

Calcul quantique basé sur la mesure

Léo Gagnon et Julien Codsi

March 16, 2021

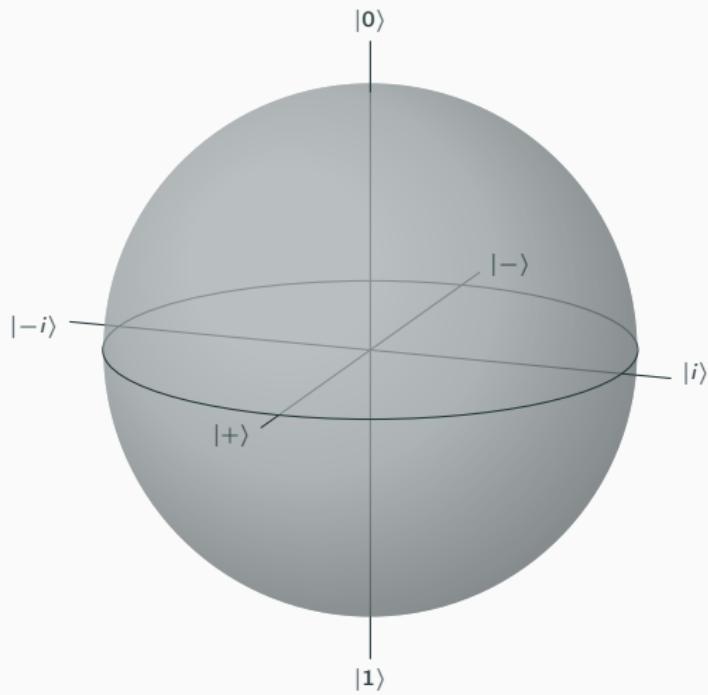
Université de Montréal

Structure de la présentation

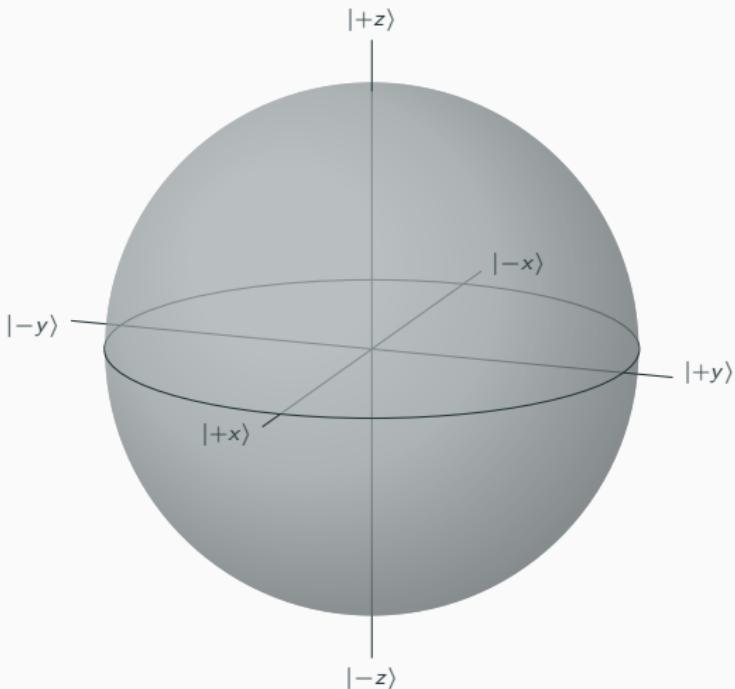
- 1 : Préliminaires et idée générale
- 2 : Définitions et notation
- 3 : Démonstration du fonctionnement
- 4 : Équivalence avec les circuits quantiques
- 5 : Applications : Calcul quantique aveugle et parallélisation.

Préliminaire : Sphère de Bloch

Représentation de l'état d'un qubit



Représentation de l'état d'un qubit



Remarques :

- $R_x(180) = X = N$
- $R_x(90) = S = \sqrt{N}$
- $R_z(180) = Z = P$
- $R_z(\theta)X = XR_z(-\theta)$
- $R_x(\theta)Z = ZR_x(-\theta)$

Calculer en mesurant

Qu'est-ce qu'un modèle de calcul?

Nouveau modèle

Circuits quantique

- États séparables comme ressource
- Séquence d'application de portes entre plusieurs qubits
- Résultat : l'état final des qubits

Circuits quantique

- États séparables comme ressource
- Séquence d'application de portes entre plusieurs qubits
- Résultat : l'état final des qubits

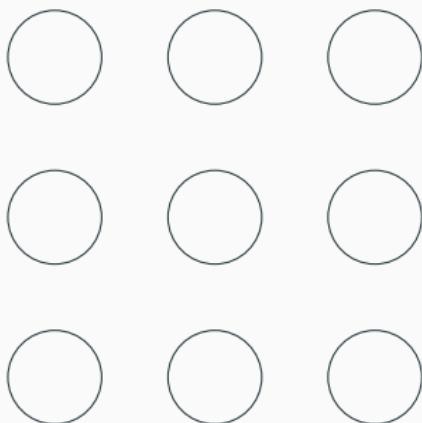
Nouveau modèle

- Ensemble d'états intriqués comme ressource
- Séquence de mesures en base particulières d'un sous-ensemble de l'état de base
- Résultat : les qubits non-mesuré.

Définitions et notation

Ressource : Graphe d'état

Graphe d'états :



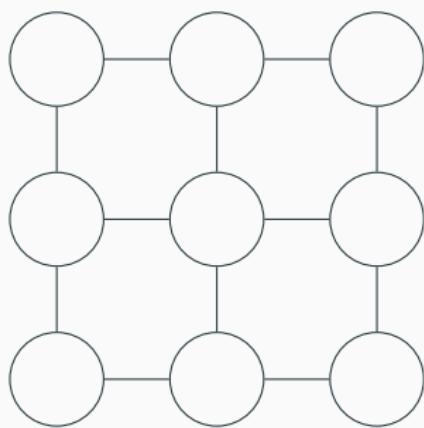
Éléments :

- Qubit en état $|+\rangle$:



Ressource : Graphe d'état

Graphe d'états :



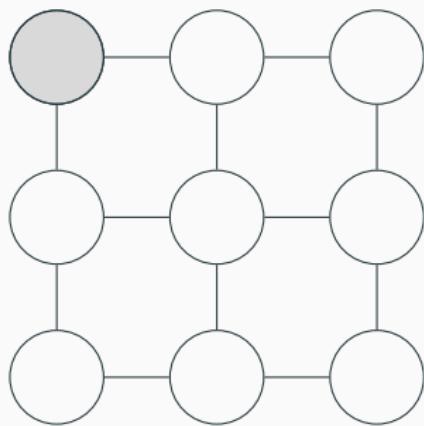
Éléments :

- Qubit en état $|+\rangle$:
- Ctrl-Z :



Ressource : Graphe d'état

Graphe d'états :



Éléments :

- Qubit en état $|+\rangle$:



- Ctrl-Z :

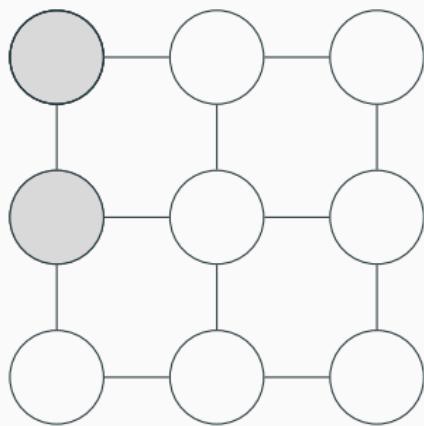


- Qubit en état $|\psi\rangle$:



Ressource : Graphe d'état

Graphe d'états :



Éléments :

- Qubit en état $|+\rangle$:



- Ctrl-Z :

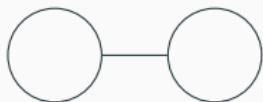


- Qubit en état $|\psi\rangle$:



Ressource : Graphe d'état

Graphe d'états :

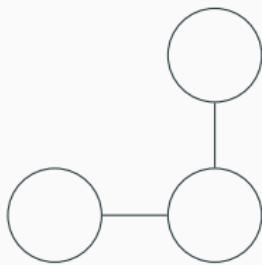


Circuit équivalent :



Ressource : Graphe d'état

Graphe d'états :

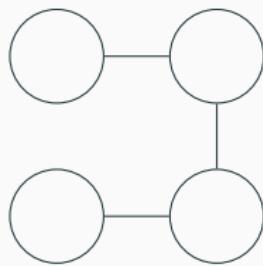


Circuit équivalent :



Ressource : Graphe d'état

Graphe d'états :

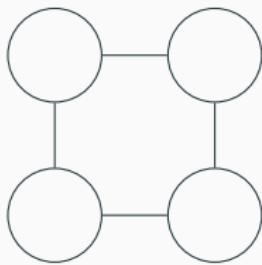


Circuit équivalent :

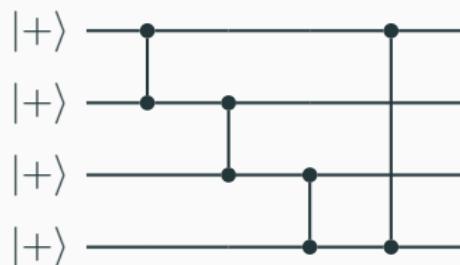


Ressource : Graphe d'état

Graphe d'états :

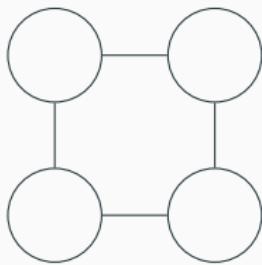


Circuit équivalent :

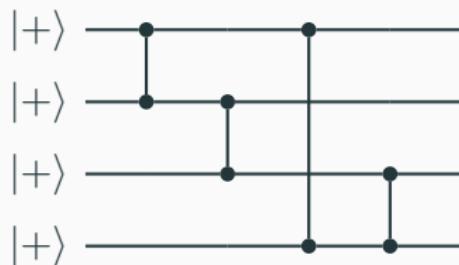


Ressource : Graphe d'état

Graphe d'états :



Circuit équivalent :



Ressource : Graphe d'état

Graphe d'états :



Remarques :

- Le graphe de 2 qubits donne l'état $\frac{1}{\sqrt{2}} |0+\rangle + \frac{1}{\sqrt{2}} |1-\rangle$

Ressource : Graphe d'état

Graphe d'états :

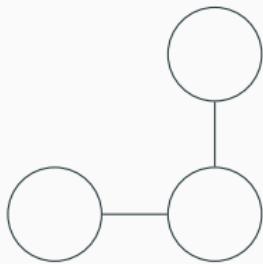


Remarques :

- Le graphe de 2 qubits donne l'état $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle^*$

Ressource : Graphe d'état

Graphe d'états :

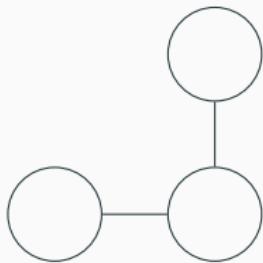


Remarques :

- Le graphe de 2 qubits donne l'état $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle^*$
- Le graphe de 3×3 donne l'état $\frac{1}{\sqrt{2}} |+0+\rangle + \frac{1}{\sqrt{2}} |-1-\rangle$

Ressource : Graphe d'état

Graphe d'états :

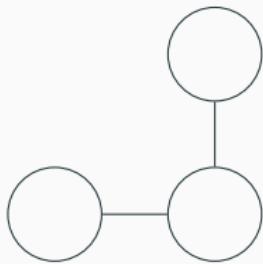


Remarques :

- Le graphe de 2 qubits donne l'état $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle^*$
- Le graphe de 3×3 donne l'état $\frac{1}{\sqrt{2}} |000\rangle + \frac{1}{\sqrt{2}} |111\rangle^*$

Ressource : Graphe d'état

Graphe d'états :



Remarques :

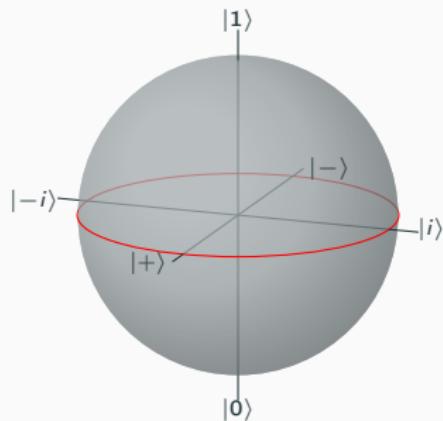
- Le graphe de 2 qubits donne l'état $\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle^*$
- Le graphe de 3×3 donne l'état $\frac{1}{\sqrt{2}} |000\rangle + \frac{1}{\sqrt{2}} |111\rangle^*$
- En général, les graphes de cette sorte sont très intriqués.

Méthode de calcul : Pattern de mesure

Théorème

Dans le calcul quantique basé sur la mesure, on peut se limiter aux bases de mesures suivantes :

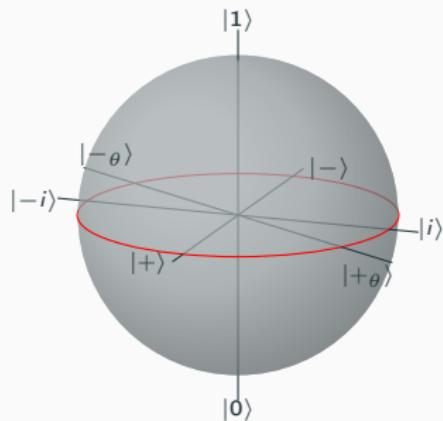
$$\mathcal{B}(\theta) = \left\{ \frac{|0\rangle + e^{i\theta}|1\rangle}{\sqrt{2}}, \frac{|0\rangle - e^{i\theta}|1\rangle}{\sqrt{2}} \right\}.$$



Méthode de calcul : Pattern de mesure

Théorème

Dans le calcul quantique basé sur la mesure, on peut se limiter aux bases de mesures suivantes :
 $\mathcal{B}(\theta) = \{|+\theta\rangle, |-\theta\rangle\}$.



Méthode de calcul : Pattern de mesure

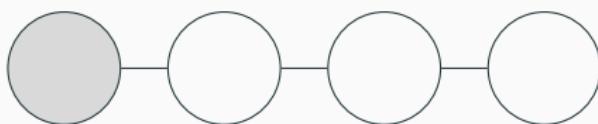
Définition :

Un pattern de mesure est une liste de règles spécifiant l'ordre des mesures à effectuer ainsi que la base. La base d'une mesure peut dépendre du résultat d'une mesure précédante.

Méthode de calcul : Pattern de mesure

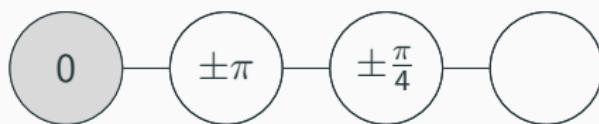
- $\mathcal{B}(\theta) = \{|+\theta\rangle, |-\theta\rangle\}$

Notation :



Méthode de calcul : Pattern de mesure

Notation :



- $\mathcal{B}(\theta) = \{|+\theta\rangle, |-\theta\rangle\}$

- Mesure en base $\mathcal{B}(\theta)$:



Méthode de calcul : Pattern de mesure

Notation :



- $\mathcal{B}(\theta) = \{|+\theta\rangle, |-\theta\rangle\}$

- Mesure en base $\mathcal{B}(\theta)$:

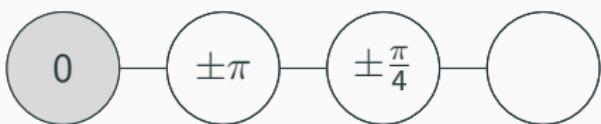


- Mesure adaptative :



Méthode de calcul : Pattern de mesure

Notation :



- $\mathcal{B}(\theta) = \{|+\theta\rangle, |-\theta\rangle\}$
- Mesure en base $\mathcal{B}(\theta)$:
- Mesure adaptative :
- L'ordre des mesures doit être spécifiée

Calcul quantique basé sur la mesure

Procédure :

1. Générer un graphe d'état de la structure souhaitée

Calcul quantique basé sur la mesure

Procédure :

1. Générer un graphe d'état de la structure souhaitée
2. Mesurer les états du graphe en suivant un pattern de mesure

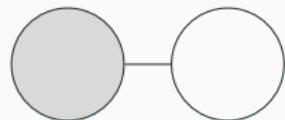
Calcul quantique basé sur la mesure

Procédure :

1. Générer un graphe d'état de la structure souhaitée
2. Mesurer les états du graphe en suivant un pattern de mesure
3. Le résultat du calcul est soit les état restants (quantique) soit la mesure des états restants (classique). Nous allons voir que du post-processing classique est nécessaire pour interpréter le résultat.

Examples et équivalence avec les circuit quantiques

Propagation de l'information



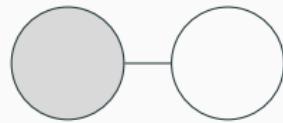
=



=

$$\alpha |0+\rangle + \beta |1+\rangle$$

Propagation de l'information



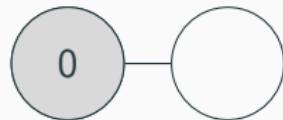
=



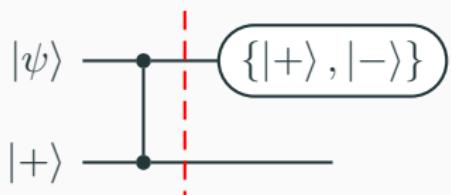
=

$$\alpha |0+\rangle + \beta |1-\rangle$$

Propagation de l'information



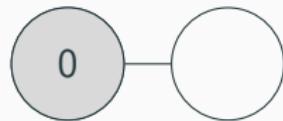
=



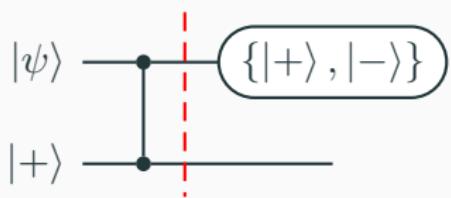
=

$$\alpha |0+\rangle + \beta |1-\rangle$$

Propagation de l'information



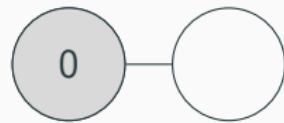
=



=

$$\frac{|+\rangle \otimes H|\psi\rangle}{\sqrt{2}} + \frac{|-\rangle \otimes XH|\psi\rangle}{\sqrt{2}}$$

Propagation de l'information



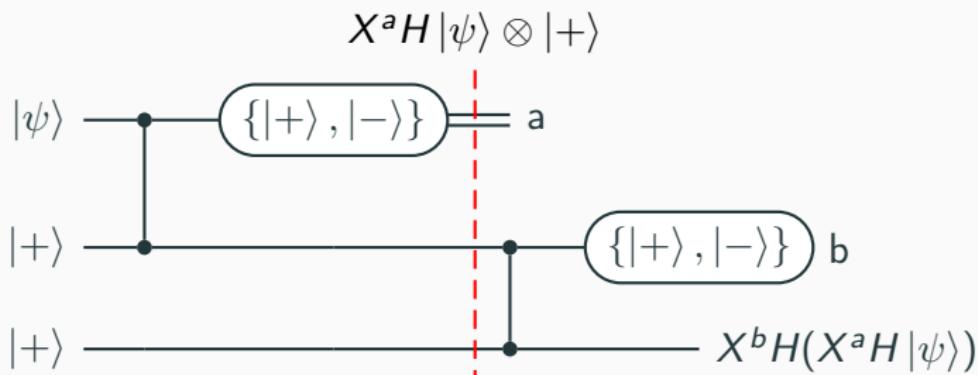
=



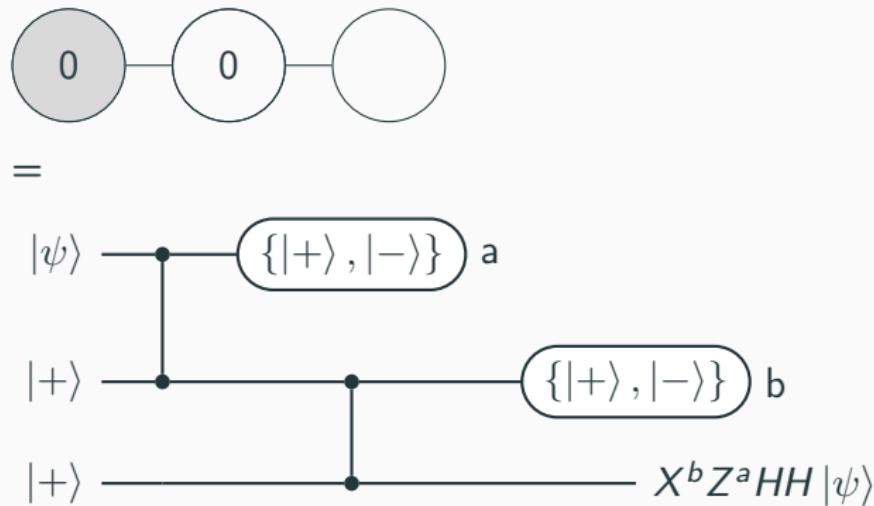
Propagation de l'information



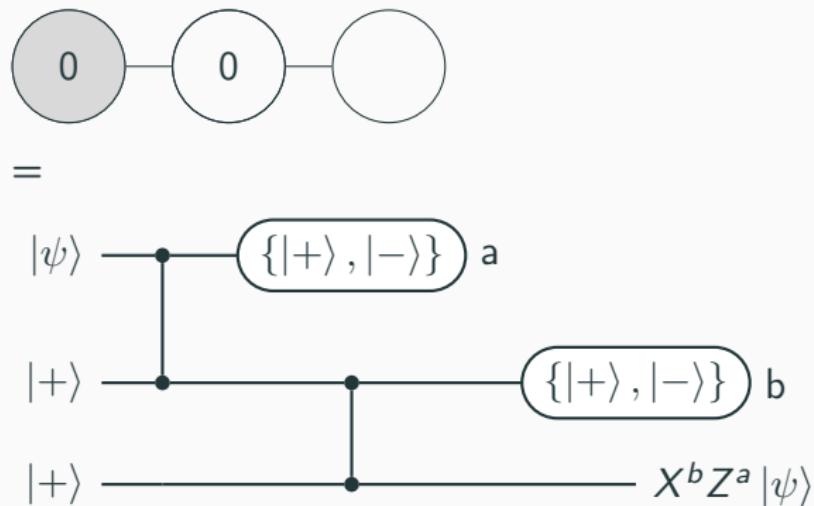
=



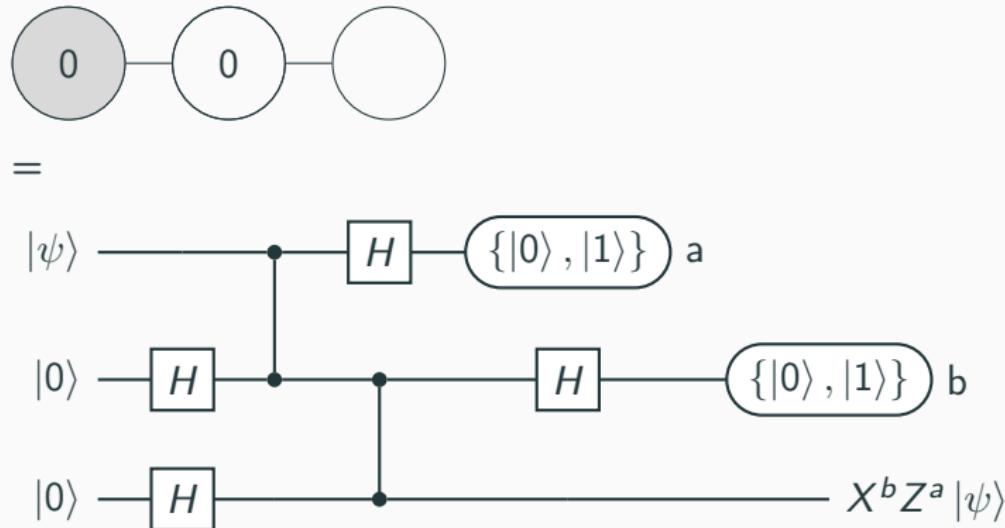
Propagation de l'information



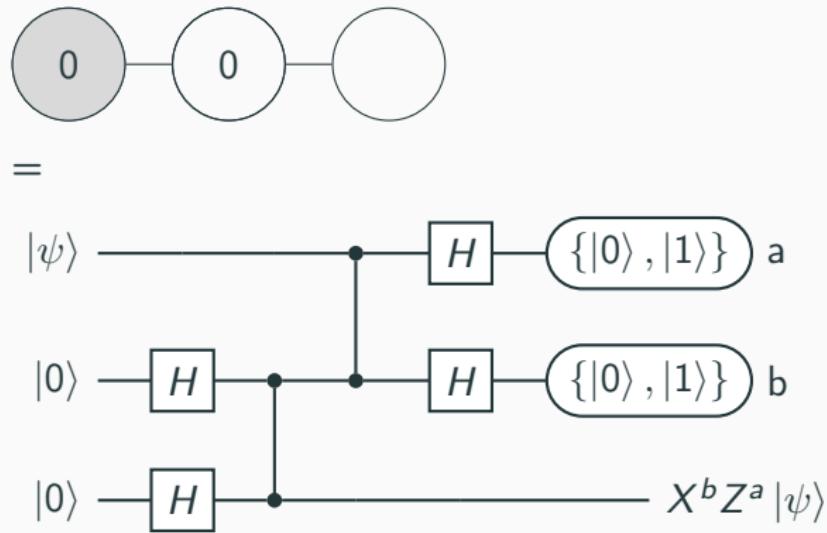
Propagation de l'information



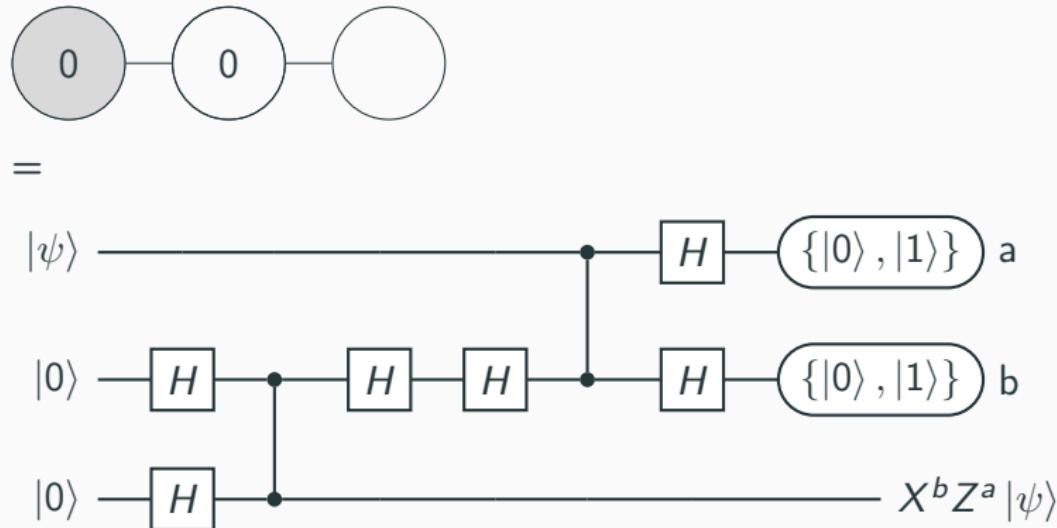
Propagation de l'information



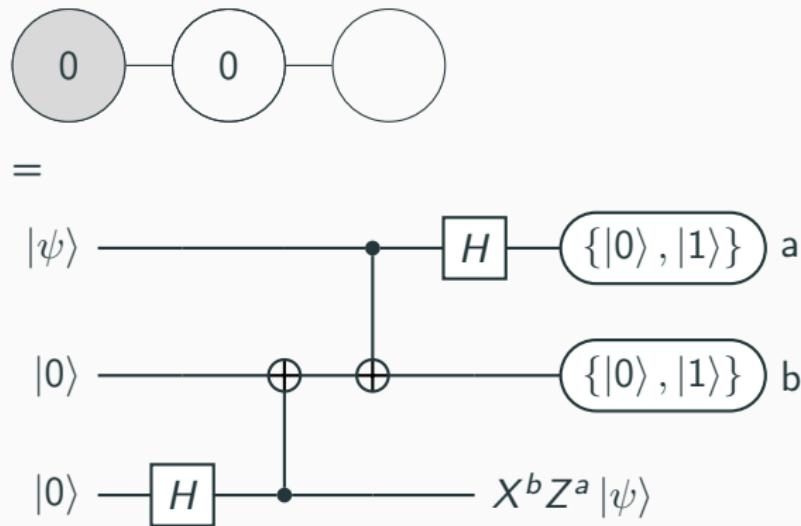
Propagation de l'information



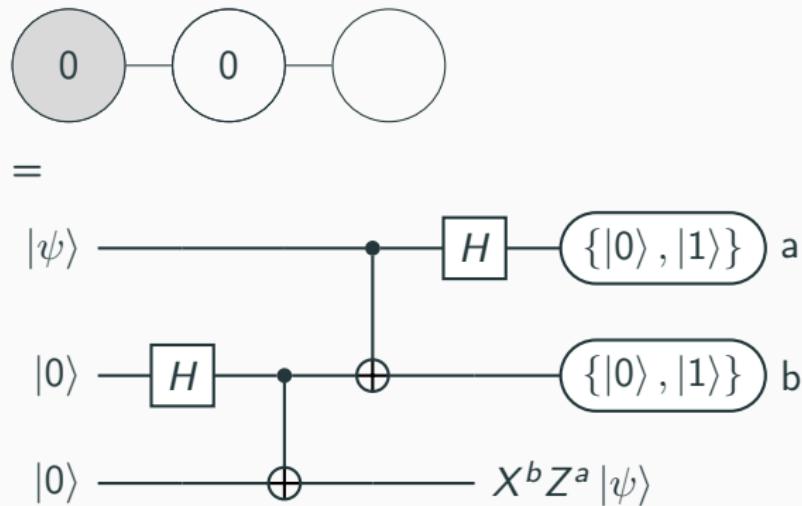
Propagation de l'information



Propagation de l'information

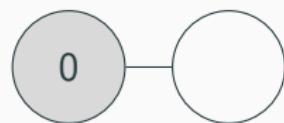


Propagation de l'information



Propagation de l'information

Observation importante



"téléporte" $H |\psi\rangle$ sur le deuxième qubit à une correction près.

Propagation de l'information

Observation importante



"téléporte" $HH |\psi\rangle$ sur le deuxième qubit
à une correction près.

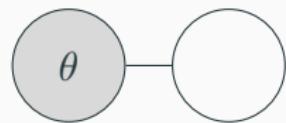
Propagation de l'information

Observation importante

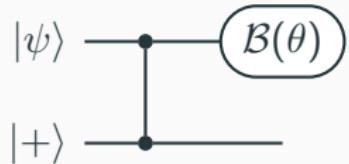


"téléporte" $|\psi\rangle$ sur le deuxième qubit à une correction près.

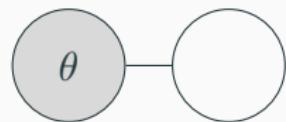
Mesures plus générales



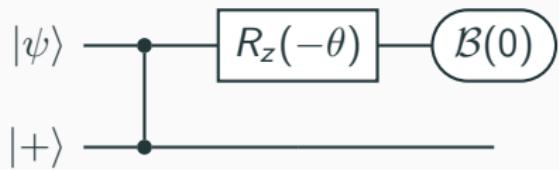
=



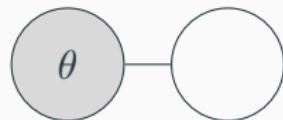
Mesures plus générales



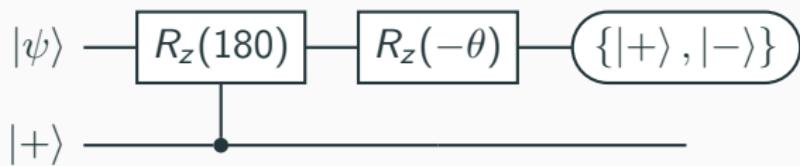
=



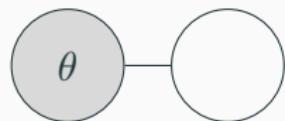
Mesures plus générales



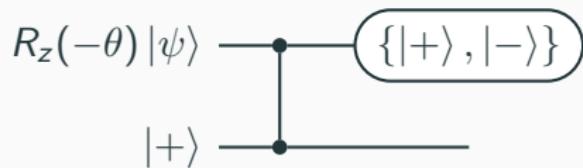
=



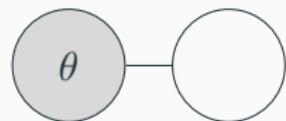
Mesures plus générales



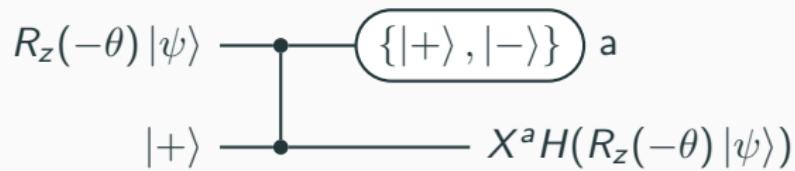
=



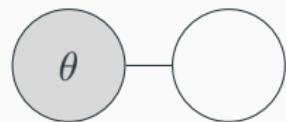
Mesures plus générales



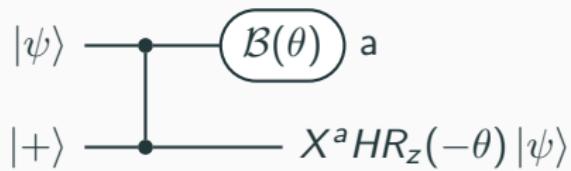
=



Mesures plus générales



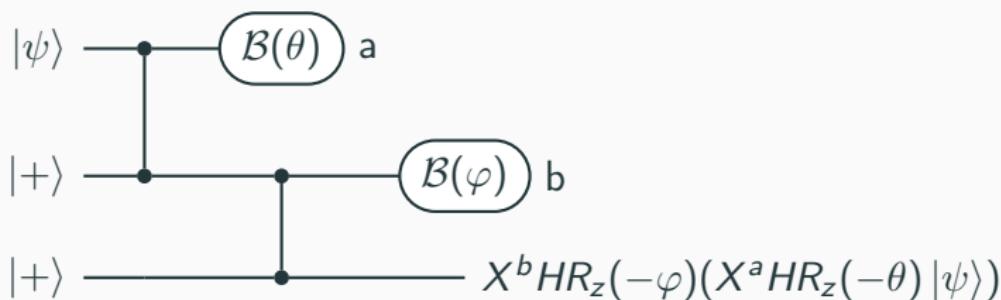
=



Mesures plus générales



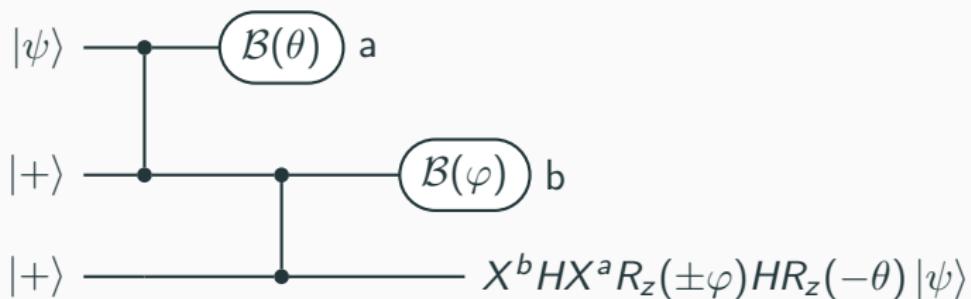
=



Mesures plus générales



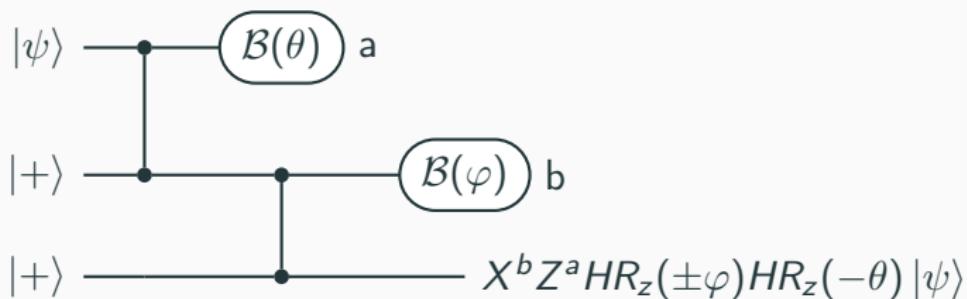
=



Mesures plus générales



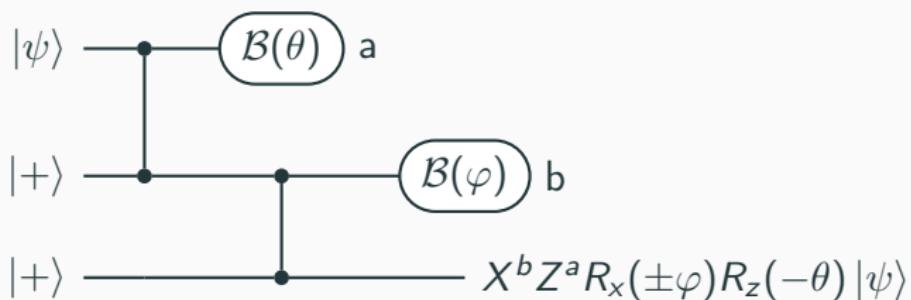
=



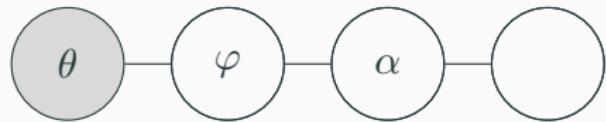
Mesures plus générales



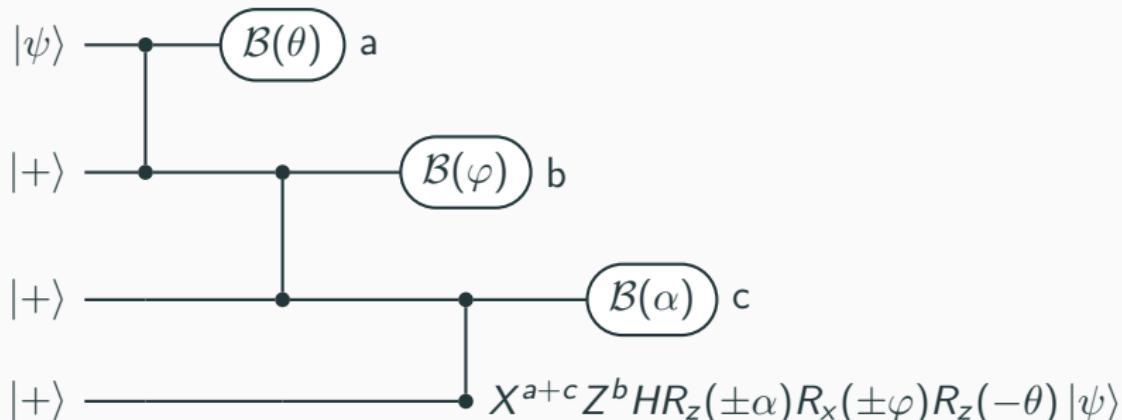
=



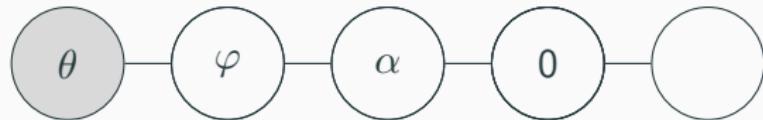
Mesures plus générales



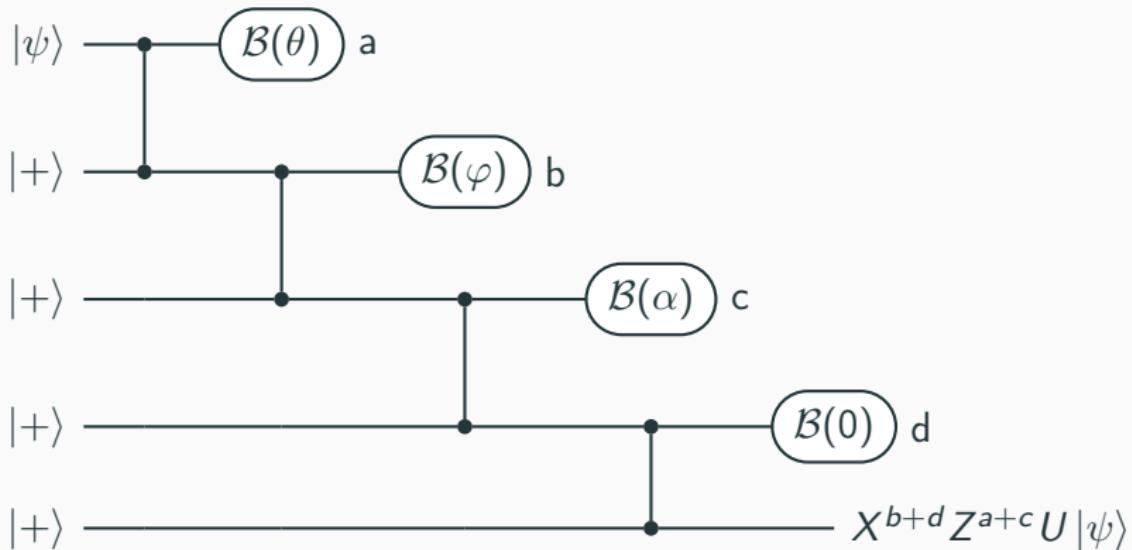
=



Mesures plus générales



=



Simulation d'un circuit quantique



Observations importantes

1. Mesurer en base θ un sommet contenant l'état $|\psi\rangle$ "téléporte" l'état $HR_z(-\theta)|\psi\rangle$ au sommet suivant à une correction près (X^a).

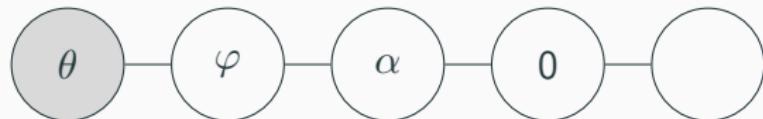
Simulation d'un circuit quantique



Observations importantes

1. Mesurer en base θ un sommet contenant l'état $|\psi\rangle$ "téléporte" l'état $HR_z(-\theta)|\psi\rangle$ au sommet suivant à une correction près (X^a).
2. Les corrections générées par les mesures peuvent toujours être propagés vers la gauche en ne changeant rien à par le signe des rotations.

Simulation d'un circuit quantique



Observations importantes

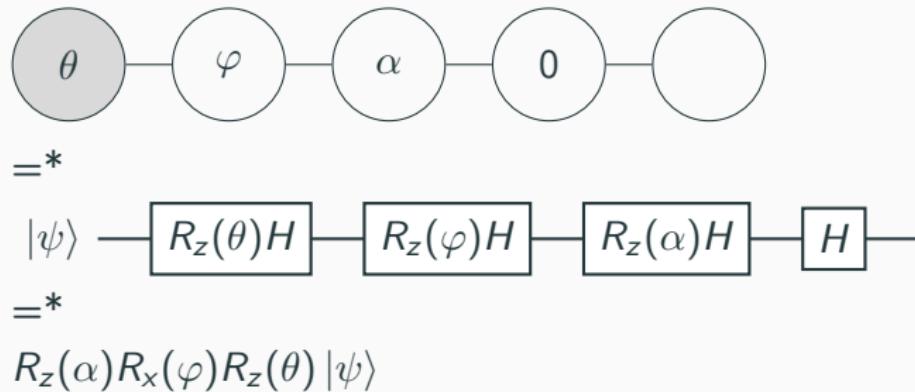
1. Mesurer en base θ un sommet contenant l'état $|\psi\rangle$ "téléporte" l'état $HR_z(-\theta)|\psi\rangle$ au sommet suivant à une correction près (X^a).
2. Les corrections générées par les mesures peuvent toujours être propagés vers la gauche en ne changeant rien à par le signe des rotations.
3. La correction finale sera toujours de la forme X^aZ^b où a et b sont des fonctions des résultats de mesure.

Simulation d'un circuit quantique

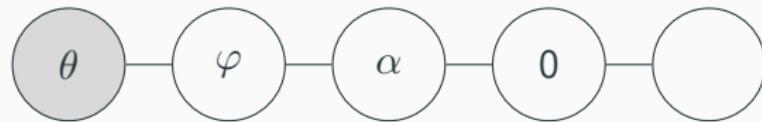
Remarque

La valeur des corrections finales et des signes de mesure peut être calculée efficacement. On peut donc prendre pour acquis que cela est fait implicitement.

Simulation d'un circuit quantique



Simulation d'un circuit quantique



=*



=*

$$R_z(\alpha)R_x(\varphi)R_z(\theta) |\psi\rangle$$

Simulation d'un circuit quantique



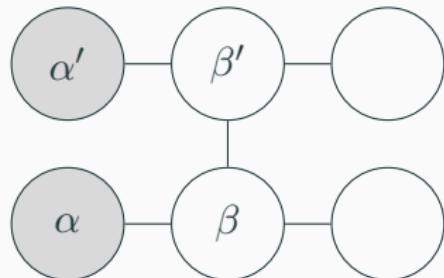
$=^*$



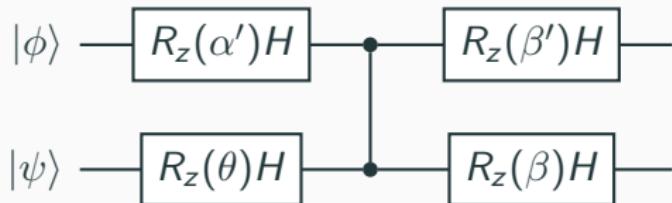
$=^*$

$$R_x(\beta')R_z(\alpha') |\phi\rangle \otimes R_x(\beta)R_z(\alpha) |\psi\rangle$$

Simulation d'un circuit quantique



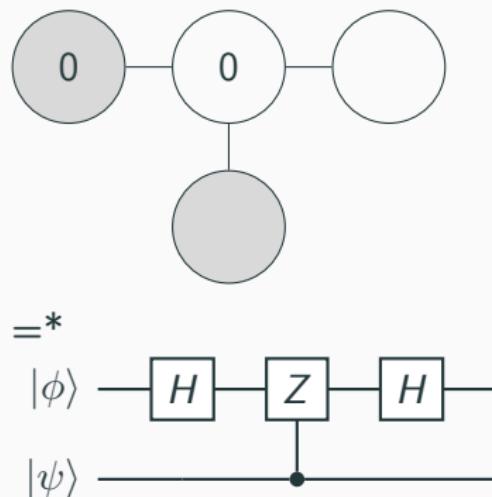
=*



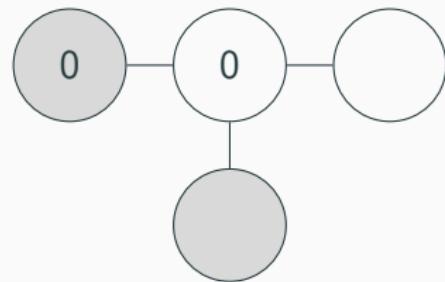
=*

$|\Gamma\rangle$ Intriqué

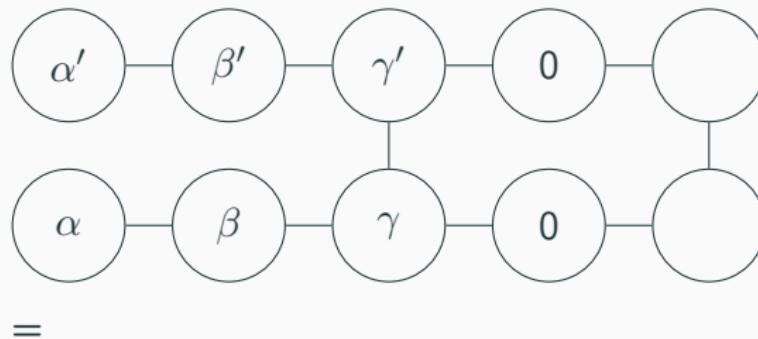
Simulation d'un circuit quantique



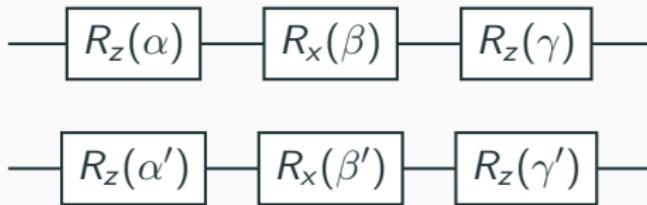
Simulation d'un circuit quantique



Universalité : Graphe du masson



=



Universalité : Graphe du masson



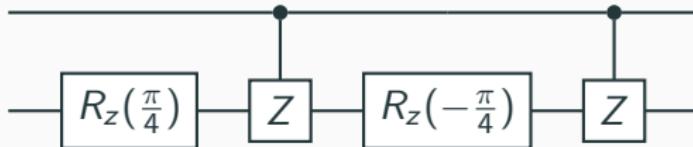
=



Universalité : Graphe du masson



=



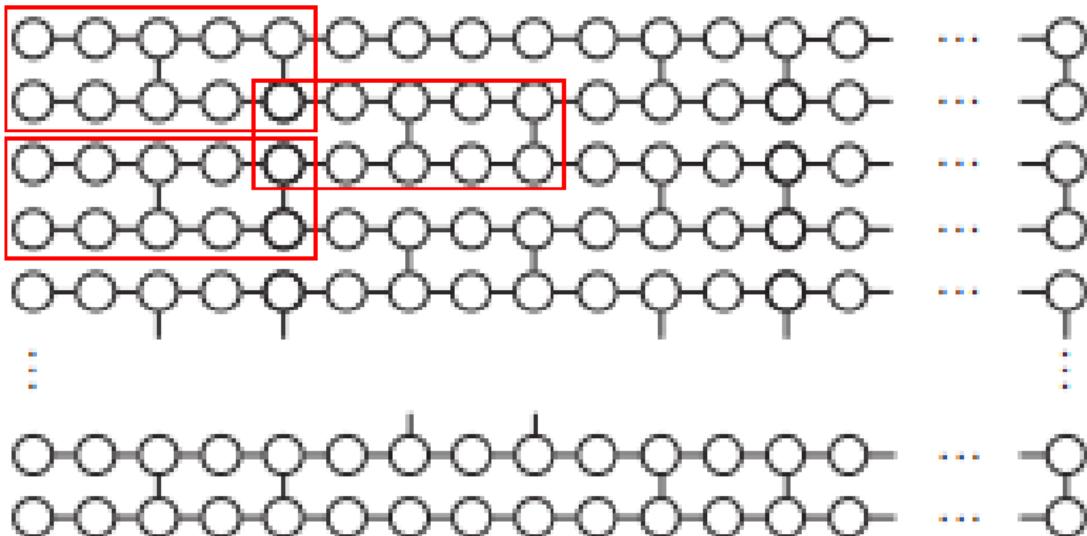
Universalité : Graphe du masson



=

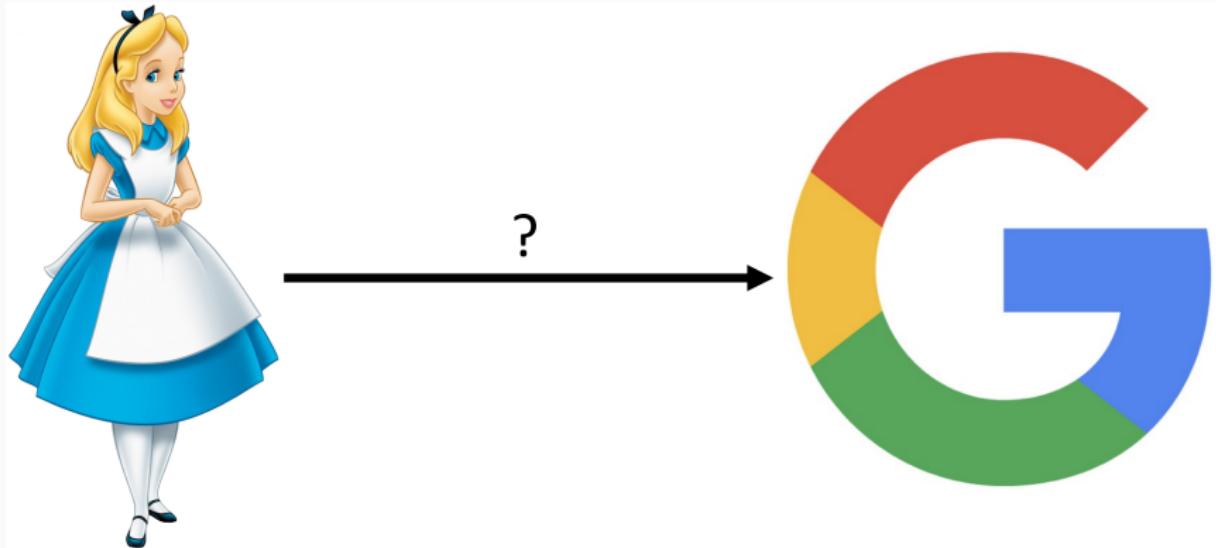


Universalité : Graphe du masson

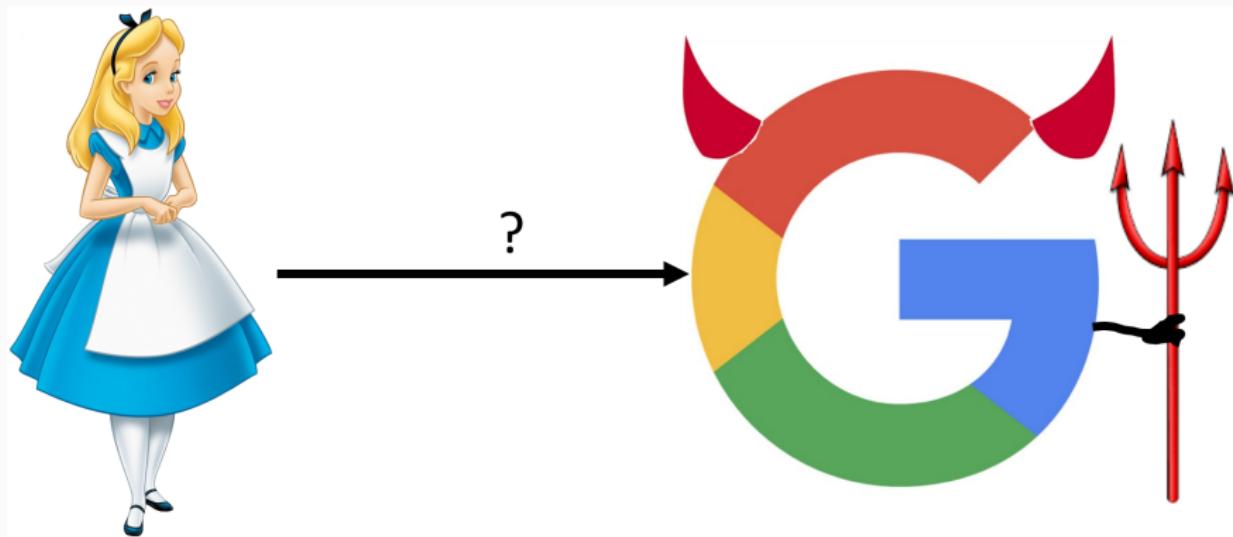


Applications : Calcul aveugle

Calcul aveugle



Calcul aveugle



L'algorithme

Protocol 1 Universal Blind Quantum Computation

1. Alice's preparation

For each column $x = 1, \dots, n$

For each row $y = 1, \dots, m$

- 1.1 Alice prepares $|\psi_{x,y}\rangle \in_R \{|+\theta_{x,y}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta_{x,y}}|1\rangle) \mid \theta_{x,y} = 0, \pi/4, \dots, 7\pi/4\}$ and sends the qubits to Bob.

2. Bob's preparation

- 2.1 Bob creates an entangled state from all received qubits, according to their indices, by applying CTRL-Z gates between the qubits in order to create a brickwork state $\mathcal{G}_{n \times m}$ (see Definition 1).

3. Interaction and measurement

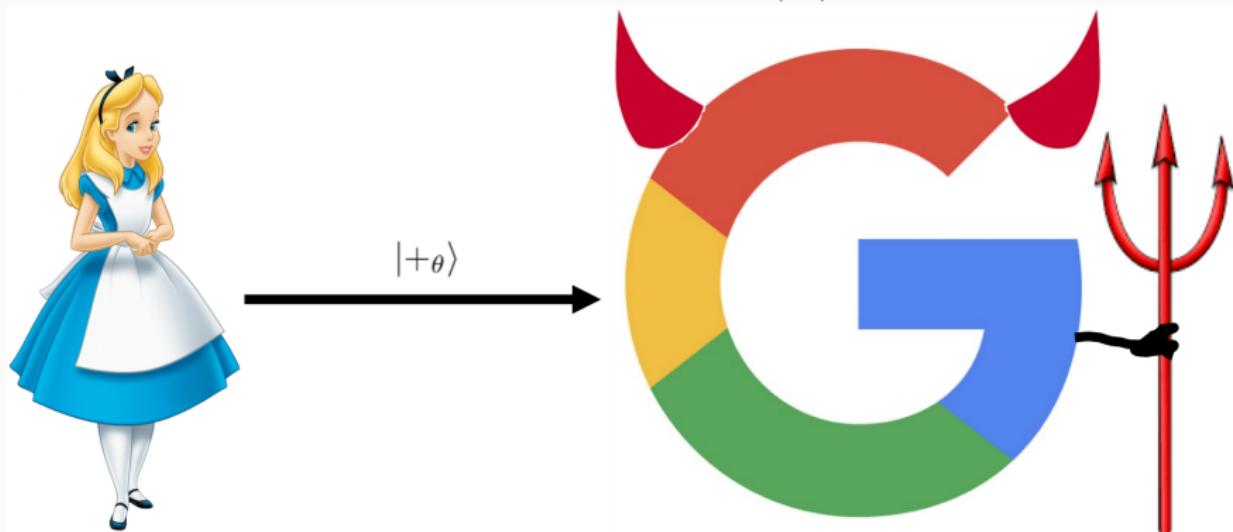
For each column $x = 1, \dots, n$

For each row $y = 1, \dots, m$

- 3.1 Alice computes $\phi'_{x,y}$ where $s_{0,y}^X = s_{0,y}^Z = 0$.
 - 3.2 Alice chooses $r_{x,y} \in_R \{0, 1\}$ and computes $\delta_{x,y} = \phi'_{x,y} + \theta_{x,y} + \pi r_{x,y}$.
 - 3.3 Alice transmits $\delta_{x,y}$ to Bob. Bob measures in the basis $\{|+\delta_{x,y}\rangle, |-\delta_{x,y}\rangle\}$.
 - 3.4 Bob transmits the result $s_{x,y} \in \{0, 1\}$ to Alice.
 - 3.5 If $r_{x,y} = 1$ above, Alice flips $s_{x,y}$; otherwise she does nothing.
-

Masquer les mesures

Pour chaque qubit du futur graphe, Alice choisit un angle θ aléatoire, et envoie une version modifiée de $|+\rangle$



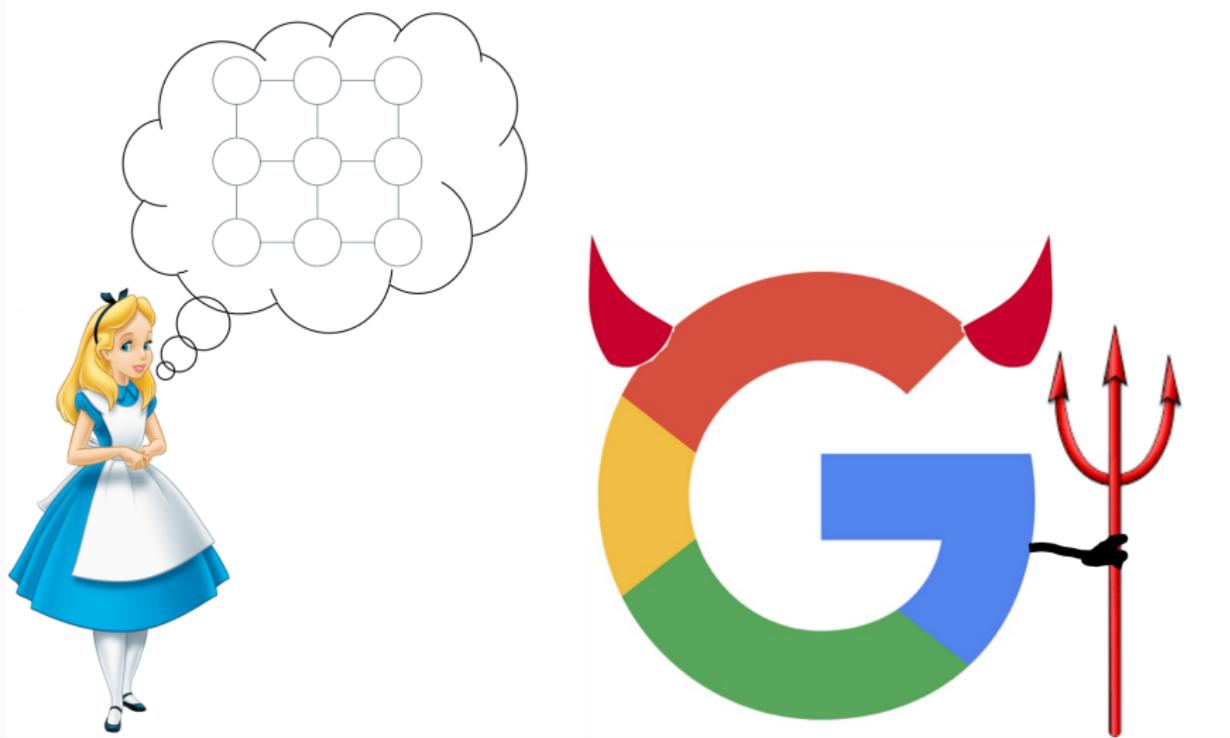
Masquer les mesures

Google construit le graphe d'états avec les qubits d'Alice

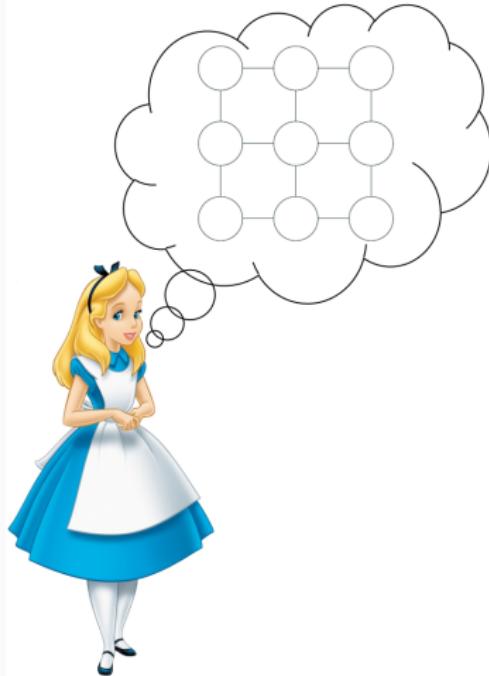


Masquer les mesures

Alice connaît la disposition du graphe et fait ses mesures en fonction des rotations qu'elle a fait au départ.



Masquer les mesures



Alice «voit» le graphe où elle fait ses mesures, mais pas le méchant Google!

Masquer les mesures

Le méchant Google ne sait pas qu'elles sont les mesures qu'Alice veux vraiment faire (avec les corrections de rotations)

Masquer les résultats

Alice tire à pile ou face pour savoir si elle fait une mesure dans la base voulue ou dans la base «inversée»



Masquer les résultats

Si face...



et utilise le résultat de la mesure de Google

Masquer les résultats

Si pile...



et utilise la négation du résultat de la mesure de Google

Masquer les résultats

Google ne connaît pas le résultat qu'Alice désirait réellement!



Google ne sait vraiment pas grand chose!



Autre utilités

- Parallélisation du calcul quantique
- Donne une autre façon de voir le calcul quantique
- Permet une séparation clair entre la section classique et quantique des calculs
- Implémentations potentiellement viables

Merci et Joyeux Noël!

