1. Les procédés physiques macroscopiques

Les moyens physiques pour engendrer le « hasard » sont nombreux... et pas toujours équitables. On retrouve périodiquement lors de fouilles des dés romains *(à gauche en bas de la page ci-contre)*. Les mêmes dés sont utilisés dans le jeu de Craps des pays anglo-saxons. Les roues de loterie où l'on pouvait gagner des kilos de sucre attiraient les badauds des années 1950 qui avaient été privés de sucre pendant la Seconde Guerre mondiale (on notera l'escroquerie de l'épaisseur des bandes de gain des gros montants de kilos de sucre).

La roulette et sa variante la boule sont les instruments du casino. Le rééquilibrage des roues et les plots que heurtent la bille lors de sa descente augmentent la sensibilité aux conditions initiales.

Les machines à sous, dénommées parfois bandits manchots, ont été inventées à San Francisco par Charles Fey vers 1890. Deux méthodes différentes sont utilisées pour engendrer le hasard. Dans un premier temps, le mécanisme à produire du hasard était macroscopique et déterministe : la force avec laquelle on lançait les roues (initialement il y en avait trois) en tirant sur le bras de la machine déterminait le résultat. Le mécanisme était conçu pour qu'aucun contrôle précis ne soit possible et la machine était assimilable à une loterie ou à une roulette de casino enfermée dans une boîte. Bien sûr, des trucages mécaniques favorisant certaines combinaisons étaient possibles.

À partir des années 1960, ces machines sont devenues électroniques : un générateur algorithmique pseudo-aléatoire produit plusieurs dizaines de fois par seconde des chiffres sans jamais s'arrêter. Ces chiffres sont effacés de ses mémoires et ce n'est qu'au moment où l'utilisateur joue (en appuyant sur un bouton ou en tirant le bras de la machine) que les derniers chiffres produits sont exploités. Ils déterminent alors une combinaison qui est affichée sur l'écran de la machine (après un délai et une animation factices) et qui fixe le résultat du jeu, provoquant, lorsque c'est nécessaire, la chute d'une quantité de pièces.

Ce procédé est-il convenable ? Si on exclut les tricheries passant inaperçues aux yeux des organismes officiels chargés de contrôler les machines, le procédé est satisfaisant aussi bien pour les joueurs que pour les propriétaires des machines.

D'une part, le propriétaire peut choisir la machine qu'il veut (ou plus tard la modifier en changeant certains composants électroniques) pour que le pourcentage d'argent redonné en moyenne aux joueurs soit celui qu'il décide (en général entre 75 % et 99 %). Ce pourcentage sert parfois d'argument publicitaire. Il peut aussi choisir une machine qui donne souvent de petits lots et rarement des gros, ou le contraire (cela tout en respectant le pourcentage d'argent redonné en moyenne aux joueurs et fixé à l'avance).

D'autre part, une fois la machine fermée, personne ne peut tricher. Personne n'a d'informations sur l'état du générateur pseudo-aléatoire qui tourne en continu et, de plus, le geste du joueur n'est pas assez précis pour qu'il contrôle l'instant où il joue.

Le fait que ce mode de fonctionnement soit convenable pour tous ne signifie pas que le processus général du jeu produit des suites aléatoires au sens fort. En interne, il n'y a pas d'aléa puisque ce qui se passe est algorithmique. Quant au joueur, il se peut qu'il appuie inconsciemment d'une manière régulière. Rien n'assure donc que les suites de résultats d'une machine de casino soient aléatoires au sens de Martin-Löf.

Watling Rol-A-Top

The Gamble Gurus

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 :

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

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

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

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