$$\mathrm{val}^*(\mathfrak{G}) = \sup_{p \in C_q(n,k)} \sum_{x,y} \mu(x,y) \sum_{a,b} D(x,y,a,b) p_{abxy}$$

▲ *Cette formule donne la probabilité maximale pour un joueur qui utilise le quantique de gagner au jeu $\mathfrak{G}$ (les paramètres du jeu sont μ et D; μ étant la distribution avec laquelle on choisit les questions et D une fonction qui représente quelles réponses on valide ou non – les règles du jeu). Dans certains jeux, comme le carré magique décrit dans l'article, cette probabilité de succès peut être rendue égale à 1: à tous les coups on gagne.*

Prouver la complexité du quantique

En 1935, Albert Einstein propose, avec Boris Podolsky et Nathan Rosen, que deux particules puissent être liées, même si elles sont séparées par de très grandes distances – c'est l'intrication quantique. L'année suivante, le Britannique Alan Turing formule la première théorie générale du calcul et prouve qu'il existe un problème que les ordinateurs ne pourront jamais résoudre – le problème de l'arrêt. Ces deux idées ont jeté les bases de la physique quantique et de l'informatique. Or cinq mathématiciens viennent d'établir que l'intrication quantique peut – en théorie – servir de base à la vérification d'un vaste nombre de problèmes. Cette correspondance entre intrication et calcul est ici expliquée par l'un de ses auteurs belge.

Les lois de la mécanique quantique défient la pensée. Du chat de Schrödinger (en superposition d'un état vivant et d'un état mort) au paradoxe Einstein-Podolsky-Rosen (EPR), qui semble indiquer une forme de corrélation instantanée entre particules distantes (intrication), les surprises n'en finissent pas. Mais les progrès expérimentaux récents dans la course mondiale à l'ordinateur quantique révèlent l'importance d'un autre phénomène au cœur du potentiel du quantique pour le calcul : la complexité. En effet, c'est précisément cette complexité – celle d'exprimer, de représenter, de calculer le quantique – que physiciens et ingénieurs ont bon espoir d'exploiter, avec l'objectif de mettre au point un jour un calculateur à la puissance inégalée. Mais il y a un « hic ». Presque par définition, la complexité inégalée du quantique défie toute tentative de simulation classique. Dès lors, comment appréhender cette théorie ? En effet, les lois physiques ne sont des lois que tant qu'elles sont expérimentalement vérifiables : s'il est impossible en pratique de détecter la complexité du quantique, est-elle réelle ? Cela pose donc la question de l'existence de « signatures » classiques – vérifiables – des phénomènes quantiques fondamentaux. Une telle signature a été mise en évidence par le physicien nord-irlandais John Bell en 1964 pour le phénomène de « non-localité » quantique. Que signifie ce terme ? La mécanique quantique prédit qu'une paire de particules peut être dans un certain état dit « intriqué », tel qu'une mesure faite sur chacune des particules, de manière indépendante, donnera une paire de résultats (un résultat par particule) qui sont fortement et instantanément corrélés. Ces corrélations

CALIFORNIA INSTITUTE OF TECHNOLOGY

Thomas Vidick
PROFESSEUR D'INFORMATIQUE ET DE SCIENCES MATHÉMATIQUES, INSTITUT DE TECHNOLOGIE DE CALIFORNIE (CALTECH), ÉTATS-UNIS

Les recherches de Thomas Vidick se situent à l'interface de l'informatique théorique, de l'information quantique et de la cryptographie. Il s'intéresse à l'application des techniques de l'informatique, telles que la théorie de la complexité, pour étudier les problèmes de l'informatique quantique.

$$|E(a,b) - E(a,b') + E(a',b) + E(a',b')| \leq 2$$

▲ *Expression du théorème de Bell. E est une mesure de la corrélation pour deux systèmes a et b sur lesquels on peut faire deux mesures (avec ou sans prime, a et a' par exemple). Dans un système classique, cette expression est toujours inférieure ou égale à 2. Si on viole cette inégalité (par exemple, si on trouve 2,1), alors on a la certitude que le système est quantique.*

fortes sont au cœur du paradoxe EPR formulé en 1935 par Albert Einstein, Boris Podolsky et Nathan Rosen. Ce que les prédictions faites par la mécanique quantique ont de particulier, et qui posa problème à Einstein et ses collaborateurs, est qu'elles n'ont pas de modèle dit « à variables cachées ».

SI LA COMPLEXITÉ DU QUANTIQUE EST RÉELLE, COMMENT LA VÉRIFIER ?

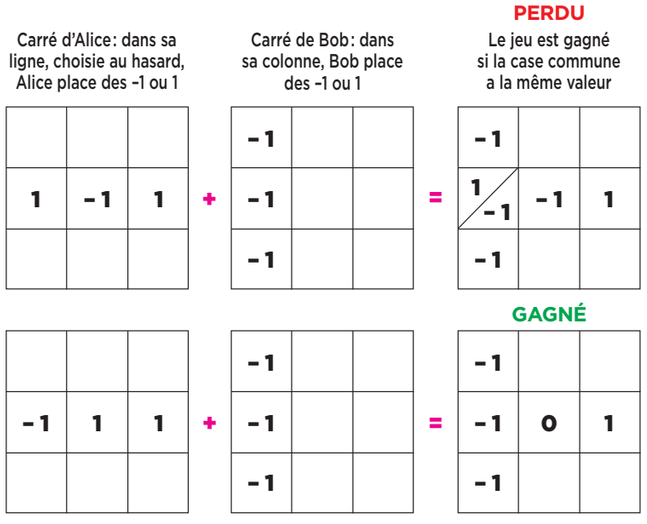
Un modèle à variables cachées est une description de l'état des particules telle qu'il serait possible de prédire la distribution des résultats de chaque mesure à partir de l'état seul de la particule sur laquelle la mesure est effectuée – sans référence aucune à la mesure faite sur l'autre particule. Bien qu'une telle condition puisse paraître fort raisonnable, la mécanique quantique prédit que certains systèmes quantiques – les systèmes intriqués – peuvent ne pas la satisfaire ; on parle alors de « corrélations non-locales ».
Ainsi, le travail de Bell nous fournit une première signature classique du quantique : il suffit de préparer un état intriqué et d'effectuer une série de mesures locales sur cet état. On peut vérifier (cela se fait facilement avec un ordinateur portable) si les données recueillies admettent un modèle à variables cachées. Si ce n'est pas le cas, on a la preuve que le système physique à la source des données obtenues est un système réellement quantique. Une telle expérience a été réalisée dans le groupe du physicien français Alain Aspect dans les années 1980, et reproduite maintes fois depuis (1). Ces expériences démontrent de manière virtuellement irréfutable que le monde est quantique – et ceci, uniquement sur la base des données expérimentales classiques (de simples nombres) recueillies lors de l'expérience. Même Einstein aurait eu à s'incliner !
L'intrication mise en évidence par l'expérience d'Aspect concerne seulement deux particules, que l'on peut modéliser en utilisant un espace à 4 dimensions, ce qui se fait très bien en pratique.

Au moment de l'expérience, dans les années 1980, il était ainsi tout à fait possible d'en prédire le résultat escompté. Cependant, la complexité du quantique est de nature exponentielle : 4 particules demandent 16 dimensions (2^4), pour 10 particules il en faut 1024 (soit 2^{10}), et, arrivé à 80 particules, on a largement dépassé la capacité (estimée) de l'ensemble des centres de données de Google ! Ainsi se pose une réelle difficulté : au-delà des phénomènes à petite échelle, la complexité du quantique se manifeste-t-elle aux observateurs humains ou est-elle un simple artefact d'une théorie plus compliquée qu'il ne se doit ? Supposant que la complexité soit réelle, comment la vérifier ? Un observateur humain est-il capable de jauger la complexité qui sous-tend certaines observations – avec beaucoup de particules – sans être capable de lui-même reproduire une telle complexité ? C'est ce que nous appelons le « problème de vérification ».
Avec mes collègues Henry Yuen de l'université de Toronto, au Canada, Zhengfeng Ji de l'université de technologie de Sydney, en Australie, Anand Natarajan de l'Institut de technologie du Massachusetts (MIT), aux États Unis, et John Wright de l'université du Texas à Austin, aux États-Unis, nous avons donné une réponse à cette question en démontrant l'existence de signatures classiques associées à des niveaux de complexité du quantique qui défient l'entendement (on verra plus loin pourquoi cette formule est appropriée). Notre résultat établit un lien profond entre complexité, vérification et non-localité (2).
Pour expliquer ces nouvelles connexions et leur importance pour le problème de vérification, il convient de faire deux détours : un premier au travers de la théorie des jeux non-locaux, et un second par les preuves interactives. Un jeu non-local est une expérience de pensée dont le but est de fournir une présentation précise autant qu'intuitive du phénomène de non-localité. Prenons un exemple : le « carré magique » introduit par l'Américain David Mermin et l'Israélien Asher Peres en 1990 (3). Dans un carré magique traditionnel, il s'agit de remplir les cases avec des nombres entiers, de sorte que la somme des nombres dans chaque ligne et dans chaque colonne soit égale à une certaine valeur prédéterminée – un sudoku avant l'heure, en quelque sorte. Les règles du carré magique de Mermin et Peres semblent a priori plus faciles à satisfaire : en effet, il s'agit simplement de remplir les 9 cases d'un carré 3 × 3 avec un signe choisi parmi –1 et +1, tel que le produit des signes associés avec chaque ligne soit +1 et le produit des entrées de chaque colonne soit –1. Cela peut sembler facile, parce qu'il ne s'agit que de nombres –1 ou +1. Pourtant, pour des raisons de parité, il n'y a pas de solution.
Mermin et Peres ont eu l'idée de présenter le carré magique comme un petit jeu. Imaginons deux joueurs, Alice et Bob, qui coopèrent pour maximiser leurs chances de gagner. L'arbitre commence par choisir une question pour chaque joueur et la lui envoie. Pour Alice, l'arbitre choisit une ligne au hasard (3 questions possibles, choisies avec probabilité 1/3 chacune) ; pour Bob, il choisit une colonne au hasard (trois questions possibles). Chaque joueur est alors sommé de fournir une réponse sans communiquer avec son partenaire – à la manière d'un système d'interrogatoire où deux suspects seraient placés dans deux pièces isolées. Une fois les deux réponses reçues, l'arbitre vérifie que le produit des réponses d'Alice est +1 et le produit des réponses de Bob est –1, comme il se doit. Observons que, sans règle supplémentaire, ce jeu est facile à gagner : par exemple, Alice pourrait toujours répondre (1,1,1) et Bob (–1,–1,–1), quelle que soit leur question ; ceci satisfait toutes les règles.

LES MATHÉMATIQUES MONTRENT QU'ON NE PEUT PAS GAGNER À TOUS LES COUPS

Ce qu'il nous manque est une condition de « cohérence » : puisque la ligne d'Alice et la colonne de Bob ont une case commune, l'arbitre demande que, pour cette case, leurs signes soient égaux. Par exemple, pour la première ligne et la première colonne, les réponses (1,1,1) et (1,–1,1) sont valables, mais pas (1,1,1) et (–1,–1,–1). C'est cette condition de cohérence qui fait l'intérêt du jeu : tels deux suspects, Alice et Bob sont en difficulté lorsqu'on leur pose des questions corrélées. On démontre mathématiquement qu'il est impossible à deux joueurs de gagner à tous les coups. Au mieux, ils peuvent gagner avec une probabilité 8/9 (voir figure p. 104).
Jusqu'à présent, rien de magique : un jeu où il est impossible de gagner avec certitude, c'est courant. Mais est-ce vraiment impossible ? La grande surprise révélée par Mermin et Peres est que, si l'on autorise Alice et Bob à faire usage de phénomènes quantiques – toujours abso-

JEU DU CARRÉ MAGIQUE



Les joueurs doivent remplir les cases d'une ligne ou une colonne avec 1 ou -1 en respectant une règle : le produit des termes d'une ligne ou d'une colonne doit être -1. L'arbitre juge ensuite si c'est gagné ou perdu en comparant la case commune. Les joueurs ne peuvent pas communiquer. Ils peuvent gagner avec une probabilité maximale de 8/9. En ajoutant l'intrication quantique, ils peuvent gagner à coup sûr.

$$p(a,b|x,y) = \langle \psi \quad | A_a^x \otimes B_b^y | \psi \rangle$$

▲ *Loi quantique de probabilité avec deux systèmes. Elle exprime la probabilité pour les joueurs (Alice et Bob) d'obtenir les réponses a et b quand on leur pose les questions x et y. Par exemple, quand on pose la question a à Alice, elle fait une mesure qui donne le résultat A (Ψ est leur état quantique). Les symboles à droite sont des lois de composition d'algèbre linéaire.*

lument sans communication –, alors il leur est possible de gagner avec une probabilité 1. À tous les coups ! Or le raisonnement mathématique montre que ce n'est pas possible puisqu'on gagne avec une probabilité de 8/9 au maximum. Les lois de la mécanique quantique violeraient-elles les principes mathématiques les plus simples ? Heureusement pour nous, mathématiciens, ce n'est pas le cas.
Pour comprendre le phénomène à l'œuvre, il est utile d'imaginer l'exécution du jeu d'un point de vue physique concret. Dans ce jeu, Alice et Bob reçoivent chacun une question et ils produisent une réponse. Comment cette réponse est-elle obtenue ? En général, Alice peut réfléchir, faire quelques calculs, et finalement donner sa réponse. De même pour Bob. Et si Alice et Bob faisaient usage de particules quantiques

L'intrication quantique permet des corrélations non-locales fortes, telles que les joueurs quantiques puissent gagner avec certitude

pour les aider ? Tant que chacun a ses propres particules et qu'il n'y a pas d'échange d'information entre les joueurs, les règles du jeu sont respectées. Mais Mermin et Peres ont identifié un état quantique pour 4 particules (2 pour Alice et 2 pour Bob), tel que cet état leur permet de gagner le jeu à tous les coups ! Concrètement, une fois leur question reçue, Alice et Bob, chacun de leur côté, font une certaine mesure sur leurs deux particules quantiques ; le joueur détermine alors sa réponse en fonction du résultat de la mesure. Le point crucial est que ces résultats sont corrélés d'une manière très spéciale, « non-locale » pour reprendre le terme introduit plus tôt. Un exemple de corrélation forte, mais simple (et locale), consisterait par exemple à imaginer que les particules ont une certaine « couleur » et que cette couleur est la même pour Alice et Bob. Alors, mesurer la couleur leur donne toujours le même résultat, mais ce n'est pas très utile. Dans le cas de l'état de Mermin-Peres, la corrélation n'est pas une loi d'identité, comme dans le cas de la couleur, mais une loi plus complexe qui dépend de la mesure même que chaque joueur décide d'effectuer. On comprend à présent ce qui a pu choquer Einstein et ses collaborateurs dans le paradoxe EPR ! L'intrication quantique permet des corrélations non-locales fortes, telles que les joueurs quantiques puissent s'en servir pour gagner avec certitude dans un jeu a priori impossible à gagner, et ceci sans pour autant violer la règle de non-communication.
En informatique, les jeux non-locaux sont associés avec la notion de preuve interactive. Pour comprendre, donnons d'abord un exemple simple de preuve non interactive. Supposons donné comme problème un très grand graphe – comme la carte des villes de Russie (chaque ville est un nœud du graphe) avec les routes carrossables indiquées (chaque route est une arête entre deux nœuds) ; la question posée est de déterminer s'il est possible d'associer une couleur (rouge, vert ou bleu) à chaque nœud de sorte que deux nœuds connectés par une arête n'aient jamais la même couleur. Si le graphe est très grand – par exemple constitué de plusieurs milliers de villes – il n'est pas facile de déterminer la réponse à cette question de manière directe. Cependant, le problème admet une preuve non interactive. Il s'agit d'une information supplémentaire, qui n'est pas nécessairement fiable mais qui peut aider à déterminer la solution.
Dans le cas qui nous concerne, une possibilité de preuve est tout simplement un coloriage du graphe. Si le graphe admet un coloriage valide, alors, étant donné n'importe quel coloriage valide donné, sa validité peut être déterminée de manière efficace en testant chaque arête. En revanche, si le graphe n'admet pas de coloriage valide, alors, quel que soit le coloriage avancé, il est possible de détecter que celui-ci est invalide. L'ensemble des problèmes qui admettent de telles preuves porte le nom de NP (pour « non-déterministe polynomial », c'est-à-dire les problèmes qui admettent une preuve qui peut être difficile à trouver – c'est l'aspect « non-déterministe » –, mais peut être vérifiée de manière efficace, c'est-à-dire en « temps polynomial »).

UN NOUVEAU MODÈLE DE PREUVES INTERACTIVES « MULTIPARTIES »

Des systèmes de preuves plus élaborées que celui que l'on vient de décrire, dites « preuves interactives », ont été introduits dans les années 1980, avec des motivations à la fois mathématiques (4) et cryptographiques (5). D'un point de vue mathématique, il s'agit de trouver la bonne modélisation de la notion intuitive de « preuve ». En cryptographie, il s'agit de développer des protocoles tels que ceux qui sont aujourd'hui utilisés entre, par exemple, notre carte bancaire et le lecteur à puces du commerçant : lors de cette interaction, la carte démontre à la banque qu'elle correspond bien à un compte en bonne et due forme – et ceci sans révéler notre identité. En quoi cette preuve est-elle interactive ? La banque, par l'intermédiaire de la machine, pose une question (« Code ? »), à laquelle nous donnons une réponse qui est ensuite validée (ou non). Une découverte importante en théorie de la complexité est que les preuves interactives (IP) peuvent permettre la vérification de problèmes dont on ne connaît pas de preuve non interactive. Cette découverte est résumée dans l'équation IP = PSPACE issue du travail de l'informaticien israélien Adi Shamir notamment (6). Ici, PSPACE désigne l'ensemble des problèmes dont la solution peut être déterminée en utilisant une quantité d'espace mémoire polynomial, mais sans borne de temps. Cette classe est considérée comme étant beaucoup plus étendue que la classe NP ; ainsi le résultat de Shamir démontre-t-il la puissance de l'interaction pour la vérification.
Il est possible d'aller plus loin : les preuves interactives peuvent faire intervenir plusieurs parties en charge d'établir la « preuve ». Cette extension est motivée par des considérations liées à la protection des données privées, ce qu'on nomme les preuves « *zero-knowledge* » (ou « preuve à divulgation nulle de connaissance ») en cryptographie. Grâce à ce type de preuve, les informaticiens sont capables de concevoir des systèmes d'identification distribués tels que la procédure de vérification d'identité n'entraîne aucune fuite de données. Après l'introduction de preuves interactives par les cryptographes, à la fin des années 1980, la théorie de la complexité s'est emparée du nouveau modèle de preuves interactives « multiparties » pour en étudier la portée : quels problèmes peuvent être vérifiés de manière efficace dans ce modèle ?
Une réponse complète à cette question a été obtenue en 1991 dans un autre résultat important du domaine de la complexité (7). Ce résultat peut se résumer par l'égalité MIP = NEXP. Ici MIP *(« multiprover interactive proof »)* dénote l'ensemble des problèmes qu'il est possible de vérifier en utilisant une preuve interactive multipartie, et NEXP désigne l'ensemble des problèmes qui admettent des preuves exponentiellement longues, vérifiables en temps exponentiel. Ainsi donc, selon MIP = NEXP, certains problèmes qui a priori requièrent un temps exponentiel pour être vérifiés (NEXP) admettent cependant une vérification efficace dans le modèle multipartite (MIP). Cette découverte surprenante continue d'avoir des ramifications dans de multiples domaines de l'informatique, y compris en cryptographie, pour le développement de systèmes de calcul dans le nuage *(cloud)*, et même pour les algorithmes liés aux cryptomonnaies.
Faisons à présent le lien avec les jeux non-locaux introduits précédemment. Celui-ci est direct : une preuve interactive multipartie n'est, en fin de compte, rien d'autre qu'un jeu non-lo-

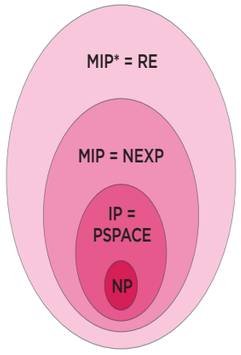

Des travaux précurseurs

Dans les années 1970, le mathématicien français Alain Connes (à gauche) avait postulé l'existence de certaines approximations finies d'un objet en dimension infinie. De manière indépendante, dans les années 1980, le mathématicien russe Boris Tsirelson (à droite) avait posé le problème de l'équivalence entre les deux modèles possibles pour les jeux non-locaux. Trente ans plus tard, plusieurs mathématiciens ont montré l'équivalence de ces deux problèmes. Le résultat décrit ici apporte une réponse négative au problème de Tsirelson. En d'autres termes, les deux modèles considérés par Tsirelson sont distincts, et l'objet infini de Connes n'admet pas d'approximation finie.

CREDIT PHOTO

$$\mathcal{E}\left(\mathfrak{G}'_n, \frac{1}{2}\right) \geq \max\left\{ \mathcal{E}\left(\mathfrak{G}_{2^n}, \frac{1}{2}\right), 2^{2^{\Omega(n)}} \right\}$$

▲ *Comparaison de la quantité d'intrication nécessaire pour gagner dans différents jeux. Le $\mathfrak{G}$ du terme de gauche, plus haut dans la hiérarchie élaborée par les auteurs pour leur démonstration (par rapport au jeu $\mathfrak{G}$ du terme de droite), a besoin de beaucoup plus d'intrication, le terme de droite croissant très rapidement.*



▲ *Imbrication des différentes classes de complexité qui apparaissent dans l'article. Chaque égalité est un résultat marquant de la théorie de la complexité obtenu depuis quelques décennies. Le résultat principal décrit ici est MIP* = RE. Cela signifie que l'ensemble des problèmes qu'il est possible de vérifier en utilisant une preuve interactive multipartie quantique (MIP*) est égal à l'ensemble des problèmes récursivement énumérables (RE).*

cal. À la base d'une preuve interactive se situe un problème dont on désire déterminer la solution. Par exemple, un graphe dont il faut déterminer s'il admet un coloriage valide. Imaginons que l'on associe un jeu non-local à ce graphe, de sorte que, si le graphe a un coloriage valide, alors il existe une stratégie pour les joueurs qui leur permet de gagner avec certitude. Mais si le graphe n'a pas de coloriage valide, cette victoire est impossible. Ce que je viens de décrire est précisément une preuve interactive pour le problème de coloriage. En effet, si la réponse au problème est « Oui, il y a un coloriage », alors cette réponse admet une preuve qui est vérifiable (il existe des joueurs qui gagnent au jeu ; leurs réponses déterminent la « preuve » qui est vérifiable par l'arbitre du jeu). En revanche, si la réponse est non, alors il n'existe pas de preuve qui puisse tromper la vérification (aucune paire de joueurs ne peut gagner).

Dans ce contexte, le jeu du carré magique de Mermin et Peres peut lui aussi être considéré comme une preuve interactive. Le problème de départ est la question de savoir si le carré magique a une solution. Comme on l'a vu, si le carré magique avait une solution, il existerait une stratégie gagnante pour les joueurs. Or, le carré magique n'a pas de solution et, ainsi, il n'existe pas de stratégie gagnante. Ce système de preuve est donc correct… tant que l'on se restreint à des joueurs classiques ! En effet, comme on l'a vu dans le cas de joueurs quantiques, il devient possible de gagner avec certitude, bien que le carré n'ait pas de solution. Ainsi, il existe des preuves interactives qui sont correctes lorsque l'on se restreint à des joueurs classiques, mais complètement incorrectes dès que l'on considère des joueurs quantiques.

Cette découverte a des conséquences en cryptographie comme en théorie de la complexité. En cryptographie, il s'agit de reconsidérer l'utilisation des preuves interactives pour, par exemple, le problème d'identification, et de vérifier au cas par cas s'il pourrait exister de nouvelles stratégies utilisant l'intrication quantique pour des attaques malicieuses. En complexité, il s'agit de caractériser la portée des nouvelles preuves multiparties. Pour le cas de joueurs classiques, cette complexité est encapsulée dans l'égalité MIP = NEXP. Dans le cas de joueurs quantiques, on note l'ensemble des problèmes qu'il est possible de vérifier au travers d'une interaction avec des joueurs quantiques par MIP*, l'astérisque symbolisant la présence d'intrication. Comme on l'a vu avec l'exemple du carré magique, il semblerait que le quantique augmente la possibilité pour les joueurs de tricher, ce qui voudrait dire que la classe de problèmes vérifiables est plus limitée : MIP* serait plus petit que MIP. Par ailleurs, il n'est pas exclu que l'on puisse développer de nouveaux jeux, qui soient, eux, « robustes » à l'utilisation de l'intrication, ou même en tirent parti : ainsi, MIP* pourrait être plus grand que MIP.

CHAQUE PROBLÈME DE RE PEUT ÊTRE ENCODÉ DANS UN JEU NON-LOCAL

Les spécialistes du calcul quantique se penchent sur cette question depuis près de deux décennies. Au-delà du problème de vérification en soi, cette exploration est motivée par le rôle central que l'intrication joue en physique quantique, de la distribution de clé quantique en cryptographie aux phénomènes de supraconduction dans les nouveaux matériaux. En janvier 2020, avec mes collègues, nous avons obtenu une caractérisation exacte de l'étendue des problèmes qu'il est possible de vérifier en utilisant des preuves interactives multiparties quantiques. Cette étendue est vaste ! La caractérisation fait intervenir la classe de complexité RE, pour « récursivement énumérable ». Un problème est dans la classe RE dès lors qu'il existe un algorithme qui détermine si le problème a une solution positive – sans limite de temps ! Par exemple le problème de coloriage mentionné plus tôt est dans la classe RE : étant donné un graphe, il est possible de vérifier soi-même que le graphe est bien coloriable, avec trois couleurs et de sorte que deux nœuds connectés soient toujours colorés différemment, comme il se doit. Autre exemple : le problème qui consiste à décider si une proposition mathématique admet une preuve (dans un certain système d'axiomes) est également RE. En effet, si la proposition a une preuve, même si cela peut prendre du temps, on finira bien par la trouver. Pour finir, notons que le problème d'arrêt de Turing, qui consiste à déterminer si un programme informatique donné s'arrête à terme ou bien s'il entre dans une boucle infinie, est un problème complet pour RE. Cela signifie que, d'une part, ce problème est dans RE et, d'autre part, qu'il est au moins aussi difficile que n'importe quel autre problème dans RE.

Ainsi, RE désigne la classe de tous les problèmes qui possèdent une solution identifiable en temps fini, quel que soit le temps qu'il faille pour la trouver ou la vérifier. Notre résultat est que chaque problème de RE peut être encodé dans un jeu non-local, de sorte que le jeu a une stratégie gagnante si et seulement si le problème a une solution positive : c'est l'égalité MIP* = RE. Reprenant un exemple déjà mentionné, ce résultat implique, entre autres, qu'à n'importe quelle proposition mathématique, vraie ou fausse, il est possible d'associer un jeu non-local simple (une variante du carré magique, dont les règles dépendent de la proposition) tel que, si la proposition est vraie, alors il y a une stratégie quantique gagnante dans le jeu et, si elle est fausse, il n'y a pas de stratégie gagnante. Ce qui est fascinant est que, d'une part, les règles du jeu elles-mêmes peuvent être calculées de manière très simple à partir de la proposition, sans chercher à en déterminer la validité (pas besoin d'être mathématicien !) et, d'autre part, que la procédure de vérification de l'arbitre dans le jeu est également très simple. Toute la complexité a été déplacée du côté des joueurs.

Ainsi, le système quantique qui sous-tend une stratégie gagnante, si elle existe, aura nécessairement une complexité proportionnelle à la complexité de déterminer si la proposition est vraie ou pas. Pour peu qu'il existe des propositions dont la preuve est arbitrairement longue, alors il existe des jeux qui vérifient que les joueurs gagnants doivent avoir préparé un système quantique arbitrairement complexe. Or Turing a démontré en 1936 que le problème d'arrêt, qui, comme on l'a rappelé, est un problème RE, est indécidable (8). Ceci parce qu'il est impossible de déterminer lorsque la réponse est « non », autrement dit que le programme ne s'arrête jamais.

LE PHÉNOMÈNE DE NON-LOCALITÉ TIENT LA MAIN À LA COMPLEXITÉ DU QUANTIQUE

Ainsi donc, il existe des problèmes arbitrairement complexes, et même indécidables, qui peuvent être encodés dans un système quantique pour lequel existe néanmoins une « signature classique » vérifiable de manière efficace.

En résumé, le résultat obtenu est que la complexité du quantique peut en principe être utilisée pour encoder la solution à des problèmes de complexité arbitrairement grande. Cela de manière que la solution puisse néanmoins être vérifiée de manière efficace à travers l'exécution d'un jeu non-local, que l'on peut imaginer comme une expérience avec certains choix de mesures et certains résultats obtenus. Le phénomène de non-localité tient la main à cette complexité du quantique, qui en fait la richesse. Se trouve ainsi justifiée la difficulté de la tâche du physicien quantique : n'ayant accès qu'aux manifestations classiques des phénomènes qu'il étudie, et étant donné que cette complexité peut être arbitraire, quel espoir y a-t-il pour dompter le quantique ? Alors que de véritables ordinateurs quantiques sont à l'horizon, il s'agit d'une question pour les futures générations de chercheurs. ■

(1) A. Aspect, *Physics, 8,* 123, 2015.

(2) Zh. Ji *et al.,* MIP*= RE, arXiv:2001.04383, 2020.

(3) N. D. Mermin, *Phys. Rev. Lett., 65,* 3373, 1990 ; A. Peres, *Phys. Lett. A, 151,* 107, 1990.

(4) L. Babai, *ACM STOC'85,* 421, 1985.

(5) S. Goldwasser *et al., ACM STOC'85,* 291, 1985.

(6) A. Shamir, *JACM, 39,* 869, 1992.

(7) L. Babai *et al., Comput. Comp., 1,* 3, 1991.

(8) A. Turing, *Alan Turing Collection, s2-42,* 230, 1937.