L'ordinateur quantique : un objectif impossible à atteindre ?

Michel Dyakonov [1]

Cet article a déjà fait l'objet d'une publication sur le blog de Mediapart [2] *et est une réaction personnelle à la stratégie nationale sur les technologies quantiques présentée par le Président de la République à l'université Paris-Saclay* [3] *le 21 janvier 2021.*

Depuis près de 30 ans, nous assistons à une ruée mondiale vers « l'informatique quantique » accompagnée d'un battage médiatique d'un niveau sans précédent. Les fonds sont généreusement distribués, des centres d'informatique quantique s'ouvrent partout dans le monde et des perspectives à couper le souffle sont présentées au profane par des scientifiques enthousiastes et des journalistes encore plus enthousiastes. L'impression a été créée que l'informatique quantique sera la prochaine percée technologique du XXIe siècle. Le grand public, ainsi que les agences de financement, sont convaincus que la révolution quantique, apportant la finance quantique, l'internet quantique, la sécurité quantique, la santé quantique et d'autres miracles quantiques, est à notre porte.

Le mot « quantum » est entré dans le vocabulaire des foyers et des rock stars et a acquis le sens de merveilleux, moderne, puissant, cool et génial. Il est maintenant librement utilisé par les journalistes, les politiciens et toutes sortes de représentants du gouvernement qui n'ont absolument aucune idée du vrai sens de ce mot, ni de la

1. Physicien, professeur émérite à l'université de Montpellier, membre d'honneur de l'institut physico-technique à Saint-Pétersbourg.

2. https://blogs.mediapart.fr/edition/au-coeur-de-la-recherche/article/220221/lordinateur-quantique-un-objectif-impossible-atteindre.

3. http://www.c2n.universite-paris-saclay.fr/fr/visite-m-macron.

DOI:10.48556/SIF.1024.18.23 **1024** – Bulletin de la SiF, numéro 18, Novembre 2021, pp. 23–33

physique quantique en général. La science de « l'informatique quantique et le calcul quantique » est enseignée dans de nombreuses universités et écoles d'ingénieurs à travers le monde (dont la France) attirant les meilleurs étudiants qui rêvent de contribuer à cette entreprise audacieuse [4].

C'est devenu une course aux armements qui s'auto-entretient, de nombreuses organisations et institutions restant apparemment dans la course, ne serait-ce que pour éviter d'être laissées pour compte. Certains des plus grands scientifiques du monde, chez Google, IBM, Intel, Microsoft et d'autres, travaillent dur et avec des ressources somptueuses dans des laboratoires à la pointe de la technologie, pour réaliser leur vision d'un avenir quantique.

Bref historique

L'algorithme de Shor. Les premières idées assez vagues de l'informatique quantique ont été exprimées par Paul Benioff (1980), Yuri Manin (1980) et Richard Feynman (1981), mais le sujet n'a vraiment attiré l'attention qu'en 1994 lorsque Peter Shor [9] a proposé un algorithme qui, avec un ordinateur quantique idéal, pourrait factoriser des nombres extrêmement grands beaucoup plus rapidement que l'ordinateur classique. Ce résultat mathématique exceptionnel a engendré tout le domaine de l'informatique quantique ! L'excitation a été causée par la possibilité pour le futur ordinateur quantique de casser des codes de sécurité, dont certains, mais pas tous, sont basés sur l'énorme difficulté, voire l'impossibilité, pour les ordinateurs conventionnels de factoriser des nombres à 1000 chiffres, qui sont des produits de très grands nombres premiers [5]. Plusieurs autres algorithmes quantiques ont également été proposés plus tard.

Factorisation expérimentale de 15 par l'algorithme de Shor. La première expérience consacrée à la factorisation de 15 par Shor a été rapportée par Vandersypen et al. [12] en utilisant la technique de résonance magnétique nucléaire (RMN). Toutes les portes ont été mises en œuvre par des impulsions micro-ondes appliquées en 1 seconde environ, ce qui est inférieur au temps de décohérence nucléaire. Les spectres RMN obtenus correspondaient très bien aux prédictions de la procédure de Shor.

Lanyon et al. [4] ont effectué la même tâche dans une expérience optique utilisant la polarisation de quatre photons, tandis que Lucero et al. [5] ont utilisé des qubits. Selon Josephson, « ... nous exécutons une version compilée de trois qubits de l'algorithme de Shor pour factoriser le nombre 15, et trouver avec succès les facteurs premiers 48 % du temps ».

4. Les âmes innocentes ne savent pas encore que dans un avenir pas très lointain, il pourrait devenir prudent de dissimuler leur éducation en « informatique quantique ».

5. Notez que 27 ans plus tard, la démonstration de $15 = 3 \times 5$ par l'algorithme de Shor n'est toujours pas possible (voir plus loin). Nous n'avons donc pas de raison de nous inquiéter pour nos codes de sécurité.

Mais, dans toutes ces expériences, la soi-disant version compilée de l'algorithme de Shor a été utilisée. Comme l'ont montré Beckman et al. [1], l'algorithme complet peut factoriser un nombre de k bits en utilisant de l'ordre de $72k^3$ portes quantiques élémentaires. Par exemple, la factorisation de 15 nécessite 4 608 portes fonctionnant sur 21 qubits. Reconnaissant que ces exigences vont bien au-delà des possibilités expérimentales, Beckman et al. ont introduit une technique de compilation qui exploite les propriétés du nombre à factoriser, permettant l'exploration de l'algorithme de Shor avec un nombre considérablement réduit de ressources.

On pourrait dire que c'est une sorte de triche (innocente) sachant à l'avance que $15 = 3 \times 5$, on peut prendre quelques raccourcis, ce qui ne serait pas possible si le résultat n'était pas connu à l'avance.

Tous les tests expérimentaux existants de l'algorithme de Shor utilisent cette approche simplifiée. Dans un travail très remarquable de Martin-Lopez et al. [7], la même approche a permis pour la première fois de factoriser 21 dans une expérience optique, où une procédure itérative de recyclage d'un seul qubit a été mise en œuvre avec succès.

La simple factorisation du nombre 15 en utilisant l'algorithme de Shor complet est encore bien au-delà de la portée des possibilités expérimentales (comme je l'ai prédit en 2001 [2]). Ainsi, il semble que dans un avenir prévisible, nous n'avons pas à nous soucier de la sécurité des codes de cryptographie en raison de la difficulté à factoriser de très grands nombres, qui sont des produits de nombres premiers à cent chiffres.

Cartes routières

Le document récent « stratégie nationale sur les technologies quantiques » est en fait une feuille de route détaillée sur cinq ans pour la recherche sur l'informatique quantique et ses applications avec l'objectif annoncé : « 5 ans pour asseoir la France dans le premier cercle mondial ».

Auparavant, des feuilles de route « quantiques » similaires avaient déjà été créées, mais n'ont jamais été réalisées concrètement. La première est apparue en 2002 lorsque, à la demande de l'agence *Advanced Research and Development Activity* (ARDA) du gouvernement américain, une équipe d'éminents experts de l'information quantique avait établi une feuille de route audacieuse [12] pour l'informatique quantique avec pour objectifs à cinq ans (d'ici 2007) :

— coder un seul qubit dans l'état d'un qubit logique formé de plusieurs qubits physiques ;
— effectuer une correction d'erreur répétitive du qubit logique ;
— transférer l'état du qubit logique dans l'état d'un autre ensemble de qubits physiques avec une grande fidélité ;

et un objectif à 10 ans (d'ici 2012) : implémenter un code correcteur d'erreurs quantiques concaténé [6].

Alors qu'un jury très bienveillant pourrait considérer que le premier des objectifs de 2007 est en partie atteint à présent, les attentes pour les autres objectifs de 2007, et pour l'objectif de 2012, sont reportées *sine die*. Il en va de même pour les autres prédictions : « Au fur et à mesure que les ordinateurs quantiques à plus grande échelle seront développés au cours des cinq et dix prochaines années, la simulation quantique continuera probablement à être l'application pour laquelle les ordinateurs quantiques peuvent apporter des améliorations substantielles par rapport au calcul classique ».

Cependant, rien de ressemblant, même de loin, à des ordinateurs quantiques à plus grande échelle, ni aucune amélioration par rapport au calcul classique, n'a été produit jusqu'à présent.

Apparemment, passer de 5 qubits à 50 (l'objectif fixé par la feuille de route du panel d'experts ARDA pour l'année 2012) présente des difficultés expérimentales pratiquement insurmontables. Ils sont très probablement liés au simple fait que $2^5 = 32$, tandis que $2^{50} = 1125899906842624$ (voir ci-dessous l'explication de l'augmentation exponentielle de la difficulté à augmenter le nombre de qubits).

Quatorze ans plus tard (mai 2016), un groupe de scientifiques européens renommés a contacté la Commission européenne avec un « Manifeste quantique » [4], un appel à lancer une initiative européenne ambitieuse dans les technologies quantiques, nécessaire pour assurer le rôle de premier plan de l'Europe dans la deuxième révolution quantique en cours dans le monde entier. La Commission semble avoir été assez sensible à cet appel [7] et a alloué 1 milliard d'euros [8] pour atteindre cet objectif. Les résultats attendus pour l'informatique quantique sont :

— 0 – 5 ans : fonctionnement d'un qubit logique protégé par correction d'erreur ou topologiquement ; nouveaux algorithmes pour ordinateur quantique (4 ans se sont déjà écoulés, sans résultats visibles !) ;
— 5 à 10 ans : petit processeur quantique exécutant des algorithmes technologiquement pertinents ; résolution de problèmes de chimie et de science des matériaux avec un ordinateur quantique à usage spécial ;
— supérieur à 10 ans : intégration du circuit quantique et du matériel de contrôle classique cryogénique ; les ordinateurs quantiques à usage général dépassent la puissance de calcul des ordinateurs classiques.

On peut remarquer une similitude entre les projections à 5 et 10 ans des feuilles de route 2002 et 2016, d'autant plus que l'objectif quinquennal 2016 du Manifeste

6. La « concaténation » dans ce contexte signifiait distribuer l'information d'un qubit dans l'état d'un certain ensemble de plusieurs qubits, de sorte que le qubit logique soit codé par plusieurs qubits physiques.

7. Les américains dépensent des milliards de dollars sur ce projet, ils ne feraient rien de complètement stupides n'est-ce pas ?

8. Il apparaît que 1 milliard est l'unité quantique élémentaire pour le financement de la recherche en information quantique.

quantique est en fait le même que l'objectif quinquennal ARDA 2002. Verrons-nous une autre feuille de route similaire en 2030, avec un objectif de 5 ans d'encodage de qubits simples dans l'état d'un qubit logique ?

Plus récemment, fin 2018, un autre groupe d'experts réuni par les *National Academies of Science, Engineering and Medicine* des États-Unis a publié un rapport détaillé de 205 pages discutant de certains des défis pour lesquels l'informatique quantique serait une technologie de valeur [5]. Les auteurs du rapport déclarent sèchement qu'au cours de la prochaine décennie, aucun ordinateur quantique ne sera capable de casser des codes cryptographiques basés sur la factorisation des nombres premiers (un exemple d'une tâche pour laquelle les ordinateurs quantiques sont censés être particulièrement bien adaptés [9]), ils ne donnent aucun avis sur la possibilité de casser ces chiffres dans un avenir plus lointain.

Pour l'instant, il n'existe toujours aucun dispositif quantique capable de faire de l'arithmétique élémentaire comparable aux capacités d'un abaque, et encore moins de surpasser la règle à calcul ou la plus simple calculatrice électronique, dans tout type de calcul.

Stratégie nationale sur les technologies quantiques (2021)

Il semble très probable que ce document suivra les feuilles de route précédentes citées ci-dessus, qui, n'ayant aucun rapport avec la réalité, sont toutes allées à la poubelle. Regardons de plus près ce nouveau projet. Cela commence par la déclaration péremptoire suivante [6] : « *Le raccourcissement des temps de calcul d'un facteur de un milliard, qu'apporteront les ordinateurs quantiques d'ici 5 à 10 ans, constitue une rupture technologique majeure* ».

Le facteur d'un milliard, c'est vraiment beaucoup ! Un raccourcissement des temps de calcul d'un facteur de 2 seulement serait déjà assez important, mais pour le moment, il n'y a absolument aucune raison, même pour des attentes aussi modestes, et encore moins le facteur d'un milliard. Le projet se poursuit avec une liste d'impacts socio-économiques :

— mieux se soigner ;
— mieux se nourrir ;
— mieux combattre le changement climatique et ses effets ;
— mieux anticiper les catastrophes naturelles ;
— mieux se déplacer ;
— mieux produire ;
— mieux se protéger des menaces sur la sécurité des communications ;
— mieux se préparer aux conflits de demain.

9. Nous rappelons qu'il y a 27 ans, cette idée a été le déclencheur de la recherche en informatique quantique.

Comme nous le savons, il n'est toujours pas possible d'utiliser le calcul quantique pour vérifier que $15 = 3 \times 5$. Au vu de cela, on a du mal à croire que dans les cinq prochaines années, les ordinateurs quantiques pourraient vraiment nous aider à « combattre le changement climatique et ses effets », voire à « mieux se nourrir »...

Puisqu'aucune responsabilité n'est engagée, pour augmenter encore l'effet comique, on pourrait facilement ajouter de nombreux autres « impacts socio-économiques » tels que :

— mieux passer le bac en candidat libre ;
— mieux se marier ;
— mieux élever les enfants ;
— etc.

Mesdames, messieurs, auteurs de ce projet, un peu d'humain s'il vous plait !

La section « Les objectifs clés » définit les principaux objectifs à fixer d'ici cinq ans : « *maîtriser les technologies quantiques offrant un avantage stratégique décisif, dont les accélérateurs, simulateurs et ordinateurs quantiques, les logiciels métiers pour le calcul quantique, les capteurs, les systèmes de communication.*

Dans le domaine du calcul, le thème central de la stratégie : devenir le premier Etat à disposer d'un prototype complet d'ordinateur quantique généraliste de première génération dès 2023 [...]. »

La question est de savoir si le prototype complet d'ordinateur quantique généraliste de première génération sera capable de prouver que $15 = 3 \times 5$, ou en général de faire quelque chose de raisonnable, aussi simple cela soit-il. Sinon (comme le suggère notre expérience des précédentes feuilles de route « quantiques »), il ne méritera guère le titre de « prototype complet d'ordinateur quantique généraliste ».

Le document décrit également « Les faits marquants dans l'écosystème quantique national, ces 6 derniers mois ». Voici une liste de différents résultats dont certains sont certes impressionnants, mais pas directement liés à la possibilité de construire un ordinateur quantique. Parmi eux, le simulateur quantique amélioré *Quantum Learning Machine* d'Atos (QLM), qui est en fait un puissant ordinateur classique qui sert à simuler un petit ordinateur quantique, ce qui pourrait être assez intéressant.

Ordinateurs NISQ

La part du lion du financement total (352 M€) est censée être consacrée aux ordinateurs *Noisy Intermediate Scale Quantum* (NISQ, abréviation introduite par John Preskill). Pour comprendre ce que cela signifie, remplacez Q par C : que pourrait bien vouloir dire *ordinateur classique bruyant à l'échelle intermédiaire* ? De toute évidence, ce serait juste un assemblage qui ne peut rien calculer du tout et dont la destination naturelle serait la poubelle ; il en va de même pour un ordinateur NISQ.

Une expression plus polie du même jugement sur les ordinateurs NISQ a été faite dans le rapport du groupe d'experts réuni par les *National Academies of Science, Engineering and Medecine* des États-Unis (2018), mentionné ci-dessus : « Il n'existe actuellement aucun algorithme connu ni application qui pourrait utiliser efficacement cette classe de machine ».

Qubits vs bits : le principal problème de l'informatique quantique

Nos ordinateurs classiques sont essentiellement un assemblage d'interrupteurs marche / arrêt très rapides, réalisés physiquement initialement avec des tubes à vide, et plus tard, en utilisant de minuscules transistors. Les performances de l'ordinateur consistent à faire fonctionner ces interrupteurs selon un programme donné. Chaque commutateur représente un bit d'information oui / non.

À un moment donné, l'état de l'ordinateur classique est décrit par une séquence ($\uparrow\downarrow\uparrow\uparrow\uparrow\downarrow\downarrow$ ...), où $\uparrow$ et $\downarrow$ représentent des bits d'information matériellement réalisés comme les états marche et arrêt de transistors individuels. Avec n transistors, il y a 2^n états différents possibles de l'ordinateur, ce qui devient rapidement gigantesque quand n devient grand. Le processus de calcul consiste en une séquence de commutation de certains transistors entre leurs états $\uparrow$ et $\downarrow$ selon un programme prescrit.

En informatique quantique, l'élément classique à deux états est remplacé par un élément quantique à deux états de base, que nous représentons à nouveau symboliquement par $\uparrow$ et $\downarrow$. Dans la littérature, un objet quantique arbitraire avec deux états de base est appelé un « qubit » (i.e. bit quantique).

Le choix des états de base $\uparrow$ et $\downarrow$ est une question de convention, et ces états ne sont pas les seuls possibles. L'état général du qubit est décrit par la fonction d'onde :

$$\psi = a\uparrow + b\downarrow \tag{1}$$

où les amplitudes quantiques a et b sont des nombres complexes arbitraires satisfaisant la condition de normalisation

$$|a|^2 + |b|^2 = 1 \tag{2}$$

De plus, $|a|^2$ et $|b|^2$ donnent les probabilités que le qubit soit dans les états $\uparrow$ et $\downarrow$, respectivement.

Il est important de comprendre que les valeurs de a et b dépendent de notre choix des états de base et qu'il existe un nombre infini de possibilités équivalentes pour le faire (similaire au nombre infini de possibilités de choisir les axes x et y dans le plan).

Contrairement au bit classique qui ne peut être que dans l'un des deux états marche ou arrêt, $\uparrow$ ou $\downarrow$, le qubit peut être dans un continuum d'états définis par

les amplitudes quantiques a et b. Contrairement au bit classique, qui est un interrupteur marche / arrêt, le qubit est un objet continu ! Deux qubits ont quatre états de base : $\uparrow\uparrow$, $\uparrow\downarrow$, $\downarrow\uparrow$ et $\downarrow\downarrow$; ainsi l'état général de deux qubits est décrit par la fonction d'onde :

$$\square\square = a\uparrow\uparrow + b\uparrow\downarrow + c\downarrow\uparrow + d\downarrow\downarrow \tag{3}$$

avec quatre amplitudes quantiques a, b, c, et d, contraintes par la condition de normalisation $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$ (et, bien sûr $|a|^2$ est la probabilité d'être dans l'état $\uparrow\uparrow$, idem pour les autres états).

Avec n qubits, il y a 2^n états de base, donc l'état général de n qubits est défini par une fonction d'onde avec 2^n amplitudes quantiques, qui sont des nombres complexes arbitraires restreints par la condition de normalisation uniquement. En revanche, un système classique de n pointeurs qui peuvent tourner librement autour de points fixes, est défini par 2^n paramètres (deux angles polaires pour chaque pointeur). Par exemple, 10 pointeurs sont décrits par $2 \times 10 = 20$ paramètres continus, tandis que 10 qubits sont caractérisés par $2^{10} = 1024$ paramètres continus. Évidemment, il est considérablement plus difficile de garder sous contrôle 1024 paramètres que 20 paramètres !

Ainsi, l'ordinateur quantique hypothétique est une machine analogique. Il a un nombre infini (continuum) d'états, définis par les valeurs de 2^n amplitudes complexes qui sont des variables continues. C'est la raison principale pour laquelle le calcul quantique est impossible : pour un nombre raisonnable de qubits ($n = 100$ ou 1000) le nombre de paramètres continus définissant l'état de notre machine (2^n) est incroyablement énorme, et en présence de bruit, erreurs, etc., il ne sera jamais possible de les garder toutes sous notre contrôle. On peut dire qu'il est exponentiellement plus difficile de construire un ordinateur quantique qu'un ordinateur analogique classique.

Correction des erreurs

En réponse à des préoccupations similaires, Peter Shor [10] et Andrew Steane [11] ont proposé une méthode de correction d'erreur quantique, basée sur la redondance, qui est une généralisation de la méthode de correction d'erreur dans les ordinateurs conventionnels (classiques), mais beaucoup plus sophistiquée. Il est largement reconnu que le calcul quantique sans correction d'erreur efficace est impossible. Expérimentalement, il existe plusieurs articles décrivant la « preuve de principe » de correction d'erreur d'un seul qubit. Le résultat le plus récent, plutôt modeste [8] consiste à augmenter la durée de vie d'un qubit corrigé unique à 320 microsecondes, soit environ deux fois plus que la durée de vie d'un qubit non corrigé. Jusqu'à présent, 25 ans après l'avancée du concept de correction d'erreur quantique, il n'existe

toujours pas de dispositif quantique, qui effectue une correction d'erreur efficace, même à très petite échelle.

Conclusion

Le champ gigantesque de l'informatique quantique avec plusieurs milliers de chercheurs actifs, des centaines de milliers de publications, de nombreuses conférences, écoles et ateliers, des annonces quotidiennes de nouvelles percées et de nombreux milliards de dollars dépensés, a été déclenché par l'invention de Shor de son célèbre algorithme de factorisation de très grands nombres (ouvrant ainsi éventuellement la porte aux ordinateurs quantiques pour casser les codes de sécurité), et par le développement de méthodes de correction d'erreur quantique, généralement considérées comme absolument indispensables.

L'euphorie mondiale de l'informatique quantique et l'excitation générale durent déjà depuis 27 ans ! Avant de s'engager pendant encore un quart de siècle, il serait peut-être judicieux de jeter un œil aux réalisations atteintes à ce jour au cours de cette période.

Le résultat observable peut se résumer comme suit :

— la factorisation du nombre 15 par l'algorithme de Shor n'est toujours pas possible ;

— la correction d'erreur n'a toujours pas été réalisée, même à très petite échelle (le calcul quantique sans correction d'erreur efficace est généralement considéré comme impossible) ;

— aucun dispositif quantique n'existe, capable de faire de l'arithmétique élémentaire, comme 3×5 ou $3 + 5$.

Ainsi, après un quart de siècle, il n'y a pas de résultats significatifs en informatique quantique. Les seules machines quantiques fonctionnelles à ce jour sont celles introduites par la société D-wave Systems en 1999, et actuellement étudiées et développées de manière intensive par Amazon, Google, IBM et d'autres géants de la technologie, ainsi que par la société D-wave elle-même. Ces machines peuvent effectuer un « recuit quantique » mais jusqu'à présent ne sont pas capables de correction d'erreurs et ne sont donc *pas* des ordinateurs quantiques au sens généralement accepté de ce terme. Elles non plus ne sont pas capables de factoriser 15, ni de calculer $3 + 5$. Cependant, ces machines sont intéressantes du point de vue scientifique et permettent d'obtenir des résultats intéressants.

En l'absence de raisons claires de croire que cette situation va changer au cours des prochaines décennies, les perspectives de l'informatique quantique semblent extrêmement douteuses.

Le scepticisme est une attitude normale et saine en science, par opposition à la religion, et il appartient au croyant de donner une preuve convaincante que le miracle

attendu est sur le point de se produire. Après 27 ans d'efforts considérables d'une armée de chercheurs, une telle preuve est toujours absente.

Le niveau sans précédent de battage médiatique et de promesses infondées accompagnant l'entreprise de calcul quantique n'est pas non plus un bon signe, de même que la multitude de propositions pour la plupart assez irresponsables du type « calcul quantique avec... ». Il est vraiment dommage qu'ils ne contiennent jamais, comme il se doit, le fameux avertissement de Landauer [2] : « Ce schéma, comme tous les autres schémas de calcul quantique, repose sur une technologie spéculative, ne prend pas en compte dans sa forme actuelle toutes les sources possibles de bruit, de manque de fiabilité et d'erreur de fabrication, et ne fonctionnera probablement pas ».

En faisant du vélo, après quelques entraînements, nous apprenons à contrôler avec succès trois degrés de liberté : la vitesse, la direction et l'angle que notre corps fait par rapport au trottoir. Un artiste de cirque parvient à conduire un vélo à une roue avec quatre degrés de liberté. Maintenant, imaginez un vélo ayant 1000 (ou plutôt 2^{1000}) articulations qui permettent des rotations libres de leurs pièces les unes par rapport aux autres. Quelqu'un sera-t-il capable de conduire cette machine ?

Il semble assez évident que nous n'aurons jamais d'ordinateur quantique.

Au lieu de cela, nous pourrions avoir des dispositifs quantiques spéciaux extrêmement coûteux fonctionnant à des températures de l'ordre du millikelvin. La saga de l'informatique quantique attend une analyse sociologique approfondie, et quelques leçons pour l'avenir devraient être tirées de cette aventure fascinante.

Une discussion plus détaillée du projet d'informatique quantique peut être trouvée dans mon livre [3].

Références

[1] David Beckman, Amalavoyal N. Chari, Srikrishna Devabhaktuni, and John Preskill. Efficient networks for quantum factoring. *Phys. Rev. A*, 54 :1034–1063, Aug 1996.

[2] M I Dyakonov. Quantum computing : A view from the enemy camp. *Optics and Spectroscopy*, 95(2) :261–267, 2003.

[3] Mikhail I. Dyakonov. *Will We Ever Have a Quantum Computer ?* Springer, Cham, 2020.

[4] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White. Experimental demonstration of a compiled version of shor's algorithm with quantum entanglement. *Phys. Rev. Lett.*, 99 :250505, Dec 2007.

[5] Erik Lucero, R Barends, Y Chen, J Kelly, M Mariantoni, A Megrant, P O'Malley, D Sank, A Vainsencher, J Wenner, T White, Y Yin, A N Cleland, and John M Martinis. Computing prime factors with a Josephson phase qubit quantum processor. *Nature Physics*, 8(10) :719–723, 2012.

[6] « Stratégie nationale sur les technologies quantiques », allocution présidentielle (Emmanuel Macron), Saclay, 21 janvier 2021.

[7] Enrique Martín-López, Anthony Laing, Thomas Lawson, Roberto Alvarez, Xiao-Qi Zhou, and Jeremy L O'Brien. Experimental realization of Shor's quantum factoring algorithm using qubit recycling. *Nature Photonics*, 6(11) :773–776, 2012.

[8] Nissim Ofek, Andrei Petrenko, Reinier Heeres, Philip Reinhold, Zaki Leghtas, Brian Vlastakis, Yehan Liu, Luigi Frunzio, S M Girvin, L Jiang, Mazyar Mirrahimi, M H Devoret, and R J Schoelkopf. Extending the lifetime of a quantum bit with error correction in superconducting circuits. *Nature*, 536(7617) :441–445, 2016.

[9] Peter W Shor. Algorithms for quantum computation : discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[10] Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52 :R2493–R2496, Oct 1995.

[11] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77 :793–797, Jul 1996.

[12] Lieven M K Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S Yannoni, Mark H Sherwood, and Isaac L Chuang. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414(6866) :883–887, 2001.