DOSSIER DE PRESSE – PARIS, le 17-03-2021

Algorithmes quantiques : quand la physique quantique défie la thèse de Church-Turing

- Leçon inaugurale de Frédéric Magniez : le jeudi 1er avril 2021 à 18h00 –

***en direct* sur notre site internet**

Chaire annuelle *Informatique et sciences numériques* 2020-2021 du Collège de France

Frédéric Magniez, mathématicien et informaticien, est directeur de l'Institut de recherche en informatique fondamentale (www.irif.fr) et directeur adjoint de la Fondation des sciences mathématiques de Paris. Ses travaux de recherche portent 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 les algorithmes, la cryptographie et ses interactions avec la physique. Il est invité à occuper la chaire ***Informatique et sciences numériques*** **2020-2021** du Collège de France, créée en 2009 en partenariat avec Inria.

Il prononcera sa leçon inaugurale « **Algorithmes quantiques : quand la physique quantique défie la thèse de Church-Turing** », le **jeudi 1er avril 2021, à 18h**. Celle-ci sera retransmise **en direct** sur le site internet du Collège de France et ne sera pas ouverte au public, au vu des conditions sanitaires en vigueur.

Son cours sur l'algorithmique quantique au Collège de France, ouvert à tous, commencera le 7 avril 2021. Frédéric Magniez organisera également un colloque international sur ces questions le 16 juin 2021.

Tous les calculs informatiques sont actuellement exécutés sur des ordinateurs contraints par les lois de la physique newtonienne, dite encore physique classique. Cependant, comme l'a suggéré Richard Feynman dans les années 80, un ordinateur quantique pourrait tirer profit des phénomènes de superposition et d'intrication de la physique quantique afin d'accélérer ses calculs. Alors que des prototypes d'ordinateur quantique encore très limités voient progressivement le jour, startups, grandes entreprises du numérique, et aussi gouvernements orientent peu à peu leur recherche, stratégie et financement afin d'être prêts à exploiter le potentiel de ce futur ordinateur.

Alors que la France a officiellement lancé son Plan Quantique national en janvier 2021, la leçon inaugurale et le cours prononcé dans le cadre de cette chaire présenteront les fondements de la cryptographie et de la communication quantiques, en partant des premiers paradoxes quantiques. Frédéric Magniez introduira également ses auditeurs aux concepts du calcul quantique par le biais des circuits, qui permettront de présenter les principales méthodes algorithmiques quantiques : mise en évidence de propriétés algébriques permettant de déchiffrer les messages secrets, et optimisation ouvrant la voie à un vaste champ d'applications algorithmiques. Il abordera également les limites du calcul quantique, qu'elles soient théoriques ou liées aux technologies actuelles. Enfin, il décrira comment une partie de la recherche actuelle est motivée par l'utilisation à court terme de prototypes d'ordinateurs quantiques limités, mais pouvant potentiellement trouver des applications concrètes, comme notamment en intelligence artificielle ou encore en usage décentralisé de type Internet.

L'enseignement de Frédéric Magniez est ouvert à tous, sans aucune condition d'inscription ni de diplôme, selon la vocation du Collège de France. Il sera librement disponible sur notre site internet sous forme de captations audiovisuelles.

Frédéric Magniez, 2020. Crédits : Patrick Imbert, Collège de France

Ressources complémentaires :

Texte original de présentation par Frédéric Magniez ci-dessous inclus dans le dossier de presse, pouvant faire l'objet de reprise.

Vidéo de présentation de Frédéric Magniez (4 minutes) :
https://www.college-de-france.fr/site/frederic-magniez/Lecon-inaugurale-du-Pr-Frederic-Magniez.htm
Pages de Frédéric Magniez sur le site internet du Collège de France :
https://www.college-de-france.fr/site/frederic-magniez/index.htm

Lien de retransmission en direct de la leçon inaugurale du 1er avril 2021 :
https://www.college-de-france.fr/site/frederic-magniez/inaugural-lecture-2020-2021.htm

Article sur les travaux de Frédéric Magniez dans *CNRS le journal*
https://lejournal.cnrs.fr/articles/une-informatique-a-reinventer-pour-le-calcul-quantique

Site de l'Institut de recherche en informatique fondamentale
https://www.irif.fr/

Liste des chercheurs invités depuis 2009 sur la chaire Informatique et sciences du numérique, en partenariat avec Inria
https://www.college-de-france.fr/site/chaires-annuelles/Chaire-Informatique-et-sciences-numeriques.htm

CONTACT PRESSE :
David Adjemian, chargé de la presse et de la communication
06 38 54 80 87 – presse@college-de-france.fr
www.college-de-france.fr
@cdf1530

Algorithmes quantiques
Quand la physique quantique défie la thèse de Church-Turing

par Frédéric Magniez

NB : ce texte original de Frédéric Magniez peut librement être repris par les organes de presse, sous réserve de la mention de l'auteur et de l'occasion (leçon inaugurale de la chaire annuelle Informatique et sciences numériques du Collège de France – 1er avril 2021).

Une prouesse inutile ?

L'année 2021 sera sans aucun doute quantique ! Il y a à peine plus d'un an, Google réalisait un calcul sur un prototype de circuit quantique programmable. D'un point de vue technologique la prouesse était encore inimaginable il y a seulement quelques années. D'un point de vue de la puissance de calcul, la tâche demandée est certes très spécifique, mais nécessiterait plusieurs milliers d'années de calcul sur tout autre machine existante, aussi puissante soit-elle ! Un vrai tournant venait donc d'être engagé. Cette année, un consortium européen va lancer une plateforme de simulation et de programmation quantique rassemblant chercheurs et industriels issus de la physique et de l'informatique. Cette plateforme utilisera une technologie quantique fournie par la start-up française Pasqal. Enfin, l'État va lancer un plan national quantique qui va voir la création de plusieurs centres dédiés à la recherche sur les technologies quantiques, dont l'informatique.

Le calcul effectué par Google fin 2019 revenait à lancer un gigantesque dé truqué ou faussé. Le calcul des probabilités de chaque face du dé est lié au circuit quantique programmé dans la machine de Google. La simulation d'un circuit quantique, même de petite taille (53 bits dans l'expérience de Google), est d'une telle complexité pour nos ordinateurs actuels qu'elle ne peut être réalisée en moins de plusieurs millénaires par ces derniers. En revanche, le lancé de ce dé est quasiment instantané sur le prototype quantique de Google, puisque ce dernier implémente directement ledit circuit quantique, et ce avec une précision satisfaisante, c'est-à-dire pour vérifier que le bon dé avait été lancé. Cette réalisation, même imparfaite, semble pour le moment impossible à réaliser autrement que quantiquement.

Cette prouesse semble loin de toute application pratique. Néanmoins, elle valide un courant de pensée remontant aux années 1980, en particulier aux propos de Feynman, affirmant que notre interprétation et compréhension de ce qui est calculable devait évoluer. Elle remet en cause les fondements du calcul remontant à la thèse de Church-Turing. Cette thèse, qui a évolué au fil des années, tendait à affirmer que tout progrès technologique ne remettrait jamais en cause le modèle mathématique du calcul défini par Church et Turing en 1936. Ce modèle permet de discerner ce qui est calculable par une machine de ce qui ne l'est pas. Quelques décennies après, cette thèse avait été reformulée ainsi : tout modèle de calcul raisonnable peut être simulé efficacement par une machine de Turing probabiliste (i.e. ayant accès à une source d'aléa). La notion de complexité y avait donc été ajoutée, rendant la thèse plus ambitieuse mais aussi plus fragile.

Les fondations - Enigma bis ?

Cette thèse étendue de Church-Turing a donc été remise en question au tout début de l'informatique quantique, lorsque Deutsch définit en 1985 la notion de machine de Turing quantique, avec son lot de premiers algorithmes exponentiellement plus rapides que leurs équivalents déterministes (mais pas encore probabilistes). D'abord perçu comme une curiosité, ce modèle de calcul finit par susciter intérêt et questionnements dans la communauté scientifique. Finalement en 1993, Bernstein et Vazirani construisent mathématiquement une machine universelle quantique efficace, c'est-à-dire le premier

compilateur quantique (l'existence d'une machine programmable) qui valide mathématiquement le modèle de calcul (mais pas sa réalisation physique). En même temps arrive l'évidence qu'un ordinateur quantique peut être exponentiellement plus rapide qu'un ordinateur classique, i.e. qu'une machine de Turing probabiliste. Cependant les problèmes résolus sont tous artificiels et semblent encore bien loin de toute application concrète.

C'est Simon puis Shor qui arrivent avec la première application algorithmique, et pas des moindres, en 1994, soit seulement une année après l'acceptation par la communauté du concept même de calcul quantique. En effet, cette application permettait de déchiffrer la plupart des messages cryptés par les mécanismes dits à clé publique, et de réduire à néant les procédés cryptographiques les utilisant (monnaie électronique, CB, vote électronique, authentification, ...). Heureusement, l'ordinateur quantique n'existe pas (encore) ! Pourtant cette découverte n'est pas sans rappeler les découvertes de Turing et la construction de la machine qui a permis de déchiffrer les messages allemands eux-mêmes chiffrés par la machine Enigma durant la deuxième guerre mondiale…

Les algorithmes quantiques - Une nouvelle façon de penser

Néanmoins, deux décennies plus tard, alors que la possibilité d'une construction future d'un ordinateur quantique commençait à être prise au sérieux, une compétition scientifique internationale a été lancée en 2016 afin de définir les nouveaux standards de chiffrement post-quantique, ouvrant la voie à une longue recherche puis standardisation toujours en cours. Une autre alternative repose pourtant dans l'utilisation relativement simple de fibre optique afin de communiquer en encodant l'information directement sur des photons. Il s'agit du protocole quantique d'échange de clé proposé par Bennett et Brassard en 1984, soit 10 années avant la découverte de l'algorithme de Shor. En quelque sorte l'attaque et la parade reposent sur la même technologie, à ceci près que le protocole en question a déjà été construit et testé sur de grandes distances, un satellite dédié à même été envoyé par la Chine en 2016. L'Europe n'est pas en reste avec des projets d'infrastructure de grande envergure dédiés au déploiement de solutions quantiques de chiffrement. Cependant ces solutions quantiques nécessitent des technologies spécifiques, alors que les solutions algorithmiques dites post-quantiques pourraient être déployées sur les structures et ordinateurs actuels.

Depuis 1994, les applications (calcul scientifique, optimisation, recherche opérationnelle, simulation, apprentissage automatique, IA…) foisonnent dans tous les domaines où l'informatique joue un rôle crucial, et pour des tâches où nos ordinateurs actuels ne sont pas assez puissants. Mais surtout les outils développés (transformée de Fourier quantique, estimation de phase, amplification d'amplitude, estimateur quantique, marche quantique, …) progressent continuellement, impactant toutes les thématiques de l'informatique, en en créant de nouvelles (information quantique, complexité hamiltonienne, simulation quantique, …), ou encore en tissant de nouveaux liens de l'informatique vers d'autres disciplines dont la physique, la chimie et les mathématiques.

Mais avant tout l'informatique quantique a introduit une nouvelle façon d'analyser, raisonner et démontrer. Les outils existants précédemment n'étant plus adaptés, il a fallu en créer de nouveaux. Apportant un nouveau regard mathématique à des questions anciennes, ces nouveaux outils ont permis de progresser sur des questions ouvertes depuis de nombreuses années. Cette démarche a été baptisée preuve ou méthode quantique. Une preuve quantique est un peu l'analogue des nombres complexes pour la trigonométrie ou encore l'électricité : un outil très puissant permettant de mener facilement des calculs difficiles, ou encore d'établir des preuves inaccessibles jusque là, y compris dans des domaines pour lesquels ils n'ont pas été construits initialement. La dernière démonstration en date est la réfutation d'une célèbre conjecture en mathématiques (conjecture de Connes) à l'aide d'un résultat en théorie de la complexité quantique.

Vision et formations nécessaires

Une fois tous ces algorithmes quantiques découverts, dont l'utilisation de certains serait à n'en pas douter révolutionnaire, la question de la possibilité de construire un ordinateur les exécutant fut donc de plus en plus pressante. L'importance d'un plan d'envergure a d'abord émané de tous les acteurs concernés, scientifiques comme industriels, avec une feuille de route et des jalons intermédiaires appropriés, puis fut largement soutenue par les politiques. Plusieurs plans ont vu le jour, dont un au niveau européen à travers le Quantum Flagship en 2018, et le Plan Quantique national en 2021. L'avantage industriel que pourrait procurer la construction d'un ordinateur quantique, même imparfait, a créé une frénésie stimulante qui touche tous les secteurs stratégiques (finance, industrie, santé, sécurité…). Les progrès technologiques de grands groupes industriels, tels que Google et IBM par exemple, ont été de véritables locomotives, laissant apparaître rapidement que le plus grand défi serait de trouver une application à ces premiers prototypes, certes révolutionnaires, mais très éloignés des machines nécessaires aux applications précédemment découvertes en algorithmique quantique. En effet, non seulement ces machines sont petites, mais elles ont un taux d'erreur encore trop grand. Pourtant elles sont capables d'effectuer des calculs impossibles à réaliser classiquement, mais des calculs sans impact industriel actuellement.

Un véritable travail de fourmi s'est donc enclenché, mais, pour l'instant, avec une communauté encore trop petite. Les mêmes personnes ont actuellement en charge de comprendre et de maîtriser toutes les facettes du calcul quantique, de la modélisation à la réalisation expérimentale en passant par la solution algorithmique, son analyse, sa programmation et sa vérification, là où la chaine de production constitue habituellement un véritable écosystème de l'informatique. Il nous faut donc nouer de multiples partenariats, construire et enseigner dans de nouvelles formations, afin de saisir cet unique défi que pourrait constituer ce nouveau tournant technologique.

C'est dans ce contexte que le Collège de France m'a donc invité à occuper pour un an sa chaire Informatique et sciences numériques, et à donner dans ce cadre un cours sur les algorithmes quantiques. Ce cours tâchera de répondre à une demande croissante d'information et de formation de nombreux publics. Le public ciblé va des esprits curieux de saisir les possibilités et les limites du calcul quantique, aux acteurs des sciences informatiques au sens large : informaticiens, mathématiciens du numérique et physiciens des technologies quantiques, qu'ils soient étudiants, chercheurs, développeurs, entrepreneurs ou encore futurs utilisateurs des algorithmes quantiques.

En guise de conclusion, il convient de rappeler que c'est en France, en 1980, qu'a débuté la révolution quantique expérimentale lorsque l'expérience du groupe d'Alain Aspect (CNRS) a validé à Orsay les prédictions de la physique quantique, qui ne pouvaient s'expliquer par la physique classique seule. Puis le prix Nobel a été décerné en 2012 à Serge Haroche (Collège de France) pour ses travaux sur la manipulation de systèmes quantiques. Le versant informatique de cette révolution a, lui, débuté en 1994 conjointement aux travaux outre-Atlantique, grâce à la vision de Miklos Santha (CNRS). Alors étudiant de master, j'ai suivi le mouvement de son équipe, qui était basée aussi à Orsay. Rapidement, Miklos a su constituer un groupe qui essaime, fait des émules en France et attire des talents internationaux. A l'époque, le pari pouvait sembler risqué, mais dans les années 2000, les possibilités de recrutement au CNRS et à l'Université sont plus nombreuses, et plusieurs chercheurs sont recrutés afin de mieux comprendre les liens que tisse le traitement de l'information quantique entre informatique, mathématiques et physique.

Frédéric Magniez

Biographie de Frédéric Magniez

Ancien étudiant de l'ENS Cachan, Frédéric Magniez est agrégé de mathématiques et docteur en informatique. Sa thèse reçoit le prix de l'Association Française d'Informatique Théorique en 2000. Il devient ensuite chercheur au CNRS et travaille à l'Université Paris Sud, avant de rejoindre l'Institut de Recherche en Informatique Fondamentale (IRIF) à l'Université de Paris en 2010. Ses travaux de recherche portent sur la conception et l'analyse d'algorithmes probabilistes pour le traitement des grandes masses de données, ainsi que le développement de l'informatique quantique et plus particulièrement les algorithmes, la cryptographie et ses interactions avec la physique.

Professeur à l'École Polytechnique de 2003 à 2015, Frédéric Magniez co-construit le premier cours de l'école dédié à l'informatique quantique. Il crée et anime en 2006 le groupe de travail national d'Informatique quantique, qui rassemble actuellement 20 équipes de recherche. De 2013 à 2017, il dirige l'équipe Algorithmes et Complexité, dont la recherche en informatique quantique est mondialement reconnue. En 2015, il devient directeur adjoint de la Fondation des Sciences Mathématiques de Paris, un réseau d'excellence regroupant 1 200 chercheurs en sciences mathématiques et informatiques, avant de prendre la direction de l'IRIF en 2018.

Enseignements 2020-2021 de Frédéric Magniez au Collège de France :

Cours : *Algorithmes quantiques*

7 avril 2021 : *Information quantique, premières utilisations calculatoires : superposition, mesure, transformation, non-clonage, distribution quantique de clés.*

7 avril 2021 : séminaire d'Eleni Diamanti : *Réseaux de communication quantique*

14 avril 2021 : *Cryptographie et communication quantiques : inégalités de Bell, tirage à pile ou face, mise en gage, certification*

14 avril 2021 : séminaire de Thomas Vidick : *Certifier la génération de nombres aléatoires avec le quantique*

5 mai 2021 : *Circuits quantiques, premiers algorithmes : portes universelles, algorithmes de Deutsch-Jozsa et Bernstein-Vazirani, supériorité des algorithmes quantiques*

5 mai 2021 : séminaire de Simon Perdrix : *Langages graphiques pour programmer et raisonner en informatique quantique*

12 mai 2021 : *Transformée de Fourier quantique I : réalisation, estimation de phase, algorithmes de Simon et de Shor (recherche de période et factorisation) et généralisations récentes*

12 mai 2021 : séminaire de Miklos Santha : *Le problème du sous-groupe caché*

19 mai 2021 : *Optimisation quantique : algorithme de Grover, estimateurs quantiques, chaînes de Markov quantiques, heuristiques quantiques*

19 mai 2021 : séminaire de Stacey Jeffery : *A Unified Framework for Quantum Walk Search*

26 mai 2021*: Transformée de Fourier quantique II : résolution ultra-rapide de systèmes linéaires et applications en technique d'apprentissage automatique*

26 mai 2021: séminaire de Iordanis Kerenidis : *Quantum Machine Learning*

2 juin 2021 : *Limites et impact du calcul quantique : complexité en requêtes, simulation classique, déquantization d'algorithmes quantiques*

2 juin 2021 : séminaire d'André Chailloux : *Suprématie quantique : où en sommes-nous aujourd'hui ?*

9 juin 2021 : *Derniers développements pour l'internet et intelligence artificielle quantique : apprentissage, optimisation, calcul délégué et sécurisé, calcul distribué*

9 juin 2021 : séminaire d'Elham Kashefi : *Quantum Computing as a Service: Secure and Verifiable Multi-Tenant Quantum Data Centre*

En savoir plus : https://www.college-de-france.fr/site/frederic-magniez/index.htm

Colloque :

Algorithmes quantiques **-** 16 juin 2021.

En savoir plus : https://www.college-de-france.fr/site/frederic-magniez/symposium-2020-2021.htm

A propos du Collège de France

Le Collège de France, établissement public d'enseignement supérieur et de recherche établi à Paris depuis 1530 répond à une double vocation : être à la fois le lieu de la recherche la plus audacieuse et celui de son enseignement. On y enseigne ainsi à tous les publics intéressés, sans aucune condition d'inscription ni de diplôme, « le savoir en train de se constituer dans tous les domaines des lettres, des sciences ou des arts ». Le Collège de France a également pour mission de favoriser l'émergence de disciplines nouvelles, l'approche multidisciplinaire de la recherche de haut niveau et de diffuser les connaissances en France et à l'étranger. Les enseignements qui y sont dispensés sont librement disponibles sur son site internet dans des formats variés : films et enregistrements des cours, podcasts, iconographie et références bibliographiques, publications originales des éditions du Collège de France…

Le Collège de France est membre associé de l'Université PSL.
www.college-de-france.fr