

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 :

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

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

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

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 tourne, 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

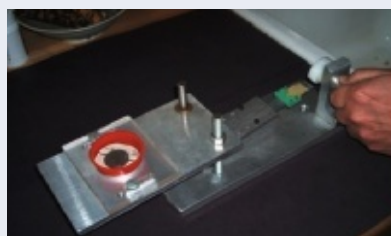
P. Diaconis et son équipe ont construit un dispositif mécanique de lancer de pièce qui, une fois réglé, donne le même résultat dans 100 pour cent des lancers. Il n'y a pas de surprise à cela : la mécanique newtonienne est déterministe et une bonne connaissance (ou un bon contrôle) des conditions initiales 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/mg/index.html>). Ces tests contrôlent la nature aléatoire d'une suite et repèrent les générateurs pseudo-aléatoires défectueux. 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.