Stochastic Formal Methods for Hybrid Systems

Marc Daumas, David Lester, Erik Martin-Dorel, Annick Truffert

Stochastic Formal Methods for Hybrid Systems

Marc Daumas*, Erik Martin-Dorel*†, David Lester‡ and Annick Truffert†

*ELIAUS (EA 3679 UPVD) and †LAMPS (EA 4217 UPVD)
Perpignan, France 66860, emails: firstname.lastname@univ-perp.fr

‡School of Computer Science, University of Manchester
Manchester, United Kingdom M13 9PL, email: david.r.lester@manchester.ac.uk

***Abstract*— We provide a framework to bound the probability that accumulated errors were never above a given threshold on hybrid systems. Such systems are used for example to model an aircraft or a nuclear power plant on one side and its software on the other side. This report contains a simple formula based on Lévy's and Markov's inequalities and it continues a formal theory of random variables with a special focus on producing concrete results. About a fourth of the bits of all the results of our archetype application remain continuously significant with a probability of failure of one against almost a billion, where worst case analysis considers that no significant bit remains. We are using PVS as such formal tools force explicit statement of all hypotheses and prevent incorrect uses of theorems. As our theorem contains hypotheses on the individual errors, we introduce Hoeffding's inequality and Kolmogorov-Smirnov's test to check that the hypotheses are almost certainly satisfied. The test can also be used to outline sources of errors that need to be analyzed in more details.**

I. Introduction

Formal proof assistants are used in areas where errors can cause loss of life or significant financial damage as well as in areas where common misunderstandings can falsify key assumptions. For this reason, formal proof assistants have been much used for floating point arithmetic [1], [2], [3], [4], [5] and probabilistic or randomized algorithms [6], [7]. Previous references link to a few projects using proof assistants such as ACL2 [8], HOL [9], Coq [10] and PVS [11].

All the above projects that deal with floating point arithmetic aim at containing worst case behavior. Recent work has shown that worst case analysis may be meaningless for systems that evolve for a long time as encountered in the industry. A good example is a process that adds numbers in ± 1 with a measure error of $\pm 2^{-25}$. If this process adds 2^{25} items, then the accumulated error is ± 1, and note that 10 hours of flight time at operating frequency of 1 kHz is approximately 2^{25} operations. Yet we easily agree that provided the individual errors are not correlated, the actual accumulated error will be much smaller.

We present in Section II the formal background on probability with Markov's inequality after a quick survey and analysis of previously published results [12]. Section III presents Lévy's inequality and how to use it to assert software reliability. Section IV presents Hoeffding's inequality and Kolmogorov-Smirnov's test and how to use it to assert the quality of the hypotheses of the result of the preceding section.

Lévy's inequality assumes that the random variables are symmetric though Doob's inequality combined with Jensen's one may overcome this restriction in future formal developments. Future developments will also provide statistical analyzes based on failure models (transient, temporary, time correlation...).

II. Formal background on probability

A. Long accumulation of individual errors

We use only one example of a very long accumulation as it singles out the main contributions of this work. More complex applications require techniques that have been presented in previous publications. Interval arithmetic [4], [5] would help providing possibly overestimated bounds to some of the theorems presented in this report. A semantic-sound definition of first vs. higher order errors [13] is necessary before one may focus only on first order errors. Yet these techniques can be used directly as implemented for worst case analysis.

The example given in Listing 1 sums n data produced by a fixed point sensor d_i with a measure error X_i. This report presents techniques **amenable to formal methods** for n **counting in billions** and a probability of failure about **one against a billion**. Should one of these constraints be removed or lessened, the problems

becomes much simpler and so we focus on this archetype accumulation.

Listing 1. Simple discrete integration

```
1 a_1 = 0;
2 for (i = 1; i <= n; i = i + 1)
3     a_{i+1} = a_i + d_i;
```

The accumulation deals with fixed point numbers but this work can also be applied to floating point arithmetic. A floating point number represents $v = m \times 2^e$ where e is an integer and m is a fixed point number [14]. IEEE 754 standard [15] uses sign-magnitude notation for the mantissa and the first bit b_0 of the mantissa is implicit in most cases ($b_0 = 1$) leading to the following definition where s and all the b_i are either 0 or 1 (bits).

$$v = (-1)^s \times b_0.b_1 \cdots b_{p-1} \times 2^e$$

Some circuits such as the TMS320 use two's complement notation for m leading to the following definition [16].

$$v = (b_0.b_1 \cdots b_{p-1} - 2 \times s) \times 2^e$$

In fixed point notation e is a constant provided by the data type and bit b_0 cannot be forced to 1.

We define for any representable number v, the unit in the last place function where e is the exponent of v as above.

$$\text{ulp}(v) = 2^{e-p+1}$$

In fixed point notation, one unit in the last place does not depend on the value of v so we write ulp instead of $\text{ulp}(v)$.

We can assume that as d_i is a data obtained by an accurate sensor, the difference between d_i and the actual value $\overline{d_i}$ is uniformly distributed in the range $\pm\text{ulp}/2$ or follow a normal distribution very close to a uniform distribution on this range. In both cases, we model the error $d_i - \overline{d_i}$ by a symmetric random variable X_i with moments

$$\begin{cases} \mathbb{E}(X) & = & 0, \\ \mathbb{E}\left(X^2\right) & \leq & \text{ulp}^2/12, \\ \mathbb{E}\left(X^4\right) & \leq & \text{ulp}^4/80. \end{cases}$$

The sensor may be less accurate leading to larger moments.

Data are fixed point meaning that the sum $a_i + d_i$ does not introduce any rounding error. Errors created by operators are discrete and they are not necessarily distributed uniformly [17]. The distribution is very specific but as soon as we verify that the error is symmetric we only have to bound the moments involved in our main result.

After n iterations and assuming that X_i are independent, we want the probability that the accumulated errors, $S_i = \sum_{j=1}^{i} X_j$, have always been constrained into user specified bounds ϵ. Using the Doob-Kolmogorov's inequality [12] we have that

$$\mathbb{P}\left(\max_{1 \leq i \leq n}(|S_i|) \leq \epsilon\right) \geq 1 - \frac{n\,\text{ulp}^2}{12\epsilon^2}.$$

We will see in Section III that we can exhibit tighter bounds using Lévy's inequality followed by Markov's one. We will see in Section IV that we may check the hypotheses of Lévy's inequality with an extremely low probability of failure.

B. A generic and formal theory of probability

Daumas and Lester [12] presented an account of probability with an informal approach while taking foundational matters seriously. The PVS system underlying these results was built on firm foundations for probability theory (using measure theory) [18], [19]. A middle way between extreme formality and an accessible level of informality is to be found in [20].

We rebuilt the theory of probability spaces as a theory of Lebesgue integration became fully available. The new PVS development in Figure 1, still takes three parameters: $\mathtt{T}$, the sample space, $\mathcal{S}$, a σ-algebra of permitted events, and, $\mathbb{P}$, a probability measure, which assigns to each permitted event in $\mathcal{S}$, a probability between 0 and 1. Properties of probability that are independent of the particular details of $\mathtt{T}$, $\mathcal{S}$ and $\mathbb{P}$ are then provided in this file.

A random variable X is a measurable application from $(\mathtt{T}, \mathcal{S})$ to any other measurable space $(\mathtt{T}', \mathcal{S}')$. In most theoretical developments of probability $\mathtt{T}$, $\mathcal{S}$ and $\mathbb{P}$ remain generic as computations are carried on $\mathtt{T}'$. Results on real random variables use $\mathtt{T}' = \mathbb{R}$ whereas results on random vectors use $\mathtt{T}' = \mathbb{R}^n$. Yet both theories refer explicitly to the Borel sets of T'.

As the Borel sets of $\mathbb{R}^n$ are difficult to grasp, most authors consider countable $\mathtt{T}$ and $\mathcal{S} = \mathcal{P}(\mathtt{T})$ for discrete random variables in introductory classes. This simpler analysis is meant only for educational purposes and most results of probability considered for formal methods can be implemented with generic $\mathtt{T}$, $\mathcal{S}$ and $\mathbb{P}$ parameters.

Handling discrete and continuous random variables through different $\mathtt{T}$ and $\mathcal{S}$ parameters is not necessary and it is contrary to most uses of probability spaces in mathematics. Such variables can be described on the

```
probability_space[T:TYPE+,          (IMPORTING topology@subset_algebra_def[T])
                  S:sigma_algebra,  (IMPORTING probability_measure[T,S])
                  P:probability_measure]: THEORY
BEGIN
   IMPORTING topology@sigma_algebra[T,S],
             probability_measure[T,S],
             continuous_functions_aux[real],
             measure_theory@measure_space[T,S],
             measure_theory@measure_props[T,S,to_measure(P)]

   limit: MACRO [(convergence_sequences.convergent)->real]
                                                = convergence_sequences.limit
   phi: VAR borel_function
   A,B: VAR (S)
   x,y: VAR real
   n0z: VAR nzreal
   t:   VAR T
   n:   VAR nat
   X,Y: VAR random_variable
   XS:  VAR [nat->random_variable]

   null?(A)         :bool = P(A) = 0
   non_null?(A)     :bool = NOT null?(A)
   independent?(A,B):bool = P(intersection(A,B)) = P(A) * P(B)

   zero: random_variable = (LAMBDA t: 0)
   one:  random_variable = (LAMBDA t: 1)

   <=(X,x):(S) = {t | X(t) <= x}; % Needed for syntax purposes! < > = /= >= omitted

   complement_le1: LEMMA complement(X <= x) = (x <  X) % More omitted

   +(X,x)  :random_variable = (LAMBDA t: X(t) + x); % Needed for syntax purposes! More omitted

   borel_comp_rv_is_rv: JUDGEMENT o(phi,X) HAS_TYPE random_variable

   partial_sum_is_random_variable:
     LEMMA random_variable?(LAMBDA t: sigma(0,n,LAMBDA n: XS(n)(t)))

   distribution_function?(F:[real->probability]):bool
                                     = EXISTS X: FORALL x: F(x) = P(X <= x)

   distribution_function: TYPE+ = (distribution_function?) CONTAINING
                                    (LAMBDA x: IF x < 0 THEN 0 ELSE 1 ENDIF)

   distribution_function(X)(x):probability = P(X <= x)

   convergence_in_distribution?(XS,X):bool
     = FORALL x: continuous(distribution_function(X),x) IMPLIES
                 convergence((LAMBDA n: distribution_function(XS(n))(x)),
                                        distribution_function(X)(x))

   invert_distribution:   LEMMA LET F = distribution_function(X) IN
                                P(x < X) = 1 - F(x)
   interval_distribution: LEMMA LET F = distribution_function(X) IN
                                x <= y IMPLIES
                                P(intersection(x < X, X <= y)) = F(y) - F(x)
   limit_distribution:    LEMMA LET F = distribution_function(X) IN
                                P(X = x) = F(x) - limit(LAMBDA n: F(x-1/(n+1)))

   F: VAR distribution_function

   distribution_0:                LEMMA convergence(F o (lambda (n:nat): -n),0)
   distribution_1:                LEMMA convergence(F,1)
   distribution_increasing:       LEMMA increasing?[real](F)
   distribution_right_continuous: LEMMA right_continuous(F)

END probability_space
```

Fig. 1. Abbreviated probability space file in PVS

same generic $\mathtt{T}$, $\mathcal{S}$ and $\mathbb{P}$ parameters in spite of their differences. In practice, we use $\mathtt{T}' = \mathbb{R}$ or $\mathtt{T}' = \mathbb{R}^n$ and the ranges of discrete variables are countable.

Similarly, many authors work on sections $\{X \leq x\}$ rather than using *the inverse images of Borel sets* of $\mathtt{T}'$ because the latter are difficult to visualize. Such a simplification is valid thanks to Dynkin's systems. But using abstract Borel sets rather than sections in formal methods often leads to easier proofs.

Of particular interest later is the fact that the sum of two random variables is itself a random variable, and consequently any finite sum of random variables is a random variable.

C. A concrete theory of expectation

The previous theory of random variables [12] made it possible to define them and to use and derive their properties. Very few results were enabling users to actually compute concrete results on random variables. Most of such results lie on a solid theory of the expected value. As most theorems in the later theory are corollaries of a good theory of Lebesgue's integration, we have developed a full fledged formal measure theory based on Lebesgue integration and we develop formal theorems on expected values as needed in our applications.

The expected value is the (unique) linear and monotonous operator $\mathbb{E}$ on the set of $\mathbb{P}$-integrable random variables that satisfies Beppo-Lévy's property and such that $\mathbb{E}(\chi_A) = \mathbb{P}(A)$ for all $A \in \mathcal{S}$. We can also use the following definition when Lebesgue's integral exists:

$$\mathbb{E}(X) = \int_{\mathtt{T}} X \; d\,\mathbb{P}$$

Markov's theorem below is heavily used to obtain concrete properties on random variables.

Theorem 1 (Markov's inequality): For any random variable X and any constant ϵ,

$$\mathbb{P}\left(|X| \geq \epsilon\right) \leq \frac{\mathbb{E}\left(|X|\right)}{\epsilon}.$$

Many theorems relate to independent random variables and their proof are much easier once independence is well defined. We write

$$(X_1, \ldots, X_n) \;\amalg$$

if and only if, for any family of Borel sets $(B_1, \ldots, B_n)$,

$$\mathbb{P}\left(\bigwedge_{i=1}^{n} X_i \in B_i\right) = \prod_{i=1}^{n} \mathbb{P}\left(X_i \in B_i\right)$$

The following characteristic property is used a lot on families of independent variables for any family of Borel-measurable functions $(f_1, \ldots, f_n)$,

$$\mathbb{E}\left(\prod_{i=1}^{n} f_i(X_i)\right) = \prod_{i=1}^{n} \mathbb{E}\left(f_i(X_i)\right).$$

It is worth noting that the fact that n random variables are independent is not equivalent to the fact that any pair of variables is independent and cannot be built recursively from $n-1$ independent random variables.

Hoeffding's inequality (see Section IV) relies on the generating function associated to a random variable X when it is defined,

$$M_X(t) = \mathbb{E}\left(e^{tX}\right).$$

This function was introduced because its derivatives are linked with the moments of X,

$$M_X^{(k)}(0) = \mathbb{E}\left(X^k\right).$$

Theorem 2: For a bounded random variable such that $\mathbb{P}(a \leq X \leq b) = 1$ and $\mathbb{E}(X) = 0$,

$$M_X(t) \leq \exp\left((t^2(b-a)^2/8\right)$$

Proof: We represent $X = (1-U)a + Ub$ with U between 0 and 1. It follows that $U = (X-a)/(b-a)$ and as the exponential function is convex

$$\mathbb{E}(e^{tX}) \leq (1 - \mathbb{E}(U))e^{ta} + \mathbb{E}(U)e^{tb}.$$

As X is centered, $\mathbb{E}(U) = -a/(b-a)$ and

$$M_X(t) \leq e^{\Phi(t(b-a))}$$

with

$$\Phi(s) = -s\,\mathbb{E}(U) + \ln\left(1 - \mathbb{E}(U) + \mathbb{E}(U)e^s\right).$$

The bound is obtained using Taylor series since $\Phi(0) = 0$, $\Phi'(0) = 0$ and $\Phi''(0) \leq 1/4$. ∎

A complete study of M_X for absolutely continuous random variables would ultimately lead to a theory of Laplace transform.

Future work may lead us to implement a theory of probability the law $\mathbb{P}_X$ associated to each random variable X with a transfer theorem for a function f from $\mathtt{T}'$ to $\mathbb{R}$

$$\mathbb{E}(f(X)) = \int_{\mathtt{T}} f \circ X \; d\,\mathbb{P} = \int_{\mathtt{T}'} f \; d\,\mathbb{P}_X,$$

and most properties of Lebesgue integral including Fubini's theorem.

III. Almost certain a priori error bound

What we are actually interested in is whether a series of calculations might accumulate a sufficiently large error to become meaningless. In the language we have developed, we are computing the probability that a sequence of n calculations has failed because it has exceeded the ϵ error-bound somewhere.

A. Use of Lévy's Inequality

More formally, we have a sequence of random variables (X_n) and we define their partial sums as a sequence of random variables (S_n).

$$S_n = \sum_{i=1}^{n} X_i.$$

Theorem 3 (Lévy's inequality): Provided the (X_n) are independent and symmetric the following property holds for any constant ϵ.

$$\mathbb{P}\left(\max_{1\leq i\leq n}(|S_i|) \geq \epsilon\right) \leq 2\,\mathbb{P}\left(|S_n| \geq \epsilon\right)$$

Proof: We use a proof path similar to the one published in [21]. We define $S_n^{(j)}$ with Dirichlet's operator δ_P that is equal to 1 if the predicate holds and 0 otherwise.

$$S_n^{(j)} = \sum_{i=1}^{n} (-1)^{\delta_{i>j}} X_i$$

As the X_n are symmetric, the random variables S_n and $\left(S_n^{(j)}\right)$ share the same probability density function.

We now define $N = \inf\{k \text{ such that } |S_k| \geq \epsilon\}$ with the addition that $\inf\emptyset = \infty$ and similarly $N^{(j)} = \inf\{k \text{ such that } |S_k^{(j)}| \geq \epsilon\}$. Events $\max_{1\leq i\leq n}(|S_i|) \geq \epsilon$ and $N \leq n$ are identical. Furthermore

$$\begin{aligned}\mathbb{P}\left(|S_n| \geq \epsilon\right) &= \sum_{j=1}^{n} \mathbb{P}\left(|S_n| \geq \epsilon \ \wedge \ N = j\right) \\ &= \sum_{j=1}^{n} \mathbb{P}\left(|S_n^{(j)}| \geq \epsilon \ \wedge \ N = j\right).\end{aligned}$$

As soon as $j \leq n$, $2S_j = S_n + S_n^{(j)}$ and $2|S_j| = |S_n| + |S_n^{(j)}|$. Therefore, the event $\{|S_j| \geq \epsilon\}$ is included in $\{|S_n| \geq \epsilon\} \cup \{|S_n^{(j)}| \geq \epsilon\}$ and

$$\mathbb{P}\left(N \leq n\right) = \sum_{j=1}^{n} \mathbb{P}\left(|S_j| \geq \epsilon \ \wedge \ N = j\right)$$

is bounded by

$$\begin{aligned}&\sum_{j=1}^{n} \mathbb{P}\left(|S_n| \geq \epsilon \ \wedge \ N = j\right) \\ + \ &\sum_{j=1}^{n} \mathbb{P}\left(|S_n^{(j)}| \geq \epsilon \ \wedge \ N = j\right)\end{aligned}$$

This ends the proof of Lévy's inequality. ■

Doob-Kolmogorov's inequality was used in previous work. It is an application of Doob's inequality that can be proved with elementary manipulations for second order moment. It is better than Lévy's inequality in the sense that it can applied to any sum of independent and centered variables X_n. Yet it is limited by the fact that it bounds only second order moments.

Should we need to provide some formula beyond the hypotheses of Lévy's inequality, we may have to prove in PVS Doob's original inequality for martingales and sub-martingales [22]. It follows a proof path very different from Doob-Kolmogorov's inequality but it is not limited to second order moment and it can be applied to any sub-martingale $|S_i^{2k}|$ with $k \geq 1$ to lead to

$$\mathbb{P}\left(\max_{1\leq i\leq n}(|S_i|) \geq \epsilon\right) \leq \frac{\mathbb{E}\left(S_n^{2k}\right)}{\epsilon^{2k}}.$$

Shall we need to create a sub-martingale different from $|S_i^{2k}|$, we may have to prove Jensen's conditional inequality that let us introduce $h(|S_i|)$ where $h : \mathbb{R}_+ \to \mathbb{R}_+$ is convex. The inequality becomes

$$\mathbb{P}\left(\max_{1\leq i\leq n}(|S_i|) \geq \epsilon\right) \leq \frac{\mathbb{E}\left(h\left(S_n\right)\right)}{h(\epsilon)}.$$

B. Use of Markov's Inequality

We use Markov inequality applied to $X = S_n^k$.

$$\mathbb{P}\left(|S_n| \geq \epsilon\right) = \mathbb{P}\left(|S_n^k| \geq \epsilon^k\right) \leq \frac{\mathbb{E}\left(|S_n^k|\right)}{\epsilon^k}$$

We derive for second order moments when X_n are uniformly distributed over $[-\text{ulp}/2, \text{ulp}/2]$ a formula that is less accurate than the one obtained using Doob-Kolmogorov's inequality. We focus on the fourth moment and we easily check the following identity from the property of the expectation operator since X_n are

independent and symmetric.

$$\begin{aligned}\mathbb{E}\left(|S_n^4|\right) &= \mathbb{E}\left(S_n^4\right) = \mathbb{E}\left(\left(\sum_{i=1}^{n} X_i\right)^4\right)\\ &= \mathbb{E}\left(\sum_{i,j,k,l=1}^{n} X_i X_j X_k X_l\right)\\ &= \sum_{i,j,k,l=1}^{n} \mathbb{E}\left(X_i X_j X_k X_l\right)\\ &= \sum_{i=1}^{n} \mathbb{E}\left(X_i^4\right) + \sum_{i,j=1 \text{ and } i\neq j}^{n} \mathbb{E}\left(X_i^2 X_j^2\right)\\ &= \frac{n\,\mathrm{ulp}^4}{80} + \frac{n(n-1)\mathrm{ulp}^4}{144}\end{aligned}$$

Quick highest order instantiation of the variable show that

$$\mathbb{P}\left(\max_{1\leq i\leq n}\left(|S_i|\right) \geq \epsilon\right) \lesssim \mathrm{ulp},$$

leads to

$$2\left(\frac{n}{80} + \frac{n(n-1)}{144}\right)\frac{\mathrm{ulp}^4}{\epsilon^4} \approx \frac{\mathrm{ulp}^2}{72\epsilon^4} \lesssim \mathrm{ulp}$$

and

$$\sqrt[4]{\frac{\mathrm{ulp}}{72}} \lesssim \epsilon.$$

This means that about a fourth of the bits are still significant with a probability of failure of one against almost a billion.

We conclude that if the individual errors are random variables uniformly distributed over $[-\mathrm{ulp}/2, \mathrm{ulp}/2]$, we can bound the probability that the accumulated errors were never above ϵ with

$$\mathbb{P}\left(\max_{1\leq i\leq n}\left(|S_i|\right) \leq \epsilon\right) \geq 1 - n\left(n + \frac{4}{5}\right)\frac{\mathrm{ulp}^4}{72\epsilon^4}.$$

Notice that this bound can be applied to any sequence of random variables (X_n) provided that X_n are independent, symmetric and they admit second and fourth order moments such that

$$\mathbb{E}(X_i^2) \leq \frac{\mathrm{ulp}^2}{12} \qquad \text{and} \qquad \mathbb{E}(X_i^4) \leq \frac{\mathrm{ulp}^4}{80}.$$

We may use and prove better bounds based on the binomial formula as $\mathbb{E}\left(S_n^{2k}\right)$ is equal to

$$\sum_{k_1+k_2+\cdots k_n=k} (2k)! \frac{\mathbb{E}\left(X_1^{2k_1}\right)}{(2k_1)!}\frac{\mathbb{E}\left(X_2^{2k_2}\right)}{(2k_2)!}\cdots\frac{\mathbb{E}\left(X_n^{2k_n}\right)}{(2k_n)!}.$$

Proof: We first prove that $\mathbb{E}\left(S_n^m\right)$ is equal to the following formula by induction on n for any exponent m.

$$\sum_{m_1+m_2+\cdots m_n=m} m! \frac{\mathbb{E}\left(X_1^{m_1}\right)}{m_1!}\frac{\mathbb{E}\left(X_2^{m_2}\right)}{m_2!}\cdots\frac{\mathbb{E}\left(X_n^{m_n}\right)}{m_n!}$$

It holds for $n = 1$. We now write the following identity based on the facts that X_n are independent and centered. $\mathbb{E}\left(S_{n+1}^m\right) = \mathbb{E}\left(\left(S_n + X_{n+1}\right)^m\right)$ is also equal to

$$\mathbb{E}\left(\sum_{m_{n+1}=0}^{p} \frac{m!}{(m-m_{n+1})!m_{n+1}!} X_{n+1}^{m_{n+1}} S_n^{m-m_{n+1}}\right)$$

and

$$\sum_{m_{n+1}=0}^{p} \frac{m!}{(m-m_{n+1})!m_{n+1}!}\mathbb{E}\left(X_{n+1}^{m_{n+1}}\right)\mathbb{E}\left(S_n^{m-m_{n+1}}\right)$$

We expand the terms of the sum for $m_{n+1} = 0, \ldots, p$ and $\sum_{i=1}^{n} m_i = m - m_{n+1}$

$$\frac{m!}{(m-m_{n+1})!m_{n+1}!}\frac{(m-m_{n+1})!}{\prod_{i=1}^{n} m_i!}\prod_{i=1}^{n+1}\mathbb{E}\left(X_i^{m_i}\right)$$

We end the proof for the even values of m after noticing that $\mathbb{E}\left(X_i^{2k+1}\right) = 0$ for any i and any k since X_n are symmetric. ∎

We easily check that for a random variables X_i uniformly distributed over $[-\mathrm{ulp}/2, \mathrm{ulp}/2]$,

$$\begin{aligned}\mathbb{E}\left(X_i^p\right) &= \frac{1}{\mathrm{ulp}}\int_{-\mathrm{ulp}/2}^{\mathrm{ulp}/2} x^p dx = \frac{1}{\mathrm{ulp}}\left[\frac{x^{p+1}}{p+1}\right]_{-\mathrm{ulp}/2}^{\mathrm{ulp}/2}\\ &= \frac{\mathrm{ulp}^p}{(p+1)2^p}.\end{aligned}$$

IV. Almost certain validation in-situ

A. Checking moments used in Lévy's inequality

Following Hoeffding's inequality [23], [24, p. 165], we compute E_1, E_2 and E_4 the observed mean, second order moment and fourth order moment of the X_n.

Theorem 4 (Hoeffding's inequality): Provided X_n are independent and such that $\mathbb{P}(a_i \leq X_i \leq b_i) = 1$ then

$$\mathbb{P}(S_n - \mathbb{E}(S_n) \geq \epsilon) \leq \exp\left(-\frac{2\epsilon^2}{\sum_{i=1}^{n}(b_i - a_i)^2}\right)$$

Proof: We may replace X_i by $X_i - \mathbb{E}(X_i)$ and we will continue this proof for $\mathbb{E}(X_i) = 0$. The following inequality is satisfied for any positive real t thanks to Markov's inequality:

$$\mathbb{P}(S_n \geq \epsilon) = \mathbb{P}\left(\exp(tS_n) \geq e^{t\epsilon}\right) \leq \frac{\mathbb{E}(\exp(tS_n))}{e^{t\epsilon}}.$$

Since the X_n are independent, we obtain

$$\mathbb{P}(S_n \geq \epsilon) \leq e^{-t\epsilon} \prod_{i=1}^{n} \mathbb{E}(\exp(tX_i)).$$

The proof is finished by using a simple bound presented Section II and finding a positive t such that the following upper bound is as low as possible.

$$\mathbb{P}(S_n \geq \epsilon) \leq exp\left(-t\epsilon + t^2 \sum_{i=1}^{n} (b_j - a_j)^2/8\right).$$

The value is

$$t = \frac{4\epsilon}{\sum_{i=1}^{n}(b_j - a_j)^2}$$

■

Assuming that the X_n are identically distributed, the $-a_i$ and b_i are bounded by a constant c, and we deduce that

$$\mathbb{P}\left(\left|\frac{E_k - \mathbb{E}(X^k)}{c^k}\right| \geq \epsilon\right) \leq 2e^{-n\epsilon^2/2}$$

B. Comparison with a reference uniform distribution

We have just seen how to check the hypotheses on the mean, second order and fourth order moment used in Lévy's inequality in Section III. It seems that the round-off errors should be continuous or discrete and uniformly distributed in the range $[-\text{ulp}/2, \text{ulp}/2]$ as trailing digits of numbers randomly chosen from a logarithmic distribution [25, p. 254-264] are approximately uniformly distributed [26]. Any other distribution may mean that the round-off error contains more than trailing digits.

Parameters a and b of a uniform distribution over $[a, b]$ can be estimated through the observed lower and upper bounds that tends to the actual lower and upper bound of the distribution,

$$I_n = \min_{1 \leq i \leq n} X_i \qquad \text{and} \qquad M_n = \max_{1 \leq i \leq n} X_i.$$

As the observed bounds are biased

$$\mathbb{E}(I_n) = a + \frac{b-a}{n+1} \qquad \text{and} \qquad \mathbb{E}(M_n) = b - \frac{b-a}{n+1},$$

we need to correct them to

$$\begin{cases} \overline{I}_n &= \dfrac{n}{n-1} I_n - \dfrac{1}{n-1} M_n, \\ \overline{M}_n &= \dfrac{n}{n-1} M_n - \dfrac{1}{n-1} I_n. \end{cases}$$

These two bounds are converging estimators. As statistic (I_n, M_n) is complete and sufficient, we deduce from Lehmann-Scheffé's theorem that they are minimum-variance unbiased estimators [27].

Now we want to know if it is reasonable with a very low probability of failure to assume that the X_n are identical random variables distributed evenly between a and b. We build $F_n(x)$ the empirical distribution function,

$$F_n(x) = \frac{1}{n} \sum_{i=1}^{n} \chi_{(-\infty, x)}(X_i).$$

We easily check that (F_n) is a sequence of random variable converging almost everywhere to F, the distribution function common of X_n. Furthermore $\mathbb{E}(F_n(x)) = F(x)$ and $F_n(x)$ is an unbiased estimator of $F(x)$.

Now we define F_0 as the distribution function of X_0, a random variable uniformly distributed between a and b. The test should decide on

$$\begin{cases} (H_0) & F = F_0, \\ (H_1) & F \neq F_0. \end{cases}$$

Kolmogorov-Smirnov's test is based under statistics (functions of F_n and F_0), that can be considered as pseudo-distances between probability laws. It uses the following result [28].

Theorem 5: If X_n are identically distributed to X_0, then $\sqrt{n}\,\|F_n - F_0\|_\infty$ converge almost surely to a law characterized by its distribution function:

$$R(x) = 1 - \sum_{i=1}^{\infty} (-1)^{k-1} e^{-2k^2x^2}.$$

Under hypothesis (H_0), the X_n are uniformly distributed between a and b and the answer is easy. We will accept null hypothesis if statistic

$$K_n = \|F_n - F_0\|_\infty = \sup_x |F_n(x) - F_0(x)|$$

takes only low values. The critical domain of the test is therefore $W = \{(x_1, x_2, \ldots, x_n) \text{ such that } K_n > c\}$ where c is found from $\alpha = \mathbb{P}(W)$ and first order error α (reject (H_0) thought it was true) satisfies

$$\alpha = \mathbb{P}(W) = \mathbb{P}(\sqrt{n}\,K_n > c\sqrt{n}) \approx 1 - R(c\sqrt{n})$$

Therefore $c\sqrt{n}$ is the quantile of order $1 - \alpha$ of the asymptote distribution function R of $\sqrt{n}\,K_n$. The asymptotic law has been tabulated for $\alpha = 0.05$ or $\alpha = 0.01$ [27], [29]. It yields $c = 1.63/\sqrt{n}$ for $\alpha = 0.01$ and $c = 1.36/\sqrt{n}$ for $\alpha = 0.05$ assuming $n > 100$.

V. Perspectives and concluding remarks

To the best of our knowledge this paper presents the first application of Lévy's and Hoeffding's inequalities combined with Kolmogorov-Smirnov's test to software reliability of very long sums with an extremely low rate of failure. Our results allow any one to develop safe upper limits on the number of operations that a piece of numeric software should be permitted to undertake. In addition, we are finishing certification of our results with PVS. The major restriction lies in the fact that the slow process of proof checking has forced us to insist that individual errors are symmetric.

At the time we are submitting this work, the bottleneck is the full certification of more results using PVS proof assistant. Yet this step is compulsory to provide full certification to future industrial uses. We anticipate no problem as these results are gathered in textbooks in computer science and mathematics. This library and future work will be included into NASA Langley PVS library[1] as soon as it becomes stable.

The main contribution of this work is that we carefully chose theorems that produce significant results for extremely low probabilities of failure of systems that run for a long time and that are amenable to formal methods. During our work, we discarded many mathematical methods that would need too many operations or that would be too technical to be implemented with existing formal systems.

It is worth pointing out one more time that violating our assumption (independence of errors) would lead to worse results, so one should treat the limit we have deduced with caution, should this assumption not be met.

Acknowledgment

This work has been partially funded by CNRS PICS 2533 and by the EVA-Flo project of the ANR. It was initiated while one of the authors was an invited professor at the University of Perpignan Via Domitia.

References

[1] D. M. Russinoff, "A mechanically checked proof of IEEE compliance of the floating point multiplication, division and square root algorithms of the AMD-K7 processor," *LMS Journal of Computation and Mathematics*, vol. 1, pp. 148–200, 1998. [Online]. Available: http://www.onr.com/user/russ/david/k7-div-sqrt.ps

[2] J. Harrison, "Formal verification of floating point trigonometric functions," in *Proceedings of the Third International Conference on Formal Methods in Computer-Aided Design*, W. A. Hunt and S. D. Johnson, Eds., Austin, Texas, 2000, pp. 217–233. [Online]. Available: http://www.springerlink.com/link.asp?id=wxvaqu9wjrgc8l99

[3] S. Boldo and M. Daumas, "Representable correcting terms for possibly underflowing floating point operations," in *Proceedings of the 16th Symposium on Computer Arithmetic*, J.-C. Bajard and M. Schulte, Eds., Santiago de Compostela, Spain, 2003, pp. 79–86. [Online]. Available: http://perso.ens-lyon.fr/marc.daumas/SoftArith/BolDau03.pdf

[4] M. Daumas and G. Melquiond, "Generating formally certified bounds on values and round-off errors," in *Real Numbers and Computers*, Dagstuhl, Germany, 2004, pp. 55–70. [Online]. Available: http://hal.inria.fr/inria-00070739

[5] M. Daumas, D. Lester, and C. Muñoz, "Verified real number calculations: A library for interval arithmetic," *IEEE Transactions on Computers*, 2008, to appear.

[6] J. Hurd, "Formal verification of probabilistic algorithms," Ph.D. dissertation, University of Cambridge, 2002. [Online]. Available: http://www.cl.cam.ac.uk/~jeh1004/research/papers/thesis.pdf

[7] P. Audebaud and C. Paulin-Mohring, "Proofs of randomized algorithms in Coq," in *Proceedings of the 8th International Conference on Mathematics of Program Construction*, T. Uustalu, Ed., Kuressaare, Estonia, 2006, pp. 49–68. [Online]. Available: http://dx.doi.org/10.1007/11783596_6

[8] M. Kaufmann, P. Manolios, and J. S. Moore, *Computer-Aided Reasoning: An Approach*. Kluwer Academic Publishers, 2000.

[9] M. J. C. Gordon and T. F. Melham, Eds., *Introduction to HOL: A theorem proving environment for higher order logic*. Cambridge University Press, 1993.

[10] G. Huet, G. Kahn, and C. Paulin-Mohring, *The Coq proof assistant: a tutorial: version 8.0*, 2004. [Online]. Available: ftp://ftp.inria.fr/INRIA/coq/current/doc/Tutorial.pdf.gz

[11] S. Owre, J. M. Rushby, and N. Shankar, "PVS: a prototype verification system," in *11th International Conference on Automated Deduction*, D. Kapur, Ed. Saratoga, New-York: Springer-Verlag, 1992, pp. 748–752. [Online]. Available: http://pvs.csl.sri.com/papers/cade92-pvs/cade92-pvs.ps

[12] M. Daumas and D. Lester, "Stochastic formal methods: an application to accuracy of numeric software," in *Proceedings of the 40th IEEE Annual Hawaii International Conference on System Sciences*, Waikoloa, Hawaii, 2007, p. 7 p. [Online]. Available: http://hal.ccsd.cnrs.fr/ccsd-00081413

[13] M. Martel, "Semantics of roundoff error propagation in finite precision calculations," *Higher-Order and Symbolic Computation*, vol. 19, no. 1, pp. 7–30, 2006. [Online]. Available: http://dx.doi.org/10.1007/s10990-006-8608-2

[14] D. Goldberg, "What every computer scientist should know about floating point arithmetic," *ACM Computing Surveys*, vol. 23, no. 1, pp. 5–47, 1991. [Online]. Available: http://doi.acm.org/10.1145/103162.103163

[15] D. Stevenson *et al.*, "An American national standard: IEEE standard for binary floating point arithmetic," *ACM SIGPLAN Notices*, vol. 22, no. 2, pp. 9–25, 1987.

[16] *TMS320C3x — User's guide*, Texas Instruments, 1997. [Online]. Available: http://www-s.ti.com/sc/psheets/spru031e/spru031e.pdf

[17] J. Bustoz, A. Feldstein, R. Goodman, and S. Linnainmaa, "Improved trailing digits estimates applied to optimal computer arithmetic," *Journal of the ACM*, vol. 26, no. 4, pp. 716 – 730,

[1] `http://shemesh.larc.nasa.gov/fm/ftp/larc/PVS-library/pvslib.html`.

1979. [Online]. Available: http://doi.acm.org/10.1145/322154.322162

[18] P. R. Halmos, “The foundations of probability,” *American Mathematical Monthly*, vol. 51, pp. 493–510, 1944.

[19] ——, *Measure Theory*. Van Nostrand Reinhold, 1950.

[20] G. R. Grimmett and D. R. Stirzaker, *Probability and Random Processes*. Oxford University Press, 1982.

[21] J. Bertoin, “Probabilités,” 2001, cours de licence de mathématiques appliquées. [Online]. Available: http://www.proba.jussieu.fr/cours/bertoin.pdf

[22] J. Neveu, Ed., *Martingales à temps discret*. Masson, 1972.

[23] W. Hoeffding, “Probability inequalities for sums of bounded random variables,” *Journal of the American Statistical Association*, vol. 58, no. 301, pp. 13–30, 1963. [Online]. Available: http://www.jstor.org/stable/2282952

[24] A. B. Tsybakov, *Introduction à l’estimation non-paramétrique*. Springer, 2003.

[25] D. E. Knuth, *The Art of Computer Programming: Seminumerical Algorithms*. Addison-Wesley, 1997, third edition.

[26] A. Feldstein and R. Goodman, “Convergence estimates for the distribution of trailing digits,” *Journal of the ACM*, vol. 23, no. 2, pp. 287–297, 1976. [Online]. Available: http://doi.acm.org/10.1145/321941.321948

[27] P. Tassi, *Méthodes statistiques*. Economica, 2004.

[28] B. L. Van der Waerden, *Statistique mathématique*. Dunod, 1967.

[29] Z. W. Birnbaum, “Numerical tabulation of the distribution of Kolmogorov’s statistic for finite sample size,” *Journal of American Statistical Association*, vol. 47, no. 259, pp. 425–441, 1952. [Online]. Available: http://www.jstor.org/stable/2281313