ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Faculté Informatique et Communications

Calcul Quantique — Heure de début: 08h15

8 Juillet 2021 — Heure de fin: 11h15

Examen Final – CS 308 –

Il y a 4 problèmes: trois problèmes réguliers et un problème qui consiste de quelques questions courtes. Utilisez le papier brouillon si nécessaire, mais écrivez vos solutions dans les espaces indiqués.

Vous avez droit à une page A4 recto-verso avec votre résumé personnel.

Nom Prénom: _____

Section: _____

Sciper No.: _____

Problème 1	/ 16 pts
Problème 2	/ 12 pts
Problème 3	/ 16 pts
Problème 4	/ 16 pts
Total	**/60 pts**

Problème 1 (16 pts)**.** *Variante sur l'algorithme de Deutsch et Josza*

Soit $f : \mathbb{F}_2^n \to \mathbb{F}_2$ une fonction Booléenne qui est balancée ou constante. Soit U_f la représentation unitaire de f. Concrètement pour $b_1, \cdots, b_n$ et y dans $\{0, 1\}$:

$$U_f|b_1 \dots b_n\rangle \otimes |y\rangle = |b_1 \dots b_n\rangle \otimes |y \oplus f(b_1, \dots, b_n)\rangle$$

Soit aussi l'opération unitaire suivante:

$$U = (H^{\otimes n} \otimes I)\, U_f\, (H^{\otimes n} \otimes (HX))$$

où $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ est la matrice de Hadamard, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ la porte NOT, et $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

1. (2 pts) Dessinez le circuit quantique associé à U.

2. (6 pts) Supposons que les n premiers qubits sont initialisés dans l'état habituel $|0\rangle$ mais que le dernier qubit est corrompu et initialisé dans l'état "imparfait" $\sqrt{1-\epsilon^2}|0\rangle + \epsilon|1\rangle$ avec $0 < \epsilon < 1$. C'est à dire que l'état d'entrée du circuit est $|0\rangle^{\otimes n} \otimes (\sqrt{1-\epsilon^2}|0\rangle + \epsilon|1\rangle)$. Calculez l'état de sortie du circuit quantique.

3. (6 pts) On mesure les n premiers qubits dans la base computationelle (le dernier ancilla qubit n'est pas mesuré comme dans l'algorithme habituel de Deutsch et Josza). Quelle est la probabilité $\mathbb{P}(c_1, \dots, c_n)$ d'obtenir l'état $|c_1 \dots c_n\rangle$, $c_i \in \{0, 1\}$ après la mesure ?

4. (2pts) Calculez les probabilités $\mathbb{P}(0, \dots, 0)$ dans les cas f constante ou f balancée.

Solution du problème 1:

1. Faire le dessin. Mettre les portes dans le bon ordre! Les produit matriciel s'applique sur les états de droite à gauche, et sur le dessin les portes sont dessinées de gauche à droite.

2. La sortie du circuit se calcule comme cela:

$$
\begin{aligned}
&H^{\otimes n}U_f H^{\otimes n} \otimes HX|0\rangle^{\otimes n} \otimes (\sqrt{1-\epsilon^2}|0\rangle + \epsilon|1\rangle) \\
&= \frac{1}{2^{n/2}} H^{\otimes n}U_f \sum_{b_1,\ldots,b_n} |b_1 \ldots b_n\rangle \otimes (\sqrt{1-\epsilon^2}\frac{(|0\rangle - |1\rangle)}{\sqrt{2}} + \epsilon\frac{(|0\rangle + |1\rangle)}{\sqrt{2}}) \\
&= \frac{1}{2^{n/2}}\sqrt{1-\epsilon^2} \sum_{b_1,\ldots,b_n} (-1)^{f(b_1\ldots b_n)} H^{\otimes n}|b_1 \ldots b_n\rangle \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \\
&+ \frac{1}{2^{n/2}}\epsilon \sum_{b_1,\ldots,b_n} H^{\otimes n}|b_1 \ldots b_n\rangle \otimes \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \\
&= \frac{1}{2^n}\sqrt{1-\epsilon^2} \sum_{c1,\ldots,c_n} \left\{ \sum_{b_1,\ldots,b_n} (-1)^{f(b_1\ldots b_n)+\sum_i c_i b_i} \right\} |c_1 \ldots c_n\rangle \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \\
&+ \frac{1}{2^n}\epsilon \sum_{c1,\ldots,c_n} \left\{ \sum_{b_1,\ldots,b_n} (-1)^{\sum_i b_i c_i} \right\} |c_1 \ldots c_n\rangle \otimes \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \qquad (1)
\end{aligned}
$$

3. La probabilité est

$$\mathbb{P}(c_1, \ldots, c_n) = \frac{1-\epsilon^2}{2^{2n}} \left| \sum_{b_1,\ldots,b_n} (-1)^{f(b_1\ldots b_n)+\sum_i c_i b_i} \right|^2 + \frac{\epsilon^2}{2^{2n}} \left| \sum_{b_1,\ldots,b_n} (-1)^{\sum_i c_i b_i} \right|^2 \qquad (2)$$

4.

$$\mathbb{P}(0, \ldots, 0) = \frac{1-\epsilon^2}{2^{2n}} \left| \sum_{b_1,\ldots,b_n} (-1)^{f(b_1\ldots b_n)} \right|^2 + \epsilon^2 \qquad (3)$$

Si f est BAL on a $\text{Prob}(0, \ldots, 0) = \epsilon^2$ et si f est CONST $\text{Prob}(0, \ldots, 0) = 1-\epsilon^2+\epsilon^2 = 1$

Problème 2 (12 pts)**.** *Recherche de l'ordre et estimation de phase*

Nous avons vu dans les exercices et le mini-projet que pour une matrice unitaire U et un vecteur propre $|u\rangle$ tel que $U|u\rangle = e^{2\pi i\theta}|u\rangle$, le circuit pour l'estimation de phase peut être utilisé pour estimer les n bits les plus significatifs de θ. Dans ce problème nous montrons que cet algorithme sert aussi à estimer *l'ordre d'un entier modulo* N. Nous rappelons que le calcul de l'ordre est crucial pour l'algorithme de Shor.

Soit x un entier plus petit que N et premier avec N, c'est à dire $\text{PGCD}(x, N) = 1$. Nous rappelons que *l'ordre de* x *modulo* N est l'entier minimal $r \neq 0$ tel que $x^r = 1 \bmod N$.

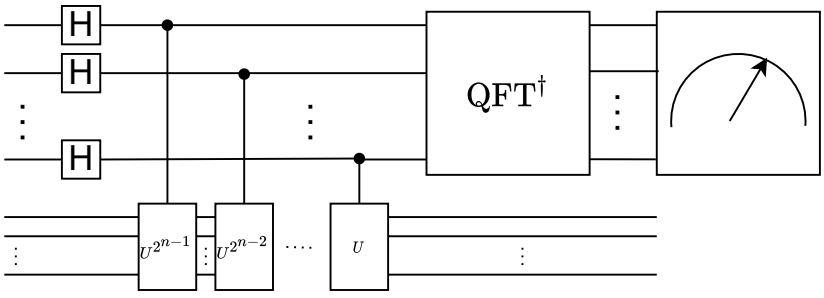
Soit U_x la matrice unitaire définie par

$$U_x|y\rangle = |xy \,(\text{mod N})\rangle.$$

Pour $0 \leq s < r$, soit

$$|\psi_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s \frac{k}{r}} |x^k \,(\text{mod N})\rangle$$

1. (2pts) Verifiez que U_x est unitaire.
2. (5pts) Montrez que $|\psi_s\rangle$ est un vecteur propre de U_x avec valeur propre $e^{2\pi i \frac{s}{r}}$.
3. (5pts) Dans le circuit de l'estimation de phase de la figure quel doit étre létat initial si on veut estimer $1/r$? Combien de bits quantiques faut-il utiliser pour estimer les n bits les plus significatifs de $1/r$? (on ne vous demande pas de refaire les calculs de l'analyse de l'algorithme mais juste de donner les réponses).



Solution du problème 2:

1. Il faut vérifier que $U_x U_x^\dagger = U_x^\dagger U_x = I$. On a

$$\langle z|U_x^\dagger U_x|y\rangle = \langle xz|xy\rangle = \begin{cases} 1 & \text{if } xy \equiv xz(\text{mod } N) \\ 0 & \text{otherwise} \end{cases}$$

   Puisque x est premier avec N, $xy \equiv xz(\text{mod } N)$ est équivalent à $z = y$. Donc $U_x^\dagger U_x$ est effectivement égal à la matrice identité.

2.

$$\begin{aligned} U_x|\psi_s\rangle &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s \frac{k}{r}} U_x|x^k \text{ (mod N)}\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s \frac{k}{r}} |x^{k+1} \text{ (mod N)}\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{k=1}^{r} e^{-2\pi i s \frac{k-1}{r}} |x^k \text{ (mod N)}\rangle \\ &= e^{2\pi i \frac{s}{r}} \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s \frac{k-1}{r}} |x^k \text{ (mod N)}\rangle = \mathrm{e}^{2\pi \mathrm{i} \frac{\mathrm{s}}{\mathrm{r}}} |\psi_\mathrm{s}\rangle \end{aligned}$$

   où nous avons utilisé $k \to k+1$ pour obtenir la troisième ligne et pour la quatrième ligne le fait que l'ordre de x mod N est r.

3. On applique le circuit d'estimation de phase avec $|\psi_{s=1}\rangle$ pour l'entrée sur les ancilla qubits et $|0\rangle$ sur les autres qubits. Le nombre de qubits total doit être $n + [\log_2 N]$ (ici $[\log_2 N]$ la partie entière de $\log_2 N$).

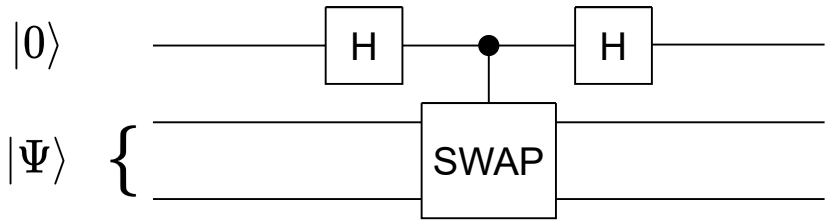
Problème 3 (16 pts)**.** *Un circuit avec la porte de Fredkin*

La porte SWAP est une porte à deux qubits implementant l'opération unitaire:
SWAP$|\chi\rangle \otimes |\phi\rangle = |\phi\rangle \otimes |\chi\rangle$, pour deux états arbitraires de $\mathbb{C}^2$.

La porte de Fredkin est le control-SWAP qui s'applique sur 3 qubits:
control-SWAP$|0\rangle \otimes |\chi\rangle \otimes |\phi\rangle = |0\rangle \times |\chi\rangle \otimes |\phi\rangle$ et control-SWAP$|1\rangle \otimes |\chi\rangle \otimes |\phi\rangle = |1\rangle \otimes |\phi\rangle \otimes |\chi\rangle$.

1. (4pts) Ecrivez les matrices SWAP et control-SWAP dans la base computationelle. *Note*: les questions suivantes sont indépendantes.

2. (4pts) Considérez le circuit quantique ci-dessous. Ecrivez l'état de sortie en terme des deux états $(|\Psi\rangle + \text{SWAP}|\Psi\rangle)$ and $(|\Psi\rangle - \text{SWAP}|\Psi\rangle)$.



3. (4pts) Calculez la probabilité de mesurer 0 pour le premier qubit quand $|\Psi\rangle$ est un état de Bell. Donnez cette probabilité pour chacun des 4 états de Bell.
Rappel: les états de Bell sont $\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ et $\frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$.

4. (4pts) Supposez que l'on vous donne deux états $|\chi\rangle$ and $|\phi\rangle$ à un qubit dans $\mathbb{C}^2$, avec la promesse qu'ils sont identiques ou bien orthogonaux. Soit $|\Psi\rangle = |\chi\rangle \otimes |\phi\rangle$. On mesure le premier qubit de sortie une seule fois (celui du haut sur la figure).

   (a) Si les états sont identiques quels sont les résultats possible de la mesure et leur probabilité ?

   (b) Si les états sont orthogonaux quels sont les résultats possible de la mesure et leur probabilité ?

   (c) Si on observe que le résultat de la mesure est 1, peut-on en tirer une conclusion avec certitude (et si oui laquelle) ?

   (d) Si on observe que le résultat de la mesure est 0, peut-on en tirer une conclusion avec certitude (et si oui laquelle) ?

Solution du problème 3:

1.

$$\mathrm{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\mathrm{CSWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

2.

$$\begin{aligned}(H \otimes I_4)\mathrm{CSWAP}(\mathrm{H} \otimes \mathrm{I}_4)|0\rangle|\Psi\rangle &= (H \otimes I_4)\mathrm{CSWAP}\frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)|\Psi\rangle \\ &= (H \otimes I_4)\frac{1}{\sqrt{2}}\Big(|0\rangle|\Psi\rangle + |1\rangle\mathrm{SWAP}|\Psi\rangle\Big) \\ &= \frac{1}{2}\Big[\big(|0\rangle + |1\rangle\big)|\Psi\rangle + \big(|0\rangle - |1\rangle\big)\mathrm{SWAP}|\Psi\rangle\Big] \\ &= \frac{1}{2}|0\rangle\Big(|\Psi\rangle + \mathrm{SWAP}|\Psi\rangle\Big) + \frac{1}{2}|1\rangle\Big(|\Psi\rangle - \mathrm{SWAP}|\Psi\rangle\Big)\end{aligned}$$

3.

$$|\Psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \Rightarrow \text{état de sortie: } \frac{1}{\sqrt{2}}|0\rangle \otimes \Big(|00\rangle + |11\rangle\Big) \Rightarrow \mathbb{P}(0) = 1$$

$$|\Psi\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \Rightarrow \text{état de sortie: } \frac{1}{\sqrt{2}}|0\rangle \otimes \Big(|00\rangle - |11\rangle\Big) \Rightarrow \mathbb{P}(0) = 1$$

$$|\Psi\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}} \Rightarrow \text{état de sortie: } \frac{1}{\sqrt{2}}|0\rangle \otimes \Big(|10\rangle + |01\rangle\Big) \Rightarrow \mathbb{P}(0) = 1$$

$$|\Psi\rangle = \frac{|10\rangle - |01\rangle}{\sqrt{2}} \Rightarrow \text{état de sortie: } \frac{1}{\sqrt{2}}|1\rangle \otimes \Big(|10\rangle - |01\rangle\Big) \Rightarrow \mathbb{P}(0) = 0$$

4. (a) L'entrée est $|0\rangle \otimes |\chi\rangle \otimes |\phi\rangle$ et la sortie

$$\frac{1}{2}|0\rangle \otimes \Big(|\chi\rangle \otimes |\phi\rangle + |\phi\rangle \otimes |\chi\rangle\Big) + \frac{1}{2}|1\rangle \otimes \Big(|\chi\rangle \otimes |\phi\rangle - |\phi\rangle \otimes |\chi\rangle\Big)$$

Si les états sont identiques la mesure donnera $|0\rangle$ avec probabilité 1.

(b) Si les état sont orthogonaux on obtient $|0\rangle$ ou $|1\rangle$ avec probabilité 1/2.

(c) Si on observe 1 les états ne peuvent pas être identiques et sont donc certainement orthogonaux.

(d) Si on observe 0 on ne peut pas conclure avec certitude.

Problème 4 (16pts)**.** *Répondez à ces questions par une courte justification ou un calcul simple.*

1. (4.5 pts) Vrai ou faux ?

   - Un ensemble de portes universelles pour les circuits quantiques doit nécessairement inclure au moins une porte à trois qubits (comme pour les circuits classiques réversibles).
     Réponse:

   - Un circuit quantique idéal est toujours réversible tant qu'on ne prend pas en compte l'opération de mesure ?
     Réponse:

   - Soit l'état à un qubits $\alpha|0\rangle + \beta|1\rangle$ avec α et β des nombres complexes non-nuls et tels que $|\alpha|^2 + |\beta|^2 = 1$. Puisque les nombres complexes forment un continuum on peut extraire une infinité de bits classiques lors d'une mesure *idéale*.
     Réponse:

2. (4.5 pts) Les matrices suivantes sont des *portes logiques quantiques* permises. Vrai ou faux ?

   - $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.
     Réponse:

   - $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.
     Réponse:

   - Une matrice 4×4 telle que $A^{-1} = A^\dagger$ (on rappelle la notation $A^\dagger = A^{T*}$).
     Réponse:

3. (3 pts) Est-il possible de construire des circuits quantiques avec les états initiaux et finaux suivants ? Oui ou non ? (on ne vous demande pas de montrer les éventuels circuits mais juste une courte justification)

   - Etat initial: $(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \otimes |0\rangle$, pour tous $\alpha, \beta \in \mathbb{C}^2$, $|\alpha|^2 + |\beta|^2 = 1$.
     Etat final: $(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$
     Réponse:

   - Etat initial: $(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle^{\otimes 8}$, pour tous $\alpha, \beta \in \mathbb{C}^2$, $|\alpha|^2 + |\beta|^2 = 1$.
     Etat final $\alpha|0\rangle_S + \beta|1\rangle_S$ avec

     $$|0\rangle_S = \frac{|000\rangle + |111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle + |111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

     et

     $$|1\rangle_S = \frac{|000\rangle - |111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle - |111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle - |111\rangle}{\sqrt{2}}.$$

     Réponse:

4. (4 pts) Représentez la porte controle-Z avec une porte CNOT et des portes de Hadamard $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. La porte Z pure est $\mathrm{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
   Réponse:

Solution du problème 4:

1.
   - faux (les portes à un et deux qubits suffisent)
   - vrai (un circuit quantique est unitaire donc réversible)
   - faux (on peut extraire au maximum un bit classique)

2.
   - vrai ce produit tensoriel est unitaire
   - faux le deuxième menbre du produit tensoriel est un projecteur non-unitaire.
   - vrai A est unitaire.

3.
   - non, à cause du no-cloning theorem.
   - oui, il s'agit du code de Shor pourlequel nous avons vu une implémentation par circuit unitaire

4. On peut montrer:

$$(I \otimes H)\mathrm{CNOT}(\mathrm{I} \otimes \mathrm{H}) = \mathrm{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

   Donc