A CLASS OF OPTIMIZED ENCODER FOR BLOCK CODES

*Ramasethu L[1] , Dr.Poongodi P [2]

[1]*Assistant Professor, department of Electronics and communication engineering, Hindusthan college of engineering and technology,othakalmandabam post, coimbatore, Tamil Nadu - 641032, India.*
Email:*ramasethul.ec@gmail.com*

[2]*Professor, department of Electronics and communication engineering, Kalaignar Karunanidhi Institute of Technology, Kannampalayam, coimbatore, Tamil Nadu - 641402, India.*
Email: *poongodiravikumar@gmail.com*

Abstract : *Error correcting codes are used broadly,in particularapplications such asin deep satellite communication and fault tolerant memory. In this papera new block code of (32, 19) optimised encoder is proposed. Compared with extended Golay code (24,12)the existing codesare capable of correcting three adjacent errors and detecting six errors. Optimization is achieved by an algorithm which finds the "Majority Message" bits (M). The proposed work is only on the encoder section of block and cyclic codes.As of now most of the work for error correcting codes are carried only on decoder section because of its complexity. A speed encoder is proposed which is not complex through the optimised algorithm. The delay in encoder is reduced thereby it contributes to the efficient error correcting code when considered with decoder section. The codes are programmed in HDL and synthesised using cadence tool of 180 nm library. The result on encoder with optimised new block code for delay, area and power which is at par to the cyclic code. For an increased number of message bits the proposed code is much efficient in correcting triple adjacent error.*

Keywords : *Optimised encoder, Golaycode, Encoder formation.*

1. Introduction : The real idea of coding technique is to send out reliable data. In memories particularly main memory [1], much frequently occurring data's are stored due to scaling of transistors to a great extentrepeatedly subjected to highly ionised particles [2],[3], asa result the content stored in main memory are flipped from previously stored value.This change in values from 0 to 1 else from 1 to 0 is called soft errors [4] [5]. More over spreading of error to adjacent bits occur and that leads to multiple bit upset [6],[7].Viable and cost effective solution to fault secure memory is a must and this is achieved through Error Correction Code(ECC) [8].C.E.Shannon[17]proposed a method to correct error in a channel with noise as a mathematical model, Golay [16] proposed a mathematical outline for triple bit error correction in code word length of 23. Later R.W.Hamming[15] proposed a single bit error detection, single bit error correction and double bit error detection for computers. R.W.Hamming proposed the error detection method and C.E.Shannon proposed error correction technique. D.E.Muller suggested how to correct multiple bit error on a given code word and dealt "Code for Multiple Error". Next development of coding theory moved towards the decoding scheme of correcting multiple errors proposed by Irving S. Reed [18] based on D.E.Muller's "Code for Multiple Errors".

The major classifications of information theory areError Detection,Forward Error Correction (FEC)and Automatic Repeat reQuest (ARQ).Error detection codes are capable of only detection of error, forward error correction codes are capable of detecting and correcting errors, FEC are further sub classified as block codes formed by generation matrix (G) and parity matrix (H).Cyclic codes are formed by polynomials and convolutioncodes are built using trillisor code tree. In the case of ARQ, the codes transmit error control signals.

The proposed work is on coding theory of block codesof size (*n, k*).The key aspect in block codes and cyclic codes are code rate efficiency, error detection and error correction capability. Code rate determines the available width of information or data compared to the number of parity given in a code word of size *n*. For any Error Correction Code (ECC) minimum distance (d_{min}) determines the error detection and correction capability. Based on d_{min}single [19], [20]double [9], [14]and a triple adjacent error occur.Among them,triple adjacent errors [10] are very much associated to burst errors and it can be corrected. In general, detection capability of ECC is higher when it is comparedwith correction. To increase the number of correction capability hamming bound condition should be satisfied. If the number of correction capability increases, parity bits increases which leads to the decrease in number of data bits in a code word. A class of SEC-DAED- TAEC of (31, 19) is found to be efficient in detection and correction capability[11], but this codes lags in satisfying the hamming bound which in turn contributes to the unreliable correction of TAEC. Even though the proposed work is not related with decoding, a new block code is introduced to satisfythe hamming bound condition and anoptimised encoder for the same.

Coded messages are much efficient and reliable than uncoded data. In this regard ECC is unavoidable. Encoders are very much essential for the generation of message or data bits with parity bit which is the first source for the formation of reliable data communication. An encoder for a block code is implemented using registers and mod 2 operations, for cyclic codes flip-flops with a minimum number of XOR function based on the polynomial is formed. An Encoder for cyclic codes such as Extended Golay [12], Bose ChaudhariHocquenghes[13], and Reed Solomon codes encoder are simple to design and implement. In the case of block codes, the encoders are simple to construct except if the length of the code increases the encoder delay increases linearly. To fix this issue an algorithm is proposed to reduce the delay that occurs in the block codes even if the size increases. The proposed algorithm is suitable only for block codes if the size of the code increases the delay in an encoder.

2. Proposed work:

Mathematical approach for the (32, 19) block code formation is given below in the form of equations. Equation (1) to (4) is used for design of encoder, Equation (5) to (8) used to design decoder. As the proposed work is on encoder, decoder part of this block code is not explained. To get the code word 'X' generation matrix 'G' should be formed; this is a matrix formation of identity 'I' and coefficient'P' of size as shown in equation (2) and (3).where *n* is 32 and *k* is 19 bits. Encoded data is the combination of information or message '*m*' and parity '*p*'. Generation matrix is shown in Figure.1.

Encoder formation

$$X = mG \quad \text{---(1)}$$

$$G = \left[P_{(k\ by\ n-k)} : I_k\right] \quad \text{---(2)}$$

$$p = mP_{(k\ \ by\ n-k)} \quad \text{---(3)}$$

$$X = [p : m] \quad \text{---(4)}$$

Decoder formation

$$H = \left[P^T : I_{n-k}\right] \quad \text{---(5)}$$

$$S = EH^T{}_{(n\ by\ n-k)} \quad \text{---(6)}$$

$$S = YH^T{}_{(n\ by\ n-k)} \quad \text{---(7)}$$

$$Y = X \oplus E \quad \text{---(8)}$$

$$G=\begin{bmatrix}
10011111000001000000000000000000\\
01001111100000100000000000000000\\
00100111110010010000000000000000\\
00010011111000001000000000000000\\
00001001111110000100000000000000\\
11111100000000000010000000000000\\
01111110000010000001000000000000\\
00111111000000000000100000000000\\
00011111100010000000010000000000\\
00001111110010000000001000000000\\
00000111111010000000000100000000\\
00000011111110000000000010000000\\
10101010101000000000000001000000\\
01010101010100000000000000100000\\
11100011100000000000000000010000\\
00011100011110000000000000001000\\
11001100110010000000000000000100\\
00110011001100000000000000000010\\
00110011001100000000000000000010\\
00001011111010000000000000000001
\end{bmatrix}$$

Figure 1:Generation Matrix 'G'

3. Algorithm

1. Formation of generation matrix according to the specific size of block code.
2. Find the parity bits.
3. On information bits XOR operation should be performed which in turn is determined from coefficient of G matrix.
4. Find the majority message bits in every parity bit.
5. Majority message bits are grouped to a minimum of 3 bits.
6. Grouped majority message bits are representedby a constant variable.
7. Constant variables should be unlike
8. Grouped majority messages are replaced by constant variables.

As given in the algorithm the parity bits are formed from the coefficient of G matrix and message bits. In the proposed work grouping of minimum three majority message '*M*' bits is done and it can even be beyond 3 grouping.In addition if the block size is increased the *M* grouping will be better. Grouped majority message bits should not be repeated or overlapped in other grouped message bits.Using the proposed algorithm the parity bits are formed and shown below from equation (9) to (21). In equation (11) first grouping of majority message bits are highlighted by a dotted arrow towards right direction, and denoted by a constant variable *M*, similarly other grouping is shown under message grouping in Table.1. In the proposed case the grouped messages bits are of minimum three, other possibility of grouping are in two messages that are similar are found more in all the parity bit equation but not considered because computation time of two messages for XOR operation is much similar when represented as *M* bit or majority message bit in other parity equations. Table.1also shows the repeated grouping in other parity bits. In the case of equation (14) parity bit is *p*6 and it holds two majority message grouping *M2* and*M3*. This grouping is repeated in other parity bits such as*p*7, *p8* and *p*7, *p8, p9, p13*respectively. In the same equation previously grouped majority message is represented and recalled as constant variable *M1*.

$$p1 = m1 \oplus m6 \oplus m13 \oplus m15 \oplus m17 \quad \text{---(9)}$$

$$p2 = m2 \oplus m6 \oplus m7 \oplus m14 \oplus m15 \oplus m17 \quad \text{---(10)}$$

$$p3 = m3 \oplus m6 \oplus m7 \oplus m8 \oplus m13 \oplus m15 \oplus m18 \quad \text{---(11)}$$

$$\text{---------->} \boldsymbol{M1}$$

$$p4 = m1 \oplus m4 \oplus \boldsymbol{M1} \oplus m9 \oplus m14 \oplus m16 \oplus m18 \quad \text{---(12)}$$

$$p5 = m1 \oplus m2 \oplus m5 \oplus \boldsymbol{M1} \oplus m9 \oplus m10 \oplus m13 \oplus m16 \oplus m17 \oplus m19 \quad \text{---(13)}$$

$$p6 = m1 \oplus m2 \oplus m3 \oplus \boldsymbol{M1} \oplus m9 \oplus m10 \oplus m11 \oplus m14 \oplus m16 \oplus m17 \quad \text{---(14)}$$

$$\text{------->} \boldsymbol{M2}$$

$$\text{------->} \boldsymbol{M3}$$

$$p7 = \boldsymbol{M2} \oplus m4 \oplus m7 \oplus m8 \oplus \boldsymbol{M3} \oplus m12 \oplus m13 \oplus m15 \oplus m18 \oplus m19 \quad \text{---(15)}$$

$$p8 = \boldsymbol{M2} \oplus m4 \oplus m5 \oplus m8 \oplus \boldsymbol{M3} \oplus m12 \oplus m14 \oplus m18 \oplus m19 \quad \text{---(16)}$$

$$p9 = m2 \oplus m3 \oplus m4 \oplus m5 \oplus \boldsymbol{M3} \oplus m12 \oplus m13 \oplus m15 \oplus m17 \oplus m19 \quad \text{---(17)}$$

$$\text{------->} \boldsymbol{M4}$$

$$p10 = \boldsymbol{M4} \oplus m10 \oplus m11 \oplus m12 \oplus m14 \oplus m16 \oplus m17 \oplus m19 \quad \text{---(18)}$$

$$---------> \boldsymbol{M5}$$

$$p11 = m4 \oplus m5 \oplus m11 \oplus m12 \oplus m16 \oplus m18 \oplus m19 \quad \text{---(19)}$$

$$p12 = m5 \oplus m12 \oplus m14 \oplus m16 \oplus m18 \quad \text{---(20)}$$

$$p13 = m3 \oplus m5 \oplus m7 \oplus \boldsymbol{M3} \oplus m12 \oplus \boldsymbol{M5} \quad \text{---(21)}$$

Parity bits	Message grouping	Represented in other parity bits	Repeated grouping in other parity
$p3$	$m6 \oplus m7 \oplus m8$	$M1$	$p4, p5, p6$
$p6$	$m1 \oplus m2 \oplus m3$	$M2$	$p7, p8$
	$m9 \oplus m10 \oplus m11$	$M3$	$p7, p8, p9, p13$
$p9$	$m3 \oplus m4 \oplus m5$	$M4$	$p10$
$p10$	$m16 \oplus m17 \oplus m19$	$M5$	$p13$

Table: 1 Message grouping.

In addition to grouping, prediction of grouped data is used. Grouping is in three for which the prediction is shown inTable.2. In Message Grouping *M*if 1's are odd in numbers the prediction is 1, similarly if 1's are even the prediction is 0. For any combination of width three, the prediction is either 1 or 0 based on the number of 1's.

Grouped Message Bits (*M*)			Prediction
1	1	1	1
1	0	0	1
0	1	1	0
0	0	0	0

Table 2: Prediction of Grouped Messages

4. Results

In the proposed algorithm, the block code for the encoder is programmed in Verilog language and synthesized using cadence tool. Result for the encoder is tabulated in table 3, 4, 5 for proposed code without and with grouping compared with extended Golay code respectively. From the tabulation it is meant, grouping with prediction had reduced the delay considerably Extended Golay code is compared since, in general for cyclic codes encoding of the message in speedy when compared with block codes to reduce this gap our code with an optimized algorithm is a feasible solution. Area for proposed encoder with grouping is 2.42 % higher than extended Go1ay code similarly it's the same percentage for power also, in the case of delay 7.87 % higher compared with the Extended Golay code, although the results are slightly higher compared to (24, 12) code, comparison with grouping and without grouping had to show a considerable reduction in all the parameters. In without grouping, there is 4 % increase in area, 13 % increase in delay and 2 % increase in power when compared with the grouping of majority message bits. In with grouping, there is an increase in delay of encoder because of prediction and an initial grouping of *M*, when the same is called as constant it reduces the delay in computing approaching parity bits.

n	*k*		Max Effort in area	Max Effort in delay
32	19	Proposed code – without grouping	730	1387
32	19	Proposed code – with grouping	702	1154
24	12	Extended Golay code	685	1002

Table 3: Area Estimates Area in μm^2

n	*k*		Max Effort in area	Max Effort in delay
32	19	Proposed code – without grouping	2.66	1.51
32	19	Proposed code – with grouping	2.25	1.31
24	12	Extended Golay code	2.09	1.22

Table 4: Delay Estimates Delay in ns

n	*k*		Max Effort in area	Max Effort in delay
32	19	Proposed code – without grouping	7.34	28.25
32	19	Proposed code – with grouping	7.20	22.87
24	12	Extended Golay code	7.03	20.46

Table 5: Power Estimates Power in mW

5. Conclusion:

In this brief, new block code of (32, 19) optimized encoder is proposed. Even though our proposed block code results are closer to the existing cyclic codes, the message bits are comparatively higher (19-bit) than Extended Golay code (12-bit). As a result of this recommended block code methodology, there is a marginal increase in delay. It concludes that proposed block code with optimized algorithm may be introduced for other lengthy block codes. It is observed that, when the grouping of majority message bits is repeated in significant parity bits, the delay might be brought down apparently. Proposed (32, 19) code is not compared with similar code length of cyclic codes since presented work is first part of a fault secure memory design, second part will be TAEC for which most suitable bench mark code is Extended Golay code, other cyclic codes of proposed length will lag in correction capability. In the case of (31, 16); and (31, 21) BCH codes correction ability is 2 and 1 respectively. Also for a memory with reduced gate width is much prone to alpha particles, in a practical aspect with moderate data and good correction capability our optimised proposed code is suitable option for fault secure memory.

References:

[1] C. L. Chen and M. Y. Hsiao, "Error-correcting codes for semiconductor memory applications: A state-of-the-art review," in Res. Develop., IBM J. (1984). vol. 28, no. 2, pp. 124–134.

2] E. Ibe, H. Taniguchi, Y. Yahagi, K. Shimbo, and T. Toba, "Impact of scaling on neutron-induced soft error in SRAMs from a 250 nm to a 22 nm design rule," in Electron Devices, IEEE Trans (2010). vol. 57, no. 7, pp. 1527–1538.

[3] S. Satoh, Y. Tosaka, and S. A. Wender, "Geometric effect of multiple-bit soft errors induced by cosmic ray neutrons on DRAM's," in Electron Device Lett., IEEE (2000). vol. 21, no. 6, pp. 310–312.

[4] R. Baumann, "Soft errors in advanced computer systems," in Test. Comput. IEEE Des (2005). vol. 22, no. 3, pp. 258–266.

[5] S. Baeg, S. Wen, and R. Wong, "SRAM interleaving distance selection with a soft error failure model," in Nucl. Sci., IEEE Trans. (2009). vol. 56, no. 4, pp. 2111–2118.

[6] A. Neale and M. Sachdev, "A new SEC-DED error correction code subclass for adjacent MBU tolerance in embedded memory," in Device Mater. Rel., IEEETrans(2013). vol. 13, no. 1, pp. 223–230.

[7] Z. Ming, X. L. Yi, and L. H. Wei, "New SEC-DED-DAEC codes for multiple bit upsets mitigation in memory," in Proc. Of 19th Int. Conf. VLSI Syst.-Chip, IEEE/IFIP (2011), pp. 254–259.

[8] P. Reviriego, J. A. Maestro, S. Baeg, S. Wen, and R. Wong, "Protection of memories suffering MCUs through the selection of the optimal interleaving distance," inNucl. Sci.,IEEE Trans (2010).vol. 57, no. 4, pp. 2124–2128.

[9] Pedro Reviriego, Jorge Martinez, Salvatore Pontarelli, and Juan Antonio, "A Method to design SEC-DED- DAEC codes with optimized Decoding," in device and materials reliability, IEEE Trans (2014) Vol 14,No:3,pp 884 – 889.

[10] Luis-J. Saiz-Adalid, Pedro Reviriego, Pedro Gil, Salvatore Pontarelli, and Juan Antonio Maestro, "MCU Tolerance in SRAMs Through Low-Redundancy Triple Adjacent Error Correction," on very large scale integration systems, IEEE trans (2015), vol. 23, no. 10, pp .2332-2336.

[11] L. Ramasethu, P. Poongodi "A Class of SEC-DAED-TAEC Codes forFault Secure SRAM" in Journal of Computational and Theoretical Nanoscience (2017). vol. 14, pp 5897–5900. doi:10.1166/jctn.2017.7032

[12] Pedro Reviriego, Shanshan Liu, Liyi Xiao, and Juan Antonio Maestro "An Efficient Single and Double-Adjacent Error Correcting Parallel Decoderfor the (24,12) Extended Golay Code" in IEEE transactions on very large scale integration (vlsi) systems, (2016). vol. 24, no. 4, pp. 1603 – 1606.

[13] Chi-Heng Yang, Yi-Min Lin, Hsie-Chia Chang, and Chen-Yi Lee, "An MPCN-Based BCH Codec Architecture WithArbitrary Error Correcting Capability", (2015). vol. 23, no. 7, pp. 1235 – 1244.

[14] Morris Plotkin "Binary Codes with Specified Minimum Distance", (1960). IRETransaction On Information Theory, pp. 445 – 450.

[15] R. W. Hamming, "Error detecting and error correcting codes,"Bell Sys. Tech. J., vol. 29, pp. 147-160; April, 1950.

[16] M. J. E. Golay, "Notes on digital coding," PROC. IRE, vol.37, p. 657; June, 1949.

[17] C. E. Shannon "A Mathematical Theory of Communication"*The Bell System Technical Journal,*Vol. 27, pp. 379–423, 623–656, July, October, 1948.

[18] I. S. Reed, "A class of multiple-error-correcting codes and thedecoding scheme," IRE trans. On information theory, no.PGIT-4, pp. 38-49; September, 1954.

[19] Shan Shan Liu✉, Pedro Reviriego, Alfonso Sánchez-Macián,Liyi Xiao and Juan Antonio Maestro "Odd-weight-column SEC–DED–TAED codes" ELECTRONICS LETTERS 21st January 2016 Vol. 52 No. 2 pp. 119–120.

[20] P. G. Farrell Z. AL-Bandar"Multilevel single-error-correctingcodes" *ELECTRONICS LETTERS 8th August 1974 Vol.10 No*