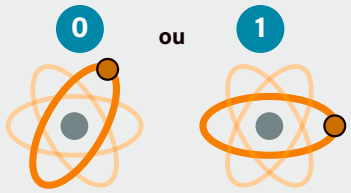
CIRCUITS QUANTIQUES

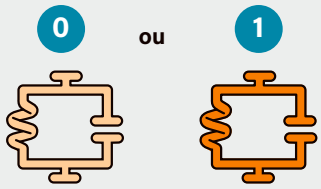
Les circuits quantiques sont des représentations abstraites de l'informatique quantique, analogues aux circuits de l'informatique théorique classique. Avec ces diagrammes, on met de côté les aspects physiques du système (peu importe ici que les qubits soient portés par des circuits supraconducteurs ou autre) et on se concentre sur les opérations de manipulation des qubits.

Un ordinateur quantique peut être réalisé de différentes façons, le qubit est alors représenté par diverses propriétés du système. Trois exemples d'approches.

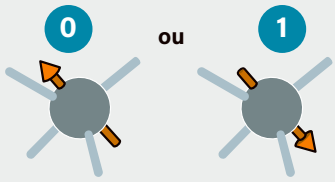
Ion
L'orbite électronique définit le qubit



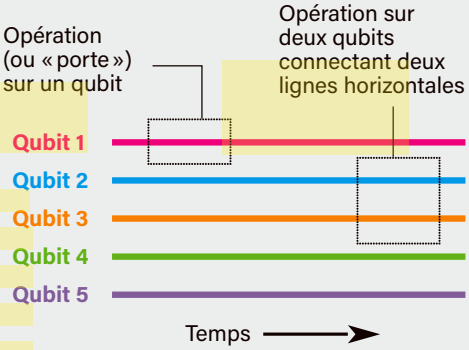
Supraconducteur
La superposition de différents états de charge du circuit définit le qubit



Spin dans la matière
Le spin d'un atome dans un réseau définit l'état quantique

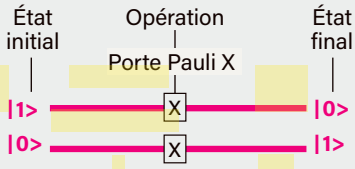


Peu importe la réalisation physique, les opérations peuvent toujours être représentées par le même type de diagrammes, les circuits quantiques.
Ils ressemblent à des partitions musicales. Chaque ligne horizontale représente un qubit. Les « notes » représentent les opérations, on parle de « portes logiques ». Comme pour la musique, la progression dans le diagramme est temporelle. Elle montre la séquence des opérations que l'on applique aux différents qubits.

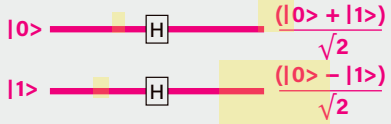


Différentes opérations sont représentées par différents symboles pour les portes.

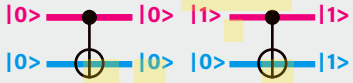
Un *bit flip* (nommée la porte « Pauli-X », et notée [X]) inverse un qubit. Il transforme un 1 en 0, et inversement.



Une porte de Hadamard [H] place un qubit dans une superposition.

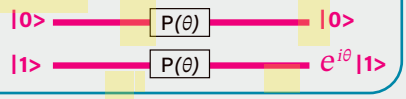


Si deux qubits sont connectés par une ligne verticale, l'inversion du second est conditionnée par la valeur du premier. La porte est dite « contrôlée ».

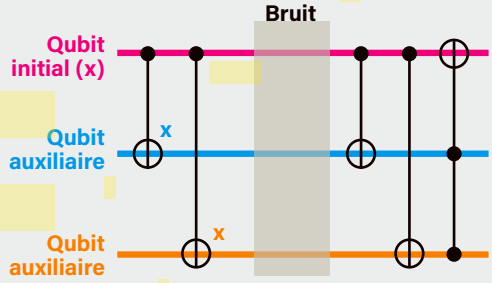


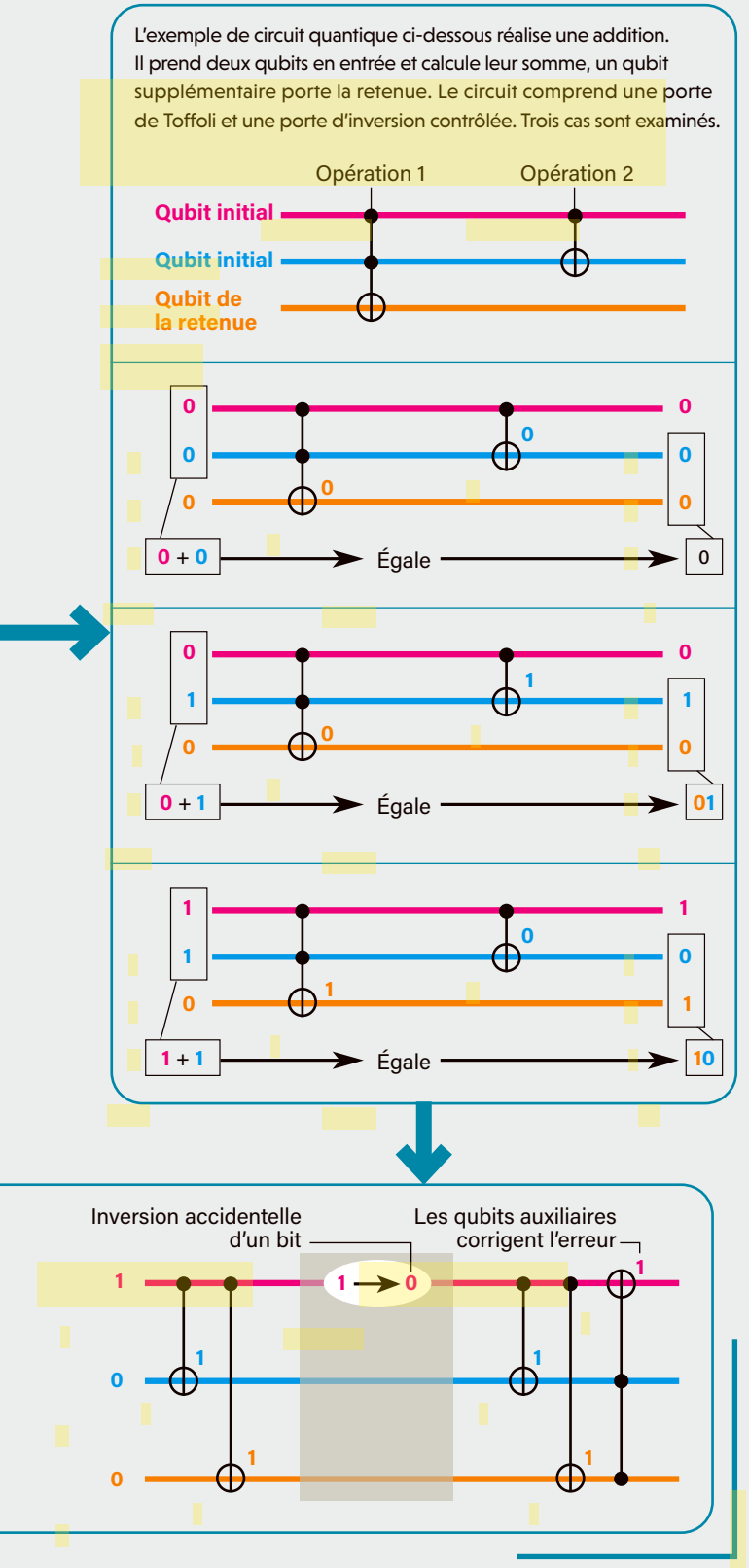
Une porte d'inversion contrôlée qui implique trois qubits est nommée « porte de Toffoli ».

Une porte peut également modifier la phase du qubit d'un angle arbitraire [P(θ)].



Chaque porte présente un taux d'erreur – la probabilité que le système physique qui réalise la porte donne une mauvaise valeur, de la même façon qu'un musicien risque de jouer une fausse note. En l'absence d'un système de correction des erreurs, un circuit livre un mauvais résultat avec une probabilité proportionnelle au taux d'erreur des portes : le nombre de fausses notes devient alors si grand qu'on ne reconnaît plus le morceau de musique. Grâce à des qubits auxiliaires, il est possible de détecter la présence d'erreurs et de les corriger. Ci-contre, un exemple simple de circuit corrigeant les erreurs. Pour un qubit d'information, il nécessite trois qubits. Le circuit compare des paires de qubits. Une paire indique qu'une erreur s'est produite, deux paires indiquent où elle s'est produite, et la porte de Toffoli applique la correction. Avec cette stratégie, on extrait l'information sur l'erreur sans révéler l'information quantique du qubit.





© Jen Christiansen

rendre le matériel aussi fiable que possible, puis à ajouter une couche de redondance pour éliminer les erreurs résiduelles.

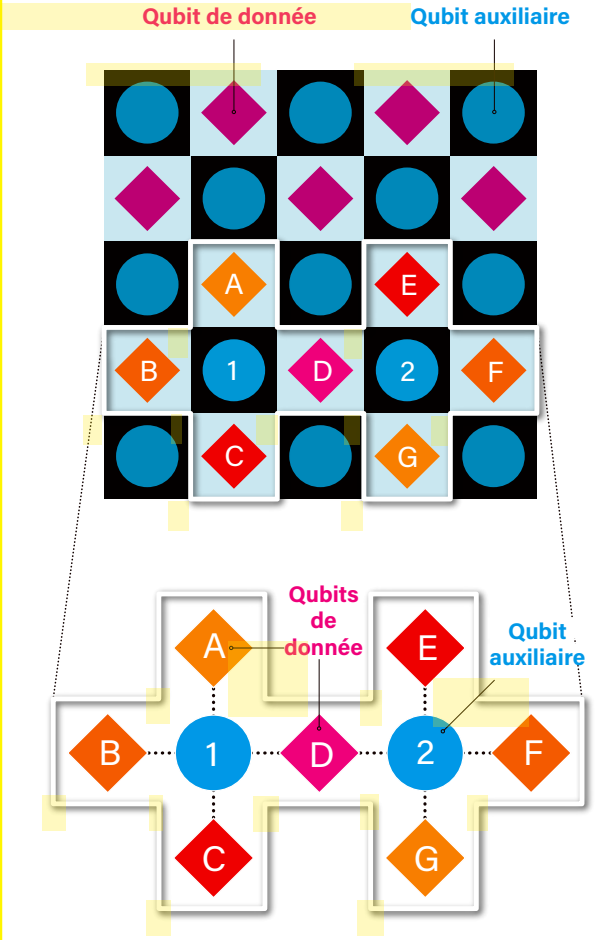
Il existe de nombreux codes correcteurs plus ou moins optimisés. Cependant, il était difficile de voir comment adapter ces méthodes classiques aux ordinateurs quantiques. En effet, un théorème stipule que l'information quantique ne peut être clonée, c'est-à-dire qu'il est impossible de copier à l'identique un état quantique inconnu. Cela supposerait de mesurer l'état avant de le dupliquer; mais quand on mesure un système quantique, on détruit la superposition des états et un seul état est mesuré. Or toute la puissance de ces dispositifs repose dans la préservation de la superposition des états. Autre difficulté, les qubits subissent deux types d'erreurs: la première est équivalente à celle des bits classiques, la valeur du bit s'inverse, un 0 devient un 1, par exemple; la seconde est spécifique et influe sur la phase des ondes qui décrivent les qubits.

DES QUBITS AUXILIAIRES À LA RESCOUSSE

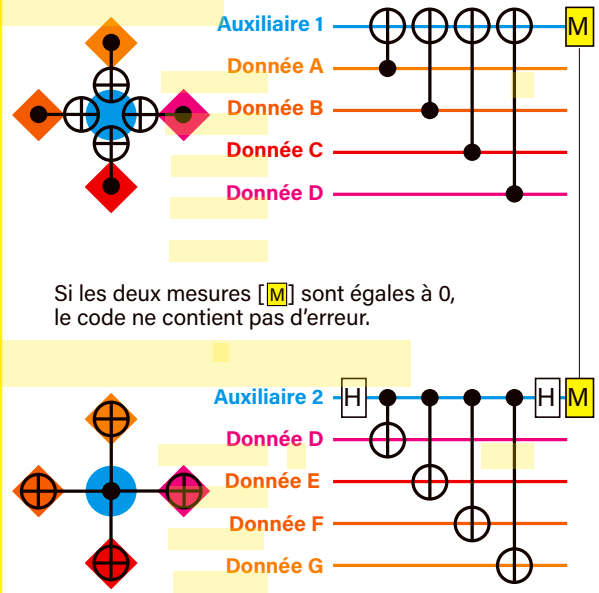
Pour résoudre tous ces problèmes, les stratégies de correction des erreurs quantiques utilisent des qubits auxiliaires. Ceux-ci sont intriqués avec les qubits initiaux. Quand deux qubits sont intriqués, leurs propriétés sont fortement corrélées. L'idée est de transférer le bruit du système (les erreurs) aux qubits auxiliaires. Une mesure directe des qubits auxiliaires révélerait l'état du qubit initial, ce qui détruirait la superposition des états. Cependant, il est possible de réaliser des mesures indirectes de sorte à interroger le système pour savoir s'il contient une erreur ou non, mais sans livrer d'information sur l'état du système. Cette stratégie donne assez d'indices pour éventuellement corriger le système.

Comme pour la correction classique des erreurs, le succès dépend de la nature du bruit. Pour les ordinateurs quantiques, les erreurs surviennent lorsque le système quantique interagit et s'intrique avec l'environnement. Pour que l'ordinateur opère de façon efficace, le rythme d'accumulation des erreurs physiques doit être faible. On définit alors une valeur critique. En dessous de ce seuil, il est possible de corriger les erreurs pour rendre arbitrairement faible la probabilité qu'un calcul échoue. Au-dessus de ce seuil, le matériel introduit des erreurs à une vitesse trop élevée pour être corrigées. Ce changement de comportement en fonction d'un seuil est typiquement ce qu'on nomme en physique une transition de phase entre un état ordonné et un état désordonné. Spécialiste de la matière condensée ayant passé la majeure partie de ma carrière à étudier des transitions de phases quantiques, ce constat m'a fascinée.

Configuration du code de surface



Détection d'erreur



Si les deux mesures [M] sont égales à 0, le code ne contient pas d'erreur.

Le défi aujourd'hui est donc de trouver des moyens pour améliorer les codes correcteurs afin qu'ils puissent gérer des taux d'erreurs plus élevés, une plus grande variété d'erreurs et s'adapter aux contraintes du matériel.

Les codes correcteurs d'erreurs les plus populaires sont les « codes quantiques topologiques ». Leur origine remonte à 1982, lorsque Frank Wilczek, du MIT (l'institut de technologie du Massachusetts), aux États-Unis, a proposé que l'Univers pouvait contenir une toute nouvelle catégorie de particules. Contrairement aux types connus, dont le spin a une valeur entière (comme le photon) ou demi-entière (comme l'électron), ces particules auraient des valeurs fractionnaires intermédiaires (mais elles n'existeraient que dans des géométries bidimensionnelles). Le physicien les a nommées « anyons » et pensait que les applications pratiques de ces objets étaient probablement lointaines.

DES ANYONS POUR LA CORRECTION

Mais les physiciens ont vite découvert que les anyons n'étaient pas si inutiles que cela. En fait, ils sont liés à des phénomènes du monde réel, dans certains systèmes de matière condensée. Pour achever leur passage de la théorie aux besoins pratiques de la technologie, Alexei Kitaev, de Caltech (l'institut de technologie de Californie), a constaté que les anyons constituaient un outil efficace pour exprimer certains calculs quantiques. Il a alors montré qu'ils avaient une application directe dans des systèmes qui manipulent un grand nombre de particules pour en faire un code quantique.

Dans ces systèmes, les particules sont connectées dans un réseau bidimensionnel où leur état d'énergie le plus bas est fortement intriqué. Les erreurs correspondent à des états d'énergie plus élevée du système, on parle d'excitations. Ces excitations sont représentées par des anyons. Ces idées ont marqué la naissance des codes topologiques (et avec eux, un autre pont entre le calcul quantique et la physique de la matière condensée). Comme le bruit est censé agir localement sur le réseau et que les codes topologiques ont des excitations localisées, ils sont rapidement devenus le système préféré pour protéger les informations quantiques.

Le « code de surface » (ou « code de Kitaev ») et le « code de couleur » sont deux exemples de codes topologiques. Le premier a été développé par Alexei Kitaev et Sergey Bravyi, un de mes collègues chez IBM. Le code de surface est composé des qubits initiaux portant l'information et de qubits auxiliaires, disposés de façon alternée sur un carré bidimensionnel, comme sur un échiquier, les premiers occupant les cases blanches, les seconds les noires.