



Veille informatique quantique

12

Informatique quantique

Programme

- Explication basique des notions de physique et d'informatique quantique – **1h**
- Exercices simples de mathématiques : exercices sur les nombres complexes, les probabilités etc. et la programmation en qubits – **1h**
- Suite orienté classe inversée – **Suite et fin du cours**
 - Veille quantique sur un sujet spécifique de votre choix
 - Oral devant la classe

Informatique quantique

Sommaire

I. Introduction et mise en contexte

II. Les fondements de la physique quantique

III. Les mathématiques pour la physique quantique

IV. Les concepts de base de l'informatique quantique

V. Algorithmes quantiques et protocoles

VI. Les plateformes matérielles et la technologie quantique

VII. Avantages et limites de l'informatique quantique

VIII. Applications actuelles et futures

IX. Conclusion et perspectives

Chapitre I :

Introduction et mise en contexte

Informatique quantique

Objectifs du chapitre

- Présenter la notion de calcul et d'information telle qu'elle a évolué historiquement.
- Comprendre les limitations des systèmes de calcul classiques et les raisons qui poussent à explorer de nouvelles approches.
- Introduire les promesses de l'informatique quantique et son potentiel dans divers domaines d'application.

Informatique quantique

Structure

1. La notion de calcul et d'information
2. Pourquoi l'informatique quantique ?

Informatique quantique

1. La notion de calcul et d'information

1. La notion de calcul et d'information

1.1. Rappel de l'évolution des paradigmes de calcul classiques

1.2. Limites fondamentales des systèmes de calcul actuels (loi de Moore, miniaturisation, dissipation d'énergie)

2. Pourquoi l'informatique quantique ?

2.1. Les besoins en puissance de calcul pour des problèmes complexes (chiffrement, optimisation, simulation de systèmes moléculaires)

2.2. Présentation globale des promesses de l'informatique quantique

Informatique quantique

1.1. Rappel de l'évolution des paradigmes de calcul classiques

- Le calcul et la manipulation de données étaient initialement réalisés manuellement (abaques, tables de calcul, etc.).
- Au fil du temps, le besoin d'automatiser le calcul est devenu crucial
- **Premiers appareils mécaniques (XVIIe – XIXe siècles)**
- **Informatique émergente (XXe siècle)**
- **Ère du transistor et du microprocesseur (milieu – fin du XXe siècle)**

Informatique quantique

1.1. Le bit classique et la représentation de l'information

- Le calcul moderne repose sur la manipulation binaire de l'information : le bit, unité élémentaire, peut être 0 ou 1.
- Cette codification permet le traitement de l'information par des circuits électroniques logiques (portes AND, OR, NOT...).
- L'informatique classique se fonde alors sur des opérations séquentielles de bits, menant à des algorithmes implémentés sur des architectures de type
 - von Neumann
 - Harvard.

Informatique quantique

1.2. Limites fondamentales des systèmes de calcul actuels

Malgré les progrès fulgurants de la miniaturisation, quelques enjeux majeurs se dessinent :

- **Loi de Moore et fin de la scalabilité facile**
<https://www.youtube.com/watch?v=xZIZ3LWyhvc&t=80s>
- **Coût énergétique et dissipation thermique**
- **Complexité exponentielle de certains problèmes**

Ces limites incitent à repenser le paradigme de calcul, cherchant des alternatives pour surmonter ou contourner ces verrous.

Informatique quantique

2. Pourquoi l'informatique quantique ?

2.1. Pressions et motivations pour de nouveaux paradigmes de calcul

Face à la stagnation des performances dans l'informatique classique, la question se pose : peut-on exploiter d'autres lois fondamentales de la nature ?

La mécanique quantique, qui décrit le comportement de la matière et de la lumière à l'échelle atomique et subatomique, offre des phénomènes inédits – superposition d'états, intrication – qui n'ont pas d'équivalent dans la physique classique.

De tels phénomènes pourraient permettre de traiter l'information selon de nouveaux principes.

Informatique quantique

2. Pourquoi l'informatique quantique ?

2.2. Les nouveaux besoins en puissance de calcul

Certains problèmes particuliers sont hors de portée des supercalculateurs actuels :

- Cryptographie et factorisation
- Optimisation complexe
- Simulation quantique de la matière

Informatique quantique

2. Pourquoi l'informatique quantique ?

2.3. Présentation globale des promesses de l'informatique quantique

L'informatique quantique ne remplace pas l'informatique classique, elle la complète. Son intérêt réside dans :

- Superposition
- Intrication
- Gain de complexité sur certains algorithmes

Cette promesse doit toutefois être relativisée : l'informatique quantique est encore un domaine émergent, soumis à des défis technologiques (décohérence, correction d'erreurs, mise à l'échelle). Mais les progrès rapides du domaine et le fort intérêt de la communauté scientifique et industrielle soulignent son potentiel.

Informatique quantique

Conclusion du Chapitre I

Ce chapitre d'introduction a clarifié la position de l'informatique quantique dans l'histoire du calcul et de l'information.

Partant de la mécanique classique et du bit binaire, nous avons vu pourquoi les limites physiques et la complexité exponentielle de certains problèmes incitent à explorer un nouveau paradigme.

L'informatique quantique, exploitant les propriétés fondamentales de la mécanique quantique, ouvre ainsi des perspectives inédites.

Les chapitres suivants approfondiront les notions physiques, mathématiques et technologiques qui forment la base de ce domaine en plein essor.

Chapitre II

Les fondements

de la physique quantique

Informatique quantique

Objectifs du chapitre

- Acquérir une vision historique de l'émergence de la mécanique quantique, replacer ses découvertes clés dans le cadre plus large de l'histoire des sciences.
- Comprendre les principes fondamentaux qui différencient la physique quantique de la physique classique, en particulier la notion d'état quantique, la superposition, l'incertitude et le rôle central de la mesure.
- Saisir l'importance de la révolution conceptuelle qu'elle a induite, ainsi que les implications sur notre compréhension de la matière, de l'énergie et de l'information.

Informatique quantique

Structure

1. Contexte historique de la naissance de la physique quantique
2. Principes fondamentaux de la mécanique quantique
3. Physique quantique dans le contexte des sciences et de la technologie

Informatique quantique

1.1. Crise de la physique classique au tournant du XXe siècle

À la fin du XIXe siècle, la physique classique (mécanique newtonienne, électromagnétisme de Maxwell, thermodynamique) semblait pouvoir tout expliquer. Cependant, plusieurs phénomènes restaient mystérieux et en contradiction avec les lois établies :

- Rayonnement du corps noir
- Effet photoélectrique
- Spectres atomiques discrets

Informatique quantique

1.2. Les pionniers de la physique quantique

- Max Planck (1900)
- Albert Einstein (1905)
- Niels Bohr (1913)
- Werner Heisenberg, Erwin Schrödinger, Paul Dirac (1920-1930)

Informatique quantique

1.3. Du déterminisme classique à la vision probabiliste

Une caractéristique majeure de la physique quantique est le passage d'un déterminisme strict, hérité de Newton, à une description probabiliste et intrinsèquement incertaine des phénomènes.

Ce changement conceptuel marque une révolution dans l'histoire de la science, changeant notre compréhension des lois naturelles.

Informatique quantique

2. Principes fondamentaux de la mécanique quantique

2.1. L'état quantique et l'espace de Hilbert

Dans la mécanique quantique, l'état d'un système n'est plus décrit par une position et une vitesse précises, mais par un vecteur d'état (ou fonction d'onde) dans un espace mathématique appelé espace de Hilbert.

Ce vecteur contient toutes les informations mesurables du système.

Informatique quantique

2. Principes fondamentaux de la mécanique quantique

2.2. Superposition des états

L'un des principes clés de la mécanique quantique est que les états peuvent se superposer.

Si $|\psi_1\rangle$ et $|\psi_2\rangle$ sont deux états permis, alors une combinaison linéaire $\alpha|\psi_1\rangle + \beta|\psi_2\rangle$ est aussi un état possible.

Cette superposition conduit à des effets d'interférences, qui n'ont pas d'analogues classiques et sont cruciaux pour la puissance de calcul des futurs ordinateurs quantiques.

Informatique quantique

2. Principes fondamentaux de la mécanique quantique

2.3. Mesure et effondrement de la fonction d'onde

La mesure quantique diffère fondamentalement d'une mesure classique.

Avant la mesure, le système peut être dans une superposition d'états.

La mesure "provoque" l'effondrement de la fonction d'onde vers un état propre de l'observable mesurée.

Ce processus est probabiliste : on ne peut prédire avec certitude le résultat d'une mesure, seulement la probabilité de chaque issue.

Informatique quantique

2. Principes fondamentaux de la mécanique quantique

2.4. Le principe d'incertitude d'Heisenberg

Heisenberg a montré que certaines paires de grandeurs physiques (comme la position et la quantité de mouvement, ou l'énergie et le temps) ne peuvent pas être mesurées simultanément avec une précision arbitrairement grande.

Cette incertitude n'est pas due à des limitations technologiques, mais est un aspect fondamental de la nature quantique.

Informatique quantique

2. Principes fondamentaux de la mécanique quantique

2.5. Dualité onde-particule

En physique quantique, les objets microscopiques (électrons, photons) peuvent se comporter comme des particules ou comme des ondes, selon le contexte expérimental.

Les expériences de fentes de Young avec des électrons illustrent cette dualité : si on ne cherche pas à savoir par quelle fente passe l'électron, il donne un schéma d'interférences typiquement ondulatoire.

Informatique quantique

3. Physique quantique dans le contexte des sciences et de la technologie

3.1. Impact sur la compréhension de la matière

La mécanique quantique explique la structure électronique des atomes, la formation de liaisons chimiques, la stabilité de la matière, et les propriétés des solides (conductivité, semi-conducteurs, supraconductivité).

Sans la quantification de l'énergie, il serait impossible de comprendre la cohésion du monde microscopique.

Informatique quantique

3. Physique quantique dans le contexte des sciences et de la technologie

3.2. Avancées technologiques dérivées

La quantification et le contrôle de la matière à l'échelle atomique ont mené à d'innombrables innovations :

- Laser
- Transistor
- RMN (Résonance Magnétique Nucléaire) et IRM
- Capteurs et horloges atomiques

Informatique quantique

3. Physique quantique dans le contexte des sciences et de la technologie

3.3. Genèse de l'idée d'information quantique

Richard Feynman (années 1980) a proposé que pour simuler efficacement des systèmes quantiques, il faudrait un système quantique lui-même, ouvrant la voie à l'idée d'un "ordinateur quantique".

David Deutsch a formalisé le concept d'information quantique et jeté les bases du calcul quantique.

L'information quantique tire parti des fondements de la mécanique quantique (superposition, intrication) pour développer un nouveau type de calcul.

Informatique quantique

Conclusion du Chapitre II

Ce chapitre a présenté le contexte historique et les fondements conceptuels de la physique quantique. De la crise de la physique classique aux développements théoriques de Planck, Einstein, Bohr, Heisenberg, Schrödinger et Dirac, la mécanique quantique a renouvelé notre vision du monde microscopique.

Elle offre un cadre probabiliste et non intuitif, où la superposition, l'intrication et le rôle central de la mesure bouleversent nos repères classiques.

Les retombées technologiques et conceptuelles de cette révolution ont non seulement transformé la physique et la chimie, mais aussi préparé la voie à l'émergence de l'informatique quantique, qui exploite pleinement ces principes fondamentaux.

Le chapitre suivant approfondira les outils mathématiques nécessaires à la description formelle des systèmes quantiques, préalable indispensable à la compréhension de l'informatique quantique.

Informatique quantique

Perspectives

Au choix :

- Vidéo accessible de Arte :
https://www.youtube.com/watch?v=cJjmx3MEB3U&ab_channel=ARTE
- Vidéo un peu poussée de Science Étonnante :
https://www.youtube.com/watch?v=1hVm_SyUcwE&ab_channel=ScienceEtonnante

Chapitre III

Les mathématiques pour la physique quantique

Informatique quantique

Objectifs du chapitre

Comprendre pourquoi les mathématiques utilisées en physique quantique sont un peu différentes de celles utilisées en physique classique.

Se familiariser avec les notions de base sur les vecteurs, les opérateurs (un type de “fonctions” mathématiques), et les nombres complexes.

Voir comment on passe d’un point de vue purement mathématique à la description des systèmes quantiques, qui servent de fondations à l’informatique quantique.

Informatique quantique

Structure

Pourquoi des mathématiques "différentes" ?

Les espaces de Hilbert : un "endroit" où vivent les états quantiques

Les opérateurs : des "outils" pour changer et mesurer les états

Les portes quantiques : l'équivalent quantique des portes logiques classiques

Informatique quantique

Pourquoi des mathématiques "différentes" ?

En physique classique, on décrit souvent la position, la vitesse ou l'accélération d'un objet avec des nombres simples. On résout des équations du type "lois de Newton" pour savoir où ira une balle, par exemple.

En mécanique quantique, l'état d'une particule (comme un électron) n'est pas juste un nombre ou une position précise, mais plutôt un "vecteur" qui contient toutes les informations possibles sur cet état.

De plus, ces vecteurs ne sont pas seulement décrits avec des nombres réels (comme 2, 3, ou 3,14), mais aussi avec des nombres complexes (avec la forme $a + bi$, où i est la racine carrée de -1)

Ces mathématiques peuvent sembler un peu moins intuitives, mais elles sont très puissantes pour décrire des phénomènes où la notion de certitude et de position exacte s'efface, et où les probabilités et les superpositions d'états jouent un rôle central.

Informatique quantique

Les espaces de Hilbert : un "endroit" où vivent les états quantiques

Un espace de Hilbert est, en simplifiant, un "espace mathématique" spécial, un peu comme un grand "contenant" où l'on peut mettre des vecteurs. Chaque vecteur représente l'état d'un système quantique. Par exemple, si on a un système simple comme un qubit (l'équivalent quantique d'un bit classique), son état peut être vu comme un point dans cet espace.

Vecteurs et bases : Pour décrire un état, on choisit une "base", un peu comme un système de repères. Par exemple, pour un qubit, on a deux états de base souvent notés $|0\rangle$ et $|1\rangle$. Tout état possible du qubit peut s'écrire comme une combinaison de $|0\rangle$ et $|1\rangle$. On dit alors que l'état du qubit est une "superposition" de ces deux états de base.

Nombres complexes et amplitudes de probabilité : Quand on dit qu'un qubit est dans une combinaison $\alpha|0\rangle + \beta|1\rangle$, les coefficients α et β sont des nombres complexes. Le carré de leur "longueur" (leur module) indique la probabilité de mesurer l'état $|0\rangle$ ou $|1\rangle$. C'est grâce à ces coefficients complexes que la mécanique quantique peut décrire des phénomènes très étranges et contre-intuitifs par rapport à notre expérience quotidienne.

Informatique quantique

Les opérateurs : des "outils" pour changer et mesurer les états

Un opérateur est, en mathématiques, comme une "fonction" qui prend un vecteur (un état) et le transforme en un autre vecteur (un autre état). En mécanique quantique, les opérateurs servent à :

Décrire l'évolution d'un système dans le temps : On utilise des opérateurs "unitaires" pour faire évoluer un état d'un instant à un autre, sans perdre d'information. Par exemple, l'équation de Schrödinger, qui décrit comment un état évolue, peut se comprendre comme l'application d'un opérateur à votre état quantique.

Représenter les mesures : Quand on mesure une grandeur physique (comme la position ou le spin), on utilise un opérateur "hermitien" qui a des valeurs propres (des sortes de "résultats possibles"). La mécanique quantique dit que quand vous faites une mesure, l'état "s'effondre" sur un de ces résultats, avec une certaine probabilité.

Comprendre la structure des systèmes multiples : Pour décrire plusieurs qubits ensemble, on utilise le "produit tensoriel", une façon d'assembler deux espaces de Hilbert (par exemple celui d'un qubit A et celui d'un qubit B) pour obtenir un espace plus grand. Dans cet espace plus grand, vous pouvez décrire non seulement des états séparés, mais aussi des états intriqués où les qubits sont fortement reliés.

Informatique quantique

Les portes quantiques : l'équivalent quantique des portes logiques classiques

Vous savez que les portes logiques (AND, OR, NOT) transforment des bits d'entrée en bits de sortie. En informatique quantique, on a des "portes quantiques", qui sont des opérateurs unitaires appliqués aux qubits. Par exemple, la porte Hadamard transforme $|0\rangle$ en une superposition égale de $|0\rangle$ et $|1\rangle$, créant ainsi un état où la mesure devient incertaine (50% $|0\rangle$, 50% $|1\rangle$).

Ces portes quantiques sont mathématiquement représentées par des matrices unitaires, c'est-à-dire des tableaux de nombres complexes qui, lorsqu'ils agissent sur nos vecteurs (états des qubits), produisent de nouveaux états. Certaines portes, comme la porte CNOT, permettent d'intriquer deux qubits, ce qui est essentiel pour tirer profit de la puissance du calcul quantique.

Exercices

Informatique quantique

Exercice 1 : Manipulation de nombres complexes simples

- **Énoncé :**

1. Soit le nombre complexe $z = 3 + 4i$.
 - a. Calculer son module $|z|$.
 - b. Normaliser ce nombre en construisant $z' = z/|z|$ de sorte que $|z'| = 1$.
2. Donner un nombre complexe w tel que $|w| = 1$ et $w \neq 1$. (Par exemple, choisir $w = e^{i\theta}$ pour un certain angle θ .)
3. Interpréter géométriquement le fait qu'un nombre complexe de module 1 puisse représenter une "phase" ou une rotation dans le plan complexe.

Informatique quantique

Exercice 2 : Probabilités et amplitudes complexes pour un qubit

- **Énoncé :**

Considérons un "état" (purement imaginaire pour l'analogie) représentant un qubit :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

où $\alpha = (\sqrt{2})/2$ et $\beta = (\sqrt{2})/2 * i$.

1. Vérifier que $|\alpha|^2 + |\beta|^2 = 1$.

Rappeler que $|x + yi|^2 = x^2 + y^2$ pour un nombre complexe $x + yi$.

2. Interpréter le sens de $|\alpha|^2$ et $|\beta|^2$ comme des probabilités.

Quelles sont les probabilités de trouver le qubit dans l'état $|0\rangle$ et dans l'état $|1\rangle$?

3. Si on devait programmer un tirage aléatoire pour simuler une mesure, on génère un nombre aléatoire r entre 0 et 1. Si $r < |\alpha|^2$, on conclut que le résultat de la mesure est "0", sinon c'est "1". Mettre cela en perspective avec un code informatique.

Informatique quantique

Exercice 3 : Probabilités et distributions

- **Énoncé :**

On considère un système pouvant donner trois résultats distincts A, B ou C. Supposons qu'avant la mesure, l'état du système indique que les probabilités sont : $P(A) = 1/2$, $P(B) = 1/3$ et $P(C) = 1/6$.

1. Vérifier que la somme des probabilités vaut 1.
2. Calculer l'espérance si on associe à chaque résultat une valeur numérique, par exemple $A = 0$, $B = 1$, $C = 2$.
3. Comparer avec un tirage classique en programmation. Comment simuler un tel système en code (pseudo-code) pour illustrer un comportement probabiliste, comme pour un état quantique à plusieurs résultats ?

Informatique quantique

Exercice 4 : Nombres complexes et matrices 2x2 (introduction)

- **Énoncé :**

Dans un contexte quantique, une porte logique sur un qubit peut être représentée par une matrice 2x2 unitaire. Considérons la matrice de Hadamard H définie par :

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

1. Vérifier qu'appliquer H à l'état $|0\rangle = (1, 0)$ donne un état superposé $(|0\rangle + |1\rangle)/\sqrt{2}$.
2. Exprimer cet état en notation complexe et calculer les probabilités d'obtenir $|0\rangle$ ou $|1\rangle$ si on mesure cet état.
3. Mettre en perspective : dans un programme, cette opération revient à multiplier un vecteur complexe par une matrice unitaire, ce qui simule l'application d'une porte quantique.

Chapitre IV

Les concepts de base de l'informatique quantique

Informatique quantique

Objectifs du chapitre

- Découvrir le « qubit », l'unité fondamentale de l'information quantique, et voir en quoi il diffère du bit classique.
- Comprendre les notions de superposition et d'intrication, deux propriétés clés qui distinguent l'informatique quantique de l'informatique classique.
- Découvrir les portes quantiques et les circuits quantiques, qui permettent de réaliser des opérations sur des qubits.

Informatique quantique

Structure

- Le qubit : l'unité élémentaire de l'information quantique
- Superposition et intrication : deux ressources quantiques essentielles
- Mesure et lecture de l'information quantique
- Les portes quantiques et les circuits

Informatique quantique

1. Le qubit : l'unité élémentaire de l'information quantique

- Dans un ordinateur classique, l'information est codée avec des bits qui valent soit 0, soit 1. C'est binaire, tout est noir ou blanc. En informatique quantique, on utilise des « qubits », qui sont comme des bits mais en version quantique.
- Un qubit peut être vu comme un état entre $|0\rangle$ et $|1\rangle$. Au lieu d'être juste 0 ou 1, il peut être dans une combinaison des deux. Cela ne veut pas dire qu'il est « entre » 0 et 1 de façon floue, mais plutôt qu'il a les deux possibilités « en même temps », jusqu'à ce qu'on le mesure. Cette propriété, appelée superposition, est la base de la puissance de l'informatique quantique.

Informatique quantique

2. Superposition et intrication : deux ressources quantiques essentielles

- La superposition : Imaginez une pièce de monnaie. Avant de la lancer, vous ne savez pas si elle va tomber sur face ou pile. Mais ce n'est pas qu'elle est dans les deux états à la fois, juste que vous l'ignorez. Le qubit, lui, est réellement dans une combinaison de plusieurs états (0 et 1) simultanément. Cette possibilité de « calcul parallèle » à l'échelle quantique est ce qui permet à certains algorithmes quantiques d'être plus rapides.
- L'intrication (enchevêtrement) : L'intrication est un phénomène encore plus surprenant. Si vous avez deux qubits intriqués, les mesurer, c'est comme si l'état de l'un dépendait instantanément de l'état de l'autre, même s'ils sont très éloignés l'un de l'autre. Cela ne signifie pas que l'information voyage plus vite que la lumière, mais que les deux qubits partagent un état commun. Cette corrélation extrêmement forte n'existe pas dans le monde classique et constitue une ressource précieuse pour le calcul et la communication quantiques.

3. Mesure et lecture de l'information quantique

- La mesure d'un qubit est un acte un peu « destructeur » dans le sens où, une fois mesuré, le qubit n'est plus en superposition. Il « choisit » l'un des deux résultats possibles, avec une certaine probabilité. Par exemple, si un qubit était dans un état avec 50% de chance d'être $|0\rangle$ et 50% de chance d'être $|1\rangle$, une fois la mesure effectuée, il ne vous donnera qu'un résultat : 0 ou 1. Après la mesure, il ne reste plus que ce résultat, et l'état de superposition disparaît.
- Cette opération de mesure, particulièrement délicate, fait de la lecture de l'information quantique un véritable défi. C'est comme observer une bulle de savon : dès que vous la touchez, elle éclate.

Informatique quantique

4. Les portes quantiques et les circuits

- Dans un ordinateur classique, des portes logiques (ET, OU, NON) transforment les bits d'entrée en bits de sortie. En informatique quantique, on a également des portes, mais elles sont « quantiques ». Cela signifie qu'elles sont représentées par des opérations unitaires (détaillées au chapitre précédent, mais qu'on peut juste voir comme des transformations réversibles) qui agissent sur les qubits en conservant leur nature quantique.
- Quelques portes quantiques de base :
 - La porte Hadamard, qui crée des superpositions équilibrées.
 - Les portes Pauli (X, Y, Z), un peu comme des opérations de rotation qui transforment $|0\rangle$ en $|1\rangle$, ou changent la phase de l'état.
 - La porte CNOT, qui peut intriquer deux qubits, crucial pour construire des algorithmes quantiques puissants.
- En combinant ces portes, on forme des circuits quantiques, un peu comme des circuits électroniques, mais destinés à manipuler des qubits. Ces circuits constituent la base des algorithmes quantiques, qui peuvent résoudre certains problèmes plus rapidement que des algorithmes classiques.

Chapitre V

Algorithmes quantiques et protocoles

Informatique quantique

Objectifs du chapitre

- Découvrir comment les algorithmes quantiques utilisent la superposition et l'intrication pour résoudre certains problèmes plus vite qu'un ordinateur classique.
- Présenter quelques algorithmes quantiques célèbres (Shor, Grover, etc.) et leurs implications.
- Introduire la téléportation quantique et la correction d'erreurs, qui sont des briques essentielles pour réaliser des calculs quantiques fiables.

Informatique quantique

Structure

- Qu'est-ce qu'un algorithme quantique ?
- Des exemples marquants : Shor et Grover
- Téléportation quantique et communication sécurisée
- Correction d'erreurs quantiques

Informatique quantique

1. Qu'est-ce qu'un algorithme quantique ?

- Un algorithme quantique est une liste d'instructions, comme un algorithme classique, mais conçu pour un ordinateur quantique. Il utilise les propriétés quantiques (superposition, intrication) pour effectuer certaines opérations de façon plus efficace que les méthodes classiques.
- L'idée est la suivante : alors qu'un ordinateur classique essaie différentes solutions l'une après l'autre, un ordinateur quantique peut, dans certains cas, exploiter la superposition pour « explorer » plusieurs solutions en parallèle, puis, grâce à des interférences intelligemment contrôlées, amplifier la bonne solution et atténuer les autres.
- Tous les problèmes ne deviennent pas faciles pour autant. Mais pour certains d'entre eux, les algorithmes quantiques offrent un gain de vitesse impressionnant.

Informatique quantique

2. Des exemples marquants : Shor et Grover

- **L'algorithme de Shor (1994)** : Cet algorithme est célèbre car il permet de factoriser de grands nombres entiers beaucoup plus rapidement qu'un ordinateur classique. Cela a de grandes implications pour la cryptographie, car la sécurité de nombreux systèmes de chiffrement sur Internet repose sur la difficulté de factoriser des nombres géants. Avec un ordinateur quantique suffisamment puissant, l'algorithme de Shor pourrait briser ces codes.
- **L'algorithme de Grover (1996)** : Grover a montré comment chercher un élément précis dans une liste non triée (par exemple, chercher un nom dans un annuaire gigantesque) plus rapidement qu'un ordinateur classique. Bien que le gain ne soit pas aussi spectaculaire que celui de Shor (il n'est pas exponentiel, mais « seulement » quadratique), c'est déjà un exploit, car il démontre que l'informatique quantique peut accélérer certaines tâches de recherche et d'optimisation.
- D'autres algorithmes quantiques utilisent la « Transformée de Fourier Quantique » (une opération mathématique quantique clé) comme brique de base pour effectuer des calculs complexes plus vite que leurs homologues classiques.

3. Téléportation quantique et communication sécurisée

- La téléportation quantique n'a rien à voir avec la téléportation de personnes dans la science-fiction, mais consiste à transmettre l'état complet d'un qubit d'un endroit à un autre sans le mesurer, à l'aide de paires intriquées et de mesures judicieuses. On ne « déplace » pas la matière, mais on envoie l'information quantique de manière parfaitement reconstruite à l'arrivée.
- Ce concept est la base de protocoles de communication quantique ultra-sécurisés. Par exemple, le chiffrement quantique et la distribution de clés quantiques garantissent une sécurité théorique à toute tentative d'espionnage, car la simple tentative de lire l'information quantique modifie l'état et se détecte aussitôt.

4. Correction d'erreurs quantiques

- La mécanique quantique est fragile. Les qubits sont sensibles au moindre bruit, à la chaleur, aux perturbations de l'environnement, ce qui provoque des erreurs. Pour construire un ordinateur quantique fiable, il faut des codes de correction d'erreurs quantiques qui permettent de détecter et de corriger ces erreurs sans détruire l'information quantique.
- Contrairement à l'informatique classique, où on peut facilement recopier un bit (0 ou 1), copier un qubit est très compliqué à cause de la mécanique quantique (c'est le « no-cloning theorem »). Les méthodes de correction d'erreurs quantiques contournent ce problème avec des techniques mathématiques sophistiquées, en utilisant plusieurs qubits pour protéger l'information et s'approcher d'un calcul quantique « tolérant aux fautes ».

Chapitre VI

Plateformes matérielles et technologie quantique

Informatique quantique

Objectifs du chapitre

- Découvrir les différentes manières de construire physiquement des qubits, les défis qu'elles posent et leurs avantages respectifs.
- Comprendre pourquoi il est difficile de fabriquer un ordinateur quantique stable et fiable.
- Avoir un aperçu du paysage industriel, des acteurs majeurs et des progrès récents.

Informatique quantique

Structure

- Comment fabriquer un qubit dans le monde réel ?
- Les défis expérimentaux : stabilité, cohérence et environnement
- Les principaux candidats et plateformes technologiques
- Le paysage industriel et les avancées récentes

Informatique quantique

1. Comment fabriquer un qubit dans le monde réel ?

Un qubit n'est pas une simple abstraction mathématique. Pour faire de l'informatique quantique, il faut un support physique pour le qubit. Il existe plusieurs manières d'en créer un, en utilisant des particules ou des systèmes quantiques qui peuvent prendre deux états distincts. Par exemple, on peut utiliser :

- Des ions piégés : On utilise des ions (atomes chargés) confinés dans un champ électrique. Les états quantiques de leurs niveaux d'énergie servent de $|0\rangle$ et $|1\rangle$.
- Des circuits supraconducteurs : De minuscules « boucles » de matériau supraconducteur refroidies à très basse température, dans lesquelles des courants quantiques peuvent circuler. On encode l'information quantique dans les états électromagnétiques de ces circuits.
- Des photons : Les particules de lumière peuvent aussi servir de qubits, codant l'information dans la polarisation de la lumière, par exemple.
- Des spins d'électrons ou de noyaux atomiques : Le « spin » est une propriété quantique des particules, et on peut utiliser ce spin comme un qubit.

Chaque méthode a ses avantages et ses inconvénients. Le choix d'une plateforme dépend de critères comme la facilité de fabrication, la stabilité des qubits, leur temps de cohérence, la possibilité de les connecter entre eux, etc.

Informatique quantique

2. Les défis expérimentaux : stabilité, cohérence et environnement

- La mécanique quantique est fragile. Un qubit est très sensible à son environnement : une vibration, une fluctuation de température, un champ électromagnétique parasite peuvent provoquer la décohérence, c'est-à-dire la perte de l'état quantique « pur » et de l'intrication. Une fois la décohérence survenue, le qubit se comporte comme un bit classique et l'ordinateur quantique perd son avantage.
- Il faut donc isoler soigneusement les qubits, par exemple en travaillant à des températures proches du zéro absolu ($-273,15^{\circ}\text{C}$), dans des chambres à vide ultra-pures, et en réduisant au minimum tout bruit ou interférence. Cet isolement demande une technologie de pointe et des conditions extrêmes, ce qui rend la construction d'un ordinateur quantique complexe et coûteuse.

Informatique quantique

3. Les principaux candidats et plateformes technologiques

- **Qubits supraconducteurs** : Très populaires, ils sont utilisés par des entreprises comme IBM et Google. Ils sont faciles à contrôler avec des micro-ondes, mais nécessitent un refroidissement cryogénique poussé.
- **Ions piégés** : Les qubits sont très cohérents (ils gardent leur état plus longtemps), mais sont plus difficiles à mettre à l'échelle (à construire en grande quantité). IonQ, par exemple, est une entreprise qui travaille sur cette technologie.
- **Photons** : Les qubits de photons ont l'avantage de voyager facilement dans la fibre optique, ce qui est pratique pour la communication quantique. En revanche, les interactions entre photons pour créer des portes quantiques sont plus délicates.
- **Spins dans des semi-conducteurs ou des centres colorés dans le diamant** : Ces qubits peuvent être plus compacts et s'intégrer à la technologie du silicium, mais le contrôle et la mise à l'échelle sont encore des défis.

Dans la recherche actuelle, il n'y a pas encore de "gagnant" clair. On explore plusieurs approches en parallèle, en espérant trouver le chemin le plus efficace vers un ordinateur quantique capable de gérer des milliers, voire des millions de qubits.

Informatique quantique

4. Le paysage industriel et les avancées récentes

Aujourd'hui, non seulement les laboratoires de recherche académiques, mais aussi de grandes entreprises (IBM, Google, Microsoft, Intel) et des startups spécialisées (Rigetti, IonQ, Xanadu, etc.) investissent massivement dans l'informatique quantique. Les gouvernements et les institutions publiques soutiennent aussi ces efforts, voyant dans l'informatique quantique une technologie stratégique.

- **Prototypes disponibles dans le cloud** : Certains acteurs permettent déjà d'accéder à de petits ordinateurs quantiques via Internet. Même s'ils sont encore limités, ils permettent aux chercheurs et aux développeurs de tester des algorithmes quantiques sur du matériel réel.
- **Course à la « suprématie quantique »** : Des annonces comme celle de Google en 2019 (réalisation d'un calcul spécifique plus rapide qu'un supercalculateur classique) montrent les premiers jalons. Cependant, le chemin reste long avant qu'un ordinateur quantique pleinement pratique et très puissant soit disponible.

Chapitre VII

Avantages et limites de l'informatique quantique

Informatique quantique

Objectifs du chapitre

Comprendre pourquoi l'informatique quantique suscite autant d'intérêt : quelles tâches peut-elle accélérer, et dans quels domaines peut-elle apporter une véritable différence ?

Réaliser que, malgré le potentiel, la technologie en est encore à ses débuts et comporte de nombreuses contraintes.

Appréhender la notion de calcul tolérant aux fautes, indispensable pour rendre les ordinateurs quantiques réellement utiles et fiables.

Informatique quantique

1. Les avantages théoriques : quand l'informatique quantique brille

L'informatique quantique promet d'accélérer la résolution de certains problèmes :

- **Factorisation et cryptographie** : L'algorithme de Shor, évoqué précédemment, pourrait casser les schémas de chiffrement classiques basés sur la difficulté de la factorisation d'entiers. Cela donne à l'informatique quantique un poids énorme dans le domaine de la sécurité et de la confidentialité des données.
- **Simulation de systèmes quantiques complexes** : Simuler de grosses molécules, des réactions chimiques, ou certains matériaux sur des ordinateurs classiques est très difficile, parfois impossible, parce que le comportement de ces systèmes est lui-même quantique. Un ordinateur quantique, étant quantique par nature, peut en principe reproduire ces phénomènes bien plus efficacement. Cela pourrait accélérer la recherche de nouveaux médicaments, de nouveaux matériaux et de nouveaux catalyseurs chimiques.
- **Optimisation et intelligence artificielle** : De nombreuses tâches en logistique, finance, et même en apprentissage machine, sont liées à des problèmes mathématiques complexes. Certains algorithmes quantiques offrent des vitesses de résolution améliorées, aidant potentiellement à trouver plus rapidement des solutions optimales à des problèmes difficiles.

En résumé, l'informatique quantique ne fera pas tout plus vite, mais pour certains problèmes spécifiques, elle promet des gains spectaculaires, parfois impossibles à obtenir avec un ordinateur classique, même très puissant.

Informatique quantique

2. Les limites actuelles : des obstacles à surmonter

Cependant, ces promesses s'accompagnent de nombreuses difficultés :

- **Décohérence et erreurs** : Les qubits sont fragiles. Ils perdent rapidement leur caractère quantique s'ils ne sont pas parfaitement isolés. Cela crée des erreurs, qui faussent les résultats des calculs.
- **Coûts et complexité expérimentale** : Maintenir un ordinateur quantique dans des conditions extrêmes (températures ultra-basses, vide poussé, etc.) demande un matériel coûteux et complexe. À l'heure actuelle, cela limite la taille et la performance des machines.
- **Manque de qubits de qualité et de quantité** : Pour profiter pleinement des algorithmes quantiques, il faut des dizaines, des centaines, voire des milliers de qubits fiables. Aujourd'hui, on atteint difficilement quelques dizaines de qubits « cohérents ». L'augmentation à grande échelle (la « mise à l'échelle ») est un défi majeur.

Ces limites font que, pour le moment, l'informatique quantique en est encore au stade de la recherche et du développement, avec des démonstrations de principe et des prototypes, mais sans application industrielle véritablement révolutionnaire disponible dès maintenant.

Informatique quantique

3. Vers l'informatique quantique tolérante aux fautes

Pour que l'informatique quantique devienne vraiment pratique, il faut parvenir à corriger les erreurs et à rendre le calcul « tolérant aux fautes ». Cela signifie construire une architecture dans laquelle, même si chaque qubit est imparfait, l'ordinateur dans son ensemble peut continuer à calculer correctement sur de longues durées.

- **Codes de correction d'erreurs quantiques** : Comme mentionné dans le chapitre précédent, ces codes permettent de repérer et de corriger les erreurs sans détruire les informations quantiques. C'est un domaine de recherche actif et complexe, mais essentiel.
- **Seuil de tolérance aux erreurs** : Les chercheurs cherchent à atteindre un taux d'erreur par opération suffisamment bas pour que, combiné avec des codes de correction, l'ordinateur puisse fonctionner de façon fiable à grande échelle. On parle souvent de « seuil » : en dessous d'un certain pourcentage d'erreurs, la correction d'erreurs devient efficace, et on peut ainsi grossir l'ordinateur quantique sans que tout s'effondre.

Parvenir à construire une machine tolérante aux fautes serait un tournant majeur, car cela signifierait pouvoir réellement exploiter la puissance de l'informatique quantique dans des conditions industrielles.

Chapitre VIII

Applications actuelles et futures

Informatique quantique

Objectifs du chapitre

Illustrer comment l'informatique quantique peut améliorer, à moyen ou long terme, divers domaines : chimie, matériaux, optimisation, cryptographie.

Montrer que certaines premières applications sont déjà à l'étude, malgré l'immaturité de la technologie.

Souligner l'importance des applications dans le développement et le financement de la recherche en informatique quantique.

Informatique quantique

Structure

Chimie, science des matériaux et recherche médicale

Optimisation, logistique et finance

Cryptographie, sécurité et communication quantique

Vers des domaines plus lointains : intelligence artificielle quantique et physique fondamentale

Informatique quantique

1. Chimie, science des matériaux et recherche médicale

La simulation quantique de molécules et de matériaux est une des applications les plus prometteuses de l'informatique quantique. Aujourd'hui, même les supercalculateurs ont du mal à prédire précisément les propriétés de molécules complexes, ou à simuler avec exactitude les réactions chimiques.

Avec un ordinateur quantique, on pourrait :

- **Accélérer la découverte de nouveaux médicaments** : En simulant finement la manière dont les molécules interagissent avec les protéines du corps humain, les chercheurs pourraient mieux concevoir de nouveaux médicaments, plus ciblés et plus efficaces.
- **Concevoir de nouveaux matériaux** : Des matériaux à haute conductivité, plus solides, plus légers ou résistants à la corrosion pourraient être découverts en simulant plus rapidement et plus précisément leurs structures électroniques.
- **Optimiser des procédés industriels** : Réduire les coûts et l'impact environnemental de certaines réactions chimiques ou processus de production.

Informatique quantique

2. Optimisation, logistique et finance

De nombreux problèmes en logistique, transport, planification ou finance sont des casse-têtes mathématiques extrêmement complexes. Par exemple, trouver le meilleur itinéraire pour des centaines de livreurs, ou la meilleure combinaison d'actifs financiers pour un portefeuille, peut vite devenir très difficile à résoudre classiquement.

Certains algorithmes quantiques offrent des gains de vitesse ou de précision pour ces problèmes d'optimisation. À terme, cela pourrait :

- **Améliorer la gestion des chaînes d'approvisionnement** : Réduire les coûts et les délais, limiter l'empreinte carbone.
- **Aider en finance** : Évaluer plus rapidement le risque de certains placements, trouver les meilleures stratégies d'investissement.
- **Rendre l'intelligence artificielle et le machine learning plus puissants** : Même si ce domaine est encore très exploratoire, certaines approches de machine learning quantique (QML) pourraient accélérer la formation de modèles complexes.

Informatique quantique

3. Cryptographie, sécurité et communication quantique

Comme vu dans les chapitres précédents, l'arrivée d'un ordinateur quantique suffisamment puissant pourrait menacer les systèmes de chiffrement classiques (comme RSA) en rendant la factorisation plus facile.

Cependant, l'informatique quantique apporte aussi des solutions :

- **Cryptographie post-quantique** : Les chercheurs travaillent déjà à développer de nouvelles méthodes de chiffrement résistantes aux attaques quantiques.
- **Distribution quantique de clés (QKD)** : Il est déjà possible, avec des systèmes optiques, de distribuer des clés cryptographiques de manière ultra-sécurisée. Toute tentative d'écouter la ligne perturbe les états quantiques et se détecte immédiatement. Ce type de communication quantique protégée pourrait devenir un standard de sécurité dans l'avenir.

Informatique quantique

4. Vers des domaines plus lointains : intelligence artificielle quantique et physique fondamentale

À plus long terme, on peut imaginer :

- **Intelligence artificielle quantique** : Appliquer les concepts quantiques à des algorithmes d'apprentissage automatique pourrait permettre de résoudre des problèmes que l'IA classique a du mal à traiter, ou d'accélérer l'entraînement de certains modèles complexes.
- **Recherche fondamentale en physique** : Simuler des systèmes quantiques exotiques, explorer des théories complexes sur la gravité quantique, mieux comprendre la structure de l'espace-temps, sont des directions où l'informatique quantique pourrait apporter de nouveaux outils conceptuels.

Pour le moment, ces applications sont encore très spéculatives, mais elles montrent que le champ des possibles est vaste.

Chapitre IX

Conclusion et perspectives

Informatique quantique

Objectifs du chapitre

Récapituler les notions fondamentales vues dans les chapitres précédents : du cadre théorique aux applications concrètes.

Mettre en évidence les enjeux actuels et futurs : défis techniques, formation, réglementation, collaboration internationale.

Donner des pistes pour approfondir et rester informé des avancées rapides dans ce domaine.

Informatique quantique

Structure

Récapitulatif des acquis

Les défis encore à relever

Les perspectives et les dynamiques du domaine

Informatique quantique

1. Récapitulatif des acquis

Au cours des précédents chapitres, nous avons :

- **Compris les fondements quantiques** : La physique quantique, avec ses concepts de superposition et d'intrication, fournit la base théorique sur laquelle repose l'informatique quantique.
- **Vu les outils mathématiques et informatiques** : L'espace de Hilbert, les opérateurs unitaires, les portes quantiques, et la façon de décrire et manipuler un qubit.
- **Exploré les algorithmes et protocoles** : Des algorithmes emblématiques (Shor, Grover) qui démontrent la puissance potentielle du calcul quantique, ainsi que la téléportation quantique et la correction d'erreurs.
- **Découvert les défis matériels** : Différentes approches matérielles pour fabriquer des qubits, et la difficulté de maintenir la cohérence quantique et de mettre à l'échelle un système de plusieurs centaines ou milliers de qubits.
- **Examiné les avantages et les limites** : Le potentiel de résolution de problèmes complexes, mais aussi la fragilité actuelle des machines quantiques et l'importance des codes correcteurs d'erreurs.
- **Analysé les applications potentielles** : De la chimie à la cryptographie, en passant par l'optimisation et la finance, l'informatique quantique pourrait un jour changer la donne dans de nombreux domaines.

Informatique quantique

2. Les défis encore à relever

- Malgré l'enthousiasme et les progrès réalisés :
- **Mise à l'échelle** : Passer de quelques qubits à des centaines, voire des milliers, reste un défi majeur. Plus on a de qubits, plus le système devient difficile à stabiliser.
- **Fiabilité et correction d'erreurs** : Les taux d'erreurs doivent être suffisamment faibles et compensés par la correction d'erreurs quantiques pour permettre des calculs de longue durée.
- **Coûts et accessibilité** : Le matériel nécessaire est cher et complexe, ce qui limite la disponibilité des machines quantiques. Il faudra du temps et des efforts pour rendre cette technologie plus abordable.
- **Formation et compétences** : L'informatique quantique requiert un ensemble de compétences pointues (physique quantique, mathématiques, informatique, ingénierie). Former une nouvelle génération d'ingénieurs, de chercheurs et de développeurs est essentiel.

Informatique quantique

3. Les perspectives et les dynamiques du domaine

L'informatique quantique évolue rapidement :

- **Collaboration internationale** : Des programmes publics (Union Européenne, États-Unis, Chine, etc.), privés (entreprises technologiques, startups), et des partenariats entre universités et industries accélèrent la recherche.
- **Émergence d'un écosystème** : Des logiciels quantiques, des simulateurs, des langages de programmation dédiés (Qiskit, Cirq, etc.) sont déjà disponibles. Même s'ils tournent sur des machines encore limitées, ils familiarisent les ingénieurs et les scientifiques avec ce nouveau paradigme.
- **Innovation continue** : De nouvelles idées émergent chaque année, qu'il s'agisse de méthodes de fabrication, de protocoles plus robustes, ou d'algorithmes quantiques plus efficaces.
- **Quid de la régulation et de l'éthique ?** : À plus long terme, l'usage de l'informatique quantique pourrait soulever des enjeux éthiques, de sécurité et de régulation internationale, en particulier si elle bouleverse les méthodes de cryptage et la protection des données.

Informatique quantique

Conclusion

Dans les années et décennies à venir, l'informatique quantique pourrait devenir un outil standard de l'ingénieur, du scientifique et de l'industriel, au même titre que l'informatique classique l'est aujourd'hui.

En attendant, il s'agit d'un domaine passionnant, en évolution rapide, qui réunit des personnes de tous horizons (physique, mathématiques, informatique, ingénierie) pour repousser les frontières de ce qui est calculable.

Informatique quantique

Ateliers

1. Exploration des Qubits et des Portes Logiques (2 heures)
Activité pratique : Utiliser un simulateur d'informatique quantique (comme IBM Quantum Experience ou Qiskit) pour construire des circuits quantiques simples.
Exercice : Réaliser des opérations avec des portes quantiques comme X, H, CNOT et mesurer les résultats.
2. Introduction aux Algorithmes Quantique (1.5 heure)
Théorie : Présenter l'algorithme de Grover (recherche dans une base de données non triée) et l'algorithme de Shor (factorisation).
Activité : Simuler un exemple simplifié de l'algorithme de Grover avec un faible nombre de qubits.
3. Cryptographie Quantique et Protocoles (1.5 heure)
Explication : Introduire la cryptographie quantique, comme le protocole BB84 pour le partage de clés.
Activité : Faire un jeu de rôle où vous simulez un échange de clés sécurisé en utilisant les concepts de qubits polarisés.
4. Défis et Applications Réels (1 heure)
Débat : Les défis actuels en informatique quantique (bruit, décohérence, etc.).
Cas pratiques : Discuter des domaines d'application (chimie quantique, optimisation, finance).
5. Atelier Final : Construire un Problème et le Résoudre (1 heure)
Objectif : Par petits groupes, concevez un problème simple que l'informatique quantique pourrait résoudre. Ensuite, proposez une solution théorique ou simulez là sur un outil.

Informatique quantique

Atelier 1

1. Exploration des Qubits et des Portes Logiques (2 heures)
 - Créer un compte Quantum sur IBM : <https://quantum-computing.ibm.com/>
 - Utilise Qiskit, un SDK Python open-source pour travailler avec des ordinateurs quantiques. <https://docs.quantum.ibm.com/start/hello-world>
 - Installer Python et pip si pas déjà fait, puis :
 - `pip install qiskit` (le package principal)
 - `pip install qiskit-ibm-runtime` (le client IBM pour Qiskit)
 - `pip install qiskit_serverless` (une interface pour exploiter les ressources IBM quantum)
Non disponible sur Mac Intel x86_64

Informatique quantique



Atelier 1 suite : Exercice évalué

- Objectif : obtenir un output de ce type : `>>> Job ID: cyttv5478z600082p4m0`
- Marche à suivre : Créer un compte Quantum sur IBM : <https://quantum-computing.ibm.com/>
- Utilise Qiskit, un SDK Python open-source pour travailler avec des ordinateurs quantiques.
<https://docs.quantum.ibm.com/start/hello-world> Installer python et les dépendances via pip
 - Si nécessaire : exécuter dans un WSL
 - passer dans un venv Rendu :
- Mettre votre travail sur un espace git avec votre clef API dans un .env que vous n'oubliez pas de gitignore
- M'envoyer le lien de votre github par mail à thibault.vincent@campus-cd.com

Informatique quantique

Atelier 2 facultatif




1. Introduction aux Algorithmes Quantiques

- Objectif : comprendre comment les algorithmes quantiques surpassent les algorithmes classiques dans certains cas, en explorant Grover (recherche) et Shor (factorisation). Les étudiants simuleront une version simplifiée de Grover.
-  Contexte
Les algorithmes quantiques exploitent la superposition et l'intrication pour résoudre des problèmes plus rapidement que les algorithmes classiques.
-  1. Algorithme de Grover : Recherche dans une base non triée
 - Problème classique : Chercher un élément dans une base non triée prend $O(N)$ opérations.
 - Solution quantique : L'algorithme de Grover réduit ce temps à $O(\sqrt{N})$.

Informatique quantique

Atelier 2 facultatif - suite

1. Introduction aux Algorithmes Quantiques

-  2. Algorithme de Shor : Factorisation de grands nombres
- Problème classique : Factoriser un grand nombre $N = p \times q$ prend un temps exponentiel pour un ordinateur classique. Solution quantique : L'algorithme de Shor factorise en temps polynomial, menaçant ainsi la cryptographie RSA.
-  Idée clé : Recherche du plus petit exposant périodique
- On transforme la factorisation en un problème périodique : trouver r tel que $a^r \equiv 1 \pmod{N}$.
- Une Transformée de Fourier Quantique (QFT) identifie la période efficacement.
- On en déduit les facteurs premiers.
-  Impact : Menace potentielle pour RSA, développement de la cryptographie quantique.