Zeitschrift: Tracés : bulletin technique de la Suisse romande
Herausgeber: Société suisse des ingénieurs et des architectes
Band: 130 (2004)
Heft: 13: Ordinateur quantique

Artikel: La course aux calculateurs quantiques
Autor: Baquiast, Jean-Paul / Jacquemin, Christophe
DOI: https://doi.org/10.5169/seals-99321

Jean-Paul Baquiast et Christophe Jacquemin

La course aux **calculateurs quantiques**

Les chercheurs en rêvent depuis une vingtaine d'années: construire une nouvelle génération d'ordinateurs, basés sur les lois de la mécanique quantique. Les capacités de calcul potentielles de ces machines sont immenses et dépasseraient celle d'un ordinateur classique de la taille du système solaire et fonctionnant à la vitesse de la lumière.

Le département de la défense américain (DOD) dispose au *Los Alamos National Laboratory* du deuxième ordinateur le plus puissant du monde, nommé *ASCI Q*, avec à terme 30 teraflops[1]. Celui-ci complète les ressources du précédent, *Blue Mountain* (3 teraflops). Le DOD a demandé récemment au Laboratoire de concevoir pour 2008 une machine capable d'effectuer un million de milliards d'opérations par seconde, soit un petaflops. Ces machines servent à la simulation d'essais nucléaires. Des ordinateurs de même puissance ont dans le civil de nombreux autres usages, par exemple la simulation des molécules biologiques en bio-informatique. Ils coûtent extrêmement cher, sont très encombrants et, finalement, de très mauvais rendement car ils ne peuvent utiliser qu'environ 10% de la puissance informatique totale, le reste servant essentiellement à faire coopérer les processeurs.

La course à la puissance des ordinateurs classiques n'a pas atteint son terme. Et pourtant la limite approche, notamment parce que les composants commencent à travailler au niveau de l'atome, ce qui représente une barrière infranchissable si l'on veut détecter les signaux. Au-delà, on passe dans la physique subatomique ou quantique. Conscients de cette barrière technologique inéluctable, des chercheurs en informatique se sont demandé, depuis une vingtaine d'années déjà, comment utiliser les propriétés de la matière au niveau quantique. Ces réflexions ont donné naissance à de nombreux projets visant à définir, puis à expérimenter un ordinateur quantique.

[1] C'est-à-dire capable d'exécuter 30 mille milliards d'opérations par seconde (1 flops = 1 FLoating-point Operation Per Second). Un PC moyen atteint environ 0,0001 teraflops, à partir de 0,1 teraflops on parle d'un ordinateur à haute capacité.

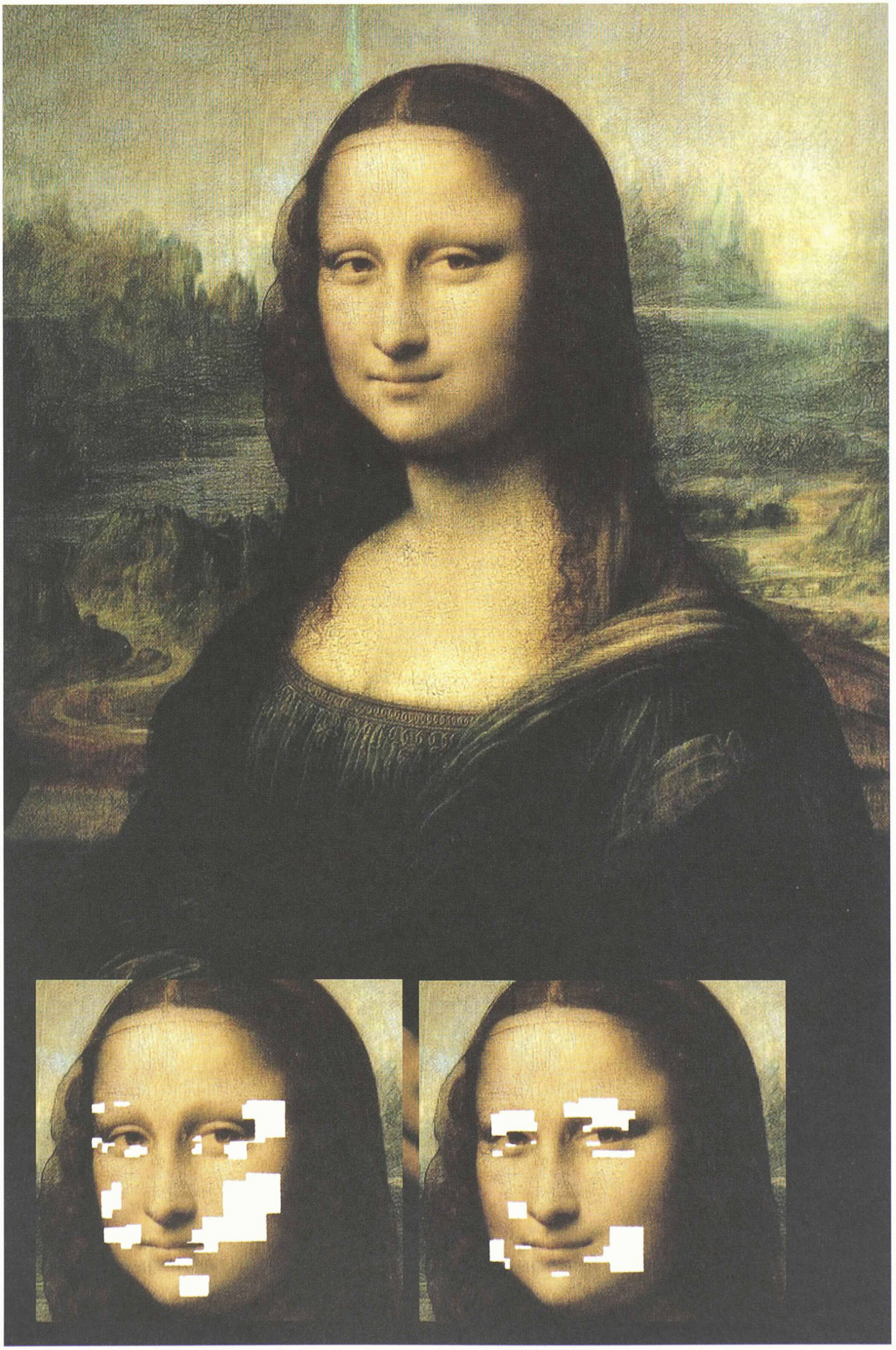
Le bit quantique

On ne décrira pas ici un ordinateur quantique possible. Disons seulement qu'il utilisera les propriétés des bits quantiques ou qubits (de *quantum bit*). Un qubit est un système quantique monté en laboratoire. Il peut s'agir d'un atome ou d'une particule, plongé dans un champ magnétique intense et subissant des impulsions radio de haute fréquence qui modifient sa rotation (c'est-à-dire son spin). On attribuera la valeur 1 à une rotation dans le sens des aiguilles d'une montre et la valeur 0 à la rotation en sens inverse, c'est-à-dire les deux valeurs utilisées dans le langage binaire des informaticiens. Compte tenu de la difficulté à manipuler de tels atomes, le nombre maximum des qubits qui ont pu être mis en œuvre dans les prototypes les plus récents d'ordinateur quantique ne dépasse pas sept - ce qui paraît risible au regard des dizaines de millions d'unité composant le processeur d'un simple micro-ordinateur.

Mais la particule isolée peut, comme l'enseigne la mécanique quantique, se trouver dans deux états à la fois (fig. 1). C'est ce que l'on appelle l'état de superposition cohérente (voir aussi p. 11). Si l'on veut s'en servir comme unité de représentation de l'information (bit), elle peut donc présenter simultanément l'état 1 et l'état 0. L'ordinateur quantique est donc d'abord un calculateur massivement parallèle. Avec 13 qubits (ce qui n'est pas réalisable pour le moment), il atteindrait la puissance de calcul en parallèle de l'ordinateur *Blue Mountain* évoqué ci-dessus.

Un ordinateur quantique peut utiliser n'importe quelle particule susceptible d'avoir deux états en superposition. Des ordinateurs quantiques peuvent être construits à partir d'atomes qui sont à la fois excités et non excités au même moment. Ils peuvent être construits à partir de photons de lumière qui sont à deux endroits au même moment. Ils peuvent être construits à partir de protons et de neutrons ayant un spin soit positif soit négatif ou les deux en même temps. Une molécule peut contenir plusieurs millions de protons et de neutrons. Elle peut donc, théoriquement, être utilisée comme ordinateur quantique doté de plusieurs millions de qubits. Les capacités potentielles de calcul correspondraient,

Fig. 1 : Mona Lisa comme superposition de deux états, « triste » et « joyeux ». En enlevant certains éléments de l'image (dans les deux fragments en bas), on perçoit une expression soit triste soit joyeuse. Le portrait principal par contre réunit les deux expressions, et la prédominance de l'une ou de l'autre change selon l'observateur. (Document TRACÉS, *d'après une idée de S. Prvanovi, Université de Belgrade)*



1

avec un ordinateur classique, à des durées de plusieurs fois l'âge de l'univers. On imagine ainsi le gain en temps de calcul et utilisation de la mémoire à laquelle peut conduire cette nouvelle technologie. Mais elle promet beaucoup plus : les progrès viendront aussi de nouveaux algorithmes qui vont permettre de résoudre des problèmes jusqu'alors inaccessibles pour l'informatique classique.

Conserver l'état de superposition

Il y a donc un intérêt stratégique majeur à maîtriser cette puissance. De nombreux laboratoires se sont mis en piste, mais une énorme difficulté a jusqu'ici arrêté les chercheurs : celle de maintenir en état de superposition un ensemble de plus d'une particule. La localisation ou l'impulsion d'une particule quantique en état de superposition ne peuvent être définies que par une probabilité statistique découlant elle-même de la fonction d'onde de la particule. Pour connaître exactement ces valeurs, il faut faire interférer la particule avec un instrument, comportant par définition une grande quantité d'atomes. Mais alors, la fonction d'onde s'effondre et l'observateur n'obtient qu'une seule des deux valeurs, l'autre étant définitivement perdue, en application du principe d'indétermination (voir aussi p. 11).

Pour qu'un ou plusieurs qubits conservent leur caractère quantique, et puissent donc travailler en état de superposition, il faut les isoler de toute matière ou énergie avec laquelle ils interféreraient - ce qui paraissait impossible ou très difficile dès que le nombre de qubits dépassait deux ou trois. Aujourd'hui cependant, en utilisant diverses techniques, un certain nombre de laboratoires ont annoncé avoir maintenu à l'état quantique de courtes séquences de bits (quatre à sept) et pour des durées de temps suffisantes à la réalisation de quelques opérations.

L'avenir de l'ordinateur quantique repose donc sur les technologies qui seront utilisées pour générer et maintenir en état de superposition cohérente des chaînes de bits de plus en plus longues. C'est là l'enjeu essentiel de la course à l'ordinateur quantique, engagée depuis une dizaine d'années dans les principaux pays du monde. Différents substrats et différentes méthodes de détection (par exemple la Résonance Magnétique Nucléaire) sont actuellement expérimentés (voir encadré).

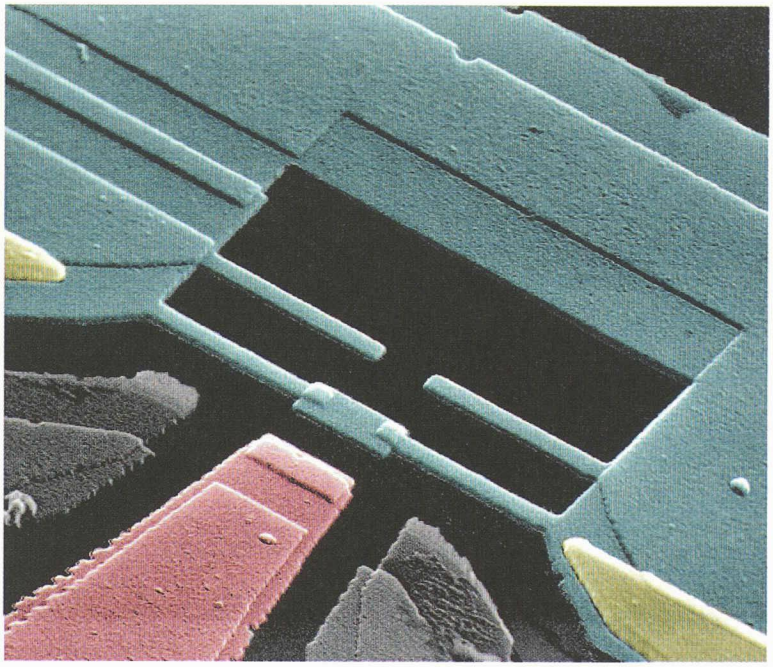
Il semble aujourd'hui possible que la solution au problème du maintien de l'état cohérent d'un qubit apparaisse plus vite que prévu. Elle viendrait d'une des théories les plus abstraites de la physique contemporaine, la théorie des cordes (*strings*). On a montré qu'il était possible d'entremêler les trajectoires dans le temps de particules quantiques pour former des tresses (*braids*) comportant des nœuds. Ceux-ci peuvent encoder de l'information et procéder à des calculs tout en résistant à la décohérence. Pour observer ces *braids*, on fait appel à des particules spéciales appelées *non-Abelian anyons* (dont on soupçonne l'existence sans avoir pu la mettre en évidence). Bornons-nous ici à signaler ces nouveaux concepts, qui seront à la base du fonctionnement des futurs ordinateurs quantiques dits topologiques, si ceux-ci voient le jour. Les recherches évoquées ici sont conduites dans différents laboratoires américains et surtout chez *Microsoft*, ce qui est significatif.

De nouveaux algorithmes

Une autre difficulté devra être résolue. Il s'agit des modalités de la programmation d'un ordinateur quantique. On comprend bien que l'on ne puisse utiliser une programmation classique pas à pas. Il faut définir de nouveaux algorithmes qui exploitent un état de superposition pouvant contenir un nombre exponentiel de termes différents. Ainsi une instruction pourra être de la forme suivante : « prendre la superposition de tous les nombres résultant de l'opération précédente ». De telles instructions permettent de programmer la résolution d'un problème de factorisation, qui est encore actuellement considéré comme le domaine d'excellence de l'ordinateur quantique. Ainsi, différents langages de programmation ont été créés avant même que des ordinateurs quantiques opérationnels aient été réalisés.

Toujours dans le cadre des difficultés, insistons sur le fait qu'avec l'ordinateur quantique, le résultat final d'un calcul n'étant déterminé que par des lois de probabilités, un

Fig. 2 : Photographie au microscope électronique d'un petit circuit supraconducteur, baptisé quantronium. Premier bit quantique sur une puce électronique, réalisé par une équipe de chercheurs du CEA, en 2002. La largeur de la boucle de ce nano-circuit est de 3 microns. (Document CEA)



2

L'ordinateur quantique : solide, liquide ou gazeux ?

Comment se présentera l'ordinateur quantique dont certains prévoient des applications industrielles dès 2020 ? Aura-t-il la taille d'un immeuble ou tiendra-t-il dans la main ? Bien malin qui aujourd'hui pourrait le dire...

Dans le passé, l'une des réalisations ayant le plus défrayé la chronique est celle de l'équipe d'Isaac Chuang, du centre de recherche *IBM* d'Almaden : un ordinateur quantique à sept qubits, qui a réussi la factorisation du nombre 15. En l'occurrence, les chercheurs ont travaillé avec la Résonance Magnétique Nucléaire (RMN) appliquée sur des molécules dans un milieu liquide. Il s'agit de molécules à sept spins conçues par des chimistes (noyau de cinq atomes de fluor et deux atomes de carbone) et qui peuvent interagir avec les autres comme des bits quantiques. Elles sont programmées par des pulsations d'ondes radio.

Rappelons qu'Isaac Chuang avait déjà réalisé en 1998 un premier ordinateur quantique à deux qubits, dans un dé à coudre de chloroforme, pour rechercher les diverses périodicités d'une fonction. L'année suivante, il passe à l'ordinateur à trois qubits, dans une base à huit états. Enfin, en 2000, c'est la réalisation d'un ordinateur à cinq qubits, en utilisant les cinq atomes de fluor d'une molécule complexe.

Mais il existe aussi d'autres approches, par exemple celle des « pièges à ions », faisant également appel à un milieu fluide (notamment étudiée aux Etats-Unis et en Autriche).

Cela dit, certains chercheurs pensent qu'il sera désormais très difficile de développer et de synthétiser des molécules dotées d'un nombre de qubits supérieur à sept. Chuang lui-même, avec son système, n'imagine pas pouvoir aller beaucoup plus loin que 10 à 20 qubits parce que les signaux magnétiques qui mesurent l'orientation du spin et déterminent sa valeur (1 ou 0 ou les deux) deviennent de plus en plus faibles au fur et à mesure que le nombre de qubits augmente.

C'est pour cela que d'autres scientifiques - tel Colin Williams du Jet Propulsion Laboratory de la Nasa - préfèrent tabler sur des qubits fixés sur des substrats solides (fig. 2) ou sur des photons prisonniers dans des cavités optiques.

Les systèmes étudiés (y compris par *IBM*) vont des spins d'électrons confinés dans des nanostructures semi-conductrices (voir aussi pp. 18 et 19) aux spins de noyaux associés à des impuretés mono-atomiques dans un semi-conducteur, en passant par les flux électroniques ou magnétiques à travers des super-conducteurs.

calcul peut a priori donner n'importe quel résultat. Il faut donc disposer d'algorithmes qui permettent d'augmenter la probabilité que le système « décohère » dans l'état correspondant à la bonne réponse, sachant que lorsqu'on regarde un résultat dans un registre quantique (réseaux de qubits), tous les autres états disparaissent... Un vrai défi pour les théoriciens.

Qui a besoin de l'ordinateur quantique ?

Les scientifiques reconnaissent que l'on est encore bien loin du but : produire un ordinateur quantique de grande puissance et manipulable comme un micro-ordinateur. D'autres comparent la situation actuelle de la recherche à celle où se trouvait la connaissance de l'atome quand Marie Curie étudiait la désintégration du radium. Cependant, les progrès seront d'autant plus rapides que les recherches disposeront de plus de moyens. Une question d'ordre stratégique est désormais posée non pas aux chercheurs mais aux autorités qui financent les recherches fondamentales en matière de physique quantique : convient-il de laisser les recherches sur l'ordinateur quantique se poursuivre dans un grand nombre de laboratoires, au rythme nécessairement lent que suppose l'expérimentation de techniques difficiles et souvent différentes, alors que les hommes et les crédits y affectés sont rares ? Faut-il au contraire changer de vitesse ? Si oui, comment ?

On ne s'étonnera pas de nous voir recommander ce dernier choix. Il faut bien voir que les industriels de l'informatique qui, les premiers, mettront sur le marché un ordinateur quantique performant prendront sur leurs concurrents une avance industrielle et commerciale considérable. C'est pourquoi chez *IBM*, les recherches sur le sujet bénéficient de moyens importants[2]. Il en est de même pour les investissements consentis par *Microsoft* aux recherches concernant l'ordinateur topologique.

Mais les industriels informatiques ne sont pas seuls en cause. Dans un monde ou les technologies sont aussi et surtout question de souveraineté, les pays qui disposeront en premier d'une industrie du calcul quantique compétitive en bénéficieront pour maintenir ou accroître leur influence sur le reste du monde[3]. Chacun sait que la capacité de la science et de l'industrie américaine à s'appuyer sur des réseaux de très grands calculateurs constitue l'un des principaux moyens leur permettant d'assurer leur suprématie.

L'histoire risque de se répéter dans le domaine des calculateurs quantiques, comme sans doute dans celui des calculateurs à ADN[4], si ces derniers voient le jour avant ceux-là. Les perspectives offertes par les premiers sont très attrayantes, dans les domaines de la cryptographie, de la recherche en base de données avec multiples entrées et bien évidemment aussi en matière de calcul numérique, calcul dont les applications seront de plus en plus importantes. Plus généralement, toutes les modélisations supposant des calculs massivement parallèles, dans le domaine militaire, en bio-informatique, en économie et surtout en physique quantique elle-même (gravitation quantique), comme en cosmologie, pourront enregistrer des progrès d'une efficacité considérable avec ces ordinateurs révolutionnaires. On peut imaginer aussi qu'implanter de petits calculateurs quantiques dans des robots autonomes devrait accroître sensiblement leurs capacités d'auto-adaptation. Dans tous ces cas, les recherches concernent le long terme de 10 à 30 ans. Mais les gains en retour seront, dès maintenant et bien entendu plus tard, considérables. Financer ces projets ne peut être laissé aux entreprises. Les Etats doivent s'y engager de façon importante, continue et croissante.

Jean-Paul Baquiast et Christophe Jacquemin
Rédacteurs en chef du site <www.automatesintelligents.com>
jp.baquiast@wanadoo.fr, c.jacquemin@noos.fr

[2] A ce titre, voir les publications du centre de recherche *IBM* d'Almaden consacrées à la computation quantique : <www.almaden.ibm.com/st/quantum_information/index.shtml>

[3] En Europe, les laboratoires travaillant sur l'ordinateur quantique sont relativement nombreux, comme le montre une carte établie par le *Centre for Quantum Computation* britannique <www.qubit.org> (lacunaire en ce qui concerne la Suisse, ndlr.). Mais ils sont dispersés et abordent souvent des domaines très spécialisés qu'il sera difficile de mettre en synergie.

[4] Sous forme liquide, l'ADN peut en effet être déposé sur de très fins supports, composants de futurs ordinateurs biologiques.