

Accromath

Volume 20 • été-automne 2025

De la science-fiction à l'informatique:
**les mathématiques
pour expliquer les
qubits**

Autres *articles*

- Retour sur le jeu des noyaux
- Points, droites et plans (suite)
- Triplets pythagoriciens
- Dialogue géométrico-algébrique à saveur hippocratique
- Calculer une racine carrée de tête?
- Mettre en mémoire et analyser une image
- La règle des 37 %
- On ne peut pas résoudre tous les puzzles!
Place au coloriage et aux invariants
- Jeu de couleurs, jeu de quantas

Rubrique des
Paradoxes

Le lancer
des dés

Éditorial α

Cette année 2025 marque le 100^e anniversaire du développement initial de la mécanique quantique et, pour cette raison, a été proclamée *Année internationale de la science et de la technologie quantique* (AIQ 2025). *Accromath* célèbre cette année internationale avec deux articles consacrés à la mécanique quantique.

Dans ce numéro, nous présentons des *Accro-flashes* et d'autres articles accessibles pour le niveau secondaire. Christian Genest et Jeffrey R. Stribling présentent **Retour sur le jeu des noyaux** et nous donnent un complément d'informations sur ce jeu. **Points, droites et plans (suite)** présente la réponse de Cantor à l'objection de Dedekind sur le jumelage des points du segment $[0; 1[$ à ceux du carré construit sur ce segment. **Triplets pythagoriciens** nous montre comment cacher tous ces triplets dans le premier quadrant du cercle unitaire.

Bernard Hodgson présente **Dialogue géométrico-algébrique à saveur hippocratique**, une courte pièce de théâtre où fourmillent des connaissances issues tant de la géométrie de la Grèce antique que de l'algèbre de la Renaissance.

Dans l'article **Calculer une racine carrée de tête?**, Tommy Mastromonaco nous montre comment calculer mentalement une valeur approchée d'une racine carrée.

Dans **Mettre en mémoire et analyser une image**, Christiane Rousseau nous explique comment sont traitées les images dans le format JPEG 2000.

Si la direction peut offrir un poste à la personne interviewée ou rejeter sa candidature, mais que la décision une fois prise est irrévocable, quelle stratégie adopter pour maximiser les chances de recruter la meilleure candidature? C'est la question que se pose Christian Genest dans **La règle des 37%**.

Dans **On ne peut pas résoudre tous les puzzles! Place au coloriage et aux invariants**, Frédéric Gourdeau nous montre que les puzzles permettent de mettre en action des idées fondamentales en mathématiques, que ce soit pour résoudre ces puzzles ou pour montrer que leur solution est impossible.

Dans le premier des articles sur la mécanique quantique, **De la science-fiction à l'informatique: les mathématiques pour expliquer les qubits**, Tania Belabbas montre que les mathématiques permettent de donner un sens à des notions qui échappent à la compréhension intuitive.

Dans **Jeu de couleurs, jeu de quantas**, de Claude Crépeau, deux protagonistes, Alice et Bob, sont soumis à un jeu *rouge, vert ou bleu*, qui, selon les inspecteurs, permettra de prouver qu'ils sont coupables de « pratique de la magie ».

Dans **Le lancer de dés**, Jean-Paul Delahaye fait ressortir un paradoxe dans le choix entre deux dés dont les faces de l'un sont notées 6, 3, 3, 3, 3 et 3, celles de l'autre sont notées 5, 5, 5, 2, 2 et 2.

Bonne lecture!

André Ross

Rédacteur en chef

André Ross

Professeur de mathématiques

Comité éditorial

France Caron

*Professeure de didactique
des mathématiques
Université de Montréal*

Christian Genest

*Professeur de statistique
Université McGill*

Bernard R. Hodgson

*Professeur de mathématiques
Université Laval*

Tomasz Kaczynski

*Professeur de mathématiques
Université de Sherbrooke*

Nadia Lafrenière

*Professeure de mathématiques
Université Concordia*

Bruno Martin

*Professeur de mathématiques
École secondaire Pointe-Lévy*

Christiane Rousseau

*Professeure de mathématiques
Université de Montréal*

Christian Sévigny

*Professeur de physique
École secondaire Pointe-Lévy*

Anik Trahan

*Professeur de mathématiques
Cégep de Sherbrooke*

Robert Wilson

*Professeur de mathématiques
Cégep de Lévis-Lauzon*

Production et Iconographie

Alexandra Haedrich

Institut des sciences mathématiques

Conception graphique

Pierre Lavallée

Néograf Design inc.

Illustrations de scientifiques et caricatures

Noémie Ross

Illustrations mathématiques

André Ross

Révision linguistique

Robert Wilson

*Professeur de mathématiques
Cégep de Lévis-Lauzon*

Accromath

*Institut des sciences mathématiques
Université du Québec à Montréal
Case postale 8888, succ. Centre-ville
Montréal (Québec)
H3C 3P8 Canada*

redaction@accromath.ca
www.accromath.ca

Accromath

Volume 20 • été – automne 2025

Sommaire

Dossier *Accro-flashes*

Retour sur le jeu des noyaux

Christian Genest et Jeffrey R. Stribling

Points, droites et plans (suite)

André Ross

Triplets pythagoriciens

André Ross

Dialogue géométrico-algébrique à saveur hippocratique

Bernard R. Hodgson

Calculer une racine carrée de tête?

Tommy Mastromonaco

Dossier *Applications des mathématiques*

Mettre en mémoire et analyser une image

Christiane Rousseau

La règle des 37 %

Christian Genest

On ne peut pas résoudre tous les puzzles! Place au coloriage et aux invariants

Frédéric Gourdeau

Dossier *Mécanique quantique*

De la science fiction à l'informatique: les mathématiques pour expliquer les qubits

Tania Belabbas

Jeu de couleurs, jeu de quantas

Claude Crépeau

Rubrique des **Paradoxes**

Le lancer des dés

Jean-Paul Delahaye

Solution du paradoxe précédent

Jean-Paul Delahaye

Section problèmes

42



2

4

6

8

12

16

22

28

32

36

42

42

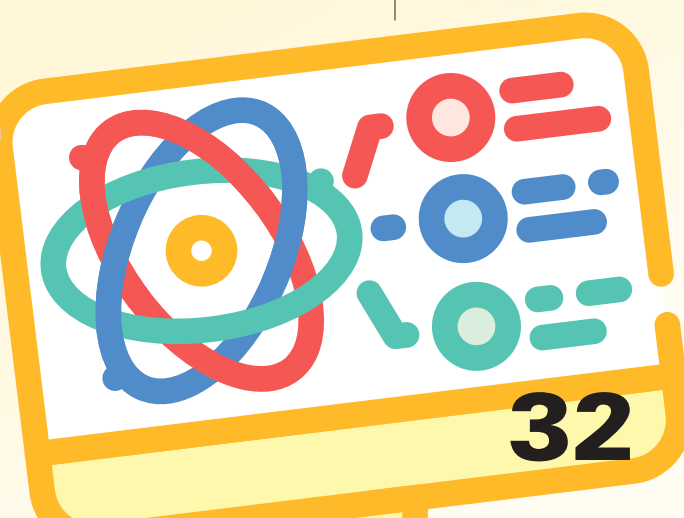
44



12



28



32

Retour sur le jeu des noyaux

Dans un récent numéro d'Accromath, un article était consacré au jeu des noyaux, pratiqué par les autochtones d'Amérique du Nord¹.

Christian Genest
Université McGill

Jeffrey R. Stribling
Université Stanford



Louis-Armand de Lom D'Arce, baron de La Hontan



Pierre Rémond de Montmort

Ce jeu avait d'abord été rapporté en 1706 par le Baron de la Hontan (1666-1716) dans le second tome de ses *Mémoires de l'Amérique Septentrionale*, ou *La suite des voyages de Mr. le baron de La Hontan*. La brève description qu'il en donne est la suivante :

« Celui des Noyaux est un jeu de hazard, ils sont noirs d'un côté & blancs de l'autre, on n'y joue qu'avec huit seulement. On les met dans un plat, qu'on pose à terre, après avoir fait sauter ces Noyaux en l'air. Le côté noir est le bon ; le nombre impair gagne, & les 8 blancs ou noirs gagnent double, ce qui n'arrive pas souvent. »

Étudié quelques années plus tard par le mathématicien français Pierre Rémond de Montmort (1678-1719) dans son *Essay d'Analyse sur les Jeux de Hazard*, ce jeu se révèle presque équitable, comme le montre un calcul assez simple. Sachant que la personne qui lance les noyaux a misé A unités et que son adversaire en a misé B , le gain espéré du premier vaut $(132B - 126A)/256$ de sorte que si $A = B$, le jeu procure un très léger avantage à la personne qui lance les noyaux¹.

Généralisation

Dans son ouvrage, Montmort propose en outre l'extension suivante du problème :

« L'on suppose que les huit noyaux ont chacun quatre faces, savoir une blanche, une noire, une verte & une rouge. Pierre sera celui qui jette les noyaux, Paul sera l'autre Joueur. »

« Si les noyaux ayant été jettés au hazard, il se trouve les quatre couleurs, Paul donnera B à Pierre. S'il n'y en a que de trois couleurs, Paul lui donnera $3B$; & s'il n'y en a que d'une seule couleur, c'est à dire, si les huit noyaux sont ou tous blancs ou tous noirs, ou tous verts ou tous rouges, Paul lui donnera $4B$; enfin s'il n'y en a que de deux couleurs, Pierre donnera à Paul $2A$. »

« Cela posé, on demande de quel côté est l'avantage, & quel est cet avantage, en supposant que A ait à B un rapport quelconque. »

Montmort écrit alors ce qui suit, sans fournir de détails :

« L'on trouvera ... que si $B = A$, Paul aura de l'avantage à ce jeu ; mais ce ne seroit que de cette fraction $233/16\ 384$, ce qui n'est à peu près que la soixante & dixième partie de l'unité ; & par conséquent afin que la condition de Pierre & de Paul fussent égales, il faudroit que B fût $= 11\ 592A/11\ 359$, c'est à dire que Pierre devoit mettre au jeu onze mil cinq cens cinquante-deux contre Paul onze mil trois cens cinquante-neuf. »

Est-ce bien le cas ?

Cette question, posée de façon énigmatique à la toute fin de l'article¹, laissait entendre que non. De fait, on va montrer ici que la solution, telle qu'énoncée, est erronée. Mais on verra aussi qu'une légère modification de la formulation du problème conduit à une solution très proche de celle annoncée par Montmort.

Résolution du problème original

Pour tout $i \in \{1, 2, 3, 4\}$, le nombre de façons d'obtenir exactement i couleurs parmi 4 est donné par la formule

$$C_4^i \times S(8, i) \times i!,$$

où, en général,

- le coefficient C_k^i donne le nombre de façons de choisir i couleurs parmi k ;
- le nombre de Stirling de deuxième espèce, $S(n, i)$, fournit le nombre de façons de partitionner un ensemble de n éléments en i sous-ensembles non vides ;
- la factorielle $i!$ représente le nombre de permutations de i objets distincts.

1. C. Genest (2024). Le jeu des noyaux. *Accromath*, 19 (2), 18-21.

On dispose en outre de la formule suivante pour le calcul du terme b) :

$$S(n, i) = \sum_{j=0}^i (-1)^{i-j} \frac{j^n}{j!(i-j)!}.$$

Les calculs sont détaillés dans le tableau ci-contre. Noter que le total est $65\,536 = 4^8$, comme il se doit.

Procédant comme dans l'article déjà paru sur le sujet¹, observons maintenant que si Pierre mise A et que Paul mise B , alors le gain algébrique Y de Pierre satisfait aux conditions suivantes :

- Y vaut $4B$ si $i=1$; • Y vaut $-2A$ si $i=2$;
- Y vaut $3B$ si $i=3$; • Y vaut B si $i=4$.

Le gain moyen de Pierre est donc

$$E(Y) = (4 \times 4B + 23\,184 \times 3B + 40\,824 \times B - 1\,524 \times 2A) / 65\,536,$$

ou encore

$$E(Y) = (110\,392B - 3\,048A) / 65\,536.$$

Si $A = B$, c'est donc Pierre qui a l'avantage, et non Paul, comme Montmort l'affirme. De plus, l'avantage de Pierre est énorme car pour rendre le jeu équitable, il faudrait que

$$A/B = 110\,392 / 3\,048 \approx 36,21785.$$

Manifestement, il y a mal donne. Soit Montmort s'est trompé dans ses calculs, soit l'énoncé du problème ne correspond pas à ce qu'il avait en tête.

Une solution possible

Connaissant la réputation de Montmort, mathématicien royal, il semble peu probable qu'il ait commis une faute aussi grossière. Il faut donc chercher ailleurs une explication.

Une option très attrayante consiste à interchanger les paiements correspondant aux cas $i=2$ et $i=3$. On obtient alors la structure de gains suivante :

- Y vaut $4B$ si $i=1$; • Y vaut $3B$ si $i=2$;
- Y vaut $-2A$ si $i=3$; • Y vaut B si $i=4$.

Par suite, on trouve

$$E(Y) = (4 \times 4B + 1\,524 \times 3B + 40\,824 \times B - 23\,184 \times 2A) / 65\,536,$$

ou encore

$$E(Y) = (45\,412B - 46\,368A) / 65\,536.$$

Si $A = B$, c'est alors bel et bien Paul qui a l'avantage, comme Montmort l'affirme. De plus, le jeu s'avère équitable lorsque $A/B = 45\,412 / 46\,368 = 11\,353 / 11\,592$.

Cette solution se rapproche beaucoup de celles proposées par Montmort, selon que l'on se fie à son expression en chiffres ou en lettres.

Conclusion

De toute évidence, la solution du problème tel que formulé par Montmort est erronée. Toutefois, elle devient correcte sous les trois conditions suivantes :

a) On interchange les paiements pour les cas $i=2$ et $i=3$.

b) On remplace un 9 par un 3 dans la représentation chiffrée de la solution de Montmort, c'est-à-dire que l'on remplace $A/B = 11\,359 / 11\,592$ par $A/B = 11\,353 / 11\,592$.

c) On fait fi de la formulation en mots de sa solution.

Les énoncés b) et c) sont raisonnables puisque, d'une part, il est assez facile de confondre un 3 et un 9 à l'écrit, et que d'autre part, la réponse en lettres a suivi et non précédé le calcul numérique.

Quant à l'énoncé a), il semble d'autant plus plausible que si $A = B$, l'avantage de Paul est de l'ordre de $239 / 16\,384 \approx 0,01458$, qui est également très proche de la valeur annoncée par Montmort, soit $233 / 16\,384 \approx 0,01422$. Encore une fois, il semble qu'un 9 et un 3 aient été confondus. Mais dans un cas comme dans l'autre, on remarque, à l'instar de Montmort, que ceci

« n'est à peu près que la soixante & dixième partie de l'unité »,

puisque $1/70 \approx 0,01428$.

D'aucuns s'étonneront peut-être que des fautes se glissent parfois dans les ouvrages de mathématiques. Cela pourra même leur paraître d'autant plus improbable lorsque l'auteur est célèbre. Cependant, nul n'est à l'abri d'une distraction et, comme le rappelle le dicton latin, *Errare humanum est... perseverare diabolicum!*

Termes				
i	a	b	c	Produit
1	4	1	1	4
2	6	127	2	1 524
3	4	966	6	23 184
4	1	1 701	24	40 824
Σ				65 536

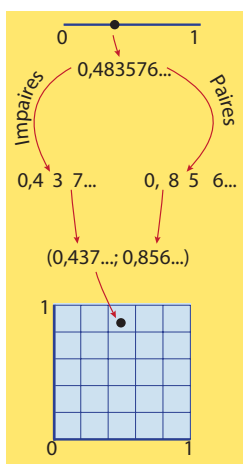


Points, droites et plans (suite)



André Ross
Professeur retraité

Zia et Léo échangent sur la démonstration de Georg Cantor à l'effet que le segment ouvert $[0; 1[$ contient autant de points que le carré construit sur ce segment.



Léo

J'ai parlé à ma prof de maths de la démonstration que tu m'as présentée lors de notre dernière discussion, à l'effet qu'il y a autant de points dans le segment $[0; 1[$ que dans le carré construit sur ce segment.

Zia

Tu parles de la démonstration où on décompose la partie décimale d'un nombre en deux parties selon la position des chiffres de ce développement (voir image). Qu'en pense ton enseignante ?

Léo

Elle dit que cette explication est incomplète. Selon elle, il faut préciser comment gérer les nombres selon leur développement¹ :

- Pour les nombres rationnels, dont le développement est soit fini, soit infini périodique, elle indique de regarder particulièrement les nombres ayant un développement infini périodique se terminant par 9.
- Puis de regarder plus précisément les nombres irrationnels, dont le développement est infini sans être périodique.

1. La méthode présentée dans la première partie est la méthode initiale de Cantor, qu'il a par la suite modifiée pour répondre aux objections de Dedekind. Voir Buildings Cantor's bijection, Simon Nicolay et Laurent Simons, Université de Liège, Institut de Mathématique

https://www.researchgate.net/publication/265414991_Building_Cantor's_Bijection

Développement rationnel

Zia

Voyons ceux qui ont un développement infini périodique. Prenons par exemple $x=0,333\ 333\ \dots$ en le multipliant par 10, j'obtiens

$$10x = 3,333\ 333\ \dots$$

Et en soustrayant alors $x=0,333\ 333\ \dots$ de $10x$, j'ai alors

$$9x = 3,333\ 333\ \dots - 0,333\ 333\ \dots = 3.$$

J'obtiens l'expression rationnelle donnant la valeur de x , puisqu'à partir de $9x=3$, je tire $x=1/3$. Je peux faire la même chose avec, par exemple, $0,077\ 777\ \dots$ et obtenir que $x=7/90$.

Léo

Dans l'énumération des éléments d'un ensemble, on n'accepte pas les répétitions. Que l'on écrive $0,333\ 333\ \dots$ ou $1/3$ ou encore $0,077\ 777\ \dots$ plutôt que $7/90$, ça ne change rien.

Zia

Tu as raison, mais ça pose problème lorsque la période est composée de 9. Posons $x=0,999\ 999\ \dots$ alors $10x=9,999\ 999\ \dots$, et en lui soustrayant $x=0,999\ 999\ \dots$, on a $9x=9$. Donc $x=1$.

Léo

Je vois! 1 n'est pas un élément du segment de droite $[0; 1[$. Le point $0,999\ 999\ \dots$ ne fait donc pas partie des développements admissibles dans notre énumération.

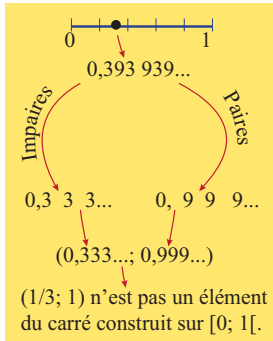
Zia

Mais il faut aussi tenir compte qu'un développement comme $0,999\ 999\ \dots$ peut être obtenu en scindant le nombre choisi sur le segment de droite $[0; 1[$.



Léo

En effet, mais prenons plutôt le point $0,3\overline{9} = 0,393\ 939\dots$ (illustration ci-bas). En scindant la partie décimale en prenant les décimales en position impaire pour former un premier développement, j'ai $0,333\dots$, et



les décimales en position paire pour le second développement infini donnent $0,999\dots$. Avec ces deux développements, j'obtiens donc le couple de coordonnées

$$(0,3\overline{3}; 0,9\overline{9}) = (3/9; 1) = (1/3; 1).$$

Cependant, le correspondant $(1/3; 1)$ n'est pas un couple du carré construit sur le segment $[0; 1[$. Là, on a un problème !

Zia

Ce qui signifie qu'il faut modifier la façon de scinder le point choisi au départ.

Léo

Oui! Imposons une restriction sur le choix des coupures. Supposons que j'ajoute que la coupure ne peut pas être après un 9. Pour identifier les coupures à faire, j'alterne les couleurs noir et rouge, $0,3\overline{9} = 0,3\overline{93}93\overline{93}93\overline{93}\dots$ et, après avoir scindé, j'ai le couple $(0,3\overline{93}; 0,9\overline{3})$. Ce point est bien un élément du carré. En effet, en l'exprimant sous forme rationnelle, ce point est $(39/99; 93/99)$ (Illustration ci-contre).

Zia

Regardons ce que ça donne avec $0,23\overline{92}$. En alternant les couleurs de ce nombre, j'obtiens $0,2\overline{392}92\overline{392}92\overline{392}\dots$, d'où $(0,2\overline{392}; 0,3\overline{92})$. Ce point est bien dans le carré construit sur $[0; 1[$ que l'on peut exprimer sous forme rationnelle pour obtenir $(290/990; 389/990)$.

Léo

Super! Ça marche aussi dans l'autre sens (illustration ci-contre). Supposons que je choisis le point $(290/990; 389/990)$. En exprimant les composantes sous forme de déve-

loppements infinis, j'obtiens alors le point $(0,292\ 92\ 92\dots; 0,392\ 92\ 92\dots)$. En combinant les composantes sous la contrainte que les coupures ne sont pas après les 9, j'ai donc $0,2\overline{392}92\overline{392}92\overline{392}\dots$. C'est un point unique sur le segment $[0; 1[$ que je peux exprimer sous forme rationnelle, pour obtenir $2\ 369/9\ 900$. (Illustration en bas de page à droite).

Développement irrationnel

Zia

Un nombre ayant un développement infini non périodique, peut-il poser un problème ?

Léo

Oui, en le scindant, on peut obtenir une partie ayant un développement infini non périodique et une partie périodique se terminant par des 9.

Prenons sur $[0; 1[$ le point associé à l'irrationnel $0,1949\ 2919393959692949\dots$. En écrivant en noir les décimales impaires et en rouge les décimales paires, j'aurais

$$0,1\overline{949}\ 2919393959692949\dots$$

auquel je ferais correspondre

$$(0,142\ 133\ 562\ 4\dots; 0,999\ 999\ 999\dots).$$

Ce point n'est pas dans le carré construit sur le segment $[0; 1[$. Mais si j'impose que les coupures ne peuvent pas être après un 9, j'obtiens alors

$$0,1\overline{949}\ 29193\overline{939}59692949\dots$$

auquel je fais correspondre le point

$$(0,192\ 939\ 592\dots; 0,949\ 193\ 969\dots)$$

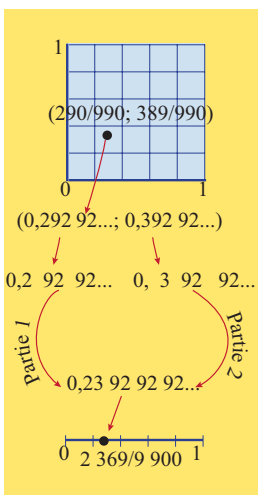
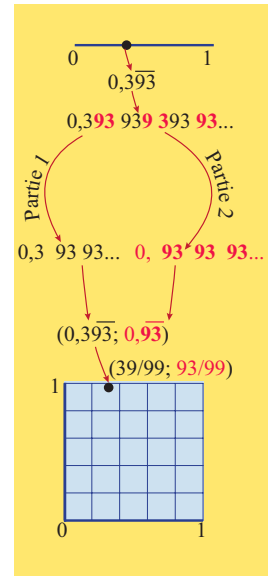
Zia

On fractionne de la même façon que pour les rationnels.

Il faut donc préciser que le développement décimal du nombre ne se termine pas par des 9 et que dans la scission de celui-ci, la coupure ne doit pas être après un 9.

Zia

En respectant cette contrainte, l'application est injective et bijective, c'est donc une bijection et on a autant de points dans le segment de droite $[0; 1[$ que dans le carré construit sur ce segment.



TRIPLETS PYTHAGORIENS

Zia explique à Léo comment cacher tous les triplets pythagoriens.

André Ross
Professeur retraité



Zia

J'ai quelques questions pour toi. Est-ce que tu connais les triplets pythagoriens?

Léo

Bien sûr, ce sont les triplets $(a; b; c)$ qui sont une solution du théorème de Pythagore

$$a^2 + b^2 = c^2,$$

comme $(3; 4; 5)$ ou $(5; 12; 13)$.

Zia

Sais-tu, par exemple, que $(3; 4; 5)$ et $(5; 12; 13)$ sont appelés *triplets pythagoriens primitifs* et leurs multiples, comme $(6; 8; 10)$ ou $(15; 36; 39)$ ne sont pas primitifs?

Léo

Je ne connaissais pas l'appellation triplets pythagoriens primitifs.

Zia

Savais-tu qu'on peut associer chaque triplet à un point du quart du cercle trigonométrique?

Léo

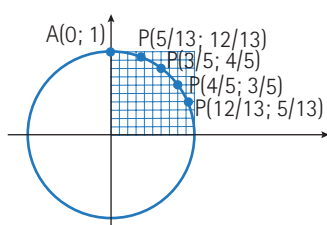
Ça n'a pas rapport, l'équation du cercle trigonométrique est

$$x^2 + y^2 = 1.$$

Zia

Au lieu de multiplier par un nombre entier positif, tu multiplies par l'inverse multiplicatif du plus grand des nombres du triplet. Tu obtiens alors

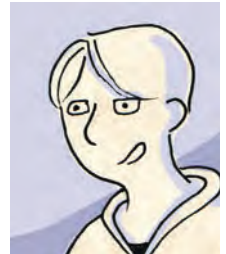
$$\left(\frac{3}{5}; \frac{4}{5}; 1\right) \text{ et } \left(\frac{5}{13}; \frac{12}{13}; 1\right).$$



Le point $(3/5; 4/5)$ est bien un point du cercle trigonométrique, tout comme $(5/13; 12/13)$.

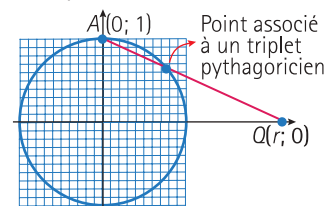
Léo

C'est vrai aussi pour les couples $(4/5; 3/5)$ et $(12/13; 5/13)$ qui correspondent aux triplets $(4; 3; 5)$ et $(12; 5; 13)$.

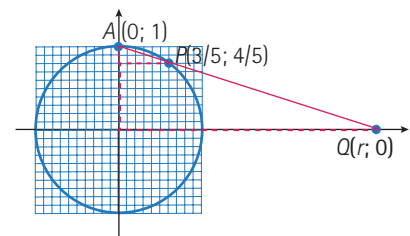


Zia

Tu as sans doute remarqué qu'à partir du point $A(0; 1)$, on peut tracer une droite passant par le point P associé à un triplet pythagorien et que cette droite coupe l'axe horizontal en un point Q de coordonnées $(r; 0)$.



Essayons de trouver la valeur de r en connaissant le triplet pythagorien. Prenons le point $P(3/5; 4/5)$ qui correspond au triplet $(3; 4; 5)$, essayons de trouver la valeur de r du point $Q(r; 0)$, prolongement de la droite AQ jusqu'à sa rencontre avec l'axe des x.



Le rapport des côtés est le même dans les deux triangles rectangles tracés entre les trois points. On a donc

$$\frac{1 - 4/5}{0 - 3/5} = \frac{1 - 0}{0 - x}, \text{ d'où } x = 3.$$

Si je choisis plutôt le point $(4/5; 3/5)$ associé au triplet $(4; 3; 5)$, j'obtiens:

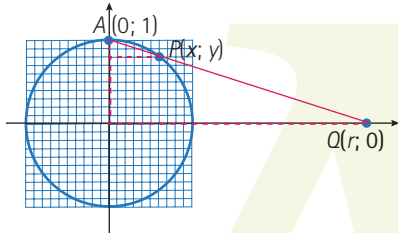
$$\frac{1 - 3/5}{0 - 4/5} = \frac{1 - 0}{0 - x}, \text{ d'où } x = 2.$$

Léo

La valeur de r n'est pas toujours un nombre entier. En prenant le point $(12/13; 5/13)$, je trouve $r = 3/2$.

Zia

Supposons que les coordonnées du point associé à un nombre pythagoricien sont $P(x; y)$.



Le rapport des côtés est alors

$$\frac{1-y}{0-x} = \frac{1-0}{0-r}, \text{ d'où } y = 1 - \frac{x}{r},$$

c'est l'équation de la droite AQ .

Léo

Je vois, il faut rechercher le point de rencontre de la droite AQ et du cercle trigonométrique. On a vu en classe qu'il faut substituer les données de l'équation de la droite dans celle du cercle. On obtient

$$\begin{aligned} x^2 + \left(1 - \frac{x}{r}\right)^2 &= 1 \\ x^2 + 1 - \frac{2x}{r} + \frac{x^2}{r^2} &= 1 \\ x^2 + \frac{x^2}{r^2} - \frac{2x}{r} &= 0 \end{aligned}$$

Zia

C'est une équation quadratique, on peut trouver ses zéros en factorisant, puisque la constante est nulle. On obtient

$$x^2 \left(1 + \frac{1}{r^2}\right) = \frac{2x}{r}$$

Ce qui donne $x = 0$ et $x \left(1 + \frac{1}{r^2}\right) = \frac{2}{r}$,
d'où

$$x = \frac{2/r}{1 + 1/r^2} = \frac{2/r}{(r^2 + 1)/r^2} = \frac{2r}{r^2 + 1}.$$

Qu'est-ce qu'on peut dire de plus?

Léo

Cette valeur est l'abscisse du point P en la substituant dans l'équation de la droite, on obtient

$$\begin{aligned} y &= 1 - \frac{2r/(r^2 + 1)}{r} = 1 - \frac{2}{r^2 + 1} \\ &= \frac{r^2 + 1}{r^2 + 1} - \frac{2}{r^2 + 1} = \frac{r^2 - 1}{r^2 + 1}. \end{aligned}$$

Les coordonnées du point sur le cercle trigonométrique sont donc

$$\left(\frac{2r}{r^2 + 1}, \frac{r^2 - 1}{r^2 + 1}\right).$$

Zia

Vérifions que tout fonctionne, si $r = 3$, les coordonnées du point sont

$$\left(\frac{2 \times 3}{3^2 + 1}, \frac{3^2 - 1}{3^2 + 1}\right) = \left(\frac{6}{10}, \frac{8}{10}\right) = \left(\frac{3}{5}, \frac{4}{5}\right).$$

Et, en posant $r = 2$, on obtient $(4/5; 3/5)$.

Léo

Puisque le point P représente un triplet pythagoricien, ses coordonnées sont des nombres rationnels. Par conséquent, la pente de la droite AQ est un nombre rationnel et, puisqu'un des points de la droite, soit $(0; 1)$, est formé de deux nombres rationnels, les coordonnées du point Q sont des nombres rationnels. Réciproquement, si r est un nombre rationnel, les coordonnées du point P sont des nombres rationnels.

Zia

Puisque r est un nombre rationnel, on peut le représenter par p/q . En substituant dans les coordonnées, on obtient

$$\left(\frac{2pq}{p^2 + q^2}, \frac{p^2 - q^2}{p^2 + q^2}\right),$$

où p et q , tels que $p > q > 0$ sont des nombres rationnels.

Léo

Prenons le nombre rationnel $r = p/q = 5/2$ qui donne

$$\left(\frac{2pq}{p^2 + q^2}, \frac{p^2 - q^2}{p^2 + q^2}\right) = \left(\frac{20}{29}, \frac{21}{29}\right).$$

Ce point est donc associé au triplet pythagoricien primitif $(20; 21; 29)$.

Zia

Si j'essaie avec $r = p/q = 7/3$, j'obtiens

$$\left(\frac{2pq}{p^2 + q^2}, \frac{p^2 - q^2}{p^2 + q^2}\right) = \left(\frac{42}{58}, \frac{40}{58}\right).$$

Ce point est associé au triplet $(42; 40; 58)$, celui-ci n'est pas primitif. Le triplet primitif associé est $(21; 20; 29)$.

Léo

Super! On peut tous les trouver.

DIALOGUE GÉOMÉTRICO-ALGÈBRIQUE À SAVEUR HIPPOCRATIQUE

Courte pièce de théâtre en un seul acte et à deux personnages, se déroulant à une époque incertaine – mais où fourmillent des connaissances issues tant de la géométrie de la Grèce antique que de l'algèbre de la Renaissance. Le rideau s'ouvre sur un parc. Assises sur un banc, Madame Figure Géométrique et Madame Équation Algébrique conversent, tandis que les abondantes progénitures de l'une et de l'autre jouent dans un vaste carré de sable en y traçant des figures et des signes divers.

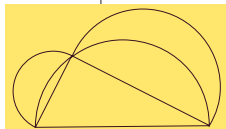
Bernard R. Hodgson
Université Laval

Madame Figure Géométrique (F.G.)

J'ai reçu ce matin même un colis contenant une foule de documents, dont certains en rapport avec Hippocrate.

Madame Équation Algébrique (É.A.)

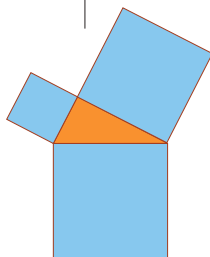
Le toubib?¹



F.G. Non, notre Hippocrate, le géomètre.² J'y ai trouvé entre autres une figure vraiment fascinante. Regardez.

É.A. C'est en effet assez joli. Mais vous savez bien, chère amie, que ce genre de figure, pour moi c'est du chinois. Je préfère l'algèbre!

F.G. On n'est pourtant pas ici dans les maths chinoises, mais bien chez les Grecs de l'Antiquité. De fait, il s'agit, à mes yeux, d'un petit bijou de la géométrie dont le point de départ serait la figure suivante.



(Avec un bâton, Madame F.G. commence à tracer une série de figures sur le sol)

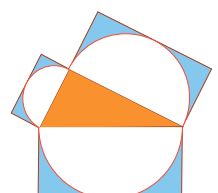
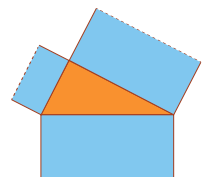
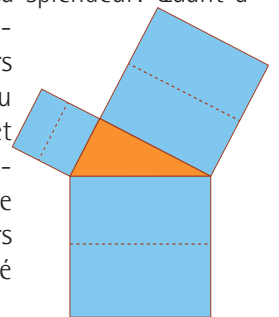
1. Hippocrate de Kos (env. -460 – -377), considéré comme le père de la médecine — on peut penser ici au célèbre serment d'Hippocrate, prêté traditionnellement par les médecins en Occident.
2. Hippocrate de Chios (env. -470 – -410), mathématicien et astronome grec, qui s'est intéressé notamment aux problèmes de la quadrature du cercle et de la duplication du cube.

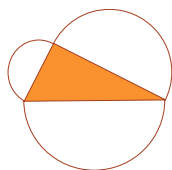
Vous la reconnaissez certainement : c'est celle qui accompagne la proposition 47 du Livre I des *Éléments* de ce cher Euclide.

On est là, je vous assure, dans de la géométrie fort belle, avec le fameux *théorème de l'hypoténuse*, auquel l'histoire a attribué le nom de Pythagore, notre maître à tous : *les carrés construits sur les deux côtés de l'angle droit d'un triangle rectangle sont égaux, en aire, à celui construit sur l'hypoténuse.*

É.A. Je vois bien sûr ce dont vous parlez. Mais sachez qu'il y a là aussi en action de l'algèbre dans toute sa splendeur! Quant à moi, convenant d'appeler a et b les longueurs des deux cathètes du triangle rectangle et c , celle de son hypoténuse, je vois dans cette figure qu'on a alors la célèbre égalité $a^2 + b^2 = c^2$.

F.G. Je veux bien. Dites-moi, n'est-il pas vrai que si on enlève à chacun des trois carrés sa moitié, et qu'on inscrit dans chacun des rectangles résultants un demi-cercle de diamètre le côté correspondant du triangle, alors les deux demi-cercles sur les cathètes,





considérés selon leur aire, sont égaux au demi-cercle sur l'hypoténuse?

É.A. Vraiment?

F.G. C'est de fait ce qu'affirme Euclide, dans un cadre plus général, à la proposition VI.31 de ses *Éléments* : dans un triangle rectangle, la figure construite sur l'hypoténuse est égale en aire à celles sur les deux côtés de l'angle droit, semblablement décrites.

É.A. Attendez. Oui, oui, je vois que cela revient, algébriquement parlant, à généraliser l'égalité de Pythagore en multipliant ses deux membres, à chacune des étapes de votre processus, par une constante k bien choisie. Partant de l'égalité $a^2 + b^2 = c^2$, on la transforme de la sorte en $k(a^2 + b^2) = kc^2$, c'est-à-dire $ka^2 + kb^2 = kc^2$.

Ainsi, reprenant votre série de figures, on passe d'abord d'un carré à sa moitié en multipliant les trois aires par le facteur $1/2$:

$$\frac{1}{2}a^2 + \frac{1}{2}b^2 = \frac{1}{2}c^2.$$

Facile! Cette étape nous parle donc de certains rectangles construits sur les trois côtés du triangle. Et pour le demi-cercle... hum, chaque côté du triangle est le diamètre du demi-cercle correspondant. Si on pensait au cercle total construit sur ce diamètre, on aurait donc un facteur $\pi/4$ qui interviendrait ici. Mais comme il s'agit d'un demi-cercle, il faut couper en deux.

Bref, la transformation de chaque carré en demi-cercle s'opère donc algébriquement par le truchement du facteur $\pi/8$, de sorte que l'égalité de Pythagore devient alors

$$\frac{\pi}{8}a^2 + \frac{\pi}{8}b^2 = \frac{\pi}{8}c^2.$$

C'est bon, je suis d'accord avec votre affirmation : en additionnant les aires des deux demi-cercles ayant pour diamètre l'un et l'autre des deux cathètes, on obtient bien l'aire du demi-cercle de diamètre l'hypoténuse!

F.G. Parfait! Nous arrivons maintenant à la pirouette fabuleuse! Prenez le demi-cercle sur l'hypoténuse et faites-le pivoter autour de cet axe. Que va-t-il lui arriver?

É.A. (feignant l'inquiétude) Je me le demande bien. J'espère qu'il ne va pas s'épivarder!

F.G. Point du tout! Il va finir par tomber pile-poil sur le sommet de l'angle droit du triangle! N'est-ce pas magnifique?

É.A. Vous m'en direz tant.

F.G. Mais évidemment! En parlant de faire pivoter le demi-cercle autour de son diamètre, c'était une façon imagée de dire : considérons le cercle ayant pour diamètre l'hypoténuse du triangle rectangle. N'est-il pas bien connu que ce cercle est circonscrit au triangle?

É.A. (hésitante) Hum...

F.G. Cela est relié au fait que le point milieu de l'hypoténuse d'un triangle rectangle est équidistant de ses trois sommets.

É.A. (à nouveau hésitante) Hummm...

F.G. Vous n'avez qu'à penser au rectangle sous-entendu dans cette dernière figure.

É.A. Oui... le rectangle! Oui, oui, oui, je vois! (en aparté) Je ne vois rien du tout! Mais je vais y repenser tout à l'heure calmement chez moi...³

F.G. Eh bien! alors, poursuivons. En éliminant quelques traits superflus, on se retrouve avec une jolie figure, sur laquelle repose celle que j'ai trouvée dans mon colis de ce matin. Et en y mettant un peu de couleur, on peut même faire ressortir les deux lunules sur les cathètes.

É.A. Les deux lu... quoi?

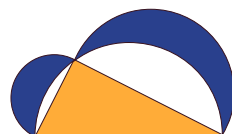
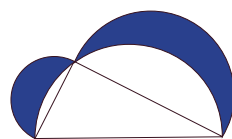
F.G. Les deux lunules, les régions, en forme de croissant de lune, délimitée chacune par des arcs de cercles passant par deux points donnés.⁴ Et rappelez-vous, ma chère, que les demi-cercles sur les cathètes ont même aire que le demi-cercle sur l'hypoténuse.

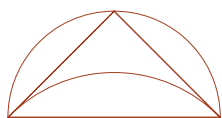
É.A. Oui, je sais, c'est ce que dit mon égalité en $\pi/8$. Mais attendez! Je vois alors que si on considère une à une chacune des cinq plages composant votre dernière figure, on a que vos deux lunules, prises ensemble, ont même aire que le triangle de départ!

F.G. Vous avez tout vu! C'est bien cela, le beau résultat démontré par notre bon Hippocrate.³

3. Voir la Section problèmes

4. Voir le Pour en savoir plus!





Et comme Hippocrate savait que tout triangle peut facilement être transformé en un carré de même aire, il savait donc aussi comment « quarrer » les lunules en question.

É.A. Oui, oui, je me rappelle bien la construction géométrique pour la quadrature du triangle : on passe graduellement d'un triangle quelconque à un triangle rectangle de même aire, puis à un rectangle toujours de même aire, et enfin au carré – et toutes ces étapes peuvent être exécutées à la règle et au compas!⁵

F.G. Exactement! Je vois que vous vous souvenez fort bien de ce processus.

Mais ce n'est pas tout. J'ai ici quelque chose d'encore plus étonnant à vous montrer. Voici une autre figure qui se trouvait aussi parmi les documents que j'ai reçus ce matin.

É.A. Encore une lunule! Mais celle-ci me semble un peu étrange. On voit comme une grosse lunule accrochée à ce qui me paraît être un triangle à la fois rectangle et isocèle.

F.G. Vous avez tout à fait raison! Il s'agit d'un autre type de lunule étudiée par Hippocrate. Et qu'y retrouve-t-on au juste? Sans surprise, on considère d'une part, pour le grand arc supérieur, le demi-cercle ayant pour diamètre l'hypoténuse d'un tel triangle. À noter que cet arc se trouve ainsi divisé en deux petits arcs égaux, correspondant chacun à un quart du cercle total ici sous-entendu.

La bonne question maintenant est : que dire de l'autre arc, au bas de la lunule?

É.A. Il est plus aplati que l'autre. Mais encore...

F.G. Vous voulez peut-être un indice? Pensez à Euclide VI.31...

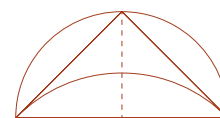
É.A. Oh vous savez, moi, les numéros des propositions d'Euclide, ce n'est pas mon fort...

5. Voir André Ross, « Comparaison d'aires : 1. la règle et le compas. » Accromath, vol.17(1) (2022) pp. 26-29.

F.G. Chère amie, je vous en parlais il y a quelques minutes : la proposition 31 du Livre VI des *Éléments* d'Euclide généralise le théorème de Pythagore au cas de figures « semblables et semblablement décrites » sur les trois côtés d'un triangle rectangle.

On voit bien sur la figure les deux segments circulaires⁶ identiques construits sur les deux cathètes du triangle. Que peut-on dire à propos de leur forme?

Pour vous aider, qu'arrive-t-il si on abaisse la hauteur du triangle relative à l'hypoténuse?



É.A. Je vois le demi-disque, c'est-à-dire la région déterminée par le demi-cercle et l'hypoténuse, être partagé en deux parties identiques. On obtient ainsi deux secteurs circulaires⁶ égaux.

F.G. Et c'est précisément là que réside la clé du mystère : les deux segments circulaires au haut de la figure sont un peu comme des boules de crème glacée qui débordent de cornets – j'entends par cornets la partie inférieure des secteurs circulaires, c'est-à-dire les deux moitiés du triangle de départ dont les pointes se rencontrent au milieu de l'hypoténuse.

É.A. Je pense que je comprends ce que vous voulez dire. Il s'agit alors de trouver quel est le cornet qui aurait une boule de crème glacée de même proportion, au bas de la figure.

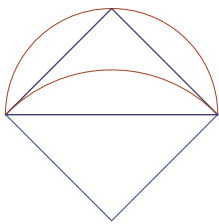
F.G. En plein dans le mille! Ou pour le dire à la Euclide, une boule de crème glacée semblable et semblablement construite, comparativement aux deux boules sur les cathètes du triangle.

De fait, en décrivant la situation de façon un peu plus précise, on se demande quel est le secteur circulaire qui correspond au segment circulaire sous la lunule. On est donc à la recherche d'un autre cercle...

6. Un segment circulaire est la région de l'intérieur d'un cercle délimitée par une corde et l'arc correspondant. Un secteur circulaire est la région délimitée par deux rayons et l'arc correspondant.

Or n'oublions pas que sur la figure, chacun des deux petits arcs au haut de la lunule vaut un quart de cercle. Il s'agit donc de trouver quel est le cercle tel que l'arc au bas de la lunule en serait le quart. Auriez-vous une suggestion pour le situer, ce cercle?

É.A. Tout à l'heure, pour la première figure, vous parliez d'un rectangle (*en aparté* : que je n'ai jamais vu...). Comme le triangle rectangle est maintenant isocèle, serions-nous par hasard à la recherche d'un carré?



F.G. Jolie intuition! C'est tout à fait ça! Et le voici, le carré recherché. Il s'agit tout simplement du carré qui vient dupliquer le triangle de départ et qui a comme diagonale l'hypoténuse de ce triangle.

É.A. Oooh! Et là, je vois bien le cornet dont la boule de crème glacée est délimitée par l'arc au bas de la lunule. Ou, pour reprendre un vocabulaire géométrique de bon aloi, on voit bien le secteur circulaire qui vaut donc le quart d'un certain disque. Et ce disque, ma foi, semble correspondre au cercle circonscrit au carré ayant pour côté la diagonale du carré précédent, c'est-à-dire l'hypoténuse du triangle de départ. Est-ce bien cela?

F.G. Voilà, tout est dit!

É.A. Pas tout à fait en ce qui me concerne, car il me reste à algébriser cette dernière figure. Voyons voir... Il me faut donc trouver l'aire du cercle circonscrit à un carré de côté donné, puis trouver l'aire de tous les segments circulaires tout autour de ce carré, et diviser par 4, et finalement comparer avec les deux segments circulaires au haut de la lunule...

(Elle réfléchit tout en marmonnant)

F.G. Je suis sûre que ça ne devrait pas être trop tordue comme algèbre : le cadre géométrique est tellement beau!

É.A. Je suis d'accord, quoique les détails ne me viennent pas *hic et nunc*. Mais je sens en effet que ça devrait marcher.⁷

Merci pour cette balade géométrique. Allez, je vous laisse. Je rencontre cet après-midi mon club de résolution d'équations polynomiales par radicaux. Au programme aujourd'hui : rafraîchir nos souvenirs sur le 4^e degré! Allez, venez, mes enfants!

F.G. (*un brin moqueuse*) Amusez-vous bien avec vos équations! Pour ma part, je m'en vais rejoindre mes petiots et petiotes pour explorer quelques figures dans le sable, comme le grand Archimède, tout juste avant de se faire trucher.

(*Madame Équation Algébrique quitte le parc, suivie de sa ribambelle de rejetons. Rideau.*)

7. Voir la Section problèmes.



La mort d'Archimède

À propos de cette illustration: voir la section Pour en savoir plus!

Calculer une racine carrée de tête?

Roméo, excité d'avoir tout juste appris une nouvelle astuce mathématique, va voir sa cousine Clara pour la lui montrer.

Tommy Mastromonaco
UQÀM

Roméo

Clara, aimerais-tu voir un tour de magie?

Clara

Bien sûr, montre-moi!

Roméo

Donne-moi un nombre au hasard entre 10 et 100.

Clara

Disons 37.

Roméo

Eh bien, je t'affirme que la racine de ce nombre est d'environ... 6,083.

Clara

Ah oui? Attends un peu que je sorte ma calculatrice... la racine carrée de 37 est 6,0828... Mais comment as-tu fait?

Roméo

Un magicien ne révèle jamais ses secrets! Mais comme je ne suis pas réellement un magicien, je vais te l'expliquer. Ma prof de maths m'a appris un truc pour calculer mentalement une valeur approximative d'une racine carrée. Voici comment j'ai fait.

D'abord, j'ai cherché le carré parfait le plus proche du nombre 37. C'est 36, dont la racine carrée est 6. Ensuite, j'ai calculé la différence entre le nombre de départ et le carré parfait, soit ici $37 - 36 = 1$, puis j'ai divisé ce résultat par 2 et par la racine du carré parfait, 6. J'obtiens ainsi 1 divisé par 2 divisé par 6, soit $1/12$. Pour terminer, j'ai tout simplement ajouté $1/12$ à 6, pour obtenir 6 et $1/12$, qui est environ 6,083.

Clara

C'est fascinant! Mais qu'arrive-t-il si le carré parfait le plus proche est plus grand que le nombre de départ, comme avec 23 par exemple?

Roméo

C'est une bonne question. Dans ce cas, je fais exactement la même chose, mais à la dernière étape, je soustrais la fraction au lieu de l'ajouter.

Clara

Donc, si j'ai bien compris, pour la racine carrée de 23, le calcul est le suivant. Ici, le nombre carré le plus proche de 23 est 25, dont la racine carrée est 5. J'ai $25 - 23 = 2$, donc la fraction à calculer est 2 divisé par 2, que je divise par 5, soit $1/5$. Enfin, je la soustrais à 5, ce qui me donne $5 - 1/5 = 4,8$.

Vérifions avec la calculatrice. Je trouve que la racine carrée de 23 est 4,7958... Encore une fois, c'est très proche.

Roméo

J'aimerais tellement savoir pourquoi ça fonctionne!

Clara

Je crois qu'on peut le découvrir par nous-mêmes. Prenons n comme étant le nombre dont on souhaite calculer \sqrt{n} , et c comme étant un carré parfait proche de n . Autrement dit, n est approximativement égal à c

$$n \approx c.$$

Essaie d'exprimer ton calcul avec ces variables.

Roméo

D'accord. Je fais d'abord la différence $n - c$ que je divise par 2 et par la racine de c . J'obtiens

$$\frac{n - c}{2\sqrt{c}}.$$

Enfin, j'ajoute \sqrt{c} à ce résultat, ce qui me donne

$$\sqrt{c} + \frac{n - c}{2\sqrt{c}}.$$

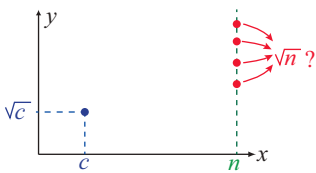
Clara

Parfait. Ce qu'on déduit de tout cela, c'est que

$$\sqrt{n} \approx \sqrt{c} + \frac{n-c}{2\sqrt{c}}$$

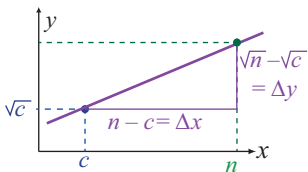
vu que ce calcul donne un résultat très proche de \sqrt{n} . Essayons de voir pourquoi cette approximation fonctionne. Gardons cette expression de côté pour le moment. Pour simplifier, supposons que $n > c$. Plaçons sur le plan cartésien les points de coordonnées $(c; \sqrt{c})$ et $(n; \sqrt{n})$.

Roméo



On ne connaît pas l'ordonnée du point $(n; \sqrt{n})$ vu que c'est précisément ce qu'on cherche à calculer.

Clara



Exact. Relions ces deux points par une droite, et construisons un triangle rectangle dont la longueur de la projection horizontale est $n - c$, et la longueur de la projection verticale est $\sqrt{n} - \sqrt{c}$, qui elle est inconnue.

Roméo

Attends un peu... si on arrive à déterminer la pente de cette droite, on peut alors déduire la longueur de la droite horizontale, et donc trouver \sqrt{n} !

Clara

Et quelle est la pente de cette droite?

Roméo

C'est
$$m = \frac{\Delta y}{\Delta x} = \frac{\sqrt{n} - \sqrt{c}}{n - c}$$

Cela ne nous aide pas beaucoup...

Clara

Mais bien sûr! Essayons de transformer algébriquement cette fraction. Il y a une différence de radicaux au numérateur. Faisons apparaître le conjugué :

$$\frac{\sqrt{n} - \sqrt{c}}{n - c} = \frac{\sqrt{n} - \sqrt{c}}{n - c} \times \frac{\sqrt{n} + \sqrt{c}}{\sqrt{n} + \sqrt{c}}$$

Au numérateur, on obtient une différence de carrée de la forme

$$(a - b)(a + b) = a^2 - b^2,$$

avec $a = \sqrt{n}$ et $b = \sqrt{c}$. Le numérateur est donc

$$(\sqrt{n} - \sqrt{c})(\sqrt{n} + \sqrt{c}) = (\sqrt{n})^2 - (\sqrt{c})^2 = n - c.$$

Ainsi, la pente devient

$$m = \frac{\sqrt{n} - \sqrt{c}}{n - c} = \frac{n - c}{(n - c)(\sqrt{n} + \sqrt{c})} = \frac{1}{\sqrt{n} + \sqrt{c}}$$

Roméo

Et que fait-on avec cela, maintenant?

Clara

Puisque que $n \approx c$, alors $\sqrt{n} \approx \sqrt{c}$. On va ainsi approximer la pente de la droite en remplaçant l'inconnue \sqrt{n} par \sqrt{c} :

$$\frac{\sqrt{n} - \sqrt{c}}{n - c} \approx \frac{1}{\sqrt{c} + \sqrt{c}} = \frac{1}{2\sqrt{c}}$$

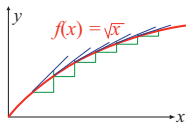
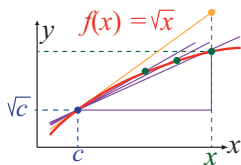
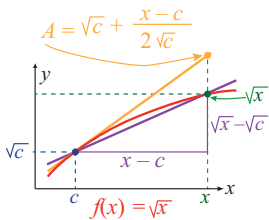
Autrement dit,

$$\frac{\sqrt{n} - \sqrt{c}}{n - c} \approx \frac{1}{2\sqrt{c}}$$

Maintenant, isole \sqrt{n} dans cette équation.



1. Voir également Extraction d'une racine dans un carré, par Bernard Hodgson, Accromath, volume 1, 2006, p. 16.



Roméo

D'accord. Je multiplie chaque côté de l'expression par $n - c$, ce qui donne

$$\sqrt{n} - \sqrt{c} \approx \frac{n - c}{2\sqrt{c}},$$

Et j'ajoute \sqrt{c} de chaque côté :

$$\sqrt{n} \approx \sqrt{c} + \frac{n - c}{2\sqrt{c}}.$$

Eh! C'est exactement mon calcul!

Clara

Tout à fait, et on l'a déduit avec seulement quelques manipulations algébriques. Mais ce n'est pas tout! Reprenons le schéma de tout à l'heure. Traçons la courbe de la fonction racine carrée $f(x) = \sqrt{x}$. Prenons x au lieu de n , et la variable A pour dénoter l'approximation

$$A = \sqrt{c} + \frac{x - c}{2\sqrt{c}}.$$

La droite dont nous voulions approximer la pente est la *droite sécante* reliant les points $(c; \sqrt{c})$ et $(x; \sqrt{x})$. La pente approximative $1/2\sqrt{c}$ que nous avons obtenu est celle de la *droite tangente* au point $(c; \sqrt{c})$, et qui relie les points $(c; \sqrt{c})$ et $(x; A)$. Rappelle-toi que l'approximation donnée par ton calcul repose sur l'approximation $\sqrt{x} \approx \sqrt{c}$ que l'on a utilisé pour déterminer la pente approximative. Dans ce cas, plus x et c sont rapprochés, alors plus \sqrt{x} et \sqrt{c} sont proches, et donc l'approximation est de plus en plus précise. Par conséquent, le calcul est plus juste lorsque le carré parfait est proche du nombre de départ!

Roméo

Graphiquement, cela correspond à ce que les droites sécantes se rapprochent de plus en plus de la droite tangente au point $(c; \sqrt{c})$, incluant leur pente!

Clara

Exactement. Je te fais remarquer qu'on peut tracer une droite tangente en plusieurs points de la fonction, pas seulement au point $(c; \sqrt{c})$. Ces droites tangentes sont essentielles parce qu'elles nous informent sur la croissance de la fonction! Regarde attentivement la pente de ces droites.

Roméo

Elles deviennent de moins en moins pentues à mesure que x augmente; leur pente diminue.

Clara

Et que peux-tu dire de la croissance de la fonction $f(x) = \sqrt{x}$?

Roméo

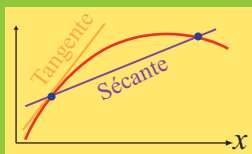
Elle est croissante, mais moins quand x est élevé.

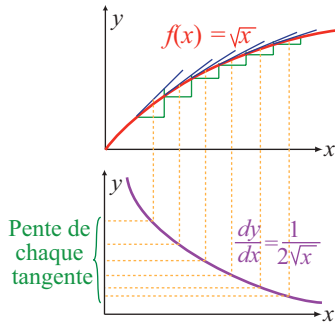
Clara

J'en déduis que la pente d'une tangente en un point mesure la croissance de la fonction en ce point! Vu qu'il est possible de tracer la tangente en chaque point de la courbe, on arrive dans ce cas à mesurer sa croissance en chaque point. Autrement dit, nous pouvons générer une fonction, à partir de la fonction de départ $f(x) = \sqrt{x}$, qui indique en tout point la croissance de cette fonction. On l'appelle la « dérivée de f ». Elle est écrite souvent de différentes manières : parfois f' , ou bien $\frac{df}{dx}$ ou alors $\frac{dy}{dx}$, justement pour bien mettre en évidence qu'elle provient de la pente $m = \frac{\Delta y}{\Delta x}$ d'une droite tangente.

Les droites sécantes et tangentes

On dit qu'une droite est sécante à une courbe lorsqu'elle intercepte la courbe en deux points. Autrement dit, elle « sépare » ou « coupe » la courbe (sécante vient du latin secans qui signifie « coupant »). Une droite est dite tangente à une courbe en un point lorsqu'elle touche la courbe seulement en ce point au voisinage du point (tangente vient du latin tangere signifiant « toucher ».)





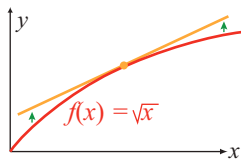
Roméo

Est-ce qu'on connaît la dérivée de la fonction racine carrée?

Clara

Bien sûr : on l'a déjà calculée! Rappelle-toi que la pente de la tangente de cette fonction au point $(c; \sqrt{c})$ est $m = 1/2\sqrt{c}$. Autrement dit, pour $x = c$, la dérivée de f est égale à $m = 1/2\sqrt{c}$. Ici, c peut bien être n'importe quel nombre réel positif! La dérivée de f est par conséquent

$$f'(x) = \frac{1}{2\sqrt{x}}$$



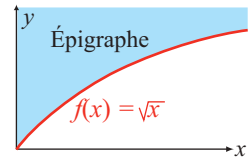
La fonction dérivée est positive lorsque f est croissante, parce que les tangentes sont de pente positive. Et la dérivée est décroissante en x , c'est-à-dire que la pente des tangentes diminue quand x augmente. Ceci fait en sorte que les droites tangentes sont toutes au-dessus de la courbe de f ; on dit que la fonction f est concave. Puisque l'approximation A de la racine carrée d'un nombre n est sur l'une de ces droites tangentes, alors l'approximation sera toujours supérieure à la valeur exacte, peu importe que le nombre n soit inférieur ou supérieur au carré parfait c . Ton calcul sera toujours au-dessus de la vraie racine carrée.

Roméo

Je me souviens d'un cours de géométrie dans lequel on avait appris la différence entre des figures géométriques concaves et convexes. Y a-t-il un lien entre cela et les fonctions concaves?

Clara

Certainement. Regarde la zone au-dessus de la courbe d'une fonction concave comme la fonction racine carrée : cette zone, que l'on appelle *épigraphe*, forme une figure géométrique concave!



Roméo

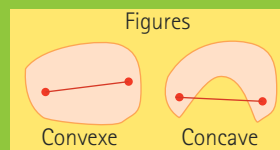
J'ignorais qu'il se cachait autant de choses derrière le tour de magie de ma prof.

Clara

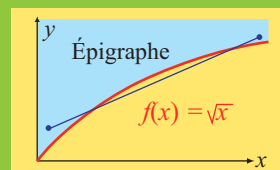
En effet, et ce tour est magique non pas parce qu'il est inexplicable et mystérieux, mais justement parce qu'on peut l'expliquer si simplement. C'est là que réside toute la beauté des mathématiques! Nous avons réussi à comprendre le fonctionnement de ce calcul tout en découvrant des objets et des concepts qui ont une étendue si vaste dans beaucoup de domaines!

Figures convexes et concaves

Une figure géométrique est *convexe* si tout segment reliant deux points quelconques de la figure reste à l'intérieur de cette figure. Au contraire, une figure géométrique est *concave* s'il existe un segment formé par deux points de la figure qui quitte cette figure.



Il est facile de se convaincre que l'épigraphe de la fonction $f(x) = \sqrt{x}$ est une figure concave. Il suffit de déterminer deux points de l'épigraphe dont le lien quitte la figure.



Mettre en mémoire et analyser une image

Comment mettre en mémoire une image ? Très simple ! Il suffit de mettre en mémoire la couleur de chaque pixel. Très simple ? Mais cela demande une quantité énorme de mémoire ! Alors, il vaut mieux faire usage d'astuces et utiliser une méthode qui permet à la fois d'économiser de la mémoire et de comprendre la structure de l'image. Mettre en mémoire une image de manière économique, c'est ce qu'on appelle la compression d'images. Ici, nous allons explorer le format JPEG 2000.

Christiane Rousseau
Université de Montréal



Regardons la photo ci-contre. Elle a 816 pixels de large, et 608 de haut. La couleur de chaque pixel est un mélange des trois couleurs de base : rouge, vert, bleu, et, pour chacune, on a $256 = 2^8$ intensités possibles. Donc, pour chaque pixel il faut $3 \times 8 = 24$ bits d'information, ou encore 3 octets, car un octet vaut 8 bits. Au total, pour donner la couleur des $816 \times 608 = 496\,128$ pixels il faut $496\,128 \times 3 = 1\,488\,384$ octets, soit autour de 1,49 Mo¹. Pourtant, le fichier JPEG de cette photo n'a que 237 Ko, soit autour de 237 000 octets, de l'ordre de 6,28 fois moins !

Effectivement, sur cette photo on a de grandes régions de ciel bleu uniforme, et également de grandes régions blanches très uniformes. On peut imaginer que dans une région très uniforme on peut faire mieux que de lister la couleur de chacun des pixels. Aussi, on n'a pas besoin du même degré de détail si on regarde une petite photo que si on l'agrandit pour en faire une affiche.

1. Quoique le mégaoctet (Mo) soit officiellement défini comme 10^6 octets depuis 1998, cette norme n'est pas universellement appliquée et on trouve encore, en particulier chez les constructeurs de matériel informatique (microprocesseurs, etc.), que le mégaoctet représente $2^{20} = 1\,048\,576$ octets. La différence est de l'ordre de 4,49 %.

Revenons au cas d'une grande région de couleur presque uniforme. Il est plus simple de se donner la couleur globale et de seulement noter les pixels qui ne sont pas de cette couleur. C'est un peu cette idée qu'utilise le standard JPEG 2000, un standard plus performant que le standard JPEG de nos appareils de photo, mais surtout utilisé par les professionnels de l'image. Nous allons le décrire pour une image en tons de gris, un ton de gris étant un nombre de 0 à $255 = 2^8 - 1$, où 0 correspond au noir et 255 au blanc (voir encadré pour la conversion en ton de gris).

La première étape est de transformer l'information. Ainsi, se donner deux nombres, a et b , c'est la même chose que se donner leur moyenne, $x = (a + b)/2$ et la moitié de leur différence, $y = (b - a)/2$. En effet, $b = x + y$ et $a = x - y$.

Appliquons ceci aux 16 pixels des positions 212 à 227 de la ligne 220 en les regroupant 2 par 2.



Leurs tons de gris sont donnés par :

25 23 23 22 31 115 124 125 130 127 138 222 222 228 229 229

Cela nous donne huit moyennes,

24 22,5 73 124,5 128,5 180 225 229

et huit demi-différences.

-1 -0,5 42 0,5 -1,5 42 3 0

Que voit-on ? Que plusieurs des différences sont très petites. Si on garde les nombres tels qu'ils sont, on garde toute l'information sur

la photo. Si on veut compresser l'information, alors on va se permettre d'arrondir à 0 les petits nombres.

On voit aussi que la deuxième ligne met en évidence les endroits où on a un saut de ton de gris.

On va appliquer la même idée en deux dimensions.

L'idée est que toute l'information contenue dans un carré 2x2

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

est contenue dans un nouveau carré 2x2 construit ainsi :

		Transformation	
Avant		Après	
a	b	$\frac{a+b+c+d}{4}$	$\frac{(b-a)+(d-c)}{4}$
c	d	$\frac{(c-a)+(d-b)}{4}$	$\frac{(b+c)-(a+d)}{4}$

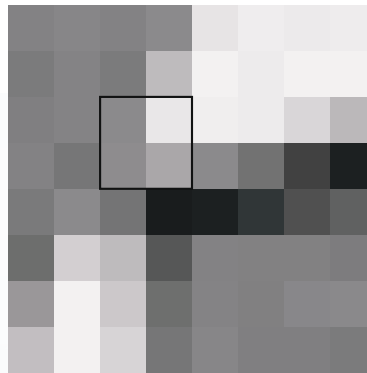
On va appliquer cela à un rectangle $2n \times 2m$ que l'on considère comme un rectangle formé de m rangées de n blocs 2x2 et on va disposer les éléments rouges, bleus, verts et mauves dans des rectangles $n \times m$ disposés comme suit

$$\begin{bmatrix} n \times m & n \times m \\ n \times m & n \times m \end{bmatrix}$$

Regardons la construction. Le coefficient bleu est obtenu en faisant la moyenne des demi-différences horizontales. Il mesure donc des différences verticales. De même, le coefficient vert est la moyenne des demi-différences verticales et mesure des différences horizontales.

Quant au coefficient violet il est la demi-différence de la moyenne sur l'antidiagonale et de la moyenne sur la diagonale. Il mesure les différences obliques.

Regardons le carré 8x8 ci-dessous : il représente les pixels 226 à 233 vers la droite et 216 à 223 vers le bas à partir du coin en haut à gauche de la photo. Sur ce carré on a mis en évidence un petit carré 2x2 sur lequel on va suivre les transformations.



Les tons de gris sont donnés dans le tableau (en caractères gras notre carré 2x2)

126	130	126	134	221	231	228	230
120	127	120	181	234	229	235	234
123	127	134	224	231	228	207	179
126	116	137	162	135	112	64	22
119	135	114	17	24	48	78	96
108	202	182	86	127	125	125	122
146	234	194	108	128	124	131	134
185	234	205	115	130	123	124	120

Maintenant, pour le carré rouge, on va faire les moyennes de chaque carré 2x2 et arrondir.

126	140	229	232
123	164	176	118
141	100	81	106
200	155	126	127

Ci-contre on a, en tons de gris, le carré rouge obtenu de notre carré.

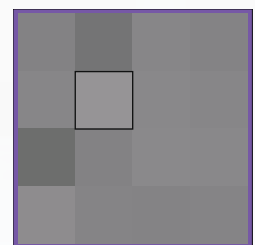
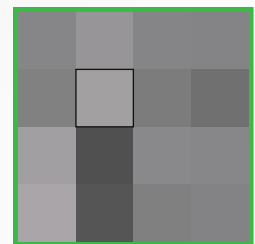
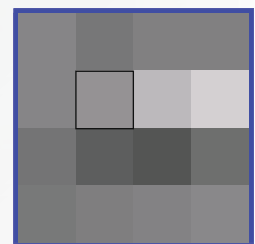
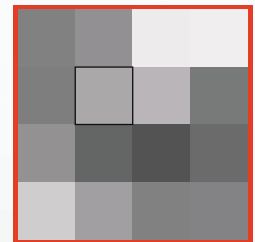
Faisons la même chose pour les carrés bleu, vert et violet, dont les valeurs sont données dans les tableaux suivants et les carrés correspondants ci-contre.

On ne peut comme tel visualiser les tableaux bleu, vert et violet car les entrées sont dans $(-127,5; 127,5)$. Pour visualiser le contenu on va ajouter 127,5 à toutes les valeurs et les représenter (après arrondi) comme des tons de gris.

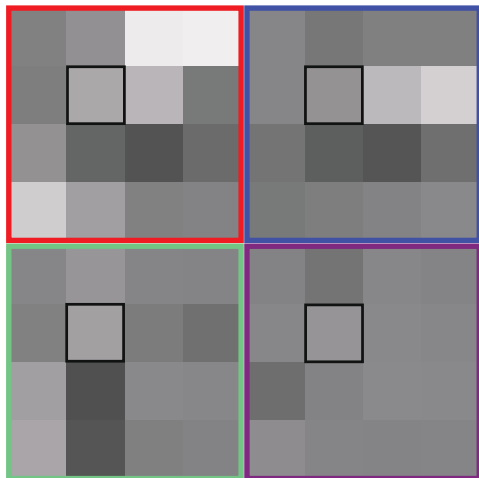
2,25	-10,25	-2,75	-2,75
2	14,75	53	75
-14	-34,25	-45	-18,25
-9,75	-4,5	-0,25	5,25

2,75	17,25	1,25	0,25
-1,5	28,75	-6,5	-17,5
27,5	-48,25	5,5	3,75
34,25	-44	-2,75	-0,25

-0,75	-13,25	3,75	0,75
3,5	16,25	5	3,5
-19,5	-0,25	6,5	5,25
9,75	1	0,75	1,75



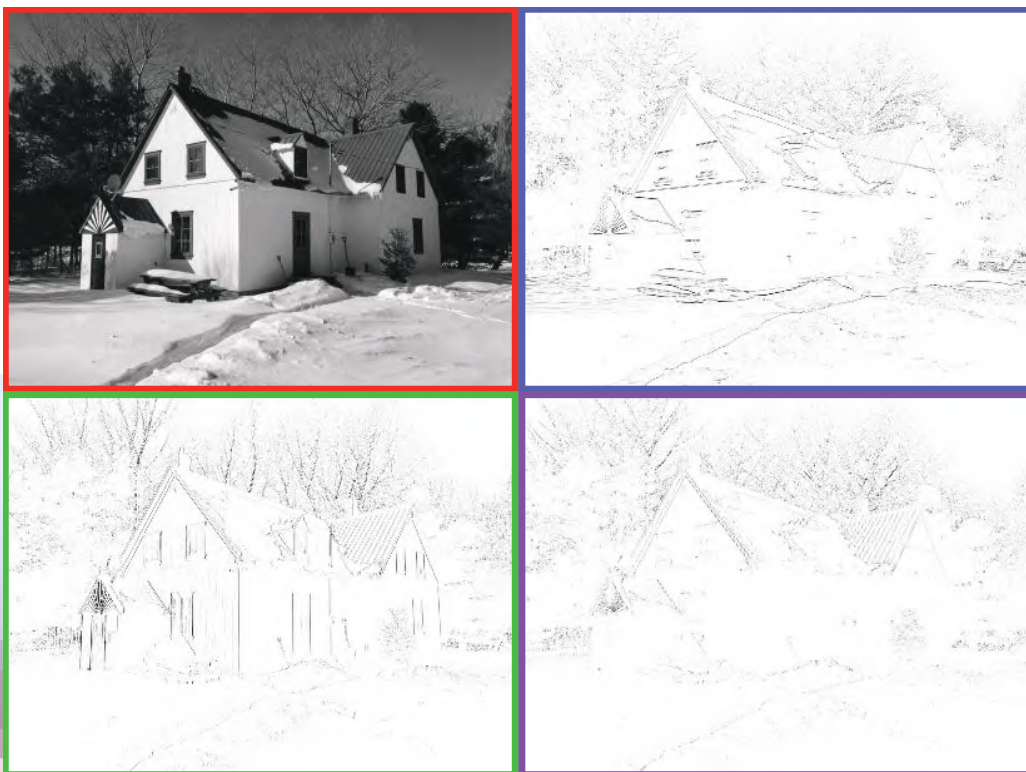
Les quatre tableaux contiennent toute l'information sur l'image, et de manière organisée.



Le carré rouge donne la *structure* de l'image, et les carrés bleu, vert et violet, les *nuances* horizontales, verticales et obliques.

On va maintenant appliquer cela sur le fichier de la photo en tons de gris. Mais les nuances horizontales, verticales et obliques sont difficiles à voir comme différences avec le ton de gris moyen. On va tricher un peu et choisir de représenter en très pâle les petites différences et en foncé les grandes différences, indépendamment de leur signe. Voici ce que cela donne l'illustration en bas de page².

On voit bien que les rectangles bleu, vert et violet font ressortir les contours horizontaux, verticaux et obliques.



2. Les images ont été programmées par Olivier Rousseau.

On peut itérer le processus une deuxième fois sur l'image en haut à gauche. Ceci permet de mettre en lumière de nouvelles structures à l'échelle 4.



Une troisième itération permet de mettre en lumière les structures à l'échelle 8, une quatrième itération met en évidence les structures à l'échelle 16, etc. Voici la quatrième itération.



À chaque étape, on découvre de nouvelles structures à une nouvelle échelle. Ceci nous donne un outil très polyvalent pour analyser l'image.

Comment reconstruire l'image ?

Remarquons que le processus décrit est réversible. On peut donc récupérer l'image en reconstruisant les rectangles rouges (les images moyennes) en partant du plus petit et en s'aidant des rectangles bleu, vert et violet de la même taille pour reconstruire le rectangle rouge précédent et, en itérant jusqu'à reconstruire l'image finale.

A-t-on vraiment avancé ?

Oui ! À condition d'encoder astucieusement l'information. Rappelons que chaque valeur était représentée par 8 bits. On peut décider que certaines valeurs qui apparaissent souvent soient représentées par moins de 8 bits et que les valeurs rares soient représentées par plus de 8 bits ; aussi, que certains groupes de valeurs (par exemple des petits carrés 2x2 qui apparaissent souvent) soient représentés par un unique petit symbole. On pourrait décider d'encoder 30 zéros de suite par l'information 30 et 0. Etc. Encoder astucieu-

sement sans perte d'information est un très grand chapitre de la théorie de l'information, dont l'exemple le plus simple est le codage de Huffman pour l'encodage d'un texte. Un tel encodage pour le format JEG2000 est très sophistiqué et nous ne rentrerons pas dans les détails. Il permet une très bonne compression sans aucune perte d'information !

On peut pousser plus loin la compression en choisissant d'arrondir les entrées et, en particulier, de mettre à zéro toutes les petites entrées. Ensuite, à partir des données compressées on reconstruit l'image initiale. Que signifie « petite entrée » ? Cela dépend du degré de compression voulu. Plus on arrondit les entrées et plus on en annule, plus on compresse !

De multiples applications du format JPEG 2000

La première application du format JPEG 2000 est bien sûr celle qu'on a annoncée, soit de compresser l'image.

Lors de l'encodage, on a regardé l'image à différentes échelles. On peut choisir de la reconstruire en privilégiant une échelle particulière et ainsi mettre en évidence des motifs subtils à cette échelle, mais pouvant passer inaperçus quand tous les détails sont présents.

La conversion en tons de gris et le standard YCbCr

Pour une image en couleurs, on se donne les niveaux d'intensité de rouge, vert et bleu de chaque pixel. Selon les standards, on fonctionne avec 256 niveaux pour chaque couleur, allant de 0 à 255, ou encore avec un nombre entre 0 et 1 correspondant au niveau de couleur divisé par 255. Nous prenons ce deuxième point de vue. La couleur d'un pixel est donc un vecteur

$$V = (r, v, b) \in [0, 1]^3.$$

C'est le format RGB.

La luminance, qui correspond au niveau de gris, est donnée par

$$Y = 0,299r + 0,587v + 0,114b.$$

En fait, même quand on compresse une image en couleurs, il existe un meilleur choix de coordonnées pour donner la couleur de chaque pixel que r, v, b . La première coordonnée est la luminance Y définie ci-dessus.

Comme la lumière blanche est la somme des trois couleurs, pour obtenir toutes les couleurs, il faut retrancher du bleu ou du rouge au ton de gris. Les deux quantités obtenues sont deux informations de *chrominance*, soit la *différence bleu* et la *différence rouge*, données respectivement par

$$C_b = 0,565(b - Y)$$

et

$$C_r = 0,713(r - Y).$$

Le standard YCbCr consiste à se donner le vecteur V par ses coordonnées (Y, C_b, C_r) .

Les coordonnées Y, C_b, C_r sont en général beaucoup moins corrélées que les coordonnées r, v, b , ce qui est plus adapté à la compression.

Les ondelettes et le format JPEG

On a utilisé dans nos exemples des moyennes et des demi-différences. Prendre la moyenne ou la demi-différence de deux pixels voisins, c'est passer un *filtre* sur les données. Les ondelettes sont des *filtres* qu'on passe sur les données d'un signal ou d'une image pour en extraire de l'information. Ici on a utilisé une *ondelette* discrète, l'*ondelette de Haar*. Il existe toute une famille d'ondelettes discrètes, la plus simple étant l'ondelette de Haar qui agit sur deux pixels à la fois

dans chaque direction. On utilise en général dans le format JPEG 2000 des ondelettes plus compliquées que l'ondelette de Haar, et qui agissent sur plus de deux pixels à la fois dans chaque direction. Plusieurs de ces ondelettes ont été construites par la mathématicienne Ingrid Daubechies. C'est l'ondelette 9/7 de Daubechies qui est la plus utilisée dans la compression avec perte d'information du format JPEG 2000.

On peut choisir de garder l'information très précise pour une petite région d'une image et compresser énormément l'information dans les autres régions de l'image. C'est un atout très important lorsqu'on doit gérer des quantités très grandes de données et qu'on a besoin d'énormément de précision dans une petite région. Pour ce but précis, le format JPEG 2000 surpasse de loin les autres méthodes de compression d'images.

JPEG versus JPEG 2000

Même s'il date de près de 25 ans, le format JPEG 2000 est peu répandu, alors que le format JPEG est presque universellement supporté par les outils de lecture d'images. Ainsi, Safari est le seul navigateur supportant JPEG 2000 en 2025. C'est parce que l'encodage et le décodage de JPEG 2000 demandent beaucoup plus de calculs que celui de JPEG ou d'autres formats standards d'images. Cependant, le format JPEG 2000 est privilégié lorsque la qualité des images est importante. En particulier, le rendu des contours contrastés est meilleur. Sur le site d'Adobe, qui supporte ce format, il est écrit : « Grâce à ses taux de compression élevés, JPEG 2000 peut également compresser une image jusqu'à 200% de plus que JPEG tout en conservant la même qualité par rapport à un fichier de même taille. »³ L'Organisation météorologique mondiale a intégré JPEG 2000 dans

son nouveau format de fichier GRIB2, lequel est conçu pour la distribution mondiale des données météorologiques. Le protocole standard international DICOM utilisé en imagerie médicale (Digital Imaging and Communications in Medicine) supporte le format JPEG 2000. Ce format est idéal puisqu'il permet une meilleure compression tout en respectant l'intégrité de l'image.⁴

Ingrid Daubechies

Ingrid Daubechies est une mathématicienne et physicienne d'origine flamande. En 1987, elle s'installe définitivement aux États-Unis. Ses travaux sur les ondelettes lui vaudront d'être conférencière plénière au Congrès international des mathématiciens de 1994 et d'être la première femme à recevoir le très prestigieux prix Wolf de mathématiques en 2023. Ingrid Daubechies a également été la première femme présidente de l'Union mathématique internationale de 2011 à 2014. Elle a travaillé avec des conservateurs de musées à analyser des peintures. En particulier, à l'aide de techniques d'analyse d'images, elle a pu reconstruire une ancienne peinture de van Gogh cachée sous une peinture beaucoup plus récente. En collaboration avec des géophysiciens, elle a aussi utilisé des techniques d'analyse de signaux sismiques pour « voir » les *plumes volcaniques*, ces cheminées au travers du manteau terrestre qui sont à l'origine des chapelets d'îles comme Hawaii.

3. <https://www.adobe.com/ca/creativecloud/file-types/image/comparison/jpeg-vs-jpeg-2000.html>

4. <https://minnovaa.com/jpeg-2000/>

Supposons que des candidat.e.s en nombre fini et connu se présentent à une entrevue d'emploi dans un ordre aléatoire et qu'après chaque entretien, la direction puisse offrir le poste à la personne interviewée ou rejeter sa candidature mais que la décision, une fois prise, soit irrévocable. Quelle stratégie adopter pour maximiser les chances de recruter la meilleure candidature ?

La règle des 37 %

Christian Genest
Université McGill

Ce problème d'optimisation aux origines obscures est attesté dans la littérature scientifique depuis le milieu des années 1950. Formulé tantôt comme la quête d'un.e secrétaire, d'une propriété, d'un.e partenaire de vie, voire d'une dot, il doit sa popularité à la forme étonnante de sa solution, qui fait intervenir le nombre d'Euler, $e = 2,71828\dots$

Comme nous le verrons, la stratégie optimale consiste à laisser passer un certain nombre de candidatures et à sélectionner ensuite, si possible, la première personne qui se révèle meilleure que toutes celles qui l'ont précédée. Fait remarquable, il se trouve qu'à mesure que croît le nombre de candidatures, la proportion d'entre elles à rejeter d'emblée tend vers $1/e \approx 37\%$. Qui plus est, la probabilité que la meilleure personne soit retenue s'approche de $1/e$ et la probabilité que nul ne soit embauché tend aussi vers $1/e$. Nous évoquerons ensuite certaines variantes du problème.

Formulation précise

Supposons que le nombre $n \geq 2$ de candidatures au poste soit connu à l'avance. Dénотons ces candidatures C_1, \dots, C_n dans leur ordre d'arrivée et supposons qu'il soit possible de les classer sans ambiguïté. Ainsi, après avoir interviewé l'individu C_n , la personne chargée du recrutement possède un classement relatif de C_1, \dots, C_n et peut choisir ou non d'offrir le poste à C_n en fonction de cette information. On dénote C_s la candidature retenue à la fin de ce processus, s'il en est.

Si l'on savait à l'avance que les candidatures se présenteraient dans l'ordre, de la meilleure à la pire, on embaucherait évidemment la première personne interviewée. De même, si les candidatures étaient classées dans l'ordre

contraire, on offrirait alors le poste à la toute dernière personne rencontrée. On poserait ainsi $S = 1$ dans le premier cas et $S = n$ dans le second.

Pour que le problème ait un intérêt, supposons plutôt que les entrevues se déroulent dans un ordre aléatoire, de sorte que la probabilité que la candidature C_i soit la meilleure, dénoté $C_i = C_M$ soit $1/n$. Exprimé en ces termes, le problème consiste à identifier une règle de décision qui maximise la probabilité que C_s , la candidature sélectionnée, s'il en est, soit effectivement C_M .

Exemple dans le cas $n = 3$

Supposons que trois candidatures soient numérotées 1, 2, 3, de la pire à la meilleure. Il y a alors six ordres d'arrivée possibles. L'un d'eux serait $(C_1, C_2, C_3) = (1, 2, 3)$, les cinq autres étant $(1, 3, 2)$, $(2, 1, 3)$, $(2, 3, 1)$, $(3, 1, 2)$ et $(3, 2, 1)$. On les suppose équiprobables.

Si par exemple on choisit d'offrir le poste au premier venu, on embauchera la meilleure personne si et seulement si les candidat.e.s sont interviewé.e.s dans l'ordre $(3, 1, 2)$ ou $(3, 2, 1)$. La probabilité de succès associée à cette stratégie est donc $2/6 = 1/3$.

On peut toutefois faire mieux en rejetant d'emblée la première candidature et en offrant le poste à la deuxième personne si elle est jugée meilleure que la première. Sinon, on fait l'offre à la troisième personne, pourvu qu'elle se classe mieux que les deux précédentes.

Selon cette stratégie, la meilleure candidature sera retenue dans les trois cas suivants : $(1, 3, 2)$, $(2, 1, 3)$ et $(2, 3, 1)$. La probabilité de succès est donc $3/6 = 1/2 > 1/3$. Aussi cette stratégie est-elle préférable à la première, quoiqu'elle ait le désavantage de ne pas toujours mener

à une embauche. En effet, personne ne sera retenu si les entrevues ont lieu dans l'ordre (3, 1, 2) ou (3, 2, 1), tandis que dans le cas (1, 2, 3), on sélectionnera la seconde candidature, qui n'est pas la meilleure.

Forme de la règle optimale

Fixons $i \in \{1, \dots, n\}$ et supposons que les candidat.e.s C_1, \dots, C_i aient été interviewé.e.s. Pour maximiser ses chances de recruter la meilleure candidature, la direction ne devrait offrir le poste à la personne C_i que si les deux conditions suivantes sont réunies :

- a) La candidature doit être éligible, c'est-à-dire s'avérer la meilleure parmi C_1, \dots, C_i .
- b) La probabilité que $C_i = C_M$ doit être plus grande que pour n'importe quelle stratégie qui pourrait être employée une fois que la candidature C_i aura été rejetée, soit

$$\Pr(E_i) > \Pr(F_i), \quad (1)$$

où E_i est l'événement que $C_i = C_M$ sachant que C_i est éligible, tandis que F_i est l'événement « recruter C_M avec la meilleure stratégie fondée sur C_{i+1}, \dots, C_n ». Or, le terme de gauche de l'inégalité (1) est strictement croissant en i , puisque $\Pr(E_i) = i/n$. En effet, la probabilité que C_i soit éligible n'est autre que la probabilité que la meilleure des i premières candidatures soit la dernière, soit $1/i$. Par ailleurs, la probabilité que la candidature i soit la meilleure de toutes est $1/n$. Remarquez que si $C_i = C_M$, alors C_i est la meilleure et est donc automatiquement éligible. Par la définition de probabilité conditionnelle, on a donc

$$\Pr(E_i) = (1/n) / (1/i) = i/n.$$

En revanche, le terme de droite de l'inégalité (1) est strictement décroissant en i , puisque si $i < j$, toute stratégie qui s'appuie sur C_{j+1}, \dots, C_n fait partie des stratégies fondées sur C_{i+1}, \dots, C_n .

Par conséquent, la meilleure stratégie est forcément de la forme suivante :

- a) Rejeter les $r-1$ premières candidatures, pour un certain $r \in \{1, \dots, n\}$.
- b) Choisir la première candidature $i \geq r$ qui s'avère éligible, c'est-à-dire qui se classe mieux que toutes les précédentes.

La figure 1 illustre cette règle pour deux valeurs de r , soient 3 et 6, lorsque le nombre de candidatures est $n=10$. Dans la figure, la taille de chaque personne reflète sa valeur et le x indique la meilleure d'entre elles. La zone bleue correspond à la phase d'exploration et la zone jaune à celle pendant laquelle la direction s'autorise à faire une offre ou pas. La zone verte regroupe les candidatures non rencontrées. Enfin, l'individu encerclé est celui qui est choisi au terme du processus. Dans le volet inférieur, on sélectionne la meilleure personne du lot ; dans le volet supérieur, ce n'est pas le cas.

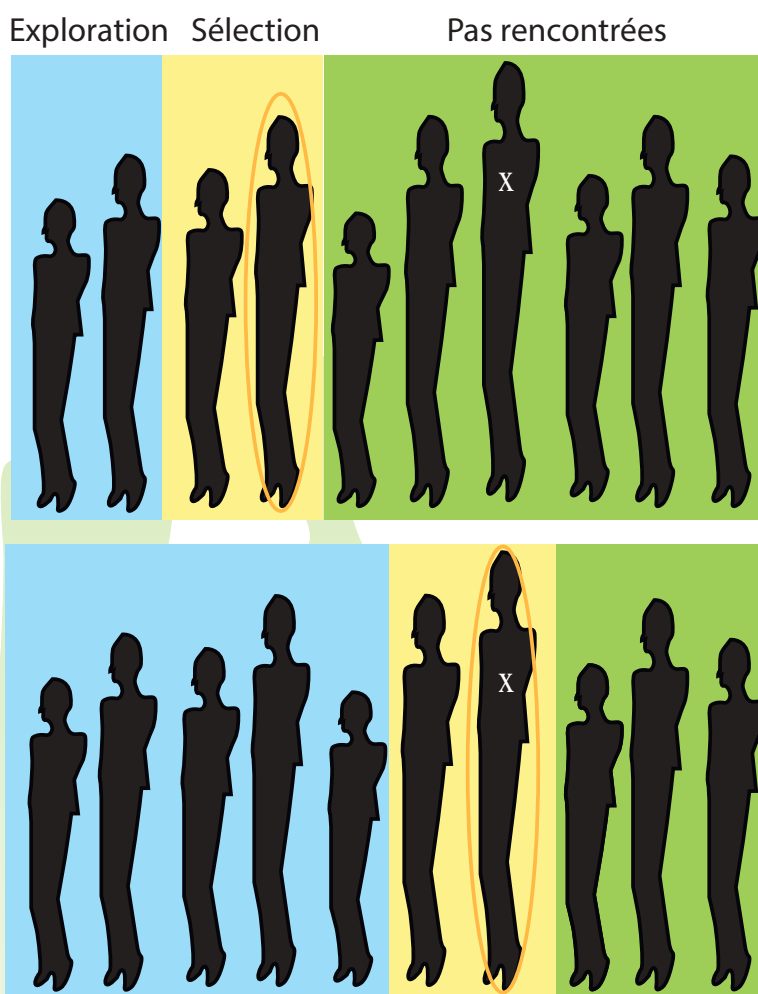


Figure 1.

Illustration de la stratégie d'embauche selon que l'on rejette d'emblée les $r = 2$ premières ou les $r = 5$ premières candidatures d'un lot de $n = 10$, la personne la plus grande étant la meilleure.

Détermination de la valeur de r

Étant donné $r \in \{1, \dots, n\}$, dénotons par $P_n(r)$ la probabilité que la stratégie ci-dessus conduise à choisir la meilleure candidature dans l'ensemble $\{C_1, \dots, C_n\}$. Quand $r = 1$, la stratégie se réduit à sélectionner la première personne interviewée, puisque l'ensemble $\{C_1, \dots, C_{r-1}\}$ est vide. On a alors $S = 1$ et la probabilité que $C_S = C_M$ est $1/n$. On a donc $P_n(1) = 1/n$.

Si $r \geq 2$, la probabilité $P_n(r)$ peut être calculée en distinguant $n - r + 1$ cas distincts, selon que pour $i \in \{r, \dots, n\}$, la candidature C_i est à la fois éligible et la meilleure de toutes. On peut donc écrire

$$P_n(r) = \sum_{i=r}^n \Pr(C_i = C_S \text{ et } C_i = C_M).$$

Par la formule de probabilité conditionnelle, on a

$$\begin{aligned} \Pr(C_i = C_S \text{ et } C_i = C_M) \\ = \Pr(C_i = C_S \mid C_i = C_M) \times \Pr(C_i = C_M) \end{aligned}$$

et $\Pr(C_i = C_M) = 1/n$ du fait que l'ordre dans lequel les candidatures sont examinées est aléatoire.

Par ailleurs, si $C_i = C_M$, c'est-à-dire si C_i est la meilleure candidature, elle ne pourra être sélectionnée que si la meilleure des $i - 1$ candidatures qui la précèdent se trouve parmi les $r - 1$ candidatures qui ont été rejetées d'emblée. Si tel n'était pas le cas, on se serait arrêté avant !

Sachant que l'ordre dans lequel les candidatures sont étudiées est aléatoire, cet événement se produit avec probabilité $(r - 1)/(i - 1)$. Ainsi, pour tout $r \in \{2, \dots, n\}$, la probabilité recherchée est

$$\begin{aligned} P_n(r) &= \sum_{i=r}^n \frac{r-1}{i-1} \times \frac{1}{n} \quad (2) \\ &= \frac{r-1}{n} \left(\frac{1}{r-1} + \frac{1}{r} + \dots + \frac{1}{n-1} \right). \end{aligned}$$

Remarquons que pour tout $n \geq 2$, on a

$$\begin{aligned} P_n(2) &= \frac{1}{n} \left(\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{n-1} \right) \\ &> \frac{1}{n} = P_n(1), \end{aligned}$$

tel que déjà illustré plus haut dans le cas $n = 3$. Comme on l'a aussi observé dans cet exemple, le rejet automatique d'un certain nombre de candidatures entraîne un risque de ne retenir personne à l'issue du processus d'embauche. La probabilité que cela se produise est la même que celle que la meilleure candidature figure parmi les $r - 1$ candidatures rejetées, soit $Q_n(r) = (r - 1)/n$. Notons en outre que $P_n(n) = 1/n$, comme il se doit.

Calcul de r et $Q_n(r)$ pour n donné

Étant donné une valeur de $n \geq 2$, on peut aisément calculer la valeur de $P_n(r)$ pour tout choix de $r \in \{2, \dots, n\}$. Si $n = 5$, par exemple, on pose successivement $r = 2, 3, 4, 5$ dans la formule (2) et on trouve

$$P_5(2) = \frac{1}{5} \left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \right) \approx 0,417,$$

$$P_5(3) = \frac{2}{5} \left(\frac{1}{2} + \frac{1}{3} + \frac{1}{4} \right) \approx 0,433,$$

$$P_5(4) = \frac{3}{5} \left(\frac{1}{3} + \frac{1}{4} \right) \approx 0,35,$$

$$P_5(5) = \frac{4}{5} \left(\frac{1}{4} \right) \approx 0,20.$$

Par conséquent, la probabilité $P_5(r)$ est maximisée lorsque $r = 3$, ce que l'on dénote $r_5 = 3$. De plus, la probabilité de ne sélectionner personne est alors égale à $Q_5(r_5) = 2/5 = 0,4$.

De façon générale, on peut démontrer que pour une valeur de n donnée, la fonction $r \mapsto P_n(r)$ est « unimodale ». On entend par là que cette fonction est d'abord croissante en r , qu'elle atteint éventuellement un sommet en une valeur r_n , après quoi elle se met à décroître. Une illustration de cette remarque se trouve à la figure 2, qui correspond au cas $n = 10$.

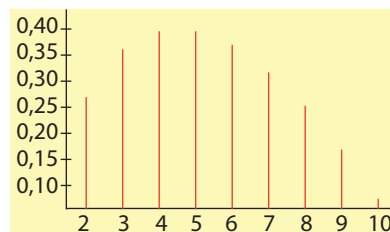


Figure 2.

Graphique des valeurs de $P_n(r)$ lorsque $n = 10$ et que r varie entre 2 et 10. La fonction $r \mapsto P_{10}(r)$ est unimodale et son maximum se trouve en $r = 4$, soit $P_{10}(4) \approx 0,39869$, valeur légèrement supérieure à $P_{10}(5) \approx 0,39825$.

Le tableau 1 donne, pour chaque valeur de $n \in \{2, \dots, 5, 10, 20, 30, 40, 50, 100\}$, la valeur de $r \in \{2, \dots, n\}$, dénotée r_n qui maximise $P_n(r)$. La valeur de $P_n(r_n)$ y est également précisée, de même que la probabilité $Q_n(r_n)$ de ne sélectionner personne en adoptant cette stratégie.

En consultant le tableau 1, on observe que la probabilité $P_n(r_n)$ est monotone décroissante en n , ce qui reflète le fait que même avec une stratégie optimale, il devient de plus en plus ardu d'identifier la meilleure personne à mesure que le nombre de candidatures augmente.

n	r_n	$P_n(r_n)$	$Q_n(r_n)$
2	2	0,5	0,5
3	2	0,5	0,33
4	2	0,458	0,25
5	3	0,433	0,4
10	4	0,399	0,3
20	8	0,384	0,35
30	12	0,379	0,367
40	16	0,376	0,375
50	19	0,374	0,36
100	38	0,371	0,37

Tableau 1. Valeur r_n de r permettant de maximiser $P_n(r)$ et valeurs de $P_n(r_n)$ et $Q_n(r_n)$ correspondantes pour $n \in \{2, 3, 4, 5, 10, 20, 30, 40, 50, 100\}$.

Limite de r_n et $P_n(r_n)$ quand $n \rightarrow \infty$

Il est instructif de déterminer comment le rapport r_n/n varie au fur et à mesure que n augmente. Les données du tableau 1 suggèrent que ce rapport tend à décroître, bien que pas de façon monotone. Soit t la limite de r_n/n quand $n \rightarrow \infty$. Puisqu'alors on a $1/n \rightarrow 0$, il s'ensuit que

$$Q_n(r_n) = (r_n - 1)/n = r_n/n - 1/n \rightarrow t.$$

Par ailleurs, on peut montrer que si $n \rightarrow \infty$, on a

$$P_n(r_n) \rightarrow P(t) = -t \ln(t). \tag{3}$$

Se référer à l'encadré pour une démonstration de ce fait.

Or, t est par définition la proportion qui maximise $P(t)$. En prenant la dérivée de $P(t)$ par rapport à t , on trouve que $P'(t) = -\ln(t) - 1$ et $P'(t) = 0$ si et seulement si $t = 1/e$. Puisqu'en

outre $P''(t) = -1/t < 0$ pour tout $t \in]0, 1[$, on conclut qu'asymptotiquement, c'est-à-dire lorsque $n \rightarrow \infty$, la proportion optimale de candidatures à rejeter d'office est de $1/e \approx 37\%$, tel qu'annoncé. Ce faisant, la probabilité $Q_n(r_n)$ de ne recruter personne est aussi égale à $1/e$. Et puisque $P(1/e) = 1/e$, l'emploi de cette règle donne à son utilisateur une probabilité $1/e \approx 37\%$ d'identifier la meilleure candidature.

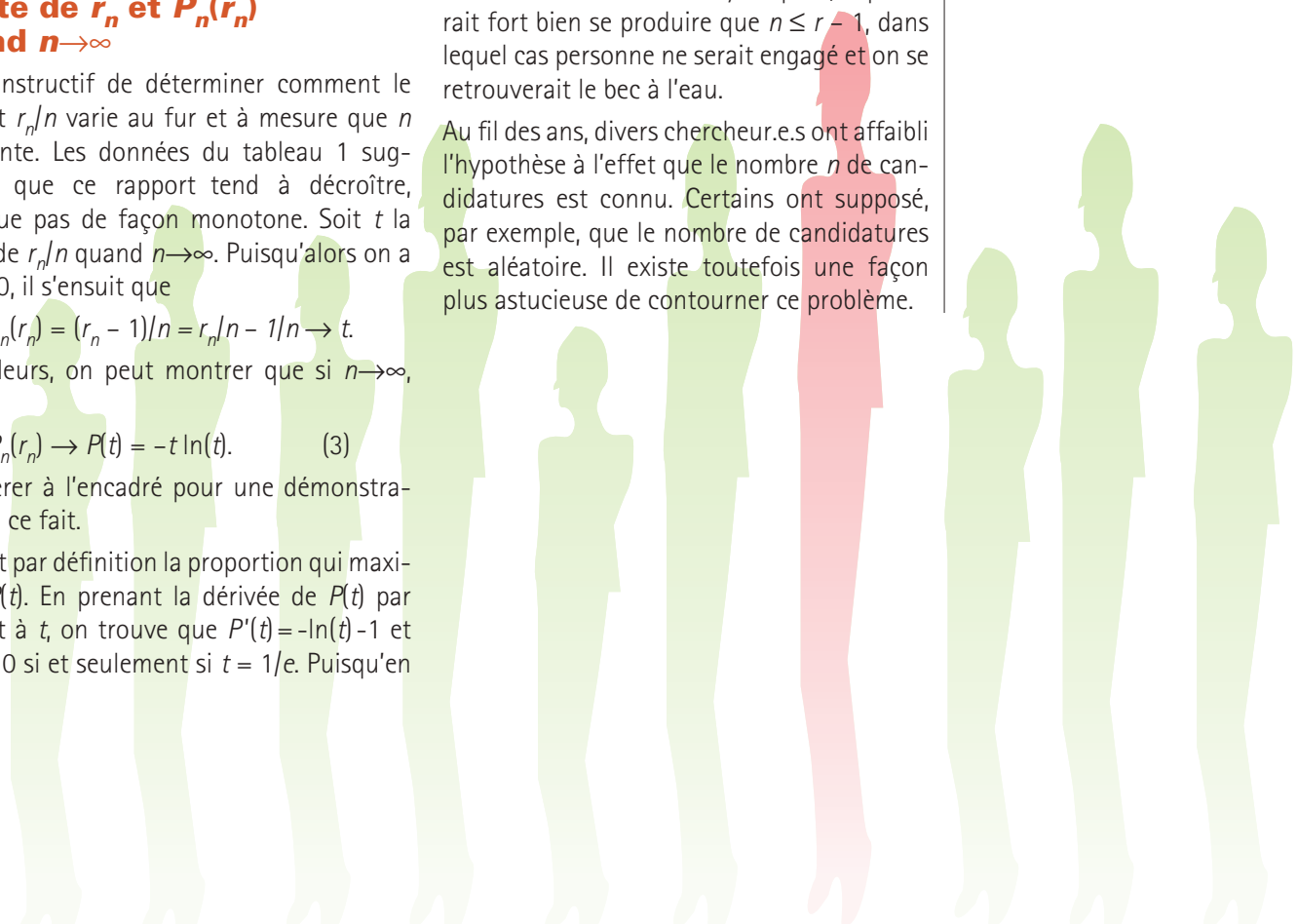
La fraction $1/e$ est donc tout à la fois la proportion optimale de candidatures à rejeter d'office, la probabilité d'identifier la meilleure candidature et la probabilité de n'embaucher personne, ce qui est remarquable !

Limitations

Bien que séduisante, la solution du problème précédent n'a de sens que si les candidat.e.s au poste ne sont pas informé.e.s de la stratégie qui sera employée pour opérer la sélection. Autrement, personne ne se bousculerait au portillon pour passer l'entrevue tôt !

Par ailleurs, il est crucial que le nombre total de candidatures, n , soit connu à l'avance. Sinon, il est impossible de fixer d'entrée de jeu le nombre $r - 1$ de dossiers qui seront écartés d'emblée. Si on s'y risquait, il pourrait fort bien se produire que $n \leq r - 1$, dans lequel cas personne ne serait engagé et on se retrouverait le bec à l'eau.

Au fil des ans, divers chercheur.e.s ont affaibli l'hypothèse à l'effet que le nombre n de candidatures est connu. Certains ont supposé, par exemple, que le nombre de candidatures est aléatoire. Il existe toutefois une façon plus astucieuse de contourner ce problème.



Une approche différente

Au début des années 1980, le mathématicien allemand Thomas Bruss a proposé une formulation ingénieuse du problème du choix de la meilleure candidature dans laquelle on ne fixe pas le nombre de candidatures à examiner, mais plutôt la période de temps pendant laquelle on cherche à combler le poste. Cette approche a aussi le mérite d'être plus proche de la pratique.

Soit $[0, T]$ l'intervalle de temps prédéterminé à l'intérieur duquel on cherche à combler le poste. Formulons en outre les hypothèses suivantes quant au processus d'arrivée des candidatures :

- Un nombre aléatoire N de candidatures est observé dans l'intervalle $[0, T]$.
- Sachant $N = n$, les temps d'arrivée des n candidatures sont mutuellement indépendants et tous de même loi de probabilité représentée par une densité continue f concentrée sur l'intervalle $[0, T]$.
- Les $n!$ classements possibles des candidatures, au plan de leur aptitude à l'emploi, sont équiprobables.

Démonstration de l'énoncé (3)

Pour démontrer l'énoncé (3), on exploite le fait que pour tout entier m suffisamment grand, la somme $1 + 1/2 + \dots + 1/m$ est à peu près égale à $\ln(m) + e$. Ainsi, pour de grandes valeurs de r et m , on a

$$\sum_{i=r}^n \frac{1}{i} = \sum_{i=1}^n \frac{1}{i} - \sum_{i=1}^{r-1} \frac{1}{i} \approx \ln\left(\frac{n}{r-1}\right).$$

On peut alors déduire de la formule (2) que quand $n \rightarrow \infty$,

$$\begin{aligned} P_n(r_n) &= \frac{r_n - 1}{n} \times \sum_{i=r_n-1}^{n-1} \frac{1}{i} \\ &\approx \frac{r_n - 1}{n} \times \ln\left(\frac{n-1}{r_n-2}\right). \end{aligned}$$

Comme -1 et -2 deviennent négligeables lorsque n est grand, on peut écrire

$$P_n(r_n) \approx \frac{r_n}{n} \times \ln\left(\frac{n}{r_n}\right).$$

Puisque $r_n/n \rightarrow t$ quand $n \rightarrow \infty$, il s'ensuit que

$$P_n(r_n) \rightarrow P(t) = -t \ln(t).$$

La figure 3 montre une densité de probabilité continue f dont toute la masse est concentrée sur l'intervalle $[0, 1]$. L'aire sous la courbe est égale à l'unité. La partie en bleu correspond au quantile d'ordre $1/e \approx 37\%$ de cette loi. Dans cet exemple précis, le quantile d'ordre 37% est d'environ 0,63.

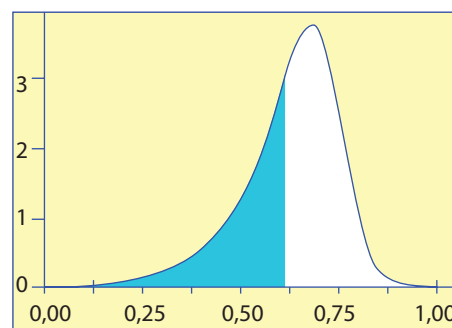


Figure 3. Une densité de probabilité sur l'intervalle $[0, 1]$ dont le nombre 0,628 est le 37^e centile. L'aire tracée en bleu, à gauche de 0,628, représente 37% de l'aire sous la courbe.

En général, soit τ le quantile d'ordre $1/e$ de la loi continue f , c'est-à-dire le plus petit nombre $\tau \in [0, T]$ à la gauche duquel se situe une proportion de $1/e$ de la masse de probabilité :

$$\int_0^{\tau} f(x) dx = 1/e.$$

Considérons la stratégie consistant à rejeter d'emblée toutes les candidatures reçues dans l'intervalle $[0, \tau]$ et à offrir ensuite le poste à la première personne éligible, c'est-à-dire qui se classe mieux que toutes celles qui la précèdent (en supposant qu'une telle personne se présente). Dans ces conditions, Bruss est parvenu à démontrer les faits suivants :

- La probabilité de recruter ainsi la meilleure candidature qui se présente dans l'intervalle $[0, T]$ est supérieure ou égale à $1/e$, peu importe f et la loi du nombre N de candidatures.
- La probabilité que cette stratégie ne permette d'embaucher personne est aussi de $1/e$.

Ce résultat, publié en 1984 dans les prestigieuses *Annals of Probability*, a généré beaucoup d'émoi dans la communauté mathématique, du fait que $1/e$ constitue ici une borne inférieure !

Et quoi encore ?

Il existe de nombreuses autres variantes du problème. Citons notamment :

- La possibilité d'exploiter non pas seulement un classement relatif mais plutôt la valeur intrinsèque des candidatures, telle que le prix demandé dans la recherche d'une propriété.
- La possibilité de revenir en arrière et d'offrir le poste à une personne déjà interviewée.
- La possibilité que certaines personnes refusent une offre.

On pourrait aussi imaginer qu'il y ait plus d'un poste à combler, ou inversement que l'on puisse sélectionner plus d'une personne pour un seul poste et que l'on considère l'opération comme réussie dès lors que la meilleure candidature figure dans le lot.

Une autre option consisterait à chercher dès le départ à recruter, non pas la meilleure personne possible, mais plutôt la seconde meilleure. Cet objectif pourrait être motivé, entre autres, par la crainte que la meilleure candidature reçoive plusieurs offres et préfère aller ailleurs.

Dans ce dernier cas, on peut montrer que la meilleure stratégie consiste à rejeter la première moitié des candidatures et à offrir le poste à la première personne qui se qualifie ensuite comme meilleure deuxième. La probabilité de succès associée à cette stratégie est d'environ $\frac{1}{4}$. Curieusement, il appert qu'il est plus facile de choisir la meilleure candidature que la seconde en lice !

Conclusion

S'il faut tirer une leçon de toutes ces considérations, c'est sans doute qu'en amour ou en affaires, il est généralement sage de voir venir et de prendre le temps d'explorer un peu le marché avant de s'engager... Gare, donc, aux décisions hâtives !

Choix d'une épouse

Dans un article de synthèse sur la règle des 37% paru en 1989 dans la revue *Statistical Science*, le mathématicien américain Tom Ferguson relate comment le célèbre astronome allemand Johannes Kepler (1571-1630) s'y est pris pour choisir sa seconde épouse, après que la première ait été emportée par le choléra en 1611.

Dans un processus élaboré qu'il a décrit dans une lettre adressée au Baron Strahlendorf en octobre 1613, Kepler raconte avoir considéré pas moins de 11 candidates. Après avoir pris en compte toutes sortes de variables (qualités et défauts de ces dames, existence ou taille de la dot, négociations avec les parents, conseils des amis, etc.), Kepler a finalement opté pour la cinquième.

On peut remarquer facétieusement que $r_{11} = 5$. Cependant, Kepler ne s'en est pas tenu exactement aux règles du problème tel qu'énoncé ici. En particulier, bien qu'il ait été fortement attiré par la candidate n° 5 après l'avoir rencontrée, il a ensuite fait une proposition de mariage à la candidate n° 4 sur l'avis de ses amis. Cette offre ne s'est toutefois pas concrétisée.

Pour de plus amples détails, consulter l'article de Ferguson ou la biographie de Kepler réalisée par Arthur Koestler parue en 1960 chez Anchor Books (Garden City, NY).

Dédicace

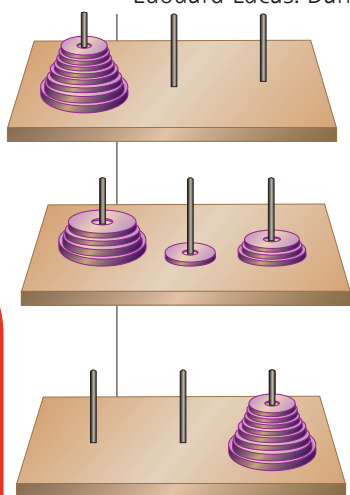
Je souhaite dédicacer cet article à Thomas Bruss et Tom Ferguson, que j'ai côtoyés au quotidien en 1997-98 à la faveur d'une année d'étude et de recherche à l'Université libre de Bruxelles. Ils m'ont beaucoup appris et je les considère comme des amis. Cet article s'inspire énormément de leurs travaux.

On ne peut pas résoudre tous les puzzles !

Place au coloriage et aux invariants.

Que ce soit pour les résoudre ou pour montrer qu'on ne peut le faire, les puzzles permettent de mettre en action des idées fondamentales en mathématiques.

Frédéric Gourdeau
Université Laval



Un bel exemple est donné par le jeu des tours de Hanoï dont l'invention est attribuée à Édouard Lucas. Dans la version illustrée ici, il faut déplacer la tour de départ (image du haut), formée de huit disques empilés sur la tige de gauche, pour la placer sur la tige de droite (image du bas), en respectant les consignes suivantes :

- on ne peut déplacer plus d'un disque à la fois, d'une tige à une autre ;
- on ne peut placer

un disque que sur un autre disque plus grand que lui ou sur un emplacement vide.

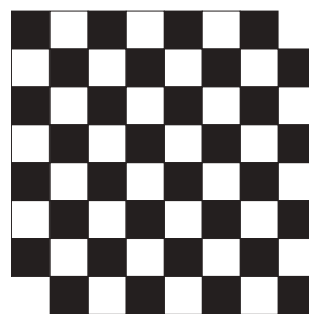
Il y a plusieurs questions à saveur mathématique que l'on peut se poser, une fois que l'on a résolu le puzzle. Combien de déplacements doit-on faire, au minimum, pour y arriver? S'il y avait eu une tour formée par sept disques, combien de déplacements cela prendrait-il? Lorsque le jeu est dans la position illustrée dans l'image du milieu, combien de coups reste-t-il à faire? Répondre à ces questions nous permet de mieux comprendre le jeu, et sa complexité, une fois qu'on l'a résolu. L'article de Benoît Rittaud sur les tours de Hanoï¹ l'illustre fort bien.

Dans d'autres cas, l'utilisation des mathématiques peut permettre de comprendre pourquoi il est impossible de résoudre un puzzle.

Cela peut sembler surprenant. Pourquoi considérer un puzzle qu'on ne peut résoudre? Et comment être certain que la résolution est bel et bien impossible?

Un puzzle simple et une idée fondamentale

Prenons un échiquier de 64 cases auquel on enlève les deux cases situées aux extrémités de l'une des deux diagonales. Il reste alors 62 cases. On vous donne 31 dominos rectangulaires qui couvrent chacun exactement deux cases. Le but du puzzle est de placer les 31 dominos de manière à couvrir exactement ces 62 cases. Vous pouvez essayer : vous verrez que c'est impossible. Mais sauriez-vous expliquer pourquoi cela est impossible?



1. Accromath vol. 11.1, Hiver-Printemps 2016

On peut remarquer que l'échiquier illustré a 32 cases noires et 30 cases blanches : comme chaque domino couvre exactement une case de chaque couleur, il restera toujours 2 cases noires une fois placés les 30 premiers dominos, et on ne peut donc pas le recouvrir entièrement. Cet énoncé coloré se prête moins bien à une généralisation que le suivant.

Attribuons les valeurs -1 et 1 en alternance aux cases de l'échiquier, en débutant avec 1 dans une des cases d'un coin, et en poursuivant de sorte que deux cases voisines horizontalement ou verticalement aient une valeur différente. Alors chaque domino couvre exactement deux cases dont la somme des valeurs est 0 . Avec 31 dominos, on couvrirait donc 62 cases dont la somme des valeurs est aussi 0 . Mais la somme des valeurs des 62 cases est en fait 2 , et on ne peut donc pas couvrir les 62 cases.

Voyons le tout comme un jeu

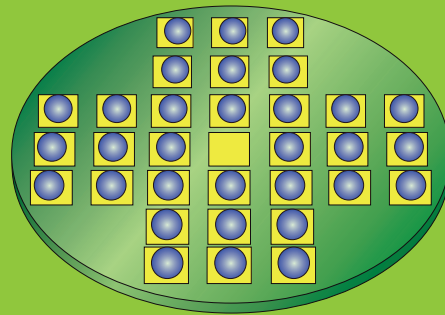
Décrivons le tout comme un jeu. On a une position initiale du jeu, soit les 62 cases non recouvertes, et un coup consiste à placer un domino rectangulaire.

- En attribuant des valeurs aux cases, on peut attribuer une valeur initiale au jeu en sommant la valeur des 62 cases non recouvertes: cela donne une valeur de 2 .
- Après chacun des coups, la valeur du jeu formé par les cases non recouvertes est aussi calculée : cette valeur demeure 2 , peu importe de coup joué.

Jouer un coup ne change donc pas la valeur du jeu, qui ne peut donc jamais devenir nulle. On ne peut donc pas recouvrir toutes les cases du jeu.



Le solitaire



Dans le jeu classique du solitaire, des billes sont placées sur un plateau comme celui illustré, et la position centrale est vide. Une bille peut « sauter » par-dessus une bille horizontalement ou verticalement pour atteindre une position vide, et la bille par-dessus laquelle on a fait le saut est retirée.

Dans le jeu illustré ici, le premier coup est donc unique, à une rotation près du plateau.

L'objectif est de retirer toutes les billes sauf une, et que cette bille soit alors au centre du plateau.

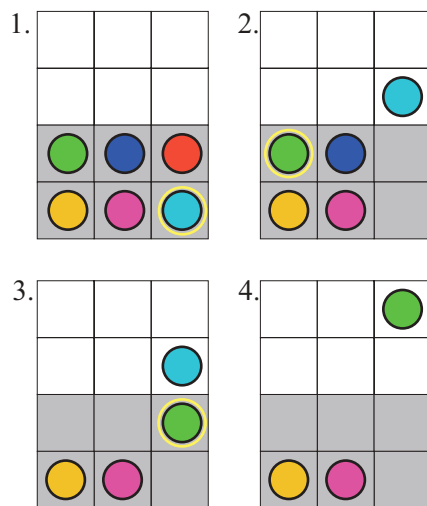
Dans ce jeu, il y a bel et bien une solution! On ne révèle rien pour vous laisser le plaisir de résoudre le puzzle vous-même.

La clé

Pour qu'une telle idée fonctionne, on doit trouver une manière d'attribuer une valeur aux différents états d'un jeu de telle sorte que les coups joués ne puissent pas permettre de passer de la valeur du jeu dans sa position initiale à la valeur du jeu dans la position finale souhaitée.

Une variante du solitaire : les soldats de Conway

Le jeu du solitaire est très connu (voir encadré). Dans la variante que nous présentons, on imagine un échiquier de taille infinie séparé en deux par un trait horizontal. Des jetons sont disposés sur la moitié inférieure (cases en gris) et les mouvements sont les mêmes que ceux du jeu de solitaire : un jeton peut sauter par-dessus un jeton qui lui est adjacent horizontalement ou verticalement (mais pas en diagonale) pour atteindre une position vide, et le jeton par-dessus lequel on a sauté est retiré. Voici un exemple sur une partie de l'échiquier qui permet de placer un jeton à la 2^e rangée de la moitié du haut en 3 mouvements. (Le jeton cerclé en jaune est celui qui effectue le prochain saut.)



Jusqu'où peut-on monter?

Ici, le jeu consiste à amener des jetons aussi haut que possible. Peut-on aller à la 3^e rangée? Et à la 4^e, et ainsi de suite? Comme il y a une infinité de jetons, on serait porté à croire que l'on peut atteindre n'importe quelle rangée. Après avoir fait quelques essais, on atteint la 3^e rangée, puis la 4^e rangée en persévérant. Mais aller au-delà de la 4^e rangée peut sembler impossible. Doit-on persévérer?

Lorsque l'on regarde des problèmes de ce genre, on peut être porté à vouloir regarder tous les détails : on veut expliquer pourquoi certains coups sont « clairement » mieux que d'autres, et donc que si on n'y arrive pas, c'est que c'est impossible! Et cela devient vite très compliqué à suivre, et encore plus à vraiment bien justifier.

La clé, encore une fois!

On va montrer qu'on ne peut pas atteindre la 5^e rangée. Pour ce faire, on attribue une valeur (appelée un poids) à chacune des cases de l'échiquier, et la valeur du jeu est la somme des valeurs des cases occupées par un jeton. Comme on voudra avoir la valeur du jeu dans sa position initiale, et qu'il y a une infinité de jetons, il faut bien choisir les poids. L'idée est de prendre un nombre réel a tel que $0 < a < 1$ et d'attribuer des poids selon la méthode suivante.

On choisit une case de la 5^e rangée auquel on donne la valeur 1. Elle est en jaune sur la figure. On va montrer que cette case ne peut pas être atteinte.

On attribue la valeur a à la position immédiatement en dessous, puis la valeur a^2 , et ainsi de suite sur la colonne contenant la position choisie. On augmente donc l'exposant de 1 à chaque fois que l'on s'éloigne de la position choisie, vers le bas.

Pour les cases qui ne sont pas dans la colonne centrale, on augmente l'exposant de 1 à chaque fois que l'on s'éloigne de la colonne centrale. Le résultat apparaît dans la grille, que l'on imagine infinie.

a^3	a^2	a	1	a	a^2	a^3
a^4	a^3	a^2	a	a^2	a^3	a^4
a^5	a^4	a^3	a^2	a^3	a^4	a^5
a^6	a^5	a^4	a^3	a^4	a^5	a^6
a^7	a^6	a^5	a^4	a^5	a^6	a^7
a^8	a^7	a^6	a^5	a^6	a^7	a^8
a^9	a^8	a^7	a^6	a^7	a^8	a^9
a^{10}	a^9	a^8	a^7	a^8	a^9	a^{10}

La valeur de la position initiale du jeu, qui est la somme des valeurs des cases occupées au début, est $\frac{a^5 + a^6}{(1-a)^2}$ (voir encadré).

Bien choisir la valeur de a

Peut-on choisir la valeur de a pour que les coups ne modifient pas la valeur du jeu? On voit que les coups vers le haut ainsi que ceux vers l'axe central (qui contient la case de valeur 1) consistent tous à ce qu'un jeton dans une position de valeur a^{n+2} saute par-dessus un jeton dans une case de valeur a^{n+1} pour atteindre la position de valeur a^n . On voudrait donc que $a^{n+2} + a^{n+1} = a^n$ pour toute valeur positive de n , ce qui sera vrai si $a^2 + a = 1$. Prenons donc comme valeur de a la racine positive du polynôme $p(x) = x^2 + x - 1 = 0$ (On peut vérifier que $a = \frac{-1 + \sqrt{5}}{2}$, qui est bien entre 0 et 1.)

Et les autres coups possibles?

Les autres coups possibles consistent à descendre ou à s'éloigner de l'axe central, ou encore à sauter par-dessus un jeton de l'axe central. On a alors un jeton dans une case de valeur a^n qui saute par-dessus un jeton dans une case de valeur a^{n+1} pour atteindre une case de valeur a^{n+2} ou une case de valeur a^n . Dans les deux cas, on diminue la valeur du jeu puisque $a^n + a^{n+1} > a^{n+2}$ et $a^n + a^{n+1} > a^n$.

La valeur initiale du jeu est 1, et celle de la position finale souhaitée est > 1 .

Avec cette valeur de a , on a $a^2 = 1 - a$ et la valeur initiale du jeu est donc

$$\frac{a^5 + a^6}{(1-a)^2} = \frac{a^4(a+a^2)}{a^4} = a + a^2 = 1.$$

S'il y a un jeton à la case de poids 1, dans la 5^e rangée, alors la valeur du jeu sera strictement supérieure à 1 car il y aura aussi d'autres jetons dont le poids n'est pas nul. Comme aucun coup ne permet d'augmenter la valeur du jeu, on ne peut pas en arriver à cela.

LES SOMMATIONS

si $0 < a < 1$, alors $(1 + a + a^2 + \dots) = 1/(1 - a)$.

On peut voir d'où vient cette égalité en considérant tout d'abord la somme d'un nombre fini de puissances, soit $(1 + a + a^2 + \dots + a^n)$. En remarquant que

$(1 - a)(1 + a + a^2 + \dots + a^n) = 1 - a^{n+1}$, on peut diviser par $(1 - a)$ des deux côtés de l'équation pour obtenir

$$(1 + a + a^2 + \dots + a^n) = \frac{1 - a^{n+1}}{1 - a}.$$

On remarque alors que plus n est grand, plus a^{n+1} est près de 0, de telle sorte qu'à la limite, on aura bien

$$1 + a + a^2 + \dots = \frac{1}{1 - a}.$$

Une fois que l'on a cela, que donne la somme de tout ce qu'il y a dans le tableau?

Si on somme les valeurs des cases grises dans la colonne centrale, on a

$$\begin{aligned} a^5 + a^6 + a^7 + \dots &= a^5(1 + a + a^2 + \dots) \\ &= \frac{a^5}{1 - a}. \end{aligned}$$

Puis, pour les cases grises des deux colonnes voisines, on obtient deux fois le terme $a^6/(1 - a)$. Et ainsi de suite, de sorte qu'on obtient finalement

$$\begin{aligned} &\frac{a^5 + 2a^6 + 2a^7 + \dots}{1 - a} \\ &= \frac{a^5 + a^6 + a^7 + \dots}{1 - a} + \frac{a^6 + a^7 + a^8 + \dots}{1 - a} \\ &= \frac{a^5 + a^6}{(1 - a)^2}. \end{aligned}$$

Invariant et monovariant

John Conway a lui-même résolu de cette manière la variante du jeu du solitaire qui porte son nom. Il a de fait introduit une valeur qui n'est pas invariante mais qui ne peut pas croître avec les coups joués. On parlera alors de monovariant, ici décroissant.

L'utilisation d'invariant ou de monovariant est fréquente en mathématiques. Elle peut permettre de montrer que des objets mathématiques appartiennent à des classes différentes, ou que des configurations ne peuvent être atteintes en utilisant certains processus précis, comme dans le cas que nous venons de résoudre.

De la science-fiction à l'informatique : les mathématiques pour expliquer les qubits

Le début des années 1900 marque une remarquable révolution scientifique : la naissance de la mécanique quantique. C'est dans ces années que les scientifiques soulèvent plusieurs questions : comment se fait-il que l'électron de l'atome d'hydrogène ne s'écrase pas sur le noyau ? Comment expliquer la variation d'émission en électrons d'une surface métallique éclairée par de la lumière ? Et bien plus encore...

Tania Belabbas

AlgoLab quantique
Université de Sherbrooke



Peter Shor
1959-

Face à l'apparition de phénomènes étranges et non intuitifs à l'échelle atomique et subatomique, des figures emblématiques comme Einstein, Bohr ou Dirac se lancent dans une quête fascinante : construire une théorie capable de rendre compte de ces bizarreries. Peu à peu, des concepts étonnants émergent – la dualité onde-corpuscule, le principe d'incertitude fondamentale, ou encore la superposition d'états – et redéfinissent en profondeur notre compréhension du monde. Dans l'interprétation la plus répandue aujourd'hui, l'interprétation de Copenhague de la mécanique quantique, on propose une vision probabiliste de la réalité, où une particule peut exister dans plusieurs états à la fois... tant qu'on ne la mesure pas. Cette révolution a, au fil du temps, inspiré bien plus que la physique : elle a ouvert la voie à une nouvelle façon de traiter l'information.

Dès les années 1980, physiciens, mathématiciens et informaticiens commencent à croiser leurs idées. Paul Bénéioff imagine une version quantique de la machine de Turing, et Richard Feynman propose d'utiliser des systèmes quantiques pour simuler la physique – une tâche ardue pour les ordinateurs classiques. De là est née l'idée de l'ordinateur quantique : une machine exploitant les lois de la mécanique quantique pour réaliser des calculs autrement impossibles à cause du temps que prennent les machines classiques à les exécuter.

Un tel ordinateur pourrait, en principe, faire tout ce qu'une machine classique peut faire... mais pour certains problèmes bien définis, il irait beaucoup, beaucoup plus vite. Par exemple, un algorithme quantique célèbre, celui de Shor, permettrait de factoriser de très grands nombres bien plus rapidement qu'un ordinateur classique – ce qui pourrait briser les systèmes de cryptographie utilisés aujourd'hui. Un autre, l'algorithme de Grover, permettrait d'accélérer considérablement la recherche d'un élément dans une base de données non triée. Alors qu'un ordinateur classique doit tester chaque possibilité une à une, un ordinateur quantique peut tester une combinaison de possibilités à la fois. Ce potentiel gain en performance, appelé avantage quantique, propulse alors l'informatique quantique sous les projecteurs. Et ce n'est qu'un début ! Non seulement une telle machine s'avère être un défi d'ingénierie colossal, mais en plus, la logique utilisée pour développer un algorithme quantique est aussi très différente.



Cela ouvre ainsi la porte à plusieurs branches de recherche sous le chapeau de l'information quantique.

Bits classiques VS Bits quantiques

Les ordinateurs classiques stockent l'information sous forme de bits, qui peuvent prendre la valeur 0 ou 1. En combinant plusieurs de ces bits en une chaîne, il est possible d'encoder de l'information et de réaliser des manipulations et des calculs pour obtenir le résultat à un problème donné. Un qubit (bit quantique) est, de façon analogue, l'unité de base de l'information quantique.

Contrairement à un bit, un qubit peut être dans une *superposition* de 0 et de 1 en même temps. L'état d'un qubit est décrit avec une combinaison linéaire de deux états de base, conventionnellement l'état $|0\rangle$ et l'état $|1\rangle$. Remarquez l'utilisation des symboles $| \rangle$. Cette écriture se nomme la *notation de Dirac* et le symbole $| \rangle$ est appelé un ket. La notation indique la manipulation d'états quantiques. Plus précisément, en notation matricielle, ces états sont des vecteurs colonnes. Pour les états de base à un qubit, on écrit

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ et } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

L'état général $|\psi\rangle$ d'un qubit en superposition se dénote $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. On parle ainsi d'un qubit qui est à la fois dans l'état $|0\rangle$ et dans l'état $|1\rangle$. Les coefficients α et β sont des *amplitudes de probabilité* et décrivent la probabilité de trouver un système quantique dans un état spécifique. Ce fait est reflété par la relation

$$|\alpha|^2 + |\beta|^2 = 1 \quad (*)$$

La section sur la mesure développera cette idée plus en profondeur. Mais voici le hic : α et β ne sont pas des nombres ordinaires - ce sont des *nombres complexes*, ce qui signifie qu'ils ont à la fois une amplitude r , et une phase θ , comme des vecteurs dans un plan (voir Figure 1).

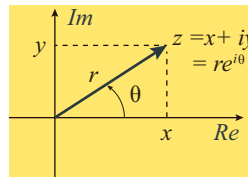


Figure 1

Représentation d'un nombre complexe $z=re^{i\theta}$, illustrant la construction d'une amplitude de probabilité (comme α ou β) avec une amplitude r et une phase θ dans le plan complexe.

Les coefficients α et β sont donc représentés par des vecteurs dans le plan complexe, ce qui nous permet d'obtenir une structure géométrique du qubit. La nécessité que ces coefficients soient complexes vient des postulats de la mécanique quantique et du fait que les particules se comportent comme des ondes (interférence).

Écrivons $\alpha = se^{i\gamma}$ et $\beta = re^{i\delta}$. Alors,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = e^{i\gamma}(s|0\rangle + re^{i(\delta-\gamma)}|1\rangle),$$

où s et r sont des nombres réels positifs et par la relation (*), on a $s^2+r^2=1$. Les nombres r et s représentent respectivement les amplitudes des états $|0\rangle$ et $|1\rangle$ du qubit $|\psi\rangle$. En posant $\delta-\gamma=\phi$, le facteur $e^{i\phi}$ correspond à une rotation de phase appliquée à la composante $|1\rangle$ du qubit. En revanche, le facteur $e^{i\gamma}$ correspond à une rotation globale de phase qui, elle, n'a pas d'effet observable. Elle ne change pas les probabilités d'observer le qubit dans un état ou l'autre, et peut donc être ignorée dans la plupart des cas. Pour cette raison on se contente de décrire l'ensemble des qubits pour lesquels $\gamma=0$, et donc $e^{i\gamma}=1$. Cet ensemble est décrit par la sphère de Bloch.

Sphère de Bloch

La sphère de Bloch est un moyen utile pour visualiser un qubit $|\psi\rangle$. Il s'agit d'une sphère unitaire où chaque point de la surface représente un état possible du qubit.

Puisque $r, s \geq 0$ et $s^2+r^2=1$, on peut écrire $s = \cos(\theta/2)$ et $r = \sin(\theta/2)$ où $\theta \in [0, \pi]$. Un état général

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle.$$

est représenté par le point de coordonnées sphériques (θ, ϕ) sur la sphère (voir Figure 2).



Paul Adrien Maurice Dirac
1902-1984



Felix Bloch
1905-1983

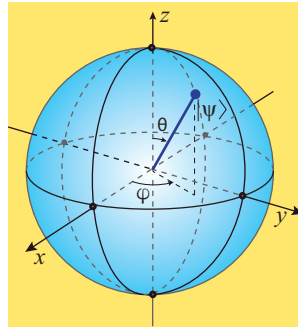


Figure 2

Représentation sur la sphère de Bloch d'un état général $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi} \sin(\theta/2)|1\rangle$.

Un qubit dans l'état $|0\rangle$ se retrouvera donc représenté sur la sphère de Bloch par une flèche en direction du pôle nord. (Voir Figure 3).

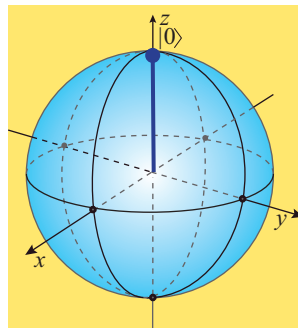


Figure 3

Représentation sur la sphère de Bloch de l'état $|\psi\rangle = |0\rangle$.

alors que l'état $|1\rangle$, sera orienté vers le pôle sud (voir Figure 4).

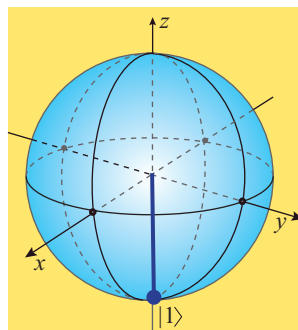


Figure 4

Représentation sur la sphère de Bloch de l'état $|\psi\rangle = |1\rangle$.

La visualisation d'états de qubits avec la sphère de Bloch se limitent aux états à un qubit. On ne peut représenter graphiquement les états à deux qubits et plus. En effet, nous verrons plus tard que ceux-ci peuvent être intriqués, résultant en un grand nombre de dimensions nécessaires pour les visualiser.

Superposition

La superposition, cette capacité du qubit d'exister simultanément dans plusieurs états, est fondamentale à l'informatique quantique. Imaginez avoir plus d'un qubit, une chaîne de N qubits. Chacun d'entre eux peut être en superposition des états $|0\rangle$ et $|1\rangle$. L'état décrivant cette chaîne de qubits s'exprime par un vecteur de dimension 2^N . Par exemple, pour 2 qubits, on aura

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

avec la relation $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. Des manipulations sur une chaîne de qubits en superposition peuvent donc être équivalentes à manipuler toutes ces combinaisons à la fois!



<https://tenor.com/en-CA/view/mind-blown-shocked-astounded-explosion-gif-4927161>

C'est cette capacité qui est exploitée dans l'algorithme de Shor, capable de factoriser rapidement de très grands nombres entiers – une tâche réputée difficile pour les ordinateurs classiques. Or, la sécurité du chiffrement RSA (utilisé dans la cryptographie moderne) repose justement sur la difficulté de cette factorisation. Un ordinateur quantique du futur, utilisant la superposition (et l'intrication) peut exécuter l'algorithme de Shor pour trouver les facteurs premiers d'un grand entier en un temps exponentiellement plus court qu'un ordinateur classique. Ainsi, la superposition n'est pas seulement une curiosité théorique – elle constitue une ressource computationnelle puissante.

Mesure

Revenons à l'état quantique en superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Tant qu'un qubit n'est pas mesuré, ou observé, il existe dans cette superposition d'états – cette combinaison de 0 et 1 en même temps, avec certaines probabilités associées. Ces probabilités sont dictées par les coefficients α et β .

Dès qu'on effectue une mesure – qu'on observe ou regarde le qubit, celui-ci s'effondre instantanément dans l'un de ces deux états de base, $|0\rangle$ ou $|1\rangle$, selon les probabilités associées à α et β . Plus précisément, la probabilité de mesurer le qubit dans l'état 0 sera égale à $|\alpha|^2$ et la probabilité de le mesurer dans l'état 1 sera de $|\beta|^2$. Bien sûr, il est requis que les probabilités somment à 1 (100%) de telle sorte que, comme mentionné précédemment, $|\alpha|^2 + |\beta|^2 = 1$. La mesure est donc cruciale : c'est le pont entre le monde quantique et le monde classique. C'est grâce à elle qu'on peut lire le résultat d'un calcul quantique.

En revanche, les postulats de la mécanique quantique nous mettent en garde : on ne peut pas simplement observer un état sans le modifier. C'est pourquoi on parle d'effondrement de l'état quantique. Les algorithmes quantiques consistent donc à exploiter les phénomènes quantiques de façon à maximiser les chances d'obtenir la bonne réponse au moment où on observe les résultats.

Intrication

Un autre phénomène fondamental des sciences quantiques est l'intrication. Étant donné deux qubits, il est possible de les intriquer de telle façon que l'état de l'un est corrélé avec l'état de l'autre qubit. La distance qui les sépare, une fois intriqués, n'a aucun impact sur la corrélation des deux qubits, celle-ci est instantanée. Cela rend possible une dépendance entre qubits qui n'est pas locale. Ce phénomène n'a pas d'équivalent en informatique classique.

Lors du développement d'un algorithme quantique, l'intrication est très importante pour la manipulation de systèmes à plusieurs qubits. La superposition, l'intrication et les phénomènes quantiques peuvent être

Fait intéressant

L'intrication n'est pas une histoire de science-fiction. En effet, une des plus impressionnantes expériences d'intrication a été accomplie par le laboratoire de recherche de l'Université des Sciences et des Technologie de Beijing qui a réussi à obtenir des particules intriquées entre une station terrestre et un satellite à 1200 kilomètres de distance!

exploités pour débloquent le *parallélisme quantique*, cette capacité d'un ordinateur quantique à explorer de nombreuses solutions d'un problème en une seule opération. Cela ouvre la voie à l'avantage quantique et à l'atteinte d'un seuil où l'ordinateur quantique peut résoudre un problème qu'aucun ordinateur classique ne peut résoudre dans un délai raisonnable.

Conclusion

L'informatique quantique, encore en pleine évolution, représente un paradigme de programmation fondamentalement différent. En s'appuyant sur des phénomènes quantiques comme la superposition, l'intrication et la mesure, elle redéfinit notre manière de penser le calcul. Un ordinateur quantique est non pas une version plus rapide de l'ordinateur classique, mais bien un outil radicalement différent, capable de traiter certains problèmes d'une manière que la technologie classique ne peut pas imiter. Si les défis techniques sont encore nombreux, les progrès constants laissent entrevoir un futur où la puissance du quantique pourrait transformer des domaines entiers, de la science des matériaux à la cryptographie.

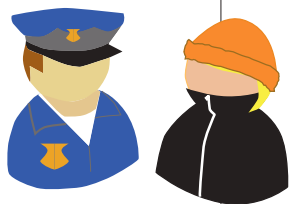
Imaginez un interrogatoire de police un peu particulier. Deux suspects, Alice et Bob, sont amenés dans des salles distinctes du poste de police et questionnés séparément par des inspecteurs. Le crime qu'on leur reproche est la « pratique de la magie ». Il paraît que les deux complices sont capables de télépathie. Rien de moins.

Jeu de couleurs, jeu de quantas

Claude Crépeau

École de technologie supérieure (ETS)

Institut national de recherche en sciences et technologies du numérique (INRIA)



Les inspecteurs ont donc pour mission de démontrer qu'Alice et Bob sont en mesure d'accomplir une tâche que seule la communication pourrait leur permettre de réaliser, bien qu'on les ait maintenus séparés à tout moment. Alice et Bob sont bons joueurs; ils acceptent le défi de démontrer leur talent, mais sont convaincus qu'aucun juge (suffisamment instruit) n'acceptera de les condamner... Alice et Bob ont un tour de magie où ils arrivent à gagner systématiquement à un jeu simple qu'on appelle le jeu RVB. Ce jeu consiste à donner une couleur A parmi « rouge », « vert » ou « bleu » à Alice et une telle couleur B à Bob indépendamment¹. Face à la couleur A , Alice doit répondre immédiatement une couleur A' telle que $A' \neq A$ et Bob une couleur B' telle que $B' \neq B$. Jusque là rien de bien difficile. Néanmoins, pour gagner le jeu, Alice et Bob doivent en plus répondre de façon à ce que $A' \neq B'$ sans pouvoir se consulter...

Pensez à cette situation un peu. Comment Alice et Bob peuvent-ils avoir $A' \neq B' \neq B$ tout le temps? Je parie que d'ici quelques minutes vous aurez trouvé une façon pour Alice et Bob de gagner 8 fois sur 9 à ce jeu. Je parie aussi que vous n'arriverez pas à faire mieux. Pour ne pas gâcher votre plaisir d'essayer par vous-même, n'allez pas lire tout de suite l'encadré *Le jeu des couleurs*, où je vous donne une telle stratégie conjointe pour Alice et Bob. Mais à quoi Alice et Bob ont-ils droit s'ils ne peuvent pas se parler?

On dit qu'une stratégie conjointe est *locale déterministe* si Alice et Bob peuvent se mettre d'accord avant le début du jeu sur deux fonctions F_A et F_B telles que $A' = F_A(A)$ et $B' = F_B(B)$.

1. La paire (A, B) est choisie au hasard uniformément parmi les 9 paires possibles.

Il est assez facile de trouver deux fonctions telles que 8 des 9 couples de couleurs (A, B) satisfont $A \neq F_A(A) \neq F_B(B) \neq B$. De plus, il est assez facile de se convaincre qu'aucune paire de fonctions ne peut réussir cet exploit plus de 8 fois sur 9. On dit alors que la *valeur classique* du jeu RVB est de $8/9$. Pour être le plus inclusif possible et afin de considérer des stratégies pour Alice et Bob qui pourraient faire intervenir du hasard, en plus de leurs paires de fonctions, on leur donne la possibilité d'avoir partagé au moment de se séparer de nombreux résultats de tirages à pile ou face, autant que bon leur semble. Les stratégies résultant de cet ensemble de ressources sont tout simplement dites *locales*.



Le jeu des couleurs

Considérez les fonctions :

$$F_A(\text{bleu}) = F_A(\text{vert}) = \text{rouge},$$

$$F_B(\text{bleu}) = F_B(\text{rouge}) = \text{vert},$$

$$\text{et } F_A(\text{rouge}) = F_B(\text{vert}) = \text{bleu}.$$

Vous pouvez vérifier que $F_A(A) \neq A$, $F_B(B) \neq B$ tout le temps et que $F_A(A) \neq F_B(B)$ sauf pour le cas $A=\text{rouge}$ et $B=\text{vert}$. On aura donc

$$A \neq F_A(A) \neq F_B(B) \neq B,$$

sauf dans ce dernier cas (marqué du X dans la table ci-bas).

A est sur la première colonne et $F_A(A)$ sur les triangles inférieurs et B sur la première rangée et $F_B(B)$ sur les triangles supérieurs.

Avec un peu plus de travail, on arrive à se convaincre qu'aucune stratégie locale ne peut gagner au jeu RVB plus de 8 fois sur 9. Point à la ligne. L'introduction du hasard permet à Alice et Bob de transformer une

stratégie déterministe qui gagne pour 8 des 9 paires de couleurs, en une stratégie qui gagne 8 fois sur 9 pour chaque paire (A, B) , mais sans plus. Faut-il alors conclure que si Alice et Bob réussissent à gagner tout le temps au jeu RVB c'est la preuve qu'ils communiquent?

Eh bien non. Supposons qu'au lieu de se limiter aux ressources locales décrites ci-haut², on permet à Alice et Bob de s'équiper de mémoires quantiques dans lesquelles ils ont préalablement partagé des états quantiques intriqués de leur choix et qu'on leur permet d'apporter avec eux leur mémoire quantique pour l'interrogatoire. Il s'avère que dans un tel contexte Alice et Bob (voir l'encadré : *Utiliser une mémoire quantique pour jouer au jeu RVB*) seront capables de faire des mesures³ Π_R , Π_V et Π_B sur leur mémoire quantique dont les résultats vont leur permettre de gagner au jeu RVB avec probabilité 11/12. C'est-à-dire 1/36 de mieux qu'avec n'importe quelle stratégie locale. Ce qui se cache derrière cette affirmation est ce que les physiciens appellent le « *théorème de Bell* » publié par John Stewart Bell en 1964 [Be64] où celui-ci démontra que la physique quantique, si elle est juste, implique qu'il est possible de corrélérer des variables de façon quantique plus *fortement* que de façon classique.

Ce n'est qu'à partir des années 70-80 que des expériences un tant soit peu concluantes sur le sujet ont permis d'établir la supériorité de la physique quantique en cette matière. Le prix Nobel de physique de 2022 aux chercheurs Alain Aspect, John Clauser, et Anton Zeilinger a été attribué pour la réalisation expérimentale de démonstrations établissant que Bell avait bel et bien raison. Personne n'a démontré en laboratoire que l'on peut gagner au jeu RVB plus de 8 fois sur 9 en moyenne, mais ce n'est qu'une question de temps. Avec un ordinateur quantique général, une telle démonstration sera un jeu d'enfant.

2. Ces ressources sont F_A , F_B et un nombre arbitraire de résultats de tirages à pile ou face.
3. Le projecteur Π_X sert à mesurer quand Alice ou Bob reçoit la couleur X comme donnée.



John Stewart Bell



Alain Aspect



John Clauser



Anton Zeilinger



Avec des mémoires et des appareils de mesure quantiques, il s'avère donc qu'Alice et Bob peuvent gagner 11 fois sur 12 au jeu RVB (voir les deux prochains encadrés), mais il s'avère également qu'on ne peut pas faire mieux. (Ne cherchez pas une preuve simple de cette impossibilité; la seule preuve connue est assez compliquée [CRC19]). On dit dans ce cas que la *valeur quantique* du jeu RVB

est de 11/12. Alors, reposons donc la question: « Faut-il conclure que si Alice et Bob réussissent à gagner tout le temps au jeu RVB c'est la preuve qu'ils communiquent ? »

Toute cette histoire se rend finalement devant le juge. Heureusement pour Alice et Bob, celui-ci est plutôt féru de physique. Les policiers présentent le cadre où ils ont réalisé l'interrogatoire et le constat qu'Alice et

Utiliser une mémoire quantique pour jouer au jeu RVB

Alice et Bob commencent par se munir d'un état intriqué $|\psi^-\rangle$ qui est une juxtaposition de deux qubits, et que l'on peut visualiser comme un vecteur dans l'espace à quatre dimensions complexes⁴:

$$|\psi^-\rangle = (R, S) = \frac{1}{\sqrt{2}} |01\rangle - \frac{1}{\sqrt{2}} |10\rangle.$$

Nos deux complices se partagent $|\psi^-\rangle$: Alice obtient le premier qubit, R , et Bob, le second, S . Notons que R correspond au 0 de $|01\rangle$ et au 1 de $|10\rangle$, alors que S correspond au 1 de $|01\rangle$ et au 0 de $|10\rangle$. Alice et Bob emmagasinent chacun leur qubit dans leur unité de mémoire quantique portable respective en attendant de le mesurer ultérieurement. Remarquons aussi que le choix de $|\psi^-\rangle$ n'est pas arbitraire ici car il est le seul état quantique ayant les bonnes propriétés mathématiques permettant d'obtenir le résultat escompté.

Les qubits R et S sont conjointement dans un état superposé. Mais, surtout, ils se trouvent corrélés par l'intrication de $|\psi^-\rangle$. Ceci signifie qu'ils ne se comportent pas de manière indépendante et que tout ce qui se passe sur l'un se répercute sur la description de l'autre: c'est le fameux phénomène d'intrication identifié par Einstein, Podolsky et Rosen dès 1935 [EPR35].

Alice et Bob vont chacun vouloir regarder leur qubit dans une base. Mais, la base choisie va dépendre de la couleur de A pour R , et de la couleur de B pour S . Pour la couleur « rouge » on choisit la base $\{|0\rangle, |1\rangle\}$, pour la couleur « vert », la base

$\{|v^-\rangle, |w^-\rangle\}$, et pour la couleur « bleu », la base $\{|v^+\rangle, |w^+\rangle\}$, où

$$|v^+\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle,$$

$$|v^-\rangle = \frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle,$$

$$|w^+\rangle = \frac{1}{2}|1\rangle + \frac{\sqrt{3}}{2}|0\rangle,$$

$$\text{et } |w^-\rangle = \frac{1}{2}|1\rangle - \frac{\sqrt{3}}{2}|0\rangle.$$

Alice va mesurer R et Bob S selon l'un des trois projecteurs suivants

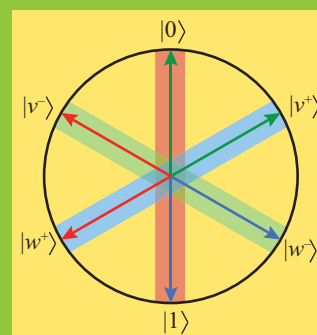
$$\Pi_R = |0\rangle\langle 0| \text{ vs } |1\rangle\langle 1|$$

$$\Pi_V = |v^-\rangle\langle v^-| \text{ vs } |v^+\rangle\langle v^+|$$

$$\Pi_B = |w^+\rangle\langle w^+| \text{ vs } |w^-\rangle\langle w^-|.$$

La mesure va donner l'un des vecteurs de la base.

Les trois projecteurs sont organisés dans le plan tels qu'illustré dans la figure ci-bas. Le projecteur Π_R est sur fond rouge, et ses deux valeurs possibles de sortie sont pour « vert » et pour « bleu ». On interprète les deux autres projecteurs de la même façon: le projecteur Π_V est sur fond vert et le projecteur Π_B est sur fond bleu.



4. Pour la notion de qubits et la notation, vous pouvez vous référer à l'article « La Mécanique quantique: quand les mots échouent, les maths parlent », Accromath 20.2

Bob ont gagné tout le temps, quand questionnés séparément et indépendamment. Les policiers ont bien pris soin de brouiller les ondes durant les interrogatoires pour être sûrs qu'Alice et Bob ne communiquent pas entre eux. Néanmoins, le juge n'est pas convaincu hors de tout doute raisonnable. Il connaît bien les possibilités dues à la physique quantique et le fait que gagner plus

de 8/9 du temps n'est pas une preuve. Il sait que de gagner plus de 11/12 du temps n'est pas une preuve non plus. Pour constituer une preuve, il faudrait que « la seule façon possible de gagner au jeu RVB tout le temps soit grâce à la communication ». Une façon de prouver cela serait de démontrer que toute stratégie permettant de réaliser cet exploit permettrait aussi à Alice et Bob de communiquer entre eux.

Gagner 11 fois sur 12

Les mesures Π_R , Π_V et Π_B donnent clairement toujours des résultats tels que $A' \neq A$ et $B' \neq B$, car la couleur X n'est jamais un résultat possible du projecteur Π_X . Quand on mesure un même projecteur (demande « laquelle de ces deux valeurs es-tu ? ») sur les qubits V et W de $|\psi^-\rangle$, les réponses opposées seront toujours produites: c'est la magie unique à cet état. Donc, quand $A = B$, on aura que $\Pr[A' \neq B' | A = B] = 1$ (3 des 9 cas). Quand au contraire $A \neq B$, on aura que $\Pr[A' \neq B' | A \neq B] = 7/8$ (6 des 9 cas). Voyons les détails.

Afin de bien comprendre la suite, vous pouvez vérifier que

$$\begin{aligned} |\psi^-\rangle &= \frac{1}{\sqrt{2}} |01\rangle - \frac{1}{\sqrt{2}} |10\rangle \\ &= \frac{1}{\sqrt{2}} |v^- w^-\rangle - \frac{1}{\sqrt{2}} |w^- v^-\rangle \\ &= \frac{1}{\sqrt{2}} |v^+ w^+\rangle - \frac{1}{\sqrt{2}} |w^+ v^+\rangle. \end{aligned}$$

Prenons par exemple les cas $A = \text{« rouge »}$ et $B = \text{« vert »}$:

- Si Alice mesure son qubit R selon l'opérateur Π_R et (avec probabilité 1/2) obtient $|0\rangle$ ($A' = \text{« vert »}$), alors le qubit de Bob se comportera comme $|1\rangle$. Lorsque Bob mesurera son qubit S avec Π_V , il obtiendra $B' \neq B = A'$ dans les deux cas possibles.
- Si au contraire Alice mesure son qubit R selon l'opérateur Π_R et (avec probabilité 1/2) obtient $|1\rangle$ ($A' = \text{« bleu »}$), alors le qubit S de Bob se comportera comme $|0\rangle$. On travaille avec les demi-angles car les vecteurs orthogonaux sont à 180° l'un de l'autre dans cette figure. Comme les options $|0\rangle$ et $|v^-\rangle$ forment un angle

de 60° entre eux, quand $|0\rangle$ sera observé selon Π_V , il se comportera comme $|v^-\rangle$ (soit $B' = \text{« vert »} \neq A'$), avec probabilité $3/4 = \cos^2 30^\circ$. Sinon, il se comportera comme $|w^-\rangle$ (soit $B' = \text{« bleu »} = A'$).

- Donc, dans cet exemple, la probabilité que $B' \neq A'$ vaut $1/2 \times (1 + 3/4)$.

Dans l'exemple précédent, c'est Alice qui a mesuré son qubit en premier. Supposons que ce soit plutôt Bob qui fasse la première mesure et voyons qu'on obtient la même probabilité. Comme $B = \text{« vert »}$, Bob doit obligatoirement utiliser l'opérateur Π_V et, en mesurant son qubit S , il obtiendra nécessairement une des deux réponses $|v^-\rangle$ ou $|w^-\rangle$ avec probabilité 1/2 pour chacune.

- S'il obtient $|v^-\rangle$ ($B' = \text{« rouge »}$), alors le qubit R d'Alice se comportera comme $|w^-\rangle$. Lorsque Alice le mesurera avec Π_R , elle obtiendra $A' \neq A = B'$ dans les deux cas possibles.
- Si au contraire Bob obtient $|w^-\rangle$ ($B' = \text{« bleu »}$), alors le qubit V d'Alice se comportera comme $|v^-\rangle$. Comme les options $|0\rangle$ et $|v^-\rangle$ forment un angle de 60° entre eux, quand $|v^-\rangle$ sera observé selon Π_R , il se comportera comme $|0\rangle$ (soit $A' = \text{« vert »} \neq B'$), avec probabilité $3/4 = \cos^2 30^\circ$. Sinon, il se comportera comme $|1\rangle$ (soit $A' = \text{« bleu »} = B'$).

Les cinq autres cas sont identiques. La probabilité que $B' \neq A'$ pour l'ensemble de ces six cas vaut :

$$6/9 \times 1/2 \times (1 + 3/4).$$

Ce qui donne bel et bien

$$3/9 \times 1 + 6/9 \times 7/8 = 11/12.$$

Pour en avoir le coeur net, le juge propose aux policiers de réaliser un interrogatoire un peu plus sophistiqué, inspiré de la physique relativiste. Alice et Bob seront séparés dans deux postes de police situés à plusieurs kilomètres l'un de l'autre. Les enquêteurs auront synchronisé leurs montres de façon très précise. Les paires de questions seront posées exactement en même temps à Alice et Bob. L'un comme l'autre devra répondre immédiatement à la question qui lui est posée, et ceci assez rapidement pour qu'il soit physiquement impossible, à des vitesses de communication inférieures ou égales à celle de la lumière, de connaître les deux questions avant de répondre.

L'expérience que je viens de décrire ressemble assez à celle qu'Alain Aspect a réalisée en 1981 [AGR81]. Si l'on croit que, selon la relativité restreinte, il est impossible de communiquer plus rapidement qu'à la vitesse de la lumière, nous sommes forcés de croire qu'Alice et Bob ne peuvent communiquer avant de répondre à leur question respective. Des expériences similaires ont été réalisées en laboratoire depuis à plusieurs reprises.

Un grand interrogatoire public est donc mis sur pied et Alice et Bob réussissent haut la main à gagner à tous les coups, même dans ces conditions extrêmes. Le juge est ravi de pouvoir démontrer sa subtile connaissance de la logique élémentaire et affirme qu'il est prêt à rendre son verdict. « Non coupables », s'exclame-t-il. Dans la version longue de son jugement, on peut ensuite lire: « Bien que je ne comprenne pas comment Alice et Bob ont fait pour gagner tout le temps au jeu RVB, le simple fait de gagner au jeu ne constitue pas en soit un acte de communication. » En effet, le jeu RVB est un exemple de ce que l'on

appelle un *jeu non signalant*. C'est-à-dire où l'on peut identifier une corrélation permettant de gagner au jeu, mais ne permettant pas de communiquer. On dit alors que la *valeur non signalante* (voir l'encadré: *Ici on ne signale pas*) du jeu RVB est de 1.

Le mystère plane. La magie opère. L'exploit d'Alice et Bob n'a jamais été réalisé en pratique pour la simple et bonne raison que notre modèle actuel de la physique ne connaît rien de plus puissant que les corrélations quantiques (mis à part la communication). Les corrélations non signalantes supra-quantiques existent sur papier, mais pas en laboratoire. Nous n'avons strictement aucune idée, comment en réalité on pourrait corréler des systèmes physiques de façon supérieure aux quantiques. Néanmoins, l'existence de telles corrélations ne serait pas en contradiction avec la relativité restreinte. On peut voir cette situation comme un vide entre ce que peut accomplir la physique quantique et ce que ne permet pas la relativité restreinte. Toute démonstration de l'existence d'une corrélation non signalante supra-quantique impliquerait que la physique quantique est incomplète et tout résultat d'impossibilité de telles corrélations impliquerait que l'énoncé selon lequel « aucune communication ne peut se produire plus vite que la vitesse de la lumière » doit être remplacé par un énoncé plus général qu'« aucune corrélation supra-quantique ne peut se propager plus vite que la vitesse de la lumière ». Dans un cas comme dans l'autre, ce serait une immense percée pour la physique telle que nous la connaissons. Peut-être qu'Alice et Bob connaissent déjà la réponse à cette énigme, mais pour le moment ils refusent de nous la communiquer...

Ici on ne signale pas

Soit A, B des valeurs d'entrées et A', B' des valeurs de sortie. Soit C une corrélation établissant les probabilités de chaque paire en sortie (A', B') étant donné (A, B) en entrée. On écrit $(A', B') = C(A, B)$.

En termes simples, C est non signalante si le fait de changer la valeur de B ne change pas la distribution marginale de $A'|A$ et pareillement pour A et $B'|B$.

En termes mathématiques, C est *non signalante* si pour tout a, a', b, b', u, v on a que

$$\Pr[A' = a' | A = a, B = u] = \Pr[A' = a' | A = a, B = v] \quad (*)$$

et

$$\Pr[B' = b' | B = b, A = u] = \Pr[B' = b' | B = b, A = v] \quad (**)$$

Il n'existe en théorie qu'une seule stratégie gagnante pour Alice et Bob et qui soit non-signalante. Décrivons-la dans les deux cas $A = B$ et $A \neq B$.

Le cas $A = B$. Dans ce cas, Alice et Bob répondent le couple (A', B') tiré conjointement à pile ou face, dans l'une ou l'autre des deux seules combinaisons gagnantes utilisant les deux couleurs différentes de A (et B). Voici deux exemples :

$A = B$	A	A'	B'	B
	A	A'	B'	B

Dans le cas contraire, $A \neq B$, il y a trois combinaisons gagnantes (A', B'), dont la combinaison (A', B') = (B, A). Pour que la stratégie soit non-signalante Alice et Bob ne doivent jamais utiliser cette réponse.

Les deux autres réponses possibles sont celles où, soit Alice, soit Bob, répond la couleur de l'autre, et l'autre répond la troisième couleur. Encore une fois, la réponse est le couple (A', B') tiré conjointement à pile ou face, dans l'une ou l'autre des deux combinaisons gagnantes utilisant la troisième couleur. Voici deux exemples :

$A \neq B$	A	A'	B'	B
	A	A'	B'	B

Trois choses sont à discuter :

1. Cette stratégie est non-signalante.
2. Cette stratégie est la seule possible.
3. Cette stratégie est-elle réalisable en pratique sans communiquer?

Discutons ces questions :

1. Cette stratégie est non-signalante. Dans cette stratégie, quel que soit le couple (A, B), il y a toujours exactement deux réponses possibles (A'_1, B'_1) et (A'_2, B'_2), telles que $A'_1 \neq A'_2$ et $B'_1 \neq B'_2$. Donc, toutes les probabilités conditionnelles apparaissant en (*) et (**) valent 1/2, ce qui garantit que la stratégie satisfait à (*) et (**).
2. Cette stratégie gagnante est la seule possible qui soit non-signalante. En effet, quand $A = B$, il y a deux réponses gagnantes possibles, et quand $A \neq B$ il y en a trois. Lorsqu'on change la valeur de B dans (*) on peut passer du cas $A = B$ au cas $A \neq B$ ou le contraire. La seule manière que les probabilités restent égales pour toutes les valeurs de B est qu'il n'y ait que deux réponses possibles pour chaque couple (A, B). On peut aussi se convaincre que toutes les probabilités doivent être égales à 1/2 pour pouvoir satisfaire à (*) et (**).
3. Cette stratégie est-elle réalisable en pratique sans communiquer? Pour le moment on ne connaît pas de façon physique pour Alice et Bob de l'utiliser sans pour autant communiquer. C'est une question actuellement ouverte. La recherche se poursuit.



Le lancer des dés

Rubrique des Paradoxes

Jean-Paul Delahaye
Université de Lille



Le même Julien que dans l'énoncé précédent propose à nouveau un pari à Alain. « Voici deux dés A et B. Ils possèdent la propriété suivante: en les lançant simultanément, le dé A gagne contre le dé B dans précisément 21 des 36 cas possibles, soit avec une probabilité de 58,33 %. Les faces de A portent respectivement les numéros 6, 3, 3, 3, 3 et 3. Les faces de B portent, elles, les numéros 5, 5, 5, 2, 2, 2. Le dé A gagne quand il obtient 6 – il y a 6 cas sur 36 de ce type – ou quand il obtient 3 et que B obtient 2 – il y a 15 cas sur 36 de ce type – ; le dé A gagne donc dans 21 cas sur 36, ce qui fait 58,33 %. Je précise que ces dés à 6 faces ne sont pas truqués, chaque face tombe avec la probabilité 1/6. Voici le pari que je propose. Nous engagerons chacun 100 euros. Tu prendras le dé que tu

voudras et je prendrai l'autre. Ensuite, nous lancerons chacun notre dé deux fois de suite. Tu feras la somme des résultats des deux lancers de ton dé. Je ferai la somme des résultats des deux lancers de mon dé. Celui dont le total sera le plus élevé gagnera et emportera les 200 euros. »

Alain réfléchit un moment. Il raisonne ainsi : « Le dé A est plus fort que le dé B, puisqu'il gagne dans 58,33 % des lancers et j'ai vérifié le raisonnement, c'est juste. En le lançant deux fois de suite, cela augmente encore son avantage sur le dé B et les chances qu'il a donc de gagner. Le pari que me propose Julien est stupide. Je vais l'accepter et je choisirai le dé A qui m'assurera au moins 58,33 % de chances de gagner. »

Alain accepte le pari et choisit le dé A.

Julien s'en réjouit et dit : « C'est parfait, les chances sont de mon côté, j'ai plus de 59 % de chances de gagner ».

N'est-ce pas paradoxal ? Comment expliquer cette affirmation de Julien ?

Solution du paradoxe précédent

La longueur des fleuves

Julien adore les paris et les chiffres. Durant le cours de géographie, il s'ennuie et propose à son voisin Alain de parier sur les nombres que va mentionner le professeur qui est en train d'expliquer les réseaux hydrographiques terrestres. Julien propose à Alain de miser vingt euros sur les neuf prochains nombres qui seront mentionnés (des longueurs de fleuves ou de rivières). Julien dit à Pierre : - « On ne considérera que le premier chiffre significatif des longueurs des cours d'eau mentionnés. Je prends le paquet des trois premiers chiffres $A = \{1, 2, 3\}$ et je te laisse le paquet des six autres chiffres $B = \{4, 5, 6, 7, 8, 9\}$. Celui qui, dans les neuf nombres qui vont venir, aura le plus souvent un premier chiffre dans son paquet gagnera et recevra donc vingt euros de l'autre. Si les longueurs mentionnées sont par exemple 243 km, 876 km, 1222 km, 92 km, 4330 km, 982 km, 3445 km, 2122 km, 832 km, dont les

premiers chiffres sont 2, 8, 1, 9, 4, 9, 3, 2, 8, tu auras gagné, puisqu'il y a cinq chiffres du paquet B et quatre du paquet A ». Alain est enchanté, il va certainement gagner les vingt euros car, ayant en sa faveur le paquet B de 6 chiffres alors que Julien n'en a que 3 dans le paquet A, il a toutes les chances de gagner. C'est une illusion et Julien – qui est un rusé parieur – a, en réalité, une probabilité de gagner égale à 73,77 %. Cela semble paradoxal. Saurez-vous expliquer et justifier ce 73,77 % ?

ii) Supposons que c'est vrai pour $n=0, 1, \dots, k$, c'est-à-dire que la dérivée de la fonction $x \rightarrow x^n$ est nulle :

$$(x^n)' = 0 \text{ pour } n=0, 1, \dots, k.$$

Utilisons maintenant la formule de dérivation d'un produit $(uv)' = u'v + uv'$. On a : $(x^{k+1})' = (x \cdot x^k)' = x' \cdot x^k + x \cdot (x^k)'$

On obtient 0 car, d'après l'hypothèse de récurrence, on a $x' = (x^1)' = 0$ (on utilise

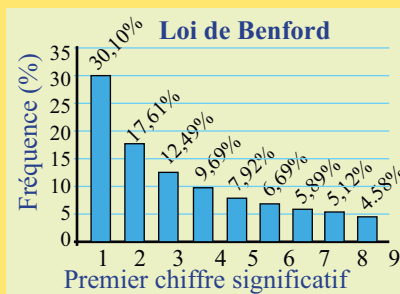
Solution du paradoxe précédent (suite)

l'hypothèse avec $n=1$) et $(x^k)' = 0$ (on utilise l'hypothèse avec $n=k$).

Nous avons donc $(x^{k+1})' = 0$, ce que nous souhaitons. Qu'est-ce qui cloche ?

Solution

La solution est liée à ce qu'on nomme la *loi de Benford*. Celle-ci indique que la probabilité qu'un nombre provenant d'une donnée comme la longueur d'un fleuve, ou la population d'une ville (et cela vaut aussi pour bien d'autres données statistiques), commence par le chiffre i est égale à $\log_{10}(1 + 1/i)$. Concrètement, quand une longueur de cours d'eau est mentionnée, il y a donc 30,1 % de chance que le premier chiffre de cette longueur soit « 1 ». Les autres probabilités sont données dans le tableau ci-dessous :



Cette loi étonnante a été vérifiée empiriquement et elle possède des explications mathématiques diverses, sujets aujourd'hui encore de travaux de recherche. Voir par exemple :

https://fr.wikipedia.org/wiki/Loi_de_Benford

La probabilité pour que le premier chiffre d'un nombre que va citer le professeur soit un « 1 », un « 2 » ou un « 3 » est donc :

$$a = (\log_{10}(1 + 1) + \log_{10}(1 + 1/2) + \log_{10}(1 + 1/3)) = 0,60205.$$

La probabilité pour que ce soit l'un des autres chiffres est obtenue est celle de l'évènement complémentaire :

$$b = 1 - a = 0,39795.$$

Si on ne prenait en compte qu'un seul nombre, Julien gagnerait avec une probabilité de 60,205%. Cependant, le pari prend en compte neuf nombres et non pas un seul. La probabilité pour que Ju-

lien gagne est donc la probabilité pour que, parmi les 9 nombres que va citer le professeur, il y en ait 5, 6, 7, 8 ou 9 dans le paquet $A = \{1, 2, 3\}$. Les méthodes usuelles pour traiter ce type de questions (loi de Bernoulli, loi binomiale) donnent que cette probabilité est :

$$a^9 + (9!/8!)a^8b + (9!/7!2!)a^7b^2 + (9!/6!3!)a^6b^3 + (9!/5!4!)a^5b^4 = 0,7377$$

(Sur la loi binomiale, voir par exemple :

http://fr.wikipedia.org/wiki/Loi_binomiale)

La loi binomiale

La loi binomiale est une loi de probabilité discrète définie par deux paramètres : n le nombre d'expériences réalisées, et p la probabilité de succès. La probabilité de l'échec est parfois notée $q = (1 - p)$. La loi binomiale décrit une suite d'expériences appelées *épreuve de Bernoulli*. La variable aléatoire X représente la somme k de succès pour les n répétitions de l'expérience et sa probabilité est :

$$\Pr(X = k) = \binom{n}{k} p^k (1 - p)^{n - k}.$$

Dans cette expression le coefficient est,

$$\binom{n}{k} = \frac{n!}{(n - k)!k!}.$$

Ainsi, la probabilité d'obtenir un 6 deux fois en lançant un dé trois fois de suite est :

$$\Pr(X = 2) = \binom{3}{2} \left(\frac{1}{6}\right)^2 \left(\frac{5}{6}\right)^1.$$

Lorsque $p = 1/2$, comme dans le lancer d'une pièce de monnaie,

la loi binomiale tend vers la loi normale.

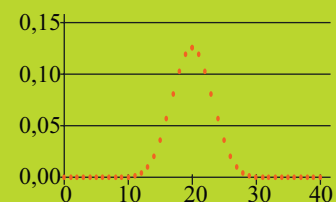
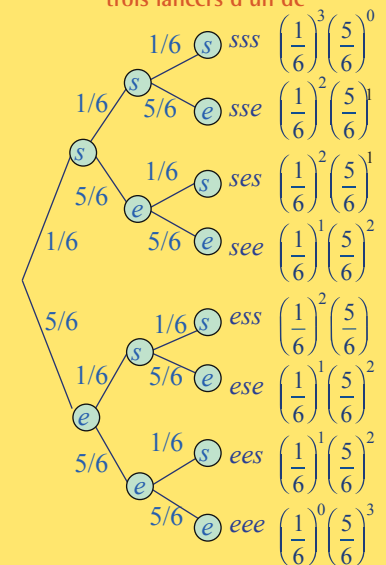


Diagramme de Bernoulli. trois lancers d'un dé



Section problèmes

Points, droites et plans (suite)

- Déterminer quelles sont, selon la méthode finale de Cantor, les coordonnées du point associé à
 - $0,\overline{6} = 0,666\dots$
 - $0,0\overline{8} = 0,088\dots$
 - $0,5\overline{9} = 0,599\dots$
 - $0,4\overline{95} = 0,49595\dots$
 - $0,79392909590989097996\dots$
 - $0,1949195992969959396\dots$

Dialogue géométrico-algébrique à saveur hippocratique

- Étant donné un triangle rectangle, montrer que le point milieu de son hypoténuse est équidistant des trois sommets du triangle.
Tuyau: Introduire le rectangle dont l'une des diagonales est l'hypoténuse du triangle donné, et tirer profit des propriétés des diagonales d'un rectangle.
 - En conclure que le cercle ayant pour diamètre l'hypoténuse d'un triangle rectangle est circonscrit à ce triangle (et donc qu'il passe par le sommet de l'angle droit).
- Nous reprenons la démonstration du résultat du #1-b en utilisant maintenant la notion d'angle inscrit dans un demi-cercle (et donc sous-tendant le diamètre).

- Montrer que tout angle inscrit dans un demi-cercle est droit.
- En prenant appui sur la partie a), montrer que tout angle sous-tendant le diamètre d'un demi-cercle et dont le sommet est à l'intérieur de celui-ci est plus grand qu'un angle droit.
- Montrer de même que tout angle sous-tendant le diamètre d'un demi-cercle et dont le sommet est à l'extérieur de celui-ci est plus petit qu'un angle droit.

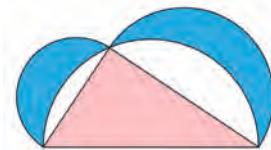
1. Bernard Vitrac, *Euclide d'Alexandrie, Les Éléments, volume 2. PUF, 1994, p. 236.*

- En conclure (comme au #1-b) que le demi-cercle construit sur l'hypoténuse d'un triangle rectangle passe forcément par le sommet de l'angle droit.

Tuyau: Supposer au contraire que le sommet de l'angle droit n'est pas sur le demi-cercle.

Remarque: On pourrait aussi travailler à partir des résultats généraux sur un angle quelconque dans un cercle : *angle inscrit, angle intérieur et angle extérieur.*

- Du #1-b, il découle que la figure qui suit correspond bien au cas de deux lunules construites à partir des demi-cercles sur les trois côtés d'un triangle rectangle.



En prenant appui sur ce fait, et aussi sur la relation entre les aires des trois demi-cercles en jeu, démontrer le résultat d'Hippocrate affirmant que *la somme des aires des deux lunules construites sur les cathètes d'un triangle rectangle est égale à l'aire du triangle lui-même.*

- On s'intéresse au résultat d'Hippocrate à propos d'un triangle rectangle isocèle sur lequel on considère une lunule unique, telle que décrite dans le texte.

- La figure ci-dessous sous-entend deux cercles, chacun étant circonscrit à un certain carré. Caractériser ces cercles et ces carrés et donner une figure les illustrant.



- En vous appuyant sur la proposition VI.31 des *Éléments* d'Euclide (voir l'encadré), donner la relation entre les aires des trois segments circulaires de la figure qui précède.
 - À l'aide des formules usuelles pour les aires, caractériser algébriquement la relation entre les trois aires de la partie b) – comme le souhaite Madame É.A. (p. 11).
- En prenant appui sur le #4, démontrer le résultat d'Hippocrate affirmant que *l'aire de la lunule ainsi construite à partir d'un triangle rectangle isocèle est égale à l'aire du triangle lui-même.*

Euclide VI.31

Dans les triangles rectangles, la figure sur le côté sous-tendant l'angle droit est égale aux figures sur les côtés contenant l'angle droit, semblables et semblablement décrites.¹

Pour en savoir plus!

Accro-flashes

Dialogue géométrico-algébrique à saveur hippocratique

- Le thème des lunules à la Hippocrate a déjà été abordé dans *Accromath*, notamment dans Jean-Paul Delahaye, « Preuves sans mots. » *Accromath*, vol. 3(1) (2008) pp. 14-17, et André Ross, « Comparaison d'aires : 1. la règle et le compas. » *Accromath*, vol. 17(1) (2022) pp. 26-29.
- Le mot lunule provient du mot latin *lunula*, « petite lune, petit croissant », lui-même un diminutif du latin *luna*, « lune ». De nos jours, ce terme sert notamment à désigner un verre en forme de croissant délimitant le foyer inférieur des lunettes à double foyer, ou encore la partie blanchâtre demi-circulaire située à la base de l'ongle, près de sa racine. En géométrie, le mot lunule désigne une figure plane « en forme de croissant comprise entre deux arcs de cercles sécants de rayons différents » (*Le Robert*).
- Une riche discussion des résultats d'Hippocrate est proposée par Bartel Leendert van der Waerden, *Science Awakening*, Oxford University Press, 1961, pp. 131-133. L'auteur y explique notamment comment les résultats d'Hippocrate sont parvenus jusqu'à nous. Il fait également ressortir l'utilisation par le mathématicien grec du principe suivant : *des segments circulaires semblables sont dans le même rapport que les carrés sur les bases de ces segments*.
- On trouvera dans George Pólya, *Les mathématiques et le raisonnement « plausible »*. Paris, Gauthier-Villars, 1958, pp. 13-15, une discussion stimulante et originale autour de l'égalité de Pythagore. L'auteur souligne comment la multiplication de cette égalité par une certaine constante — processus qu'il met en lien avec la proposition VI.31 des *Éléments* d'Euclide — permet un va-et-vient entre des démarches de *généralisation*, de *particularisation* et d'*analogie* en mathématiques. Pólya indique également comment une telle approche peut mener à une preuve remarquablement limpide du théorème de Pythagore — voir aussi à ce propos la discussion dans Bernard R. Hodgson, « Sommes à la sauce pythagoricienne. » *Accromath*, vol. 5(2) (2010) pp. 25-27.
- L'illustration représentant Archimède, lors de la prise de Syracuse en -212 par le général romain Marcus Claudius Marcellus, est tirée de la revue *Le Magasin pittoresque* 45 (1877), p. 301. Elle porte comme légende : « La Mort d'Archimède, peinture par Gustave Courtois. — Dessin de Henri Girardet. » De nombreuses illustrations existent à propos d'Archimède et des circonstances de son décès. Voir par exemple, sur le site math.nyu.edu/Archimedes/ dû à Chris Rorres et consacré à Archimède, les pages *Pictures of Archimedes* et *Death of Archimedes*.
- Sur le plan géographique, notons que les îles de Chios et de Kos sont situées dans l'est de la mer Égée, près des côtes de la Turquie. Entre les deux se trouve l'île de Samos, d'où est originaire Pythagore.

Mécanique quantique

Jeu de couleur, jeu de quantas

- [CRC19] X. Coiteux-Roy et C. Crépeau. «The RGB No-Signalling Game.» *14th Conference on the Theory of Quantum Computation, Communication and Cryptography*, TQC 2019, June 3-5, 2019, University of Maryland, College Park, Maryland, USA, pp. 4:1–4:17, 2019.
- [Be64] Bell, J. S., «On the Einstein Podolsky Rosen paradox.» *Physics Physique Fizika* 1, pp. 195–200, Nov 1964.
- [AGR81] Aspect, Alain, Grangier, Philippe et Roger, Gérard, «Experimental Tests of Realistic Local Theories via Bell's Theorem.» *Phys. Rev. Lett.* 47, pp. 460–463, Aug 1981.
- [EPR35] A. Einstein, N. Rosen et B. Podolsky, *Phys. Rev.* 47, (1935); voir aussi N. Bohr, *Ibid.* 48, (1935), W. H. Furry, *Ibid.* 49, (1936), et D. R. Inglis, *Rev. Mod. Phys.* 33, (1961).

Accromath est une publication de l'Institut des sciences mathématiques (ISM) et du Centre de recherches mathématiques (CRM). La revue s'adresse surtout aux étudiantes et étudiants d'école secondaire et de cégep ainsi qu'à leurs enseignantes et enseignants.

ISM

Institut des sciences mathématiques

L'Institut des sciences mathématiques est une institution unique dédiée à la promotion et à la coordination de l'enseignement et de la recherche en sciences mathématiques au Québec. En réunissant huit départements de mathématiques des universités québécoises (Concordia, Université Laval, McGill, Université de Montréal, UQAM, UQTR, Université de Sherbrooke, Bishop's), l'Institut rassemble un grand bassin d'expertises en recherche et en enseignement des mathématiques. L'Institut anime de nombreuses activités scientifiques, dont des séminaires de recherche et des colloques à l'intention des professeurs et des étudiants avancés, ainsi que des conférences de vulgarisation données dans les cégeps. Il offre également plusieurs programmes de bourses d'excellence.

L'ISM est financé par le Ministère de l'Enseignement supérieur et par ses huit universités membres.

CRM

CENTRE
DE RECHERCHES
MATHÉMATIQUES

Le Centre de recherches mathématiques est un centre national pour la recherche fondamentale en mathématiques et ses applications. Les scientifiques du CRM comptent plus d'une centaine de membres réguliers et de stagiaires postdoctoraux. Lieu privilégié de rencontre, le Centre est l'hôte chaque année de nombreux visiteurs et d'ateliers de recherche internationaux.

Les activités scientifiques du CRM comportent deux volets principaux : les projets de recherche qu'entreprennent ses laboratoires, et les activités thématiques organisées à l'échelle internationale. Ces dernières, ouvertes à tous les domaines, impliquent des chercheurs du CRM et d'autres universités. Afin d'assurer une meilleure diffusion des résultats de recherches de ses collaborateurs, le CRM a lancé en 1989 un programme de publications en collaboration avec l'American Mathematical Society et avec Springer.

Le CRM est principalement financé par le CRSNG (Conseil de recherches en sciences naturelles et en génie du Canada), le FQRNT (Fonds québécois de recherche sur la nature et les technologies), l'Université de Montréal, et par six autres universités au Québec et en Ontario.

Accromath bénéficie de l'appui de la Dotation Serge-Bissonnette du CRM.

