Bornes quasi-certaines sur l'accumulation d'erreurs infimes dans les systèmes hybrides

Marc Daumas, Erik Martin-Dorel, Annick Truffert

Bornes quasi-certaines sur l'accumulation d'erreurs infimes dans les systèmes hybrides

Marc Daumas[1], Érik Martin-Dorel[1,2] et Annick Truffert[2]

1 : Éliaus (*Électronique, Informatique, Automatique et Systèmes*), éa 3679 upvd
2 : Lamps (*Laboratoire de Mathématiques, Physique et Systèmes*), éa 4217 upvd

Université de Perpignan Via Domitia, *52 avenue Paul Alduy, 66860 France*
Courriel : {marc.daumas,erik.martin-dorel,truffert}@univ-perp.fr

Résumé

Les gros systèmes industriels constituent, soit seuls, soit avec leur environnement, des systèmes hybrides (logiciel, matériel) qui évoluent pendant un grand laps de temps. Les méthodes d'analyse au pire cas aboutissent souvent à la conclusion que ces systèmes ne peuvent que tomber en panne. Pour ces raisons, il est admis que ces systèmes ont une probabilité de ne pas fonctionner correctement. Nous présentons ici nos premiers travaux pour fournir une certification par les méthodes formelles de ce type de bon fonctionnement. Ce travail nous a amené à nous pencher sur les développements existants en probabilité et à définir une feuille de route pour de nouveaux développements formels en probabilités et en statistiques. Cette présentation replace les différente tâches dans l'architecture générale d'une chaîne de certification contenant à la fois des éléments formels et des mesures empiriques d'un code instrumenté.

1. Introduction et motivations

Les méthodes formelles sont utilisées dans des domaines où des erreurs peuvent causer des pertes en vies humaines, des dommages financiers importants ou quand des erreurs courantes viennent invalider les cheminements de pensées usuels. Pour ces raisons, les méthodes formelles ont été utilisées en arithmétique à virgule flottante [1, 2, 3, 4, 5] et sur des algorithmes randomisés et des analyses randomisées d'algorithmes [6, 7]. Ces références présentent quelques travaux utilisant des outils formels tels que ACL2 [8], HOL [9], Coq [10] et PVS [11].

Tous les travaux précédents sur l'arithmétique à virgule flottante ont pour objectif de borner l'erreur dans le pire cas. Des travaux récents ont montré que cette analyse peut être dépourvue de sens pour des systèmes qui évoluent pendant un très long laps de temps comme on en trouve couramment dans l'industrie. Un exemple de ce type ajoute des nombres entre -1 et 1 avec une erreur de mesure de $\pm 2^{-25}$. Si ce processus ajoute 2^{25} nombres, l'erreur accumulée peut atteindre ± 1. Malheureusement, un vol de 10 heures avec une fréquence d'échantillonnage de 1 kHz engendre environ 2^{25} échantillons. D'un autre coté, il semble évident que l'erreur accumulée observée sera beaucoup plus faible pourvu que ces erreurs ne soient pas corrélées.

Nous revenons dans la section 2 sur une théorie générique sur les probabilités [12] et les compléments concrets dont nous avons eu besoin [13]. Nous insistons sur les enseignements que nous avons tirés de ces travaux en ce qui concerne les méthodes formelles, les outils actuellement disponibles et leur bon usage. Il ne s'agit pas là de critiques mais de mises en lumière des difficultés de mise en œuvre d'une théorie conséquente dans les assistants de preuve actuels. Les réponses que ces outils donneront à ces remarques joueront dans leur développement futur. La section 3 présente notre vision d'une chaîne de certification complète d'un système industriel avec en début une analyse formelle *a priori* et en fin des mesures *in situ* sur un code instrumenté dans un simulateur, un prototype ou le produit fini. La

méthode de la seconde partie peut être validée formellement même s'il serait impossible d'en valider les résultats, car ceux-ci seront obtenus par des mesures.

Nous nous concentrons dans ce travail sur l'usage des **méthodes formelles** pour valider le bon fonctionnement de **systèmes hybrides** (logiciel, matériel) devant évoluer pendant **très longtemps** (quelques milliards d'opérations) et dont la probabilité d'échec doit rester **infime** (un pour quelques milliards). Des outils existent déjà pour étudier des systèmes dont l'une de ces contraintes serait relâchée ou atténuée.

2. Élaboration d'une théorie formelle des probabilités

Notre première constatation est qu'il est dans la pratique impossible de coopérer activement sur une théorie aussi vaste que la théorie de la mesure avec l'intégrale de Lebesgue, les probabilités et les statistiques sans se référencer à un ou plusieurs livres. Ces références [14] permettent de savoir quels théorèmes sont démontrés, quels théorèmes ont été écartés (pour quelles raisons), et enfin quels théorèmes vont être démontrés dans un futur proche. Ce besoin de recourir à des références communes n'est pas fondé sur des différences sensibles dans la théorie qui est relativement stable mais sur quelques différences mineures dans les approches.

2.1. Les fondements des probabilités

Si la théorie des probabilités voit le jour avec l'étude des jeux de hasard (Bernoulli, Fermat, Pascal, *etc.*), il faut attendre les années 1930 pour que Kolmogorov donne aux probabilités une axiomatique générale et efficace. Elle est essentiellement basée sur la théorie de la mesure, introduite par Borel et Lebesgue. La vaste majorité des résultats mathématiques en probabilités est établie pour $\mathtt{T}$, $\mathcal{S}$ et $\mathbb{P}$ fixés, dont nous allons voir la signification tout de suite.

En français, on parle pour $\mathtt{T} \neq \emptyset$ de l'univers des possibles ou de l'ensemble des éventualités. L'exemple de la mesure de Lebesgue sur $[0, 1]$ nous indique que l'on ne peut généralement pas définir la mesure de toute partie de $\mathtt{T}$. D'où l'intérêt d'introduire la notion de tribu de référence $\mathcal{S}$, qui répertorie la classe des « événements autorisés » parmi les sous-ensembles de $\mathtt{T}$. Lorsqu'on munit l'univers $\mathtt{T}$ d'une telle tribu $\mathcal{S}$, on obtient un espace mesurable ou *probabilisable*. Cet espace peut ensuite devenir un espace probabilisé (de référence) si l'on y adjoint une mesure de probabilité $\mathbb{P}$. Cette dernière est une fonction particulière définie sur $\mathcal{S}$, qui vérifie les axiomes d'une mesure, plus la propriété $\mathbb{P}(\mathtt{T}) = 1$, ce qui est conforme à notre intuition.

Le terme « espace probabilisable » est mathématiquement un synonyme d'« espace mesurable », mais il ajoute une connotation très utile en pratique. Un espace probabilisable est un espace mesurable susceptible d'être muni d'une mesure toute particulière, une probabilité. Toutefois ce terme supplémentaire n'a pas d'équivalent en anglais.

La notation $(\mathtt{T}, \mathcal{S}, \mathbb{P})$ pour l'espace probabilisé de référence ne correspond pas aux habitudes des mathématiciens français. $\mathtt{T}$ est l'initiale du terme anglais Type souvent utilisé en méthodes formelles pour qualifier un ensemble arbitraire et $\mathcal{S}$ est l'initiale de "sigma-algebra" qui correspond à notre tribu nationale. Nous adoptons ces notations afin de faciliter les échanges entre ce rapport et les travaux dans les assistants de preuve auxquels nous faisons référence [12, 13].

Ce cadre abstrait permet de modéliser toutes les expériences aléatoires, qu'elles soient quantitatives ou qualitatives. Chaque élément de $\mathtt{T}$ représente un résultat possible de l'expérience considérée, de sorte que le déroulement de l'expérience aléatoire revient à tirer au sort un élément ω de $\mathtt{T}$. Par la suite, un événement E est une partie mesurable de $\mathtt{T}$ ($E \in \mathcal{S}$) où $\mathbb{P}$ est définie ($E \in \mathrm{Dom}(\mathbb{P})$). On dit que x réalise un événement si x est dans E. Ainsi, le vide est l'événement impossible, tandis que $\mathtt{T}$ est l'événement certain.

Quand $\mathtt{T}$ est fini ou dénombrable ($\mathtt{T} = \mathbb{N}$), on choisit souvent $\mathcal{S} = \mathcal{P}(\mathtt{T})$. On constate alors que toutes les fonctions définies sur $\mathtt{T}$ sont des variables aléatoires, c'est-à-dire des applications mesurables. Elles sont discrètes en ce sens que leur image est au plus dénombrable. Elle ne sont toutefois pas forcément intégrables.

Le deuxième cas fondamental d'espace probabilisable est un espace topologique arbitraire $\mathtt{T}$ muni de sa tribu borélienne associée. Cette dernière tribu, notée $\mathcal{B}(\mathtt{T})$, est tout simplement la tribu engendrée par les ouverts de $\mathtt{T}$. Dans le cas général, $(\mathtt{T}, \mathcal{S}, \mathbb{P})$ est abstrait et inconnu. En pratique, $\mathtt{T}$ est envoyé dans $\mathbb{R}$ voire $\mathbb{R}^n$ par les variables aléatoires que l'on étudie, puis on raisonne systématiquement sur les espaces probabilisables d'arrivée, typiquement $(\mathbb{R}^n, \mathcal{B}(\mathbb{R}^n))$.

On retrouve dans l'ensemble des livres de cours cette présentation avec deux branches selon que $\mathtt{T}$ est au plus dénombrable ou $\mathtt{T}$ est arbitraire. Cela tend à faire croire qu'elle est essentielle, ce qui pose un problème de « typage » dans PVS lorsque l'on veut énoncer des théorèmes sur des vecteurs de variables aléatoires dont certaines sont discrètes et d'autres sont continues. La solution *classique* à ce problème consiste à mettre en place deux types de variables aléatoires, le premier pour les variables discrètes et le second pour les variables continues. Cette solution n'est pas satisfaisante parce qu'elle exclut de fait toute autre type de variable aléatoire, sauf à énoncer un nouveau théorème et à en faire la preuve.

Il est vrai que ce problème est plus ardu avec l'outil de preuve PVS qu'avec d'autres outils. Toutefois, la distinction entre variables définies sur un espace discret et variables aléatoires arbitraires est purement pédagogique car $\mathcal{B}(\mathbb{R})$ est beaucoup plus difficile à appréhender que $\mathcal{P}(\{1 \cdots N\})$. Dans les faits, l'ensemble des théorèmes considérés [12, 13] sont énoncés pour $\mathtt{T}$, $\mathcal{S}$ et $\mathbb{P}$ fixés. En pratique nous utilisons $\mathtt{T} = \mathbb{R}$ et $\mathcal{S} = \mathcal{B}(\mathbb{R})$ pour prendre en compte à la fois les variables discrètes et les variables continues.

Les travaux que nous venons de présenter [12] permettent de définir formellement les probabilités. Les travaux que nous allons maintenant présenter [13] permettent de borner formellement les probabilités d'événements par des formules jusqu'à obtenir des valeurs numériques.

2.2. Les aspects concrets

Une théorie de l'espérance est intrinsèquement liée à une théorie de l'intégrale de Lebesgue. On peut définir l'espérance comme étant l'unique opérateur linéaire croissant $\mathbb{E}$ sur l'ensemble des variables aléatoires $\mathbb{P}$-integrables qui vérifie la propriété de Beppo-Lévy et tel que $\mathbb{E}(\chi_A) = \mathbb{P}(A)$ pour tout $A \in \mathcal{S}$. Dans la pratique, il n'est pas utile de démontrer que $\mathbb{E}$ est unique et l'on peut prendre la définition suivante, basée sur l'intégrale de Lebesgue, quand la quantité considérée existe dans $\mathbb{R}$:

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

L'effort de migration des résultats sur l'intégrale de Lebesgue, parmi lesquels on trouve le théorème de Fubini, dans une théorie de l'espérance devrait être minime. Une liaison entre l'intégrale de Lebesgue et l'intégrale de Riemann s'avère aussi nécessaire pour valider des calculs d'intégrales. Un des premiers résultats de l'espérance non directement importé de la théorie de l'intégrale de Lebesgue est l'inégalité de Markov.

Théorème 1 (Inégalité de Markov). *Pour toute variable aléatoire X et toute constante ϵ,*

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

Le lemme suivant est nécessaire à l'établissement de l'inégalité de Hoeffding et sa preuve reste somme toute assez élémentaire. Comme toute théorie mathématique, la théorie de l'espérance fait rapidement intervenir des nombreux résultats éparpillés dans plusieurs théories mathématiques comme

ici le théorème de Taylor sur la fonction exponentielle. La difficulté n'est donc pas de mettre en place des raisonnements compliqués mais de mettre en oeuvre des résultats partiels provenant de théories variées.

Théorème 2. *On définit quand elle existe, la fonction génératrice* $M_X(t) = \mathbb{E}\left(e^{tX}\right)$ *pour toute variable aléatoire* X*, et on vérifie que si* X *est bornée avec* $\mathbb{P}(a \leq X \leq b) = 1$ *et* $\mathbb{E}(X) = 0$*, alors*

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

Il faut ensuite se garder de définir l'indépendance de deux variables aléatoires. La définition pour deux variables se déduit facilement d'une définition générale pour n variables, mais on ne peut pas faire l'inverse. Nous développons un exemple dans ce sens.

On considère deux lancers successifs d'un même dé non truqué. On note X_1 le résultat du premier lancer et X_2 celui du deuxième. On calcule $X_3 = X_1 + X_2$. Nous introduisons les 3 événements suivants pour montrer que ces 3 variables aléatoires ne sont pas indépendantes :

$$A_i = [X_i \text{ est impair}], \text{ pour tout } i \in \{1,2,3\}.$$

On vérifie ensuite que

$$\begin{cases} \mathbb{P}(A_1) = \mathbb{P}(A_2) = \mathbb{P}(A_3) & = & 1/2, \\ \mathbb{P}(A_1 \cap A_2) = \mathbb{P}(A_1 \cap A_3) = \mathbb{P}(A_2 \cap A_3) & = & 1/4, \end{cases}$$

et

$$\begin{cases} \mathbb{P}(A_1 \cap A_2) = \mathbb{P}(A_1) \times \mathbb{P}(A_2), \\ \mathbb{P}(A_1 \cap A_3) = \mathbb{P}(A_1) \times \mathbb{P}(A_3), \\ \mathbb{P}(A_2 \cap A_3) = \mathbb{P}(A_2) \times \mathbb{P}(A_3), \end{cases}$$

ce qui prouve que ces événements sont deux-à-deux indépendants. Mais $A_1 \cap A_2 \cap A_3 = \varnothing$ et

$$\mathbb{P}\left(\bigcap_{i=1}^{3} A_i\right) = 0 \neq \frac{1}{8} = \prod_{i=1}^{3} \mathbb{P}(A_i).$$

Revenons formellement sur la définition de l'indépendance d'une suite finie $(X_i)_{1 \leqslant i \leqslant n}$ de n variables aléatoires. Elles sont indépendantes si et seulement si $\left(X_i^{-1}(B_i)\right)_{1 \leqslant i \leqslant n}$ est une famille d'événements mutuellement indépendants pour toute famille de boréliens $(B_i)_{1 \leqslant i \leqslant n} \in (\mathcal{B}(\mathbb{R}))^n$.

Cela signifie que l'égalité suivante est satisfaite pour toute sous-famille $\left(A_{i_j}\right)_{1 \leqslant j \leqslant m}$ de $(A_i)_{1 \leqslant i \leqslant n}$ en posant $A_i = X_i^{-1}(B_i)$ pour chaque i :

$$\mathbb{P}\left(\bigcap_{j=1}^{m} A_{i_j}\right) = \prod_{j=1}^{m} \mathbb{P}\left(A_{i_j}\right).$$

Notons que l'on a $2 \leqslant m \leqslant n$.

Certains livres utilisent une définition légèrement différente de la notion d'indépendance de n variables aléatoires. Notre définition nous force à considérer l'image réciproque d'un sous-ensemble et à bien distinguer éventualité, événement et tribu (on parle de *sauts cantoriens*). Ainsi, on doit écrire $X(t)$ ou $\mathbb{P}(\{t\})$ car une variable aléatoire X est une fonction définie sur $\mathtt{T}$ et $\mathbb{P}$ est définie sur $\mathcal{S}$, une tribu de parties de $\mathtt{T}$. Enfin $A = X^{-1}(B)$ correspond à un événement.

Afin de simplifier la présentation de l'indépendance tout en restant parfaitement rigoureux, de nombreux livres remplacent les images inverses d'éléments de $\mathcal{S}$ dans la définition précédente par des sections $\{X \leq x\}$. Cette simplification est justifiée par l'étude du système de Dynkin engendré par ces

sections, elle reste toutefois uniquement motivée par la pédagogie. Son implantation dans un système formel correspondrait à un travail supplémentaire important qui s'avère inutile.

Le dernier point pour retrouver l'ensemble des propriétés de l'intégrale de Lebesgue consiste à définir la loi $\mathbb{P}_X$ associée à une variable aléatoire X. Nous établissons ensuite un théorème de transfert avec uune fonction f de $\mathtt{T}$ dans $\mathtt{T}'$ pour arriver à :

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

3. Borne quasi-certaine sur l'accumulation d'erreurs infimes

Nous présentons ici l'architecture générale d'une chaîne de certification du bon fonctionnement de systèmes hybrides (logiciel, matériel) quand l'analyse au pire cas n'aboutit pas ou aboutit à des bornes trop importantes pour certifier le bon fonctionnement du logiciel.

Comme dans l'analyse au pire cas [15], on associe un label ℓ à chaque opération apparaissant dans le texte du programme. Le label définit l'opération. Celle-ci pouvant être exécutée plusieurs fois, comme par exemple si l'opération apparaît dans une boucle, on indice les exécutions avec une seconde variable i. Cette construction nous permet d'introduire la variable intermédiaire $x_{\ell,i}$ qui stocke le résultat de la $i$ème exécution de l'opération indiquée par le label ℓ. La variable d'erreur d'arrondi $X_{\ell,i}$ stocke l'erreur individuelle introduite quand cette opération n'est pas exacte.

Nous cherchons la différence cumulée entre une quantité x_{ℓ_0,i_0} manipulée par le programme et la quantité $\overline{x}_{\ell_0,i_0}$ mathématiquement considérée en supposant que le programme n'introduit pas d'erreurs d'arrondi. Nous écartons les problèmes liés au contrôle du flot de programme (tests et branchements) et nous utilisons au besoin des théorèmes de Taylor. Cette différence peut s'écrire sous la forme

$$x_{\ell_0,i_0} - \overline{x}_{\ell_0,i_0} = \sum_{\ell} \sum_{i} \kappa_{\ell,i} X_{\ell,i} + E$$

où l'expression des $\kappa_{\ell,i}$ ne fait pas apparaître d'opérations arrondies et E représente les erreurs d'ordre supérieur. Cela signifie que les $\kappa_{\ell,i}$ peuvent être définis uniquement à partir des $\overline{x}_{\ell,i}$ et E est une somme ou une série de termes contenant des facteurs $X_{\ell_1,i_1} X_{\ell_2,i_2}$ pour des ℓ_1, ℓ_2, i_1 et i_2 variés.

Notre chaîne de certification se concentre sur le cas où l'analyse au pire cas de $x_{\ell_0,i_0} - \overline{x}_{\ell_0,i_0}$ aboutit à des bornes trop grandes pour garantir que le programme prenne les bonnes décisions et effectue des actions suffisamment précises. Elle opère en deux étapes. La première étape consiste à fournir une borne quasi-certaine sur $x_{\ell_0,i_0} - \overline{x}_{\ell_0,i_0}$ sous des hypothèses raisonnables. La seconde étape consiste à valider les hypothèses par l'observation.

La première étape peut être entièrement certifiée par les méthodes formelles. L'inégalité de Lévy que nous présentons en premier pour cette étape peut être facilement vérifiée par un outil formel et la théorie que nous avons présentée à la section précédente. L'inégalité de Doob est plus puissante mais elle nécessite des moyens théorique qui ne sont pas encore disponibles dans les outils formels.

Le résultat de la seconde étape ne peut pas être certifié car il est basé sur des observations. Nous pouvons par contre en certifier la méthode en validant l'inégalité de Hoeffding et le test de Kolmogorov-Smirnov dans les outils formels. Ces tests étant relativement légers, ils peuvent être implantés dans un simulateur, dans un prototype ou sur le produit final.

3.1. Première étape — Établissement d'une borne quasi-certaine

Nous ne traitons que les longues accumulations par une approche probabiliste. Les autres quantités sont bornées par l'analyse du pire cas. Dans la différence $x_{\ell_0,i_0} - \overline{x}_{\ell_0,i_0}$, nous cherchons donc à établir

des inégalités quasi-certaines

$$\left|\sum_i \kappa_{\ell,i} X_{\ell,i}\right| \leq \epsilon_\ell$$

pour un ℓ fixé dans le cas où $D_{\ell,i}$ ne dépend pas de i_0. Dans la suite nous omettons la référence à ℓ et afin de simplifier notre exposé, nous remplaçons $\kappa_i X_i$ par X_i et X_i par $X_i - \mathbb{E}(X_i)$ si X_i n'est pas centré.

Les outils d'analyse supposent souvent que l'on puisse borner toutes les sommes préfixes $S_i = \sum_{j=1}^{i} X_j$ pour $i \leq n$. Le but de cette première étape est donc de trouver une borne ϵ telle que $\mathbb{P}\left(\max_{1\leqslant i\leqslant n}(|S_i|) \geqslant \epsilon\right)$ soit infime en supposant que les variables X_i sont indépendantes. L'inégalité de Doob-Kolmogorov a fourni un premier résultat [12] pour des X_i indépendants et identiquement distribués,

$$\mathbb{P}\left(\max_{1\leqslant i\leqslant n}(|S_i|) \geqslant \epsilon\right) \leqslant \frac{n\mathbb{E}(X_i)}{\epsilon^2}.$$

Cette inégalité peut être obtenue par des manipulations simples sur la variance mais elle est limitée aux moments d'ordre 2. Nous présentons maintenant l'inégalité de Lévy qui permet de traiter des moments de tout ordre pour obtenir des bornes plus précises.

Théorème 3 (Inégalité de Lévy). *Si les $\{X_n\}$ sont indépendants et symétriques, alors la propriété suivante est vraie pour toute constante positive ϵ.*

$$\mathbb{P}\left(\max_{1\leqslant i\leqslant n}(|S_i|) \geqslant \epsilon\right) \leqslant 2\mathbb{P}\left(|S_n| \geqslant \epsilon\right)$$

On peut se passer de l'hypothèse de symétrie sur les variables en utilisant l'inégalité de Doob à la place de l'inégalité de Lévy mais la preuve de celle-ci fait intervenir des manipulations complexes sur les martingales et les sous-martingales [16]. L'inégalité de Jensen permet même d'étudier des sous-martingales plus élaborées que $|S_i^{2k}|$. Ces deux résultats semblent toutefois bien au delà des zones accessibles avec l'arsenal théorique actuellement implanté dans les assistants de preuve.

Nous utilisons l'inégalité de Markov pour $X = S_n^k$,

$$\mathbb{P}\left(|S_n| \geqslant \epsilon\right) = \mathbb{P}\left(|S_n^k| \geqslant \epsilon^k\right) \leqslant \frac{\mathbb{E}\left(|S_n^k|\right)}{\epsilon^k},$$

et nous nous concentrons sur $k = 4$.

Afin de fixer les esprits, nous allons supposer que les variables X_i sont uniformément réparties dans l'intervalle $[-u, u]$. On vérifie aisément que :

$$\mathbb{E}\left(X_i^p\right) = \frac{1}{2u}\int_{-u}^{u} x^p dx = \frac{1}{2u}\left[\frac{x^{p+1}}{p+1}\right]_{-u}^{u} = \frac{u^p}{2(p+1)}.$$

Les propriétés de l'espérance nous indiquent que

$$\begin{aligned}
\mathbb{E}\left(|S_n^4|\right) &= \mathbb{E}\left(S_n^4\right) = \mathbb{E}\left(\left(\sum_{i=1}^{n} X_i\right)^4\right) = \mathbb{E}\left(\sum_{i,j,k,l=1}^{n} X_i X_j X_k X_l\right) \\
&= \sum_{i,j,k,l=1}^{n} \mathbb{E}\left(X_i X_j X_k X_l\right) = \sum_{i=1}^{n} \mathbb{E}\left(X_i^4\right) + \sum_{i,j=1 \text{ et } i\neq j}^{n} \mathbb{E}\left(X_i^2 X_j^2\right) \\
&= \frac{nu^4}{10} + \frac{n(n-1)u^4}{18}
\end{aligned}$$

Afin de vérifier la validité de notre approche, nous instancions les variables à $n = 2^{30}$ et $u = 2^{-25}$. La contrainte

$$\mathbb{P}\left(\max_{1\leqslant i\leqslant n}(|S_i|)\geqslant\epsilon\right)\leqslant 2^{-30},$$

implique alors

$$2\left(\frac{n}{10}+\frac{n(n-1)}{18}\right)\frac{u^4}{\epsilon^4}\leqslant 2\times\frac{2^{60}\times 2^{-100}}{2^4\times\epsilon^4}\leqslant 2^{-30}\qquad\text{et}\qquad\sqrt[4]{2^{-13}}=2^{-3,25}\leqslant\epsilon.$$

Cela signifie qu'un peu plus de 3 chiffres sont significatifs pour des nombres en simple précision compris entre -1 et 1. Cela peut être suffisant. Dans le cas contraire, il faut utiliser un moment d'ordre supérieur avec une formule basée sur la formule du binôme.

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

Cette propriété est d'abord prouvée par récurrence sur n pour tout m avant d'être appliquée à $m = 2k$.

3.2. Deuxième étape — Vérification des hypothèses

Déterminer analytiquement la distribution de X_i est en pratique impossible sur un code de taille raisonnable. Notons toutefois que les inégalités de Lévy et Doob ne sont basées que sur les moments. Il suffit donc en pratique de vérifier les bornes utilisées dans l'étape précédente pour valider le recours à l'inégalité de Lévy ou Doob. C'est le propos de l'inégalité de Hoeffding [17].

Théorème 4 (Inégalité de Hoeffding). *Si les X_n sont indépendants et bornés avec $\mathbb{P}(a_i \leq X_i \leq b_i) = 1$ alors*

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

Nous calculons E_1, E_2 et E_4 moyennes empiriques de X_i, X_i^2 et X_i^4 et nous simplifions cette inégalité avec l'hypothèse que les X_i sont bornés uniformément en valeur absolue par c. Il s'ensuit que

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

Ces quantités entrent uniquement en jeu dans la qualité de la majoration de l'étape précédente. Ainsi $\epsilon = 0,25$ semble tout à fait acceptable en supposant que toutes les valeurs ont été normalisées entre -1 et 1. Il s'ensuit que pour garder une probabilité infime d'échec, c'est à dire de l'ordre de 2^{-30}, il suffit de calculer les moyennes empiriques sur 1000 valeurs.

D'un point de vue formel, nous avons fini la validation de notre chaîne en vérifiant empiriquement les hypothèses de nos théorèmes avec une probabilité d'échec infime. Nous utilisons toutefois l'instrumentation du code pour vérifier son bon fonctionnement d'un point de vue statistique.

Les erreurs sont produites par des opérations à virgule flottante ou à virgule fixe. On représente un nombre à virgule flottante par $v = m \times 2^e$ où e est l'exposant et m est la mantisse [18]. La norme IEEE 754 [19] utilise la notation signe-valeur absolue pour la mantisse et le premier bit de la mantisse b_0 est implicite dans la plupart des cas ($b_0 = 1$). On aboutit à la définition suivante où s et les b_i sont des bits (0 ou 1).

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

Certains circuits comme le TMS320 [20] sont utilisés dans des logiciels critiques et ont recours au complément à 2 pour la mantisse et à la définition suivante.

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

En notation à virgule fixe, e est une constante fournie par le système et b_0 ne peut être forcé à 1.

Pour tout nombre représentable v, nous définissons la fonction *unit in the last place*

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

où e est l'exposant de v que nous venons juste de définir.

Il paraît normal que les erreurs d'arrondi soient distribuées uniformément dans l'intervalle $[-\mathrm{ulp}/2, \mathrm{ulp}/2]$ du résultat. Similairement l'arrondi de représentation [21] d'une distribution logarithmique comme celle observée pour les constantes naturelles [22, p. 254-264] converge très vite vers une distribution uniforme. Toute autre situation indique que l'arrondi peut éventuellement détruire plus d'information que prévu.

Un exemple pour s'en convaincre. Dans l'addition à virgule flottante de deux nombres où l'un est beaucoup plus petit que l'autre, l'erreur d'arrondi est exactement celui-ci. Si ce phénomène se produit systématiquement dans un programme, on observera que l'erreur d'arrondi n'est pas répartie uniformément dans l'intervalle $[-\mathrm{ulp}/2, \mathrm{ulp}/2]$ du résultat mais suit plutôt la loi de la plus petite variable. Cela ne signifie pas que le code est erroné. Cela signifie toutefois que le programme calcule une quantité sans en tenir compte par la suite. Cette situation mérite d'être signalée aux concepteurs du programme.

Les paramètres a et b de la distribution peuvent être estimés à partir de bornes empiriques,

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

Comme elles sont biaisées

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

nous les corrigeons

$$\overline{I}_n = \frac{n}{n-1} I_n - \frac{1}{n-1} M_n \qquad \text{et} \qquad \overline{M}_n = \frac{n}{n-1} M_n - \frac{1}{n-1} I_n.$$

Nous voulons maintenant savoir si nous pouvons supposer que la distribution empirique correspond bien à une distribution uniforme entre a et b. Nous construisons virtuellement la distribution empirique $F_n(x)$ en triant les valeurs observées dans une queue de priorité,

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

Théorème 5. *Si les X_n sont identiquement distribuées à X_0, alors $\sqrt{n}\,\|F_n - F_0\|_\infty$ converge en loi vers une loi fixe caractérisée par sa fonction de répartition,*

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

Le problème général de test est :

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

Sous l'hypothèse (H_0), les X_n sont de loi uniforme sur $[a, b]$ et la réponse au test est assez intuitive, on acceptera l'hypothèse nulle si la statistique

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

prend des valeurs faibles ; la région critique du test est donc $W = \{(x_1, x_2, \ldots, x_n) \ / \ K_n > c\}$ avec $\alpha = \mathbb{P}(W)$ et l'erreur α de première espèce (rejeter (H_0) alors qu'elle est vraie) satisfait

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

$c\sqrt{n}$ est donc le fractile d'ordre $1-\alpha$ de la fonction de répartition asymptotique R de $\sqrt{n}\, K_n$. Pour $\alpha = 0,05$ ou $\alpha = 0.01$ la loi asymptotique de a été tabulée [23, 24] ; lorsque $n > 100$, $c = 1,63/\sqrt{n}$ pour $\alpha = 0.01$ et $c = 1.36/\sqrt{n}$ pour $\alpha = 0,05$.

4. Perspectives et conclusions

Nous venons de présenter une solution concrète à un problème concret dans la certification formelle de logiciels sûrs comme ceux utilisés dans les avions et les centrales nucléaires. Cette solution novatrice est à notre connaissance la seule fondée sur une théorie appropriée à l'obtention du niveau d'évaluation maximal (EAL7) dans les critères communs pour la sécurité des systèmes d'information. La chaîne de certification que nous proposons est similaire aux travaux présentés par deux projets ayant atteint ce niveau d'évaluation [25, 26].

Notre chaîne de certification valide les hypothèses nouvelles que nous avons ajoutées afin d'utiliser les théorèmes de Lévy ou Doob. Nous n'avons pas encore attaqué l'hypothèse classique de l'indépendance des erreurs créées. La littérature en la matière est vaste et basée sur le test du χ^2. La complexité du test augmente très vite. Elle est de l'ordre de $\prod p_i$ où p_i est le nombre de classes distinguées pour le caractère i. Le choix des modèles de panne est donc crucial. L'approche que nous avons mis en place pour ce travail peut toutefois être étendu et donner des résultats quasi-certains quand les pannes qui se produisent appartiennent toutes à un petit nombre de pannes prises en compte.

Une autre de nos contribution a été de proposer une feuille de route constituée d'un petit nombre de résultats de probabilité et de statistique, pouvant être prouvés de façon élémentaire afin de résoudre complètement un problème concret. Il s'agit là d'une contribution importante en regard de l'énorme corpus mathématique accumulé dans ces deux domaines. Certains résultats que nous utilisons n'ont été publiés que dans la deuxième moitié du XXème siècle et ne sont mentionnés dans des livres de cours qu'au XXIème siècle.

Les enseignements concernant les méthodes formelles, leurs outils et leur bon usage sont déjà nombreux et recoupent ceux exprimés par d'autres communautés sur d'autres problèmes. Des solutions sont en cours de mise en place et d'exploitation et nous comptons nous associer à un groupe travaillant sur ce sujet pour voir en quel sens leurs solutions correspondent à ce que nous cherchons et quels sont éventuellement les points qu'il restent à développer.

Remerciements

Ce travail est partiellement financé par le projet EVA-Flo de l'ANR.

Références

[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, p. 148–200, 1998.

[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 et S. D. Johnson, éds), (Austin, Texas), p. 217–233, 2000.

[3] S. Boldo et M. Daumas, « Representable correcting terms for possibly underflowing floating point operations », *in Proceedings of the 16th Symposium on Computer Arithmetic* (J.-C. Bajard et M. Schulte, éds), (Santiago de Compostela, Spain), p. 79–86, 2003.

[4] M. Daumas, G. Melquiond et C. Muñoz, « Guaranteed proofs using interval arithmetic », *in Proceedings of the 17th Symposium on Computer Arithmetic* (P. Montuschi et E. Schwarz, éds), (Cape Cod, Massachusetts), p. 188–195, 2005.

[5] C. Muñoz et D. Lester, « Real number calculations and theorem proving », *in 18th International Conference on Theorem Proving in Higher Order Logics*, (Oxford, England), p. 239–254, 2005.

[6] J. Hurd, *Formal verification of probabilistic algorithms*. Thèse doctorat, University of Cambridge, 2002.

[7] P. Audebaud et C. Paulin-Mohring, « Proofs of randomized algorithms in Coq », *in Proceedings of the 8th International Conference on Mathematics of Program Construction* (T. Uustalu, éd.), (Kuressaare, Estonia), p. 49–68, 2006.

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

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

[10] G. Huet, G. Kahn et C. Paulin-Mohring, *The Coq proof assistant : a tutorial : version 8.0*, 2004.

[11] S. Owre, J. M. Rushby et N. Shankar, « PVS : a prototype verification system », *in 11th International Conference on Automated Deduction* (D. Kapur, éd.), (Saratoga, New-York), p. 748–752, Springer-Verlag, 1992.

[12] M. Daumas et 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), p. 7 p, 2007.

[13] M. Daumas, D. Lester, É. Martin-Dorel et A. Truffert, « Stochastic formal methods for hybrid systems », Rap. tech. hal-00107495, Centre pour la Communication Scientifique Directe, Villeurbanne, France, 2008.

[14] S. K. Berberian, *Fundamentals of Real Analysis*. Springer, 1999.

[15] M. Martel, « Semantics of roundoff error propagation in finite precision calculations », *Higher-Order and Symbolic Computation*, vol. 19, no. 1, p. 7–30, 2006.

[16] J. Neveu, éd., *Martingales à temps discret*. Masson, 1972.

[17] W. Hoeffding, « Probability inequalities for sums of bounded random variables », *Journal of the American Statistical Association*, vol. 58, no. 301, p. 13–30, 1963.

[18] D. Goldberg, « What every computer scientist should know about floating point arithmetic », *ACM Computing Surveys*, vol. 23, no. 1, p. 5–47, 1991.

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

[20] Texas Instruments, *TMS320C3x — User's guide*, 1997.

[21] A. Feldstein et R. Goodman, « Convergence estimates for the distribution of trailing digits », *Journal of the ACM*, vol. 23, no. 2, p. 287–297, 1976.

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

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

[24] 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, p. 425–441, 1952.

[25] Schlumberger, « Schlumberger leads the way in smart card security with common criteria EAL7 security methodology ». Press Releases, 2003.

[26] Rockwell Collins, « Rockwell Collins receives MILS certification from NSA on microprocessor ». Press Releases, 2005.