



Fault Secure Encoder and Decoder For Memory Applications

V.Jeevitha¹

ME-VLSI Design, Shreenivasa Engineering College, B.Pallipatti, Dharmapuri, Tamilnadu, India¹

Abstract: In a recent paper, a method was proposed to accelerate the majority logic decoding of difference set low density parity check codes. This is useful as majority logic decoding can be implemented serially with simple hardware but requires a large decoding time. For memory applications, this increases the memory access time. The method detects whether a word has errors in the first iterations of majority logic decoding, and when there are no errors the decoding ends without completing the rest of the iterations. Since most words in a memory will be error-free, the averaged encoding time is greatly reduced. In this brief, we study the application of a similar technique to a class of Euclidean geometry low density parity check (EG-LDPC) codes that are one step majority logic decodable. The results obtained show that the method is also effective for EG-LDPC codes.

Key Words:-Error correction codes, Euclidean geometry low-density parity check (EG-LDPC) codes, majority logic decoding, memory.

I. INTRODUCTION

Error correction codes are commonly used to protect memories from so-called soft errors, which change the logical value of memory cells without damaging the circuit. As technology scales, memory devices become larger and more powerful error correction codes are needed. To this end, the use of more advanced codes has been recently proposed. These codes can correct a larger number of errors, but generally require complex decoders. To avoid a high decoding complexity, the use of one step majority logic decodable codes was first proposed in for memory applications. One step majority logic decoding can be implemented serially with very simple circuitry, but requires long decoding times. In a memory, this would increase the access time which is an important system parameter. Only a few classes of codes can be decoded using one step majority logic decoding. Among those are some Euclidean geometry low density parity check (EG-LDPC) codes which were used in, and difference set low density parity check (DS-LDPC) codes. A method was recently proposed in to accelerate a serial implementation of majority logic decoding of DS-LDPC codes. The idea behind the method is to use the first iterations of majority logic decoding to detect if the word being decoded contains errors. If there are no errors, then decoding can be stopped without completing the remaining iterations, therefore greatly reducing the decoding time.

II. EXISTING SYSTEM

The information bits are fed into the encoder to encode the information vector, and the fault secure detector of the encoder verifies the validity of the encoded vector. If the detector detects any error, the encoding operation must be redone to generate the correct codeword. The codeword is then stored in the memory. During memory access operation, the stored codewords will be accessed from the memory unit. Codewords are susceptible to transient faults while they are stored in the memory; therefore a corrector unit is designed to correct potential errors in the retrieved codewords.

In Existing design all the memory words pass through the corrector and any potential error in the memory words will be corrected. Similar to the encoder unit, a fault-secure detector monitors the operation of the corrector unit. All the units showing Fig 2 are implemented in fault-prone, nano scale circuitry; the only component which must be implemented in reliable circuitry are two OR gates that accumulate the syndrome bits for the detectors (shown in Fig 2).

Data bits stay in memory for a number of cycles and, during this period, each memory bit can be upset by a transient fault with certain probability. Therefore, transient errors accumulate in the memory words over time. In order to avoid accumulation of too many errors in any memory word that surpasses the code correction capability, the system must perform memory scrubbing. Memory scrubbing is the process of periodically

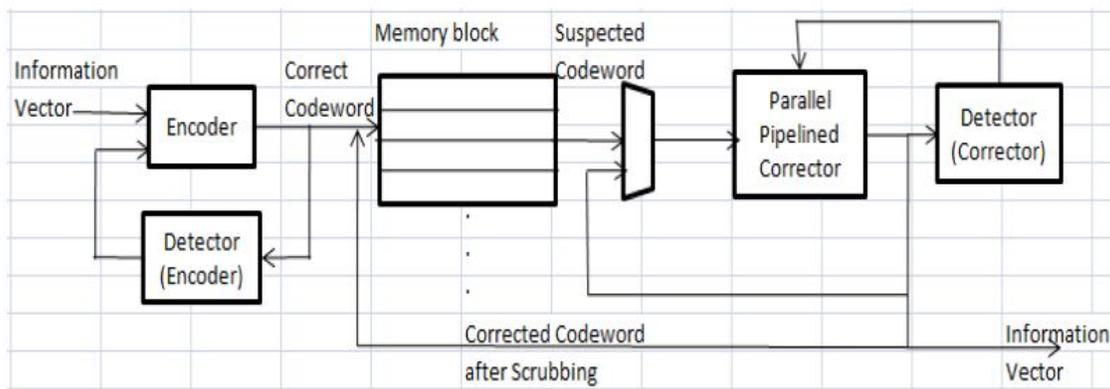


Fig:1 Existing EG LDPC

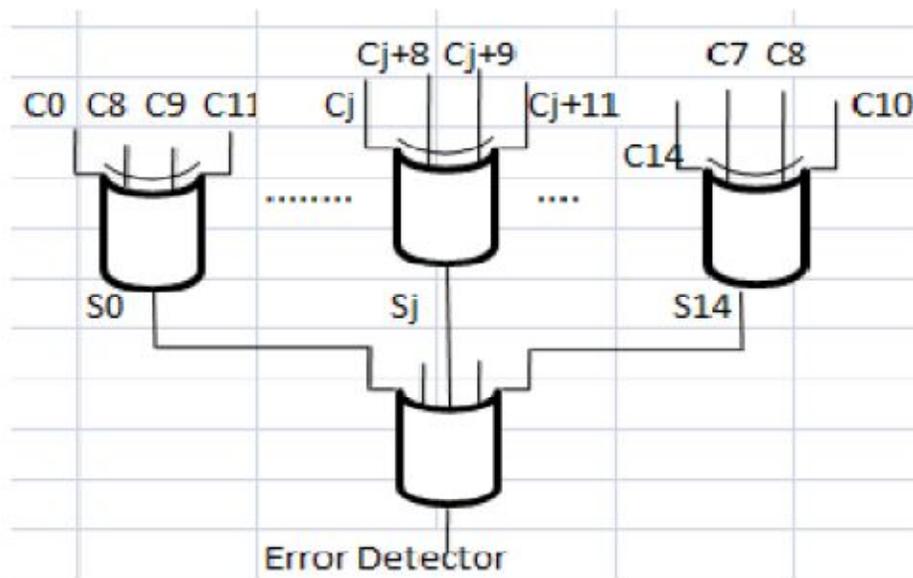


Fig :2 fault-secure detector for (15,7,5) EG-LDPC code

For a code with block length N , majority logic decoding (when implemented serially) requires N iterations, so that as the code size grows, so does the decoding time.

An n -bit codeword, which encodes a n -bit information Vector I is generated by multiplying the n -bit information vector with $k \times n$ bit generator matrix; i.e., $c = i \cdot G$. EG-LDPC codes are not systematic and the information bits must be decoded from the encoded vector, which is not desirable for our fault-tolerant approach due to the further complication and

delay that it adds to the operation. However, these codes are cyclic codes.

We used the procedure to convert the cyclic generator matrices to systematic generator matrices for all the EG-LDPC codes under consideration shown in Fig.3. The encoded vector consists of information bits followed by parity bits, where each parity bit is simply an inner product of information vector and a column of X, from $G=[I:X]$ note the identity matrix in the left columns.

$$\begin{array}{c}
 c_0 \ c_1 \ c_2 \ c_3 \ c_4 \ c_5 \ c_6 \ c_7 \ c_8 \ c_9 \ c_{10} \ c_{11} \ c_{12} \ c_{13} \ c_{14} \\
 \begin{array}{l}
 i_0 \\
 i_1 \\
 i_2 \\
 i_3 \\
 i_4 \\
 i_5 \\
 i_6
 \end{array}
 \left[\begin{array}{ccccccccccccccc}
 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1
 \end{array} \right]
 \end{array}$$

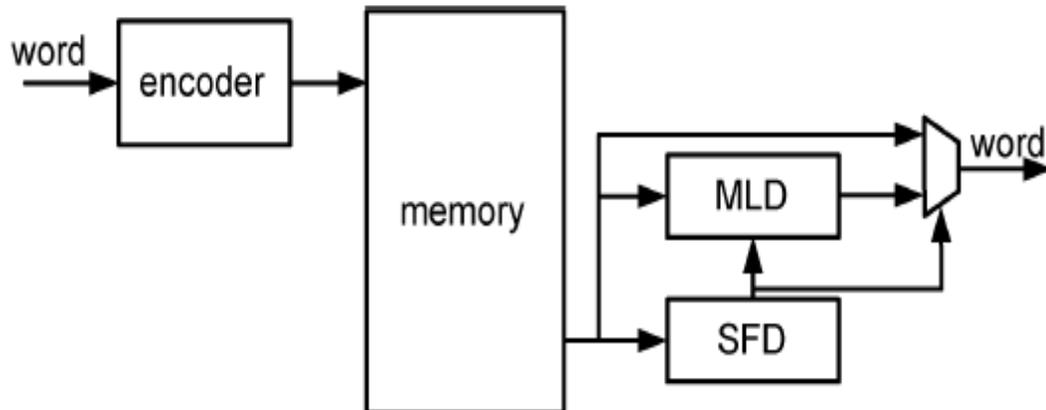
I

X

Fig. 3. Generator matrix for the (15, 7, 5) EG-LDPC in systematic format;

2.1 PLAIN MLD WITH SYNDROME FAULT DETECTOR (SFD)

The SFD is an XOR matrix that calculates the syndrome based on the parity check matrix. Each parity bit results in a syndrome equation.

**Fig: 4. Schematic of an ML with SFD**

Therefore, the complexity of the syndrome calculator increases with the size of the code. A faulty codeword is detected when at least one of the syndrome bits is “1.” This triggers the MLD to start the decoding, as explained before. On the other hand, if the codeword is error-free, it is forwarded directly to the output, thus saving the correction cycles. In this way, the performance is improved in exchange of an additional module in the memory system: a matrix of XOR gates to resolve the parity check matrix, where each check bit results into a syndrome equation. This finally results in a quite complex module, with a large amount of additional hardware and powerconsumption in the system.

III. PROPOSED SYSTEM

3.1 MAJORITY LOGIC DETECTOR/ DECODER (MLDD)

If errors can be detected in the first few iterations of MLD, thenwhenever no errors are detected in those iterations, the decoding canbe stopped without completing the rest of the iterations. In the first iteration, errors will be detected when at least one of the check equationsis affected by an odd number of bits in error. In the second iteration, as bits are cyclically shifted by one position, errors will affect otherequations such that some errors undetected in the first iteration will bedetected. As iterations advance, all detectable errors will eventually bedetected.

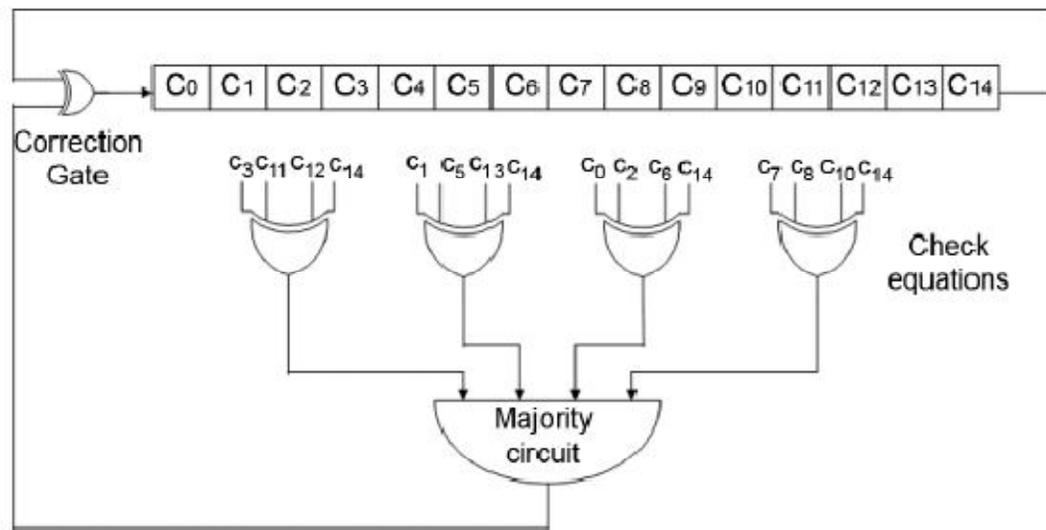


Fig: 5 serial one-step majority logic decoder for the(15,7)EG-LDPC code

ADVANTAGES

1. In the proposed approach, only the first three iterations are used to detect errors, thereby achieving a large speed increase when N is large. In [10] it was shown that for DS-LDPC codes, all error combinations of up to five errors can be detected in the first three iterations.
2. Errors affecting more than five bits were detected with a probability very close to one.
3. The probability of undetected errors was also found to decrease as the code block length increased. For a billion error patterns only a few errors (or sometimes none) were undetected. This may be sufficient for some applications.
4. Another advantage of the proposed method is that it requires very little additional circuitry as the decoding circuitry is also used for error detection. The additional area required to implement the scheme was only around 1% for large word sizes.

3.2 CORRECTOR

One-step majority-logic correction is a fast and relatively compact error-correcting technique. There is a limited class of ECCs that are one-step-majority correctable which include type-I two-dimensional EG-LDPC.

ONE-STEP MAJORITY-LOGIC CORRECTOR

One-step majority logic correction is the procedure that identifies the correct value of each bit in the codeword directly from the received codeword; this is in contrast to the general message-passing error correction strategy which may demand multiple iterations of error diagnosis and trial correction. Avoiding iteration makes the correction latency both small and deterministic. This technique can be implemented serially to provide a compact implementation or in parallel to minimize correction latency. This method consists of two parts:

- 1) Generating a specific set of linear sums of the received vector bits
- 2) Finding the majority value of the computed linear sums.

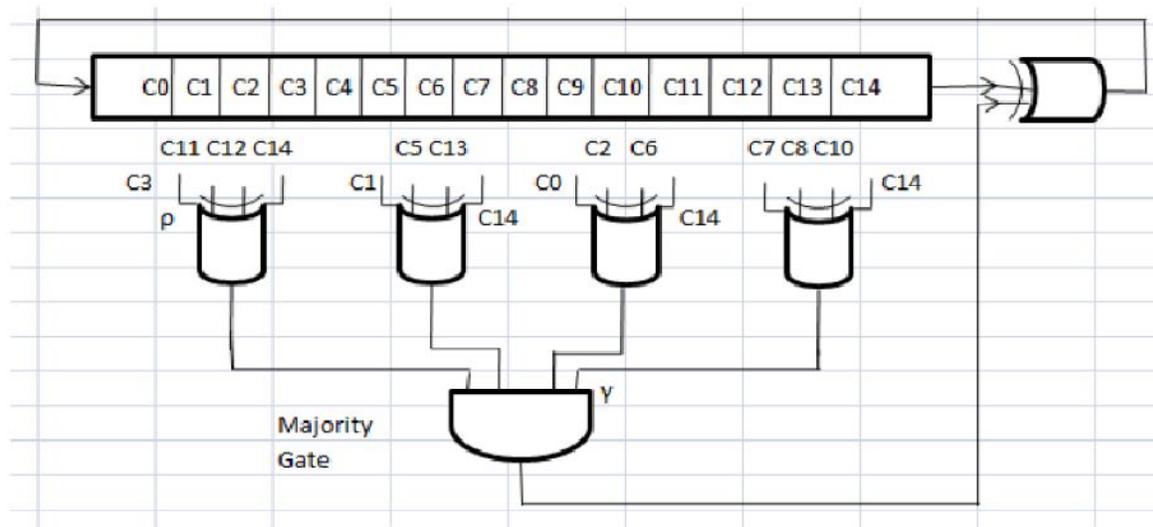


Fig: 6 Serial one-step majority logic corrector structure to correct last bit (bit 14th) of 15-bit (15, 7, 5) EG-LDPC code.

The majority value indicates the correctness of the codebit under consideration; if the majority value is 1, the bit is inverted, otherwise it is kept unchanged. The circuit implementing a serial one-step majority logic corrector for (15, 7, 5) EG-LDPC code is shown in Fig 6

3.3 MAJORITY LOGIC DETECTOR/DECODING ALGORITHM

The Modified MLDD algorithm performs the decoding as in the MLDD with some modifications. Modified MLDD algorithm requires additional logic compared to the MLDD algorithm. The corrections are performed during the first n iterations. A counter is used to determine if there have been more than t errors in those iterations and based on the result the corrected or the original register is sent to the output. If the majority gate detects any error in codeword the iterations take place depends upon the length of the codeword's.

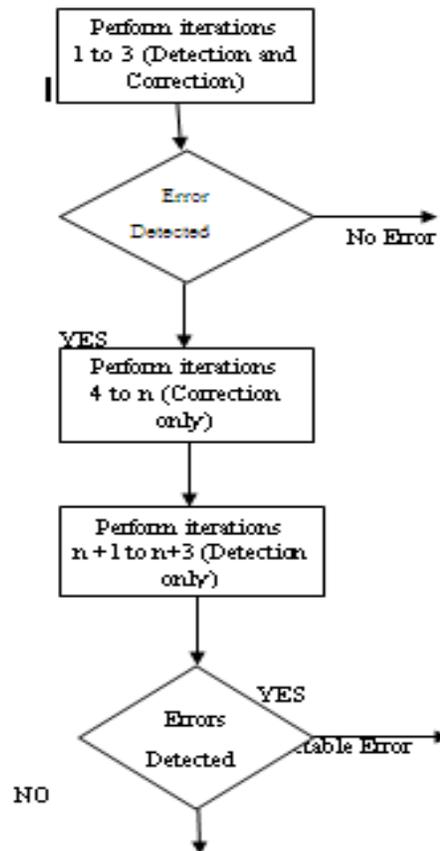


Fig. 7. Flow diagram of the MLDD algorithm.

Modified MLDD detect more than five bit-flips and high efficiency compare to Majority logic decoder. The control unit manages the detection process. It uses a counter that counts up to three, which distinguishes the first three iterations of the ML decoding. Data bits stay in memory for a number of cycles and, during this period, each memory bit can be upset by a transient fault with certain probability. Therefore, transient errors accumulate in the memory words over time. The process stops after three iteration if the codeword length less than ten and six iteration for codeword less than twenty, if the codeword greater than 20 then nine iterations are performed.

In order to avoid accumulation of too many errors in any memory word that surpasses the code correction capability, the system must perform memory scrubbing. Memory scrubbing is the process of periodically reading memory words from the memory, correcting any potential errors, and writing them back into the memory.

IV. CONCLUSION

In this brief, the detection of errors during the first iterations of serial one step Majority Logic Decoding of EG-LDPC codes has been studied. The objective was to reduce the decoding time by stopping the decoding process when no errors are detected. The simulation results show that all tested combinations of errors affecting up to four bits are detected in the first three iterations of decoding. These results extend the ones recently presented for DS-LDPC codes, making the modified one step majority logic decoding more attractive for memory applications. The designer now has a larger choice of word lengths and error correction capabilities. Future work includes extending the theoretical analysis to the cases of three



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

and four errors. More generally, determining the required number of iterations to detect errors affecting a given number of bits seems to be an interesting problem. A general solution to that problem would enable a fine-grained tradeoff between decoding time and error detection capability.

REFERENCES

- [1] R. C. Baumann, "Radiation-induced soft errors in advanced semiconductor technologies," IEEE Trans. Device Mater. Reliab., vol. 5, no. 3, pp. 301–316, Sep. 2005.
- [2] M. A. Bajura, Y. Boulghassoul, R. Naseer, S. DasGupta, A. F. Witulski, J. Sondeen, S. D. Stansberry, J. Draper, L. W. Massengill, and J. N. Damoulakis, "Models and algorithmic limits for an ECC-based approach to hardening sub-100-nm SRAMs," IEEE Trans. Nucl. Sci., vol. 54, no. 4, pp. 935–945, Aug. 2007.
- [3] R. Naseer and J. Draper, "DEC ECC design to improve memory reliability in sub-100 nm technologies," Proc. IEEE ICECS, pp. 586–589, 2008.
- [4] S. Ghosh and P. D. Lincoln, "Dynamic low-density parity check codes for fault-tolerant nano-scale memory," presented at the Foundations of Nanoscience (FNANO), Snowbird, Utah, 2007.
- [5] S. Ghosh and P. D. Lincoln, "Low-density parity check codes for error correction in nanoscale memory," SRI Computer Science Lab., Menlo Park, CA, Tech. Rep. CSL-0703, 2007.
- [6] H. Naeimi and A. DeHon, "Fault secure encoder and decoder for memory applications," in Proc. IEEE Int. Symp. Defect Fault Toler. VLSI Syst., 2007, pp. 409–417.
- [7] B. Vasic and S. K. Chilappagari, "An information theoretical framework for analysis and design of nanoscale fault-tolerant memories based on low-density parity-check codes," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 54, no. 11, pp. 2438–2446, Nov. 2007.