Proceedings of the 7th Military and Aerospace Programmable Logic Devices (MAPLD) International Conference, Washington, District of Columbia, September, 2004

Monte Carlo Analysis of Uncertain Digital Circuits

Houssain Kettani
Department of Computer Science
Jackson State University
Jackson, MS 39217
houssain.kettani@jsums.edu

Abstract

Unlike the classical deterministic digital circuit analysis, we consider a Monte Carlo simulation in the context of uncertain digital circuits. In other words, given a binary function of n uncertain input binary variables, we express the probability of this binary function in terms of the probabilities of the corresponding input binary variables. This in turn, allows us to estimate appropriate probabilistic measure of the output of a digital circuit with uncertain input parameters.

1 Introduction

The theory of deterministic digital circuits has been studied extensively — See [4] for example. Typically, a binary variable x_j is allowed to take only two values; 0 and 1. A binary function of n binary variables $f(x_n, x_{n-1}, \ldots, x_1)$, is also allowed to take only the values 0 and 1.

The introduction of uncertainty in digital circuits has been used in different areas to model complex systems. For example, see [6] for the introduction of probabilistic Boolean networks to model gene regulatory networks. In such a model, the x_j's represent the state of gene j, where $x_j = 1$ denotes the fact that gene j is expressed and $x_j = 0$ means it is not expressed. The binary function $f_j(x_n, x_{n-1}, \ldots, x_1)$, on the other hand, is referred to as a predictor, and is used to determine the value of x_j in terms of some other gene states.

In this paper, we consider the case when the binary variable x_j is a random variable. Thus, if we consider a binary function of the n random binary variables $f(x_n, x_{n-1}, \ldots, x_1)$, then this in turn would be a random binary variable. In this context, all the variables under consideration are Bernoulli random variables since they take only the values 0 and 1.

Hence, throughout this paper, we consider the case when the x_j's are independent random variables with probabilities $P(x_j = 1) = p_j = E[x_j]$. Next, we consider the probability or expectation

$$\mathcal{P} \doteq P(f(x_n, x_{n-1}, \ldots, x_1) = 1).$$

We then, pose the following questions: Given a logic function, $f(x_n, x_{n-1}, \ldots, x_1)$, with known probabilities x_j's, what can we say about the probability $\mathcal{P}$? How can we address the problem of maximizing or minimizing $\mathcal{P}$? The latter may refer to best case and worst case scenarios.

The flow of this paper is as follows. In Section 2, we present and prove a result that expresses the probability $\mathcal{P}$ in terms of the probabilities p_j's, with $j = n, n-1, \ldots, 1$. Section 3 answers the question of maximizing and minimizing $\mathcal{P}$. We present a numerical example in Section 4 to illustrate the ideas presented in this paper. Finally, a summary and a suggestion of further research directions is presented in Section 5.

2 Stochastic Measures

Suppose the variables x_j's are independent random variables with given probabilities $P(x_j = 1) = p_j$. Given a logic function, $f(x_n, x_{n-1}, \ldots, x_1)$, let us define

$$\begin{aligned} \mathcal{P} &\doteq P(f(x_n, x_{n-1}, \ldots, x_1) = 1) \\ &= E[f(x_n, x_{n-1}, \ldots, x_1)]. \end{aligned}$$

Then what can we say about the probability (or expectation) $\mathcal{P}$? How can we address the problem of maximizing or minimizing $\mathcal{P}$?

To answer these questions, let us consider the following theorem.

2.1 Theorem

Let $f(x_n, x_{n-1}, \ldots, x_1)$ be a binary function of n independent binary random variables with $P(x_j = 1) = p_j$. Let I be the set of minterm indices for which $f(x_n, x_{n-1}, \ldots, x_1)$ is 1. Then

$$\mathcal{P} = \sum_{i \in I} \prod_{j=1}^{n} P(x_j = \lfloor i2^{-j+1} \rfloor - 2\lfloor i2^{-j} \rfloor). \qquad (1)$$

2.2 Proof of Theorem

We devote this section to proving Theorem 2.1. Let $f(x_n, x_{n-1}, \ldots, x_1)$ be a binary function of n variables. Let I be the set of minterm indices for which $f(x_n, x_{n-1}, \ldots, x_1)$ is 1. Clearly we have $0 \leq i < 2^n$ for $i \in I$. Now note that any binary function can be written as a sum of its minterms — see [4] for details. Thus, we write

$$f(x_n, x_{n-1}, \ldots, x_1) = \sum_{i \in I} m_i,$$

where m_i is the ith minterm.

Let us now write $(i)_{10} = (i_n i_{n-1} \ldots i_1)_2$, where $i_j \in \{0, 1\}$. Hence, we have

$$m_i = x_n^{i_n} x_{n-1}^{i_{n-1}} \ldots x_1^{i_1} = \prod_{j=1}^{n} x_j^{i_j},$$

where we adopt the notion that $x_i^0 = \overline{x}_j$; which is the complement of x_j, and $x_j^1 = x_j$. Suppose now that $P(x_j = 1) = p_j$, and let

$$\mathcal{P} \doteq P(f(x_n, x_{n-1}, \ldots, x_1) = 1).$$

Now, since the events $\{m_i = 1\}$ are mutually exclusive, we have

$$P(f(x_n, x_{n-1}, \ldots, x_1) = 1) = \sum_{i \in I} P(m_i = 1).$$

Next, note that

$$P(m_i = 1) = \prod_{j=1}^{n} P(x_j = i_j),$$

since x_j's are independent. Now, note that

$$i_j = \lfloor i2^{-j+1} \rfloor - 2\lfloor i2^{-j} \rfloor.$$

A general version of the latter result is proven in [2]. Thus, (1) follows and this concludes the proof.

2.3 Remarks

In Theorem 2.1, the set I consists of those minterms that are equal to 1. Thus, if a minterm is a "don't-care," it will not be included in the sum in (1). In other words, the index of such a minterm is not a member of I. This is the case since, by definition, a "don't care" is a condition that does not happen.

On another note, the variance of the binary function can easily be obtained and is expressed as

$$Var[f(x_n, x_{n-1}, \ldots, x_1)] = \mathcal{P} - \mathcal{P}^2.$$

3 Stochastic Optimization

Suppose that the probabilities p_j can be picked from intervals $\mathcal{I}_j = [p_j^-, p_j^+]$. Consequently, the tuple $(p_1, p_2, \ldots, p_n)$ can be picked from the hypercube

$$\mathcal{I} = \mathcal{I}_1 \times \mathcal{I}_2 \times \ldots \times \mathcal{I}_n.$$

Then, what value should we set the probabilities p_j to in order to maximize or minimize $\mathcal{P}$? To answer this question, we first introduce the following definition.

3.1 Essential Variables

A binary variable x_k is said to be *essential* if the following condition holds: There does not exist admissible values of the $(n-1)$ remaining variables $x_j \in \mathcal{I}_j$, $j \neq k$ making the probability $\mathcal{P}$ independent of $x_k \in \mathcal{I}_k$.

If x_k is essential, it can readily be shown that the partial derivative $\partial\mathcal{P}/\partial p_k$ is non-zero over $\mathcal{I}$. Hence, by an intermediate value argument, if the variable x_k is essential, the partial derivative $\partial\mathcal{P}/\partial p_k$ has one sign over $\mathcal{I}$. In view of this, let

$$s_k \doteq \text{sign}\left(\frac{\partial\mathcal{P}}{\partial p_k}\right)$$

denote this invariant sign; i.e., s_k is constant over $\mathcal{I}$ having the value $s_k = -1$ or $s_k = 1$.

The following theorem answers the question posed in the introduction of this section.

3.2 Theorem

Let $\mathcal{P}$ be a function of some p_j's. Then, for the case of maximizing $\mathcal{P}$, if the variable x_k is essential, then pick $p_k = p_k^-$ when $s_k = -1$, and pick $p_k = p_k^+$ when $s_k = 1$.

For the case of minimizing $\mathcal{P}$, if the variable x_k is essential, then pick $p_k = p_k^+$ when $s_k = -1$, and pick $p_k = p_k^-$ when $s_k = 1$.

If x_k is not essential, then for either case pick $p_k = p_k^-$ or $p_k = p_k^+$.

3.3 Proof of Theorem

To prove Theorem 3.2 we first note that Theorem 2.1 shows that $\mathcal{P}$ is multilinear in the p_i's. Thus, to maximize or minimize $\mathcal{P}$ we invoke the well-known result that a multilinear function on a hypercube is both maximized and minimized at its vertices — see [3] for example. Vertex points here are the tuples $(p_1^\pm, p_2^\pm, \ldots, p_n^\pm)$, where $p_j^\pm$ stands for the extreme values p_j^- or p_j^+.

Now, if the variable x_j is essential, then $s_j = -1$ implies that $\mathcal{P}$ is decreasing with respect to p_j. Thus, to maximize $\mathcal{P}$, we decrease p_j, and to minimize $\mathcal{P}$, we increase p_j. Similarly, $s_j = 1$ implies that $\mathcal{P}$ is increasing with respect to p_j. Thus, to maximize $\mathcal{P}$, we increase p_j, and to minimize $\mathcal{P}$, we decrease p_j. Since $p_j \in [p_j^-, p_j^+]$, the result of the theorem follows.

4 Numerical Examples

To illustrate the use of the ideas introduced in this paper, we consider two logic functions:

$$f_1(x_3, x_2, x_1) = x_3 + \overline{x}_1,$$

and

$$f_2(x_3, x_2, x_1) = \overline{x}_2 x_1 + x_3 \overline{x}_1,$$

with $p_1 \in [0.4, 0.6]$, $p_2 \in [0.1, 0.5]$, and $p_3 \in [0.2, 0.8]$.

Let I_1 and I_2 be the sets of minterm indices for which $f_1(x_3, x_2, x_1) = 1$ and $f_2(x_3, x_2, x_1) = 1$, respectively. Then $I_1 = \{0, 2, 4, 5, 6, 7\}$ and $I_2 = \{1, 4, 5, 6\}$. Thus, from (1), we have

$$\mathcal{P}_1 = (1 - p_3)(1 - p_1) + p_3$$

and

$$\mathcal{P}_2 = (1 - p_2)p_1 + (1 - p_1)p_3.$$

We note here that $\mathcal{P}_2$ can be expressed directly from the expression of $f_2(x_3, x_2, x_1)$. This is because $f_2(x_3, x_2, x_1)$ is expressed as the sum of products that are mutually exclusive. Note that a similar argument cannot be made with regard to $f_1(x_3, x_2, x_1)$.

Now, suppose we would like to maximize $\mathcal{P}_1$. Then note that both x_1 and x_3 are essential with respect to f_1 with $s_1^{(1)} = -1$ and $s_3^{(1)} = 1$, respectively. Thus, the maximum $\mathcal{P}_1^+$ is obtained with $p_1 = 0.4$ and $p_3 = 0.8$. Consequently, $\mathcal{P}_1^+ = 0.92$.

Suppose now that we would like to minimize $\mathcal{P}_2$. Then note that both x_2 and x_3 are essential with respect to f_2 with $s_2^{(2)} = -1$ and $s_3^{(2)} = 1$, respectively. Thus, the minimum $\mathcal{P}_2^-$ is obtained with

$p_2 = 0.5$ and $p_3 = 0.2$. However, the variable x_1 is not essential. Thus, we try both values 0.4 and 0.6 for p_1, which results in $\mathcal{P}_2 = 0.32$ and $\mathcal{P}_2 = 0.38$, respectively. Consequently, $\mathcal{P}_2^- = 0.32$.

5 Summary and Further Research

We considered the case of digital circuits with uncertain input variables. We have presented a probabilistic measure of the output function in terms of the probabilities of the input. The result is a multilinear function, which facilitates the optimization problem of the probability measure of the output.

In what follows, we suggest three research directions. Firstly, it would be of interest to consider the case when the input variables are dependent. In this case, the challenge is that the joint distribution cannot be expressed as the product of the marginal distributions. Thus, we have

$$\mathcal{P} = \sum_{i \in I} P(x_n = i_n, x_{n-1} = i_{n-1}, \ldots, x_1 = i_1).$$

The second suggested research direction is in b-ary logic. Although binary logic is by far the most practical among any b-ary logic, there is some use of the trinary (or ternary) logic — see [1] and [5] for more information. A fundamental issue in this case is that minterm concept is not properly defined. As a consequence, the events of the term in which all the variables appear exactly once may not be mutually exclusive.

Finally, it would be of interest to broaden the concept of uncertain digital networks to include uncertain logic gates and extend the results of this paper to such case. For example, an uncertain AND gate would have a corresponding probability $P(xy = 1) = p$. This in turn, would lead to a new probabilistic Boolean algebra.

References

[1] `S. Grubb (2001), http:\\www.trinary.cc.`

[2] H. Kettani (2004), "*On the Conversion Between Number Systems,*" Proceedings of the 2004 International Conference on Algorithmic Mathematics and Computer Science (AMCS'04), Las Vegas, Nevada, June, 2004.

[3] D. G. Luenberger (1973), "*Introduction to Linear and Nonlinear Programming.*" Addison-Wesley Publishing Company.

[4] M. M. Mano and C. R. Kime (2001), "*Logic and Computer Design Fundamentals,*" second edition, Prentice Hall.

[5] T. Sasao (1999), "*Arithmetic Ternary Decision Diagrams Applications and complexity,*" Proceedings of the Fourth International Workshop on Applications of the Reed-Muller Expansion in Circuit Design, (Reed-Muller 99), Victoria, Canada, August, 1999.

[6] I. Shnulevich, E. R. Dougherty, S. Kim, and W. Zhang (2002), "*Probabilistic Boolean Networks: A Rule-Based Uncertainty Model for Gene Regulatory Networks,*" Bioinformatics, Vol. 18, pp. 261–274.