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

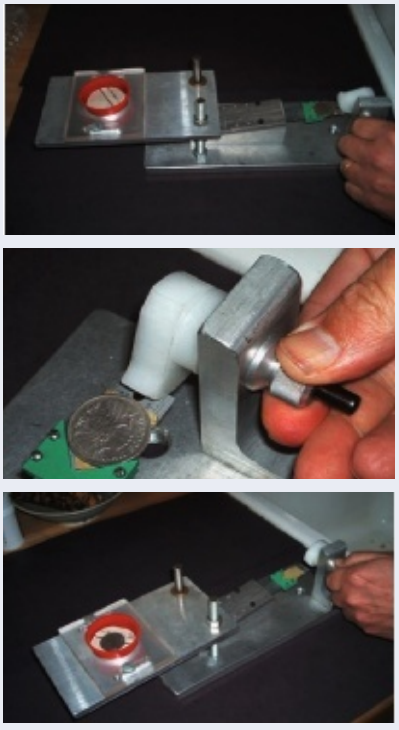
P. Diaconis et son équipe ont construit un dispositif mécanique de lancer de pièce qui, une fois réglé, donne le même résultat dans 100 pour cent des lancers. Il n'y a pas de surprise à cela : la mécanique newtonienne est déterministe et une bonne connaissance (ou un bon contrôle) des conditions initiales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