Aujourd'hui la tradition de l'édition des tables de nombres aléatoires s'est adaptée, et un CD-ROM de plus de quatre milliards de bits aléatoires a été récemment édité par Marsaglia selon une méthode que je vais décrire. Des sites Internet proposent aussi des monceaux de bits aléatoires à qui veut bien.

Partant du constat que *(a)* les méthodes purement physiques produisent souvent des séquences avec des déviations de fréquences et autres défauts de mélange et qu'il faut donc s'en méfier en simulation, mais que *(b)* les méthodes par générateurs algorithmiques ne sont pas sûres, principalement à cause de leur prévisibilité, Marsaglia a additionné les deux procédés.

Il a pris des séries de bits engendrées par des procédés physiques et des séries générées par des générateurs algorithmiques ayant passé les tests de bon mélange, et a opéré un *ou-exclusif* entre les deux séries : '0' et '0' donnent '0' ; '0' et '1' donnent '1' ; '1' et '0' donnent '0' ; '1' et '1' donnent '1'. Cela combine les bonnes propriétés des deux méthodes : l'imprévisibilité est garantie par la composante physique, le bon mélange par la composante algorithmique. Bien sûr, ces séries ont été soumises aux batteries de tests dont on dispose. Notons que ces même batteries indiquaient clairement que la plupart des générateurs physiques ne fonctionnaient pas de manière très satisfaisante.

Même s'il a été produit avec soin et qu'il sera certainement utile, le CD-ROM n'est malheureusement pas la solution ultime. D'une part, pour la simulation, il se peut qu'on ait besoin de séries aléatoires encore plus longues que celles du CD-ROM. D'autre part, en cryptographie, le fait que le CD-ROM soit disponible à tous est quelque peu inquiétant !

Les générateurs physiques fondés sur le bruit thermique tel QNG de la Société *ComScire* (http://shell.rmi.net/~comscire), ou sur la diode Zener exploitant l'effet tunnel des électrons, comme ORION (http://195.11.242.249/ave/com/orion/home.html) ont encore de beaux jours devant eux. Selon les applications, on conseillera donc de les utiliser en les combinant (en utilisant un *ou-exclusif*, par exemple) avec des méthodes simples (par exemple, des générateurs congruentiels linéaires) ou des méthodes dont l'imprévisibilité est admise.

L'ERREUR DE NETSCAPE

Dans les applications où peu de bits aléatoires sont nécessaires, l'idée ancienne de mesurer un paramètre dépendant du contexte physique est bonne, surtout si on la combine avec une autre.

C'est ce qui est fait dans les machines à sous des casinos où un générateur simple tourne en permanence, dont on ne prend en compte le résultat qu'à l'instant précis où le joueur joue (ce qui assure une forme d'imprévisibilité). Des mécanismes de mesure de la date ou des caractéristiques de la frappe de celui qui est devant l'ordinateur peuvent être utilisés pour obtenir un petit nombre de bits aléatoires, et c'est ce que fait PGP (*Pretty Good Privacy*, le fameux logiciel de cryptographie utilisé sur *Internet*) pour engendrer ses clefs aléatoires.

Mais là encore attention : il y a deux ans, le protocole de communication confidentielle de *Netscape*, célèbre logiciel de navigation sur *Internet*, a été cassé par des étudiants. Ils avaient remarqué que les clefs étaient engendrées par lecture de certaines parties de la mémoire de l'ordinateur selon un procédé qui ne pouvait conduire qu'à des clefs appartenant à une partie assez réduite de l'ensemble des clefs possibles (ensemble *a priori* trop grand pour être exploré exhaustivement). Les clefs possibles étant en nombre réduit, l'approche exhaustive devenait utilisable et permettait de décrypter les messages secrets. L'erreur a été corrigée.

Cette mésaventure s'est produite fréquemment, et c'est pourquoi une note intitulée *Randomness Recommendation for Security*, rédigée par des experts en sécurité, insiste sur une erreur commune : en piochant dans une très grande base de données (par exemple, le disque dur de l'ordinateur de l'utilisateur), on ne tombe pas toujours sur des bits aléatoires.

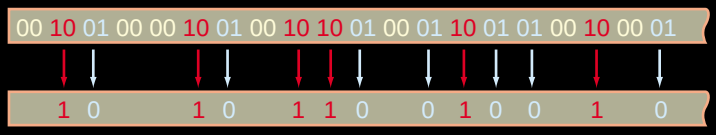
Les disques des ordinateurs (surtout s'ils sont neufs) comportent de grandes zones vides ; de plus, les fréquences d'utilisation des caractères ne sont pas uniformes, ce qui conduit à fausser gravement l'uniformité *a priori* sur les clefs engendrées et rend parfois, comme dans le cas évoqué ci-dessus, envisageable une approche exhaustive.

Les recommandations des experts sont là encore de mélanger plusieurs sources non corrélées, en utilisant le *ou-exclusif* déjà mentionné ou d'autres fonctions plus perfectionnées. Ils insistent aussi sur la taille des clefs qui protègent contre les attaques par énumération exhaustive : elles doivent comporter au moins 50 bits (10^9 clefs pourraient bientôt être traitées par seconde, et donc plus de 10^{15} par mois, ce qui correspond à 50 bits).

Ces exemples confirment que, dans le domaine de la génération de suites aléatoires, courtes ou longues, à usage cryptographique ou pas, les pièges sont partout présents et infiniment variés : on ne se méfie jamais assez du hasard.

6. UNIFORMISATION D'UN GÉNÉRATEUR BIAISÉ

Lorsqu'on utilise un générateur physique, il est souvent difficile d'avoir autant de «0» que de «1» (c'est-à-dire un générateur équilibré). Il y a plus de 40 ans, von Neumann a proposé un moyen très simple de corriger un tel défaut : prendre les bits deux par deux ; supprimer tous les couples «00» et tous les couples «11» ; transformer tous les couples «01» en «0» et tous les couples «10» en «1». Exemple :



On perd quelques bits, mais on corrige un éventuel déséquilibre entre le nombre moyen de «0» et le nombre moyen de «1».
Si la suite initiale donne «1» avec une probabilité p et «0» avec une probabilité $1 - p$, le couple «01» a pour probabilité $p(1–p)$ comme le couple «10», et donc la suite obtenue par le procédé de von Neumann donne bien «0» et «1» avec la même probabilité, c'est-à-dire 1/2.

Jean-Paul DELAHAYE est directeur adjoint du Laboratoire d'informatique fondamentale de Lille du CNRS.

e-mail : delahaye@lifl.fr

L. BLUM, M. BLUM et M. SHUB, *A simple unpredictable pseudo-random number generator,* SIAM J Computing 15.2 pp. 364-383, 1986.

J.-P. DELAHAYE, *Le fascinant nombre Pi*, Éditions *Pour La Science*, Paris, 1997.

L. GOUBIN et J. PATARIN, *La génération d'aléas sur l'ordinateur,* in *Quadrature*, oct.-nov.-déc. 1997, pp. 27-36.

P. L'ÉCUYER, *Random number generation. Hanbook on Simulation*, Ed. Jerry Banks, Wiley, 1997.

B. SCHNEIER, *Cryptographie appliquée*, Thompson Publishing, 1995.

C. P. SCHNORR, *A survey of the theory of random sequences*, in *Basic Problems in Methodology and Linguistics*, Dordrecht, pp. 193-210, 1977.

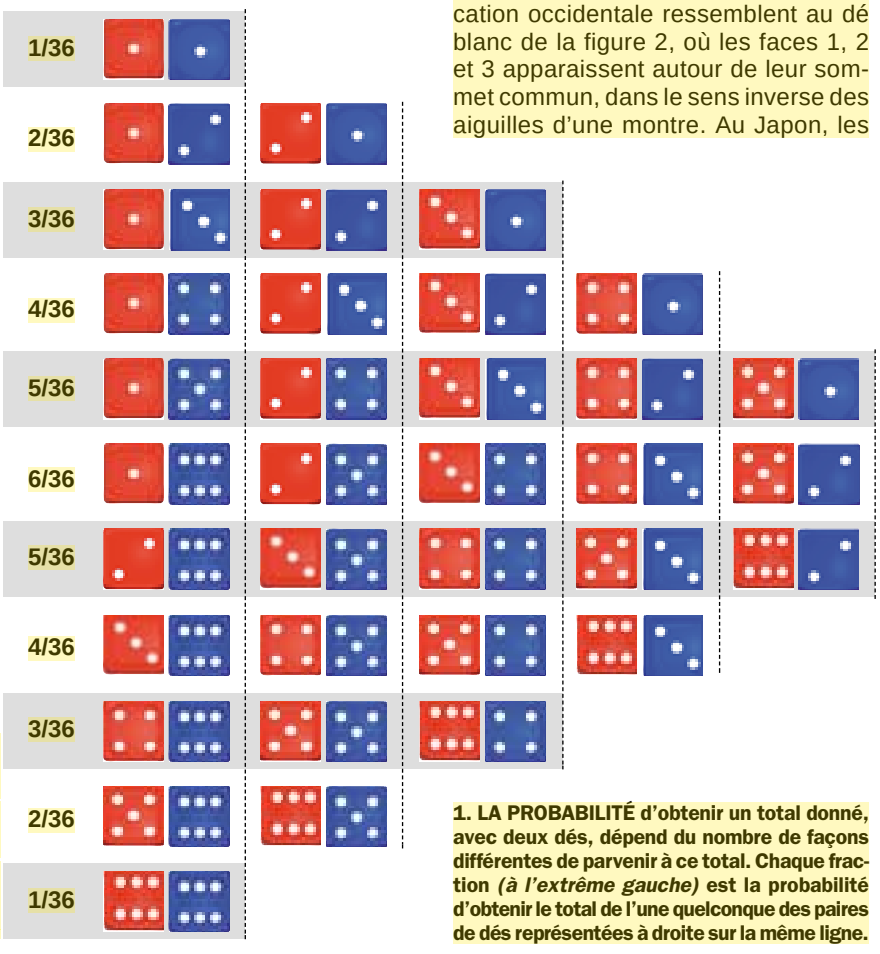
Us et charmes des dés

IAN STEWART

Comme le révèlent les dés, les probabilités vont souvent à l'encontre de l'intuition.

Qui dit dés dit jeux. Selon Hérodote ils remontent aux Lydiens du temps du roi Atys ; selon Sophocle, ils ont été inventés par le Grec Palamède, au cours du siège de Troie. Qu'ils soient la création d'assiégeants désœuvrés semble plausible, mais des archéologues ont découvert des dés cubiques, analogues à ceux d'aujourd'hui, dans des tombes égyptiennes datant de 2 000 ans avant notre ère. Des dés ont également été mis au jour dans des ruines chinoises de 200 ans avant notre ère.

Des dés de toutes formes et aux marques étranges, faits dans des matériaux allant des dents de castors à la porcelaine, ont été utilisés par les Indiens d'Amérique du Nord, par les Aztèques, par les Mayas, par les Polynésiens, par les Inuits et par nombre de tribus africaines. Dans cet article, nous nous limiterons aux dés modernes standards : des cubes dont chaque face porte entre 1 et 6 points, de sorte que la somme des points sur deux faces opposées soit égale à 7. Ainsi, sur les trois paires de faces opposées, on trouve : 1 et 6, 2 et 5, 3 et 4. Cette règle autorise encore deux arrangements, image l'un de l'autre dans un miroir. Aujourd'hui, tous les dés de fabrication occidentale ressemblent au dé blanc de la figure 2, où les faces 1, 2 et 3 apparaissent autour de leur sommet commun, dans le sens inverse des aiguilles d'une montre. Au Japon, les dés ayant cette orientation sont utilisés dans tous les jeux, excepté au mahjong, où l'on adopte l'image miroir (le dé noir de l'illustration). Ces derniers sont aussi utilisés en Chine. Sauf mention contraire, nous n'utiliserons ici que des dés occidentaux.



Illustrations de Jennifer C. Christiansen

1. LA PROBABILITÉ d'obtenir un total donné, avec deux dés, dépend du nombre de façons différentes de parvenir à ce total. Chaque fraction *(à l'extrême gauche)* est la probabilité d'obtenir le total de l'une quelconque des paires de dés représentées à droite sur la même ligne.

2. LES DÉS STANDARDS ressemblent aux dés blancs : les faces marquées 1, 2 et 3 se regroupent dans le sens inverse des aiguilles d'une montre autour de leur sommet commun. Ces faces sont placées en sens inverse dans le dé noir.

On lance souvent les dés par deux, afin d'obtenir un total compris entre 2 et 12. Supposons d'abord que les dés soient «normaux», chaque face ayant la probabilité 1/6 de sortir. La probabilité d'un total donné est égale au quotient du nombre de configurations qui donnent ce total par le nombre de configurations possibles, soit 36.

Imaginons qu'un dé est rouge et l'autre bleu. Un total de 12, ne s'obtient que d'une manière : si le dé rouge et le dé bleu tombent sur 6. La probabilité d'obtenir 12 est donc 1/36. En revanche, un total de 11 s'obtient de deux manières : la première est que le dé rouge indique 6 et le bleu 5 ; la seconde, que le dé rouge indique 5 et le bleu 6. La probabilité d'obtenir 11 est donc 2/36 = 1/18.

Le grand mathématicien et philosophe Gottfried Leibniz (1646-1716) pensait que les probabilités de tirer 12 ou 11 étaient égales, car il ne distinguait pas les dés. Il se fourvoyait ! Tout d'abord l'expérience montre que le 11 sort deux fois plus souvent que le 12. En outre, si l'on ne distinguait pas les dés, la somme des probabilités de tous les totaux possibles serait inférieure à 1. Or, par définition, la probabilité d'obtenir un total entre 2 et 12 lorsque l'on lance deux dés est égale à 1. L'illustration à gauche indique les probabilités des divers totaux possibles, de 2 à 12.

LE CRAPS

Le craps est un jeu où une perception naturelle de ces probabilités est cruciale. Dans ce jeu, qui date des années 1840, le lanceur parie une somme d'argent contre d'autres joueurs. Puis le lanceur jette les deux dés. Avec un résultat de 7 ou de 11 au premier jet, il gagne ; avec 2, 3 ou 12 («craps»), il perd. Un résultat de 4, 5, 6, 8, 9 ou 10 devient son «point». Dans ces derniers cas, il doit alors relancer les dés jusqu'à ce qu'il obtienne à nouveau son «point», mais sans faire 7 (le «craps sortant»!). S'il réussit, il gagne tout l'argent, sinon il le perd.

À l'aide de ces règles du jeu, on calcule que les chances de gain du lanceur sont égales à 244/495 (49,3 pour cent), légèrement défavorables. De quelle manière les joueurs professionnels tournent-ils ce léger désavantage à leur profit? En acceptant ou en rejetant divers «paris additionnels» avec des joueurs. Une autre manière est de tricher, usant de leur dextérité manuelle pour introduire des dés pipés.

Les dés peuvent être truqués de nombreuses façons. Lorsque leurs coins sont rognés ou lorsqu'ils sont «plombés», certains lancers sont plus probables que d'autres. Pis encore, les dés standards peuvent être remplacés par des dés ne portant que trois nombres distincts de points, les faces opposées en ayant le même nombre. La figure 3 en montre un exemple avec seulement des faces 1, 3 et 5. Comme chaque joueur voit au plus trois faces du dé en même temps, et que deux faces adjacentes n'ont jamais le même nombre de points, tout peut sembler normal au cours du jeu. Notons cependant que l'arrangement autour des sommets ne saurait être dans l'ordre standard partout. Si l'ordre 1-3-5 est dans le sens des aiguilles d'une montre autour d'un sommet, il sera dans le sens contraire autour d'un sommet adjacent.

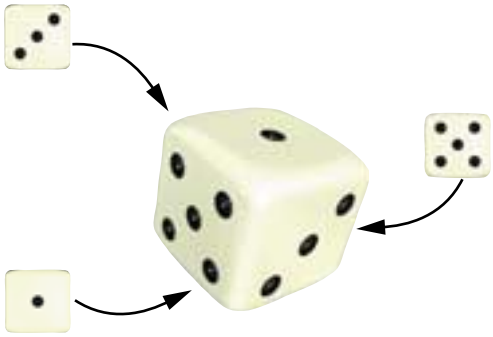
Comment les tricheurs utilisent-ils ces dés? Une paire de dés 1-3-5, par exemple, ne totalise jamais 7, de sorte qu'avec elle, un joueur n'obtient jamais le «craps sortant» éliminatoire. À l'aide d'une combinaison d'un dé 1-3-5 et d'un dé 2-4-6, on n'obtient jamais de total pair 2, 4, 6, 8, 10 ou 12. Ces dés ne doivent être utilisés qu'exceptionnellement si on ne veut pas qu'ils soient détectés : même les joueurs les plus naïfs finissent par s'étonner de ne tirer que des totaux pairs.

LA MAGIE DES DÉS

Nombre de tours de passe-passe ou de prestidigitation utilisent les dés et beaucoup s'appuient sur le fait que les faces opposées ont pour somme 7. Un tour est décrit par Martin Gardner dans son livre *Math' Festival* (Éditions Pour la Science, 1981). Le magicien tourne le dos et demande à une personne de l'assistance de jeter trois dés standards, puis d'additionner les nombres tirés. Ensuite, la personne doit choisir l'un quelconque des dés et ajouter le nombre de sa face cachée au total. Enfin, elle relance ce même dé et ajoute le nombre tiré au précédent total, sans dévoiler aucun de ces totaux. Alors le magicien se retourne et indique immédiatement le dernier total obtenu (il voit les dés, mais ne sait pas quel dé a été relancé).

Comment est-ce possible? Supposons que le premier jet ait donné *a, b, c* et que le dé choisi porte *a*. Le total initial est $a + b + c$. On lui ajoute $7 - a$, ce qui donne $b + c + 7$. Le dé *a* est alors relancé, donnant *d*, et le résultat final est donc $b + c + d + 7$. Or le magicien lit *b*, *c* et *d* sur les dés ; il lui suffit donc de les ajouter entre eux et à 7.

Henry Ernest Dudeney inclut un artifice différent dans son ouvrage *Amusements in Mathematics* (Dover Publications, 1958). Ici encore, le magicien, dos tourné, demande de lancer trois dés. Cette fois, le volontaire double la valeur d'un premier dé et ajoute 5, puis il multiplie le total par 5 et ajoute la valeur d'un second dé, puis multiplie le résultat par 10 et, enfin,



3. AVEC UNE PAIRE DE DÉS PIPÉS ayant seulement 1, 3 ou 5 points sur les faces, le total 7 (le «craps sortant») n'apparaît jamais.

A	3	4	8
B			
1	A	A	A
5	B	B	A
9	B	B	B

A	1	5	9
B			
2	C	B	B
6	C	C	B
7	C	C	B

A	2	6	7
B			
3	A	C	C
4	A	C	C
8	A	A	A

4. LES DÉS NON TRANSITIFS, notés *A, B* et *C*, ont la propriété particulière suivante : en moyenne, *B* bat *A* et *C* bat *B* mais *A* bat *C*. Le dé *A* est marqué 3 3 4 4 8 8, le dé *B*, 1 1 5 5 9 9 et le dé *C*, 2 2 6 6 7 7. Le tableau montre les tirages possibles lorsque deux quelconques de ces étranges dés sont opposés.

Réactions

Le sac de courrier concernant mon article «Le jeu de Junniper Green» (voir *Pour la Science*, juillet 1997) fut à ce point volumineux que «Réactions» lui rendra encore moins justice qu'à l'accoutumée. D'abord, mes excuses pour plusieurs erreurs. La plus grave étant ma référence à «Richard Porteous» comme inventeur du jeu : ce n'est pas Richard, mais Rob. Marc Loveday, de Fruita, Colorado, fait remarquer que le coup 18 de l'encadré omet d'observer que Bob peut choisir 18 au lieu de 2. Beaucoup de lecteurs, dont Arlin Anderson, de Madison, Alabama, et William Shlaer, de Vashon Island, Washington, ont corrigé mes statuts de JG-1 (jeu à une carte), ce qui est secondaire, car Alice ne peut jouer 1 en ouverture, et donc ne peut pas jouer du tout. A. Anderson me corrige aussi sur JG-9, qui est secondaire.

R. Porteous m'a envoyée une analyse de JG-100 effectuée par Peter Conlon, Monique Barendse et Laurie Fischer, trois de ses élèves actuels. Ils montrent en particulier l'existence de stratégies gagnantes si vous commencez par 58 ou par 62. Michael Tibbetts, de Clearwater, Floride, est arrivé à la même conclusion. Il note que les nombres premiers jouent un rôle dans tous les aspects du jeu et les répartit en quatre types : grands (53, 59, 61, 67, 71, 73, 79, 83, 89, 97), assez grands (37, 41, 43, 47), moyens (29, 31) et petits (17, 19). Les ouvertures gagnantes sont les doubles des moyens.

Paul Blatz, de Van Nuys, Californie, rappelle que ce jeu fut étudié dans un cours de théorie des nombres donné à Princeton par Eugene Wigner à la fin des années 1930. Un critère de jeu gagnant dans tous les cas y figurait. L'existence d'une stratégie gagnante à JG-*n* dépend de la parité des exposants des facteurs premiers de la factorisation de *n!* (avec *n!* = factorielle de $n = n \times (n-1) \times (n-2) \times \ldots \times 3 \times 2 \times 1$).