Portes et circuits quantiques

Pierre FIMA

Contents

1 Introduction

Le but de cet exposé est de présenter les principes fondamentaux du calcul quantique. Le concept fondamental de l'information classique est le bit. L'information quantique est construite à partir d'un concept analogue, le bit quantique ou qubit. Un bit classique possède un état, 0 ou (exclusif) 1, de même, un qubit possède un état. La différence réside dans le fait qu'il est également possible de considérer des combinaisons linéaires d'états, parfois appelées superpositions :

$$\mid \psi\rangle = \alpha \mid 0\rangle + \beta \mid 1\rangle$$

où α et β sont deux nombres complexes tels que $\mid \alpha \mid^2 + \mid \beta \mid^2 = 1$. Lorsque l'on mesure l'état de ce qubit on trouve 0 avec une probabilité $\mid \alpha \mid^2$ ou (exclusif) 1 avec une probabilité $\mid \beta \mid^2$. Après la mesure, le qubit devient un bit classique. C'est cette superposition d'états qui permet la résolution rapide de problèmes considérés comme "difficiles" en information classique (voir par exemple l'algorithme de Grover dans [2]).

Dans le premier chapitre on décrira en détail le modèle fondamental du calcul quantique: les circuits quantiques. On définira tout d'abord les qubits puis l'analogue des portes logiques, les portes quantiques. Enfin, on cherchera un ensemble de portes permettant l'implémentation de toutes les portes quantiques ainsi qu'une estimation de la longueur des circuits nécessaire à l'implémentation. On verra alors une autre différence entre l'information classique et l'information quantique : en information classique, lorsque l'on cherche toutes les opérations possibles pour transformer un n-bit en un n-bit, c'est à dire toutes les applications de $\{0,1\}^n$ dans $\{0,1\}^n$ on trouve un nombre fini. On verra qu'en information quantique l'ensemble des opérations sur les n-qubits est indénombrable. Comment alors réaliser toutes les opérations sur les n-qubits à partir d'un ordinateur quantique qui n'aurait que des possibilités finies ? La solution consiste à faire des approximations de portes quantiques avec une erreur arbitrairement petite. C'est l'objet du second chapitre. On définira d'abord la notion d'approximation puis on cherchera un ensemble fini de portes permettant l'approximation de toutes les portes quantiques avec une erreur arbitrairement petite. Enfin, on cherchera, étant donnée une erreur ϵ, une majoration de la longueur d'un circuit minimum nécessaire pour l'implémentation de toutes les portes à ϵ près. On verra que le coût sur la longueur pour un gain de précision n'est que d'un facteur logarithmique en ϵ !

2 Portes quantiques, circuits quantiques, bases universelles

2.1 Qubits, portes quantiques

Dans toute la suite on fixe M un opérateur hermitien agissant sur $\mathbb{C}^2$ et ayant deux valeurs propres distinctes . Soit (v_0, v_1) une base orthonormée associée à la décomposition spectrale de M et Π_0, Π_1 les projecteurs spectraux.

$M^{\otimes n}$ est hermitien, agit sur $\mathbb{C}^{2^{\otimes n}}$ et possède 2^n valeurs propres distinctes. La base $(v_{\bar{k}})_{\bar{k}\in\{0,1\}^n}$ où $v_{\bar{k}} = v_{i_1}\otimes\ldots\otimes v_{i_n}$, $\bar{k} = (i_1, \ldots, i_n)$ est une base orthonormée de $\mathbb{C}^{2^{\otimes n}}$ associée à la décomposition spectrale de $M^{\otimes n}$. On note $\Pi_{\bar{k}}$ les projecteurs spectraux.

Dans ces conditions, on pose :

Définition 1 *Un n-qubit est un vecteur de $\mathbb{C}^{2\otimes n}$ de norme 1.*

Tout ψ n-qubit induit une mesure de probabilité sur l'ensemble $\{0,1\}^n$ des n-bits donnée par :

$$P_\psi(\bar{k}) := \|\Pi_{\bar{k}}\psi\|^2 \ , \ \bar{k} \in \{0,1\}^n.$$

En particulier, si $\psi_1 \sim \psi_2$ mod $\mathbb{U}(1)$ (ie. $\psi_1 = \lambda\psi_2$ avec $\mid \lambda \mid = 1$) alors $P_{\psi_1} = P_{\psi_2}$ et si $U \sim V$ mod $\mathbb{U}(1)$ où U, $V \in \mathbb{U}(2^n)$ alors $\forall\, \psi$ n-qubits on a $P_{U\psi} = P_{V\psi}$. Cette remarque conduit à la définition suivante :

Définition 2 *Une porte quantique à n entrées est un élément de $\mathbb{U}(2^n)/\mathbb{U}(1)$.*

On utilisera la notation de Dirac :
Si ψ est un vecteur on le note $\mid \psi\rangle$. Le produit tensoriel est noté $\psi \otimes \phi = \mid \psi\phi\rangle$ et v_0, v_1 sont notés respectivement $\mid 0\rangle$, $\mid 1\rangle$. Cette notation est assez ambigue mais elle permet de noter des indices comme des vecteurs.

En mécanique quantique, l'espace d'état d'un système physique est un espace de Hilbert $\mathcal{H}$, l'état du système est un vecteur de norme 1 dans $\mathcal{H}$. La dynamique quantique est décrite par un opérateur unitaire agissant sur $\mathcal{H}$ et vérifiant l'équation de Schrödinger. Une mesure sur $\mathcal{H}$ est la donnée d'une famille $(M_i)_{i\in I}$ d'opérateurs linéaires sur $\mathcal{H}$ vérifiants $\sum_{i\in I} M_i M_i^* = 1$. L'ensemble I correspond aux différents résultats possibles. Si le système est dans l'état Ψ_0 alors la probabilité que le résultat de la mesure soit i est $P(i) = \|M_i\Psi_0\|^2$, la condition de normalisation sur les M_i assure que P est bien une mesure de probabilité sur I. Après la mesure, le système a évolué et se trouve dans l'état $\Psi_1 = \frac{M_i\Psi_0}{\|M_i\Psi_0\|}$. Ces postulats assurent que le résultat d'une mesure est aléatoire c'est à dire que l'on peut, en mesurant plusieurs fois un même un système physique dans un même état avec la même mesure trouver des résultats différents. La seule chose que l'on connait est la probabilité de trouver un résultat donné. Un cas particulier de la mesure est la mesure projective : c'est la donnée d'un opérateur hermitien M sur $\mathcal{H}$. Si l'on note $M = \sum_{\lambda\in Sp(M)} \lambda P_\lambda$ la décomposition spectrale de M où $Sp(M)$ est le spectre de M et P_λ le projecteur associé à la valeur propre λ alors la famille $(P_\lambda)_{\lambda\in Sp(M)}$ est une mesure car $\sum_{\lambda\in Sp(M)} P_\lambda P_\lambda^* = 1$. Si maitenant on a deux systèmes physique d'espaces d'états $\mathcal{H}_1$ et $\mathcal{H}_2$ alors le système physique global a pour espace d'état $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Dans notre cas particulier, un qubit correspond à l'état d'un système physique d'espace d'états $\mathcal{H} = \mathbb{C}^2$. L'opérateur M introduit précédemment correspond à une mesure projective avec deux résultats différents possibles (pour l'existence des qubits voir l'expérience de Stern et Gerlach dans [2]). Un qubit est une superposition d'états classiques 0 et 1 :

$$\mid \psi\rangle = \alpha \mid 0\rangle + \beta \mid 1\rangle, \quad \mid \alpha \mid^2 + \mid \beta \mid^2 = 1.$$

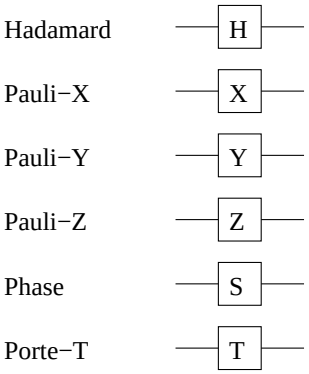
Le résultat de la mesure d'un tel ψ est 0 avec une probabilité $\mid \alpha \mid^2$ ou 1 avec une probabilité $\mid \beta \mid^2$. Après la mesure le qubit est dans l'état $\mid i\rangle$ où i correspond au résultat de la mesure. Si deux opérateurs unitaires U et V appartiennent à la même porte quantique alors quelque soit l'état initial du système, le faire évoluer à l'aide de U ou de V ne change pas les probabilités des résultats de la mesure du nouvel état.

2.2 Exemples de portes et de circuits

Dans toute la suite, on écrit les matrices dans la base $(|\ \overline{k}\rangle)_{\overline{k}\in\{0,1\}^n}$, où les $\overline{k}$ sont ordonnés dans l'ordre croissant en base deux. Cette base est appelée base de calcul. Par exemple si $n = 2$ la base de calcul est (e_1, e_2, e_3, e_4) où $e_1 =| 00\rangle$, $e_2 =| 01\rangle$, $e_3 =| 10\rangle$,et $e_4 =| 11\rangle$.

2.2.1 Portes quantiques simples

Voici des représentant de portes quantiques classiques : Soit $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$, $X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, $Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$, $Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$, $S = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$ et $T = \begin{pmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}}\end{pmatrix}$. On schématise par :



2.2.2 Porte U-Contrôlé

En informatique classique, on utilise des opérations qui contrôlent l'état d'un ou plusieurs bits et qui, suivant l'état des bits contrôlés effectuent (ou n'effectuent pas) une opération sur d'autres bits. L'exemple typique est le $CNOT$. Il agit sur un 2-bits et échange le dernier bit si et seulement si le premier est dans l'état 1. On peut définir des opérations analogues en informatique quantique.

Définition 3 *Soit $U \in \mathbb{U}(2^n)$. On appelle U-contrôlé à k qubits de contrôle et n qubits de cible l'opérateur $\Lambda^k U$ défini par :*

$$\Lambda^k U := \begin{pmatrix}1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & U\end{pmatrix}.$$

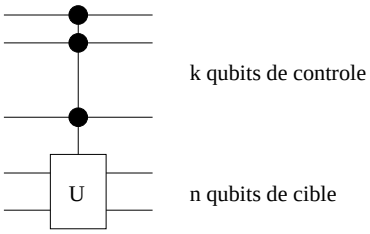
La matrice est donnée dans la base de calcul définie précédemment, elle agit donc sur l'espace vectoriel engendré par la famille :

$$(|\ 1\dots1\ \underbrace{0\dots0}_{n-qubits}\rangle, |\ 1\dots1\ \underbrace{0\dots0}_{(n-1)-qubits}\ 1\rangle, \dots, |\ 1\dots1\rangle)$$

Son action sur la base de calcul est donc donnée par :

$$\Lambda^k U(|\ x_1 \dots x_k x_{k+1} \dots x_{n+k}\rangle) = |\ x_1 \dots x_k U^{x_1 \dots x_k}(|\ x_{k+1} \dots x_{k+n}\rangle)\rangle$$

i.e, U agit sur les n derniers qubits de la base de calcul si et seulement si les k premiers sont tous à $|\ 1\rangle$. On schématise $\Lambda^k U$ par :



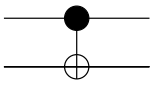
Cas particuliers :

- $\boldsymbol{CNOT = \Lambda^1 X}$

  C'est l'opérateur : $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. Il agit sur la base de calcul par :

  $$\Lambda^1 X(|\ 00\rangle) = |\ 00\rangle,\ \Lambda^1 X(|\ 01\rangle) = |\ 01\rangle,\ \Lambda^1 X(|\ 10\rangle) = |\ 11\rangle,\ \Lambda^1 X(|\ 11\rangle) = |\ 10\rangle.$$

  Il échange donc le dernier qubit de la base de calcul si et seulement si le premier est à $|\ 1\rangle$. On schématise par :



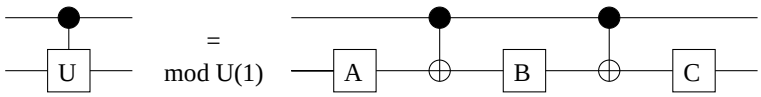
- $\boldsymbol{\Lambda^1 U,\ U \in \mathbb{U}(2)}$

  Le cas général à un qubit de contrôle se simplifie par l'exercice suivant :

  Exercice : *Soit $U \in \mathbb{U}(2)$, $\exists\ A,\ B,\ C \in \mathbb{U}(2)$ et $\alpha \in \mathbb{R}$ tels que :*

  $$U = e^{i\alpha} AXBXC \ et\ ABC = I.$$

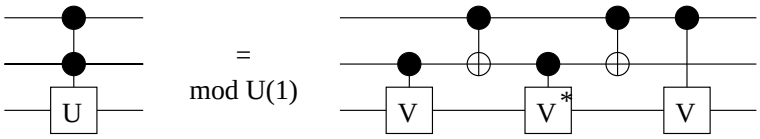
  On en déduit :



  De plus le circuit de droite utilise 5 portes de l'ensemble $\mathbb{U}(2) \cup \{CNOT\}$. On dira que la longueur L est 5 à partir de $\mathbb{U}(2) \cap \{CNOT\}$ (pour une définition générale de la longueur, voir la définition 5).

- $\boldsymbol{\Lambda^2 U,\ U \in \mathbb{U}(2)}$

  On voit facilement que :



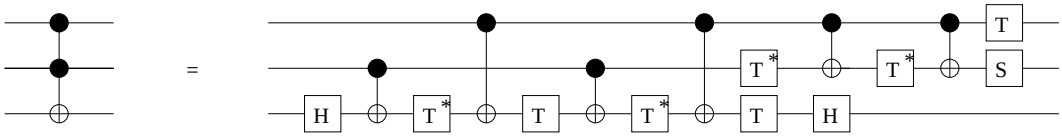
où $V \in \mathbb{U}(2),\ V^2 = U$.

$L = 5$ à partir de $\{\Lambda^1 U,\ U \in \mathbb{U}(2)\} \cup \{CNOT\}$.

$L = 17$ à partir de $\mathbb{U}(2) \cup \{CNOT\}$. Le circuit de $\Lambda^2(U)$ parait plus simple que $\Lambda^1(U)$ car le fait de contrôler sur deux niveaux permet de choisir quand appliquer V^* pour revenir à l'identité.

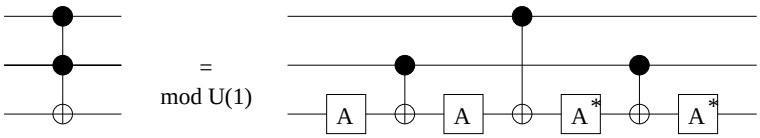
- **Toffoli : $\Lambda^2 X$**

  En faisant tourner à la main le circuit, on peut vérifier que :



$L = 16$ à partir de $\{H, T, CNOT, S\}$.

De même, on vérifie que :



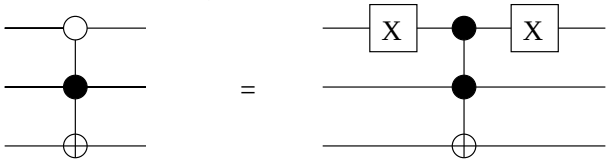
où $A = \begin{pmatrix} \cos(\frac{\pi}{8}) & -\sin(\frac{\pi}{8}) \\ \sin(\frac{\pi}{8}) & \cos(\frac{\pi}{8}) \end{pmatrix}$

$L = 7$ à partir de $A \cup \{CNOT\}$.

2.2.3 CNOT à contrôle inversé, CNOT mixte

La définition est la même mais cette fois ci, on échange le dernier qubit si et seulement si le premier est à $|\,0\rangle$:

De même, on définit le $Cnot$ mixte :



2.3 Circuits quantiques

Dans cette section, on donne une définition formelle de la notion intuitive de circuit quantique.

Définition 4 *Une base est un sous-ensemble de* $\bigcup_{n\in\mathbb{N}} \mathbb{U}(2^n)$.

On note I_n l'identité sur $M_n(\mathbb{C})$. Soit $n,\ r \in \mathbb{N}^*$ avec $r \leq n$. Si $X \in M_2(\mathbb{C})$, on note $X[r] = I_{r-1} \otimes X \otimes I_{n-r} \in M_n(\mathbb{C})$. Si X est unitaire, alors $X[p]$ l'est aussi. Si X est un opérateur unitaire sur $\mathbb{C}^{2\otimes r}$ on le décompose en une somme finie : $\sum_m X_{1,m} \dots X_{r,m}$ où $X_{i,m} \in M_2(\mathbb{C})$. Soit $A \subset \{1, \dots, n\}$ ordonné, de cardinal r. On pose $X[A] = \sum_m X_{1,m}[p_1] \dots X_{r,m}[p_r] \in \mathbb{U}(2^n)$ où $A = \{p_1, \dots, p_r\}$.

Intuitivement, $X[A]$ correspond à une étape d'un circuit à n-entrées où l'on choisi de faire agir X sur les r lignes définies par A et de ne rien faire sur les $n - r$ autres lignes du circuit.

On peut maitenant formaliser la notion de circuit quantique :

Définition 5 *Soit $\mathcal{A}$ une base. Un circuit de $\mathcal{A}$, à n-entrées et de longueur L est une suite finie :*

$$C = (U_1[A_1], \dots, U_L[A_L])$$

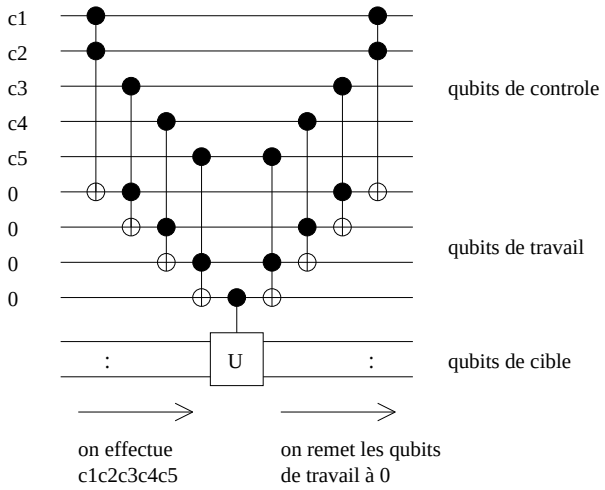
où $\forall\, i,\ 1 \leq i \leq L,\ U_i \in \mathcal{A} \cap \mathbb{U}(2^{CardA_i}),\ CardA_i \leq n.$

$W = U_L[A_L] \dots U_1[A_1]$ est l'opérateur réalisé par C. On dit alors que la porte quantique P dont W est un représentant est réalisée par C.

Un opérateur U est implémenté par $\mathcal{A}$ si il existe un circuit C de $\mathcal{A}$ qui réalise U. On dit alors que la porte quantique P dont U est un représentant est implémentée par $\mathcal{A}$.

Pour accélérer certaines opérations on utilise souvent en informatique classique des bits de travails. Le problème de la définition précédente est qu'elle ne permet pas l'utilisation de qubits de travail. Avant de définir la notion de qubits de travail construisons un circuit qui en utilise.

Pour réaliser $\Lambda^k U$ dans le cas général, on utilise le circuit suivant à $k - 1$ qubits de travail (représenté ici dans le cas où $k = 5$) :



On peut facilement vérifier que l'implémentation est bonne. On utilise $2(k-1)$ portes Toffoli et une porte $\Lambda^1 U$. Donc, si $U \in \mathbb{U}(2)$, $L = 2(k-1) \times 7 + 5 = 14k - 9 = O(k)$ à partir de $\mathbb{U}(2) \cup \{CNOT\}$

Si on fait du contrôle mixte, aux points de contrôle inversé il faut rajouter X avant et après. Si on a parmis les k qubits de contrôle, p qubits ($p \leq k$) de contrôle inversé, on rajoute $2p$ portes X donc :

$L = 14k + 2p - 9 \leq 16k - 9 = O(k)$ à partir de $\mathbb{U}(2) \cup \{CNOT\}$, et toujours $k-1$ qubits de travail.

On pose donc :

Définition 6 *Soit $\mathcal{A}$ une base et $U \in \mathbb{U}(2^n)$. On dit que U est implémenté par $\mathcal{A}$ avec p qubits de travail si il existe $W \in \mathbb{U}(2^{n+p})$ implémenté par $\mathcal{A}$ tel que :*

$$\forall \mid \xi\rangle \in \mathbb{C}^{2\otimes n},\ W(\mid \xi\rangle \otimes \mid 0^p\rangle) = U(\mid \xi\rangle) \otimes \mid 0^p\rangle.$$

où $\mid 0^p\rangle = \mid \underbrace{0 \ldots 0}_{p\ fois}\rangle$.

Remarque :

Il est important que les qubits de travail reviennent à l'état $\mid 0^p\rangle$ afin de pouvoir mesurer le résultat. En effet si à la sortie d'un tel circuit on obtient un état $\mid \xi^{'}\rangle \otimes \mid \phi\rangle$ où $\mid \phi\rangle$ est inconnu, on ne peut pas effectuer de mesure sur $\mid \xi^{'}\rangle$ par contre si on obtient un état $\mid \xi^{'}\rangle \otimes \mid 0^p\rangle$ alors la probabilité que le résultat de la mesure sur $\mid \xi^{'}\rangle \otimes \mid 0^p\rangle$ soit $x_1 \ldots x_n \underbrace{0 \ldots 0}_{p\ fois}$ (où $x_i \in \{0,1\}$) est égale à la probabilité que le résultat de la mesure sur $\mid \xi^{'}\rangle$ soit $x_1 \ldots x_n$.

2.4 Bases universelles

Il nous faut maintenant trouver des ensemble de portes qui permettent l'implémentation de toutes les portes quantiques. C'est l'objet de cette section.

Soit $\mathcal{A}$ une base. On note $C(\mathcal{A})$ l'ensemble des circuits de $\mathcal{A}$.

Définition 7 *Une base $\mathcal{A}$ est dite universelle si pour toute porte quantique P il existe $C \in C(\mathcal{A})$ réalisant P (avec ou sans qubits de travail).*

Le thérème suivant est le résultat principal de ce chapitre. Il permet de se ramener aux portes quantiques simples et au $CNOT$ pour l'implémentation de toutes les portes quantiques. Il donne également une majoration de la longueur minimale nécessaire pour l'implémentation d'une porte quantique quelconque à partir des portes simples et du $CNOT$.

Théorème 8 *La base $\mathcal{A} = \mathbb{U}(2) \cup \{CNOT\}$ est universelle. De plus pour tout entier naturel $n \geq 3$, pour toute porte quantique P à n-entrées, $\exists C \in C(\mathcal{A})$ réalisant P avec $n-2$ qubits de travail et de longeur $L = O(4^n n^2)$.*

Démonstration.

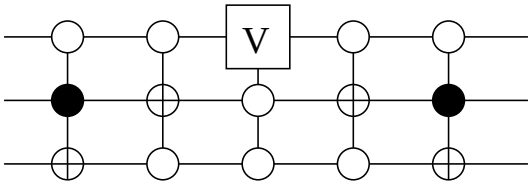
Voyons d'abord l'implémentation sur un exemple :

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & b & 0 & 0 & 0 \\ 0 & 0 & 0 & c & d & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Soit $V = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. U agit sur $<| 011\rangle, | 100\rangle >$. On construit une suite de 3-bits joignant 011 à 100 et dans laquelle 2 3-bits consécutifs diffèrent en exactement un bit :

A	B	C
0	1	1
0	1	0
0	0	0
1	0	0

On construit alors un circuit à partir de $\{V, CNOT\}$ en utilisant la suite de 3-bits que l'on vient de construire. La première porte du circuit est un $CNOT$ mixte de cible le bit C qui diffèrent entre les deux premiers termes de la suite. Le contrôle porte sur les deux autres bits, c'est un contrôle inversé lorsque les deux sont égaux à 0, c'est à dire en A, c'est un contrôle classique lorsque les deux sont égaux à 1, en B. L'autre $CNOT$ est construit de la même facon en comparant le second et le troisième 3-bits de la suite. Enfin en comparant le dernier et l'avant dernier 3-bit de la suite on construit le V-contrôlé mixte, la cible étant sur le bit A qui diffère, et le contrôle inversé ou simple est choisi comme précédemment. Enfin on replace les deux mêmes $CNOT$ mixtes mais dans l'ordre inverse.



On vérifie facilement que ce circuit réalise U.

Cela nous amène à la définition suivante :

Définition 9 *Soit s et t deux n-bits. Un Gray code de s à t est une suite finie de n-bits $(g_1, \ldots, g_m)$ où $g_1 = s$, $g_m = t$, et $\forall\, i \in \{1, \ldots, m-1\}$, g_i et g_{i+1} diffèrent en exactement un bit.*

Dans le cas plus général d'un opérateur à deux niveau, si $U \in \mathbb{U}(2^n)$ agit sur $| s\rangle, | s+1\rangle$ on construit un Gray code de s à $s+1$. Comme s et $s+1$ diffèrent d'au plus n-bits on peut trouver un Gray code de s à $s+1$ de longueur $m \leq n+1$. On prend celui-ci. On construit alors un circuit à n-entrées et de longueur $2(m-2)+1$ de la facon suivante :

Pour $1 \leq i \leq m-2$, la $i^{ème}$ porte du circuit est un $CNOT$ mixte, la cible étant le bit qui diffère entre g_i et g_{i+1} et les $n-1$ qubits de contrôle étant les bits restants (égaux entre eux dans g_i et g_{i+1}), contrôlés par 0 si ils sont égaux à 0 ou bien par 1 si ils sont égaux à 1. La $(m-1)^{ième}$

porte est alors un $\tilde{U}$ contrôlé, où $\tilde{U} \in \mathbb{U}(2)$ correspond aux deux niveaux de U, la cible étant le bit qui diffère entre g_{m-1} et g_m, les autres qubits sont des qubits de contrôle (mixte) définis comme précédemment. Enfin, les $m-2$ dernières portes du circuit sont les mêmes que les $m-2$ premières, en inversant l'ordre des portes.

On a donc $2(m-2) \leq 2(n-1) = O(n)$ $CNOT$ mixtes dont l'implémentation est en $O(n)$ et utilisant $n-2$ qubits de travail à partir de $\mathcal{A}$ et un $\Lambda^{n-1}(\tilde{U})$ dont l'implémentation est également en $O(n)$ et utilise aussi $n-2$ qubits de travail à partir de $\mathcal{A}$. Soit un circuit de longueur $O(n^2)$ et utilisant $n-2$ qubits de travail pour l'implémentation d'un opérateur à deux niveaux.

Si maintenant $U \in \mathbb{U}(2^n)$ quelconque, on le décompose en un produit d'opérateurs à deux niveaux par le lemme suivant :

Lemme 10 *Soit $M \geq 2$ et $U \in \mathbb{U}(M)$. Il existe $U_1, \ldots, U_k \in \mathbb{U}(M)$ de la forme :*

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & a & b & & \\ & & c & d & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}$$

tels que $U = U_1 \ldots U_k$ et $k = \frac{M(M-1)}{2}$.

Démonstration.

Soit $(v_1, \ldots, v_M)$ une base orthonormée de $\mathbb{C}^M$. En remarquant que :

$$\forall\, c_1,\, c_2 \in \mathbb{C},\, \exists V \in \mathbb{U}(2),\, V \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} \sqrt{|\, c_1 \,|^2 + |\, c_2 \,|^2} \\ 0 \end{pmatrix}$$

on déduit par une récurrence immédiate que :

$$\forall \xi \in \mathbb{C}^M,\, \|\xi\| = 1,\, \exists V^{(M-1)}, \ldots, V^{(1)} \in \mathbb{U}(M),\, V^{(1)} \ldots V^{(M-1)}(\xi) = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

où $V^{(s)}$ agit sur $< v_s, v_{s+1} >$.

Soit maintenant $U \in \mathbb{U}(M)$. La première colonne de U^{-1} est un vecteur de $\mathbb{C}^M$ de norme 1 donc $\exists V^{(1,1)}, \ldots, V^{(1,M-1)} \in \mathbb{U}(M)$, où $V^{(1,s)}$ agit sur $< v_s, v_{s+1} >$ tels que :

$$V^{(1,1)} \ldots V^{(1,M-1)} U^{-1} = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{pmatrix}$$

On termine par récurrence et on trouve $V^{(j,s)}$, $1 \leq j \leq s \leq M-1$, $V^{(j,s)}$ agit sur $< v_s, v_{s+1} >$ et :

$$V^{(M-1,M-1)}(V^{(M-2,M-2)} V^{(M-2,M-1)}) \ldots (V^{(1,1)} \ldots V^{(1,M-1)}) U^{-1} = I.$$

Les matrices $V^{(j,s)}$ sont de la forme demandée et il y en a $\frac{M(M-1)}{2}$.

■

Pour finir la démonstration du théorème, on se donne $U \in \mathbb{U}(2^n)$ quelconque, on a $U = U_1 \dots U_k$ avec U_i à deux niveaux et $k = 2^{n-1}(2^n - 1) = O(4^n)$. Soit pour implémenter U un circuit de longueur $O(4^n n^2)$ et $n-2$ qubits de travail d'après ce qui précède.

■

Remarque :

Il est possible d'implémenter $\Lambda^k(U)$ où $U \in \mathbb{U}(2)$ en $O(n^2)$ à partir de $\mathbb{U}(2) \cup \{CNOT\}$ sans utiliser de qubits de travail (cf. [1]). L'implémentation de $U \in \mathbb{U}(2^n)$ quelconque se fait alors sans qubits de travail mais en $O(4^n n^3)$.

Exercice : *Soit $\mathcal{A}$ une base. Supposons que $\exists\, n \in \mathbb{N}^*, \exists\, M > 0$ tels que toute porte quantique à n-entrées soit implémentable par $\mathcal{A}$ avec un nombre de qubits de travail borné par M. Alors $\mathcal{A}$ est indénombrable.*

Remarque :

Supposons que les ordinateurs quantiques existent. Les capacités d'un tel ordinateur seraient finies. Il serait munit d'une base finie $\mathcal{A}$ et d'un nombre d'entrées k maximum de ses circuits fini. Il ne pourrait, bien sûr, réaliser que des opérateurs de taille $l \leq k$. L'exercice précédent nous dit que $\forall\, n \in \mathbb{N}^*$, en particulier $\forall\, n \leq k$, il existe une porte quantique à n-entrées qui n'est pas implémentable par $\mathcal{A}$.

3 Approximation de portes quantiques, bases finies complètes

Dans le chapitre précédent, on a vu qu'une base finie n'est pas universelle. L'objet de ce chapitre est de définir la notion d'approximation de porte quantique (section 3.1) afin de construire une base finie permettant l'approximation de toutes les portes quantiques avec une erreur arbitrairement petite (section 3.2). Enfin, on cherchera une estimation de la longueur minimum nécessaire à l'approximation d'une porte quantique quelconque avec une erreur ϵ donnée (section 3.3).

3.1 Définitions

Soit $U, V \in \mathbb{U}(2^n)$, $\psi \in \mathbb{C}^{2\otimes n}$ et $\bar{k} \in \{0,1\}^n$. Posons $\delta = (U - V)\psi$ on a :

$$| P_{U\psi}(\bar{k}) - P_{V\psi}(\bar{k}) | = | (\Pi_{\bar{k}} U\psi, \Pi_{\bar{k}} U\psi) - (\Pi_{\bar{k}} V\psi, \Pi_{\bar{k}} V\psi) | = | (\delta, \Pi_{\bar{k}} U\psi) + (V\psi, \Pi_{\bar{k}}\delta) | \leq 2\|\delta\| \leq 2\|U - V\|$$

où $\|U - V\|$ est la norme d'opérateurs classique.

Ce calcul nous conduit à la :

Définition 11

1. *Soit U et $\tilde{U} \in \mathbb{U}(2^n)$. On dit que $\tilde{U}$ est une approximation de U à ϵ près si $\|U - \tilde{U}\| < \epsilon$.*
2. *Soit $U \in \mathbb{U}(2^n)$ et $W \in \mathbb{U}(2^{n+p})$. On pose :*

$$A : \mathbb{C}^{2\otimes n} \to \mathbb{C}^{2\otimes(n+p)}, \quad |\psi\rangle \mapsto |\psi\rangle \otimes |0^p\rangle.$$

On dit que W est une approximation de U à ϵ près et p qubits de travail si $\|WA - AU\| < \epsilon$.

3. *On dit qu'un circuit C est une approximation à ϵ près d'un opérateur U (respectivement d'une porte quantique P) si l'opérateur implémenté par C est une approximation de U à ϵ près (respectivement d'un représentant de P).*

4. *Une base $\mathcal{A}$ est dite complète si $\forall\, P$ porte quantique, $\forall\, \epsilon > 0$, $\exists\, C \in C(\mathcal{A})$ approximation de P à ϵ près (avec ou sans qubits de travail).*

La proposition suivante nous dit que l'erreur s'accumule linéairement.

Proposition 12 *Soit $U_1, \ldots, U_k, W_1, \ldots, W_k \in \mathbb{U}(2^n)$ on a :*

$$\|(U_1 \ldots U_k) - (W_1 \ldots W_k)\| \leq \sum_{i=1}^{k} \|U_i - W_i\|$$

Démonstration.
C'est une récurrence évidente car :

$$\|U_1U_2 - W_1W_2\| = \|(U_1 - W_1)(U_2) + (W_1)(U_2 - W_2)\|$$

et si $U \in \mathbb{U}(2^k)$, $\|U\| = 1$.

■

Proposition 13 *Soit $A \subset \mathbb{U}(2)$ tel que $A^{-1} := \{U^{-1}, U \in A\} \subset \mathbb{U}(1)A$ et $\overline{< A \cup \mathbb{U}(1) >} = \mathbb{U}(2)$; alors la base $A \cup \{CNOT\}$ est complète.*

Démonstration.
C'est un corrolaire du théorème 8. En effet, soit $n \in \mathbb{N}^*$, $\epsilon > 0$ et P une porte quantique à n-entrées on peut trouver $C = (U_1[A_1], \ldots, U_L[A_L]) \in C(\mathbb{U}(2) \cup \{CNOT\})$ réalisant P. $\forall\, i$, $1 \leq i \leq L$ tels que $U_i \in \mathbb{U}(2)$ on peut trouver $\phi \in \mathbb{R}$ et $W_i = V_{i,1} \ldots V_{i,k_i}$ tels que $e^{i\phi}W_i$ est une approximation de U_i à $\frac{\epsilon}{L}$ près et $V_{i,j} \in A$. Pour les i tels que $U_i = CNOT$, on pose $W_i = CNOT$. On pose $\tilde{C} = (W_1[A_1], \ldots, W_L[A_L]) \in C(A \cup \{CNOT\})$. En remarquant que l'on a toujours $\|X[p] - Y[p]\| = \|X - Y\|$, où $X, Y \in M_2(\mathbb{C})$ et $p \leq n$ et en utilisant l'accumulation linéaire de l'erreur (voir proposition 12) on conclut.

■

Construisons maintenant un exemple de base finie complète.

3.2 Bases finies complètes

Soit $E = \{M \in M_2(\mathbb{C}),\, hermitiennes,\, de\, trace\, nulle\}$. C'est un espace euclidien de dimension 3. Le produit scalaire est $< A, B >= \frac{1}{2}Tr(AB)$, et la famille (X, Y, Z) (matrices de Pauli) est une base orthonormée. $\mathbb{U}(2)$ agit sur E par :

$$U.P = UPU^{-1},\ U \in \mathbb{U}(2),\, P \in E$$

. Cette action induit un isomorphisme :

$$\mathbb{U}(2)/\mathbb{U}(1) \simeq SO(3).$$

Sous cette action, l'élément de $\mathbb{U}(2)$ défini par :

$$R_{\hat{n}}(\theta) := \cos(\frac{\theta}{2})I - i\sin(\frac{\theta}{2})(n_xX + n_yY + n_zZ),\ \hat{n} = (n_x, n_y, n_z) \in \mathbb{R}^3,\ \|\hat{n}\| = 1,\ \theta \in \mathbb{R}$$

est la rotation d'axe $\hat{n}$ et d'angle θ.

Voici maitenant un critère de complétude :

Lemme 14 *Soit $\hat{n},\ \hat{m} \in \mathbb{R}^3$, $\|\hat{n}\| = \|\hat{m}\| = 1$, $\hat{n} \nparallel \hat{m}$ et $\alpha,\ \beta \in \mathbb{R}$, $\frac{\alpha}{2\pi}, \frac{\beta}{2\pi} \in \mathbb{R} - \mathbb{Q}$ alors :*

$$\overline{< \{R_{\hat{n}}(\alpha), R_{\hat{m}}(\beta)\} \cup \mathbb{U}(1) >} = \mathbb{U}(2).$$

La démonstration de ce lemme se déduit de l'exercice suivant :

Exercice :

1. *Soit $\theta \notin 2\pi\mathbb{Q}$ alors : $\overline{< \{R_{\hat{n}}(\theta)^n,\ n \in \mathbb{N}\} >} = \{R_{\hat{n}}(\alpha),\ \alpha \in \mathbb{R}\}\ \forall \hat{n} \in \mathbb{R}^3,\ \|\hat{n}\| = 1$.*
2. *Soit $\hat{n},\ \hat{m} \in \mathbb{R}^3,\ \|\hat{n}\| = \|\hat{m}\| = 1,\ \hat{n} \nparallel \hat{m}$. Soit $U \in \mathbb{U}(2)\ \exists \psi, \alpha_1, \ldots, \alpha_k, \ldots, \beta_1, \ldots, \beta_k \in \mathbb{R}$ tels que :*
$$U = e^{i\psi}R_{\hat{n}}(\alpha_1)R_{\hat{m}}(\beta_1)\ldots R_{\hat{n}}(\alpha_k)R_{\hat{m}}(\beta_k).$$

Démontrons maintenant le lemme. Soit $U \in \mathbb{U}(2)$ et $\epsilon > 0$. On écrit

$$U = e^{i\psi}R_{\hat{n}}(\alpha_1)R_{\hat{m}}(\beta_1)\ldots R_{\hat{n}}(\alpha_k)R_{\hat{m}}(\beta_k).$$

On trouve $n_i,\ m_i \in \mathbb{N}\ 1 \leq i \leq k$ tels que $\|R_{\hat{n}}(\alpha)^{n_i} - R_{\hat{n}}(\alpha_i)\| < \frac{\epsilon}{2k}$ et $\|R_{\hat{n}}(\beta)^{m_i} - R_{\hat{n}}(\beta_i)\| < \frac{\epsilon}{2k}$. Alors $W = e^{i\psi}R_{\hat{n}}(\alpha)^{n_1}R_{\hat{m}}(\beta)^{m_1}\ldots R_{\hat{n}}(\alpha)^{n_k}R_{\hat{m}}(\beta)^{m_k} \in < \{R_{\hat{n}}(\alpha), R_{\hat{m}}(\beta)\} \cup \mathbb{U}(1) >$ et $\|W - U\| < \epsilon$ (par la proposition 12).

On peut enfin construire une base finie complète :

Proposition 15 *La base $\{H, T, CNOT\}$ est complète.*

Démonstration.

Comme $H^2 = I$ et $T^8 = I$ il suffit de construire, modulo $\mathbb{U}(1)$, deux rotations d'axes non parallèles et d'angles des multiples irrationnels de 2π en utilisant H et T. On a :

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} = e^{i\frac{\pi}{8}} \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} = e^{i\frac{\pi}{8}}(\cos(\frac{\pi}{8})I - i\sin(\frac{\pi}{8})Z \sim R_{\hat{z}}(\frac{\pi}{4}).$$

De plus, comme $HZH = X$, on a $HTH \sim R_{\hat{x}}(\frac{\pi}{4})$. Puis :

$$R_{\hat{z}}(\frac{\pi}{4})R_{\hat{x}}(\frac{\pi}{4}) = \cos^2(\frac{\pi}{8})I - i\sin(\frac{\pi}{8})(\cos(\frac{\pi}{8})(X + Z) + \sin(\frac{\pi}{8})Y)\ (carZX = -\frac{1}{i}Y).$$

Si on pose $\overrightarrow{n} = (\cos(\frac{\pi}{8}), \sin(\frac{\pi}{8}), \cos(\frac{\pi}{8}))$ et $\hat{n} = \frac{\overrightarrow{n}}{\|\overrightarrow{n}\|}$, on a $\cos^4(\frac{\pi}{8}) + \sin^2(\frac{\pi}{8})\|\overrightarrow{n}\|^2 = 1$ donc $\exists \theta \in \mathbb{R},\ \cos(\frac{\theta}{2}) = \cos^2(\frac{\pi}{8})\ et\ \sin(\frac{\theta}{2}) = \sin(\frac{\pi}{8})\|\overrightarrow{n}\|$. Alors on a $R_{\hat{z}}(\frac{\pi}{4})R_{\hat{x}}(\frac{\pi}{4}) = R_{\hat{n}}(\theta)$.

Lemme 16 *Soit $\theta \in \mathbb{R}$ vérifiant $\cos(\frac{\theta}{2}) = \cos^2(\frac{\pi}{8})$ alors $\theta \notin 2\pi\mathbb{Q}$.*

Démonstration.

On vérifie que le polynôme minimal de $\alpha = e^{2i\pi\lambda}$ où $\lambda = \frac{\theta}{2\pi}$ est $X^4 + X^3 + \frac{1}{4}X^2 + X + 1$ qui n'est pas cyclotomique car il n'est pas à coefficients entiers. On note Φ_n le $n^{ième}$ polynôme cyclotomique.

Supposons que λ soit rationnel, $\lambda = \frac{p}{q}$. Alors $\alpha^q - 1 = 0$ et donc, si l'on note $P_\alpha(X)$ le polynôme minimal de α on a $P_\alpha(X)|X^q - 1$ dans $\mathbb{Q}[X]$ or $X^q - 1 = \prod_{d|q} \Phi_d(X)$ donc $P_\alpha(X)|\Phi_n(X)$ pour un $n|q$. Comme les deux sont irréductibles et unitaires, on a $P_\alpha(X) = \Phi_n(X)$, contradiction.

■

On termine la proposition en remarquant que $HYH = -Y$ et $HXH = Z$ donc $HR_{\hat{n}}(\theta)H = R_{\hat{m}}(\theta)$ avec $\hat{m} = \frac{\overrightarrow{m}}{\|\overrightarrow{m}\|}$ et $\overrightarrow{m} = (\cos(\frac{\pi}{8}), -\sin(\frac{\pi}{8}), \cos(\frac{\pi}{8})) \nparallel \overrightarrow{n}$.

■

Remarque : On peut construire d'autres bases finies complètes par des méthodes similaires (voir par exemple [2]).

3.3 Théorème de Solovay-Kitaev

Etant donnés une base finie et complète , $\epsilon > 0$, et $n \in \mathbb{N}^*$, on cherche une borne supérieur à la longueur minimal des circuits capables d'approximer à ϵ près toutes les portes quantiques à n-entrées.

On ne s'interesse désormais qu'aux bases finies complètes de la forme $G \cup \{CNOT\}$ où $G \subset \mathbb{U}(2)$, G fini, $G^{-1} \subset \mathbb{U}(1)G$, $\overline{< G \cup \mathbb{U}(1) >} = \mathbb{U}(2)$, c'est le cas de tous les exemples précédents.

3.3.1 Enoncés

Le résultat suivant donne la borne voulue :

Théorème 17 *Soit $A \subset \mathbb{U}(2)$, A fini, $A^{-1} \subset \mathbb{U}(1)A$ et $\overline{< A \cup \mathbb{U}(1) >} = \mathbb{U}(2)$ alors $\forall\, n \in \mathbb{N}^*$, $\forall\, \epsilon > 0$, $\forall\, P$, porte quantique à n-entrées, $\exists\, C \in C(A \cup \{CNOT\})$ approximation de P à ϵ près et $n-2$ qubits de travail, de longueur :*

$$L = O(4^n n^2 \log^c(\frac{4^n n^2}{\epsilon})), \quad c = \frac{\log(5)}{\log(\frac{3}{2})} \approx 4.$$

L'importance de ce théorème réside dans l'aspect logarithmique de la borne qui ne pénalise pas trop la longueur par rapport au gain de précision. Une échelle logarithmique est réellement nécessaire comme le montre la proposition suivante :

Proposition 18 *Soit $\mathcal{A}$ une base finie complète telle que l'approximation de toute porte quantique se fait avec un nombre de qubits de travail borné alors $\exists\, n \in \mathbb{N}^*$, $\exists\, U \in \mathbb{U}(2^n)$ tel que l'approximation de U à ϵ près à partir de $\mathcal{A}$ demande un circuit de longueur :*

$$L = \Omega(2^n \log(\frac{1}{\epsilon})\frac{1}{\log(n)}).$$

3.3.2 Démonstration du théorème 17

Soit S_ϵ la boule de centre l'identité et de rayon ϵ dans $S\mathbb{U}(2)$. Pour la démonstration du théorème 17 on aura besoin du lemme suivant.

Lemme 19 *Soit* $G \subset S\mathbb{U}(2),\ G^{-1} \subset G,\ \overline{< G >} = S\mathbb{U}(2)$, *G fini.* $\exists\, \epsilon_0 > 0$ *ne dépendant pas de G tel que :*

$$\forall\, \epsilon \leq \epsilon_0,\ G_l\ \epsilon^2 - dense\ dans\ S_\epsilon \Rightarrow G_{5l}\ C\epsilon^3 - dense\ dans\ S_{\sqrt{C}\epsilon^{\frac{3}{2}}},\ C = constante.$$

Démonstration.

Exercice :

1. $\forall\, U \in S\mathbb{U}(2)\, \exists\, \overrightarrow{a} \in \mathbb{R}^3,\ U = e^{-i\frac{\overrightarrow{a}.\overrightarrow{\sigma}}{2}} := u(\overrightarrow{a})$, *où* $\overrightarrow{\sigma} = (X, Y, Z)$ *et* $\overrightarrow{a}.\overrightarrow{\sigma} = a_1X + a_2Y + a_3Z$ *si* $\overrightarrow{a} = (a_1, a_2, a_3)$.
2. *si* $U = u(\overrightarrow{a}),\ V = u(\overrightarrow{b})$ *avec* $\|\overrightarrow{a}\|,\ \|\overrightarrow{b}\| < \epsilon$ *alors* $\|[U, V]_{gp} - u(\overrightarrow{a} \times \overrightarrow{b})\| = O(\epsilon^3)$

   où $[U, V]_{gp} = UVU^{-1}V^{-1}$ *et* $\overrightarrow{a} \times \overrightarrow{b} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \times \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} a_1b_1 \\ a_2b_2 \\ a_3b_3 \end{pmatrix}$.
3. (a) $\|u(\overrightarrow{x}) - u(\overrightarrow{y})\| = 2\sqrt{2}\sqrt{1 - \cos(\frac{x}{2})\sin(\frac{y}{2}) - \sin(\frac{x}{2})\sin(\frac{y}{2})\hat{x}.\hat{y}}$ *où* $\overrightarrow{x},\ \overrightarrow{y} \in \mathbb{R}^3$, $x = \|\overrightarrow{x}\|,\ y = \|\overrightarrow{y}\|$.

   (b) $\|u(\overrightarrow{x}) - I\| = 4\sin(\frac{x}{4})$

   (c) *Si* $x,\ y < \epsilon$ *alors* $\|u(\overrightarrow{x}) - u(\overrightarrow{y})\| = \|\overrightarrow{x} - \overrightarrow{y}\| + O(\epsilon^3)$.

Etape 1 : $\exists\, \epsilon_0 > 0$, *indépendant de G, tel que,* $\forall\, \epsilon \leq \epsilon_0$ *:*

$$G_l\ \epsilon^2 - dense\ dans\ S_\epsilon \Rightarrow [G_l, G_l]_{gp}\ C\epsilon^3 - dense\ dans\ S_{\epsilon^2},\ C = constante.$$

En effet, soit $U \in S_{\epsilon^2}, \exists\, \overrightarrow{x} \in \mathbb{R}^3,\ U = u(\overrightarrow{x})$. Alors $x \leq \epsilon^2 + O(\epsilon^6)$. Soit maintenant $\overrightarrow{y},\ \overrightarrow{z} \in \mathbb{R}^3$ tels que $\overrightarrow{x} = \overrightarrow{y} \times \overrightarrow{z}$ et $y,\ z \leq \epsilon + O(\epsilon^5)$. On a alors :

$$\|u(\overrightarrow{y}) - I\| \leq \epsilon + O(\epsilon^5)\ \ et\ \ \|u(\overrightarrow{y}) - I\| \leq \epsilon + O(\epsilon^5)$$

.

Supposons $G_l\ \epsilon^2 - dense$ dans S_ϵ alors :

$$\exists\, U_1, U_2 \in G_l \cap S_\epsilon,\ \|U_1 - u(\overrightarrow{y})\| < \epsilon^2 + O(\epsilon^5)\ \ et\ \ \|U_2 - u(\overrightarrow{z})\| < \epsilon^2 + O(\epsilon^5).$$

On écrit alors $U_1 = u(\overrightarrow{y_0}),\ U_2 = u(\overrightarrow{z_0})$ et on a donc :

$$y_0,\ z_0 \leq \epsilon + O(\epsilon^2)\ \ et\ \ \|\overrightarrow{y_0} - \overrightarrow{y}\|,\ \|\overrightarrow{z_0} - \overrightarrow{z}\| < \epsilon^2 + O(\epsilon^3).$$

En remarquant que $\|\overrightarrow{a} \times \overrightarrow{b}\| \leq ab$, on déduit :

$$\begin{aligned}
\|[U_1, U_2]_{gp} - U\| &\leq \|U - u(\overrightarrow{y_0} \times \overrightarrow{z_0})\| + \|u(\overrightarrow{y_0} \times \overrightarrow{z_0}) - [U_1, U_2]_{gp}\| \\
&\leq \|\overrightarrow{x} - \overrightarrow{y_0} \times \overrightarrow{z_0}\| + O(\epsilon^3) \\
&\leq \|[(\overrightarrow{y} - \overrightarrow{y_0}) + \overrightarrow{y_0}][(\overrightarrow{z} - \overrightarrow{z_0}) + \overrightarrow{z_0}] - \overrightarrow{y_0} \times \overrightarrow{z_0}\| + O(\epsilon^3) \\
&\leq \|(\overrightarrow{y} - \overrightarrow{y_0}) \times (\overrightarrow{z} - \overrightarrow{z_0})\| + \|(\overrightarrow{y} - \overrightarrow{y_0}) \times \overrightarrow{z_0}\| + \|\overrightarrow{y_0} \times (\overrightarrow{z} - \overrightarrow{z_0})\| + O(\epsilon^3) \\
&\leq O(\epsilon^3) \\
&\leq C\epsilon^3
\end{aligned}$$

où C est une constante bien choisie et $\epsilon \leq \epsilon_0$ avec ϵ_0 suffisament petit. D'où l'étape 1.

Etape 2 : *Résultat par translation :*

Quitte à diminuer ϵ_0 on suppose que $(C\epsilon_0^3)^{\frac{1}{2}} < \epsilon_0$. Soit $\epsilon \leq \epsilon_0$ et $U \in S_{\sqrt{C}\epsilon^{\frac{3}{2}}}$. Supposons G_l $\epsilon^2 - dense$ dans S_ϵ. On peut donc trouver $V \in G_l$ tel que $\|U - V\| < \epsilon^2$. Alors $UV^* \in S_{\epsilon^2}$ et donc, par l'étape 1, $\exists W_1,\ W_2 \in G_l$ tels que :

$$\|[W_1, W_2]_{gp} - UV^*\| = \|[W_1, W_2]_{gp}V - U\| < C\epsilon^3$$

et comme $[W_1, W_2]_{gp}V \in G_{5l}$, le lemme est démontré.

■

Le théorème 17 est en fait un corollaire du résultat suivant démontré par Solovay en 1995 (manuscrit non publié), et indépendament par Kitaev ([3]) :

Proposition 20 *Soit $G \subset S\mathbb{U}(2),\ G^{-1} \subset G,\ \overline{< G >} = S\mathbb{U}(2)$, G fini, alors G_l est $\epsilon - dense$ dans $S\mathbb{U}(2)$ pour $l = O(\log^c(\frac{1}{\epsilon}))$ où $c = \frac{\log(5)}{\log(\frac{3}{2})} \approx 4$.*

Démonstration. Par compacité de $S\mathbb{U}(2)$, $\exists l_0$ tel que G_{l_o} est $\epsilon_0^2 - dense$ dans $S\mathbb{U}(2)$, en particulier dans S_{ϵ_0}.

Etape 1 : *En intérant le lemme 19 on construit :*

$$\epsilon(k) = \frac{(C\epsilon_0)^{(\frac{3}{2})^k}}{C},\ \forall k \in \mathbb{N},\ G_{5^k l_0}\ est\ \epsilon(k)^2 - dense\ dans\ S_{\epsilon(k)}.$$

Etape 2 : *Résultat par translations :*

Soit $U \in S\mathbb{U}(2)$. Quitte à diminuer ϵ_0 on suppose $C\epsilon_0 < 1$ et $\epsilon(k)^2 < \epsilon(k+1)$.

Comme G_{l_o} est $\epsilon_0^2 - dense$ dans $S\mathbb{U}(2)$ on choisi $U_0 \in G_{l_0},\ \|U - U_0\| < \epsilon_0^2 < \epsilon(1)$. Alors $UU_0^* \in S_{\epsilon(1)}$. Par l'étape 1 on trouve $U_1 \in G_{5l_0},\ \|UU_0^* - U_1\| = \|U - U_1U_0\| < \epsilon(1)^2 < \epsilon(2)$. En itérant l'étape 1 et le procédé de translation on trouve :

$$U_i \in G_{5^i l_0},\ 0 \leq i \leq k,\ \|U - U_k \ldots U_0\| < \epsilon(k)^2.$$

Il faut donc un produit de $l = l_0 + 5l_0 + \ldots + 5^k l_0 < \frac{5}{4}5^k l_0$ éléments de G pour une approximation de U à $\epsilon(k)^2$ près.

Soit $\epsilon > 0$. On veut que $\epsilon(k)^2 < \epsilon$. Quitte à diminuer légèrement ϵ on suppose k tel que $\epsilon(k)^2 = \epsilon$. Ce qui donne :

$$(\frac{3}{2})^k = \frac{\log(\frac{1}{C^2\epsilon})}{\log(\frac{1}{(C\epsilon_0)^2})}.$$

On pose $c = \frac{\log(5)}{\log(\frac{3}{2})}$ alors $(\frac{3}{2})^{kc} = 5^k$ et donc :

$$l < \frac{5}{4}5^k l_0 = O(\log^c(\frac{1}{\epsilon})).$$

■

On en déduit facilement le théorème 17. En effet, si on note G l'ensemble des représentants des éléments de $A \ mod \ \mathbb{U}(1)$, G vérifie les hypothèses du théorème 20. Soit $n \in \mathbb{N}^*$, $\epsilon > 0$ et P une porte quantique à n-entrées. Par le théorème 8, $\exists C \in C(\mathbb{U}(2) \cup \{CNOT\})$ de longueur $m = O(4^n n^2)$ réalisant P avec $n-2$ qubits de travails. On approxime alors, $mod \ \mathbb{U}(1)$, chacun des opérateurs du circuit C qui sont dans $\mathbb{U}(2)$ à $\frac{\epsilon}{m}$ près en utilisant des éléments de G_l avec $l = O(\log^c(\frac{m}{\epsilon}))$. Le nouveau circuit est alors de longueur $L = O(4^n n^2 \log^c(\frac{4^n n^2}{\epsilon})$ et par la proposition 12, c'est une approximation à ϵ près de P.

3.3.3 Démonstration de la proposition 18

On note $V_k(r)$ et $S_k(r)$ le volume et la surface d'une boule de dimension k et de rayon r. On représente l'ensemble des états des n-qubits par $\mathbb{S}^{2^{n+1}-1}$. Soit $\epsilon > 0$, on recouvre $\mathbb{S}^{2^{n+1}-1}$ par des boules B_ϵ de rayon ϵ. Comme $Surface(\mathbb{S}^{2^{n+1}-1} \cap B_\epsilon) \sim V_{2^{n+1}-2}(\epsilon)$ on peut recouvrir $\mathbb{S}^{2^{n+1}-1}$ par ou moins :

$$N_1 = \frac{S_{2^{n+1}-1}(1)}{V_{2^{n+}-2}(\epsilon)}$$

boules de rayon ϵ. Or $V_k(r) = \frac{(2\pi)^{\frac{k+1}{2}} r^{k+1}}{(k+1)\Gamma(\frac{k+1}{2})}$ et $S_k r = \frac{(2\pi)^{\frac{k+1}{2}} r^k}{\Gamma(\frac{k+1}{2})}$ donc :

$$N_1 = \Omega(\frac{1}{\epsilon^{2^{n+1}-1}}).$$

Notons $g = Card\mathcal{A}$ et $f = Max\{n, U \in A \cap \mathbb{U}(2^n)\}$. Soit $C \in C(\mathcal{A})$, de longueur m, à n-entrées. On fixe $\mid 0^n\rangle$ comme l'état initialement introduit dans le circuit. Soit $n \in \mathbb{N}$, $f \leq [\frac{n}{2}+1]$ (où $[.]$ désigne la partie entière). A chaque étape du circuit on peut générer au plus $(C_n^f)^g$ états différents (car les coefficient binômiaux sont croissants jusqu'à $[\frac{n}{2}+1]$). Soit sur un circuit de taille m au plus :

$$N_2 = O(n^{fgm})$$

états différents. Pour pouvoir réaliser tous les états possibles à ϵ près il faut :

$$\begin{aligned} & N_2 \geq N_1 \\ \Longrightarrow & O(n^{fgm}) \geq \Omega(\frac{1}{\epsilon^{2^{n+1}-1}}) \\ \Longrightarrow & m \geq \Omega(2^n \log(\frac{1}{\epsilon})\frac{1}{\log(n)}) \end{aligned}$$

En particulier, il existe un état $\mid e\rangle$ qui demande un circuit de $\mathcal{A}$ de longueur au moins $\Omega(2^n \log(\frac{1}{\epsilon})\frac{1}{\log(n)})$ pour être réalisé à partir de de l'état initial $\mid 0^n\rangle$ sans utiliser de qubits de travail. En choisissant un $U \in \mathbb{U}(2^n)$ tel que $U \mid 0^n\rangle = \mid e\rangle$ la proposition est démontrée dans le cas où on n'utilise pas de qubits de travail mais si on utilise un nombre de qubits de travail borné par p, quitte à tensorialiser convenablement par l'identité, on peut supposer que tous les circuits ont exactement p qubits de travail et si on pose N le nombre d'états de n-qubits réalisables par un circuit de longeur m, à $n+p$ entrées dont p qubits de travail on a :

$$N \leq O((n+p)^{fgm}) = O(n^{fgm})$$

et on obtient le même résultat.

References

[1] A. Yu Kitaev et A. H. Shen et M. N. Vyalyi. *Classical and quantum computation*. American mathematical society, 2002.

[2] Michael A. Nielson et Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge New York Oakleigh : Cambridge University Press, 2000.

[3] A. Yu Kitaev. *Quantum computations: algorithms and error correction*. Russ. Math. Surv., 52(6):1191-1249, 1997.