LES NOMBRES OMÉGA

JEAN-PAUL DELAHAYE

Les nombres oméga sont déroutants : ils sont parfaitement définis et pourtant incalculables. Toutefois, plus on examine les nombres oméga, plus leurs propriétés apparaissent extraordinaires.

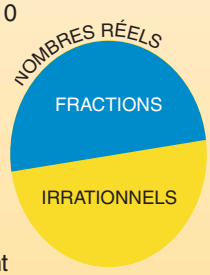
Il y a un peu plus de vingt ans – en 1979 – Martin Gardner aidé de Charles Bennett publiait un article sur un nouveau nombre aux propriétés tellement étranges qu'il fut perçu comme un paradoxe. Ce nombre, découvert par Grégory Chaitin, fut appelé oméga et noté Ω. Le symbole Ω a été fréquemment utilisé en mathématiques pour désigner divers objets, mais on a pris l'habitude de réserver ce symbole au nombre de Chaitin, comme, au début du XVIII^{e} siècle, l'usage s'est établi de n'utiliser la lettre π que pour la constante d'Archimède.

Le nombre Ω appartient à une famille infinie de nombres, les nombres oméga de Chaitin. Ces nombres oméga sont déconcertants, car chacun concentre une conjonction invraisemblable d'étrangetés. Une sous-classe des nombres oméga de Chaitin, les nombres oméga de Solovay aggravent encore le tableau. Ces classes de nombres bizarres sont aussi importantes que les classes des nombres rationnels, algébriques ou transcendants. Nous allons examiner ces êtres abstraits extrêmes, à la frontière de l'absurde, qui nous interrogent sur la nature de la connaissance mathématique.

Nombres calculables

Procédons pas à pas en cheminant dans l'univers des nombres réels, pour examiner la définition et les propriétés des nombres oméga et en goûter toutes les singularités.

Les nombres réels sont les nombres, comme $e = 2{,}7182818284590\ldots$, qui écrits en base 10 par exemple, peuvent se poursuivre indéfiniment (c'est le cas du nombre e). Ceux qui ne se poursuivent pas indéfiniment (comme le fameux 6,55957) sont les décimaux. Parmi ceux qui se poursuivent indéfiniment, certains le font d'une manière périodique comme $24/110 = 0{,}21818181818\ldots$ et les nombres qui sont périodiques à partir d'un certain endroit de leur développement sont des quotients de deux entiers (dénommés nombres rationnels). Les nombres irrationnels (exemple $\sqrt{2}$) ne sont pas les quotients de nombres entiers et leurs décimales ne sont pas périodiques.



À cause de l'infinité de leurs décimales, les nombres réels introduisent subrepticement des difficultés logiques dont la gravité est plus grande que nous l'imaginons

1. HIÉRARCHIE DES INCALCULABILITÉS

René Daumal imagina le Mont Analogue, montagne mystérieuse symbolisant la recherche, au sommet inaccessible par définition, malgré une base abordable. Les différents nombres envisagés dans cet article sont tous comparables au sommet du Mont Analogue.

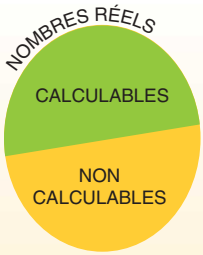
Les nombres rationnels sont calculables et périodiques, mais ils ont une infinité de décimales.

Les nombres transcendants comme π et e sont calculables : on ne connaîtra jamais toutes leurs décimales, mais la différence entre ces nombres et leurs approximations est aussi petite qu'on le désire.

Le nombre τ dont les décimales binaires sont 0 quand le programme associé à cette décimale se termine, 1 s'il ne se termine pas. On sait calculer un nombre infini de ses décimales, mais une infinité d'autres sont inconnaissables.

Les nombres Ω de Chaitin, indiquant la probabilité pour qu'un programme s'arrête sur une machine universelle : on ne sait calculer qu'un nombre fini de leurs décimales.

Les nombres de Solovay, dont on ne sait calculer aucune décimale bien que leur définition soit parfaitement précise.



et ce sont ces difficultés que les nombres oméga exacerbent. Examinons-les.

D'abord l'infinité des décimales entraîne que les nombres réels ne sont pas dénombrables : il n'existe aucune numérotation r_0, r_1,..., r_n,... qui fasse la liste exhaustive des réels (c'est à Cantor que nous devons ce résultat). Ainsi, l'ensemble des nombres réels constitue un ensemble infini plus gros que les ensembles infinis des nombres entiers et des nombres rationnels (puisque, merci Cantor, cet ensemble de rationnels a la même taille que l'ensemble des entiers).

Une conséquence parfois oubliée de cette non-dénombrabilité est que nous ne pourrons jamais calculer tous les nombres réels : les nombres réels calculables sont, par définition, ceux pour lesquels il existe un programme d'ordinateur qui, lorsque nous le laissons fonctionner indéfiniment, en égraine les décimales les unes après les autres. Or il n'y a qu'une infinité dénombrable de programmes : nous pouvons, par exemple, les numéroter tous en considérant les ensembles de programmes qui ont 1,2,3,... n, $n+1$, ... symboles. Chaque ensemble contient un nombre fini de programmes, donc est numérotable, et tous les programmes sont ainsi dénombrés ; c'est

2. La structure de ce Mandala inclut quatre fois le symbole Ω. C'est le cas d'un grand nombre de mandalas et une belle théâtralisation des nombres Ω.

3. DÉFINITION DES NOMBRES OMÉGA

Un nombre oméga de Chaitin est la probabilité qu'une machine universelle à programmes autodélimités s'arrête.

Une machine universelle U est une machine capable de calculer toute fonction calculable par programme. Les programmes (qu'on suppose écrits en binaire) sont dits autodélimités si l'indication de leur fin est donnée en eux-mêmes. Cette fin est par exemple 1111 et la séquence 1111 signifie qu'on est arrivé à la fin du programme.

Épreuve conduisant à un succès ou à un échec.

• On tire des 0 ou des 1 au hasard en utilisant un procédé équitable, par exemple en lançant une pièce de monnaie.

• On poursuit le tirage jusqu'à obtenir un programme pour U. Il se peut que cela ne se produise jamais (car on ne tire jamais les symboles 1111), on considère alors qu'on a un échec.

• Dans le cas où l'on obtient 1111, cela donne un programme pour U, on confie ce programme à U qui le fait fonctionner. Si U avec ce programme s'arrête, on considère qu'on a un succès, sinon on considère qu'on a un échec.

Lorsqu'on effectue cette épreuve, on aboutit soit à un succès soit à un échec. La probabilité d'avoir un succès est, par définition, le nombre oméga associé à U. Pour avoir une approximation de Ω_U, on répète l'épreuve n fois en comptant le nombre de succès m, puis on évalue le rapport m/n.

Cette définition n'est satisfaisante que dans l'abstrait, car elle présuppose qu'on puisse tirer indéfiniment des 0 ou des 1 et qu'on puisse savoir qu'un programme ne s'arrête jamais (or c'est là un problème indécidable).

Pour effectuer réellement le calcul d'une approximation de Ω_U, on rend l'épreuve réaliste de la manière suivante. On se fixe un entier n. On tire une suite de 0 et de 1 en s'arrêtant dès qu'on a obtenu 1111 ou dès qu'on a fait n tirages. Si on atteint n tirages sans avoir 1111 on considère que l'épreuve a échoué. Pour déterminer si un programme s'arrête, on le fait fonctionner pendant n secondes et s'il ne s'est pas arrêté au bout de ces n secondes on considère qu'on a échoué. En répétant cette épreuve (cette fois totalement réaliste) n fois de suite, et en faisant le rapport m/n du nombre de succès m sur le nombre d'essais n, on obtient une approximation de Ω_U.

ce classement des programmes que nous utiliserons par la suite. Il s'ensuit qu'il n'y a donc pas assez de programmes pour calculer tous les réels. Bien sûr, tout rationnel est calculable, ainsi que toutes les constantes habituelles des mathématiques classiques : π, e, $\log 2$, $e+\pi$, $\sin(1)$, etc. Dans chaque cas, leur définition (par exemple par une série $e = 1+1/1!+1/2!+1/3!+ \ldots$) donne des programmes calculant une à une leurs décimales.

Les nombres réels non calculables doivent-ils être pris au sérieux et ne pourrions-nous pas ignorer leur existence ? Non, car la théorie du calcul, développée dans les années 1930 par Kurt Gödel, Alan Turing et quelques autres logiciens, en plus d'en démontrer abstraitement l'existence (à partir de considérations sur la non-dénombrabilité), définit avec une parfaite précision des nombres non calculables, qui, de ce fait, ont un statut d'objet mathématique comparable à π et e.

Un procédé simple pour définir un nombre non calculable va nous rapprocher des nombres oméga. Il est fondé sur le problème de l'arrêt des programmes. La question de l'arrêt des programmes est d'importance théorique et pratique : nous avons tous écrit des programmes qui tournaient à dessein sans jamais s'arrêter comme le programme c := 1 ; tant que c > 0 faire c : =c + 1 ; fin. Il n'y a qu'une alternative : un programme lancé peut, soit s'arrêter au bout d'un temps fini, soit au contraire, se poursuivre indéfiniment.

Établissons la liste de tous les programmes possibles P_0, P_1,..., P_n,... écrits, par exemple, en Java (un langage de programmation très utilisé aujourd'hui) en les classant par famille de taille comme décrit précédemment. Considérons alors le nombre réel dont le développement décimal est : $\tau = 0, a_0a_1\ldots a_n\ldots$ où chaque a_n vaut 1 si le programme P_n s'arrête, et 0 s'il continue indéfiniment.

L'indécidabilité de l'arrêt d'un programme («il est impossible d'écrire un programme A qui, examinant un programme quelconque, ici chaque programme P_n, indique, en un temps fini si P_n s'arrête ou s'il tourne indéfiniment») démontrée en 1936 par Alan Turing a pour conséquence que le nombre réel τ n'est pas calculable : le programme A n'existe pas. Notons que, si le programme A existait, il appartiendrait à la liste de P_n, et nous voyons qu'il devrait opérer sur lui-même pour déterminer s'il s'arrête : l'application de A à lui-même est le cœur de la démonstration de Turing.

Ainsi certains nombres comme τ ne sont pas calculables, mais ils sont connus, car définis sans la moindre ambiguïté, et pourtant sont inconnaissables, car aucun programme ne peut en égrainer les chiffres. Le monde mathématique est ainsi fait : certains de ses nombres peuvent être vus (définis), mais pas touchés (calculés).

LES OMÉGA SONT BIEN PIRES

Les nombres oméga sont comme ce nombre τ, mais en pire. Remarquons qu'il existe de nombreux programmes (une infinité dénombrable) dont nous savons s'ils s'arrêtent, par exemple les programmes PRINT 0, PRINT 1, PRINT 2, PRINT 3, etc., ou s'ils ne s'arrêtent pas. Donc nous pouvons connaître une infinité de chiffres du nombre τ ; il n'empêche, τ n'est pas calculable en totalité ! En revanche, pour les nombres oméga de Chaitin, nous ne pouvons connaître qu'un nombre *fini* de chiffres d'un nombre oméga de Chaitin.

Qu'entendons-nous par connaître ? En mathématiques, depuis que la logique a permis, au début du XX^e siècle, la formalisation de théories puissantes, les mathématiciens ont pris l'habitude d'indiquer (au moins implicitement) dans quelle théorie ils raisonnent et avec quel langage ils écrivent les preuves qu'ils proposent. La théorie des ensembles ZFC (Zermelo-Fraenkel avec l'axiome du choix) est une théorie satisfaisante pour pratiquement toutes les mathématiques et elle sert d'ailleurs de base au grand traité de mathématiques de Nicolas Bourbaki. Les preuves que nous évoquerons ici sont des preuves formulables dans ZFC et il nous suffira de penser que lorsque nous disons «nous pouvons connaître P», ou «nous prouvons P», cela signifie : il existe une preuve de ZFC qui démontre P. Cette remarque étant formulée, nous n'y reviendrons pas : quand nous affirmerons qu'une telle propriété est démontrable, nous sous-entendrons «avec les axiomes de ZFC».

Les nombres oméga de Chaitin sont des nombres réels parfaitement bien définis qui, comme nous le verrons dans la suite, non seulement ne sont pas calculables (aucun programme ne peut en égrainer les chiffres, comme c'était déjà le cas pour τ), mais dont nous ne connaîtrons qu'un nombre fini de chiffres. La théorie mathématique est incapable de donner des précisions sur les chiffres des nombres oméga que, pourtant, elle définit parfaitement !

Si Ω est un nombre oméga de Chaitin donné et si n est un entier fixé, alors l'un des deux énoncés suivants est vrai :

– le n-ième chiffre binaire de Ω est un 0,
– le n-ième chiffre binaire de Ω est un 1.

Pourtant, dès que n est assez grand, aucun de ces deux énoncés n'est démontrable. Énoncé brièvement, si Ω est un nombre de Chaitin alors les chiffres de Ω, sauf un nombre fini d'entre eux, sont indécidables.

Un concentré pur d'indécidabilité

Tout cela avait étonné dans la décennie 1970 où les mathématiciens avaient réalisé à quel point des objets définis pouvaient être inconnaissables. Cette quintessence d'indécidabilité des nombres oméga de Chaitin vient pourtant d'être dépassée !

En effet, en étudiant les nombres oméga de G. Chaitin et en exploitant un vieux théorème démontré par Stephen Kleene en 1952 (le théorème de récursion), le mathématicien Robert Solovay a découvert que certains d'entre eux (que nous appellerons nombres oméga de Solovay) tout en étant parfaitement définissables, sont totalement inconnaissables. En clair, si Ω est un nombre oméga de Solovay alors *aucun* chiffre de Ω ne peut en être connu. Notons que Solovay avait déjà acquis une certaine célébrité en 1970 pour un résultat important de logique. Trente ans plus tard, il est le héros d'un nouvel exploit contredisant ainsi un préjugé tenace qui veut que la productivité d'un mathématicien s'épuise très rapidement avec l'âge.

Ces sommets d'indécidabilité que sont les oméga de Solovay montrent à quel point l'introduction en apparence anodine de nombres ayant une infinité de décimales peut, lorsque l'on en tire toutes les conséquences, conduire à des situations au bord de l'absurde et, en tout cas, propres à plonger dans un abîme de perplexité tout être doué de bon sens : comment, ce qui est parfaitement défini, peut-il être parfaitement et définitivement inconnaissable ?

Mais quelle est la définition pratique des nombres oméga ?

Les nombres oméga de Chaitin sont «les probabilités d'arrêt des machines universelles à programmes autodélimités». Ourk ! Quelques explications vont éclairer cette définition.

Une machine universelle U est une machine qui, moyennant de bons programmes, est capable de calculer toute fonction définie par un programme. Tous les ordinateurs contemporains sont de telles machines universelles, dont le concept a été introduit par Turing en 1936. L'exigence que les programmes soient autodélimités signifie qu'il faut interdire que le début d'un programme correct pour la machine U, soit un *autre* programme correct pour U. Une façon d'obtenir cette propriété est de prévoir dans le langage de programmation de la machine une séquence indiquant la fin des programmes : nous conviendrons, par exemple, de terminer tout programme de U par la suite des quatre symboles «E»«N»«D»«.», suite qu'on ne pourra utiliser qu'une seule fois dans un même programme. Il existe, dans les séquences d'ADN, de telles séquences de bases indiquant la fin d'un gène.

Le fait que les programmes soient autodélimités (quelque chose en eux-mêmes indique leur fin) permet d'attribuer une probabilité à chaque programme P de la machine U. Pour ce faire, tirons à pile ou face les décimales consécutives d'un programme P jusqu'à ce que l'on obtienne la suite correspondant à la transcription en binaire de «E»«N»«D»«.». Le programme P sera une suite de n chiffres binaires telle que 0110101101001. La probabilité d'obtenir une telle suite, donc le programme P, est $1/2^n$, car chaque chiffre a une probabilité 1/2 d'être le bon, c'est-à-dire celui de P. Il s'agit bien d'une probabilité, car on peut effectivement tirer au hasard des programmes par un procédé qui donne P avec la probabilité $1/2^n$ *(voir la figure 3)*.

Imaginons maintenant qu'on utilise ce procédé pour engendrer au hasard des programmes de la machine universelle U, et qu'à chaque fois qu'on trouve un programme correct pour U, on le fasse fonctionner. Alors, ou bien le programme tourne indéfiniment, ou bien il finit par s'arrêter. La suite de lancés de la pièce conduit donc parfois à l'arrêt, parfois à un calcul infini (soit parce qu'on ne tombe jamais sur un programme correct, soit parce que le programme ainsi déterminé ne s'arrête pas). La probabilité, lorsque ce procédé concret est mis en œuvre, d'arriver à l'arrêt de U, est le nombre oméga de Chaitin associé à la machine universelle U que l'on note Ω_U. Pour chaque machine universelle, le nombre Ω_U est parfaitement défini et aussi bien caractérisé que les nombres π ou e.

À chaque machine universelle à programmes autodélimités U correspond un nombre oméga de Chaitin ; or comme il y a une infinité dénombrable de telles machines U, il y a une infinité dénombrable de nombres oméga de Chaitin Ω_U.

Les nombres oméga de Solovay sont définis à partir d'une classe particulière de machines universelles spécialement concoctées pour que la théorie ZFC ne puisse rien en savoir. La méthode pour définir les nombres oméga de Solovay consiste à transformer une machine universelle U de façon à en modifier les premiers chiffres pour qu'ils échappent à ZFC. Cette définition

4. NOMBRES CALCULABLES ET APPROCHABLES

A. Par définition un nombre réel x (pris entre 0 et 1) est calculable s'il est la limite d'une suite croissante et calculable par programme de nombres rationnels $x_n = p_n/q_n$, cette suite vérifiant, de plus, que pour tout entier n : $|x_n - x| < 1/2^n$.

Les constantes usuelles sont toutes des nombres réels calculables, car pour chacune d'elles, x, on connaît une suite de nombres rationnels qui converge vers x, et on sait évaluer l'erreur commise (on sait donc s'arranger pour que l'erreur commise par x_n soit inférieure à $1/2^n$).

On montre que cette définition est équivalente à :

• x s'écrit en binaire sous la forme : $x = 0,a_0a_1a_2\ldots$ avec une fonction $n \to a_n$ (chaque a_i vaut 0 ou 1) qui est calculable par programme (autrement dit, il existe un programme qui égraine les chiffres de x) ;

• il existe un programme qui énumère tous les nombres rationnels inférieurs à x, et un autre qui énumère tous les nombres rationnels supérieurs à x.

B. Un nombre réel est approchable si, par définition, il est la limite d'une suite croissante et calculable par programme de nombres rationnels $x_n = p_n/q_n$ (c'est la même chose que pour calculable, mais sans la deuxième condition portant sur la majoration d'erreur). Une définition équivalente est :

• il existe un programme qui énumère les nombres rationnels inférieurs au nombre réel x considéré.

La nuance entre nombres approchables et nombres calculables est subtile, mais, en réalité, elle est énorme et les nombres oméga de Chaitin sont justement des nombres à la fois approchables et non calculables. Les nombres approchables sont tous parfaitement définis (on connaît des suites qui convergent vers eux) et pourtant certains, comme les nombres oméga, ne sont pas calculables. R. Solovay a d'ailleurs démontré que certains nombres oméga sont tels qu'on ne peut connaître aucun de leurs chiffres avec certitude. Parfaitement définis, ils sont inconnaissables.

est un tantinet sibylline, mais le détail est techniquement trop compliqué pour être présenté ici, ce qui est compréhensible : elle a échappé pendant plus de 20 ans aux mathématiciens…

Remarquons que le nombre Ω_U de Chaitin est, par définition, une somme de nombres dont chacun est égal à $1/2^n$. Précisément : $\Omega_U = \sum 1/2^n$, la somme étant prise sur tous les n qui sont des longueurs de programmes de U s'arrêtant.

La définition peut donner lieu à un procédé pratique d'approximation de Ω_U. On prend un certain nombre de programmes (par exemple tous ceux dont la longueur i est inférieure à n), on les fait fonctionner un certain temps (par exemple pendant n étapes de calcul) et on additionne les $1/2^i$ de tous ceux qui se sont arrêtés. La suite croissante x_n ainsi définie converge vers Ω_U.

De qui se moque-t-on?

Vous devez être inquiet et vous commencez à vous dire que je me moque de vous. D'une part, je prétends que les Ω_U ne sont pas calculables (et même totalement inconnaissables dans le cas des nombres de Solovay) et en même temps je propose un procédé concret pour approcher ces Ω_U, c'est-à-dire les calculer!

Non, je ne me moque pas de vous et toute la subtilité des nombres oméga est concentrée là. Si U est une machine universelle à programmes autodélimités, on peut réellement construire une suite croissante de nombres rationnels qui converge vers Ω_U, mais cette suite convergera très lentement. Si lentement que vous n'aurez jamais la certitude d'avoir plus que quelques chiffres exacts de Ω_U. Dans le cas des nombres de Solovay, vous n'aurez même jamais aucun chiffre avec certitude. La convergence vers Ω_U est plus lente que la convergence de n'importe quelle suite calculable croissante vers un nombre calculable (on a récemment démontré le beau résultat que cette lenteur extrême est une propriété caractéristique des nombres oméga).

Pour les constantes mathématiques habituelles comme π, on connaît en général plusieurs méthodes de calcul, chacune produisant une suite de nombres x_n qui converge vers la constante. Certaines méthodes sont rapides (par exemple on gagne un chiffre exact en passant de x_n à x_{n+1}), d'autres peuvent être plus lentes. Le numéricien préfère bien sûr les méthodes rapides et on peut dire que son art face aux constantes mathématiques consiste à inventer des méthodes à convergence rapide. Lorsqu'on a affaire à un oméga de Chaitin, on sait de manière définitive et absolue que cet art du numéricien sera impuissant. Non seulement aucune méthode ne sera rapide, mais de plus à chaque fois qu'on disposera d'une méthode d'approximation on ne pourra pas savoir avec quelle vitesse elle fournit les chiffres de la constante oméga calculée.

Les propriétés des nombres oméga

On peut envisager toutes les machines universelles et tous les nombres oméga associés. La classe infinie des nombres oméga de Chaitin est donc dénombrable, comme l'est d'ailleurs celle des oméga de Solovay. De plus, de nombreuses connaissances ont été accumulées les concernant. Il n'y a pas de paradoxe dans le fait qu'on puisse démontrer des propriétés précises des oméga (y compris des oméga de Solovay) alors qu'on ne peut pas calculer leurs chiffres. Dans le monde réel, pour avoir accès à une connaissance générale – par exemple que «le poids moyen des Américains est supérieur au poids moyen des Européens» – il faut assembler des connaissances particulières. Dans le monde mathématique, ce n'est pas toujours le cas : on peut connaître quelque chose de général concernant un nombre Ω – par exemple «la fréquence des 1 et celle des 0 sont les mêmes dans l'écriture binaire de Ω» – et en même temps ne connaître aucun chiffre particulier de Ω. Encore une étrangeté du monde mathématique!

Voici quelques-unes des propriétés démontrées des nombres oméga :

– Tous les nombres oméga sont irrationnels et transcendants (aucune équation polynomiale à coefficients entiers n'a pour solution un nombre oméga).

– Tous les nombres oméga ont des décimales équiréparties : la suite de leurs chiffres en base 10 comporte un dixième de «0», un dixième de «1»,… , un dixième de «9» et on a une propriété analogue dans toute base de numération.

– Tous les nombres oméga sont des «nombres-univers» en toute base : toute séquence finie de chiffres y est présente. On peut même préciser que toute séquence finie de n chiffres décimaux y est présente avec la fréquence $1/10^n$ (bien sûr, on a une propriété analogue dans toutes les bases de numération). En conséquence, dans tout nombre oméga, on sait que quelque part il y a une série d'un milliard de 0 consécutifs (rien de tel n'a été démontré pour les constantes comme π ou e).

– Tous les nombres oméga sont aléatoires au sens mathématique le plus fort (le terme consacré est «aléatoire au sens de Martin-Löf» en l'honneur du mathématicien suédois qui

5. LE CALCUL DE QUELQUES CHIFFRES D'UN OMÉGA

Il existe des procédés qui à partir d'une machine universelle à programmes autodélimités permettent d'en construire d'autres (qu'on qualifiera d'artificielles) qui seront elles aussi universelles, mais dont le nombre oméga commencera par certains chiffres binaires fixés à l'avance, par exemple 01010101010101.

Les nombres oméga associés à de telles machines universelles artificielles sont eux aussi artificiels et leurs premiers chiffres (choisis arbitrairement) ne portent aucune information.

En revanche, connaître les chiffres d'une machine universelle U à programmes autodélimités précise qui n'a pas été construite de manière adéquate pour avoir des chiffres connus à l'avance est réellement une tâche difficile, car Ω_U contient alors sous forme concentrée l'information sur l'arrêt des programmes de U. Peut-on tenter de calculer quelques chiffres d'un tel Ω_U ?

Oui et c'est ce qu'ont fait récemment Ch. Calude, M.J. Dinneen et C.K. Shu. Ils ont d'abord défini la machine universelle la plus naturelle possible en considérant un jeu d'instructions aussi simple que possible et en adoptant des conventions de notations aussi concises que possible. Ils ont ensuite tenté de connaître le comportement d'un grand nombre de programmes courts pour U. Ils ont réussi à analyser tous les programmes dont la longueur est inférieure à 84 chiffres binaires (certains conduisent à l'arrêt d'autres non). Ils ont pu en déduire avec certitude les 64 premiers chiffres de Ω_U. Ces chiffres sont : 0000001000000100000110001000011010001111110010111011101000010000.

C'est la première fois qu'on s'attaque au calcul explicite des chiffres d'un nombre aléatoire. Notons qu'il s'agit d'un jeu, car en pratique 64 chiffres binaires sont très insuffisants pour envisager d'aborder des conjectures intéressantes. Peut-être pourra-t-on aller un peu au-delà de 64, mais très vite un blocage grave se produira et il est très improbable que de tels calculs puissent aider à résoudre des problèmes mathématiques ouverts.

6. Ω DÉTIENT LE SECRET DE TOUTES LES ÉNIGMES MATHÉMATIQUES

Si, par exemple par un exercice de méditation transcendantale, on pouvait connaître le nombre oméga Ω_U d'une machine universelle U (ou même si on réussissait à en connaître 10 000 chiffres binaires) alors on pourrait résoudre l'essentiel des questions que se posent les mathématiciens. La justification de cette affirmation se fait en deux étapes.

A. La connaissance de m chiffres binaires de Ω_U permet de savoir pour tout programme P de U dont la longueur est inférieure à m, s'il s'arrête ou pas en mettant en œuvre le procédé suivant.

On calcule les termes successifs d'une suite x_n qui converge vers Ω_U en croissant. Pour connaître x_n, on prend tous les programmes de U dont la longueur i est inférieure à n et on les fait fonctionner pendant n étapes de calcul, puis on additionne les probabilités $1/2^i$ de chacun des programmes qui se sont arrêtés, ce qui donne x_n. À un moment le nombre x_n écrit en base 2 aura les mêmes m premiers chiffres binaires que Ω_U. On a supposé qu'on connaît ces m chiffres, donc on saura reconnaître cet instant. Or à ce point du calcul ou bien P a été comptabilisé dans x_n, car il s'est arrêté (on sait donc que P est un programme qui s'arrête) ou bien il ne s'est pas arrêté et alors on sait qu'il ne s'arrêtera jamais, car sa probabilité $1/2^m$ en l'ajoutant à x_n conduirait à dépasser Ω_U.

B. Toutes les conjectures ouvertes des mathématiques peuvent se mettre sous la forme «le système formel ZFC permet-il de démontrer P?» Pour P, on prendra l'énoncé exprimant la conjecture. Or chacune de ces questions est équivalente à un problème d'arrêt de programme pour U, précisément à l'arrêt du programme de U qui énumère les démonstrations correctes de ZFC jusqu'à avoir une démonstration de P.

Donc, si on connaît un nombre de chiffres de Ω_U supérieur à la longueur du programme d'énumération correspondant à P alors on dispose d'un moyen pour répondre à la question «le système formel ZFC permet-il de démontrer P?». Une fois mis en marche, ce moyen fournira la réponse en un temps fini. Hélas, ce temps de calcul risque d'être très long et est, de toute façon, impossible à évaluer à l'avance.

introduisit ce concept en 1966). Cela implique en particulier que : *(a)* une méthode programmable pour prédire le n-ième chiffre d'un oméga à partir des $n-1$ premiers ne fait jamais mieux que le hasard ; *(b)* si l'on extrait une sous-suite de la suite des chiffres d'un oméga par un procédé algorithmique (par exemple en retenant les chiffres dont les rangs sont des nombres premiers), cette suite sera celle des chiffres d'un nombre irrationnel, transcendant, équiréparti et aléatoire et sera même celle d'un autre nombre oméga de Chaitin.

– Tous les nombres oméga sont incompressibles. Précisément, pour chaque nombre oméga Ω_U, il existe une constante c telle que le plus court programme donnant les n premiers chiffres binaires de Ω_U a au moins la longueur $n-c$. (on ne gagne jamais plus de c bits d'information quand on cherche à comprimer le début des chiffres de Ω_U).

– Tous les oméga sont non calculables et pourtant chacun est la limite d'une suite calculable croissante de nombres rationnels (on dit qu'ils sont approchables, voir la figure 4). La dite convergence est plus lente que la convergence de toute suite calculable de rationnels vers un nombre calculable.

– Un nombre oméga peut commencer par n'importe quelle séquence finie de chiffres. Il y a donc un nombre oméga qui commence par 3,14, un autre qui commence par 3,1415 un autre qui commence par 3,141592 etc.). Notons toutefois que les machines universelles, ayant pour nombre oméga ces nombres-là, seront construites artificiellement.

– La somme de deux nombres oméga, si elle est inférieure à 1, est un nombre oméga, de même que le produit (ces belles propriétés ne sont pas vraies pour les nombres irrationnels, ou pour les nombres transcendants (par exemple, $\pi/4 + (2 - \pi/4) = 2$)).

La raison profonde de toutes ces propriétés est le fait que la connaissance des n premiers chiffres du nombre de Chaitin Ω_U associée à la machine universelle U, permet de savoir pour tous les programmes de U, de longueur inférieure ou égale à n, s'ils s'arrêtent ou non (alors que pour cela il faudrait 2^n chiffres binaires du nombre τ associé à U). En clair, Ω_U contient une forme hyperconcentrée d'informations sur le problème indécidable de l'arrêt des programmes de U. De nombreuses conjectures pourraient être résolues (en théorie) si on connaissait les 10 000 premiers chiffres binaires d'un Ω_U pour une machine universelle U «naturelle» (par exemple celle associée au langage de programmation Java de votre ordinateur).

Une conjecture comme «tout nombre pair strictement supérieur à 2 peut être écrit comme somme de deux nombres premiers» (conjecture de Goldbach) est en effet équivalente au non-arrêt du programme qui cherche un contre-exemple, programme qui a une longueur de quelques centaines de chiffres binaires. Toutes les conjectures de la forme «ZFC permet de démontrer P» si P est un énoncé assez court, seraient, elles aussi, résolues (en théorie) par la connaissance de quelques centaines de chiffres binaires du oméga d'une machine universelle naturelle.

Les nombres oméga sont donc non seulement des concentrés d'informations sur l'arrêt des programmes, mais ce sont aussi des concentrés d'information mathématique.

Pour nous consoler du fait que nous ne connaîtrons jamais, ne serait-ce que 1 000 chiffres d'un nombre oméga «naturel», nous pouvons nous dire qu'extraire l'information de nombres oméga est un travail fini, mais invraisemblablement long (d'où les «en théorie» que j'ai utilisés dans les paragraphes précédents) et qu'en conséquence même si on connaissait 1 000 chiffres d'un nombre oméga de Chaitin associé à une machine naturelle on ne pourrait pas vraiment l'utiliser. Comme l'écrivait Martin Gardner et Charles Bennett : «Oméga est, dans bien des sens différents, un nombre cabalistique. Il peut être connu par un humain (vous pourriez l'apprendre si on vous le confiait), mais pas sur la base de la raison. Pour le connaître en détail, il faudrait faire un acte de foi, comme on accepte les mots d'un texte sacré.»

C. H. BENNETT et M. Gardner, *Le nombre aléatoire oméga,* in *Le Monde mathématique de Martin Gardner*, Bibliothèque Pour la Science, pp. 45-49, 1986.

C. S. CALUDE, *Chaitin Ω Numbers, Solovay Machines, and Incompleteness*, in *Theoretical Computer Science*, 2002.

http://citeseer.nj.nec.com/calude99chaitin.html (à lire pour un exposé précis et complet)

J. P. DELAHAYE, *Information, complexité et hasard,* Hermès Science Publication, Paris, 1999 (seconde édition).

J. P. DELAHAYE, *L'intelligence et le calcul*, Pour la science/Belin, Paris, 2002.

R. M. SOLOVAY, *A Version of Ω for Which ZFC Can Not Predict a Single Bit*, in C.S. Calude, G. Paun *Finite Versus Infinite. Contribution to an Eternal Dilemma,* Springer-Verlag, 2000.