

$b - 1$, d'où l'on déduit que $a = b$, ce que nous souhaitons.

Maintenant, soit un entier positif ou nul quelconque b . Soit n le maximum de 0 et b (bien sûr $n = b$). Le raisonnement précédent a montré que 0 et b étaient égaux, donc $b = 0$. En conclusion, tous les entiers positifs ou nuls sont nuls.

Si tel était le cas, là aussi les entiers seraient majorés par 0! Où est l'erreur?

Solution : Simplement dans le fait que, même si a et b sont des entiers positifs ou nuls, $a - 1$ et $b - 1$ ne le sont pas nécessairement (car $0 - 1 = -1$). On ne peut donc pas appliquer l'hypothèse de récurrence au couple $a - 1, b - 1$.

DÉSOLANTES DÉRIVÉES

Calculons la dérivée de x^3 de deux façons différentes :

(a) Par la formule habituelle $(x^n)' = nx^{n-1}$. Pour tout x , on a donc $(x^3)' = 3x^2$

(b) Par le raisonnement suivant. Pour x entier, on écrit :

$x^3 = x^2 + x^2 + x^2 + \dots + x^2$ (la somme comporte x fois le terme x^2)

On dérive de chaque côté :

$(x^3)' = (x^2)' + (x^2)' + (x^2)' + \dots + (x^2)'$ (la dérivée d'une somme est la somme des dérivées).

$(x^3)' = 2x + 2x + 2x + \dots + 2x$ (application de la formule générale rappelée plus haut).

$(x^3)' = 2x^2$ (car, sur la ligne précédente il y a x fois le terme $2x$, ce qui permet de remplacer le second membre par $2x^2$).

Pour tout x entier, on a donc :

$(x^3)' = 3x^2 = 2x^2$.

En prenant pour x un entier non nul et en simplifiant par x^2 , on a : $2 = 3$.

Où est l'erreur?

Solution : Le raisonnement (b) suppose que x est entier (sinon, on ne pourrait pas écrire : $x^3 = x^2 + x^2 + x^2 + \dots + x^2$). Appelons n l'entier auquel on s'intéresse.

Les fonctions $x \rightarrow x^3$ et $x \rightarrow x^2 + x^2 + x^2 + \dots + x^2$ (n fois le terme x^2) ont effectivement la même valeur au point $x = n$, et cette valeur est n^3 . Mais, autour de la valeur n , ces deux fonctions n'ont plus les mêmes valeurs, car : $(n+\epsilon)^3 \neq (n+\epsilon)^2 + (n+\epsilon)^2 + \dots + (n+\epsilon)^2 = n(n+\epsilon)^2$. Puisque les deux fonctions sont différentes, il est sans surprise que leur dérivée le soit.

L'endroit où se produit l'erreur est lorsqu'on écrit «on dérive de chaque côté» car, l'égalité $x^3 = x^2 + x^2 + x^2 + \dots + x^2$ désigne une égalité valable entre deux fonctions différentes en un point précis, et non pas une égalité entre deux fonctions sur tout leur ensemble de définition. L'erreur est en fait la même que celle qu'on commettrait en disant :

$\sin 45^\circ = \cos 45^\circ = \sqrt{2}/2$, et donc que $(\sin 45^\circ)' = (\cos 45^\circ)'$, ce qui est absurde car en utilisant que $\sin x' = \cos x$ et que $\cos x' = -\sin x$, on en déduirait que $\cos 45^\circ = -\sin 45^\circ$, soit $\sqrt{2}/2 = -\sqrt{2}/2$.

5. LA PLUS BELLE PROPRIÉTÉ DE π

L'importance mathématique du nombre π n'est plus à démontrer. Pourtant la propriété suivante de π ne manquera pas de vous étonner : toute série converge vers π .

En effet, soit une série quelconque (par prudence, vous pouvez considérer une série absolument convergente) :

$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + \dots$

Les égalités (finies) suivantes sont immédiates :

$a_1 = \pi + (a_1 - \pi)$

$a_2 = -(a_1 - \pi) + (a_1 + a_2 - \pi)$

$a_3 = -(a_1 + a_2 - \pi) + (a_1 + a_2 + a_3 - \pi)$

$a_4 = -(a_1 + a_2 + a_3 - \pi) + (a_1 + a_2 + a_3 + a_4 - \pi)$. Etc.

En ajoutant toutes ces égalités, nous obtenons :

$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + \dots = \pi + (a_1 - \pi) - (a_1 - \pi) + (a_1 + a_2 - \pi) - (a_1 + a_2 - \pi) + (a_1 + a_2 + a_3 - \pi) - (a_1 + a_2 + a_3 - \pi) + (a_1 + a_2 + a_3 + a_4 - \pi) - \dots$

Toutes les parenthèses se simplifient deux à deux et disparaissent. Donc :

$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + \dots = \pi$.

Pensez-vous vraiment que cela soit normal?

Solution

Non, bien sûr, et d'ailleurs le même raisonnement, s'il était juste, s'appliquerait à n'importe quelle constante. Le raisonnement est faux, car l'expression obtenue au second membre après l'addition infinie est une série qui n'est pas même convergente (ni les parenthèses, ni leurs composants ne tendent vers zéro en général). Or avec une série de nombres réels qui n'est pas convergente, toute manipulation, même les simplifications les plus simples, est dangereuse et susceptible de nous entraîner dans l'absurde. Si vous en doutez, considérez l'exemple classique suivant :

$1 - 1 + 1 - 1 + 1 - 1 + 1 - 1 + \dots = (1 - 1) + (1 - 1) + (1 - 1) + (1 - 1) + (1 - 1) + \dots = 0$
 $1 - 1 + 1 - 1 + 1 - 1 + 1 - 1 + \dots = 1 + (-1 + 1) + (-1 + 1) + (-1 + 1) + \dots = 1$

SOMMES INFINIES

En analyse, on démontre que la série : $\ln(2) = 1 - 1/2 + 1/3 - 1/4 + 1/5 - 1/6 + \dots$ est une série convergente, c'est-à-dire qu'en prenant 1, puis 2, puis 3, ... termes de la série, on obtient des nombres qui s'approchent de plus en plus d'une constante, qui est ici le logarithme népérien de 2 : $\ln 2 = 0,6931\dots$

Groupons les termes positifs d'une part et les termes négatifs de l'autre :

$\ln 2 = (1 + 1/3 + 1/5 + \dots) - (1/2 + 1/4 + 1/6 + \dots)$.

Par ailleurs nous avons certainement :

$0 = (1/2 + 1/4 + 1/6 + \dots) - (1/2 + 1/4 + 1/6 + \dots)$.

ce qui, en ajoutant membre à membre avec l'égalité au-dessus, donne :

$\ln 2 = (1 + 1/2 + 1/3 + 1/4 + 1/5 + 1/6 + \dots) - 2(1/2 + 1/4 + 1/6 + \dots)$,

c'est-à-dire :

$\ln 2 = (1 + 1/2 + 1/3 + 1/4 + 1/5 + 1/6 + \dots) - (1 + 1/2 + 1/3 + 1/4 + 1/5 + 1/6 + \dots) = 0$,

Donc, $\ln 2 = 0$.

D'où vient cette absurdité?

Solution : L'absurdité provient du fait général qu'on ne peut manipuler les séries sans précaution et qu'en particulier on ne peut changer l'ordre des termes sans risque. Il existe deux sortes de séries convergentes :
 - celles (dénommées «absolument convergentes») dont la série des valeurs absolues est convergente,
 - celles (dénommées «semi-convergentes») dont la série des valeurs absolues est infinie. C'est le cas de :

$\ln(2) = 1 - 1/2 + 1/3 - 1/4 + 1/5 - 1/6 + \dots$

Pour les premières, on peut changer l'ordre des termes, additionner termes à termes, etc, comme nous l'avons fait ici. Pour les autres, Riemann a démontré au contraire que changer l'ordre des termes pouvait conduire à n'importe quelle valeur entre $-\infty$ et $+\infty$, et en fait toutes sortes d'absurdités peuvent être déduites de la manipulation sans précaution de séries semi-convergentes. L'exemple proposé est l'un des plus brefs qui le montre.

ARISTOTE, Organon VI, Réfutation des arguments sophistiques. Traduction J. Tricot. Librairie philosophique J. Vrin, Paris, 1987.

Edward BARREAU, Mathematical Fallacies, Flaws, and Flimflam, édité par The Mathematical Association of America, 2000, (ISBN 0-88385-529-1).

E.P. NORTHROP, Fatales et paradoxes mathématiques, Dunod, Paris, 1956, (tra-

duction de : **Riddles in Mathematics**, D. Van Nostrand Company Inc., New York, 1944).

Sylviane GASQUET-MORE, Plus vite que son nombre. Déchiffrer l'information. Éditions du Seuil, Paris 1999.

Massimo PIATELLI-PALMARINI, Inevitable Illusions : How Mistake of Reason Rule our Minds, John Wiley and Sons, New York, 1994 (ISBN 0-471-58126-7).



Un démineur millionnaire

IAN STEWART

Ou comment un jeu informatique peut faire de vous un homme riche.

En manque d'argent? L'Institut mathématique Clay, une fondation éducative à but non lucratif de Cambridge, dans le Massachusetts, offre des prix de un million de dollars pour la résolution de sept problèmes. L'un d'eux est le célèbre problème de l'égalité de la classe P et de la classe NP , dont nous éclaircirons plus loin l'énoncé hermétique. Bien qu'il s'agisse d'une question très difficile, un amateur astucieux peut y répondre grâce au démineur, un jeu populaire accessible à la plupart des ordinateurs personnels.

Richard Kaye, de l'Université de Birmingham, a récemment mis en évidence les relations entre ce jeu et la question « $P = NP?$ » dans un article intitulé «le démineur est-il NP -complet?». Rappelons d'abord les règles du démineur. L'ordinateur commence la partie en présentant une grille de carrés dont certains dissimulent des mines explosives. Il s'agit de les localiser sans en faire exploser une seule. Au premier coup, vous

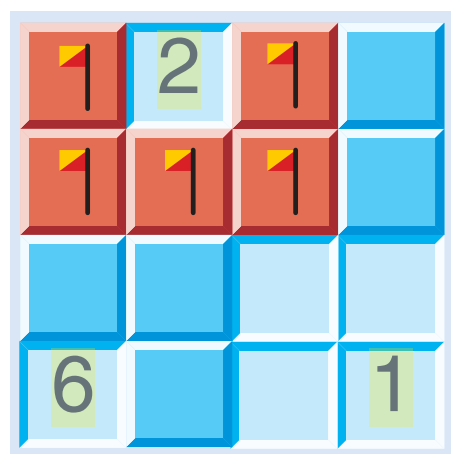
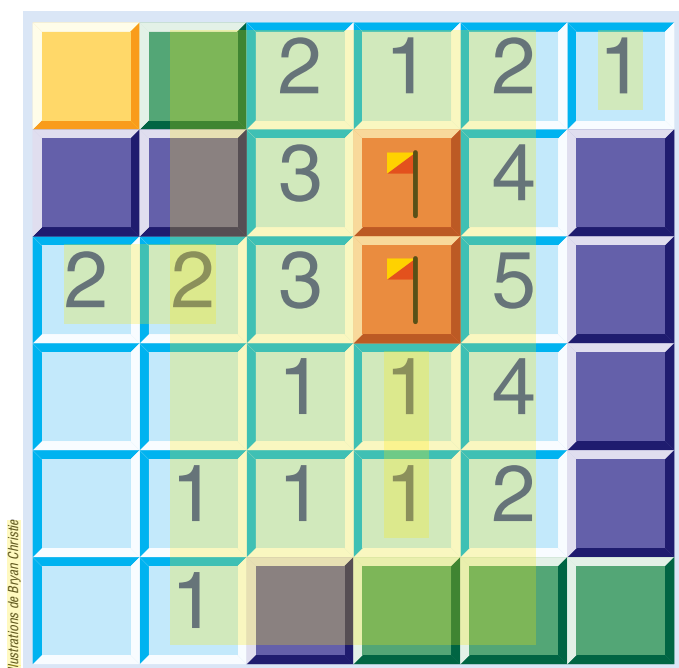
découvrez l'un des carrés : s'il cachait une mine, vous n'avez pas de chance et vous perdez, sinon l'ordinateur affiche dans le carré que vous avez choisi le nombre de mines dans les trois, cinq ou huit carrés adjacents.

Vous utilisez alors cette information pour choisir un autre carré, et de nouveau une mine explose ou un nombre est affiché. Lorsque vous pouvez déduire de ces informations la présence d'une mine dans un carré, vous marquez ce dernier d'un petit drapeau (voir la figure 1). Vous gagnez quand toutes les mines de la grille sont localisées.

Revenons à la question « $P = NP?$ ». Un algorithme est une procédure pas à pas qu'utilise un ordinateur pour résoudre un problème. Pour les informaticiens, il est crucial de savoir avec quelle efficacité un algorithme résout un problème donné, ou, en d'autres termes, comment le temps de traitement, c'est-à-dire le nombre de calculs exigés pour la réponse, varie suivant la taille des don-

nées initiales. On distingue principalement les problèmes de classe P (P comme polynôme) et les autres. Un problème est de classe P quand on peut le résoudre avec un algorithme dont le temps de traitement est majoré par un polynôme de la taille des données, c'est-à-dire par une somme de différentes puissances de la taille des données. Lorsqu'une telle solution n'existe pas, le problème est de classe non- P .

À l'inverse des problèmes de classe P , les problèmes de classe non- P ne sont pas efficacement traités par les ordinateurs : tout algorithme mis au point pour les résoudre requiert un temps trop long. On peut prouver qu'un problème est de classe P en trouvant un algorithme qui le résolve en un temps polynomial, par exemple, ordonner par ordre croissant un ensemble d'entiers est un problème de classe P que des programmes peuvent traiter sur des banques de données commerciales, même très importantes. En revanche, trouver les facteurs premiers



1. Une position typique du démineur (à gauche). Après les premiers coups, le joueur a localisé deux mines (sous les drapeaux). L'examen des chiffres montre que les carrés violets dissimulent d'autres mines tandis que les verts sont sans danger. L'état du carré jaune est encore inconnu, mais peut être déterminé après un coup judicieux. En revanche, la position à droite n'est pas consistante : aucune disposition de mines dans la grille ne peut respecter les chiffres indiqués.

d'un entier et le problème du voyageur de commerce, qui consiste à déterminer le plus court chemin reliant plusieurs villes données, sont des problèmes de classe non- P (bien que cela n'ait pas encore été démontré).

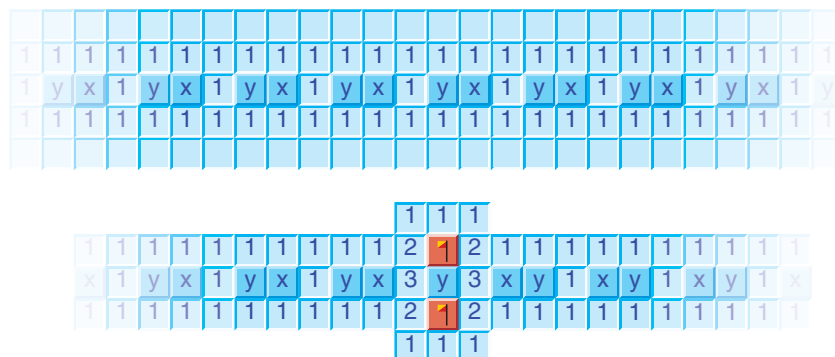
Pourquoi prouver qu'un problème est de classe non- P est-il si difficile ? Parce qu'il faut traiter tous les algorithmes possibles – et non pas un seul – et montrer qu'aucun ne résout le problème en un temps polynomial. Aujourd'hui, on sait qu'une vaste catégorie de problèmes candidats à la classe non- P sont sur un pied d'égalité : si l'un d'eux peut être résolu en un temps polynomial, alors tous peuvent l'être. Ces problèmes ont un comportement polynomial non déterministe, c'est-à-dire qu'avec de la chance – l'algorithme inclut une étape aléatoire –, on peut les résoudre en un temps polynomial ; ils sont de la classe NP .

NON- P , NP ET NP -COMPLET

Les classes non- P et NP sont différentes : un problème est NP dès qu'une solution proposée est bien en temps polynomial. Il est plus facile de vérifier qu'une solution proposée est bien en temps polynomial que de trouver la solution elle-même. Mon exemple favori qui illustre cette différence est le puzzle : en venir à bout peut être difficile, mais vérifier une solution proposée ne requiert souvent que quelques secondes ; le temps d'examiner que chaque pièce s'ajuste aux pièces voisines. Ce temps, environ proportionnel au nombre de pièces, est polynomial. En revanche, on ne peut effectuer un puzzle en un temps polynomial : le nombre de solutions croît plus vite que toute puissance donnée du nombre de pièces.

Beaucoup de problèmes NP ont des temps de traitement équivalents. Un problème NP est dit NP -complet quand l'existence d'une solution en un temps polynomial déterministe, c'est-à-dire sans processus aléatoire, entraîne que tout problème NP a une solution en un temps polynomial. Ainsi, si on peut résoudre un problème NP -complet en un temps polynomial, on peut résoudre tous les problèmes NP en un temps polynomial. Et la question « $P = NP$?» ? Bien que les apparences soient contraires, on peut s'interroger sur l'égalité des classes P et NP . La réponse attendue est négative, cependant, au cas où tous les problèmes NP -complets ont une solution en temps polynomial, alors les deux classes P et NP sont égales.

Nombre de problèmes sont NP -complets : un des plus simples est le problème SAT, qui inclut des circuits booléens.



2. L'électronique du démineur convertit des circuits booléens en position de jeu. Un seul type de carrés (x ou y) cache des mines. Des connexions propagent un signal (y suivi de x) le long de la grille (en haut). Un opérateur *non* inverse l'ordre des x et des y (en bas).

Ces circuits sont construits avec des opérateurs logiques, tel «*et*», «*ou*» et «*non*», qui s'appliquent à des valeurs soit vraies (V), soit fausses (F). Chaque opérateur fournit à partir de valeurs d'entrée une valeur de sortie : par exemple, l'opérateur *non* transforme la valeur V en la valeur F . Le problème SAT s'intéresse à l'existence pour un circuit booléen donné de valeurs d'entrée tel que la valeur de sortie soit V . Pour des circuits simples, le problème est un jeu d'enfants ; il devient ardu lorsque le circuit a un grand nombre d'opérateurs et d'entrées.

LA CONSISTANCE DU DÉMINEUR

Le lien avec le démineur apparaît quand on s'intéresse à la consistance du jeu, c'est-à-dire à la vraisemblance d'une position du jeu. Par exemple, la figure 1 montre une position inconsistante : aucune répartition des mines ne peut mener aux nombres affichés dans les carrés de la grille.

R. Kaye a montré que le problème SAT pour un circuit booléen donné peut-être transformé en un problème de consistance pour une certaine grille du jeu du démineur. En outre, il montre que la conversion des circuits booléens en positions du démineur s'exécute en un temps polynomial. Dans cette conversion, les entrées et les sorties du circuit deviennent une répartition des mines sur la grille : à un carré miné correspond une valeur V , et à un carré sans mine, une valeur F . Les connexions des opérateurs du circuit sont représentées sur la figure 2 : les carrés marqués y ont des valeurs opposées de celles des carrés marqués x . Notons que les chiffres des autres carrés sont corrects que x soit V ou F . Tels des «câbles électroniques», les connexions propagent chaque valeur (V ou F) sur la longueur de la grille.

On représente les opérateurs logiques par le même type de procédé. Par

exemple, la position du démineur de la figure 2 illustre l'opérateur *non* : le bloc du milieu échange les positions de x et de y ; x suit y avant le bloc et précède y après le bloc. Les valeurs des carrés sont inversées, que x soit V ou F , comme après un opérateur *non* dans un circuit booléen.

L'électronique du démineur est plus complexe : elle requiert par exemple de plier ou de scinder des «fils». R. Kaye franchit tous ces obstacles et conclut que quiconque prouve la consistance d'une position donnée du démineur en un temps polynomial, résout aussi le problème SAT du circuit équivalent en un temps polynomial. En d'autres termes, le démineur est un problème NP -complet : une solution en un temps polynomial à la consistance du démineur entraîne que tous les problèmes NP -complets ont des solutions en un temps polynomial : les classes P et NP sont égales. À l'inverse, si l'on montre qu'il n'existe pas de telle solution au problème du démineur, alors les classes P et NP sont différentes. Dans les deux cas, la question serait résolue.

Avant de vous lancer sur votre ordinateur, rappelez-vous que le problème de la consistance du démineur n'est pas une mince affaire : déterminer si une position de jeu est consistante devient vite difficile quand la taille de la grille augmente et la plupart des mathématiciens et des informaticiens pensent qu'il n'y a pas de solution générale traitable en un temps polynomial. De surcroît, l'Institut Clay a imposé des règles strictes au concours : avant d'accepter une solution, elle doit être publiée dans un journal important et être «généralement acceptée» par la communauté mathématique dans les deux années de sa publication.

Richard Kaye, *Minesweeper is NP-Complete*, in *Mathematical Intelligencer*, vol. 22, n° 2, 2000.