Comment produire du hasard

Jean-Paul Delahaye [1]

Avons-nous la capacité de produire du hasard, et sommes-nous certains que ce que nous croyons être du hasard en est réellement ? Ces questions sont importantes pour assurer que les loteries et les jeux où il intervient sont équitables. En informatique, elles nous concernent quand nous voulons mener des simulations, justement parce que le hasard semble présent partout dans le monde que nous voulons reproduire. Ces questions sont aussi essentielles pour la mise en œuvre des méthodes mathématiques de calcul de type Monte-Carlo où la justesse et la précision de ce qu'on obtient dépendent de la qualité du hasard utilisé. Enfin, en cryptographie, le hasard est au cœur de nombreuses méthodes, dont la robustesse aux attaques est liée à sa plus ou moins grande perfection. Nous allons nous concentrer sur le hasard de la physique et particulièrement sur celui des pièces de monnaie qu'on lance en l'air ou que des dispositifs quantiques semblent produire à grande vitesse. Auparavant, revenons sur ce que les mathématiques nous ont récemment appris du hasard.

Tests, compression et prédiction

La théorie des probabilités, dont les développements depuis un siècle ont été considérables, 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 chercher à indiquer ce qu'est une suite aléatoire particulière de lancers de dé ou de *pile ou face*. Définir précisément ce qu'est une suite aléatoire fut un défi et longtemps toutes les tentatives ont échoué (voir [De 1999, Chap. 2]).

1. Université de Lille 1, Sciences et Technologies, Laboratoire d'Informatique Fondamentale de Lille, UMR 8022 CNRS, Bât M3-ext, 59655 Villeneuve d'Ascq Cedex. E-mail : delahaye@lifl.fr.

En 1966, Per Martin-Löf trouve la solution [ML 1966]. Pour lui, une suite infinie de '0' et de '1' doit être qualifiée d'aléatoire lorsqu'elle réussit tous les *tests statistiques raisonnables* du type « la limite de fréquence des '0' doit être 1/2, comme celle des '1' ». La notion de *test statistique raisonnable* est un peu technique (c'est le complémentaire d'un ensemble constructivement de mesure nulle ; voir par exemple [Ta 2013, Chap. 3]), mais il n'est pas nécessaire de la détailler car l'idée de Martin-Löf a été acceptée quand on a su établir qu'elle était équivalente à deux idées plus simples. D'une part, à l'idée qu'une suite est aléatoire si elle est *incompressible* — il est impossible de représenter les k premiers digits de la suite infinie par un programme d'une longueur sensiblement plus petite que k. D'autre part, à l'idée qu'une suite est aléatoire si elle est *imprévisible* — aucun système de pari algorithmique ne gagne contre elle (en termes un peu plus précis : connaissant le début de la suite, un procédé de pari algorithmique garde une chance sur deux au plus de gagner en pariant sur le digit qui vient). Cette triple caractérisation mathématique de la notion de suite infinie aléatoire est un succès remarquable des mathématiques de la seconde moitié du XXe siècle. Aujourd'hui, elle fixe le sens précis des questions qu'on se pose sur les dispositifs inventés pour engendrer du hasard. Récemment, plusieurs livres et thèses ont fait le point sur cet apport fondamental de la théorie de la calculabilité à la compréhension du hasard : [Da 2011], [DH 2010], [Ni 2009], [Ta 2013], [Ve 2013], [Ze 2011]. Le bilan théorique est que, parmi les nombreuses définitions possibles de la notion de suite infinie aléatoire, celle de Martin-Löf est d'assez loin la meilleure et doit servir de référence. Au sujet de ce choix, on parle parfois de « Thèse de Martin-Löf », comme il y a une « Thèse de Church » pour la notion de fonction calculable par algorithme (voir [Da 2011], [De 1993]).

La suite "000...000..." n'est pas aléatoire. La suite des chiffres binaires du nombre π ne l'est pas non plus, car elle se calcule facilement, et est donc compressible. La suite des chiffres d'un nombre oméga de Chaitin [2] est aléatoire. En accord avec une idée déjà notée par Émile Borel, il y a plus d'un siècle, on montre que presque toutes les suites infinies sont aléatoires au sens de Martin-Löf.

Notons bien, car c'est le cœur du problème, qu'aucun procédé algorithmique déterministe ne produira ce hasard véritable que la théorie mathématique a enfin identifié. En effet, si une suite est le résultat d'un algorithme, on peut la comprimer et la prédire, et donc la suite n'est pas aléatoire. En termes techniques : une suite calculable par algorithme n'est pas aléatoire au sens de Martin-Löf (l'inverse n'est pas vrai, bien sûr).

La question de savoir si les suites produites physiquement par des dés, les lancers d'une pièce de monnaie, des loteries ou par des dispositifs quantiques a donc pris un sens scientifique parfaitement précis. En même temps, elle est devenue importante

2. Un nombre oméga de Chaitin est un réel défini comme la probabilité d'arrêt d'un ordinateur universel à programmes auto-délimités [De 2002].

puisqu'on découvrait que l'informatique seule n'avait pas la capacité de produire du bon hasard, ce qui d'ailleurs explique les nombreux déboires rencontrés par les applications utilisant des générateurs pseudo-aléatoires fonctionnant par programme.

Pièces de monnaie, dés et loteries

Sophocle prétendait que les dés furent inventés par Palamède durant le siège de Troie, alors qu'Hérodote soutenait qu'on les doit aux Lydiens sous le règne du roi Atys, au VIe siècle avant J.-C.. L'archéologie leur donne tort à tous les deux : on a trouvé des dés dans des ruines plus anciennes. En Égypte, en particulier, l'astragale d'usage courant était une sorte de dé irrégulier (obtenu à partir de l'os éponyme) dont l'usage pour jouer serait venu d'Asie. Quant au jeu de pile ou face, son origine est impossible à identifier du fait que les pièces ont une fonction commerciale préexistant à leur usage comme générateur de hasard. Les mécanismes de loterie et de roulette sont plus récents. La roulette de casino est attribuée à Blaise Pascal qui, en 1655, en fabriqua un premier modèle... alors qu'il cherchait à concevoir un mouvement perpétuel.

Chacun sait qu'il existe des dés pipés, obtenus en s'arrangeant pour que le centre de gravité du dé soit décalé du centre géométrique, ce qui force le dé à donner presque toujours '6', ou '6' avec une probabilité supérieure à $1/6$. De même, une roulette de casino est parfois mal équilibrée ou possède des cases de profondeurs inégales qui faussent l'équiprobabilité des numéros. On mentionne qu'exploitant cela, plusieurs joueurs auraient fait fortune, dont le premier, Joseph Jagger, aurait 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 fasse soigneusement la différence entre les méthodes utilisées pour pratiquer le pile ou face. 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 [GD 2002].

En revanche, plusieurs techniques permettent de fausser l'équilibre des chances à pile ou face. Un peu d'entraînement vous permettra de lancer la pièce en la faisant plus ou moins pivoter autour de son axe, vous autorisant alors à la rattraper du côté que vous souhaitez. Si, au lieu de lancer la pièce, vous la faites tourner comme une toupie sur une surface plane, le tirage sera rarement équitable, car cette fois 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% des cas.

Biais de 51%

Une étude minutieuse, menée par Persi Diaconis (le célèbre mathématicien illusionniste de l'université de Stanford), Susan Holmes et Richard Montgomery, a établi un autre étonnant résultat [DHM 2007]. Une pièce de monnaie, soigneusement lancée en la rattrapant après qu'elle a tourné en l'air (et sans manipulation délibérée de la part du lanceur), donne de manière stable un biais de 51% en faveur de la face qui est au-dessus au moment du lancer.

Ce biais a été identifié en écrivant soigneusement les équations du mouvement et en les étudiant. Il a été partiellement confirmé expérimentalement [Al 2014]. 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, dans le cas d'un lancement imparfait de la pièce (la normale à la pièce décrivant une courbe non-plane), un biais existe en faveur du côté de la pièce initialement vers le haut. Ce biais, qui est plus ou moins fort selon la trajectoire de la normale, explique qu'en moyenne on ait le 51% trouvé par Diaconis. Même sans intention de tricher, le mouvement qu'on opérera sera rarement parfait et donc, en rattrapant la pièce, il y aura un biais général en faveur du côté de la pièce placé au-dessus à l'instant du lancer. 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 alors à des biais encore plus importants, comme on l'a déjà indiqué.

Méfiance

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). Lancer la pièce au sol doit être évité car elle pourrait tournoyer, ce qui est mauvais.

Cas 2. Vous n'avez pas confiance en celui qui lance la pièce.

Ne le laissez pas lancer la pièce lui-même, car il lui serait relativement facile de tricher. Choisissez vous-même une pièce (que vous n'avez pas testée) et demandez-lui de la lancer au sol. Même s'il y a un biais favorable à l'une des faces quand la pièce tournoie, aucun d'entre vous ne saura lequel, et le tirage sera donc équitable.

Si aucun des joueurs n'a confiance en l'autre, une assez bonne méthode existe quand même :

– les joueurs prennent chacun une pièce de leur choix ;

– l'un choisit « même côté » et l'autre « côtés différents » ;
– ils lancent chacun leur pièce en cachant le résultat ;
– ils dévoilent simultanément leurs résultats ;
– si les pièces montrent le même côté, celui qui avait choisi cette option gagne, sinon c'est l'autre.

Casino Newtonien

La mesure très précise des paramètres d'un lancer de pièce par un système mécanique pas trop violent pour que la pièce ne reste en l'air que peu de temps permet de savoir avec une assez bonne précision de quel côté la pièce va tomber. D'ailleurs, Diaconis et son équipe ont construit un dispositif mécanique de lancer de pièce qui, une fois réglé, donne un résultat constant [DHM 2007]. 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 détermine l'état du système quelques secondes après, c'est-à-dire 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 et qu'elle rebondit sur un sol irrégulier, la prédiction par le calcul n'est plus possible. Les zones de l'espace des phases conduisant à *pile* se mélangent si étroitement avec celles conduisant à *face* qu'il faudrait, pour formuler une prédiction correcte, disposer des paramètres du lancer avec une précision impossible même aux plus perfectionnés des caméras et des systèmes à laser.

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 très vraisemblablement 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 ces fables — reprises dans des livres et des films — suggérant qu'on peut savoir à l'avance sur quels numéros — ou dans quelle zone du cylindre — la bille lancée par le croupier va s'arrêter, pour peu qu'on mesure son geste, la vitesse de la bille et sa position, et qu'on mène les bons calculs.

Claude Shannon, le père de la théorie de l'information, travailla sur un tel projet avec le spécialiste des jeux de casino Edward Thorp, inventeur du système de comptage qui permet, au jeu de Blackjack, de faire basculer l'avantage en faveur du joueur. Leur système pour la roulette avait la taille d'un paquet de cigarettes. Il fut testé en 1961 dans les établissements de Las Vegas mais, au dire de Thorp [Th 1998], « un problème mineur de matériel les empêcha d'en tirer des profits ». Cela semble assez étrange et laisse plutôt penser que le problème de la précision limitée 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 [Ba 1991]) sans jamais fournir de preuve de la capacité véritable des systèmes cachés à prédire les numéros de la roulette. Des escrocs mettent d'ailleurs en vente sur internet de petits appareils dont

ils prétendent qu'ils réalisent ces prédictions *newtoniennes*. Ne les achetez surtout pas : aucune démonstration en laboratoire n'a jamais pu établir rigoureusement que ces appareils fonctionnent, et ce qu'on sait sur le mélange des zones de l'espace des phases dans le cas de tels systèmes physiques rend certain que ces appareils ne vous feront rien gagner.

Un article de Jaroslaw Strzalko, Juliusz Grabski et Tomasz Kapitaniak [SG 1999] 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* [SG 2009], ces spécialistes du hasard mécanique formulent la conclusion suivante qui devrait calmer les rêveurs : « Les données présentées ici 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 ce sont des processus inéquitables. Cependant, ces conclusions sont théoriques, et en pratique, pour réussir une prévision fiable, il faut connaître les conditions initiales avec une précision impossible à atteindre dans des expériences réelles. » Cette conclusion est conforme à l'analyse qu'en faisait Albert Einstein, à qui l'on attribue la phrase : « il est impossible de battre la roulette à moins de prendre l'argent pendant que le croupier ne regarde pas » (« *No one can win at roulette unless he steals money from the table while the croupier isn't looking* »).

Du point de vue de la définition mathématique évoquée au début de l'article, la conclusion est sans appel. Les résultats d'un lancer de pièce, de dé ou de roulette, sont des phénomènes prédictibles, *en théorie*, car déterministes : les suites produites ne sont donc pas aléatoires au sens de Martin-Löf. Le plus souvent, les résultats sont biaisés (pas d'équilibre entre les '0' et les '1'), ce qui est une seconde raison de ne pas considérer les suites produites comme aléatoires au sens de Martin-Löf. Cependant, *en pratique*, dès que les lancers sont faits avec suffisamment de soin, nous ne disposons pas de technologies permettant la prédiction.

La mécanique quantique

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

La question est d'une nature différente de celle des méthodes mécaniques. D'ailleurs, des machines assez variées sont vendues pour produire du hasard à partir de phénomènes microscopiques. Par exemple, la firme suisse ID Quantique [3] propose des appareils générant des suites aléatoires de '0' et de '1' exploitant un procédé d'optique quantique. Des photons sont envoyés un par un sur un miroir semi transparent ; avec une probabilité égale (autant que possible !), le photon traverse le miroir ou est réfléchi, ce qui donne '0' ou '1'. Les différentes versions de leurs

3. `http://www.idquantique.com/`

appareils produisent jusqu'à 16 000 000 de bits par seconde, ce qu'évidemment aucun procédé mécanique ne peut égaler.

La firme ComScire[4], de son côté, propose un appareil qui produit jusqu'à 32 000 000 de bits par seconde, et combine 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. D'autres appareils sont en vente, mais qui tous reposent finalement sur l'idée que la mécanique quantique produit un hasard qui, une fois bien contrôlé et rectifié (pour en équilibrer les productions), serait ce hasard véritable, défini par les mathématiques, que le déterminisme de la mécanique newtonienne n'est pas en mesure d'atteindre.

Cette idée que la mécanique quantique donne une meilleure garantie que la mécanique newtonienne pour créer du hasard est-elle justifiée et fondée théoriquement ? Parle-t-on ici vraiment du hasard caractérisé en 1966 par Martin-Löf en termes de satisfaction à tous les tests raisonnables ou par l'incompressibilité ?

La réponse n'est pas tranchée car le lien entre la mécanique quantique et les définitions mathématiques des suites aléatoires n'a pas été fait. Au sens strict, 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 tirer que l'ensemble des suites produites par un tel dispositif est semblable à ce 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 puisque les suites provenant de tirages indépendants équilibrés ne sont pas toutes aléatoires au sens de Martin-Löf.

Une multitude de travaux menés par des physiciens ont consisté à produire des suites à l'aide de procédés microscopiques et à leur faire passer des tests statistiques pour en détecter des régularités. Une fois surmontées les difficultés de réglage des appareils pour que les suites soient équilibrées (autant de '0' que de '1') et les artefacts techniques éliminés, tous les tests donnent de bons résultats. Autant que les batteries de tests permettent de le juger, les suites « quantiques » semblent bien aléatoires. Même si la théorie ne le dit pas, la conclusion expérimentale est donc positive : l'aléa quantique apparaît expérimentalement parfait. Voir [CD 2010], [FW 2010], [Gi 2012], [PG 2013], [Pi 2010], [St 2004].

Cependant, cette constatation empirique limitée ne constitue pas une preuve et ne signifie rien de définitif. En effet, on sait par exemple que les chiffres du nombre π passent eux aussi tous ces tests statistiques, en même temps qu'on sait que les

4. http://comscire.com/

chiffres de π ne constituent pas une suite aléatoire au sens de Martin-Löf (du fait que des programmes courts peuvent les produire).

Le paradoxe des suites aléatoires

Si on considère la notion de suite aléatoire telle que les mathématiques la définissent depuis 1966, il n'existe aucune méthode dont on puisse dire avec certitude qu'elle produit des suites aléatoires. Les méthodes algorithmiques n'en produisent certainement pas et cela concerne :

(1) les chiffres des nombres irrationnels comme π, $\sqrt{2}$, etc. [Ma 2005] ;

(2) les méthodes proposées dans les langages de programmation, qui produisent un hasard assez bien équilibré (souvent à l'aide de générateurs congruentiels linéaires [Kn 1997]), mais parfois prédictible et souvent imparfait quand on va y voir de près (il est fortement déconseillé de les utiliser pour des applications en cryptographie [St 1987], [GP 1997]) ;

(3) les méthodes cryptographiques (dont le fameux BBS [GP 1997], [DP 2014]) qui sont conçues pour ne pas pouvoir être aussi facilement prédictibles mais qui — du fait de leur nature algorithmique — n'en donnent pas pour autant des suites aléatoires au sens de Martin-Löf.

Pour les procédés mécaniques, comme on l'a vu, on ne réussit même pas à garantir une bonne uniformité dans le cas des pièces, des dés, des loteries et des roulettes. La physique newtonienne affirme que même dans les cas de bassins convenables (suffisamment emmêlés), les tirages successifs sont déterministes et donc n'ont aucune raison de donner des suites incompressibles ou imprévisibles.

Quant aux méthodes microscopiques, qui se fondent en dernier ressort sur la mécanique quantique, elles sont un peu mieux loties, puisque la mécanique quantique énonce certaines affirmations d'imprédictibilité. Cependant, rien dans les principes même de la mécanique quantique ne garantit que chaque suite produite est une véritable suite aléatoire au sens de Martin-Löf. À moins de compléter les axiomes de la théorie, aujourd'hui, il n'est pas justifié de dire qu'un procédé quantique produit avec une certitude absolue l'aléa fort que Martin-Löf a défini. Il faut peut-être reformuler la théorie quantique pour que cela change — mais personne pour l'instant ne le propose — et donc il faut cesser d'affirmer que les méthodes quantiques de production d'aléa sont bien fondées à l'opposé des méthodes mécaniques ou algorithmiques.

Contradiction ?

Malgré tout cela — et c'est ici qu'il y a une sorte de paradoxe — pour les tests conçus depuis un siècle et qui sont soigneusement collectés — par exemple par le NIST (*National Institute of Standards and Technology*) 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 (sous réserve qu'elles soient produites avec précaution), et les suites aléatoires quantiques. (Notons qu'il faut être méfiant concernant le NIST qui a délibérément proposé un générateur pseudo-alétaoire prétendument cryptographiquement sûr alors qu'il y avait glissé une "*backdoor*" à la demande de la NSA ; voir [Ha 2014]).

Régulièrement, certains chercheurs ([PK 1997], [So 2009], [TF 2005], [Ma 2003], etc.) 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 affirmaient repérer des nuances mesurables entre suites aléatoires. George Marsaglia (un grand spécialiste de l'aléa informatique) conclut de manière formelle après l'utilisation des meilleures batteries de test disponibles que « les chiffres des développements de nombres irrationnels comme π, e, $\sqrt{2}$, aussi bien d'ailleurs que ceux des nombres rationnels k/p pour p un nombre premier assez grand, semblent se comporter comme s'ils provenaient d'une suite de tirages indépendants équitables » [Ma 2005].

L'aléa produit par les chiffres de π apparaît statistiquement parfait, de même que lorsqu'il s'agit d'un bon procédé mécanique (quoi que les casinos essaient de faire croire) ou un bon procédé microscopique.

Ici, la théorie et la pratique divergent au maximum :

– aucun procédé n'est bien fondé *en théorie* pour produire du hasard fort, défini en 1966 par Martin-Löf, et aucune démonstration n'a jamais été fournie pour aucune méthode (algorithmique, mécanique ou quantique) ;

– cependant, *en pratique*, une multitude de procédés produisent des suites qui passent tous les tests statistiques.

Références

[Al 2014] David Aldous. 40,000 coin tosses yield ambiguous evidence for dynamical bias, `http://www.stat.berkeley.edu/~aldous/Real-World/coin_tosses.html`.

[Ba 1991] Thomas Bass. *The Newtonian Casino.* Penguin Books Ltd, 1991.

[CD 2010] Cristian Calude, Michael Dinneen. Experimental Evidence of Quantum Randomness Incomputability. *Physical Review A* 82, 022102, 2010.

[Da 2011] Abhijit Dasgupta. Mathematical Foundation of Randomness. In : *Philosophy of Statistics*, North-Holland, 641-710, 2011, `http://dasgupab.faculty.udmercy.edu/Dasgupta-JSfinal.pdf`.

[De 1993] Jean-Paul Delahaye. Randomness, Unpredictability and Absence of Order. In "*Philosophy of Probability*", J. Dubucs Ed., Kluwer Academic, 145–167, 1993, `http://www.lifl.fr/~delahaye/dnalor/Randomness1993.pdf`.

[De 1999] Jean-Paul Delahaye. *Information, complexité et hasard.* Hermès, Seconde Édition, 1999.

[De 2002] Jean-Paul Delahaye. Les nombres oméga. *Pour la Science* 295, 98–103, 2002, http://www.lifl.fr/~delahaye/pls/093.pdf.

[DH 2010] Rodney G. Downey, Denis R. Hirschfieldt. *Algorithmic Randomness and Complexity.* Series : Theory and Applications of Computability, Springer, 2010.

[DHM 2007] Persi Diaconis, Susan Holmes, Richard Montgomery. Dynamical Bias in the Coin Toss. *SIAM Rev.* 49, 211–235, 2007.

[DP 2014] Ankur Divyanjali, Vikas Pareek. An Overview of Cryptographically Secure Pseudorandom Number Generators and BBS. *IJCA Proceedings on International Conference on Advances in Computer Engineering and Applications, ICACEA* 2, 19–28, 2014.

[FW 2010] Harald Fürst, Henning Weier, Sebastian Nauerth, Davide G. Marangon, Christian Kurtsiefer, Harald Weinfurter. High Speed Optical Quantum Random Number Generation. *Opt. Express* 18-12, 13029–13037, 2010.

[Ga 2009] Nicolas Gauvrit. *Vous avez dit hasard ? Entre mathématiques et psychologie.* Bibliothèque scientifique, Éditions Belin / Pour la science, 2009.

[GD 2002] Andrew Gelman, Deborah Nolan. You Can Load a Die but You Can't Bias a Coin. *The American Statistician* 56-4, 306–311, 2002.

[Gi 2012] Nicolas Gisin. *L'impensable hasard.* Éditions Odile Jacob, 2012.

[GP 1997] Louis Goubin, Jacques Patarin. La génération d'aléas sur ordinateur. *Quadrature* 30, 27–36, 1997.

[Ha 2014] Thomas Hales. The NSA Backdoor to NIST. *Notice of the AMS* 61-2, 190–192, 2014, http://math.ipm.ac.ir/combin/useful_material/rnoti-p190.pdf.

[Kn 1997] Donald Knuth. *The Art of Computer Programming, Vol 2 : Seminumerical Algorithms.* Third Edition, Addison-Wesley. Section 3.2.1 : The Linear Congruential Method, 10—26, 1997.

[Ma 2003] George Marsaglia. Refutation of claims such as "Pi is less random than we thought". http://yaroslavvb.com/papers/marsaglia-refutation.pdf, 2003.

[Ma 2005] Georges Marsaglia. On the Randomness of Pi and other Decimal Expansions. *InterStat : statistics on the Internet*, page 17, October 2005, http://www.yaroslavvb.com/papers/marsaglia-on.pdf.

[ML 1966] Per Martin-Löf. The Definition of Random Sequences. *Information and Control* 9, 602—619, 1966.

[Ni 2009] André Nies. *Computability and Randomness.* Oxford University Press, 2009.

[PG 2013] Matthew Peloso, Ilja Gerhardt. Statistical Tests of Randomness on Quantum Keys Distributed Through a Free-Space Channel Coupled to Daylight Noise. *Journal of Lightwave Technology* 31-23, 3794–3805, 2013.

[Pi 2010] Stefano Pironio *et al.* Random Numbers Certified by Bell's Theorem. *Nature* 464, 1021–1024, 2010.

[PK 1997] Steve Pincus, Rudolf Kalman. Not All (possibly) "random" sequences are created equal. *PNAS* 94-8, 3513–3518, April 15, 1997.

[PLS 2009] *Hasard et incertitude, les défis qu'ils posent.* Pour la science 385, numéro spécial, novembre 2009.

[SG 1999] Jaroslaw Strzalko, Juliusz Grabski, Tomasz Kapitaniak. Les dés sont pipés. *Pour la science* 385, novembre 1999.

[SG 2009] Jaroslaw Strzalko, Juliusz Grabski, Przemyslaw Perlikowski, Andrzej Stefanski, Tomasz Kapitaniak. *Dynamics of Gambling : Origins of Randomness in Mechanical Systems.* Lecture Notes in Physics 792, Springer, 2009.

[So 2009] Suman Kumar Sourabh. Are Subsequences of Decimal Digits of Pi Random ? *Anale Seria Informatica* VII-2, 87–96, 2009.

[St 1987] Jacques Stern. Secret Linear Congruential Generators are not Cryptographically Secure. Proceedings of the 28th Annual Symposium on Foundations of Computer Science, 421–426, 1987.

[St 2004] Mario Stipčević. Fast nondeterministic Random bit Generator Based on Weakly Correlated Physical Events. *Rev. Sci. Instr.* 75, 4442–4449, 2004.

[Ta 2013] Antoine Taveneaux. *Puissance logique et calculatoire de l'aléa algorithmique.* Thèse, Université Paris Diderot, 2013.

[TF 2005] Shu-Ju Tu, Ephaim Fischbach. A Study on the randomness of the digits of π. *International Journal of Modern Physics C* 16-2, 281–294, 2005.

[Th 1998] Edward Thorp. The Invention of the First Wearable Computer. Proceedings of the 2nd IEEE International Symposium on Wearable Computers, ISWC '98, 4–8, 1998, `http://www.cs.virginia.edu/~evans/thorp.pdf`.

[Ve 2013] Stijn Vermeeren. *Notions and Applications of Algorithmic Randomness.* PhD Thesis, University of Leeds, 2013.

[Ze 2011] Hector Zenil. *Randomness Through Computation : Some Answers, More Questions.* World Scientific Publishing, 2011.