Informatique quantique, les raisons de l'engouement

DevCon#10 *Programmez!* - spéciale Informatique quantique, 24 mars 2021

Benoît Prieur - Soarthec -

Présentation succincte

Benoît Prieur, développeur logiciel

Rapport à l'informatique quantique :

- *Informatique quantique - de la physique quantique à la programmation quantique en Q#*. Éditions ENI, 2019, ISBN : 978-2409021688, 244 p. lien
- [WEBINAIRE] Introduction à l'informatique quantique, Éditions ENI, mai 2019, 48', disponible sur Youtube, lien
- Chargé de cours, travaux pratiques d'informatique quantique à l'ECE Paris (école d'ingénieurs) à l'automne 2019
- « Programmation quantique : comprendre l'essentiel pour écrire et exécuter ses premiers programmes avec IBM QisKit ». *Programmez!*, 2020, numéro 239, pp.39-41, lien

Une accélération de la couverture presse depuis 2018

- Presse spécialisée (informatique, sciences, vulgarisation scientifique).

Mais aussi :

- Presse généraliste et presse économique.
  - *Angles fréquemment repris :*
    - Enjeux stratégiques.
    - Course à la machine quantique (nombre de qubits d'une machine opérationnelle).
    - Suprématie quantique.

Angles fréquents
(presse économique ou généraliste)

- Enjeux stratégiques :
  - Course technologique entre États et/ou multinationales.
  - Dispositions nationales ou supra-nationales : pôle de compétitivité, projets européens etc.
- Course à la machine quantique et suprématie quantique :
  - Annonces de constructeurs (communiqués de presse).
  - Peu de mise en perspective.
  - Flou sur la notion de suprématie quantique :
    - Instance de problème à résoudre et nombre de qubits.
    - Nécessite de connaître les quelques fondamentaux rarement évoqués dans les articles.

Informations fréquemment omises
(presse économique ou généraliste)

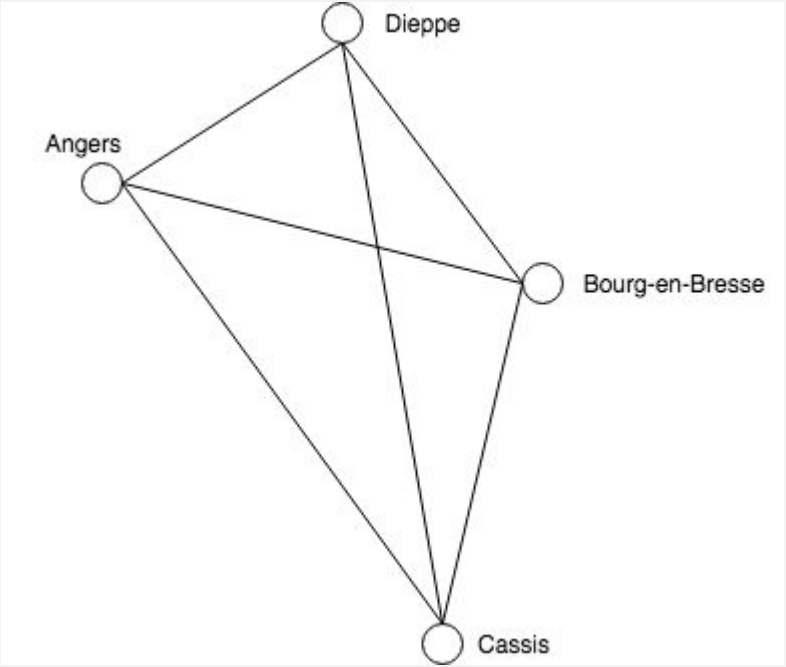
- L’informatique quantique utilise les fondements de la physique quantique ; mais le fait que la physique quantique correspond à la physique de l’infiniment petit n’est que rarement expliqué.
- Parmis ces fondements, la superposition quantique offre une combinatoire à même d’envisager la résolution de problèmes difficiles ou impossibles à résoudre aujourd’hui.
- Le fait que des catégories de problèmes sont impossibles à résoudre encore aujourd’hui par l’informatique classique est omis (d’autant que la rhétorique à propos de l’intelligence artificielle et du big data pourrait laisser penser le contraire).
- La mise à disposition d’une machine quantique n’exonère pas de créer un algorithme quantique spécialement pour le problème à résoudre.
- L’informatique quantique ne remplace pas l’informatique classique ; cette dernière délègue à l’informatique quantique la résolution d’un problème donné.

Des problèmes difficiles à résoudre. Comment les caractériser ?

- En informatique classique : notion de complexité.
- Plusieurs types de complexité.
- On se limite ici à celle qui consiste à déterminer le nombre d'itérations nécessaires d'un algorithme à partir du nombre d'entrées *n*.
    - On utilise pour expliciter cette complexité la notation de Landau (grand O).
- Ainsi à partir du nombre d'échantillons *n*, on détermine si la complexité est plutôt polynomiale ou exponentielle.
- Prenons un exemple de problème : le voyageur de commerce.

Complexité et problème dit du voyageur de commerce

- Trouver le plus court chemin, en passant une fois et une seule par chaque ville (A, B, C, D).
- Ici, $n = 4$.
- Première approche, examiner chaque chemin.
- Nombre de chemins différents : $(n-1)! / 2$; on divise par 2 car on ne tient pas compte de l'orientation du graphe.
- En notation de Landau : $O(n!)$



Le voyageur de commerce : plus loin dans la caractérisation

- Prenons une instance de ce problème tel que $n = 20$.
- Considérons que chaque chemin s'examine en 1 microseconde.
- Il faut alors 115 jours pour déterminer de façon exacte le plus court chemin.
- Si l'on considère le nombre total de chemins, $(20 - 1)! / 2$ et que l'on songe à utiliser la combinatoire de l'informatique quantique (*cf.* superposition) avec 2^k étant égal à ce nombre de chemins et k le nombre de qubits. On obtient $k = 55$.
- Aujourd'hui cela reste un nombre de qubits élevés, mais l'on voit qu'il y a là une puissance probable de résolution de manière exacte des problèmes (rappel : exemple à 20 villes).

Simplification des problèmes et solutions approchées

- Le problème du voyageur de commerce illustre l'impossibilité d'obtenir une solution exacte (informatique classique) alors même que ce type de problème correspond à des problématiques concrètes (industrie, santé, militaire, etc.).
- Recours à des heuristiques (algorithmes visant une solution approchée).
- En Machine Learning, on ignore les paramètres les moins influents pour avoir un temps de calcul raisonnable en production (prédiction).

Les classes de problèmes comme marqueur des problèmes à visée stratégique

- **Classe P** : problème qui peut être résolus en un temps polynomial.
- **Classe NP** : problème décidable en un temps polynomial (exprimé autrement une solution possible est vérifiée en un temps polynomial).
- Il est assez intuitif de déduire que P est inclus dans NP.
- Par contre la réciproque reste à démontrer (probablement fausse) : conjecture du siècle (P = NP ?).
- **Classe NP-complet**, deux conditions :
    - Le problème est NP.
    - Tous les problèmes NP sont réductibles en ce problème, par une réduction polynomiale.
    - Exprimé autrement, si on pouvait trouver une résolution de NP-complet en un temps polynomial (probablement impossible en informatique classique), on pourrait résoudre polynomialement tout NP.

Cette classe de problèmes correspond à des problématiques humaines à fort enjeux

- Problème d'optimisation, à forte combinatoire, santé (génome), théorie des graphes (stratégie), planification et ordonnancement (industrie). Mais également échanges bancaires, cryptographie, blockchain (smart contract, minage).
- Les limites de l'informatique classique face à ce type de problèmes induisent à elles seules l'engouement pour l'informatique quantique.
- C'est la clé de la résolution de problèmes, à grand nombre d'entrées, à forte combinatoire, dans des secteurs stratégiques pour les organisations humaines.
- Big Data + Informatique quantique maîtrisée => omniscience des décisions (?).

Merci de votre attention :)

- Merci à François Tonic et au magazine *Programmez!* pour l'organisation de cette DevCon#10.
- Remarques, questions, compléments.