AVIS D'EXPERT

Calcul quantique pour les applications dans l'aérospatial et la défense. État des lieux

Les besoins en matière de simulation numérique – en particulier dans la défense – exigent des puissances de calculs toujours plus importants, menant à l'adoption de machines exascales particulièrement gourmandes en consommation. Dans ce contexte, Alain Refloch (Onera) revient dans cet article sur les différents défis que l'ordinateur quantique devra relever.

Alain Refloch

Alain Refloch chargé de mission Calcul Haute Performance, responsable de l'axe calcul quantique du laboratoire Qtech de l'Onera

La simulation numérique est aujourd'hui omniprésente dans l'industrie, les grands industriels du monde aéronautique spatial et défense ont accès à des supercalculateurs soit en interne, en Cloud d'entreprise ou à travers des centres de calcul comme le CCRT. Les calculs réalisés sont loin d'être négligeables ; dans le domaine le plus consommateur qu'est la mécanique des fluides énergétique (domaine qui englobe l'aérodynamique et la combustion), on traite aujourd'hui couramment des maillages de 50 millions de cellules sur 2 000 cœurs de calcul. Cependant, les besoins en puissance de calcul sont toujours plus importants (maillages plus fins pour plus de précisions, temps physique de simulation plus longs, plus de calculs pour explorer plus de paramètres et plus récemment plus de calcul pour nourrir des bases de données destinés à l'apprentissage de modèles dans l'approche Deep Learning).

Néanmoins, l'augmentation de la puissance des processeurs stagne pour deux raisons. D'une part, il devient difficile d'augmenter la fréquence de processeurs car ceci a un impact direct sur la consommation électrique. D'autre part, les progrès technologiques ont conduit à réduire la finesse de gravure, impliquant d'augmenter le nombre de transistors sur une surface constante et donc la puissance de calcul potentiel… « potentiel » car accroître la puissance de calcul suppose aussi d'accroître l'accès à la mémoire, or si le nombre de cœurs de calcul n'a eu de cesse d'augmenter, le nombre de canaux mémoire n'évolue que très peu, provoquant un goulot d'étranglement.

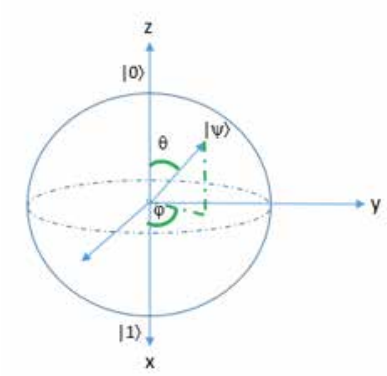
Disponibles à partir de 2024, les machines exascales affichent des consommations énergétiques de l'ordre de 20 Mw, ce qui représente en frais de fonctionnement annuels des dizaines de millions d'euros. Face à ces problèmes, l'ordinateur quantique apparait comme une technologie disruptive avec des promesses de gain exponentiel de puissance (mais seulement pour certains types de problèmes) avec une consommation électrique limitées à quelques dizaines de KWh.

RAPPEL

En calcul classique, on manipule des bits, états qui ne prennent que deux valeurs réelles : 0 et 1. C'est aussi le cas pour les qubits lorsqu'on fait la mesure de l'état mais pendant le calcul, la valeur du qubit (bit quantique) est représentée par un état $|\Psi>$, lequel

peut être représenté sur une sphère de rayon unité.

$|\Psi> = \alpha|0> + \beta|1>$, avec α et β nombres complexes et $\alpha^2 + \beta^2 = 1$ et une probabilité respective α^2 ou β^2 d'obtenir 0 ou 1



Un calcul quantique est donc probabiliste et nécessitera d'être reproduit un certain nombre de fois pour définir une distribution de la solution. Avec seulement n qubits, on peut représenter 2n états, rajouter 1 qubit à son système permet de multiplier par 2 la puissance de calcul.

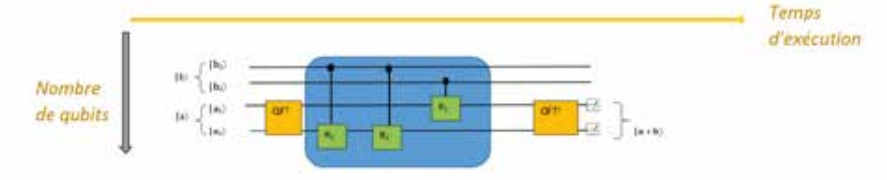
LA TECHNOLOGIE

Un grand nombre de technologies est susceptible de produire des états pouvant prendre comme valeur 0 ou 1 lors de leurs mesures. Mais quelle sera la meilleure technologie ? Si la question est encore ouverte, c'est qu'elles ont toutes des points forts mais aussi des points faibles. L'utilisation de qubits supraconducteur implique la production industrielle de ces qubits et donc potentiellement un coût de fabrication de l'élément de base et des problèmes de fiabilité d'un qubit à l'autre, ce qui n'est pas le cas si le qubit est à base d'atomes, d'ions ou de photons, ces ingrédients étant disponibles naturellement.

Disposer de qubits est une chose mais les manipuler et les associer entre eux en est une autre. C'est donc un ensemble d'éléments à prendre en compte (temps de relaxation et de décohérence, fiabilité de lecture, rapidité des opérations, variabilité, nombre de qubits intriqués, passage à l'échelle – comment on arrive à augmenter le nombre de qubits sans perte de fiabilité et de flexibilité). Il est fort probable qu'en fonction du problème ciblé, plusieurs technologies spécialisées soient présentes sur le marché. Notons qu'il existe sur le plateau de Saclay un vivier de start-up de tout premier plan (telles qu'Alice et Bob, C12, Quandela, Pasqal).

LA PROGRAMMATION

Comme le calcul classique, un calcul quantique universel se programme sous forme de porte. On a essayé de regrouper dans la figure ci-dessous la problématique :



Les lignes noires représentent les qubits (ici 4) ; le circuit pourrait représenter une addition. On fait la somme de deux entiers valant respectivement 1 et 2 (en représentation binaire avec deux bits, on peut représenter 22 valeurs (0=00, 01=1, 10=2 et 3=11)) ; ainsi a1 et a2 seraient utilisés pour coder a et b1, b2 pour coder b. En sortie, la somme étant 3, elle peut être aussi codée sur 2 bits. On aurait pour la partie mesure, représentée par les 2 petits ampèremètres comme mesure 1 et 1 (soit 11 en binaire =3)). Les portes vertes Ri sont des rotations et le rond noir désigne des portes contrôlées (si le 1er bit de contrôle est à |0> , on ne fait rien ; s'il est à |1> , on applique la porte). Les boites orange sont des portes à deux entrées (deux qubits) ; ici, QFT veut dire que l'on applique une Transformée de Fourier Quantique.

Il faut garder à l'esprit qu'un ordinateur quantique a besoin d'un algorithme quantique pour donner un gain ; reproduire un algorithme classique brute de force sur un ordinateur quantique n'a pas de sens. En raison des contraintes (nombre de qubits disponible et cohérences du système), le jeu consiste à trouver l'algorithme qui demande le moins de qubits et le moins de portes. Il existe aujourd'hui des start-up qui travaillent sur l'algorithmique quantique (par exemple ColibriTD).

OÙ EN EST-ON ?

On peut commencer dès aujourd'hui à prendre le sujet en main à travers des simulateurs, soit lié à un hardware propriétaire comme Perceval pour Quandela ou la QLM d'Atos qui est agnostique hardware et qui permet d'optimiser son circuit ; celui-ci représente un algorithme et permet de tester sa robustesse en simulant le bruit.

Si un calcul classique n'est pas limité en temps (mises à part des contraintes de production de la machine), un calcul quantique doit se faire dans un temps très court, le temps où le système quantique est cohérent. Le problème de correction des erreurs est un problème difficile à traiter en quantique. Cette problématique des erreurs a conduit à définir deux grandes périodes dans l'évolution du calcul quantique. D'une part, la période NISQ (Noisy Intermediate-Scale Quantum), où nous nous trouvons ; elle consiste à rechercher des problèmes qui pourraient être résolus avec un avantage par rapport à l'ordinateur classique en utilisant un nombre de qubits bruités limités (~100). D'autre part, la période LSQ (Large Scale Quantum) qui permettra de traiter des problèmes plus industriels (après 2030)

où les algorithmes manipuleront des qubits logiques (qubits sans erreurs) qui utiliseront un très grand nombre de qubits physiques pour réaliser le calcul.

Un ordinateur quantique, c'est un ordinateur. On pense donc à ses deux composants que sont la partie calcul, le CPU et la mémoire RAM. Dans le cas d'un ordinateur quantique, on parle de QPU et de QRAM ; cependant, les travaux sur les mémoires quantiques sont bien moins avancés que la partie calcul. Autrement dit, il n'existe pas à ce jour de mémoire quantique. C'est l'une des raisons pour laquelle on parle actuellement d'accélérateur quantique et non plus d'ordinateur quantique (à l'image des accélérateur GPU dans le calcul classique). De même, on parle de calcul hybride, à savoir une partie du calcul se faisant sur un ordinateur classique et une partie sur l'accélérateur quantique. Lorsque l'on parle d'ordinateur classique, on sous-entend malgré tout un super calculateur (le traitement d'un problème mettant en œuvre 50 qubits, représente 250 états qui demanderaient pour être stocké presque 1 Poctets).

L'ÉCOSYSTÈME

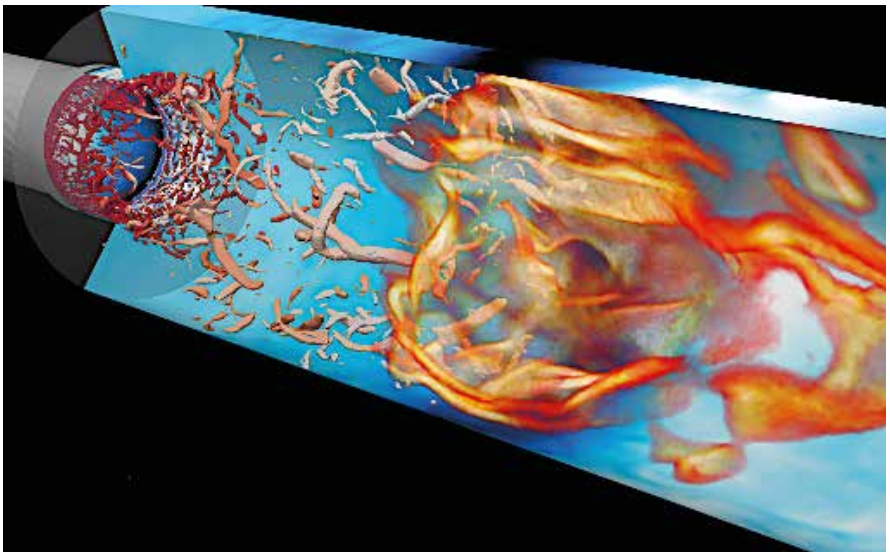
L'écosystème est favorable. Les financements au niveau national sont disponibles à travers le plan quantique annoncé par le Président de la République en janvier 2021, mais qui était plus que nécessaire en raison de la forte compétition internationale ; il existe en effet un plan quantique allemand ; aussi, la Chine et les États-Unis mènent des investissements colossaux dans le domaine. Pour ces derniers, les investissements sont aussi largement portés par le privé (Google par exemple). La région Île-de-France est très active dans le domaine du calcul quantique où il existe des projets Pack IdF sur le sujet et un DIM (Domaine d'intérêt majeur) QuantIP.
Le sujet de la suprématie quantique fait toujours l'objet d'annonce et de contre-annonce (Google/IBM) en raison des enjeux financiers, mais ce qui importe vraiment aux utilisateurs, c'est d'effectuer un calcul utile apportant un plus : faire un calcul en un temps identique mais avec un gain financier sur le coût de calcul, obtenir une solution qui n'est pas la meilleure en absolue mais meilleure que celle de la concurrence.

LES APPLICATIONS

Il existe un ensemble d'algorithmes quantiques ayant des débouchés dans un grand nombre de domaines : recherche de chemin optimal, marche quantique, algèbre linéaire, moindre carré… Pour le domaine aéronautique spatial et défense (en dehors de la cryptographie qui est un sujet à part entière), il existe de nombreux sujets où un gain est attendu : le traitement des données (au bémol près du passage de données du monde « réel » en état quantique), la détection d'anomalies, la prise de décision, la planification de missions (rover…), l'optimisation pour le calcul haute performance classique (placement de tâches, partitionnement de maillage), processus de vérification/validation, placement optimum de capteurs, radars, satellites, management du trafic aérien (avions, drones, satellites…), prédiction et génération de nouveaux polymères, application pour la robotique (diagnostique, perception…).

Les sujets aujourd'hui traités par l'IA sont de bons candidats au calcul quantique (système de recommandation, traitement d'images, réseaux de neurones, apprentissage par renforcement, télédétection, …). À court terme, le gain attendu se porte plutôt sur les problèmes d'optimisation combinatoire. Mais plus un sujet est consommateur de ressources, plus le gain du calcul quantique sera important… et c'est bien ce qui motive les recherches autour de la résolution des équations différentiels (CFD, Combustion).

CONCLUSION

L'aventure du calcul quantique en est à ses débuts, et le chantier est de taille, développement technologique sur les qubits, sur la QRAM, informatique au sens création de langage plus adapté à la programmation quantique, optimisation des circuits pour en réduire la profondeur, et bien entendu le développement de l'algorithmique quantique •

Alain Refloch (Onera)