Variation Aware Analysis of Bridging Fault Testing

Urban Ingelsson, Bashir M. Al-Hashimi
School of Electronics and Computer Science
University of Southampton, UK.
Email: bui05r@ecs.soton.ac.uk, bmah@ecs.soton.ac.uk

Peter Harrod
ARM Limited
Cambridge, UK.
Email: peter.harrod@arm.com

Abstract

This paper investigates the impact of process variation on test quality with regard to resistive bridging faults. The input logic threshold voltage and gate drives strength parameters are analysed regarding their process variation induced influence on test quality. The impact of process variation on test quality is studied in terms of test escapes and measured by a robustness metric. It is shown that some bridges are sensitive to process variation in terms of logic behaviour, but such variation does not necessarily compromise test quality if the test has high robustness. Experimental results of Monte-Carlo simulation based on recent process variation statistics are presented for ISCAS85 and -89 benchmark circuits, using a 45nm gate library and realistic bridges. The results show that tests generated without consideration of process variation are inadequate in terms of test quality, particularly for small test sets. On the other hand, larger test sets detect more of the logic faults introduced by process variation and have higher test quality.

Keywords: Resistive Bridging Faults, Process Variation, Test Quality, Probability, Static Voltage Testing

1 Introduction

Testing ICs is important because fabricated units may suffer physical defects and process variation. Defects that escape production testing incur extra cost as return of defective products. Resistive bridging fault is a major defect type in deep-submicron ICs and studies have addressed modelling [1], test generation [2] and more recently, multi-Vdd testing [3]. This work is concerned with a fault model that relies on nominal process parameters, the parametric bridging fault model [1]. Its reliance on fixed parameter values raises the question: How does a test that is based on nominal process parameters perform in the presence of process variation? To answer this question, this paper analyses the impact of process variation on bridge behaviour and test quality. In relation to this topic, there has been no reported work apart from [4, 5]. In [4] a new bridging fault model was developed, considering process variation. The fault model is independent of IC parameters, motivated by the need for fast fault simulation. In [5], the fault model was improved and a test generator was presented. Previous work on process variation also include delay fault testing [6] which is outside the scope of this work.

The parametric bridging fault model [1] defines defect coverage (which reflects the test quality) as the amount of covered bridge resistances divided by the amount of resistances that cause malfunction. The fault model in [4, 5] is abstracted from the bridge resistance, which means that it cannot be used analyse how the test quality is affected by process variation, which is the main aim of this paper. Therefore, our approach considers in detail the bridge resistance and parameters such as transistor threshold voltage (VTH), geometry (W,L), gate oxide thickness (TOX), logic threshold voltage (Th) of gate inputs and gate drive strength. To quantify the impact of process variation, we propose a robustness metric for resistive bridging faults which considers the process parameters in a probabilistic manner. This approach enables analysis regarding the probability and the amount of undetected resistance for permutations of process parameter values. Such analysis was not performed in [4, 5]. This paper is structured as follows. Section 2 and 3 describes the impact of process variation on the behaviour of resistive bridges. Section 4 and 5 discusses test escapes and presents a test robustness metric. Section 6 provides experimental results and Section 7 concludes the paper.

2 Background

Bridges are unintended resistive connections between two nets, like net A and B in Figure 1 (resistance R). The defect affects the voltages V(A) and V(B) on the bridged nets when they are driven to opposite logic values. The voltages on the bridged nets depend on the defect resistance [1], as shown by Figure 2. For a 0Ω bridge, V(A)=V(B). For higher values of resistance, V(A) and V(B) diverge. The intended voltages are reached only if the resistance is sufficiently high. Figure 2 shows the logic threshold voltages (Th) for the inputs that are driven by net A and B. Resistance values with the same logic behaviour (BH) are shown...
as grey boxes separated by critical resistances (CR).

The logic behaviour depends on the voltages on the bridged nets and the logic threshold voltage (Th) of driven gate inputs. The logic threshold is the input voltage at which the gate changes its output behaviour (not to confuse with transistor threshold, VTH). Voltage above the logic threshold, is Logic-1, otherwise Logic-0. In Figure 1, net A drives two inputs with logic thresholds Th1 and Th2 and net B drives an input with logic threshold Th3. In Figure 2, V(A)<Th1 in the resistance range [0,CR1nom]. That means that for defect resistances in that range, Th1 will see Logic-0, which is the faulty value. Similarly, Th2 sees faulty Logic-0 for defects in [0,CR2nom] and Th3 sees faulty Logic-1 in [0,CR3nom]. The resistances CR1nom, CR2nom and CR3nom mark changes in the logic behaviour and are called critical resistances [2]. The faulty logic behaviours are BH1={0,0,1} (the logic values seen for Th1, Th2 and Th3) for [0,CR2nom]. BH2={0,1,1} for [CR2nom,CR3nom] and BH3={0,1,0} for [CR3nom,CR1nom]. It should be noted that a test that detects a logic fault covers a range of defect resistance.

3 Analysis

To analyse the behaviour of resistive bridges in the presence of process variation, we have performed SPICE-type simulations. It was found that variation in parameters such as transistor threshold voltage (VTH), transistor geometry (W,L) and gate oxide thickness (TOX) gives rise to variation in gate drive strength (gate output conductance) and logic threshold voltage (Th). These two parameters influence the behaviour of resistive bridges as will be shown next. Besides these two parameters it was found that the bridge behaviour depends on Vdd, bridge resistance and temperature, but those effects are not due to process variation.

We investigated the impact of drive strength shift on resistive bridges by performing Monte-Carlo simulation. The length of the transistors in the gates that drive the bridged nets were varied with a Gaussian distribution (µ=45nm, σ=5nm), to model line edge roughness. We observed a mean of 0.4V and a standard deviation of 0.18V on the voltage on the bridged nets for low bridge resistance values. For increasing values of resistance, there was decreasing variance. Figure 3 shows a parameter permutation, where the voltages on the bridged nets are increased by 0.025V (from 0.4V to 0.425V) for 0 bridge resistance (the left-most edge of the graph in Figure 3) and increased by less and less for increasing values of resistance. The shift is reduced length of the PMOS transistor of the inverter (Figure 1), from 45nm to 44nm. The inverter is stronger in driving high due to the shift, resulting in increased voltage on the bridged nets. This shows that process variation influences gate drive strength and the voltages on the bridged nets. In Figure 3, the voltages are increased, Vnom(A) and Vnom(B) compared to Vdss(A) and Vdss(B) (Drive Strength Shift dss). The logic behaviour includes BH4, which did not occur in the nominal scenario (Figure 2). The faulty logic behaviours are BH2 in [0,CR1dss] and BH4={1,1,1} in [CR1dss,CR3dss]. This shows that drive strength shift may change the logic behaviour of a bridge.

Similarly, we investigated the impact of logic threshold shift on resistive bridges. Monte-Carlo simulation was performed on an AND gate while varying the VTH for the NMOS transistor that is closest to the second input, with a Gaussian distribution (µ=0.471V, σ=0.045V). It was found that the logic threshold voltage had a bell-shaped distribution (µ=0.42V, σ=0.05V). Figure 4 shows how increasing Th2 from 0.42V to 0.455V affects the bridge behaviour. The shift in Th2 is due to a shift in VTH of the NMOS transistor closest to Th2, from 0.471V (nominal value) to 0.59V. This shows that process variation may change the logic threshold voltage of a gate input. Figure 4 shows the logic threshold shifted from Th2nom to Th2lts (Logic Threshold Shift lts). Th2lts>Th1, causing a change in logic behaviour.
behaviour so that logic behaviour BH1 covers the resistances in [0, CR3_{lt}], and there are two new logic behaviours, BH5 (for [CR3_{lt}, CR1_{lt}]) and BH6 (for [CR1_{lt}, CR2_{lt}]). This shows that a shift in logic threshold can change the logic behaviour of a bridge.

4 Test escapes

Test escapes are defects that cause malfunction but are not covered by the test. Possible causes of test escapes are process sensitivities [7], test conditions (temperature, supply voltage [3]) or inaccurate estimations of defect behaviour [8], for example the assumption of fixed process parameters. In this section, test escapes due to process variation are analysed. To put the focus on process variation, other variables (like temperature) are kept constant.

Figure 5 shows process variation induced test escapes for the three scenarios, nominal parameters (Figure 2), drive strength shift (Figure 3) and logic threshold shift (Figure 4). The shaded boxes are the logic behaviours and their resistances. Faulty values are marked ’x’ and fault-free ’v’. Consider the nominal scenario (top row Figure 5). Test generation would expose as much defect resistance as possible by propagating the fault effect through Th1. The reason is that Th1 sees faulty Logic-0 for the logic behaviours BH1, BH2 and BH3, which contains all detectable bridge resistance. Therefore it is assumed that the test detects BH1, BH2, BH3 and BH5. (In Figure 5, L(Th1) is a faulty Logic-0 for these logic behaviours.) That means that in the drive strength shift scenario (middle row Figure 5), bridges with behaviour BH4 are test escapes, because a faulty logic value is exposed only on Th3 and not on Th1. Similarly, in the logic threshold shift scenario (bottom row Figure 5), bridges with behaviour BH6 are escapes, because faulty behaviour is exposed only by Th2. This shows that process variation may cause test escapes for undetected logic faults.

5 Robustness

Test escape can be seen as a reduction in defect coverage. It should be noted that any test escape has a probability - the probability that the drive strengths and logic thresholds are such that the undetected logic fault is possible (not including the probability of a bridge defect). Therefore, defect coverage and probability are two main factors in the test robustness metric. The robustness of a test T is given in Equation 1 for a set of parameter permutations PP, where $P(c)$ is the probability for permutation c. The defect coverage is the amount of covered resistances (CADI) divided by the amount of detectable resistances (GADI) [2]. Full robustness has the value one, as adjusted by the denominator.

\[
\text{Robustness}(T) = \frac{1 - \frac{\sum_{c \in PP} (P(c)) \cdot |CADI(c,T)|}{|GADI(c)|}}{\sum_{c \in PP} P(c)}
\]

(1)

The robustness for a test T and a given bridging fault is, according to Equation 1, determined by the defect coverage and the probability for each item in a set of parameter permutations. The robustness is a probabilistic metric based on the considered permutations. The accuracy of the robustness metric increases with the number of permutations. A method for calculating the defect coverage was presented in [3]. As a side-effect of the method in [3], it identifies undetected faults and corresponding resistance intervals. Thus, it is possible to identify undetected resistance values (test escapes, see Section 4).

Using the circuit in Figure 1, Table 1 shows how robustness is calculated. There are ten parameter permutations c0 to c9. The values for the logic thresholds (columns Th1, Th2 and Th3) and for the drive strength balance (represented by $\min(V(A))$) are taken from Gaussian distributions according to the mean ($\mu$) and standard deviation.

<table>
<thead>
<tr>
<th>c</th>
<th>$P(c)$</th>
<th>DC</th>
<th>$P(c) \cdot DC$</th>
</tr>
</thead>
<tbody>
<tr>
<td>c0</td>
<td>0.440</td>
<td>0.380</td>
<td>0.400</td>
</tr>
<tr>
<td>c1</td>
<td>0.440</td>
<td>0.380</td>
<td>0.425</td>
</tr>
<tr>
<td>c2</td>
<td>0.440</td>
<td>0.380</td>
<td>0.400</td>
</tr>
<tr>
<td>c3</td>
<td>0.430</td>
<td>0.321</td>
<td>0.422</td>
</tr>
<tr>
<td>c4</td>
<td>0.488</td>
<td>0.437</td>
<td>0.456</td>
</tr>
<tr>
<td>c5</td>
<td>0.507</td>
<td>0.431</td>
<td>0.392</td>
</tr>
<tr>
<td>c6</td>
<td>0.387</td>
<td>0.352</td>
<td>0.341</td>
</tr>
<tr>
<td>c7</td>
<td>0.501</td>
<td>0.313</td>
<td>0.319</td>
</tr>
<tr>
<td>c8</td>
<td>0.369</td>
<td>0.441</td>
<td>0.469</td>
</tr>
<tr>
<td>c9</td>
<td>0.394</td>
<td>0.401</td>
<td>0.368</td>
</tr>
</tbody>
</table>

Robustness 0.788

Table 1: Example robustness calculation

![Image](image-url)
(σ) given at the bottom of each column. The mean and standard deviation values are assumed for demonstration but could be obtained by Monte-Carlo simulation as discussed in Section 3. Column P(c) gives the parameter permutation probability, the product of the probability for each value, e.g. \( P(c_0) = P(Th_1 = 0.44) \cdot P(Th_2 = 0.42) \cdot P(Th_3 = 0.38) \cdot P(min(V(A)) = 0.40) = 0.0366 \). The parameter values for permutation c0 are the closest to the mean values, and therefore this permutation has the highest probability (0.0366). Permutation c0 causes the behaviour shown in Figure 2. Column DC is the defect coverage \( CADI(c, T) / GADI(c) \), for test T. These values are assumed for the example of a test that propagates only from Th1 (Figure 1). DC=1 means that there is no test escape. DC<1 means that test escapes occur with the probability shown in column P(c). Column P(c) · DC shows the product of the probability of the permutation (from column P(c)) and the defect coverage for the permutation (from column DC). Summing column P(c) gives the denominator in Equation 1 and summing the column P(c) · DC gives the numerator. The robustness is 0.788. It is less than full (< 1) because, for some parameter permutations, c1, c2, c3, c6, c8 and c9, there are test escapes reducing the defect coverage. The robustness reflects the probability of full defect coverage with the given test. Even though there is test escape for c8, it has little impact on the robustness, because of the low probability (0.0006). Permutation c1 is more probable (0.0281) and reduces the defect coverage, which affects the robustness. Permutation c1 is the scenario of Figure 3 and the defect coverage drop is due to the test escape of BH4 (see Section 4). Permutation c2 is the scenario of Figure 4. The drop in defect coverage is due to BH6.

## 6 Experimental results

We measured the mean and standard deviation for the logic thresholds and the drive strengths for a 45nm gate library [9] by Monte-Carlo simulation based on Table 2. The table holds on variation data for relevant process parameters based on [10, 11] and transistor models from [12]. Vdd is not a process parameter, but is varied by 2.5% (0.022V) around 0.878V for a 0.9V nominal Vdd to account for voltage drop in practise. For line edge roughness, σ=5nm is assumed for L and W. For gate oxide thickness, σ=1.5Å reflects the thickness of one atom layer. For the transistor threshold, 10% standard deviation is for random dopant fluctuations and other effects.

The Monte-Carlo simulation resulted in 11% to 15% standard deviation for the logic thresholds and 5% to 20% standard deviation for the voltage on the bridged nets (depends on drive strengths). Both parameters had a bell-shaped distribution around the mean. This is in-line with [13], where it was observed that the transistor threshold voltage is Gaussian. Based on such observations, we assume the logic threshold voltage and the drive strength to have Gaussian distribution. The probability distributions for logic thresholds and drive strength were used to experiment on benchmark circuits, synthesised for a 45nm gate library [9]. Cadence Encounter was used to extract realistic bridge locations from layout. A defect-aware test generator, based on [3] was used to generate tests assuming nominal values for the process parameters. The robustness is calculated using a fault simulator that calculates the defect coverage, for permutations of the logic threshold and gate drive strength values. We have used 160 permutations for each bridge, 8 permutations for the gate drive strengths times 20 permutations of the logic thresholds, as a trade-off between accuracy and computation time. Two experiments are performed. Experiment 1 investigates the impact of process variation on the logic behaviour of bridges, with regard to test escapes and their impact on defect coverage. Experiment 2 calculates the robustness for tests of benchmark circuits.

### Experiment 1

As shown in Section 3, process variation may cause logic faults to arise that do not occur for nominal values for the process parameters. This section analyses such logic faults for a small ISCAS89 benchmark circuit, S838, with 28 bridges and a test that has 10 test patterns and provides full defect coverage for nominal process parameters. This means that any undetected logic fault is caused by process variation. Figure 6 shows detected logic faults as dark bars and as light bars undetected logic faults in a graph where full height is the total amount of (detected and undetected) logic faults. The height of the dark bars is the logic fault coverage considering process variation. Bridge 3, 6 and 22 are highlighted in Figure 6 for clarity. The total number of logic faults, those occurring for nominal parameters and those that are due to process variation, depend on the bridge location as shown by the numbers on top of each bar. For example, 107 logic faults were encountered while simulating bridge 5, of which 20% are detected by the test. In contrast, bridge 27 has only 6 logic faults and all of them are detected by the test. Where the dark bars are at full height (bridge 23-28) there is full coverage of the logic faults. In contrast, bridge 1 only covers 3% of the logic faults. The remaining 97% of the logic faults (light bar) are not covered by the test, which was generated based on nominal process parameters. It should be noted that the logic fault coverage, as influenced by process variation, depend on the bridges as shown in Figure 6. The results show that process variation
causes logic faults that are not detected by the test. Figure 7 shows the test robustness for each of the 28 bridges. Although bridge 3 and bridge 6 have similar logic fault coverage in Figure 6, it is shown in Figure 7 that bridge 3 has the lowest robustness of all bridges, 0.68, whereas bridge 6 has high robustness, 0.98. This is explained by studying the test escapes for the two bridges as shown in Figure 8. Each dot is a test escape with an amount of undetected bridge resistance and a probability for the corresponding permutation. Both the undetected resistance and the probability of the test escape needs to be high in order to have a high impact on robustness. Dots that are close to the axes have only little impact on robustness.

The amount of undetected resistance for a test escape is the difference between the set of detected bridge resistances (CADI) and the set of bridge resistance that cause malfunction (GADI) and is the cause for reduced defect coverage, see Equation 1. Bridge 3 (left-most graph in Figure 8) has 468 test escapes, of which several have both large amounts of undetected resistance and high probability. These test escapes cause the low robustness. Bridge 6 (middle graph) have 83 test escapes, but they are all of low probability or small amount of defect resistance, compared to bridge 3. That is why the robustness of bridge 6 is high (0.98) in spite of its low logic fault coverage (about 20% in Figure 6). This shows that the test tolerates process variation better for bridge 6 than for bridge 3. Tests with low coverage of process variation induced logic faults may still have high robustness, like bridge 6. Failing to obtain high logic fault coverage does not necessarily mean compromise in test quality. Consider bridge 22, although it has higher logic fault coverage than bridge 6 in Figure 6, it has less robustness (0.91) than bridge 6 (0.98), as can be seen in Figure 7. Bridge 22 has only one logic fault out of 15 that is not covered. In Figure 8 fault causes test escape for 48 out of the 160 permutations. Some of these escapes have high probabilities and large amounts of undetected defect resistance which leads to reduced robustness. This shows that tests with high (but not full) logic fault coverage may still have low robustness, as the case with bridge 22.

To analyse how robustness relates to defect coverage, consider Figure 9 which shows the defect coverage probability distribution of the given test for bridges 3, 6 and 22. The bars represent the probability of permutations (vertical axis) with corresponding defect coverage (horizontal axis). Bridge 3 has nearly 0.48 probability of defect coverage in 95% to 100% and ≈0.22 probability of zero defect coverage, reflected by a robustness of 0.68. Bridge 6 has a high probability of full defect coverage, ≈0.88 (middle graph) and 0.98 robustness. Furthermore, bridge 22, has ≈0.73 probability of full defect coverage (right-most graph) and 0.91 robustness. These results demonstrate that low robustness corresponds to low probability of full defect coverage.

**Experiment 2**

The robustness was calculated for process variation unaware bridge fault tests for ISCAS benchmarks in order to quantify the impact of process variation on test quality. Table 3 shows for each design the number of gates, the number of bridge locations, the number of test patterns and the average robustness for the bridges. For example, S838 has 265 gates, 28 bridge locations and a test with 10 test patterns. The test has the lowest robustness in the table, 0.915
Table 3: Robustness for benchmark tests

<table>
<thead>
<tr>
<th>Design</th>
<th>Gates</th>
<th>Bridges</th>
<th>Test size</th>
<th>Robustness</th>
</tr>
</thead>
<tbody>
<tr>
<td>C432</td>
<td>176</td>
<td>37</td>
<td>30</td>
<td>0.964</td>
</tr>
<tr>
<td>C499</td>
<td>211</td>
<td>108</td>
<td>37</td>
<td>0.961</td>
</tr>
<tr>
<td>C880</td>
<td>323</td>
<td>96</td>
<td>46</td>
<td>0.988</td>
</tr>
<tr>
<td>C1355</td>
<td>307</td>
<td>111</td>
<td>46</td>
<td>0.973</td>
</tr>
<tr>
<td>C1908</td>
<td>278</td>
<td>154</td>
<td>55</td>
<td>0.974</td>
</tr>
<tr>
<td>C2670</td>
<td>500</td>
<td>154</td>
<td>68</td>
<td>0.983</td>
</tr>
<tr>
<td>C3540</td>
<td>1001</td>
<td>695</td>
<td>137</td>
<td>0.997</td>
</tr>
<tr>
<td>C7552</td>
<td>1420</td>
<td>1133</td>
<td>211</td>
<td>0.994</td>
</tr>
<tr>
<td>S641</td>
<td>177</td>
<td>44</td>
<td>19</td>
<td>0.965</td>
</tr>
<tr>
<td>S838</td>
<td>265</td>
<td>28</td>
<td>10</td>
<td>0.915</td>
</tr>
<tr>
<td>S1488</td>
<td>723</td>
<td>875</td>
<td>123</td>
<td>0.997</td>
</tr>
<tr>
<td>S5378</td>
<td>1410</td>
<td>727</td>
<td>167</td>
<td>0.996</td>
</tr>
<tr>
<td>S9234</td>
<td>1062</td>
<td>318</td>
<td>88</td>
<td>0.984</td>
</tr>
</tbody>
</table>

Average robustness 0.976

and is the smallest test. It can be seen in Table 3, that tests with high robustness also have many test patterns, for example C3540, C7552, S1488 and S5378, all with >0.99 robustness and >100 test patterns. This indicates that the majority of process variation induced logic faults are easy to detect in these designs. Where there are many easy-to-detect faults, large test sets contribute to the logic fault coverage by accidental detection (tests generated for the nominal set of logic faults also detect some logic faults that are due to variation). Thus, large test sets and a majority of logic faults due to process variation that are easy to detect, explain the high robustness. In the case of C3540, C7552, S1488 and S5378, the impact of process variation on test quality is minimised by the test sets. Table 3 also shows some small test sets, such as the 10 test patterns for design S838, with low robustness. For small test sets, there is less opportunity for accidental detection. To increase the robustness of such tests, additional test patterns that target the remaining test escapes are required. In the case of S838, such additional test patterns would make the dark bars in Figure 6 higher (increased logic fault coverage) and there would be less dots representing test escapes (Figure 8), because they correspond to undetected logic faults, some of which would be detected by the added test patterns. As a result, the probability of full defect coverage would increase compared to the bars shown in Figure 9.

7 Conclusion

This paper presented the first investigation into the impact of process variation on test quality in the context of resistive bridging faults. By considering two parameters (logic threshold voltage and gate drive strength) that are influenced by process variation, we have shown how the logic behaviour of resistive bridging faults is affected. We proposed a robustness metric that quantifies the impact of process variation on test quality. It was found that some bridges are sensitive to process variation in terms of logic behaviour. However, a test with high robustness does not necessarily have to target all logic faults, but has to target the most probable logic faults and the logic faults that correspond to significant amounts of otherwise undetected defect resistance. Experimental results for synthesised ISCAS designs with realistic bridge locations for a 45nm gate library demonstrate that large test sets are more robust than small test sets. For tests with low robustness, there is a need for additional test patterns targeting test escapes, so that the impact of process variation on bridge defect coverage is minimised. Continuing work involves developing process variation aware generation of such test patterns.

Acknowledgement

We are thankful to S.S. Khursheed and Dr. H.E. Oldham for useful discussions and to EPSRC(UK) for funding this work under grant no. EP/D057663/1.

References