobello, Giuseppe Patane`, and Marco Russo, "Parallel CRC Realization", IEEE TRANSACTIONS ON COMPUTERS, VOL. 52, NO. 10, OCTOBER 2003.

[10] G. Solomon, "Golay encoding/decoding via BCH-hamming," *Comput.Math. Appl.*, vol. 39, no. 11, pp. 103–108, Jun. 2000.

[11] I. Boyarinov, I. Martin, and B. Honary, "High-speed decoding of extended Golay Code," *IEE Proc. Commun.*, vol. 147, no. 6, pp. 333–336, Dec. 2000.

[12] D. C. Hankerson*et al., Coding Theory and Cryptography The Essentials*, 2nd ed. New York, NY, USA: Marcel Dekker, 2000.

[13] 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., SignalProcess. (ICICS)*, Dec. 2009, pp. 1–4.

[14] 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.