4

Le désordre total existe-t-il?

Comment faire pour se comporter de manière quelconque?

Être ordonné est difficile, chacun le sait bien. Plus étonnant, être vraiment désordonné est aussi très difficile... Examinons un exemple.

Monsieur Hasard chaque matin prend du café ou du thé et, comme il désire ne pas prendre toujours la même chose, il oscille régulièrement : café, thé, café, thé, café, thé, etc. Mais cette oscillation l'ennuie aussi! Il décide donc de ne jamais répéter la même séquence, en particulier de ne jamais répéter deux fois de suite, café, thé. Bien sûr, c'est impossible : s'il ne veut jamais répéter deux séquences identiques consécutivement, alors, après un jour avec café, il doit boire du thé et, après un jour avec thé, il doit boire du café, ce qui au quatrième jour le conduit obligatoirement à la répétition de la paire café-thé. Très bien, se dit-il, puisque ne jamais boire deux fois de suite la même chose est impossible, je me contenterai de ne jamais répéter trois fois de suite la même séquence, et ainsi je me comporterai de la manière la plus désordonnée possible.

La suite de Thue-Morse

Est-ce faisable, et Monsieur Hasard a-t-il raison de croire que cela lui évitera l'ennui? Autrement dit, existe-t-il des suites de 0 et de 1 ne comportant jamais trois fois consécutivement la même séquence? Si oui, peut-on les considérer comme totalement désordonnées?

La réponse – oui à la première question, non à la seconde – est donnée par ce qu'on appelle la suite de Thue-Morse. Pour obtenir cette suite, on commence par 01, puis on remplace chaque 0 par 01 et chaque 1 par 10, ce qui donne 0110 ; on recommence alors la même substitution, ce qui donne 01101001, puis 0110100110010110, etc. Vous constatez – ce que je trouve assez merveilleux, vu la simplicité du procédé – que jamais il n'y a trois fois de suite la même séquence dans la suite infinie que l'on obtient *(voir sur la figure 2 une démonstration de cette propriété)*.

Le fait que cette suite ne répète jamais trois fois consécutivement la même séquence permet-il de dire qu'elle est vraiment désordonnée? Non, et Monsieur Hasard se trompe gravement s'il le croit. En effet, la définition en quelques lignes qui en a été donnée montre que la suite de Thue-Morse n'est pas du tout désordonnée. De plus, on peut la définir encore plus simplement en 22 mots par : «le nième élément est un 0 si et seulement si le nombre de 1 dans l'écriture binaire de n est pair».

Nous nous trouvons dans une situation désagréable, qui apparaît souvent quand on cherche une définition de la notion de suite aléatoire : imposer la condition «jamais deux fois de suite la même séquence» est trop fort, car aucune suite de 0 et de 1 ne vérifie cette condition ; et, à l'opposé, imposer «jamais trois fois de suite la même séquence» est trop faible, car des suites très régulières et parfaitement prévisibles comme la suite de Thue-Morse satisfont cette condition. Subrepticement, nous ajoutons une contrainte nouvelle à la notion de désordre : nous souhaitons que les suites ne soient pas «prévisibles». Nous reviendrons sur ce point.

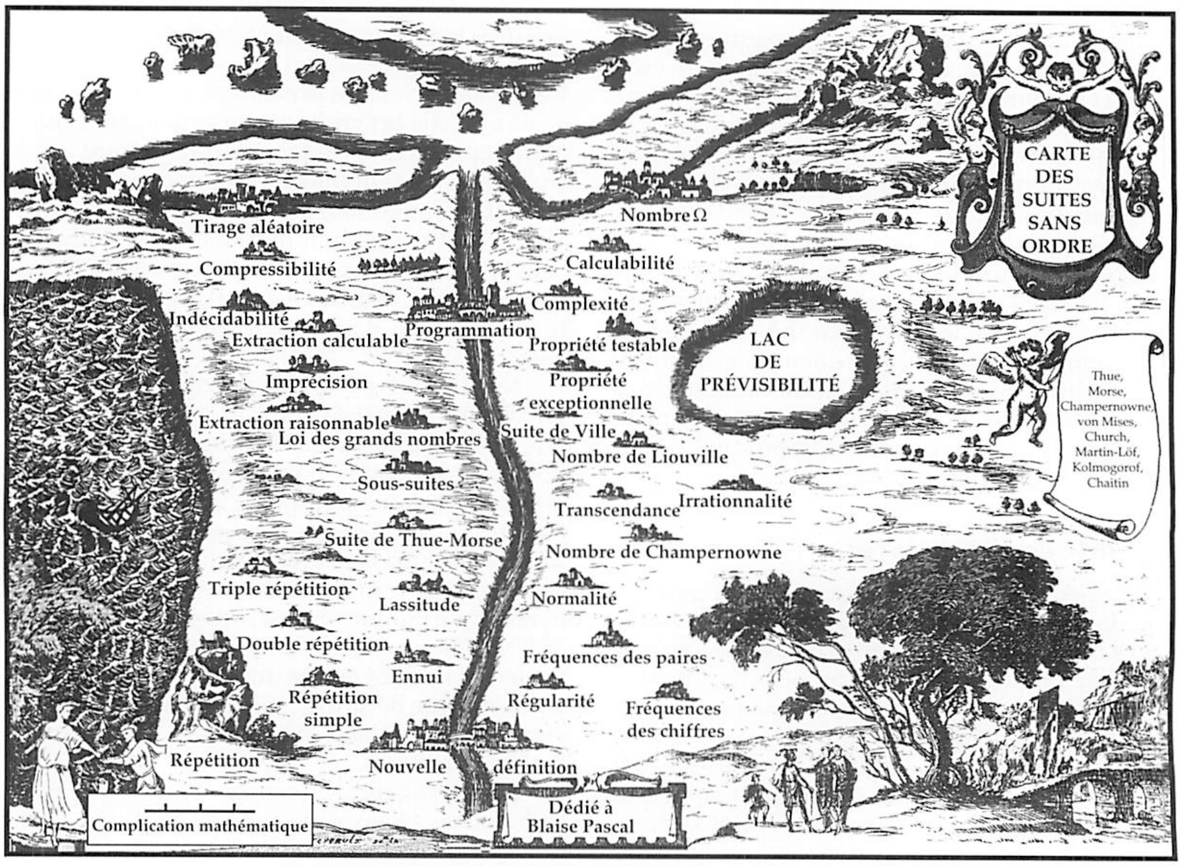
Pour avancer, réfléchissons à ce que nous recherchons. Nous voudrions trouver une condition simple qui, lorsqu'elle est vérifiée par une suite de 0 et de 1, permette d'affirmer qu'il s'agit d'une suite totalement désordonnée – autrement dit, aléatoire – et, bien sûr, nous voudrions que la condition ne soit pas trop forte, c'est-à-dire qu'il existe des suites répondant à cette condition.

Fréquences limites

La théorie classique des probabilités s'est révélée impuissante, car elle ne permet pas d'affirmer qu'une suite donnée est aléatoire ou ordonnée (la suite 01010101... peut parfaitement résulter d'une suite de lancers d'une pièce, avec 0 pour pile et 1 pour face). Toutefois, la théorie classique des probabilités établit que certaines propriétés sont vérifiées avec une probabilité 1, et cela va nous guider. En particulier une suite produite par les lancers successifs d'une pièce de monnaie non truquée vérifie, avec une probabilité 1, qu'il y a, à l'infini, autant de 1 que de 0. Plus précisément, une telle suite vérifie, avec une probabilité 1 ce qu'on appelle la loi des grands nombres : la fréquence limite des 1 est 1/2, ainsi que celle des 0. Est-ce suffisant pour définir le désordre absolu? Bien sûr que non : la suite alternée que nous avons évoquée : 010101010101..., très ordonnée, car elle ne comporte que les paires 01, ou 10, vérifie cette propriété.

Et si l'on imposait, en plus, que les fréquences limites d'apparition de 00, de 10, de 01 et de 11 soient toutes égales à 1/4? Cela reste insuffisant, car par exemple 1100110011001100 ... vérifie à la fois la condition sur les 1/2 et les 1/4. Soyons encore plus exigeants : imposons simultanément que les fréquences limites d'apparition de toutes les séquences de 1 élément soient 1/2, de 2 éléments soient 1/4, de 3 éléments soient 1/8, etc. Appelons une telle suite une suite normale en base 2. Avons-nous une définition satisfaisante des suites aléatoires?

Dans une telle suite, on ne retrouve jamais indéfiniment la même séquence autrement dit, la suite n'est jamais périodique à partir d'un certain rang comme la suite 0110001010101010.... C'est bon signe. Est-ce suffisant? Deux questions se posent : existe-t-il de telles suites? Peuvent-elles être considérées comme vraiment quelconques?



1. La recherche d'une bonne définition des suites désordonnées est un long cheminement.

Là encore, la réponse – oui à la première question, non à la seconde – est connue depuis bien longtemps, grâce aux travaux du grand mathématicien français Émile Borel et à ceux du mathématicien anglais D. Champernowne. E. Borel montra en 1909 que «presque» toutes les suites de 0 et de 1 sont normales en base 2, et Champernowne donna un exemple de suite normale qu'on ne peut considérer comme désordonnée. La suite de Champernowne est obtenue en écrivant successivement tous les entiers en base 2 (0 = 0, 1 = 1, 2 = 10, 3 = 11, 4 = 100, 5 = 101, 6 = 110, 7 = 111, etc.) les uns derrière les autres, ce qui donne : 0110111001011101111000... En réalité, Champernowne donna son exemple en base 10, ce qui le conduisit au nombre 0,12345678910111213... La définition de la notion de suite aléatoire par les fréquences limites des séquences n'est donc pas bonne : à tout moment, connaissant le début de la suite de Champernowne, on peut la continuer et, de plus, elle est très régulière.

Nombres irrationnels et transcendants

On sait qu'un nombre réel est rationnel, c'est-à-dire peut s'écrire sous la forme p/q avec p et q entiers si, et seulement si, son développement binaire est périodique à partir d'un certain moment *(voir la figure 2)*. Par exemple, 2/3 est rationnel et s'écrit 0,101010 ... en base 2. Le nombre $\sqrt{2}$ est irrationnel, comme on le sait depuis l'Antiquité, et donc son développement en base 2 (ou en n'importe quelle base) n'est pas périodique. L'idée naturelle consiste alors à dire qu'une suite de 0 et de 1 est aléatoire si c'est «le développement en base 2 d'un nombre irrationnel». Mais, là encore, le nombre de Champernowne, qui n'est pas périodique et donc définit un nombre irrationnel, montre que cela n'est pas une bonne définition de la notion de suite aléatoire.

Des nombres sont encore plus extraordinaires que les nombres irrationnels, ce sont les nombres transcendants. Par définition, ce sont les nombres qui ne sont solutions d'aucune équation polynomiale à coefficients entiers. Le nombre irrationnel $\sqrt{2}$ n'est pas transcendant, car il est solution de l'équation $X^2 - 2 = 0$. On sait que π et e sont transcendants. Imposer à une suite de 0 et de 1 d'être le développement binaire d'un nombre transcendant ne serait-il pas la bonne méthode pour définir la notion de suite aléatoire?

Malheureusement encore, la réponse est non. Pour le voir, il suffit de considérer le nombre L = 0,101001000000100... (entre les «1», il y a une fois

LA SUITE DE THUE-MORSE

$0 \to 01 \to 0110 \to 01101001 \to$
$0110100110010110 \to ...$

La suite de Thue-Morse est la suite infinie qu'on obtient en poursuivant la même opération de substitution : $f: 0 \to 01\ 1 \to 10$.

Cette suite ne comporte jamais trois fois de suite la même séquence :
jamais trois fois de suite "0"
jamais trois fois de suite "01",
etc.

Pour montrer que la suite de Thue-Morse ne comporte jamais trois fois consécutivement la même chose – on dit "est sans cube" –, il suffit de montrer que, pour toute suite x ne comportant pas de cube, la suite $f(s)$ obtenue à l'étape suivante n'en comporte pas non plus.

Pour cela, supposons que s est sans cube et que $f(s)$ comporte un cube : alors $f(s)$ = ... aaa... et cherchons une contradiction. Nous distinguons trois cas.

Cas 1 : la suite a comporte un nombre pair de chiffres binaires, et le cube aaa commence à un emplacementde numéro impair dans $f(s)$. Il est clair alors que s comporte un cube aussi, obtenu en remplaçant, dans a, 01 par 0 et 10 par 1, ce qui contredit l'hypothèse.

Cas 2 : la suite a comporte un nombre pair de chiffres binaires, et le cube aaa commence à un emplacement de numéro pair dans $f(s)$. Par construction de $f(s)$, le chiffre binaire de numéro $2n + 1$ est 0 (respectivement 1) si et seulement si celui de numéro $2n + 2$ est 1 (respectivement 0). Donc, en enlevant le dernier chiffre binaire de a et en ajoutant devant a le chiffre binaire complémentaire du premier chiffre binaire de a, on obtient un mot a' ayant un nombre pair de chiffres binaires qui est répété trois fois dans $f(s)$, la répétition commençant un emplacement avant celle de a. On est donc ramené au cas 1.

Cas 3 : la suite a comporte un nombre impair de chiffres binaires. Alors il résulte de l'équivalence notée au cas 2 que la suite, apparaissant en commençant à un rang pair dans $f(s)$ et aussi en commençant à un rang impair, est nécessairement composée d'une alternance de 0 et de 1 : 01010, par exemple. La suite a commence et finit donc par le même chiffre binaire. Il en résulte que, dans $f(s)$, il y aura deux chiffres binaires, de rang $2n + 1$; $2n + 2$, qui seront égaux (soit à la jonction entre le premier a et le second a du cube, soit à la jonction entre le second a et le troisième, ce qui, toujours à cause de l'équivalence notée plus haut, est impossible).

«0», puis 2 = 2! fois «0», puis 6 = 3! fois, puis 24 = 4! fois, etc.). Cette suite de chiffres binaires étant très régulière, on ne peut pas la considérer comme aléatoire. Pourtant le nombre L est transcendant, comme Liouville le démontra en 1844 (ce fut d'ailleurs l'un des premiers nombres dont on prouva la transcendance, bien avant e et π), donc il y a des nombres transcendants dont le développement est régulier, ce qui interdit de fonder une définition des suites aléatoires sur les nombres transcendants. Une autre raison pour ne pas définir la notion de suite aléatoire à partir de la notion de nombre transcendant provient de la difficulté qu'il y a à connaître les propriétés du plus célèbre d'entre eux, π. En effet, on ne sait même pas si la suite des chiffres binaires du développement binaire de π est normale en base 2, ce que l'on constate pourtant sur les chiffres binaires connus.

Pour l'instant, toutes nos tentatives de définition ont été infructueuses.

Tentatives par les sous-suites de von Mises

Le mathématicien von Mises, qui chercha obstinément toute sa vie à définir la notion de suite aléatoire, proposa l'idée suivante : imposons à la suite de vérifier la loi des grands nombres (autant de 0 que de 1 à l'infini), ainsi qu'à toutes les sous-suites extraites «par des moyens raisonnables». La suite 01010101... vérifie bien la loi des grands nombres, mais pas la sous-suite obtenue en prenant un élément sur deux, car cela donne 000000... Selon l'idée de von Mises, la suite 010101... n'est donc pas aléatoire, ce qui est satisfaisant. Sur cet exemple, ainsi que sur d'autres comme les suites obtenues à partir du nombre de Champernowne ou du nombre de Liouville, la définition de von Mises indique qu'il ne s'agit pas de suites aléatoires.

Malheureusement, il y a un grave problème : la définition de von Mises est imprécise, et, lorsqu'on cherche à préciser, on rencontre des difficultés insurmontables. Elle est imprécise, car elle ne dit pas ce que c'est qu'extraire une sous-suite par des moyens raisonnables. Tentons de remédier à l'imprécision. La première idée consiste à supprimer la condition «par des moyens raisonnables». Malheureusement, il n'y aura alors pas de suite aléatoire, car aucune suite de 0 et de 1 n'est telle que toutes ses sous-suites vérifient la loi des grands nombres (de toute suite infinie de 0 et de 1, on peut extraire une sous-suite composée uniquement de 1 ou uniquement de 0 et qui ne satisfait donc pas la loi des grands nombres).

La deuxième idée pour éviter l'imprécision de la définition de von Mises, proposée en 1940 par le mathématicien américain Alonzo Church, est beaucoup plus subtile et intéressante. Elle consiste à ne considérer que les sous-suites extraites par des moyens calculables. Alonzo Church, en même temps que d'autres mathématiciens comme les très célèbres K. Gödel et A. Turing, avait quelques années auparavant proposé une définition précise de la notion de fonction calculable : une fonction est calculable si on peut la définir à l'aide d'un programme d'ordinateur *(voir les chapitres 1 et 2)*. La suite extraite en prenant tous les termes de rang pair est évidemment extraite par des moyens calculables. Donc, avec la définition de von Mises et Church, 0101010101... ne doit pas être tenue pour aléatoire (elle possède une sous-suite extraite par un procédé calculable qui ne satisfait pas la loi des grands nombres). De même, la définition de von Mises et Church permet de ne pas considérer comme aléatoires les suites

Tout nombre rationnel p/q a un développement en base 10 (c'est vrai aussi en base 2) périodique à partir d'un certain moment.

Lorsqu'on fait la division de p par q, les restes possibles sont en nombre fini ; donc à un moment, on retrouve nécessairement un reste qu'on a déjà trouvé avant. À partir de là, tout recommence. Exemple 22/7.

22,000000000	7
1	3,14285714...
3	
2	
6	
4	
5	
1	
3...	

Le calcul recommence ensuite, redonnant 142857 142857...

Inversement, tout nombre dont le développement est périodique à partir d'un certain moment est rationnel (on le voit grâce à la formule

$$1 + p + p^2 + p^3 + ... = 1/(1 - p)).$$

Le nombre de Champernowne : 0,1234567891011-1213... n'est pas périodique à partir d'un certain moment, donc il est irrationnel.

Mais, comme la structure est ordonnée, les nombres irrationnels ne sont pas nécessairement aléatoires.

2. Le nombre de Champernowne montre que l'idée de définir la notion de suite aléatoire à partir de la notion de nombre irrationnel ne convient pas.

obtenues à partir des nombres de Champernowne et de Liouville, ce qui est bien ce qu'on souhaite. Elle permet aussi de ne pas considérer comme aléatoires les constantes mathématiques π et e, ce qui, à bien y réfléchir, est naturel aussi, puisque ce sont des nombres parfaitement prévisibles que l'on sait calculer et qui ne sont donc pas quelconques du tout! On peut aussi montrer – c'est un peu plus difficile – que la définition de von Mises et Church n'est pas exagérément restrictive et que de nombreuses suites répondent à cette définition. Un exemple d'une telle suite est le nombre Ω de Chaitin *(voir la figure 5)*.

On a cru, un moment, que c'était la définition attendue de suite aléatoire. Malheureusement encore, un résultat assez délicat – mais sans appel – condamna la définition de von Mises et Church. Le mathématicien français J. Ville prouva l'existence d'une suite (trop compliquée pour être définie ici) aléatoire, au sens de von Mises et Church, ayant la propriété suivante : pour tout n, le nombre de 1 dans les n premiers chiffres binaires de la suite est supérieur au nombre de 0. Cette propriété, qui est contraire à ce qu'on attend d'une suite aléatoire (car elle contredit en particulier ce qu'on appelle la loi du logarithme itéré, qui impose non seulement la loi des grands nombres, mais aussi des contraintes sur l'écart entre le nombre de 1 et le nombre de 0), empêche de considérer que la suite de Ville est aléatoire, alors que la définition de von Mises et Church conduirait à la considérer comme aléatoire. La définition de von Mises et Church n'est pas acceptable : elle permettrait de dire aléatoires des suites qu'il n'est pas naturel d'appeler ainsi!

Enfin la bonne définition!

La bonne solution, dont certains mathématiciens avaient fini par douter qu'elle puisse exister, fut proposée, en 1965, par le jeune mathématicien suédois P. Martin-Löf. Elle est un peu compliquée, mais il vaut la peine de faire l'effort nécessaire pour la comprendre, puisque, cette fois, la définition est satisfaisante.

L'idée est de dire qu'une suite aléatoire ne doit vérifier aucune propriété exceptionnelle qu'on peut réellement tester. Pour rendre précise cette idée, il faut définir *(a)* ce qui signifie propriété exceptionnelle ; *(b)* ce qu'est une propriété réellement testable.

Une propriété exceptionnelle d'une suite est une propriété que seule une infime partie – on dit un ensemble de mesure nulle – de l'ensemble des suites de 0 et de 1 vérifie. La propriété «se terminer par une infinité de 0», ou «être le développement d'un nombre rationnel» (qui équivaut, nous l'avons déjà dit, à la propriété «ne pas être périodique à partir d'un certain moment») sont des propriétés exceptionnelles, car une proportion infiniment faible de suites de 0 et de 1 les vérifient. Comme ce sont aussi des propriétés réellement testables, cela signifie que, par définition, une suite aléatoire, au sens de Martin-Löf, ne se terminera pas par une infinité de 0 et ne sera pas périodique à partir d'un certain rang. Les résultats d'E. Borel en théorie des probabilités montrent que «ne pas satisfaire la loi des grands nombres» est aussi une propriété exceptionnelle, de même que «ne pas satisfaire la loi du logarithme itéré» (qui a été la cause du rejet de la proposition de von Mises et Church). Comme ce sont aussi des propriétés réellement testables, les suites aléatoires, au sens de Martin-Löf, satisferont par définition à la loi des grands nombres et à la loi du logarithme itéré.

Pour comprendre ce que signifie «être une propriété réellement testable», considérons les 30 premiers chiffres binaires d'une suite infinie :

110011110011000011000011110011.

Nous remarquons que les «1» vont deux par deux, ainsi que les «0» (dit autrement : le chiffre binaire de rang $2n$ est le même que le chiffre binaire de rang $2n - 1$). Cela est peu ordinaire, et donc si nous avions à prendre la décision d'accepter ou de refuser cette suite comme suite aléatoire, nous la refuserions : elle est louche! Une

Nombre normal en base 10

La fréquence limite des "0" est 1/10
La fréquence limite des "1" est 1/10
...
La fréquence limite des "9" est 1/10
La fréquence limite des "00" est 1/100
La fréquence limite des "01" est 1/100
La fréquence limite des "02" est 1/100
...
La fréquence limite des "000" est 1/1000
...
...

Tout nombre normal en base 10 est irrationnel et semble devoir être désordonné, mais le nombre de Champernowne 0,12345678910111213... est normal en base 10.

3. Les nombres normaux en base 10 (ou en base 2) semblent devoir être quelconque et ressembler au résultat d'un tirage aléatoire équitable. Le nombre de Champernowne montre encore que ce n'est qu'une illusion, car, bien que très régulier, il est normal. L'idée de dire qu'une suite est aléatoire si elle est la suite des chiffres binaires d'un nombre normal est donc mauvaise.

propriété réellement testable est simplement une propriété comme «les «0» et les «1» vont deux par deux», qu'on peut tester par programme avec une précision de plus en plus grande en fonction du nombre de chiffres dont on dispose. La condition que le test soit définissable par programme est très importante : si on ne l'imposait pas, alors toute suite particulière s vérifierait la propriété exceptionnelle «être égal à s», et il n'y aurait donc aucune suite aléatoire. La réussite de la définition de Martin-Löf provient de ce qu'elle associe une condition provenant de la théorie des probabilités («ne satisfaire aucune propriété exceptionnelle») à une condition d'effectivité qui tempère la première condition, indispensable pour avoir une définition non vide.

La définition de Martin-Löf, qui est parfaite sur le plan mathématique, mais un peu dure à avaler (nous n'avons d'ailleurs pas explicité la définition complète de propriété réellement testable), a été clarifiée, une dizaine d'années plus tard, grâce à la théorie de la complexité de Kolmogorov.

La complexité de Kolmogorov

Cette théorie définit la complexité d'un objet fini (par exemple, une suite finie de 0 et de 1) par la taille du plus petit programme d'ordinateur qui permet d'imprimer l'objet en question. La complexité de Kolmogorov d'une suite de un million de «1» est très faible, car il existe des programmes très courts comme «pour i = 1 jusqu'à 1 000 000 ; imprimer 1 ; fin.» qui impriment cette suite. La suite du premier million de chiffres du développement binaire de π possède une complexité de Kolmogorov plus importante, car le plus court programme qui l'imprime comporte plusieurs lignes (on ne le connaît pas vraiment, mais sa longueur, qui dépasse probablement 100, est bien inférieure à un million). Les programmes courts qui permettent d'imprimer des objets longs peuvent être vus comme des versions comprimées de ces objets. À l'opposé, une suite de longueur 1 000 000 qui a une complexité de Kolmogorov supérieure ou égale à 1 000 000 (il en existe) est totalement incompressible : aucun moyen ne permet de la décrire sous forme condensée.

Nombre de Liouville

L = 0,1010010000001000...
1! 2! 3! 4!

4. Liouville montra que le nombre décrit ci-dessus est un nombre transcendant, c'est-à-dire qu'il ne vérifie aucune équation polynomiale à coefficients entiers. Comme c'est un nombre très régulier, on en déduit que l'idée de dire qu'une suite est aléatoire si elle est la suite des chiffres d'un nombre transcendant est encore une mauvaise idée.

Cette notion de compression issue de la théorie de la complexité de Kolmogorov permet de prouver le résultat suivant, qui confirme que la définition de Martin-Löf est la bonne : une suite infinie de 0 et de 1 est aléatoire, au sens de Martin-Löf, si et seulement elle est incompressible, c'est-à-dire si et seulement s'il existe une constante c telle que, pour tout n, la complexité de Kolmogorof des n premiers chiffres binaires de la suite est supérieure à $n - c$.

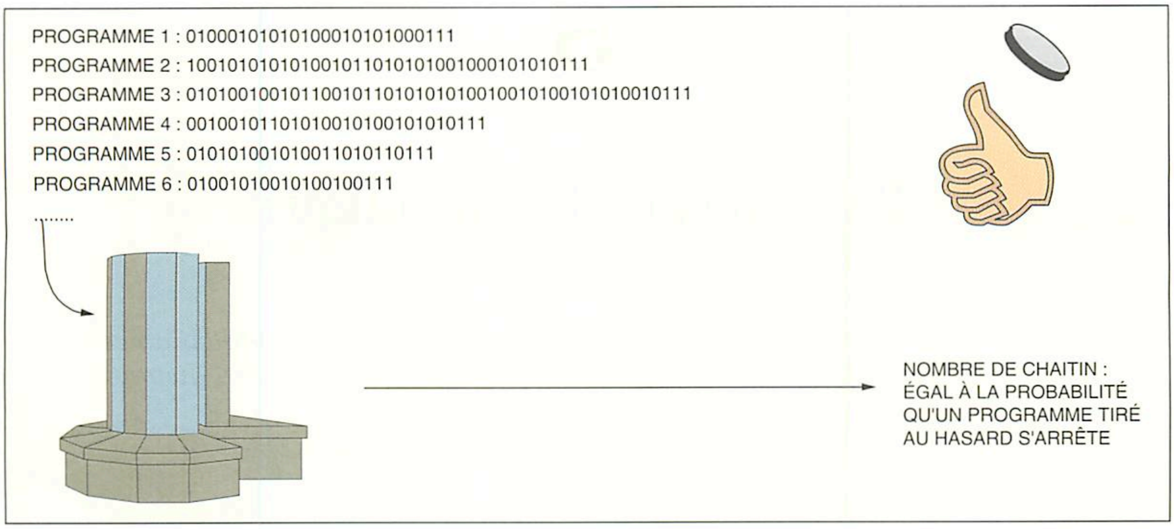
Aléatoire est donc, dans ce sens, équivalent à incompressible. Ce n'est pas inattendu. Ce qui l'est plus peut-être, c'est qu'il ait fallu attendre les années 1970 pour le découvrir, ce qu'on doit indépendamment au mathématicien allemand C.P. Schnorr, au mathématicien russe L. Levin (aujourd'hui aux États-Unis) et au mathématicien américain G. Chaitin.

Les propriétés des suites aléatoires au sens de Martin-Löf sont remarquables ; en voici quelques-unes.

La suite des chiffres binaires d'une telle suite infinie ne peut pas être définie par un programme. Si elle pouvait l'être, on utiliserait le programme qui la définit pour obtenir une version compressée de ses chiffres binaires. Cette propriété a deux conséquences remarquables. D'abord, la suite des chiffres binaires de π ou des constantes usuelles des mathématiques qu'on sait calculer par algorithmes (par exemple, à partir de leurs développements en série) ne sont pas aléatoires dans le sens absolu de Martin-Löf. Ensuite, puisque qu'un programme ne peut jamais produire de suites aléatoires, les fonctions *random* des langages de programmation, engendrées par programmes, ne peuvent qu'être imparfaitement aléatoires.

La suite des chiffres binaires d'une suite aléatoire est toujours normale et définit toujours un nombre transcendant.

La suite des chiffres binaires d'une suite aléatoire est imprévisible : quand on parie à l'aide d'un programme sur le n + 1-ième chiffre binaire d'une suite aléatoire en connaissant seulement les n premiers chiffres binaires, on n'obtient en moyenne pas mieux que si l'on pariait au hasard. Cette propriété d'imprévisibilité confirme l'idée intuitive qu'on ne gagne pas contre le hasard, et qui, sous des formes différentes, avait déjà été mathématisée par la théorie des martingales.



5. À chaque ordinateur on peut associer un nombre oméga de Chaitin Ω : pour cela, on tire un programme au hasard par des lancers successifs d'une pièce de monnaie qui déterminent une suite de chiffres binaires correspondant à un programme, et l'on fait fonctionner l'ordinateur avec ce programme. Le plus souvent, le programme provoque un arrêt immédiat, mais il existe des programmes qui conduisent l'ordinateur dans une boucle infinie. Le nombre Ω est la probabilité que l'ordinateur s'arrête, c'est-à-dire la somme infinie de tous les termes $2^{-\text{longueur}\,(Pr)}$, où *Pr* est un programme qui s'arrête. Ce nombre est mathématiquement défini, mais n'est pas calculable : pour le calculer il faudrait savoir reconnaître les programmes qui ne s'arrêtent pas, tâche impossible.

La suite des chiffres binaires d'une suite aléatoire, ainsi que toutes les suites infinies qu'on peut en extraire par programme satisfont la loi des grands nombres : les suites aléatoires de Martin-Löf sont donc aléatoires, au sens de von Mises et Church (la définition qu'ils proposaient était donc simplement trop faible).

Bien! Mais quelles consignes doit-on donner à Monsieur Hasard pour la suite de ses petits déjeuners? Nous n'avons pour l'instant défini aucune suite précise qui soit aléatoire, au sens de Martin-Löf. En existe-t-il réellement? Oui, et en fait presque toutes les suites de 0 et de 1 sont aléatoires, au sens de Martin-Löf. On est donc dans une situation paradoxale : presque toutes les suites sont aléatoires, au sens de Martin-Löf, mais on ne peut en définir aucune par algorithme. Elles sont partout, mais on ne peut jamais les toucher!

Attention, les mathématiques sont subtiles! «Ne pas pouvoir définir par programme des suites aléatoires de Martin-Löf» ne signifie pas «ne pas pouvoir en définir dans l'abstrait». G. Chaitin a proposé un moyen mathématique de définir ce qu'il appelle le nombre oméga. La suite des chiffres de ce nombre est aléatoire, au sens de Martin-Löf. Le nombre oméga est – par définition – la probabilité de l'arrêt d'un ordinateur lorsqu'on lui fournit un programme écrit chiffre binaire par chiffre binaire à l'aide de tirages successifs d'une pièce de monnaie *(voir la figure 5)*. À chaque ordinateur est ainsi associé un nombre aléatoire parfait, mais qui échappe à tout jamais à notre pouvoir d'investigation (car sa définition ne permet pas de le calculer, à cause de l'indécidabilité de l'arrêt d'un programme).

Le seul conseil qu'on puisse finalement donner à Monsieur Hasard pour «organiser» ses petits déjeuners, c'est de prendre une pièce de monnaie et de l'utiliser pour déterminer à pile ou face, chaque matin, s'il doit prendre du café ou du thé. Puisque toutes les suites, sauf une infime minorité sont aléatoires au sens de Martin-Löf : en procédant ainsi, il sera presque sûr d'éviter toute monotonie.

Tout cela pour en arriver là, me direz-vous! Oui, et c'est bien là l'un des inconvénients majeurs de la théorie des suites aléatoires de Martin-Löf. Elle est très belle, merveilleuse même, elle semble fondamentale et apporte un éclaircissement essentiel à bien des questions ; aussi intéresse-t-elle de plus en plus de monde, y compris les physiciens, mais sa gravissime ineffectivité rend difficile, et presque impossible, toute utilisation pratique de ses résultats.