

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-aléa-

toires 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 véri-

table 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