Microelectronics Reliability 54 (2014) 316–326

Contents lists available at ScienceDirect

Microelectronics Reliability

journal homepage: www.elsevier.com/locate/microrel

A generalized modular redundancy scheme for enhancing fault tolerance of combinational circuits

Aiman H. El-Maleh [a], Feras Chikh Oughali [a,b,*]

[a] Department of Computer Engineering, King Fahd University of Petroleum & Minerals, Dhahran, Saudi Arabia
[b] Center for Communications & Information Technology Research, Research Institute, King Fahd University of Petroleum & Minerals, Dhahran, Saudi Arabia

ARTICLE INFO

Article history:
Received 30 March 2013
Received in revised form 16 July 2013
Accepted 6 September 2013
Available online 29 September 2013

ABSTRACT

Nano-scale devices are continuously shrinking, operating at lower voltages and higher frequencies. This makes them more susceptible to environmental perturbations and distinguished by their high dynamic fault rates. Redundancy techniques are widely used to increase the reliability of combinational logic circuits. In this work, soft error reliability is improved by using such techniques, and based on probability of occurrence for combinations at the outputs of circuits. A generalized modular redundancy scheme to enhance the reliability of combinational circuits is proposed. Additionally, several aspects regarding the application of this scheme are explored. This comprises types of redundant modules, complexity of voters and single versus multiple outputs protection. Also, a methodology for applying the generalized modular redundancy scheme is developed. Reliability analysis for various benchmarks from the LGSynth91 suite shows that the proposed methodology can achieve reliability figures higher than that of triple modular redundancy. In general, significant overhead savings are accomplished in addition to that superior reliability.

1. Introduction

In nanometric technologies, circuits are increasingly sensitive to various kinds of perturbations. The reduced noise margin of these nano-scale devices increases the effect of external fault sources. Moreover, operating at low voltages and high frequencies makes these devices more fragile and sensitive to environmental influences. The soft error rate (SER) produced by these effects may exceed the failure in time (FIT) specifications in various application domains. In such applications, soft-error mitigation schemes should be employed for both memories and logic.

All fault tolerance approaches rely on some sort of redundancy. Otherwise, there will be no way to tell that a device has changed its state into an incorrect one. Many researches have investigated increasing the reliability of circuits using various redundancy schemes [1–5]. Their main concern is to increase reliability while minimizing the inevitable overhead of area, power, or time.

In [6], a generalized reliability model that unifies the notations for various existing fault tolerant models is given. It is shown that existing fault tolerant systems such as those based on N modular redundancy (NMR) as well as static and dynamic systems are particular cases of the given generalized reliability model.

In the work done by Mohanram et al. [1], two soft error rate reduction heuristics were introduced. They are cluster sharing reduction and dominant value reduction. These two reduction procedures are then combined to form the partial error masking scheme. It starts with a triple modular redundancy (TMR) realization for error masking that is first reduced using cluster sharing. The soft error failure rate of the resulting implementation is then estimated along with the area overhead. Dominant value masking is then used to further reduce area overhead. Another similar approach to the dominant value reduction is also proposed by Krishnaswamy et al. in [2]. Their technique increases logic masking at high-impact nodes by exploiting redundancy already present in the circuit as identified by covering relationships among existing nodes.

In [7], the authors proposed a method that selects the best subset among possible redundant architectures. It is built upon the progressive module redundancy technique and the block grading concept. Efficiency is achieved by taking into account grades of blocks with respect to reliability, by adding redundancy progressively and by considering mixed modular redundancy. The idea is to add redundancy first on the blocks that have higher weights, because they contribute to higher reliability improvements, and then on the blocks with lower weights. The authors in [8] suggest that simple replication of micro-architecture modules will no longer suffice, as all replicated modules will have faults. They introduce the concept of history index of correct computation (HICC), where they developed a technique to tolerate the expected flawed nano-

[*] Corresponding author at: Department of Computer Engineering, King Fahd University of Petroleum & Minerals, Dhahran, Saudi Arabia. Tel.: +966 569077842.
E-mail addresses: aimane@kfupm.edu.sa (A.H. El-Maleh), foughali@kfupm.edu.sa (F.C. Oughali).

0026-2714/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.microrel.2013.09.002

chips at run time. The HICC is a measure of a hardware unit's reliability. The HICC module transmits the correct computation based on the history indices of redundant units that implement the identical function. The redundant unit with the highest history index is considered to be the most reliable one, and is selected to transmit its computation.

In [9], two algorithms for the selective assignment of input don't cares (DCs) are proposed to enhance input error resilience. They showed that selective reliability-driven DC assignment can enhance robustness and avoid the high overheads associated with complete reliability-driven DC assignment. In [10], the authors introduced the idea of synthesizing combinational circuits to increase their tolerance for soft errors. Their idea is based on extracting sub-circuits from the original multilevel circuit and re-synthesizing each extracted sub-circuit to increase fault masking. After that, the re-synthesized sub-circuits are merged back to the original circuit.

In this work, we are targeting the reliability issue in the logic based on probabilities of signals and output combinations. We will make use of this information to build up a reliable version from the original circuit, while maintaining the minimum possible area overhead based on a proposed generalized modular redundancy scheme.

The paper is organized as follows. Section 2 introduces the generalized modular redundancy (GMR) concept. In Section 3, we discuss various aspects concerning the application of the GMR scheme. Based on that, the developed methodology of applying GMR to enhance the reliability of combinational circuits is then presented. In Section 4, the fault model and reliability evaluation methodology are presented. Section 5 provides some analyses and evaluations of different aspects about the proposed methodology. Reliability results of various benchmarks are also reported. Finally, Section 6 concludes this work.

2. Generalized modular redundancy

Given a combinational logic circuit with multiple inputs, outputs, and a set of output combinations. Each combination at the output of the circuit has a probability of occurrence. Based on these probabilities, reliability of the logic will be enhanced by protecting those combinations with high probability of occurrence. Reductions in area overhead will be achieved by not protecting combinations with low probability of occurrence.

Based on their probability of occurrence, combinations at the primary outputs of a combinational circuit can be classified into two types: dominant combinations with high probability of occurrence, and those combinations with low probability. When the probability of occurrence for a certain combination is greater than a certain threshold, it is considered as a dominant combination. Other combinations are the ones with low probability of occurrence. Therefore, dominant combinations will be considered for reliability enhancement due to their highly skewed susceptibility to soft errors.

To increase reliability of circuits, extra redundant modules will be introduced to the logic. New combinations now consist of original outputs and the outputs of redundant modules, as shown in Fig. 1. Modules R1 and R2 are redundant modules. As faults appear in the logic, faulty combinations might be observed at the outputs. These faulty combinations have to be identified. Then, correct combinations will be recovered from these faulty ones through a correction logic.

To recover from single errors in protected combinations, their faulty combinations have to be individually identified. The Hamming distance between a protected combination *A*, and its faulty combination is 1. Similarly, the Hamming distance between a protected combination *B* and any of its faulty combinations is also 1. To insure that no two combinations are identical, the Hamming distance between combinations *A* and *B* must be kept at least 3. For the same reason, Hamming distances between protected and unprotected combinations must be at least 2. Finally, no logic sharing is allowed between different outputs, so that no single error can propagate to more than one output. These Hamming distance requirements have been investigated in previous work for enhancing sequential circuits reliability [5]. Original outputs plus outputs of redundant modules will be then fed to correction logic to produce the protected outputs, as shown in Fig. 2. Redundant modules should be carefully selected in order to meet previously stated Hamming distance requirements. The introduction of redundant modules and correction logic does not introduce new combinations in the final output (after the correction logic), otherwise the function of the circuit would no more be the desired one. But of course, we get new intermediate combinations before the correction logic (as inputs to the correction logic).

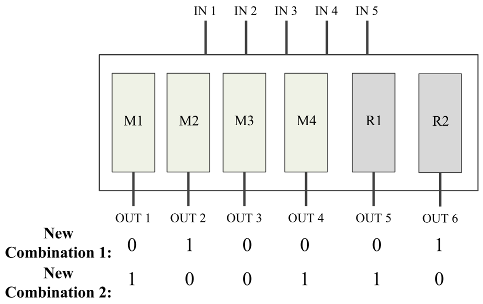

Fig. 1. New intermediate combinations after introducing redundant modules.

2.1. Single output protection

Consider the case of a single output circuit or one module. combinations at the output are the simple combination 0 or combination 1. In some cases, the probability of having one combination is far larger than the probability of having the other. So, the dominant combination will be selected for protection, while the other will not. Assume that logic 0 is dominant. New redundant modules have to be introduced to the logic. By replicating the module one time, the Hamming distance requirements are satisfied. After adding the extra module, combination "0" will become "00" and combination "1" will become "11". The first requirement of having a Hamming distance of 3 between protected combinations is not applicable as there is only one combination to protect. The Hamming distance between the protected combination and the unprotected combination equals to 2. The third requirement is met while synthesizing the circuit by selecting the option of single output optimization to disable logic sharing between different outputs.

If an error hits and alters the output, while the circuit is at combination "00", the resulting faulty combination will be either "01" or "10". In order to obtain the correct output, both original and redundant outputs will be fed to a correction logic. In this case, dominance of combination 0, it turns out that this correction logic is an *AND* gate. Fig. 3(a) demonstrates these findings. The same observations can be found when the dominant combination is "1". However, the correction logic in this case is an *OR* gate, Fig. 3(b). The use of these dominant combinations along with simple correction logic (And, OR) has been observed earlier in the literature, but without this derivation [1].

For the case of protecting the "0" output combination, if "11" was the expected output and it changed to "01" or "10" due to a soft error, correction logic will produce a "0" and the output will be in error. However, as the probability of having "11" combination