A Probabilistic Boolean Logic and its Meaning

Lakshmi N. B. Chakrapani , Krishna V. Palem*
Department of Computer Science
Rice University
Houston, Texas, USA
{chakra,palem}@rice.edu

We introduce a novel *probabilistic Boolean logic* (PBL) in which the probabilistic disjunction, conjunction and negation operators, provide the "output" expected of their deterministic counterparts, with a probability p. By design, this output can be *incorrect* with a probability $(1-p)$. In order to distinguish our approach to injecting probabilities into Boolean logic from past approaches, we introduce a semantic model based on the novel notion of *event sets.* To the best of our knowledge, event sets provide a novel meaning to *truth* when Boolean logic and probability are combined. Building on this, we continue to show that while several of the standard properties (or laws) of Boolean logic are preserved in PBL, we unearth some surprises by showing that the analogs of *distributivity* and *associativity*, are not preserved. In fact, the amount by which associativity is not preserved in PBL can be quantified as the *degree of non-associativity* Δ_n which grows as $\Omega(n)$, where n is the length of the formula, and $p = (1 - \frac{1}{n^c})$. An obvious question is to ask whether PBL is essentially equivalent to a logic whose formulae are formed from deterministic operators, but where (some of) the inputs are random variables. We show that the latter approach to injecting probabilistic behavior is distinguishable semantically, and separable—since it is provably more expensive if energy consumption is the complexity measure—from an equivalent approach based on PBL. We show this difference to be true both in the combinational context of logic as well as in that of models of computation with state based on *probabilistic automata.* Our interest in PBL is motivated in large part, by an increasing need to model transistors, gates and circuits—the building blocks of *very large scale integration* (VLSI)—probabilistically as they approach nanometer sizes, creating a need to shift away from deterministic models and logics that have been successfully used in the past.

1. INTRODUCTION

Automated computing, ranging from machine models such as Turing machines [62] to programming languages, has its roots in the study and advances in logic (see Davis [16] for an excellent overview and a historical perspective, which relates advances in logic to the birth of "modern" computers and computer science in its present form). One aspect of these foundational developments, two-valued Boolean logic, is at the heart of advances in the specification, automated construction and verification of silicon-based digital VLSI circuits—the bedrock of the information technology revolution. Curiously and counter-intuitively, the notion of probability, when coupled with models of computing derived from logic, have proved to be very effective in realizing highly efficient algorithms for computing. Notable work which introduced considerations of probability in models of computing, include Rabin's introduction of probabilistic automata [55] and randomized algorithms. Their impact was eloquently anticipated by Schwartz [60]—*"The startling success of*

This work is supported in part by DARPA under seedling contract F30602-02-2-0124 and by an award from Intel Corporation.

*This author also wishes to thank the the Moore distinguished faculty fellow program at the California Institute of Technology and the Canon distinguished professorship program of the Nanyang Technological University at Singapore during the 2007 academic year, which enabled pursuing this work in part.

the Rabin-Solovay-Strassen algorithm (see Rabin [56]), together with the intriguing foundational possibility that axioms of randomness may constitute a useful fundamental source of mathematical truth independent of, but supplementary to, the standard axiomatic structure of mathematics (see Chaitin and Schwartz [9]) suggests that probabilistic algorithms ought to be sought vigorously.". These contributions have led to vast areas of study that explore the power that probability and randomness add to computing (we note in passing that Chaitin and Schwartz's work extended the reach of probability into the heart of mathematics itself and studied the power of axiomatic systems and mathematical proof of a probabilistic nature [9]).

Historically, probabilistic behavior was realized by adding an external source of randomness to conventional logic based constructs, such as gates and automata, to *induce* randomness and hence probabilistic behavior. To achieve this, pseudo-random bits are coupled with deterministic mechanisms. We refer to this as an *explicit* style of realizing probabilistic computing. By contrast, an *implicit* approach to realizing probabilistic computing could be based on using naturally probabilistic phenomena, and thus, there is *no* need for an external random source. Here, sources of randomness could include various types of noise [11, 47, 59]—an increasingly perceptible phenomenon in physically deterministic devices [35]—and others. We note in passing that probabilistic behavior of the implicit type is anticipated increasingly in CMOS devices, gates and circuits—the building blocks of modern computers—and are caused by manufacturing deficiencies and noise susceptibility [28] as physical sizes of individual transistors approach $20nm$. This is viewed as an impediment to realizing deterministic switches and hence to Moore's law [45]. Characterizing this implicit approach to probabilistic computing and logic formally, and providing an approach to distinguishing it from its explicit counterpart, serve as the overarching philosophical themes of this paper. To achieve this, probability and Boolean logic need to be treated in an unified manner.

To this end, we introduce a novel *Probabilistic Boolean Logic* (PBL) as well as a model of computation—essentially a probabilistic automata (PA) in the Rabin sense [55]—whose transition functions are realized through PBL. In PBL, the canonical operations—disjunction, conjunction, and negation, denoted respectively by $\vee_p, \wedge_q, \neg_r$—have an associated probability p, q, r $(1/2 \leq p, q, r \leq 1)$ of being "correct", and can be used to construct *probabilistic boolean formulae* (PBF). Akin to formulae in classical Boolean logic, those in PBL can be constructed as compositions of probabilistic operators, variables, and the constants $\{0, 1\}$. Informally, for any input assignment to the (deterministic) variables in a probabilistic Boolean formula, its "value" is the outcome of a random experiment, whose *sample space* (for examples, see Feller [24]) is determined by the input assignment to the variables in the the formula, its structure, *as well as* the associated probabilities of correctness of its constituent operators.

Next, to formally characterize and "interpret" this informal notion of correctness of a PBF, we introduce the foundational concept of an *event set*: it consists of a set of *events* from a sample space, each of which is associated with a conventional (deterministic) Boolean formula. Given an input assignment I to a PBF, its event set can be used characterize the possible set of events associated with the input assignment. This characterization helps us to unambiguously determine the correctness and truth of the PBF in a unified way. We note that the assignment I is deterministic, and the probabilistic behavior is induced *entirely* by the (implicitly) probabilistic operators of the PBF. This has to be contrasted with an approach to *explicitly* injecting probabilistic behavior into conventional Boolean formulae with deterministic operators, by considering some of the elements of the input assignment to be random variables (ranging over the set $\{0, 1\}$). Based on the event set semantics, we will distinguish the implicit and explicit approaches of melding logic with probability. Furthermore, we define the conditions under which two or more probabilistic Boolean formulae can be characterized as being equivalent using event sets. This formal notion of equivalence through event sets serves as a cornerstone of characterizing the significant identities or properties of PBL.

The properties of PBL for the most part, correspond to those of classical Boolean logic. However, intriguingly, PBL does not preserve distributivity and associativity. In the latter context, a novel contribution of our work is to help quantify the "amount" by which a formula is non-associative. When we consider reassociations of the same formula—for example $((x \vee_p y) \vee_q z)$ and $(x \vee_p (y \vee_q z))$ are reassociations of each other—the probability with which it is satisfied, varies. We use this variation as a basis for quantifying the *degree of non-associativity* of PBL. Specifically, we show that there exist formulae of size $n \to \infty$ such that the degree of non-associativity grows as $\Omega(n)$ where $p = 1 - 1/n^c$. Conversely, the degree of non-associativity demonstrates how the probability of correctness of a given PBF F may be improved through considering reassociations of F. As discussed in Section 4, we anticipate that this characterization will prove to be useful in (automatically) synthesizing circuits from specifications.

Next, we introduce and study *Probabilistic Boolean Circuits*, a model of computation based on PBL, and characterize its relationship to conventional explicitly probabilistic circuit constructs from computer science, that have randomness injected into them as "coin tosses"[1]. It might seem natural to view these implicit and explicit formulations as being equivalent and consequently, the probabilistic Boolean circuit model based on PBL and the classical randomized circuit model as being interchangeable. While PBL and the associated constructs in the implicit context might be closely related to randomized circuits employing explicit randomness in terms of conventional complexity measures such as size or depth, we will infer that *the implicit variety is more efficient or less expensive, through the measure of energy consumption.* Thus, (physical) energy consumption provides a second approach to distinguishing explicit and implicit approaches beyond semantic differences.

This characterization of the difference between implicitly probabilistic and explicitly random constructs based on energy considerations, builds on prior work: (i) A theoretical framework establishing such a separation based on the energy complexity of probabilistic algorithms and deterministic algorithms (of identical time complexity) in the BRAM model of computation [50] as well as in a model employing networks of switches [51] and (ii) An empirical demonstration of the energy efficiency of CMOS devices rendered probabilistic by thermal noise, referred to as probabilistic CMOS or PCMOS [11, 39, 40]. Finally, moving beyond circuit based models and considering computational models with a notion of *state* in the form of a PA, we show that these gains, or energy advantages persist. To demonstrate this, we consider the transition function of a PA and show that any transition function of such an automaton realized as an implicitly probabilistic circuit consumes less energy than an equivalent explicitly realized circuit.

1.1 A Short Note on Related Work

Our work on PBL has connections to three distinct areas with a potential for further research: *mathematical logic*, *computer science*, and applications to *electrical engineering*. We describe the connections in greater detail and sketch future directions of inquiry in Section 6. In this section, we briefly distinguish our work from prior results of a similar theme.

Historically, developments in probability theory have been intertwined with advances in logic with *probable*

[1] In this work, we distinguish between *probabilistic* and *randomized* Boolean circuits. We use the terminology "probabilistic Boolean circuits" to refer to Boolean circuits whose gates correspond to one of the three probabilistic operators of PBL and hence are implicitly probabilistic. On the other hand, we use the terminology "randomized Boolean circuits" to refer to conventional Boolean circuits, some of whose inputs may be random variables and hence have probability explicitly injected into them.

inference as one of the main motivators. As a background to probable inference, we first consider the rule of inference in propositional logic. In propositional logic, if P and Q are sentences then by the rule of Modus ponens [42] $((P \rightarrow Q), P)$ logically entails Q. Certain real world situations merit the question, *If P is not known to be true with certainty, is Q true ?*. For example, in several artificial intelligence applications and expert systems, rules and data are not known with certainty and only strongly indicated by evidence. With this as motivation, several researchers (see Cox [15], Nilsson [49], Fagin and Halpern [22], Fagin, Halpern and Megiddo [23], for example) have generalized logic to deal with uncertainties. In such logics, sentences are associated with probabilities or *confidences* using which, rules of inference yield probabilities of other sentences. It should be noted that the connectives themselves are deterministic.

In contrast, the individual variables in PBL are associated with truth values from the set $\{0, 1\}$, and are deterministic, while probability is incorporated into PBL through probabilistic operators. Our dual approach to the treatment of probability and logic stems in part from differing motivations. Whereas the former work has been motivated by inference in the presence of *probabilistic truth*, our work has been motivated by the characterization of models of computing (more specifically Boolean circuits) elements (such as gates) of which which may exhibit probabilistic behavior.

Specifically, in the context of computing devices whose physical realizations may be probabilistic, computing elements such as gates susceptible to probabilistically quantified erroneous behavior were studied in the context of unreliable computing elements, with an aim of overcoming such probabilistic (unreliable) behavior. In this context, von-Neumann's classical work [65] was inspired by the need for realizing reliable computing in the presence of faults. Other researchers have improved upon von Neumann's techniques to calculate the necessary and sufficient amount of redundancy to realize Boolean functions [19, 20]. This line of work culminated on Pippenger's demonstration of reliably realizing Boolean functions, with constant multiplicative redundancy of gates susceptible to noise, and hence error [52, 53, 54]. More recently, in the more technological context of CMOS transistors, Bahar et al. demonstrate methods for improving the noise immunity of logic circuits by using techniques based on Markov Random Fields [2, 48].

In all of these cases, a combinational logic element or a gate, is deemed to be either erroneous or correctly functioning—there is no attempt to characterize and use it with varying degrees of reliability characterized through the probability of correctness (parameter) p, q or r. More significantly, none of these earlier formulations attempted to distinguish the explicit and implicit forms in general, and through a complexity measure in particular. Our work in part is intended to help redress this situation.

1.2 Roadmap

The rest of this paper is organized as follows. The syntax of probabilistic Boolean formulae and the structure of well formed probabilistic Boolean formulae are outlined in Section 2. In Section 2.3, we introduce probabilistic Boolean truth tables as an aid to interpreting the meaning of truth and satisfiability of probabilistic formulae. Next, we formalize this notion of truth characterized by probabilistic truth tables, through the (semantic) concept of an *event set* in Section 3, and provide a framework for expressing an equivalence between arbitrary probabilistic Boolean formulae. Here, we are able to distinguish the explicit and implicit approaches in a preliminary way through event set semantics. Next, in Section 4 we show that a number of identities from Boolean logic can be extended and demonstrated to be valid in PBL. In Section 4.2, we show that extensions of distributivity and associativity are not preserved, and quantify the degree of non-associativity Δ_n in Section 4.5. A further distinction between PBL and explicitly probabilistic logic is made in Section 5 first in the context of a circuit model. In Section 5.3, we extend this result to models with state through PA [55], and show that such automata based on probabilistic Boolean circuits are more energy efficient than their explicit counterparts based on randomized Boolean circuits. We remark on the implication of this work to technology, Moore's law, discuss related work, conclude and outline directions for future research in Section 6.

2. PROBABILISTIC BOOLEAN LOGIC AND WELL FORMED FORMULAE

Informally, probabilistic Boolean formulae—like their deterministic counterparts—can be constructed from the Boolean constants $0, 1$, Boolean variables, and *probabilistic* Boolean *operators*: *probabilistic disjunction, probabilistic conjunction* and *probabilistic negation*. Probabilistic disjunction, conjunction and negation will be represented by the symbols $\vee_p, \wedge_q$ and $\neg_r$ respectively, where p, q, r are the corresponding probability parameters or *probabilities of correctness*. The probabilities of correctness associated with the disjunction, conjunction and negations operators are such that $\frac{1}{2} \leq p, q, r \leq 1$ and $p, q, r \in \mathbb{Q}$, the set of rationals. Initially, for clarity of exposition and for a model of finite cardinality, we consider only rational probabilities of correctness. We seek the indulgence of the reader and will defer a more detailed discussion of the justification underlying our choice of considering rational probabilities, to Section 3. A pair of probabilistic operators, say in the case of probabilistic disjunction, $\vee_p, \vee_{\hat{p}}$, will be deemed identical whenever $p = \hat{p}$. They will be considered to be *comparable* whenever $p \neq \hat{p}$. Similarly for probabilistic conjunction and negation. Analogous to well-formed Boolean formulae, well formed *probabilistic Boolean formulae* are defined as follows:

(1) Any Boolean variable $x, y, z, \cdots$ and the constants 0,1 are well formed probabilistic Boolean formulae[2].

(2) If F, G are well formed probabilistic Boolean formulae, $(F \vee_p G)$, $(F \wedge_p G)$ and $(\neg_p F)$ are well formed probabilistic Boolean formulae.

Henceforth, we will use the term probabilistic Boolean formula, or PBF to refer to a well-formed probabilistic Boolean formula and the term Boolean formula (BF) to refer to a classical well formed Boolean formula (which is deterministic). In addition, the length of a probabilistic Boolean formula is the number of operators n in the formula. Given a PBF F, we will use $\textsc{var}_F$ to denote the set of variables in F. If $\textsc{var}_F = \phi$, that is if F is a formula over Boolean constants, F will be referred to as a *closed* well-formed probabilistic Boolean formula or a *closed* PBF.

2.1 Boolean Logic Preliminaries

For any Boolean formula or BF J consider the set of its constituent Boolean variables, $\{x_1, x_2, x_3, \cdots, x_k\}$ denoted by $\textsc{bvar}_J$ where $|\textsc{bvar}_J| = k$. Consider any assignment $I \in \langle 0, 1 \rangle^k$. Let J_I be the closed formula obtained by replacing each variable of J with the Boolean constant it is assigned. The value of the formula J, when x_i is assigned the i^{th} element (bit) of I, or equivalently, the value of the formula J_I, will be referred to as the *truth value* of J with (input) assignment I and will be denoted by $T(J_I)$. Given two Boolean formulae J, K, without loss of generality, let $\textsc{bvar}_K \subseteq \textsc{bvar}_J$. If I is an assignment to variables in J, I' is a *consistent assignment* to variables in K if and only if whenever $x_i \in \textsc{var}_K$, x_i is assigned to the same Boolean constant under the assignments I and I'.

Two Boolean formulae J and K where $|\textsc{bvar}_J| = k$ are considered to be equivalent, whenever $T(B_I) = T(C_{I'})$ for all input assignments. We recall that one approach to specifying the truth value of Boolean

[2] Typically we shall denote Boolean variables using lower case alphabets.

Input x y z	Truth Value
0 0 0	0
0 0 1	0
0 1 0	0
0 1 1	1
1 0 0	0
1 0 1	1
1 1 0	1
1 1 1	1

Figure 1. A Boolean truth table for the formula $(((x \wedge y) \vee (x \wedge z)) \vee (y \wedge z))$

formulae is through a Boolean truth table. A truth table with 2^k, $k > 0$ rows and two columns is illustrated in Figure 1. Conventionally, the first column of each row contains the input assignment, where the n^{th} row, $0 \leq n < 2^k$, corresponds to the k bit binary representation of n, which we denote by N. The second column of each row contains an element of $\{0, 1\}$ where the symbols 1 and 0 denote the *true* and *false* values respectively. Referring to the example in Figure 1, the truth table corresponds to the Boolean formula $(((x \wedge y) \vee (x \wedge z)) \vee (y \wedge z))$. The third row of the table with the input 010, is interpreted as the assignment $\langle x = 0, y = 1, z = 0 \rangle$, and yields the truth value of the formula to be 0 and hence the second column of this row contains a 0. In contrast, the fourth row which contains the input 011, with the symbol 1 in the second column, implying that the value of the formula for this assignment is 1.

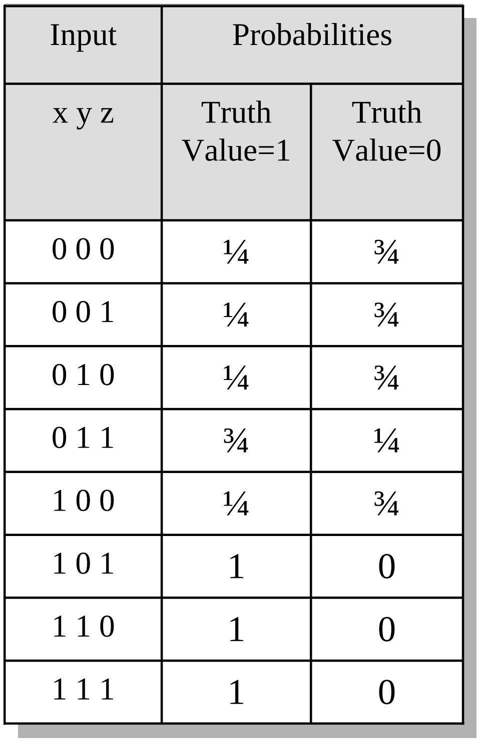
2.2 The Operational Meaning of Probabilistic Boolean Operators

Let F, G, H denote $(x \vee_p y)$, $(x \wedge_q y)$ and $(\neg_r x)$ respectively, and let $T(F_\alpha), T(G_\beta)$ and $T(H_\gamma)$ denote their truth value under the assignments α, β and γ respectively. Then an informal operational approach to assigning or determining "truth" in the case of a PBF is

$$T(F_\alpha) = \begin{cases} \text{Truth value of } (x \vee y) & \text{under the input assignment } \alpha \text{ with probability } p \\ \text{Truth value of } \neg(x \vee y) & \text{under the input assignment } \alpha \text{ with probability } (1-p) \end{cases}$$

$$T(G_\beta) = \begin{cases} \text{Truth value of } (x \wedge y) & \text{under the input assignment } \beta \text{ with probability } q \\ \text{Truth value of } \neg(x \wedge y) & \text{under the input assignment } \beta \text{ with probability } (1-q) \end{cases}$$

$$T(H_\gamma) = \begin{cases} \text{Truth value of } (\neg x) & \text{under the input assignment } \gamma \text{ with probability } r \\ \text{Truth value of } (x) & \text{under the input assignment } \gamma \text{ with probability } (1-r) \end{cases}$$



Input	Probabilities	
x y z	Truth Value=1	Truth Value=0
0 0 0	¼	¾
0 0 1	¼	¾
0 1 0	¼	¾
0 1 1	¾	¼
1 0 0	¼	¾
1 0 1	1	0
1 1 0	1	0
1 1 1	1	0

Figure 2. A probabilistic Boolean truth table for the PBF $(((x \wedge_1 y) \vee_1 (x \wedge_1 z)) \vee_1 (y \wedge_{3/4} z))$

2.3 Probabilistic Boolean Formulae and their Truth Tables

Let us now extend this notion of truth with associated probability to arbitrary formulae in PBL. Our initial approach will be through a *probabilistic Boolean truth table.* As shown in Figure 2 and analogous to conventional truth tables, in a probabilistic truth table with $l = 2^k$ $(k > 0)$ rows and three columns, the first column of the n^{th} row contains N, the k bit binary representation of n, $0 \leq n < 2^k$. The second and the third columns of the n^{th} row contain rational numbers $0 \leq p_n, q_n \leq 1$ where $p_n + q_n = 1$. The first column of the n^{th} row, which contains the binary representation N of n, is an assignment of Boolean constants to the variables in the formula as shown in the Figure 2. The second column of the n^{th} row, which is labeled p_n, represents the fact that the probability that value of the formula F_N is 1 is p_n for the assignment N, whereas the third column labeled q_n is the probability that the value of the *same formula* for the *same input assignment* is 0. For example, if F is a PBF over the variables x, y, z, and considering the row of the table with the assignment 010, the probability that the value of F is 1 for this assignment is $p_2 = 1/4$ whereas the probability that the value of F is 0 is $q_2 = 3/4$.

3. THE EVENT SET SEMANTICS OF PBL

In Section 2.2, we have introduced an operational meaning of PBL and established the fact that probabilistic Boolean formulae in this logic can be represented by probabilistic Boolean truth tables. Given a PBF, intuitively, for any assignment of values to the variables in the PBF, the value of the PBF is determined by

(i) the operators (probabilistic disjunction, conjunction or negation) in the PBF and (ii) the probabilities of correctness of each of the operators. Whereas the former captures the notion of the "underlying" deterministic Boolean formula, the latter characterizes the probability that the truth value of the PBF matches that of the underlying deterministic Boolean formula. Note that this probability might vary with the input assignments, and in general, indeed it does. Based on these two observations, we will formalize the meaning of PBF in PBL based on the meaning of Boolean logic, and the frequentist interpretation of probability [64], for a given input I.

3.1 A Frequentist View of PBL

If F is any PBF and I is an assignment to variables in F, then F_I will be used to denote the closed PBF where every variable in F is replaced by the Boolean constant it is assigned. We will use the symbol $\overset{r}{=}$ to mean "is equal to with a probability r". Also, for any assignment I to the variables in F, we will use $\mathscr{S}_I$ to denote the *sentence* $F_I \overset{r}{=} 1$ (and $\bar{\mathscr{S}}_I$ to denote the sentence $F_I \overset{\bar{r}}{=} 0$). Our goal is to provide a semantic framework that gives meaning to sentences formally. To this end, consider a closed PBF F_I of the form $(1 \vee_p 0)$ where $p = 3/4$. We recall that from the operational meaning given to the $\vee_p$ operator, the probability that the truth value of F_I is equal to $T(1 \vee 0)$ is $3/4$, whereas the probability that the truth value of F_I is equal to $T(\neg(1 \vee 0))$ is $1/4$. Since the symbol $\overset{r}{=}$ means "*is equal to with a probability* r", the sentence $\mathscr{S}_I$ which denotes $(1 \vee_p 0) \overset{r}{=} 1$ is *valid* if and only if $p = r$; $\mathscr{S}_I$ is an *invalid* sentence otherwise.

Considering $\mathscr{S}_I$, under the frequentist interpretation of probability, an infinite sequence Υ consists of two types of events, each associated with a sentence in classical (deterministic) Boolean logic as follows: in our example (Figure 3(b)), one type of event corresponds to those instances where F_I "behaves like" $(1 \vee 0)$ and hence the event is associated with the sentence in Boolean logic $(1 \vee 0) = 1$, whereas the latter corresponds to those instances where F_I "behaves like" $\neg(1 \vee 0)$ and hence the event is associated with the sentence $\neg(1 \vee 0) = 0$. This concept is illustrated in Figure 3(a) which shows the infinite sequence of events, each associated with a sentence. With $p = 3/4$, we note that the relative frequency of the events which correspond to sentences of the form $(1 \vee 0) = 1$ is $3/4$. Thus, our semantic interpretation of the validity of a sentence in our example, is based on the validity (and the ratio) of the two types of sentences in Boolean logic, $(1 \vee 0) = 1$ and $\neg(1 \vee 0) = 0$. The first type of event is characterized by the sentence $(1 \vee 0) = 1$ being *valid* whereas the second type of event is characterized by the *validity*[3] of the sentence $\neg(1 \vee 0) = 0$. The probability parameter p determines the relative frequency of these events as n, the number of events $\to \infty$.

Rather than considering the infinite sequence of events Υ, we will use its finite representation or encoding of probability parameter, as follows: in our example, we consider a set (an "event set") of 4 distinct events, three of which correspond to the sentence in Boolean logic, $(1 \vee 0) = 1$ and one event which corresponds to $\neg(1 \vee 0) = 0$. Such a succinct representation for the infinite sequence in Figure 3(a) is shown in Figure 3(b). To reinforce this point further, consider longer formulae, say H, of the form $((x \vee_p y) \vee_q z)$ where $p = 3/4$ and $q = 5/6$. Again, we will consider the sequence which corresponds to the sentence $\mathscr{S}'_I$ which denotes $H \overset{r}{=} 1$ where I denotes the assignment $\langle x = 1, y = 0, z = 1\rangle$. The sequence Υ' associated with $\mathscr{S}'_I$ would consist of events $((1 \vee 0) \vee 1) = 1$, $(\neg(1 \vee 0) \vee 1) = 1$, $\neg((1 \vee 0) \vee 1) = 0$ or $\neg(\neg(1 \vee 0) \vee 1) = 0$ with relative frequencies of $15/24$, $5/24$, $3/24$ and $1/24$ respectively. This infinite sequence may be represented

[3] For a notion of validity of sentences and the semantics of Boolean logic—in fact the whole of predicate calculus—please see Mendelson [42].

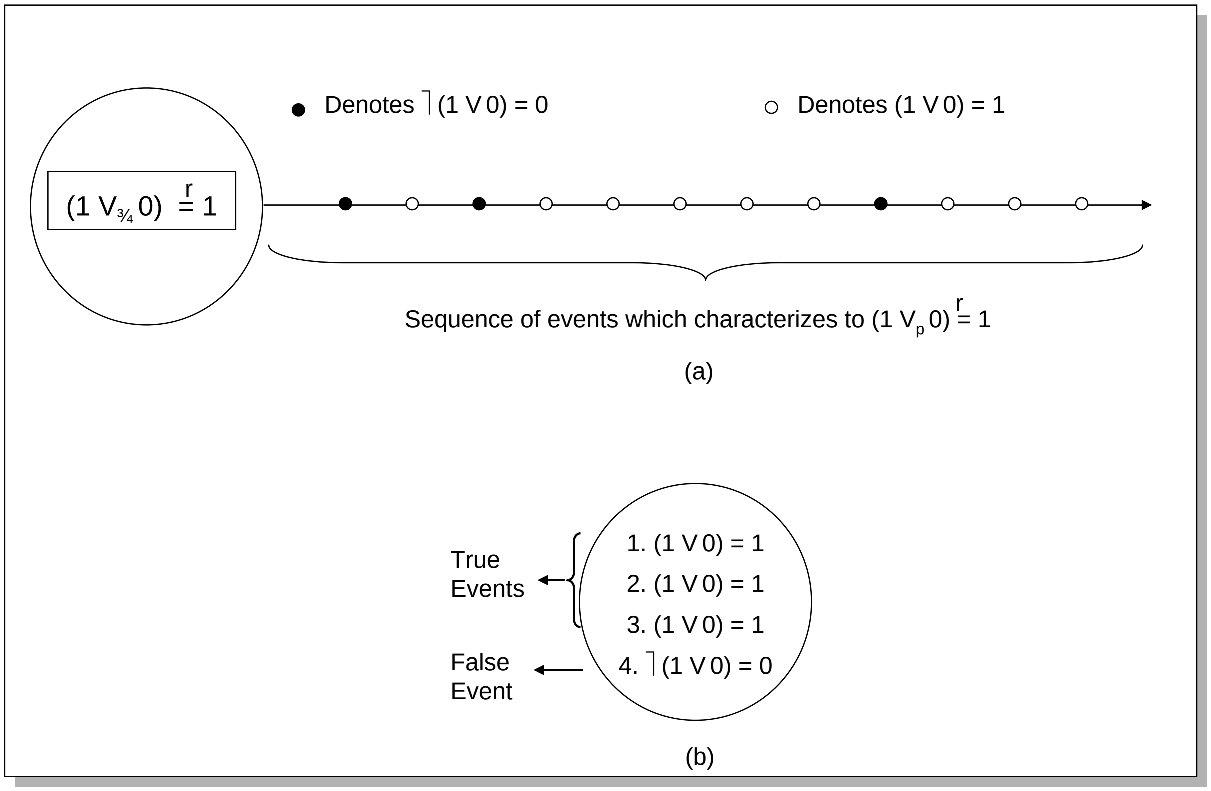


Figure 3. (a) A frequentist interpretation of a sentence $(1 \vee_{\frac{3}{4}} 0) \overset{r}{=\!=} 1$ in PBL through an infinite sequence of events (b) a succinct representation of this sequence as an event set

in a succinct manner with a set of 24 elements, 15 of which are copies[4] of the sentence $((0 \vee 1) \vee 0) = 1$, 5 elements being copies of $(\neg(0 \vee 1) \vee 0) = 0$, 3 elements being copies of $\neg((0 \vee 1) \vee 0) = 0$ and a single element of the form $(\neg(0 \vee 1) \vee 0) = 0$. From such a succinct representation, the sequence Υ' may be generated by picking elements uniformly at random and constructing an infinite sequence of such trials. Since events are picked at random, the sequence Υ' satisfies both the axiom of convergence and the axiom of randomness (please see Reichenbach [58] and Section 3.1.1 below) in the frequentist interpretation of probability.

A motivation towards developing PBL is to design efficient algorithms to synthesize implicitly probabilistic circuits and the computational efficiency of such algorithms is dependent on the size of the event sets. Therefore, we expect that it is advantageous to represent the sequence Υ' as a finite set, which is the basis for restricting the probability parameter of the operators of PBL to be the member of the set of rationals $\mathbb{Q}$. We note that if probabilities are drawn from the unit interval $[0, 1]$, the cardinality of the event set will not be finite and a notion of probability measure [37] has to be introduced. However, we note that the subsequent development of the semantics of PBL can be extended naturally to the case where the probability

[4] Since our intention is to characterize the elements as a set, for element distinctness, we ensure that the copies of each sentence is indexed uniquely from the set of naturals $\{0, 1, 2, \ldots\}$, and thus individual copies can be distinguished from each other through this index. For ease of exposition, we will omit these indices in the body of the paper, but will include it in a rigorous formulation of these concepts in Appendix A.

parameters of the operators are chosen from the interval $[0, 1]$.

3.1.1 *A Digression into The Frequentist Interpretation of Probability.* The concept of probability has had differing *interpretations*, where the two important interpretations have been the *frequentist* approach, championed by Venn [63], von Mises [64], Reichenbach [58], and others, and the *Bayesian* interpretation, of which de Finetti [17], Ramsey [57], Jaynes [30] and others are prominent proponents (for a detailed discussion, please see Cox [14] and Bergmann [3]). The word "frequentist" is used to refer to the proponents as well as to the *frequency theoretic* interpretation of probability, and is attributed to Kendall [33]. Efron [21] outlines the controversies between the Bayesian interpretation and the frequentist interpretation). The notion of probability under the frequentist interpretation, is outlined elegantly by von Mises [64] *"It is possible to speak about probabilities only in reference to a properly defined collective"* and Bergmann [3] *"Probability theory deals with mass phenomena and repetitive events"*. Whereas, the interpretation of probability according to the Bayesian approach, quoting Cox is *"A relation between a hypothesis and a conclusion, corresponding to the degree of rational belief and limited by the extreme relations of certainty and impossibility"*.

Our motivation in choosing the frequentist approach is based on the fact that we wish to apply methods based on our interpretation of PBL, to derive techniques not only for designing and synthesizing integrated circuits, but also for verifying them. Here, measurement to ascertain the behavior of probabilistic Boolean circuits is crucial. Ascertaining the behavior would typically involve testing the circuit not only over a large number of inputs, but also over a large number of trials without using known priors[5], resulting in a sequence of outcomes which are elements of the "event set".

The frequentist approach, broadly speaking, defines the probability of an event A in a sequence of trials, as simply the ratio of the number of occurrences of A to the total number of trials, as the number of trials tends to infinity. For example, the probability of occurrence of heads in any toss of a coin would simply be the ratio of the number of occurrences of heads to the total number of trials in an infinite sequence of trials. This interpretation, while satisfying the requirement of ascertainability—in principle, probabilities can be assigned to each event—introduces paradoxes. von Mises addresses these concerns through the axiom of convergence and the axiom of randomness. In particular, the axiom of convergence states that the *limiting* relative frequency of any event exists in a sequence of infinite trials. The axiom of randomness states that this limiting relative frequency of any event in an infinite sequence and the limiting relative frequency in any infinite sub-sequence are the same, thereby attributing some property of uniform "randomness" to the infinite sequence under consideration. This notion of "similarity" of an infinite sequence to any infinite sub sequence was formalized by Church [13] and ultimately refined by Kolmogorov [38] and Chaitin [8].

3.2 A Interpretation of PBF for a Fixed Assignment Through Event Sets

With the frequentist interpretation of probability as a background, we will define the succinct representation of the infinite sequence of trials which characterizes a sentence in PBF. Revisiting the example in Figure 3, let $\mathscr{S}_I$ denote $(1 \vee_p 0) \overset{r}{=} 1$ and Υ is the sequence which characterizes $\mathscr{S}_I$. We will refer to $\mathbf{E}_{\mathscr{S},I}$, the succinct representation of Υ as an *event set* of $\mathscr{S}_I$. In our example, any *event* $E \in \mathbf{E}_{\mathscr{S},I}$ will be associated with either the sentence $(1 \vee 0) = 1$ in Boolean logic, or with the sentence $\neg(1 \vee 0) = 0$. If $p = m/n$ ($p \in \mathbb{Q}$), $\mathbf{E}_{\mathscr{S},I}$ is a set of n elements (each element referred to as an event), m of which correspond to $(1 \vee 0) = 1$ and the rest to

[5] For an eloquent defense of the use of known priors, please see Jaynes [30], whose book is reviewed in a most stimulating manner by Diaconis [18].

$\neg(1 \vee 0) = 0$. We will refer to the former type of events as being true whereas the latter type of events will be deemed to be false. Intuitively, the true events are witnesses to the formula under assignment I yielding a value of 1 whereas the false events correspond to those which yield a value of 0. Let $\psi(\mathbf{E}_{\mathscr{S},I})$ represent the fraction of the event set made up of copies of true events, the sentence $(1 \vee 0) = 1$.

Revisiting Figure 3, if $r = 3/4$, $\mathscr{S}_I$ is a valid sentence and it is invalid otherwise. We can either say "$r = 3/4$ is the value for which the sentence $F_I \stackrel{r}{=} 1$ is valid", or this fact can be stated as "F is *satisfied with probability* $r = 3/4$ *for the assignment* I". Given the event set $\mathbf{E}_{\mathscr{S},I}$ the rational number r and the Boolean constant 1, they are said to be in a relationship R, that is $(1, r, \mathbf{E}_{\mathscr{S},I}) \in R$, if and only if $\psi(\mathbf{E}_{\mathscr{S},I}) = r$. If $(1, r, \mathbf{E}_{\mathscr{S},I}) \in R$, then the sentence $(1 \vee_p 0) \stackrel{r}{=} 1$ is said to be *valid* under our interpretation; it is *invalid* otherwise.

Now consider the assignment $\bar{I}$ which denotes $\langle x = 0, y = 0\rangle$. As shown in Figure 4(a), a majority of the events in the event set are false events. In this context, it is more natural to reason about the validity of the sentence $\bar{\mathscr{S}_{\bar{I}}}$, which denotes $F_{\bar{I}} \stackrel{\bar{r}}{=} 0$ or $(0 \vee_p 0) \stackrel{\bar{r}}{=} 0$. If $\bar{\psi}(\mathbf{E}_{\bar{\mathscr{S}},\bar{I}})$ is the fraction of events in $\mathbf{E}_{\bar{\mathscr{S}},\bar{I}}$ which are copies of false events, $\bar{\mathscr{S}_{\bar{I}}}$ is a valid sentence if and only if $\bar{r} = \bar{\psi}(\mathbf{E}_{\bar{\mathscr{S}},\bar{I}})$. In this case, $\bar{r} = 3/4$ is the value for which the sentence $F_{\bar{I}} \stackrel{\bar{r}}{=} 0$ is valid. Equivalently, we can say that F is *unsatisfied with probability* $\bar{r} = 3/4$ *for the assignment* $\bar{I}$. We note that $\bar{\psi}(\mathbf{E}_{\mathscr{S},I}) = 1 - \psi(\mathbf{E}_{\mathscr{S},I})$ and therefore, a sentence $F_I \stackrel{r}{=} 1$ is a valid sentence if and only if $F_I \stackrel{\bar{r}}{=} 0$ is a valid sentence, where $\bar{r} = (1 - r)$. For ease of exposition, in the body of the paper and unless specified otherwise, we consider only sentences of the form $F_I \stackrel{r}{=} 1$, and reason about the probabilities with which F is satisfied. A rigorous formulation of validity of sentences in each case—sentences of the form $F_I \stackrel{r}{=} 1$ as well as those of the form $F_{\bar{I}} \stackrel{\bar{r}}{=} 0$—is treated in a complete manner in Appendix A.

We observe that, as illustrated in Figure 4(b), for a formula F, for each of the three remaining assignments $I \in \{\langle x = 0, y = 1\rangle, \langle x = 1, y = 0\rangle, \langle x = 1, y = 1\rangle\}$, three valid sentences, each of the form $F_I \stackrel{r}{=} 1$ can be constructed, and each sentence is associated with its own event set. The collection of events sets and the notion of validity provides a *model* [42] in the sense of symbolic logic.

Consider any PBF G of the form (z) where z is a Boolean variable. For the assignment I which assigns 0 to z, if $\mathscr{S}_I$ is the sentence $G_I \stackrel{r}{=} 1$, the event set $\mathbf{E}_{\mathscr{S},I}$ consists of one event determined by the sentence in Boolean logic, $(0) = 0$. Similarly, for the assignment I' which is $\langle z = 1\rangle$, the event set $\mathbf{E}_{\mathscr{S},I'}$ consists of one event determined by the sentence $(1) = 1$.

We will now consider the event set of a PBF H of length $k+1$ where $k \geq 0$. To illustrate the way in which event sets of sub-formulae combine, we consider an example where F and G are the formulae $(x \vee_q y)$ and (z) respectively, where H is of the form $(F \vee_p G)$, $q = 3/4$ and $p = 5/6$. We will consider the assignment $I = \langle x = 1, y = 0, z = 1\rangle$ to the variables in H, where $I' = \langle x = 1, y = 0\rangle$ and $I'' = \langle z = 1\rangle$ are the corresponding consistent assignments to F and G. Consider the valid sentences $\mathscr{S}_I, \mathscr{S}'_{I'}, \mathscr{S}''_{I''}$ which denote $H_I \stackrel{r}{=} 1$, $F_{I'} \stackrel{r'}{=} 1$ and $G_{I''} \stackrel{r''}{=} 1$ respectively, where $\mathbf{E}_{\mathscr{S},I}$, $\mathbf{E}_{\mathscr{S}',I'}$ and $\mathbf{E}_{\mathscr{S}'',I''}$ are the event sets of $\mathscr{S}_I$, $\mathscr{S}'_{I'}$ and $\mathscr{S}''_{I''}$ respectively. Referring to Figure 4, the event set of $\mathscr{S}'_{I'}$ consists of 4 events, 3 of which are true Boolean sentences $(0 \vee 1) = 1$ and one false Boolean sentence $\neg(0 \vee 1) = 0$. This is shown in Figure 5(a), where for the ease of exposition, we omit the indices of the events. With $z = 1$, as shown in Figure 5(b), the event set of $\mathscr{S}''_{I''}$ has one true event associated with the Boolean sentence $(1) = 1$. Let $\tilde{\mathbf{E}} = \mathbf{E}_{\mathscr{S}',I'} \times \mathbf{E}_{\mathscr{S}'',I''}$. As shown in Figure 5(c), we note that $|\tilde{\mathbf{E}}| = 4 \times 1 = 4$, and any element of $\tilde{\mathbf{E}}$ is of the form $(B = c, \hat{B} = \hat{c})$, where $B, \hat{B}$ are closed BF and $c, \hat{c} \in \{0, 1\}$. For each element of $\tilde{\mathbf{E}}$, as shown in Figure 5(d), we create 5 copies (since $p = 5/6$) each of the form $(B \vee \hat{B}) = T(c \vee \hat{c})$ and 1 element of the form $\neg(B \vee \hat{B}) = T(\neg(c \vee \hat{c}))$

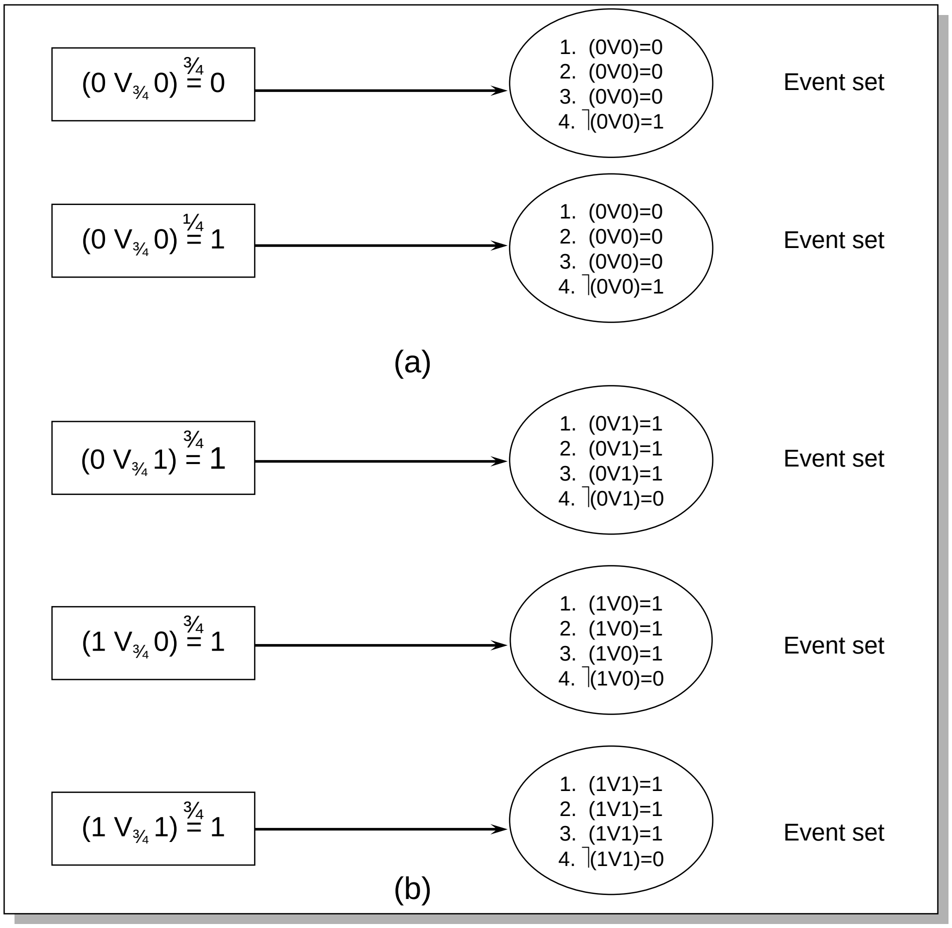


Figure 4. (a) The event set for the valid sentence $(0 \vee_{\frac{3}{4}} 0) \xlongequal{\frac{3}{4}} 0$ and $(0 \vee_{\frac{3}{4}} 0) \xlongequal{\frac{1}{4}} 1$ (b) three valid sentences and their event sets for the three remaining assignments to $(x \vee_{\frac{3}{4}} y)$

to get $\mathbf{E}_{\mathscr{S},I}$. Hence it follows that $|\mathbf{E}_{\mathscr{S},I}| = 6 \times |\tilde{\mathbf{E}}| = 24$, of which 20 events are true and the rest are false. Therefore, whenever $r = 5/6$, $\mathscr{S}_I$ is a valid sentence, since $P_H = \psi(\mathbf{E}_{\mathscr{S},I}) = 20/24 = 5/6$. A rigorous formulation can be found in Appendix A. We will however describe some attributes of the event sets for sentences which correspond to arbitrary formulae and assignments. These attributes will be used in Section 4 to characterize some of the properties of PBL.

In general, let H be of the form $(F \vee_p G)$ where $p = m/n$. To reiterate, for any assignment I to H, let I' and I'' denote the corresponding consistent assignment to variables in F and G respectively. Let the number of events in $\mathbf{E}_{\mathscr{S}',I'}$ be denoted by the symbol a, and let $|\mathbf{E}_{\mathscr{S}',I'}| = b$. Similarly, let the number of true events in $\mathbf{E}_{\mathscr{S}'',I''}$ be denoted by the symbol c, and let $|\mathbf{E}_{\mathscr{S}'',I''}| = d$.

OBSERVATION 3.2.1. *Under assignment I, $|\mathbf{E}_{\mathscr{S},I}|$ is (bdn) where $\mathbf{E}_{\mathscr{S},I}$ has $(acm + a(d-c)m + (b-a)cm + (b-a)(d-c)(n-m))$ true events. Therefore, if P_F, P_G and P_H denote the probabilities with which $F_{I'}, G_{I''}$ and H_I are respectively satisfied, $P_H = (P_F)(P_G)p + (1-P_F)(P_G)p + (P_F)(1-P_G)p + (1-P_F)(1-P_G)(1-p)$.*

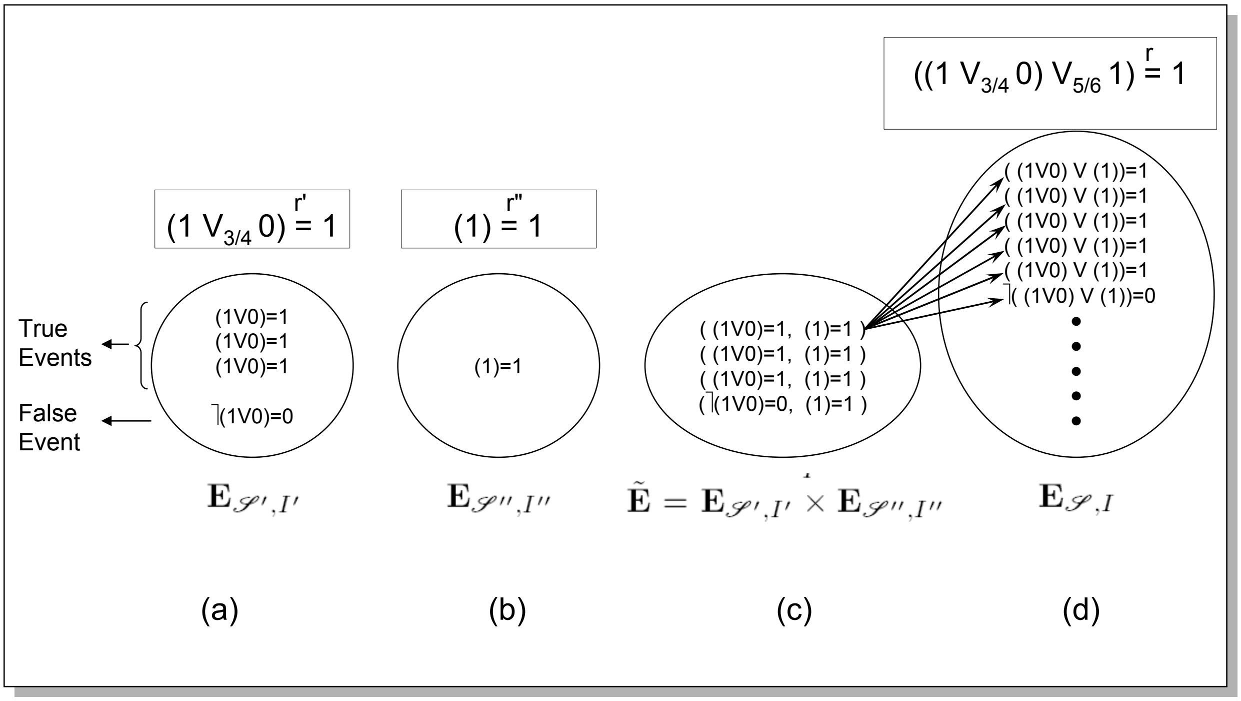


Figure 5. (a) Event set $\mathbf{E}_{\mathscr{S}',I'}$ of $(1 \vee_{\frac{3}{4}} 0) \xlongequal{r'} 1$ (b) event set $\mathbf{E}_{\mathscr{S}'',I''}$ of $(1) \xlongequal{r''} 1$ (c) $\tilde{\mathbf{E}} = \mathbf{E}_{\mathscr{S}',I'} \times \mathbf{E}_{\mathscr{S}'',I''}$ (d) constructing the event set for $((1 \vee_{\frac{3}{4}} 0) \vee_{\frac{5}{6}} 1) \xlongequal{r} 1$ from $\tilde{\mathbf{E}}$.

Proof. Based on the frequentist interpretation of PBL and the event set semantics, we know that the probability that H is satisfied for the assignment I, is the ratio of the number of true events to the total number of events in $\mathbf{E}_{\mathscr{S},I}$. Hence $P_H = \psi(\mathbf{E}_{\mathscr{S},I})$. Similarly, $P_F = \psi(\mathbf{E}_{\mathscr{S}',I'}) = a/b$, $P_G = \psi(\mathbf{E}_{\mathscr{S}'',I''}) = c/d$. The number of true events in $\mathbf{E}_{\mathscr{S},I}$ is $(acm+a(d-c)m+(b-a)cm+(b-a)(d-c)(n-m))$ and $|\mathbf{E}_{\mathscr{S},I}| = (bdn)$ (from Observation A.0.1 in Appendix A). Hence,

$$\psi(\mathbf{E}_{\mathscr{S},I}) = \frac{(acm + a(d-c)m + (b-a)cm + (b-a)(d-c)(n-m))}{bdn} \quad \text{or}$$
$$P_H = \psi(\mathbf{E}_{\mathscr{S},I}) = (P_F)(P_G)p + (1-P_F)(P_G)p + (P_F)(1-P_G)p + (1-P_F)(1-P_G)(1-p)$$

□

Note: Again, we note that there might exist an assignment I, such that a majority of events in $\mathbf{E}_{\mathscr{S},I}$ may be false events (and hence $P_H < 1/2$). In this context, it is more natural to reason about the validity of the sentence $\bar{\mathscr{S}}_I$ which denotes $H_I \xlongequal{\bar{r}} 0$, and the probability with which H_I is unsatisfied rather than P_H, the probability with which it is satisfied. However, since Observation 3.2.1 is only a combinatorial relation between the event sets of $\mathscr{S}'_{I'}, \mathscr{S}''_{I''}$, the probability parameter p, and the event set of $\mathscr{S}_I$, we have derived a relation using the function ψ. In combinatorial arguments such as in Observation 3.2.1, it is sufficient to use the function ψ without having to to explicitly invoke $\bar{\psi}$ keeping in mind that for any event set $\mathbf{E}$, $\psi(\mathbf{E}) = (1 - \bar{\psi}(\mathbf{E}))$.

Akin to Observation 3.2.1, similar relationships between the event sets can be established for PBF of the form $H = (F \wedge_p G)$ and $H = \neg F$ as follows:

Observation 3.2.2. *If H denotes $(F \wedge_p G)$, $|\mathbf{E}_{\mathscr{S},I}| = (bdn)$ where $acm + (b-a)c(n-m) + (b-a)(d-c)(n-m) + (a)(d-c)(n-m)$ events in $\mathbf{E}_{\mathscr{S},I}$ are correct events. Furthermore, with $P_F = \psi(\mathbf{E}_{\mathscr{S}',I'}) = a/b$ and $P_G = \psi(\mathbf{E}_{\mathscr{S}'',I''}) = c/d$, $P_H = \psi(\mathbf{E}_{\mathscr{S},I}) = (P_F)(P_G)p + (1-P_F)(P_G)(1-p) + (P_F)(1-P_G)(1-p) + (1-P_F)(1-P_G)(1-p)$.*

Observation 3.2.3. *If H denotes $(\neg_p F)$, $|\mathbf{E}_{\mathscr{S},I}| = bn$ where $a(n-m) + (b-a)(m)$ events in $\mathbf{E}_{\mathscr{S},I}$ are correct events. Furthermore with $P_F = \psi(\mathbf{E}_{\mathscr{S}',I'}) = a/b$, $P_H = \psi(\mathbf{E}_{\mathscr{S},I}) = (P_F)(1-p) + (1-P_F)p$.*

3.2.1 *Equivalence of* PBF *Through Event Sets.* Consider two formulae H and H' where $\text{VAR}_H \subseteq \text{VAR}_{H'}$ (or vice-versa). Then H and H' are equivalent under the assignment I (where I' is the corresponding consistent assignment) if and only if

$$\psi(\mathbf{E}_{\mathscr{S},I}) = \psi(\hat{\mathbf{E}}_{\mathscr{S}',I'})$$

Finally PBF H and H' are equivalent, denoted $H \equiv H'$, if they are equivalent for every assignment $I \in \mathbf{I}$ (we claim without proof that the individual event sets $\mathbf{E}_{\mathscr{S},I}$ for a sentence $\mathscr{S}$ and its input $I \in \mathbf{I}$ can be combined across all the inputs to yield a single finite representation common to all inputs. We will introduce such a specification in a future report centered around the question of synthesizing circuits from PBL specifications).

4. THE IDENTITIES OF PROBABILISTIC BOOLEAN LOGIC

Through the construct of event sets and the accompanying notion of equivalence of PBF, we will now characterize some identities of PBL in Section 4.1. Specifically, we show that several of the identities of conventional Boolean logic, such as commutativity, are preserved in PBL. Also, identities such as that introduced by DeMorgan [66], which relate pairs of dual logical operators—$\vee$ and $\wedge$ in conventional Boolean logic for example—are preserved in a suitably modified manner as described below. Properties such as distributivity and associativity are *not* preserved. We will use the letters, p, q, r, a, b, c to denote probabilities where as before, $1/2 \leq p, q, r, a, b, c \leq 1$ and $p, q, r, a, b, c \in \mathbb{Q}$.

4.1 Classical Identities That are Preserved

We have enumerated the significant identities of PBL in Table 4.1. As an illustrative example, let us consider commutativity (identity (1) in Table 4.1). Now, consider F and G which denote $(x \vee_p y)$ and $(y \vee_p x)$ respectively, where $p = m/n$. For any assignment I, in particular $\langle x = 1, y = 0 \rangle$, let $\mathbf{E}_{F,I}$ be the event set of F. In $\mathbf{E}_{F,I}$, m events are associated with $(1 \vee 0) = 1$ and hence associated with $(0 \vee 1) = 1$ since $(1 \vee 0) \equiv (0 \vee 1)$ in classical Boolean logic. Similarly, $n-m$ events in $\mathbf{E}_{F,I}$ are associated with the $\neg(1 \vee 0) = 1$ and hence $\neg(0 \vee 1) = 1$. Similarly for each possible input assignment $I \in \{\langle x = 0, y = 0 \rangle, \langle x = 0, y = 1 \rangle, \langle x = 1, y = 0 \rangle, \langle x = 1, y = 1 \rangle\}$. Hence, from the definition of equivalence of PBF, $(x \vee_p y) \equiv (y \vee_p x)$, or the operator $\vee_p$ is commutative[6].

[6] A straight forward induction will allow us to extend this to PBF of arbitrary length.

1. Commutativity	$(x \vee_p y) \equiv (y \vee_p x)$ $(x \wedge_p y) \equiv (y \wedge_p x)$
2. Double Complementation	$\neg_q(\neg_p x) \equiv \neg_p(\neg_q x)$ $\neg_p 0 \equiv \neg_1(\neg_p 1)$ $\neg_p 1 \equiv \neg_1(\neg_p 0)$
3. Operations with 0 and 1	$(0 \wedge_p x) \equiv (\neg_p 1)$ $(1 \wedge_p x) \equiv \neg_1(\neg_p x)$ $(0 \vee_p x) \equiv \neg_1(\neg_p x)$ $(1 \vee_p x) \equiv (\neg_p 0)$
4. Identity	$(x \vee_p x) \equiv \neg_1(\neg_p x)$ $(x \wedge_p x) \equiv \neg_1(\neg_p x)$
5. Probabilistic Tautology	$(x \vee_p (\neg_1 x)) \equiv \neg_p 0$ $(x \wedge_p (\neg_1 x)) \equiv \neg_p 1$
6. Probabilistic DeMorgan Identity	$\neg_p(x \vee_q y) \equiv (\neg_1 x) \wedge_r (\neg_1 y)$ $\neg_p(x \wedge_q y) \equiv (\neg_1 x) \vee_r (\neg_1 y)$ where $r = pq + (1-p)(1-q)$

Table 1. Identities of PBL

4.2 Identities that are not Preserved

Surprisingly, not all properties from conventional Boolean logic can be extended to the probabilistic case. In particular, associativity, distributivity and absorption as stated in Boolean logic are not preserved in PBL.

4.2.1 *Associativity.* Let F and G denote $(x \vee_p (y \vee_p z))$ and $((x \vee_p y) \vee_p z)$ respectively, where VAR $= \{x, y, z\}$ is the set of variables in F as well as in G.

THEOREM 1. *There exists an assignment I to* VAR *such that $\psi(\mathbf{E}_{F,I}) \neq \psi(\mathbf{E}_{G,I})$ and therefore $F \not\equiv G$. Hence* PBL *is not associative.*

PROOF. Consider the assignment I which denotes $\langle x = 1, y = 0, z = 0\rangle$. If $\mathbf{E}_{F,I}$ and $\mathbf{E}_{G,I}$ are the event sets of F_I and G_I respectively, it follows from the definition of event sets, that $\psi(\mathbf{E}_{F,I}) = p^2$ whereas $\psi(\mathbf{E}_{G,I}) = p^2 + (1-p)^2$ (from Observation 3.2.1). Hence there exist values of p, $1/2 \leq p \leq 1$ such that $\mathbf{E}_{F,I} \not\approx \mathbf{E}_{G,I}$, and therefore $F \not\equiv G$. □

4.2.2 *Distributivity.* Consider as a natural extension of distributivity in the PBL context, expressed as

$$(x \vee_p (y \wedge_q z)) \equiv ((x \vee_a y) \wedge_b (x \vee_c z))$$

We shall now show that this identity does not hold for PBL.

THEOREM 2. *There exist p, q, $1/2 < p, q < 1$ such that $(x \vee_p (y \wedge_q z)) \not\equiv ((x \vee_a y) \wedge_b (x \vee_c z))$ for any $1/2 \leq a, b, c \leq 1$, and therefore $\vee_p$ does not distribute over $\wedge_q$.*

PROOF. Without loss of generality, let F represent $(F' \vee_p F'')$ where F', F'' respectively denote (x), $(y \wedge_q z)$, and G denotes the formula $((x \vee_a y) \wedge_b (x \vee_c z))$. In particular, let $1/2 < p, q < 1$. Also, let I, J, the input assignments to F, represent $\langle x = 1, y = 0, z = 0\rangle, \langle x = 0, y = 1, z = 1\rangle$ respectively where I'', J'' are the corresponding consistent assignments to F''.

We will first show that $\psi(\mathbf{E}_{F,I}) \neq \psi(\mathbf{E}_{F,J})$. Suppose $\psi(\mathbf{E}_{F,I}) = \psi(\mathbf{E}_{F,J})$. Since $\langle x = 1\rangle$ in I, from the definition of probabilistic disjunction operator, $\psi(\mathbf{E}_{F,I}) = p$. Furthermore, since $\langle y = 1, z = 1\rangle$ in J, from the definition of the probabilistic conjunction operator, $\psi(\mathbf{E}_{F'',J''}) = q$ and from Observation 3.2.1, $\psi(\mathbf{E}_{F,J}) = pq + (1-p)(1-q)$. Since, $\psi(\mathbf{E}_{F,J}) = \psi(\mathbf{E}_{F,I})$,

$$\begin{aligned} pq + (1-p)(1-q) &= p \qquad\qquad \text{or} \\ (1-2p)(1-q) &= 0 \end{aligned}$$

Then, $(1-2p) = 0$ or $(1-q) = 0$ or both, which contradicts the fact that $1/2 < p, q < 1$.

Now, let $F \equiv G$. Then from the definition of equivalence of PBF, it must be the case that $\psi(\mathbf{E}_{F,I}) = \psi(\mathbf{E}_{G,I})$ and $\psi(\mathbf{E}_{F,J}) = \psi(\mathbf{E}_{G,J})$. Furthermore, we have shown that $\psi(\mathbf{E}_{F,I}) \neq \psi(\mathbf{E}_{F,J})$ and hence $\psi(\mathbf{E}_{G,I}) \neq \psi(\mathbf{E}_{G,J})$.

For the assignments I and J, and from the definition of a probabilistic disjunction and Observation 3.2.2,

$$\psi(\mathbf{E}_{G,I}) \;=\; \psi(\mathbf{E}_{G,J}) = 1 - b - ac + 2abc$$

which is a contradiction □

4.3 Degree of Non-Associativity

We know from Section 4.2 and Theorem 2 that formulae in PBL are not associative. We will now quantify the *degree* to which a PBF is non-associative. Besides inherent intellectual interest, such a characterization is of interest from a pragmatic perspective, since tools for synthesizing logic circuits from formulaic specifications (logic synthesis tools), use "reassociation" as a ubiquitous transformation for optimizing digital logic circuits [43]. This transformation is legal or valid in the Boolean logic context, since associativity is truth preserving. Typically, this transformation is applied to improve the performance (time) while preserving the cost (size) of a Boolean circuit. In contrast to Boolean logic, in the case of PBL, a reassociation can result in a significant change to the probability with which the formula is satisfied, depending on the input assignment. As a simple example, consider Figure 6(a), where we illustrate a PBF F and its reassociation F' in Figure 6(c). For those who are computationally minded, F and F' are depicted as trees, explicitly indicating the order in which their constituent operators would be evaluated. Continuing, for an input assignment $\langle x_1 = 1, x_2 = 1, x_3 = 1, x_4 = 1\rangle$, it is easy to verify that the probability that F is satisfied is p whereas the probability that F' is satisfied is $p^2 + p^2(1-p) + (1-p)^3$; very different probability values for, $1/2 < p < 1$.

More generally, let $\mathbf{F}$ be a maximal set of formulae where $F, F' \in \mathbf{F}$ if and only if they are reassociations of each other. For $F, F' \in \mathbf{F}$ and for a particular input assignment[7] I to F as well as to F', let the probabilities that F_I and F'_I are unsatisfied be q_I and q'_I respectively. If $\mathbf{I}$ is the set of all input assignments to F (and F'), we can quantify the *amount* by which F and F' are non-associative as,

$$NA(F, F') = \max_{\forall I \in \mathbf{I}} \left\{ \frac{q'_I}{q_I}, \frac{q_I}{q'_I} \right\} \tag{1}$$

[7] Since F and F' are defined on (exactly) the same set of Boolean variables, the same assignment I is valid in both cases.

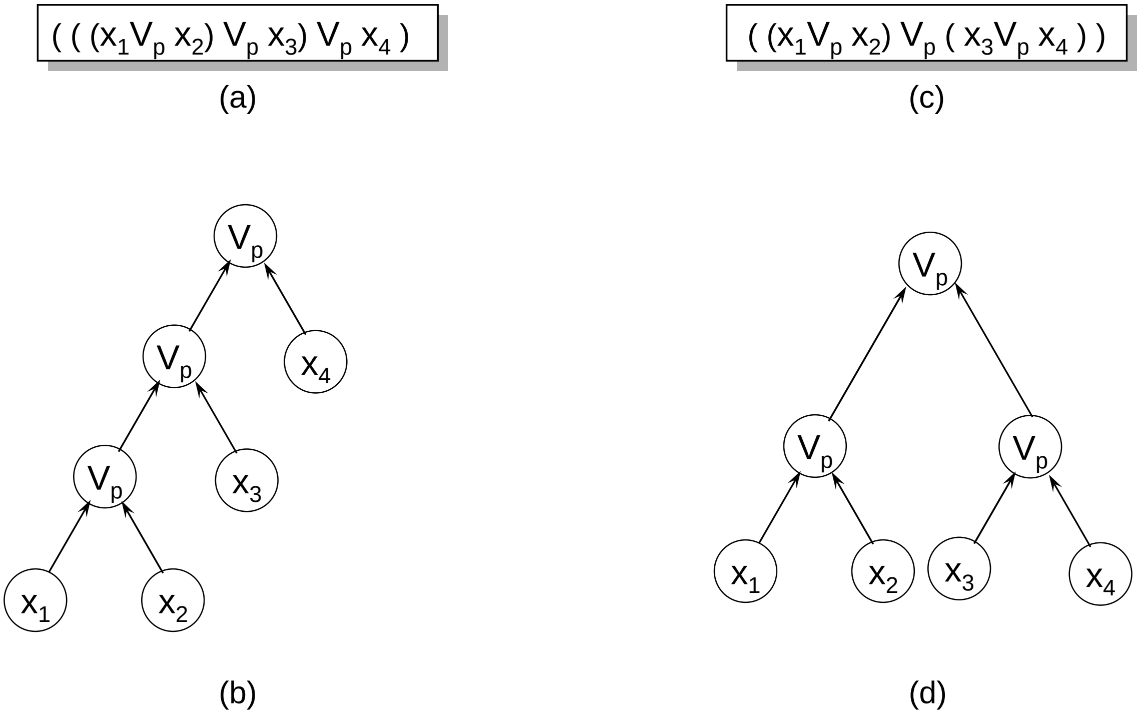


Figure 6. (a) A linear PBF over n variables in syntactic form (b) as a tree structure illustrating the linear form (c) a reassociation of the same PBF (d) its balanced binary representation in tree form

Building on this, we can quantify the non-associativity of the set $\mathbf{F}$ to be

$$\eta_{\mathbf{F}} = \max_{\forall (F,F') \in \mathbf{F}} \{NA(F,F')\} \tag{2}$$

The *degree of non-associativity* of PBL with formulae of length no greater than n, Δ_n is

$$\Delta_n = \max_{\forall \mathbf{F} \in \mathcal{F}_n} \{\eta_{\mathbf{F}}\} \tag{3}$$

where $\mathbf{F} \in \mathcal{F}_n$ if and only if the length of F is at most n for any $F \in \mathbf{F}$.

4.4 Balanced Binary and Linear PBF

We will now consider two associations of the same base formula F, a "linear" formula L (Figure 6(a)) and a "balanced binary" formula B(Figure 6(c)). In order to bound Δ_n from below, we will bound the probability Q_L that L is not satisfied from below, and the probability Q_B that B is not satisfied from above. Then we will use the fact that $\Delta_n \geq Q_L/Q_B$.

Consider n PBF, $C^1, C^2, C^3, \cdots, C^n$ where $C^i = (x_i)$ and without loss of generality let $n = 2^m$ for some positive integer m. For $1 \leq i \leq n/2$, H^i is $(C^{2i-1} \vee_p C^{2i})$ and for $n/2 \leq i \leq n-1$, H^i is of the form $(H^j \vee_p H^{j+1})$ where $j = (2i - n - 1)$. For example, with four variables $\{x_1, x_2, x_3, x_4\}$, C^1, C^2, C^3, C^4 would be $(x_1), (x_2), (x_3), (x_4)$ respectively H^1 would denote $(x_1 \vee_p x_2)$, H^2 would denote $(x_3 \vee_p x_4)$, and H^3 or B would be $(H^1 \vee_p H^2)$ which is $((x_1 \vee_p x_2) \vee_p (x_3 \vee_p x_4))$ as shown in Figure 6(c),(d). Thus, PBF B is of length

3 and height 2. For convenience, B denotes H^{n-1}. We shall refer to B as a *balanced binary* probabilistic Boolean formula of height m and length $(n-1)$, since, as illustrated in Figure 6(d), B is a balanced binary tree.

For the same set of n variables, we can construct the probabilistic Boolean formula L, a reassociation of B, as follows: For some $1/2 \leq p << \leq 1$ (and $q = (1-p)$ as before) construct the probabilistic Boolean formula L where L is defined as follows: $G^2 = (C^1 \vee_p C^2)$ and for $2 < i \leq n$, $G^i = (G^{i-1} \vee_p C^i)$ and for notational convenience, we will use the symbol L to represent G^n, where L is a *linear* probabilistic Boolean formula of length $(n-1)$, since topologically L is a linear structure with $(n-1)$ probabilistic disjunction operators (as in Figure 6(b)).

We will now state a useful fact to be used subsequently in multiple contexts as we estimate Δ_n.

LEMMA 4.1. *Given any* PBF F *of the form* $(F' \vee_p F'')$ *with an assignment* I *and corresponding consistent assignments* I', I'' *to* F' *and* F''*, if* $Q_F, Q_{F'}$ *and* $Q_{F''}$ *are the probabilities that they are unsatisfied,* $Q_F = q + Q_{F'}Q_{F''}(1-2q)$.

PROOF. This Lemma follows from the the fact that $P_F = (1 - Q_F)$, $P_{F'} = (1 - Q_{F'})$ and $P_{F''} = (1 - Q_{F''})$, and therefore from Observation 3.2.1,

$$\begin{aligned} Q_F &= (q)(1-Q_{F'})(1-Q_{F''}) + (q)(1-Q_{F'})(Q_{F''}) \\ &\quad +(q)(Q_{F'})(1-Q_{F''}) + (1-q)(Q_{F'})(Q_{F''}) & (4) \\ &= q + Q_{F'}Q_{F''}(1-2q) & (5) \end{aligned}$$

□

Now, consider a balanced binary PBF of length n and consider H_i of length k where $n/2 \leq i \leq n-1$. From the definition of a Balanced binary PBF, H^i is of the form $(H^j \vee_p H^k)$, where $j = (2i-n-1), k = (2i-n)$. If H^j is satisfied with a probability P_j, we observe from Lemma 4.1 that

OBSERVATION 4.4.1. *The probability with which* H^i *is satisfied is at least* pP_j

4.4.1 *An Upper bound on the Probability of Unsatisfiability of a Balanced Binary* PBF

LEMMA 4.2. *Let* Q_B *be the probability that a* PBF B *of length* $(n-1)$*, where* $n = 2^k$ *for some integer* $k \geq 2$*, is unsatisfied with an input assignment* α*, where* $\alpha(x) = 1$ *for all* $x \in$ VAR$_B$. *Then* $Q_B < \sum_{i=1}^{\log(n)} q^i$ *with* $q = (1-p)$.

PROOF. We will prove the lemma by induction on the length of B. For the basis, consider a balanced binary PBF $\hat{B}$ of length $2^2 - 1 = 3$ with 4 variables, where $\hat{B} = (\hat{B}' \vee_p \hat{B}'')$. Now consider an input assignment $\hat{\alpha}(x_i) = 1$ for $1 \leq i \leq 4$. Since B' and B'' are identical in a balanced binary PBF, we have $Q_{\hat{B}'} = Q_{\hat{B}''} = q$ and therefore from Lemma 4.1,

$$\begin{aligned} Q_B &= q + q^2(1-2q) \\ &\qquad \text{and since } q > 0 \\ Q_B &< q + q^2 & (6) \end{aligned}$$

Now Consider B of the form $(B' \vee_p B'')$, where B' and B'' are balanced binary PBF of length $(2^{k-1}-1)$, $k \geq 3$ and B is of length $(2^k - 1)$. By definition of α, an identical value (of 1) is assigned to all the variables of B' and B'' and $Q_{B'} = Q_{B''}$. As an induction hypothesis, let $Q_{B'} = Q_{B''} < \sum_{i=1}^{k-1} q^i$. From this hypothesis and Lemma 4.1, we have

$$\begin{aligned} Q_B &\leq q + \left(\sum_{i=1}^{k-1} q^i\right)\left(\sum_{i=1}^{k-1} q^i\right)(1-q) = q + \left(\sum_{i=1}^{k-1} q^i\right)(q - q^k) \\ &\text{hence} \\ Q_B &< \sum_{i=1}^{k} q^i \qquad \text{for } q > 0 \end{aligned}$$

With $k = \log(n)$, we have the proof. □

Building on this lemma, we will now determine an upper-bound on the probability Q_B that a (balanced binary) PBF is not satisfied, when a constant fraction $\lambda = n\epsilon$ for $0 < \epsilon < 1$ of its variables are assigned a value of 1 (and the rest are assigned a value of 0) through an assignment[8] α. We will continue to consider the case where all of the probabilistic disjunction operators have the same associated probability parameter p where $n \geq 4$.

THEOREM 3. *Let Q_B be the probability that a balanced binary* PBF *B of length $n-1$ is unsatisfied for an assignment α, where $\alpha(x_i) = 1$ for $0 < i \leq \lambda$, $\alpha(x_i) = 0$ for $\lambda < i \leq n$, and $q\log(n/\lambda) \leq 1$. Then, $Q_B < (1 + \log(\frac{n}{\lambda}))q$ for $n \geq 4$ whenever $n = 2^k$, $\lambda = 2^l$ for $l < k$.*

PROOF. Let B be a balanced binary PBF of length $n \geq 4$. Consider an assignment α such that $\alpha(x_i) = 1$ for $0 < i \leq \lambda$, and $\alpha(x_i) = 0$ for $\lambda < i \leq n$. Consider the sub-formula H^m of B, with variables $\text{VAR}_{H^m} = \{x_1, x_2, x_3, \cdots, x_\lambda\}$. Since $\lambda = 2^l$, from the definition of a balanced binary PBF, H^m is a balanced binary PBF and $m = (n + 1 - 2n/\lambda)$. Let P_m be the probability that H^m is satisfied for the assignment α.

Since $\lambda \leq n/2$, there exists a sub formula H^o of B, which is of length $2\lambda - 1$, such that $H^o = (H^m \vee_p H^{m+1})$ and $o = (n + 1 - n/\lambda)$. The probability that H^o is satisfied (from Observation 4.4.1) is at least pP_m. Continuing, a straight forward induction will show that P_B, the probability that $B = H^{n-1}$ is satisfied, is (at least) $p^{\log(n/\lambda)}P_m$.

If Q_m is the probability that H^m is unsatisfied, from Lemma 4.2, $Q_m < \sum_{i=1}^{\log(\lambda)} q^i$. Since $P_m = 1 - Q_m$, $P_m > 1 - \sum_{i=1}^{\log(\lambda)} q^i = 1 - \frac{(q - q^{(\log(\lambda)+1)})}{(1-q)}$,

$$\begin{aligned} P_B > p^{\log(\frac{n}{\lambda})}P_m = (1-q)^s\left[1 - \frac{(q-q^t)}{(1-q)}\right] &= (1-q)^s - (1-q)^{s-1}(q - q^t) \\ \text{where } s = \log(n/\lambda) \text{ and } t = \log(\lambda) + 1 & \\ (1-q)^s - (1-q)^{s-1}(q-q^t) &> (1-q)^s - (1-q)^{s-1}(q) \\ \text{since } 0 < q < 1/2, \text{ and therefore} & \\ P_B &> (1-q)^{s-1}(1-2q) \end{aligned} \tag{7}$$

[8] The symbol α is reused with varying constraints throughout the paper, which entails some abuse of notation

Using the binomial theorem[9] to expand $(1-q)^{s-1}$, we get $(1-q)^{s-1} = \left[\sum_{k=0}^{s-1} \binom{s-1}{k} (-q)^k\right]$. There are s terms in the expansion and where we refer to 1 as the first term, $(s-1)(-q)$ as the second term and so on. For convenience, the j^{th} term when $j > s$ will be taken to be 0. Since $\lambda \leq n/2$, $s \geq 1$, and whenever $1 \leq s \leq 2$, $(1-q)^{s-1} = 1-(s-1)q$. Consider the case when $s > 2$, and let j be odd and $2 < j \leq s$, then the sum of j^{th} and $j+1^{th}$ term of the binomial expansion of $(1-q)^{s-1}$ is $u_j = \frac{(s-1)!q^{j-1}}{(j-1)!(s-j)!}(1-(s-j)q/j)$. Since $sq \leq 1$, $u_j \geq 0$ and therefore $(1-q)^{(s-1)} \geq (1-(s-1)q)$. Therefore, from (7),

$$\begin{aligned} P_B &> (1-(s-1)q)(1-2q) \\ Q_B &= 1 - P_B < (1-(1-(s-1)q)(1-2q)) \\ &\text{or} \\ Q_B &< (s+1)q \\ \text{and hence} & \\ Q_B &< \left(1 + \log\left(\frac{n}{\lambda}\right)\right) q \end{aligned}$$

□

We note in passing that due to symmetry, it is easy to see that the result derived in Theorem 3 holds even if the last λ variables are set to 1 and the rest of the variables to zero. In fact, it can be shown that the result derived in Theorem 3 holds irrespective of the position of the "runs" of variables assigned a value 1, due to the inherent symmetry in a balanced binary PBF.

4.4.2 *A Lower bound on the Probability of Unsatisfiability of a Linear* PBF. We will now consider the case of a linear PBF L. Recall that L is of the form $(((x_1 \vee_p x_2) \vee_p x_3) \cdots \vee_p x_n)$ where, again, the value 1 is assigned to x_i if and only if $1 \leq i \leq \lambda$ and the value 0 to x_i whenever $\lambda < i \leq n$.

THEOREM 4. *Given a linear* PBF *L, of length $n-1$, where Q_L is the probability that L is unsatisfied with the input assignment α where $\alpha(x_i) = 1$ if $1 \leq i \leq \lambda < n$ and 0 otherwise,*

$$Q_L \geq \max\{0, (n-\lambda+1)q - (n-\lambda)(n-\lambda+1)q^2\}$$

PROOF. Let $\lambda + k = n$. Since $\lambda < n$, it follows that $k \geq 1$. Consider the case when $k = 1$. Then the PBF L is of the form $(L' \vee_p x_{\lambda+1})$, where L' is a linear PBF of length $\lambda - 1$ with $\text{VAR}_{L'} = \{x_1, x_2, x_3, \cdots, x_\lambda\}$. If Q_L is the probability that L is unsatisfied by the assignment α, using Lemma 4.1 and recalling that $x_i = 1$ for $1 \leq x_i \leq \lambda$ and 0 otherwise,

$$\begin{aligned} Q_L &= q + Q_{L'}(1-2q) \\ &= q + q(1-2q) \\ &= 2q - 2q^2 \end{aligned}$$

Hence the theorem is true whenever $k = 1$ (since $n - \lambda = k = 1$).

Let $k \geq 2$ and let us suppose that the theorem is false. Furthermore, let $\hat{L}$ be the shortest sub-formula of L, for which the theorem is false and therefore $Q_{\hat{L}} < \max\left\{0, (\hat{k}+1)q - (\hat{k}+1)(\hat{k})q^2\right\}$. If the length of $\hat{L}$ is $\lambda + \hat{k}$,

[9] The interested reader is referred to [29] (page 86) where the binomial theorem is derived for $(a+b)^n$ where a, b are elements of a commutative ring and n is any positive integer

where $\text{VAR}_{\hat{L}} = \{x_1, x_2, x_3, \cdots, x_{\lambda+\hat{k}+1}\}$, it must be the case that $\hat{k} > 1$ (since we have shown to theorem to be true for $\hat{k} = 1$). From the definition of a linear PBF, $\hat{L}$ is of the form $(\hat{\hat{L}} \vee_p x_{\lambda+\hat{k}+1})$ where $\hat{\hat{L}}$ is of length $\lambda+\hat{k}-1$. From the hypothesis, the theorem is true for $\hat{\hat{L}}$, or equivalently $Q_{\hat{\hat{L}}} \geq \max\left\{0, q + \left[(\hat{k})q - (\hat{k})(\hat{k}-1)q^2\right]\right\}$. From Lemma 4.1, it follows that

$$\begin{aligned}
Q_{\hat{L}} &= q + Q_{\hat{\hat{L}}}(1-2q) \geq \max\left\{0, q + \left[(\hat{k})q - (\hat{k})(\hat{k}-1)q^2\right](1-2q)\right\} \\
&\text{and hence} \\
Q_{\hat{L}} &\geq \max\left\{0, (\hat{k}+1)q - (\hat{k}+1)(\hat{k})q^2\right\}
\end{aligned}$$

A contradiction. □

4.5 The Degree of Non-associativity of PBL

THEOREM 5. *There exist two probabilistic Boolean formulae B and L, both of length $(n-1) \to \infty$ and $n \geq 4$ such that B is a reassociation of L and furthermore $NA(B, L)$ grows as $\Omega(n)$.*

PROOF. Consider $n = 2^m$, $m \geq 2$ variables $\{x_1, x_2, x_3, \cdots, x_n\}$ where B and L are respectively the balanced binary Boolean formula and the linear probabilistic Boolean formula over this set of variables. From Theorem 3, for the assignment α and $1/2 \leq p < 1$ and $q = (1-p)$, a λ exists such that

$$Q_B \leq \left(1 + \log\left(\frac{n}{\lambda}\right)\right) q \tag{8}$$

And furthermore, from Theorem 4 also for the same assignment α, and the value λ,

$$Q_L \geq \max\{0, (n-\lambda+1)q - (n-\lambda)(n-\lambda+1)q^2\} \tag{9}$$

Consider

$$\begin{aligned}
\mathbf{Q} &= \frac{(n-\lambda+1)q - (n-\lambda)(n-\lambda+1)q^2}{(1+\log(\frac{n}{\lambda}))q} \\
&= \frac{(n-\lambda+1) - (n-\lambda)(n-\lambda+1)q}{(1+\log(\frac{n}{\lambda}))} \qquad \text{since } q \neq 0
\end{aligned}$$

For all $n \in \mathbb{N}^+$, $n \geq 4$, $q = \frac{1}{n^c}$ for $c \geq 2$, and $\lambda = n/2$,

$$\mathbf{Q} = \frac{n}{4} + \frac{1}{2} - \frac{1}{4n^{c-1}} - \frac{1}{8n^{c-2}} > 0$$

Recall from the definition of NA, the amount of non-associativity that

$$NA(B, L) = \max_{\forall I \in \mathbf{I}} \left\{\frac{Q'_I}{Q''_I}, \frac{Q''_I}{Q'_I}\right\}$$

where Q'_I, Q''_I are respectively the probabilities that B and L are unsatisfied with an input assignment I. Whenever $\mathbf{Q} > 0$, it follows that

$$NA(B, L) \geq \frac{Q_L}{Q_B} \geq \mathbf{Q} = \frac{(n - \lambda + 1)q - (n - \lambda)(n - \lambda + 1)q^2}{(1 + \log(\frac{n}{\lambda}))q}$$

Therefore, for any $n \in \mathbb{N}^+$, $n \geq 4$, $q = \frac{1}{n^c}$ for $c \geq 2$, and $\lambda = n/2$,

$$NA(B, L) \geq \frac{n}{4} + \frac{1}{2} - \frac{1}{4n^{c-1}} - \frac{1}{8n^{c-2}} \geq \frac{n}{4} = \Omega(n)$$

□

Therefore, it immediately follows that

Corollary 6. The degree of non-associativity, Δ_n of PBL grows as $\Omega(n)$

5. DISTINGUISHING PROBABILISTIC (IMPLICIT) AND RANDOMIZED (EXPLICIT) MODELS OF COMPUTING THROUGH ENERGY CONSIDERATIONS

We will now distinguish the implicitly and explicitly realized probabilistic behaviors—the latter referred to as randomized for terminological clarity—using a measure based on the *energy consumed* in computing the result by a computational step. In Section 5.1.1, we first review the known results from past work which provide a foundation, both in theoretical and in experimental terms. This immediately provides a way of distinguishing the implicitly probabilistic and explicitly randomized approaches to realizing Boolean operations, through energy considerations. We will use the background from Section 5.2 to separate probabilistic and randomized (implicit and explicit) Boolean circuits. Building on this, in Section 5.3, we will extend this concept beyond combinational (Boolean) logic to a model of computation with state. Here we distinguish implicitly realized PA with PBL as a foundation, from their explicitly realized counterparts through explicit coin tosses, using the energy consumed by each state transition.

5.1 Thermodynamic Separation of Implicitly and Explicitly Probabilistic Gates and The Circuit Model of Computation

We will define *probabilistic Boolean circuits*, a model of computing, based on PBL and then distinguish them from their explicit counterpart, the randomized Boolean circuit with coin tosses.

5.1.1 PBF *and Probabilistic Boolean Circuits.* Analogous to conventional Boolean circuits, a *probabilistic Boolean circuit* is defined as follows: a directed acyclic connected graph $\hat{\mathbb{C}} = (\hat{V}, \hat{E})$, where $\hat{V}$ is the set of vertices and $\hat{E}$ the set of directed edges. The vertices are of three kinds. *Input* vertices, of in-degree 0 associated with Boolean variables (called input variables of the circuit) or Boolean constants $\{0, 1\}$, *internal* vertices associated with one of three operators $\vee_p, \wedge_q, \neg_r$ where $1/2 \leq p, q, r \leq 1$ and one distinguished output vertex of in-degree 1 and out-degree 0. Internal vertices associated $\vee_p$ and $\wedge_q$ have in-degree 2 and out-degree 1, whereas those associated with $\neg_r$ have in-degree and out-degree 1. For any assignment of Boolean constants 0 or 1 to the input variables of the circuit, the value of the input vertex is either the Boolean constant assigned to the corresponding Boolean variable, or the Boolean constant directly associated with the vertex. The value of any internal vertex u, is the value obtained by applying the probabilistic Boolean operator associated with the vertex, to values associated with its input edges. The value of a directed edge $(u, v) \in \hat{E}$ is the value associated with the vertex u. Finally, the value *computed* by the probabilistic Boolean circuit is the value associated with the output vertex. If the cardinality of the set of input vertices is k, $\hat{\mathbb{C}}$ *computes* a probabilistic Boolean truth table $\mathcal{T}$ with no more than 2^k rows.

OBSERVATION 5.1.1. *For any* PBF F *and the probabilistic truth table* $\mathcal{T}$ *it represents, there exists a probabilistic Boolean circuit* $\hat{\mathbb{C}}_F$ *which computes* $\mathcal{T}$.

This observation is straightforward since a well formed PBF is obtained by the application of the rules outlined in Section 2. An equivalent probabilistic Boolean circuit can be constructed by creating input vertices for every Boolean variable and constant in the PBF, and an internal vertex for every Boolean operator.

5.1.2 *Randomized Boolean Circuits and Their Relationship to Probabilistic Boolean Circuits.* Randomized Boolean circuits have been used as a computational model to study randomized algorithms [1, 46]. Analogous to conventional Boolean circuits, a randomized Boolean circuit is a directed acyclic connected graph $\mathbb{C} = (V, E)$. As before, V can be partitioned into subsets, where the input vertices are associated with Boolean variables (called input variables of the circuit), Boolean constants or Boolean random variables. The internal vertices are associated with one of three operators or labels $\vee, \wedge, \neg$ from Boolean logic. Any internal vertex $v \in V$ has the property that there is at most one edge (u, v) such that $u \in V$ is an input vertex associated with a Boolean random variable. As before, there is one distinguished output vertex of in-degree 1 and out-degree 0. Notions of values associated with vertices and edges correspond to those introduced in Section 5.1.1 above.

OBSERVATION 5.1.2. *For any* PBF F *and its truth table* $\mathcal{T}$, *there exists a randomized Boolean circuit which computes it.*

We will now establish the fact that *any* randomized Boolean circuit (or more specifically its truth table) can be realized by a probabilistic Boolean circuit. Let $U \subseteq V$ denote input vertices associated with Boolean random variables in $\mathbb{C}$. Consider vertex $u \in U$ and a set of internal vertices V' such that whenever $v \in V'$, $(u, v) \in \mathbb{C}$. Let u be associated with Boolean random variable x_u such that probability that $x_u = 1$ is $p_u \in \mathbb{Q}$. The source of randomness in this case, which as part of an assignment binding values to the variables labeling the vertices in U, is explicit. By this, we mean that (informally) these bits are pseudo random and are produced by a suitable combination of deterministic gates. We formalize this as a "thesis" as follows.

THESIS 1. *Each input bit bound to the random variable* x_u *where* $u \in U$ *is produced by a pseudo random source*[10] *constituted of gates all with a probability of correctness* $p = 1$.

We will predicate the development in the sequel on Thesis 1 being valid.

Returning to the goal of relating randomized Boolean circuits to its probabilistic counterpart, for any vertex $u \in \mathbb{C}$ as described above, let $p_u \geq 1/2$. We replace u with a new input vertex u'' associated with

[10] There is a rich body of work, which seeks to address the cost for producing a (pseudo) random bit through techniques ranging from recycling of random bits [27], to techniques which extract randomness from weak random sources [12] and methods to "amplify" randomness through pseudo-random number generators [4, 67]. While Thesis 1 is claimed only for pseudo random generators, we opine that it is also valid for alternate sources of (pseudo) randomness.

Boolean constant 0, a new internal vertex u' associated with $\neg_{\hat{p}}$ where $\hat{p} = p_u$, and a new edge (u'', u'). Now for all edges (u, v) where $v \in V$, we replace it with edge (u', v) (when $p_u < 1/2$, u'' is associated with 1 and $p = 1 - p_u$). We shall refer to this circuit as $\mathbb{C}/\{u\}$.

Lemma 5.1. *The Boolean random variable x_u representing the value of any edge (u, v) in $\mathbb{C}$, where $v \in V$, is equivalent to the Boolean random variable $\hat{x}_{u'}$ representing the value of the edge (u', v) in $\mathbb{C}/\{u\}$.*

Proof. Immediate from the definition of a probabilistic negation operator and the equivalence of random variables. □

Let $\hat{\mathbb{C}} = \mathbb{C}/U$ denote the probabilistic Boolean circuit derived from $\mathbb{C}$ by applying the above transformation for all vertices $u \in U$.

Theorem 7. *Given a randomized Boolean circuit $\mathbb{C}$, there exists a probabilistic Boolean circuit $\hat{\mathbb{C}}$ such that $\mathbb{C}$ and $\hat{\mathbb{C}}$ compute identical truth tables.*

Proof. (Outline) For any $u \in U$, from Lemma 5.1 and a straightforward induction on the elements of U, it can be shown that $\mathbb{C}$ and $\mathbb{C}/U$ compute identical probabilistic Boolean truth tables. □

5.1.3 *Energy Advantages of Probabilistic Boolean Circuits.* Based on Theorem 7 and the manner in with $\hat{\mathbb{C}}$ is constructed from $\mathbb{C}$, we can claim

Claim 5.1.1. *The energy consumed by the implicitly probabilistic circuit $\hat{\mathbb{C}} = \mathbb{C}/U$, is less than that consumed by $\mathbb{C}$ which is explicitly randomized whenever the energy cost for producing each (pseudo) random bit x_u as an input to $\mathbb{C}$ is higher than that of a probabilistic inverter realizing the probabilistic operation $\neg_{p_u}$.*

We will subsequently see (in Section 5.2) that the energy cost of producing a random (or pseudo random) bit is indeed higher than that of realizing a PBL operation $\neg_{\hat{p}}$. This is true based both on thermodynamic principles and through empirical studies based on physical realization of gates through randomness, thereby converting the conditional claim 5.1.1 above into an unconditional claim in these two contexts.

5.2 Energy Considerations For Realizing Probabilistic and Randomized Boolean Operators

The central result of Section 5.1 above, was to distinguish randomized and probabilistic Boolean circuits of identical size and depth through a metric which quantifies the *energy consumed* by these circuits. In the physical domain, probabilistic switches [51] serve as a foundational model relating the thermodynamic (energy) cost of computing, to the probability of correctness of computing. In this context, if T is the temperature at which switching takes place k is the Boltzmann constant [5] and as before, p is probability of correctness, Palem showed that probabilistic switches are thermodynamically (with energy consumption as a metric) more efficient than deterministic switches

Theorem 8. *(Palem [51]) The potential for saving through probabilistic switching over deterministic switching is $kT \ln \frac{1}{p}$ joules per switching step.*

This theoretical evidence was substantiated empirically, in the domain of switches implemented using complementary metal oxide semiconductor (CMOS) technology, where the relationship between the probability of correctness of switching and its energy consumption was established through analytical modeling, as well as actual measurements of manufactured *probabilistic* CMOS (PCMOS) based devices [10]. The basic building block in CMOS technology is the ubiquitous transistor, whose (feature) size, typically measured in nanometers these days, is denoted by the symbol ν. Cheemalavagu et. al [10] established a relationship between the energy consumed by a switch and its probability of correctness p, and σ, the noise magnitude (quantified as the standard deviation of the associated distribution) inducing the probabilistic behavior[11]. With this as background, we have the relationship between E, the energy consumed by a switch (gate) and p, which we paraphrase as follows.

Law 1: Energy-probability Law:([10, 40]) *For any fixed transistor feature size ν and a noise magnitude σ, the switching energy $E_{\nu,\sigma}$ consumed by a probabilistic switch grows as $\Omega(e^p)$ where $p \in [0,1]$ denotes the probability of correct switching.*

To reiterate, whenever Law 1 holds, given any randomized Boolean circuit $\mathbb{C}$ and its equivalent probabilistic Boolean circuit $\mathbb{C}$, the energy consumed by the latter is less than the energy consumed by the former.

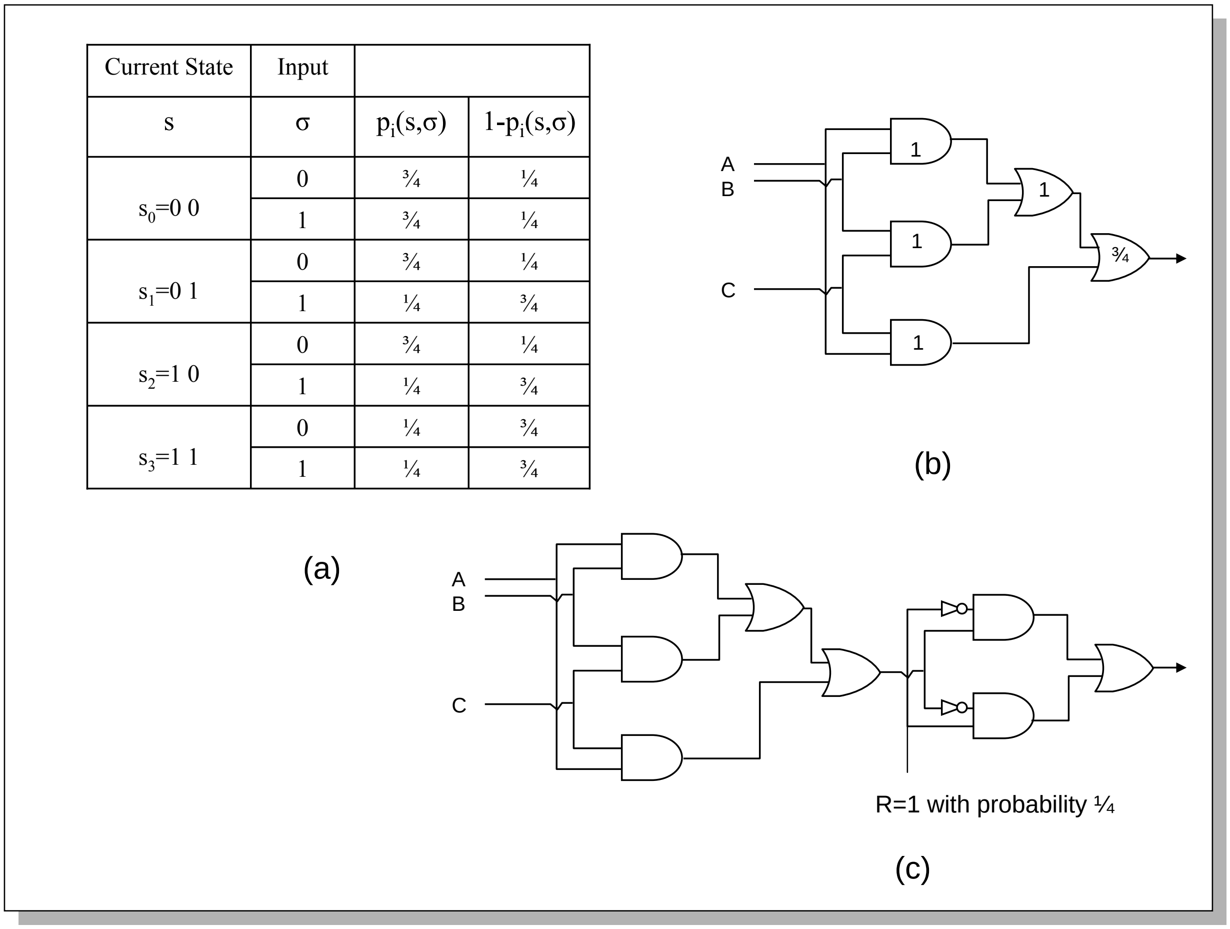
5.3 Extending to Computational Model with State

PA in the Rabin sense [55], with incorporate probabilistic transition functions. A PA over an alphabet Σ is a system $\langle S, M, s_0, Q\rangle$ where $S = \{s_0, \cdots, s_n\}$ is a finite set (of states), M is a function from $(S \times \Sigma)$ into the interval $[0,1]^{n+1}$ (the transition probabilities table) such that for $(s,\sigma) \in (S \times \Sigma)$, the transition function $M(s,\sigma) = (p_0(s,\sigma), \cdots, p_n(s,\sigma))$ where $0 \le p_i(s,\sigma)$ and $\sum p_i(s,\sigma) = 1$. The initial state is denoted by s_0 where $s_0 \in S$ and $Q \subseteq S$ is the set of designated final states.

To establish that the distinction between the implicitly probabilistic and explicitly randomized variants established in Section 5.1 persists, we consider a *restricted probabilistic automaton* $\mathcal{P}$ over an alphabet $\hat{\Sigma} = \{0,1\}$. Given a state $\hat{s} \in \hat{S}$ and an input $\hat{\sigma} \in \hat{\Sigma}$, the cardinality of the set of possible successor states (with non zero transition probability) is at most two. That is for $(\hat{s},\hat{\sigma}) \in (\hat{S} \times \hat{\Sigma})$, where $\hat{M}(\hat{s},\hat{\sigma}) = (\hat{p}_0(\hat{s},\hat{\sigma}), \cdots, \hat{p}_n(\hat{s},\hat{\sigma}))$, there exist distinct indices i and j, $0 \le i, j \le n$ such that $\hat{p}_i(\hat{s},\hat{\sigma}) + \hat{p}_j(\hat{s},\hat{\sigma}) = 1$ and for $0 \le k \le n$, $k \ne i$ and $k \ne j$, $\hat{p}_k(\hat{s},\hat{\sigma}) = 0$. Furthermore, $\hat{p}_i(\hat{s},\hat{\sigma}), \hat{p}_j(\hat{s},\hat{\sigma}) \in \mathbb{Q}$; Rabin's formulation of PA is not restricted to rational probabilities since $p_i(s,\sigma)$ can be any value in the unit interval.

We observe here without proof, illustrated for completeness through an example in Figure 7 that the transition function of any (restricted) PA $\mathcal{P}$ can be represented as a probabilistic truth table. An example PA is illustrated in Figure 7 whose (transition) truth table is shown in Figure 7(a), where Figure 7(b) is a probabilistic Boolean circuit which computes this transition truth table, and Figure 7(c) is a randomized Boolean circuit which computes the transition truth table (with the random source labeled R). If each element of $\hat{S}$ is encoded in binary, any $K \in (\hat{S} \times \hat{\Sigma})$ can be represented by a binary string (with the state concatenated to the input alphabet). For any state $\hat{s}$ and an input alphabet $\hat{\sigma}$, the two possible successor states $\hat{s}_i, \hat{s}_j$ (with non zero transition probabilities) can be represented by 0 and 1 respectively. Then, the transition function $\hat{M}$ can be represented by a probabilistic Boolean truth table, with $2|\hat{S}|$ rows and 3 columns, where the first column of the k^{th} row contains K, the binary representation of k where K is an element of $(\hat{S} \times \hat{\Sigma})$. The second column contains $\hat{p}_{\hat{s}_j,\hat{\sigma}}$. From Claim 5.1.2 and Theorem 7, the (transition) truth table of $\mathcal{P}$ can be computed using a probabilistic or randomized Boolean circuit respectively. This construction immediately allows us to extend the separation between probabilistic and randomized Boolean

[11] A deterministic gate (or switch) is rendered probabilistic by (additive) ambient noise and the study by Cheemalavagu et al [10] characterized noise magnitude through σ, which is the accepted approach



Current State	Input		
s	σ	$p_i(s,\sigma)$	$1\text{-}p_i(s,\sigma)$
s_0=0 0	0	¾	¼
	1	¾	¼
s_1=0 1	0	¾	¼
	1	¼	¾
s_2=1 0	0	¾	¼
	1	¼	¾
s_3=1 1	0	¼	¾
	1	¼	¾

Figure 7. (a) A transition function encoded as a transition truth table (b) A probabilistic circuit which computes this transition truth table (c) An equivalent randomized Boolean circuit which computes the transition truth table

circuits to be applicable to the PA $\mathcal{P}$. Let $\hat{\mathbb{C}}_{\mathcal{P}}$ and $\mathbb{C}_{\mathcal{P}}$ respectively be the probabilistic and randomized Boolean circuit implementations of the transition function of $\mathcal{P}$. Then

Observation 5.3.1. *The energy consumed by $\hat{\mathbb{C}}_{\mathcal{P}}$ is less than that consumed by $\mathbb{C}_{\mathcal{P}}$ whenever the energy cost for producing each (pseudo) random bit x_u as an input to $\mathbb{C}_{\mathcal{P}}$ is higher than that of a probabilistic inverter realizing the probabilistic operation $\neg_{p_u}$.*

Again, based on the discussion in Section 5.2, we conclude that Claim 5.3.1 can be made unconditionally in the contexts when Theorem 8 or Law 1 are valid, in conjunction with Thesis 1.

6. HISTORICAL REMARKS AND NEW DIRECTIONS FOR INQUIRY

Our work on PBL has connections to three distinct areas with a potential for further research: *mathematical logic*, *computer science*, and applications to *electrical engineering*. We will remark on each of these areas and outline the most interesting questions that we think arise, out of our development of PBL. We wish to note that PBL was developed as a logic throughout this paper, thus diverging from the classical approach of treating Boole's work on two-valued logic as an algebra with a concomitant–often unspecified–axiomatization. This choice was deliberate since we wished to introduce a simple and explicit semantics to our particular approach to introducing probability into logic on the one hand, and furthermore, to cast it in a form that is natural to the two application domains of interest, computer science (Section 6.2) and electrical engineering (Section 6.3). Recall that, our own interest stemmed significantly from the generally expected trend that gates and switches used to design circuits and computing architectures are going to be probabilistic, since deterministic designs are unlikely to be feasible as device (transistor) sizes approach ten nanometers.

6.1 PBL, Logic and Probability

For philosophical and ontological reasons, probabilities have been associated with logics in the past, where the two notable approaches involve associating confidences with sentences as probabilities, and also where the truth value of the sentence—sentences with quantifiers—ranges over the interval $[0, 1]$ and is therefore many-valued. This approach has a long and distinguished history (see Keynes [34] and Reichenbach [58] as good introductions). Relatively recently, considerations of probability in first order languages were treated by Scott and Kraus [61] who attribute Gaifman's investigation of probability measures [25] on (finitary) first-order languages as an inspiration[12]. Hailperin [26] and Nilsson [49] also consider variations of these notions, again with quantifiers and the confidence of the sentence associated with probability measures. The former author also offers an excellent historical analysis of this work. The work of Fagin and Halpern, and Fagin, Halpern and Megiddo continues in this rich tradition and represents a significant milestone [22, 23].

We note that PBL is a significantly simpler logic since it does not admit quantification. So, a reasonable approach is to try and compare PBL to a suitable subset of the richer logics cited above, richer since they use the predicate calculus as a basis. We will now sketch such a comparison informally. The essence of the difference between the previous approaches which can be broadly referred to as *sentential probability* logics on the one hand and PBL on the other, can be understood through the event set semantics (Section 3). In particular, we draw the readers attention to Observation 3.2.1 which clearly identifies the effect of the probability parameter p in an identity of the form $F \equiv (F' \vee_p F'')$. The main point worth noting here is that the event set of F is dependent on the parameter p associated with the operator $\vee_p$, *in addition* to the event sets associated with its constituent probabilistic formulae F' and F''. *It is important to note that this is not true of of the previous approaches—in these cases, the operators are always deterministic.* Thus, based on previous approaches, the probability associated with a formula of the form $G \equiv (G' \vee G'')$ would entirely depend on the probabilities associated with the sub-formulae G', G'' and *not* on the operator $\vee$.

6.1.1 *Some Interesting Questions*

(1) Extend PBL to a logic wherein each operator is associated with a *probability interval*, as opposed to a definite probability value. We note that this extension is also of considerable interest in the context of circuit design, discussed in Section 6.3.

(2) Extend PBL to include quantification, wherein the primitive operators are probabilistic as in PBL augmented with deterministic quantification. For the resulting *probabilistic predicate calculus* (PPC),

  (a) extend the event set semantics from this paper to be applicable

[12] The Scott-Kraus development extends it to infinitary languages.

   (b) establish the usual consistency and completeness properties as well as other interesting properties known for the predicate calculus.
   (c) Establish $0-1$ laws [36] which we conjecture are true

(3) Extend the work further to demonstrate the distinction between PPC and
   (a) probability logics whose operators are deterministic; in particular finitary variants of the logic due to Scott and Kraus, Hailperin's sentential probability logic and Nilsson's versions are of interest.

6.2 PBL in Computer Science

We remind the reader that in PBL, the variables range over the two values from the set $\{0,1\}$ and the input assignments are always deterministic. As discussed previously, the question arises whether this approach is (implicitly) equivalent to working with formulae whose operators are deterministic, and whose constituent variables are permitted to be random (Boolean) variables. Computer scientists have studied models using the latter approach extensively. This alternate approach has been the basis for significant progress in characterizing the power of randomness. Based on this observation, we wish to suggest the following directions for further inquiry.

6.2.1 *Some interesting questions*

(1) Characterize the significant properties of an explicitly probabilistic Boolean logic. We conjecture that the properties very similar to PBL (Section 4) will also be valid here.
(2) We also conjecture that a circuit realized using probabilistic operators (gates) and hence PBL is smaller in size than an equivalent circuit realized using standard Boolean logic that uses explicit coin tosses. Establishing this separation rigorously will further strengthen the difference we have seen in Section 5.
(3) It is well-known that formulae in conventional Boolean logic exhibit a threshold in their satisfiability [31] when the inputs are drawn uniformly from a distribution—hence correspond to an explicitly probabilistic Boolean logic—using the style of average case analysis advocated by Karp [32]. We conjecture that a similar threshold is also valid in the case of formulae in PBL and that again the threshold value also ≈ 4.2.

6.3 Applications of PBL to *U*ltra *L*arge *S*cale *I*ntegrated (ULSI) systems

To reiterate our interest PBL is due in large part motivated by its connection to the physical characteristics of transistors, the ubiquitous building blocks of ULSI circuits[13]. With nanometer transistor sizes looming on the horizon, the resulting ULSI circuits designs with over a billion transistors are facing severe challenges [44], not least of which is the fact that their physical characteristics are expected to vary dramatically within a single chip[14]. Such variation is well beyond the tolerances of a design methodology based on deterministic Boolean logic and automata (state machines), and the need for probabilistic models, logics and design methodologies is anticipated [6].

6.3.1 *Some interesting questions*

[13] As transistor (feature) sizes approach the low nanometer range, current very large integrated circuits (VLSI) circuits will evolve into *ultra* large scale integrated circuits [41].

[14] Technically, the variations are modeled within a single die.

(1) The question identified in Section 6.1 aimed at extending PBL to model probability intervals, we believe is an important next step of practical significance in the ULSI regime.

(2) Currently, *logic synthesis* is an extremely successful technology, where, given an input specification as a formula, a (heuristically) optimized circuit is produced, based on VLSI cost considerations [43]. Extending this to PBL especially with intervals are important next steps that we intend to pursue.

(3) *Binary decision diagrams* (BDDs) [7] are widely used as a tool to verify the correctness of logic designs based on deterministic (Boolean) logic. With the increasingly probabilistic nature of transistors in the ULSI context, we anticipate that it will be of great value if a PBL based probabilistic BDD framework can be created, to mirror the success of its deterministic counterpart.

(4) The event set semantics of PBL suggest a probability attribute for each operator (or gate) based in a set of trials associated with it. This implicitly connotes an interpretation where the set of trials resulting in the events occur over time. However, as noted before, in the context of ULSI circuits, the observed statistical variations occur spatially across the the transistors or gates on the surface of the chip, whereas individual transistors or gates, once manufactured, need not exhibit randomness. While it is straightforward to reinterpret the concept of an event set and the associated semantics to the case of spatial variations, given its importance to the design of integrated circuits, detailing this extension will be a step that we wish to undertake next.

A. A FORMAL MODEL FOR PBL

Let $\mathscr{L}$ denote the *language* of PBL, which is a set of well formed *sentences* in PBL. The *signature* of $\mathscr{L}$ consists of

— A countable set VAR of variables.
— A countable set P of probability parameters.
— The connectives $\vee_p, \wedge_{p'}, \neg_{p''}$ where $p, p', p'' \in P$.
— The punctuation symbols (and).
— The set of constants $\{c^0, c^1\}$.
— Denumerable set of predicate letters $\overset{r}{=}$ where $r \in P$.

Any well formed *sentence* $\mathscr{S}[I]$ in this language is of the form $F_I \overset{r}{=} c^1$ or $F_I \overset{\bar{r}}{=} c^0$ where F is a well formed PBF, $r, \bar{r} \in P$, and I is an assignment which assigns one of $\{c^0, c^1\}$ to any variable $x \in \text{VAR}_F \subseteq \text{VAR}$.

The model $\mathbf{M}$ for this language consists of

— The punctuation symbols (and).
— The set $\mathbb{N} = \{0, 1, 2, \ldots\}$, of natural numbers.
— The set $C = \{0, 1\}$ of Boolean constants.
— A set $\mathbb{B}$ of valid closed sentences from classical Boolean logic of the form $B = 1$ or $B = 0$, where B is a closed well formed formula in Boolean logic. Conventionally, the former sentences will be called *true* sentences and the latter are called *false* sentences.
— the set $\mathbb{Q}$, of non-negative rationals.
— A set $\mathbb{E}$ where any $\mathbf{E}_{\mathscr{S},I} \in \mathbb{E}$ is referred to as an *event set* where $\mathbf{E} \subseteq \mathbb{N} \times \mathbb{B}$, and any $(i, \mathscr{B}) \in \mathbf{E}_{\mathscr{S},I}$ will be called an *event* (the index $i \in \mathbb{N}$ and Boolean sentence $\mathscr{B} \in \mathbb{B}$). Furthermore, if the classical Boolean sentence $\mathscr{B}$ is true, the event $(i, \mathscr{B})$ will be referred to as a *true event*; it is a *false event* otherwise.

— Let $\mathscr{S}_I$ denote $H_I \overset{r}{=\!=} \hat{c}$ where H is a well formed PBF and $\hat{c} \in \{c^0, c^1\}$. If H is of length 0, H is of the form (x) where x is a Boolean variable. For the assignment I which denotes $\langle x = c^1 \rangle$, $\mathbf{E}_{\mathscr{S},I}$ consists of one event of the form $(0, (1) = 1)$. Similarly for the assignment $\hat{I}$ which denotes $\langle x = c^0 \rangle$, $\mathbf{E}_{\mathscr{S},\hat{I}}$ consists of one event of the form $(0, (0) = 0)$.

Let H be a PBF of length $k \geq 1$, and let H be of the form $(F \vee_p G)$ where F and G are PBF of length $k-1$ or less. For an assignment I to H and the corresponding consistent assignments I', I'' to F and G respectively, let $\mathscr{S}'_{I'}, \mathscr{S}''_{I''}$ respectively denote $F_{I'} \overset{r'}{=\!=} c'$ and $G_{I''} \overset{r''}{=\!=} c''$, $c', c'' \in \{c^0, c^1\}$. Let $\mathbf{E}_{\mathscr{S}',I'}$, $\mathbf{E}_{\mathscr{S}'',I''}$ be the event sets of $\mathscr{S}'_{I'}$ and $\mathscr{S}''_{I''}$ respectively. Let $p^M = m/n$ where m, n are relatively prime and $\tilde{\mathbf{E}} = (\mathbf{E}_{\mathscr{S}',I'} \times \mathbf{E}_{\mathscr{S}'',I''})$. For any $((i, \mathscr{B}'), (j, \mathscr{B}'')) \in \tilde{\mathbf{E}}$ let $\mathscr{B}'$ denote $B' = t'$ and let $\mathscr{B}''$ denote $B'' = t''$, where B', B'' are well formed closed Boolean formulae and $t', t'' \in \{0, 1\}$. Let the number of true events in $\mathbf{E}_{\mathscr{S}',I'}$ be denoted by the symbol a, $|\mathbf{E}_{\mathscr{S}',I'}| = b$. Similarly, the number of true events in $\mathbf{E}_{\mathscr{S}'',I''}$ is c and $|\mathbf{E}_{\mathscr{S}'',I''}| = d$. Then,

$$\begin{aligned}
\hat{\mathbf{E}}_{\mathscr{S},I} &= \{ \text{ for } 0 \leq k < m, (f, (B' \vee B'') = T(t' \vee t'')) : ((i, \mathscr{B}'), (j, \mathscr{B}'')) \in \tilde{\mathbf{E}}\} && (10)\\
&\quad \text{where } f = (di + j) * n + k \\
\hat{\hat{\mathbf{E}}}_{\mathscr{S},I} &= \{ \text{ for } m \leq k < n, (g, (B' \vee B'') = T(\neg(t' \vee t''))) : ((i, \mathscr{B}'), (j, \mathscr{B}'')) \in \tilde{\mathbf{E}}\} && (11)\\
&\quad \text{where } g = (di + j) * n + k \\
\mathbf{E}_{\mathscr{S},I} &= \hat{\mathbf{E}}_{\mathscr{S},I} \cup \hat{\hat{\mathbf{E}}}_{\mathscr{S},I}
\end{aligned}$$

— A function $\psi : \mathbb{E} \rightarrow \mathbb{Q}$ such that $\psi(\mathbf{E}_{\mathscr{S},I})$ is the ratio of the number of true events in $\mathbf{E}_{\mathscr{S},I}$ to $|\mathbf{E}_{\mathscr{S},I}|$. A function $\bar{\psi} : \mathbb{E} \rightarrow \mathbb{Q}$ where $\bar{\psi}(\mathbf{E}_{\mathscr{S},I})$ is the ratio of the number of false events in $\mathbf{E}_{\mathscr{S},I}$ to $|\mathbf{E}_{\mathscr{S},I}|$.

— A relationship $R \subseteq C \times \mathbb{Q} \times \mathbb{E}$ where $(1, r, \mathbf{E}_{\mathscr{S},I}) \in R$ if and only if $\psi(\mathbf{E}_{\mathscr{S},I}) = r$ and $(0, \bar{r}, \mathbf{E}_{\mathscr{S},I}) \in R$ if and only if $\bar{\psi}(\mathbf{E}_{\mathscr{S},I}) = \bar{r}$.

OBSERVATION A.0.1. *Under the assignment I, $|\mathbf{E}_{\mathscr{S},I}| = bdn$ where the number of true events in $\mathbf{E}_{\mathscr{S},I}$ is $(acm + a(d-c)m + (b-a)cm + (b-a)(d-c)(n-m))$.*

PROOF. We recall that the the number of true events in $\mathbf{E}_{\mathscr{S}',I'}$ is a, $|\mathbf{E}_{\mathscr{S}',I'}| = b$, the number of true events in $\mathbf{E}_{\mathscr{S}'',I''}$ is c and $|\mathbf{E}_{\mathscr{S}'',I''}| = d$. We know that $T(1 \vee 0) = T(1 \vee 1) = T(0 \vee 1) = 1$. From this, and from (10), $(ad + (b-a)c)m$ events in $\hat{\mathbf{E}}_{\mathscr{S},I}$ are true events. Furthermore $T(\neg(0 \vee 0)) = 1$, and hence from (11), $(b-a)(d-c)(n-m)$ events in $\hat{\hat{\mathbf{E}}}_{\mathscr{S},I}$ are true events. Hence the number of true events in $\mathbf{E}_{\mathscr{S},I}$ is $(ad + (b-a)c)m + (b-a)(d-c)(n-m) = (acm + a(d-c)m + (b-a)cm + (b-a)(d-c)(n-m))$. Furthermore, from (10), the number of events in $\hat{\mathbf{E}}_{\mathscr{S},I}$ is bdm and from (11), the number of events in $\hat{\hat{\mathbf{E}}}_{\mathscr{S},I}$ is $bd(n-m)$. Hence the total number of events in $\mathbf{E}_{\mathscr{S},I}$ is $bdm + bd(n-m) = (bdn)$. □

Given any well formed sentence $\mathscr{S}[I] \in \mathscr{L}$ of the form $F_I \overset{r}{=\!=} c$, the *interpretation* of the sentence $\mathscr{S}[I]$ in the model $\mathbf{M}$, maps

— The constants c^0 to 0, c^1 to 1, c to $c^{\mathbf{M}} \in \{0, 1\}$.

— The probability parameters $p, q, \cdots$ to $p^{\mathbf{M}}, q^{\mathbf{M}}, \cdots \in \mathbb{Q}$ such that $1/2 \leq p^{\mathbf{M}}, q^{\mathbf{M}}, \cdots \leq 1$.

— The probability parameter r of the predicate symbol to $r^{\mathbf{M}} \in Q$ such that $0 \leq r^{\mathbf{M}} \leq 1$.

— The sentence $\mathscr{S}[I]$ to an event set $\mathbf{E}_{\mathscr{S},I}$.

— The sentence $\mathscr{S}[I]$ is *valid* under this interpretation if and only if $(c^{\mathbf{M}}, r^{\mathbf{M}}, \mathbf{E}_{\mathscr{S},I}) \in R$.

As an example consider a sentence $\mathscr{S}[I] \in \mathscr{L}$ of the form $(x \vee_p y) \stackrel{r}{=} c^1$ where the assignment I denotes $\langle x = c^0, y = c^1 \rangle$. Then under the interpretation $\mathbf{M}$, c^0 is mapped to 0, c^1 to 1, p to some $p^{\mathbf{M}} \in \mathbb{Q}$, where $1/2 \leq p^{\mathbf{M}} \leq 1$ and r to $r^{\mathbf{M}} \in Q$ such that $0 \leq r^{\mathbf{M}} \leq 1$. Let $p^{\mathbf{M}} = m/n$ for positive, relatively prime integers m, n. Then the number of true events in the event set $\mathbf{E}_{\mathscr{S},I}$ of $\mathscr{S}[I]$ is m and these elements are $(0, (0 \vee 1) = 1), (1, (0 \vee 1) = 1), \cdots, (m-1, (0 \vee 1) = 1)$ and the number of false events in $\mathbf{E}_{\mathscr{S},I}$ is $(n-m)$ and these events are $(m, \neg(0 \vee 1) = 0), (m+1, \neg(0 \vee 1) = 0), \cdots, (n-1, \neg(0 \vee 1) = 0)$. The sentence $\mathscr{S}[I]$ is valid under this interpretation if and only if $(1, r^{\mathbf{M}}, \mathbf{E}_{\mathscr{S},I}) \in R$, or equivalently, if and only if $\psi(\mathbf{E}_{\mathscr{S},I}) = r^{\mathbf{M}}$.

Similarly if H is of the form $(F \wedge_p G)$ and as before $p^M = m/n$,

$$\begin{aligned}
\hat{\mathbf{E}}_{\mathscr{S},I} &= \{ \text{ for } 0 \leq k < m, (f, (B' \wedge B'') = T(t' \wedge t'')) : ((i, \mathscr{B}'), (j, \mathscr{B}'')) \in \tilde{\mathbf{E}}\} \\
&\quad\ \text{where } f = (di + j) * n + k \\
\hat{\hat{\mathbf{E}}}_{\mathscr{S},I} &= \{ \text{ for } m \leq k < n, (g, (B' \wedge B'') = T(\neg(t' \wedge t''))) : ((i, \mathscr{B}'), (j, \mathscr{B}'')) \in \tilde{\mathbf{E}}\} \\
&\quad\ \text{where } g = (di + j) * n + k \\
\mathbf{E}_{\mathscr{S},I} &= \hat{\mathbf{E}}_{\mathscr{S},I} \cup \hat{\hat{\mathbf{E}}}_{\mathscr{S},I}
\end{aligned}$$

Similarly if H is of the form $\neg_p(F)$,

$$\begin{aligned}
\hat{\mathbf{E}}_{\mathscr{S},I} &= \{ \text{ for } 0 \leq k < m, (i * n + k, \neg(B') = T(\neg(t'))) : (i, (B' = t')) \in \mathbf{E}_{\mathscr{S}',I'}\} \\
\hat{\hat{\mathbf{E}}}_{\mathscr{S},I} &= \{ \text{ for } m \leq k < n, (i * n + k, (B' = t')) : (i, (B' = t')) \in \mathbf{E}_{\mathscr{S}',I'}\} \\
\mathbf{E}_{\mathscr{S},I} &= \hat{\mathbf{E}}_{\mathscr{S},I} \cup \hat{\hat{\mathbf{E}}}_{\mathscr{S},I}
\end{aligned}$$

REFERENCES

[1] L. M. Adleman. Two theorems on random polynomial time. In *19th Annual Symposium on Foundations of Computer Science*, pages 75–83, 1978.

[2] R. I. Bahar, J. Mundy, and J. Chen. A probabilistic-based design methodology for nanoscale computation. In *The 2003 IEEE/ACM International Conference on Computer-aided Design*, pages 480–486, 2003.

[3] G. Bergmann. The logic of probability. *American Journal of Physics*, 9:263–272, 1941.

[4] M. Blum and S. Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM Journal on Computing*, 13(4):850–864, 1984.

[5] L. Boltzmann. *Lectures on Gas Theory.* University of California Press, Berkeley, 1964.

[6] S. Borkar. Exponential challenges, exponential rewards - the future of moore's law. In *VLSI-SOC*, page 2, 2003.

[7] R. E. Bryant. Symbolic Boolean manipulation with ordered binary-decision diagrams. *ACM Computing Surveys*, 24(3):293–318, 1992.

[8] G. Chaitin. Algorithmic information theory. *IBM Journal of Research and Development*, 21:350–359, 1977.

[9] G. J. Chaitin and J. T. Schwartz. A note on monte carlo primality tests and algorithmic information theory. *Communications on Pure and Applied Mathematics*, 31:521–527, 1978.

[10] S. Cheemalavagu, P. Korkmaz, and K. V. Palem. Ultra low-energy computing via probabilistic algorithms and devices: CMOS device primitives and the energy-probability relationship. In *The 2004 International Conference on Solid State Devices and Materials*, pages 402–403, Sept. 2004.

[11] S. Cheemalavagu, P. Korkmaz, K. V. Palem, B. E. S. Akgul, and L. N. Chakrapani. A probabilistic CMOS switch and its realization by exploiting noise. In *The IFIP international conference on very large scale integration*, 2005.

[12] B. Chor and O. Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity (extended abstract). In *IEEE Symposium on Foundations of Computer Science*, pages 429–442, 1985.

[13] A. Church. On the concept of a random sequence. *Bulletin of the American Mathematical Society*, 46:130–135, 1940.

[14] R. T. Cox. Probability, frequency and reasonable expectation. *American Journal of Physics*, 14:1–13, 1946.

[15] R. T. Cox. *Algebra of Probable Inference.* Johns Hopkins University Press, 2002.

[16] M. Davis. *Engines of Logic: Mathematicians and the Origin of the Computer.* W. W. Norton and Company, New York, USA, 2001.

[17] B. de Finetti. Foresight, its logical laws, its subjective sources. *Translated and reprinted in: H. Kyburg, H. Smolka (Eds.), Studies in Subjective Probability*, pages 93–159, 1964.

[18] P. Diaconis. A frequentist does this, a bayesian that. *SIAM News*, mar 2004.

[19] R. L. Dobrushin and S. I. Ortyukov. Lower bound for the redundancy of self-correcting arrangements of unreliable functional elements. *Problems of Information Transmission*, 13(3):59–65, 1977.

[20] R. L. Dobrushin and S. I. Ortyukov. Upper bound on the redundancy of self-correcting arrangements of unreliable elements. *Problems of Information Transmission*, 13(3):201–20, 1977.

[21] B. Efron. Controversies in the foundations of statistics. *The American Mathematical Monthly*, 85(4):231–246, 1978.

[22] R. Fagin and J. Y. Halpern. Reasoning about knowledge and probability. *Journal of the ACM*, 41(2):340–367, 1994.

[23] R. Fagin, J. Y. Halpern, and N. Megiddo. A logic for reasoning about probabilities. *Information and Computation*, 87(1):78–128, 1990.

[24] W. Feller. *An Introduction to Probability Theory and its Applications.* Wiley Eastern Limited, 1984.

[25] H. Gaifman. Concerning measures in first order calculi. *Israel Journal of Mathematics*, 2(1):1–18, 1964.

[26] T. Hailperin. *Sentential Probability Logic: Origins, Development, Current Status, and Technical Applications.* Lehigh University Press, 1996.

[27] R. Impagliazzo and D. Zuckerman. How to recycle random bits. In *IEEE Symposium on Foundations of Computer Science*, pages 248–253, 1989.

[28] ITRS. International technology roadmap for semiconductors, 2007.

[29] N. Jacobson. *Basic Algebra I.* W H Freeman and Company, 1974.

[30] E. Jaynes. *Probability Theory: The Logic of Science.* Cambridge University Press, Cambridge, UK, 2003.

[31] A. Kamath, R. Motwani, K. V. Palem, and P. G. Spirakis. Tail bounds for occupancy and the satisfiability threshold conjecture. *Random Structures and Algorithms*, 7(1):59–80, 1995.

[32] R. M. Karp. The probabilistic analysis of some combinatorial search algorithms. In *Algorithms and complexity: New Directions and recent results (Traub, J. P., ed.)*, pages 1–19. Academic Press, New York, USA, 1976.

[33] M. G. Kendall. On the reconciliation of theories of probability. *Biometrika*, 36(1-2):101–116, 1949.

[34] J. M. Keynes. *A Treatise on Probability.* Macmillan, London, 1921.

[35] L. B. Kish. End of Moore's law: Thermal (noise) death of integration in micro and nano electronics. *Physics Letters A*, 305:144–149, 2002.

[36] P. G. Kolaitis and M. Y. Vardi. 0-1 laws and decision problems for fragments of second-order logic. *Information and Computation*, 87(1-2):302–338, 1990.

[37] A. N. Kolmogorov. *Foundations of the Theory of Probability (Trans. Nathan Morrison).* Chelsea Publishing Company, New York, 1956.

[38] A. N. Kolmogorov. Three approaches to the quantitative definition of information. *Problems of Information Transmission*, 1(1):1–7, 1965.

[39] P. Korkmaz. *Probabilistic CMOS (PCMOS) in the Nanoelectronics Regime.* PhD thesis, Georgia Institute of Technology, 2007.

[40] P. Korkmaz, B. E. S. Akgul, L. N. Chakrapani, and K. V. Palem. Advocating noise as an agent for ultra low-energy computing: Probabilistic CMOS devices and their characteristics. *Japanese Journal of Applied Physics*, 45(4B):3307–3316, Apr. 2006.

[41] J. Meindl. Theoretical, practical and analogical limits in ulsi. *IEEE International Electron Device Meeting Technical Digest*, pages 8–13, 1983.

[42] E. Mendelson. *Introduction to Mathematical Logic.* Chapman and Hall, 1997.

[43] G. D. Micheli. *Synthesis and Optimization of Digital Circuits.* McGraw-Hill Higher Education, 1994.

[44] G. Moore. No exponential is forever: But forever can be delayed! In *IEEE International Solid-State Circuits Conference*, pages 20–23, 2003.

[45] G. E. Moore. Cramming more components onto integrated circuits. *Electronics Magazine*, 38(8), 1965.

[46] R. Motwani and P. Raghavan. *Randomized Algorithms.* Cambridge University Press, 1995.

[47] K. Natori and N. Sano. Scaling limit of digital circuits due to thermal noise. *Journal of Applied Physics*, 83:5019–5024, 1998.

[48] K. Nepal, R. I. Bahar, J. Mundy, W. R. Patterson, and A. Zaslavsky. Designing logic circuits for probabilistic computation in the presence of noise. In *The 42nd Design Automation Conference*, pages 485–490, 2005.

[49] N. J. Nilsson. Probabilistic logic. *Artificial Intelligence*, 28(1), 1986.

[50] K. V. Palem. Proof as experiment: Probabilistic algorithms from a thermodynamic perspective. In *The International Symposium on Verification (Theory and Practice),*, Taormina, Sicily, June 2003.

[51] K. V. Palem. Energy aware computing through probabilistic switching: A study of limits. *IEEE Transactions on Computers*, 54(9):1123–1137, 2005.

[52] N. Pippenger. On networks of noisy gates. In *The 26th Annual IEEE Symposim on Foundations of Computer Science*, pages 30–38, 1985.

[53] N. Pippenger. Invariance of complexity measures for networks with unreliable gates. *Journal of the ACM*, 36:531–539, 1989.

[54] N. Pippenger, G. D. Stamoulis, and J. N. Tsitsiklis. On a lower bound for the redundancy of reliable networks with noisy gates. *IEEE Transactions on Information Theory*, 37(3):639–643, 1991.

[55] M. O. Rabin. Probabilistic automata. *Information and Control*, 6:230–245, 1963.

[56] M. O. Rabin. Probabilistic algorithms. In J. F. Traub, editor, *Algorithms and Complexity, New Directions and Recent Trends*, pages 29–39. 1976.

[57] F. P. Ramsey. Truth and probability (reprinted 1990). In *Philosophical Papers, D. H. Mellor (ed.).* Cambridge University Press, Cambridge, 1926.

[58] H. Reichenbach. *The Theory of Probability.* University of California Press, Berkeley, USA, 1949.

[59] N. Sano. Increasing importance of electronic thermal noise in sub-0.1mm Si-MOSFETs. *The IEICE Transactions on Electronics*, E83-C:1203–1211, 2000.

[60] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.

[61] D. Scott and P. Krauss. Assigning probabilities to logical formulas. *Aspects of Inductive Logic (J. Hintikka and P. Suppes, ed.)*, pages 219–264, 1966.

[62] A. M. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, 2(42):230–265, 1936.

[63] J. Venn. *The Logic of Chance (reprinted 1962).* Macmillan and co, New York, USA, 1876.

[64] von Mises R. *Probability, Statistics and Truth, revised English edition.* Macmillan and co, New York, USA, 1957.

[65] J. von Neumann. Probabilistic logics and the synthesis of reliable organizms from unreliable components. *Automata Studies*, pages 43–98, 1956.

[66] J. E. Whitesitt. *Boolean Algebra and Its Applications.* Dover Publications, 1995.

[67] A. Yao. Theory and application of trapdoor functions. In *The 23rd Symposium on The Foundations of Computer Science*, pages 80–91, 1982.