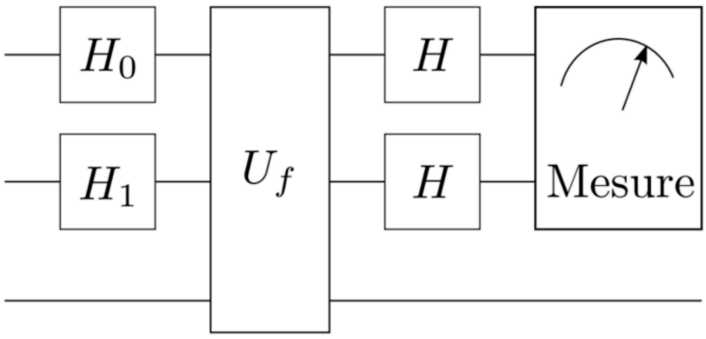
CS–308 — Calcul Quantique

Homework VI — François Dumoncel — 314420

Exercice 1. *Effet des imperfections sur l'algorithme de Simon*

On considère le problème de Simon pour $n = 2$. Soit $H = \{x \in \mathbb{F}_2^2 : x = (0, x_2), \text{ avec } x_2 \in \{0, 1\}\}$. C'est le "sous-espace vectoriel caché" de $\mathbb{F}_2^2$. Soit $f : \mathbb{F}_2^2 \to \{0, 1\}$ telle que $f(x) = f(y)$ si et seulement si $x - y \in H$. 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* :

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

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

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

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 $|0, 0\rangle \otimes |0\rangle$.

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

Solution. On calcule

$$\begin{aligned} |\Psi(t_1)\rangle &= (H_0 \otimes H_1 \otimes \mathbb{I})(|0\rangle \otimes |0\rangle \otimes |0\rangle) \\ &= \frac{|0\rangle + e^{i\phi_0} |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i\phi_1} |1\rangle}{\sqrt{2}} \otimes |0\rangle \\ &= \frac{1}{2}(|00\rangle + e^{i\phi_0} |10\rangle + e^{\phi_1} |01\rangle + e^{i(\phi_0+\phi_1)} |11\rangle) \otimes |0\rangle \end{aligned}$$

$$= \frac{1}{2} \sum_{\boldsymbol{x}=(x_0,x_1)\in\mathbb{F}_2^2} e^{i\boldsymbol{\phi}\cdot\boldsymbol{x}} |x\rangle \otimes |0\rangle$$

2. 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).

Solution. On calcule encore que

$$\begin{aligned} |\Psi(t_2)\rangle &= U_f |\Psi(t_1)\rangle \\ &= \frac{1}{2} \sum_{\boldsymbol{x}=(x_0,x_1)\in\mathbb{F}_2^2} e^{i\boldsymbol{\phi}\cdot\boldsymbol{x}} U_f |x\rangle \otimes |0\rangle \\ &= \frac{1}{2} \sum_{\boldsymbol{x}=(x_0,x_1)\in\mathbb{F}_2^2} e^{i\boldsymbol{\phi}\cdot\boldsymbol{x}} |x\rangle \otimes |f(\boldsymbol{x})\rangle \end{aligned}$$

et juste avant la mesure on a

$$\begin{aligned} |\Psi(t_3)\rangle &= (H^{\otimes 2} \otimes \mathbb{I}) |\Psi(t_2)\rangle \\ &= \frac{1}{2} \sum_{\boldsymbol{x}=(x_0,x_1)\in\mathbb{F}_2^2} e^{i\boldsymbol{\phi}\cdot\boldsymbol{x}} H^{\otimes 2} |x\rangle \otimes |f(\boldsymbol{x})\rangle \\ &= \frac{1}{2} \sum_{\boldsymbol{x}=(x_0,x_1)\in\mathbb{F}_2^2} e^{i\boldsymbol{\phi}\cdot\boldsymbol{x}} \left\{ \frac{1}{2} \sum_{\boldsymbol{y}=(y_0,y_1)\in\mathbb{F}_2^2} (-1)^{\boldsymbol{x}\cdot\boldsymbol{y}} |y\rangle \right\} \otimes |f(\boldsymbol{x})\rangle \end{aligned}$$

et en utilisant que $f(0,0) = f(0,1) = 0$ et $f(1,0) = f(1,1) = 1$ on a

$$\begin{aligned} |\Psi(t_3)\rangle &= \frac{1}{2} \left\{ \frac{1}{2} \sum_{\boldsymbol{y}=(y_0,y_1)\in\mathbb{F}_2^2} (-1)^{(0,0)^T\cdot\boldsymbol{y}} e^{i\boldsymbol{\phi}\cdot(0,0)^T} |y\rangle \right\} \otimes |f(0,0)\rangle \\ &+ \frac{1}{2} \left\{ \frac{1}{2} \sum_{\boldsymbol{y}=(y_0,y_1)\in\mathbb{F}_2^2} (-1)^{(1,0)^T\cdot\boldsymbol{y}} e^{i\boldsymbol{\phi}\cdot(1,0)^T} |y\rangle \right\} \otimes |f(1,0)\rangle \\ &+ \frac{1}{2} \left\{ \frac{1}{2} \sum_{\boldsymbol{y}=(y_0,y_1)\in\mathbb{F}_2^2} (-1)^{(0,1)^T\cdot\boldsymbol{y}} e^{i\boldsymbol{\phi}\cdot(0,1)^T} |y\rangle \right\} \otimes |f(0,1)\rangle \\ &+ \frac{1}{2} \left\{ \frac{1}{2} \sum_{\boldsymbol{y}=(y_0,y_1)\in\mathbb{F}_2^2} (-1)^{(1,1)^T\cdot\boldsymbol{y}} e^{i\boldsymbol{\phi}\cdot(1,1)^T} |y\rangle \right\} \otimes |f(1,1)\rangle \\ &= \left\{ \frac{1}{4} \sum_{\boldsymbol{y}=(y_0,y_1)\in\mathbb{F}_2^2} |y\rangle \right\} \otimes |0\rangle + \left\{ \frac{1}{4} \sum_{\boldsymbol{y}=(y_0,y_1)\in\mathbb{F}_2^2} (-1)^{y_0} e^{i\phi_0} |y\rangle \right\} \otimes |1\rangle \\ &+ \left\{ \frac{1}{4} \sum_{\boldsymbol{y}=(y_0,y_1)\in\mathbb{F}_2^2} (-1)^{y_1} e^{i\phi_1} |y\rangle \right\} \otimes |0\rangle + \left\{ \frac{1}{4} \sum_{\boldsymbol{y}=(y_0,y_1)\in\mathbb{F}_2^2} (-1)^{y_0+y_1} e^{i(\phi_0+\phi_1)} |y\rangle \right\} \otimes |1\rangle \end{aligned}$$

ce qui se ré-écrit

$$
\begin{aligned}
|\Psi(t_3)\rangle &= \left\{ \frac{1}{4} \sum_{\boldsymbol{y}=(y_0,y_1)\in\mathbb{F}_2^2} (1+(-1)^{y_1} e^{i\phi_1}) \right\} |y\rangle \otimes |0\rangle + \left\{ \frac{e^{i\phi_0}}{4} \sum_{\boldsymbol{y}=(y_0,y_1)\in\mathbb{F}_2^2} ((-1)^{y_0} + (-1)^{y_0+y_1} e^{i\phi_1}) \right\} |y\rangle \otimes |1\rangle \\
&= \frac{1}{4}((1+e^{i\phi_1})\,|00\rangle + (1-e^{i\phi_1})\,|01\rangle + (1+e^{i\phi_1})\,|10\rangle + (1-e^{i\phi_1})\,|11\rangle)) \otimes |0\rangle \\
&+ \frac{e^{i\phi_0}}{4}((1+e^{i\phi_1})\,|00\rangle + (1-e^{i\phi_1})\,|01\rangle - (1+e^{i\phi_1})\,|10\rangle - (1-e^{i\phi_1})\,|11\rangle) \otimes |1\rangle
\end{aligned}
$$

3. On mesure les deux premiers qu-bits dans la base définie par les projecteurs

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

Le qubit de stockage n'est pas mesuré, ce qui est reflété par la matrice $\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Calculez les probabilités d'obtenir les états $|00\rangle, |10\rangle, |01\rangle, |11\rangle$ juste après la mesure.

Solution. On a que

$$
\begin{aligned}
\mathbb{P}(\boldsymbol{y}=(0,0)) &= \left|\frac{1+e^{i\phi_1}}{4}\right|^2 + \left|\frac{e^{i\phi_0}(1+e^{i\phi_1})}{4}\right|^2 = \frac{2}{16}|1+e^{i\phi_1}|^2 = \frac{1}{2}\cos^2\left(\frac{\phi_1}{2}\right) \\
\mathbb{P}(\boldsymbol{y}=(0,1)) &= \left|\frac{1-e^{i\phi_1}}{4}\right|^2 + \left|\frac{e^{i\phi_0}(1-e^{i\phi_1})}{4}\right|^2 = \frac{2}{16}|1-e^{i\phi_1}|^2 = \frac{1}{2}\sin^2\left(\frac{\phi_1}{2}\right) \\
\mathbb{P}(\boldsymbol{y}=(1,0)) &= \left|\frac{1+e^{i\phi_1}}{4}\right|^2 + \left|\frac{e^{i\phi_0}(1+e^{i\phi_1})}{4}\right|^2 = \frac{2}{16}|1+e^{i\phi_1}|^2 = \frac{1}{2}\cos^2\left(\frac{\phi_1}{2}\right) \\
\mathbb{P}(\boldsymbol{y}=(1,1)) &= \left|\frac{1-e^{i\phi_1}}{4}\right|^2 + \left|\frac{e^{i\phi_0}(1-e^{i\phi_1})}{4}\right|^2 = \frac{2}{16}|1-e^{i\phi_1}|^2 = \frac{1}{2}\sin^2\left(\frac{\phi_1}{2}\right)
\end{aligned}
$$

et notons que

$$\sum_{\boldsymbol{y}=(y_0,y_1)\in\mathbb{F}_2^2} \mathbb{P}(\boldsymbol{y}) = \cos^2\left(\frac{\phi_1}{2}\right) + \sin^2\left(\frac{\phi_1}{2}\right) = 1.$$

4. Déduire 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 quelque chose d'étonnant dans vos résultats ?

Solution. Rappelons que

$$H = \left\{ \boldsymbol{x} \in \mathbb{F}_2^2 \;\middle|\; \boldsymbol{x} = (0,x_2), \text{ avec } x_2 \in \{0,1\} \right\}$$

On calcule facilement que

$$
\begin{aligned}
H^\perp &= \left\{ \boldsymbol{x} \in \mathbb{F}_2^2 \;\middle|\; \forall \boldsymbol{y} \in H,\ \langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0 \right\} \\
&= \left\{ \boldsymbol{x} \in \mathbb{F}_2^2 \;\middle|\; \forall \boldsymbol{y} \in H,\ \langle (x_1,x_2), (0,y_2) \rangle = 0 \right\}
\end{aligned}
$$

$$= \left\{ \boldsymbol{x} \in \mathbb{F}_2^2 \;\middle|\; \forall \boldsymbol{y} \in H,\ x_2 y_2 = 0 \right\}$$
$$= \left\{ \boldsymbol{x} \in \{(0,0)^T, (1,0)^T\} \right\}$$

On a donc que

$$\mathbb{P}(\boldsymbol{y} \in H) = \mathbb{P}(\boldsymbol{y} = (0,1) \cup \boldsymbol{y} = (1,1)) = \frac{1}{2}\sin^2\left(\frac{\phi_1}{2}\right) + \frac{1}{2}\sin^2\left(\frac{\phi_1}{2}\right) = \sin^2\left(\frac{\phi_1}{2}\right)$$
$$\mathbb{P}(\boldsymbol{y} \in H^\perp) = \mathbb{P}(\boldsymbol{y} = (0,0) \cup \boldsymbol{y} = (1,0)) = \frac{1}{2}\cos^2\left(\frac{\phi_1}{2}\right) + \frac{1}{2}\cos^2\left(\frac{\phi_1}{2}\right) = \cos^2\left(\frac{\phi_1}{2}\right)$$

encore une fois on observe bien que

$$\mathbb{P}(\boldsymbol{y} \in H) + \mathbb{P}(\boldsymbol{y} \in H^\perp) = 1.$$

L'algorithme de Simon, sans les portes de Hadamard imparfaites donne comme résultat

$$\mathbb{P}(\boldsymbol{y}) = \begin{cases} \dfrac{1}{2^{2-1}} = \dfrac{1}{2} & \text{si } \boldsymbol{y} \in H^\perp, \\ 0 & \text{si } \boldsymbol{y} \in H. \end{cases}$$

On retrouve ce résultat classique lorsque $\phi_1 = 0$ et $\phi_2 \in [0, 2\pi]$. Ce résultat peut paraître étonnant, car il montre qu'en fait on peut réaliser l'algorithme de Simon avec des portes de Hadamard imparfaites, tant et aussi longtemps que ces dernières n'affectent pas les probabilités d'observer un vecteur $\boldsymbol{y}$ de $H^\perp$.

Exercise 2 *Variation sur le problème de Simon*

Un qu-trit est un système quantique à 3 "niveaux d'énergies" (c'est l'analogue quantique du trit classique). Les 3 états de base orthonormés correspondants sont notés $|0\rangle$, $|1\rangle$ et $|2\rangle$. Un état général appartient à l'espace d'Hilbert 3-dimensionnel $\mathbb{C}^3$,

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

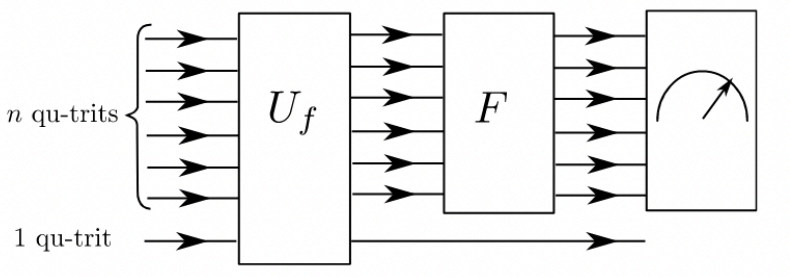
avec $\alpha, \beta, \gamma \in \mathbb{C}$ et $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$. Soit $\mathbb{F}_3^n$ l'espace vectoriel des vecteurs $\boldsymbol{x} = (x_1, x_2, ..., x_n)$ à n composantes avec chaque composante prise modulo 3. Le corps de l'espace vectoriel est $\mathbb{F}_3$ (entiers avec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

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

On se donne une fonction telle que

$$f : \mathbb{F}_3^n \to \{0,1,2\}$$
$$\boldsymbol{x} \mapsto f(\boldsymbol{x})$$

avec $f(\boldsymbol{x}) = f(\boldsymbol{y})$ si et seulement si $\boldsymbol{x} - \boldsymbol{y} \in H$. On considère le circuit quantique suivant :



L'état d'entrée est initialisé à :

$$|\psi\rangle = \frac{1}{\sqrt{3^n}} \sum_{\boldsymbol{x}\in\mathbb{F}_3^n} |x\rangle \otimes |0\rangle \,.$$

La porte U_f (unitaire) est définie par

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

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

$$F \,|x\rangle = \frac{1}{\sqrt{3^n}} \sum_{\boldsymbol{x}\in\mathbb{F}_3^n} \exp\left\{\frac{2\pi i}{3}\boldsymbol{x}\cdot\boldsymbol{y}\right\} |y\rangle \,.$$

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

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

Solution. Le fait que 3 soit un nombre premier, assure que le groupe $\mathbb{F}_3^n$ est un *corps*. Il est donc en particulier abélien et cela fait du groupe H, un sous groupe normal : $H \lhd \mathbb{F}_3^n$. Il est également facile de voir que $(H, +)$ est un sous-groupe de $\mathbb{F}_3^n$.

- H contient $\boldsymbol{e} = (0, \ldots, 0) \in \mathbb{F}_3^n$
- H est stable par produit et inverses

$$\begin{aligned} \forall \boldsymbol{x}, \boldsymbol{y} \in H, \quad \boldsymbol{x} + \boldsymbol{y}^{-1} &= (0, \boldsymbol{x'}) + (0, (\boldsymbol{y'})^{-1}) \\ &= (0, \boldsymbol{x'} + (\boldsymbol{y'})^{-1}) \\ &= (0, \boldsymbol{z'}) \in H. \end{aligned}$$

Notons que $|\mathbb{F}_3^n| = 3^n$. Il est facile de voir que le quotient de $\mathbb{F}_3^n$ par H partitionne $\mathbb{F}_3^n$ en 3 classes d'équivalences qui sont

$$\begin{aligned} C_0 &= \left\{ \boldsymbol{x} \in \mathbb{F}_3^n \;\middle|\; \boldsymbol{x} = (0, \boldsymbol{x'}),\ \text{avec } \boldsymbol{x'} \in \mathbb{F}_3^{n-1} \right\} \\ C_1 &= \left\{ \boldsymbol{y} \in \mathbb{F}_3^n \;\middle|\; \boldsymbol{y} = (1, \boldsymbol{y'}),\ \text{avec } \boldsymbol{y'} \in \mathbb{F}_3^{n-1} \right\} \\ C_2 &= \left\{ \boldsymbol{z} \in \mathbb{F}_3^n \;\middle|\; \boldsymbol{z} = (2, \boldsymbol{z'}),\ \text{avec } \boldsymbol{z'} \in \mathbb{F}_3^{n-1} \right\}. \end{aligned}$$

On voit que $C_0 = H$, ce qui implique que $|H| = \frac{1}{3}|G| = 3^{n-1}$, ceci est également vrai pour C_1 et C_2. Le théorème de Lagrange permet de retrouver ce résultat

$$|\mathbb{F}_3^n / H| = \frac{|\mathbb{F}_3^n|}{|H|} = \frac{3^n}{3^{n-1}} = 3$$

qui est bien égal au nombre de classe à gauche de H dans $\mathbb{F}_3^n$ décrite ci-dessus.

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

$$U_f |\psi\rangle = \frac{1}{\sqrt{3^n}} \sum_{\boldsymbol{x} \in H} \Big\{ |a + x\rangle \otimes |0\rangle + |b + x\rangle \otimes |1\rangle + |c + x\rangle \otimes |2\rangle \Big\}.$$

Solution. H partitionne $\mathbb{F}_3^n$ de telle sorte que

$$\mathbb{F}_3^n = C_0 \cup C_1 \cup C_2.$$

Quotienter par H nous donne aussi que pour toute les classes d'équivalence, peu importe le représentant choisi, celui ci engendre toujours la totalité de la classe i.e :

$$\begin{aligned} C_0 &= \{\boldsymbol{a} + \boldsymbol{h}, \boldsymbol{h} \in H\} \\ C_1 &= \{\boldsymbol{b} + \boldsymbol{h}, \boldsymbol{h} \in H\} \\ C_2 &= \{\boldsymbol{c} + \boldsymbol{h}, \boldsymbol{h} \in H\} \end{aligned}$$

Donc on a que

$$\begin{aligned} U_f |\psi\rangle &= \frac{1}{\sqrt{3^n}} \sum_{\boldsymbol{x} \in \mathbb{F}_3^n} U_f |x\rangle \otimes |0\rangle \\ &= \frac{1}{\sqrt{3^n}} \sum_{\boldsymbol{h} \in H} U_f \Big\{ |a + h\rangle \otimes |0\rangle + |b + h\rangle \otimes |0\rangle + |c + h\rangle \otimes |0\rangle \Big\} \\ &= \frac{1}{\sqrt{3^n}} \sum_{\boldsymbol{h} \in H} \Big\{ |a + h\rangle \otimes |f(\boldsymbol{a})\rangle + |b + h\rangle \otimes |f(\boldsymbol{b})\rangle + |c + h\rangle \otimes |f(\boldsymbol{c})\rangle \Big\} \\ &= \frac{1}{\sqrt{3^n}} \sum_{\boldsymbol{h} \in H} \Big\{ |a + h\rangle \otimes |0\rangle + |b + h\rangle \otimes |1\rangle + |c + h\rangle \otimes |2\rangle \Big\} \end{aligned}$$

Remplaçez $\boldsymbol{h}$ par $\boldsymbol{x}$ pour retrouver le résultat attendu.

3. Montrez que l'état juste après la porte F peut s'écrire :

$$(F \otimes \mathbb{I}) U_f |\psi\rangle = \frac{1}{3} \sum_{y_1 = 0,1,2} |y_1, 0, \ldots 0\rangle \otimes \Big\{ e^{\frac{2\pi i}{3} y_1 a_1} + e^{\frac{2\pi i}{3} y_1 b_1} + e^{\frac{2\pi i}{3} y_1 c_1} \Big\}$$

Indication : utilisez la formule

$$\sum_{\boldsymbol{x} \in H} \exp\left\{ \frac{2\pi i}{3} \boldsymbol{x} \cdot \boldsymbol{y} \right\} = \begin{cases} 3^{n-1} & \text{si } \boldsymbol{y} \in H^\perp, \\ 0 & \text{si } \boldsymbol{y} \notin H^\perp. \end{cases}$$

Prouvez cette formule avec une méthode analogue à celle vue en cours sur $\mathbb{F}_2$

Solution. On commence par prouver l'indication :

- Si $\boldsymbol{y} \in H^\perp$ alors $\boldsymbol{x} \cdot \boldsymbol{y} = 0$ et on a

$$\sum_{\boldsymbol{x}\in H} \exp\left\{\frac{2\pi i}{3}\boldsymbol{x}\cdot\boldsymbol{y}\right\} = \sum_{\boldsymbol{x}\in H} 1 = |H| = 3^{n-1}$$

- Si $\boldsymbol{y} \notin H^\perp$ alors il existe $\boldsymbol{x}_0 \in H$ tel que $\boldsymbol{x}_0 \cdot \boldsymbol{y} = 1, 2$ car H est un sous-espace vectoriel sur le corps $\mathbb{F}_3$. En utilisant le l'invariance de H au changement de variable $\boldsymbol{x} = \boldsymbol{x'} + \boldsymbol{x}_0$ on obtient

$$\begin{aligned}\sum_{\boldsymbol{x}\in H} \exp\left\{\frac{2\pi i}{3}\boldsymbol{x}\cdot\boldsymbol{y}\right\} &= \sum_{\boldsymbol{x'}\in H} \exp\left\{\frac{2\pi i}{3}(\boldsymbol{x'}+\boldsymbol{x}_0)\cdot\boldsymbol{y}\right\} \\ &= \exp\left(\frac{2\pi i}{3}\boldsymbol{x}_0\cdot\boldsymbol{y}\right)\sum_{\boldsymbol{x'}\in H} \exp\left\{\frac{2\pi i}{3}\boldsymbol{x'}\cdot\boldsymbol{y}\right\}\end{aligned}$$

  En regroupant les termes et en factorisant on trouve que

$$\left(1 - \exp\left(\frac{2\pi i}{3}\boldsymbol{x}_0\cdot\boldsymbol{y}\right)\right)\sum_{\boldsymbol{x}\in H} \exp\left\{\frac{2\pi i}{3}\boldsymbol{x}\cdot\boldsymbol{y}\right\} = 0$$

  Observons maintenant que facteur devant la somme ne vaut jamais 0. En effet

$$1 - \exp\left(\frac{2\pi i}{3}\boldsymbol{x}_0\cdot\boldsymbol{y}\right) = 0 \iff \exp\left(\frac{2\pi i}{3}\boldsymbol{x}_0\cdot\boldsymbol{y}\right) = 1$$

  mais comme le produit scalaire $\boldsymbol{x}_0\cdot\boldsymbol{y} = 1, 2$ on a alors que l'exponentiel du membre de gauche ne vaut jamais 1, si bien que le produit

$$\left(1 - \exp\left(\frac{2\pi i}{3}\boldsymbol{x}_0\cdot\boldsymbol{y}\right)\right)\sum_{\boldsymbol{x}\in H} \exp\left\{\frac{2\pi i}{3}\boldsymbol{x}\cdot\boldsymbol{y}\right\}$$

  est nul car

$$\sum_{\boldsymbol{x}\in H} \exp\left\{\frac{2\pi i}{3}\boldsymbol{x}\cdot\boldsymbol{y}\right\} = 0$$

□

Avant de montrer la formule demandée, il convient de caractériser $H^\perp$

$$\begin{aligned}H^\perp &= \left\{\boldsymbol{x}\in\mathbb{F}_3^n \;\middle|\; \forall \boldsymbol{y}\in H,\ \langle \boldsymbol{x},\boldsymbol{y}\rangle = 0\right\} \\ &= \left\{\boldsymbol{x}\in\mathbb{F}_3^n \;\middle|\; \forall \boldsymbol{y}\in H,\ (x_1,\boldsymbol{x'})\cdot(0,\boldsymbol{y'}) = 0\right\} \\ &= \left\{\boldsymbol{x}\in\mathbb{F}_3^n \;\middle|\; \forall \boldsymbol{y}\in H,\ \boldsymbol{x'}\cdot\boldsymbol{y'} = 0\right\}\end{aligned}$$

ce qui implique que

$$H^\perp = \left\{\boldsymbol{y}\in\mathbb{F}_3^n \;\middle|\; \boldsymbol{y} = (y_1, 0, \ldots, 0),\ \text{avec } y_1 \in \{0,1,2\}\right\}$$

Calculons maintenant l'état final juste avant la mesure

$$
\begin{aligned}
(F\otimes\mathbb{I})U_f\left|\psi\right\rangle &= \frac{1}{\sqrt{3^n}}\sum_{\boldsymbol{x}\in H}\Big\{F\left|a+h\right\rangle\otimes\left|0\right\rangle + F\left|b+h\right\rangle\otimes\left|1\right\rangle + F\left|c+h\right\rangle\otimes\left|2\right\rangle\Big\}\\
&= \left(\frac{1}{\sqrt{3^n}}\right)^2\sum_{\boldsymbol{x}\in H}\left\{\sum_{\boldsymbol{y}\in\mathbb{F}_3^n} e^{\frac{2\pi i}{3}(\boldsymbol{a}+\boldsymbol{x})\cdot\boldsymbol{y}}\left|y0\right\rangle + e^{\frac{2\pi i}{3}(\boldsymbol{b}+\boldsymbol{x})\cdot\boldsymbol{y}}\left|y1\right\rangle + e^{\frac{2\pi i}{3}(\boldsymbol{c}+\boldsymbol{x})\cdot\boldsymbol{y}}\left|y2\right\rangle\right\}\\
&= \frac{3^{n-1}}{3^n}\sum_{\boldsymbol{y}\in H^\perp} e^{\frac{2\pi i}{3}\boldsymbol{a}\cdot\boldsymbol{y}}\left|y0\right\rangle + e^{\frac{2\pi i}{3}\boldsymbol{b}\cdot\boldsymbol{y}}\left|y1\right\rangle + e^{\frac{2\pi i}{3}\boldsymbol{c}\cdot\boldsymbol{y}}\left|y2\right\rangle \qquad \textit{(indication)}\\
&= \frac{1}{3}\sum_{\boldsymbol{y}\in H^\perp}\left|y\right\rangle\otimes\left\{e^{\frac{2\pi i}{3}\boldsymbol{a}\cdot\boldsymbol{y}}\left|0\right\rangle + e^{\frac{2\pi i}{3}\boldsymbol{b}\cdot\boldsymbol{y}}\left|1\right\rangle + e^{\frac{2\pi i}{3}\boldsymbol{c}\cdot\boldsymbol{y}}\left|2\right\rangle\right\}\\
&= \frac{1}{3}\sum_{y_1=0,1,2}\left|y_1,0,\ldots,0\right\rangle\otimes\left\{e^{\frac{2\pi i}{3}a_1y_1}\left|0\right\rangle + e^{\frac{2\pi i}{3}b_1y_1}\left|1\right\rangle + e^{\frac{2\pi i}{3}c_1y_1}\left|2\right\rangle\right\} \qquad \textit{(caractérisation de } H^\perp\textit{)}\\
&= \left|\Phi\right\rangle
\end{aligned}
$$

qui était le résultat attendu.

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

$$\mathbb{P}(\boldsymbol{y}) = \begin{cases}\frac{1}{3} & \text{si } \boldsymbol{y} = (y_1,0,\ldots,0),\\ 0 & \text{sinon.}\end{cases}$$

Solution. En appliquant le principe de la mesure à l'état final avec le projecteur suivant

$$\left|y\right\rangle\left\langle y\right|\otimes\mathbb{I}, \qquad \text{avec } \left|y\right\rangle = \left|y_1,0,\ldots,0\right\rangle.$$

on a que

$$
\begin{aligned}
\left\langle\Phi\right|(\left|y\right\rangle\left\langle y\right|\otimes\mathbb{I})\left|\Phi\right\rangle &= \left\langle\Phi\;\middle|\;\left(\frac{1}{3}\left|y_1,0,\ldots,0\right\rangle\otimes\left\{e^{\frac{2\pi i}{3}a_1y_1}\left|0\right\rangle + e^{\frac{2\pi i}{3}b_1y_1}\left|1\right\rangle + e^{\frac{2\pi i}{3}c_1y_1}\left|2\right\rangle\right\}\right)\right.\\
&= \frac{1}{9}(e^{\frac{2\pi i}{3}a_1y_1}e^{-\frac{2\pi i}{3}a_1y_1} + e^{\frac{2\pi i}{3}b_1y_1}e^{-\frac{2\pi i}{3}b_1y_1} + e^{\frac{2\pi i}{3}c_1y_1}e^{-\frac{2\pi i}{3}c_1y_1})\\
&= \frac{3}{9} = \frac{1}{3}.
\end{aligned}
$$

5. 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 $1-\epsilon$ (ϵ très petit) ?

Solution. Si $\dim H = n-1$ alors $\dim H^\perp = 1$. En mesurant l'état on observe forcément

$$\begin{cases}(0,0,\ldots,0) & \text{avec probabilité } \frac{1}{3}\\ (1,0,\ldots,0) & \text{avec probabilité } \frac{1}{3}\\ (2,0,\ldots,0) & \text{avec probabilité } \frac{1}{3}\end{cases}$$

Un échec arrive lorsque la mesure révèle le vecteur $(0,0,\ldots,0)$, nous empêchant de déterminer $H^\perp$. Les deux autres vecteurs nous permettent de déterminer $H^\perp$ et donc H. Soit $\epsilon \ll 1$. Soit $T \gg 0$,

le nombre de run

$$\begin{aligned}\mathbb{P}(\text{au moins un succès en } T \text{ runs}) &= 1 - \mathbb{P}(\text{au plus 1 échec en } T \text{ runs}) \\ &= 1 - (1 - \mathbb{P}(\text{succès en un run}))^T \\ &= 1 - \left\{1 - \left(\frac{2}{3}\right)\right\}^T \\ &= 1 - \left(\frac{1}{3}\right)^T\end{aligned}$$

et donc on trouve que

$$\mathbb{P}(\text{succès}) = 1 - \epsilon = 1 - \left(\frac{1}{3}\right)^T \iff T = \frac{|\log \epsilon|}{|\log \frac{1}{3}|}.$$

Exercise 3 *Implementation of Simon's algorithm*

In this exercise, you will implement Simon's Algorithm to find a hidden subspace H of codewords within the vector space $\mathbb{F}_2^n$ of binary strings of length n. The dimension of the hidden subspace is $k = 4$. To implement the algorithm, you are given an oracle whose function is to apply the parity check matrix P to any binary vector $v\boldsymbol{v}$ of length $n = 7$, where $P\boldsymbol{v} = 0$ if and only if $\boldsymbol{v} \in$ the hidden subspace H. In other words, consider two vectors $\boldsymbol{v}_1, \boldsymbol{v}_2$, $P(\boldsymbol{v}_1 - \boldsymbol{v}_2) = 0$ iff $(\boldsymbol{v}_1 - \boldsymbol{v}_2) \in H$. The parity check matrix P is given by

$$P = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

You are asked to implement a notebook in the Qiskit language to implement Simon's algorithm circuit for this oracle (see https ://quantum-computing.ibm.com/). Make a jupyter notebook using Qiskit. Run it on the simulator only.

Initialisation du notebook

```
# initialization
import matplotlib.pyplot as plt
import numpy as np

#%pip install qiskit
#%pip install pylatexenc

# importing Qiskit
from qiskit import IBMQ, Aer
from qiskit.providers.ibmq import least_busy
from qiskit import QuantumCircuit, ClassicalRegister, QuantumRegister, transpile, assemble
from qiskit.quantum_info.operators import Operator, Pauli
from qiskit import IBMQ, Aer
from qiskit.providers.ibmq import least_busy
from qiskit import QuantumCircuit, transpile, assemble

# import basic plot tools
from qiskit.visualization import plot_histogram
```

1. How many qubits does your circuit need in total ?

Solution. Puisque $\dim H = 4$ on a que $\dim H^\perp = 3$. Donc nous allons avoir besoin de $n+(n-k) = 10$ qubits.

2. Which of those will be measured ?

Solution. Seulement les 7 premiers qubits vont être mesurés.

3. How many shots (at least) do you need to run the circuit ? In other words, how many linearly independent output vectors do you need to determine the hidden subspace ? Don't forget to check that the output vectors are linearly independent !

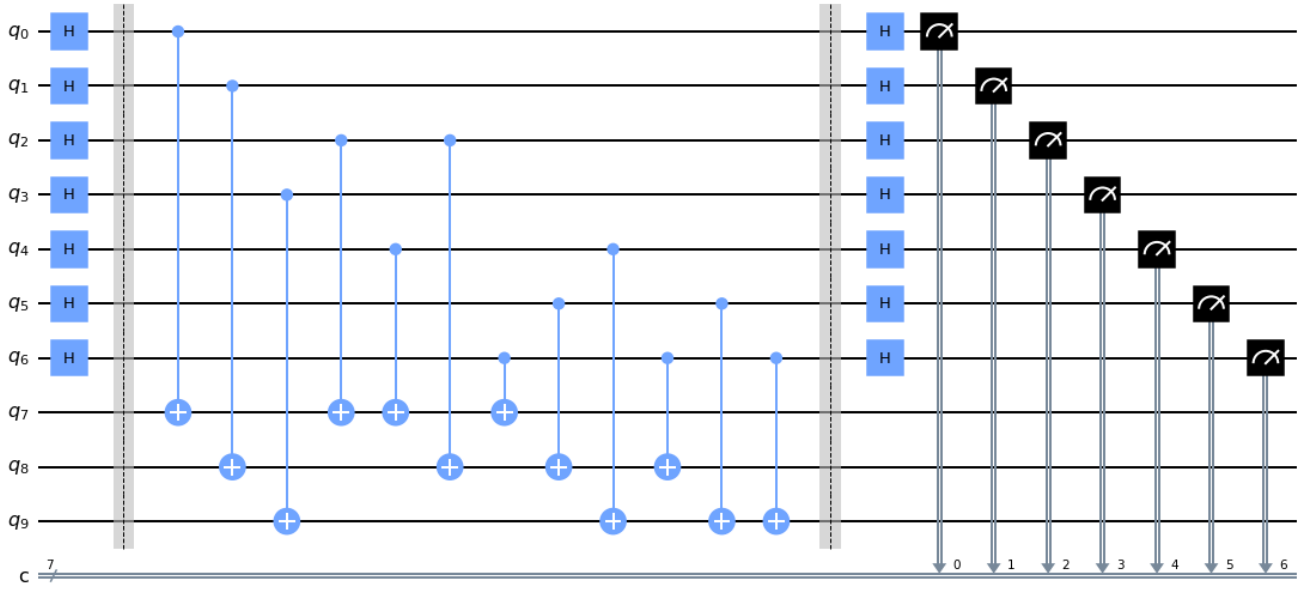
Solution. Une base de $H^\perp$ possède 3 vecteurs linéairement indépendants. Donc, avec un peu de chance, il nous faudra seulement 3 runs de l'algorithme pour déterminer complétement $H^\perp$ et donc H.

4. It suffices to run the simulator and real device to get the basis vectors of the orthogonal subspace $H^\perp$ (you don't have to do Gaussian elimination).

Solution.

```
n = 7
k = 3

simon_circ = QuantumCircuit(n + k, n)

# First level of hadamard gates :
#     Put the qbits in a coherent superposition of all possible states
for i in range(n):
    simon_circ.h(i)

simon_circ.barrier()

# ORACLE (constructed with P)
####################
simon_circ.cx(0, 7)
simon_circ.cx(2, 7)
simon_circ.cx(4, 7)
simon_circ.cx(6, 7)

simon_circ.cx(1, 8)
simon_circ.cx(2, 8)
simon_circ.cx(5, 8)
simon_circ.cx(6, 8)

simon_circ.cx(3, 9)
simon_circ.cx(4, 9)
simon_circ.cx(5, 9)
simon_circ.cx(6, 9)
####################

simon_circ.barrier()

# Second  level of hadamard gates :
#     Fourier Analysis
for i in range(n):
    simon_circ.h(i)

# Measurement of all n-qubit
for i in range(n):
    simon_circ.measure(i, i)

simon_circ.draw('mpl')
```

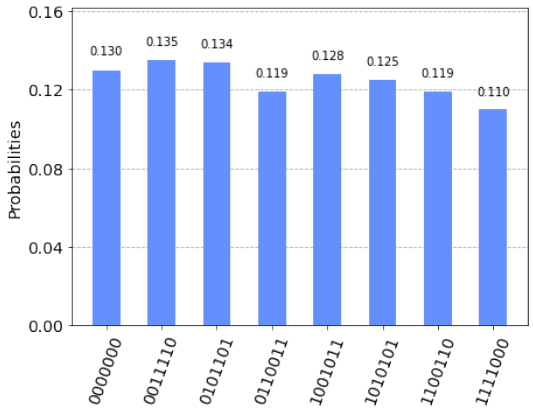
ce qui donne le circuit suivant



En executant l'algorithme sur un simulateur

```
# Running on simulator
aer_sim = Aer.get_backend('aer_simulator')
shots = 1
qobj = assemble(simon_circ)
results = aer_sim.run(qobj).result()
answer = results.get_counts()

plot_histogram(answer)
```

on trouve



et on vérifie que les vecteurs trouvés forment bien une base de $H^{\perp}$

```
matrix_result = [
                 [0, 1, 1, 1, 1, 0, 0],
                 [1, 0, 1, 1, 0, 1, 0],
                 [1, 1, 0, 0, 1, 1, 0],
                 [1, 1, 0, 1, 0, 0, 1],
                 [1, 0, 1, 0, 1, 0, 1],
                 [0, 1, 1, 0, 0, 1, 1],
                 [0, 0, 0, 1, 1, 1, 1],
                ]

# To see that the result are linearly independent
assert(np.linalg.det(matrix_result) != 0)

H = np.matrix(
    [
      [1, 1, 1, 0, 0, 0, 0],
      [1, 0 ,0 ,1 ,1 ,0 ,0],
      [0, 1, 0, 1, 0, 1, 0],
      [1, 1, 0, 1, 0, 0, 1]
    ])

y_1 = np.array([0, 1, 1, 1, 1, 0, 0])
y_2 = np.array([1, 0, 1, 1, 0, 1, 0])
y_3 = np.array([1, 1, 0, 0, 1, 1, 0])

assert(np.array_equal(H.dot(y_1.T)%2, [[0,0,0,0]]))
assert(np.array_equal(H.dot(y_2.T)%2, [[0,0,0,0]]))
assert(np.array_equal(H.dot(y_3.T)%2, [[0,0,0,0]]))
```