A N D S I

Association Nationale des Dirigeants en Sciences de l'Information
www.andsi.fr

Informatique quantique, corrections d'erreur et feedback

Compte rendu rédigé par ANDSI et Pierre Delort

En bref…

Pierre ROUCHON est enseignant-chercheur au Centre Automatique et Systèmes (CAS) de Mines Paris – PSL et membre de l'équipe ENS-INRIA-Mines Quantic. Spécialiste de l'automatique et des technologies quantiques, il a contribué à des avancées majeures, notamment dans le contrôle en temps réel des systèmes quantiques, ouvrant la voie à des applications innovantes dans ce domaine de pointe.

L'Association Nationale des Directeurs des Systèmes d'Information organise des débats et en diffuse des comptes rendus, les idées restant de la seule responsabilité de leurs auteurs. Elle peut également diffuser les commentaires que suscitent ces documents.

Contexte

Pierre ROUCHON explique que Google travaille sur le quantum *machine learning*. On entend par simulateur quantique la simulation d'un système quantique au moyen d'un autre système quantique. La course aux algorithmes quantiques permet de faire progresser les algorithmes classiques. Il n'est pas possible de simuler un système quantique de grande taille à l'aide d'un système classique pour des raisons de taille : en quantique la dimension d'un système composite est le produit des dimensions de chacun sous-système, alors qu'en classique il s'agit de la somme. En France, le gouvernement est à l'initiative de nombreux projets.

Quantum bits : plateformes physiques

Actuellement, trois types de plateformes principales (atomes froids, ions piégés et circuits supraconducteurs) permettent de construire ces machines. Pour les atomes et les ions, c'est à température ambiante, sous ultravide et contrôlé par impulsions laser. Pour les circuits supraconducteurs, c'est à basse température dans des cryostats avec des impulsions micro-ondes.

Quantum versus classique

L'évolution temporelle d'un système quantique est gouvernée par l'équation Schrödinger, une équation différentielle et linéaire sur un espace vectoriel dans lequel évolue la fonction d'onde, i.e., l'état quantique du système. Le système quantique le plus simple est le qubit où l'espace correspond à un plan : l'état quantique d'un qubit est alors une combinaison linéaire à coefficients complexes de deux vecteurs d'une base orthonormale, vecteurs notés par les kets |0> et |1>. L'information quantique correspond alors à deux coefficients, deux nombres complexes. C'est très différent de l'information classique d'un qubit qui correspond à un bit, deux entiers 0 et 1.

Un état quantique se présente comme une sorte de loi de probabilités. Elle est modifiée lorsque l'on effectue une mesure sur le système, le résultat de cette mesure étant alors une information classique. Il faut alors changer l'état quantique pour prendre en compte cette information classique issue du processus de mesure. Il s'agit de la rétroaction de la mesure sur le système. Pour résumer, l'évolution d'un système quantique est la

combinaison de deux dynamiques : une dynamique déterministe régie par l'équation de Schrödinger et une dynamique stochastique liée à la mesure et régie par la réduction du paquet d'onde (i.e. de l'état quantique).

La première expérience de *feedback d'états quantiques* a été réalisée en 2011 avec un système composite de photons micro-ondes et d'atomes-sondes assurant une mesure indirecte du nombre de photons piégés entre deux miroirs. Le contrôle est réalisé par une antenne qui envoie à la demande des impulsions micro-ondes d'amplitude et de phase réglables. A partir des impulsions micro-ondes passées et des informations obtenues via les atomes-sondes, il est alors possible de suivre en temps réel l'état quantique des photons (filtre quantique analogue quantique du filtre de Kalman) et ainsi de réguler le nombre de photons en ajustant le contrôle par un feedback d'état. Il s'agit d'une boucle de rétroaction où le contrôleur est un système classique.

Très schématiquement un calcul quantique avec N qubits se décompose en 3 étapes :
-1- initialisation au temps t=0 de chacun des qubits dans l'état |0>.
-2- évolution selon Schrödinger entre t=0 et t=T : il s'agit d'une sorte de rotation, une transformation unitaire notée U, dans l'espace vectoriel des N qubits qui est de dimension 2^N. Quand N est grand, disons plusieurs milliers cette dimension est absolument gigantesque.
-3- mesure de chacun des qubits à l'instant final T : on obtient alors une suite de N bits classiques valant 0 ou 1.

L'algorithme et les données de départ (par exemple la factorisation d'un grand nombre RSA) sont alors encodés dans la transformation U, qui peut toujours se décomposer en portes quantiques élémentaires (portes quantiques universelles faisant intervenir uniquement un ou deux qubits). La complexité de l'algorithme est alors donnée approximativement par le nombre des portes élémentaires nécessaires à la réalisation de la transformation U. On dira que le calcul est très facile si ce nombre est proportionnel à N. Il est de complexité polynomiale (resp. exponentielle) si ce nombre de portes élémentaires est approximativement une puissance de N (resp. exp(c N), c constante positive). Noter que le temps T est proportionnel au nombre de portes quantiques nécessaires pour générer U. Ainsi l'algorithme de factorisation de Shor donne dans la mesure finale des qubits l'un des facteurs premiers du grand nombre RSA avec un nombre de portes qui est de l'ordre de N^3 : il est polynômial.

Correction des erreurs quantiques

En informatique classique, une erreur corresponds uniquement à un « bit-flip », 0 devient 1 ou 1 devient 0 . Comme le système physique subjacent est un système classique bi-stable avec deux équilibres, 0 et 1, séparés par une haute barrière de potentiel, les erreurs de bit-flip sont très-très faibles : une porte classique élémentaire à une probabilité d'erreur plus petite que 10^{-20}. En quantique c'est très différent : un qubit est sujet à deux types d'erreurs fondamentales : le bi-flip et le phase-flip. Il n'est pas possible d'éliminer ces deux types d'erreurs en imposant une simple une barrière de potentiel entre [0> et |1>. C'est bien plus difficile. Actuellement, quelques soient les plateformes développées, le taux d'erreur par porte élémentaire quantique est autour de 10^{-3} à 10^{-4}. Pour pouvoir faire des calculs impossibles à faire en un temps raisonnable en classique, il faudrait un taux d'erreur logique bien plus petit au-delà de 10^{-10} .

Int : Le fait de mesurer ne génère-t-il pas des erreurs ?
PR : Effectivement, il faut prendre en compte aussi ce type d'erreur en plus des bit-flips et phase-flips. Noter les erreurs non détectées représentent des fuites d'informations dans l'environnement, correspondent à la décohérence et induisent à des évolutions irréversibles, dissipatives en quelques sortes.

Pour atteinte des taux au-delà de 10^{-10} avec des qubits physiques ayant des taux bien supérieurs, il va être nécessaire d'utiliser des codes correcteurs où un qubit logique est encodé dans plusieurs qubits physiques. On

exploite une redondance pour détecter les erreurs et les compenser par une boucle de feedback. Prenons le cas simple d'un simple bit logique classique encodé sur trois bits physiques. Si l'erreur de départ d'un bit physique est P proche de 0, le taux d'erreur sera autour P^2 pour le bit logique avec le feedback. Ainsi, avec $P=10^{-5}$ on passe à P^2 de l'ordre de 10^{-10}. En quantique c'est un peu la même situation mais en plus compliquée. D'une part, il faut une double redondance afin de corriger bit-flip et phase-flip mais aussi un processus de mesure subtile pour détecter les erreurs sans détruite l'information quantique du qubit logique. Ici encore les contributions de Peter Shor ont été déterminantes.

Int : L'erreur est-elle due à une particule ou à un atome qui passe alors qu'il n'aurait pas dû le faire ?
PR : Pour les plateformes à base de circuits quantiques supraconducteurs une particule cosmique avec assez d'énergie heurte le circuit, produit des quasi-particules et peut ainsi générer des erreurs corrélées sur plusieurs qubits physiques.

Correction autonome d'erreurs

La correction d'erreur repose donc sur deux points fondamentaux : la redondance où l'information quantique d'un qubit-logique est encodé dans un espace vectoriel dont la dimension peut être très grande si la redondance est importante ; une boucle de feedback.
L'encodage bosonique et les qubits de chat (cat-qubit) reposent sur ces deux points : l'espace d'encodage est directement de dimension infinie et correspond à celui d'un oscillateur harmonique quantique ; le feedback est assuré par un contrôleur qui est lui aussi quantique. On retrouve ici la situation du régulateur de Watt pour les machines à vapeur : le système mécanique formé par la machine à vapeur est contrôlé par un second système mécanique, le régulateur à boules, qui pilote directement la vanne de vapeur à l'entrée de la machine en fonction de la vitesse de rotation.
Pour les cat-qubits à base de circuits supraconducteurs, de tels contrôleurs quantiques sont aussi des circuits supraconducteurs où les bit-flips sont quasiment supprimés et où seuls les phase-flips sont à corriger via une redondance réduite et un feedback avec contrôleur classique.

Débat

Int : « Alice et Bob » disposent-ils d'une technologie spécifique ?
PR : Oui, celles des cat-qubits. Cette même idée a été reprise par Amazon web services. Elle a été créée par d'anciens étudiants du groupe Quantic et de l'ENS Lyon.
Int : Comment a-t-elle été financée ?
PR : A ma connaissance, elle l'a été au départ surtout par des financements français et européens. Plus récemment elle s'est ouverte à des financements étrangers.

Int : Combien de temps est-il nécessaire pour gagner trois ordres de grandeur ?
PR : Difficile de répondre précisément. Pour l'instant, on observe une progression continue de la qualité des qubits physiques : on est passé de taux de 1/100 à 1/1000 en peu d'années.

Int : Pouvez-vous nous donner des prévisions concernant la mise en place des premières applications concrètes ?
PR : J'ignore quand elles interviendront.

Int : L'algorithme RSA est donc voué à être utilisé encore longtemps.
PR : Oui et non : nous ne savons pas montrer qu'il n'existe pas d'algorithme polynomial classique factorisant les entiers RSA. En quantique, ce n'est plus le cas avec l'algorithme de Shor. Si un ordinateur quantique universel voit le jour, il faudra probablement abandonner le RSA et le remplacer par un chiffrement plus

robuste. C'est l'objet du post-quantique, où de nouveaux algorithmes de chiffrement ont été proposés qui semblent pour l'instant pouvoir résister à un ordinateur quantique, sans l'avoir jamais démontré. La situation est donc similaire en classique avec le RSA : on l'utilise intensivement sans avoir démontré qu'il n'existe pas d'algorithme classique rapide (i.e. polynomial) de factorisation.

PD : Les GAFAM ont annoncé des applications pratiques. Leurs technologies sont-elles différentes ?
PR : A ma connaissance, Amazon, Google et IBM utilisent la technologie des circuits supraconducteurs, une technologie très similaire à celle d'Alice&Bob. Maintenant d'autres technologies concurrentes et très intéressantes existent comme celle de atomes froids et développée par la startup française Pasqal.

Int : Pourquoi, dans le jeu qui consiste à deviner un trésor qui se cache derrière l'une des trois portes (jeu de Monty Hall), le joueur double ses chances en changeant son choix initial après l'aide de l'animateur : les deux portes restantes ont une probabilité de 2/3 et 1/3 d'être devant le trésor, et non de ½ et ½ ?

PR : Au départ, le joueur ne dispose d'aucune information. Il pense donc que chaque porte correspond à une probabilité de 1/3. Après l'indication de l'animateur qui sait au départ derrière quelle porte est le trésor, la probabilité de 2/3 associée à l'ensemble des deux portes non choisies initialement pour le joueur, se concentre uniquement sur la porte non ouverte par l'animateur. Ainsi avec l'information dévoilée par l'animateur, le joueur change sa loi de probabilité : sur la porte initialement choisie reste à 1/3 ; celle non choisie et est restée fermée passe à 2/3. Il s'agit d'une mise à jour des probabilités selon la loi de Bayes. En quantique, c'est un peu similaire, la mesure donne une information et comme l'état quantique est associé à une loi de probabilité certes spécifique (probabilité non commutative correspondant à l'opérateur densité), il n'est pas étonnant de changer cette probabilité pour intégrer les dernières informations issues de la mesure : cette mise à jour correspond à la réduction du paquet d'ondes (collapse of the wave-packet).

Présentation des orateurs

Pierre Rouchon, ingénieur général des mines et membre de l'Académie des Sciences, est professeur à Mines Paris. Il fait partie de l'équipe Quantic (Mines, ENS, Inria, CNRS) qui travaille sur la mise au point d'un ordinateur quantique à base de codes correcteurs bosoniques et de circuits supraconducteurs.