Quelques raisons montrant que l'ordinateur quantique ne sera pas utile

Alexandre Gondran

ÉNAC, École Nationale de l'Aviation Civile, Toulouse, France
alexandre.gondran@recherche.enac.fr

Mots-clés : *calcul quantique, mécanique quantique.*

Les calculateurs quantiques prétendent résoudre certains problèmes plus rapidement que les ordinateurs classiques. Cependant, les réalisations des vingt dernières années sont très loin de montrer que l'on avance dans ce sens.

L'objet de cette présentation est d'exposer plusieurs raisons pour expliquer qu'un calculateur quantique permettant de factoriser rapidement de grand nombre (algorithme de Shor) ou de chercher un élément dans une liste non triée de n éléments en une complexité temporelle de $O(\sqrt{n})$ (algorithme de Grover) ne verra sans doute jamais le jour.

Chacune des raisons suffit indépendamment à montrer que le passage à l'échelle ne sera pas possible.

1 Les limites actuelles

Sur les frises chronologiques de la figure 1 sont représentées les principales réalisations de calculateurs quantiques pour implémenter respectivement l'algorithme de Grover et de Shor. On constate que quelle que soit la technologie utilisée, il est encore impossible de factoriser un nombre plus grand que 21 et que la recherche d'un élément dans une liste non triée n'est possible que sur une liste de 8 éléments. Le passage à échelle vers de données de plus grande taille

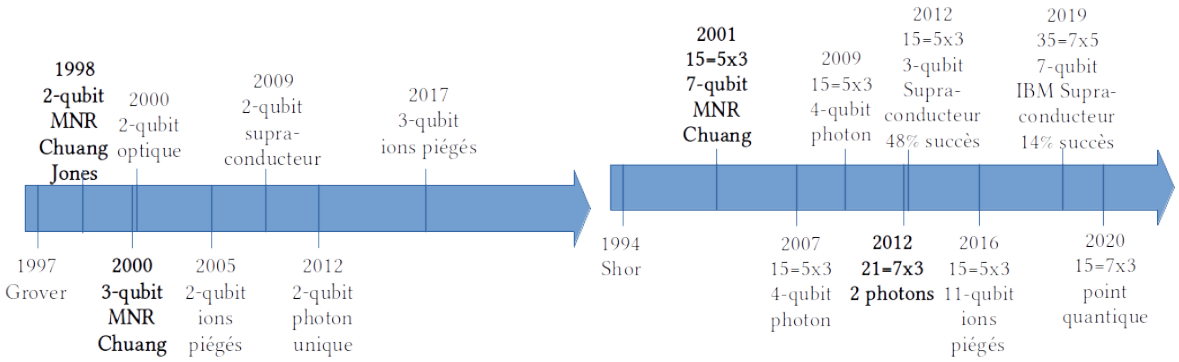

FIG. 1 – Frises chronologiques des principales implémentations des algorithmes de Grover (gauche) et de Shor (droite), d'après [1].

butte sur des problèmes sérieux. Nous donnons quelques raisons qui expliqueraient pourquoi ce passage à l'échelle est impossible.

2 Quelques raisons du non-passage à l'échelle

2.1 Raison 1 : le qubit n'est pas ponctuel

Le qubit logique utilisé en informatique quantique est idéal, car son extension spatiale n'est pas considérée. Or, en mécanique quantique, rien n'est ponctuel, c'est d'ailleurs un principe

fondamental que l'on retrouve par exemple dans les inégalités d'Heisenberg. Négliger l'extension spatiale pour le qubit logique a pour conséquence de négliger des interactions physiques entre les qubits alors qu'elles ne le sont pas forcément. Cela peut provoquer des approximations acceptables à petite échelle (pour quelques qubits) mais rendre impossible le passage à l'échelle. Ce constat reste vrai que le qubit logique soit représenté par un système quantique unique (comme un ion piégé) ou par un ensemble considérable d'objets quantiques (comme plusieurs centaines de milliers de spins nucléaires pour un qubit RMN).

2.2 Raison 2 : la porte cNOT parfaite n'existe pas

En théorie de l'informatique quantique, toutes les opérations (transformation unitaire) sur un nombre k de qubits peuvent se décomposer en produit de transformations unitaires sur **un** qubit et de portes cNOT sur **deux** qubits. Cependant la porte cNOT idéale $= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ n'existe pas. Si on ajoute une petite erreur à cette matrice, notée $\widetilde{cNOT}$, le cumul des erreurs devient vite exponentielle. Un simple exemple montre que l'application de la porte $\widetilde{cNOT}$ $2p$ fois successivement sur un qubit quelconque $|\psi>$: $\widetilde{cNOT}^{2p}|\psi> \neq |\psi>$ alors qu'idéalement $cNOT^{2p}|\psi> = |\psi>$ même pour p très grand. Sachant que pour factoriser 15 (codés sur $k = 4$ qubits), il est nécessaire de 4608 ($= 72k^3$) portes logiques, la factorisation de grand nombre s'avère impossible.

2.3 Raison 3 : les diverses interprétations de la superposition

Le débat sur l'interprétation de la superposition est toujours très actif parmi les physiciens et provient du problème appelé *problème de la mesure*, et plus connu sous le nom du paradoxe du chat de Schrödinger. Nous présenterons rapidement le débat et les hypothèses que fait chacune des interprétations : hypothèse d'existence d'un aléa fondamental d'un type nouveau en mécanique quantique pour les interprétations de Copenhague et des mondes multiples ; hypothèse d'existence d'un modèle sous-jacent aux résultats statistique de la mécanique quantique la théorie de de Broglie-Bohm. Selon l'interprétation, le *parallélisme* de l'informatique quantique est réel (interprétations de Copenhague et des mondes multiples) ou fictif (théorie de de Broglie-Bohm).

2.4 Raison 4 : la durée de cohérence trop courte

On pourra montrer une limite et difficulté de passage à l'échelle due à la durée trop courte de cohérence des qubits. Cela a pour conséquence de limiter la durée totale d'un calcul quantique et donc le nombre de portes logiques utilisable dans un algorithme.

3 Conclusions

Le calcul quantique est une nouvelle discipline scientifique qui s'est considérablement développée ces dernières années de part les défis intellectuels qu'il suscite et les intérêts industriels qu'il inspire ; L'exposé tente d'apporter des raisons pour montrer que le calcul quantique restera une discipline hors-sol, sans applications utiles.

Références

[1] A. Gondran. *Les bases de la mécanique quantique pour le calcul quantique* Cours donné à l'ENSEEIHT, octobre 2021.