IFT503/711 – Théorie du calcul

Université de Sherbrooke

Devoir 6

Enseignant:	Dave Touchette
Date de remise:	lundi 15 avril 2024 à 23h59
À réaliser:	individuellement ou à deux au 1er cycle individuellement aux cycles supérieurs
Modalités:	à remettre par Turnin
Pointage:	sur 30 points au 1er cycle (+ 3pts bonus pour ★) sur 36 points aux cycles supérieurs

Question 1.

En utilisant la notation bra-ket, vérifiez les identités de circuits suivantes. Donnez assez de détails pour que je puisse suivre votre raisonnement. Qui sait, peut-être que certaines de ces identités pourraient vous être utiles pour la suite ! 10 pts

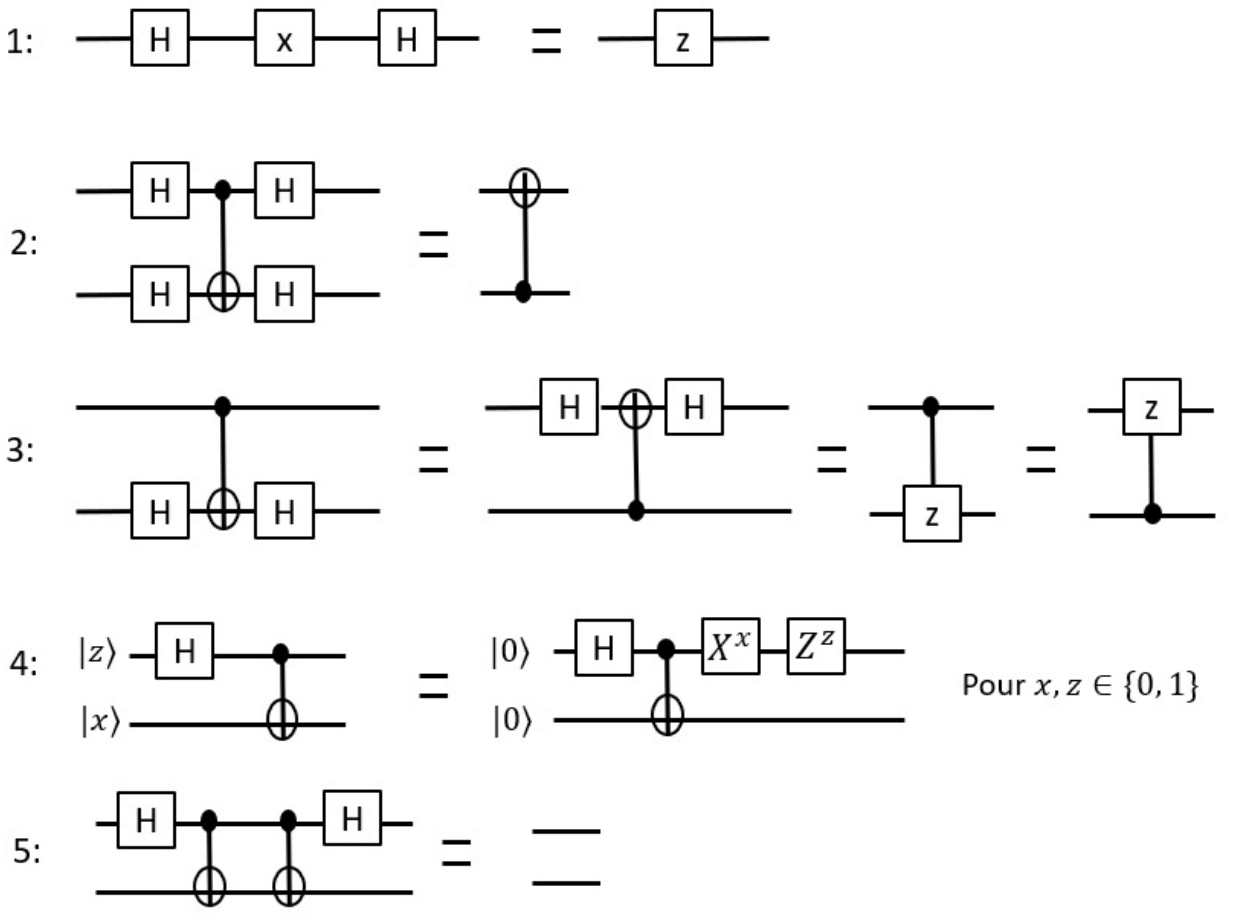

Figure 1 – Identités de circuits

Question 2.

Dans le problème de recherche non-structurée, on reçoit en entrée une fonction $f : \{0,1\}^n \to \{0,1\}$ et on cherche une valeur de $x \in \{0,1\}^n$ tel que $f(x) = 1$. Sans plus d'information sur f et avec la possibilité de faire des requêtes pour évaluer f sur la valeur x de notre choix, et avec $N = 2^n$, on a besoin en moyenne de $\Theta(N)$ requêtes à f classiquement pour trouver un tel x. Quantiquement, l'algorithme de Grover permet de trouver un tel x avec seulement $O(\sqrt{N})$ requêtes quantiques à f. Voyons la version simplifiée du circuit de Grover pour le cas $n = 2$, $N = 4$. Ici, R est la porte qui envoie $|0^n\rangle$ vers $|0^n\rangle$ et $|x\rangle$ vers $-|x\rangle$ si $x \in \{0,1\}^n$ mais $x \neq 0^n$.

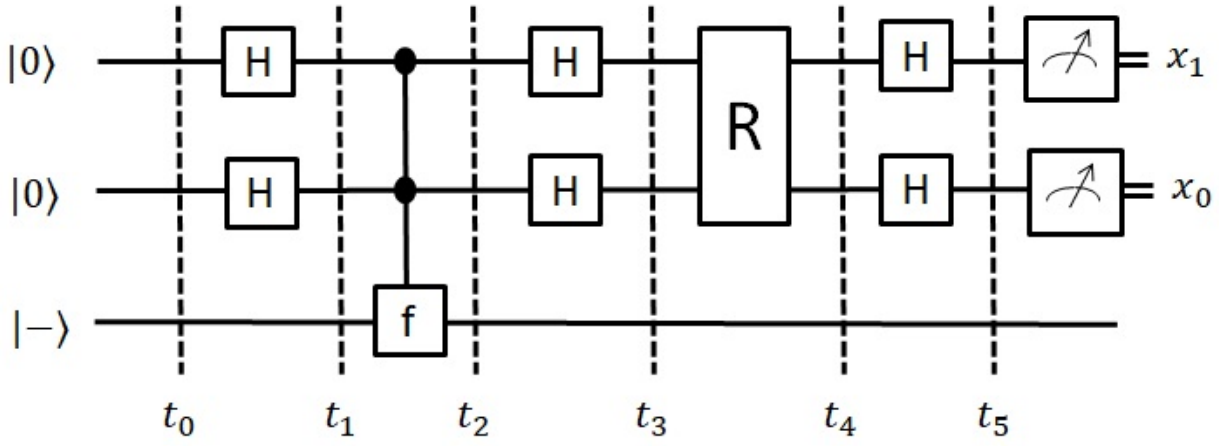

FIGURE 2 – Circuit de Grover sur entrée de deux qubits

(a) S'il n'y a qu'une seule valeur de x, appelons le $\hat{x}$, tel que $f(\hat{x}) = 1$, quels sont les états $|\psi_0\rangle, |\psi_1\rangle, \ldots, |\psi_5\rangle$ aux temps $t_0, t_1, \ldots, t_5$ en fonction de ce $\hat{x}$? Montrez votre calcul. 9 pts

(b) Avec quelle probabilité est-ce que les $x = x_1x_0$ obtenus à la mesure en sortie donnent le résultat $x = \hat{x}$? 1 pt

Question 3.

Le codage superdense permet à deux participants qui ont déjà distribué un état de Bell entre eux avant de recevoir leur entrée de deux bits de transmettre deux bits d'information avec la transmission d'un seul qubit après réception des entrées. Voyons comment.

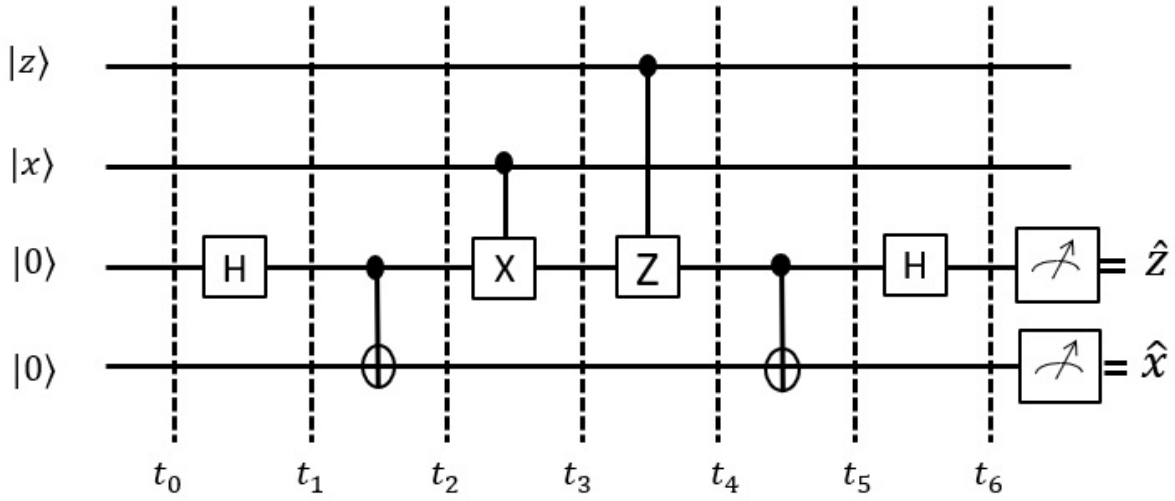

FIGURE 3 – Codage superdense

(a) Quels sont les états $|\psi_i\rangle$ aux différents temps t_i en fonction de $x, z \in \{0,1\}^2$? Montrez votre calcul. 8 pts

(b) Avec quelle probabilité est-ce que les $\hat{z}\hat{x}$ obtenus à la mesure en sortie donnent le résultat zx ? 1 pt

(c) Comment interpréter ce circuit pour implémenter le codage superdense ? 1 pt

★ Question 4. (cycles supérieurs)

L'algorithme de Shor donne une solution au problème de trouver la période d'une fonction périodique injective sur sa période. Voyons comment le problème de factorisation peut se réduire à ce problème.

Pour $a, b, m \in \mathbb{N} = \{0, 1, 2 \ldots\}$, nous écrivons $a = b \mod m$ s.si $a = b + km$ pour un certain $k \in \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$.

Le problème **PF** de trouver la période d'une fonction périodique injective sur sa période est défini comme suit:

entrée : une fonction $f : \mathbb{N} \to \{0, \ldots, N-1\}$ périodique et injective sur sa période.

sortie : $r \in \{0, \ldots, N-1\}$ tel que $f(a) = f(b)$ s.si $a = b \mod r$, la période de f.

Le problème de **factorisation** est défini comme suit:

entrée : $N \in \mathbb{N}$, $N \geq 4$ un nombre qui n'est pas premier.

sortie : p un facteur de N.

Nous allons montrer comment réduire efficacement le problème de factorisation au problème PF.

Premièrement, vérifier que N est ni pair ni une puissance d'un nombre premier. Cela peut être fait efficacement, et dans le cas où ceci n'est pas satisfait, nous obtenons un facteur de N efficacement.

Ensuite, choisir au hasard un $x \in \{2, \ldots, N-1\}$. Vérifier que x ne divise pas N. Cela peut être fait efficacement, et dans le cas où ceci n'est pas satisfait, nous obtenons un facteur de N efficacement.

Considérer la suite suivante: $x^0 = 1 \mod N, x^1, x^2, \ldots, x^r = 1 \mod N, x^{r+1} = x^1 \mod N, x^{r+2} = x^2 \mod N \ldots$, ou r est le plus petit nombre entier strictement positif tel que $x^r = 1 \mod N$. Cette suite cycle donc tout les r termes, et on appelle r la période de la suite.

Avec probabilité au moins $1/2$ sur le choix de x, un événement X se produit qui nous garantie que r est pair et que ni $x^{r/2} + 1$ ni $x^{r/2} - 1$ ne sont des multiples de N.

(a) Définissez une fonction f_x à donner en entrée au problème PF et dont la sortie r correspondrait à la période r de la suite si haut pour un x donné. ★ 2 pts

(b) Montrez dans le cas où l'événement X se produit, $(x^{r/2} + 1)(x^{r/2} - 1) = 0 \mod N$. Nous avons alors $(x^{r/2} + 1)(x^{r/2} - 1) = kN$ pour un certain $k \in \mathbb{N}$, $k > 0$. ★ 2 pts

(c) À partir de ces constatations, dites comment réduire efficacement le problème de factorisation au problème PF. Indice: chercher le web pour un algorithme efficace pour trouver le "gcd" de deux nombres. ★ 2 pts