Série 5
Traitement quantique de l'information II

Exercice 1 *Variation sur le problème de Simon*

Un qu-trit est un système quantique à 3 niveaux d'énergie. Les 3 états de base correspondants sont notés $|0\rangle$, $|1\rangle$ et $|2\rangle$. Un état général appartient à l'espace d'Hilbert $\mathbb{C}^3$,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle$$

avec $\alpha, \beta, \gamma \in \mathbb{C}$ et $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$. Soit $\mathbb{F}_3^n$ l'espace vectoriel des vecteurs $\vec{x} = (x_1, x_2, ..., x_n)$ à n composantes avec chaque composante prise $\bmod 3$. Le corps de l'espace vectoriel est $\mathbb{F}_3$ (entiers avec $+$ et $\times \bmod 3$). Soit H le sous-espace vectoriel

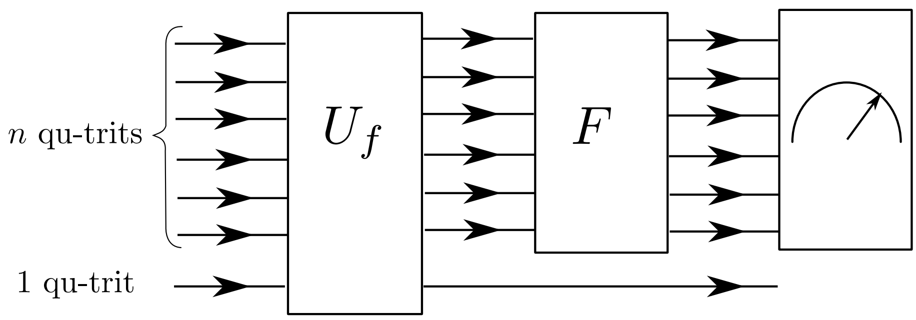
$$H = \left\{\vec{x} \in \mathbb{F}_3^n |\; \vec{x} = (0, \vec{x}') \text{ avec } \vec{x}' \in \mathbb{F}_3^{n-1}\right\}.$$

On se donne une fonction telle que

$$\begin{aligned} f : &\mathbb{F}_3^n \to \{0,1,2\} \\ &\vec{x} \longmapsto f(\vec{x}) \end{aligned}$$

avec $f(\vec{x}) = f(\vec{y})$ si et seulement si $\vec{x} - \vec{y} \in H$.

On considère le circuit quantique suivant :



– L'état d'entrée est initialisé à :

$$|\psi_{in}\rangle = \frac{1}{3^{n/2}} \sum_{\vec{x} \in \mathbb{F}_3^n} |\vec{x}\rangle \otimes |0\rangle$$

– La porte U_f (unitaire) est définie par

$$U_f\,|\vec{x}\rangle \otimes |y\rangle = |\vec{x}\rangle \otimes |y + f(\vec{x})\rangle \text{ avec } y = 0,1,2$$

Ici $y + f(\vec{x})$ est calculé $\bmod 3$.

– La porte F est une version de la transformée de Fourier quantique

$$F\,|\vec{x}\rangle = \frac{1}{3^{n/2}} \sum_{\vec{y}\in\mathbb{F}_3^n} \exp\left(\frac{2\pi i}{3}\vec{x}\cdot\vec{y}\right)|\vec{y}\rangle$$

où $\vec{x}\cdot\vec{y} = \sum_{i=1}^n x_i y_i \mod 3$.

a) Montrez que H est un sous-groupe de $\mathbb{F}_3^n$ pour l'addition $\bmod 3$. Donnez sa cardinalité. Montrez qu'il y a 3 classes d'équivalence de H dans $\mathbb{F}_3^n$ et donnez leur cardinalité.

b) Soit $\vec{a}, \vec{b}, \vec{c}$ des représentants des 3 classes d'équivalence avec $f(\vec{a}) = 0$, $f(\vec{b}) = 1$, $f(\vec{c}) = 2$. Montrez que l'état juste après la porte U_f est

$$U_f\,|\psi_{in}\rangle = \frac{1}{3^{n/2}} \sum_{\vec{x}\in H} \left\{ |\vec{a}+\vec{x}\rangle \otimes |0\rangle + \left|\vec{b}+\vec{x}\right\rangle \otimes |1\rangle + |\vec{c}+\vec{x}\rangle \otimes |2\rangle \right\}$$

c) Montrez que l'état juste après la porte F peut s'écrire :

$$(F\otimes\mathbb{I})\,U_f\,|\psi_{in}\rangle = \frac{1}{3} \sum_{y_1=0,1,2} |y_1, 0, ..., 0\rangle \otimes \left\{ e^{\frac{2\pi i}{3}y_1 a_1}|0\rangle + e^{\frac{2\pi i}{3}y_1 b_1}|1\rangle + e^{\frac{2\pi i}{3}y_1 c_1}|2\rangle \right\}$$

Indication : utilisez la formule

$$\sum_{\vec{x}\in H} \exp\left(\frac{2\pi i}{3}\vec{x}\cdot\vec{y}\right) = \begin{cases} 3^{n-1} & \text{si } \vec{y}\in H^\perp \\ 0 & \text{sinon} \end{cases}$$

Facultatif : prouvez cette formule.

d) Appliquez le postulat de la mesure sur les n premiers qu-trits et montrez que

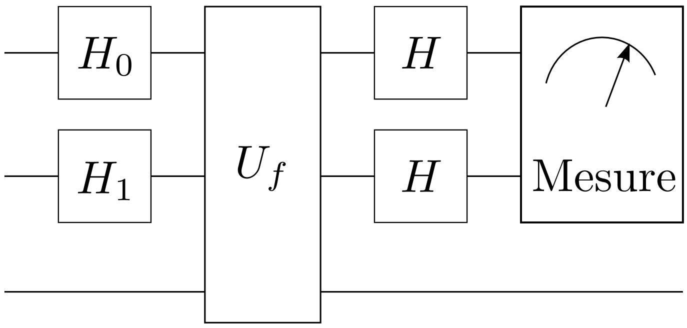
$$\Pr(\vec{y}) = \begin{cases} \frac{1}{3} & \text{si } \vec{y} = (y_1, 0, ..., 0) \text{ avec } y_1 = 0, 1, 2 \\ 0 & \text{sinon} \end{cases}$$

e) En admettant que H est un sous-groupe caché de dimension connue $n-1$, combien de mesures faut-il faire pour reconstruire H avec une probabilité de succès égale à $1-\varepsilon$ (ε très petit) ?

Exercice 2 *Effet des imperfections sur l'algorithme de Simon*

On considère le problème de Simon pour $n = 2$. Soit $H = \{\underline{x} \in \mathbb{F}_2^2 \mid \underline{x} = (0, x_2), \text{avec } x_2 \in \{0,1\}\}$. C'est le "sous-espace vectoriel caché" de $\mathbb{F}_2^2$. Soit $f : \mathbb{F}_2^2 \longrightarrow \{0,1\}$ telle que $f(\underline{x}) = f(\underline{y})$ si et seulement si $\underline{x} - \underline{y} \in H$. Pour fixer les idées on prendra la fonction $f(0,0) = f(0,1) = 0$ et $f(1,0) = f(1,1) = 1$.

Considérez le circuit (de l'algorithme de Simon) :



où H_0 et H_1 sont des portes de Hadamard *imparfaites* :

$$H_0 |b\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^b e^{i\phi_0} |1\rangle\right)$$
$$H_1 |b\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^b e^{i\phi_1} |1\rangle\right)$$

et ϕ_0 et ϕ_1 sont des phases dans $[0, 2\pi]$. Les deux dernières portes du circuit sont des portes de Hadamard standard

$$H |b\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^b |1\rangle\right)$$

et $U_f |x_1, x_2\rangle \otimes |z\rangle = |x_1, x_2\rangle \otimes |z \oplus f(x_1, x_2)\rangle$. Le circuit est initialisé à $|0,0\rangle \otimes |0\rangle$.

a) Calculez l'état juste après les deux premières portes de H_0 et H_1.

b) Calculez l'état après U_f, puis enfin calculez l'état juste après les deux dernières portes de Hadamard (c.à.d. juste avant la mesure).

c) On mesure les deux premiers qu-bits dans la base définie par les projecteurs

$$\left\{ |\underline{y}\rangle \langle \underline{y}| \otimes \mathbb{1} \;\middle|\; \underline{y} \in \{00, 01, 10, 11\} \right\}.$$

Le qu-bit de stockage n'est pas mesuré, ce qui est reflété par la matrice $\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Calculez les probabilités d'obtenir les états $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ juste après la mesure.

d) Deduire la probabilité de tomber sur un vecteur de $H^{\perp}$ et celle de tomber sur un vecteur de H. Pour quelles valeurs de ϕ_0 et ϕ_1 retrouve-t-on les cas où les portes de Hadamard sont parfaites ? Y a-t-il quelquechose d'étonnant dans vos resultats ?