LOGIQUE & CALCUL

L'impossible hasard

Depuis les premiers dés, il y a trois millénaires, l'homme imagine et fabrique des objets pour produire du hasard. A-t-il réussi ?

Jean-Paul DELAHAYE

La nouvelle de Jorge Luis Borges intitulée *La loterie à Babylone* se déroule dans l'antique Mésopotamie. Cette loterie distribue des lots aux gagnants et, forte de son succès, se diversifie en prenant une importance grandissante. On y gagne et l'on y perd toutes sortes de biens matériels ; elle intervient dans les décisions familiales, sociales et politiques : elle vous envoie en prison, fait de vous un ministre, fixe le sort de vos enfants, etc. Elle évolue à nouveau, pour devenir cachée et obligatoire. Finalement, plus personne ne sait ce qu'elle décide pour les gens et les choses et l'on doute même de son existence !

Ce hasard, que Borges imagine, joue avec nous à chaque instant. Que savons-nous de lui ? Avons-nous la capacité de le produire et sommes-nous certains que ce que nous croyons être du hasard l'est réellement ?

Ces questions sont importantes pour assurer que les loteries et les jeux sont équitables. Elles sont essentielles quand nous voulons mener des simulations et cruciales pour la mise en œuvre des méthodes mathématiques de calcul de type Monte-Carlo où la justesse et la précision du résultat dépendent de la qualité du hasard utilisé ou de certaines propriétés du pseudo-hasard mis en œuvre (voir l'article de Brian Hayes dans *Pour la Science* de décembre 2011). Enfin, en cryptographie, le hasard est au cœur de nombreuses méthodes, dont la résistance aux attaques est liée à sa plus ou moins grande perfection.

Nous aborderons ici le hasard de la physique et particulièrement celui des lancers de pièces et des dispositifs quantiques.

Tests, compression et prédiction

La théorie des probabilités contourne le problème de la définition du hasard en raisonnant sur l'ensemble des cas possibles – par exemple les six faces d'un dé – sans indiquer ce qu'est une suite aléatoire de lancers de dé ou de pile ou face. En fait, définir ce qu'est une suite aléatoire a longtemps semblé impossible. En 1965, le Suédois Per Martin-Löf a proposé une définition : une suite infinie de 0 et de 1 est aléatoire lorsqu'elle passe tous les tests statistiques raisonnables. Cette idée a été acceptée

Forum de la détection

Roulette Poker Shop

1. Les procédés physiques macroscopiques

Les moyens physiques pour engendrer le « hasard » sont nombreux... et pas toujours équitables. On retrouve périodiquement lors de fouilles des dés romains *(à gauche en bas de la page ci-contre)*. Les mêmes dés sont utilisés dans le jeu de Craps des pays anglo-saxons. Les roues de loterie où l'on pouvait gagner des kilos de sucre attiraient les badauds des années 1950 qui avaient été privés de sucre pendant la Seconde Guerre mondiale (on notera l'escroquerie de l'épaisseur des bandes de gain des gros montants de kilos de sucre).

La roulette et sa variante la boule sont les instruments du casino. Le rééquilibrage des roues et les plots que heurtent la bille lors de sa descente augmentent la sensibilité aux conditions initiales.

Les machines à sous, dénommées parfois bandits manchots, ont été inventées à San Francisco par Charles Fey vers 1890. Deux méthodes différentes sont utilisées pour engendrer le hasard. Dans un premier temps, le mécanisme à produire du hasard était macroscopique et déterministe : la force avec laquelle on lançait les roues (initialement il y en avait trois) en tirant sur le bras de la machine déterminait le résultat. Le mécanisme était conçu pour qu'aucun contrôle précis ne soit possible et la machine était assimilable à une loterie ou à une roulette de casino enfermée dans une boîte. Bien sûr, des trucages mécaniques favorisant certaines combinaisons étaient possibles.

À partir des années 1960, ces machines sont devenues électroniques : un générateur algorithmique pseudo-aléatoire produit plusieurs dizaines de fois par seconde des chiffres sans jamais s'arrêter. Ces chiffres sont effacés de ses mémoires et ce n'est qu'au moment où l'utilisateur joue (en appuyant sur un bouton ou en tirant le bras de la machine) que les derniers chiffres produits sont exploités. Ils déterminent alors une combinaison qui est affichée sur l'écran de la machine (après un délai et une animation factices) et qui fixe le résultat du jeu, provoquant, lorsque c'est nécessaire, la chute d'une quantité de pièces.

Ce procédé est-il convenable ? Si on exclut les tricheries passant inaperçues aux yeux des organismes officiels chargés de contrôler les machines, le procédé est satisfaisant aussi bien pour les joueurs que pour les propriétaires des machines.

D'une part, le propriétaire peut choisir la machine qu'il veut (ou plus tard la modifier en changeant certains composants électroniques) pour que le pourcentage d'argent redonné en moyenne aux joueurs soit celui qu'il décide (en général entre 75 % et 99 %). Ce pourcentage sert parfois d'argument publicitaire. Il peut aussi choisir une machine qui donne souvent de petits lots et rarement des gros, ou le contraire (cela tout en respectant le pourcentage d'argent redonné en moyenne aux joueurs et fixé à l'avance).

D'autre part, une fois la machine fermée, personne ne peut tricher. Personne n'a d'informations sur l'état du générateur pseudo-aléatoire qui tourne en continu et, de plus, le geste du joueur n'est pas assez précis pour qu'il contrôle l'instant où il joue.

Le fait que ce mode de fonctionnement soit convenable pour tous ne signifie pas que le processus général du jeu produit des suites aléatoires au sens fort. En interne, il n'y a pas d'aléa puisque ce qui se passe est algorithmique. Quant au joueur, il se peut qu'il appuie inconsciemment d'une manière régulière. Rien n'assure donc que les suites de résultats d'une machine de casino soient aléatoires au sens de Martin-Löf.

Watling Rol-A-Top

The Gamble Gurus

2. Les algorithmes

Une multitude de méthodes ont été imaginées et mises en œuvre en informatique pour engendrer rapidement des suites pseudo-aléatoires. Avant de les utiliser, on vérifie qu'elles passent les batteries de tests comme celles du NIST *(National Institute of Standards and Technology)*. Il faut distinguer deux types de méthodes algorithmiques :

Les méthodes rapides

Exemple : Les générateurs congruentiels linéaires.

Trois entiers positifs a, b et c étant fixés et x_0 un entier initial choisi (on parle de germe, ou de graine), on calcule :

$$x_{n+1} = a\,x_n + b \bmod c,$$

Cela donne une suite de nombres entiers compris entre 0 et $c - 1$, dont on extrait (en les écrivant en binaire) une suite de bits 0 ou 1.

C'est la méthode la plus courante. Si les paramètres sont bien choisis, elle donne des résultats acceptables, sauf pour les usages cryptographiques, car, connaissant quelques points de la suite, on peut en déduire assez aisément les suivants.

Les méthodes plus lentes, mais utilisables en cryptographie.

Exemple : L'algorithme BBS de Leonore et Manuel Blum et Michael Shub.

On se donne un entier positif : M et une graine x_0, et on calcule

$$x_{n+1} = x_n^2 \bmod M$$

dont on ne retient que la parité (0 si on a un nombre pair, 1 sinon).

C'est un peu plus coûteux qu'un générateur congruentiel linéaire, mais, à condition de bien choisir M, on est assuré que la connaissance d'une série de bits ainsi produits ne permet pas de deviner les suivants en un temps raisonnable.

En pratique et selon les usages qu'on veut en faire, on connaît donc aujourd'hui des méthodes satisfaisantes pour engendrer plus ou moins rapidement des bits qui satisferont les batteries de test statistiques *(voir l'encadré 4)*. En revanche, il est certain que ces méthodes, du fait qu'elles se fondent sur des algorithmes déterministes, ne donnent pas des suites aléatoires au sens fort de Martin-Löf.

quand on a montré qu'elle est équivalente à deux idées plus simples : d'une part, qu'une suite est aléatoire si elle est incompressible (impossible à représenter par un programme plus court qu'elle-même) ; d'autre part, qu'une suite est aléatoire si elle est imprévisible, aucun système de pari mécanique ne gagnant contre elle. Cette triple caractérisation mathématique d'une suite infinie aléatoire est un succès scientifique du XX^{e} siècle. Ainsi la suite d'« un milliard de zéros » n'est pas aléatoire, car sa définition, la phrase précédente, est bien plus courte que l'écriture du milliard de zéros de la suite ; la suite des chiffres du nombre π ne l'est pas non plus, car elle se calcule facilement et est donc prévisible.

Le cœur du problème est qu'aucun procédé algorithmique (fondé sur des programmes) ne produira un hasard véritable, car une suite calculée par un algorithme est prédictible, donc non aléatoire. Comme l'informatique n'a pas la capacité de produire du bon hasard, nous nous rabattons sur les suites produites physiquement par des dés, des lancers de pièce de monnaie, des loteries ou des dispositifs quantiques. La question se pose à nouveau : sont-elles aléatoires ?

Pièces, dés et loteries

Bien sûr, on peut tricher et piper un dé en décalant son centre de gravité par rapport au centre géométrique, le forçant à donner presque toujours 6. De même, une roulette de casino peut être déséquilibrée ou avoir des cases de profondeurs inégales qui faussent l'équiprobabilité des numéros. Exploitant cela, plusieurs joueurs auraient fait fortune ; le Britannique Joseph Jagger aurait ainsi empoché l'équivalent de plusieurs centaines de milliers d'euros à Monte-Carlo en 1873.

Peut-on piper de la même façon une pièce de monnaie pour fausser le pile ou face ? La question est intéressante, mais sa réponse exige qu'on distingue les méthodes utilisées pour lancer la pièce.

Si, après avoir lancé la pièce en l'air, vous la rattrapez dans la main (sans manipulation particulière), il semble qu'aucun moyen ne permette de « piper » la pièce. Des expériences avec une pièce dont une face avait été recouverte d'une rondelle de balsa n'ont montré aucun biais en faveur de la face la plus légère ou la plus lourde.

En revanche, plusieurs techniques permettent de fausser l'équilibre des chances à pile ou face. Avec un peu d'entraînement, vous maîtriserez la rotation de la pièce autour de son axe et la rattraperez du côté que vous souhaitez. Si vous la faites tourner comme une toupie sur une surface plane, le tirage sera rarement équitable, car la forme du bord et l'équilibre des masses faussent l'égalité des chances des deux faces. En menant des expériences avec une pièce neuve de deux euros (belge), j'ai trouvé que le côté face était obtenu dans plus de 60 pour cent des cas. Il existerait même des pièces qui, lorsqu'on les fait tourner ainsi, donnent toujours face.

Biais de 51 pour cent

Une étude réalisée en 2007 par Persi Diaconis (le mathématicien illusionniste de l'Université de Stanford), Susan Holmes et Richard Montgomery a établi qu'une pièce de monnaie lancée en la rattrapant après qu'elle a tourné en l'air (sans manipulation délibérée du lanceur) donne un biais de 51 pour cent en faveur de la face qui est au-dessus au moment du lancer.

Ce biais a été expliqué en étudiant les équations du mouvement. Lorsque la pièce tourne parfaitement (la normale au centre de la pièce restant toujours dans un même plan), les probabilités de pile et de face sont presque identiques dès que la pièce tourne un assez grand nombre de fois (et parfaitement identiques lorsque le nombre de rotations tend vers l'infini). En revanche, pour un lancement imparfait (la normale à la pièce décrivant une courbe gauche), un biais existe en faveur du côté de la pièce initialement vers le haut. Ne pas rattraper la pièce n'est pas une solution, car lorsque la pièce frappe sur le sol, elle risque fort de se mettre à tourner comme une toupie, ce qui conduit à des biais plus importants.

La conclusion à laquelle on arrive alors est assez subtile. Si vous voulez opérer

un tirage équitable à pile ou face, deux cas sont à distinguer.

Cas 1. Vous avez confiance en celui qui lance la pièce ou vous la lancez vous-même… sans tricher. Alors la méthode consistant à rattraper la pièce dans la main assure une assez bonne équité (et une totale équité si celui qui lance ne choisit pas et ne regarde pas le côté de la pièce situé au-dessus au moment du lancer).

Cas 2. Vous n'avez pas confiance en celui qui lance la pièce. Alors vous choisissez vous-même une pièce (que vous n'avez pas testée) et demandez à votre adversaire de la lancer au sol. Même s'il existe un biais favorable à l'une des faces quand la pièce tournoie, aucun d'entre vous ne saura lequel, et le tirage sera équitable.

Si aucun des joueurs n'a confiance en l'autre, une assez bonne méthode existe : les joueurs prennent chacun une pièce de leur choix ; l'un choisit « mêmes côtés » et l'autre « côtés différents » ; ils lancent chacun leur pièce et dévoilent simultanément leurs résultats. Si les pièces montrent le même côté, celui qui avait choisi cette option gagne, sinon c'est l'autre.

Notons aussi qu'une étude de Daniel Murray et Scott Teare a établi que la pièce américaine de cinq cents (le « nickel ») a une chance sur 6 000 de ne donner ni pile ni face, en tombant sur la tranche.

Casino newtonien

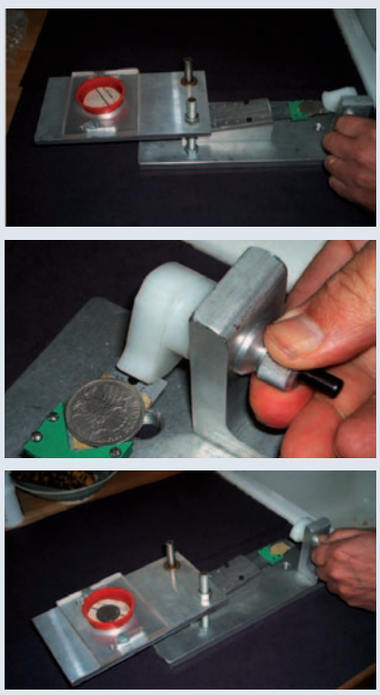
P. Diaconis et son équipe ont construit un dispositif mécanique de lancer de pièce qui, une fois réglé, donne le même résultat dans 100 pour cent des lancers. Il n'y a pas de surprise à cela : la mécanique newtonienne est déterministe et une bonne connaissance (ou un bon contrôle) des conditions initiales permet de calculer l'état du système quand la pièce s'est immobilisée.

En revanche, dès que le lancer est moins contrôlé et surtout si la pièce reste un long moment en l'air, il faudrait, pour effectuer une prédiction correcte, connaître les paramètres du lancer avec une précision impossible, même avec les caméras et les lasers les plus perfectionnés.

3. Pile ou… pile !

Les tirages au sort fondés sur des procédés macroscopiques pour engendrer des suites aléatoires (dé, lancer de pièce, roue de loterie, roulette, tirage de cartes, etc.) cumulent les inconvénients : ils sont très lents et l'on sait, d'après la physique classique (ce que de nombreuses expériences ont confirmé), qu'ils sont fréquemment biaisés et prédictibles dès qu'on dispose de moyens de mesure suffisants.

Lorsque le mécanisme physique est compliqué et implique par exemple de nombreux chocs (pièce qui rebondit sur un sol irrégulier, boule de roulette qui cogne les petits obstacles disposés sur sa trajectoire, etc.), toute prévision des résultats devient pratiquement impossible. Cependant, cette imprévisibilité pratique ne signifie pas qu'une série de tirages sera aléatoire au sens fort, car dans un monde newtonien déterministe le hasard fort est impossible. Le dispositif de catapulte ci-contre, utilisé par Persi Diaconis pour ses expériences, lance une pièce qui tombe dans un récipient *(en rouge)*. Quand il est réglé, tous les tirages donnent le même résultat.



The Mermaid tale

4. Les tests statistiques

Les statisticiens étudient et élaborent des tests pratiques s'appliquant à une suite finie de chiffres (on ne peut pas en pratique tester des suites infinies !).

Ils indiquent, pour une suite donnée, s'il est raisonnable ou non de croire qu'elle provient d'une suite de tirages aléatoires indépendants et équitables de 0 et de 1. Une telle suite doit par exemple posséder à peu près autant de 0 que de 1. Bien sûr, elle peut avoir plus de 0 ou plus de 1, mais l'écart doit être raisonnable. Le calcul donne des informations du type :

– Si une suite de 100 bits (0 ou 1) provient de tirages indépendants et équitables, la probabilité que l'écart entre les nombres de 0 et de 1 soit supérieur à 30 est inférieure à 0,18 pour cent.

– Si une suite de 10 000 bits provient de tirages indépendants et équitables, la probabilité que l'écart entre les nombres de 0 et de 1 soit supérieur à 400 est inférieure à 0,007 pour cent.

Il est ainsi peu vraisemblable qu'une suite de 10 000 bits donnant 6 000 fois 0 et 4 000 fois 1 provienne d'une suite de tirages équitables.

Une multitude de tests de cette nature évaluent des dizaines de propriétés que doivent posséder des suites provenant de tirages indépendants et équitables. L'Institut américain de la normalisation et de la technologie, le NIST, propose une telle batterie de tests (voir http://csrc.nist.gov/groups/ST/toolkit/rng/index.html). Ces tests contrôlent la nature aléatoire d'une suite et repèrent les générateurs pseudo-aléatoires déficients. Prudent dans son rapport de 2010, le NIST précise : « Aucun ensemble de tests statistiques ne peut certifier de manière absolue qu'un générateur donné est approprié à certains usages donnés. »

Malheureusement, les suites de décimales de nombres irrationnels comme π, e, $\sqrt{2}$, $\sqrt{3}$ ou les suites de chiffres obtenus en faisant des divisions du type k/p (où p est un grand nombre premier et k un entier positif), passent tous ces tests. En pratique, ces suites ressemblent autant que possible à des suites aléatoires, mais n'en sont pas, au sens de Martin-Löf.

5. Les procédés physiques microscopiques

De nombreux modèles de petites machines à produire du hasard à partir de phénomènes microscopiques, donc d'origine quantique, sont proposés à la vente. Connectés à un ordinateur, ces appareils, comme celui de la Société genevoise *ID Quantique*, créent ce que l'informatique classique (où tout est déterministe) ne peut pas produire : de l'incertitude.

Ces appareils sont souvent présentés comme engendrant d'authentiques suites aléatoires. C'est là une affirmation discutable. En effet, si les suites produites passent les tests statistiques standards, c'est aussi le cas des décimales de π ou de nombreuses suites pseudo-aléatoires algorithmiques dont on sait avec certitude qu'elles ne sont pas aléatoires au sens fort.

De plus, aucun argument théorique n'assure que les suites produites sont aléatoires au sens mathématique. On considère que la mécanique quantique laisse indéterminées certaines variables et que les opérations de mesure sur de telles variables ne dépendent d'aucun paramètre caché et sont assimilables aux variables aléatoires de la théorie des probabilités. Cependant, ces hypothèses (qu'on énonce rarement clairement) n'impliquent pas que les suites de tirages obtenus par un procédé quantique sont aléatoires au sens fort défini en 1965 par Martin-Löf, ce qui, par exemple, en assurerait l'incompressibilité. Il semble raisonnable d'avoir un peu plus confiance dans cet aléa quantique que dans l'aléa mécanique (qui est prouvé mauvais !), mais il est faux de croire qu'il correspond à l'aléa mathématique absolu. Comme l'indique David Branning du *Trinity College* dans un récent article sur la question : « L'aléa des phénomènes quantiques peut être considéré comme une hypothèse testable de plein droit et indépendante des autres questions que posent les fondements de la théorie quantique. »

ID-Quantique

Il en résulte que les histoires de tricherie à la roulette du casino impliquant des équipes de techniciens munis d'appareils de mesure et de calcul dissimulés dans leurs vêtements sont probablement fausses. Les casinos dont la politique a toujours été de faire croire qu'il existait des martingales et des méthodes favorables aux joueurs sont heureux de laisser circuler les fables affirmant qu'on peut savoir à l'avance sur quels numéros, ou quelle zone du cylindre, la bille lancée par le croupier va s'arrêter pour peu qu'on mesure son geste et qu'on mène les bons calculs.

Claude Shannon, l'un des pères de la théorie de l'information, travailla sur un tel projet avec le grand spécialiste des jeux de casino Edward Thorp, inventeur du système de comptage qui permettait au jeu de black jack de faire basculer l'avantage en faveur du joueur. Leur système fut testé en 1961 pour la roulette et, au dire de Thorp, « un problème mineur de matériel les empêcha d'en tirer des profits », ce qui laisse penser que le problème de la précision insuffisante des mesures n'a pas été surmonté.

D'autres histoires du même type ont été racontées (par exemple dans le livre *The Newtonian Casino* de Thomas Bass) sans jamais fournir de preuve de la capacité véritable des systèmes cachés à prédire les numéros de la roulette.

L'article de Jaroslaw Strzalko, Juliusz Grabski et Tomasz Kapitaniak (*Pour la Science* de novembre 2009) donne des détails sur la prédictibilité des lancers de dé et sur la possibilité de les considérer comme des phénomènes chaotiques. Dans leur livre *Dynamics of Gambling Origins of Randomness in Mechanical Systems,* paru en 2009, ces spécialistes du hasard mécanique formulent la conclusion suivante, qui devrait calmer les rêveurs : « Si les données montrent que les résultats d'un lancer de pièce, de dé ou d'une roulette sont prédictibles au sens de la définition [mathématique] et que ces processus sont inéquitables, ces conclusions sont théoriques, et, en pratique, pour réussir une prévision fiable, il faut connaître les conditions initiales avec une précision inatteignable dans des expériences réelles. »

Donc, en pratique, nous ne disposons pas aujourd'hui d'une technologie permettant de prédire les résultats d'un lancer de pièce, de dé ou de roulette. Cependant, il s'agit de phénomènes prédictibles (car déterministes) et le plus souvent biaisés. Ils ne satisfont donc pas les critères mathématiques de la définition de Martin-Löf ou les critères équivalents d'incompressibilité et d'imprédictibilité absolue.

Qu'en est-il du monde microscopique, dont les physiciens pensent très sérieusement qu'il fonctionne de manière non déterministe ?

Hasard quantique

Différentes machines sont vendues pour produire du hasard à partir de phénomènes microscopiques. Les appareils de la Société suisse *ID Quantique* exploitent un procédé d'optique quantique pour engendrer des suites aléatoires de 0 et de 1. Des photons sont envoyés un par un sur un miroir semi-transparent ; avec une probabilité égale, le photon traverse le miroir ou est réfléchi, ce qui donne 0 ou 1. Les différentes versions de leurs appareils produisent jusqu'à 4 000 000 de bits par seconde (ce qu'aucun procédé mécanique ne peut égaler).

La Société américaine *ComScire* propose un appareil qui produit seulement 2 000 000 de bits par seconde, mais en combinant plusieurs méthodes microscopiques différentes (bruit thermique, transistor saturé, etc.). À chaque fois, cependant, le principe théorique se fonde sur la nature quantique de ce qui se passe aux très petites échelles. Tous les

appareils mis en vente reposent sur l'idée que la mécanique quantique produit un hasard qui, une fois bien contrôlé (pour en équilibrer les productions), serait le hasard véritable caractérisé en 1965 par Martin-Löf et que le déterminisme de la mécanique newtonienne n'est pas en mesure d'atteindre.

Cette idée est-elle justifiée et fondée théoriquement ? La réponse n'est pas tranchée, car il n'est pas possible de tirer, des principes de la mécanique quantique, l'affirmation que les suites produites par exemple par les photons du dispositif vendu par *ID Quantique* sont aléatoires au sens de Martin-Löf. De l'indétermination concernant le passage ou non du photon à travers le miroir que la mécanique quantique exprime comme un axiome, on peut sans doute conclure que les suites produites par un tel dispositif sont semblables à celles que produisent des variables aléatoires uniformes indépendantes. Cependant, rien ne permet d'affirmer qu'une suite particulière tirée des photons (ou d'un autre procédé microscopique) est une suite aléatoire au sens de Martin-Löf : les suites provenant de tirages indépendants équilibrés ne sont pas toutes aléatoires au sens mathématique.

Il n'existe ainsi aucune méthode dont on puisse dire avec certitude qu'elle produit des suites aléatoires, et celles de la mécanique quantique ne font pas exception.

Les méthodes algorithmiques n'en produisent certainement pas et cela concerne :

– les chiffres des nombres irrationnels tels que π, $\sqrt{2}$, etc.

– les méthodes proposées dans les langages de programmation qui produisent un hasard assez bien équilibré, mais parfois prédictible et souvent imparfait quand on y regarde de près.

– les méthodes cryptographiques, qui sont conçues pour ne pas être aussi facilement prédictibles, mais qui, du fait de leur nature algorithmique, n'en donnent pas pour autant des suites aléatoires au sens absolu.

Pour les procédés mécaniques, la physique newtonienne affirme que les tirages successifs sont déterministes et, par conséquent, n'ont aucune raison de donner des suites incompressibles ou imprévisibles.

Quant aux méthodes microscopiques, rien dans les principes mêmes de la mécanique quantique ne garantit la production de véritables séquences aléatoires au sens fort. À moins de compléter les axiomes de la théorie, il n'est aujourd'hui pas justifié de dire qu'un procédé quantique produit avec une certitude absolue de l'aléa fort comme Martin-Löf l'a défini. Il faut peut-être reformuler la théorie quantique pour que cela change, mais personne pour l'instant ne le propose. Il faut donc cesser d'affirmer que les méthodes quantiques de production d'aléa sont bien fondées, à l'opposé des méthodes mécaniques ou algorithmiques.

Insaisissable hasard

Malgré tout cela, et c'est ici qu'il y a un paradoxe, pour les tests conçus depuis un siècle et qui sont soigneusement collectés, par exemple par le NIST aux États-unis, tout semble aller très bien. Il n'y a pas de différences repérables entre les moins assurées (théoriquement) des suites pseudo-aléatoires (comme la suite des chiffres de π), les suites aléatoires mécaniques (produites avec précautions) et les suites aléatoires quantiques.

Régulièrement, certains chercheurs ont prétendu repérer et mesurer des différences entre diverses suites aléatoires (par exemple entre les chiffres de π et ceux d'autres constantes). Cependant, jamais ces affirmations n'ont été confirmées et, au contraire, on a en général découvert des erreurs méthodologiques de la part de ceux qui annonçaient avoir repéré des nuances mesurables entre suites aléatoires. Un article de George Marsaglia, grand spécialiste de l'aléa informatique, publié en 2005 conclut de manière formelle après l'utilisation des meilleures batteries de tests disponibles que les chiffres des développements de nombres irrationnels tels que π, e, $\sqrt{2}$, aussi bien d'ailleurs que ceux des nombres rationnels k/p, où p est un nombre premier assez grand, semblent se comporter comme s'ils provenaient d'une suite de tirages indépendants équitables : la théorie et la pratique divergent au maximum ! ■

L'AUTEUR

Jean-Paul DELAHAYE est professeur à l'Université de Lille et chercheur au Laboratoire d'informatique fondamentale de Lille (LIFL).

✔ BIBLIOGRAPHIE

H. Zenil, **Randomness Through Computation : Some Answers, More Questions**, World Scientific Publishing, 2011.

B. Hayes, **Excursions quasi-aléatoires**, *Pour la Science*, décembre 2011.

A. Dasgupta, **Mathematical foundation of randomness**, dans *Philosophy of Statistics*, North-Holland, pp. 641-710, 2011 (http://dasgupab.faculty.udmercy.edu/Dasgupta-JSfinal.pdf).

R. Downey et D. Hirschfeld, **Algorithmic Randomness and Complexity**, Springer-Verlag, 2010.

N. Gauvrit, **Vous avez dit hasard ?**, Belin/Pour la Science, 2009.

Hasard et incertitude, *Pour la Science*, numéro spécial, novembre 2009.

J. Strzalko *et al.*, **Dynamics of Gambling : Origins of Randomness in Mechanical Systems**, Springer, 2009.

P. Diaconis *et al.*, **Dynamical bias in the coin toss**, *SIAM Rev.*, vol. 49, pp. 211-235, 2007.

J.-P. Delahaye, **Information, complexité et hasard**, Hermès, 2e édition, 1999.