Opinions Libres
le blog d'Olivier Ezratty

Decode Quantum avec Frédéric Magniez de l'IRIF et du Collège de France

Pour ce **48e épisode** de rentrée scolaire des entretiens **Decode Quantum**, toujours coproduits avec Frenchweb, j'accueille **Frédéric Magniez** du laboratoire IRIF et du Collège de France. Je suis sans **Fanny Bouton** qui est de plus en plus occupée chez **OVHcloud** maintenant qu'ils ont annoncé officiellement qu'ils s'intéressaient de près aux technologies quantiques mais elle nous reviendra bien entendu dans les prochains épisodes.

*Crédit photo : **Collège de France**.*

Frédéric Magniez est ancien élève de l'Ecole Normale Supérieure Paris-Saclay (ex ENS Cachan), agrégé de mathématiques et docteur en informatique. Il est entré au CNRS en 2000, au Laboratoire de Recherche en Informatique (LRI). Il rejoint en 2013 l'Institut de Recherche en Informatique Fondamentale (IRIF) qu'il dirige depuis 2018. Il a également été professeur associé de l'École Polytechnique de 2003 à 2015. Il travaille sur la conception et l'analyse d'algorithmes probabilistes pour le traitement des grandes masses de données, ainsi que sur le développement de l'informatique quantique et plus particulièrement des algorithmes, de la cryptologie et ses interactions avec la physique.

Il est aussi titulaire de la chaire Informatique et sciences numériques au Collège de France pour 2020-2021. On vous recommande de visionner les **8 séances de 3 heures** de 2021 en plus d'une séance inaugurale, avec quelques intervenants invités que nous avons déjà reçus dans Decode Quantum : Iordanis Kerenidis, Eleni Diamanti, Jonas Landman, Elham Kashefi, Simon Perdrix.

Synopsis

Voici les principaux éléments de cet entretien :

- Comment il est tombée dans la **marmite du quantique** ? Il nous raconte la préparation d'un mémoire sur l'argent quantique et ses rencontres avec Claude Crépeau (Canadien), un pionnier de la cryptographie ainsi qu'avec Alain Faquel et Gilles Brassard, qu'il a rencontrés alors qu'il était en master. A la fin de son mémoire, il rencontre aussi Serge Haroche qui démarre ses expériences qui mèneront à son prix Nobel décernée en 2012.

- Il réalise un DEA/Master en 1995 sur le **calcul quantique**. Il s'intéresse notamment aux algorithmes probabilistes et aux preuves holographiques. Comment vérifier au hasard par échantillonnage qu'un algorithme a généré de bon résultats. Il évoque le théorème PCP qui est utilisé en cryptographie.

- Sa rencontre avec **Miklos Santha** (actuellement à Singapour dans le laboratoire MajuLab du CNRS et au CQT) au sujet de la machine de Turing quantique. C'est pendant la rédaction de son mémoire que le fameux algorithme de factorisation de Peter Shor est créé.

- A l'époque, Frédéric pensait avoir résolu un problème dans la hiérarchie polynomiale et avoir démontré que l'ordinateur quantique allait résoudre tous les problèmes de niveau 2 (au sens NP). Mais le résultat était faux.

- Il a continué de travailler sur des **algorithmes plus classiques**, sur les preuves dites holographiques, les auto-tests, les auto-tests "device independent". Il a travaillé avec Dominique Mayers.

- Nous évoquons ensuite différentes **classes d'algorithmes quantiques**. Le rôle de la transformée de Fourier quantique. Les problèmes à Oracle. Les classes de complexité P vs NP. L'algorithme de Bernstein-Vazirani. Nous revenons sur la définition de ce qu'est qu'un algorithme quantique. Ce sont des programmes avec des instructions qui agissent sur une mémoire quantique. Ils transforment un problème difficile pour un ordinateur classique en un autre problème résolu de manière plus rapide sur ordinateur quantique. Un algorithme quantique ne comprend pas forcément beaucoup d'instructions. La résolution d'isomorphismes de graphes, utile en Chimie.

- La notions de **gains polynomiaux et exponentiels**. Quand arrive l'avantage exponentiel ? Cela dépend de la taille du problème. Il est important d'étudier les comportements asymptotiques des algorithmes.

- Comment se créer une **image mentale** d'un algorithme quantique ? Le calcul probabiliste aide à la compréhension. Il faut raisonner avec un grand nombre de dimensions. Les notions d'analyse spectrale, avec la transformée de Fourier quantique. Les algorithmes récursifs et la recherche de structures compliquées. Les algorithmes quantiques distribués. L'algorithme HHL et la résolution de système linéaire. La matrice de départ n'est pas forcément unitaire. Le paradoxe de la création d'une exponentielle de matrice !

- Comment **enseigner la programmation** d'un ordinateur quantique ? Faut-il connaître la physique quantique ? Quels sont les prérequis ? Son enseignement à l'Ecole Polytechnique où il se partage les rôles avec Philippe Grangier qui couvre la physique quantique.

- Les simulations quantiques pour simuler des Hamiltoniens de systèmes physiques complexes.

- Ingéniérie logicielle : vérification, certification, debug ? En quoi est-ce différent dans le quantique ?

- Comment s'y retrouver entre **émulation** et **simulation** quantique ?

- Un point sur le laboratoire **IRIF** qu'il dirige qui associe le CNRS, l'Université Paris Cité (ex Diderot + Descartes) et l'équipe Picube d'Inria. Avec une centaine de permanents, 200 personnes en tout, réparties dans 9 équipes de recherche. Ils couvrent tous les concepts informatiques, les fondements de l'informatique, un pilier sur les langages de programmation, sur les questions de vérification, les liens avec d'autres sciences, comme pour le quantique, les liens avec la physique quantique. Le laboratoire travaille aussi sur l'explication du vivant, sur sa modélisation algorithmique, ainsi que sur l'explication des trous noirs. Iordanis Kerenidis et lui-même sont dans l'équipe qui travaille sur algorithmes et complexité. Ils ont 4 permanents dans le cœur du quantique et une quinzaine en tout à s'intéresser au quantique.

Voilà pour cet épisode !

Rendez-vous au suivant !

Cet article a été publié le 31 août 2022 et édité en PDF le 1 septembre 2022.
(cc) Olivier Ezratty – "Opinions Libres" – **https://www.oezratty.net**