

# FPGA Implementation of Bose Chaudhuri Hocquenghem Code (BCH) Encoder and Decoder for Multiple Error Correction Control

Gnana Prakash<sup>1</sup>, M.Muthamizhan<sup>2</sup>PG Student, Dept. of ECE, Sri Venkateswara College of Engineering and Technology, Thiruvallur, India<sup>1</sup>Associate Professor, Dept. of ECE, Sri Venkateswara College of Engineering and Technology, Thiruvallur., India<sup>2</sup>

**ABSTRACT:** Reduction of delay is a main concern in VLSI (Very Large Scale Integration), throughput of the CODEC is effectively increased. A (15, 7) BCH (Bose ChaudhuriHocquenghem Code) Encoder and Decoder for text message is implemented using Verilog HDL. BCH can corrected double error in any position of 15 bit codeword. Initially each character in a text message is converted into binary data of 7 bits. This 7 bit is encoded into 15 bit codeword. The corrected data is converted into an ASCII character. The decoder is implemented using the Peterson and chine's Search algorithm. Simulation was carried out by using Xilinx simulator and verified results for an arbitrarily chosen message data.

## I. INTRODUCTION

Rapid growth in internet and mobile technology ,exchange of information is common practice. Information may betext,audio,videotc form. Transmission of information through a physical medium or wireless medium ,possibility that data get corrupted this leads to an error in a random only selected locations of a symbol or the entire symbol. To have a reliable communication through a communication channel that has an acceptable Bit Error Rate(BER) and High Signal to Noise Ratio(SNR) error correcting codes are used .These codes are used to detect and correct a specific number of error which may occur during transmission of message over a communication chennal.

There are different types of Error correction codes are used in present digital communication system based on the type of channel noise. few of them are Hamming code ,Low Density Parity check code (LDPC),Bose ChaudhuriHocquenghem code (BCH),Reed Solomon Code (RSC),and Turbo Code(TC).These codes are different from each other in their complexity and implementation .BCH codes are widely used in the area like ,mobile communication, Digital communication, Satellite communication ,Optical and Magnetic storage system and Computer Network etc.

In this work(15,7)BCH encoder and decoder is implemented on Spartan 3E FPGA.For designing the BCH codes, two coding techniques are used .They are systematic codes and Non systematic codes. In case of systematic codes original message  $d(x)$  is as it is in the encoded word  $c(x)$ .where as in case of non –systematic code encoded word  $c(x)$  is obtained by multiplying message  $d(x)$  with generator polynomial  $G(x)$ .

At the transmitter side using encoder circuits binary digits are encoded by appending some extra bits with message bits also know as parity bits. The parity bits and message bits together called as 'codeword'. If error presents in received data within a correction limits,the error will be corrected and original message is retrived.

Digital filters are widely used in signal processing and communication systems. In some cases, the reliability of those systems is critical, and fault tolerant filter implementations are needed. Over the years, many techniques that exploit the filters' structure and properties to achieve fault tolerance have been proposed.

As technology scales, it enables more complex systems that incorporate many filters. In those complex systems, it is common that some of the filters operate in parallel, for example, by applying the same filter to different input signals. Recently, a simple technique that exploits the presence of parallel filters to achieve fault tolerance has been presented. In this brief, that idea is generalized to show that parallel filters can be protected using error correction codes (ECCs) in

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

which each filter is the equivalent of a bit in a traditional ECC. This new scheme allows more efficient protection when the number of parallel filters is large. The technique is evaluated using a case study of parallel finite impulse response filters showing the effectiveness in terms of protection and implementation cost.

FPGA-based designs are more susceptible to single-event upsets (SEUs) compared to ASIC designs, since SEUs in configuration bits of FPGAs result in permanent errors in the mapped design. Moreover, the number of sensitive configuration bits is two orders of magnitude more than user bits in typical FPGA-based circuits. A high-reliable low-cost mitigation technique which can significantly improve the availability of designs mapped into FPGAs. Experimental results show that, using this technique, the availability of an FPGA mapped design can be increased to more than 99%. A low-cost and high-reliable soft error mitigation technique based on checkpointing. A very small auxiliary FPGA is utilized to store checkpoints, compare the checksums, and reconfigure the main FPGA. Experimental as well as analytical results show that the availability of a protected design based on this technique increases to more than 99.6%.

## II. ERROR CONTROL CODING

In recent years there has been an increasing demand for digital transmission and storage systems. This demand has been accelerated by the rapid development and availability of VLSI technology and digital processing. It is frequently the case that a digital system must be fully reliable, as a single error may shutdown the whole system, or cause unacceptable corruption of data, e.g. in a bank account. In situations such as this error control must be employed so that an error may be detected and afterwards corrected. The simplest way of detecting a single error is a parity checksum, which can be implemented using only exclusive-or gates. But in some applications this method is insufficient and a more sophisticated error control strategy must be implemented.

To have a reliable communication through a noisy medium that has an unacceptable bit error rate (BER) so, we need to have Error Correcting Codes (ECC). The error correction is based on mathematical formulas, which are used by Error correcting codes (ECC). Error correction is taken place by adding parity bits to the original message bits during transmission of the data.

Because of the addition of parity bits to message bits makes the size of the original message bits longer. Now this longer message bits is called a word is received by the receiver at destination, and could be decoded to retrieve the original message bits. Error correcting codes are used in most of the digital applications, space and satellite communication and cellular telephone network.

Pioneers of coding theory are Shannon and Hamming who were colleagues at Bell Labs. Hocquenghem in 1959 and independently Bose and Ray-Chaudhuri in 1960 were responsible for a class of codes known as BCH codes. Reed and Solomon followed with a set of cyclic codes, which are BCH codes, but are well-suited for detecting and correcting burst errors and erasures. It was not until almost a decade later when Berlekamp invented a decoding algorithm which was simplified by Massey in 1969. In 1982 the compact disc (CD) was the first mass-produced device that used these error correcting codes.

Multiple error correcting codes can be developed by the method of forming standard arrays, with the required value of H.D.  $> 2t$ ,  $t$ =number of errors in the received vector. More elegant methods however have been developed for  $t$ -error correcting codes, and these have resulted in BCH, RS, Golay, Reed-Muller, Simplex and other codes.

Fortunately, some of these codes are also majority logic decodable and the decoders for them are very simple. So in this project we are encoding the BCH codes by using LFSR and decoding by majority logic decoders and Meggitt decoder.

The BOSE-CHAUDHURI-HOCQUENGHEM (BCH) codes, discovered in 1959-60, are a class of cyclic codes with powerful error-correcting properties and well-known implementation algorithms.

BCH (binary) codes may also be considered as a binary group code, where the necessary and sufficient conditions to be satisfied are:

(a) For a  $t$ -error correcting  $(n, k)$  binary group code, an  $(n \times r) = [HT]$  matrix exists, such that any  $2t$  row vectors of the matrix are mutually independent,  $(r = n - k)$ .

(b) For any positive integer's  $m$  and  $t$  ( $t < 2m - 1$ ), a BCH code has the parameters:

Block length  $n = 2^m - 1$

No. Of parity check bits  $r = n - k < m \times t$

Minimum H.D.  $> 2t + 1$

### 3.3.1. ERROR DETECTION AND ERROR CORRECTION

When a message is transmitted or stored it is influenced by interference which can distort the message. Radio transmission can be influenced by noise, multipath propagation or by other transmitters. In different types of storage, apart from noise, there is also interference which is due to damage or contaminant in the storage medium. There are several ways of reducing the interference. However, some interference is too expensive or impossible to remove. One way of doing so is to design the messages in such ways that the receiver can detect if an error has occurred or even possibly correct the error.

This can be achieved by Error – Correcting Coding. In such coding the number of symbols in the source encoded message is increased in a controlled manner, which means that redundancy is introduced.

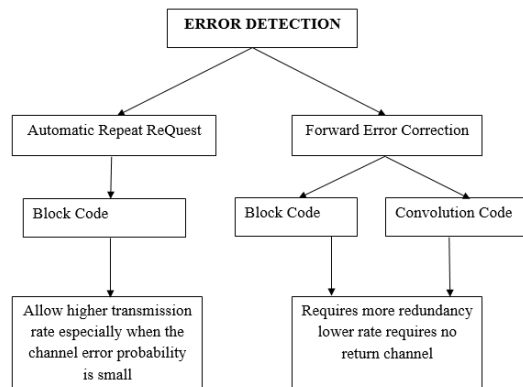
To make error correction possible the symbol errors must be detected. When an error has been detected, the correction can be obtained in the following ways:

- (1) Asking for a repeated transmission of the incorrect codeword (Automatic Repeat Request (ARQ)) from the receiver.
- (2) Using the structure of the error correcting code to correct the error (Forward Error Correction (FEC)).

It is easier to detect an error than it is to correct it. FEC therefore requires a higher number of check bits and a higher transmission rate, given that a certain amount of information has to be transmitted within a certain time and with a certain minimum error probability. The reverse is also true; if the channel offers a certain possible transmission rate, ARQ permits a higher information rate than FEC, especially if the channel has a low error rate.

Another advantage of the FEC is that the transmission is never completely blocked even if the channel quality falls below such low levels that ARQ system would have completely asked for retransmission.

In a system using FEC, the receiver has no real time contact with the transmitter and cannot verify if the data was received correctly. It must make a decision about the received data and do whatever it can to either fix it or declare an alarm. In the other one a convolution operation is applied to the symbol stream. This is called Convolution Coding.



**Fig.3.1 Error detection and correction.**

FEC techniques repair the signal to enhance the quality and accuracy of the received information, improving system performance. Various techniques used for FEC are described in the following sections.

The telecom industry has used FEC codes for more than 20 years to transmit digital data through different transmission media. Claude Shannon first introduced techniques for FEC in 1948. These error-correcting codes compensated for noise and other physical elements to allow for full data recovery. For an efficient digital communication system early detection of errors is crucial in preserving the received data and preventing data corruption. This reliability issue can be addressed Error Detection Automatic Repeat reQuest Forward Error Correction Block code Block Code Convolution Code Allows higher transmission rate especially when the channel error probability is small. Requires more redundancy, Lower rate, Requires no return channel making use of the Error Detection And Correction (EDAC) schemes for concurrent error detection (CED).

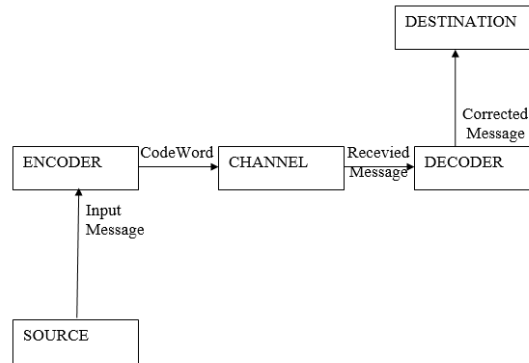
The EDAC schemes employ an algorithm, which expresses the information message, such that any of the introduced error can easily be detected and corrected, based on the redundancy introduced into it. Such a code is said to be e-error detecting, if it can detect any error affecting at most e-bits e.g. parity code, two-rail code, m-out-of-n, Berger ones

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

etc. Similarly it is called e-error correcting, if it can correct e-bit errors e.g. Hamming codes, Single Error Correction Double Error Detection (SEDED) codes, Bose Chaudhuri– Hocquenghem (BCH) Codes, Residue codes, Reed Solomon codes etc. As mentioned earlier both error detection and correction schemes require additional check bits for achieving CED. An implementation of this CED scheme is shown in Fig.3.2



**Fig.3.2 Concurrent error detection implementation**

Here the message generated by the source is passed to the encoder which adds redundant check bits, and turns the message into a codeword. This encoded message is then sent through the channel, where it may be subjected to noise and hence altered. When this message arrives at the decoder of the receiver, it gets decoded to the most likely message. If any error had occurred during its transmission, the error may either get detected and necessary action taken (Error Detection scheme) or the error gets corrected and the operations continue (Error Correction Scheme).

Detection of an error in an error detection scheme usually leads to the stalling of the operation in progress and results in a possible retry of some or all of the past computations.

On the other hand the error correction scheme permits the process to continue uninterrupted, but usually requires higher amount of redundancy than the error detection. Each of these schemes has varied applications, depending on the reliability requirements of the system.

### III. BCH CODE

The Bose, Chaudhuri and Hocquenghem (BCH) codes form a large class of powerful random error-correcting cyclic codes. Binary BCH codes were discovered by Hocquenghem in 1959 and independently by Bose and Chaudhuri in 1960. The cyclic nature on these codes was proved by Peterson in 1960. The decoding algorithms for BCH codes have been developed by Peterson, Gorenstein, Zierler, Chien, Forney, Berlekamp, Massey, Burton and others. A BCH code over  $GF(q)$  of length  $n$  and designed error correcting capability of  $t$  errors is the code having

$$\alpha^{b+1}, \alpha^{b+2}, \alpha^{b+3}, \dots, \alpha^{b+2t}$$

as the zeroes of its generator polynomial, which is of the smallest possible degree, where  $\alpha \in GF(q)$  is the primitive  $n$ th root of unity i.e.  $\alpha^n = 1$ ,  $b$  is a non-negative integer

Special cases:

$b = 0$  Narrow-sense BCH codes.

$n = qs - 1$  Primitive BCH codes.

$s = 1, n = q - 1$  Reed Solomon (RS) codes.

Let  $q(t+i)$  be the minimal polynomial of  $\alpha^{b+i}$ . Then the generator polynomial is:

$$g(x) = \text{LCM}\{\phi(\alpha^{b+1}), \phi(\alpha^{b+2}), \dots, \phi(\alpha^{b+2t})\}$$

Noise is defined as any unwanted disturbance which affects the recovery of information that is stored in or transmitted over a medium. In a digital system, noise manifests itself by causing the bits that represent the information to be in error. To achieve reliable transmission/storage of information, error correcting or detecting means are required.

A simple and an almost intuitive way to achieve this is by the use of a parity bit. A fixed rule is used to generate the parity bit. The application of a rule to generate additional bits from the information bits generated

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

parity bits form a codeword. The set of all possible codeword's is called a code. If even parity is desired, then if an information word has an odd number of ones, a one is chosen as the parity bit. If the information word has an even number of one's then a zero is the parity bit. This parity bit is sent along with the information bits. While recovering the information, if the number of ones in a codeword is odd when an even parity encoding has been done, then an error is detected. This scheme can detect only an odd number of errors. If correction of the errors is also desired then additional parity bits must be generated. The addition of the redundant parity bits leads to a decrease in the rate of transmission of information. Thus, an increase in the reliability causes a decrease in the rate of transmission of information .

## A. Definitions

**Source:** A source randomly generates elements chosen from a finite set of symbols. This set of symbols is known to the destination or the receiver. The order of generation of the symbols is not known to the receiver.

**Message:** The sequence of information symbols generated by the source is called the message. Generally the source is assumed to generate  $k$  symbols in unit time.

**Encoder:** The device which assigns redundancy to information by the application of certain rules, is called the encoder.

The mapping done by the encoder from the  $k$  information symbols to  $n$ ,  $k$  symbols must be one-one onto to allow recovery of information. The mapping process may be viewed as a matrix multiplication of the  $1 \times k$  message matrix with a  $k \times n$  generator matrix or as a polynomial multiplication of the message polynomial and the generator polynomial ( $g(x)$ ). The formed codeword itself may be considered as a polynomial called  $c(x)$ .

Non-systematic encoding:  $c(x) = g(x) \times m(x)$ .

Systematic encoding:  $c(x) = x^{n-k} \times m(x) + b(x)$ , where  $b(x)$  is the remainder obtained by dividing  $x^{n-k} \times m(x)$  by  $g(x)$ . Here as shown in Fig.4.1, a code word is divided into two parts, the unaltered message part of  $k$  digits and the redundant checking part of  $n - k$  parity-check digits.

Rapid growth in internet and mobile technology, exchange of information is common practice. Information may be text ,audio, video etc form. Transmission of information through a physical medium or wireless medium, possibility that data get corrupted this leads to an error in a random only selected locations of a symbol or the entire symbol. To have a reliable communication through a communication channel that has an acceptable Bit Error Rate (BER) error correcting codes are used .These codes are used to detect and correct a specific number of errors which may occur during transmission of message over a communication channel.

There are different types of Error correction codes are used in present digital communication system based on the type of channel noise. few of them are Hamming code ,Low Density Parity check code (LDPC),Bose ChaudhuriHocquenghem code (BCH),Reed Solomon Code (RSC),and Turbo Code(TC).These codes are different from each other in their complexity and implementation .BCH codes are widely used in the area like ,mobile communication, Digital communication, Satellite communication ,Optical and Magnetic storage system and Computer Network etc.

In this work (15, 7) BCH encoder and decoder is implemented on Spartan 3E FPGA. For designing the BCH codes, two coding techniques are used .They are systematic codes and Non systematic codes. In case of systematic codes original message  $d(x)$  is as it is in the encoded word  $c(x)$ .

where as in case of non –systematic code encoded word  $c(x)$  is obtained by multiplying message  $d(x)$  with generator polynomial  $G(x)$ .Hence message data will not be same in the encoded code word .

At the transmitter side using encoder circuits binary digits are encoded by appending some extra bits with message bits also know as parity bits.

At the Receiver end codeword will be received and error detection and correction process is applied. This process is known as decoding. If error presents in received data within a correction limits, the error will be corrected and original message is retrieved.

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

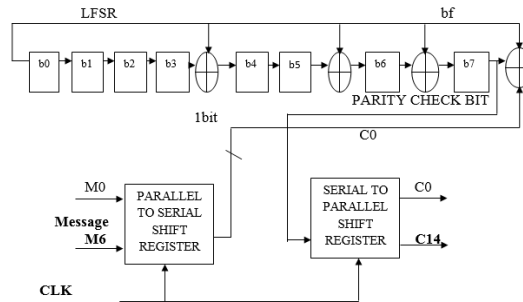


Fig.5.1 Block diagram of (15, 7) BCH encoder.

The output of parallel to serial shift register will be sent to (15, 7) BCH Encoder module. Using these message bits parity bits are computed and sent to serial to parallel shift register. These parity bits are appended to original message bits to obtain 15bit encoded data. This entire encoding process requires 15clock cycles.

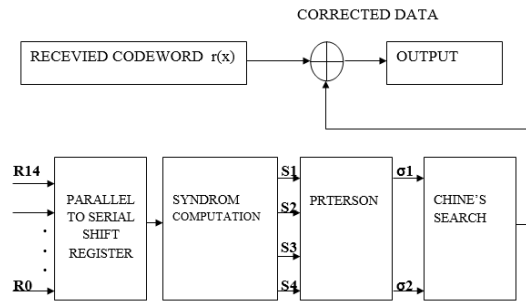


Fig.5.2 Block diagram of (15, 7) BCH decoder.

The syndrome is the receive sequence multiplied by the transposed parity check matrix H.

$$S(x) = r(x) * HT$$

The syndrome is a (n-k)-tuple that has a one to one correspondence with the correctable error patterns. The syndrome depends only on the error pattern and is independent of the transmitted codeword. Most codes do not use all of the redundancy that has been added for error correction.

The only two codes known to do this are Hamming (2m- 1, 2m- m - 1) and Golay codes. These codes are called perfect codes.

## IV. RESULTS



Fig.6.2 Simulation result for encoder.



## International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

Fig.6.1 shows the simulation result of encoder. The reset and load pin is high encoded data or received vector  $r(x)$  is loaded as input to encoder and all other intermediated signal are set to zero.

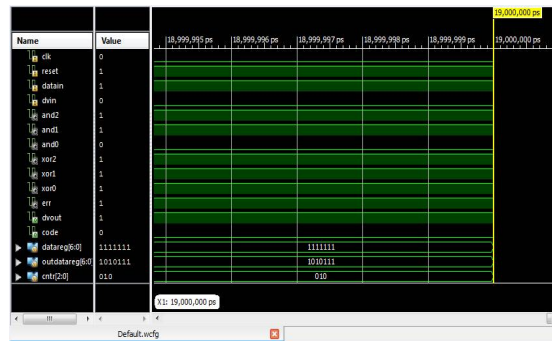


Fig.6.2 Simulation result for decoder.

Fig.6.2 shows the simulation result of decoder. The reset and lode pin is high received vector  $r(x)$  is loaded as input to decoder and all other intermediated signal are set to zero.

### V. CONCLUSION

Hamming filtering is based on applying ECC's to the parallel filter outputs to detected and correct error. In which at a single cycle it accepts one bit as an input it can detect two error and clear one bit error through which there will be an increase in the delay ,therefore throughput of the system is reduced drastically. Hence by analyzing these factor ,To enhance the performance of area and delay , BCH code is introduced at a single cycle it can accept n-bit as input and two error can be detected and corrected by using Peterson's algorithm and chine's search algorithm. Experimental results of Hamming filter shows that the performance is satisfactory, hence in the proposed approach of BCH code the result will be enhanced to reduced the area and delay.

A (15, 7) BCH Encoder and Decoder are more advantageous over than other codes; according to speed requirement.BCH can correct the error at the receiver side when the original data corrupt by the noise. The decoder is implemented using the Peterson and chine's search algorithm. Simulation was carried out by using Xilinx simulator and verified results for an arbitrarily chosen message data. Also design of both encoder and decoder successfully implemented on FPGA hardware.

Synthesis was successfully done by using the cadence RTL compiler, area and delay is estimated.

### REFERENCES

- Asadi .G and Tahoori .M.B , "Soft Error Rate Estimation and Mitigation for SRAM-Based FPGAs," Proc. of the13thACM Intl. Symp. On Field-Programmable Gate Arrays (FPGA), Monterey, CA, Feb. 2005.
- BoovigaPriyadharsini.S, Saranya.T, Sneha.S, Suganya.C and Manjula.G "Highly Reliable Parallel Filter Design Based On Reduced Precision Error Correction Codes" in IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)Volume 5, Issue 1, Ver. III (Jan - Feb. 2015).
- Eltayeb S. Abuelyaman and Abdul-Aziz S. Al-Schibani "Optimization of the Hamming Code for Error Prone Media" in IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.3, March 2008.
- Ghazanfar-HosseinAsadi, Mehdi BaradaranTahoori "Soft Error Mitigation for SRAM-Based FPGAs" Proc. of the13thACM Intl. Symp. On Field-Programmable Gate Arrays (FPGA), Monterey, CA, Feb. 2005.
- Gao. Z, Yang. W, Chen. X, Zhao. M, and J. Wang, "Fault missing rate analysis of the arithmetic residue codes based fault-tolerant FIR filter design," in Proc. IEEE IOLTS, Jun. 2012, pp. 130–133.
- Huang. Y.H, "High-efficiency soft-error-tolerant digital signal processing using fine-grain sub word-detection processing," IEEE Trans. Very Large Scale Integer. (VLSI) Syst., vol. 18, no. 2, pp. 291–304, Feb. 2010.
- Hitana. T and Deb. A.K, "Bridging concurrent and non-concurrent error detection in FIR filters," in Proc. Nor chip Conf., 2004, pp. 75–78.
- Hamming. R.W, "Error correcting and error detecting codes," Bell Syst. Tech. J., vol. 29, pp. 147–160, Apr. 1950.
- Lin. S and Costello. D.J, Error Control Coding, 2nd ed. Englewood Cliffs, NJ, and USA: Prentice-Hall. 2004.
- Nicolas. M, "Design for soft error mitigation," IEEE Trans. Device Mater. Rel., vol. 5, no. 3, pp. 405–418, Sep. 2005.
- Oppenheim. A.V and Schaffer. R.W, Discrete Time Signal Processing. Upper Saddle River, NJ, USA: Prentice-Hall 1999.
- Pedro Reviriego, Chris J. Bleakley, and Juan Antonio Maestro "Structural DMR: A Technique for Implementation of Soft-Error-Tolerant FIR Filters" in IEEE transactions on circuits and systems—ii: express briefs, vol. 58, no. 8, august 2011.

# International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 3, March 2016**

13. Pontarelli. S, Cardarilli. G.C, Re. M, and Salsano. A, "Totally fault tolerant RNS based FIR filters," in Proc. IEEE IOLTS, Jul.2008, pp. 192–194.
14. Reddy. A and Banarjee. P "Algorithm-based fault detection for signal processing applications," IEEE Trans. Compute., vol. 39, no. 10, pp. 1304–1308, Oct. 1990.
15. Shim. B and Shanbhag. N, "Energy-efficient soft error-tolerant digital signal processing," IEEE Trans. Very Large Scale Integrated. (VLSI) Syst., vol. 14, no. 4, pp. 336–348, Apr. 2006.