Informatique Quantique - Exercices

Nicolas Boutry

Année 2023

1 Addition de deux bits quantiques

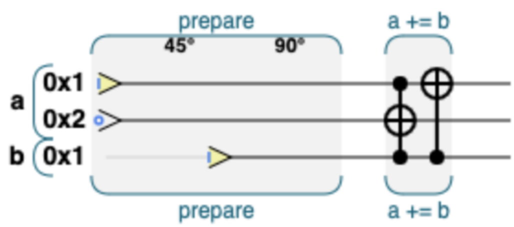


Figure 1: Algorithme d'addition

Montrer que pour $a \in \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, nous obtenons en sortie la valeur $a + b$ (sur les deux premières lignes quantiques) où $b \in \{|0\rangle, |1\rangle\}$ (à l'overflow près), autrement dit, que a devient $a + b$. Le justifier dans un premier temps avec les mains (penser *retenue*), puis le démontrer ensuite par un calcul formel.

2 Déphasage conditionnel

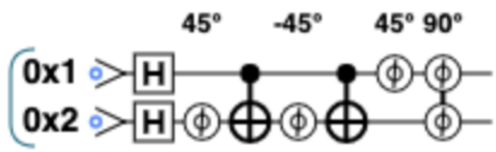


Figure 2: Algorithme de déphasage conditionnel

Montrer que lorsque l'on part de l'état $|00\rangle$, on arrive à l'état:

$$|00\rangle + |01\rangle + |10\rangle - |11\rangle,$$

autrement dit on a déphasé de π l'état $|11\rangle$ uniquement.

3 Swap-Test

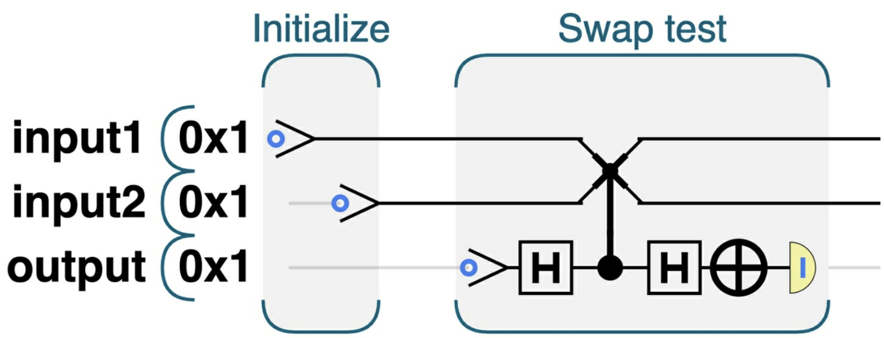


Figure 3-23. Using the swap test to determine whether two registers are in the same state

Figure 3: Algorithme de swap

Question 1 : en vous référant à la figure 3, montrer que lorsque les deux qubits ont la même valeur en entrée, alors le qubit d'output affiche toujours 1.

Question 2 : montrer cette fois ci que lorsque les bits en entrée sont différents, alors il y a une probabilité non nulle que l'output affiche que les états sont égaux à tort (output à 1).

Question 3 : Calculer cette probabilité.

Question 4 : quelle méthodologie proposez-vous pour que l'on s'assure avec une confiance aussi grande que l'on veut que les deux bits d'entrée étaient bien égaux.

Question 5 : combien de mesures devez-vous faire pour être sûrs à 99% que les deux états d'entrée sont différents ?

4 Spy-Hunter

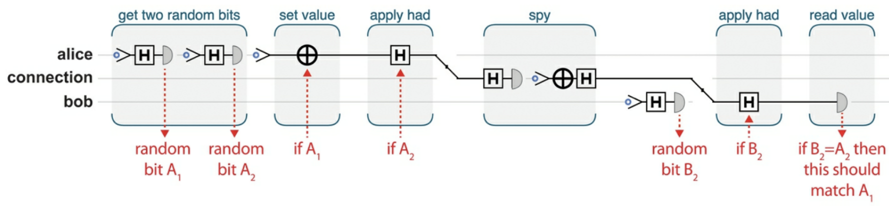


Figure 2-19. The quantum spy hunter program

Figure 4: Algorithme de détection d'espion

Rappel du cours: Alice transmet le bit classique $A_1 \in \{0,1\}$, et change sa polarisation par un Hadamard si et seulement si $A_2 = 1$ (elle ne change pas la polarisation pour $A_2 = 0$). De la même façon, Bob à la réception changera la polarisation par un Hadamard si et seulement le bit B_2 est à 1.

Question 1 (cas sans espion) : en vous référant à la figure 4 privée de l'espion (c'est-à-dire en remplaçant le morceau de circuit représentant l'espion par un court-circuit), calculer la probabilité que Bob reçoive ce que Alice a émis (c'est-à-dire A_1) pour toutes les valeurs possibles (0 ou 1) de A_1, A_2, B_2. En déduire la probabilité globale que Bob ait reçu la valeur émise par Alice.

Question 2 (cas avec espion) : mêmes questions mais en supposant cette fois-ci que l'espion est bien présent (laissez donc cette fois-ci le circuit intact pour le calcul des probabilités).

Question 3 : qu'est-ce qui a changé entre les deux premières questions au niveau de la transmission ?

Question 4 : supposons maintenant qu'après leur transmission sur la ligne quantique, Alice et Bob se téléphonent pour comparer ce qu'ils ont émis/reçu chacun de leur côté (en terme de A_1, A_2, B_2). Alors montrer que certains des qubits correspondant à $A_2 = B_2$ sont fiables pour détecter si un espion était présent sur la ligne quantique, et calculer les probabilités que l'espion soit détecté si il était présent (séparément pour chaque cas).

Question 5 : en déduire la probabilité que l'espion soit détecté si il y a n bits de transmis tels que $A_2 = B_2$ sur un total de $N \geq n$ bits transmis, sachant qu'on ne prendrait en compte que le cas $A_2 = B_2 = 1$ avec de surcroît $A_1 = 0$.

5 Téléportation quantique

Rappel : Z est la porte quantique $ROT(180)$ (ici, elle est contrôlée par le bit *decode*).

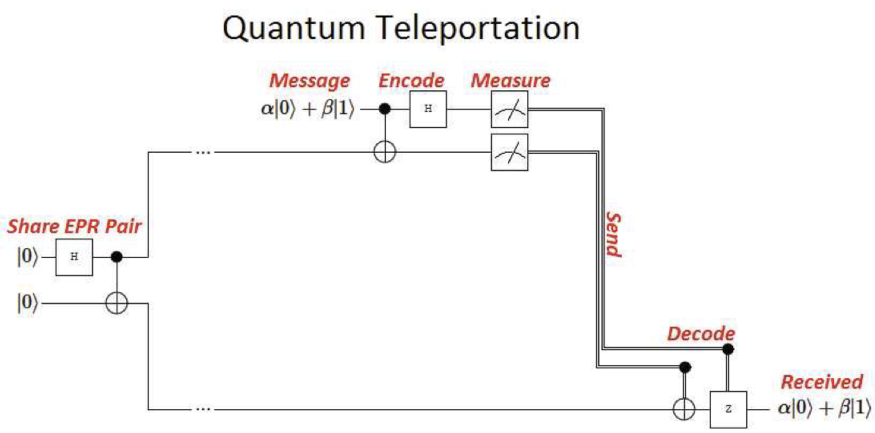
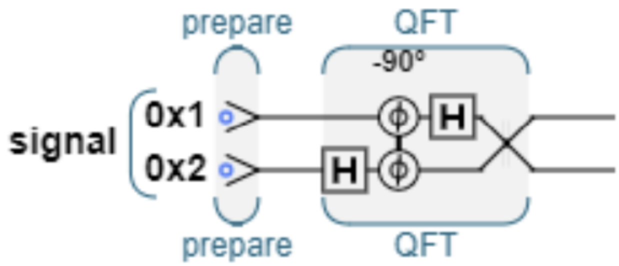


Figure 5: Algorithme de téléportation quantique.

Alice transmet (voir figure 5) le message $\alpha|0\rangle + \beta|1\rangle$ qui agit sur la paire (intriquée) de qubits de Bell (voir EPR pair). Ensuite, un des deux qubits intriqués est transmis sur une ligne quantique (voir bas de la figure), et après les actions d'Alice (voir bits classiques nommées "Send" et "Decode"), Bob reçoit exactement l'état initial $\alpha|0\rangle + \beta|1\rangle$.

Démontrer l'algorithme de téléportation quantique.



6 Transformée de Fourier Quantique

Partez de l'hypothèse que vous avez une entrée sous la forme:

$$A\,|00\rangle + B\,|01\rangle + C\,|10\rangle + D\,|11\rangle,$$

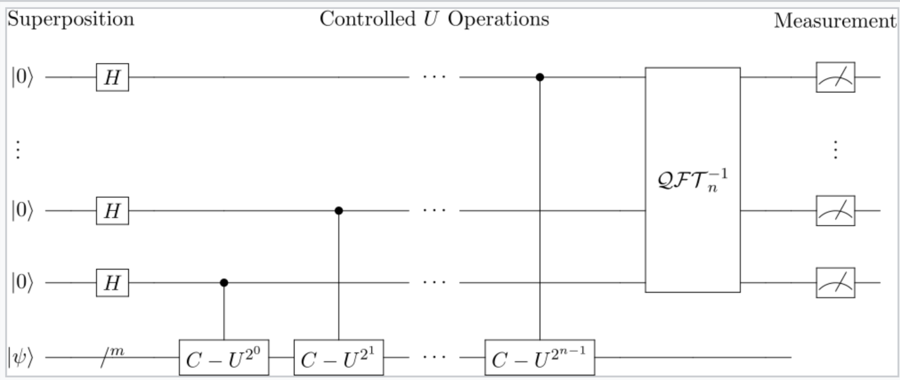
avec la deuxième ligne quantique correspondant au poids fort, c'est-à-dire que $|XY\rangle$ a pour poids fort X et pour poids faible Y, et après avoir appliqué les différents opérateurs, observer les coefficients que vous obtenez dans la forme :

$$A'\,|00\rangle + B'\,|01\rangle + C'\,|10\rangle + D'\,|11\rangle.$$

Qu'observez-vous alors au niveau des nouveaux coefficients en terme de phase, c'est à dire mettre sous forme de suite logique complexe chaque coefficient. Qu'est-ce qui les lie ?

Maintenant, imaginez que la sortie soit "0", c'est à dire l'état $|00\rangle$, qu'aviez vous en entrée ? Et pour "1", "2" et "3'. En particulier, que s'est-il passé à "3" en terme de traitement du signal ?

Justifiez pourquoi on peut dire que l'entrée correspond à une fréquence en observant la sortie correspondante en notation circulaire.



Quantum phase estimation circuit

7 Estimation de phase

On rappelle que la formule de la QFT est la suivante : pour un état

$$|\xi\rangle = \sum_{k=0}^{2^n-1} \xi_k \, |k\rangle,$$

la transformée de Fourier quantique est :

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} \xi_k \, \exp\left(\frac{j2\pi kx}{2^n}\right) |x\rangle,$$

et inversement, la transformée de Fourier inverse est :

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} \xi_k \, \exp\left(-\frac{j2\pi kx}{2^n}\right) |x\rangle.$$

Redémontrez donc que l'angle θ de sortie du circuit est bien la phase du signal d'entrée. Vous remarquerez que la somme des n opérateurs unitaires a permis d'utiliser la QFT (inverse), justifiez pourquoi.

Note : comme U est un opérateur unitaire, on pourra supposer que sa phase propre θ vérifie :

$$U(|\psi\rangle) = \exp(2i\pi\theta) \, |\psi\rangle.$$