# Formal Analysis of Soft Errors using Theorem Proving

Naeem Abbasi, Osman Hasan, and Sofiène Tahar

Department of Electrical and Computer Engineering,
Concordia University, Montreal, Canada
{n_ab,o_hasan,tahar}@ece.concordia.ca

## Technical Report

April, 2011

**Abstract**

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 computer assisted 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 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 application, such as in avionics, electronic equipment operates in harsh environments and experiences extreme temperatures and excessive doses of solar and cosmic radiation. This can often result in changing 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 [15] and are usually caused by thermal noise or exposure to radiation. These nonrecurrent and non permanent errors can cause an electronic system to behave in an un predictable way. For example, such errors can cause electronic systems to crash in an unrepeatable way making the task of system debugging practically impossible.

There are four commonly known causes of soft errors in logic and memory circuits: 1) undesirable capacitive coupling of circuit elements [13], 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 [4]. In order to deal with the other two types of soft errors accurate analysis of the design is required [16, 15].

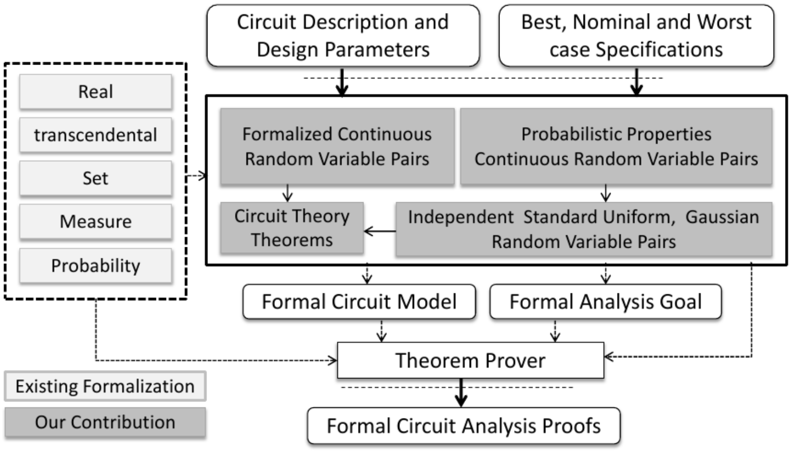
Soft error occurrence mechanism is random in nature and is usually analyzed using simulation based techniques such as Monte carlo simulation methods [17]. These techniques tend to be inaccurate and slow and are unsatisfactory for safety critical applications. In this paper, we apply the higher-order logic theorem proving method [5] to the problem of random effect modeling and analysis in electronic circuits. An equivalence or an implication relation involving the electronic circuit model and its specification is formed and is then proved using mathematical reasoning in the sound core of the HOL theorem prover. This method utilizes formalized real numbers, real and random variables and alleviates the limitations of the simulation based analysis technique.

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 [11]. Hasan, building on Hurds work, formalized continuous random variables with various distributions using inverse transform method [6] and verified their probabilistic and statistical properties [7]. However, 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 CDF properties, and the formalization of Gaussian random variable pair do not exist in open literature and is presented for the very first time in this report.

The rest of the report is organized as follows: Section 2 presents our proposed modeling and analysis method. Section 3 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 4. Finally, Section 5 concludes the report.

## 2 Proposed Methodology

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



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

Fig. 1: Proposed circuit analysis method

infrastructure includes formalization of a continuous random variable pair using an approach similar to [6]. We have formalized important notions of joint and marginal cumulative distribution functions and the independence of random variable pairs. 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 can be 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 sound core of the HOL theorem prover and formal circuit and system analysis proofs are constructed.

## 3 Formalization of Pairs of Random Variables

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 is given in Table III (row 1). 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 higher-order logic functions `seven` and `sodd` take a random boolean sequence `s` as input and return the even and odd segments of the infinite boolean sequence, respectively. 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`.

We also formalize important concepts of Joint and Marginal Cumulative Distribution Functions and the Independence of a pair of random variables. Our formalization of these concepts is based on [14].

### 3.1 Verification of CDF Properties of CRV Pairs

We have also verified the classical CDF properties of pairs of continuous random variables. In the following, we list the mathematical description as well as the HOL formalization.

### 3.2 Formal Specification of CDF of Pairs of Random Variables

**The Joint CDF Function**

Definition 2 describes the HOL formalization of the joint CDF of a pair of random variables mathematically expressed as: $(F_{X_1,X_2} = P(X_1 \leq x_1 \wedge X_2 \leq x_2))$.

**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.

**Marginal CDF Function**

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≤x1) and $F_{X2}(x2) = \lim_{x1 \to \infty} F_{X1,X2}(x1, x2)$ = P(X2≤x2).
The HOL formalization of the 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)})
```

The HOL functionlim P in Definition 3 represents the limit of a real sequence P.

### 3.3 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.

**CDF Bounds**

$0 \leq F_{X_1,X_2}(x_1, x_2) \leq 1$

For any pair of real numbers x1 and x2, this property immediately follows as the joint CDF function is defined as a probability.

**Theorem: 1** *CDF Bounded*

```
⊢ ∀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 is a Monotonic and Non-decreasing Function**

This property can be mathematically stated as:

$F_{X_1,X_2}(a, c) \leq F_{X_1,X_2}(b, d)$ for all a,b,c and d, such that $a \leq b$ and $c \leq d$

The assumption CDF_pair_in_events_bern X1 X2 x1 x2 states that the events of the form {s | X1 s ≤ x1 ∧ X2 s ≤ x2} are measurable.

**Theorem: 2** *The joint CDF of a pair is a Monotonic and Non-decreasing Function*

```
⊢ ∀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) )
```

This property formally states that the joint CDF function is a monotonic and non-decreasing function in each variable, respectively. The proof of Theorem 2 relies on the proofs of Lemmas 1 and 2. We first describe the proofs of these two Lemmas.

**Lemma: 1** *Joint CDF is Monotonic and Non-decreasing in first variable of the Pair*

```
⊢ ∀a b c. (a < b) ∧
     (∀x1 x2.  CDF_pair_in_events_bern X1 X2 x1 x2) ⇒
             (joint_cdf X1 X2 a c ≤ joint_cdf X1 X2 b c)
```

The proof of Lemma 1 is based on the fact that $\{ s \mid X1\ s \le b \wedge X2\ s \le d\} = \{ s \mid X1\ s \le b \wedge X2\ s \le c\} \cup \{ s \mid X1\ s \le b \wedge c < X2\ s \le d\}$ where the events on the right hand side are mutually exclusive. Then using the additive property of probability theory which states that for all sets A and B, that are disjoint, the probability of the union of events is equal to the sum of probabilities $(\forall A\ B.\ A \cap B = 0 \Rightarrow P(A \cup B) = P(A) + P(B))$, verified in [11], we show that:

$P\{ s \mid X1\ s \le b \wedge X2\ s \le d\} = P\{ s \mid X1\ s \le b \wedge X2\ s \le c\} + P\{ s \mid X1\ s \le b \wedge c < X2\ s \le d\}$
since $0 \le P\{ s \mid X1\ s \le b \wedge c < X2\ s \le d\} \le 1$ because it is a probability measure of a measurable event. It then follows from Theorem 1 that:

$P\{ s \mid X1\ s \le b \wedge c < X2\ s \le d\} \le P\{ s \mid X1\ s \le b \wedge X2\ s \le d\}$
which concludes the proof of Lemma 1.

**Lemma: 2** *Joint CDF is Monotonic and Non-decreasing in second variable of the Pair*

```
⊢ ∀a c d. (c < d) ∧
     (∀x1 x2.  CDF_pair_in_events_bern X1 X2 x1 x2) ⇒
             (joint_cdf X1 X2 a c ≤ joint_cdf X1 X2 a d)
```

The proof steps for Lemma 2 are very similar to the ones used for Lemma 1. Both of these lemmas lead to the formal verification of Theorem 2.

**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 $P(a < X1 \le b,\ c < X2 \le d) = F_{X1,X2}(b,d) - F_{X1,X2}(b,c) - F_{X1,X2}(a,d) + F_{X1,X2}(a,c)$. The property is formally stated in Theorem 3.

**Theorem: 3** *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 )
```

The proof of this property begins by first showing that the events $(a < X1 \le b \wedge c < X2 \le d)$ and $(X1 \le a \wedge c < X2 \le d)$ are disjoint. Then we show that $P(a < X1 \le b \wedge c < X2 \le d) + P(X1 \le a \wedge c < X2 \le d) = P(X1 \le b \wedge c < X2 \le d)$, using the additive law of probabilities, that is, $(\forall A\ B.\ A \cap B = 0 \Rightarrow P(A \cup B) = P(A) + P(B))$, which is verified in the HOL probability theory [11].

Similarly, we prove that, $P(X1 \le b \wedge c < X2 \le d) + P(X1 \le b \wedge X2 \le c) = P(X1 \le b \wedge X2 \le d)$ and $P(X1 \le a \wedge c < X2 \le d) + P(X1 \le a \wedge X2 \le c) = P(X1 \le a \wedge X2 \le d)$

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.

**CDF of a Pair at Positive Infinity**

This property for a pair of random variables can be mathematically expressed as: $\lim_{x2 \to \infty} \lim_{x1 \to \infty} F_{X1,X2}(\texttt{x1, x2}) = F_{X1,X2}(\infty,\ \infty) = 1$.

**Theorem: 4** *CDF of a Pair at Positive Infinity in all variables*

```
⊢  (∀ 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)
```

The CDF functions tends to 1 as all of its real arguments approach positive infinity. The proof of this property utilizes the fact that for an expanding sequence of events $A_n$, that is, (∀n. $An \subset A_{n+1}$) of S, $\lim_{n \to \infty} A_n = \bigcup_{n=1}^{\infty} A_n =$ S.

The proof also uses the continuity property of probabilities which states that $\forall A_n.\ \lim_{n \to \infty} P(A_n) = P(\bigcup_n^{\infty} A_n)$. In this case, the increasing sequence of events are represented in lambda calculus as `(λn.  {s | X1 s ≤ &n1 ∧ X2 s ≤ &n} )`

The countable union of all events in this sequence is given by `(λn.  {s | X1 s ≤ &n1 } ∩ { s | X2 s ≤ &n} )` = `(λn.  {s | X1 s ≤ &n1 } ∩ UNIV )` = `(λn.  {s | X1 s ≤ &n1 } )`

Instantiating the continuity property of probabilities, we show that the countable union of sequence of events (`(λn1.  {s | X1 s ≤ &n1 } )`) is equal to the universal set `UNIV`. Then using the basic probability law `P(UNIV) = 1`, which states that the probability of the universal set is 1, we conclude the proof.

**CDF Pair at Negative Infinity**

This property states that the value of the CDF function tends to `0` as any one of its two real arguments approaches minus infinity.

$$\lim_{x2 \to -\infty} F_{X1,X2}(x1, x2) = 0 = \lim_{x1 \to -\infty} F_{X1,X2}(x1, x2)$$

**Theorem: 5** *CDF pair at Negative Infinity in any variable*

```
⊢  (∀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) )
```

The proof goal is first broken in to two subgoals. Each of these subgoals state that as any one of the real arguments of the joint CDF function approaches $-\infty$, the joint CDF function approaches 0. The proof of this property utilized the continuity property of probabilities for contracting sequences of sets. The property states that, $\forall A_n.\ \lim_{n \to \infty} P(A_n) = P(\bigcap_n^{\infty} A_n)$

These sequence of events are expressed in lambda calculus as: `(λn.  {s | X1 s ≤ -&n1 ∧ X2 s ≤ x2 } )`, where `n` is a natural number. It is first shown that this contracting sequence of sets is equal to an empty set. Finally, using the basic probability law that the probability measure of an empty set is 0 (`P{} = 0`), we conclude the proof. The proof of the two subgoals is very similar. In Theorem 5, `lim` is the HOL function for limit of a real sequence.

**Joint CDF Continuous from Top Right**

CDF is continuous from the right in each of the variables. That is, for any fixed `x1`, say `a`, $F_{X1,X2}$(`x1, x2`) is continuous from right in `x2`, say `b`, $F_{X1,X2}$(`x1, x2`) is continuous from the right in `x1`. These properties can be mathematically expressed as:

$$\lim_{x1 \to a^+} F_{X1,X2}(\texttt{x1, b}) = F_{X1,X2}(\texttt{a, b})$$
$$\lim_{x2 \to b^+} F_{X1,X2}(\texttt{a, x2}) = F_{X1,X2}(\texttt{a, b})$$
$$\lim_{x1 \to a^+} \lim_{x2 \to b^+} F_{X1,X2}(\texttt{x1, x2}) = F_{X1,X2}(\texttt{a, b})$$

**Theorem: 6** *Joint CDF Continuous from Top Right*

```
⊢ ∀f1 f2 a b.
     (∀x.  CDF_pair_in_events_bern f1 f2 x1 x2) ∧
     ( ∀n2 a b.  {s | f1 s ≤ a + inv (& (SUC n2)) ∧
      f2 s ≤ b + inv (& (SUC n2))} IN events bern ) ⇒
      lim (λn2.
         lim (λn1.
         joint_cdf f1 f2 ((λn.  a + inv (&(SUC n))) n1)
                     ((λn.  b + inv (&(SUC n))) n2)) n2 ) =
                                        joint_cdf f1 f2 a b
```

The proof of Theorem 6 involves the use of continuity properties of probabilities, which states that: $\forall A_n. \lim_{n\to\infty} P(A_n) = P(\bigcap_n^\infty A_n)$, for a contracting sequence of events, the probability of countable intersections of such sets is equal to the limit of probability of the sequence of events as `n` tends to $\infty$.

We first show that the countable intersection of all the sets in the sequence ($\lambda$`n2.` { `s | X1 s` $\leq$ `a +` $\frac{1}{n1+1}$ $\wedge$ `X2 s` $\leq$ `b +` $\frac{1}{n2+1}$ }) is given by the set { `s | X1 s` $\leq$ `a +` $\frac{1}{n1+1}$ $\wedge$ `X2 s` $\leq$ `b` }

Similarly, we also show that the countable intersection of the sequence of sets ($\lambda$`n1.` { `s | X1 s` $\leq$ `a +` $\frac{1}{n1+1}$ $\wedge$ `X2 s` $\leq$ `b` }) is given by the set { `s | X1 s` $\leq$ `a` $\wedge$ `X2 s` $\leq$ `b` } using the continuity property of probabilities. Finally, by rewriting with the definition of the joint CDF of a pair of continuous random variables we conclude the proof.

**CDF Pair limit from Bottom Left**

This property states that the joint CDF function is continuous from bottom left and the limit from bottom left is given by:

$$\lim_{x2 \to a^-} F_{X1,X2}(\texttt{x1, x2}) = \texttt{P}\{\texttt{ s | X1 s } \leq \texttt{ x1 } \wedge \texttt{ X2 s < a}\}$$

**Theorem: 7** *CDF Pair limit from Left*

```
⊢ ∀f1 f2 x1 a.
    (∀x1 x2.  CDF_pair_in_events_bern f1 f2 x1 x2) ∧
    (∀n.{s | f1 s ≤ x1 ∧ f2 s ≤ a - inv (& (SUC n))} IN events bern)
    ⇒ lim (λn.  joint_cdf f1 f2 x1 ((λn.  a - inv (& (SUC n))) n))
                         = prob bern {s | f1 s ≤ x1 ∧ f2 s < a}
```

The proof of this theorem begins with the rewriting of the proof goal with the definitions of limit of a real sequence, and joint CDF function. The rest of the proof uses reasoning from HOL set, real, and probability theories. In particular, we use continuity property of probabilities for an expanding sequence of sets to complete the proof.

The next section describes the formalization of Standard Uniform random variable pairs with various distributions commonly used in engineering analysis.

### 3.4 Formalization of Standard Uniform Random Variable Pairs

We build on Hasan's work and first formalize a pair of standard continuous uniform random variable as a special case of a pair of standard discrete random variables.

**Definition 4:** *Standard Continuous Uniform Random Variable Pair*

```
⊢ ∀ s.  std_unif_pair_cont s =
      ( lim(λn. fst (std_unif_disc n (seven s))),
        lim(λn. fst (std_unif_disc n (sodd s))) )
```

In this definition, `seven` and `sodd` are two functions that take the boolean sequence `s` as input and return the even and the odd portions of the boolean sequence as output, respectively. We use the methodology described in [6] to formalize pairs of Uniform, Triangular, Exponential, Rayleigh and Weibull random variables in HOL using the Inverse Transform Method [6]. Table 1 describes the HOL formalizations of these random variables.

| **Distribution** | **Formalized Random Variable Pair** |
|---|---|
| Standard<br>Uniform<br>(0,1) | $\vdash \forall\texttt{s. std\_unif\_pair\_cont s} =$<br>$(\lim_{n\to\infty}(\lambda\texttt{n. fst (std\_unif\_disc n (seven s))}),$<br>$\lim_{n\to\infty}(\lambda\texttt{n. fst (std\_unif\_disc n (sodd s))}))$<br>$\texttt{X1\_STD\_UNIF s = fst (std\_unif\_pair\_cont s)}$<br>$\texttt{X2\_STD\_UNIF s = snd (std\_unif\_pair\_cont s)}$ |
| Uniform<br>(a1,b1) (a2,b2) | $\vdash \forall\texttt{a1 b1 a2 b2 s. unif\_pair\_rv\_cont a1 b1 a2 b2 s =}$<br>$\texttt{(((b1 - a1)(X1\_STD\_UNIF s) + a1),}$<br>$\texttt{((b2 - a2)(X2\_STD\_UNIF s) + a2))}$ |
| Triangle<br>(0,a1) (0,a2) | $\vdash \forall\texttt{m s. triangle\_pair\_rv a1 a2 s} =$<br>$(\texttt{a1}(1-\sqrt{\texttt{(1 - X1\_STD\_UNIF s)}})),$<br>$(\texttt{a2}(1-\sqrt{\texttt{(1 - X2\_STD\_UNIF s)}}))$ |
| Exponential<br>(m1, m2) | $\vdash \forall\texttt{s m1 m2. exp\_pair\_rv m1 m2 s} =$<br>$(-\frac{1}{\texttt{m1}}\ln\texttt{(1 - X1\_STD\_UNIF s)},$<br>$-\frac{1}{\texttt{m2}}\ln\texttt{(1 - X2\_STD\_UNIF s)})$ |
| Rayleigh<br>(d1, d2) | $\vdash \forall\texttt{s d1 d2. rayleigh\_pair\_rv d1 d2 s} =$<br>$((\texttt{d1}\sqrt{\texttt{-2 ln (1 - X1\_STD\_UNIF s)}}),$<br>$(\texttt{d2}\sqrt{\texttt{-2 ln (1 - X2\_STD\_UNIF s)}}))$ |
| Weibull<br>(a1,b1) (a2,b2) | $\vdash \forall\texttt{s a1 b1 a2 b2. weibull\_pair\_rv a1 b1 a2 b2 s} =$<br>$(\frac{1}{\texttt{b1}}(\texttt{-(ln (1 - X1\_STD\_UNIF s)}^{\frac{1}{\texttt{a1}}})),$<br>$\frac{1}{\texttt{b2}}(\texttt{-(ln (1 - X2\_STD\_UNIF s)}^{\frac{1}{\texttt{a2}}})))$ |

Table 1: Continuous random variable pairs in HOL

These random variables in the pairs in Table 1 have the same distribution function and different distribution parameters. The distribution parameters for the two random variables in the pair can be the same. Such a pair of random variables would be called identically distributed pair of random variables.

### 3.5 Formalization of Gaussian Random Variable Pairs

According to the Box-Muller method [2], 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 Definition 5.

**Definition 5:** *Gaussian Random Variable Pair*

```
⊢ ∀ s. std_g_pair_rv s =
       ((√(-2 ln (X1_S_UNIF s)) cos(2π(X2_S_UNIF s))),
        (√(-2 ln (X1_S_UNIF s)) sin(2π(X2_S_UNIF s))))
⊢ ∀ 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))
⊢ ∀ s.  X1_GAUSS μ σ s = fst (g_pair_rv μ σ s)
⊢ ∀ s.  X2_GAUSS μ σ s = snd (g_pair_rv μ σ s)
```

### 3.6 Independent Random Variables

In many engineering applications independent random behaviour needs to be modeled. The formalization of the notion of independence of random variables is described in this section. We also describe some useful results related to identically distributed random variables.

#### 3.6.1 Independent CRV Pairs

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 ≤ x1} and {X2 ≤ x2} are independent. Mathematically the notion of independence is defined as:
P{X1 ≤ x1 ∧ X2 ≤ x2} = P{X1 ≤ x1}.P{X2 ≤ x2}

The HOL formalization is given in Definition 6.

**Definition 6:** *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})
```

#### 3.6.2 Identically Distributed Random Variables

Pairs of random variables with same or different distributions and parameter values are needed in reliability analysis. Our formalization of pair of continuous random variables allows the flexibility of having two independent random variables with same or different distribution functions. In the case when random variables have same distribution type, it is possible to have same or different parameters.

In this section, we describe the verification of joint CDF property of commonly used continuous random variable pairs. We first verify the joint CDF properties of two continuous random variables with same distribution function but different parameters. Theorems 8 through 12 state the verified joint CDF properties of uniform, triangular, exponential, rayleigh, and weibull random variables.

In Theorem 8, the first assumption states that the shape and the scale parameters of the two weibull random variables are positive and greater than zero. The second assumption states that the two random variables are independent. The goal of the theorem states that the distribution function of two independent continuous random variables with same distribution function but different parameters is given by the product of their individual distribution function for positive values of the random variable and is zero for values of x less than or equal to 0.

**Theorem 8:** *Joint CDF of Two Independent Weilbull Random Variables*

```
⊢ ∀a b c d x y.  (0 < a) ∧ (0 < b) ∧ (0 < c) ∧ (0 < d) ∧
 (∀a b c d x y.
   independent_rv_pair (λs.  weibull_rv a b (s_even s))
                     (λs.  weibull_rv c d (s_odd s)) x y) ⇒
  (prob bern {s | weibull_rv a b (s_even s) ≤ x ∧
                  weibull_rv c d (s_odd s) ≤ y } =
  (if (x ≤ 0 ∨ y ≤ 0) then 0 else
      (1 - exp -((b * x) powr a)) * (1 - exp -((d * y) powr c))))
```

Similarly, In Theorems 9, 10, 11, and 12 we verify similar relations for independent exponential, uniform, triangle and rayleigh random variable pairs.

**Theorem 9:** *Joint CDF of Two Independent Exponential Random Variables*

```
⊢ ∀m1 m2 x y.  (0 < m1) ∧ (0 < m2) ∧
(∀m1 m2 x y.
        independent_rv_pair (λs.  exp_rv m1 (s_even s))
                          (λs.  exp_rv m2 (s_odd s)) x y) ⇒
  (prob bern {s | exp_rv m1 (s_even s) ≤ x ∧
                  exp_rv m2 (s_odd s) ≤ y } =
  (if (x ≤ 0 ∨ y ≤ 0) then 0 else
                     (1 - exp (-m1 * x)) * (1 - exp (-m2 * y))))
```

**Theorem 10:** *Joint CDF of Two Independent Uniform Random Variables*

```
⊢ ∀a b c d x y.  a < b ∧ a < b ∧
  (∀a b c d x y.
   independent_rv_pair (λs.  uniform_rv a b (s_even s))
                      (λs.  uniform_rv c d (s_odd s)) x y) ⇒
  (prob bern {s | uniform_rv a b (s_even s) ≤ x ∧
                  uniform_rv c d (s_odd s) ≤ y } =
  (if (x ∧ a ∨ y ∧ c) then 0 else
   (if (a < x ∧ x < b ∧ c < y ∧ y < d) then
      (x - a) / (b - a) * ((y - c) / (d - c)) else
    (if (a < x ∧ x < b ∧ d ≤ y) then (x - a) / (b - a) else
     (if (b ≤ x ∧ c < y ∧ y < d) then (y - c) / (d - c) else 1)))))
```

**Theorem 11:** *Joint CDF of Two Independent Triangular Random Variables*

```
⊢ ∀m1 m2 x y.  0 < m1 ∧ 0 < m2 ∧
(∀m1 m2 x y.
   independent_rv_pair (λs.  triangular_rv m1 (s_even s))
                      (λs.  triangular_rv m2 (s_odd s)) x y) ⇒
   (prob bern {s | triangular_rv m1 (s_even s) ≤ x ∧
                   triangular_rv m2 (s_odd s) ≤ y } =
   (if (x ≤ 0 ∨ y ≤ 0) then 0 else
    (if (0 < x ∧ x < m1 ∧ 0 < y ∧ y < m2) then
         2 / m1 * (x - x pow 2 / (2 * m1)) *
        (2 / m2 * (y - y pow 2 / (2 * m2)))
     else
      (if (0 < x ∧ x < m1 ∧ m2 ≤ y) then
          2 / m1 * (x - x pow 2 / (2 * m1)) else
       (if (m1 ≤ x ∧ 0 < y ∧ y < m2) then
          2 / m2 * (y - y pow 2 / (2 * m2)) else 1)))))
```

**Theorem 12:** *Joint CDF of Two Independent Rayleigh Random Variables*

```
⊢ ∀m1 m2 x y.  (0 < m1) ∧ (0 < m2) ∧
(∀m1 m2 x y.
        independent_rv_pair (λs.  rayleigh_rv m1 (s_even s))
                   (λs.  rayleigh_rv m2 (s_odd s)) x y) ⇒
(prob bern {s | rayleigh_rv m1 (s_even s) ≤ x ∧
               rayleigh_rv m2 (s_odd s) ≤ y } =
(if x ≤ 0 ∨ y ≤ 0 then 0 else
   (1 - exp (-(x pow 2) / (2 * m1 pow 2))) *
   (1 - exp (-(y pow 2) / (2 * m2 pow 2)))))
```

The proof of these theorems utilizes the definition of independence of pairs of random variables and the CDF relations for the respective random variables.

If the distribution function parameters of the two random variables in Theorem 8 through Theorem 12 were equal respectively, then such random variable pairs would be called independent and identically distributed random variable pairs. Similarly, it is possible to verify the properties of random variables that are independent but have different distributions.

In this section, standard properties of cumulative distribution function of random variable pairs were verified. These properties are useful in formal modeling and analysis of reliability of engineering systems and verification of their safety critical properties.

## 4 Formal Analysis of Soft Errors in DRAMs

Many safety critical application such as in avionics applications the electronic equipment operates in harsh environments such as in upper atmosphere or space under extreme temperatures and solar and cosmic radiation. The radiation dose depends on the effective area of crossection of the electronic device and the angle of incidence of the particle radiation.

A soft error is an abnormal change in the state of a storage node in an electronic circuit due to thermal noise or exposure to radiation. These nonrecurrent and non permanent errors can cause an electronic system to behave in an un predictable ways and even crash in a nonreconstructable way making the task of system debugging practically impossible.

There are four known causes of soft errors in logic and memory circuits: 1) undesirable capacitive coupling of circuit elements [13, 9], 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 [10, 4]. In order to deal with the other two types of soft errors accurate analysis of the design is required [16, 3, 15].

Soft error occurrence mechanism is random in nature and is usually analyzed using simulation based techniques. These techniques tend to be inaccurate and slow and are unsatisfactory for safety critical applications. Analysis of soft error causing mechanisms and their effects on the electronic devices is usually done using statistical simulation techniques such as Monte carlo simulation methods [17],[25, 23, 26, 19], [20, 21, 22]. [22] [1]. In this paper we for the very first time apply formal methods to the modeling and analysis problem in a theorem prover. In this paper, we propose a theorem proving based modeling and analysis approach.

### 4.1 Dynamic Random Access Memory

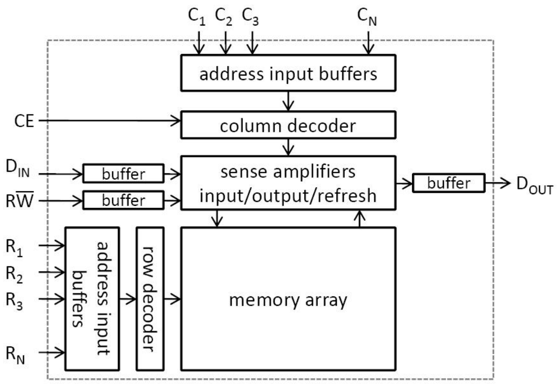


Fig. 2: Dynamic Random Access Memory

Figure 2 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. A memory array consists of densely packed cells capable of storing a small amount of charge for a finite period of time. The stored charge is gradually lost due to leakage and is usually replenished using a memory refresh operation. Individual memory cells are accessed using uniquely decoded row and column select lines. Sensitive amplifier circuits are used to read the contents of the memory. The memory read operation consist of four main steps: 1) precharging the two bit lines, 2) enabling the word select line as the bit lines float, 3) enabling of the sense amplifier, and finally, 4) writing the data back to the memory cell. During the memory write operation the bit line is driven to either high or low, and as the the word line is enabled, data is written to the memory cell. A memory refresh operation consists of a read operation followed by a memory write operation.

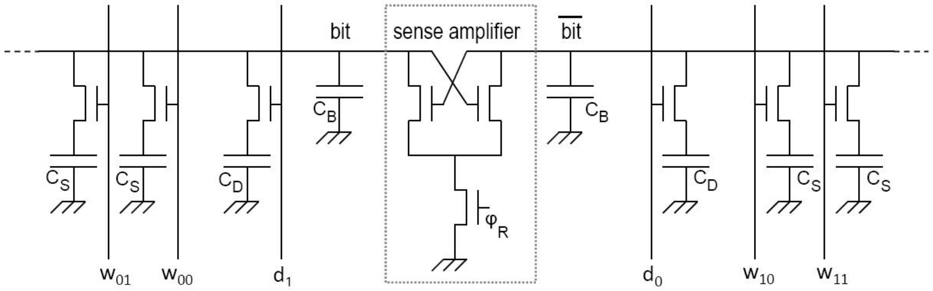


Fig. 3: Simple balanced bit line architecture

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 3, lines bit,$\overline{\text{bit}}$). The third input is used to enable the sense amplifier (Figure 3, $\phi_{\text{R}}$). The amplifier increases the amplitude of the difference signal between the two bit lines. This allows DRAMs to sense data in the memory cells even with a very small signal swing. This results in the improvement of speed and power consumption. This improvement however comes at the cost of reduced noise immunity. Internal and external source of noise can affect the operation of the sense amplifier. One such source of noise is called the Thermal noise. Thermal noise in electronic system components is an unwanted and unpredictably varying signal. It is caused by the random motion of charge particles (electrons and holes) and depends on the operating temperature. Thermal noise is modeled using a Gaussian distribution. A gaussian distribution can be completely specified using its mean and standard deviation parameters.

Various memory array and sense amplifier arrangements are possible and have been studied for their performance. These arrangements are some times also referred to as DRAM architectures. Figure 3 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 pre-charge, refresh and the input output devices of the DRAM are not shown in this simplified circuit diagram. The loading effects of the these devices are included in $C_B$. More details can be found elsewhere [12].

### 4.2 Thermal Noise and Parameter Variation Modeling

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 $V_1$(-$V^L_{B\overline{B}}$,$v_{B\overline{B}n}$) and $V_2$($V^H_{B\overline{B}}$,$v_{B\overline{B}n}$), where $v_{B\overline{B}n}$ represents the standard deviation of the thermal noise [15].

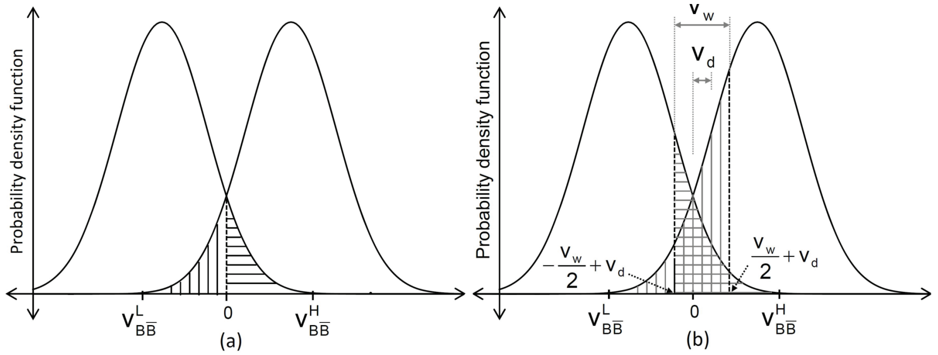


Fig. 4: Probability density functions for ideal and non-ideal error analysis [15]

Figure 4(b) 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, $P(-\frac{v_w}{2} + v_d < V_1) = Q\left(\frac{-\frac{v_w}{2}+v_d-(-V^L_{B\bar{B}})}{\sqrt{v^2_{BB}}}\right)$, and $P(V_2 \leq \frac{v_w}{2} + v_d) = 1 - Q\left(\frac{\frac{v_w}{2}+v_d-V^H_{B\bar{B}}}{\sqrt{v^2_{BB}}}\right)$, 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 $0 \leq \chi, \delta \leq 1$ [15]. Using these assumptions and that both 0 and 1 errors are equally likely to occur, the soft error rate is given by: $P_{error} = \frac{1}{4}\text{erfc}\left[\frac{V^L_{B\bar{B}}}{\sqrt{2}\sqrt{\bar{v}^2_{B\bar{B}}}}\left(1-\frac{\delta}{2}+\chi\right)\right] + \frac{1}{4}\text{erfc}\left[\frac{V^H_{B\bar{B}}}{\sqrt{2}\sqrt{\bar{v}^2_{B\bar{B}}}}\left(1-\frac{\delta}{2}-\chi\right)\right]$. Next, we formally verify this result using our foundational formalization of Section 3.

### 4.3 Verification of Soft Error Rates

Based on the proposed methodology of Section 2, the first step is to formally represent the Non-ideal sense amplifier soft error rate model, which can be done as follows:

**Definition 7:** *Non-ideal Sense Amplifier SER Model*
$\vdash \forall\ V^L_{BB}\ V^H_{BB}\ v_{BBn}\ v_w\ v_d.$
`non_ideal_ser` $V^L_{BB}\ V^H_{BB}\ v_{BBn}\ v_w\ v_d$ =
$\frac{1}{2}(\mathbb{P}\{s|(v_d - \frac{v_w}{2}) < (V_1\ \ (-V^L_{BB})\ \ v_{BBn}\ \ s)\}$ +
$\mathbb{P}\{s|(V_2\ \ V^H_{BB}\ \ v_{BBn}\ \ s) \leq (v_d + \frac{v_w}{2})\})$

In Theorem 13, we formally verify the soft error rate expression for a non-ideal sense amplifier in the presence of thermal noise and parameter variations. The predicate `((f diffl (`$\lambda$`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 ($\lambda$t. $\frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}$). 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 ($\lambda$t. $\frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}$). 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`). Assumptions 5 and 6 explicitly state that the probabilities of the random variables $V_1$ and $V_2$ 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 $\delta$ and $\chi$ which relate the insensitivity width ($v_w = \delta V^H_{BB}$) and the sensitivity deviation ($v_d = \chi\ V^H_{BB}$) parameters to the mean values of the gaussian random variables $V_1$ and $V_2$, 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 ($0 < v_{BB_n}$ ). The fourteenth assumption ($V^L_{BB} = -V^H_{BB}$) states that the sense amplifier at its inputs sees two equal and opposite polarity dc signals represented by $V^H_{BB}$ and $V^L_{BB}$, respectively. The fifteenth assumption states an important property of the Q function that the total area under the Q function is equal to 1.

**Theorem 13:** *Non-ideal Sense Amplifier Soft Error Rate*
$\vdash \forall$ `a b f` $V^H_{BB}\ V^L_{BB}\ v_{BBn}\ \delta\ \chi.$
`((a`$\leq$`b)` $\wedge$ `(`$\forall$`x. (a`$\leq$`x)` $\wedge$ `(x`$\leq$`b)` $\Rightarrow$ `(f diffl (`$\lambda$`t.` $\frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}$`) x) x)` $\wedge$ `(Q1 a b = f b - f a)` $\wedge$ `(Q y =` $\lim_{n\to\infty}$ `(`$\lambda$`n. Q1 y (&n)))` $\wedge$ `(`$\forall$`x. Q x =` $\frac{1}{2}$ `erfc (`$\frac{x}{\sqrt{2}}$`))` $\wedge$ `(`$\forall$`z` $\mu\ \sigma$`. (0 <` $\sigma$`)` $\Rightarrow$ `(`$\mathbb{P}$`{s | z <` $V_1\ \mu\ \sigma$ `s} = Q (`$\frac{z-\mu}{\sigma}$`))` $\wedge$ `(`$\forall$`z` $\mu\ \sigma$`. (0 <` $\sigma$`)` $\Rightarrow$ `(`$\mathbb{P}$`{s | z <` $V_2\ \mu\ \sigma$ `s} = Q (`$\frac{z-\mu}{\sigma}$`))` $\wedge$ `(0`$\leq\delta$`)` $\wedge$ `(`$\delta\leq$`1)` $\wedge$ `(0`$\leq\chi$`)` $\wedge$ `(`$\chi\leq$`1)` $\wedge$ `(`$v_w$ `=` $\delta V^H_{BB}$`)` $\wedge$ `(`$v_d$ `=` $\chi\ V^H_{BB}$`)` $\wedge$ `(0 <` $v_{BBn}$`)` $\wedge$ `(`$V^L_{BB} = -V^H_{BB}$`)` $\wedge$ `(Q(y) + Q(-y) = 1)`

$\Rightarrow$ `non_ideal_ser` $V_{BB}^{L}\ V_{BB}^{H}\ v_{BBn}$ = $\frac{1}{4}\texttt{erfc}\left(\frac{V_{BB}^{H}}{\sqrt{2}\ \ v_{BBn}}\left[1-\frac{\delta}{2}+\chi\right]\right)$ + $\frac{1}{4}\texttt{erfc}\left(\frac{V_{BB}^{L}}{\sqrt{2}\ \ v_{BBn}}\left[1-\frac{\delta}{2}-\chi\right]\right)$

**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, $v_w = \delta V_{BB}^{H}$, $v_d = \chi\ V_{BB}^{H}$ and $V_{BB}^{L} = -V_{BB}^{H}$. This reduces the righthand side of the proof goal to: $\frac{1}{2}\left[1-\mathbb{P}\{s|(v_d+\frac{v_w}{2})\ \ <\ \ (V_2\ V_{BB}^{H}\ v_{BBn}\ s)\}\right]$ + $\frac{1}{2}\mathbb{P}\{s|(v_d-\frac{v_w}{2}) < (V_1\ (V_{BB}^{H})\ v_{BBn}\ s)\}$. 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:$\frac{1}{2}\left[\mathbb{P}\{s|(V_2\ V_{BB}^{H}\ v_{BBn}\ s)\ \ \leq\ \ (v_d+\frac{v_w}{2})\}\right]$ + $\frac{1}{2}\mathbb{P}\{s|(v_d-\frac{v_w}{2}) < (V_1\ (-V_{BB}^{L})\ v_{BBn}\ s)\}$. Finally, rewriting the left hand side of the proof goal with the definition of the `non_ideal_ser` and the assumption $V_{BB}^{L} = -V_{BB}^{H}$, we conclude the proof.

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.

## 5 Conclusion

In this report, 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 performs 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.

The formalization described in this report can be used to formalize a gaussian random variable pair using two independent and identically distributed standard continuous random variables and the box-muller method. Such formalization would allow reasoning about problems involving the use of gaussian random variable.

## References

[1] N. Battezzati, L. Sterpone, and M. Violante. Monte carlo analysis of the effects of soft errors accumulation in sram-based fpgas. *Nuclear Science, IEEE Transactions on*, 55(6):3381 –3387, 2008.

[2] G. E. P. Box and Mervin E. Muller. A note on the generation of random normal deviates. *Ann. Math. Statist.*, 29(2):610–611, 1958.

[3] D. L. Wendell D. L. Segers and D. J. Koesters. Circuit design methodologies. *IEDM Technical Digest*, 1983.

[4] H. Masuda et. al. A 5 v-only 64k dynamic ram based on high s/n design. *, IEEE Journal of Solid-State Circuits*, SC-15(5):846 – 853, October 1980.

[5] M.J.C. Gordon. Mechanizing Programming Logics in Higher-0rder Logic. In *Current Trends in Hardware Verification and Automated Theorem Proving*, pages 387–439. Springer, 1989.

[6] O. Hasan. *Formal Probabilistic Analysis using Theorem Proving*. PhD Thesis, Concordia University, Montreal, QC, Canada, 2008.

[7] O. Hasan, N. Abbasi, B. Akbarpour, S. Tahar, and R. Akbarpour. Formal Reasoning about Expectation Properties for Continuous Random Variables. In *Formal Methods*, volume 5850 of *LNCS*, pages 435–450, 2009.

[8] L. G. Heller. Cross-coupled charge-transfer sense amplifier. In *IEEE International Solid-State Circuits Conference, Digest of Technical Papers*, 1979.

[9] B. Hoeneisen and C. A. Mead. Fundamental limitations in microelectronics-i. mos technology. *Solid-State Electron.*, 1972.

[10] Y. Itoh. K. Nakagawa. K. Sakui. F. Horiguchi and M. Ogura. Noise-generation analysis and noise-suppression design techniques in megabit drams. *, IEEE Journal of Solid-State Circuits*, SC-22(4):619 – 622, August 1987.

[11] J. Hurd. *Formal Verification of Probabilistic Algorithms*. PhD Thesis, University of Cambridge, Cambridge, UK, 2002.

[12] B. Keeth. *DRAM Circuit Design: Fundamentals and High-Speed Topics*. IEEE, 2008.

[13] R. W. Keyes. Effect of randomness in the distribution of impurity ions on fet thresholds in integrated electronics. *, IEEE Journal of Solid-State Circuits*, SC-10, August 1975.

[14] R. Khazanie. *Basic Probability Theory and Applications*. Goodyear, 1976.

[15] P. A. Layman and S. G. Chamberlain. A compact thermal model for investigation of soft error rates in mos vlsi digital circutis. *IEEE Journal of Solid-State Circuits*, 24(1):79 – 89, February 1989.

[16] T. C. May and M. H. Woods. Alpha-particle-induced soft errors in dynamic memories. *IEEE Transactions on Electron Devices*, ED-26(1):2 – 9, January 1979.

[17] Nicholas Metropolis and S. Ulam. The monte carlo method. *Journal of the American Statistical Association*, 44(247):pp. 335–341, 1949.

[18] K. Natori. Effect of randomness in the distribution of impurity ions on fet thresholds in integrated electronics. *IEEE Transactions on Electron Devices*, ED-33(4):482–488, April 1986.

[19] R. Rajaraman, J.S. Kim, N. Vijaykrishnan, Y. Xie, and M.J. Irwin. Seat-la: a soft error analysis tool for combinational logic. In *VLSI Design, 2006. Held jointly with 5th International Conference on Embedded Systems and Design., 19th International Conference on*, page 4 pp., 2006.

[20] P. Ramachandran, P. Kudva, J. Kellington, J. Schumann, and P. Sanda. Statistical fault injection. In *Dependable Systems and Networks With FTCS and DCC, 2008. DSN 2008. IEEE International Conference on*, pages 122 –127, 2008.

[21] K. Ramakrishnan, R. Rajaramant, N. Vijaykrishnan, Y. Xie, M.J. Irwin, and K. Unlu. Hierarchical soft error estimation tool (hseet). In *Quality Electronic Design, 2008. ISQED 2008. 9th International Symposium on*, pages 680 –683, 2008.

[22] Amith Singhee and Rob A. Rutenbar. Statistical blockade: A novel method for very fast monte carlo simulation of rare circuit events, and its application. In Rudy Lauwereins and Jan Madsen, editors, *Design, Automation, and Test in Europe*, pages 235–251. Springer Netherlands.

[23] G. R. Srinivasan. Modeling the cosmic-ray-induced soft-error rate in integrated circuits: An overview. *IBM Journal of Research and Development*, 40(1):77 –89, 1996.

[24] Y. Ohmori T. Yano. N. Ieda and K. Takeya. Highly sensitive sense circuit for single transistor mos ram. *Review of the Electrical Communication Laboratory*, 27(1-2):10–17, 1979.

[25] Y. Tosaka, H. Kanata, T. Itakura, and S. Satoh. Simulation technologies for cosmic ray neutron-induced soft errors: Models and simulation systems. *Nuclear Science, IEEE Transactions on*, 46(3):774 –780, June 1999.

[26] K. M. Warren, B. D. Sierawski, R. A. Weller, R. A. Reed, M. H. Mendenhall, J. A. Pellish, R. D. Schrimpf, L. W. Massengill, M. E. Porter, and J. D. Wilkinson. Predicting thermal neutron-induced soft errors in static memories using tcad and physics-based monte carlo simulation tools. *Electron Device Letters, IEEE*, 28(2):180 –182, 2007.

# 6 Appendix

## 6.1 Thermal noise and parameter variation modeling

We model the voltages on the two bit lines connected to the inputs of an ideal sense amplifier as two independent gaussian random variables $V_1$(-$V^L_{B\overline{B}}$,$v_{B\overline{B}n}$) and $V_2$($V^H_{B\overline{B}}$,$v_{B\overline{B}n}$). Where $v_{B\overline{B}n}$ represents the standard deviation of the thermal noise [15].

Figure 4(a) 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 PDF ($f_X(x)$) and the CDF ($F_X(x)$) of gaussian random variables are defined as:

$$f_X(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} \tag{1}$$

$$F_X(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt \tag{2}$$

The complementary error function (erfc(x)) and the Q function (Q(x)), appear very frequently in the error rate analysis literature and, are defined as:

$$Q(x) = \frac{1}{2}\text{erfc}\left(\frac{x}{\sqrt{2}}\right) = \int e^{-\frac{t^2}{2}} dt \tag{3}$$

$$\text{erfc}(x) = 2Q\left(\sqrt{2}x\right) \tag{4}$$

The probability 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 Equations 5 and 6,respectively.

$$P(0 < V_1) = Q\left(\frac{0 - (-V^L_{B\bar{B}})}{\sqrt{v^2_{BB}}}\right) \tag{5}$$

$$P(V_2 \leq 0) = 1 - Q\left(\frac{0 - V^H_{B\bar{B}}}{\sqrt{v^2_{BB}}}\right) \tag{6}$$

It can be shown that the probability of error for an ideal sense amplifier is given Equation 7.

$$P_{error} = \frac{P(0 < V_1) + P(V_2 \leq 0)}{2} = \frac{1}{4}\text{erfc}\left(\frac{V^L_{B\bar{B}}}{\sqrt{2}\sqrt{\bar{v}^2_{B\bar{B}}}}\right) + \frac{1}{4}\text{erfc}\left(\frac{V^H_{B\bar{B}}}{\sqrt{2}\sqrt{\bar{v}^2_{B\bar{B}}}}\right) \tag{7}$$

The behavior of a practical sense amplifier often deviates from the ideal behavior due to parameter variations. The analysis in [18], [24], and [8] focuses on finite sense time and parameter variations in practical circuits. In [18], Natori characterized the sensitivity of the sense amplifier using two parameters $v_w$ and $v_d$. $v_w$ is the insensitivity width which is the difference between the minimum sensible high and low levels. Its value depends on the operation of the sense amplifier. $v_d$ is the sensitivity center deviation which is related to the asymmetry of the flip-flop and bit-lines. Layman in [15] assumes that both insensitivity width and the sensitivity center deviation are given by $v_w = \delta V_{B\bar{B}}$ and $v_d = \chi V_{B\bar{B}}$, and $0 \leq \chi, \delta \leq 1$. He takes the effects of non-ideal behavior into account by adjusting the "0" and "1" decision thresholds in the analysis from "0" and "0" to $-\frac{v_w}{2} + v_d$ and $\frac{v_w}{2} + v_d$, respectively, as shown in Figure 4(b).

Based on these assumptions the soft error rate can be determined as before and is given by Equation 8.

$$P_{error} = \frac{1}{4}\text{erfc}\left[\frac{V^L_{B\bar{B}}}{\sqrt{2}\sqrt{\bar{v}^2_{B\bar{B}}}}\left(1 - \frac{\delta}{2} + \chi\right)\right] + \frac{1}{4}\text{erfc}\left[\frac{V^H_{B\bar{B}}}{\sqrt{2}\sqrt{\bar{v}^2_{B\bar{B}}}}\left(1 - \frac{\delta}{2} - \chi\right)\right] \tag{8}$$

Our formal analysis in the following section verifies these DRAM soft error rate expressions in HOL theorem prover.

### 6.2 Verification of soft error rates

We model the ideal sense amplifier soft error rate according to Equation 7, assuming that both 0 and 1 errors are equally likely.

**Definition A1:** *Ideal Sense Amplifier Soft Error Rate Model*
$\vdash \forall\ V^L_{BB}\ V^H_{BB}\ v_{BBn}.$
$\quad$ `ideal_soft_error_rate` $V^L_{BB}\ V^H_{BB}\ v_{BBn}$ =
$\qquad \frac{1}{2}(\mathbb{P}\{s | 0 < (V_1\ (-V^L_{BB})\ v_{BBn}\ s)\}$ +
$\qquad\qquad \mathbb{P}\{s | (V_2\ V^H_{BB}\ v_{BBn}\ s) \leq 0\})$

In Definition A1, the two bit line voltages are modeled using two independent gaussian random variables $V_1$ and $V_2$. $V^L_{BB}$ and $V^H_{BB}$ are the means of the two gaussian random variables. Both random variables are assumed to have the same standard deviation $v_{BBn}$.

**Definition A2:** *Non-ideal Sense Amplifier Soft Error Rate Model*
$\vdash \forall\ V^L_{BB}\ V^H_{BB}\ v_{BBn}\ v_w\ v_d.$
$\quad$ `non_ideal_soft_error_rate` $V^L_{BB}\ V^H_{BB}\ v_{BBn}\ v_w\ v_d$ =
$\qquad \frac{1}{2}(\mathbb{P}\{s | (v_d - \frac{v_w}{2}) < (V_1\ (-V^L_{BB})\ v_{BBn}\ s)\}$ +
$\qquad\qquad \mathbb{P}\{s | (V_2\ V^H_{BB}\ v_{BBn}\ s) \leq (v_d + \frac{v_w}{2})\})$

In Definition A2, we model the soft error rate behavior of a practical sense amplifier in the presence of parameter variations. $v_d$ and $v_w$ are the sensitivity center deviation and the insensitivity widths, respectively.

Theorem A1 formally states that the ideal sense amplifier soft error rate due to thermal noise is given by Equation 7. The theorem has six assumptions. The predicate `((f diffl` (`λt.` $\frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}$`) x) x)` in the first assumption states that `f` is the differential of the function `f` with respect to `x` is the function ($\lambda$t. $\frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}$). 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 ($\lambda$t. $\frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}$). The third assumption then formally represents the `Q` function as the case when the second argument of `Q1` tends to infinity. The fourth assumption describes the relationship between the Q function and the error function (erfc). The fifth assumption states an important property of the Q function that the total area under the Q function is equal to 1. The sixth assumption makes sure that the standard deviation of the thermal noise is a non zero positive value. Assumptions 7 and 8 explicitly state that the probabilities of the random variables $V_1$ and $V_2$ taking values greater than an arbitrary real number z is given by Q $(\frac{z-\mu}{\sigma})$.

**Theorem A1:** *Ideal Sense Amplifier Soft Error Rate*

$\vdash \forall$ a b f $V_{BB}^H$ $V_{BB}^L$ $v_{BBn}$.
((a$\leq$b) $\wedge$ ($\forall$x. (a$\leq$x) $\wedge$ (x$\leq$b) $\Rightarrow$ (f diffl ($\lambda$t. $\frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}$) x) x) $\wedge$ (Q1 a b = f b - f a) $\wedge$
(Q y = $\lim\limits_{n\to\infty}$ ($\lambda$n. Q1 y (&n))) $\wedge$ ($\forall$x. Q x = $\frac{1}{2}$ erfc $(\frac{x}{\sqrt{2}})$) $\wedge$
(Q(y) + Q(-y) = 1) $\wedge$ (0 < $v_{BBn}$) $\wedge$
($\forall$z $\mu$ $\sigma$. (0 < $\sigma$) $\Rightarrow$ ($\mathbb{P}${s | z < $V_1$ $\mu$ $\sigma$ s} = Q $(\frac{z-\mu}{\sigma})$)
($\forall$z $\mu$ $\sigma$. (0 < $\sigma$) $\Rightarrow$ ($\mathbb{P}${s | z < $V_2$ $\mu$ $\sigma$ s} = Q $(\frac{z-\mu}{\sigma})$) $\Rightarrow$
ideal_soft_error_rate $V_{BB}^L$ $V_{BB}^H$ $v_{BBn}$ =

$$\frac{1}{4}\mathtt{erfc}\left(\frac{V_{BB}^H}{\sqrt{2}\ v_{BBn}}\right) + \frac{1}{4}\mathtt{erfc}\left(\frac{V_{BB}^L}{\sqrt{2}\ v_{BBn}}\right)$$

**Proof:** We begin by rewriting the right hand side of Theorem A1 with the definition of the complementary error function ($\forall$x. Q x = $\frac{1}{2}$ erfc $(\frac{x}{\sqrt{2}})$), and with some rewriting arrive at the following subgoal.

$$\mathtt{ideal\_soft\_error\_rate}\ V_{BB}^L\ V_{BB}^H\ v_{BBn} = \frac{1}{2}\mathtt{Q}\left(\frac{(0-(-V_{BB}^H))}{v_{BBn}}\right) + \frac{1}{2}\mathtt{Q}\left(\frac{(0-(-V_{BB}^L))}{v_{BBn}}\right)$$

Using one of the properties of Q function (Q(x)+Q(-x)=1), we rewrite the right hand side of the above subgoal as follows:

$$\frac{1}{2}\left[1 - \mathtt{Q}\left(-\frac{(0-(-V_{BB}^H))}{v_{BBn}}\right)\right] + \frac{1}{2}\mathtt{Q}\left(\frac{(0-(-V_{BB}^L))}{v_{BBn}}\right)$$

Now using the cumulative distribution function of the gaussian random variable, we further rewrite both terms in the above expression,

$$\frac{1}{2}\left[1 - \mathbb{P}\{s|0 \ < \ (V_2\ V_{BB}^H\ v_{BBn}\ s)\}\right] + \frac{1}{2}\mathbb{P}\{s|0 < (V_1\ (-V_{BB}^L)\ v_{BBn}\ s)\}$$

Then using the fact that $\mathbb{P}(x \leq a) + \mathbb{P}(a < x) = 1$, we rewrite the first term in the above expression as:

$$\frac{1}{2}\left[\mathbb{P}\{s|(V_2\ V_{BB}^H\ v_{BBn}\ s) \ \leq \ 0\}\right] + \frac{1}{2}\mathbb{P}\{s|0 < (V_1\ (-V_{BB}^L)\ v_{BBn}\ s)\}$$

Finally, rewriting with the definition of the ideal_soft_error_rate shows that the left and the right hand side of the equation are equal and thus concludes the proof.

In Theorem A2, we verify the soft error rate expression (Equation 8) for a non ideal sense amplifier in the presence of thermal noise and parameter variations. Theorem 2 has seven extra assumptions in addition to those stated in Theorem 1. These assumptions state that $\delta$ and $\chi$ which relate the insensitivity width ($v_w = \delta V_{BB}^H$) and the sensitivity deviation ($v_d$ = $\chi$ $V_{BB}^H$) parameters to the mean values of the gaussian random variables $V_1$ and $V_2$, are real numbers and can only take values in the closed real interval [0,1]. The assumption ($V_{BB}^L = -V_{BB}^H$) states that the sense amplifier at its inputs sees two equal and opposite polarity dc signals represented by $V_{BB}^H$ and $V_{BB}^L$, respectively.

**Theorem A2:** *Non-ideal Sense Amplifier Soft Error Rate*

$\vdash \forall$ a b f $V_{BB}^{H}$ $V_{BB}^{L}$ $v_{BBn}$ $\delta$ $\chi$.
((a$\leq$b) $\wedge$ ($\forall$x. (a$\leq$x) $\wedge$ (x$\leq$b) $\Rightarrow$ (f diffl ($\lambda$t. $\frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}$) x) x) $\wedge$ (Q1 a b = f b - f a) $\wedge$
(Q y = $\lim\limits_{n\to\infty}$ ($\lambda$n. Q1 y (&n))) $\wedge$ ($\forall$x. Q x = $\frac{1}{2}$ erfc ($\frac{x}{\sqrt{2}}$)) $\wedge$
($\forall$z $\mu$ $\sigma$. (0 < $\sigma$) $\Rightarrow$ ($\mathbb{P}$\{s | z < $V_1$ $\mu$ $\sigma$ s\} = Q ($\frac{z-\mu}{\sigma}$)) $\wedge$
($\forall$z $\mu$ $\sigma$. (0 < $\sigma$) $\Rightarrow$ ($\mathbb{P}$\{s | z < $V_2$ $\mu$ $\sigma$ s\} = Q ($\frac{z-\mu}{\sigma}$)) $\wedge$ (0$\leq\delta$) $\wedge$ ($\delta\leq$1) $\wedge$
(0$\leq\chi$) $\wedge$ ($\chi\leq$1) $\wedge$ ($v_w$ = $\delta V_{BB}^{H}$) $\wedge$ ($v_d$ = $\chi$ $V_{BB}^{H}$) $\wedge$
(0 < $v_{BBn}$) $\wedge$ ($V_{BB}^{L} = -V_{BB}^{H}$) $\wedge$ (Q(y) + Q(-y) = 1) $\Rightarrow$
non_ideal_soft_error_rate $V_{BB}^{L}$ $V_{BB}^{H}$ $v_{BBn}$ =

$$\tfrac{1}{4}\texttt{erfc}\left(\frac{V_{BB}^{H}}{\sqrt{2}\ \ v_{BBn}}\left[1-\tfrac{\delta}{2}+\chi\right]\right) + \tfrac{1}{4}\texttt{erfc}\left(\frac{V_{BB}^{L}}{\sqrt{2}\ \ v_{BBn}}\left[1-\tfrac{\delta}{2}-\chi\right]\right)$$

**Proof:** We begin by rewriting the right hand side of Theorem A2 with the definition of the complementary error function ($\forall$x. Q x = $\frac{1}{2}$ erfc ($\frac{x}{\sqrt{2}}$)), and with some rewriting arrive at the following subgoal.

$$\texttt{non\_ideal\_soft\_error\_rate}\ V_{BB}^{L}\ V_{BB}^{H}\ v_{BBn}\texttt{=}$$
$$\tfrac{1}{2}\texttt{Q}\left(\frac{(v_d+\frac{v_w}{2}-(-V_{BB}^{H}))}{v_{BBn}}\left[1-\tfrac{\delta}{2}+\chi\right]\right)\texttt{+}\tfrac{1}{2}\texttt{Q}\left(\frac{(v_d-\frac{v_w}{2}-(-V_{BB}^{L}))}{v_{BBn}}\left[1-\tfrac{\delta}{2}-\chi\right]\right)$$

Using one of the properties of Q function (Q(x)+Q(-x)=1), we rewrite the right hand side of the above subgoal as follows:

$$\tfrac{1}{2}\left[1-\texttt{Q}\left(-\frac{(v_d+\frac{v_w}{2}-(-V_{BB}^{H}))}{v_{BBn}}\left[1-\tfrac{\delta}{2}+\chi\right]\right)\right]\texttt{+}\tfrac{1}{2}\texttt{Q}\left(\frac{(v_d-\frac{v_w}{2}-(-V_{BB}^{L}))}{v_{BBn}}\left[1-\tfrac{\delta}{2}-\chi\right]\right)$$

Now using the cumulative distribution function of the gaussian random variable, $v_w = \delta V_{BB}^{H}$, $v_d = \chi\ V_{BB}^{H}$ together with an additional assumption that the average voltage on the two bit lines is equal, $V_{BB}^{L} = -V_{BB}^{H}$, we rewrite both terms in the above expression as:

$$\tfrac{1}{2}\left[1-\mathbb{P}\{s|(\tfrac{v_d}{2}+v_w)\ \ <\ \ (V_2\ \ V_{BB}^{H}\ \ v_{BBn}\ \ s)\}\right]\ \texttt{+}\ \tfrac{1}{2}\mathbb{P}\{s|(\tfrac{v_d}{2}-v_w)<(V_1\ \ (V_{BB}^{H})\ \ v_{BBn}\ \ s)\}$$

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:

$$\tfrac{1}{2}\left[\mathbb{P}\{s|(V_2\ \ V_{BB}^{H}\ \ v_{BBn}\ \ s)\ \ \leq\ \ (\tfrac{v_d}{2}+v_w)\}\right]\ \texttt{+}\ \tfrac{1}{2}\mathbb{P}\{s|(\tfrac{v_d}{2}-v_w)<(V_1\ \ (-V_{BB}^{L})\ \ v_{BBn}\ \ s)\}$$

Finally, rewriting with the definition of the ideal_soft_error_rate, and the assumption that $V_{BB}^{L} = -V_{BB}^{H}$ shows that the left and the right hand side of the equation are equal and thus concludes the proof.

**A few other definitions**

The PDF ($f_X(x)$), and CDF ($F_X(x)$) of gaussian random variables are defined as:

$$f_X(x) = \frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}$$

$$F_X(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-\frac{t^2}{2}}dt$$

The complementary error function and the Q function very frequently appear in error rate analysis literature and are defined as:

$$Q(x) = \frac{1}{2}erfc\left(\frac{x}{\sqrt{2}}\right)$$

$$erfc(x) = 2Q\left(\sqrt{2}x\right)$$