April 1993

UILU-ENG-93-2211
DAC-37

Analog and Digital Circuits

STATISTICAL ESTIMATION OF THE SIGNAL PROBABILITY IN VLSI CIRCUITS

Farid Najm

Coordinated Science Laboratory
College of Engineering
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION
Unclassified

1b. RESTRICTIVE MARKINGS
None

2a. SECURITY CLASSIFICATION AUTHORITY

2b. DECLASSIFICATION / DOWNGRADING SCHEDULE

3. DISTRIBUTION / AVAILABILITY OF REPORT
Approved for public release; distribution unlimited

4. PERFORMING ORGANIZATION REPORT NUMBER(S)
UILU-ENG-93-2211 (DAC-37)

5. MONITORING ORGANIZATION REPORT NUMBER(S)

6a. NAME OF PERFORMING ORGANIZATION
Coordinated Science Lab
University of Illinois

6b. OFFICE SYMBOL *(If applicable)*
N/A

7a. NAME OF MONITORING ORGANIZATION
ECE Dept and CSL

6c. ADDRESS *(City, State, and ZIP Code)*
1308 W Main St
Urbana, IL 61801

7b. ADDRESS *(City, State, and ZIP Code)*
155 Everitt Lab, 1406 W Green St, Urbana
202 CSRL, 1308 W Main St, Urbana

8a. NAME OF FUNDING / SPONSORING ORGANIZATION
ECE Dept & CSL

8b. OFFICE SYMBOL *(If applicable)*

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c. ADDRESS *(City, State, and ZIP Code)*
1406 W Green St, Urbana, IL 61801
1308 W Main St, Urbana, IL 61801

10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.

11. TITLE *(Include Security Classification)*
Statistical Estimation of the Signal Probability in VLSI Circuits

12. PERSONAL AUTHOR(S)
Najm, Farid N.

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Technical	FROM _____ TO _____	93/04/09	15

16. SUPPLEMENTARY NOTATION

17. COSATI CODES

FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
Signal probability VLSI circuits

19. ABSTRACT *(Continue on reverse if necessary and identify by block number)*
(attached)

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS

21. ABSTRACT SECURITY CLASSIFICATION
Unclassified

22a. NAME OF RESPONSIBLE INDIVIDUAL

22b. TELEPHONE *(Include Area Code)*

22c. OFFICE SYMBOL

DD Form 1473, JUN 86 *Previous editions are obsolete.*

The signal probability of a node in a digital circuit is the fraction of time that that node remains at logic 1. The importance of the signal probability concept has been recognized for testability analysis and for power estimation. It is also known that the problem of finding the exact probabilities is $\cal NP$-hard. As a result, all previous work in this area has focused on approximating the signal probability values, while maintaining reasonable execution time. However (as recent review article has observed), there is no existing robust technique for solving this problem. The accuracy of all existing efficient techniques is unpredictable and unreliable, making them unattractive in practice. In this work, we present a new approximate technique for computing the signal probabilities that is based on statistical estimation. A key feature of our approach is that the desired accuracy can be specified up-front, along with a desired measure of confidence. This approach has been implemented in a prototype C program, which we have verified on a large number of test cases. The direct accuracy control is very attractive in practice, boosting designers' confidence in the tool. The method is also quite efficient, solving a 22,000 gate circuit in a little over an hour on a SUN sparc ELC.

Statistical Estimation of the Signal Probability in VLSI Circuits

Farid N. Najm

University of Illinois at Urbana-Champaign
Coordinated Science Laboratory
1308 West Main Street
Urbana, IL 61801

Abstract

The *signal probability* of a node in a digital circuit is the fraction of time that that node remains at logic 1. The importance of the signal probability concept has been recognized for *testability analysis* and for *power estimation*. It is also known that the problem of finding the exact probabilities is $\mathcal{NP}$-hard. As a result, all previous work in this area has focused on approximating the signal probability values, while maintaining reasonable execution time. However (as recent review article has observed), there is no existing robust technique for solving this problem. The accuracy of all existing *efficient* techniques is unpredictable and unreliable, making them unattractive in practice. In this work, we present a new approximate technique for computing the signal probabilities that is based on statistical estimation. A key feature of our approach is that the *desired accuracy can be specified up-front*, along with a desired measure of confidence. This approach has been implemented in a prototype C program, which we have verified on a large number of test cases. The direct accuracy control is very attractive in practice, boosting designers' confidence in the tool. The method is also quite efficient, solving a 22,000 gate circuit in a little over an hour on a SUN sparc ELC.

Submitted to the IEEE Transactions on Computer-Aided Design, 1993.

1. Introduction

Consider a combinational circuit that is part of a larger synchronous sequential circuit. The *signal probability* [1] of a node is defined as the fraction of clock cycles in which the final state of that node is a logic 1. The signal probability is completely determined by the Boolean function implemented at that node, and by the signal probabilities at the primary inputs of the combinational circuit.

The importance of the signal probability concept has been recognized for testability analysis [2–4] and power estimation [5]. In testability analysis, the signal probability of a node is a measure of *controllability*, i.e., of how easy it is to control the logic value at that node from the primary inputs. In power estimation, the signal probability gives the fraction of clock cycles in which a node makes a (power consuming) logic transition.

From a computational complexity standpoint, the problem of estimating the signal probability is not trivial. In fact, it can be easily shown (by a transformation from satisfiability) that it is $\mathcal{NP}$−hard [6]. As a result, several *approximation techniques* have been developed to compute estimates of the signal probability while maintaining reasonable execution times. In [3] and [5], internal circuit nodes were assumed to be *independent*, providing a very fast but potentially very approximate solution. Improvements on these techniques were proposed in [4, 7, 8] to improve the accuracy at the cost of some reduction in speed.

A drastically different approach, proposed in [2] and refined in [10, 11], is based on estimating upper and lower *bounds* on the signal probability of a node. It can also be shown that the problem of estimating non-trivial bounds on the signal probability is also $\mathcal{NP}$-hard. The proof of this result is quite simple and, for completeness, is given in appendix A.

Yet another approach was proposed in [9] that relates the signal probability to the first spectral component of a Boolean function. Unfortunately, spectral techniques are too expensive to be used in practice, typically requiring exponential time and space.

In the review article [12], it was concluded that none of the forgoing techniques are robust enough to be of practical value. The techniques based on an independence assumption can be too approximate or otherwise too expensive, and the bounding techniques can produce very loose bounds.

In this paper, we propose a new approach to estimating the signal probability that is based on *statistical estimation*, essentially a Monte Carlo technique. Simply put, we apply randomly-generated logic patterns to the circuit inputs and, for every node, monitor the fraction of time that that node is at logic 1. Provided the input patterns are uncorrelated, the measured fractions will converge to the true probabilities (by the law of large numbers [13]). In order to determine *when* to stop this process, and whether the values obtained are at all close to the correct solution, we use the notion of *confidence interval* from statistics [13]

to provide a *stopping criterion.* Using this, it becomes possible, for instance, to stop the iterative process when we are 99% confident that the measured values are within 0.01 of the true probabilities. The desired accuracy and confidence levels can be specified up-front by the user. This is a key feature of our approach that gives the user direct control on the accuracy of the approximation, and sets this work apart from previous approximation methods, which do not offer such error-control. We will present experimental results that show that this technique is *robust* (i.e., that it works well over a wide range of circuits) and *fast* enough to be applicable to VLSI circuits.

As is the case with all previous work in this area, the technique to be presented is limited to combinational circuits. We are currently working on extensions to sequential circuits. The remainder of this paper is organized as follows. The next section contains the detailed description of the statistical estimation approach. Section 3 describes our implementation and presents experimental results. Conclusions are given in section 4. Finally, two appendices are included to present some mathematical proofs.

2. Statistical Bounds

We assume that every primary input node to the combinational circuit is assigned a signal probability value equal to the fraction of clock cycles in which it is expected to be at logic 1. As a result, some input patterns may be more probable than others. For instance, if an input node has a signal probability of 0.9, then those patterns in which it is at logic 1 are more probable. Likewise, if a node has a probability of 0, then input patterns in which that node is at 1 can not occur. These probabilities, along with the Boolean functions implemented by the circuit, completely determine the signal probabilities at all other nodes.

Suppose we repeatedly apply random input patterns to the circuit, chosen so that : (1) they are uncorrelated, and (2) their frequency of occurrence is consistent with the input signal probabilities. Let us also monitor internal circuit nodes and count the number of times each of them is at logic 1. We call the application of an input pattern a *trial* and the occurrence of a 1 at a node a *success*, while a 0 is called a *failure.* The result is what is commonly known as a process of *Bernoulli trials* [13].

If p is the (unknown) probability at an internal node, and if x successes are observed in a sequence of n trials, then by the *law of large numbers* [13] :

$$\lim_{n \to \infty} \frac{x}{n} = p \tag{1}$$

This, then, would be a straightforward way to estimate the signal probabilities. However, the problem with this simplistic approach is that there is no way to tell when x/n is close enough to p, in order for us to stop the process.

The solution comes from the study of statistical estimation of proportions [13] and can be summarized as follows. The number of possible successes in n trials is a random variable x, with a *binomial distribution* with parameter p. Since the *form* of the distribution is known, it becomes possible to assign a *confidence level* to how closely x/n approximates p. If α and E are small numbers between zero and one, this is usually expressed as "we are $(1-\alpha)\times 100\%$ confident that $|\frac{x}{n} - p| < E$." For a given value of E and α, one can look up the minimum required number of trials n in statistical tables [13]. As a result, this analysis provides a *stopping criterion* that can be used to terminate the iterative sampling process.

However, since tables are finite, this imposes a limit on n and/or leads to very large tables. The alternative option of expressing the bounds analytically based on the binomial distribution is too computationally expensive. Instead, it is much more efficient to use approximations to the binomial distribution. For instance, if np and $n(1-p)$ are greater than 5, then the binomial can be approximated by a *normal distribution* [13]. Furthermore, when $p < 0.1$ or $p > 0.9$ then according to [14] a good approximation to the binomial is given by the *Poisson distribution.* This leads to two stopping criteria, each of which applies to those nodes whose probabilities are in the corresponding range. Since we do not know the node probabilities a priori, the minimum value of n required to achieve the E error bound with $(1-\alpha)\times 100\%$ confidence is chosed as the *maximum* of those computed from the two approximations, which we consider as two separate cases below. In fact, we will further subdivide the Poisson case into two cases, according to whether x is small (less than 15) or not. The reason for this will become clear shortly. Finally, it is convenient before proceeding to *require a minimum value of 50 for* n, so that $np < 5$ is equivalent to $p < 0.1$ and $n(1-p) < 5$ is equivalent to $p > 0.9$.

2.1. The case $p \in [0.1, 0.9]$

In this case, and since $n > 50$, both np and $n(1-p)$ are greater than 5, and the binomial can be approximated by a *normal distribution*, so that in order to know with $(1-\alpha)\times 100\%$ confidence that $|\frac{x}{n} - p| < E$, we need [13] :

$$n \geq \left(\frac{z_{\alpha/2}}{2E}\right)^2 \tag{2}$$

trials, where $z_{\alpha/2}$ is defined so that the area to its right under the standard normal distribution curve is equal to $\alpha/2$, as shown in Fig. 1.

The value of $z_{\alpha/2}$ can be computed, for any given value of α, using the Gaussian distribution function **erf()** available on unix systems. To illustrate, suppose we want to compute the signal probabilities throughout the circuit to within 0.1 with 95% confidence. Then $E = 0.1$, $(1-\alpha) = 0.95$, which gives $z_{\alpha/2} = 1.96$, and therefore $n = 96$. Therefore, it is enough to

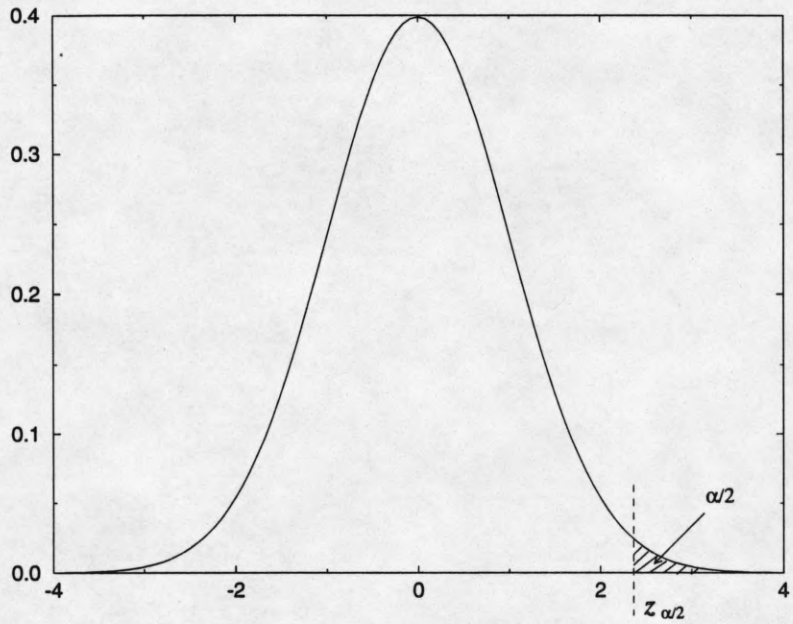

Figure 1. Definition of $z_{\alpha/2}$.

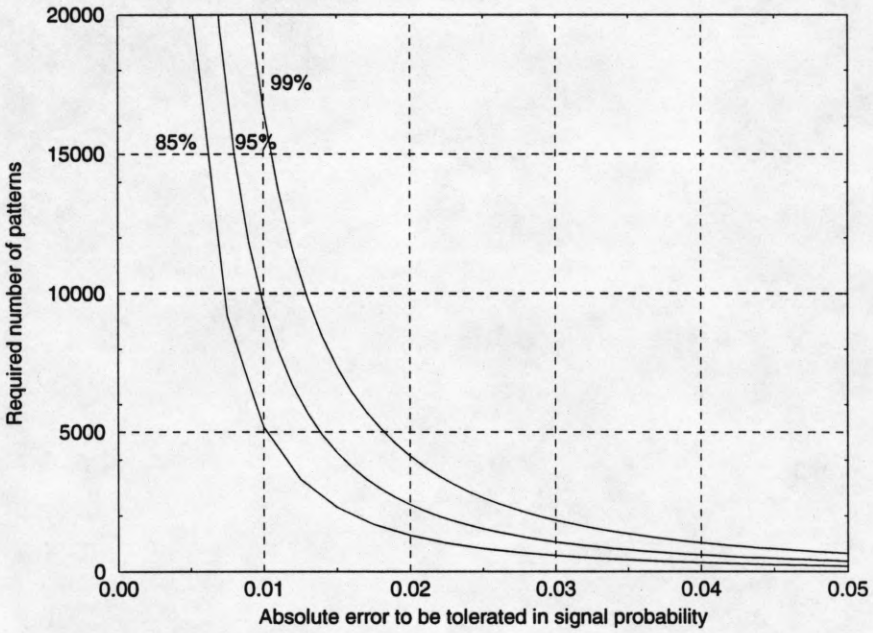

Figure 2. Stopping criterion when $p \in [0.1, 0.9]$.

apply 96 input patterns in this case. Based on (2), we can plot the minimum required n versus E for the case $p \in [0.1, 0.9]$ for different levels of confidence, as shown in Fig. 2.

As expected, the number of patterns required increases for smaller error bounds E. We

have deliberately focused on this part of the curve to show that values as low as $E = 0.01$ are feasible, provided the logic simulation of the circuit is fast enough. A best candidate for this kind of simulation would be a *compiled simulation* technique.

2.2. The case $p \notin [0.1, 0.9]$ and x is large (> 15)

According to [14], when $p < 0.1$ or $p > 0.9$, then a good approximation to the binomial is given by the *Poisson distribution.* Through a relationship between the Poisson distribution and the χ^2 (pronounced chi-square) distribution [14], it becomes possible to bound the value of p, and derive a stopping criterion, as follows.

By symmetry, it's enough to look at the case $p \leq 0.1$. In that case, we know with $(1-\alpha) \times 100\%$ confidence, that [14] :

$$\frac{1}{2n}\chi^2_{1-\alpha/2} \leq p \leq \frac{1}{2n}\chi^2_{\alpha/2} \tag{3}$$

where $\chi^2_{\alpha/2}$ is such that the area to its right under the χ^2 distribution is equal to $\alpha/2$. In the above inequality, the number of *degrees of freedom* of the χ^2 distributions is $f = 2x$ in the case of $\chi^2_{1-\alpha/2}$, and $f = 2(x+1)$ for $\chi^2_{\alpha/2}$, where x is the number of successes observed in n trials.

From the above, we have :

$$\frac{x}{n} - \frac{1}{2n}\chi^2_{\alpha/2} \leq \frac{x}{n} - p \leq \frac{x}{n} - \frac{1}{2n}\chi^2_{1-\alpha/2} \tag{4}$$

We want to take n samples such that, with $(1-\alpha)\times 100\%$ confidence, $|\frac{x}{n} - p| < E$. Using (4), it is enough to require :

$$-E < \frac{x}{n} - \frac{1}{2n}\chi^2_{\alpha/2} \qquad \text{and} \qquad \frac{x}{n} - \frac{1}{2n}\chi^2_{1-\alpha/2} < +E \tag{5}$$

Since $x > 15$, then $f > 30$ and the values of $\chi^2_{\alpha/2}$ and $\chi^2_{1-\alpha/2}$ can be approximated [14] using :

$$\chi^2_q \approx \frac{1}{2}\left(\sqrt{2f-1} + z_q\right)^2 \tag{6}$$

where q stands for $\alpha/2$ in one case, and $1-\alpha/2$ in the other. If we denote the ratio x/n by $\bar{p}$ and use the above approximation, we can rewrite the stopping criterion as :

$$4n(\bar{p} - E) < (\sqrt{4\bar{p}n - 1} - z_{\alpha/2})^2 \qquad \text{and} \qquad 4n(\bar{p} + E) > (\sqrt{4\bar{p}n + 3} + z_{\alpha/2})^2 \tag{7}$$

Each of these inequalities can be written as a quadratic in $\sqrt{n}$ whose roots give the required range of n. The lengthy analysis (see appendix B) yields :

$$n > \left(\frac{z_{\alpha/2}\sqrt{2E + 0.1} + \sqrt{(E+0.1)z^2_{\alpha/2} + 3E}}{2E}\right)^2 \tag{8}$$

2.3. The case $p \notin [0.1, 0.9]$ and x is small

The case $f = 2x \leq 30$ and/or $f = 2(x+1) \leq 30$, occurs when $x \leq 15$, so that $x/n \leq 15/n$. It is still true that an upper bound on p is given by $\frac{1}{2n}\chi^2_{\alpha/2}$, with $f \leq 32$, which may or may not mean that we can use the approximation (6). However, since the value of the χ^2 distribution increases with the number of degrees of freedom f, it follows that $p < \frac{1}{2n}\chi^2_{\alpha/2}$ with $f = 32$, for which the approximation holds, and we can write :

$$p < \frac{1}{4n}\left(\sqrt{63} + z_{\alpha/2}\right)^2 \tag{9}$$

Finally, since $x/n \leq 15/n < \frac{1}{4n}\left(\sqrt{63} + z_{\alpha/2}\right)^2$ for useful values of $z_{\alpha/2}$, we can write :

$$\left|\frac{x}{n} - p\right| < \frac{1}{4n}\left(\sqrt{63} + z_{\alpha/2}\right)^2$$

and the stopping criterion is given by :

$$n > \left(\frac{\sqrt{63} + z_{\alpha/2}}{2\sqrt{E}}\right)^2 \tag{10}$$

The comparison between the three resulting lower bounds on n are shown in Figs. 3 and 4.

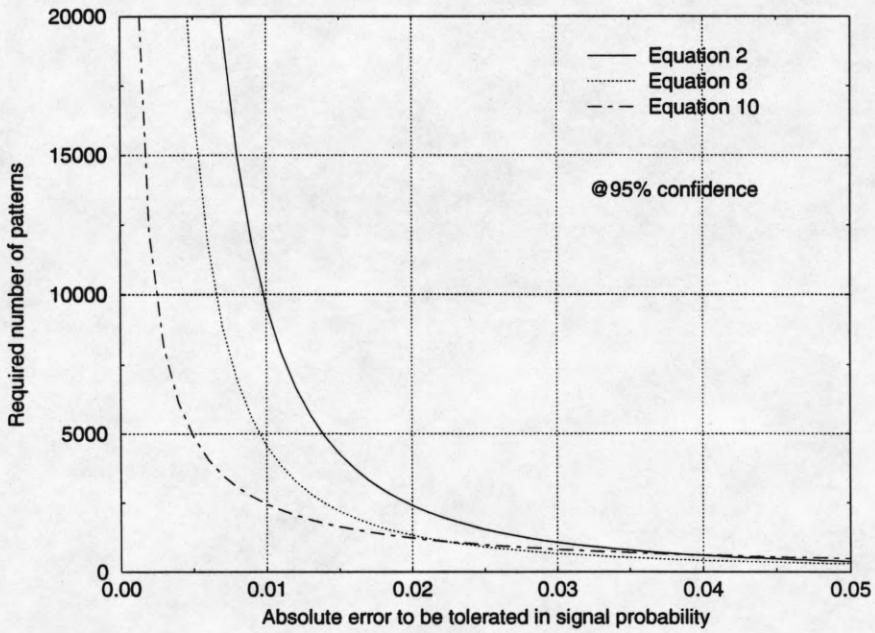

Figure 3. Comparison of the different bounds at $(1-\alpha) \times 100\% = 95\%$ confidence.

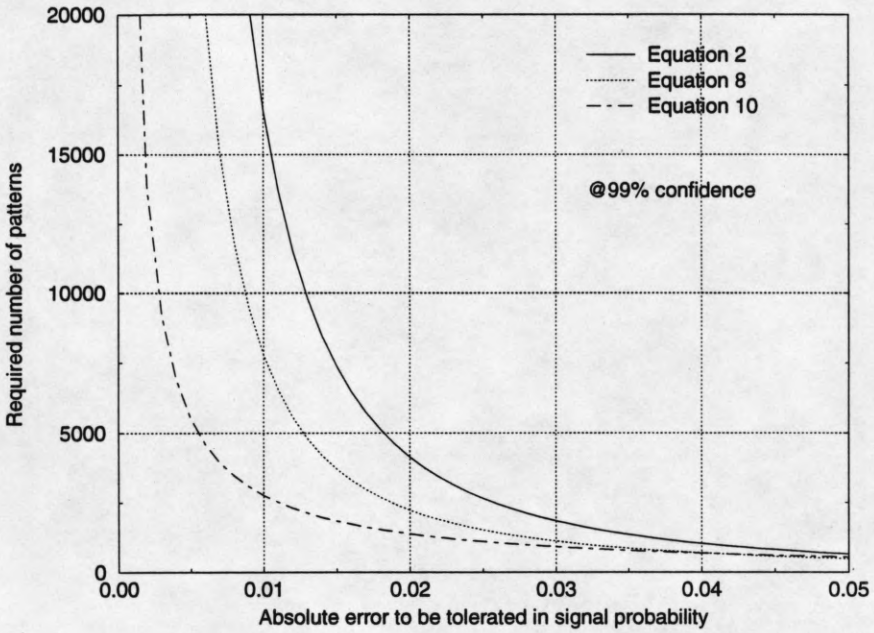

Figure 4. Comparison of the different bounds at $(1 - \alpha) \times 100\% = 99\%$ confidence.

To summarize, for a given error bound E and confidence level $(1 - \alpha) \times 100\%$, we determine the minimum number of patters n to be applied by taking the maximum of the three lower bounds predicted by equations (2), (8), and (10). In the next section, we will present some experimental results of of the application of this procedure to a variety of benchmark circuits.

3. Implementation and Results

This approach has been implemented in a prototype C program, using zero-delay logic simulation in order to evaluate the internal logic values for a given input pattern. The execution time results on a SUN Sparc ELC are shown in Table 1 for the ISCAS-85 benchmark circuits [15]. For the largest circuit, with 3512 gates, it takes under 12 minutes to find the signal probabilities to within 0.01 and with 99% confidence. This performance can be further improved by using compiled simulation to speed up the logic evaluation process.

In order to validate the accuracy of the approach, we ran the statistical estimation on c6288 for $n = 1,000,000$ patterns and used the resulting values as "accurate" signal probabilities (with $n = 10^6$, it can be shown that we have 99.99% confidence that the estimation error is less than 0.0019). We then compared the results of the runs in Table 1 to the "accurate" probability values and formed the two histograms shown in Figs. 5 and 6. These figures show the results for $(1 - \alpha) \times 100\% = 95\%$ and 99%, respectively. The

Table 1. Execution time results for the ISCAS-85 benchmark circuits.

Circuit Name	Number of gates	Number of inputs	Total Time (sec) $E = 0.01, (1-\alpha) = 95\%$	Total Time (sec) $E = 0.01, (1-\alpha) = 99\%$
c432	160	36	15.58	26.64
c499	202	41	20.89	35.70
c880	383	60	41.05	70.42
c1355	546	41	56.59	97.05
c1908	880	33	94.46	161.99
c2670	1193	157	140.68	241.32
c3540	1669	50	186.07	319.18
c5315	2307	178	269.53	462.54
c6288	2406	32	273.97	460.90
c7552	3512	206	406.39	697.30

percentage of nodes outside the specified error bounds of ± 0.01 is 2.25% in Fig. 5 and 0.899% in Fig. 6. As expected, these percentages are less than $\alpha \times 100\% = 5\%$ and 1% respectively. We should point out that c6288 is one of the hardest circuits to solve by traditional techniques because it has extensive reconvergent fanout.

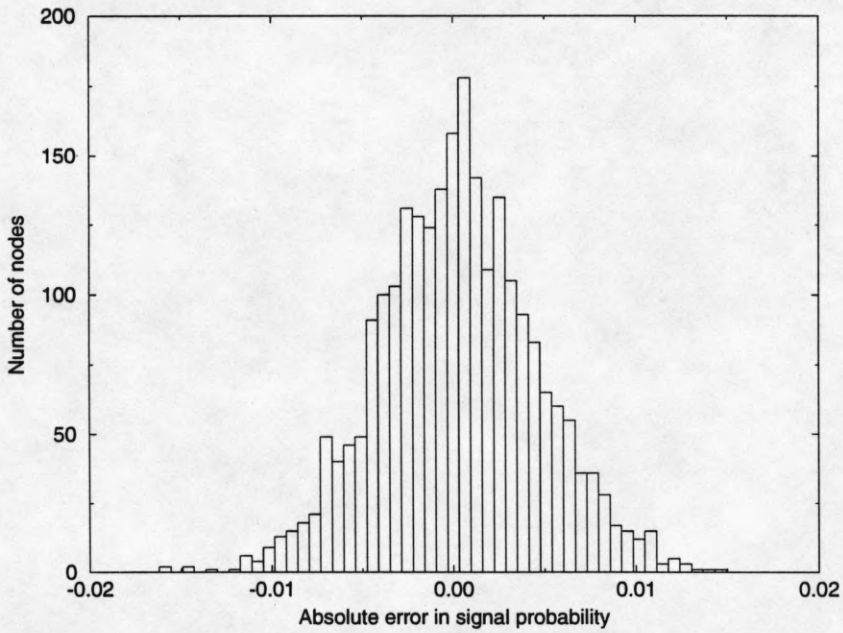

Figure 5. Error histogram for c6288, comparing the results of a $(1-\alpha) \times 100\% = 95\%$ run with a much longer $n = 1e6$ run.

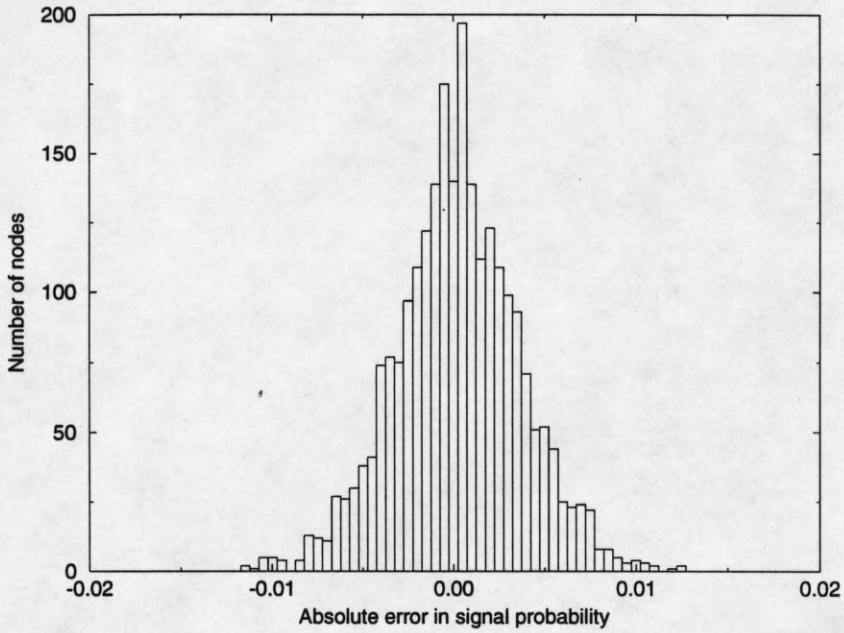

Figure 6. Error histogram for c6288, comparing the results of a $(1-\alpha) \times 100\% = 99\%$ run with a much longer $n = 1e6$ run.

Finally, we ran the program on the combinational parts of the ISCAS-89 benchmark circuits [16] and show the results in Table 2 (execution times are for a SUN Sparc ELC). We can solve a 22,000 gate circuit in under 1Hr 14mins. This indicates that this approach is practical for VLSI circuits, especially if the software is optimized and a suitable compiled simulation approach is adopted.

4. Conclusions

We have presented an efficient and reliable method for finding the node signal probabilities in combinational digital circuits. The method is based on statistical estimation, and guarantees that the user-specified error tolerance is met, with a user-specified confidence level. The fact that the desired accuracy can be specified up-front is a key feature of this technique that makes it very attractive in practice. We have presented experimental results for two common benchmark circuit sets that show that the technique is also quite efficient : we can solve a 22,000 gate circuit in a little over an hour of cpu time, on a SUN sparc ELC. This indicates that this approach is practical for VLSI circuits.

As is the case with all previous work in this area, the current implementation of this technique is limited to combinational circuits. We are currently investigating future extensions to allow the handling of sequential circuits.

Table 2. Execution time results for the ISCAS-89 benchmark circuits.

Circuit Name	Number of gates	Number of inputs	Total Time (sec) $E = 0.01, (1-\alpha) = 95\%$	Total Time (sec) $E = 0.01, (1-\alpha) = 99\%$
s1196	529	31	55.25	94.51
s1238	508	31	54.19	93.17
s13207.1	7951	650	926.30	1586.70
s1423	657	91	73.53	125.87
s1488	653	14	71.63	122.56
s1494	647	14	69.61	124.54
s15850.1	9772	600	1125.74	1914.79
s208.1	104	18	8.49	14.61
s27	10	7	1.15	1.81
s298	119	17	10.28	16.85
s344	160	24	14.90	24.94
s349	161	24	14.51	24.76
s35932	16065	1763	1968.19	3359.59
s382	158	24	13.57	23.13
s38417	22179	1524	2586.00	4430.14
s38584.1	19253	1462	2353.19	4028.00
s386	159	13	13.56	23.26
s400	164	25	14.77	25.43
s420.1	218	34	19.96	34.16
s444	181	24	17.24	29.27
s510	211	25	20.59	35.24
s526	193	24	17.59	30.44
s526n	194	24	17.95	30.98
s5378	2779	214	316.94	541.82
s641	379	54	37.11	63.23
s713	393	54	38.28	65.47
s820	289	23	29.51	51.23
s832	287	23	29.25	50.67
s838.1	446	66	46.42	78.25
s9234.1	5597	247	637.88	1084.18
s953	395	22	38.05	66.22

Appendix A

The signal probability of a node is a real number $p \in [0,1]$. We call 0 and 1 *trivial bounds* on p. We will prove that establishing non-trivial bounds on the signal probability in a general combinational circuit is $\mathcal{NP}$-hard [6].

A Boolean expression is said to be *satisfiable* if there exists an assignment of 0's and 1's to its variables that gives it the value 1. We recall the *satisfiability problem* from mathematical logic [6], to be abbreviated SAT, which is defined as follows. A Boolean variable or its complement is called a *literal*. Given a Boolean expression in *conjunctive normal form* (CNF), i.e., it is the product (logical *and*) of a set of sub-expressions called *clauses* where every clause is the sum (logical *or*) of a number of literals. The problem is to decide whether or not the expression is satisfiable. It is well known [6] that SAT is $\mathcal{NP}$-complete.

SAT is a *decision problem*, i.e., it has a true/false solution. In order to prove that some other decision problem P is also $\mathcal{NP}$-complete, it is enough to show that an *instance* I_{SAT} of SAT can be transformed in *polynomial time* to an instance I_P of P, such that I_P is true if and only if I_{SAT} is satisfiable. This is summarized by saying that SAT is *transformable in polynomial time* to P. A problem that is not a decision problem, but that is at least as hard as a decision problem that is known to be $\mathcal{NP}$-complete, is said to be $\mathcal{NP}$-hard.

With this background, the proof becomes very simple, as follows. Let f be a Boolean expression in CNF. We can build, in linear time, a digital circuit with two output nodes : f_1 implementing the function f, and f_2 implementing its negation $\bar{f}$. It's easy to see that, if all primary inputs are assigned 0.5 probabilities, then the signal probability at f_1 is strictly greater than 0 if and only if f is satisfiable, and that at f_2 is strictly less than 1 if and only if f is satisfiable. Thus the problem of deciding whether the signal probability at a node is strictly greater than 0, or strictly less than 1, is $\mathcal{NP}$-complete. This completes the proof.

Appendix B

We will derive the final form (8) of the stopping criterion in the case "$p \notin [0.1, 0.9]$ and x is large (> 15)." We start with the intermediate form (7), which we repeat for convenience :

$$4n(\bar{p} - E) < (\sqrt{4\bar{p}n - 1} - z_{\alpha/2})^2 \qquad (B.1)$$

$$4n(\bar{p} + E) > (\sqrt{4\bar{p}n + 3} + z_{\alpha/2})^2 \qquad (B.2)$$

We will consider each of these inequalities and find the minimum value of n required for it to hold. The largest of these values will be the desired answer.

We first consider (B.1) and observe that if $\bar{p} < E$ then any value of n will suffice. In the sequel, let $\bar{p} > E$, which allows one to write :

$$2\sqrt{n}\sqrt{\bar{p} - E} < \pm(\sqrt{4\bar{p}n - 1} - z_{\alpha/2}) \qquad (B.3)$$

where the "+" sign applies in case $\sqrt{4\bar{p}n-1} \geq z_{\alpha/2}$ and the "−" sign applies otherwise. This leads to :

$$(2\sqrt{n}\sqrt{\bar{p}-E} \pm z_{\alpha/2})^2 < 4\bar{p}n - 1 \qquad (B.4)$$

which can be rewritten as a quadratic in $\sqrt{n}$:

$$4En \mp 4z_{\alpha/2}\sqrt{\bar{p}-E}\sqrt{n} - (1 + z_{\alpha/2}^2) > 0 \qquad (B.5)$$

Solving the two quadratics in the left-hand-side of (B.5), we find two roots in each case :

$$\frac{+z_{\alpha/2}\sqrt{\bar{p}-E} \pm \sqrt{z_{\alpha/2}^2\bar{p} + E}}{2E} \quad \text{and} \quad \frac{-z_{\alpha/2}\sqrt{\bar{p}-E} \pm \sqrt{z_{\alpha/2}^2\bar{p} + E}}{2E} \qquad (B.6)$$

Since the smaller of the two roots is negative in both cases, and since $4E > 0$, then $\sqrt{n}$ needs to be bigger than the larger of the two positive roots in order to satisfy (B.5), leading to :

$$n > \left(\frac{z_{\alpha/2}\sqrt{\bar{p}-E} + \sqrt{z_{\alpha/2}^2\bar{p} + E}}{2E} \right)^2 \qquad (B.7)$$

In the case of (B.2), a similar sequence of steps leads to the quadratic in $\sqrt{n}$:

$$4En - 4z_{\alpha/2}\sqrt{\bar{p}+E}\sqrt{n} + (z_{\alpha/2}^2 - 3) > 0 \qquad (B.8)$$

whose larger root leads to the following requirement on n :

$$n > \left(\frac{z_{\alpha/2}\sqrt{\bar{p}+E} + \sqrt{z_{\alpha/2}^2\bar{p} + 3E}}{2E} \right)^2 \qquad (B.9)$$

By making a term-by-term comparison, it's clear that the right-hand-side of (B.9) is greater than that of (B.7). Therefore, in order to satisfy the stopping criterion (7), it is enough to require that n satisfy (B.9).

Finally, since when the stopping criterion is satisfied we have $\bar{p} - p < E$, and since $p < 0.1$, then $\bar{p} < 0.1 + E$, which leads to :

$$n > \left(\frac{z_{\alpha/2}\sqrt{2E+0.1} + \sqrt{(E+0.1)z_{\alpha/2}^2 + 3E}}{2E} \right)^2 \qquad (B.10)$$

which is the desired final form (8) of the stopping criterion.

References

[1] K. P. Parker, E. J. McCluskey, "Probabilistic treatment of general combinational networks," *IEEE Transactions on Computers*, vol. C-24, pp. 668–670, June 1975.

[2] J. Savir, G. S. Ditlow, P. H. Bardell, "Random pattern testability," *IEEE Transactions on Computers*, vol. C-33, no. 1, pp. 79–90, January 1984.

[3] F. Brglez, "On testability analysis of combinational networks," *IEEE International Symposium on Circuits and Systems*, pp. 221–225, 1984.

[4] S. C. Seth, L. Pan, V. D. Agrawal, "Predict - probabilistic estimation of digital circuit testability," *IEEE 15th International Symposium on Fault-Tolerant Computing*, pp. 220–225, June 1985.

[5] M. A. Cirit, "Estimating dynamic power consumption of CMOS circuits," *IEEE International Conference on Computer-Aided Design*, pp. 534–537, November 1987.

[6] M. R. Garey, D. S. Johnson, *Computers and Intractability, A Guide to the Theory of NP-Completeness.* San Francisco, CA: W. H. Freeman and Company, 1979.

[7] B. Krishnamurthy, I. G. Tollis, "Improved techniques for estimating signal probabilities," *IEEE Transactions on Computers*, vol. 38, no. 7, pp. 1041–1045, July 1989.

[8] S. Ercolani, M. Favalli, M. Damiani, P. Olivo, B. Ricco, "Estimate of signal probability in combinational logic networks," *IEEE European Test Conference*, pp. 132–138, 1989.

[9] B. R. Bannister, D. R. Melton, G. Taylor, "Testability of digital circuits via the spectral domain," *IEEE International Conference on Computer Design*, pp. 340–343, 1989.

[10] G. Markowsky, "Bounding signal probabilities in combinational circuits," *IEEE Transactions on Computers*, vol. C-36, no. 10, pp. 1247–1251, October 1987.

[11] R. David, K. Wagner, "Analysis of detection probability and some applications," *IEEE Transactions on Computer-Aided Design*, vol. 39, no. 10, pp. 1284–1291, October 1990.

[12] P. Camurati, P. Prinetto, M. Sonza Reorda, "Random testability analysis : comparing and evaluating existing approaches," *IEEE International Conference on Computer Design*, pp. 70–73, 1988.

[13] I. R. Miller, J. E. Freund, and R. Johnson, *Probability and Statistics for Engineers*, 4th Edition. Englewood Cliffs, NJ: Prentice-Hall Inc., 1990.

[14] A. Hald, *Statistical Theory with Engineering Applications.* New York, NY: John Wiley & Sons, Inc., 1952.

[15] F. Brglez and H. Fujiwara, "A neutral netlist of 10 combinational benchmark circuits and a target translator in Fortran," *IEEE International Symposium on Circuits and Systems*, pp. 695–698, June 1985.

[16] F. Brglez, D. Bryan, and K. Koźmiński, "Combinational profiles of sequential benchmark circuits," *IEEE International Symposium on Circuits and Systems*, pp. 1929–1934, 1989.