

# Introduction à l'informatique quantique

Philippe DENIEL ([philippe.deniel@cea.fr](mailto:philippe.deniel@cea.fr))

CEA / ENSIEE

2024

De quoi va-t-on parler pendant ces 42 heures de cours ?

# Plan

## 1 Qu'est-ce que l'informatique quantique

# Quelques citations

*Niels Bohr - Si la mécanique quantique ne vous a pas encore profondément choqué, alors vous ne l'avez pas encore comprise. Tout ce que nous appelons réel est fait de choses qui ne peuvent pas être considérées comme étant réelles.*

*Niels Bohr - Si une idée ne semble pas bizarre, il n'y a rien à espérer d'elle.*

*Heinz Pagels - Dieu a utilisé de merveilleuses mathématiques pour créer le monde.*

*Richard Feynmann - Je pense pouvoir dire sans trop me tromper que personne ne comprend la mécanique quantique.*

*Richard Feynmann, 1982 - Nature isn't classical, dammit, and if you want to make a simulation of nature, you better make it quantum mechanical*

*Albert Einstein - If you can't explain it simply, you don't understand it well enough*

# L'informatique quantique n'est pas si récente

Le *Quantum Computing* est né dans les années 80

- Une première conférence sur le QC au MIT en 1981
- Beaucoup d'études théoriques sur le QC
  - Algorithme de Shor, 1994
  - Algorithme de Grover, 1996

L'informatique quantique a de solides bases théoriques

- dans le domaine de la physique (physique quantique, physique statistique)
- dans le domaine des mathématiques (algèbre linéaire, algèbre hermitienne)

En revanche les implémentations physiques "réelles" des QPUs sont très récents.

# Les liens entre informatique quantique et physique quantique

Le *Quantum Computing* est un nouveau paradigme informatique basé sur les phénomènes à la physique quantique :

- ① la superposition,
  - qui permet d'induire une forme de parallélisme (à relativiser...)
- ② l'intrication,
  - qui permet de coupler des systèmes simples pour de bâtir des systèmes plus complexes
- ③ les interférences,
  - qui permettent de mesurer les états quantiques et d'obtenir des résultats de calcul.

# La première révolution quantique

La physique quantique est déjà très présente dans notre monde

- imagerie médicale : IRM (imagerie par résonance magnétique),
- composants électroniques : transistors à effet tunnel, LED,
- lasers,
- écrans LCD,
- panneaux solaires photovoltaïques : interaction photon/matière.

# Le QC et la deuxième révolution quantique

L'informatique quantique fait partie de la deuxième révolution quantique

Les **QPU** commencent à apparaître sur le marché.

On prévoit plusieurs phases dans le QC

- NISQ : **Noisy Intermediate Scale Quantum**
- FTQC : **Fault Tolerant Quantum Quantum**
- LSQ : **Large Scale Quantum**

On est actuellement dans la période NISQ



# Ce que l'informatique quantique n'est pas.

Le QC ne va pas remplacer le HPC

- Les QPUs appartiennent à un nouveau paradigme du HPC, comme les GPUs.
- le QC est une nouvelle arme dans l'arsenal du HPC

Attention à la "hype" autour du QC, entretenue par certains constructeurs (dont IBM et Google)

- Des annonces "publicitaires", parfois éloignées de la réalité scientifique
- Des notions "grand public" aux contours souvent très flous...
- le QC ce n'est pas "faire  $2^n$  calculs en même temps", le parallélisme exponentiel existe mais il est loin d'être systématique
- le QC est efficace pour caractériser rapidement une propriété globale d'un problème
  - périodicité d'une fonction entière (Shor)
  - parcours de graphe (marches quantiques)
  - Recherches d'optima de forme quadratiques (QUBO)

# Plan

2 Les espaces de Hilbert en avance rapide

3 Rappels sur les matrices

4 Exponentielles de matrices

5 Rappels d'algèbre hermitienne

# Les espaces de Hilbert

Un espace de Hilbert est un espace vectoriel sur les corps  $\mathbb{R}$  ou  $\mathbb{C}$  qui dispose des propriétés suivantes :

- il est euclien ou hermitien, c'est à dire qu'il dispose d'un produit scalaire (euclidien si basé sur  $\mathbb{R}$ , hermitien si base sur  $\mathbb{C}$ ), ce dernier permet de définir une distance, mais aussi des notions d'angles et d'orthogonalité ;
- il est *complet*.

Dans un espace vectoriel *complet*, les suites de Cauchy convergent.

# Suites de Cauchy

Les suites de Cauchy désignent les suites  $(u_n)_{n \in \mathbb{N}}$  qui vérifient la propriété suivante (La fonction  $d()$  désigne ici la distance dans l'espace de Hilbert) :

$$\lim_{p,q \rightarrow +\infty} d(r_p, r_q) = 0$$

Intuitivement, une suite de Cauchy est une suite dont les termes se rapprochent de plus en plus quant l'indice de la suite augmente. On a un espace de Hilbert quand ces suites convergent vers une valeur qui est dans l'espace en question.

En bref, un espace de Hilbert, c'est un espace vectoriel qui contient tous les "outils" mathématiques dont on a besoin pour y faire de l'analyse.

# Plan

2 Les espaces de Hilbert en avance rapide

3 Rappels sur les matrices

4 Exponentielles de matrices

5 Rappels d'algèbre hermitienne

# Rappels : les matrices

Une matrice à  $m$  lignes et  $n$  colonnes dont chaque case prend sa valeur dans un corps  $\mathbb{K}$ .  
Dans le périmètre de ce cours, le corps en question sera toujours le corps des nombres complexes  $\mathbb{C}$ .

On notera les éléments  $a_{i,j}$  d'une matrice  $A = (a_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}$  soit encore

$$A_{m,n} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

# Rappels : matrices transposées et adjointes

La transposée d'une matrice  $A$  de taille  $m.n$  est notée  $A^t$ , c'est une matrice de taille  $n.m$  telle que

$$A' = (a'_{i,j})_{1 \leq i \leq n, 1 \leq j \leq m} = A^t, \forall i, 1 \leq i \leq m, \forall j, 1 \leq j \leq n, a'_{j,i} = a_{i,j}$$

La matrice adjointe d'une matrice  $A$  de taille  $m.n$  est notée  $A^*$ , c'est une matrice de taille  $n.m$  telle que

$$A' = (a'_{i,j})_{1 \leq i \leq n, 1 \leq j \leq m} = A^*, \forall i, 1 \leq i \leq m, \forall j, 1 \leq j \leq n, a'_{j,i} = \overline{a_{i,j}}$$

**Matrice Adjointe = transposée + conjugaison**

# Rappels : trace d'une matrice

La trace d'une matrice carrée est une fonction qui associe à une matrice la somme des éléments sur sa diagonale. En termes mathématiques, on écrira

$$A = (a_{ij})_{1 \leq i,j \leq n}, \text{Tr}(A) = \sum_{i=1}^n a_{ii}$$

La trace possède différentes propriétés remarquables :

$$\text{Tr}(A + B) = \text{Tr}(A) + \text{Tr}(B)$$

$$\text{Tr}(\alpha A) = \alpha \text{Tr}(A)$$

$$\text{Tr}(A^t) = \text{Tr}(A)$$

$$\text{Tr}(AB) = \text{Tr}(BA)$$

La trace est un *invariant de similitude*

$$\text{Tr}(PAP^{-1}) = \text{Tr}(APP^{-1}) = \text{Tr}(A)$$

## Produit matriciel (usuel)

Le produit matriciel est plus complexe. Le produit est non-commutatif et il impose que le nombre de colonnes de l'élément de gauche est égale au nombre de lignes de l'élément de droite, on ne pourra donc former le produit  $A \times B$  que si A est une matrice de taille  $m \times n$  et B une matrice de taille  $n \times p$ . Le résultat est une matrice de taille  $m \times p$ .

Si  $a_{i,j}$ ,  $b_{i,j}$  et  $c_{i,j}$ , sont les coefficients des matrices A, B et C, le produit sera défini par

$$\forall i, 1 \leq i \leq m, \forall j, 1 \leq j \leq p, c_{i,j} = \sum_{k=1}^n a_{i,k} \cdot b_{k,j}$$

Le produit matriciel standard n'est pas commutatif, il est associatif et distributif à droite et à gauche par rapport à la somme.

# Produit de Kronecker 1/2

Le produit de Kronecker, ou produit tensoriel est très intuitif. Il n'est pas commutatif et peut agir sur tout couple de matrices, quelque soit leurs tailles.

Si  $A = (a_{ij})$  est une matrice  $m \times n$  et  $B$  une matrice  $p \times q$ , le produit  $C = A \otimes B$  sera une matrice de taille  $mp \times nq$

$$A_{m,n} \otimes B_{p,q} = C_{mp,nq} = \begin{pmatrix} a_{1,1}B & a_{1,2}B & \cdots & a_{1,n}B \\ a_{2,1}B & a_{2,2}B & \cdots & a_{2,n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1}B & a_{m,2}B & \cdots & a_{m,n}B \end{pmatrix}$$

# Produit de Kronecker 2/2

Ce qui revient à écrire :

$$A_{m,n} \otimes B_{p,q} = \begin{pmatrix} a_{1,1}b_{1,1} & a_{1,1}b_{1,2} & \cdots & a_{1,1}b_{1,q} & \cdots & \cdots & a_{1,n}b_{1,1} & a_{1,n}b_{1,2} & \cdots & a_{1,n}b_{1,q} \\ a_{1,1}b_{2,1} & a_{1,1}b_{2,2} & \cdots & a_{1,1}b_{2,q} & \cdots & \cdots & a_{1,n}b_{2,1} & a_{1,n}b_{2,2} & \cdots & a_{1,n}b_{2,q} \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\ a_{1,1}b_{p,1} & a_{1,1}b_{p,2} & \cdots & a_{1,1}b_{p,q} & \cdots & \cdots & a_{1,n}b_{p,1} & a_{1,n}b_{p,2} & \cdots & a_{1,n}b_{p,q} \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\ a_{m,1}b_{1,1} & a_{m,1}b_{1,2} & \cdots & a_{m,1}b_{1,q} & \cdots & \cdots & a_{m,n}b_{1,1} & a_{m,n}b_{1,2} & \cdots & a_{m,n}b_{1,q} \\ a_{m,1}b_{2,1} & a_{m,1}b_{2,2} & \cdots & a_{m,1}b_{2,q} & \cdots & \cdots & a_{m,n}b_{2,1} & a_{m,n}b_{2,2} & \cdots & a_{m,n}b_{2,q} \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\ a_{m,1}b_{p,1} & a_{m,1}b_{p,2} & \cdots & a_{m,1}b_{p,q} & \cdots & \cdots & a_{m,n}b_{p,1} & a_{m,n}b_{p,2} & \cdots & a_{m,n}b_{p,q} \end{pmatrix}$$

# Exemple de produit tensoriel

Par exemple :

$$\begin{aligned} \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} &= \begin{pmatrix} 1 \times \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} & 2 \times \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} \\ 3 \times \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} & 1 \times \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} 1 \times 0 & 1 \times 3 & 2 \times 0 & 2 \times 3 \\ 1 \times 2 & 1 \times 1 & 2 \times 2 & 2 \times 1 \\ 3 \times 0 & 3 \times 3 & 1 \times 0 & 1 \times 3 \\ 3 \times 2 & 3 \times 1 & 1 \times 2 & 1 \times 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 3 & 0 & 6 \\ 2 & 1 & 4 & 2 \\ 0 & 9 & 0 & 3 \\ 6 & 3 & 2 & 1 \end{pmatrix} \end{aligned}$$

# Propriétés importantes du produit tensoriel

Le produit tensoriel a des propriétés notables vis-à-vis du produit matriciel classique et de la transposition :

$$(A \otimes B) \times (C \otimes D) = (A \times C) \otimes (B \times D)$$

$$(A \otimes B)^t = A^t \otimes B^t$$

## Produit tensoriel d'espaces vectoriel - définition

Le produit tensoriel de matrice est intimement lié à une autre notion, celle de produit tensoriel d'espaces vectoriels. D'une manière très intuitive, un groupe ou un espace vectoriel sont des ensembles qui possèdent certaines structures qui leur donnent des propriétés intéressantes.

Si je dispose de deux ensemble A et B, je peux construire leur produit cartésien  $A \times B$  dont les éléments seront des couples de la forme  $(x, y)$  avec  $x \in A$  et  $y \in B$ . Le produit tensoriel, en approche simplifiée, permet de conserver les structures intéressantes des groupes ou des espaces vectoriels dans le produit cartésien.

Dans le cas des espaces vectoriels relatifs à un corps commutatif  $\mathbb{K}$ , on définira le produit tensoriel de deux espaces vectoriels E et F par l'existence d'une application bilinéaire  $\Phi$  telle que :

$$\Phi : E \times F \longrightarrow E \otimes F$$

Les éléments de  $E \otimes F$  sont définis par  $\Phi$  en posant

$$\forall x \in E, \forall y \in F, x \otimes y = \Phi(x, y)$$

## Produit tensoriel d'espace vectoriel - comment s'en servir ?

Le produit tensoriel peut être vue comme une astuce de notation car il permet de gérer des applications multilinéaires comme s'il s'agissait d'une application linéaire appliquée sur le produit tensoriel des espaces vectoriels source.

Considérons par exemple l'application bilinéaire  $g$  opérant sur  $E \times F$ , on peut lui adjoindre une unique forme linéaire  $\hat{g}$  telle que  $g = \hat{g} \circ \Phi$ , où  $\Phi$  représente l'isomorphisme entre  $E \times F$  et  $E \otimes F$ . On a donc

$$\forall x \in E, \forall y \in F, g(x, y) = \hat{g}(x \otimes y)$$

On peut substituer à  $g$ , qui est bilinéaire,  $\hat{g}$  qui est simplement linéaire. Grâce au produit tensoriel d'espaces vectoriels, traiter des formes multilinéaires revient à traiter de simples formes linéaires.

La dimension de l'espace produit tensoriel  $E \otimes F$  est égal au produit des dimensions de  $E$  et  $F$  :

$$\dim(E \otimes F) = \dim(E) \cdot \dim(F)$$

# Retour sur le produit de Kronecker

Le lien entre le produit tensoriel d'espaces vectoriels et le produit tensoriel de matrices est canonique. En effet, connaissant une application linéaire sur  $E$  décrite par la matrice  $A$ , et une application linéaire décrite par la matrice  $B$ , je peux construire une application linéaire  $A \otimes B$  sur  $E \otimes F$  avec le produit de Kronecker.

La notation de produit tensoriel est très utilisée en informatique quantique. Elle servira beaucoup quand il s'agira de gérer de multiples qubits.

**Attention :** la notation  $\otimes$  qui représente le produit tensoriel ne doit pas être confondue avec la notation  $\oplus$  qui représente le XOR booléen ou la *somme directe* d'espace vectoriel.

# Plan

2 Les espaces de Hilbert en avance rapide

3 Rappels sur les matrices

4 Exponentielles de matrices

5 Rappels d'algèbre hermitienne

# Rappels - Série de Taylor 1/2

On rappelle que la fonction exponentielle peut s'écrire comme la série suivante (série de Taylor de la fonction exponentielle) :

$$\forall x \in \mathbb{R}, e^x = \sum_{n=0}^{+\infty} \frac{x^n}{n!}$$

## Application à la trigonométrie

Si on y applique la série précédente à la forme  $e^{i\theta}$  :

$$\begin{aligned} e^{i\theta} &= \sum_{n=0}^{+\infty} \frac{(i\theta)^n}{n!} = \sum_{p=0}^{+\infty} \frac{(i\theta)^{2p}}{2p!} + \sum_{p=0}^{+\infty} \frac{(i\theta)^{2p+1}}{2p+1!} \\ &= \sum_{p=0}^{+\infty} \frac{(-1)^p \cdot \theta^{2p}}{2p!} + i \cdot \sum_{p=0}^{+\infty} \frac{(-1)^p \theta^{2p+1}}{2p+1!} \\ &= \cos(\theta) + i \cdot \sin(\theta) \end{aligned}$$

## Rappels - Série de Taylor 2/2

Par conséquent on peut en déduire les développements en série de Taylor des fonctions sinus et cosinus :

$$\cos(x) = \sum_{n=0}^{+\infty} (-1)^n \frac{x^{2n}}{(2n)!}$$

$$\sin(x) = \sum_{n=0}^{+\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}$$

# Exponentielle de matrices

Comme on sait multiplier des matrices carrées et les ajouter, il est possible d'utiliser la série de Taylor de l'exponentielle sur les matrices carrées. On aura donc la définition suivante :

$$\forall A \text{ matrice carrée}, e^A = \sum_{n=0}^{+\infty} \frac{A^n}{n!}$$

# Exponentielles de matrice et valeurs propres

Les valeurs propres d'une exponentielle de matrice sont les exponentielles des valeurs propres. Ce résultat est simple à voir. En effet, si  $D$  désigne la matrice diagonale dont les coefficients sont les valeurs propres, on a trivialement

$$\exists P, A = PDP^{-1}, \forall n \in \mathbb{N}, A^n = PD^nP^{-1}$$

Par conséquent,

$$e^A = \sum_{n=0}^{+\infty} \frac{A^n}{n!} = \sum_{n=0}^{+\infty} \frac{PD^nP^{-1}}{n!} = P \left( \sum_{n=0}^{+\infty} \frac{D^n}{n!} \right) P^{-1} = P \cdot e^D \cdot P^{-1}$$

On en déduit qu'une matrice et son exponentielle ont les mêmes vecteurs propres (et par ailleurs les mêmes vecteurs propres que toutes ses puissances).

# ATTENTION A LA COMMUTATIVITÉ !!!!!!

L'exponentielle de la somme de deux matrices n'est le produit des exponentielles des matrices que si celles-ci commutent.

En général  $e^{A+B} \neq e^A \cdot e^B$ , ce n'est vrai que si  $AB = BA$

Plus généralement, on dispose de la formule de *Glauber*

$$e^X e^Y = e^{X+Y+\frac{1}{2}[X,Y]}$$

Où  $[X, Y]$  est le commutateur  $[X, Y] = XY - YX$

# Propriétés des exponentielles de matrices

L'exponentielle de la matrice nulle est la matrice identité :  $e^0 = I$

Le déterminant de l'exponentielle d'une matrice est égal à l'exponentielle de sa trace :

$$\det(e^X) = e^{\text{Tr}(X)}$$

Si  $Y$  est une matrice inversible alors

$$e^{YXY^{-1}} = Y e^X Y^{-1}$$

# Plan

2 Les espaces de Hilbert en avance rapide

3 Rappels sur les matrices

4 Exponentielles de matrices

5 Rappels d'algèbre hermitienne

# Produit scalaire euclidien et produit scalaire hermitien

Dans  $\mathbb{R}^n$ , on peut définir le produit scalaire (à valeurs dans  $\mathbb{R}$ ) des vecteurs  $x = (x_1, x_2, \dots, x_n)$  et  $y = (y_1, y_2, \dots, y_n)$  par  $x.y = x_1.y_1 + x_2.y_2 + \dots + x_n.y_n = \sum_{k=1}^n x_k.y_k$

Dans  $\mathbb{C}^n$ , on définira le produit scalaire hermitien (à valeurs dans  $\mathbb{C}$ ) des vecteurs  $x = (x_1, x_2, \dots, x_n)$  et  $y = (y_1, y_2, \dots, y_n)$  par  $x.y = \overline{x_1}.y_1 + \overline{x_2}.y_2 + \dots + \overline{x_n}.y_n = \sum_{k=1}^n \overline{x_k}.y_k$

On rappelle que si  $x = a + i.b$  alors  $\bar{x} = a - i.b$  est son conjugué.

# Matrice adjointe

Étant donné une matrice  $(a_{ij})_{1 \leq i,j \leq n}$ , sa matrice *adjointe* est la matrice conjuguée et transposée

$$A^\dagger = (a'_{ij})_{1 \leq i,j \leq n}, \text{ adjointe de } A, \forall i, j, a'_{ij} = \overline{a_{ji}}$$

Un vecteur dans  $\mathbb{C}^n$  peut être vu comme une "matrice colonne" avec  $n$  lignes et une seule colonne. Son adjoint est donc une "matrice ligne" avec une seule ligne et  $n$  colonnes. Le produit scalaire hermitien entre les deux vecteurs peut s'écrire comme le produit matriciel suivant :

$$\forall x \in \mathbb{C}^n, \forall y \in \mathbb{C}^n, x.y = x^\dagger \times y$$

# Matrices hermitiennes et matrices unitaires

**définition : matrice hermitienne** Une matrice hermitienne est une matrice auto-adjointe, elle est également à sa matrice adjointe

$$A \text{ est une matrice hermitienne} \iff A = A^*$$

**définition : matrice unitaire** Une matrice unitaire U est telle que son inverse est sa matrice adjointe.

$$U^\dagger = U^{-1} \text{ soit } U \times U^\dagger = U^\dagger \times U = I$$

Une matrice peut être à la fois hermitienne et unitaire, c'est le cas des portes de la porte H et des portes de Pauli en particulier.

# Propriétés des matrices hermitiennes

Une matrice hermitienne

- est diagonalisable et la matrice de passage est une matrice unitaire ;
- a des valeurs propres réelles (à valeurs dans  $\mathbb{R}$ ) ;

# Propriétés des matrices unitaires

## Une matrice unitaire

- est inversible (et son inverse est sa matrice adjointe) ;
- est diagonalisable et la matrice de passage est une matrice unitaire ;
- possède une matrice adjointe qui est également unitaire (puisque étant son inverse) ;
- possède des colonnes qui forment une base orthonormale de  $\mathbb{C}^n$  vis-à-vis du produit scalaire hermitien ;
- est normale (elle commute avec son adjointe, c'est évident puisque ce produit vaut l'identité) ;
- a des valeurs propres qui sont complexes (pas forcément réelles) mais dont la norme est égale à 1, elles sont donc toutes de la forme  $e^{i\theta}$  ;
- peut s'écrire sous la forme d'une exponentielle de matrice  $e^{iH}$  où H est une matrice hermitienne (et donc  $iH$  est anti-hermitienne).

Une matrice unitaire transforme une base orthonormale en une autre base orthonormale.

# Matrices unitaires et produit scalaire

$$Ux.Uy = (Ux)^\dagger \times Uy = x^\dagger \times U^\dagger \times U \times y$$

mais  $U$  est unitaire donc  $U^\dagger \times U = \mathbb{I}$  et par conséquent

$$Ux.Uy = x^\dagger \times y = x.y$$

On a donc  $Uy.Uy = x.y$

Les opérateurs unitaires conservent le produit scalaire, ce qui signifie qu'ils ne changent ni les normes ni les angles entre vecteurs.

Disclaimer : ceci n'est pas un cours de physique quantique !!!!

# Plan

6 La superposition

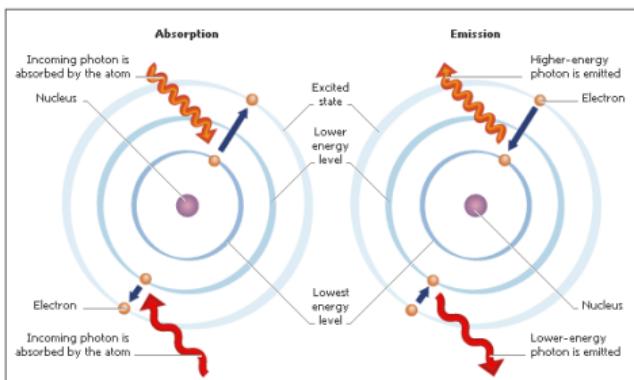
7 L'intrication

8 Zoologie des technologies de qubits

# Quantas

Les objets quantiques n'évoluent pas de manière continue. Ils possèdent différents états *discrets*, correspondant à des états énergétiques identifiés, séparés par des *quanta*.

Dans le cas des différents états d'excitation d'un électron, on aura la chose suivante :



L'électron ne "passe" pas d'une orbite à une autre, il est dans toutes les orbites à la fois, avec différentes probabilités de l'y trouver à cet endroit

# Etats superposés

Un objet quantique est **simultanément** dans plusieurs états à la fois, c'est le phénomène de **superposition d'états**.

**ATTENTION** : ce concept est très contre-intuitif

- Les électrons sont sur plusieurs orbites d'un atome en même temps
- les particules ont des *spin* de valeurs inverses.. en même temps
- les photons peuvent avoir différentes sortes de polarisation ... en même temps
- un même photon peut être simultanément dans deux fibres optiques
- dans une boucle supraconductrice, le courant circulent à la fois dans le sens direct et dans le sens rétrograde

On identifie les états de base par des numéros. Un état  $|\Psi\rangle$  sera une composition de ces états de la forme

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle + \delta|3\rangle$$

# Effondrement quantique

En physique quantique, observer, c'est consommer de l'information. En observant un état superposé, on va effondrer celui-ci sur l'un des états de bases qui le composent. Ensuite, il ne bougera plus et restera à jamais ainsi, comme s'il avait "choisi son camp".

Si on considère l'état du slide précédent

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle + \delta|3\rangle$$

L'observer donnera soit  $|1\rangle$ ,  $|2\rangle$ ,  $|3\rangle$  ou  $|4\rangle$ .

Si on observe, par exemple  $|3\rangle$ , les mesures suivantes donneront **toujours**  $|\Psi\rangle = |3\rangle$

# Densités de probabilités

Dans la formulation

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle + \delta|3\rangle$$

Les termes  $\alpha$  à  $\delta$  sont des nombres à valeurs dans  $\mathbb{C}$ , ou **densités de probabilités**.

Elles expriment les probabilités que  $|\Psi\rangle$  est à la fois dans les états  $|1\rangle$ , à  $|4\rangle$ . Ce ne sont pas des probabilités "classiques", au sens de Kolmogorov.

Si on mesure  $|\Psi\rangle$ , il y a une probabilité  $|\alpha|^2$  de mesurer  $|0\rangle$ ,  $|\beta|^2$  de mesurer  $|1\rangle$ ,  $|\gamma|^2$  de mesurer  $|2\rangle$  et  $|\delta|^2$  de mesurer  $|3\rangle$

On a en revanche, il y a 100% de chances de mesurer l'un des états, d'où la **condition de normalisation**

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

Si on sait reproduire  $|\Psi\rangle$  à volonté, on peut, de manière probabiliste, connaître les valeurs des carrés des modules, en faisant suffisamment de mesures.

# Plan

6 La superposition

7 L'intrication

8 Zoologie des technologies de qubits

# Le paradoxe EPR

L'intrication est une notion fondamentale en physique quantique. Elle a été sujette à de nombreuses controverses, dont le célèbre paradoxe EPR, dû à Einstein, Podolsky et Rosen.

Il faudra attendre 1982 et l'expérience de Alain Aspect pour clore le débat. Alain Aspect obtiendra par la suite le Prix Nobel de Physique en 2022.

# Qu'est-ce que l'intrication ?

Lorsque des objets quantiques interagissent, elles forment un système, ou **état intriqués**.

Les objets intriqués ne peuvent plus être considérés de manière autonome, il faut considérer l'ensemble du système intriqué, en particulier **agir sur une particule** c'est **agir sur l'état intriqué tout entier**.

En particulier, observer l'un quelconque des composants d'un état intriqué provoque son effondrement et l'effondrement de l'ensemble de l'état intriqué.

# Plan

6 La superposition

7 L'intrication

8 Zoologie des technologies de qubits

# La programmation quantique, c'est quoi ?

La programmation quantique consiste à :

- utiliser la superposition pour accélérer le calcul sur  $n$  qubits
- utiliser l'intrication pour construire des interactions complexes
- **mais** on ne peut mesurer qu'un seul des  $2^n$  état possible

La programmation quantique, c'est construire un opérateur unitaire, sur les qubits, tel que l'état mesuré, ou le plus probablement mesuré, représentera la solution cherchée pour le problème concerné.

# La notation de Dirac

En informatique quantique, on utilisera la notation de Dirac. Les vecteurs de  $\mathbb{C}^n$  ne seront pas notés  $x$  mais  $|x\rangle$

Cette notation se nomme "ket",  $|x\rangle$  se lira "ket  $x$ ". Elle correspond à un vecteur écrit "en

colonne" soit 
$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

L'adjoint d'un vecteur  $x \in \mathbb{C}^n$  écrit en colonne est écrit "en ligne" , soit  $x^\dagger = (\overline{x_1}, \overline{x_2}, \dots, \overline{x_n})$

Avec la notation de Dirac, l'adjoint de  $|x\rangle$  sera noté  $\langle x|$ , cette forme se nomme "bra" et lire "bra  $x$ ".

## Produit scalaire hermitien et notation de Dirac

Le produit scalaire hermitien peut être écrit comme le produit d'une matrice "ligne" et d'une matrice "colonne" :

$$\begin{aligned} x.y &= \overline{x_1}.y_1 + \overline{x_2}.y_2 + \cdots + \overline{x_n}.y_n = \sum_{k=1}^n \overline{x_k}.y_k \\ &= (\overline{x_1}, \overline{x_2}, \cdots, \overline{x_n}) \times \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \\ &= \langle x|y \rangle \end{aligned}$$

La norme d'un vecteur est quant à elle donnée par

$$\|x\| = \sqrt{\langle x|x \rangle}$$

# Matrices et notation de Dirac

Si  $A$  est une matrice de  $\mathbb{C}^{n \times n}$  représentant une application linéaire, le produit simplement noté  $A|x\rangle$ .

Si la matrice représente une forme hermitienne, elle est associée à une forme hermitienne  $F$  telle que

$$\forall x \in \mathbb{C}^n, \forall y \in \mathbb{C}^n, F(x, y) = x^\dagger A y$$

En utilisant la notation de Dirac, l'équation précédente s'écritra

$$\forall x \in \mathbb{C}^n, \forall y \in \mathbb{C}^n, F(x, y) = \langle x | A | y \rangle$$

## Base canonique et notation de Dirac

L'espace vectoriel  $\mathbb{C}^2$  dispose d'une base canonique :  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$  et  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ .

Dans la notation de Dirac, on écrira

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ et } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Les vecteurs  $|0\rangle$  et  $|1\rangle$  forment la **base canonique** de  $\mathbb{C}^2$ .

**ATTENTION!!!!**, le vecteur  $|0\rangle$  n'est pas le vecteur nul :  $\vec{0} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

# Produit tensoriel et notation de Dirac

Quand on manipule plusieurs qubits, on va rapidement devoir manipuler des produits tensoriels de ces qubits.

On notera  $|0\rangle \otimes |0\rangle = |00\rangle$  et plus généralement si  $(x, y) \in \{0, 1\}^2$ ,  $|x\rangle \otimes |y\rangle = |xy\rangle$

Le plus souvent, on n'utilise pas le symbole  $\otimes$  qui devient implicite et on pourra écrire

$$|01\rangle |0\rangle = |010\rangle$$

## Base canonique sur plusieurs qubits

Si l'on dispose de  $n$  qubits, on est dans  $\mathbb{C}^{2^n}$ , qui est isomorphe à  $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$

On construit les bases canoniques en construisant les produits tensoriels avec les bases canoniques de  $\mathbb{C}^2$ . Ainsi  $\mathbb{C}^4$  a comme base canonique  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

# Plan

9 Les circuits quantique

10 Les opérateurs sur 1 seul qubits

11 Les opérateurs sur 2 à n qubits

12 Les circuits sont des matrics

13 Mesures

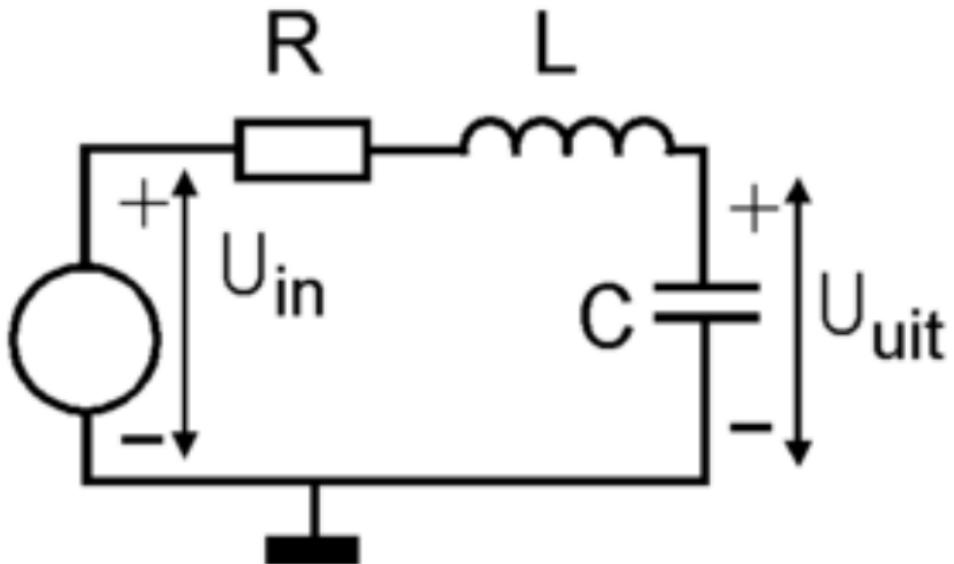
# Programmation quantique à portes

Dans la programmation quantique à portes, on programme l'opérateur unitaire sous la forme d'un "circuit"

- le circuit est composé de différentes étapes,
- le circuit est un assemblage de composants génériques, plus simples.

**ATTENTION :** Un circuit quantique est une manière "graphique" de décrire une matrice  $2^n \times 2^n$  potentiellement très complexe.

# Ceci est un circuit (électrique)

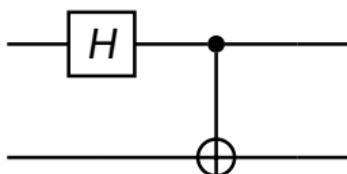


# Ceci n'est pas une pipe



# Ceci n'est pas un circuit, ceci est une matrice

le circuit suivant construit une *paire EPR*



On verra que ce circuit correspond à la matrice

$$\frac{1}{2} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}$$

# Les qubits

Un qubit est un vecteur de  $\mathbb{C}^2$ , contrairement à un bit, il ne prend pas que les valeurs 0 et 1. Un qubit est un état quantique écrit ainsi

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle \text{ avec } , \alpha \in \mathbb{C}, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

Les valeurs  $\alpha$  et  $\beta$  sont des *densités de probabilité*, en mesurant  $|\phi\rangle$  on aura

- la valeur  $|0\rangle$  avec une probabilité de  $|\alpha|^2$
- la valeur  $|1\rangle$  avec une probabilité de  $|\beta|^2$

## Mesure d'un qubit et effondrement

On mesure un qubit  $|\phi\rangle$  par rapport à une base orthonormée  $(|v_1\rangle, |v_2\rangle)$  ou il s'écrit  $|\phi\rangle = \alpha|v_1\rangle + \beta|v_2\rangle$  avec  $|\alpha|^2 + |\beta|^2 = 1$

La mesure est effectuée grâce à un opérateur dont on peut mesurer les vecteurs propres. Mesurer un état provoque son *effondrement*. Après une mesure, le qubit s'effondre sur l'une de ses deux composantes, et il reste, il devient donc toujours soit  $|v_1\rangle$  soit  $|v_2\rangle$

Mesurer c'est **perdre de l'information**, mais on est obligé de faire des mesures pour avoir des résultats.

Les circuits quantique  
oooooooo

Les opérateurs sur 1 seul qubits  
●oooooooooooo

Les opérateurs sur 2 à n qubits  
oooooooooooooooooooo

Les circuits sont des matrics  
oooooooo

Mesures  
oooooo

# Plan

9

Les circuits quantique

10

Les opérateurs sur 1 seul qubits

11

Les opérateurs sur 2 à n qubits

12

Les circuits sont des matrics

13

Mesures

# Zoologie des opérateurs sur 1 qubit

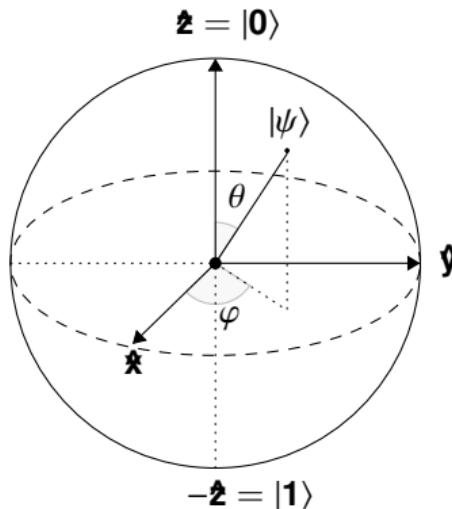
Les opérateurs sur 1 qubit sont des matrices unitaires dans  $\mathbb{C}^{2 \times 2}$

On va détailler

- la porte de Hadamard
- les portes de Pauli
- les portes de Clifford
- les portes paramétrées

# La sphère de Bloch

La sphère de Bloch est un moyen classique de représenter un qubit. C'est la vue en perspective d'une projection d'un hyperplan à trois dimensions de  $\mathbb{C}^2$



## Construire la sphère de Bloch 1/2

Un état quantique est un vecteur  $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$  avec  $\alpha$  et  $\beta$  des nombres complexes tels que  $\|\alpha\|^2 + \|\beta\|^2 = 1$ . On peut noter  $\alpha$  et  $\beta$  sous formes polaires

$$\exists! r_1 \in [0; 1], \exists! \psi_1 \in [0; 2\pi[, \alpha = r_1.e^{i\phi_1}$$

$$\exists! r_2 \in [0; 1], \exists! \psi_2 \in [0; 2\pi[, \beta = r_2.e^{i\phi_2}$$

et donc

$$\begin{aligned}
 |\Psi\rangle &= \alpha|0\rangle + \beta|1\rangle = r_1.e^{i\phi_1}|0\rangle + r_2.e^{i\phi_2}|1\rangle \\
 &= e^{i\phi_1}(r_1|0\rangle + r_2e^{i(\phi_2-\phi_1)}|1\rangle) \\
 &= e^{i\phi_1}(r_1|0\rangle + r_2e^{i\phi}|1\rangle) \text{ avec } \phi = \phi_2 - \phi_1
 \end{aligned}$$

On ne peut pas mesurer la phase  $e^{i\phi_1}$  dont la norme est 1, donc  $|\Psi\rangle \equiv e^{-i\phi_1} |\Psi\rangle$ , il est légitime d'ignorer le facteur  $e^{i\phi_1}$  dans l'équation précédente et donc

$$|\Psi\rangle \equiv r_1|0\rangle + r_2 e^{i\phi}|1\rangle, r_1, r_2 \in [0; 1], \phi \in [0; 2\pi]$$

## Construire la sphère de Bloch 2/2

Les carrés des modules composants en  $|0\rangle$  et  $|1\rangle$  vaut 1, par conséquent  $r_1^2 + r_2^2 = 1$ , ce qui est analogue à l'équation  $\cos^2(\theta) + \sin^2(\theta) = 1$

Il est donc possible de trouver un angle  $\theta$  tel que  $r_1 = \cos(\frac{\theta}{2})$  et  $r_2 = \sin(\frac{\theta}{2})$ ,

comme  $r_1$  et  $r_2$  sont dans  $[0; 1]$  alors  $\frac{\theta}{2}$  varie dans  $[0, \pi]$ . On peut donc écrire  $|\Psi\rangle$  sous la forme  $|\Psi\rangle = \cos(\frac{\theta}{2})|0\rangle + \sin(\frac{\theta}{2})e^{i\phi}|1\rangle$ ,

un état quantique est donc totalement défini par deux angles  $\theta \in [0, \pi]$  et  $\phi \in [0; 2\pi]$

**Note :** Une construction plus algébrique de la sphère de Bloch est possible, en exploitant le corps des quaternions.

# La porte X, ou porte NOT

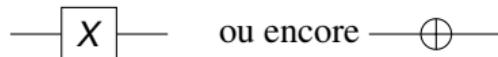
La porte X a les effets suivants sur la base canonique (bit flip)

- le qubit  $|0\rangle$  devient  $|1\rangle$ , soit  $X|0\rangle = |1\rangle$
- le qubit  $|1\rangle$  devient  $|0\rangle$ , soit  $X|1\rangle = |0\rangle$

La porte X est représentée par la matrice unitaire suivante

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

La porte X est représentée ainsi



La porte X réalise une **rotation** d'un angle  $\pi$  autour de l'axe X de la sphère de Bloch.

# La porte Z

La porte Z a les effets suivants sur la base canonique (phase flip)

- le qubit  $|0\rangle$  devient  $0\rangle$ , qui est invariant, soit  $Z|0\rangle = |0\rangle$
- le qubit  $|1\rangle$  devient  $-|1\rangle$ , soit  $Z|1\rangle = -|1\rangle$

La porte Z est aussi appelée "porte d'inversion de phase" ou *phase flip*.

Elle est représentée par la matrice unitaire suivante

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

La porte Z est représentée ainsi



La porte Z réalise une **rotation** d'un angle  $\pi$  autour de l'axe Z de la sphère de Bloch.

# La porte Y

La porte Y a les effets suivants sur la base canonique

- le qubit  $|0\rangle$  devient  $i|1\rangle$ , soit  $Y|0\rangle = i|1\rangle$
- le qubit  $|1\rangle$  devient  $-i|0\rangle$ , soit  $Y|1\rangle = -i|0\rangle$

La porte Y réalise une **rotation** d'un angle  $\pi$  autour de l'axe Y de la sphère de Bloch.  
Elle est représentée par la matrice unitaire suivante

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

La porte Y est représentée ainsi



$Y = iXZ$  : Y est un bit filp (X), plus un phase filp (Z), plus une modification de phase.

## Superposition

La base canonique n'est pas la seule base orthonormée de  $\mathbb{C}^2$ . Il est classique d'utiliser la base  $|+\rangle, |-\rangle$  définie par

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Ces deux états sont très importants car ils sont uniformément superposés, quand on mesure  $|+\rangle$  ou  $|-\rangle$  on a toujours

- $(\frac{1}{\sqrt{2}})^2 = 50\%$  de chance de mesurer  $|0\rangle$
  - 50% de chance de mesurer  $|1\rangle$

On observera aussi que  $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$  et  $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$

# La porte H, ou porte de Hadamard

La porte de Hadamard est de loin la plus célèbre de toutes les portes quantiques et de loin l'une des plus utilisées. Elle doit son nom au mathématicien français Jacques Hadamard.

La porte H transforme la base  $(|0\rangle, |1\rangle)$  en la base  $(|+\rangle, |-\rangle)$  et inversement. Elle introduit la superposition d'états

- $H|0\rangle = |+\rangle$  et  $H|1\rangle = |-\rangle$
- $H|+\rangle = |0\rangle$  et  $H|-\rangle = |1\rangle$

La porte H est représentée par la matrice unitaire suivante

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

On remarquera que

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left( \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right) = \frac{1}{\sqrt{2}} (X + Z)$$

## Racines carrées de portes

Toutes les portes à 1 qubits sont des rotations dans  $\mathbb{C}^2$ , elles ont des racines carrées.

La matrice  $\sqrt{X} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$  est telle que son carré est la matrice  $X$

Il est possible de trouver des racines n-ièmes de toutes les portes.

On verra comment ces portes sont utiles pour construire une boite à outils universelle permettant de construire toutes les portes à  $n$  qubits.

# Plan

9 Les circuits quantique

10 Les opérateurs sur 1 seul qubits

11 Les opérateurs sur 2 à n qubits

12 Les circuits sont des matrics

13 Mesures

## Représenter les états intriqués algébriquement

Certains états à  $n$  qubits peuvent se factoriser, par exemple

$$\frac{1}{2}(|00\rangle + |10\rangle - |01\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |+\rangle \otimes |-\rangle$$

En revanche, certains ne peuvent pas se factoriser, comme celui-ci (appelé **paire EPR**)

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Les états non factorisables ne permettent pas de manipuler les qubits un par un, il faut considérer les  $n$  qubits ensemble, ils correspondent aux **états intriqués**

L'espace vectoriel des états factorisables a pour dimension  $2n$ , à comparer à la dimension  $2^n$  de l'espace des qubits

Il y a **beaucoup plus** d'états intriqués que d'états non-intriqués.

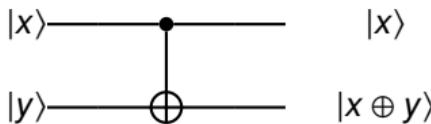
## L'intrication et la porte CNOT

La porte CNOT, ou porte CX, est une porte NOT (ou porte X) qui agit sur le second qubit mais qui est contrôlée par le premier qubit.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ donc } CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

L'effet d'une porte CNOT sur 2 qubit représenté par  $|xy\rangle$  (x et 0 sont des bits) :

- si  $x = 0$ , ne pas toucher à  $|y\rangle$ , on obtient  $|0y\rangle$  inchangé à la fin
- si  $x = 1$ , inverser  $y$ , on obtient donc  $|1\neg y\rangle$



D'une manière synthétique, la porte CNOT ne touche pas le premier qubit  $|x\rangle$  mais transforme le second qubit  $|y\rangle$  en  $|x \oplus y\rangle$ .

## Portes contrôlées (1/3)

La porte CNOT est la principale porte contrôlée. Les portes contrôlées

- permettent un traitement du type *if-then-else*
- s'appuient sur le phénomène d'intrication quantique

Si  $U$  est un opérateur unitaire de  $\mathbb{C}^2$ , il est algébriquement simple de définir une porte contrôlée  $CU$  qui est un opérateur unitaire de  $\mathbb{C}^4$ .

Considérons les *projecteurs* sur  $|0\rangle$  et  $|1\rangle$  (qui ne sont pas des opérateurs unitaires)

$$|0\rangle \times \langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ et } |1\rangle \times \langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Alors la porte CU définie par

$$CU = (|0\rangle \times \langle 0|) \otimes I + (|1\rangle \times \langle 1|) \otimes U$$

est une porte contrôlée unitaire : elle applique  $U$  sur le second qubit si le premier vaut  $|1\rangle$

## Portes contrôlées (2/3)

Il est simple de voir que  $CU$  est unitaire

$$\begin{aligned} CU &= (|0\rangle \times \langle 0|) \otimes I + (|1\rangle \times \langle 1|) \otimes U \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes I + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes U = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix} \end{aligned}$$

et

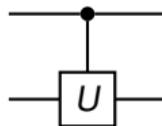
$$\begin{aligned} CU \times (CU)^\dagger &= (|0\rangle \langle 0| \otimes I + (|1\rangle \langle 1|) \otimes U) \times (|0\rangle \langle 0| \otimes I + (|1\rangle \langle 1|) \otimes U)^\dagger \\ &= (|0\rangle \langle 0| |0\rangle \langle 0|) \otimes (I \times I) + (|1\rangle \langle 1| |1\rangle \langle 1|) \otimes (U \times U^\dagger) + \\ &\quad (|0\rangle \langle 0| |1\rangle \langle 0|) \otimes (I \times U^\dagger) + (|1\rangle \langle 1| |0\rangle \langle 0|) \otimes (U \times I) \\ &= (|0\rangle \langle 0| |0\rangle \langle 0|) \otimes (I \times I) + (|1\rangle \langle 1| |1\rangle \langle 1|) \otimes (U \times U^\dagger) \\ &= (|0\rangle \langle 0| + |1\rangle \langle 1|) \otimes I = I \otimes I = I \end{aligned}$$

## Portes contrôlées (3/3)

$$\begin{aligned} CU|0x\rangle &= ((|0\rangle \times \langle 0|) \otimes I + (|1\rangle \times \langle 1|) \otimes U) \times (|0\rangle \otimes |x\rangle) \\ &= (|0\rangle\langle 0|0\rangle \otimes I|x\rangle) + (|1\rangle\langle 1|0\rangle \otimes U|x\rangle) \\ &= |0\rangle \otimes I|x\rangle = |0\rangle \otimes |x\rangle = |0x\rangle \end{aligned}$$

$$\begin{aligned} CU|1x\rangle &= ((|0\rangle \times \langle 0|) \otimes I + (|1\rangle \times \langle 1|) \otimes U) \times (|1\rangle \otimes |x\rangle) \\ &= (|0\rangle\langle 0|1\rangle \otimes I|x\rangle) + (|1\rangle\langle 1|1\rangle \otimes U|x\rangle) \\ &= |1\rangle \otimes U|x\rangle = |1\rangle \otimes U|x\rangle \end{aligned}$$

Un porte U contrôlée sera dessinée comme ceci dans les circuits quantiques :



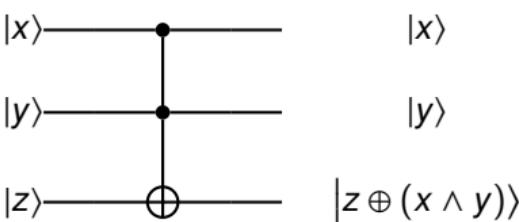
Il est légitime de faire des portes doublement contrôlées

# Porte de Toffoli

La porte de Toffoli est une porte opérant sur 3 qubits, c'est une porte CCNOT (NOT à double contrôle)

$$CCX = \begin{pmatrix} I & 0 \\ 0 & CX \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Son effet est le suivant :



## Porte SWAP 1/2

La porte SWAP permet d'échanger deux qubits. Les actions sur la base canonique de  $\mathbb{C}^4$  sont les suivants :

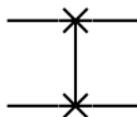
- $SWAP|00\rangle = |00\rangle$  (intervertir deux 0 donne toujours deux 0 à la fin) ;
- $SWAP|01\rangle = |10\rangle$  ;
- $SWAP|10\rangle = |01\rangle$  ;
- $SWAP|11\rangle = |11\rangle$  (intervertir deux 1 donne toujours deux 1 à la fin).

À partir de ces images des vecteurs de base, on peut déduire la matrice suivante :

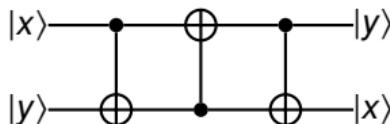
$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

## Porte SWAP 2/2

La porte SWAP s'écrit ainsi dans les circuits :



Elle peut s'implémenter à l'aide de trois portes CNOT



## Porte de Fredkin 1/2

La porte de Fredkin est une porte SWAP contrôlée : elle échange les deux derniers qubits si le premier vaut  $|1\rangle$ .

Son effet sur les vecteur de base de  $\mathbb{C}^8$  sera donc le suivant :

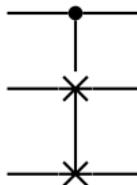
- $F|000\rangle = |000\rangle$
- $F|001\rangle = |001\rangle$
- $F|010\rangle = |010\rangle$
- $F|011\rangle = |011\rangle$
- $F|100\rangle = |100\rangle$
- $F|101\rangle = |110\rangle$
- $F|110\rangle = |101\rangle$
- $F|111\rangle = |111\rangle$

## Porte de Fredkin 2/2

La matrice de la porte de Fredkin se déduit des actions sur les vecteurs de base :

$$Fredkin = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Elle est représentée ainsi



## Racine carrée de la porte SWAP 1/2

La porte SWAP est une matrice unitaire, c'est une rotation dans  $\mathbb{C}^4$ , on peut lui trouver une racine carrée.

Si  $\overline{CX}$  représente une porte CX "tête bêche", alors on peut écrire

$$\text{SWAP} = CX \times \overline{CX} \text{ times } CX$$

On en déduit que  $\sqrt{\text{SWAP}} = CX \times \sqrt{\overline{CX}} \times CX$ , en effet, il est simple de vérifier que

$$\begin{aligned}\sqrt{\text{SWAP}} \times \sqrt{\text{SWAP}} &= (CX \times \sqrt{\overline{CX}} \times CX) \times (CX \times \sqrt{\overline{CX}} \times CX) \\ &= CX \times \sqrt{\overline{CX}} \times \sqrt{\overline{CX}} \times CX \\ &= CX \times \overline{CX} \times CX \\ &= \text{SWAP}\end{aligned}$$

## Racine carrée de la porte SWAP 2/2

De la même manière qu'on a établi la matrice de  $\overline{CX}$  il est simple d'établir la matrice de  $\sqrt{\overline{CX}}$  :

$$\sqrt{\overline{CX}} = \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1+i & 0 & 1-i \\ 0 & 0 & 2 & 0 \\ 0 & 1-i & 0 & 1+i \end{pmatrix}$$

Par conséquent, la matrice de  $\sqrt{SWAP}$  va s'écrire de la manière suivante :

$$\begin{aligned} \sqrt{SWAP} &= CX \times \sqrt{\overline{CX}} \times CX \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \times \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1+i & 0 & 1-i \\ 0 & 0 & 2 & 0 \\ 0 & 1-i & 0 & 1+i \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1+i & 1-i & 0 \\ 0 & 1-i & 1+i & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix} \end{aligned}$$

# Plan

9 Les circuits quantique

10 Les opérateurs sur 1 seul qubits

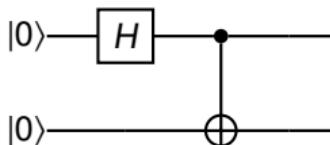
11 Les opérateurs sur 2 à n qubits

12 Les circuits sont des matrics

13 Mesures

# Base de Bell et circuit EPR

Le circuit suivant (que nous avons déjà rencontré) implémente une "paire EPR"



Il met en oeuvre à la fois de la superposition (via la porte H) et de l'intrication (via la porte CNOT).

Il change la base canonique de  $\mathbb{C}^2$  en la **base de Bell**, orthonormale, formée d'états intriqués.

- l'état  $|00\rangle$  est envoyé sur la paire EPR,  $|\Phi+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- l'état  $|01\rangle$  est envoyé sur  $|\Psi+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
- l'état  $|10\rangle$  est envoyé sur  $|\Phi-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
- l'état  $|11\rangle$  est envoyé sur  $|\Psi-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

# Fonctionnement du circuit EPR

On peut analyser le fonctionnement de ce circuit de la façon suivante : L'état de départ est  $|0\rangle \otimes |0\rangle = |00\rangle$

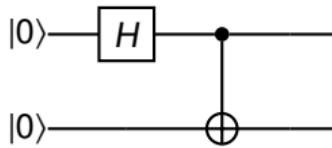
On applique une porte H au premier qubit, état devient

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

On applique ensuite une porte CNOT qui laisse  $|00\rangle$  inchangé, mais qui transforme  $|10\rangle$  en  $|11\rangle$ . Il en résulte la paire EPR.

$$\text{Paire EPR : } \text{CNOT}\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

## Calcul de la matrice de la paire EPR 1/3



Le circuit EPR se compose de deux étapes :

- une paire H sur le premier qubit, rien sur le second qbit ;
- une porte CNOT sur les deux qubits ;

La première étape peut s'écrire comme le produit tensoriel de la porte H et de l'identité :

$$\begin{aligned} Step1 &= H \otimes I = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \end{aligned}$$

## Calcul de la matrice de la paire EPR 2/3

On rappelle que la porte CNOT s'écrit ainsi

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Dans l'exécution du circuit, on applique d'abord  $H \otimes I$  puis CNOT, on applique donc le produit matriciel  $CNOT \times (H \otimes I)$ .

**Attention :** les matrices se composent comme les applications, le produit est en ordre inverse de l'application des matrices.

## Calcul de la matrice de la paire EPR 3/3

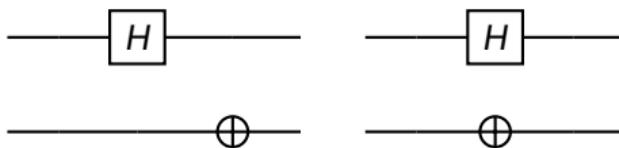
Le calcul matriciel donne le résultat suivant

$$\begin{aligned} CNOT \times (H \otimes I) &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \times \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \end{aligned}$$

On rappelle que les colonnes de cette matrice sont les images des vecteurs de la base canonique. Dans le cas du circuit de la paire EPR, on retrouve sans surprise les états de Bell.

# Attention aux étapes !

Les étapes, ou "colonnes", des circuits quantiques sont très importants. Les deux circuits suivants sont très différents



Le premier correspond à  $(I \otimes X) \times (H \otimes I)$ , le second correspond à  $H \otimes X$

# Plan

9 Les circuits quantique

10 Les opérateurs sur 1 seul qubits

11 Les opérateurs sur 2 à n qubits

12 Les circuits sont des matrics

13 Mesures

## Observables

Les observables correspondent à des grandeurs physiques qui peuvent être observées et donc mesurées. On doit ce terme à Werner Heisenberg.

Mathématiquement, Les observables sont des opérateurs dans des espaces de Hilbert tels que

- l'opérateur observable  $A$  est linéaire, il sera représenté par une matrice ;
  - les mesures correspondent aux valeurs propres de l'observable, celles-ci doivent être réelles, ce qui impose que l'observable  $A$  soit hermitien donc auto-adjoint ;
  - les vecteurs propres de l'observable sont orthogonaux, et ils forment une base de l'espace de Hilbert ;
  - cette base est normalisable, on peut modifier  $A$  pour disposer d'un observable dont les vecteurs propres forment une base orthonormée.

Fondamentalement, quand on mesure une grandeur physique par le biais d'un observable, on mesure l'une des valeurs propres de l'observable, ou plutôt la probabilité de l'occurrence d'une valeur propre d'observable.

## Mesures selon Z

On ne mesure pas un qubit par rapport à une base (par exemple  $\{|0\rangle, |1\rangle\}$  ou  $\{|+\rangle, |-\rangle\}$ ), on observe selon un opérateur hermitien dont les vecteurs propres forment la base en question.

Considérons à présent l'opérateur Z de Pauli dont la matrice est

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Il est trivial de constater que cet opérateur dispose de deux valeurs propres, 1 et  $-1$ , et que

$$Z|0\rangle = |0\rangle \text{ et } Z|1\rangle = -|1\rangle$$

La base canonique est en fait la base de vecteurs propres de Z. Réaliser une mesure dans cette base (canonique) revient à réaliser une observation, donc une mesure de valeur propre, par le biais de 2 pris comme un observable.

## Mesure selon X

Intéressons-nous à présent à la base, dite de Hadamard, de  $\mathbb{C}^2$ , à savoir  $(|+\rangle, |-\rangle)$ .

Cette fois-ci, c'est à l'opérateur X qu'on va s'intéresser. On rappelle que

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Il est simple de vérifier que  $(|+\rangle$  et  $|-\rangle$ ) sont les vecteurs propres de X, et qu'ils font associés aux valeurs propres 1 et -1. En effet

$$X|+\rangle = \frac{1}{\sqrt{2}}(H|0\rangle + H|1\rangle) == \frac{1}{\sqrt{2}}(ket1 + |0\rangle) = |+\rangle$$

$$X|-\rangle = \frac{1}{\sqrt{2}}(H|0\rangle - H|1\rangle) == \frac{1}{\sqrt{2}}(ket1 - |0\rangle) = -|1\rangle$$

Mesurer un qubit dans la base de Hadamard revient à effectuer une mesure grâce à X utilisé comme un observable.

## Autres opérateurs de mesures

On pourrait mesurer selon l'opérateur Y. Ses valeurs propres sont 1 et -1 et ses les vecteurs propres, qui figurent sur la sphère de Bloch, sont  $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$  et  $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$

Il est à noter que l'opérateur H, qui est égal à  $\frac{1}{\sqrt{2}}(X + Z)$ , est également un observable, même s'il est rarement utilisé en tant que tel dans l'informatique quantique.

# Plan

- 14 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini
- 15 Premiers algorithmes quantique : Bernstein-Vazirini
- 16 Théorème de non-clonage
- 17 Boîte à outils universelle pour construire les portes
- 18 Téléportation quantique et codage super-dense
- 19 Les mathématiques derrière RSA
- 20 Transformée de Fourier discrète et transformée de Fourier quantique
- 21 Algorithme de Simon
- 22 Algorithme de Shor

# L'algorithme de Deutsch-Josza à 2 qubits

Cette section décrit un algorithme très simple et son implémentation sous la forme d'un circuit quantique. Il n'est pas très élaboré, mais va permettre de prendre en main différentes notions propres à l'informatique quantique.

Cet algorithme a été défini en 1992 par David Deutsch et Rochard Josza . Il a été amélioré en 1998 par Richard Cleve, Artur Ekert, Chiara Macchiavello, et Michele Mosca.

L'algorithme de Deutsch-Josza se formule ainsi : étant donné une fonction booléenne  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ , comment déterminer si  $f$  est constante ?

## Approche classique

Une analyse rapide du problème montre qu'il y a 4 cas possibles pour une telle fonction booléenne :

- ①  $f(0) = 0, f(1) = 1, f(0) \oplus f(1) = 1$
  - ②  $f(0) = 1, f(1) = 0, f(0) \oplus f(1) = 1$
  - ③  $f(0) = 0, f(1) = 0, f(0) \oplus f(1) = 0$
  - ④  $f(0) = 1, f(1) = 1, f(0) \oplus f(1) = 0$

Soit deux cas avec des fonctions constantes et deux cas avec des fonctions uniformes. On peut déterminer le type de la fonction en testant la valeur de  $f(0) \oplus f(1)$  avec l'opérateur XOR, noté  $\oplus$ .

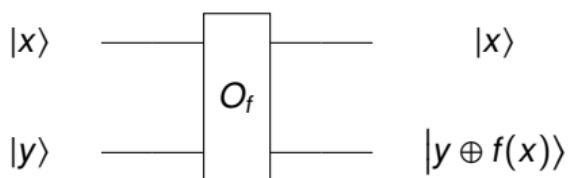
Si  $f$  est constante, on aura  $f(0) \oplus f(1) = 0$ , mais si elle est uniforme, on aura  $f(0) \oplus f(1) = 1$ .

Avec un ordinateur classique, il faudra deux appels à la fonction  $f$  pour déterminer le type de la fonction.

## Approche quantique : Oracle

La première étape consiste en la construction d'un *oracle*. Un oracle  $O_f$  est une "boîte noire" dans le circuit qui implémentera la fonction  $f$ .

Cet opérateur doit être linéaire et inversible.



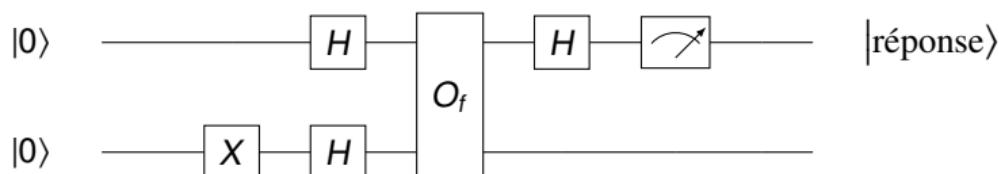
L'oracle agit ainsi :

- il agit sur 2 qubits, le premier porte l'argument, le second portera le résultat ;
  - le premier qubit, l'argument, n'est pas modifié par l'oracle ;
  - le second qubit est XORé avec la valeur  $f(x)$

Cet oracle est inversible, si on l'applique deux fois, le premier qubit ne changera toujours pas et le second deviendra  $|y \oplus x \oplus x\rangle = |y \oplus 0\rangle = |y\rangle$

# Circuit quantique implémentant l'algorithme de Deutsch-Josza

L'algorithme de Deutsch-Josza sera implémenté par le circuit suivant :



On peut dès lors commencer à dérouler le fonctionnement de ce circuit. La porte X va passer le second qubit dans l'état  $|1\rangle$ , on a donc 2 qubits dans l'état  $|01\rangle$  avant les portes H. Quand elle s'applique, on va avoir :

$$\begin{aligned}(H \otimes H)|01\rangle &= H|0\rangle \otimes H|1\rangle = |+\rangle \otimes |- \rangle \\&= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\&= \frac{1}{2}(|00\rangle + |10\rangle - |01\rangle - |11\rangle) \\&= \frac{|0\rangle (|0\rangle - |1\rangle)}{2} + \frac{|1\rangle (|0\rangle - |1\rangle)}{2}\end{aligned}$$

# Application de l'Oracle

On applique l'oracle  $O_f$  qui est linéaire, son action change l'état précédent en

$$|\phi_1\rangle = \frac{|0\rangle(|0\oplus f(0)\rangle - |1\oplus f(0)\rangle)}{2} + \frac{|1\rangle(|0\oplus f(1)\rangle - |1\oplus f(1)\rangle)}{2}$$

On distingue ensuite les cas selon les valeurs de  $f(0)$  et  $f(1)$ .

- Si  $f(0) = 0$ , on a  $|0\oplus f(0)\rangle - |1\oplus f(0)\rangle = |0\oplus 0\rangle - |1\oplus 0\rangle = |0\rangle - |1\rangle$
- Si  $f(0) = 1$ , on a  $|0\oplus f(0)\rangle - |1\oplus f(0)\rangle = |0\oplus 1\rangle - |1\oplus 1\rangle = |1\rangle - |0\rangle = -(|0\rangle - |1\rangle)$

De même

- Si  $f(1) = 0$ , on a  $|0\oplus f(1)\rangle - |1\oplus f(1)\rangle = |0\oplus 0\rangle - |1\oplus 0\rangle = |0\rangle - |1\rangle$
- Si  $f(1) = 1$ , on a  $|0\oplus f(1)\rangle - |1\oplus f(1)\rangle = |0\oplus 1\rangle - |1\oplus 1\rangle = |1\rangle - |0\rangle = -(|0\rangle - |1\rangle)$

## Une astuce de calcul

On va alors recourir à une astuce de notation qui est très courante en arithmétique booléenne en introduisant des puissances de  $-1$ , les lignes précédentes peuvent se réécrire ainsi :

$$|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle = (-1)^{f(0)}(|0\rangle - |1\rangle)$$

$$|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle = (-1)^{f(1)}(|0\rangle - |1\rangle)$$

Si l'on reporte cela dans l'état précédent  $|\phi_1\rangle$ , on peut écrire

$$\begin{aligned} |\phi_1\rangle &= \frac{|0\rangle (|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle)}{2} + \frac{|1\rangle (|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)}{2} \\ &= \frac{(-1)^{f(0)} |0\rangle (|0\rangle - |1\rangle)}{2} + \frac{(-1)^{f(1)} |1\rangle (|0\rangle - |1\rangle)}{2} \end{aligned}$$

## Suite du calcul

On a vu que multiplier par un nombre dont la norme est 1 ne change rien au fonctionnement et en particulier ne change rien à la mesure. L'état  $|\phi_1\rangle$  est donc équivalent à l'état  $|\phi_2\rangle = (-1)^{f(0)} |\phi_1\rangle$  et on notera alors que

$$\begin{aligned} |\phi_2\rangle &= \frac{(-1)^{f(0)}(-1)^{f(0)} |0\rangle (|0\rangle - |1\rangle)}{2} + \frac{(-1)^{f(0)}(-1)^{f(1)} |1\rangle (|0\rangle - |1\rangle)}{2} \\ &= \frac{|0\rangle (|0\rangle - |1\rangle)}{2} + \frac{(-1)^{f(0)+f(1)} |1\rangle (|0\rangle - |1\rangle)}{2} \\ &= \frac{|0\rangle + (-1)^{f(0)+f(1)} |1\rangle}{\sqrt{2}} \otimes |- \rangle \end{aligned}$$

# Fin du calcul

Distinguons à présent selon les valeurs relatives de  $f(0)$  et  $f(1)$ . On notera que

- Si  $f(0) = f(1)$  alors  $f(0) + f(1)$  vaut soit 0 soit 2, donc  $(-1)^{f(0)+f(1)}$  vaut 1
- Si  $f(0) \neq f(1)$  alors on a une valeur 0 et une valeur 1 dont la somme fait 1 donc  $(-1)^{f(0)+f(1)}$  vaut -1

Par conséquent

- Si  $f(0) = f(1)$  alors  $|\phi_2\rangle = \frac{|0\rangle(|0\rangle-|1\rangle)}{2} + \frac{|1\rangle(|0\rangle-|1\rangle)}{2} = \frac{(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)}{2}$
- Si  $f(0) \neq f(1)$  alors  $|\phi_2\rangle = \frac{|0\rangle(|0\rangle-|1\rangle)}{2} - \frac{|1\rangle(|0\rangle-|1\rangle)}{2} = \frac{(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)}{2}$

On peut condenser cette équation en introduisant les notations  $|+\rangle$  et  $|-\rangle$

- Si  $f(0) = f(1)$  alors  $|\phi_2\rangle = \frac{(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)}{2} = |+\rangle|-\rangle$
- Si  $f(0) \neq f(1)$  alors  $|\phi_2\rangle = \frac{(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)}{2} = |-\rangle|-\rangle$

# Analyse

En se s'intéressant qu'au premier qubit

- Si  $f(0) = f(1)$  alors le premier qubit vaudra  $|+\rangle$
- Si  $f(0) \neq f(1)$  alors le premier qubit vaudra  $|-\rangle$

En appliquant la dernière porte H sur le dernier qubit

- Si  $f(0) = f(1)$  alors le premier qubit vaudra  $H|+\rangle = |0\rangle$
- Si  $f(0) \neq f(1)$  alors le premier qubit vaudra  $H|-\rangle = |1\rangle$

Il suffira dès lors de mesurer ce qubit pour savoir si  $f$  est constante ou non.

Il suffit d'invoquer l'oracle  $O_f$  une seule fois pour avoir le résultat, alors que l'approche classique suppose d'évaluer la fonction  $f$  deux fois.

# Plan

14 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini

15 Premiers algorithmes quantique : Bernstein-Vazirini

16 Théorème de non-clonage

17 Boîte à outils universelle pour construire les portes

18 Téléportation quantique et codage super-dense

19 Les mathématiques derrière RSA

20 Transformée de Fourier discrète et transformée de Fourier quantique

21 Algorithme de Simon

22 Algorithme de Shor

## Enoncé de l'algorithme de Bernstein-Vazirini

L'algorithme de Bernstein-Vazirini peut être vu comme une variation de l'algorithme de Deutsch-Josza. Il a été proposé par Ethan Bernstein et Umesh Vazirani en 1992.

Ici, il s'agit de déterminer de manière efficace un secret codé sur  $n$  bits.

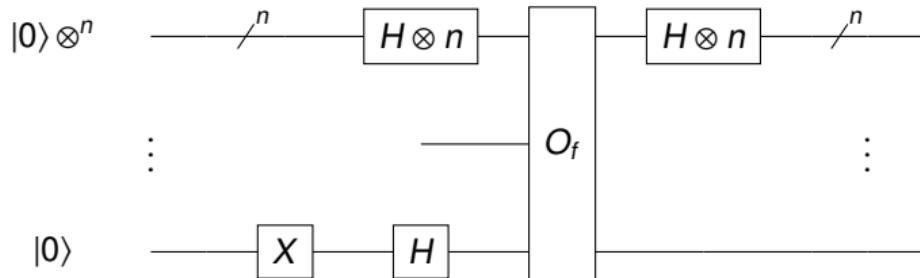
Étant donné une chaîne  $s$  de  $n$  bits, on peut construire une fonction  $f$  basé sur le produit pointé :

$$f : \{0, 1\}^n \rightarrow \{0, 1\}$$

$$x \mapsto s \cdot x = s_1 x_1 \oplus s_2 x_2 \oplus \cdots \oplus s_n x_n = s_1 x_1 + \cdots + s_n x_n \text{ modulo } 2$$

Connaissant  $f$ , et donc l'oracle  $O_f$  correspondant, on souhaite trouver la valeur de  $s$ .

## Circuit associé



## Superposition uniforme - barrière de portes H

L'application de  $n$  portes H sur  $n$  qubits permet de créer une superposition uniforme de la forme

$$\begin{aligned} |\phi_0\rangle &= \underbrace{|+\rangle \otimes |+\rangle \otimes \cdots \otimes |+\rangle}_{n \text{ termes}} \otimes |- \rangle \\ &= \frac{1}{\sqrt{2^{n+1}}} \underbrace{((|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle)) \otimes (|0\rangle - |1\rangle)}_{n \text{ termes}} \end{aligned}$$

que l'on peut écrire ainsi, si  $x$  prend toutes les valeurs binaires de 0 à  $2^n$

$$|\phi_0\rangle = \frac{1}{\sqrt{2^{n+1}}} \left( \sum_{x=0}^{2^n-1} |x\rangle \right) (|0\rangle - |1\rangle)$$

Dans cette notation, on écrira

$$|5\rangle = |0101\rangle, |3\rangle = |0011\rangle$$

# Application de l'oracle

L'application de l'oracle donne l'état  $|\phi_1\rangle$  décrit par

$$|\phi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \left( \sum_{x=0}^{2^n-1} |x\rangle \right) (|f(x)\rangle - |1 \oplus f(x)\rangle)$$

On sait que  $f$  prend les valeurs 0 ou 1, en appliquant le même raisonnement qu'au paragraphe précédent, on en déduit que  $|\phi_1\rangle$  est équivalent au qubit  $|\phi_2\rangle$

$$|\phi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \left( \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \right) (|0\rangle - |1\rangle) = \frac{1}{\sqrt{2^n}} \left( \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \right) \otimes |-\rangle$$

On peut ignorer le qubit ancillaire dans la suite du calcul, on sait qu'il portera l'état  $|-\rangle$   
On ne s'intéresse qu'aux  $n$  premiers qubits qui seront mesurés à la sortie du circuit.

## Application de la seconde barrière de portes H

La superposition uniforme est donnée par

$$|\phi\rangle = \frac{1}{\sqrt{2^{n+1}}} \left( \sum_{x=0}^{2^n-1} |x\rangle \right)$$

Si on applique une porte H sur chaque porte, on aura

$$H|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} H|x\rangle$$

Comment exprimer simplement  $H|x\rangle$  avec  $x \in \{00..0, \dots, 11..1\}$  ?

En utilisant le produit pointé entre deux nombres binaires, on peut écrire

$$H|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle$$

# Utilisation du produit pointé

Attention, dans ce qui suit on a 2 qubits, donc  $|3\rangle \mapsto |11\rangle$  et surtout  $|1\rangle \mapsto |01\rangle$

$$\begin{aligned}(H \otimes H)|01\rangle &= H|0\rangle \otimes H|1\rangle \\&= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\&= \frac{1}{2}(|00\rangle + |10\rangle - |01\rangle - |11\rangle) \\&= \frac{1}{2}((-1)^{00.01}|00\rangle + (-1)^{10.01}|10\rangle + (-1)^{01.01}|01\rangle + (-1)^{11.01}|11\rangle) \\&= \frac{1}{2} \sum_{x=0}^3 (-1)^{x.01}|x\rangle\end{aligned}$$

L'équation  $H|y\rangle = \frac{1}{2} \sum_{x=0}^3 (-1)^{x.y}|x\rangle$  se démontre facilement par récurrence.

# Retour à Bernstein-Vazirini

Avant la dernière bordée de porte  $H$  on a l'état

$$|\phi_2\rangle = \frac{1}{\sqrt{2^n}} \left( \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \right) \otimes |- \rangle = |\psi\rangle |- \rangle$$

Appliquons  $H$  sur le premier terme  $|\psi\rangle$

$$\begin{aligned} H|\psi\rangle &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} H|x\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \\ &= \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \end{aligned}$$

# Suite du calcul

$$\begin{aligned} H|\psi\rangle &= \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y} |y\rangle \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left[ \sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y} \right] |y\rangle \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left[ \sum_{x=0}^{2^n-1} (-1)^{f(x)+x \cdot y} \right] |y\rangle \end{aligned}$$

## Discussion et conclusion

La somme précédente peut s'écrire

$$\frac{1}{2^n} \sum_{y=0}^{2^n-1} \left[ \sum_{x=0}^{2^n-1} (-1)^{f(x)+x \cdot y} \right] |y\rangle = \sum_{y=0}^{2^n-1} \alpha_y |y\rangle \text{ avec } \alpha_y = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)+x \cdot y}$$

L'indice  $y$  va prendre toutes les valeurs entières possibles, il prend en particulier la valeur  $s$ , à savoir le secret que l'on cherche, or

$$\alpha_s = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(s)+s \cdot s}$$

Or  $f(x) = x \cdot s$  donc

$$\alpha_s = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{s \cdot s + s \cdot s} = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{2(s \cdot s)} = \frac{1}{2^n} \sum_{x=0}^{2^n-1} 1 = \frac{2^n}{2^n} = 1$$

## Résultat en un seul tir !

L'état final est un état quantique viable sur  $n$  qubit donc  $\sum_{y=0}^{2^n-1} |\alpha_y|^2 = 1$

Mais on sait que  $\alpha_s = 1$ , par conséquent, tous les autres coefficients  $\alpha_y$  sont nuls, donc l'état final

$$\sum_{y=0}^{2^n-1} \alpha_y |y\rangle = \alpha_s |s\rangle + \sum_{y \neq s} \alpha_y |y\rangle = |s\rangle + \sum_{y \neq s} 0 |y\rangle = |s\rangle$$

A la fin de l'exécution d'un seul tir, la valeur mesurée sera uniquement  $|s\rangle$ .

On a le résultat recherché en une seule et unique exécution de l'algorithme.

# Plan

- 14 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini
- 15 Premiers algorithmes quantique : Bernstein-Vazirini
- 16 Théorème de non-clonage**
- 17 Boîte à outils universelle pour construire les portes
- 18 Téléportation quantique et codage super-dense
- 19 Les mathématiques derrière RSA
- 20 Transformée de Fourier discrète et transformée de Fourier quantique
- 21 Algorithme de Simon
- 22 Algorithme de Shor

## Le théorème de non-clonage des états

Il est légitime de se demander s'il est possible de dupliquer un état quantique, en d'autres termes existe-t-il un opérateur unitaire  $U$  tel que  $U(|x\rangle|0\rangle) = |x\rangle|x\rangle$  .

On peut être tenté de se dire que la porte CNOT permet de faire une telle opération. En effet, si l'on considère les seuls états de base  $|0\rangle$  et  $|1\rangle$ , l'effet de la porte CNOT est  $|x\rangle|y\rangle \rightarrow |x\rangle|x \oplus y\rangle$ , et donc  $|x\rangle|0\rangle \rightarrow |x\rangle|x\rangle$ .  
Cette relation devient fausse dès lors que  $|x\rangle = \alpha|0\rangle + \beta|1\rangle$

Le théorème de non-clonage des états stipule qu'il n'existe pas d'opérateur unitaire  $U$  tel que  $U(|x\rangle|0\rangle) = |x\rangle|x\rangle$

## Démonstration sur 2 qubits

Supposons qu'il existe un opérateur  $U$  unitaire tel que  $U|x\rangle|0\rangle = |x\rangle|x\rangle$ . Par conséquent,

$$U|00\rangle = |00\rangle \text{ et } U|10\rangle = |11\rangle$$

Par conséquent

$$U\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) = U\left(\frac{|00\rangle}{\sqrt{2}}\right) + U\left(\frac{|10\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Cependant, on remarque que  $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle$

On devrait donc avoir

$$\begin{aligned} U\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) &= U\left(\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle\right) \\ &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

# Conclusion

$$U\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \text{ et } U\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)$$

On a donc un état dont l'image par  $U$  est à la fois un état intriqué  $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  et un état non intriqué (car factorisé)  $\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)$  ce qui est une évidente contradiction.

Par conséquent l'opérateur  $U$  n'existe pas, ce qui démontre le théorème.

# Plan

- 14 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini
- 15 Premiers algorithmes quantique : Bernstein-Vazirini
- 16 Théorème de non-clonage
- 17 Boîte à outils universelle pour construire les portes
- 18 Téléportation quantique et codage super-dense
- 19 Les mathématiques derrière RSA
- 20 Transformée de Fourier discrète et transformée de Fourier quantique
- 21 Algorithme de Simon
- 22 Algorithme de Shor

# Dans cette section

Cette section va aborder les points suivants

- zoologie étendue des portes
- comment construire toutes les portes possibles à 1 qubit (à une approximation près)
- comment construire toutes les portes à 2 qubits puis à  $n$  qubits

## Rappels :

- les portes et les circuits sont **toujours** des matrices unitaires
- on est dans un espace de Hilbert, on a le droit de parler de convergence de suites

# Portes paramétrées

Les portes  $X$ ,  $Y$  et  $Z$  sont des rotations d'angle  $\pi$ , les portes paramétrées agissent sur les mêmes axes de la sphère de Bloch, mais avec des angles variables.

Les portes paramétrées sont équivalentes, dans  $\mathbb{C}^4$ , aux rotations de  $\mathbb{C}$ , notée  $e^{i\theta}$

$$R_X(\alpha) = e^{-i\frac{\alpha}{2}X}, R_Y(\beta) = e^{-i\frac{\beta}{2}Y}, R_z(\gamma) = e^{-i\frac{\gamma}{2}Z}$$

**Attention au coefficient  $1/2$  !**

On rappellera que les matrices  $X$ ,  $Y$  et  $Z$  s'écrivent ainsi :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

## Formes exponentielles des portes paramétrées

Les opérations  $X$ ,  $Y$  et  $Z$  sont leurs propres inverses, donc leurs carrés valent l'identité. Par conséquent, si  $A$  représente l'un quelconque de ces trois opérateurs, on aura

$$\begin{aligned} e^{-i\theta A} &= \sum_{n=0}^{+\infty} \frac{(i\theta A)^n}{n!} = \sum_{p=0}^{+\infty} \frac{(i\theta A)^{2p}}{2p!} - \sum_{p=0}^{+\infty} \frac{(i\theta A)^{2p+1}}{2p+1!} \\ &= \sum_{p=0}^{+\infty} \frac{(-1)^p \cdot \theta^{2p} A^{2p}}{2p!} - i \cdot \sum_{p=0}^{+\infty} \frac{(-1)^p \theta^{2p+1} A \cdot A^{2p}}{2p+1!} \\ &= \sum_{p=0}^{+\infty} \frac{(-1)^p \cdot \theta^{2p}}{2p!} I - i \cdot \sum_{p=0}^{+\infty} \frac{(-1)^p \theta^{2p+1}}{2p+1!} A \\ &= \cos((\theta)I) - i \cdot \sin(\theta)A \end{aligned}$$

# Forme matricielle des portes paramétrées

Rotation  $R_X(\theta)$  par rapport à l'axe X de la sphère de Bloch

$$R_X(\theta) = e^{-i\theta/2X} = \cos(\theta/2) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - i \cdot \sin(\theta/2) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

Rotation  $R_Y(\theta)$  par rapport à l'axe Y de la sphère de Bloch

$$R_Y(\theta) = e^{-i\theta/2Y} = \cos(\theta/2) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - i \cdot \sin(\theta/2) \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

Rotation  $R_Z(\theta)$  par rapport à l'axe Z de la sphère de Bloch

$$R_Z(\theta) = e^{-i\theta/2Z} = \cos(\theta/2) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - i \cdot \sin(\theta/2) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

## Porte de déphasage

Les rotations selon l'axe Z correspondent à un changement de phase.

Les portes de déphasage sont synonymes des portes  $R_Z(\theta)$ , elles sont relativement simples à construire dans différentes technologies de qubits, on le trouve donc souvent dans les algorithmes.

- le qubit  $|0\rangle$  devient  $|0\rangle$ , qui est invariant, soit  $R_\phi|0\rangle = |0\rangle$
- le qubit  $|1\rangle$  subit un décalage de phase de  $\phi$ , il devient  $e^{i\phi}|1\rangle$ , soit  $R_\phi|1\rangle = e^{i\phi}|1\rangle$

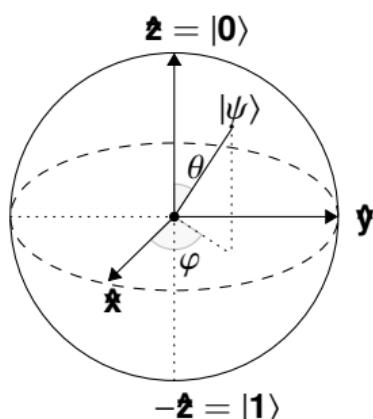
Cette porte modifie la phase entre la composante selon  $|0\rangle$  et la composante selon  $|1\rangle$

$$R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

Cette formulation est différente de celle de  $R_Z(\phi)$  à un facteur  $e^{-i\phi/2}$  près. Or on a vu que ce type de facteur n'a aucun impact sur la mesure, ces deux types de portes sont donc rigoureusement équivalents.

## Groupe de Pauli

Si l'on considère la sphère de Bloch on peut remarquer que les opérateurs de Pauli X, Y et Z permettent de "sauter" entre les six points remarquables de la sphère.



En d'autres termes, l'identité et les portes de Pauli, soit l'ensemble  $\{I, X, Y, Z\}$ , muni de la multiplication matricielle, engendre un groupe dont la structure est assez triviale et qui se compose des 16 éléments  $\{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$

## Portes S et T

La porte S est la racine carrée de la porte Z.

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

La porte S induit un déphasage de  $\pi/2$  sur la composante  $|1\rangle$  puisque  $i = e^{i\pi/2}$

La porte T est la racine carrée de la porte S.

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

La porte S induit un déphasage de  $\pi/4$  sur la composante  $|1\rangle$

## Groupe de Clifford

Le groupe de Pauli permet de "sauter" entre différents points remarquables de la sphère de Bloch, mais il est vite limité.

Il est plus intéressant de s'occuper du groupe formé par les portes de Clifford, ou groupe de Clifford. Celui-ci est généré par les portes H, CNOT et T. On s'intéressera aussi à la porte S qui est le carré de la porte T utilisée dans le théorème de Solovay-Kitaev

## Construire les portes à 1 qubit

Il est trivial de définir une porte à un qubit mathématiquement, il suffit d'écrire une matrice unitaire de  $\mathbb{C}^{2 \times 2}$ .

Les choses sont plus compliquées dans la réalité et dans le cadre d'une mise en œuvre industrielle. Comment peut-on construire toutes les portes possibles en n'utilisant qu'un nombre restreint de portes comme "briques de base" ?

La réponse est apportée par le théorème de Solovay-Kitaev.

## Théorème de Solovay-Kitaev

Si dispose de la porte T et et la porte H, on peut construire une suite convergente de portes  $P_n = A_n \times P_{n-1}$  où  $A_n$  est soit le produit THTH, soit le produit HTHT

En choisissant bien les différentes valeurs des  $A_n$ , on peut faire converger cette suite vers n'importe quel opérateur unitaire, donc vers n'importe quelle porte à un qubit.

En d'autres termes, on peut choisir  $\epsilon$  aussi petit que l'on veut et trouver une composition de portes THTH et HTHT située à une distance inférieure à  $\epsilon$  de la solution recherchée sur la sphère de Bloch.

À un facteur de précision  $\epsilon$  près, on peut construire toutes les portes en ne sachant implémenter que H et T.

## Décomposition ABC des portes à 1 qubits

Soit  $U$  une porte sur 1 qubit, il est possible de trouver 4 angles  $(\alpha, \beta, \gamma, \delta]$  (qui représentent les quatre degrés de liberté de l'opérateur) tels que

$$U = e^{i\alpha} \begin{pmatrix} e^{-i\frac{\beta+\delta}{2}} \cos(\frac{\gamma}{2}) & -e^{-i\frac{\beta-\delta}{2}} \sin(\frac{\gamma}{2}) \\ e^{i\frac{\beta-\delta}{2}} \sin(\frac{\gamma}{2}) & e^{i\frac{\beta+\delta}{2}} \cos(\frac{\gamma}{2}) \end{pmatrix}$$

On peut dès lors écrire  $U$  sous la forme suivante

$$U = e^{i\alpha} AXBXC$$

$$A \equiv e^{-\frac{i}{2}\beta Z} e^{-\frac{i}{4}\gamma Y}$$

$$B \equiv e^{\frac{i}{4}\gamma Y} e^{\frac{i}{4}(\beta+\delta)Z}$$

$$C \equiv e^{\frac{i}{4}(\beta-\delta)Z}$$

où  $X$ ,  $Y$  et  $Z$  sont les opérateurs de Pauli, leurs exponentiels complexes représentent donc des rotations autour des axes correspondant dans la sphère de Bloch.

**Remarque importante**  $ABC = I$

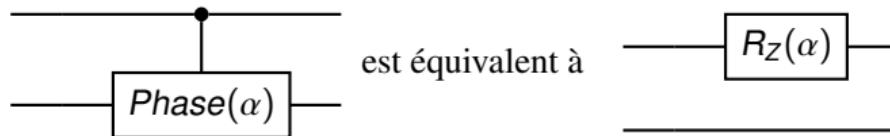
# Déphasage contrôlé

**ATTENTION :** L'opérateur  $\text{Phase}(\alpha)$  affecte à la fois la phase de  $|0\rangle$  et  $|1\rangle$ , à ne pas confondre avec  $R_Z(\alpha)$  qui n'affecte que la phase selon  $|0\rangle$ .

L'opérateur "Phase( $\alpha$ ) contrôlé" correspond à  $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \text{Phase}(\alpha)$

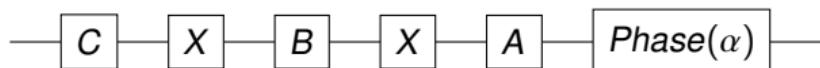
$$\text{Phase}(\alpha) = e^{i\alpha} \times I = \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \text{ donc } C\text{Phase}(\alpha) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha} & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

On déduit de l'équation précédente que

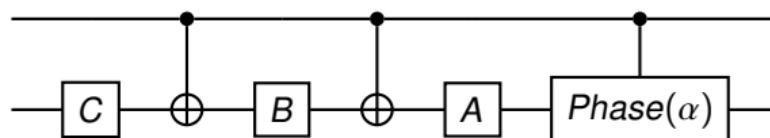


## Construire une porte contrôlée sur 2 qubits 1/2

Soit un opérateur unitaire  $U = e^{i\alpha}AXBXC$  avec  $ABC = I$

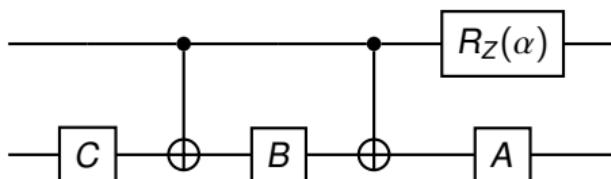


On construira CU en remplaçant les portes X par des CNOT et le déphasage par un déphasage contrôlé



## Construire une porte contrôlée sur 2 qubits 2/2

Ce circuit est équivalent à

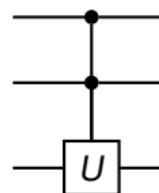


Ce circuit implémente bien  $CU$ , en effet

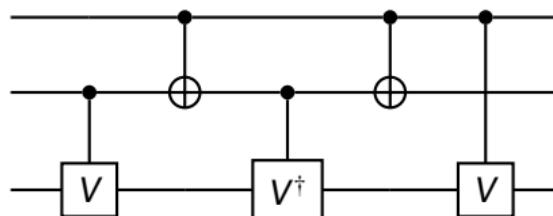
- si le qubit de contrôle vaut  $|1\rangle$ , on applique  $e^{i\alpha}AXBXC$  sur le second, donc  $U$
- si le qubit de contrôle vaut  $|0\rangle$ , on applique simplement  $ABC$  sur le second, donc on ne change rien puisque  $ABC = I$

## Porte à double contrôle - réduction de Sleathor-Weinfurter

Soit  $U$  un opérateur unitaire, soit  $V$  l'opérateur unitaire tel que  $V^2 = U$ , alors le circuit



Peut s'écrire sous la forme



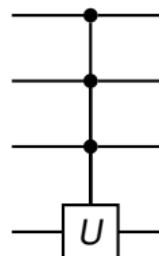
## Réduction de Sleathor-Weinfurter - discussion

- si le premier qubit vaut  $|0\rangle$  il ne change pas l'état du second qubit et,
  - si le second qubit vaut  $|0\rangle$ , aucune porte  $V$  n'est active sur le troisième qubit qui reste inchangé
  - si le second qubit vaut  $|1\rangle$ , il va activer les deux premières portes contrôlées sur le troisième qubit qui va subir  $V \times V^\dagger = I$ , donc ce dernier ne change pas ;
- si le premier qubit vaut  $|1\rangle$ , il active les portes CNOT sur le second qubit et la dernière contrôlée porte sur troisième qubit
  - si le second qubit vaut  $|0\rangle$ , il n'active pas la première porte, il passe à  $|1\rangle$  à cause de la première porte CNOT, active la porte  $V^\dagger$  sur le troisième qubit qui subit également une porte contrôlée  $V$  activée par le premier qubit, il subit  $V \times V^\dagger = I$  et ne change donc pas
  - si le second qubit vaut  $|1\rangle$ , il active la première porte  $V$ , est retourné par le premier CNOT, passe à  $|0\rangle$  et donc n'active pas  $V^\dagger$ , le troisième qubit subit également une porte  $V$  activée par le premier qubit, il subit donc  $V \times V = V^2 = U$

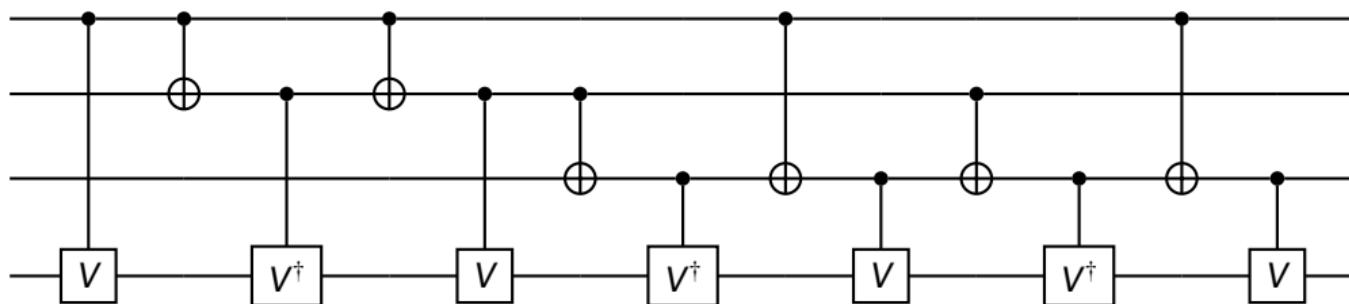
On voit donc que le troisième qubit subit l'effet d'une porte  $U$  (de deux portes  $V$ ) avec double contrôle.

## Toujours plus fort : triple contrôle !

Soit  $U$  un opérateur unitaire et soit  $V$  l'opérateur unitaire tel que  $V^4 = U$ , alors

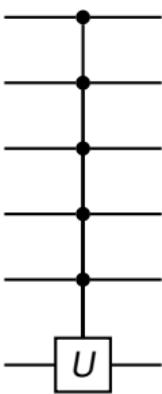


est équivalent à

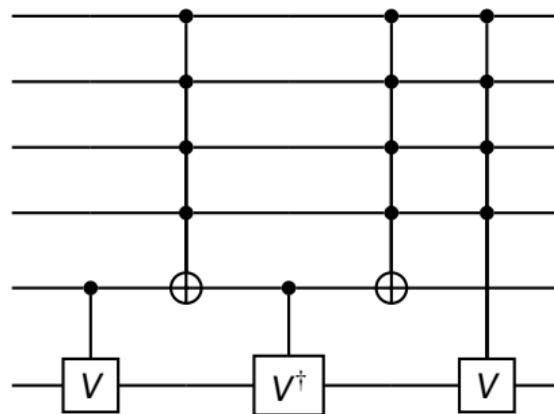


# Vers l'infini et au-delà ! Sleathor-Weinfuter revisité

Si  $U$  est unitaire et si  $V$  est sa racine carrée, alors



est équivalent à



Il suffit de savoir construire des racines carrées et des portes N à contrôles multiples.

# Une boîte à outils universelle pour construire les portes quantiques

En conclusion, nous avons vu que

- on sait construire toutes les portes à un qubit à la précision  $\epsilon$  près, via la méthode de Solovay-Kitaev
- la décomposition ABC et l'existence des portes CNOT, nous permet de construire des portes contrôlés à 2 qubits
- la décomposition de Sleathor-Weinfurter permet de construire des portes à trois qubits, en par récurrence à autant de qubits de contrôle que l'on veut. On peut donc construire de portes NOT contrôlées par autant de qubits que l'on veut
- avec des CNOT à contrôle multiples et les racines carrées de portes, on peut construire des portes avec autant de qubits de contrôle que l'on veut

Par conséquent, il suffit de savoir implémenter physiquement les H, T et CNOT pour implémenter n'importe quelle porte à  $n$  qubits. Donc n'importe quel circuit.

**ATTENTION :** Cela peut nécessiter un **très** grand nombre de portes.

# Algorithme de Shor - Introduction

L'algorithme de Shor est une pierre angulaire de la programmation quantique. Il est théoriquement capable de casser des chiffrements de type RSA, sur lesquels se basent les protocoles de sécurité d'Internet.

L'algorithme de Shor a largement contribué à la mise en lumière des principes et des ambitions de l'informatique quantique.

Nous allons voir

- quelques rappels sur le fonctionnement de RSA
- rappels sur la transformation de Fourier discrète (ou DFT)
- la QFT, l'implémentation quantique de la DFT
- l'algorithme de Simon
- l'algorithme de Shor qui utilise conjointement la QFT et l'algorithme de Simon..

# Plan

- 14 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini
- 15 Premiers algorithmes quantique : Bernstein-Vazirini
- 16 Théorème de non-clonage
- 17 Boîte à outils universelle pour construire les portes
- 18 Téléportation quantique et codage super-dense
- 19 Les mathématiques derrière RSA
- 20 Transformée de Fourier discrète et transformée de Fourier quantique
- 21 Algorithme de Simon
- 22 Algorithme de Shor

## Rappel sur la base de Bell

Etablit donné le circuit qui construit la porte EPR, celui-ci envoie la base  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$  sur la base suivante

- l'état  $|00\rangle$  est envoyé sur la paire EPR,  $|\Phi+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- l'état  $|01\rangle$  est envoyé sur  $|\Psi+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
- l'état  $|10\rangle$  est envoyé sur  $|\Phi-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
- l'état  $|11\rangle$  est envoyé sur  $|\Psi-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

# La situation

Est-il possible de déplacer un état entre deux acteurs et ainsi d'utiliser un circuit quantique pour transmettre de l'information sous la forme d'un qubit ?

Alice et Bon possède chacun un qubit de la paire EPR  $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ .

Afin de partager plus d'information, Alice et Bob vont partager un troisième qubit  $|\phi\rangle$ , non intriqué la paire EPR. Cet état est  $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ . Le système est donc dans un état global  $|\chi\rangle = (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ .

## Astuce de calcul

On va ici avoir recours à une petite astuce de calcul : on ne mesurera pas la paire EPR dans la base canonique, mais dans la base constituée par les états de Bell. On va donc réécrire cet état dans cette nouvelle base (et ce qui suit n'est que du pur calcul algébrique).

# Le calcul

On remarque que  $|00\rangle|1\rangle = |001\rangle = |0\rangle|01\rangle$ . On va donc avoir

$$\begin{aligned} |\chi\rangle &= (\alpha|0\rangle + \beta|1\rangle) \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|100\rangle + \frac{\alpha}{\sqrt{2}}|111\rangle \\ &= \frac{\alpha}{\sqrt{2}}|00\rangle|0\rangle + \frac{\alpha}{\sqrt{2}}|01\rangle|1\rangle + \frac{\beta}{\sqrt{2}}|10\rangle|0\rangle + \frac{\alpha}{\sqrt{2}}|11\rangle|1\rangle \end{aligned}$$

## Suite du calcul

Maintenant qu'on a fait apparaître l'ensemble des vecteurs de la base canonique, on transpose l'état dans la base de Bell en remplaçant les vecteurs canoniques par leurs expressions dans cette autre base .

$$\begin{aligned} |\chi\rangle &= \frac{\alpha}{\sqrt{2}} |00\rangle|0\rangle + \frac{\alpha}{\sqrt{2}} |01\rangle|1\rangle + \frac{\beta}{\sqrt{2}} |10\rangle|0\rangle + \frac{\alpha}{\sqrt{2}} |11\rangle|1\rangle \\ &= \frac{\alpha}{\sqrt{2}} \frac{1}{\sqrt{2}} (|\Phi+\rangle + |\Phi-\rangle) |0\rangle + \frac{\alpha}{\sqrt{2}} \frac{1}{\sqrt{2}} (|\Phi+\rangle - |\Phi-\rangle) |0\rangle + \\ &\quad \frac{\beta}{\sqrt{2}} \frac{1}{\sqrt{2}} (|\Psi+\rangle + |\Psi-\rangle) |0\rangle + \frac{\beta}{\sqrt{2}} \frac{1}{\sqrt{2}} (|\Psi+\rangle - |\Psi-\rangle) |1\rangle \\ &= \frac{1}{2} [|\Phi+\rangle (\alpha|0\rangle + \beta|1\rangle)] + \frac{1}{2} [|\Phi-\rangle (\alpha|0\rangle - \beta|1\rangle)] + \\ &\quad \frac{1}{2} [|\Psi+\rangle (\beta|0\rangle + \alpha|1\rangle)] + \frac{1}{2} [|\Psi-\rangle (\beta|0\rangle - \alpha|1\rangle)] \end{aligned}$$

# Constat

En résumé, on voit que  $|\chi\rangle$  s'écrit avec 4 composantes dans la base de Bell :

$$|\chi\rangle = (\alpha|0\rangle + \beta|1\rangle) \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$= \frac{1}{2}[|\Phi+\rangle(\alpha|0\rangle + \beta|1\rangle)] + (1)$$

$$\frac{1}{2}[|\Phi-\rangle(\alpha|0\rangle - \beta|1\rangle)] + (2)$$

$$\frac{1}{2}[|\Psi+\rangle(\beta|0\rangle + \alpha|1\rangle)] + (3)$$

$$\frac{1}{2}[|\Psi-\rangle(\beta|0\rangle - \alpha|1\rangle)] (4)$$

## Bilan

Si Alice effectue une mesure des deux premiers qubits dans la base de Bell, elle va mesurer chacun des états de Bell avec une probabilité de 25%, et le dernier qubit va s'effondrer sur l'un des quatre états possibles. Ces états ressemblent à  $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$  à une ou deux transformations unitaires près :

- si Alice mesure  $|\Phi+\rangle$ , on est dans le cas (1), il n'y a rien à faire sur le dernier qubit pour mesurer  $|\phi\rangle$
- si Alice mesure  $|\Phi-\rangle$ , on est dans le cas (2), il faut changer le signe de la composante sur  $|1\rangle$ , ce qui se fait en applicant une porte Z
- si Alice mesure  $|\Psi+\rangle$ , on est dans le cas (3), il faut interchanger permutez les deux coefficients, ce qui se fait avec une porte X
- si Alice mesure  $|\Psi-\rangle$ , on est dans le cas (4), il faut changer le signe et ensuite permutez les coefficients, donc appliquer une porte Z puis une porte X, ce qui revient à appliquer un opérateur composé XZ

# Beam me up, Scotty !

À son côté, Bob va lui aussi faire une mesure dans la base de Bell des deux premiers qubits et il obtiendra la même mesure qu'Alice, il saura donc quelle transformation appliquer parmi I, X, Z ou XZ et il obtiendra l'état  $|\phi\rangle$ .

On a donc déplacé l'état  $|\phi\rangle$  du premier qubit au troisième qubit, mais au prix d'une mesure et de la destruction (et l'effondrement) de l'état du premier qubit. Ce n'est donc pas en contradiction avec le théorème de non-clonage. Ce phénomène constitue la téléportation quantique.

## Codage super-dense

Bob peut éviter de mesurer les deux premiers qubits si Alice lui transmet (par des moyens non quantiques) deux bits  $a$  et  $b$  (de vrais bits, pas des qubits). Ces deux qubits décrivent lequel des quatre cas a été vu par Alice dans sa mesure. Bon n'a plus qu'à appliquer  $X^a Z^b$  pour obtenir  $|\phi\rangle$  sur le troisième qubit, attendu que  $X^0 = Z^0 = I$ . On parle alors de codage super-dense, trois qubits et deux bits standards permettent de déplacer un état quantique d'un qubit à l'autre.

# Plan

- 14 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini
- 15 Premiers algorithmes quantique : Bernstein-Vazirini
- 16 Théorème de non-clonage
- 17 Boîte à outils universelle pour construire les portes
- 18 Téléportation quantique et codage super-dense
- 19 Les mathématiques derrière RSA
- 20 Transformée de Fourier discrète et transformée de Fourier quantique
- 21 Algorithme de Simon
- 22 Algorithme de Shor

## Groupes multiplicatifs

RSA repose sur des fondements arithmétiques. Soit  $N = p \cdot q$  le produit de deux (grands) nombres premiers  $p$  et  $q$ .

On définit l'ensemble  $\mathbb{Z}/N\mathbb{Z}$ , l'ensemble des entiers modulo  $N$ , dont le cardinal est  $N$ . Si  $N$  était premier, cet ensemble serait un groupe multiplicatif (ce n'est pas le cas ici).

On définit l'ensemble  $(\mathbb{Z}/N\mathbb{Z})^*$  le sous-ensemble de  $\mathbb{Z}/N\mathbb{Z}$  des nombres qui sont premiers avec  $N$ . Cet ensemble est un groupe multiplicatif.

# Indicatrice d'Euler

Le cardinal de  $(\mathbb{Z}/N\mathbb{Z})^*$  est appelé *indicatrice d'Euler* de  $N$ , elle est notée  $\Phi(N)$ . L'indicatrice d'Euler donne le nombre d'entiers qui sont premiers avec  $N$ .

Dans le cas où  $N = p \cdot q$  avec  $p$  et  $q$  premiers, on peut montrer que  $\phi[N] = (p - 1)(q - 1)$

L'indicatrice d'Euler est associée au **théorème d'Euler**

$$\forall a \in \mathbb{N}, \forall n \in \mathbb{N}, n > 0, a \text{ premier avec } n, a^{\phi(n)} \equiv 1[n]$$

Si  $a$  et  $n$  sont premier entre eux, alors élevé à la puissance  $\phi[n]$  est congruent à 1 modulo  $n$ .

## Le fonctionnement de RSA

On choisit deux entiers  $e$  et  $d$  tels que  $e.d = 1$  modulo  $\phi[N]$ ,  $e$  premier avec  $\phi[N]$ . Le nombre  $d$  est l'inverse de  $e$  dans  $(\mathbb{Z}/N\mathbb{Z})^*$

On construit les clefs privées et publiques de la façon suivante :

- la clef publique est le produit  $N.d$
- la clef privée est le produit  $N.e$

Supposons que Alice veuille envoyer l'entier  $P$  à Bob. Alice construit le chiffrement  $C$  défini par  $C = P^e \pmod{N}$ .

La magie de RSA, ce résume dans cette formule :  $C^d \pmod{N} = P$ , on chiffre connaissant  $e$ , on déchiffre connaissant  $d$ .

## RSA - Démonstration

Sachant que  $e.d = 1[\phi(N)]$ ,  $\exists k, e.d = k\phi(N) + 1$ , et donc  $\phi(N) = (p - 1)(q - 1)$ .

Il est toujours possible de choisir N, p, q de telle sorte qu'ils soient grands par rapport à P. En fait, on découpe le message à envoyer en tronçons qui sont assez petits pour être plus petit que p et q, et donc d'être premier avec N. Par conséquent, d'après le théorème d'Euler, pour tout entier P,  $P^{\phi(N)} = 1[N]$

$$C^d[N] = P^{e.d}[N] = P^{k\phi(N)+1}[N] = P.P^{k\phi(N)}[N] = P.(P^{\phi(N)})^k = P.1^k[N] = P[N]$$

En conclusion, en découpant le message en entiers P suffisamment petits, si Alice et Bon connaissent leurs clefs publiques respectives et leurs propres clefs secrètes, et peuvent chiffrer et déchiffrer P.

# L'algorithme de Shor fragilise RSA

Pour casser RSA, il faut pouvoir calculer  $d$  connaissant  $e$  et  $N$ , donc il faut calculer l'indicatrice d'Euler qui est égale à  $\phi(N) = (p - 1)(q - 1)$ , il faut donc calculer  $p$  et  $q$ , donc factoriser  $N = p \cdot q$ .

L'algorithme de Shor permet de faire cette factorisation dans une durée raisonnable, il affaiblit les bases mêmes de l'algorithme RSA.

# Plan

- 14 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini
- 15 Premiers algorithmes quantique : Bernstein-Vazirini
- 16 Théorème de non-clonage
- 17 Boîte à outils universelle pour construire les portes
- 18 Téléportation quantique et codage super-dense
- 19 Les mathématiques derrière RSA
- 20 **Transformée de Fourier discrète et transformée de Fourier quantique**
- 21 Algorithme de Simon
- 22 Algorithme de Shor

# Transformée de Fourier classique et DFT

S f est fonction du temps (exprimé en seconde) et ν représente une fréquence (exprimée en hertz) :

$$\hat{f}(\nu) = \int_{-\infty}^{+\infty} f(t) e^{-2i\pi\nu t} dt$$

Si  $(s_n)_{0 \leq n < N}$  est une suite de N valeurs, on définira sa transformée de Fourier discrète, ou **DFT**, comme la suite  $(\hat{s}_n)_{0 \leq n < N}$

$$0 \leq n < N, \hat{s}_n = \sum_{k=0}^{N-1} s_k \cdot e^{-2i\pi \frac{kn}{N}}$$

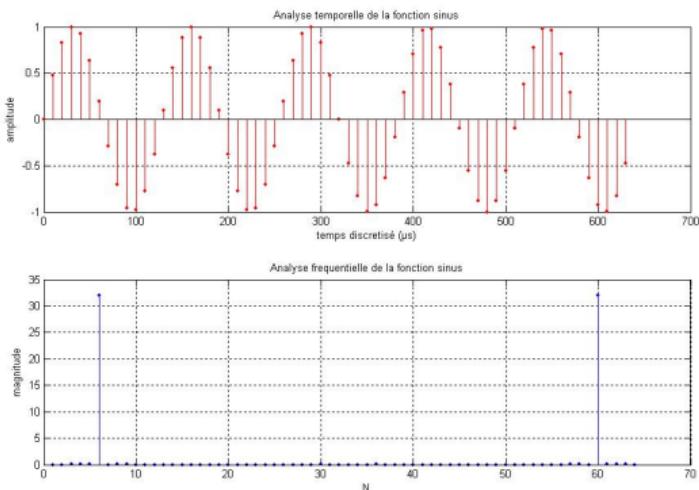
La suite  $(\hat{s}_n)$  es la décomposition spectrale de la suite  $(s_n)$ .

Si l'on pose  $\omega_N^i = e^{-2i\pi \frac{1}{N}}$ , la i<sup>ème</sup> racine N<sup>ème</sup> de l'unité, on peut écrire

$$\hat{s}_n = \sum_{k=0}^{N-1} s_k \cdot \omega_N^{kn}$$

$$s_n = \frac{1}{N} \sum_{k=0}^{N-1} \hat{s}_k \cdot \omega_N^{-kn}$$

# Décomposition spectrale discrète



La décomposition spectrale est équivalente à la suite d'origine, on passe facilement de l'une à l'autre.

$$\hat{s}_n = \sum_{k=0}^{N-1} s_k \cdot \omega_N^{kn}, \text{ et réciproquement } s_n = \frac{1}{N} \sum_{k=0}^{N-1} \hat{s}_k \cdot \omega_N^{-kn}$$

# Matrice de Vandermonde-Fourier

Connaissant les  $\omega_N^i = e^{2i\pi \frac{i}{N}}$ , on peut écrire la matrice suivante, dite *matrice de Vandermonde-Fourier*

$$W_N = (\omega_N^{(i-1)(j-1)})_{1 \leq i,j \leq N} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \omega_N^2 & \cdots & \omega_N^{N-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix}$$

# Opérateurs unitaires

La matrice de Vandermonde est presque unitaire (démonstration complète dans le poly), en effet

$$QF_N = \frac{1}{\sqrt{N}} W_N \text{ est unitaire mais non hermitienne}$$

A titre d'exemple on a

$$W_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \text{ et } W_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}$$

Au rang 2, la DFT se confond avec la porte de Hadamard.

# Transformée de Fourier quantique

La transformée de Fourier quantique (ou QFT) est une implémentation de la DFT via des méthodes d'informatique quantique.

Soit  $g()$  une fonction entière à valeurs dans  $\mathbb{C}$ .

$$g : (\mathbb{Z}/n\mathbb{Z})^* \rightarrow \mathbb{C}$$

On peut construire le vecteur suivant

$$\frac{1}{\sqrt{2^n}} \begin{pmatrix} g(0) \\ g(1) \\ \vdots \\ g(2^n - 1) \end{pmatrix}$$

qui correspondant à l'état quantique normalisé  $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$ .

On dispose d'un isomorphisme canonique entre les états quantiques et ce type de fonctions.

## QFT sous forme matricielle

$$QF_n = \frac{1}{\sqrt{N}} W_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \omega_N^2 & \cdots & \omega_N^{N-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix}$$

**Exemple :** Dans le cas où il y a 3 qubits, on aura la matrice  $8 \times 8$  suivante

$$QF_8 = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^1 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix} \text{ avec } \omega = e^{\frac{2i\pi}{8}}$$

## Images des vecteur de la base canonique par la QFT

Puisque  $QF_n$  est unitaire, ses vecteurs propres forment une base orthonormée.

Les colonnes de cette matrice sont les images des vecteurs de la base canonique.

Ainsi si  $|k\rangle$  est le  $k^{\text{ème}}$  vecteur de la base canonique, son image par  $QF_n$  est

$$QF_n \times |k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{2^n-1} \omega_{2^n}^{kj} |j\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{2^n-1} e^{2i\pi \frac{kj}{2^n}} |j\rangle$$

# QFT sous forme de circuit quantique

On n'utilisera que deux types de portes :

- des portes de Hadamard pour créer un état de superposition uniforme ;
- des portes de phases contrôlées, notées  $RP_m$ , dont la phase aura la valeur  $\frac{2\pi}{2^m}$

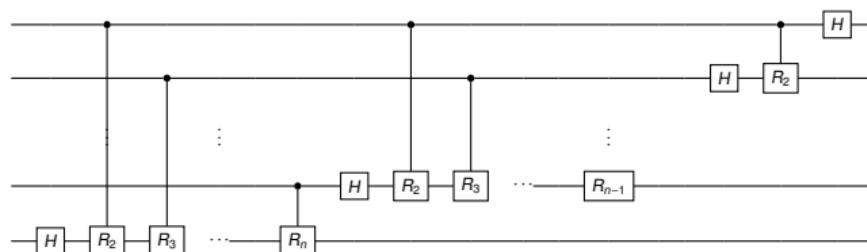


Figure – Circuit implémentant une QFT

## Autre écriture mathématique de la QFT

On peut démontrer que la QFT, définie par

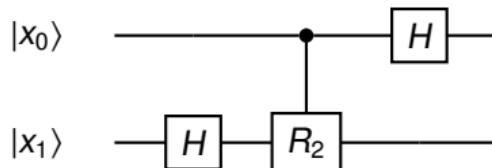
$$QF_n \times |k\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{-2i\pi \frac{kj}{2^n}} |j\rangle$$

est équivalente à la forme suivante (démonstration complète dans le poly).

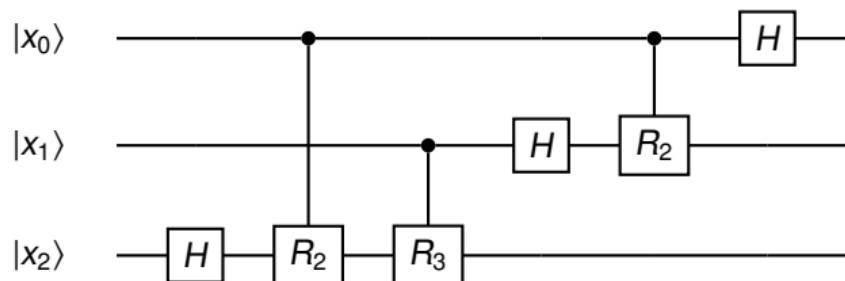
$$QF_n \times |k\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{j=1}^n (|0\rangle + e^{2i\pi \frac{k}{2^j}} |1\rangle)$$

$$QF_n \times |k\rangle = \frac{1}{\sqrt{2^n}} (|0\rangle + e^{2i\pi \frac{k}{2}} |1\rangle) \otimes (|0\rangle + e^{2i\pi \frac{k}{2^2}} |1\rangle) \otimes \cdots \otimes (|0\rangle + e^{2i\pi \frac{k}{2^n}} |1\rangle) \otimes$$

## Premiers cas simples



On sait construire les QFT pour n'importe quel nombre  $n$  de qubits, par récurrence.



# Plan

- 14 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini
- 15 Premiers algorithmes quantique : Bernstein-Vazirini
- 16 Théorème de non-clonage
- 17 Boîte à outils universelle pour construire les portes
- 18 Téléportation quantique et codage super-dense
- 19 Les mathématiques derrière RSA
- 20 Transformée de Fourier discrète et transformée de Fourier quantique
- 21 Algorithme de Simon
- 22 Algorithme de Shor

# Introduction

Daniel Simon a décrit l'algorithme qui porte son nom en 1997. Celui-ci permet de déterminer la période d'une fonction booléenne périodique. Cet algorithme exploite une nouvelle idée, à savoir l'effondrement causé par la mesure d'un état.

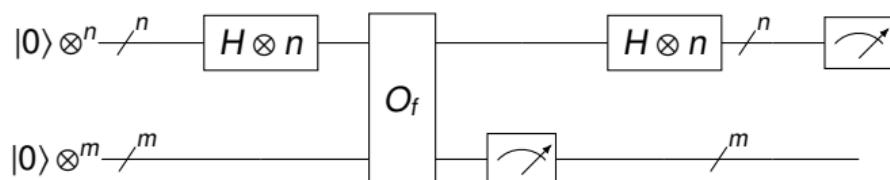
L'algorithme de Simon sert de base à l'algorithme de Shor.

**Remarque préalable :** une fonction périodique booléenne qui a N arguments possible prend exactement N valeurs. En effet, si  $f$  est L-périodique, alors  $f(x) = f(x \oplus L) = f(x \oplus L \oplus L)$ .

Avec  $n$  bits, le cardinal de  $\{0, 1\}^n$  est  $2^n$ . Il faut faire des tirages de  $x$  et de calcul de  $f(x)$  et s'arrêter lorsque l'on voit pour la seconde fois une valeur  $f(x)$  que l'on a déjà vue. Dans le cas le plus défavorable, il faudra effectuer  $2n - 1 + 1$  tirages pour être sûr de faire un tel tirage et de deviner ainsi la période.

# Approche quantique

Le circuit qui implémente l'algorithme de Simon exploite  $n$  qubits et  $m$  acillae.



La bordée initiale de portes H produit une superposition uniforme sur les  $n$  qubits de données.

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle^{\otimes m}$$

Lorsqu'on applique l'oracle qui évalue  $f()$  sur la superposition via les ancillae

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

## Impact de la mesure dans le calcul

L'astuce de cet algorithme, c'est d'exploiter l'effondrement quantique consécutif à une mesure

- On effectue une mesure des  $m$  ancilla
- cela revient à choisir une valeur  $f(a)$  arbitrairement
- comme la fonction est booléenne et  $L$ -périodique, les seuls états qui subsistent en superposition après l'effondrement causé par la mesure sont  $|a\rangle$  et  $|a \oplus L\rangle$  puisque  $f(a) = f(a \oplus L)$

Juste après la mesure, on aura donc l'état suivant :

$$\frac{1}{\sqrt{2}}(|a\rangle + |a \oplus L\rangle)|f(a)\rangle$$

# Hadamard entre dans la danse

On applique  $n$  portes de Hadamard, comme dans l'algorithme de Bernstein-Vazirini.  
On rappelle que

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle$$

Appliqué à l'état précédent

$$H^{\otimes n} \left( \frac{1}{\sqrt{2}} (|a\rangle + |a+L\rangle) |f(a)\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} ((-1)^{a \cdot y} + (-1)^{(a+L) \cdot y}) |y\rangle$$

qui peut être écrit

$$\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{a \cdot y} (1 + (-1)^{s \cdot y}) |y\rangle$$

# Discussion

Considérons l'équation obtenue

$$\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{a \cdot y} (1 + (-1)^{L \cdot y}) |y\rangle$$

- si  $s \cdot y = 1$ , on a ajouté 1 et  $-1$  et ont contribué pour 0 ;
- si  $s \cdot y = 0$ , on ajoute des contributions qui subsistent.

Il ne subsiste dans l'état que les composantes telles que  $L \cdot y = 0$ .

On a donc sur les  $n$  premiers qubits une superposition d'états  $|y\rangle$  tels que  $L \cdot y = 0$ .

Si on fait une mesure, on va découvrir l'un de ces états. On ne connaîtra pas  $L$  de manière explicite, on va connaître une variable dont le produit pointé avec  $L$  donne 0.

## Multiples tirages et systèmes linéaires

On va effectuer plusieurs tirs et construire une suite  $(y_i)$  qui vérifie  $\forall i, y_i \cdot L = 0$   
Avec  $k$  tirages on construit le système d'équations linéaires :

$$\left\{ \begin{array}{l} y_1 \cdot L = 0 \\ y_2 \cdot L = 0 \\ \vdots \\ y_k \cdot L = 0 \end{array} \right.$$

On peut démontrer qu'avec  $n - 1$  tirages, la probabilité d'avoir un système d'équations indépendantes, qui permette de trouver la valeur de  $s$ , est de 25%.

En réalisant au plus  $4n$  tirages, on est sûr d'avoir un système qui permette de connaître  $s$ .

On trouve la solution en  $4n$  étapes au plus, une approche classique aurait nécessité  $2^{n-1}$  au plus.

# Plan

- 14 Premiers algorithmes quantique : Deutsch-Josza et Bernstein-Vazirini
- 15 Premiers algorithmes quantique : Bernstein-Vazirini
- 16 Théorème de non-clonage
- 17 Boîte à outils universelle pour construire les portes
- 18 Téléportation quantique et codage super-dense
- 19 Les mathématiques derrière RSA
- 20 Transformée de Fourier discrète et transformée de Fourier quantique
- 21 Algorithme de Simon
- 22 Algorithme de Shor

## Arithmétique modulo n

L'algorithme de Shor combine habilement la QFT et les idées de l'algorithme de Simon. Shor s'intéresse à l'arithmétique modulo  $n$ .

Si  $n \in \mathbb{Z}$ , on notera  $\mathbb{Z}/n\mathbb{Z}$  le groupe quotient défini par la relation d'équivalence "a le même reste lors d'une division entière par  $n$ ".

Si  $n$  est un nombre premier, alors  $\mathbb{Z}/n\mathbb{Z}$  est un corps fini, puisque c'est un anneau quotienté par l'un de ses idéaux premiers.

On notera  $(\mathbb{Z}/n\mathbb{Z})^*$  la sous-partie de  $\mathbb{Z}/n\mathbb{Z}$  qui ne comprend que les éléments qui sont premiers avec  $n$ , c'est-à-dire qui n'ont pas de facteurs premiers communs avec  $n$ .

On peut montrer que  $(\mathbb{Z}/n\mathbb{Z})^*$  forme un groupe fini vis-à-vis du produit, en d'autre termes

$$\forall a \in (\mathbb{Z}/n\mathbb{Z})^*, \exists b \in (\mathbb{Z}/n\mathbb{Z})^*, a \times b = 1[n]$$

Il est légitime dès lors de parler d'élévation à la puissance dans  $(\mathbb{Z}/n\mathbb{Z})^*$ .

## Bases mathématiques de l'algorithme de Shor

Soit  $N$  un entier que l'on souhaite factoriser. Soit  $a$  un entier plus petit que  $\sqrt{N}$

L'idée de base de l'algorithme de Shor consiste à rechercher les valeurs  $r$  telles que

$$a^r \equiv 1[N], \text{ c'est à dire } a^r = 1 \text{ dans } (\mathbb{Z}/n\mathbb{Z})^*$$

Décrivons la fonction  $f_a$  suivante :

$$f_a : (\mathbb{Z}/n\mathbb{Z})^* \rightarrow (\mathbb{Z}/n\mathbb{Z}^*), f_a : x \mapsto a^x$$

Si  $r$  est tel que  $a^r \equiv 1[N]$  alors pour tout  $p$ , on a  $a^{r+p} = a^r \cdot a^p = a^p$  ce qui revient à dire que  $f_a(r+p) = f_a(p)$  donc que  $f_a$  admet une période  $r$ .

Inversement, si on découvre une valeur  $r$  telle que  $f_a$  est périodique, alors on a trouvé une valeur  $r$  telle que  $a^r \equiv 1[N]$ .

## Intérêt de trouver une puissance périodique

Si cette valeur  $r$  est impaire, on ne peut rien en faire, mais si  $r$  est paire, on peut trivialement trouver  $p$  tel que  $r = 2p$ .

On sait depuis longtemps que  $x^2 - 1 = (x - 1)(x + 1)$ , par conséquent

$$\text{Si } a^r \equiv 1[N], r = 2p, a^{2p} - 1 = (a^p - 1)(a^p + 1) = 0 \text{ dans } (\mathbb{Z}/n\mathbb{Z})^*$$

Si l'on sort de  $(\mathbb{Z}/n\mathbb{Z})^*$ , cela signifie que

$$\exists k \in \mathbb{N}, (a^p - 1)(a^p + 1) = kN$$

Cela signifie que les facteurs premiers de  $N$  sont répartis entre  $a^p - 1$  et  $a^p + 1$ .

Calculer le PGCD est trivial, par exemple en utilisant l'algorithme d'Euclide. Il suffit dès que de calculer  $\text{PGCD}(a^p - 1, N)$  et  $\text{PGCD}(a^p + 1, N)$  pour trouver les facteurs recherchés.

## Un exemple trivial, mais concret

Supposons que 15 soit un nombre très difficile à factoriser, et appliquons la recette précédente. On a donc  $N = 15$ .

Prenons un nombre  $a$  inférieur 15, par exemple  $a = 7$ , et évaluons  $f(a) = 7^a[15]$ .

| a | $7^a$ | f(a) |
|---|-------|------|
| 1 | 7     | 7    |
| 2 | 49    | 4    |
| 3 | 343   | 13   |
| 4 | 2401  | 1    |

On s'arrête ici car  $7^4 = 1[15]$ , et en plus 4 est le double de 2!!!

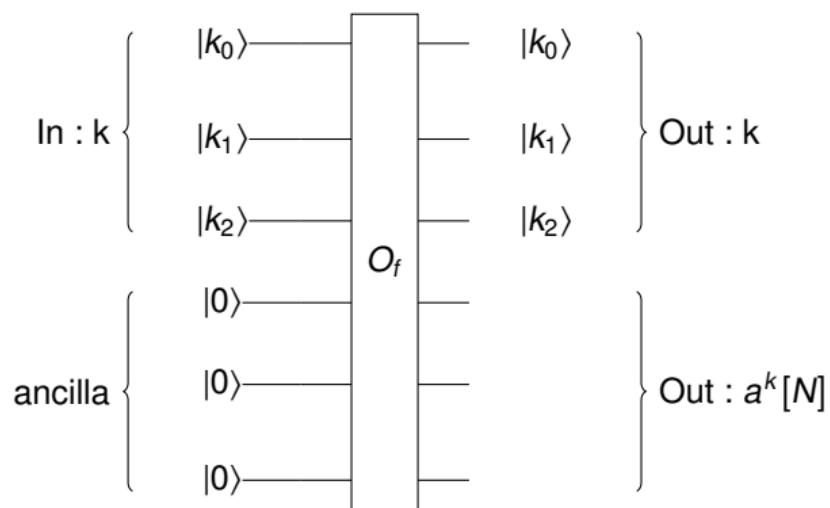
Dès lors, on calcule  $\text{PGCD}(7^2 + 1, 15) = \text{PGCD}(50, 15) = 5$  et  $\text{PGCD}(7^2 - 1, 15) = \text{PGCD}(48, 15) = 3$ .

On sait maintenant que  $15 = 3 \times 5$  !

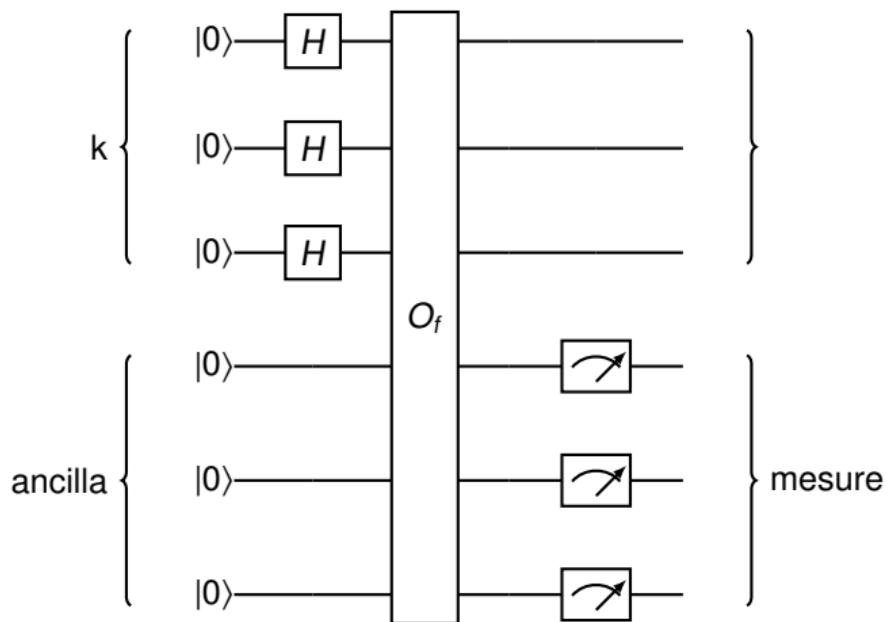
# Implémentation quantique de Shor

On souhaite factoriser l'entier  $N$ , on a  $n$  qubits et  $2^n \geq N$ , soit  $a < N$

Les qubits d'entrées représentent la valeur  $k$  sous forme binaire, ses bits sont  $k_0, k_1, \dots, k_p$ .  
L'action de l'oracle transforme  $|k\rangle \otimes |0\rangle$  en  $|k\rangle \otimes |a^k\rangle$



## Première étape du circuit



## Calcul de l'état du système après la première étape 1/2

L'état initial est  $|\phi_0\rangle = |0 \cdots 0\rangle \otimes |0 \cdots 0\rangle$ , l'application de  $n$  portes de Hadamard va le changer en  $|\phi_1\rangle$

$$|\phi_1\rangle = (H^{\otimes n} \otimes I) |\phi_0\rangle = (H^{\otimes n} \otimes I) \times (|0\rangle \otimes |0\rangle) = \left( \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle \otimes |0\rangle \right)$$

Si on applique l'oracle qui implémente  $f$ , on obtient alors  $|\phi_2\rangle$

$$|\phi_2\rangle = O_f \left( \left( \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle \otimes |0\rangle \right) \right) = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle \otimes |a^k\rangle$$

On a choisi la valeur  $a$  au hasard. On vérifie rapidement (algorithme d'Euclide) que  $a$  est premier avec  $N$ . Si  $a$  n'est pas premier avec  $N$ ... on vient de trouver un diviseur de  $N$  ! On s'arrête là le problème est résolu.

# Ce que l'on va faire avec l'algorithme

Soit  $r$  la période recherchée, on a

$$\forall p, a^{p+r} \equiv a^p[N] \text{ et donc } a^r \equiv 1[N]$$

Pour chaque entier  $k$ , on peut écrire  $k = pr + q, 0 \leq q < r$ , donc

$$|k\rangle \otimes |a^k\rangle = |pr + q\rangle \otimes |a^{pr+q}\rangle = |pr + q\rangle \otimes |a^q\rangle \text{ car } a^r \equiv 1[N]$$

On peut dès lors réécrire  $|\phi_3\rangle$

$$\begin{aligned} |\phi_3\rangle &= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle \otimes |a^k\rangle = \frac{1}{\sqrt{2^n}} \sum_{q=0}^{r-1} \sum_{p=0}^{(2^n/r)-1} |pr + q\rangle \otimes |a^{pr+q}\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{q=0}^{r-1} \sum_{p=0}^{(2^n/r)-1} |pr + q\rangle \otimes |a^q\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{q=0}^{r-1} \left( \sum_{p=0}^{(2^n/r)-1} |pr + q\rangle \right) \otimes |a^q\rangle \end{aligned}$$

## Mesure des ancillae

Comme dans l'algorithme de Simon, on effectue une mesure des qubits ancillaires. L'état  $|\phi_3\rangle$  s'effondre sur un état  $|\phi_4\rangle$  qui correspond à un certain  $q_0$  dont on sait simplement qu'il est inférieur à  $r$ .

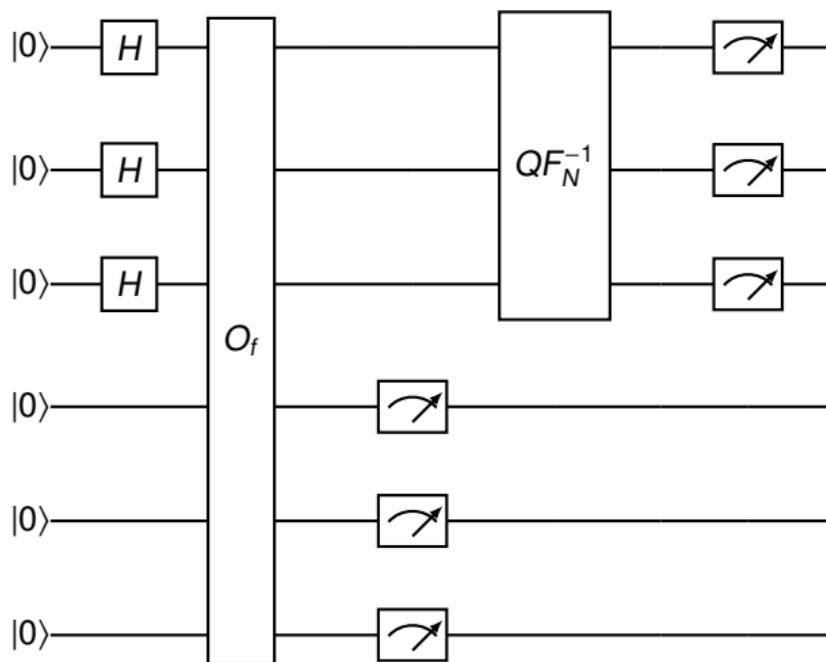
$$|\phi_4\rangle = \frac{\sqrt{r}}{\sqrt{2^n}} \left( \sum_{p=0}^{(2^n/r)-1} |pr + q_0\rangle \right) \otimes |a^{q_0}\rangle$$

La mesure des premiers qubits permet de connaître l'une des valeurs  $|pr + q_0\rangle$ .

On ne connaît pas  $r$  (la valeur que l'on cherche), et on ne peut pas déterminer  $p$ . On ne dispose de rien d'utile.

# La QFT entre en scène

On vient compléter le circuit avec une QFT inversée



# Effets de la QFT inversée

On rappelle que

$$QF_N^{-1} \times |k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{-jk} |j\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2i\pi \frac{jk}{N}} |j\rangle$$

La QFT inversée appliquée sur  $|\phi_4\rangle$  donne le résultat  $|\phi_5\rangle$  suivant

$$\begin{aligned} |\phi_5\rangle &= (QF_N^{-1} \otimes I) \times |\phi_4\rangle = (QF_N^{-1} \otimes I) \times \left( \frac{\sqrt{r}}{\sqrt{2^n}} \left( \sum_{p=0}^{(2^n/r)-1} |pr + q_0\rangle \right) \otimes |a^{q_0}\rangle \right) \\ &= \frac{\sqrt{r}}{\sqrt{2^n}} \left( \sum_{p=0}^{(2^n/r)-1} QF_N^{-1} \times |pr + q_0\rangle \right) \otimes |a^{q_0}\rangle \\ &= \frac{\sqrt{r}}{\sqrt{2^n}} \left( \sum_{p=0}^{(2^n/r)-1} \frac{1}{\sqrt{2^n}} \sum_{j=0}^{N-1} e^{-2i\pi \frac{j(pr+q_0)}{N}} |j\rangle \right) \otimes |a^{q_0}\rangle \\ &= \frac{\sqrt{r}}{2^n} \left( \sum_{j=0}^{N-1} \sum_{p=0}^{(2^n/r)-1} e^{-2i\pi \frac{j(pr+q_0)}{N}} |j\rangle \right) \otimes |a^{q_0}\rangle \\ &= \frac{\sqrt{r}}{2^n} \left( \sum_{j=0}^{N-1} \left( \sum_{p=0}^{(2^n/r)-1} e^{-2i\pi p \frac{jr}{2^n}} \right) e^{-2i\pi \frac{q_0 j}{2^n}} |j\rangle \right) \otimes |a^{q_0}\rangle \end{aligned}$$

## Simplification de l'équation

La situation est analogue à Bernstein-Vazirini : on ne le voit pas, mais beaucoup de termes sont en fait nuls !

Intéressons-nous au terme  $e^{-2ip\pi \frac{jr}{2^n}})$  et à la somme de ces termes :

- si  $\frac{jr}{2^n}$  est un entier, on élève  $e^{-2i\pi} = 1$  à la puissance et on fait en fait une somme de 1 ;
- si  $\frac{jr}{2^n}$  n'est pas un entier, on a une série géométrique de raison  $e^{-2i\pi \frac{jr}{2^n}})$

**Rappel mathématique :** On dispose du résultat suivant sur les suites

$$\forall k \neq 1, 1 + k + k^2 + k^3 + \cdots + k^{N-1} = \sum_{p=0}^{N-1} k^p = \frac{1 - k^N}{1 - k}$$

## Termes nuls et termes non-nuls

On a donc deux cas. Dans le premier  $\frac{jr}{2^n}$  est un entier et

$$\sum_{p=0}^{(2^n/r)-1} e^{-2i\pi p \frac{jr}{2^n}} = \sum_{p=0}^{(2^n/r)-1} 1 = \frac{2^n}{r}$$

Dans le second cas  $\frac{jr}{2^n}$  n'est pas un entier et

$$\sum_{p=0}^{2^n/(r-1)} e^{-2i\pi p \frac{jr}{2^n}} = \frac{1 - e^{-2i\pi \frac{jr}{2^n} \frac{2^n}{r}}}{1 - e^{-2i\pi \frac{jr}{2^n}}} = \frac{1 - e^{-2i\pi j}}{1 - e^{-2i\pi \frac{jr}{2^n}}} = \frac{1 - 1}{1 - e^{-2i\pi \frac{jr}{2^n}}} = 0$$

Donc seul le cas où  $\frac{jr}{2^n}$  est un entier donne une contribution non nulle, ce qui simplifie  $|\phi_5\rangle$

## État final du circuit avant dernière mesure

$$\begin{aligned} |\phi_5\rangle &= \frac{\sqrt{r}}{2^n} \left( \sum_{j=0}^{N-1} \left( \sum_{p=0}^{(2^n/r)-1} e^{-2i\pi p \frac{jr}{2^n}} \right) e^{-2i\pi \frac{q_0 j}{2^n}} |j\rangle \right) \otimes |a^{q_0}\rangle = \frac{\sqrt{r}}{2^n} \left( \sum_{j=0, \frac{jr}{2^n} \in \mathbb{N}}^{N-1} \frac{2^n}{r} e^{-2i\pi \frac{q_0 j}{2^n}} |j\rangle \right) \otimes |a^{q_0}\rangle \\ &= \frac{1}{\sqrt{r}} \left( \sum_{j=0, \frac{jr}{2^n} \in \mathbb{N}}^{N-1} e^{-2i\pi \frac{q_0 j}{2^n}} |j\rangle \right) \otimes |a^{q_0}\rangle \end{aligned}$$

On réalise ici une hypothèse simplificatrice : on suppose que la période recherchée  $r$  divise  $2^n$ . Dans ce cas, de 0 à  $2^n - 1$ , il y a  $r$  fois où  $\frac{jr}{2^n}$  est entier, on change l'index précédent pour écrire l'état de la manière suivante

$$\begin{aligned} |\phi_5\rangle &= \frac{1}{\sqrt{r}} \left( \sum_{j=0, \frac{jr}{2^n} \in \mathbb{N}}^{N-1} e^{-2i\pi \frac{q_0 j}{2^n}} |j\rangle \right) \otimes |a^{q_0}\rangle \\ &= \frac{1}{\sqrt{r}} \left( \sum_{l=0}^{r-1} e^{-2i\pi q_0 \frac{l}{r}} \left| \frac{2^n l}{r} \right\rangle \right) \otimes |a^{q_0}\rangle \end{aligned}$$

## Dernière mesure

Sous réserve de l'hypothèse où  $r$  divise  $2^n$ , on a

$$|\phi_5\rangle = \text{frac1} \sqrt{r} \left( \sum_{l=0}^{r-1} e^{-2i\pi q_0 \frac{l}{r}} \left| \frac{2^n l}{r} \right\rangle \right) \otimes |a^{q_0}\rangle$$

La mesure qui suit la QFT inverse va faire s'effondrer la superposition d'état vers l'un des états de bases qui la compose, on va voir un certain état  $|\phi_6\rangle$

$$|\phi_6\rangle = \left| \frac{2^n l_0}{r} \right\rangle \otimes |a^{q_0}\rangle$$

Le circuit nous permet donc de connaître une valeur entière  $\frac{2^n l_0}{r}$ , mais pas encore la valeur de la période  $r$  que nous cherchons.

## Récupération de la période - problématique

Supposons, après avoir divisé par  $2n$  que l'on obtienne 0.5, a-t-on la fraction  $1/2$  (donc  $l = 1, r = 2$ ),  $2/4$  (donc  $l = 2, r = 4$ ) ou  $4/8$  (donc  $l = 4, r = 8$ ) ?

Il est indispensable de lancer le circuit plusieurs fois pour avoir une série de couples  $(l_i, r_j)$ . Si l'on découvre un couple,  $(l_1, r_1)$  et  $(l_2, r_2)$  tels que  $r_1 = r_2$  et si  $l_1$  et  $l_2$  sont premiers entre eux alors on peut conclure sur la valeur de  $r$ .

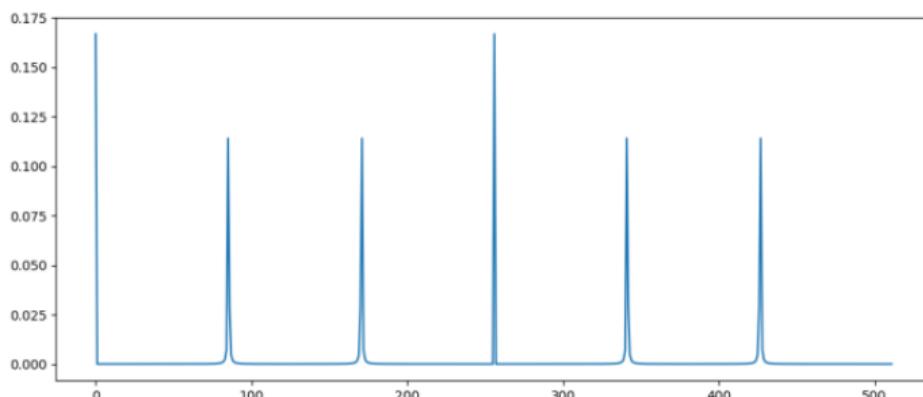
Par exemple, supposons qu'on ait échantillonné  $3/8, 1/2, 7/8$ . Les couples  $(3,8)$  et  $(7,8)$  nous permettent de conclure que  $r = 8$ .

Comme pour l'algorithme de Simon, il faut faire plusieurs runs du circuit pour conclure. On peut démontrer qu'il y a une probabilité supérieure à 5d'avoir deux  $l_i$  premiers entre eux, on est donc certain de trouver deux valeurs qui permettent de conclure avec 20 tirages

## Retour sur l'hypothèse simplificatrice

On a supposé que  $r$  divise  $2^n$ , et chaque cas  $\left| \frac{2^n I_0}{r} \right\rangle$  sera présent  $2^n/r$  fois.

Dans le cas où  $r$  ne divise pas  $2^n$ , chaque cas sera vu soit  $\lfloor 2^n/r \rfloor$  fois, soit  $\lceil 2^n/r \rceil$  fois. Les occurrences des valeurs possibles suivent une distribution qui ressemble à la figure suivante qui correspond au cas  $N=512$  (9 qubits) et la période cherchée égale à 6.



## Exploitation des fractions continues

Soit  $s = \frac{2^{n_l}}{r}$ , la mesure effectuée, il est possible de trouver un entier  $d$  tel que

$$|s.r - d.N| \leq \frac{r}{2}$$

et donc

$$\left| \frac{s}{N} - \frac{d}{R} \right| \leq \frac{1}{2N} \leq \frac{1}{M^2}$$

La décomposition en fractions continues permet de conclure.

## Entracte - éléments sur les fractions continues

Les fractions continues forment une nouvelle manière d'écrire des réels.

Une écriture décimale revient à écrire ceci :

$$x \in \mathbb{R}, x = x_0, x_1 x_2 x_3 \dots, x = x_0 + \sum_{i=1}^{+\infty} x_i \cdot 10^{-k}$$

L'écriture en fractions continues revient à écrire ceci :

$$x \in \mathbb{R}, x = [x_0; , x_1, x_2, x_3, \dots], x = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \dots}}}$$

Certains nombres bien connus adoptent des décompositions en fractions continues simples :

- le nombre d'or  $\phi$  est la racine positive de  $X^2 = X + 1$ , donc  $\phi = 1 + \frac{1}{\phi}$  et sa décomposition en fractions continues est  $[1; 1, 1, 1, 1, \dots]$ ;
- la racine de 2 vérifie  $(\sqrt{2} - 1)(\sqrt{2} - 1) = 2 - 1 = 1$  donc  $\sqrt{2} = 1 + \frac{1}{1 + \sqrt{2}}$ , soit  $\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \dots}}$  et sa décomposition en fractions continues est  $[1; 2, 2, 2, \dots]$

## N-réduites d'une fraction continue

On peut utiliser les fractions continues pour construire des approximations de nombres dont on connaît la décomposition.

Si on a  $a = [a_0; a_1, a_2, a_3, a_4, \dots]$ , on définit la **n-réduite** comme la décomposition arrêté au n<sup>ème</sup> terme.

Par exemple, on définit de la décomposition de  $\pi$  en fractions continues, soit  $[3; 7, 15, 1, 292, 1, 1, \dots]$  les approximations  $22/7$  et  $333/106$ .

## Identifier la période avec des fractions continues

Dans notre exemple, on a mesure  $s = \frac{247}{512}$ , on peut écrire

$$\frac{427}{512} = 0 + \frac{1}{\frac{512}{427}} = 0 + \frac{1}{1 + \frac{85}{427}}$$

Mais

$$\frac{85}{427} = \frac{1}{\frac{427}{85}} = \frac{1}{5 + \frac{2}{85}}$$

Et ainsi de suite... On en déduit la décomposition en fractions continues  $427/512 = [0; 1, 5, 42, 2]$ . On calcule les différents n-réduites et on obtient  $0, 1, 5/6, 211/253, 427/512$ .

On sait que la période est inférieur à M, donc à 21 dans notre cas, on retient donc l'approximation  $5/6$ , la dernière à avoir un dénominateur acceptable .

On réalise plusieurs tirages jusqu'à avoir deux fractions qui ont le même dénominateur et des numérateurs premiers entre eux.

# Plan

23 Les concepts de bases

24 Correction des erreurs

25 Les effets de l'environnement

26 Vision de Stinespring et opérateus de Kraus

27 Exemple : correction du bit-flip par encodage sur 3 qubits

# Introduction à la cryptographie quantique

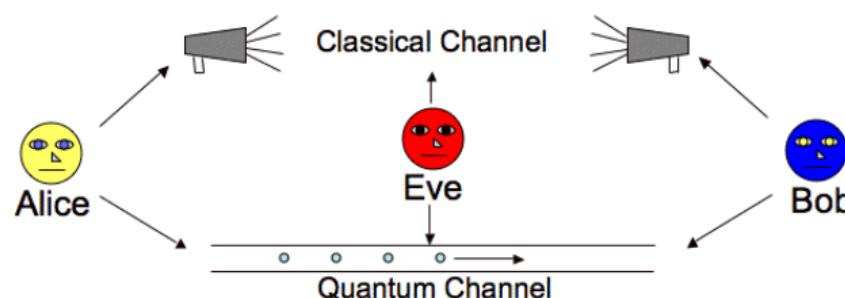
La cryptographie quantique exploite les principes de la mécanique quantique et de l'informatique quantique pour gérer des mécanismes de chiffrement.

En général, à l'état actuel des technologies, ces mécanismes vont majoritairement exploiter des "qubits volants", souvent implémentés par des photons. L'état des qubits sera implémenté par l'angle de polarisation des photons.

# Problématique

On est ici sur une logique de construction de clefs binaires entre deux parties, en s'appuyant sur des mécanismes quantiques.

Cette clef binaire pourra être utilisé pour chiffrer le message avec un simple XOR ou bien être impliquée dans un mécanisme de chiffrement plus complexe.

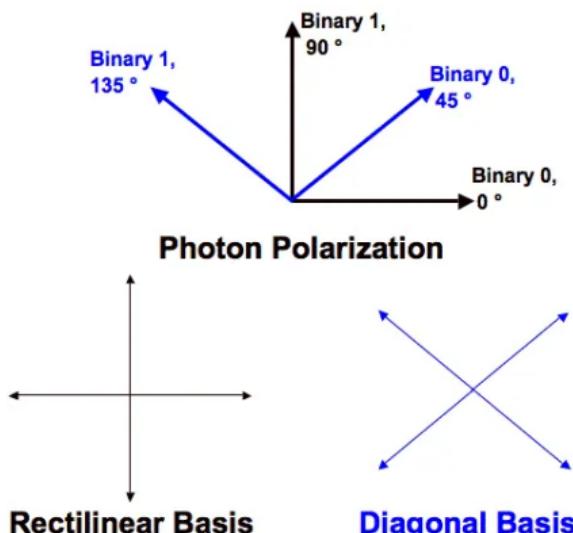


Dans ce schéma, Alice et Bob dispose d'un canal de communication quantique, et d'un canal public, non sécurisé (par ondes radio, ou par email). Eve, l'attaquant, peut facilement voir ce canal.

## Le protocole BB84 1/2

Le premier protocole de chiffrement quantique a été conçu en 1984 par Charles Bennett et Gilles Brassard.

Il s'appuie sur des qubits implémentés via des photons polarisés. Ces derniers peuvent être polarisés de deux manières différentes, une polarisation rectiligne et une polarisation diagonale



## Le protocole BB84 2/2

Du point de vue du formalisme, on utilisera des qubits individuels exprimés soit dans la base canonique ( $|0\rangle, |1\rangle$ ), soit dans la base de Bell ( $|+\rangle, |-\rangle$ ).

Le fonctionnement est le suivant :

- ① Alice choisit de manière aléatoire une chaîne de bits ;
- ② pour chaque bit, Alice choisit une base et envoie un photon encodé selon cette base, par exemple, si elle voit le bit 0 et la base ( $|+\rangle, |-\rangle$ ), elle expédie  $|+\rangle$  et si elle voit 1 et la base ( $|0\rangle, |1\rangle$ ), elle envoie  $|1\rangle$  ;
- ③ Bob reçoit les photons, mais sans savoir dans quelle base ils doivent être interprétés, il choisit alors une base de manière aléatoire parmi les deux disponibles et effectue une mesure ;
- ④ Alice et Bob communiquent alors sur le canal classique, Bob va publier la liste des bases qu'il a utilisées pour chaque photon, et Alice lui indique quels photons il a correctement interprétés ;
- ⑤ Alice et Bob supprime les photons sur lesquels ils n'ont pas des bases identiques. Ils disposent alors d'une chaîne de bits identique de chaque côté qu'ils peuvent utiliser pour chiffrer un message .

# Exemple de BB84

Voyons un exemple d'échange dans le tableau suivant :

|               |             |                         |             |                         |                         |             |                         |             |
|---------------|-------------|-------------------------|-------------|-------------------------|-------------------------|-------------|-------------------------|-------------|
| Bits / Alice  | 0           | 1                       | 1           | 0                       | 1                       | 0           | 0                       | 1           |
| Bases / Alice | 01          | 01                      | +-          | 01                      | +-                      | +-          | +-                      | 01          |
| Photons émis  | $ 0\rangle$ | $ 1\rangle$             | $ -\rangle$ | $ 0\rangle$             | $ -\rangle$             | $ +\rangle$ | $ +\rangle$             | $ 1\rangle$ |
| Bases / Bob   | 01          | +-                      | +-          | +-                      | 01                      | +-          | 01                      | 01          |
| Mesures / Bob | $ 0\rangle$ | $ +\rangle /  -\rangle$ | $ -\rangle$ | $ +\rangle /  -\rangle$ | $ 0\rangle /  1\rangle$ | $ +\rangle$ | $ 0\rangle /  1\rangle$ | $ 1\rangle$ |
| Clef          | 0           |                         | 1           |                         |                         | 0           |                         | 1           |

## Attaque MIM sur BB84

Le protocole BB84 peut souffrir d'une attaque classique de type *Man In the Middle*. Eve s'interpose entre Alice et Bob, choisit une base au hasard et tente de faire une mesure.

On peut imaginer que Eve vient intercaler un filtre polariseur entre Alice et Bob. Les photons émis par Alice arriveront jusqu'à Bob, mais ils seront changés par la lecture effectuée par Eve.

|           |                         |                         |             |                         |                         |                         |                         |             |
|-----------|-------------------------|-------------------------|-------------|-------------------------|-------------------------|-------------------------|-------------------------|-------------|
| Bits/A    | 0                       | 1                       | 1           | 0                       | 1                       | 0                       | 0                       | 1           |
| Bases/A   | 01                      | 01                      | +-          | 01                      | +-                      | +-                      | +-                      | 01          |
| Photons   | $ 0\rangle$             | $ 1\rangle$             | $ -\rangle$ | $ 0\rangle$             | $ -\rangle$             | $ +\rangle$             | $ +\rangle$             | $ 1\rangle$ |
| Bases/E   | +-                      | 01                      | +-          | 01                      | +-                      | 01                      | 01                      | 01          |
| Après E   | $ -\rangle$             | $ 1\rangle$             | $ -\rangle$ | $ 0\rangle$             | $ -\rangle$             | $ 0\rangle /  1\rangle$ | $ 0\rangle /  1\rangle$ | $ 1\rangle$ |
| Bases / B | 01                      | +-                      | +-          | +-                      | 01                      | +-                      | 01                      | 01          |
| Mesures/B | $ 0\rangle /  1\rangle$ | $ +\rangle /  -\rangle$ | $ -\rangle$ | $ +\rangle /  -\rangle$ | $ 0\rangle /  1\rangle$ | $ +\rangle /  -\rangle$ | $ 0\rangle /  1\rangle$ | $ 1\rangle$ |
| Clef E    | 0                       |                         | 1           |                         |                         | 0                       |                         | 1           |
| Clef B    | 0 / 1                   |                         | 1           |                         |                         | 0 / 1                   |                         | 1           |

La clef correcte est 0101 mais du fait de la présence d'Eve, Bob peut voir une clef erronée comme 1101 ou 1111. Seuls les bits où Alice, Eve et Bob ont choisi les mêmes bases ne seront pas corrompus, les autres sont potentiellement faussés.

## Protection de BB84 contre une attaque MIM

Alice et Bob peuvent se protéger d'une attaque MIM en choisissant de sacrifier une partie de la clef négociée.

Par exemple, ils peuvent choisir de se communiquer sur le canal classique une moitié des clefs qu'ils ont bâties. S'ils observent des valeurs différentes, ils savent qu'il y a une corruption sur le canal quantique et jettent la clef produite.

Dans notre exemple, Alice et Bob choisissent de sacrifier 2 bits sur 4, Alice expose 01 et Bob expose 11 à cause d'Eve. Ils savent qu'il y a un problème et recommencent le processus.

Pour chaque bit où Alice et Bob ont choisi les mêmes bases, il y a 1 chance sur 4 pour Eve de passer inaperçu. Si  $n$  bits sont sacrifiés pour détecter une attaque MIM, la probabilité qu'Eve ne soit pas détectée est de  $\frac{1}{4^n}$  qui tend vers 0 quand  $n$  augmente.

## Le protocole B92

Le protocole B92 est une évolution de BB84 proposée par Charles Bennett, co-auteur de BB84, en 1992. Il est moins sensible au bruit sur le canal quantique.

On dispose de deux bases,  $(|0\rangle, |1\rangle)$  et  $(|+\rangle, |-\rangle)$ , mais on n'utilisera qu'un seul vecteur de chaque base. On encodera par exemple le bit 0 toujours via le qubit  $|0\rangle$  et le bit 1 via  $|+\rangle$ .

Le protocole est le suivant :

- ➊ pour chaque bit, Alice envoie un photon  $|0\rangle$  ou  $|+\rangle$  selon la valeur du bit ;
- ➋ pour chaque photon, Bob choisit une base aléatoirement, mais il oriente son détecteur perpendiculaire aux valeurs qu'il pense avoir été utilisées par Alice.
  - s'il choisit  $(|0\rangle, |1\rangle)$ , il cherchera à détecter  $|1\rangle$ ;
  - s'il choisit  $(|+\rangle, |-\rangle)$ , il cherchera à détecter  $|-\rangle$ ;
- ➌ si Bob s'est trompé de base, il croit avoir détecté un état superposé, et le détecteur va détecter 50% de l'état
- ➍ si Bob a choisi la bonne base, le détecteur ne voit rien.
- ➎ Bob indique à Alice sur quels tirs il a choisi la bonne base, Alice rejette les autres valeurs et les deux connaissent à présent la clef commune.

# Le protocole E91

Le protocole E91 a été créé par Artur Ekert en 1991. Ce protocole a été inspiré à son auteur par l'expérience de Alain Aspect en 1982. Il s'appuie sur une paire de photons intriqués.

On rappelle cette propriété de la paire EPR :

$$\frac{1}{\sqrt{2}}(|++\rangle + |--\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

En effet

$$|++\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |11\rangle + |01\rangle + |10\rangle)$$

$$|--\rangle = \frac{1}{2}(|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle + |11\rangle - |01\rangle - |10\rangle)$$

$$\frac{1}{\sqrt{2}}(|++\rangle + |--\rangle) = \frac{1}{2\sqrt{2}}(2|00\rangle + 2|11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

## Principe de E91

Le protocole E91 est fortement associé avec l'expérience CHSH, laquelle a été concrétisée par Alain Aspect en 1982.

Dans ce mécanisme, on suppose qu'on dispose d'une source capable de produire une paire EPR de photons intriqués  $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ , l'un des photons est expédié à Alice, l'autre à Bob.

Pour chaque photon, Alice va choisir aléatoirement une base  $(|0\rangle, |1\rangle)$  ou  $(|+\rangle, |-\rangle)$ . Ce faisant, on effondre l'état de la paire intriquée, ce qui change l'état des photons de Bob.

De son côté, Bob va choisir des bases de manière aléatoire et mesurer ses photons effondrés. Il publie ensuite ses bases à Alice, qui lui indique quels choix ont été corrects. Bob et Alice ne conservent que les bons choix pour construire une clef de chiffrement.

## Exemple de run de E91

|           |                            |             |             |             |             |             |             |             |
|-----------|----------------------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| Base A    | 01                         | 01          | +-          | 01          | +-          | +-          | +-          | 01          |
| Read A    | 01<br>50/50                | 01<br>50/50 | +-<br>50/50 | 01<br>50/50 | +-<br>50/50 | +-<br>50/50 | +-<br>50/50 | 01<br>50/50 |
| Bits A    | 01<br>50/50                | 01<br>50/50 | 01<br>50/50 | 01<br>50/50 | 01<br>50/50 | 01<br>50/50 | 01<br>50/50 | 01<br>50/50 |
| Base B    | 01                         | +-          | 01          | 01          | +-          | 01          | +-          | 01          |
| Read B    | 01<br>50/50<br>+-<br>50/50 | +-<br>50/50 | 01<br>50/50 | 01<br>50/50 | +-<br>50/50 | 01<br>50/50 | +-<br>50/50 | 01<br>50/50 |
| Bits B    | 01<br>50/50<br>01<br>50/50 | 01<br>50/50 | 01<br>50/50 | 01<br>50/50 | 01<br>50/50 | 1<br>50/50  | 01<br>50/50 | 01<br>50/50 |
| Read Same | 100%                       | 50%/50%     | 50%/50%     | 100%        | 100%        | 50%/50%     | 100%        | 100%        |
| Key       | 0 ou 1                     | -           | -           | 0 ou 1      | 0 ou 1      | -           | 0 ou 1      | 0 ou 1      |