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.