

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

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

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).

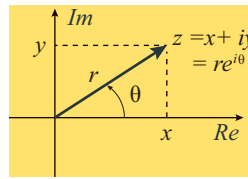


Figure 1

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

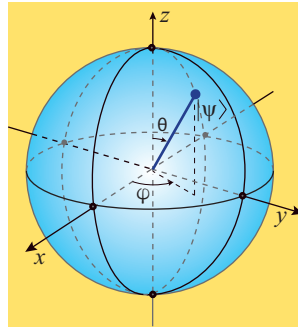


Figure 2

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).

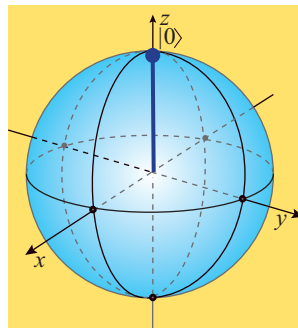


Figure 3

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).

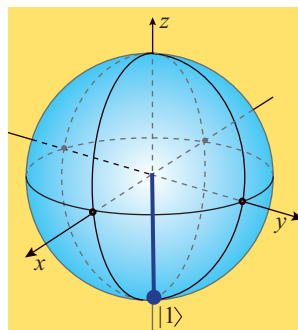


Figure 4

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.