Formal Analysis of Soft Errors using Theorem Proving

Naeem Abbasi, Osman Hasan and Sofiène Tahar
ECE Department, Concordia University, Montreal, QC, Canada
{n_ab,o_hasan,tahar}@ece.concordia.ca

Modeling and analysis of soft errors in electronic circuits has traditionally been done using computer simulations. Computer simulations cannot guarantee correctness of analysis because they utilize approximate real number representations and pseudo random numbers in the analysis and thus are not well suited for analyzing safety-critical applications. In this paper, we present a higher-order logic theorem proving based method for modeling and analysis of soft errors in electronic circuits. Our developed infrastructure includes formalized continuous random variable pairs, their Cumulative Distribution Function (CDF) properties and independent standard uniform and Gaussian random variables. We illustrate the usefulness of our approach by modeling and analyzing soft errors in commonly used dynamic random access memory sense amplifier circuits.

1 Introduction

In many safety critical applications, such as in avionics, electronic equipment operates in harsh environments and experiences extreme temperatures and excessive doses of solar and cosmic radiations. This can often result in change in the state of the charge storage nodes in electronic circuits. Such abnormal changes in the states of storage nodes in electronic circuits are called soft errors [14]. These nonrecurrent and non permanent errors can cause an electronic system to behave in an un predictable way. There are four commonly known causes of soft errors in logic and memory circuits: 1) undesirable capacitive coupling of circuit elements [12], 2) circuit parameter fluctuations and variations, 3) ionizing particle and EM radiation, and 4) built-in thermal, shot and $1/f$ noise. Good circuit design and layout techniques can be used to effectively eliminate soft errors due to undesirable capacitive coupling and circuit parameter variations [2]. In order to deal with the other two types of soft errors accurate analysis of the design is required [14, 15].

Soft error occurrence mechanism is random in nature and is usually analyzed using simulation based techniques such as Monte carlo simulation methods [16]. These techniques tend to be inaccurate and slow and are unsatisfactory for safety critical applications. Realistic analysis of most practical linear and non-linear circuits involves real and random variables. Formal methods based techniques, such as probabilistic model checking, are unsuitable for the analysis of such problems as it is usually not possible to accurately model the continuous electronic circuit behavior using finite state systems.

In this paper, we apply the higher-order logic theorem proving method [5] to the problem of random effect modeling and analysis in electronic circuits. The main reason for using higher-order logic is to leverage upon its high expressiveness, which allows us to precisely model any system that can be expressed mathematically. Thus, it allows us to construct true continuous and randomized models of electronic circuits and thus alleviates the limitations of simulation and model checking based analysis techniques. These models are then used to form an equivalence or an implication relation with their specifications. These boolean relationships are then proved using mathematical reasoning in the sound core of the HOL theorem prover.

Adel Bouhoula, Tetsuo Ida and Fairouz Kamareddine (Eds.):
Symbolic Computation in Software Science 2012 (SCSS2012)
EPTCS 122, 2013, pp. 75–84, doi:10.4204/EPTCS.122.7

© N. Abbasi, O. Hasan & S. Tahar
This work is licensed under the
Creative Commons Attribution License.

Probabilistic analysis infrastructure has been developed in HOL during the last decade. Hurd formalized discrete random variables having Uniform, Bernoulli, Binomial, and Geometric probability mass functions in the HOL theorem prover [10]. Audebaud et al., describe a method for proving properties of randomized algorithms in Coq proof assistant [3]. They use functional and algebraic properties of unit interval to show the validity of general rules for estimating the probabilities of randomized algorithms. However, similar to Hurd's work, their approach can only address discrete distributions. Hasan, building on Hurds work, formalized statistical properties of single and multiple discrete random variables, continuous random variables with various distributions using inverse transform method [7] and verified their probabilistic and some statistical properties [8]. Harrison [6] formalized the guage integration on finite-dimensional Euclidean spaces, which is quite similar to product space of Lebesgue measures. Okazaki and Shidama [19] formalized properties of real valued random vairables in Mizar. More recently, Hoelzl [9] and Mhamdi [17, 18] formalized basic notions of measure, topology and lebesgue integration. These formalisms are based on extended real numbers and are thus more expressive than Hurds formalization of probability theory. However, they do not contain a specific probability space due to which they cannot be used to verify random variable functions. Since, soft error is primarily based on modeling the uncertainties by appropriate random variables so we have chosen Hurd's formalization of measure theory for this work. To the best of our knowledge, the foremost foundations of soft error analysis of electronic circuits, such as the formalization of continuous random variable pair, its classic Cumulative Distribution Function (CDF) properties, and the formalization of Gaussian random variable pair do not exist in literature and is presented for the very first time in this paper.

Our proposed method is shown in Figure 1. We build on existing real number, transcendental function, set, measure, and probability theories in the HOL theorem prover. Our developed infrastructure includes formalization of a continuous random variable pair using an approach similar to [7]. We have formalized important notions of joint and marginal cumulative distribution functions and the independence of random variable pairs. Using the specification of random variable pairs, we then verify their CDF properties by interactively constructing the proofs of these properties for arbitrary continuous random variables. Then using Inverse Transform Method, we have formalized random variable pairs for which inverse CDF function of the cumulative probability distribution function exists.

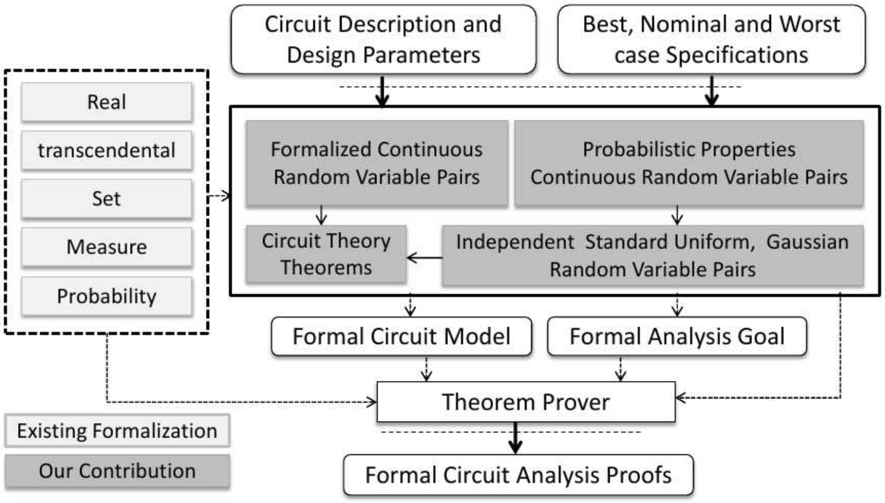
Circuit Description and Design Parameters
Best, Nominal and Worst case Specifications
Real
transcendental
Set
Measure
Probability
Formalized Continuous Random Variable Pairs
Probabilistic Properties Continuous Random Variable Pairs
Circuit Theory Theorems
Independent Standard Uniform, Gaussian Random Variable Pairs
Formal Circuit Model
Formal Analysis Goal
Theorem Prover
Existing Formalization
Our Contribution
Formal Circuit Analysis Proofs

Figure 1: Proposed methodology for circuit analysis

In this paper, we also describe the formalization of a pair of independent Gaussian random variables using the Box-Muller method [4]. We then utilize these variables in the modeling and formal analysis of soft errors caused by thermal noise in sense amplifier circuit of a DRAM. In a typical analysis using our proposed method, the design and the best, nominal and worst case specifications are first expressed using higher-order logic. Uncertain design and operating environment behaviors are then accurately modeled using formalized random variables in higher-order logic. Design uncertainties include noise and device model parameter variations. Realistic and accurate operating environment uncertainties include effects such as variations in the operating temperature, supply voltage, and varying doses of incident particle and electromagnetic radiation. Finally, the analysis is carried out interactively in the trusted kernel of the HOL theorem prover and formal circuit and system analysis proofs are constructed.

The rest of the paper is organized as follows: Section 2 describes the formalization of continuous random variable pair, verification of its classical properties, and formalization of standard Uniform and Gaussian random variable pairs. Using the developed infrastructure, we describe an accurate analysis of soft errors in the sense amplifier of dynamic random access memories in Section 3. Finally, Section 4 concludes the paper.

2 Formalization of Continuous Random Variables

In Hurd's formalization [10], a random variable $\mathscr{F}$ is a higher-order logic probabilistic function which takes a parameter of type α and an infinite Boolean sequence, ranges over values of type β and upon termination returns the remaining portion of the infinite Boolean sequence.

$$\mathscr{F} : \alpha \rightarrow B^{\infty} \rightarrow \beta \times B^{\infty}$$

Hurd formalized four probabilistic algorithms with Uniform, Bernoulli, Binomial, and Geometric probability mass functions. Hasan [7], building on Hurd's work, formalized a standard uniform random variable as a special case of the discrete version of a uniform random variable, as given in Equation 1.

$$\lim_{n\rightarrow\infty}(\lambda n. \sum_{k=0}^{n-1}(\frac{1}{2})^{k+1}X_k) \tag{1}$$

where $(\lambda n. \sum_{k=0}^{n-1}(\frac{1}{2})^{k+1}X_k)$ represents the discrete uniform random variable. Hasan's formal specification of the standard uniform random variable in HOL is given in Definition 1, and is based on Equation 1.

Definition 1: *Standard Uniform Random Variable* [7]

`⊢ ∀ s.  std_unif_cont s = lim (λn.  fst (std_unif_disc n s))`

The function `std_unif_disc` is a standard discrete uniform random variable in HOL. It takes two arguments, a natural number (`n`:num) and an infinite sequence of random bits (`s`:num→bool). The function utilizes these two arguments and returns a pair of type (real, num→bool). The real value corresponds to the value of the random variable and the second element in the pair is the unused portion of the infinite boolean sequence. The function `fst` takes a pair as input and returns the first element of the pair, and the function `lim P` in HOL is the formalization of the limit of a real sequence `P`. Using Inverse Transform Method (ITM), Hasan formalized uniform, triangular, exponential and rayleigh random variables. Hasan's HOL formalization of a standard uniform random variable `uniform_rv` is as follows:

`⊢ ∀s a b.  uniform_rv a b s = (b - a)(std_unif_cont s) + a.`

Where `a` and `b` are the two real parameters of the uniform random variable. We build upon these foundations to formalize pairs of continuous random variables in this paper.

2.1 Continuous Random Variable Pairs

Multiple independent random variables are often required to model and analyze hard to predict and random behaviour of electronic circuits and systems. To perform such modeling and analysis in a theorem proving environment formalized independent random variables are needed. Building on Hasan's work, we formalize a pair of Uniform continuous random variables as:

$$(\lim_{n\to\infty}(\lambda n. \sum_{k=0}^{n-1}(\frac{1}{2})^{k+1}X_{1k}), \lim_{n\to\infty}(\lambda n. \sum_{k=0}^{n-1}(\frac{1}{2})^{k+1}X_{2k})),$$

where $(\lambda n. \sum_{k=0}^{n-1}(\frac{1}{2})^{k+1}X_{ik})$, $i \in \{1,2\}$, represents a discrete uniform random variable. The HOL formalization of a pair of Uniform continuous random variables is given by:

$\vdash \forall$s. std_unif_pair_cont s $= (\lim_{n\to\infty}(\lambda$n. fst (std_unif_disc n (seven s))),
$\lim_{n\to\infty}(\lambda$n. fst (std_unif_disc n (sodd s))))

$\vdash \forall$s. X1_S_UNIF s = fst (std_unif_pair_cont s);

$\vdash \forall$s. X2_S_UNIF s = snd (std_unif_pair_cont s)

We also formalize important concepts of Joint and Marginal Cumulative Distribution Functions and the Independence of a pair of random variables. These concepts play a vital role in analyzing soft errors as will be demonstrated later. Our formalization of these concepts is based on [13].

Definition 2 describes the HOL formalization of the joint CDF of a pair of random variables mathematically expressed as:

$F_{X_1,X_2}(x_1,x_2) = P(X_1 \leq x_1 \wedge X_2 \leq x_2)$.

Definition 2: *Joint CDF of a Pair of Random Variables*

```
⊢ ∀ X1 X2 x1 x2.  joint_cdf X1 X2 x1 x2 =
                      prob bern {s | (X1 s ≤ x1) ∧ (X2 s ≤ x2)}
```

where X1 and X2 are the first and second element of the random variable pair and x1 and x2 are two real numbers.

The marginal CDF functions of a pair of random variables (X_1, X_2) is defined as:

$F_{X1}(x1) = \lim_{x2\to\infty} F_{X1,X2}(x1,x2)$ = P(X1 $\leq$ x1) and

$F_{X2}(x2) = \lim_{x1\to\infty} F_{X1,X2}(x1,x2)$ = P(X2 $\leq$ x2).

The HOL formalization of marginal CDF functions is given in Definition 3.

Definition 3: *Joint CDF of a Pair of Random Variables*

```
⊢ ∀ X1 X2 x1.  marginal_cdf_x1 X1 X2 x1 =
         lim (λn.  prob bern {s| (X1 s) ≤ x1 ∧ (X2 s) ≤ (&n))})
⊢ ∀ X1 X2 x2.  marginal_cdf_x2 X1 X2 x2 =
         lim (λn.  prob bern {s| (X1 s) ≤ (&n) ∧ (X2 s) ≤ x2)})
```

Two random variables X1 and X2 are said to be independent if for every pair of real numbers x1 and x2 the two events $\{X1 \leq x1\}$ and $\{X2 \leq x2\}$ are independent. Which means that the value of one random variable has no influence on the other and vice versa. This notion is very useful in accurate and realistic modeling of practical electronic circuits and systems. Mathematically the notion of independence is defined as:

P{X1 $\leq$ x1 $\wedge$ X2 $\leq$ x2} = P{X1 $\leq$ x1}.P{X2 $\leq$ x2}

The HOL formalization is given in Definition 4.

Definition 4: *Independent Random Variable Pair*

```
⊢ ∀ X1 X2 x1 x2.  independent_rv_pair X1 X2 x1 x2 =
      ({s | X1 s ≤ x1 ∧ X2 s ≤ x2} IN events bern) ∧
      (prob bern {s | X1 s ≤ x1 ∧ X2 s ≤ x2} =
       prob bern {s | X1 s ≤ x1} * prob bern {s | X2 s ≤ x2})
```

2.2 Formal Verification of CDF Properties of Pairs of Random Variables

Using the formal specification of the CDF function for a pair of random variables, we have formally verified the classical properties of the CDF of a pair of random variables. These properties are verified under the assumption that the set `{s | R s x}`, where `R` represents a pair of random variables under consideration, is measurable for all values of the pair. The formal proofs for these properties confirm our formalized specifications of the CDF of a pair of random variables. We summarize these results in Table 1.

Table 1: CDF properties of continuous random variable pairs

Property	**Mathematical Description; HOL Formalization**

CDF Bounds	$0 \leq F_{X_1,X_2}(x_1,x_2) \leq 1$;
	`⊢ ∀X1 X2 x1 x2.CDF_pair_in_events_bern X1 X2 x1 x2 ⇒`
	`((0 ≤ joint_cdf X1 X2 x1 x2) ∧ (joint_cdf X1 X2 x1 x2 ≤ 1))`

CDF Monotonic Non decreasing	$F_{X_1,X_2}(a,c) \leq F_{X_1,X_2}(b,d)$;
	`⊢ ∀a b c d. (a < b) ∧ (c < d) ∧`
	`(∀ x1 x2.  CDF_pair_in_events_bern X1 X2 x1 x2) ⇒`
	`( (joint_cdf X1 X2 a c ≤ joint_cdf X1 X2 b c) ∧`
	`(joint_cdf X1 X2 b c ≤ joint_cdf X1 X2 b d) )`

CDF Pair at +∞	$\lim_{x2 \to \infty} \lim_{x1 \to \infty} F_{X1,X2}$(x1,x2) =$F_{X1,X2}$(∞,∞) = 1;
	`⊢  (∀ X1 x1.  CDF_in_events_bern X1 x1) ∧`
	`(∀ X1 X2 x1 x2.  CDF_pair_in_events_bern X1 X2 x1 x2) ⇒`
	`(lim (λn1.  lim (λn2.  joint_cdf X1 X2 (& n1) (& n2))) = 1)`

CDF Pair at -∞	$\lim_{x2 \to -\infty} F_{X1,X2}(x1,x2)$ = $\lim_{x1 \to -\infty} F_{X1,X2}(x1,x2)$ = 0;
	`⊢  (∀X1 X2 x1 x2.  CDF_pair_in_events_bern X1 X2 x1 x2) ⇒`
	`( (lim (λn.  joint_cdf X1 X2 (- & n) x2) = 0) ∧`
	`(lim (λn.  joint_cdf X1 X2 x1 (- & n)) = 0) )`

As an example, we present the proof of one such property here called the CDF interval property. The rest of the formal proofs can be found in [1].

CDF Pair Interval Property

If `a`, `b`, `c`, and `d` are real numbers with `a < b`, and `c < d`, then the probability of an interval event of a pair of random variables is given by `P(a < X1 ≤ b, c < X2 ≤ d) =` $F_{X1,X2}$`(b,d) -` $F_{X1,X2}$`(b,c) -` $F_{X1,X2}$`(a,d) +` $F_{X1,X2}$`(a,c)`. The property is formally stated in Theorem 1.

Theorem 1: *CDF Pair Useful Interval Property*

```
⊢ ∀a b c d.  (a < b) ∧ (c < d) ∧
  {s | X1 s ≤ a ∧ c < X2 s ∧ X2 s ≤ d} IN events bern ∧
  {s | a < X1 s ∧ X1 s ≤ b ∧ c < X2 s ∧ X2 s ≤ d} IN events bern
  {s | X1 s ≤ a ∧ X2 s ≤ c} IN events bern ∧
  {s | X1 s ≤ b ∧ X2 s ≤ c} IN events bern ∧
  {s | X1 s ≤ b ∧ c < X2 s ∧ X2 s ≤ d} IN events bern ⇒
   ( prob bern {s | a < X1 s ∧ X1 s ≤ b ∧ c < X2 s ∧ X2 s ≤ d} =
     joint_cdf X1 X2 b d - joint_cdf X1 X2 b c -
     joint_cdf X1 X2 a d + joint_cdf X1 X2 a c )
```

Proof: The proof of this property begins by first showing that the events (a $<$ X1 $\leq$ b $\wedge$ c $<$ X2 $\leq$ d) and (X1 $\leq$ a $\wedge$ c $<$ X2 $\leq$ d) are disjoint. Then we show that P(a $<$ X1 $\leq$ b $\wedge$ c $<$ X2 $\leq$ d) + P(X1 $\leq$ a $\wedge$ c $<$ X2 $\leq$ d) = P(X1 $\leq$ b $\wedge$ c $<$ X2 $\leq$ d), using the additive law of probabilities [10]. Similarly, we prove that, P(X1 $\leq$ b $\wedge$ c $<$ X2 $\leq$ d) + P(X1 $\leq$ b $\wedge$ X2 $\leq$ c) = P(X1 $\leq$ b $\wedge$ X2 $\leq$ d) and P(X1 $\leq$ a $\wedge$ c $<$ X2 $\leq$ d) + P(X1 $\leq$ a $\wedge$ X2 $\leq$ c) = P(X1 $\leq$ a $\wedge$ X2 $\leq$ d). Finally, we conclude the proof by rewriting and simplifying with the definitions of the joint CDF function and the above results. This property states that the probability that the random vector (X1,X2) falls in a rectangular region and can be found by combining the values of cumulative distribution function at the four corners of the rectangular region.

2.3 Formalization of Gaussian Random Variable Pairs

Thermal noise in electronic circuits is caused by random motion of electrons in semiconductor materials and is typically modeled using Gaussian random variables. In this section, we describe the HOL formalization of a pair of independent Gaussian random variables using the Box-Muller method [4]. According to the Box-Muller method, given a pair of independent standard Uniform random variables (U_1,U_2), a pair of independent Gaussian random variable can be formalized as:

$(G_1,G_2) = (\sqrt{-2\ ln\ U_1}\ cos(2\ \pi\ U_2),\sqrt{-2\ ln\ U_1}\ sin(2\ \pi\ U_2))$.

The HOL formalization of the Gaussian random variable is given in Table 2.

Table 2: Gaussian random variable formalization in HOL

Distribution	Formalized Random Variable Pair
Standard Gaussian (0,1)	$\vdash\forall$s. std_g_pair_rv s = (($\sqrt{\text{-2 ln (X1\_S\_UNIF s)}}$ cos(2π(X2_S_UNIF s))), ($\sqrt{\text{-2 ln (X1\_S\_UNIF s)}}$ sin(2π(X2_S_UNIF s))))
Gaussian (σ,μ)	$\vdash\forall$s μ σ. g_pair_rv μ σ s = (μ + σ fst (std_g_pair_rv s), μ + σ snd (std_g_pair_rv s)) $\vdash\forall$s. V1_G μ σ s = fst (g_pair_rv μ σ s); $\vdash\forall$s. V2_G μ σ s = snd (g_pair_rv μ σ s)

In this section, we described the formalization of a standard uniform random variable pair and the formalization of a Gaussian random variable pair. These two distributions are used in modeling of realistic process, supply voltage and temperature variations in electronic circuits. Using the formalization described in this section, we can for the very first time model and analyze behavior of analog and mixed signal circuits in a higher-order logic theorem prover and reason about their functional properties in the presence of random process and environment variations. To illustrate the usefulness of our formalization, we present an application in the next section.

3 Formal Analysis of Soft Errors in DRAMs

3.1 Dynamic Random Access Memory

Figure 2(a) shows a typical block diagram of a Dynamic Random Access Memory or DRAM. It consists of address buffers, decoders, memory array, and input/output interface circuits. Sense amplifiers are very sensitive differential amplifiers. A differential amplifier usually has three inputs. A pair of inputs is connected to the two bit lines (Figure 2(b), lines bit,$\overline{\text{bit}}$). The third input is used to enable the sense amplifier (ϕ_{R}). The amplifier increases the amplitude of the difference signal between the two bit lines and thermal noise can affect the operation of the sense amplifier. Figure 2(b) shows a balanced bit-line architecture of a commercial DRAM. In this architecture one sense amplifier connects to the bit line of two identical arrays. The circuit diagram shows one transistor storage cells, C_S, dummy cells, C_D, and the sense amplifier. The loading effects of the pre-charge, refresh and the input output devices of the DRAM are included in C_B. More details can be found in [11].

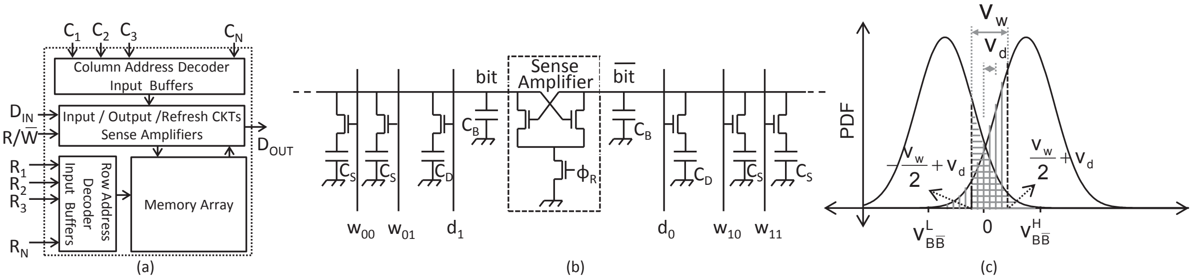

Figure 2: DRAM block diagram (a), balanced bit-line architecture (b), PDF of non-ideal sense amplifier bit line voltages [14] (c).

We model the voltages on the two bit lines connected to the inputs of a non-ideal sense amplifier as two independent Gaussian random variables V_1_G(-$V^L_{B\bar{B}}$,$v_{B\bar{B}n}$) and V_2_G($V^H_{B\bar{B}}$,$v_{B\bar{B}n}$), where $v_{B\bar{B}n}$ represents the standard deviation of the thermal noise [14]. Figure 2(c) shows the probability density functions (PDF) for the two inputs to the sense amplifier. The vertical shaded area represents the probability of detecting a logic “1” in the DRAM cell due to the noise when in fact a logic “0” is stored in that location. Similarly, the horizontally shaded region corresponds to detecting a logic “0” when in fact a logic “1” is stored in the memory. The probabilities of a low level being detected as high and that of a high level being detected as low, at the two bit lines, is given by, $P(-\frac{v_w}{2}+v_d < V_1\_G) = Q\left(\frac{-\frac{v_w}{2}+v_d-(-V^L_{B\bar{B}})}{\sqrt{v^2_{B\bar{B}}}}\right)$, and $P(V_2\_G \leq \frac{v_w}{2}+v_d) = 1-Q\left(\frac{\frac{v_w}{2}+v_d-V^H_{B\bar{B}}}{\sqrt{v^2_{B\bar{B}}}}\right)$, respectively. Where the insensitivity width and the sensitivity center deviation are given by $v_w = \delta V_{B\bar{B}}$ and $v_d = \chi V_{B\bar{B}}$, where $0 \leq \chi, \delta \leq 1$ [14]. Using these assumptions and that both 0 and 1 errors are equally likely to occur, the soft error rate is given by: $P_{error} = \frac{1}{4}\text{erfc}\left[\frac{V^L_{B\bar{B}}}{\sqrt{2}\sqrt{v^2_{B\bar{B}}}}\left(1-\frac{\delta}{2}+\chi\right)\right] + \frac{1}{4}\text{erfc}\left[\frac{V^H_{B\bar{B}}}{\sqrt{2}\sqrt{v^2_{B\bar{B}}}}\left(1-\frac{\delta}{2}-\chi\right)\right]$. Where error function (*erfc*) is defined as: $erfc(x) = 2Q\left(\sqrt{2}x\right)$. Next, we formally verify this result using the proposed formalization.

3.2 Verification of soft error rates

Based on the proposed methodology described in Section 1, the first step is to formally represent the Non-ideal sense amplifier soft error rate model, which can be done as follows:

Definition 4: *Non-ideal Sense Amplifier SER Model*

$\vdash\ \forall\ V^L_{B\bar{B}}\ V^H_{B\bar{B}}\ v_{B\bar{B}n}\ v_w\ v_d$.
`non_ideal_ser` $V^L_{B\bar{B}}\ V^H_{B\bar{B}}\ v_{B\bar{B}n}\ v_w\ v_d$ `=`
$\frac{1}{2}(\mathbb{P}\{s|(v_d-\frac{v_w}{2}) < (V_1\_G\ \ (-V^L_{B\bar{B}})\ \ v_{B\bar{B}n}\ \ s)\}$ `+`
$\mathbb{P}\{s|(V_2\_G\ \ V^H_{B\bar{B}}\ \ v_{B\bar{B}n}\ \ s) \leq (v_d+\frac{v_w}{2})\})$

Now based on this formal definition, we can formally verify the following useful probabilistic relationship regarding the soft error rate for a non-ideal sense amplifier in the presence of thermal noise and parameter variations.

Theorem 2: *Non-ideal Sense Amplifier Soft Error Rate*

$\vdash \forall\ \mathtt{a\ b\ f}\ V^{H}_{\bar{BB}}\ V^{L}_{\bar{BB}}\ v_{B\bar{B}n}\ \delta\ \chi.$
$((\mathtt{a}\leq\mathtt{b})\ \wedge\ (\forall\mathtt{x}.\ \ (\mathtt{a}\leq\mathtt{x})\ \wedge\ (\mathtt{x}\leq\mathtt{b})\ \Rightarrow\ (\mathtt{f\ diffl}\ (\lambda\mathtt{t}.\ \ \frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}})\ \mathtt{x})\ \mathtt{x})\ \wedge\ (\mathtt{Q1\ a\ b\ =\ f\ b}$
$\mathtt{-\ f\ a})\ \wedge\ (\mathtt{Q\ y\ =}\ \lim_{n\to\infty}\ (\lambda\mathtt{n}.\ \ \mathtt{Q1\ y\ (\&n)}))\ \wedge$
$(\forall\mathtt{x}.\ \ \mathtt{Q\ x\ =}\ \frac{1}{2}\ \mathtt{erfc}\ (\frac{x}{\sqrt{2}}))\ \wedge\ (\forall\mathtt{z}\ \mu\ \sigma.\ \ (0\ <\ \sigma)\ \Rightarrow\ (\mathbb{P}\{\mathtt{s}\ \mid\ \mathtt{z}\ <\ V_1\_G\ \mu\ \sigma\ \mathtt{s}\}\ =\ \mathtt{Q}$
$(\frac{z-\mu}{\sigma}))\ \wedge\ (\forall\mathtt{z}\ \mu\ \sigma.\ \ (0\ <\ \sigma)\ \Rightarrow\ (\mathbb{P}\{\mathtt{s}\ \mid\ \mathtt{z}\ <\ V_2\_G\ \mu\ \sigma\ \mathtt{s}\}\ =\ \mathtt{Q}\ (\frac{z-\mu}{\sigma}))\ \wedge\ (0\leq\delta)\ \wedge$
$(\delta\leq1)\ \wedge\ (0\leq\chi)\ \wedge\ (\chi\leq1)\ \wedge\ (v_w\ =\ \delta V^{H}_{\bar{BB}})\ \wedge\ (v_d\ =\ \chi\ V^{H}_{\bar{BB}})\ \wedge\ (0\ <\ v_{B\bar{B}n})\ \wedge$
$(V^{L}_{\bar{BB}} = -V^{H}_{\bar{BB}})\ \wedge\ (\mathtt{Q(y)\ +\ Q(-y)\ =\ 1})\ \Rightarrow\ \mathtt{non\_ideal\_ser}\ V^{L}_{\bar{BB}}\ V^{H}_{\bar{BB}}\ v_{B\bar{B}n}\ =$
$\frac{1}{4}\mathtt{erfc}\left(\frac{V^{H}_{\bar{BB}}}{\sqrt{2}\ \ v_{B\bar{B}n}}\left[1-\frac{\delta}{2}+\chi\right]\right)\ +\ \frac{1}{4}\mathtt{erfc}\left(\frac{V^{L}_{\bar{BB}}}{\sqrt{2}\ \ v_{B\bar{B}n}}\left[1-\frac{\delta}{2}-\chi\right]\right)$

The predicate `((f diffl (`λ`t.` $\frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}$`) x) x)` in the first assumption states that the differential of the function `f` with respect to `x` is the function (λt. $\frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}$). The second assumption states that `Q1` is a function with two real arguments `a` and `b`, and it returns a real value `f(b) - f(a)`, which is equal to the value of the definite integral of (λt. $\frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}$). The third assumption then formally represents the `Q` function as the limit value of function `Q1` when its second argument tends to infinity. The fourth assumption describes the relationship between the `Q` function and the error function (`erfc`, defined in [1]). Assumptions 5 and 6 explicitly state that the probabilities of the random variables V_1_G and V_2_G taking values greater than an arbitrary real number `z` is given by `Q` $(\frac{z-\mu}{\sigma})$. Assumptions 7, 8, 9, 10, 11, and 12 state that δ and χ which relate the insensitivity width (v_w = $\delta V^{H}_{\bar{BB}}$) and the sensitivity deviation (v_d = χ $V^{H}_{\bar{BB}}$) parameters to the mean values of the Gaussian random variables V_1_G and V_2_G, are real numbers and can only take values in the closed real interval [0,1]. The thirteenth assumption makes sure that the standard deviation of the thermal noise is a non zero positive value ($0 < v_{B\bar{B}_n}$). The fourteenth assumption ($V^{L}_{\bar{BB}} = -V^{H}_{\bar{BB}}$) states that the sense amplifier at its inputs sees two equal and opposite polarity dc signals represented by $V^{H}_{\bar{BB}}$ and $V^{L}_{\bar{BB}}$, respectively. The fifteenth assumption states an important property of the Q function that the total area under the Q function is equal to 1.

Proof: We begin the proof by rewriting the right hand side of Theorem 2 with the definition of the complementary error function ($\forall$`x.  Q x =` $\frac{1}{2}$ `erfc (`$\frac{x}{\sqrt{2}}$`))`, the property of Q function (Q(x)+Q(-x)=1), and three other assumptions of Theorem 2, that is, $v_w = \delta V^{H}_{\bar{BB}}$, $v_d = \chi\ V^{H}_{\bar{BB}}$ and $V^{L}_{\bar{BB}} = -V^{H}_{\bar{BB}}$. This reduces the righthand side of the proof goal to: $\frac{1}{2}\left[1-\mathbb{P}\{s|(v_d+\frac{v_w}{2})\ <\ (V_2\_G\ V^{H}_{\bar{BB}}\ v_{B\bar{B}n}\ s)\}\right]$ + $\frac{1}{2}\mathbb{P}\{s|(v_d-\frac{v_w}{2}) < (V_1\_G\ (V^{H}_{\bar{BB}})\ v_{B\bar{B}n}\ s)\}$. Now using the fact that $\mathbb{P}(x\leq a)+\mathbb{P}(a<x)=1$, we rewrite the first term in the above expression as:
$\frac{1}{2}\left[\mathbb{P}\{s|(V_2\_G\ V^{H}_{\bar{BB}}\ v_{B\bar{B}n}\ s)\ \leq\ (v_d+\frac{v_w}{2})\}\right]$ +
$\frac{1}{2}\mathbb{P}\{s|(v_d-\frac{v_w}{2}) < (V_1\_G\ (-V^{L}_{\bar{BB}})\ v_{B\bar{B}n}\ s)\}$.

Finally, rewriting the left hand side of the proof goal with the definition of the `non_ideal_ser` and the assumption $V^{L}_{\bar{BB}} = -V^{H}_{\bar{BB}}$, we conclude the proof. More detailed description of the proof can be found in [1].

The HOL code describing our formalization and the soft error rate analysis consists of approximately 1800 lines of code and took over 100 man-hours to complete. The results we presented are guaranteed to be accurate, unlike the simulation based analysis, and are generic due to the universally quantified variables. Such analysis was not possible in the HOL theorem prover earlier because of lack of formalization of pairs of continuous standard uniform and Gaussian random variables which is one of the contributions of this work.

4 Conclusion

In this paper, we presented a method for formal analysis of soft errors in electronic circuits using real and independent random variables. We presented the formalization of independent continuous random variable pairs with Uniform and Gaussian distributions. We described soft error rate analysis of a non-ideal sense amplifier circuit commonly used in DRAMs.

Our formalization of Gaussian random variable can be used to perform bit error rate analysis of communication receivers utilizing various modulation schemes such as ASK, PSK and QAM modulations in the presence of additive white Gaussian noise. We are currently working on formalization of lists of independent random variables to be able to tackle problems with more than two random variables in HOL.

References

[1] N. Abbasi, O. Hasan & S. Tahar (2011): *Formal Analysis of Soft Errors using Theorem Proving*. Technical Report, Department of Electrical & Computer Engineering, Concordia University, Canada. Available at `http://hvg.ece.concordia.ca/Publications/TECH_REP/SERTP_TR11`.

[2] H. Masuda et. al. (1980): *A 5 V-only 64K dynamic RAM based on high S/N design*. *IEEE Journal of Solid-State Circuits* SC-15(5), pp. 846 – 853, doi:`10.1109/JSSC.1980.1051481`.

[3] P. Audebaud & C. Paulin-Mohring (2009): *Proofs of Randomized Algorithms in Coq*. *Science of Computer Programming* 74(8), pp. 568–589, doi:`10.1016/j.scico.2007.09.002`.

[4] G. E. P. Box & Mervin E. Muller (1958): *A Note on the Generation of Random Normal Deviates*. *Annals of Mathematical Statistics* 29(2), pp. 610–611, doi:`10.1214/aoms/1177706645`. Available at `http://projecteuclid.org/euclid.aoms/1177706645`.

[5] M.J.C. Gordon (1989): *Mechanizing Programming Logics in Higher-0rder Logic*. In: *Current Trends in Hardware Verification and Automated Theorem Proving*, Springer, pp. 387–439, doi:`10.1007/978-1-4612-3658-0_10`.

[6] J. Harrison (2005): *A HOL Theory of Euclidean Space*. In: *Proceedings of the 18th international conference on Theorem Proving in Higher Order Logics*, *LNCS* 3603, Springer, pp. 114–129, doi:`10.1007/11541868_8`.

[7] O. Hasan (2008): *Formal Probabilistic Analysis using Theorem Proving*. PhD Thesis, Concordia University, Montreal, QC, Canada. Available at `http://spectrum.library.concordia.ca/975852/`.

[8] O. Hasan, N. Abbasi, B. Akbarpour, S. Tahar & R. Akbarpour (2009): *Formal Reasoning about Expectation Properties for Continuous Random Variables*. In: *Formal Methods*, *LNCS* 5850, Springer, pp. 435–450, doi:`10.1007/978-3-642-05089-3_28`.

[9] J. Hölzl & A. Heller (2011): *Three Chapters of Measure Theory in Isabelle/HOL*. In: *Interactive Theorem Proving*, *LNCS* 6898, Springer, pp. 135–151, doi:`10.1007/978-3-642-22863-6`.

[10] J. Hurd (2002): *Formal Verification of Probabilistic Algorithms*. PhD Thesis, University of Cambridge, Cambridge, UK. Available at `http://www.gilith.com/research/papers/thesis.pdf`.

[11] B. Keeth (2008): *DRAM Circuit Design: Fundamentals and High-Speed Topics*. IEEE.

[12] R. W. Keyes (1975): *Effect of Randomness in the Distribution of Impurity Ions on FET Thresholds in Integrated Electronics*. *IEEE Journal of Solid-State Circuits* SC-10(5), pp. 245 – 247, doi:`10.1109/JSSC.1975.1050600`.

[13] R. Khazanie (1976): *Basic Probability Theory and Applications*. Goodyear.

[14] P. A. Layman & S. G. Chamberlain (1989): *A Compact Thermal Model for Investigation of Soft Error Rates in MOS VLSI Digital Circutis*. *IEEE Journal of Solid-State Circuits* 24(1), pp. 79 – 89, doi:`10.1109/4.16305`.

[15] T. C. May & M. H. Woods (1979): *Alpha-particle-induced Soft Errors in Dynamic Memories*. *IEEE Transactions on Electron Devices* ED-26(1), pp. 2 – 9, doi:`10.1109/T-ED.1979.19370`.

[16] N. Metropolis & S. Ulam (1949): *The Monte Carlo Method*. *Journal of the American Statistical Association* 44(247), pp. 335–341, doi:`10.1080/01621459.1949.10483310`. Available at `http://www.jstor.org/stable/2280232`.

[17] T. Mhamdi, O. Hasan & S. Tahar (2010): *On the Formalization of the Lebesgue Integration Theory in HOL*. In: *Interactive Theorem Proving, LNCS* 6172, Springer, pp. 387–402, doi:`10.1007/978-3-642-14052-5_27`.

[18] T. Mhamdi, O. Hasan & S. Tahar (2011): *Formalization of Entropy Measures in HOL*. In: *Interactive Theorem Proving, LNCS* 6898, Springer, pp. 233–248, doi:`10.1007/978-3-642-22863-6_18`.

[19] H. Okazaki & Y. Shidama (2009): *Probability on Finite Set and Real-Valued Random Variables*. *Formalized Mathematics* 17(1-4), pp. 129–136, doi:`10.2478/v10037-009-0014-x`. Available at `http://versita.metapress.com/content/D3073K63W370G262`.