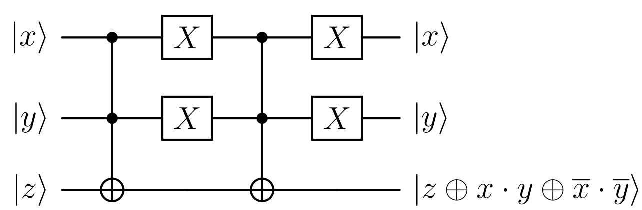
Solutions
Semaine 4

Cours Turing+

1 Circuit de Deutsch-Josza

a) En utilisant l'indication de l'énoncé, nous trouvons le circuit suivant pour la porte U_f :



b) Cette fonction f est balancée ; l'état $|0,0\rangle$ ne sort donc jamais, et les probabilités de sortie des trois autres états sont données par (cf. cours):

$$\text{prob}(0,1) = \left(\frac{1}{4}\sum_{x,y\in\{0,1\}}(-1)^{f(x,y)+y}\right)^2 = \left(\frac{1}{4}((-1)^1+(-1)^1+(-1)^0+(-1)^2)\right)^2 = 0$$

$$\text{prob}(1,0) = \left(\frac{1}{4}\sum_{x,y\in\{0,1\}}(-1)^{f(x,y)+x}\right)^2 = \left(\frac{1}{4}((-1)^1+(-1)^0+(-1)^1+(-1)^2)\right)^2 = 0$$

$$\text{prob}(1,1) = \left(\frac{1}{4}\sum_{x,y\in\{0,1\}}(-1)^{f(x,y)+x+y}\right)^2 = \left(\frac{1}{4}((-1)^1+(-1)^1+(-1)^1+(-1)^3)\right)^2 = 1$$

c) Pour cette nouvelle fonction f qui n'est ni constante, ni balancée (et pour laquelle la porte U_f est composée d'une seule porte de Toffoli encadrée par deux portes X pour chaque qubit $|x\rangle$ et $|y\rangle$), nous trouvons :

$$\text{prob}(0,0) = \left(\frac{1}{4}\sum_{x,y\in\{0,1\}}(-1)^{f(x,y)}\right)^2 = \left(\frac{1}{4}((-1)^1+(-1)^0+(-1)^0+(-1)^0)\right)^2 = \frac{1}{4}$$

$$\text{prob}(0,1) = \left(\frac{1}{4}\sum_{x,y\in\{0,1\}}(-1)^{f(x,y)+y}\right)^2 = \left(\frac{1}{4}((-1)^1+(-1)^1+(-1)^0+(-1)^1)\right)^2 = \frac{1}{4}$$

$$\text{prob}(1,0) = \left(\frac{1}{4}\sum_{x,y\in\{0,1\}}(-1)^{f(x,y)+x}\right)^2 = \left(\frac{1}{4}((-1)^1+(-1)^0+(-1)^1+(-1)^1)\right)^2 = \frac{1}{4}$$

$$\text{prob}(1,1) = \left(\frac{1}{4}\sum_{x,y\in\{0,1\}}(-1)^{f(x,y)+x+y}\right)^2 = \left(\frac{1}{4}((-1)^1+(-1)^1+(-1)^1+(-1)^2)\right)^2 = \frac{1}{4}$$

d) Si l'état observé en sortie est $|0,0\rangle$, alors nous savons en tout cas que la fonction n'est pas balancée. Ensuite, comme le montre l'exemple précédent, si f n'est ni constante, ni balancée, la probabilité d'observer l'état $|0,0\rangle$ en sortie vaut $1/4$, et vous pouvez vérifier que ce serait aussi le cas avec toute fonction qui prendrait trois fois la valeur 0 et une fois la valeur 1, ou au contraire trois fois la valeur 1 et une fois la valeur 0.

Remarque :* Pour aller plus loin, nous devons faire une hypothèse dite "bayesienne" sur la façon dont la fonction f est choisie au départ. Supposons donc que celle-ci soit choisie uniformément au hasard parmi les $2^4 = 16$ fonctions possibles : 2 fois sur 16, elle est constante ; 6 fois sur 16, elle est balancée, et 8 fois sur 16, elle est de la forme "1-3" ci-dessus. Donc par la règle de Bayes :

$$\text{prob}(f \text{ constante} \mid \text{sortie} = 0,0) = \frac{\text{prob}(f \text{ constante et sortie} = 0,0)}{\text{prob}(\text{sortie} = 0,0)}$$

$$= \frac{\text{prob}(\text{sortie} = 0,0 | f \text{ constante}) \cdot \text{prob}(f \text{ constante})}{\text{prob}(\text{sortie} = 0,0 | f \text{ constante}) \cdot \text{prob}(f \text{ constante}) + \text{prob}(\text{sortie} = 0,0 | f \text{ ``1-3''}) \cdot \text{prob}(f \text{ ``1-3''})}$$

$$= \frac{1 \cdot 1/8}{1 \cdot 1/8 + 1/4 \cdot 1/2} = \frac{1}{2}$$

Sans hypothèse sur f autre que celle d'être uniformément distribuée dans l'ensemble de toutes les fonctions possibles, observer l'état de sortie $|0,0\rangle$ ne nous donne donc pas beaucoup d'information sur la nature de celle-ci !

2 Algorithme de Bernstein-Vazirani

Le circuit quantique qui permet d'identifier les valeurs de a et b avec une seule évaluation de la fonction f est en fait strictement le même que le circuit de Deutsch-Josza !

En effet, selon le cours, pour le circuit de Deutsch-Josza, la probabilité de sortie de l'état $|u,v\rangle$ (avec $u,v \in \{0,1\}$) vaut

$$\text{prob}(u,v) = \left(\frac{1}{4}\sum_{x,y\in\{0,1\}}(-1)^{f(x,y)+u\cdot x+v\cdot y}\right)^2$$

En insérant ici la forme particulière de la fonction $f(x,y) = a \cdot x \oplus b \cdot y$, nous obtenons :

$$\text{prob}(u,v) = \left(\frac{1}{4}\sum_{x,y\in\{0,1\}}(-1)^{a\cdot x\oplus b\cdot y+x\cdot u+y\cdot v}\right)^2$$

Or il est possible de remplacer $\oplus$ par $+$ ci-dessus (en effet, la seule chose qui importe pour l'exposant de -1 est qu'il soit pair ou non), ce qui donne :

$$\text{prob}(u,v) = \left(\frac{1}{4}\sum_{x,y\in\{0,1\}}(-1)^{a\cdot x+b\cdot y+x\cdot u+y\cdot v}\right)^2 = \left(\frac{1}{4}\sum_{x,y\in\{0,1\}}(-1)^{(a+u)\cdot x+(b+v)\cdot y}\right)^2$$

Si $u = a$ et $v = b$, alors l'exposant est toujours pair et donc la probabilité vaut 1. Dans tous les autres cas, la probabilité vaut 0. Ainsi, l'état de sortie vaut, avec probabilité 1, $|u,v\rangle = |a,b\rangle$, c'est-à-dire exactement ce qu'on cherche !