LABORATOIRE D'INFORMATIQUE FONDAMENTALE D'ORLEANS

Université d'ORLÉANS

M2 informatique + GPEX Minerve

Contrôle de programmation quantique

durée : 1h30, date : 20 décembre 2024

Nicolas OLLINGER et Ioan TODINCA

Vous pouvez utiliser 3 feuilles recto-verso avec vos notes de cours, TD et TP. La notation est sur 27 points, ce qui vous laisse la possibilité de choisir les questions que vous abordez ou pas.

1 Petits circuits quantiques (9 pts)

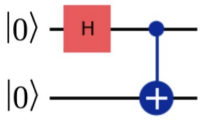
L'objectif de cet exercice est d'étudier et de concevoir certains petits circuits quantiques utiles dans les applications. Pour ce faire nous allons utiliser les portes H, X (également appelée NOT), CX (également appelée $CNOT$), ainsi que la porte Z qui agit sur un seul qubit, comme suit :

$$Z : \quad \begin{array}{lcl} |0\rangle & \mapsto & |0\rangle \\ |1\rangle & \mapsto & -|1\rangle \end{array}$$

1. Montrer que le circuit suivant produit l'état $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$:

2. Montrer le circuit ci-après est équivalent au précédent :

3. Montrer que l'état de Bell $\Psi^+ = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ peut être obtenu par ce circuit :

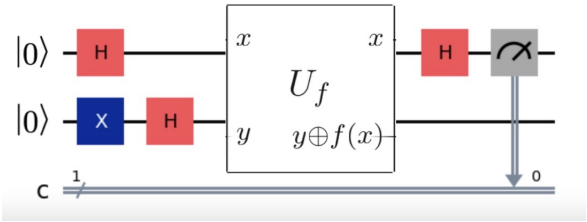


4. Proposer un circuit construisant l'état $\Psi^- = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$. Justifier votre réponse.
5. Proposer un circuit construisant l'état appelé GHZ, $\frac{|000\rangle - |111\rangle}{\sqrt{2}}$. Justifier votre réponse.

2 Algorithme de Deutsch (9 pts)

On considère ici une fonction booléenne sur un seul bit, $f : \{0,1\} \mapsto \{0,1\}$. L'objectif est de montrer que le circuit quantique ci-dessous, dû à Deutsch [1], mesure $|0\rangle$ si $f(0) = f(1)$, et $|1\rangle$ si $f(0) \neq f(1)$.

1. Oui, c'est le même circuit que pour Bernstein-Vazirani. Et c'est un cas particulier d'un problème plus général.



Nous rappelons un résultat déjà vu en cours : si l'on fixe $y = |-\rangle$ dans l'opérateur U_f et que x est un booléen, on obtient en sortie, sur le permier qubit, la valeur $(-1)^{f(x)}|x\rangle$. Formellement,

$$U_f : |x\rangle\,|-\rangle \mapsto (-1)^{f(x)}\,|x\rangle\,|-\rangle$$

1. Vérifier par le calcul que l'état à la sortie de l'opérateur U_f (avant la dernière porte H) est

$$(-1)^{f(0)}\frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{f(0)\oplus f(1)}\,|1\rangle\right)|-\rangle$$

2. Oublions le terme $(-1)^{f(0)}$ (on peut montrer qu'il n'a pas d'impact sur le résultat final). Vérifier par le calcul que, après la dernière porte H, l'état du premier qubit devient

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

3. Conclure que le circuit mesure $|0\rangle$ si et seulement si $f(0) = f(1)$.

3 Questions proches du cours (9 pts)

1. En CP, les enfants apprennent le tri par sélection d'un tableau T de N éléments. Il consiste à répéter N fois l'enchaînement suivant : (1) rechercher l'indice $imin$ du plus petit élément du tableau, (2) afficher $T[imin]$, (3) $T[imin] \leftarrow \infty$.

   Rappeler la complexité de cet algorithme classique. Imaginons maintenant un enfant post-quantique… Quelle est sa complexité de l'algorithme où l'on remplace l'instruction (1) par le recherche quantique du minimum d'un tableau, en temps $O(\sqrt{N})$?

2. Rappeler brièvement pourquoi l'algorithme de Shor, qui calcule un diviseur non trivial d'un nombre N non premier, serait une menace pour le protocole de chiffrement RSA.

3. Pourquoi les algorithmes tels que Grover (et Shor) ne sont pas implémentables avec succès sur les ordinateurs quantiques actuels ?

4. Qu'est-ce que le théorème de non clonage, et en quoi est-il utile aux protocoles d'échanges de clé tels que BB84 ou B92 ?