

Enhanced Fault Tolerant Parallel FFTs Using Parseval Checks and Error Correction Codes: A Study

Raju Katru, Kandukuri Shobha, Apuri Manasa

^{1,2,3} Assistant professor. Dept. of ECE, Ashoka Institute of Engineering and Technology, Hyderabad, Telanagana, India

Abstract: Reliability of mission critical systems is a weighty criterion for any system and is achieved by suitable fault detection techniques. Digital filters are most often integrated in modern digital signal processing systems for the processing of signals. In few utilizations, a possible activity is that use of algorithmic based fault tolerance (ABFT) approaches that are endeavor and action of recursive equalities in identify as well as rectify faults. Communications and Signal processing utilities are more compatible to algorithmic based fault tolerance. A few key building blocks in devices are FFTs. Numerous secured techniques recommended for recognize as well as rectify faults in FFTs. Amidst of techniques, most probable utilization of Sum of squares or parseval check is the most generally glorious. At a recent time, one method employs that put into effect of fault tolerance projected over similar filters. During irregularity, the system first implemented for lookout Fast Fourier Transforms.

Index Terms: Fast Fourier Transforms, Error Correction Codes, Algorithmic Based Fault Tolerance, Soft errors

I. INTRODUCTION

Electronic circuits are increasingly present in automotive, medical, and space applications where reliability is critical. In those applications, the circuits have to provide some degree of fault tolerance. This need is further increased by the intrinsic reliability challenges of advanced CMOS technologies that include, e.g., manufacturing variations and soft errors. A number of techniques can be used to protect a circuit from errors. Those range from modifications in the manufacturing process of the circuits to reduce the number of errors to adding redundancy at the logic or system level to ensure that errors do not affect the system functionality [1].

To add redundancy, a general technique known as triple modular redundancy (TMR) can be used. The TMR, which triplicates the design and adds voting logic

to correct errors, is commonly used. However, it more than triples the area and power of the circuit, something that may not be acceptable in some applications. When the circuit to be protected has algorithmic or structural properties, a better option can be to exploit those properties to implement fault tolerance. One example is signal processing circuits for which specific techniques have been proposed over the years [2]. Digital filters are one of the most commonly used signal processing circuits and several techniques have been proposed to protect them from errors. Most of them have focused on finite-impulse response (FIR) filters. For example, in [3], the use of reduced precision replicas was proposed to reduce the cost of implementing modular redundancy in FIR filters. In [4], a relationship between the memory elements of an FIR filter and the input sequence was used to detect errors. Other schemes have exploited the FIR properties at a word level to also achieve fault tolerance [5]. The use of residue number systems [6] and arithmetic codes [7] has also been proposed to protect filters. Finally, the use of different implementation structures of the FIR filters to correct errors with only one redundant module has also been proposed [8]. In all the techniques mentioned so far, the protection of a single filter is considered. However, it is increasingly common to find systems in which several filters operate in parallel. This is the case in filter banks [9] and in many modern communication systems [10]. For those systems, the protection of the filters can be addressed at a higher level by considering the parallel filters as the block to be protected. This idea was explored in [11], where two parallel filters with the same response that processed different input signals were considered. It was shown that with only one redundant copy, single error correction can be implemented. Therefore, a significant cost reduction compared with TMR was obtained. In this brief, a general scheme to protect parallel filters is presented. As in [11], parallel filters with the same response that process different input signals are considered. The new approach is based on the application of error correction

codes (ECCs) using each of the filter outputs as the equivalent of a bit in an ECC codeword.

II. BACKGROUND WORK

[12] In this paper, Triple Modular Redundancy (TMR) and Hamming Codes have been utilized to secure distinctive circuits against Single Event Upsets (SEUs). In this paper, the utilization of a Novel Hamming approach on FIR Filters is examined and actualized to give low many-sided quality, decrease deferral and region productive security methods for higher bits information.

A novel Hamming code is proposed in this paper, to build the effectiveness of higher information bits. In this paper, they have proposed a system used to illustrate, how the parcel of overhead because of scattering the repetition bits, their resulting expulsion, cushion to cushion postpone in the decoder and utilization of aggregate range of FIR channel for higher bits are lessened. These depend on the novel hamming code implementation in the FIR channel rather than traditional hamming code used to ensure FIR channel. In this plan Hamming code utilized for transmission of 7-bit information thing.

[13] In this paper, the outline of a FIR channel with self-checking abilities in view of the buildup checking is dissected. Normally the arrangement of deposits used to check the consistency of the consequences of the FIR channel are based on theoretic contemplations about the dynamic range accessible with a picked set of buildups, the mathematical attributes of the blunders caused by a blame and on the normal for the channel execution.

This investigation is regularly hard to perform and to acquire adequate blame scope the arrangement of picked buildups is overestimated. Acquired outcome and thusly requires that. Instead, in this paper they have demonstrated how utilizing a thorough blame infusion crusades permits to proficiently choose the best arrangement of buildups. Test comes about originating from blame infusion crusades on a 16 taps FIR channel exhibited that by observing the happened blunders and the location modules relating to various buildup has been conceivable to lessen the quantity of discovery module, while paying a little decrease of the level of SEUs that can be distinguished. Paired rationale rules the equipment execution of DSP frameworks.

[14] In this paper they have proposed engineering for the execution of blame-tolerant calculation inside a high throughput multirate equalizer for a deviated remote LAN. The range overhead is limited by abusing the mathematical structure of the Modulus Replication Residue Number System (MRRNS). They had exhibited that for our framework the territory cost to redress a blame in a solitary computational. The protection of parallel filters was done using Error Correction Codes basically hamming code channel is 82.7%. Adaptation to internal failure inside MRRNS design is executed through the expansion of repetitive channels. This paper has introduced a nitty gritty investigation of the cost of actualizing single blame rectification capacity in a FIR channel utilizing the MRRNS.

Table I: Relation between information bits and parity bits.

Information Bits	Parity Bits
4	3
8	4
12	5
27	6

Hamming codes are mainly used to locate whether any transmitted bit is in error and to correct it, so that error free bits are received at the receiver. To protect information bits to be transmitted from errors Hamming codes transmit some number of parity bits along with the information bits. The number of parity bits to be added is based on the Hamming rule

$$r + p + 1 \geq 2^p$$

So according to these observations to protect four information bits from errors three parity bits have to be added. It is explained in Table 1. With the same concept of hamming codes erroneous outputs and faulty filter can be corrected.

Table II: Relation between Filters to be protected and filters added as redundant filters for Fault tolerance

Filters to be protected	Redundant Filters
4	2
8	2
12	2
27	2

III. PROPOSED FRAMEWORK

The aim of error tolerant design is to protect parallel FFTs from errors. Various schemes have been proposed for error detection and correction in FFTs. One of the basic and simple methods is error correction using hamming codes.

Unlike parity code which can detect only odd bit error, the hamming code can detect two bit errors and correct one error. Similar to other error correction codes, hamming codes also utilizes the parity bit which is generated for the corresponding input sequence for detecting errors [14]. It achieves higher code rate with minimum distance of three. The number of parity bits depends on the total number of data bits.

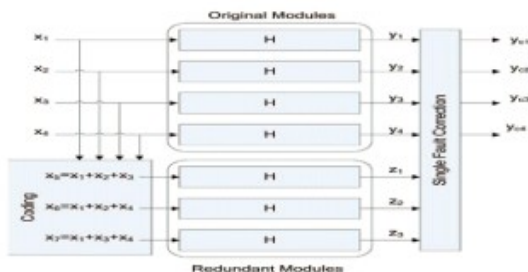


Fig.1 ECC-Based Scheme for Four Filters and a Hammingcode

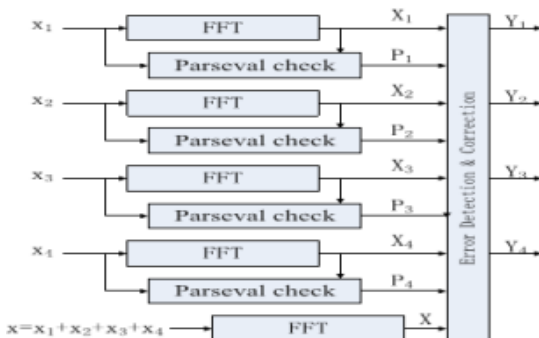


Fig. 2 Parity-SOS (first technique) Fault-Tolerant Parallel FFTs.

The place to begin for our work is that the protection theme based on the utilization of ECCs that was for digital filters. This theme is shown in Fig.1. In this example, a straightforward single error correction playacting code is employed. The initial system consists of 4 FFT modules and 3 redundant modules is value-added to sight and correct errors. The inputs to the 3 redundant modules are unit linear combos of the inputs and that they are unit used to check linear combos of the outputs. For example, the input to the primary redundant module is

$$x_5 = x_1 + x_2 + x_3.$$

And since the DFT is a linear operation, its output z_5 can be used to check that

$$Z_5 = Z_1 + Z_2 + Z_3.$$

This will be denoted as c_1 check. The same reasoning applies to the other two redundant modules that will provide checks c_2 and c_3 . For example, for an error affecting z_1 , this can be done as follows:

$$Z_1 C[n] = Z_5[n] - Z_2[n] - Z_3[n].$$

Similar correction equations can be used to correct errors on the other modules. More advanced ECCs can be used to correct errors on multiple modules if that is needed in a given application. For example, to protect four FFTs, three redundant FFTs are needed, but to protect eleven, the number of redundant FFTs is only four. This shows how the overhead decreases with the number of FFTs.

$$XIC = X - X_2 - X_3 - X_4.$$

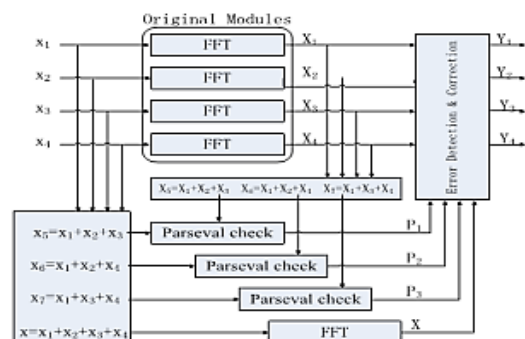


Fig. 3 Parity-SOS-ECC (second technique) Fault-Tolerant Parallel FFTs.

Another possibility to combine the SOS check and the ECC approach is instead of using an SOS check per

FFT, use an ECC for the SOS checks. Then as in the parity-SOS scheme, an additional parity FFT is used to correct the errors. This second technique is shown in Figure 3

The main benefit over the first parity SOS scheme is to reduce the number of SOS checks needed. The error location process is the same as for the ECC scheme in Figure.1 and correction is as in the parity-SOS scheme. In the following, this scheme will be referred to as parity-SOS-ECC (or second proposed technique)

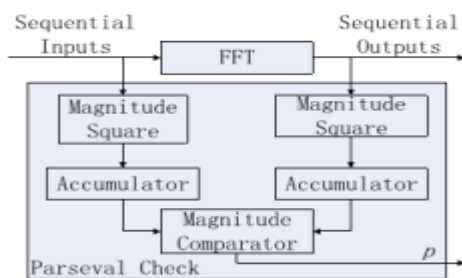


Fig. 4 Implementation of the SOS check

Results and discussion mainly includes the behavioural simulation and RTL schematic implementation of the design. RTL schematic describes the logic utilization in a FPGA.



Fig.5 Input Output Pin Diagram of Proposed Scheme Using Xilinx ISE



Fig.6 RTL Schematic of Proposed scheme Using Xilinx ISE

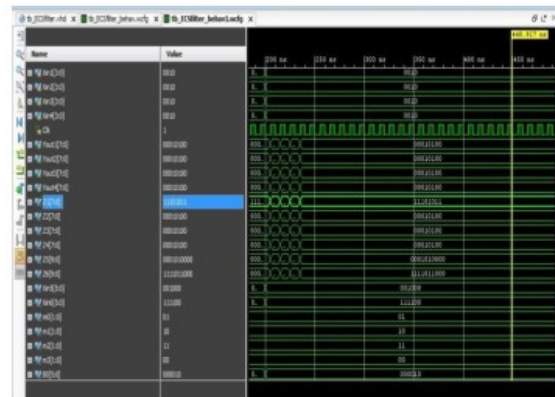


Fig. 7 Behavioral Simulation of Parallel Filters with Fault Injected at Z1 Using Xilinx ISE.

IV. CONCLUSION

Detecting and correcting errors like imperative consistency are troublesome in signal process that will increase the utilization of fault tolerant implementation. The previously proposed technique was based on the use of Error Correction Codes (ECCs). This method considers each filter as a bit in the ECC. The proposed scheme beats the ECC technique (similar fault tolerant capability with lower cost). Therefore, the proposed scheme can be useful to implement fault tolerant parallel filters. Proposed is a part economical technique to discover and correct single errors. The approach is based on applying SOS-ECC check to the parallel FFT outputs to discover and proper errors. The SOS checks are unit accustomed to discover and find the errors and an easy parity FFT is employed for correction.

REFERENCES

[1] M. Nicolaidis, Fault Tolerant Parallel FFTs Using Error Correction Codes and Parseval Checks, IEEE transactions on very large scale integration (VLSI) systems, February 26, 2015.

[2] R. Baumann, —Soft errors in advanced computer systems, IEEE Des. Test Computer., vol. 22, no. 3, pp. 258–266, May/June 2005.

[3] M. Nicolaidis, —Design for soft error mitigation, IEEE Trans. Device Mater. Rel., vol. 5, no. 3, pp. 405–418, Sep. 2005.

[4]B. Shim and N. R. Shanbhag, —Energy-efficient softerror-tolerant digital signal processing, IEEE Trans. VeryLarge Scale Integr.(VLSI) Syst., vol. 14, no. 4, pp. 336–348, Apr. 2006.

[5]RiazNaseer, RashedZafarBhatti, Jeff Draper, —Analysisof Soft Error Mitigation Techniques for Register Files inIBM Cu-08 90nm Technology, Information SciencesInstitute University of Southern California Marina Del Rey,CA 90292 USA 2006 IEEE.

[6]Z. Gao et al., —Fault tolerant parallel filters based onerror correction codes, IEEE Trans. Very Large ScaleIntegr. (VLSI) Syst., vol. 23, no. 2, pp. 384–387, Feb. 2015.

[7]Haryono, —Five Modular Redundancy with MitigationTechnique to Recover the Error Module, InternationalJournal of advanced studies in Computer Science andEngineering IJASCSE, Volume 3, Issue 2, 2014.

[8]Pedro Reviriego, Chris J. Bleakley, and Juan AntonioMaestro., —Structural DMR: A Technique forImplementation of Soft-Error-Tolerant FIR Filters,ieeetransactions on circuits and systems—ii: express briefs, vol.58, no. 8, august 2011.

[9]R. E. Lyons W. Vanderkul k., —The Use of TripleModular Redundancy to Improve Computer Reliability,IBM JOURNAL APRIL 1962.

[10]A. L. N. Reddy and P. Banerjee, —Algorithm-basedfault detection for signal processing applications, IEEETrans. Computer., vol. 39, no. 10, pp. 1304– 1308, Oct.1990.

[11]G. L. Stüber, J. R. Barry, S. W. McLaughlin, Y. Li, M.A. Ingram, and T. G. Pratt, —Broadband MIMO-OFDMwireless communications,Proc.IEEE, vol. 92, no. 2, pp.271–294, Feb. 2004.

[12] M. Nicolaidis. 2005, “Design for soft error mitigation,” IEEETransactions in Device Mater. Rel.5(3):405-418.

[13] R. Baumann. 2005, “Soft errors in advanced computer systems,” IEEEDes. Test Comput. 22(3):258-266.

[14] N.Kanekawa, E.H.Ibe, T.Suga and Y. Uematsu. 2010, “Dependability inElectronic Systems: Mitigation

of Hardware Failures, Soft Errors, andElectro-Magnetic Disturbances,” New York, NY, USA: SpringerVerilag.

BIO DATA

Author 1



RajuKatrupresently working as Assistant Professor in.Dept. of ECE, Ashoka Institute of Engineering and Technology, Hyderabad, Telanagana, India.

Co-Author-1



KandukuriShobhapresently working as Assistant Professor in.Dept. of ECE, Ashoka Institute of Engineering and Technology, Hyderabad, Telanagana, India.

Co-Author-2



ApuriManasapresently working as Assistant Professor in.Dept. of ECE, Ashoka Institute of Engineering and Technology, Hyderabad, Telanagana, India.