2022-08-30

Informatique quantique

Introduction

Logiciels

— quisquit
— ?

Infomatique quantique en trois ligne

— bits $(0, 1) \rightarrow |0\rangle\,|1\rangle$
— ?
— ?

Parallélisme quantique : n qbits $\implies$ 2^n états. On peut donc faire des calculs sur un superposition d'états très très grand. ex : 300 qbits :$200^{300} \gg$ nombre d'atome sur terre

Applications

Les ordinateurs quantique sont aussi vraiment utiles pour simuler des phénomènes qui sont fondamentalement quantique comme des simulation de molécules.

L'optimisation est fort puissante grace au parallélisme.

L'intelligence artificielle.

Communication Quantique

On peut envoyer de l'information quantique grace à des satellite.

Architectures

Il existe beaucoup de types d'ordinateurs quantique différents.

— les qbits supraconducteurs : les cicuit microondes sont très connus.
— les ions pièges
— les qbits de spins
— qbits topologiques
— qbits photoniques

On ne sait pas quel approche et la meilleur. Differentes companies et différents chercheurs ont différents approches. La plus utilisé et celle des qbits microondes.

Supprématie Quantique

Google a annocé quelque année avoir atteint la suprématie quantique (impossible à faire avec des ordinateurs quantique)

ils ont utilisé de l'ordre de 50 qbits. S'il auraient vraiment utilisé tout ces qbits au maximum de leur puissance ça aurait été le cas. Cependant leurs calculs était bruité et il été démontré que les calculs spécifique aurait thecniquement été possible sur des ordinateur classique bien que moyennant des coût très élévés. La véritable suprématie quantique n'est qu'une question de temps.

Motivations

Le but et d'éventuellement de réaliser des calculs difficiles et à grande échelle.

Communication quantique

La communications quantique est beaucoup plus facile à réaliser étant donné qu'on a pas besoin d'effecteur de calculs. Certaines companies offres déjà des services de ce type, notamment pour la distribution de clefs d'encryption

Les exigences contradictoire du calculs quantique

On veut connecter les différents qbits ensemble pour qu'il y ai de l'intrication/interaction mais les connecter mêne au bruit et la déchoérence.

La plupart des qbits sont bon pour une seule de ces deux chose : soit garder l'information mais par la partager, soit l'inverse.

Qbits supraconducteur

L'information est encodé en métant un pair de cooper d'un côté ou de l'autre.

Il faut ce qu'on appelle un élément non-linéaire pour interagir avec les qbits. Une JJ par exemple

Temps de vie des qbits

$$T_1 \text{Temps de relaxation}$$
$$T_2 : \frac{|0\rangle + |1\rangle}{\sqrt{2}} \to \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Sphère de Bloch

$$\langle\psi| \sigma_x |\psi\rangle = \sin\theta \cos\varphi$$
$$\langle\psi| \sigma_y |\psi\rangle = \sin\theta \sin\varphi$$
$$\langle\psi| \sigma_z |\psi\rangle = \cos\theta$$

$$X^2 = Y^2 = Z^2 = \mathbb{1}$$

$$XY = iZ$$

Exemple de Calcul de racine carrée

On peut prendre une racine en utilisant l'univers et la relation parbolique d'un crayon qui tombe (par exemple). C'est donc une utlisation physique de la mécanique classique pour faire des calculs.

Jeux classiques et quantiques

Les trois participants se font soit poser la question x ou y. Ils répondent par 1 ou -1. La multiplication des trois réponse doit donner -1.

Les trois participants doivent préparer un qbits dans GHZ

$$|GHZ\rangle = \frac{|000\rangle - |111\rangle}{\sqrt{2}}$$

quand on a la question X, on mesure σ_x, idem pour y

On a que
$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \quad |1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}$$

En exprimant les état $|000\rangle = |0\rangle|0\rangle|0\rangle$ et $|111\rangle = |1\rangle|1\rangle|1\rangle$ dans les base $\{|+\rangle, |-\rangle\}$ et faisant la multiplication au long, on trouve que $|GHZ\rangle = \frac{1}{2}(|++-\rangle + |+-+\rangle + |-++\rangle)$. Donc, dans tout les cas la mutiplication donne -1

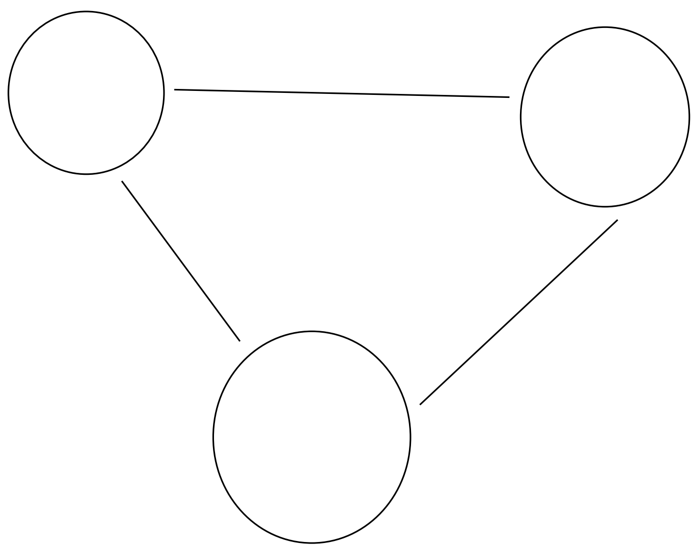


FIGURE 2 – situation

2022-09-06

1.2 Les États de Bells

Les états de Bell (aussi appelés états EPR) sont une base à deux qbits. Il représente les états intriquées.

$$\left.\begin{aligned} |\psi^{\pm}\rangle &= \tfrac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \\ |\Psi^{\pm}\rangle &= \tfrac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \end{aligned}\right\} \text{État propres de } X_A X_B \text{ et } Z_A Z_B$$

Rappel

$$|0\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle + |-\rangle\right) \quad |1\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle - |-\rangle\right)$$

(Ce sont donc des états propres de σ_z)

En effets, si je comprends bien $|0\rangle$ et $|1\rangle$ sont des états propres de σ_z et $|0\rangle = \sigma_x |1\rangle = \sigma_x^2 |0\rangle$, donc σ_x ne fait que changer le signe de $|\Psi\rangle$ et $|\Phi\rangle$

On peut qualifier les états de Bells par rapport à l'action de XX et ZZ

$ZZ\backslash XX$	$+1$	-1
$+1$	$\|\Psi^{+}\rangle$	$\|\Psi^{-}\rangle$
-1	$\|\Psi^{+}\rangle$	$\|\Psi^{-}\rangle$

Alice et Bob peuvent faire passer l'état d'un à l'aute en faisant un ou l'autre une mesure (transformation locale). Ex :

$$\left|\Phi^{+}\right\rangle = X_A I_B \left|\Psi^{+}\right\rangle = I_A X_B \left|\Psi^{+}\right\rangle$$

Les état de Bell, étant des états intriqués, ne peuvent pas s'écrire comme le produit tensoriel de deux états.

L'information contenue dans les états de Bell est contenue dans l'intrication et non dans l'état des qbits individuellement.

$$\left\langle\Phi^{+}\right| Z_a \left|\Phi^{+}\right\rangle = \left\langle\Phi^{-}\middle|\Phi^{-}\right\rangle = 0$$
$$\left\langle\Phi^{+}\right| X_a \left|\Phi^{+}\right\rangle = \left\langle\Phi^{-}\middle|\Psi^{+}\right\rangle = 0$$
$$\left\langle\Psi^{+}\right| Y_A \left|\Psi^{+}\right\rangle = 0$$

(les valeurs de X,Y et Z sont complètement aléatoires...)

On ne peut pas assigner d'état pur à l'état du qbit d'Alice (ou Bob). On a besoin d'une matrice densité (ρ)

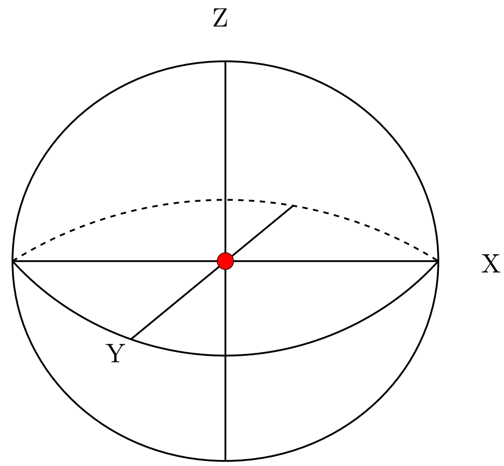


Figure 1 – Bell bloch boule

1.3 Encodage dense

A veut envoyer un message à B. Les deux sont liés par un canal quantique.

A envoie à B un qbit. Dans ce sénario, un seul bit peut être envoyé. A priori Bob ne connais pas la base dans lequel le qbit est encodé

Dans ce sénario on obtiens qu'un bit meme pas non ?

Peut-on faire mieux si on prend en compte de l'inrication ?

On suppose que Bob et Alice se partage un état de Bell ($|\Psi^+\rangle$). (Chacun un qbits)

Alice applique une transformation sur son qbits (qui est dans un état de bell). Si elle veut envoyer (00) , elle va appliquer $\mathbb{1}$ à $|\Psi^+\rangle$. Si elle veut envoyer (10) $X_A |\Psi^+\rangle$. (01) : $Z_a |\Psi^+\rangle$. (11) : $Z_A X_A |\Phi^+\rangle = |\Psi^-\rangle$ Alice envoie ensuite la moitié de sa paire à Bob.

Bob peut ensuite mesurer les qbits dans la base de la paire et obtenir 2 bits d'information.

L'information a le bonus d'être encrypté. Si on intercepte le 2eme qbits seulement, il ne gagne aucune information.

$$\boxed{e + q \geq 2c}$$

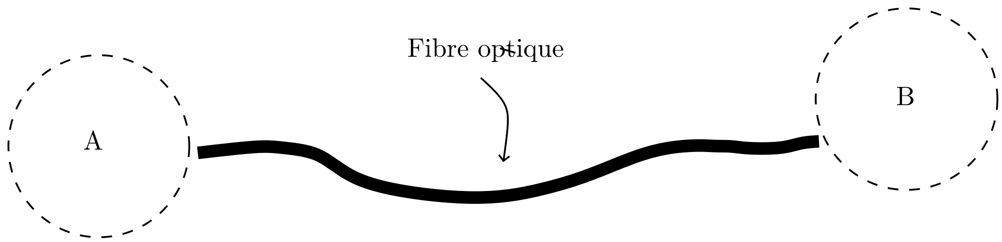


Figure 2 – canal quantique

1.4 Cryptographie Quantique (Elert "91, Bennet, Brassard '84)

Cryptographique classique : $\{0,1\}\mathbb{Z}_2$

$$\oplus : \text{addition} \quad \text{mod } 2 \qquad |\otimes| = 0 \qquad 2b = 0$$

One-time pad

Si A et B partagent une chaîne de bits aléatoires secrète (une clé $c \in \mathbb{Z}_2^n$), ils peuvent échanger un message indéchiffrable

A :

$\mathbf{c} = (c_1, c_2, \cdots, c_n) \otimes \mathbf{I} = (i_1, i_2, \cdots i_n) = \mathbf{m} = (m_1, m_2, \cdots m_n)$

B :

$\mathbf{m} = (m_1, m_2, \cdots m_n) \otimes \mathrm{c} = (\mathrm{c}_1, c_2, \cdots, c_n) = \mathbf{I} = (i_1, i_2, \cdots i_n)$

Sans connaître la clef, le message **m** est totalement aléatoire et ne contiens donc aucune information.

cryptographie quantique

Supposons que Alice et Bob partagent un grand nombre de $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Pour chaque paire, A et B mesurent aléatoirement X ou Z.

Il annoncent publiquement quel mesurent chacun a fait sur quel qbits mais pas le résultats qu'ils ont obtenus. Il gardent seulement les résultats des qbits pour lesquels ils ont fait la même mesure. Ils ont donc 100% de corrlélation pour les résultats qu'ils gardent (les autres (ces avec des mesures différents) n'aurait pas été corrélé du tout). Les résultats qu'ils obtiennent forment donc une clef puisque A et B ont tout deux exactement la même chose et sont les seuls à l'avoir.

Robustesse à une attaque de cette méthode

Ève aurait peu intéragir avec les états de Bell de sorte que les pairs soient aussi intriqué avec E. Elle aurait pu attendre l'annonce des mesures pour prendre les sienne et donc obtenir la clef aussi.

De manière générale

$$|\Gamma_{ABE}\rangle = |00\rangle_{AB} \otimes |e_{00}\rangle_E + |01\rangle_{AB} \otimes |e_{01e}\rangle + |10\rangle_{AB} \otimes |e_{10}\rangle + |11\rangle_{AB} \otimes |e_{11}\rangle_E$$

Supposons que A et B peuvent vérifier que $Z_A Z_B = 1$, i.e. les corrélations sont parfaites dans le cas ZZ.

$$\implies |\Gamma_{ABE}\rangle = |00\rangle \otimes |e_{01}\rangle + |11\rangle \otimes |e_{11}\rangle$$

idem pour XX

$$\implies |\Gamma_{ABE}\rangle = (|00\rangle + |11\rangle) \otimes |e\rangle$$

Si A et B sont un état propre de XX et ZZ, ils n'ont plus aucune intrication (corrélation) avec E

$$\implies \text{la clef est secrete}$$

Comment vérifier que les corrélations sont parfaites ?

On peu sacrifier une partie de la clef. Ils publient une partie de leur résultat et vérifie s'il ont une correlation parfaite.

Si elle l'est, la clef est sécuritaite, sinon les états on été traffiqués, il abandonnent.

Ils doivent décider de la portion à sacrifier après l'envoie afin que Eve n'evite pas sélectivement certaines paires.

Distribution de clé BB84

(résumé Ekart)

— A prépare un état $\{|0\rangle\}, |1\rangle, |+\rangle, |0\rangle$ et l'envoie à B.
— Pour chaque qubit, B choisit une base au hasard et mesure dans cette base.
— A et B publient les bases choisies.
— Les résultats aves les bases identiques constituent la clé

A mesure $Z \to |00\rangle$ ou $|11\rangle$ mesure $X \to |{+}{+}\rangle$ ou $|{-}{-}\rangle$

Chacun des ces cas est aléatoire avec 25%.

BB84 A prépare $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|11\rangle + |00\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$

A envoie a B cet état

A et B publient et comparent les choix de bases.<

Avantage Ekert

Basé sur intrication, test direct(inégalité de Bell). Pas besoin de faire confiance au système

Avantage BB84 : Pas besoin d'intrication donc plus facile à réalise.

Différence entre Ève et l'environement

Les deux sont très similaires. A vrai dire toute la discussion qu'on a eu jusqu'à maintenant est valide pour les deux.
Par conte l'environement est toujours présent.
Si les corrélation qu'on mesure sont fortes mais pas parfaites on peut faire de la correction d'erreur.

1.5 Théorème de non-clônage

Il est impossible de copier L,information quantique. (Utile de connaître cette contraite lorsqu'on pense aux algorithmes/protocols quantiques). Cette proprité découle directement de la linéarité en MQ.

On cherche une transformation unitaire U telle que

$$U|\psi\rangle|0\rangle = |\Psi\rangle|\Psi\rangle$$

$$\begin{aligned} U|00\rangle &= |00\rangle \\ U|10\rangle &= |11\rangle \end{aligned}$$

Appliquer U sur un état général

$$\begin{aligned} U|\psi\rangle|0\rangle &= u(\alpha|0\rangle + \beta|1\rangle)|0\rangle \\ &= \alpha|00\rangle + \beta|11\rangle \neq |\psi\rangle|\psi\rangle \end{aligned}$$

puisque

$$|\psi\rangle|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) = \alpha^2|00\rangle + \alpha\beta(|01\rangle + |10\rangle) + \beta^2|11\rangle$$

On peu copier un état connu d'avance

On peut aussi montrer cette proprité en utilisant le fait qu'une transformation uniraire préserve le recouvrement des fonction d'onde.

Prenons $|\psi\rangle, |\varphi\rangle$ et appliquons une transformation unitaire

$$|\psi'\rangle = V|\psi\rangle \quad |\varphi'\rangle = v|\varphi\rangle$$

$$\langle\psi|\varphi'\rangle = \langle\psi|V^\dagger V|\varphi\rangle = \langle\psi|\varphi\rangle$$

Maintenat une opération qui copie agirait comme $U\left|\psi 0\right\rangle = \left|\psi\psi\right\rangle \quad U\left|\varphi 0\right\rangle = \left|\varphi\varphi\right\rangle$

$$\left\langle\psi\psi|\varphi\varphi\right\rangle = \left\langle\psi|\varphi\right\rangle^2 \quad \left\langle\psi\psi|\varphi\varphi\right\rangle = \left\langle\psi 0\right| u^\dagger u \left|\varphi 0\right\rangle = \left\langle\psi|\varphi\right\rangle\left\langle 0|0\right\rangle = \left\langle psi|\varphi\right\rangle$$

En général $\left\langle\psi|\varphi\right\rangle^2 \neq \left\langle\psi|\varphi\right\rangle$

$$\implies U\text{n'existe pas}$$

1.6 Téléportation quantique

On peut utiliser des ressources quantique pour faire de la communication classique. La téléportation c'est l'inverse.

A veut envoyer un état $\left|\psi\right\rangle$ a B 1) Elle connaît l'état : transmet 2 nombres réels ($\geq 2c$) 2) Elle ne connaît pas l'état : Elle peut mesurer $\{\left|0\right\rangle, \left|1\right\rangle\}$ (ou dans tout autres base) et transmet le résultat de la mesure à B

$$\bar{F} = \left|\left\langle\psi_B\right|\psi_A\rangle\right|^2 = \frac{2}{3}$$

C'est mieux qu'un état aléatoire où $F = \frac{1}{\alpha}$

Protocole de téléportation quantique

Supossons que A et B partagent un état ψ^+

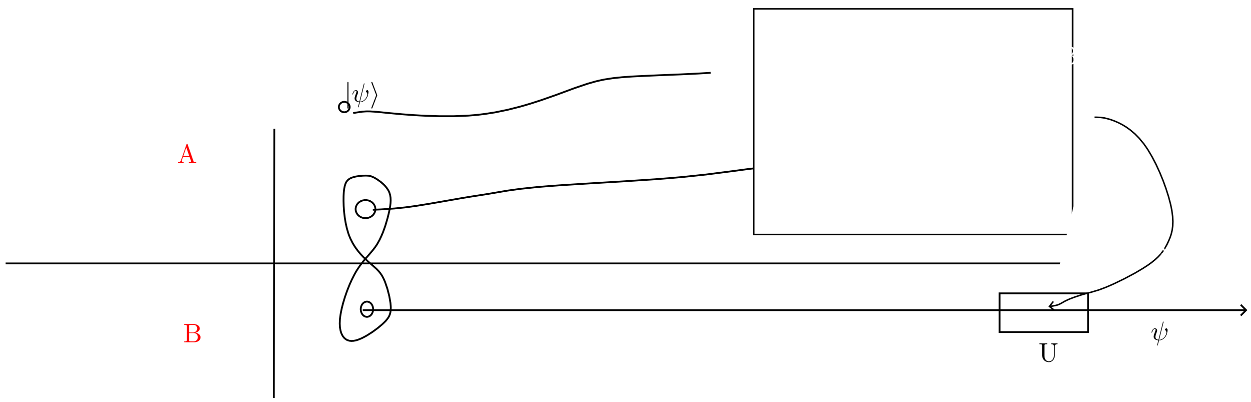


Figure 3 – Téléportation quantique

1.6 Téléportation quantique

A veut envoyer $|\psi\rangle$ à B

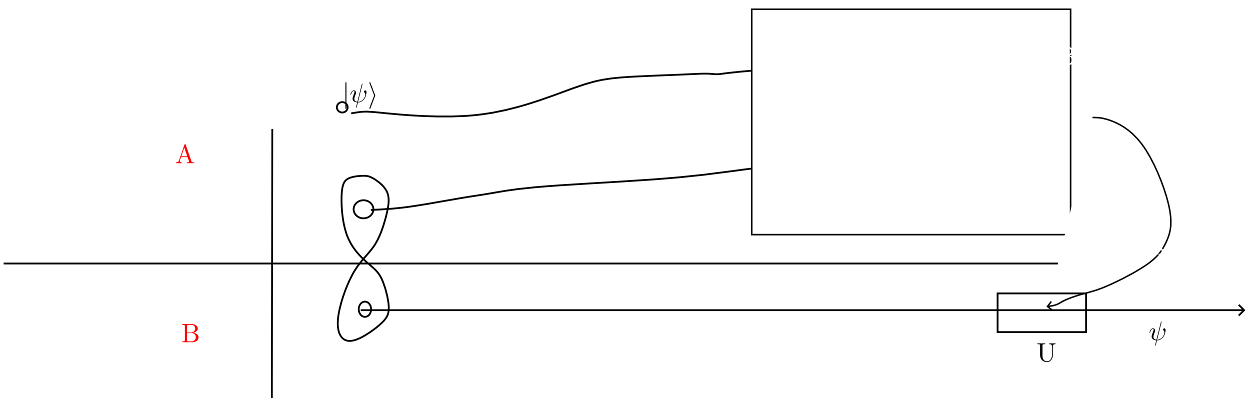


Figure 1 – Téléportation quantique 2

$$\begin{aligned}
|\Psi\rangle \otimes \left|\Phi^+\right\rangle &= (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{\sqrt{2}}\left[\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|100\rangle + \beta\,|111\rangle\right] \\
&= \frac{1}{2}\left[\alpha\left(\left|\Phi^+\right\rangle + \left|\Phi^-\right\rangle\right)|0\rangle + \alpha\left(\left|\Psi^+\right\rangle + \left|\Psi^-\right\rangle\right)|1\rangle + \beta\left(\left|\Psi^+\right\rangle - \left|\Psi^-\right\rangle\right)|0\rangle + \beta\left(\left|\Phi^+\right\rangle - \left|\Phi^-\right\rangle\right)|2\rangle\right] \\
&= \frac{1}{2}\left[\left|\Phi^-\right\rangle(\alpha\,|0\rangle + \beta\,|1\rangle) + \cdots\right] \\
&= \frac{1}{2}\left[\left|\Phi^+\right\rangle|\Psi\rangle + \left|\Phi^-\right\rangle Z\,|\Psi\rangle + |\Psi\rangle\, X\,|\Psi\rangle + \left|\Psi^-\right\rangle ZX\,|\Psi\rangle\right]
\end{aligned}$$

Alice mesure $\{|\psi^\pm\rangle, |\psi^\pm\rangle\}$ avec 25% chaque.

$$\left|\Psi^+\right\rangle : \mathbb{1} \quad \left|\Psi^-\right\rangle : \text{applique Z} \cdots$$

Aparté notation tensorielle

vecteur `-O-`
Matrice `-[]-`
état à deux qbits : `O==`

$$\Psi = \sum_{ij} c_{ij} |e_i\rangle \otimes |e_j\rangle$$

ket : `O-`
bra : `-O`

Produit tensoriel :
`O-`
$\otimes$
`O-`

Contraction : ($\langle\psi|\phi\rangle$)

`(\psi)--(\phi)`

Produit matrice-vecteur

`(\psi)--[u]-` $= u|\psi\rangle$

Matrice-Matrice

`-[A]-[B]-` $= BA =$ `-[BA]-`

Trace :

```
-----
|   |
L[M]J
```

2 Calcul Quantique

2.1 Calcul classique

ordinateur classique

$$\rho : \{0,1\}^n \to \{0,1\}^,$$

Portes universelles `NAND`

```
    ----
a---|   \
    |    )---- a NAND b
b---|___/
```

```
COPY:
      ______ a
     /
a---<
     \______ a


EX: NOT
            ----
      ______|   \
     /      |    \
a---<       |     )------- !a
     \______|    /
            |___/
```

`COPY` est impossible en quantique

Complexité

Difficulté de ρ : Nombre de portes universelle requisent pour le plus petit circuit réalisant ρ

Famille de Problème ou la taille varie

La circuit ne doit pas être adapté à la taille

P : Temps polynomial (facile)

$$|c_n| = n^\alpha$$

u

NP : Temps non-polynomial

NP-difficile : Au moins aussi difficile que le problème le plus dur de NP (Pas forcément dans NP)
NP-comlet : NP difficile **et** dans NP
clairement

$$P \subseteq NP$$

$$\boxed{\boxed{P =^? NP}}$$

2.2 Calcul quantique

Mécanique quantique : Opérateur d'évolution unitaire

$$U^\dagger U = \mathbb{1}$$

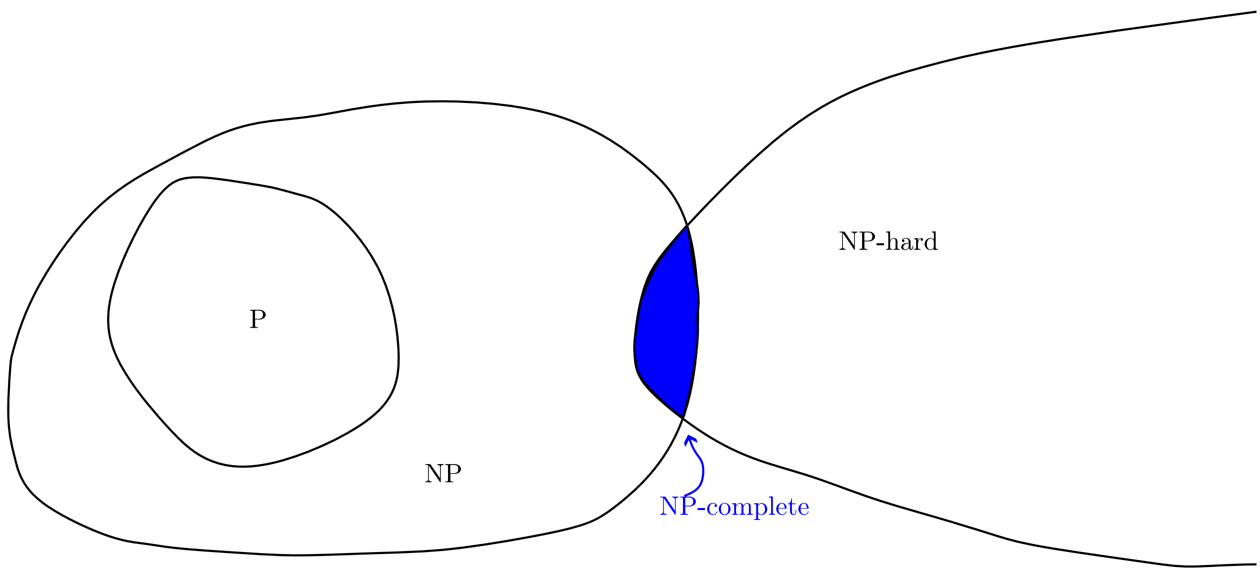


Figure 2 – La complexité

La porte `NAND` n'est pas réversible (2bits $\rightarrow$ 1bit)

Il existe des porte réversibles classiqus

Note

ON peut toujours exprimer une fonction

$$\rho : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2^m$$

sous la forme

$$g : \mathbb{Z}_2^{n+m} \mapsto \mathbb{Z}_2^{n+m}$$

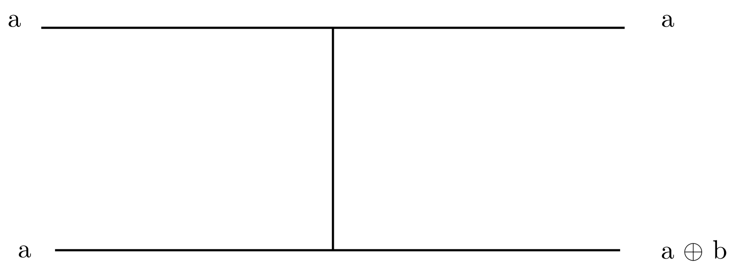
$$g(x, 0) \mapsto g(x, f(x))$$

2.3 Circuits Quantiques

a) état initial ($|0\rangle^{\otimes n}$) : Ce choix est arbitraire. Important de commencer dans un état non-intriqué

b) Transformation unitaire U : On décompose u en un ensemble de portes universelles agissant sur 1-3 qubits. Les U possibles ($U \in SU(2^n)$) forment un groupe continu. On peut générer U à partir d'un circuit fini C La complexité quantique est définie à partir de $|C|$

c) Mesure : Résultat non-détérministe On choisit de mesurer dans la base Z $\{|0\rangle, |1\rangle\}$ On peut mesurer différentes bases



CNOT

a b	CNOT
0 0	0 0
0 1	0 1
1 0	1 1
1 1	1 0

FIGURE 3 – CNOT

en chageant U. On évite de cacher la complexité dans la mesure. On aurait pu choisir de mesurer durant le circuit.

2.4 Complexité quantique

BQP (bounded-error quantum polynomial time) : Esemble des Problèmes faciles pour un ordinateur quantique (Problèmes tel que $|C| \leq n^{\infty}$)

L'ordinateur quantique doit donner la bonne réponse la plupart du temps ($\geq \frac{2}{3}$) (pas deterministe). On moyenne sur un grand nombre de calculs

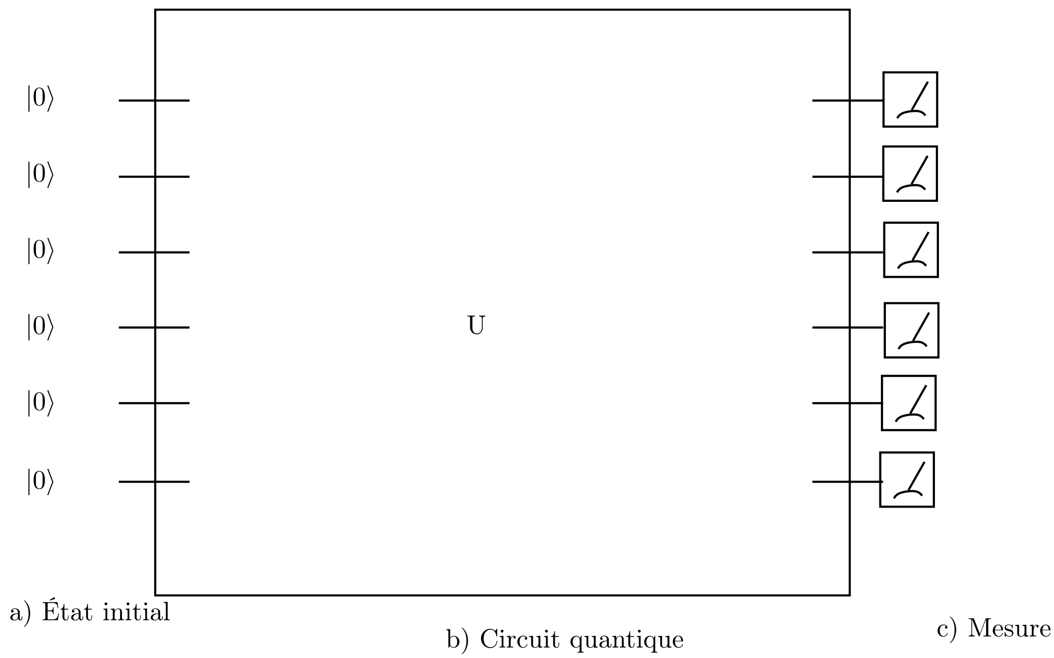


Figure 4 – Anatomie d'un circuit quantique

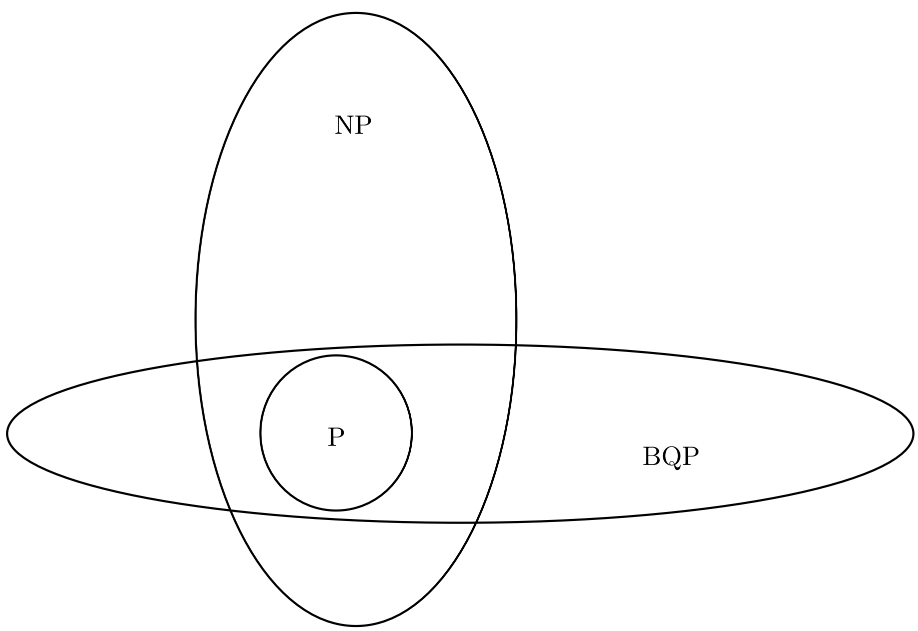


Figure 5 – Complexité quantique

Diagramme de complexité

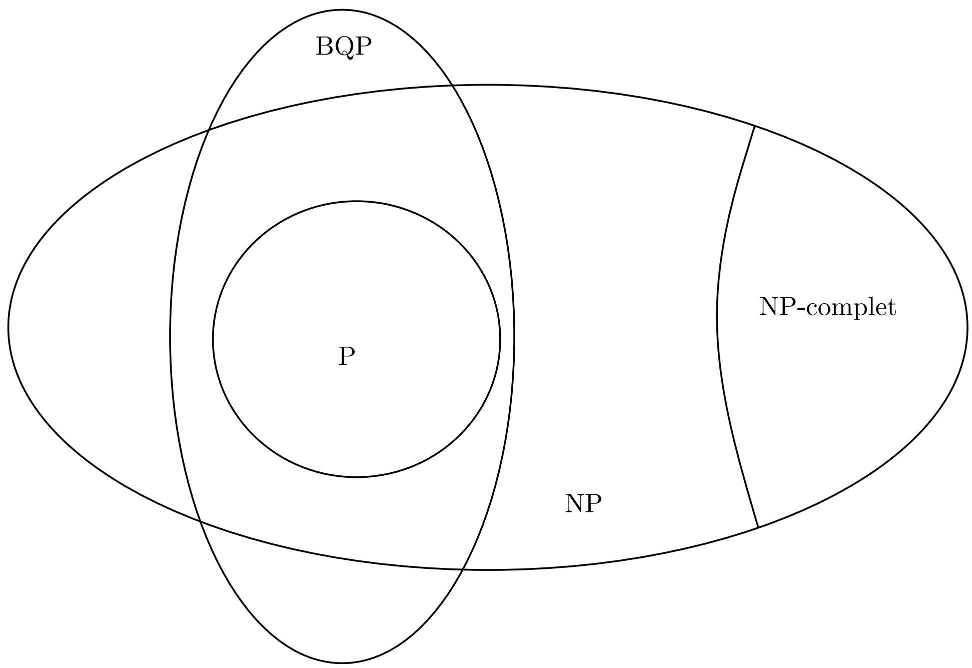


Figure 1 – diagramme de complexité

2.5 Portes logiques

2.5.1 Portes à 1 qubit

Les matrices de Paul forme une base pour décomposer n'importe quel matrice 2×2. $\mathcal{P} = \{\mathbb{1}, X, Y, Z\} = \{\sigma_0, \sigma_{1,2,3}\}$

$$\boxed{M_{2\times 2} = \sum_j m_j \sigma_j}$$

Démonstration de la complétude

Autre base :

$$B = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

$$B_1 = \frac{\mathbb{1} + Z}{2} \quad B_2 = \frac{\mathbb{1} - Z}{2} \quad B_3 = \frac{X + iY}{2} \quad B_4 = \frac{X - iY}{2}$$

Propriétés de $\mathcal{P}$

— Hermétique $\sigma^\dagger = \sigma$
— unitaire $\sigma^T = \sigma^{-1}$
— Base orthogonale $\mathrm{Tr}\left(\sigma_j^\dagger \sigma_k\right) = \delta_{ik}$

Les Matrices de Pauli génèrent des rotations sur la sphère de Bolch

$$R_x(\theta) = e^{\frac{-i\theta}{2}X} = \cos\left(\frac{\theta}{2}\right) - \sin\left(\frac{\theta}{2}\right)X$$
$$R_y(\theta) = e^{\frac{-i\theta}{2}Y} = \cdots$$
$$R_z(\theta) = e^{\frac{-i\theta}{2}Z} = \cdots$$

Plus généralement, on a une équivalence ente transformation unitaire (à un qubit) et rotation en 3D.

$$\mathrm{SU}(2) \longleftrightarrow \mathrm{SO}(3)$$

SU(2) : $\det(U) = 1$, $UU^\dagger = \mathbb{1}$, 2×2

SO(3) : $\det(O) = 1$, orthogonale, 3×3

En général, on a

$$U = e^{-i\frac{\theta}{2}\hat{n}\cdot\sigma}$$

$$U = \cos\left(\frac{\theta}{2}\right) - i\sin\left(\frac{\theta}{2}\right)\hat{n}\cdot\sigma$$

$$U = R_z(\alpha)R_x(\beta)R_z(\gamma)$$

3 opérations utiles

1. Porte d'Hadamard (H)

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

$$H\left|0\right\rangle = \left|+\right\rangle = \frac{\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}}$$

$$H\left|1\right\rangle = \left|-\right\rangle = \frac{\left|0\right\rangle - 1\left|1\right\rangle}{\sqrt{2}}$$

$$X \leftrightarrow Z \qquad Y \leftrightarrow -Y$$

2. Porte de Phase (S)

$$S = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix} = e^{-\frac{i}{2}\frac{\pi}{2}Z}$$

$$S\left|0\right\rangle = \left|0\right\rangle$$

$$S\left|1\right\rangle = i\left|1\right\rangle$$

$$S\left|+\right\rangle = \left|+i\right\rangle$$

$$S\left|+i\right\rangle = \left|-\right\rangle$$

$$S\left|-1\right\rangle = \left|-1\right\rangle$$

$$S\left|-i\right\rangle = \left|+\right\rangle$$

$$X \rightarrow Y \rightarrow -X \rightarrow -Y \rightarrow X$$

$$S^2 = Z$$

3. $\frac{pi}{8}$ (T)

$$T = \begin{pmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}}\end{pmatrix} = e^{-i\frac{\pi}{8}Z} = e^{-\frac{i}{2}\frac{\pi}{4}Z}$$

$$X \rightarrow \frac{X+Y}{\sqrt{2}} \rightarrow Y \rightarrow \frac{Y-X}{\sqrt{2}}$$

$$T^2 = S \approxeq \sqrt{Z}$$

Prendre la racine d'un opérateur est ambigu !

Aparté : on fait un état avec un circuit

$U\,|\psi\rangle = |\psi'\rangle$ `(|psi>)--[u] = (|psi'>)--`

On peut faire évoluer un opérateur

```
--[A]--[U]-- = --[U]--[U^t]--[A]--[U]--- = --[U]--[A]--
```

$$A' = UAU^\dagger$$

ex :

$$[Z]--[H]-- = --[H]--[HZH]--$$

$$\boxed{HZH = \cdots = X}$$

```
--[H]--[X]--$$
```

Un groupe de porte importantes est les portes de Clifford

$$\mathcal{P} = \{I, X, Y, Z\}$$

$$C = \{U | UPU^\dagger \in \mathcal{P}, P \in \mathcal{P}\}$$

ex :

$$H, S \in C \quad T \notin C$$

2.5.2 Portes à 2 qubits

Il faut de l'intrication pour réaliser des calculs interessant pour

$$U \in \mathrm{SU}(4)$$

```
    _______
----|      |-----
    |   U  |
----|______|-----
```

On utilisera souvents des opérateurs controllant

$$CU\,|ij\rangle = |i\rangle \otimes u^i\,|j\rangle$$

```
----.-----
    |
---[u]----
```

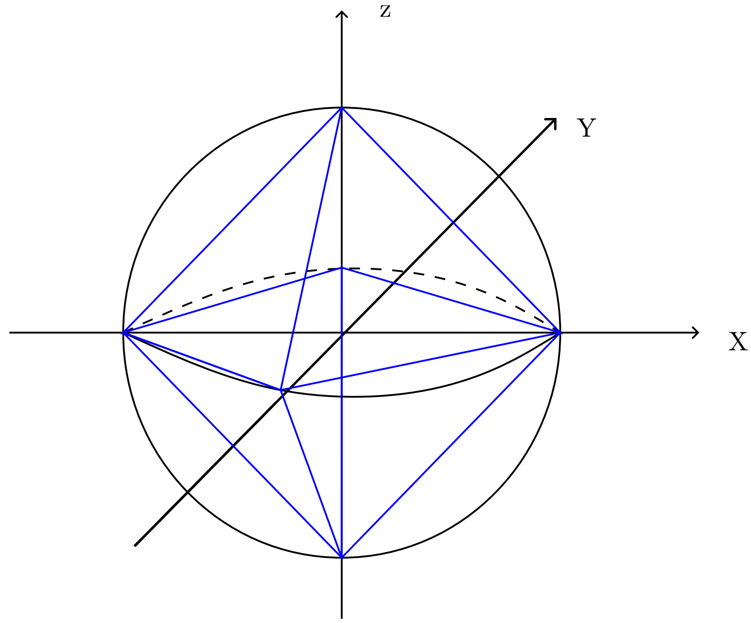


FIGURE 2 – octaèdre

Ex : CNOT (non contrôlé) CX

```
----.-----
    |
---(+)----
```

$$\text{CNOT}\,|ij\rangle = |i\rangle\, X\,|j\rangle = |i, j\otimes i\rangle$$

$$\text{CNOT} = |0\rangle\langle 0|\otimes \mathbb{1} + |1\rangle\langle 1|\otimes X$$
$$\text{CNOT} = \left(\frac{\mathbb{1}+Z}{2}\right)\otimes\mathbb{1} + \left(\frac{\mathbb{1}+z}{2}\right)\otimes X = \frac{1}{2}\left(H + Z1 + 1X - ZX\right)$$

CNOT est hermétique et unitaire !

$$\text{CNOT} = \text{CNOT}^\dagger \qquad \text{CNOT}^T = \qquad \Longrightarrow \text{CNOT}^2 = \mathbb{1}$$

$$\text{CNOT}^2\,|ij\rangle = |i, j\oplus 2i\rangle = |ij\rangle$$

$$\text{CNOT}(Z\mathbb{1})\text{CNOT} = ZI$$

$$\mathrm{CNOT}(\mathbb{1}X)\mathrm{CNOT} = \mathbb{1}X$$

$$\mathrm{CNOT}(X\mathbb{1})\mathrm{CNOT} = XX$$

<u>Porte contrôle phase</u> (CZ)

```
----.-----    ---[Z]----    ----.----
    |      =      |      =      |
---[Z]----    ----.-----    ----.----
```

$$CZ\,|ij\rangle = |1\rangle\, Z\,|j\rangle = (-1)^{ij}\,|ij\rangle$$

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

En calcul quantique, le qubit "contrôle" est aussi affecté par la porte CU

<u>Phase kick-back</u> Revenons à la porte CNOT.

```
|psi>----.----|psi>
         |
| + >----.----| + >
```

```
|psi>----.----(|0><0|-|1><1|) |psi>
         |
| + >----.----| - >
```

2.6 Universalité

Calcul Classique $\{\text{NAND}, \text{COPY}\}$

Calcul classique réversible $\{\text{Toffoli}\}$

Calcul quantique : plusieurs choix possibles

1. Matrice générique $4x4$ ($M \in \text{SU}(4)$) <u>Ex</u> $\text{CR}_x(\theta)$ $\frac{\theta}{\pi}$ irrationnel

```
----.----
    |
-[Rx(z)]-
```

2. SU(2)+CNOT 2 générateurs de rotations sont suffisant pour générer SU(2) CNOT permet de générer de l'enchevêtrement. Ce n'est pas la seul pour qui permet de faire cela et d'autre porte aurait fait le travail (Cz par exemple)
   Cz :

```
----.----   ----o----
    |     =     |
--[(+)]--   ----o----
```

3. Un ensemble discret de porte peut être universel : ex : $\{\text{H}, \text{S}, \text{T}, \text{CNOT}\}$
   Ces portes sont importantes dans la théorie du calcul tolérant au faute.
   $T^2 = S$, on pourrait donc enlever S de l'ensemble. Par contre faire des portes T est vraiment difficile donc en pratique on aime remplacer T^2 par S

   $\{\text{H}, \text{S}, \text{CNOT}\}$ n'est pas universel mais génère le groupe Clifford à plusieurs qubits. v

   Gotesman-Krill 98

   Le calcul quantique avec seulement les portes Clifford peut-être simulé classiquement. L'intrication est nécessaire mais pas suffisant pour avoir un avantage quantique. <u>Preuve Sketch</u> :
   Suivre l'évolution des opérateurs de Pauli à travers le circuit.

2.7 L'algorithme de Deustch

Soit une fonction classique $f : \mathbb{Z} \mapsto \mathbb{Z}$.On cherche à savoir si f est balancée ou constante.

$$\begin{array}{ccc} f \text{ balancé } f(0) \neq f(1) & f(0) = 0, f(1) = 1 \quad \text{ou} \quad f(0) = 1, f(1) = 0 \\ f \text{ constante } f(0) = f(1) & f(0) = 0, f(1) = 0 \quad \text{ou} \quad f(0) = 1, f(1) = 1 \end{array}$$

Calcul classique, il fait évaluer f deux fois et comparer calcul quantique. On peut évaluer qu'une seule fois ...

Puisque f n'est pas forcément réversible car utilise un registre.

$U_f \left|xy\right\rangle \equiv \left|x, y \oplus f(x)\right\rangle$

Ex : f constant $f(0) = f(1) = 1$

$$U_f \left|10\right\rangle = \left|1, 0 \oplus 1\right\rangle = \left|11\right\rangle$$

$$U_f^2 |xy\rangle = |x, y \oplus 2f(x)\rangle = |xy\rangle$$

$$\implies U_f^2 = \mathbb{1}$$

$$U_f = U_f^\dagger = U_f^{-1}$$

Ce circuit quantique est

```
|0>----[H]----|----|----[H]----[Mes]
              |    |
              | U_f|
              |    |
|0>--[X]--[H]-|----|--------[Poubelle]
```

$$|\psi_0\rangle = |00\rangle$$
$$|\psi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = |+-\rangle$$

Appliquons U_f sur $|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$

$$U_f \left(\frac{|X0\rangle - |X1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}} \left(|X, f(x)\rangle - |x, 1 \oplus f(x)\rangle\right)$$

Si $f(x) = 0$ ou 1, l'état final est le même à un signe près

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

...

Préparation d'un état de Bell

```
|0>----[H]----.----
              |    |Phi+>
|0>----------(x)---
```

$$|\Psi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |0\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |10\rangle\right)$$

$$|\psi_2\rangle = \text{CNOT} |\psi_1\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right)$$

```
|0>----[H]----.----
              |    |Psi+>
|1>----------(x)---
```

(Démarche similaire pour le démontrer)

```
|0>----[H]-,--.---,--
 !         !  |   !
|0>--------!-(x)--!--
 !         !      !
 !         !      !
 !         !      !
 Z         X      X
 I         I      X
 --------------------
 I         I      Z
 Z         Z      Z
```

$|00\rangle$ étant propre de ZI et IZ

SWAP gate

```
----x----   ----o---(+)---o----
    |     =     |    |    |
----x----   ---(x)---o---(x)---
```

$$|\psi_0\rangle = |ij\rangle$$

$$|\psi_1\rangle = |i, j \oplus i\rangle$$

$$|\psi_2\rangle = |i \oplus j \oplus i, j \oplus i\rangle = |2i \oplus j, j \oplus i\rangle = |j, j \oplus i\rangle$$

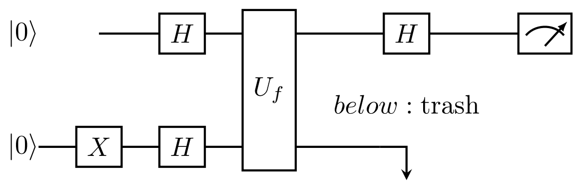
$$|\psi_3\rangle = |j, j \oplus i \oplus j\rangle = |ji\rangle = \text{SWAP}\,|ij\rangle$$

Notation binaire

On écrit le nombre binaire en décimale.

2022-09-20

Deustch



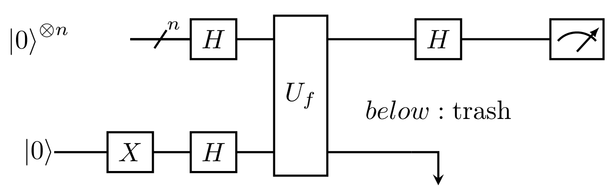
2.8 Problème de Deutsh-Jozsa

On cherche à trouver si

$$f : \mathbb{Z}_2^n \mapsto \mathbb{Z}_2$$

est balancé (la moitié des résultats est 1 et l'autre 0) ou constant (toujours 0 ou 1). On sait que f est un ou l'autre.

Classiquement, on doit calculer f $2^{n/2}+1$ fois (au pire)



> On appelle U_f un oracle en informatique quantique

$$|\psi_0\rangle = |0\rangle^{\otimes n+1}$$

$$|\psi_1\rangle = |+\rangle^{\otimes n} |-\rangle = \frac{1}{\sqrt{2}^n} \sum_{x=0}^{2^n-1} |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$x = \sum_{k=1}^{n} x_k 2^{n-k}$$

On applique maintenant U_f. On a un *phase kick-back*

$$|\psi_2\rangle = U_f |\psi_1\rangle = \sum_x \frac{(-1)^{f(x)}}{2^{n/2}} |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

L'infromation sur $f(x)$ est conteny dans la phase des n premiers qubits. On applique les Hadamard $H^{\otimes n}$ pour faire *tomber* les phases vers des probabilité

$n = 1$:

$$H\left|x\right\rangle = \begin{cases} \frac{\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}} & \text{si } x = 0 \\ \frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}} & \text{si } x = 1 \end{cases} = \sum_{z=0}^{1} \frac{(-1)^{XZ}}{\sqrt{2^n}} \left|z\right\rangle$$

On généralise à $n1$

$$H^{\otimes n}\left|x_1\, x_2\, \cdots\, x_n\right\rangle = \bigotimes_{j=1}^{n} \frac{1}{\sqrt{2}} \sum_{z_j=0}^{1} (-1)^{x_j z_j} \left|z_j\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{z_1,\cdots,z_n=0}^{1} (-1)^{x_1 z_1 + \cdots} \left|z_1\, \cdots\, z_n\right\rangle = \frac{1}{\sqrt{2}^n} \sum_{z=0}^{2^n-1} (-1)^(x \cdot z) \left|z\right\rangle$$

Donc

$$\left|\psi_3\right\rangle = H^{\otimes n} \otimes 1 \left|\psi_2\right\rangle = \sum_{x} \frac{(-1)^{f(x)}}{2^{n/2}} H^{\otimes}$$

Transformation de Fourrier Quantique

DFT

$$\mathbb{C}^n \to \mathbb{C}^n$$

$$\mathbf{x} \to \mathbf{y}$$

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{\frac{2\pi ijk}{N}}$$

QFT :

$$\mathrm{QFT}\,|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi ijk}{N}}\,|k\rangle$$

L'action sur un état arbitraire est donc

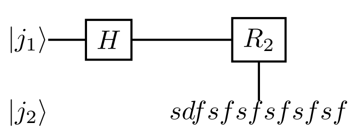
$$\mathrm{QFT}\,|\psi\rangle = \mathrm{QFT}\left(\sum_{j=0}^{N_1} x_j\,|j\rangle\right) = \sum_{k=0}^{N-1} y_k\,|k\rangle$$

avec $\mathbf{y}$ la DFT des $\mathbf{y}$ donné plus haut

On va utiliser $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i2\pi/2^n} \end{pmatrix}$

Ex :

$$Z = R_1 \qquad S = R_2 \qquad T = R_3$$



2022-09-27

2.11 Estimation de phase (QPE)

UNe tranformation unitaire U, n'est pas nécessairement hérimitique. U n'est donc pas un observable (en générale). On peut toujours écrire U avec un observable A comme

$$U = e^{2\pi i A} = \sum_{\lambda=1}^{N} e^{2\pi i \varphi_\lambda} |\lambda\rangle\langle\lambda|$$

Si on suppose qu'on peut préparer un état $|\lambda\rangle$ et qu'un oracle puisse évaluer U. On veut estimer φ_λ

Pour se faire, on sépare le circuit en 2 registres

1. Un registre de t qubits $|0\rangle$
   plus t est grand et plus l'algorithme est précis et plus le succès est probable
2. l'état $|\lambda\rangle$

2.12 Algorithme de Shor

On veut, à partir de $a \in \mathbb{N}$, trouver $a_1, a_2 \in \mathbb{N} | a = a_1 \cdot a_2$

On combine la QFT et la QPW pour résoudre ce problème avec un ordinateur quantique

Classiquement, le meilleur algorithme connu à ce jour (number field sieve) à une complexité de $\exp\left\{O(n^{1/3} \log^{2/3} n)\right\}$
Quantiquement, en revanche, la complexité est de $O(n^2 \log n \log(\log n))$. Il y a donc un avantage exponentiel.

Le record de factorization classique est un nombre de 795 bits ! L'avantage quantique devra donc attendre pour des ordinateur quantique beaucoup plus performant que ceux qui existent actuellement.

L'algorithme de factorisation est basé sur le problème de la recherche d'ordre. On commence donc par cet aspect.

Rappel de notions d'arithmétique

On travaille ici avec seulement des entiers positifis ($\in \mathbb{N}^*$). Avec 2 nombres x et n, il existe une manière unique d'écrire

$$x = kn + r$$

où r est le reste ($x \mod n = r$) et $0 \leq r \leq n-1$.

- On dit que a divise b (a|b), si $b = ca$ avec $c \in \mathbb{N}$
- Le plus grand commun diviseur entre 2 nombres $(a,\, b)$, noté pgcd(a, b), est sup$(c|(c|a)(\wedge c|b))$
- Si gcd$(a, b) = 1$, on dit que a et b sont co-premiers
- On peut trouver le gcd entre 2 nombres grace à l'algorithme d'Euclide
- Si $ab = cN$, N est composite et $a, b \neq dN$ alors soit gcd(a, N) ou gcd(b, N) est un facteur not-trivial de N

2.12.1 recherche d'ordre

Soit x, n des entiers positifs tel que $x < N$ est n'ayant aucun facteur commun. L' ordre de $x \mod n$ est le plus petit entier positif r tel que

$$x^r \mod N = 1$$

On veut déterminer r à partir de x et N (Un problème difficile classiquement)

ex : ordre de (4,7) : 3

En général, $x^{r+1} \mod N = x$ ou pour $t = ar + b$

$$x^t \mod N = x^b \mod N$$

Ce problème se résout à l'aide de l'algorithme QPE !

$$U_x \left|y\right\rangle = \left|xy \mod N\right\rangle$$

ave $y \in \mathbb{Z}_2^L$ où L est le nombre de bits nécéssaire pour représenter N ($L = \lceil \log_2 N \rceil$)

Il est important que (x,N) soit co premiers, sinon U_x n'est pas unitaire !

Pour $N \leq y \leq 2^L - 1$ on prend la convention que $xy \mod N = y$
U_x agit non-triviallemnt seulement sur $0 \leq y \leq N-1$

On peut toujours écrire $U_x = \exp\{2\pi i A_x\}$ où

$$A_x = \begin{pmatrix} A_x & 0 \\ 0 & \mathbb{1}_{2^2-N} \end{pmatrix}$$

Si on applique U_x sur l'état suivant

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\pi i s k}{r}} \left| x^k \mod N \right\rangle$$

On a

$$U_x |u_s\rangle = \cdots = e^{2\pi i s/r} |u - x\rangle$$

$\implies |u_s\rangle$ est un état propre de U_x avec valeur propre $e^{2<piis/r}$

Pour préparer $|u_s\rangle$, Il faut connaître r (et donc la réponse). Il faut donc utiliser une astuce

$$\begin{aligned}
\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle &= \frac{1}{r} \sum_{sk} e^{-2\pi i s k} r \left| x^k \mod N \right\rangle \\
&= \sum_k \left(\frac{1}{r} \sum_s e^{-2\pi i s k/r} \right) \left| x^k \mod N \right\rangle \\
&= \sum_k \delta_{k,0} \left| x^k \mod N \right\rangle \\
&= |1\rangle
\end{aligned}$$

On peut donc initialiser l'algorithme de phase avec $|1\rangle$, ce qui est simple.

Avec l'algorithme QPE, on obtiens un estimé de $\varphi \approx \frac{s}{r}$ avec un s aléatoire

Il reste à extraire r de $\varphi \approx \frac{s}{r}$

On peut faire cela avec la méthode de l'expension de fraction continues.