

écrit les différences des carrés à n (nommés les carrés réduits) dans une liste (voir la figure 10).

On détermine maintenant les carrés réduits dont tous les facteurs premiers sont dans la base de facteurs. On pourrait utiliser la méthode des divisions successives, mais un procédé de crible est plus rapide : pour trouver quels carrés réduits sont divisibles par un nombre premier p , on détermine tous les nombres u compris entre 0 et $p - 1$ pour lesquels $(m + u)^2 - n$ est divisible par p . À partir d'une valeur trouvée pour u , on trouve d'autres valeurs en ajoutant ou en soustrayant des multiples de p à cette valeur de u .

Dans l'exemple, le crible par 2 s'applique de la façon suivante : comme $(m + 1)^2 - n$ (égal à 140) est divisible par 2, il en est de même pour $(m - 1)^2 - n$, $(m - 3)^2 - n$ et $(m + 3)^2 - n$. On divise ces nombres par 2 jusqu'à ce que l'on obtienne un nombre impair (troisième ligne de la figure 10).

Le crible par 3 fonctionne de la même manière : on constate que $m^2 - n$ et $(m + 2)^2 - n$ sont divisibles par 3. En partant de $u = 0$ et $u = 2$, on se déplace par pas de longueur 3 vers la droite et vers la gauche, et on divise tant qu'on le peut par 3 les nombres ainsi obtenus. Par la même méthode, on crible par les autres nombres premiers de la base de facteurs. Partout où il y a un 1 à la fin de la liste, on peut décomposer le carré réduit sur la base de facteurs. On détermine la décomposition à l'aide de la méthode des divisions successives.

Ici, nous avons décrit la plus simple version du crible quadratique. La technique est plus vieille que l'ordinateur : l'officier français Eugène Olivier Carissan (1880-1925) construisit une machine mécanique avec laquelle on peut effectuer le crible pour plusieurs nombres premiers à la fois (voir la figure 1).

Pour décomposer un nombre de 100 chiffres, on doit encore apporter de nombreuses améliorations. La base de facteurs et l'intervalle du crible deviennent gigantesques. Pour avoir une idée de leur ordre de grandeur, examinons les paramètres de la factorisation de RSA-120, un nombre de 120 chiffres que les Laboratoires RSA avaient donné à factoriser. La base de facteurs contenait 245 810 éléments, et le système d'équations à résoudre 245 810 inconnues et 252 222 équations. Le calcul aurait duré environ 50 ans sur une seule machine. Pour factori-

ser le nombre de 129 chiffres qui ouvre l'article, c'est aussi le crible quadratique qui fut employé.

Parallélisation

En dehors de l'amélioration de l'algorithme, l'emploi simultané d'un grand nombre d'ordinateurs accélère la factorisation. On peut utiliser soit des calculateurs parallèles (mais ils sont très chers), soit des systèmes partagés, par exemple des réseaux de machines qui sont très peu utilisées pendant la nuit ou le week-end.

À Sarrebrück, nous utilisons un réseau de 250 terminaux répartis sur le campus. Le système LiPS (*Library for Parallel Systems*), que nous avons mis au point, reconnaît automatiquement quand une machine n'est pas sollicitée par son utilisateur principal, et il lance alors, par exemple, une factorisation. Quand l'utilisateur principal veut de nouveau travailler sur sa machine, LiPS arrête le programme de factorisation et le réveille de nouveau dès que la machine est libre. LiPS expédie enfin les résultats des calculs à l'ordinateur qui les centralise.

Même sur notre système réparti, le crible quadratique demande plusieurs semaines de calculs pour la factorisation d'un nombre de 130 chiffres. Le temps de calcul est doublé chaque fois que l'on ajoute trois chiffres, car les carrés réduits que l'on crible sont à peu près de la taille de $\sqrt{n}$.

Les algorithmes plus rapides, mais reposant sur le même principe que le crible quadratique doivent obtenir des

relations grâce à la décomposition de nombres plus petits (de l'ordre non plus de $\sqrt{n}$, mais de n à la puissance $1/3$ ou $1/4$, par exemple). Le seul algorithme clairement meilleur, sur ce point, que le crible quadratique est le crible algébrique, qui a décomposé le nombre de Fermat F_9 .

Avec le crible algébrique, un ensemble d'équipes dont nous faisons partie a décomposé un nombre RSA de 130 chiffres, en avril 1996. Les spécialistes s'attendent à ce qu'un crible algébrique amélioré puisse, dans un petit nombre d'années, factoriser un nombre quelconque de 160 chiffres. Ce serait un pas important, car les nombres composés qui sont employés dans la plupart des systèmes RSA ont moins de 160 chiffres : l'utilisation de tels systèmes RSA ne serait plus sûre.

La factorisation des nombres naturels est-elle un problème difficile? Pour le moment, oui : aucun algorithme au monde ne peut retrouver les facteurs d'un produit de deux nombres premiers de 150 chiffres. De tels produits constituent donc une bonne base pour la sécurité de protocoles cryptographiques, mais pour combien de temps?

Les mathématiciens, malgré des siècles de recherche, n'ont pas encore trouvé un algorithme de factorisation réellement rapide : est-ce suffisant pour affirmer que ce problème est difficile en soi? Non : grâce au développement des ordinateurs, des algorithmes ont déjà été découverts, et rien ne laisse supposer que les progrès considérables des 20 dernières années touchent déjà à leur fin.

Johannes BUCHMANN est professeur d'informatique à l'École d'enseignement supérieur technique de Darmstadt.

Martin HELLMAN, *Les mathématiques de la cryptographie à clef révélée*, in *Pour La Science*, octobre 1979.

Carl POMERANCE, *La recherche des nombres premiers*, in *Pour La Science*, février 1983.

D.M. BRESSOUD, *Factorizations and Primality Testing*, Springer, Heidelberg, 1989.

P. RIBENBOIM, *The Book of Prime Number Records*, Springer, Heidelberg, 1989.

H. COHEN, *A Course in Computational Algebraic Number Theory*, Springer, Heidelberg, 1993.

Arjen K. LENSTRA et Hendrik W. LENS-TRA, *The Development of the Number*

Field Sieve, Springer Lecture Notes in Mathematics, Band 1554, Springer, Heidelberg, 1993.

Hans RIESEL, *Prime Numbers and Computer Methods for Factorization*, 2, Auflage, Birkhäuser, Basel, 1994.

Yves HELLEGOUARCH, *Fermat enfin démontré*, in *Pour La Science*, février 1996.

François MORAIN, *La machine des frères Carissan*, in *Pour La Science*, janvier 1998.

Les bibliothèques de programmes LiDIA et LiPS sont disponibles à l'adresse Internet : <http://www.informatik.th-darmstadt.de/TI/Forschung>

Le site Internet des laboratoires RSA a pour adresse <http://www.rsa.com/rsalabs/>



Michael J. Howell - Haquai

Les martingales et autres illusions

JEAN-PAUL DELAHAYE

Au casino, on peut gagner presque certainement... en risquant beaucoup!

Un de mes amis, passionné de jeux de casino, prétendait qu'il est possible de gagner à la roulette. Je lui ai dit qu'il avait tort parce qu'il est mathématiquement démontré qu'on ne pouvait gagner. Quelle ne fut pas ma surprise lorsqu'il m'a rétorqué :

«Celui qui joue jusqu'à ne plus rien avoir va tout perdre. Il y a donc une façon (au moins) de mal jouer au casino. Mais alors, il y a certainement aussi une façon de bien jouer.»

Je suis resté interloqué et je n'ai pas su lui répondre sur le coup. J'ai l'esprit de l'escalier, aussi je lui réponds ici.

RÈGLES ET PROBABILITÉS

Dans n'importe quel jeu, à chaque fois que l'on mise, il existe une probabilité p de gagner et une probabilité q de perdre sa mise. Il est certain que, soit on gagne, soit on perd! Aussi la somme $p + q$ est-elle égale à 1, et q est égal à $1 - p$. Supposons que, comme à pile ou face, celui qui gagne récupère sa mise plus une somme égale à sa mise ; quand on perd, on laisse sa mise à l'autre joueur, que nous nommerons *la banque*. Dans les casinos, des jeux de ce type, tels le rouge et le noir à la roulette, donnent aux parieurs une chance de gagner inférieure à 1/2. Le jeu n'est alors pas équitable, et l'on soupçonne que c'est pourquoi les casinos sont des entreprises rentables. Nous verrons dans ce qui suit que la rentabilité des casinos sur le long terme est garantie par les mathématiques.

Quelle est la probabilité p des jeux qu'on vous propose? Si vous trouvez un

ami qui accepte de faire la banque et que vous jouez à pile ou face avec une pièce non truquée, votre probabilité p de gain est égale à 1/2. C'est la même probabilité que si vous jouiez sur une couleur à une roulette équitable. À la *roulette simple* (dont l'invention est attribuée à Pascal et qui a été introduite à Paris en 1765), si vous jouez sur noir, vous gagnez quand l'un des 18 numéros noirs sort ; vous perdez quand l'un des 18 numéros rouges sort et quand le zéro (qui est vert) sort. Ainsi la probabilité de gain p est égale à 18/37, soit 0,4864..., car il y a 37 numéros de 0 à 36. À la *roulette française*, la règle est un peu plus compliquée, car quand le zéro sort votre mise reste *prisonnière* jusqu'à ce qu'un prochain lancement de la bille vous la fasse perdre ou récupérer (sans gain), et votre pro-

babilité de gain p est égale à 36/73, soit 0,4931... (voir l'explication de ce 36/73 dans l'encadré 1). À la *roulette américaine*, il y a un zéro et un double zéro verts, tous les deux favorables à la banque, sans système de mises prisonnières. Votre probabilité de gain p est de 18/38, soit 0,4736... Il existe aussi une *roulette mexicaine*, avec un triple zéro, correspondant à un $p = 18/39 = 0,4615$, mais c'est pour les *gringos*.

Pour calculer le gain de la banque, imaginons que 100 francs sont misés sur le noir et comptabilisons ce que, en moyenne, la banque perd (c'est-à-dire paie) et gagne. Dans une proportion de p cas, elle perd 100 francs ; dans une proportion de $1 - p$ cas, elle gagne 100 francs. Aussi la banque gagne en moyenne : $100(1 - p) - 100p$ francs, soit $100(1 - 2p)$ francs, que l'on appelle parfois *l'espérance mathématique* de gain de la banque pour 100 francs misés. Dès que p est inférieur à 1/2, alors $1 - 2p$ est positif, et donc la banque gagne en moyenne.

Ce gain moyen de la banque pour 100 francs misés est de 0 franc à pile ou face (ce jeu n'est pas proposé dans les casinos!) ; de 1,36 franc à la roulette française (avec système des mises prisonnières) ; de 2,70 francs pour la roulette simple, de 5,26 francs pour la roulette américaine ; de 7,69 francs pour la mexicaine.

Est-il possible, par un comportement rusé, de contourner ce gain théorique moyen de la banque et de le retourner en sa faveur? La question est historique : l'idée d'étudier par la théorie des probabilités les meilleures façons de jouer

1. LES RÈGLES DE LA ROULETTE FRANÇAISE

Il y a 37 numéros (de 0 à 36). Une bille lancée par le croupier sur une sorte de disque (appelé cylindre) qui tourne et comporte des encoches où la bille se stabilise (sur un numéro). Les *chances simples* sont *pair* (le 0 n'est pas considéré comme pair!), *impair*, *passé* (de 19 à 36), *manqué* (de 1 à 18), *rouge* (1, 3, 5, 7, 9, 12, 14, 16, 18, 19, 21, 23, 25, 27, 30, 32, 34, 36), *noir* (les autres numéros, sauf zéro, qui est vert). Si on joue une *chance simple* et qu'elle tombe, on récupère sa mise accompagnée d'un gain équivalent payé par la banque. Si elle ne tombe pas, on perd sa mise, sauf si c'est le zéro qui tombe, auquel cas la mise est *prisonnière* ; il faut alors attendre le coup suivant qui, soit permet de la récupérer (sans gain) si la chance simple choisie tombe, soit la fait perdre. Si le zéro tombe à nouveau, la mise reste prisonnière, etc.

Quand le zéro tombe, il y a symétrie entre les deux hypothèses : récupérer sa mise ou la perdre, et donc on a une chance sur deux de récupérer sa mise (sans gain) et une chance sur deux de la perdre. Donc, dans 1 cas sur 74, la partie ne compte pas (zéro, puis récupération de la mise) ; dans 1 cas sur 74, la mise est perdue (un zéro, puis perte de la mise) ; dans 18 cas sur 74, gain immédiat.

En éliminant le cas où la partie ne compte pas, la probabilité de gagner est 36/73.

Si l'on met sa mise sur un «numéro plein» et qu'il sort, on gagne 36 fois sa mise. Si on utilise autre chose que les chances simples, il n'y a pas de système de mises prisonnières, et donc la part prise par la banque est plus forte : 1/37 (au lieu de 1/73).

n'est pas récente. Pascal, d'Alembert, Moivre, Lagrange, Laplace et bien d'autres mathématiciens, parmi les plus éminents, s'y sont intéressés. Si de nombreux résultats ont été obtenus très tôt, même en ce siècle, des principes nouveaux permettent de mieux comprendre les stratégies de jeu à la roulette. Pour comparer les différentes méthodes de jeu, dénommées martingales, nous nous plaçons dans la peau d'un joueur qui, au départ, a un capital de A francs et qui veut partir du casino dès qu'il a B francs. Comment doit-il s'y prendre en jouant sur le noir et le rouge ?

LA STRATÉGIE DES MISES CONSTANTES

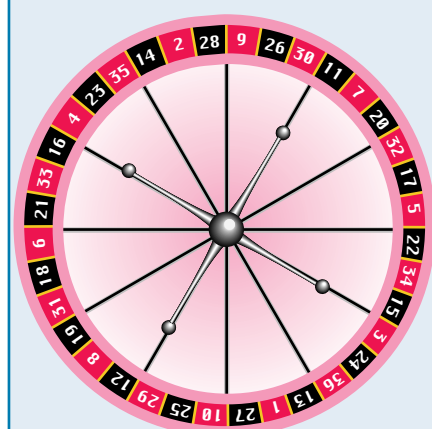
La stratégie des mises constantes consiste à jouer K francs à la fois jusqu'à, soit avoir perdu son capital de A francs, soit avoir atteint l'objectif des B francs. Cette martingale est élémentaire, pourtant nombre de gens l'utilisent.

Comment fixer la valeur de K ? Faut-il jouer 1 franc à chaque fois, ou 5 francs, ou 10 francs ? Pour répondre à cette question, deux techniques sont envisageables : la simulation informatique et l'étude mathématique (nous avons exclu l'essai dans

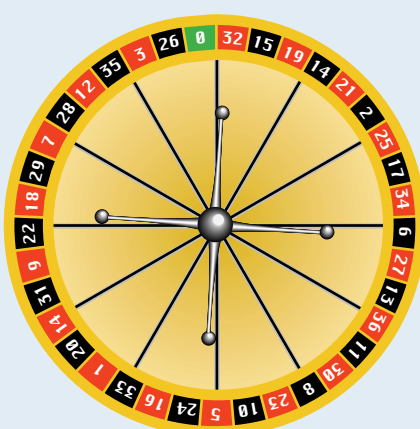
un casino, car nous ne sommes ni assez riches... ni assez patients).

C'est seulement depuis que nous disposons de machines puissantes et faciles à programmer que nous pouvons mener les simulations qui *de facto* étaient interdites aux mathématiciens avant 1945, date de la mise au point des premiers calculateurs électroniques. Comme de nombreux problèmes complexes ne pouvaient être résolus par le raisonnement, les calculateurs électroniques furent, dès leur conception, utilisés pour calculer la probabilité de succès de certaines patiences. Dans ces simulations, où sont incluses

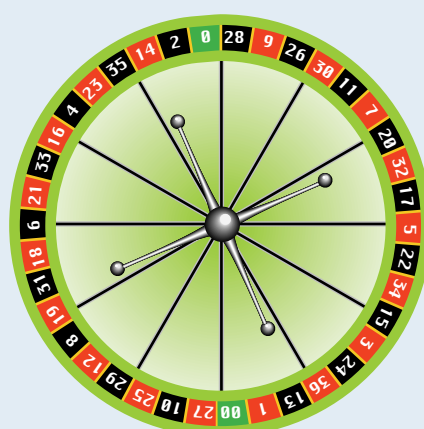
2. PROBABILITÉS DE GAIN SELON LES MARTINGALES ET LES MISES POUR TROIS ROULETTES ET UNE FORTUNE INITIALE DE 10 FRANCS



ROULETTE ÉQUITABLE OU JEU DE PILE OU FACE
 $p = 1/2$



ROULETTE FRANÇAISE AVEC MISES PRISONNIÈRES
 $p = 36/73 = 0,4931$



ROULETTE AMÉRICAINNE
 $p = 18/38 = 0,4736$

ROULETTE ÉQUITABLE OU JEU DE PILE OU FACE $p = 1/2$			ROULETTE FRANÇAISE AVEC MISES PRISONNIÈRES $p = 36/73 = 0,4931$			ROULETTE AMÉRICAINNE $p = 18/38 = 0,4736$		
PROBABILITÉS DE :			PROBABILITÉS DE :			PROBABILITÉS DE :		
1) GAGNER 10 %	0,9125		1) GAGNER 10 %	0,8956		1) GAGNER 10 %	0,8550	
2) DOUBLER SA MISE	0,4998	0,4998	2) DOUBLER SA MISE	0,4433	0,4879	2) DOUBLER SA MISE	0,2619	0,4485
3) DÉCUPLER SA MISE	0,0974	0,0994	3) DÉCUPLER SA MISE	0,0222	0,0773	3) DÉCUPLER SA MISE	0,0002	0,0323
MISES			MISES			MISES		
1 F	5 F	10 F	1 F	5 F	10 F	1 F	5 F	10 F
0,9125	0,4998	0,4995	0,8956	0,4879	0,4920	0,8550	0,4485	0,4754
0,4998	0,4998	0,4995	0,4433	0,4879	0,4920	0,2619	0,4485	0,4754
0,0974	0,0994	0,1001	0,0222	0,0773	0,0876	0,0002	0,0323	0,0615
MARTINGALE D'ALEMBERT			MARTINGALE GÉOMÉTRIQUE			MARTINGALE GÉOMÉTRIQUE		
PROBABILITÉS DE :			PROBABILITÉS DE :			PROBABILITÉS DE :		
1) GAGNER 10 %	0,9080		1) GAGNER 10 %	0,9003		1) GAGNER 10 %	0,8866	
2) DOUBLER SA MISE	0,5042	0,5018	2) DOUBLER SA MISE	0,4784	0,4908	2) DOUBLER SA MISE	0,4192	0,4558
3) DÉCUPLER SA MISE	0,1021	0,1009	3) DÉCUPLER SA MISE	0,0808	0,0908	3) DÉCUPLER SA MISE	0,0450	0,0623
MISES			MISES			MISES		
1 F	5 F	10 F	1 F	5 F	10 F	1 F	5 F	10 F
0,9080	0,5042	0,5012	0,9003	0,4784	0,4950	0,8866	0,4192	0,4743
0,5042	0,5018	0,5012	0,4784	0,4908	0,4950	0,4192	0,4558	0,4743
0,1021	0,1009	0,1018	0,0808	0,0908	0,0917	0,0450	0,0623	0,0710
JEU HARDI			JEU HARDI			JEU HARDI		
PROBABILITÉS DE :			PROBABILITÉS DE :			PROBABILITÉS DE :		
1) GAGNER 10 %	0,9087	0,9091	1) GAGNER 10 %	0,9038	0,9042	1) GAGNER 10 %	0,8901	0,8896
2) DOUBLER SA MISE	0,5018	0,5	2) DOUBLER SA MISE	0,4932	0,4931	2) DOUBLER SA MISE	0,4736	0,4736
3) DÉCUPLER SA MISE	0,1011	0,1	3) DÉCUPLER SA MISE	0,0954	0,0950	3) DÉCUPLER SA MISE	0,0820	0,0819
VALEUR EXPÉRIMENTALE			VALEUR EXPÉRIMENTALE			VALEUR EXPÉRIMENTALE		
1 F	5 F	10 F	1 F	5 F	10 F	1 F	5 F	10 F
0,9087	0,5018	0,1011	0,9038	0,4932	0,0954	0,8901	0,4736	0,0820
0,5018	0,5	0,1	0,4932	0,4931	0,0950	0,4736	0,4736	0,0819
0,1011	0,1	0,1	0,0954	0,0950	0,0950	0,0820	0,0819	0,0819

3. DEUX ARNAQUES AU CASINO

Les mises en défaut des casinos sont rares, et d'autant plus succulentes. Elles illustrent la devise de droit romain : *Nemo auditur suam turpitudinem allegans*. Nul ne peut alléguer (pour se justifier) sa propre turpitude.

La première est plus juridique que scientifique. Un joueur regardait la table de la roulette depuis un certain temps, lorsqu'il tendit un billet au croupier : «Je vous donne la mise que j'ai perdue, assura-t-il, j'ai joué mentalement le cinq et il n'est pas sorti.» Le croupier accepta la mise. Quelques instants plus tard, le même joueur apostropha le croupier : «J'ai joué dans ma tête le huit, qui vient de sortir. Vous me devez trente-six fois ma mise.» L'histoire raconte que le casino dut s'exécuter : le croupier ayant accepté la première mise «mentale», il devait payer la seconde.

La seconde nécessitait une mise en scène plus subtile. Un joueur vint trois jours de suite, en Rolls pour donner confiance, avec son valet, jouer à la roulette. Il misait sur le rouge jusqu'à ce qu'il perde 100 000 francs, puis s'en allait. Le quatrième jour, son valet vint seul et demanda à s'entretenir avec le directeur du casino. «Mon maître est malade, et je dois jouer tous les jours 100 000 francs sur le rouge. Bien sûr, je vais perdre, aussi j'entends que vous me dédommiez de 50 000 francs. Ainsi, nous gagnerons tous les deux 50 000 francs.» Le directeur du casino accepta. Il ignorait qu'un baron, de mèche avec le valet, jouait le noir quand son compère jouait le rouge, et chacun gagnait quand l'autre perdait. Ainsi le casino ne gagnait rien à la table de jeu, et nos escrocs étaient certains d'y équilibrer à peu près leurs gains et leurs pertes (car il faut compter les cas où la bille tombait sur le 0 et où tous les deux perdaient) ; ils étaient assurés de gagner à peu près la somme de 50 000 francs versée par le casino.

les règles de la patience, le programme tire aléatoirement des configurations de départ et dénombre ensuite succès et échecs, donc la probabilité de gain.

Examinons trois objectifs concrets :

- (a) passer de $A = 10$ francs à $B = 100$ francs (décupler son capital initial)
- (b) passer de $A = 10$ francs à $B = 20$ francs (doubler son capital)
- (c) passer de $A = 10$ francs à $B = 11$ francs (augmenter son capital de 10 pour cent)

Les mises jouées à chaque fois seront soit 1 franc, soit 5 francs, soit 10 francs.

Les résultats des simulations informatiques sont indiqués dans le tableau de l'encadré 2 pour le jeu de pile ou face (ou une roulette honnête), la roulette française et la roulette américaine. Chaque évaluation représente 50 000 essais (ce qui, à raison d'un essai toutes les cinq minutes, 12 heures par jour, correspond à plus d'un an de jeu en salle pour chaque case des tableaux).

Ici les simulations ne sont pas indispensables, car ce problème a une solution mathématique, découverte dans un cas particulier par Huygens en 1657, généralisée par Bernoulli en 1680, puis précisée par Moivre en 1711. Lorsque p est égal à $1/2$ et la mise égale à K , la probabilité de réussir est A/B ; lorsque p est inférieure à $1/2$, elle est de $[1 - (q/p)^{A/K}] / [1 - (q/p)^{B/K}]$

Ainsi, plus p est petit, moins vous réussirez ; ce n'est pas une surprise !

Plus B/A est grand (plus vous êtes gourmand), moins vous avez de chances de réussir ; ce n'est pas étonnant non plus.

Toutefois, lorsque p est fixé, vous maximisez vos chances de réussite en prenant K le plus grand possible. Ce résultat n'est pas évident ! Pour décupler votre fortune et passer de 10 à 100 francs en utilisant la stratégie des mises constantes, il vaut mieux miser 10 francs à chaque tirage que 5 francs, et il est plus avantageux de miser 5 francs que 1 franc.

Si l'on compare les résultats théoriques donnés par la formule de Huygens-Bernoulli-Moivre avec ceux de nos simulations réalisées en faisant 50 000 essais, on remarque que seuls deux chiffres donnés par l'expérimentation sont fiables.

LOI DE LA RUINE CERTAINE

Lorsque deux joueurs s'affrontent jusqu'à ce que l'un d'eux soit ruiné, l'un des deux joueurs finit nécessairement par perdre (même si p est égal à $1/2$ et qu'ils disposent tous deux de la même somme initiale). C'est ce qu'on appelle la loi de la ruine certaine. Si les fortunes sont inégales, la formule de Huygens-Bernoulli-Moivre montre que celui qui a la plus grande fortune gagnera plus souvent («l'argent va à l'argent»), en particulier dans le cas p égal à $1/2$, la probabilité que le joueur 1 gagne est égale à :

$$\text{Fortune du joueur 1}$$

(Fortune du joueur 1 + Fortune du joueur 2)

Si vous affrontez un joueur deux fois plus riche, il a 2 fois plus de chances de gagner que vous ; s'il est cent fois plus riche il gagnera 100 fois sur 101 ; si vous affrontez un joueur infiniment riche, vous

êtes certain de tout perdre, même lorsque le jeu est équitable. La durée moyenne d'une partie où votre fortune de départ est N francs contre un joueur infiniment riche (le casino), c'est-à-dire le nombre de mises de 1 franc que vous jouez avant d'avoir tout perdu est égale à $N/(p-q)$; à la roulette française, si vous jouez par 10 francs, il faudra en moyenne 730 coups pour que vous soyez ruiné. Lorsqu'un jeu est en votre faveur, p supérieur à $1/2$, même si vous affrontez un joueur infiniment riche avec une somme de départ finie, vous deviendrez infiniment riche dans une bonne proportion de cas.

Les tableaux et les résultats mathématiques montrent qu'avec p inférieur à $1/2$ les chances de réussir à doubler son capital sont inférieures à $1/2$. La stratégie des mises constantes n'est pas assez astucieuse pour renverser l'avantage initial du casino, il faut essayer autre chose.

LA MARTINGALE DE D'ALEMBERT

Le nom du procédé de jeu suivant ne signifie pas que d'Alembert a cru qu'il s'agissait d'une méthode permettant de gagner.

Martingale de d'Alembert (ou montante de d'Alembert) : la mise initiale est de K francs ; ensuite, à chaque fois que vous gagnez, vous diminuez votre mise de K francs (parce que vous pensez que la chance vient de vous être favorable, et qu'elle risque de l'être moins le coup suivant), et à chaque fois que vous perdez vous l'augmentez de K francs (la chance devrait maintenant mieux vous servir, croyez-vous).

Lorsque la règle conduit à miser 0 franc, on ne diminue pas la mise, qui reste donc K francs. Lorsque nous sommes près du but, nous ne misons pas plus qu'il n'est nécessaire pour l'atteindre : si, par exemple, lorsque l'objectif est 100 francs, la règle de d'Alembert nous conduit à 98 francs et nous suggère de miser 6 francs, nous ne jouons que 2 francs. Pour chaque résultat, 50 000 essais ont été faits ; les résultats sont donnés dans l'encadré 2.

Là encore, plus p est favorable à la banque, moins on réussit souvent. Ensuite, dans le cas p égal à $1/2$, les simulations retrouvent approximativement les valeurs calculées pour les mises constantes (les écarts par rapport aux valeurs théoriques, $1/10$, $1/2$ et $10/11$ ne sont pas significatifs). Cela se déduit d'un résultat théorique remarquable qui indique que, dans le cas p égal à $1/2$, pour passer de A francs à B francs, toutes les stratégies se valent. Si p est égal à $1/2$, quoi que vous fassiez vous réussirez A fois sur B , ni plus souvent, ni moins souvent.

Troisième résultat : comme dans le cas des mises constantes, on augmente

ses chances avec des valeurs de K croissantes. Pour p égal à $18/38$, par exemple, selon que vous partez de K égal à 1 franc, K égal à 5 francs, ou K égal à 10 francs, votre probabilité de réussite passe de 3,56 pour cent à 3,72 pour cent, puis à 4,79 pour cent.

Lorsque p est inférieur à $1/2$, des stratégies de jeu essayées pour l'instant, c'est la stratégie de d'Alembert avec K égal à 10 qui est la meilleure.

Peut-on améliorer la probabilité de décupler, doubler ou augmenter de 10 pour cent votre fortune initiale ?

LA MARTINGALE GÉOMÉTRIQUE

La martingale géométrique est la plus populaire de toutes, tant son principe est simple et, à première vue, infaillible. C'est *La martingale*. On commence par miser K francs ; si on perd, on double la mise, et on la double ainsi jusqu'à ce que l'on gagne. Lorsque cela arrive, on a perdu $K + 2K + 4K + \dots + 2^{n-1}K$ et on a gagné $2^n K$, donc on a gagné K francs. On recommence alors tout, avec une mise de K francs.

Exemple : vous misez 1 franc, vous perdez ; vous misez alors 2 francs, vous perdez ; vous misez alors 4 francs, vous gagnez. Au total, vous avez gagné 4 francs et perdu 3 francs, ce qui donne un bilan positif de 1 franc.

Si l'on pouvait ainsi toujours doubler, on gagnerait K francs à chaque série et, petit à petit, on accumulerait tout l'argent que l'on veut. Cherchez l'erreur.

Elle est double. D'abord, quand on n'a plus rien, on ne peut plus miser ; or il arrive qu'il y ait de longues séquences de tirages identiques (le record dans une salle de casino est une série de 42 fois le rouge). Ensuite, les mises autorisées sont limitées (à 1 000 fois la mise la plus faible pour une table donnée dans les casinos français) et donc, même si vous êtes très riche, vous ne pourrez pas appliquer la martingale géométrique plus de 10 étapes.

Rendons-la praticable en précisant nos choix en cas de blocage. On double la mise précédente si on a perdu, tant que rien ne s'y oppose, mais si on peut atteindre l'objectif de B francs en misant moins que ce que la règle indique, on le fait, et si on n'a pas assez pour miser conformément à la règle, on met le maximum dont on dispose.

K est la mise initiale. Pour chaque résultat, 50 000 essais ont été faits. Là encore, les résultats sont donnés sur la figure 2. Si p est égal à $1/2$, rien ne permet de dévier de A/B ; on vérifie, à nouveau, que la roulette américaine est bien plus productive que la roulette française (pour la banque, bien sûr!).

On découvre que la stratégie géométrique est meilleure que les deux autres méthodes de jeu envisagées auparavant, et qu'elle est meilleure pour K égal à 10 francs que pour K égal à 5 francs ou K égal à 1 franc.

Il semble que non seulement l'argent va aux riches, mais aussi qu'il va (ou reste, mieux!) à ceux qui misent plus gros! Les stratégies les plus violentes sont les meilleures. Plus grosse est la valeur de K , mieux c'est, et plus violente est la stratégie, mieux c'est (la géométrique est plus violente que la d'Alembert, elle-même plus violente que les mises constantes). Cette règle est-elle générale? Si oui, comment la formuler précisément?

Le fait que, pour p supérieur à $1/2$, nous trouvons que la martingale de d'Alembert avec K égal à 1 est très légèrement meilleure pour doubler son capital que la géométrique avec K égal à 1 (seule exception numérique à la supériorité générale de la géométrique) ne contredit pas notre remarque générale, car, dans la d'Alembert avec K égal à 1, la baisse des mises se fait plus lentement que dans la géométrique (aussi avec K égal à 1) et conduit donc, en moyenne, à un comportement plus violent. La violence du comportement semble en toute généralité le bon comportement à ce jeu.

LE THÉORÈME DU JEU HARDI

Ce résultat général que tout le monde devrait connaître sera dénommé le théorème du Jeu hardi ou loi de Dubins et Savage (ils furent les premiers à l'établir, en 1956). Le précepte est moral, il faut passer le moins de temps possible devant le tapis vert.

Théorème du Jeu hardi. La meilleure façon de jouer dans un jeu à deux options de probabilités p et $1 - p$ avec p inférieur à $1/2$, pour passer de A à B , consiste à miser toujours ce qui permet d'approcher le plus le but visé.

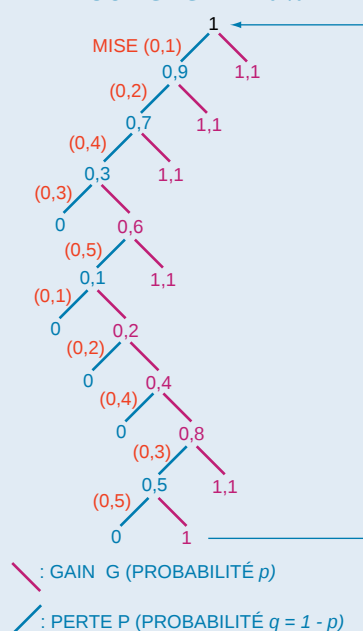
Toutes les méthodes de jeu, comme nous l'avons constaté par expérimentation, ne sont pas équivalentes. Mon ami avait raison sur un point : pour atteindre un but donné, il y a des stratégies meilleures que d'autres (ce qui ne veut pas dire qu'on peut gagner contre le casino).

Le théorème du Jeu hardi nous conduit à de meilleures stratégies que celles envisagées jusqu'à présent pour décupler, ou augmenter de 10 pour cent, notre capital. Si votre objectif est de décupler votre pécule (passer de A à $10A$), vous devez miser A la première fois (c'est le plus que vous pouvez faire) ; si vous avez gagné, misez $2A$, puis, si vous avez gagné, misez $4A$; puis finalement misez $3A$ (car cela vous suffit pour atteindre $10A$). Si vous perdez au dernier coup, vous vous trouvez avec $7A$, il vous manque $4A$, vous misez donc $4A$. Etc.

Cette stratégie ressemble à la martingale géométrique dans le cas où l'on prend K égal à A , mais elle ne lui est pas complètement équivalente, car lorsque vous venez de perdre, plutôt que de repartir de K (martingale géométrique), ici vous jouez ce qui est nécessaire pour atteindre l'objectif en un coup, si c'est possible.

Dans le cas de l'objectif du doublement du capital de 10 francs à 20 francs, la stratégie des mises constantes avec K égal à 10 francs et la martingale géométrique avec K égal à 10 francs sont identiques à

4. STRATÉGIE OPTIMALE POUR GAGNER 10 %



En suivant les divers chemins de gain, on voit que la probabilité de passer d'une somme à $1,1$ fois cette somme est : probabilité de G (p) + probabilité de P puis G (qp) + probabilité de P puis P puis G (q^2p) + probabilité de P puis P puis P puis G (q^3p) + probabilité de P puis P puis P puis P puis G (q^4p) + probabilité de P puis P puis P puis P puis P puis G (q^5p) puis boucler en revenant à 1, après simplification.

$$r = (p + qp + q^2p + q^3p + q^4p + q^5p) / (1 - q^5p)$$

Avec la stratégie du Jeu hardi à la roulette française ($p = 36/73$), si vous êtes prêt à risquer 1 000 F pour en gagner 100, vous réussirez dans 90,426 pour cent des cas.

la stratégie du Jeu hardi, qui se réduit alors à miser une fois 10 francs (la probabilité d'aboutir est évidemment p). Les résultats expérimentaux obtenus en faisant 200 000 essais pour chaque cas (l'expérimentation étant plus rapide, on a augmenté le nombre d'essais pour avoir une meilleure précision) sont indiqués dans le tableau de l'encadré 2.

Notons que, si vous êtes prêt à risquer 10 francs pour gagner 1 franc (ou 10 000 francs pour gagner 1 000 francs), en appliquant la règle de jeu donnée par le schéma, vous réussirez en France avec une probabilité 0,9042656... (voir l'encadré 4), ce qui est assez raisonnable. Ne nous réjouissons pas trop : si vous appliquez cette méthode de jeu tous les soirs régulièrement, les soirs où vous gagnez (plus de 90 pour cent des cas) ne compensent pas, à long terme, ceux où vous perdez, car quand vous perdez, vous perdez dix fois plus que quand vous ne gagnez.

INEXISTENCE DE MARTINGALE

Le résultat de Dubins et Savage est décevant, car il indique que vous devez jouer le plus vite possible. Si ce qui vous amuse est le jeu, la conclusion obtenue est la pire de toutes celles qu'on pouvait découvrir. Cela est en fait lié à la loi de la perte constante : *Quand on joue à un jeu avec une probabilité p inférieure à $1/2$ de gagner (pour le joueur), alors, quelle que soit la stratégie utilisée, on perd «en moyenne» proportionnellement à ce qu'on mise.*

Tout cela est tristement simple : les pertes moyennes ne dépendent que des sommes posées sur la table et sont déterminées par le coefficient p du jeu. La façon de jouer est sans importance, martingale géométrique ou Jeu hardi ou stratégie optimale, tout est équivalent.

Une conséquence de la loi de la perte constante est aussi qu'aucune martingale ne retourne jamais les probabilités de gains en votre faveur. Autrement dit, il n'existe pas de martingale. En particulier : (i) aucun avantage ne peut être obtenu en ne jouant que sur certains tirages ; (ii) aucun avantage ne peut être obtenu par celui qui décide de la fin de la partie (le droit de faire charlemagne ne sert à rien) ; (iii) même si l'on veut diminuer son espérance par franc misé, on ne le peut pas. Finalement, plus vous jouez, plus vous perdez, inéluctablement. Pour perdre le moins, vous devez jouer le moins possible. Pour ne pas perdre du tout, vous ne devez pas jouer du tout.

Il est difficile de se persuader complètement que prendre en compte le passé est inutile, et que ce n'est pas parce que le rouge est sorti 10 fois de suite que le noir a plus de chances au coup suivant. Cependant il faut s'y résoudre : les jeux de

casino sont idiots, et ce sont bien des entreprises commerciales dont la rentabilité est assurée sur le long terme par des lois mathématiques démontrées et testables.

Au total, mon ami qui prétendait pouvoir gagner à la roulette a tort : plus on joue plus on perd, rien n'y fait. Dans son raisonnement de départ, il y avait une erreur : si l'on vous donne un total de sommes à miser, il n'existe ni de bonnes façons de le jouer, ni de mauvaises. Ramené au total de l'argent que vous posez sur la table, vous ne pouvez ni bien jouer, ni mal jouer.

Toutefois, comme Paul Deheuvels le fait remarquer, les règles du jeu de la roulette autorisent d'autres mises que les mises simples, par exemple les numéros pleins, qui conduisent à gagner un multiple de sa mise ou à la perdre (avec une probabilité de gain plus faible qui maintient une espérance de gain positive pour le casino). Il n'est pas impossible qu'en utilisant pleinement les mises autorisées d'autres méthodes permettent par exemple d'améliorer un peu le 0,90426... trouvé pour passer de 10 à 11 à la roulette française.

Hélas, il n'y a pas grand-chose à grignoter, car pour passer de 10 à 11, à un jeu défavorable, le produit de la probabilité de réussite r par votre gain souhaité (1 franc) sera toujours inférieur à votre probabilité de perdre vos 10 francs, multipliée par cette perte. Donc : $1r < (1 - r)10$, qui implique que $r < 10/11 = 0,90909...$ (ce 10/11 que l'on obtient en faisant n'importe quoi lorsque p est égal à $1/2$ est une barrière inaccessible lorsque p est inférieur à $1/2$).

GAGNER AUTREMENT ?

Nous avons jusqu'ici supposé que le jeu était équitable, dans le sens que la roulette était bien équilibrée : chaque numéro a une chance sur 37 de sortir (une sur 38 à la roulette américaine). Il se peut que cela ne soit pas le cas parce que la roulette est truquée ou usée (la durée de vie d'une roulette utilisée tous les soirs est d'environ dix ans).

Vient alors l'idée de miser sur ce qui tombe le plus souvent, de façon à profiter de l'inégalité des chances entre numéros. L'idée générale d'exploiter l'imperfection des roulettes n'est pas absurde et elle fut effectivement utilisée par William Jaggars à la fin du XIX^e siècle. Il gagna ainsi 1 500 000 francs à Monte-Carlo, à la suite d'une analyse fine des fréquences de sortie des numéros. Depuis, les casinos ont compris que leur intérêt est que les roulettes soient bien équilibrées et ils y veillent soigneusement : l'intérêt d'un casino à la roulette est qu'il n'y ait aucun biais !

Plus récemment, en 1978 et 1979, Norman Packard et Doyné Farmer, par une technique de mesure de la vitesse de la boule et du cylindre portant les numéros réussirent à prévoir la zone où devait arriver la bille avec une précision suffisante pour renverser l'avantage du casino en leur faveur. Cela leur permit de gagner plusieurs milliers de dollars. Les mesures et les calculs étaient faits à l'aide d'appareillages qu'ils portaient sur eux, cachés dans leurs vêtements. Ayant observé une roulette attentivement, je dois avouer que je doute de la véracité de cette histoire.

Un autre jeu de casino doit être mentionné, le black jack. Contrairement à la roulette, il n'est pas toujours défavorable aux joueurs. À la suite d'études menées à l'aide d'ordinateurs depuis 1956 plusieurs mathématiciens ont mis au point des techniques de jeu (nécessitant le plus souvent de mémoriser les cartes qui passent) qui, quand elles sont appliquées rigoureusement (ce qui demande de longues semaines d'entraînement), renversent les chances en faveur du joueur. Certains joueurs tentèrent de s'aider d'ordinateurs cachés sur eux pour appliquer ces méthodes plus facilement. Les casinos ont appris à repérer et à dissuader les joueurs trop concentrés (parce qu'ils mémorisent les cartes jouées) qui tentent d'appliquer ces méthodes et qu'on appelle des «compteurs de cartes». Les joueurs se font aussi repérer par les variations brusques des mises qu'ils font et qui sont caractéristiques (il paraît qu'en France les casinos n'empêchent pas les «compteurs de cartes» de jouer ; je n'ai pas vérifié !). De plus, les casinos se sont mis à utiliser des quadruples jeux de cartes pour rendre ces méthodes inopérantes. Pour faire fortune, il n'y a décidément rien à attendre des jeux de casino.

Jean-Paul DELAHAYE est professeur d'informatique à l'Université de Lille.

T. BASS, *The Newtonian Casino*, Éditions Longman, 1990.

Y. COURCHESNE, *Les secrets du black jack*, Les Éditions de l'Homme, Montréal, 1993.

P. DEHEUVELS, *La probabilité, le hasard et la certitude*, PUF, 1990.

R. EPSTEIN, *The Theory of Gambling and Statistical Logic*, Academic Press, San Diego, 1970, 1995.

A. NEURISSE, *Les jeux d'argent et de hasard*, Éditions Hermé, 1991.

M. ORKIN, *Can you win?* W. H. Freeman and Company, New York, 1991.

P. TOUGNE, *La mathématique des jeux, chapitre 18 : «Roulette, loto et probabilités»*, Éditions Pour la Science / Belin, pp. 147-146, 1990.

