Calcul quantique

Jean-Marc Alliot[1]

[1] IRIT

16 avril 2021

Contenu

Rappels et notations

Rappels

- Le conjugué de $x = a + ib$ est $\bar{x} = x^* = a - ib$
- Soit $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$
  - Conjugué : $A^* = \begin{pmatrix} a_{11}^* & a_{12}^* \\ a_{21}^* & a_{22}^* \end{pmatrix}$
  - Transposé : $A^T = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix}$
  - Adjoint : $A^\dagger = (A^T)^* = \begin{pmatrix} a_{11}^* & a_{21}^* \\ a_{12}^* & a_{22}^* \end{pmatrix}$
  - Commutateur : $[A, B] = AB - BA$
  - Anti-commutateur $\{A, B\} = AB + BA$
- Une matrice est hermitienne si $A^\dagger = A$
- Une matrice est unitaire si $UU^\dagger = I$
- Deux matrices sont diagonalisables dans la même base orthonormales si $[A, B] = 0$

Vecteurs et opérateurs

La formalisme matriciel de la mécanique utilise certaines notations spécifiques dues à Paul Dirac :

- Un vecteur représenté en colonne $\vec{u} = \begin{pmatrix} a \\ b \end{pmatrix}$ est noté $|u\rangle$.
- Un vecteur représenté en ligne $\vec{v} = \begin{pmatrix} c & d \end{pmatrix}$ est noté $\langle v|$.
- Le produit scalaire $\vec{v}.\vec{u}$ est noté $\langle v|u\rangle = ac + bd$
- L'application d'une matrice (opérateur) A au vecteur $\vec{u}$ est noté $A\,|u\rangle$
- Attention : si $|u\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$, alors $\langle u| = \begin{pmatrix} a^* & b^* \end{pmatrix}$

Produit dyadique et produit tensoriel

- Le produit dyadique de deux vecteur $|u\rangle$ et$|v\rangle$ est noté $|u\rangle\langle v| = \begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} c & d \end{pmatrix} = \begin{pmatrix} ac & ad \\ bc & bd \end{pmatrix}$.
- Le produit de Kronecker est $|u\rangle \otimes |v\rangle = |uv\rangle = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$
- Le produit de Kronecker de deux opérateurs $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ et $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ est $A \otimes B =$
$$\begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}$$

Postulats

Définition

Postulat 1

Pour tout système physique isolé il existe un espace de Hilbert que l'on nommera espace d'états du système. Le système est entièrement décrit par un vecteur d'état, qui est un vecteur unitaire de l'espace d'états.

Attention : la mécanique quantique ne nous dit pas, pour un système physique donné, quel est son espace d'états, ni quel est le vecteur d'état du système. Répondre à ces questions est un problème difficile, qui demande dans la plupart des cas le développement de théories complexes (l'électrodynamique quantique étudie par exemple comment les atomes et la lumière interagissent, et définit donc les espaces d'états décrivant ce type de système).

Exemples

- Le système le plus simple est celui du *qubit*. C'est à dire un système qui ne peut prendre que 2 états (comme le spin d'un électron), et est représenté par un espace deHilbert à 2 dimensions.
- Si $|0\rangle$ et $|1\rangle$ forment une base orthonormale de notre espace de Hilbert, alors un vecteur d'état représentant un qubit quelconque s'écrit : $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$
- On dit qu'une combinaison linéaire quelconque $\sum_i \alpha_i\,|\psi_i\rangle$ est une superposition des états $|\psi_i\rangle$ avec une amplitude α_i pour l'état $|\psi_i\rangle$.
- Rappel : les α_i sont des nombres complexes dans le cas général.

Définition

Postulat 2

L'évolution d'un système quantique fermé est décrit par une transformation unitaire. L'état $|\psi\rangle$ du système à l'instant t_1 est lié à l'instant du système $|\psi'\rangle$ à l'instant t_2 par un opérateur unitaire U qui ne dépend que de t_1 et de t_2 :

$$|\psi'\rangle = U(t1, t2)\,|\psi\rangle$$

Attention : la mécanique quantique ne nous dit pas non plus quels sont les opérateurs unitaires qui décrivent la dynamique de systèmes quantiques réels, elle nous garantit seulement que toute évolution est unitaire. Dans le cas des qubits, nous verrons que tout opérateur unitaire peut être réalisé en pratique.

Exemples

- La matrice $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ transforme $|0\rangle$ en $|1\rangle$ et $|1\rangle$ en $|0\rangle$. On l'appelle matrice *bit-flip*, ou matrice X de Pauli.
- La matrice $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ transforme $|0\rangle$ en $i\,|1\rangle$ et $|1\rangle$ en $-i\,|0\rangle$. C'est la matrice Y de Pauli.
- La matrice $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ laisse $|0\rangle$ inchangé et transforme $|1\rangle$ en $-|1\rangle$. On l'appelle matrice *phase flip*, ou matrice Z de Pauli.
- Les matrices de Pauli sont les observables du spin suivant $(\vec{x}, \vec{y}, \vec{z})$ pour les particules de spin $1/2$
- $|0\rangle$ et $|1\rangle$ sont les vecteurs propres de Z pour les valeurs propres 1 et -1. On les note aussi parfois $|u\rangle$ et $|d\rangle$ pour *up* et *down*.

Définition

Définition

Les mesures quantiques sont représentées par un ensemble $\{M_m\}$ d'opérateurs de mesure. Si l'état du système est $|\psi\rangle$ avant la mesure, la probabilité que le résultat soit m est :

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$$

et l'état du système après la mesure est :

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

On remarque que : $\forall |\psi\rangle$, $\sum p(m) = 1 = \sum \langle\psi| M_m^\dagger M_m |\psi\rangle$ donc

Equation de complétude

$\sum_m M_m^\dagger M_m = I$

Facteur global de phase

Facteur global de phase

Soit l'état $|\psi_1\rangle$ et
$|\psi_2\rangle = e^{i\theta}|\psi_1\rangle$ avec θ réel
$e^{i\theta}$ est appelé *facteur global de phase*, et les deux états sont totalement indiscernables en terme de mesure car pour tout opérateur de mesure M_m :

$$\langle\psi_2| M_m^\dagger M_m |\psi_2\rangle = \langle\psi_1| e^{-i\theta} M_m^\dagger M_m e^{i\theta} |\psi_1\rangle = \langle\psi_1| M_m^\dagger M_m |\psi_1\rangle$$

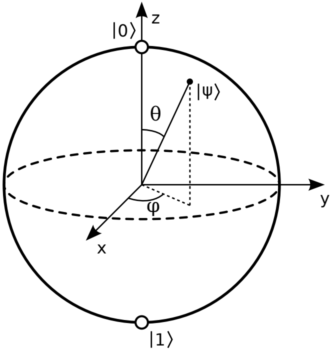
En pratique, les deux états ayant le même “comportement” pour tout opérateur de mesure, ils peuvent être considérés comme identiques.

Exemple

- Posons $M_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $M_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.
- M_0 et M_1 sont les opérateurs de mesure du qubit dans la base de calcul.
- Il est aisé de vérifier que $M_0^\dagger M_0 + M_1^\dagger M_1 = M_0^2 + M_1^2 = M_0 + M_1 = I$
- Si $|\psi\rangle = a|0\rangle + b|1\rangle$, la probabilité de mesurer l'état $|0\rangle$ est : $p(0) = \langle\psi| M_0^\dagger M_0 |\psi\rangle = |a|^2$
- L'état après la mesure de $|0\rangle$ est $\frac{M_0|\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle$ Cet état ne différant de $|0\rangle$ que par un facteur global de phase, l'état de mesure final est bien $|0\rangle$.

Sphère de Bloch

$$|\psi\rangle = a|0\rangle + b|1\rangle \text{ avec } |a|^2 + |b|^2 = 1$$
$$|\psi\rangle = \rho e^{i\alpha_1}|0\rangle + \sqrt{1-\rho^2}e^{i\alpha_2}|1\rangle$$
$$|\psi\rangle = \cos\frac{\theta}{2}e^{i\alpha_1}|0\rangle + \sin\frac{\theta}{2}e^{i\alpha_2}|1\rangle = e^{i\alpha_1}(\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i(\alpha_2-\alpha_1)}|1\rangle)$$
$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle$$



Etats parfaitement discernables par la mesure

Etats parfaitement discernables par la mesure

Soit n états $|\psi_i\rangle$. Alors il est possible de les discerner si et seulement si ils sont orthogonaux.

- Si les états sont orthogonaux, il suffit de construire des opérateurs de mesure $M_i = |\psi_i\rangle\langle\psi_i|$. On peut vérifier que cette famille vérifie les bonnes conditions qualifiant une famille de mesures, et le résultat d'une mesure par M_i sur un état $|\psi_j\rangle$ donnera δ_{ij} permettant ainsi de distinguer les états entre eux.
- Réciproquement, on voit bien que si les états ne sont pas orthogonaux, toute famille de mesure comportera une probabilité non nulle sur deux états non orthogonaux de donner des réponses non nulles.

Mesures projectives

- Une mesure projective est un observable M hermitien.
- Cet observable a une décomposition spectrale : $M = \sum_m mP_m$
- Les P_m sont les projecteurs sur les espaces propres de M associés aux valeurs propres m.
- $p(m) = \langle\psi| P_m |\psi\rangle$ et l'état devient $\frac{P_m|\psi\rangle}{\sqrt{p(m)}}$
- L'espérance de la mesure est $< M >= \sum_m m \langle\psi| P_m |\psi\rangle = \langle\psi| (\sum_m mP_m) |\psi\rangle = \langle\psi| M |\psi\rangle$
- L'écart type : $\Delta(M) = \sqrt{< (M- < M > I)^2 >} = \sqrt{< M^2 > - < M >^2}$

Définition

Espace d'états d'un système composite

L'espace d'états d'un système physique composite est le produit tensoriel des espaces d'états de chacun de ses composants. Si l'état de chaque système est $|\psi_i\rangle$ alors l'état du système complet sera $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$

On note souvent $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$ sous la forme $|\psi_1\rangle |\psi_2\rangle \cdots |\psi_n\rangle$ ou même $|\psi_1 \psi_2 \cdots \psi_n\rangle$

Quelques résultats

Equation de Schrödinger

Postulat 2'

L'évolution d'un système quantique fermé est décrit par l'équation de Schrödinger :

$$i\hbar \frac{d|\psi\rangle}{dt} = H\psi$$

H est un opérateur hermitien appelé Hamiltonien du système. Si H est connu, alors on est capable de décrire totalement l'évolution du système quantique dans le temps. En pratique, construire H est extrêmement difficile, sauf pour certains cas simples.

Etats stationnaires, état fondamental

H étant hermitien, il admet une décomposition spectrale :

Décomposition spectrale

$H = \sum_E E \left|E\right\rangle \left\langle E\right|$

Les vecteurs propres $\left|E\right\rangle$ sont appelés états stationnaires, et l'état ayant la plus petite valeur propre est l'état fondamental.
Les états stationnaires vérifient l'équation :

Etats stationnaires

$H : \left|E\right\rangle \rightarrow e^{-iEt/\hbar} \left|E\right\rangle$

Equivalence des formulations matricielle/équation de Shrodinger

- Si l'on résoud l'équation de Schrödinger, on obtient :

Solution de l'équation de Schrödinger

$|\psi(t_2)\rangle = e^{\frac{-iH(t_2-t_1)}{\hbar}} |\psi(t_1)\rangle = U(t1, t2) |\psi(t_1)\rangle$ avec
$U(t_1, t_2) = e^{\frac{-iH(t_2-t_1)}{\hbar}}$

- On voit donc qu'il y a équivalence entre les deux formulations du postulat 2.

Exemples

- En reprenant l'exemple de la transformation unitaire $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, on peut supposer que l'hamiltonien pour un qubit va s'écrire $H = \hbar\omega X$ où ω est un paramètre à déterminer expérimentalement.
- Les états stationnaires sont les vecteurs propres de X $(|0\rangle + |1\rangle)/\sqrt{2}$ et $(|0\rangle - |1\rangle)/\sqrt{2}$ avec des énergies associés valant $\hbar\omega$ et $-\hbar\omega$.
- L'état fondamental est donc $(|0\rangle - |1\rangle)/\sqrt{2}$

Relation d'incertitude d'Heinsenberg

- Soit A et B deux opérateurs hermitiens et $|\psi\rangle$ un état.
- $\langle\psi| AB |\psi\rangle = x + iy$, $\langle\psi| [A,B] |\psi\rangle = 2iy$, $\langle\psi| \{A,B\} |\psi\rangle = 2x$
- $| \langle\psi| [A,B] |\psi\rangle |^2 + | \langle\psi| \{A,B\} |\psi\rangle |^2 = 4 | \langle\psi| AB |\psi\rangle |^2$
- $| \langle\psi| [A,B] |\psi\rangle |^2 \leq 4 | \langle\psi| AB |\psi\rangle |^2$ et
- $| \langle\psi| AB |\psi\rangle |^2 \leq \langle\psi| A^2 |\psi\rangle \langle\psi| B^2 |\psi\rangle$ (Cauchy-Schwartz)
- $| \langle\psi| [A,B] |\psi\rangle |^2 \leq 4 \langle\psi| A^2 |\psi\rangle \langle\psi| B^2 |\psi\rangle$
- C et D observables, $A = C - < C > I$, $B = D - < D > I$
- Remarquons que : $[A,B] = [C,D]$

Relation d'incertitude d'Heisenberg

$$\frac{|\langle\psi|[C,D]|\psi\rangle|}{2} \leq \Delta(C)\Delta(D)$$

Interprétation et exemple

- Cette relation ne signifie pas que lorsque l'on mesure une quantité C avec une précision $\Delta(C)$, alors on perturbe la particule de telle façon que l'erreur sur la mesure de D sera supérieure à un $\Delta(D)$ permettant de satisfaire la relation d'Heisenberg.
- Elle indique simplement que si l'on prépare un ensemble de systèmes dans des états $|\psi\rangle$ identiques, et que l'on en mesure certains suivant C et d'autres suivant D alors $\Delta(C)\Delta(D) \geq \frac{|\langle\psi|[C,D]|\psi\rangle|}{2}$
- Considérons les matrices de Pauli X et Y, et l'état $|\psi\rangle = |0\rangle$, alors nous avons : $[X, Y] = 2iZ$ et $\Delta(X)\Delta(Y) \geq \frac{|\langle 0|(2iZ)|0\rangle|}{2} = 1$, donc $\Delta(X) > 0$ et $\Delta(Y) > 0$.
- En revanche si $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, alors $\langle\psi|2iZ|\psi\rangle = 0$, ce qui est normal car $\langle\psi|Y|\psi\rangle = 1$ et donc $\Delta(Y) = 0$ puisque $|\psi\rangle$ est ici un vecteur propre de Y et que la mesure du spin suivant Y retournera toujours 1.

Préliminaires

- L'observable spin est représenté par un vecteur $\vec{\sigma} = X\vec{x} + Y\vec{y} + Z\vec{z}$
- Les matrices de Pauli sont exprimés dans la base de vp de $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $|u\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|d\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $Z|u\rangle = |u\rangle$, $Z|d\rangle = -|d\rangle$,
- L'état EPR est $|\psi\rangle = \frac{|ud\rangle - |du\rangle}{\sqrt{2}}$
- Si Alice et Bob veulent mesurer le système suivant l'axe $\vec{z}$, l'observable est $Z \otimes Z$, noté ici ZZ et
  $ZZ|ud\rangle = |(Zu)(Zd)\rangle = -|ud\rangle$, $ZZ|du\rangle = |(Zd)(Zu)\rangle = -|du\rangle$,
  $ZZ|\psi\rangle = \frac{1}{\sqrt{2}}(ZZ|ud\rangle - ZZ|du\rangle) = \frac{1}{\sqrt{2}}(|du\rangle - |ud\rangle)$,
  $\langle\psi| ZZ |\psi\rangle = \frac{1}{2}(\langle ud| - \langle du|)(|du\rangle - |ud\rangle) =$
  $\frac{1}{2}(\langle ud|du\rangle - \langle ud|ud\rangle - \langle du|du\rangle + \langle du|ud\rangle) = \frac{1}{2}(0 - 1 - 1 + 0) = -1$

Version pour informaticien...

- $|\psi\rangle = \frac{1}{\sqrt{2}}(|ud\rangle - |du\rangle) = \frac{1}{\sqrt{2}}(|u\rangle \otimes |d\rangle - |d\rangle \otimes |u\rangle) =$
$$\frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} - \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix}\right) = \frac{1}{\sqrt{2}}\left(\begin{pmatrix}0\\1\\0\\0\end{pmatrix} - \begin{pmatrix}0\\0\\1\\0\end{pmatrix}\right) = \begin{pmatrix}0\\\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\\0\end{pmatrix}$$
- $Z \otimes Z = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix} = \begin{pmatrix}1 & 0 & 0 & 0\\0 & -1 & 0 & 0\\0 & 0 & -1 & 0\\0 & 0 & 0 & 1\end{pmatrix}$
- $\langle\psi|\, ZZ\, |\psi\rangle = \begin{pmatrix}0 & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} & 0\end{pmatrix} \begin{pmatrix}1 & 0 & 0 & 0\\0 & -1 & 0 & 0\\0 & 0 & -1 & 0\\0 & 0 & 0 & 1\end{pmatrix} \begin{pmatrix}0\\\frac{1}{\sqrt{2}}\\\frac{-1}{\sqrt{2}}\\0\end{pmatrix} = -1$

Mesure suivant deux axes différents...

- Alice et Bob mesurent maintenant le spin suivant deux vecteurs unitaires différents $\vec{a} = \begin{pmatrix} a_x \\ a_y \\ a_z \end{pmatrix}$ et $\vec{b} = \begin{pmatrix} b_x \\ b_y \\ b_z \end{pmatrix}$
- L'observable suivant $\vec{a}$ est : $\sigma_a = \vec{\sigma}.\vec{a} = a_x X + a_y Y + a_z Z$ et suivant $\vec{b}$: $\sigma_b = \vec{\sigma}.\vec{b} = b_x X + b_y Y + b_z Z$
- L'observable du système est : $\sigma_a \otimes \sigma_b = (a_x X + a_y Y + a_z Z) \otimes (b_x X + b_y Y + b_z Z)$
- On va calculer : $\langle\psi| (\sigma_a \otimes \sigma_b) |\psi\rangle$

Mesure suivant deux axes différents...

- $$\sigma_a = \vec{\sigma}.\vec{a} = a_x X + a_y Y + a_z Z = \begin{pmatrix} a_z & a_x - ia_y \\ a_x + ia_y & -a_z \end{pmatrix},$$
  $$\sigma_b = \vec{\sigma}.\vec{b} = b_x X + b_y Y + b_z Z = \begin{pmatrix} b_z & b_x - ib_y \\ b_x + ib_y & -b_z \end{pmatrix}$$
- $\sigma_a \otimes \sigma_b =$
  $$\begin{pmatrix} a_z b_z & a_z(b_x - ib_y) & (a_x - ia_y)b_z & (a_x - ia_y)(b_x - ib_y) \\ a_z(b_x + ib_y) & -a_z b_z & (a_x - ia_y)(b_x + ib_y) & -(a_x - ia_y)b_z \\ (a_x + ia_y)b_z & (a_x + ia_y)(b_x - ib_y) & -a_z b_z & -a_z(b_x - ib_y) \\ (a_x + ia_y)(b_x + ib_y) & -(a_x + ia_y)b_z & -a_z(b_x + ib_y) & a_z b_z \end{pmatrix}$$
- $\langle\psi| (\sigma_a \otimes \sigma_b) |\psi\rangle = -a_x b_x - a_y b_y - a_z b_z = -\vec{a}.\vec{b} = -\cos(\theta_{\widehat{ab}})$
- Si nous appelons $(sa_1, sa_2, \ldots, sa_n)$ les résultats des mesures de spin faites par Alice et $(sb_1, sb_2, \ldots, sb_n)$ ceux de Bob, nous mesurons la moyenne de $(sa_1 sb_1, sa_2 sb_2, \ldots, sa_n sb_n)$
- Rappelons que les (sa_i) et les (sb_i) ne peuvent prendre que les valeurs $+1$ ou -1
- Le calcul ci-dessus montre que le résultat ne dépend que de l'angle entre $\vec{a}$ et $\vec{b}$
- Notons enfin que la corrélation est stationnaire au voisinage des points extrémaux que sont $\vec{a} = \vec{b}$ et $\vec{a} = -\vec{b}$ puisque la dérivée du cosinus en 0 et π vaut 0.

Variables cachées

- Supposons maintenant que le résultat de la mesure d'Alice pour la particule 1 est une fonction $A(\vec{a}, \lambda)$. Pour Bob et la particule 2, le résultat de la mesure est la fonction $B(\vec{b}, \lambda)$
- A ne dépend pas de $\vec{b}$ et B ne dépend pas de $\vec{a}$
- λ représente un ensemble de valeurs, de lois, etc qui sont "cachées" à l'utilisateur mais qui déterminent avec l'angle $\vec{a}$, (resp. l'angle $\vec{b}$) le résultat de la mesure A (resp. la mesure B).
- A et B prennent les valeurs $+1$ ou -1, donc $A = \frac{1}{A}$ et $B = \frac{1}{B}$
- Si $\rho(\lambda)$ est la loi de probabilité de λ alors le résultat de la mesure de corrélation sera $P(\vec{a}, \vec{b}) = \int \rho(\lambda)A(\vec{a}, \lambda)B(\vec{b}, \lambda)d\lambda$
- Ce résultat doit être égal à celui de la MQ, c'est à dire $-\vec{a}.\vec{b}$
- Donc $P(\vec{a}, \vec{a}) = -1 = \int \rho(\lambda)A(\vec{a}, \lambda)B(\vec{a}, \lambda)d\lambda$ et comme $\int \rho(\lambda)d\lambda = 1$ et que A et B sont ≥ -1 cela impose que $B(\vec{a}, \lambda) = -A(\vec{a}, \lambda)$

Variables cachées

- $P(\vec{a},\vec{b}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)d\lambda$

Variables cachées

- $P(\vec{a}, \vec{b}) = -\int \rho(\lambda) A(\vec{a}, \lambda) A(\vec{b}, \lambda) d\lambda$
- $P(\vec{a}, \vec{b}) - P(\vec{a}, \vec{c}) = -\int \rho(\lambda)(A(\vec{a}, \lambda) A(\vec{b}, \lambda) - A(\vec{a}, \lambda) A(\vec{c}, \lambda)) d\lambda$

Variables cachées

- $P(\vec{a},\vec{b}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)d\lambda$
- $P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) = -\int \rho(\lambda)(A(\vec{a},\lambda)A(\vec{b},\lambda) - A(\vec{a},\lambda)A(\vec{c},\lambda))d\lambda$
- $P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)(1 - \frac{A(\vec{c},\lambda)}{A(\vec{b},\lambda)})d\lambda$

Variables cachées

- $P(\vec{a},\vec{b}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)d\lambda$
- $P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) = -\int \rho(\lambda)(A(\vec{a},\lambda)A(\vec{b},\lambda) - A(\vec{a},\lambda)A(\vec{c},\lambda))d\lambda$
- $P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)(1 - \frac{A(\vec{c},\lambda)}{A(\vec{b},\lambda)})d\lambda$
- $P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)(1 - A(\vec{c},\lambda)A(\vec{b},\lambda))d\lambda$

Variables cachées

- $P(\vec{a},\vec{b}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)d\lambda$
- $P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) = -\int \rho(\lambda)(A(\vec{a},\lambda)A(\vec{b},\lambda) - A(\vec{a},\lambda)A(\vec{c},\lambda))d\lambda$
- $P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)(1 - \frac{A(\vec{c},\lambda)}{A(\vec{b},\lambda)})d\lambda$
- $P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)(1 - A(\vec{c},\lambda)A(\vec{b},\lambda))d\lambda$
- Donc $|P(\vec{a},\vec{b}) - P(\vec{a},\vec{c})| \leq \int \rho(\lambda)(1 - A(\vec{c},\lambda)A(\vec{b},\lambda))d\lambda$

Variables cachées

- $P(\vec{a},\vec{b}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)d\lambda$
- $P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) = -\int \rho(\lambda)(A(\vec{a},\lambda)A(\vec{b},\lambda) - A(\vec{a},\lambda)A(\vec{c},\lambda))d\lambda$
- $P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)(1 - \frac{A(\vec{c},\lambda)}{A(\vec{b},\lambda)})d\lambda$
- $P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)(1 - A(\vec{c},\lambda)A(\vec{b},\lambda))d\lambda$
- Donc $|P(\vec{a},\vec{b}) - P(\vec{a},\vec{c})| \leq \int \rho(\lambda)(1 - A(\vec{c},\lambda)A(\vec{b},\lambda))d\lambda$
- $|P(\vec{a},\vec{b}) - P(\vec{a},\vec{c})| \leq 1 - \int \rho(\lambda)A(\vec{c},\lambda)A(\vec{b},\lambda)d\lambda$

Variables cachées

- $P(\vec{a},\vec{b}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)d\lambda$
- $P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) = -\int \rho(\lambda)(A(\vec{a},\lambda)A(\vec{b},\lambda) - A(\vec{a},\lambda)A(\vec{c},\lambda))d\lambda$
- $P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)(1 - \frac{A(\vec{c},\lambda)}{A(\vec{b},\lambda)})d\lambda$
- $P(\vec{a},\vec{b}) - P(\vec{a},\vec{c}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)(1 - A(\vec{c},\lambda)A(\vec{b},\lambda))d\lambda$
- Donc $|P(\vec{a},\vec{b}) - P(\vec{a},\vec{c})| \leq \int \rho(\lambda)(1 - A(\vec{c},\lambda)A(\vec{b},\lambda))d\lambda$
- $|P(\vec{a},\vec{b}) - P(\vec{a},\vec{c})| \leq 1 - \int \rho(\lambda)A(\vec{c},\lambda)A(\vec{b},\lambda)d\lambda$
- $|P(\vec{a},\vec{b}) - P(\vec{a},\vec{c})| \leq 1 + P(\vec{b},\vec{c})$

Variables cachées

- $|P(\vec{a},\vec{b}) - P(\vec{a},\vec{c})| \leq 1 + P(\vec{b},\vec{c})$
- Attention le calcul ci dessous est purement qualitatif, c'est une horreur mathématique
- $|P(a,b) - P(a,b+\epsilon)| \leq 1 + P(b,b+\epsilon)$
- $|\epsilon\frac{\partial P}{\partial y}(a,b) + o(\epsilon)| \leq 1 + P(b,b) + \epsilon\frac{\partial P}{\partial y}(b,b) + o(\epsilon)$
- $|\epsilon\frac{\partial P}{\partial y}(a,b) + o(\epsilon)| \leq \epsilon\frac{\partial P}{\partial y}(b,b) + o(\epsilon)$ car $P(b,b) = -1$
- $|\epsilon\frac{\partial P}{\partial y}(a,b) + o(\epsilon)| \leq o(\epsilon)$ car $P(a,b)$ est stationnaire pour $a = b$
- L'equation étant valable pour tout a et tout b, et la fonction étant symétrique, cela imposerait P constant, ce qui est impossible.

Circuits quantiques

Portes à deux bits

- Les portes de Pauli communes :
  - Porte *bit-flip*, ou *not* : $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

    $$\alpha|0\rangle + \beta|1\rangle \;—\boxed{X}—\; \beta|0\rangle + \alpha|1\rangle$$

  - Porte *phase flip* : $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

    $$\alpha|0\rangle + \beta|1\rangle \;—\boxed{Z}—\; \alpha|0\rangle - \beta|1\rangle$$

- Porte d'Hadamar :
  - $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

    $$\alpha|0\rangle + \beta|1\rangle \;—\boxed{H}—\; \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Autre portes à deux bits

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

$$\alpha|0\rangle + \beta|1\rangle \; -\boxed{Y}- \; -\beta i|0\rangle + \alpha i|1\rangle$$

- Porte Phase S : $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

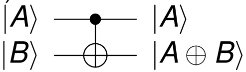
$$\alpha|0\rangle + \beta|1\rangle \; -\boxed{S}- \; \alpha|0\rangle + \beta i|1\rangle$$

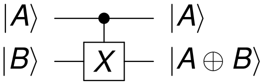
- Porte $\pi/8$ T : $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

$$\alpha|0\rangle + \beta|1\rangle \; -\boxed{S}- \; \alpha|0\rangle + \beta e^{i\pi/4}|1\rangle$$

La porte controlled-not (CNOT)

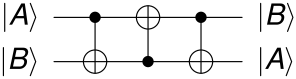
- $U_{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

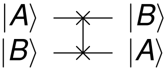
- 

- 

- $a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle \rightarrow$
  $a\,|00\rangle + b\,|01\rangle + d\,|10\rangle + c\,|11\rangle$

La porte Swap

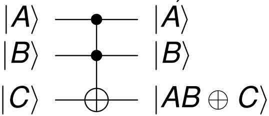
- $U_{Swap} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
- $|a, b\rangle \rightarrow |a, a \oplus b\rangle \rightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \rightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle$
- 

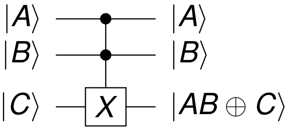
- 

- $a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle \rightarrow a\,|00\rangle + c\,|01\rangle + b\,|10\rangle + d\,|11\rangle$

La porte de Toffoli

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

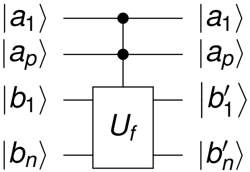
- 

- 

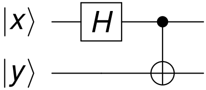
Porte contrôlée générale

Porte U_f contrôlée

Soit une porte U_f implantant une fonction f quelconque sur un nombre n de qubits. Il est possible de construire un circuit contrôlée par p bits tels que les bits $b_1 \cdots b_n$ sont inchangés si un des a_i est différent de 1, et égaux à la sortie de U_f si tous les a_i sont à 1.

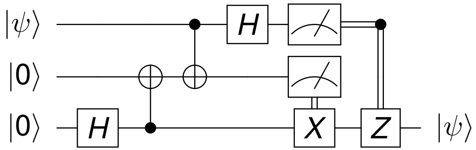


Construction d'états EPR

- 

In	Out
$\|00\rangle$	$\|\beta_{00}\rangle = (\|00\rangle + \|11\rangle)/\sqrt{2}$
$\|01\rangle$	$\|\beta_{01}\rangle = (\|01\rangle + \|10\rangle)/\sqrt{2}$
$\|10\rangle$	$\|\beta_{10}\rangle = (\|00\rangle - \|11\rangle)/\sqrt{2}$
$\|11\rangle$	$\|\beta_{11}\rangle = (\|01\rangle - \|10\rangle)/\sqrt{2}$

Téléportation quantique



- $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
- $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- $|\psi_0\rangle = |\psi\rangle\,|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|00\rangle + |11\rangle))$
- $|\psi_1\rangle = \frac{1}{\sqrt{2}}(\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle))$
- $|\psi_2\rangle = \frac{1}{2}(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)) = \frac{1}{2}(|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) + |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle))$

Porte CNOT et clonage

- $|\psi\rangle = a|0\rangle + b|1\rangle$
- Porte CNOT :
  - Input : $|\psi\rangle|0\rangle = (a|0\rangle + b|1\rangle)|0\rangle = a|00\rangle + b|10\rangle$
  - Output : $|\psi_2\rangle = a|00\rangle + b|11\rangle$
- Avons-nous cloné $|\psi\rangle$ et construit $|\psi\rangle|\psi\rangle$?
- $|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle$
- $|\psi\rangle|\psi\rangle \neq |\psi_2\rangle$ sauf si $a = 0$ ou $b = 0$

No cloning theorem

Théorème de non-clonage

Il est impossible de construire une machine quantique pouvant cloner un état quantique quelconque.

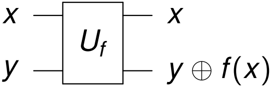
- Soit $|\psi\rangle$ l'état du slot de départ et $|s\rangle$ l'état du slot d'arrivée
- Supposons que $\exists U, \forall |\psi\rangle$, $U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$
- (1) $U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$ et (2) $U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle$
- Produit scalaire de (1) et (2) : $\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2$
- $\langle\psi|\phi\rangle = 1$ ou $\langle\psi|\phi\rangle = 0$
- $\psi = \phi$, ou ψ et ϕ sont orthogonaux.

Application à la cryptographie

Il est impossible de copier un “message” quantique avant de le retransmettre.

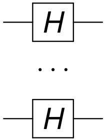
Algorithmes quantiques

Porte U_f



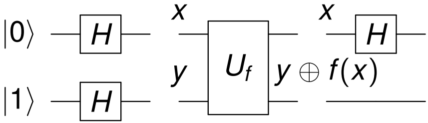
- $f : \{0, 1\} \to \{0, 1\}$
- Inputs : $x = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ et $y = |0\rangle$
- Output : $\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$
- $f(0)$ et $f(1)$ sont calculés en parallèle
- Généralisable à des fonctions à n bits grace à la transformation d'Hadamard-Walsh

Transformation d'Hadamard-Walsh



- n portes de Hadamard opérant en parallèle sur n qubits valant $|0\rangle$
- Pour $n = 2$, output : $\frac{|0\rangle+|1\rangle}{\sqrt{2}} \frac{|0\rangle+|1\rangle}{\sqrt{2}} = \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$
- On peut pour n bits générer avec seulement n portes de Hadamard et une porte U_f l'état $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$
- Attention : ici $|x\rangle$ contient n qubits.

Circuit de Deutsch

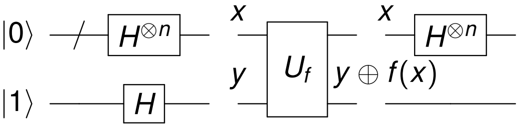


- $|\psi_0\rangle = |01\rangle$
- $|\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- $U_f(|x\rangle (|0\rangle - |1\rangle)/\sqrt{2}) = (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle)/\sqrt{2}$
- $|\psi_2\rangle = \pm \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ si $f(0) = f(1)$ et $\pm \frac{|0\rangle - |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ sinon
- $|\psi_3\rangle = \pm |0\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ si $f(0) = f(1)$ et $\pm |1\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ sinon
- $|\psi_3\rangle = \pm |f(0) \oplus f(1)\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- Le premier qubit vaut donc $f(0) \oplus f(1)$

Problème de Deutsch-Jozsa

- Alice à Amsterdam choisit $0 \leq x \leq 2^n - 1$ et l'envoie à Bob
- Bob a Boston calcule $f(x) = 0$ ou 1 et renvoie $f(x)$ à Alice
- f est équilibrée *ou* constante
- Combien faut-il qu'Alice envoie de lettres à Bob pour connaitre la nature de f ?
- Dans le cas classique, $\frac{2^n}{2} + 1$
- Peut-on faire mieux avec un ordinateur quantique ?

Circuit de Deutsch-Jozsa

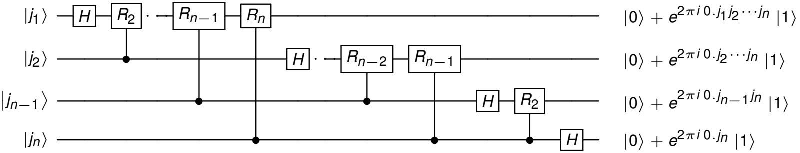


- $|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$
- $|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- $|\psi_2\rangle = \sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- Pour un qubit $|x_i\rangle$ on a : $H|x_i\rangle = \sum_{z \in \{0,1\}} \frac{(-1)^{x_i z}|z\rangle}{\sqrt{2}}$
- $H^{\otimes n}|x_1 x_2 \cdots x_n\rangle = \frac{\sum_{z_1, z_2 \cdots, z_n}(-1)^{(x_1 z_1 + \cdots + x_n z_n)}|z_1 \cdots z_n\rangle}{\sqrt{2^n}} = \frac{\sum_z (-1)^{(x.z)}|z\rangle}{\sqrt{2^n}}$
- $|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{(x.z + f(x))}|z\rangle}{2^n} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- Si f constant : amplitude$(|0\rangle^{\otimes n}) = \pm 1$,
  Si f équilibré : amplitude$(|0\rangle^{\otimes n}) = 0$

Transformée de Fourier

- $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{\frac{2\pi ijk}{N}}$
- $|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi ijk}{N}} |k\rangle$
- $\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} y_k |k\rangle$
- Posons
    - $N = 2^n$
    - $|j\rangle = |j_1 j_2 \cdots j_n\rangle$ avec $j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0$
    - $0.j_l j_{l+1} \cdots j_m = j_l/2 + j_{l+1}/4 + \cdots j_m/2^{m-l+1}$
- $|j_1, \cdots, j_n\rangle \rightarrow \frac{(|0\rangle + e^{2\pi i\, 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i\, 0.j_{n-1} j_n}|1\rangle) \cdots + (|0\rangle + e^{2\pi i\, 0.j_1 j_2 \cdots j_{n-1} j_n}|1\rangle)}{2^{n/2}}$

Circuit de la transformée de Fourier



- $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$
- $H|j_1\rangle \to \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i\, 0.j1}|1\rangle)|j2 \cdots j_n\rangle$
- $R_2 H|j_1\rangle \to \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i\, 0.j1j2}|1\rangle)|j2 \cdots j_n\rangle$
- ...

Complexité de la transformée de Fourier Quantique

Complexité de la transformée de Fourier Quantique

Un circuit quantique implante la transformée de Fourier en $O(n^2)$ opérations.

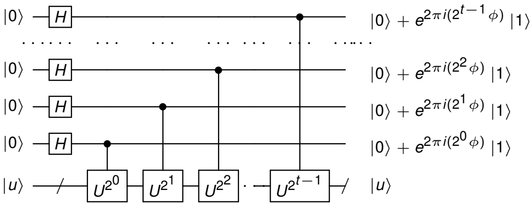
- Il faut $(1+(n-1))+(1+(n-2))+\cdots+1=\frac{n(n+1)}{2}$ portes
- Dans le cas classique il faut $O(n2^n)$ opérations.

Estimation de phase

Soit un opérateur unitaire U et un vecteur propre u de U, avec la valeur propre associée $e^{2\pi i\phi}$. Le but de l'algorithme d'estimation de phase est d'estimer la valeur de ϕ.

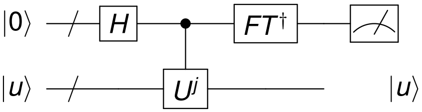
- Pour effectuer cette estimation on suppose que l'on dispose d'oracles capables de préparer l'état $|u\rangle$ et d'effectuer U^{2^j} opérations de contrôle.
- L'algorithme d'estimation de phase est plus un module qu'un véritable algorithme, puisqu'il repose sur 2^j boites noires devant effectuer les opérations appropriées.

Première étape du circuit d'estimation de phase



- $\phi = 0.\phi_1\phi_2\cdots\phi_t$
- $\frac{1}{2^{t/2}}(|0\rangle + e^{2\pi i\,0.\phi_t}|1\rangle)(|0\rangle + e^{2\pi i\,0.\phi_{t-1}\phi_t}|1\rangle)\cdots(|0\rangle + e^{2\pi i\,0.\phi_1\cdots\phi_{t-1}\phi_t}|1\rangle)$

Seconde étape du circuit d'estimation de phase



- La transformée de Fourier inverse fait : $\frac{1}{2^{t/2}} \sum_{j=0}^{2^t-1} e^{2\pi i \phi_j} |j\rangle |u\rangle \rightarrow \left|\tilde{\phi}\right\rangle |u\rangle$
- $\left|\tilde{\phi}\right\rangle$ est un estimateur de ϕ après mesure sur la base canonique du premier registre.

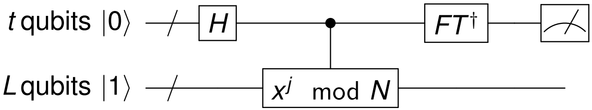
Ordre de l'élément d'un groupe

Ordre de l'élément d'un groupe

Soit un groupe multiplicatif fini $(G, .)$ et $x \in G$. On appele sous-groupe généré par x l'ensemble $G(x) = \{1, x, x^2, \cdots\}$. Le cardinal de $G(x)$ est appelé ordre de x.

- Si $G = Z/nZ$, alors l'ordre de x est le plus petit entier r tel que $x^r = 1\ [n]$

Circuit pour la recherche de l'ordre de x



- $U|y\rangle = |(xy)(\mod N)\rangle$
- $|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\pi isk}{r}} |x^k \mod N\rangle$
- $U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\pi isk}{r}} |x^{k+1} \mod N\rangle$
- $U|u_s\rangle = e^{\frac{2\pi is}{r}} \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\pi is(k+1)}{r}} |x^{k+1} \mod N\rangle$
- $U|u_s\rangle = e^{\frac{2\pi is}{r}} |u_s\rangle$
- $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = \frac{1}{r} \sum_{s=0}^{r-1} \sum_{k=0}^{r-1} e^{\frac{-2\pi isk}{r}} |x^k \mod N\rangle = |1\rangle$
- $L = \log_2(N)$, $t = 2L + 1 + \log_2(2 + \frac{1}{2\epsilon})$

Fraction continue

Fraction continue

Si s/r est un nombre rationel tel que $|\frac{s}{r} - \phi| \leq \frac{1}{2r^2}$ alors l'algorithme de fraction continue appliqué à ϕ convergera en $O(L^3)$ étapes.

- ϕ est une approximation de s/r avec $2L+1$ bits de précision, donc $|\frac{s}{r} - \phi| \leq 2^{-2L-1} \leq \frac{1}{2r^2}$ car $r \leq N \leq 2^L$

Quelques théorèmes utiles

Factorisation quadratique

Soit N un entier non premier, et x une solution non triviale de $x^2 \mod N = 1$. Alors $\gcd(x-1, N)$ ou $\gcd(x+1, N)$ est un facteur de N.

Soit $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$. Soit $1 \leq x \leq N-1$ un nombre choisi aléatoirement tel que $\gcd(x, N) = 1$. Si r est l'ordre de x alors $p((r \mod 2 = 0) \text{ et } (x^{r/2} \mod N \neq -1)) \geq 1 - \frac{1}{2^m}$

Factorisation

- Choisir un entier $2 \leq x \leq N-1$. Si $\gcd(x, N) \neq 1$, x est un diviseur de N
- Trouver l'ordre r de x
- Si r est pair et que $x^{r/2} \mod N \neq -1$ alors calculer $\gcd(x^{r/2}-1, N)$ et $\gcd(x^{r/2}+1, N)$, l'un des deux est un facteur de N
- Répéter si nécessaire.

Principe général

Principe général

En cryptographie, on utilise une fonction f pour encoder m, avec $c = f(m)$. Pour décoder c, on applique la fonction f^{-1}, avec $m = f^{-1}(c)$

Code César

Le code César consiste simplement à utiliser une bijection f de $\{a, b \cdots, z\}$ sur $\{a, b \cdots, z\}$.

Problème : ce type de code se casse aisément par analyse fréquentielle des lettres et des digrammes.

Algorithmes traditionnels

- Les algorithmes traditionnels repose sur l'utilisation d'une fonction $c = f(k, m)$ ou k est la clef et m le message à encrypter.
- La connaissance de f et de k permettent de reconstruire aisément m à partir de c.
- Ces algorithmes ont été manuels, puis electro-mécaniques (machine ENIGMA et ses dérivées) et aujourd'hui informatiques (DES, FEAL,...). Ils sont souvent basés sur des techniques de rotation de bits et d'additions modulaires.
- Bien choisis, ils sont sûrs et rapide à condition que la clef k reste secrète.

Algorithmes à clef publique

Algorithme à clef publique

Un algorithme à clef publique est un algorithme tel que la connaissance de la fonction f et de la clef de cryptage k ne permettent pas de reconstruire m à partir de c.

- Les fonctions f de ce type sont appelées *trapdoor functions*. L'idée est de trouver des fonctions dont l'inversion est très difficile dans le cas général.
- Le premier algorithme publié est celui de Merkle-Hellman (1978), mais l'algorithme était connu des organismes de cryptage britanniques et américains depuis les années 60.

Algorithme de Merkle-Hellman

- L'algorithme de Merkle-Hellman est basé sur le problème du sac à dos (*knapsack*).
- Soit un ensemble I d'entiers naturels x_i et un nombre n, trouver un sous-ensemble J de I tel que $\sum_{x_i \in J} x_i = n$.
- Ce problème est NP-complet dans le cas général
- Mais le problème est trivial si les x_i forment une suite super-croissante, c'est à dire qu'ils vérifient la propriété : $\forall i,\ x_i > \sum_{k=1}^{i-1} x_k$

Algorithme de Merkle-Hellman

- Choisir une séquence super-croissante $\{a_1, a_2, \cdots, a_n\}$ et un nombre N avec $N > a_1 + a_2 + \cdots + a_n$
- Choisir un nombre $A < N$ tel que $\gcd(A, N) = 1$
- Calculer les $b_i = (Aa_i) \mod N$
- La clef publique est l'ensemble des $b\{_i\}$
- La clef privée est $(N, \{a_i\})$
- Soit un message binaire composée de la suite de chiffre $d_1 d_2 \cdots d_n$, avec $d_i = 0$ ou $d_i = 1$. Alors, $c = \sum_{i=1}^{n} d_i b_i$
- Soit $m = A^{-1}c$, il suffit de résoudre le problème du sac à dos sur m avec les a_i.

Algorithme de Merkle-Hellman : exemple

- $\{a_1, a_2, \cdots, a_8\} = \{3, 7, 15, 31, 63, 151, 317, 673\}$.
- $N = 1511$ et $A = 643$.
- $\{b_1, b_2, \cdots, b_8\} = \{418, 1479, 579, 290, 1223, 389, 1357, 593\}$, $A^{-1} = 643^{-1} = 47[N]$.
- $m = 10011010$, $c = 418 + 290 + 1223 + 1357 = 3288$
- $f^{-1}(c) = 47 \times 3288\,[1511] = 414$
- $414 = 317 + 63 + 31 + 3$, donc $m = 10011010$

Algorithme RSA

Construction d'une clef

- Générer deux grands nombres premiers p et q et calculer $n = pq$ et $\phi = (p-1)(q-1)$
- Trouver un entier e tel que $1 < e < \phi$ et $\gcd(e, \phi) = 1$
- Calculer $d = e^{-1}$ $[\phi]$.
- La clef publique diffusée est (n, e) et la clef privée est d.

Cryptage par l'algorithme RSA

Soit $0 \leq m \leq n-1$, $c = m^e \mod n$.

Décryptage par l'algorithme RSA

$m = c^d \mod n$

Algorithme RSA : exemple

- $p = 313$ et $q = 547$, $n = pq = 171211$, $\phi = 170352$.
- $e = 83$ et $d = e^{-1} \mod n = 83^{-1}\,[171211] = 108779$.
- $m = 123456$, $c = m^e \mod n = 123456^{83}\,[171211] = 49619$
- $m = c^d \mod n = 49619^{108779}\,[171211] = 123456$