Ministère de l'Enseignement Supérieure et Recherche Scientifique

Université Mohamed Seddik Ben Yahia, Jijel

Faculté des Sciences Exactes et Informatique
Département Informatique

Support de Cours

Introduction aux algorithmes quantiques

Dr. Khalfaoui Khaled

Spécialité

Physique : Physique Théorique

Ce cours est un support pédagogique pour les étudiants intéressés par l'informatique quantique. Plus particulièrement, il est destiné à ceux qui poursuivent un parcours de master en informatique ou physique théorique. En introduction, il présente les concepts de base du calcul quantique. Ensuite, il expose les algorithmes quantiques les plus connus en donnant des exemples d'application. Afin de mettre en pratique les différentes notions abordées, une série d'exercices est proposée.

Avril 2024

Table des matières

,

Introduction

L'informatique quantique est un nouveau domaine d'études qui vise à développer des technologies basées sur les principes de la théorie quantique. L'objectif principal est de tirer profit de quelques concepts très intéressants qui n'existent pas dans le monde du calcul classique, plus particulièrement la superposition et l'intrication. Cette dernière est la ressource clé dans plusieurs protocoles multipartites tels que le codage superdense, la téléportation quantique, la distribution de clés quantiques, et de nombreuses autres applications.

Un algorithme quantique est une suite d'opérations quantiques appliquées suivant les postulats de la mécanique quantique sur des états quantiques dans un ordre bien défini. Généralement, il est exprimé sous forme de circuits quantiques. Chaque circuit quantique est constitué d'un ensemble ordonné d'opérations unitaires et de mesures, représentées graphiquement par des portes quantiques.

L'objectif de ce cours est d'introduire les étudiants à l'algorithmique quantique. Il est constitué de quatre chapitres :

- Dans un premier chapitre, on commence par les concepts de base du calcul quantique en donnant un aperçu sur les états quantiques purs et mixtes et leur mode d'évolution.
- Le deuxième chapitre est consacré aux protocoles de téléportation quantique. Un intérêt particulier est porté sur la propriété d'intrication quantique.
- Le troisième chapitre présente l'algorithme de factorisation de Shor. Un intérêt particulier est porté sur la transformée de Fourier quantique.
- Le dernier chapitre introduit les protocoles de correction d'erreurs quantique basés sur les codes stabilisateurs.

Afin de mettre en pratique les différentes notions abordées dans ces chapitres, une série d'exercices d'application est proposée à la fin de ce document.

Remarque : Ce cours est rédigé dans un cadre pédagogique comme un support pratique pour assimiler le fonctionnement de quelques algorithmes quantiques. Pour chaque protocole étudié, un exemple d'application est présenté. Les fondements et les développements mathématiques associés sont détaillés dans [1,2].

Chapitre 1

Éléments de base du calcul quantique

En information quantique, l'élément le plus élémentaire d'information est le qubit. A l'inverse du bit classique possédant deux états mutuellement exclusive 0 ou 1, un qubit peut être en superposition de ces deux états de base et tout système quantique évolue dans le temps suivant des postulats de la mécanique quantique. Pour une bonne maitrise des algorithmes quantiques, ce chapitre présente le concept d'états quantiques ainsi que leurs manipulation. Il introduit également le formalisme mathématique utilisé tout au long de ce cours.

1.1 États quantiques purs

1.1.1 Le formalisme

Dans la base canonique, un qubit est représenté par un vecteur à deux composantes complexes :

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha\begin{pmatrix}1\\ 0\end{pmatrix} + \beta\begin{pmatrix}0\\ 1\end{pmatrix} \tag{1.1}$$

tel que :

- $\alpha, \beta \in \mathbb{C}$
- $|\alpha|^2 + |\beta|^2 = 1$

En notation de Dirac, il est définit comme suit :

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad avec \tag{1.2}$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad , \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.3}$$

Un état quantique pur à n qubits est un registre de dimension 2^n.

$$|\psi\rangle \in \mathcal{H} = \underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 ..... \otimes \mathbb{C}^2}_{n\, fois}. \tag{1.4}$$

Dans le formalisme de Dirac, il est spécifié par une superposition de la forme suivante :

$$|\psi\rangle = \sum_{x \in \{0,1\}^{\otimes n}} \alpha_x |x\rangle \tag{1.5}$$

avec :

- $\alpha_x \in \mathbb{C}$
- $\sum_{x \in 0,1\}^{\otimes n}} |\alpha_x|^2 = 1$
- $\{|x\rangle_{x \in \{0,1\}^{\otimes n}}\}$: La base canonique de cet espace (dimension 2^n).

1.1.2 Opérations quantiques et mesures

Un état quantique pur à n qubits évolue en appliquant des transformations unitaires U_i de la forme :

$$\begin{aligned} U_i : \mathcal{H} &\to \mathcal{H} \\ |\psi\rangle &\to |\phi\rangle = U_i |\psi\rangle \end{aligned}$$

tel que :

$$U_i U_i^+ = U_i^+ U_i = I_{2^n} \tag{1.6}$$

Le calcul quantique se distingue du calcul classique par la notion de mesure. Cette dernière occupe une place particulière et joue le rôle du complément de l'évolution quantique. C'est une opération irréversible utilisée pour détruire la superposition et l'intrication des états quantiques. Une mesure quantique appliquée sur un état à n qubits est définie par un ensemble de projecteurs $\{M_j\}_{j=1..2^n}$ vérifiant les propriétés suivantes :

$$\sum_{j=1}^{2^n} M_j = I_H \ , \ M_j^+ = M_j \ , \ \begin{cases} M_j^2 = M_j \\ M_j M_{j'} = 0 \end{cases} \tag{1.7}$$

Si l'état du système est $|\psi\rangle$, chaque opérateur de mesure est défini par :

$$\begin{aligned} M_j \ &: \mathcal{H} \to \mathcal{H} \\ &|\psi\rangle \to |\psi\rangle_j \end{aligned}$$

C'est une projection de l'état $|\psi\rangle$ sur l'état de la mesure (j).

Juste avant la mesure, la probabilité d'avoir comme résultat la mesure (j) est calculée par la formule :

$$Prob(|\psi\rangle_j) = \langle\psi| M_j^+ M_j |\psi\rangle \tag{1.8}$$

avec bien sûr :

$$\sum_{j=1}^{2^n} Prob(|\psi\rangle_j) = 1 \tag{1.9}$$

Juste après la mesure, si la mesure donne (j), via le projecteur M_j alors :

$$|\psi\rangle_j = \frac{M_j |\psi\rangle}{\sqrt{\langle\psi| M_j^+ M_j |\psi\rangle}} \tag{1.10}$$

1.2 États quantiques mixtes

1.2.1 Le formalisme

Un état quantique mixte est défini par une matrice densité de la forme :

$$\rho = \sum_{i=1}^{n} p_i |\psi_i\rangle \langle\psi_i| \tag{1.11}$$

$\{|\psi_i\rangle\}$ est un ensemble d'états purs avec :

$$\sum_{i=1}^{n} p_i = 1 \tag{1.12}$$

La matrice densité vérifie les propriétés suivantes :

$$Trace(\rho) = 1 \ , \ \rho^+ = \rho \ , \ \rho > 0 \tag{1.13}$$

La matrice densité d'un état pur $|\psi\rangle$ est donnée par :

$$\rho = |\psi\rangle \langle\psi| \tag{1.14}$$

dans ce cas, on a :

$$\rho^2 = \rho \tag{1.15}$$

$$Trace(\rho^2) = 1 \tag{1.16}$$

1.2.2 Opérations quantiques et mesures

De même que pour les états purs, les états mixtes sont manipulés par des opérations quantiques et des mesures quantiques $\{U_i, M_j\}$ tels que :

Chaque opération quantique U_i est définie comme :

$$\begin{aligned} U_i \ : \mathcal{H} \otimes \mathcal{H} &\rightarrow \mathcal{H} \otimes \mathcal{H} \\ \rho &\rightarrow \rho_i \end{aligned}$$

avec :

$$\rho_i \ = \ U_i \, \rho \, U_i^+ \tag{1.17}$$

Chaque opération de mesure M_j est définie comme :

$$\begin{aligned} M_j \ : \mathcal{H} \otimes \mathcal{H} &\rightarrow \mathcal{H} \otimes \mathcal{H} \\ \rho &\rightarrow \rho_j : \text{(projection sur l'état de mesure)} \end{aligned}$$

Juste avant la mesure, la probabilité d'avoir comme résultat l'état ρ_j est calculée par la formule :

$$Prob(\rho_j) = Trace(M_j \rho M_j^+) \tag{1.18}$$

avec :

$$\sum_{j=1}^{2^n} Prob(\rho_j) = 1 \, , \ Trace(\rho) = 1 \tag{1.19}$$

Juste après la mesure, si la mesure donne (j) via le projecteur M_j alors :

$$\rho_j = \frac{M_j \rho M_j^+}{Trace(M_j \rho M_j^+)} \tag{1.20}$$

1.2.3 Matrice densité réduite

Dans le système composé AB spécifié par une matrice densité ρ^{AB}, on peut décrire chacune des parties A et B par deux matrices de densité réduites :

- $\rho^A = Tr_B(\rho^{AB})$: la trace partielle de ρ^{AB} sur la partie B. Elle est définie dans le sous espace $\mathcal{H}_\mathcal{A}$.
- $\rho^B = Tr_A(\rho^{AB})$: la trace partielle de ρ^{AB} sur la partie A. Elle est définie dans le sous espace $\mathcal{H}_\mathcal{B}$.

tels que :

$$Tr_B(\rho^{AB}) = \sum_{j=1}^{dim(B)} (I_A \otimes \langle\phi|_j)\rho^{AB}(I_A \otimes |\phi\rangle_j) \tag{1.21}$$

$$Tr_A(\rho^{AB}) = \sum_{i=1}^{dim(A)} (\langle\psi|_i \otimes I_B)\rho^{AB}(|\psi\rangle_i \otimes I_B) \tag{1.22}$$

où :

- I_A et I_B sont les opérateurs identités dans $\mathcal{H}_\mathcal{A}$ et $\mathcal{H}_\mathcal{B}$ respectivement.
- $\{|\psi\rangle_i\}$ et $\{|\phi\rangle_j\}$ sont des bases orthonormées dans $\mathcal{H}_\mathcal{A}$ et $\mathcal{H}_\mathcal{B}$ respectivement.

1.3 Portes et oracles quantiques

Les opérations possibles peuvent être des transformations simples ou contrôlées. Un aperçu sera donné dans les sections suivantes.

1.3.1 Portes quantiques simples :

Groupe de Pauli :

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{1.23}$$

$$U_X(\alpha\,|0\rangle + \beta\,|1\rangle) = \beta\,|0\rangle + \alpha\,|1\rangle \tag{1.24}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{1.25}$$

$$U_Y(\alpha\,|0\rangle + \beta\,|1\rangle) = -i\,\beta\,|0\rangle + i\,\alpha\,|1\rangle \tag{1.26}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{1.27}$$

$$U_Z(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha\,|0\rangle - \beta\,|1\rangle \tag{1.28}$$

Ces trois opérateurs vérifient quelques propriétés intéressantes :

- $X^2 = Y^2 = Z^2 = I_2$
- $XY = -YX\ ,\ XZ = -ZX\ ,\ YZ = -ZY$
- $XY = iZ$
- $XZ = -iY$
- $YZ = iX$
- $det(X) = det(Y) = det(Z) = -1$
- $Trace(X) = Trace(Y) = Trace(Z) = 0$

Porte Hadamard :

$$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \tag{1.29}$$

$$U_H(\alpha\,|0\rangle + \beta\,|1\rangle) = \frac{1}{\sqrt{2}}(\alpha+\beta)\,|0\rangle + \frac{1}{\sqrt{2}}(\alpha-\beta)\,|1\rangle \tag{1.30}$$

Porte de rotation :

$$R_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} \tag{1.31}$$

$$U_{R_\theta}(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha\,|0\rangle + e^{i\theta}\beta\,|1\rangle \tag{1.32}$$

Porte quantique de permutation :

$$Swap = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{1.33}$$

Cette porte quantique permet la permutation des positions de deux qubits dans un état quantique :

$$U_{Swap}\ (\alpha_0\,|00\rangle + \alpha_1\,|01\rangle + \alpha_2\,|10\rangle + \alpha_3\,|11\rangle) = \alpha_0\,|00\rangle + \alpha_2\,|01\rangle + \alpha_1\,|10\rangle + \alpha_3\,|11\rangle$$

$$U_{Swap}\ (\ |\psi\rangle\,|\phi\rangle\ ) = |\phi\rangle\,|\psi\rangle \tag{1.34}$$

1.3.2 Portes quantiques contrôlées :

L'application de ces portes quantiques dites contrôlées sur des qubits cibles est conditionnée par l'état d'un ensemble de qubits de contrôle. On appelle U-contrôlée à k qubits de contrôle et n qubits de cible l'opérateur CU défini par :

$$CU = \begin{bmatrix} 1 & 0 & 0 & . & . \\ 0 & 1 & 0 & . & . \\ 0 & 0 & . & . & . \\ . & . & . & 1 & . \\ & & & & U \end{bmatrix} \tag{1.35}$$

CU agit sur les n derniers qubits si et seulement si les k premiers sont tous à $|1\rangle$. On schématise CU par :

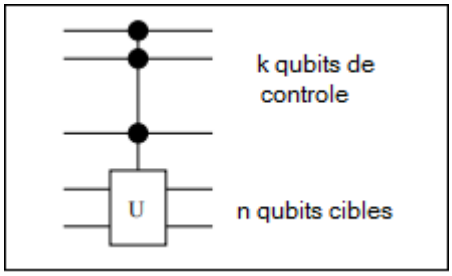


FIGURE 1.1 – Porte contrôlée

La plus simple des portes contrôlées est la porte $CNot$ ou $U = X$.

CNot :

$$CNot = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{1.36}$$

Cette transformation agit sur le deuxième qubit selon l'état du premier qubit. Pour $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$U_{CNot}(\,|0\rangle\,|\psi\rangle\,) = |0\rangle\,|\psi\rangle = |0\rangle\,(\alpha|0\rangle + \beta|1\rangle) \tag{1.37}$$

$$U_{CNot}(\,|1\rangle\,|\psi\rangle\,) = |1\rangle\,X\,|\psi\rangle = |1\rangle\,X(\alpha|0\rangle + \beta|1\rangle) = |1\rangle\,(\beta|0\rangle + \alpha|1\rangle) \tag{1.38}$$

La porte CNot est schématisée comme suit :

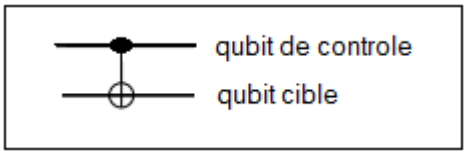


FIGURE 1.2 – La porte CNot

1.3.3 Oracles quantiques :

Un oracle quantique est une fonction quantique f dont la signature est de la forme :

$$f(x, y) = (x, y \oplus f(x)) \tag{1.39}$$

tel que : $\oplus$ est l'opération d'addition binaire. Il est implémenté par une transformation unitaire O_f qui agit de la manière suivante :

$$O_f(|x\rangle\,|y\rangle) = |x\rangle\ \ |y \oplus f(x)\rangle \tag{1.40}$$

Schématiquement, il est représenté par une boite noire (Fig.1.3).

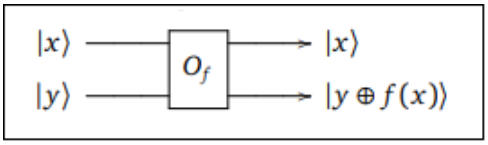
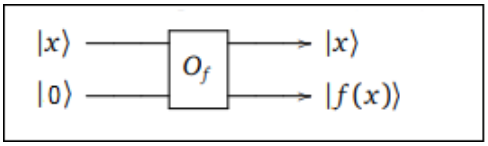


FIGURE 1.3 – Oracle quantique

En pratique, si la représentation binaire des valeurs de la fonction $f(x)$ nécessite l'utilisation d'au moins n qubits alors le registre $|y\rangle$ est initialisé par $|0\rangle^{\otimes n}$. Dans ce cas, l'oracle quantique O_f agit de la manière suivante :



et le résultat de son application est donné par :

$$O_f(|x\rangle\,|0\rangle) = |x\rangle\,|f(x)\rangle \tag{1.41}$$

Remarque : Dans un calcul quantique, et pour plus de lisibilité, les portes quantiques sont représentées graphiquement selon l'ordre 'chronologique' de leurs application dans un circuit quantique.

1.3.4 Calcul quantique

Dans un circuit quantique ayant comme entrée un état quantique pure ou mixte ($|\psi_0\rangle$ ou $|\rho_0\rangle$) à n qubits, l'application de chaque opération quantique se réalise en deux étapes. Il faut d'abord calculer la matrice de transformation globale U_k (ou M_k) de taille $2^n \times 2^n$ par un produit tensoriel des opérateurs correspondants à tous les qubits. Pour les qubits cibles (ou de contrôle), on utilise les matrices de transformation spécifiques à l'opération en question. Les autres qubits restent identiques en introduisant l'unité. Ensuite, en utilisant la matrice global, le nouveau état est calculé en appliquant les règles d'évolution vues précédemment.

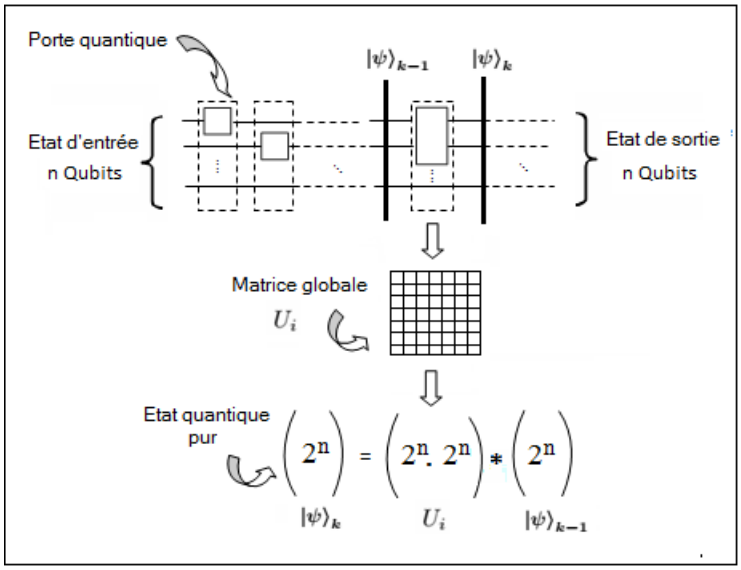


FIGURE 1.4 – Traitement quantique des états pures

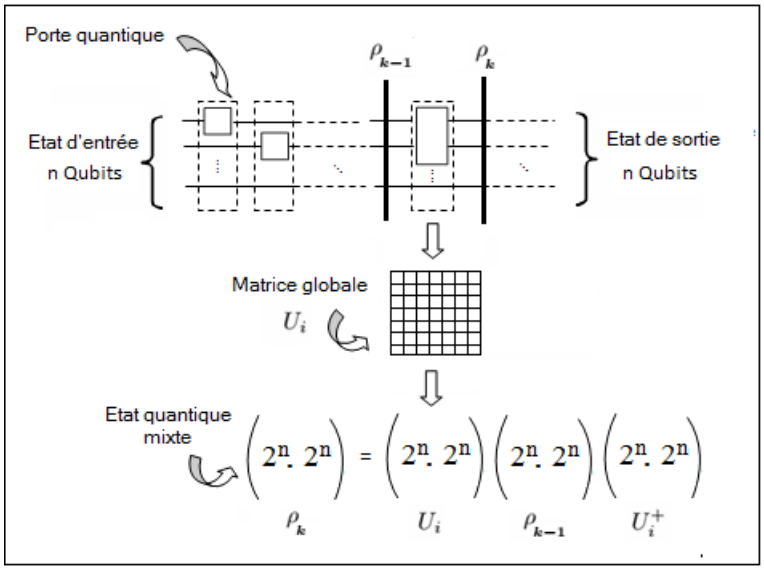


FIGURE 1.5 – Traitement quantique des états mixtes

Ce processus est réitéré du début jusqu'à la fin du circuit.

Remarque : Ces derniers années, le domaine du traitement de l'information quantique a connu d'énormes progrès théoriques et plusieurs algorithmes quantiques ont été élaborés. Le reste de ce cours est consacré à la présentation des protocoles les plus fondamentaux.

Chapitre 2

Intrication quantique et protocoles de téléportation

La téléportation quantique est une technique qui permet de transférer des états quantiques entres des régions distantes sans l'utilisation de canaux physiques. Depuis le protocole de Brassard [3], qui contient le résultat fondamental et original, cet extraordinaire exploit n'a cessé d'être augmenté et parfois changé de forme en rajoutant à son protocole des extensions telles que le contrôle [4], la bi-direction [5], la rotation [6] en plus des augmentations du nombre des qubits à téléporter.

Les protocoles de téléportation quantiques sont basés principalement sur le phénomène d'intrication. Les qubits intriqués sont intrinsèquement connectés et ont l'étrange façon de s'influencer instantanément, quelle que soit la distance qui les sépare. Cela signifie notamment qu'un changement sur l'état d'un ensemble de qubits influence directement l'état des autres qubits. Ce phénomène ne peut être expliqué ou interprété en termes de concepts de la théorie classique.

Dans la suite, on commence d'abord par introduire quelques concepts relatifs à la propriété d'intrication quantique. Ensuite, on présentera deux variantes de protocoles de téléportation en donnant tous les détails nécessaires à leur élaboration.

2.1 Intrication quantique

L'intrication quantique est un concept central au développement des protocoles quantiques. Elle décrit les corrélations entre les qubits qui n'ont pas d'analogues classiques. Malgré les avancées théoriques réalisées dans ce domaine, cette propriété reste encore difficile à maitriser de manière fiable et il n'existe que quelques méthodes générales connues permettant de quantifier cette caractéristique.

2.1.1 Critères de séparabilité

Séparabilité des états purs :

Considérons un état quantique pur bipartite $|\psi\rangle_{AB}$ composé de deux sous-systèmes A et B ayant comme matrice de densité $\rho_{AB} = |\psi\rangle_{AB} \langle\psi|_{AB}$. L'état $|\psi\rangle_{AB}$ est dit séparable s'il peut s'écrire sous la forme :

$$|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\chi\rangle_B \tag{2.1}$$

Dans ce cas, les matrices de densités réduites des deux sous-systèmes sont des états purs et s'écrivent comme :

$$\rho_A = |\phi_A\rangle \langle\phi_A| \quad et \quad \rho_B = |\chi_B\rangle \langle\chi_B| \tag{2.2}$$

D'un autre côté, si $|\psi_{AB}\rangle$ ne peut pas être exprimé comme un produit tensoriel des états de deux sous-systèmes (2.1), on dit que $|\psi_{AB}\rangle$ est un état pur intriqué. Dans ce cas, les opérateurs densité réduite ρ_A et ρ_B correspondent à des états mixtes.

Pour les états purs, le test de séparabilité est relativement simple et plusieurs critères géométriques ont été développés. Les plus intéressants sont :

- le critère basé sur le produit extérieur et l'identité de Lagrange [7].
- le critère basé sur le parallélisme des vecteurs [8,9].

Séparabilité des états mixtes :

Un état mixte ρ_{AB} est dit séparable s'il peut être écrit sous la forme :

$$\rho_{AB} = \sum_i P_i \ |\phi_i\rangle_A \langle\phi_i|_A \otimes |\chi_i\rangle_B \langle\chi_i|_B \ avec \ P_i \geq 0 \ et \ \sum_i P_i = 1 \tag{2.3}$$

sinon, ρ_{AB} est un état intriqué. Dans le cadre de la généralisation de l'équation (2.3) pour un état multipartite, un état N-partite agissant sur $H = H^{d1} \otimes H^{d2} .... \otimes H^{dn}$ est séparable s'il peut être écrit comme une somme convexe de produits tensoriels d'états des sous-systèmes :

$$\rho_N = \sum_i P_i \ \rho_i^{(1)} \otimes \rho_i^{(2)} \otimes .... \otimes \rho_i^{(N)} \quad avec \ P_i \geq 0 \ et \ \sum_i P_i = 1 \tag{2.4}$$

sinon, on dira qu'il est intriqué ou non séparable.

Le test de séparabilité des états mixtes est une tâche très complexe et les techniques proposées sont souvent limitées à l'étude des états quantiques à double qubits. Dans [10], les auteurs ont proposé un critère de séparabilité basé sur la décomposition de la matrice de densité ρ_{AB} dans l'espace de Hilbert-Schmidt sous la forme :

$\frac{1}{4}(I_2 \otimes I_2 + \sum_{i=1}^{3} r_i\,(\sigma_i \otimes I_2) + \sum_{i=1}^{3} s_i\,(I_2 \otimes \sigma_i) + \sum_{i,j=1}^{3} t_{ij}\,(\sigma_i \otimes \sigma_j))$

- I_2 is la matrice identité à deux dimensions.
- $\{\sigma_i\}_{i=1,2,3}$ sont les matrices de Pauli.
- r_i et s_i sont des réels.
- Les coefficients t_{ij} forment une matrice de réels notée T avec :

$$t_{ij} = Trace(\,\rho_{AB}\;(\sigma_i \otimes \sigma_j)\,) \tag{2.5}$$

Ils ont prouvé que l'état ρ_{AB} est inséparable si $N > 1$ tel que :

$$N = Trace(\sqrt{(T)^{+}\;T}\,) \tag{2.6}$$

Dans [11,12], un autre critère important appelé le critère de la transposition partielle positive (PPT) ou le critère de Peres-Horodecki est présenté. Les auteurs ont établit une condition nécessaire de la séparabilité pour tout état quantique mixte à double qubits ρ_{AB}. Si ρ_{AB} est séparable, sa transposition partielle de la matrice densité ρ_{AB} par rapport au premier sous-système A notée ρ^{T_a} est une matrice densité semi-définie positive, c-à-d $\rho_{AB} \geq 0$. Donc, s'il y a au moins une seule valeur propre négative, l'état ρ_{AB} est intriqué.

2.1.2 Mesure du degré d'intrication

Ces dernières années, des efforts considérables ont été déployés pour élaborer des critères permettant de quantifier le degré d'intrication des états quantiques. Pour les états purs, les plus connus de ces critères sont la concurrence et le tangle [13] :

— La concurrence : elle est utilisée dans le cas des états quantiques à double qubits telle que :

$$C_{A|B} = \sqrt{2(1 - Tr(\rho_A^2))}. \tag{2.7}$$

$\rho_A = Tr_B(\rho)$: la trace partielle de l'état global ρ^{AB} sur la partie B.

— Le tangle : le cas d'un systèmes à trois qubits, le tangle est exprimé comme :

$$\tau_{ABC} = C_{A|BC}^2 - C_{A|B}^2 - C_{A|C}^2 \tag{2.8}$$

et :

- $C_{A|BC}^2 = 2(1 - Tr(\rho_A^2))$: la trace partielle de l'état global sur la partie BC.
- $C_{A|B}^2 = |C_{A|BI_0} + C_{A|BI_1}|^2$ tel que $C_{A|BI_k}$ est la concurrence entre les qubits A et B quant le qubit C est mesuré à l'état $|I_k\rangle$.
- $C_{A|C}^2 = |C_{A|J_0C} + C_{A|J_1C}|^2$ tel que $C_{A|J_kC}$ est la concurrence entre les qubits A et C quant le qubit B est mesuré à l'état $|J_k\rangle$.

Dans [14], les auteurs ont abouti à l'élaboration d'un nouveau paramètre adapté au systèmes quantiques tripartites dit concurrence fill. Il est basé sur le calcul de la surface d'un triangle dont les cotés sont des concurrences entre ces trois parties.

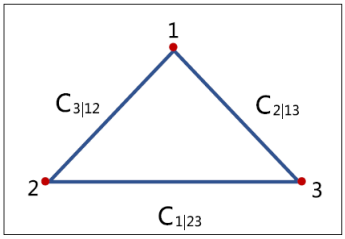


FIGURE 2.1 – Concurrence-fill

Pour tout état quantique mixte ρ^{ABC} à trois qubits, le degré d'intrication est donné par :

$$\frac{4}{\sqrt{3}}\sqrt{Q\,(Q-C^2_{A/BC})(Q-C^2_{B/AC})(Q-C^2_{C/AB})} \tag{2.9}$$

$$Q\;=\;\frac{1}{2}\;(\,C^2_{A/BC}+C^2_{B/AC}+C^2_{C/AB}\,) \tag{2.10}$$

- $C^2_{A/BC}, C^2_{B/AC}$ et $C^2_{C/AB}$ sont les concurrences bipartites données par :

$$C^2_{i|jk} = 2(1-Tr(\rho_i^2)) \tag{2.11}$$

- ρ_i est la trace partielle de l'état global ρ^{ABC} sur la partie i.

Remarques :

1. Pour tester l'intrication maximale d'un état pur $|\psi\rangle$ à n qubits, il suffit de vérifier les conditions suivantes pour chaque qubit i :
   - $({}_i\langle 0|\psi_0\rangle)^+ \,.\, ({}_i\langle 1|\psi_0\rangle) = 0$
   - $\|({}_i\langle 0|\psi_0\rangle)\| = \|({}_i\langle 1|\psi_0\rangle)\| = \frac{1}{\sqrt{2}}$

   Un exemple type des états maximalement intriqués sont les états de Bell :

$$\left|\psi^{\mp}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle \mp |11\rangle) \tag{2.12}$$

$$\left|\phi^{\mp}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle \mp |10\rangle) \tag{2.13}$$

2. Les protocoles de téléportation quantique sont basés principalement sur la corrélation entre les qubits distants. Cette propriété est assurée en intriquant un canal quantique partagé entre les différents acteurs. Dans la suite, deux exemples illustratifs sont présentés.

2.2 Protocole original de la téléportation quantique

Le premier protocole de téléportation quantique a été élaboré en 1993 par Brassard et al. [3]. Ce grand spécialiste et son équipe ont prouvé qu'il est possible de transmettre de l'information quantique entre deux acteurs distants via le phénomène d'intrication et sans l'utilisation de canal physique. Cette section est dédiée à la présentation de ce protocole avec tous les détails nécessaires. Supposons que l'émetteur s'appelle Alice et que le récepteur s'appelle Bob. Alice dispose d'un qubit quelconque $|Q\rangle$ qu'elle veut transmettre à Bob :

$$|Q\rangle_A = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.14}$$

Pour ce faire, Brassard et al. ont proposé le circuit quantique suivant :

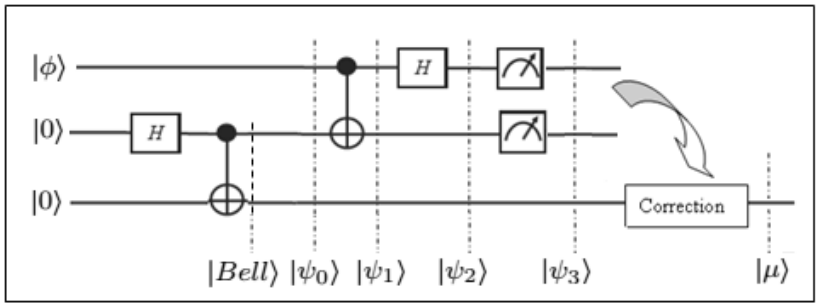


FIGURE 2.2 – Protocole original de Brassard

Ce schéma est constitué des opérations suivantes :

— Préparer un état à deux qubits maximalement intriqués ($|Bell\rangle$) pour l'utiliser comme canal quantique.

$$|Bell\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{2.15}$$

— Partager ces deux qubits entre Alice et Bob.

— Alice réalise deux opérations quantiques sur ces deux qubits (Fig.2.2).

— Alice réalise une opération de mesure dans la base canonique sur ces deux qubits et envoie le résultat à Bob via un canal classique.

— Bob corrige son qubit selon le résultat de mesure d'Alice afin de reconstituer le qubit initial $|Q\rangle_A$.

Les deux tables suivantes donnent tous les résultats obtenus en appliquant ce protocole.

TABLE 2.1 – États quantiques avant la mesure d'Alice

$\|Q\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$
$\|Bell\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
$\|\psi_0\rangle$	$\frac{1}{\sqrt{2}}(\alpha\|000\rangle + \alpha\|011\rangle + \beta\|100\rangle + \beta\|111\rangle)$
$\|\psi_1\rangle$	$\frac{1}{\sqrt{2}}(\alpha\|000\rangle + \alpha\|011\rangle + \beta\|101\rangle + \beta\|110\rangle)$
$\|\psi_2\rangle$	$\frac{1}{2}(\alpha\|000\rangle + \beta\|001\rangle + \alpha\|011\rangle + \beta\|010\rangle + \alpha\|100\rangle - \beta\|101\rangle - \beta\|110\rangle + \alpha\|111\rangle)$

TABLE 2.2 – Corrections de Bob après la mesure d'Alice

Résultats de mesure d'Alice	$\|\psi_3\rangle$	Qubit de Bob ($\|\mu\rangle$)	Correction appropriée
$\|00\rangle$	$\alpha\|000\rangle + \beta\|001\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$	I
$\|01\rangle$	$\alpha\|011\rangle + \beta\|010\rangle$	$\beta\|0\rangle + \alpha\|1\rangle$	X
$\|10\rangle$	$\alpha\|100\rangle - \beta\|101\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$	Z
$\|11\rangle$	$-\beta\|110\rangle + \alpha\|111\rangle$	$\beta\|0\rangle - \alpha\|1\rangle$	Z X

La table Tab.2.2 montre que pour toutes les mesures possibles d'Alice, son qubit initial $|Q\rangle_A$ est parfaitement téléporté à Bob en appliquant la correction appropriée.

2.3 Téléportation quantique contrôlée

Un protocole de téléportation quantique contrôlée est une extension du protocole original présenté précédemment dans lequel la transmission des qubits est assujettie au contrôle d'un superviseur. Donc, aux deux acteurs précédents Alice et Bob s'ajoute une troisième personnage Charlie. Dans la littérature, plusieurs schémas de téléportation contrôlée ont été proposés. Dans le cadre de ce cours, on se limite au plus simple, celui élaboré par Zhou et al. [15]. Dans ce protocole, le canal quantique utilisé est constitué de trois qubits maximalement intriqués (état GHZ) et partagés entre les trois acteurs : Alice, Bob et Charlie.

$$|Canal\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{2.16}$$

Alice dispose d'un qubit quelconque $|Q\rangle$ qu'elle veut transmettre à Bob :

$$|Q\rangle_A = \alpha|0\rangle + \beta|1\rangle \tag{2.17}$$

Donc, initialement, l'état quantique global est le suivant :

$$|EG\rangle_{AABC} = \frac{1}{\sqrt{2}}(\alpha\,|0000\rangle + \alpha\,|0111\rangle + \beta\,|1000\rangle + \beta\,|1111\rangle) \tag{2.18}$$

Ce protocole commence une mesure d'Alice. Elle utilise la base de Bell comme base de projection :

$$\left|\psi^{\mp}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle \mp |11\rangle) \tag{2.19}$$

$$\left|\phi^{\mp}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle \mp |10\rangle) \tag{2.20}$$

La table suivante présente les résultats de cette opération dans tous les cas possibles.

TABLE 2.3 – Téléportation quantique contrôlée : Résultats obtenus après la mesure d'Alice

Résultat de la mesure d'Alice	Qubits de Charlie et Bob
$\|\psi^+\rangle$	$\frac{1}{\sqrt{2}}(\alpha\,\|00\rangle + \beta\,\|11\rangle)$
$\|\psi^-\rangle$	$\frac{1}{\sqrt{2}}(\alpha\,\|00\rangle - \beta\,\|11\rangle)$
$\|\phi^+\rangle$	$\frac{1}{\sqrt{2}}(\alpha\,\|11\rangle + \beta\,\|00\rangle)$
$\|\phi^-\rangle$	$\frac{1}{\sqrt{2}}(\alpha\,\|11\rangle - \beta\,\|00\rangle)$

En analysant ces résultats, on remarque qu'à ce stade les deux qubits de chrlie et celui de Bob sont intriqués. Bob ne pourra jamais reproduire le qubit d'Alice sans l'intervention du contrôleur Charlie.

- Si Charlie est favorable pour la téléportation, il mesure son qubit dans une base appropriée.
- Sinon, le qubit d'Alice est perdu.

En cas de coopération de Charlie, dans cet exemple, la base de mesure utilisée est celle de Hadamard :

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{2.21}$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{2.22}$$

après cette mesure, Alice et Charlie informent Bob des projections réalisées afin de pouvoir corriger son qubit. La table suivante présente toutes les configurations possibles ainsi que les corrections correspondantes.

TABLE 2.4 – Téléportation quantique contrôlée : Résultats obtenus après la mesure d'Alice

Rest Mes d'Alice	Qubits de Charlie et Bob	Rest Mes de Charlie	Qubit de Bob	Corr Bob
$\|\psi^+\rangle$	$(\alpha\|00\rangle + \beta\|11\rangle)$	$\|+\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$	I
$\|\psi^+\rangle$	$(\alpha\|00\rangle + \beta\|11\rangle)$	$\|-\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$	Z
$\|\psi^-\rangle$	$(\alpha\|00\rangle - \beta\|11\rangle)$	$\|+\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$	Z
$\|\psi^-\rangle$	$(\alpha\|00\rangle - \beta\|11\rangle)$	$\|-\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$	I
$\|\phi^+\rangle$	$(\alpha\|11\rangle + \beta\|00\rangle)$	$\|+\rangle$	$\beta\|0\rangle + \alpha\|1\rangle$	X
$\|\phi^+\rangle$	$(\alpha\|11\rangle + \beta\|00\rangle)$	$\|-\rangle$	$\beta\|0\rangle - \alpha\|1\rangle$	Z X
$\|\phi^-\rangle$	$(\alpha\|11\rangle - \beta\|00\rangle)$	$\|+\rangle$	$\beta\|0\rangle - \alpha\|1\rangle$	Z X
$\|\phi^-\rangle$	$(\alpha\|11\rangle - \beta\|00\rangle)$	$\|-\rangle$	$\beta\|0\rangle + \alpha\|1\rangle$	X

Les résultat de la table Tab.2.4 montre que dans tous les cas le qubit d'Alice est parfaitement téléporté à Bob mais avec la permission du contrôleur Charlie.

Chapitre 3

Algorithme de factorisation de Shor

La sécurité des communications sur internet est basée sur l'arithmétique et en particulier sur le système de cryptographie RSA [16] qui repose sur la difficulté de factoriser de très grands entiers avec un ordinateur classique. En s'appuyant sur la puissance du calcul quantique, en 1993, Shor et al. a élaboré un algorithme permettant de casser cet obstacle dans un temps polynomial [17]. L'idée principale de cette solution est la suivante :

— La réduction du problème de factorisation en un problème de recherche de la période d'une fonction. Cette tache est réalisée par un traitement classique.

— L'identification de la période recherchée par un traitement quantique où ils ont proposé la transformée de Fourier qui permettant de réaliser cette tâche dans un temps polynomial.

Dans la suite, nous présentons les détails de cette solution. Une illustration par un exemple d'application sera donnée.

3.1 Algorithme Principal

Soit N un entier à factoriser en produit de deux nombres premiers $Fact_1$ et $Fact_2$. Le traitement classique déploie une stratégie itérative probabiliste qui lui assure de trouver ces deux facteurs avec une bonne probabilité. A chaque itération, on commence par choisir au hasard un entier a avec $1 < a < N$ et on calcule le pgcd de a et de N par l'algorithme d'Euclide (c'est une étape très rapide). Deux cas se présentent :

- Si $pgcd(a, N) \neq 1$ alors $pgcd(a, N)$ est un facteur non-trivial de N et l'algorithme se termine. Mais, cette situation est rare.
- Dans le cas contraire, on construit la suite $a^k mod\ N$ et on calcule sa période r. Sous certaine conditions, cette période permet d'identifier directement les deux facteurs recherchés :
  - $Fact_1 = pgcd(\ a^{\frac{r}{2}} - 1,\ N\ )$
  - $Fact_1 = pgcd(\ a^{\frac{r}{2}} + 1,\ N\ )$

Toute tentative qui a échoué peut être recommencée en choisissant au hasard un autre entier $1 < a < N$ jusqu'à ce qu'un facteur se dégage presque à coup sûr en un temps raisonnable. L'implémentation de cet algorithme est présenté dans le pseudo-code Algorithme.1 et les fonctions auxiliaires utilisées sont :

Les fonctions utilisées sont :

- *pgcd* (Nbr_1, Nbr_2) : Traitement classique qui donne le plus grand commun diviseur de deux entiers Nbr_1 et Nbr_2.
- *Puissance* (Nbr_1, Nbr_2) : Traitement classique qui calcule nbr_1 à la puissance Nbr_2.
- $Nbr_1\ mod\ Nbr_2$: Traitement classique qui donne le reste de la division de Nbr_1 par Nbr_2.
- *Période_Quantique* (a, N) : Traitement quantique qui détermine la période de la fonction $a^k\ Mod\ N$.

Remarques :

- Dans cet algorithme, tous les traitements sont classiques à l'exception de la fonction *Période_Quantique*.
- La puissance de cet algorithme réside dans l'implémentation de cette fonction par un calcul basé sur la transformée de Fourier quantique. Les détails du circuit proposé sont présentés dans la section suivante.

```
1  void Factoriser ( N : Entier )
2    {
3       Fin = faux ;
4       TQ (! Fin )
5          {
6            Choisir un entier a dans l'intervalle [2,N-1] ;
7            Si ( pgcd (N,a) != 1 )
8               {
9                  Fact_1 = pgcd (N,a) ;
10                 Fact_2 = N / Fact_1 ;
11                 Fin = Vrai ;
12                 Afficher ( Fact_1 , Fact_2) ;
13              }
14           Sinon
15              {
16                 r = Periode_Quantique ( a , N ) ;
17                 Si ( r > 0 )
18                    {
19                       Si ( ( r mod 2 ) = 0 )
20                          {
21                             Puiss_r = Puissance( a , (r / 2)) ;
22                             Modulo = ( Puiss_r mod ( N )) ;
23                            Si ( ( modulo != 1 ) et ( modulo != (N-1) ) )
24                               {
25                                  Fact_1 = pgcd( Puiss_r + 1 , N ) ;
26                                  Fact_2 = pgcd( Puiss_r - 1 , N ) ;
27                                  Afficher ( Fact_1 , Fact_2) ;
28                                  Fin = Vrai ;
29                               }
30                          }
31                    }
32              }
33          }
34    }
```

Algorithme 1 : Algorithme de factorisation

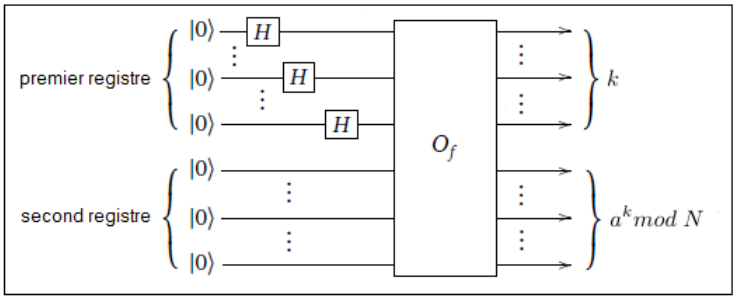
3.2 Calcul quantique de la période

La période de la fonction $a^k \, Mod \, N$ est calculée par un traitement quantique constitué des étapes suivantes :

Étape 01 : Préparer un état quantique superposé dont les constituants sont des puissances k associées aux termes correspondants de la fonction périodique $a^k \ mod \ N$. Cette tache est réalisée en utilisant deux registres quantiques de tailles n et m. Pour assurer une superposition suffisante, n et m doivent respecter les contraintes suivantes :

$$N^2 \leq n \leq 2 \, N^2 \quad et \quad m \geq \log_2(N) \tag{3.1}$$

Le circuit quantique correspondant à ce traitement est le suivant :



Les détails d'implémentation sont :

Initialisation : Les deux registres quantiques sont initialisés par des $|0\rangle$. L'état initial est donné par :

$$(|0\rangle^{\otimes^n} \otimes |0\rangle^{\otimes^m} \tag{3.2}$$

Transformation de Hadamard : On applique des transformations de Hadamard sur les qubits du premier registre, ce qui donne :

$$(H^{\otimes^n} |0\rangle^{\otimes^n}) \otimes |0\rangle^{\otimes^m} = \frac{1}{\sqrt{2^n}} \sum_{k=1}^{2^n-1} |k\rangle \otimes |0\rangle^{\otimes^m} \tag{3.3}$$

Application d'un oracle quantique : On applique un oracle quantique ayant comme fonction d'ajuster le deuxième registre à $\left|a^k \ mod \ N\right\rangle$ pour chaque entrée $|k\rangle$ du premier registre. A ce stade, l'état courant est :

$$\frac{1}{\sqrt{2^n}} \sum_{k=1}^{2^n-1} |k\rangle \left|a^k mod \ N\right\rangle \tag{3.4}$$

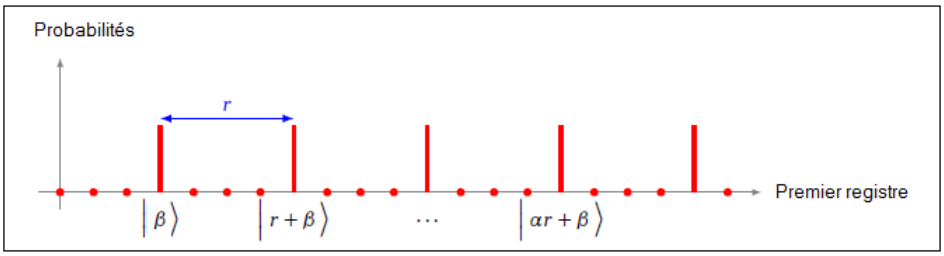
Étape 02 : On sélectionne une gamme de puissances k ayant le même reste de la division $a^k \ mod \ N$ par une mesure sur le second registre. Comme résultat, l'état du premier registre sera de la forme :

$$\frac{r}{\sqrt{2^n}} \sum_{\alpha=0}^{\frac{2^n}{r}-1} |\alpha r + \beta\rangle \tag{3.5}$$

avec :

- $0 < \beta \leq r$.
- r : la période recherchée.

Cet état peut être schématiser par la figure suivante :



A ce stade, le premier registre est projeté dans une superposition d'états dont les numéros d'ordre forment une suite périodique de période précisément égale à r. Peu importe le détail des termes de la suite, r est le paramètre vital qu'il nous faut extraire. On y parvient en utilisant une transformée de Fourier discrète et la technique des fractions continues.

Étape 03 : On applique d'abord la transformée de Fourier quantique sur le premier registre. Il s'agit d'un traitement itératif réalisé par le circuit présenté dans la figure Fig.3.1. Ensuite, on réalise une mesure sur ce registre. Admettons que cette opération donne comme résultat la fréquence v_i.

Étape 04 : On calcule la période r sur base d'un développement en fractions continues de la fraction $\frac{v_i}{2^n}$. La période cherchée r est égale au dénominateur de l'approximant le plus précis dont le dénominateur n'excède pas N.

Remarque : En terme de complexité algorithmique, l'efficacité de cet algorithme est due à l'introduction de la transformée de Fourier quantique. Pour plus de clarté, la section suivante présentera un exemple à titre d'illustration de cette fonction simulé en utilisant notre plate-forme [9].

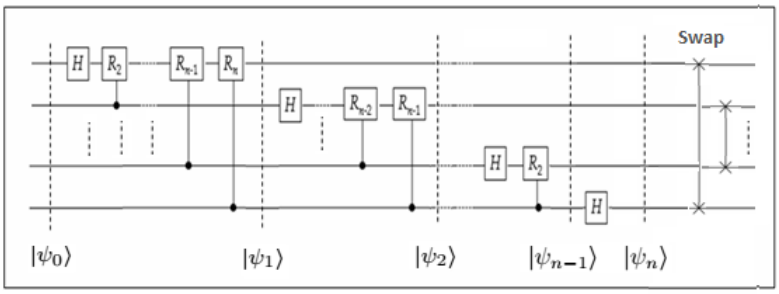


FIGURE 3.1 – Transformée de Fourier quantique

3.3 Simulation de la transformée de Fourier quantique

Dans cette section, nous présentons les résultats de simulation de la transformée de Fourier quantique utilisée dans le processus de factorisation de l'entier $N = 15$ à titre d'exemple. Dans ce cas, après la mesure du deuxième registre (Étape 02), l'état du premier registre, superposé par des puissances, est présenté dans la table Tab.3.1.

$\|\psi_0\rangle$	$0,108\|000000101\rangle$	+	$0,108\|000001011\rangle$	+	$0,108\|000010001\rangle$	+
	$0,108\|000010111\rangle$	+	$0,108\|000011101\rangle$	+	$0,108\|000100011\rangle$	+
	$0,108\|000101001\rangle$	+	$0,108\|000101111\rangle$	+	.....	+
	$0,108\|111010011\rangle$	+	$0,108\|111011001\rangle$	+	$0,108\|111011111\rangle$	+
	$0,108\|111100101\rangle$	+	$0,108\|111101011\rangle$	+	$0,108\|111110001\rangle$	+
	$0,108\|111110111\rangle$	+	$0,108\|111111101\rangle$			

TABLE 3.1 – État initial du deuxième registre

Cet état quantique correspondant à la suite suivante dont on souhaite identifier la période.

5, 11, 17, 23, 29, 35, 41, 47, 53, 59, ..., 473, 479, 485, 491, 497, 503, 509.

Comme présenté dans la figure Fig.3.1, le calcul de la transformée de Fourier quantique est implémenté par des transformations quantiques de manière itérative. Les tables Tab.3.2 et Tab.3.3 présentent les résultats de simulation obtenus à chaque niveau.

$\|\psi_1\rangle$	$0,077\,\|000000001\rangle + 0,077\,\|000000101\rangle + 0,077\,\|000000111\rangle + 0,077\,\|000001011\rangle + 0,077\,\|000001101\rangle + 0,077\,\|000010001\rangle + 0,077\,\|000010011\rangle + 0,077\,\|000010111\rangle + \ldots\ldots + (-0,075 + i0,016)\,\|111101111\rangle + (0,075 - i0,014)\,\|111110001\rangle + (-0,076 + i0,010)\,\|111110101\rangle + (0,076 - i0,008)\,\|111110111\rangle + (-0,077 + i0,005)\,\|111111011\rangle + (0,077 - i0,003)\,\|111111101\rangle$
$\|\psi_2\rangle$	$0,054\,\|000000001\rangle + 0,054\,\|000000011\rangle + 0,108\,\|000000101\rangle + 0,054\,\|000000111\rangle + 0,054\,\|000001001\rangle + 0,108\,\|000001011\rangle + 0,054\,\|000001101\rangle + 0,054\,\|000001111\rangle + \ldots\ldots + (-0,050 + i0,021)\,\|111110101\rangle + (0,034 - i0,069)\,\|111110111\rangle + (0,014 + i0,052)\,\|111111001\rangle + (-0,053 + i0,010)\,\|111111011\rangle + (0,048 - i0,060)\,\|111111101\rangle + (0,002 + i0,054)\,\|111111111\rangle$
$\|\psi_3\rangle$	$0,115\,\|000000001\rangle + 0,077\,\|000000011\rangle + 0,115\,\|000000101\rangle + 0,115\,\|000000111\rangle + 0,077\,\|000001001\rangle + 0,115\,\|000001011\rangle + 0,115\,\|000001101\rangle + 0,077\,\|000001111\rangle + \ldots\ldots + (0,009 - i0,013)\,\|111110101\rangle + (0,000 - i0,016)\,\|111110111\rangle + (-0,016 + i0,025)\,\|111111001\rangle + (0,014 - i0,007)\,\|111111011\rangle + (0,008 - i0,014)\,\|111111101\rangle + (-0,026 + i0,014)\,\|111111111\rangle$
$\|\psi_4\rangle$	$0,136\,\|000000001\rangle + 0,136\,\|000000011\rangle + 0,163\,\|000000101\rangle + 0,136\,\|000000111\rangle + 0,136\,\|000001001\rangle + 0,163\,\|000001011\rangle + 0,136\,\|000001101\rangle + 0,136\,\|000001111\rangle + \ldots\ldots + (0,004 + i0,009)\,\|111110101\rangle + (-0,005 - i0,018)\,\|111110111\rangle + (0,001 + i0,009)\,\|111111001\rangle + (-0,006 + i0,008)\,\|111111011\rangle + (0,014 - i0,013)\,\|111111101\rangle + (-0,008 + i0,005)\,\|111111111\rangle$
$\|\psi_5\rangle$	$0,211\,\|000000001\rangle + 0,192\,\|000000011\rangle + 0,211\,\|000000101\rangle + 0,211\,\|000000111\rangle + 0,192\,\|000001001\rangle + 0,211\,\|000001011\rangle + 0,211\,\|000001101\rangle + 0,192\,\|000001111\rangle + \ldots\ldots + (-0,003 + i0,006)\,\|111110101\rangle + (-0,006 + i0,003)\,\|111110111\rangle + (0,012 + i0,005)\,\|111111001\rangle + (-0,002 - i0,006)\,\|111111011\rangle + (0,001 - i0,006)\,\|111111101\rangle + (-0,011 + i0,006)\,\|111111111\rangle$
$\|\psi_6\rangle$	$0,285\,\|000000001\rangle + 0,285\,\|000000011\rangle + 0,298\,\|000000101\rangle + 0,285\,\|000000111\rangle + (0,013 + i0,005)\,\|000001001\rangle + (-0,005 - i0,013)\,\|000001011\rangle + (-0,013 + i0,005)\,\|000001111\rangle + (-0,013 - i0,003)\,\|000010001\rangle + \ldots\ldots + -0,001\,\|111110101\rangle + (-0,012 + i0,006)\,\|111110111\rangle + (-0,003 - i0,003)\,\|111111001\rangle + (0,003 - i0,003)\,\|111111011\rangle + (-0,006 - i0,006)\,\|111111101\rangle + (-0,003 + i0,003)\,\|111111111\rangle$

TABLE 3.2 – Résultats Intermédiaires

A ce stade, l'état quantique obtenu est en superposition des fréquences. On procède alors par une opération de mesure afin de sélectionner l'une des valeurs calculées. Admettons que le résultat de la mesure est $|110101011\rangle$. Cela correspond à la fréquence $v_i = 427$. Le développement en fractions continues donne les convergents suivants : 0 , 1 , 5/6 , 211/253 et 427/512. L'approximant le plus

$\|\psi_7\rangle$	$0,412\,\|000000001\rangle + 0,403\,\|000000011\rangle + (-0,007 - i0,007)\,\|000000101\rangle + (0,009 + i0,004)\,\|000001001\rangle + (-0,013 - i0,005)\,\|000001011\rangle + (0,004 + i0,009)\,\|000001101\rangle + (0,005 + i0,013)\,\|000001111\rangle + (0,004 + i0,001)\,\|000010001\rangle + \ldots\ldots\ldots\ldots + (-0,012 - i0,005)\,\|111110011\rangle + (0,004 + i0,010)\,\|111110101\rangle + (0,006 + i0,013)\,\|111110111\rangle + (-0,007 - i0,007)\,\|111111001\rangle + i0,003\,\|111111101\rangle + i0,006\,\|111111111\rangle$
$\|\psi_8\rangle$	$0,576\,\|000000001\rangle + (0,007i)\,\|000000011\rangle + (-0,005 - i0,005)\,\|000000101\rangle + (0,005 - i0,005)\,\|000000111\rangle + (-0,003 - i0,001)\,\|000001001\rangle + (-0,006 + i0,015)\,\|000001011\rangle + (0,006 + i0,015)\,\|000001101\rangle + (0,003 - i0,001)\,\|000001111\rangle + \ldots\ldots\ldots\ldots + (0,007 + i0,016)\,\|111110101\rangle + (0,003 - i0,001)\,\|111110111\rangle + (-0,005 - i0,005)\,\|111111001\rangle + (0,005 - i0,005)\,\|111111011\rangle + (0,007i)\,\|111111101\rangle + 0,002\,\|111111111\rangle$
$\|\psi_9\rangle$	$0,407\,\|000000000\rangle - 0,407\,\|000000001\rangle + (-0,170 - i0,292)\,\|101010100\rangle + (0,170 + i0,292)\,\|101010101\rangle + (0,170 - i0,292)\,\|110101010\rangle + (-0,170 + i0,292)\,\|110101011\rangle$
$\|\psi_{10}\rangle$	$0,407\,\|000000000\rangle + (-0,170 - i0,292)\,\|001010101\rangle + (0,170 - i0,292)\,\|010101011\rangle + -0,407\,\|100000000\rangle + (0,170 + i0,292)\,\|101010101\rangle + (-0,170 + i0,292)\,\|110101011\rangle$

TABLE 3.3 – Résultats Intermédiaires

précis dont le dénominateur n'excède pas $N = 15$ est $5/6$. D'après l'algorithme, la période recherchée est égale au dénominateur : $r = 6$. On remarque que cette valeur coïncide exactement avec la période de la suite en entrée.

Chapitre 4

La correction d'erreurs quantiques

Malgré les avancées théoriques réalisées dans le domaine du traitement de l'information quantique, la réalisation physique des équipement de calcul se heurte à de nombreuses difficultés. Les erreurs dues à l'interaction du système quantique avec son environnement constituent l'un des obstacles majeurs. Plutôt que de tenter de faire face à ce problème inévitable et complexe, les chercheurs tentent d'élaborer des techniques de détection et de correction des anomalies possibles en proposant plusieurs solutions.

Ce chapitre est dédié à la présentation de l'approche de détection et de correction d'erreurs quantiques basée sur les codes stabilisateurs [18]. Elle utilise principalement une intrication particulière d'un nombre de qubits supplémentaires avec les qubits à protéger via un processus de codage préalable. Les erreurs quantiques sont détectées par le calcul d'un syndrome quantique associé à l'état courant. Pour des fins d'illustration, un exemple d'application est donné.

4.1 L'idée de Base

Afin d'introduire le concept de la correction d'erreurs quantiques par les codes stabilisateurs, commençons par le cas le plus simple. Soit un qubit $|\psi\rangle$ quelconque :

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

Supposons que l'interaction de ce qubit avec son environnement peut provoquer des erreurs de type bit-flip (X). Pour protéger le qubit $|\psi\rangle$, on doit d'abord l'intriquer maximalement avec deux qubits supplémentaires. Le circuit correspondant à ce traitement est représenté dans la figure Fig.4.1

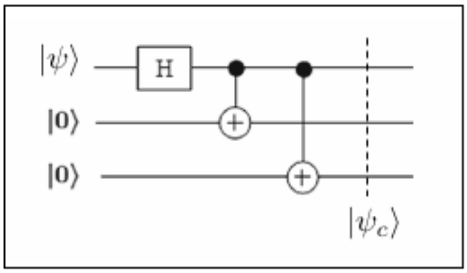


FIGURE 4.1 – Circuit d'encodage : Erreur bit-flip

On obtient alors un nouveau état encodé à trois qubits $|\psi_c\rangle$ tel que :

$$|\psi_c\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$$

Au cours du temps, en admettant qu'il peut y avoir une seule erreur de type bit-flip sur n'importe quel qubit de $|\psi_c\rangle$, cet état peut se retrouver dans l'un des quatre cas suivants :

- $|\psi_c\rangle_0 = |\psi_c\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$
- $|\psi_c\rangle_1 = X_1\,(\alpha\,|000\rangle + \beta\,|111\rangle) = \alpha\,|100\rangle + \beta\,|011\rangle$
- $|\psi_c\rangle_2 = X_2\,(\alpha\,|000\rangle + \beta\,|111\rangle) = \alpha\,|010\rangle + \beta\,|101\rangle$
- $|\psi_c\rangle_3 = X_3\,(\alpha\,|000\rangle + \beta\,|111\rangle) = \alpha\,|001\rangle + \beta\,|110\rangle$

La détection d'erreur consiste à identifier l'état courant sans aucune ambiguïté. Dans la technique des codes stabilisateurs, ce processus est implémenté par le calcul d'un syndrome associé à l'état courant en utilisant un ensemble d'opérateurs spécifiques U_i vérifiant les conditions suivantes :

— Les quatre états $|\psi_c\rangle_k$ sont des vecteurs propres des opérateurs U_i.

— Pour chaque état $|\psi_c\rangle_k$, les valeurs propres associées aux opérateurs U_i sont différentes des autres cas. Elle sont appelées syndrome.

— Tous les opérateurs U_i commutent.

Un fois l'état courant identifié, il suffit d'apporter la correction appropriée. Dans notre exemple, les opérateurs de syndrome adaptés sont :

$U_1 = Z_1\,Z_2$.
$U_2 = Z_1\,Z_3$.

La table Tab.4.1 résume les syndromes associés aux quatre états $|\psi_c\rangle_k$.

$\|\psi_c\rangle_k$	Valeur propre associé à U_1	Valeur propre associé à U_2
$\alpha\|000\rangle + \beta\|111\rangle$	+1	+1
$\alpha\|100\rangle + \beta\|011\rangle$	-1	-1
$\alpha\|010\rangle + \beta\|101\rangle$	-1	+1
$\alpha\|001\rangle + \beta\|110\rangle$	+1	-1

Pour chaque opérateur U_i, le calcul de la valeur propre associée à l'état courant est réalisé en suivant la technique suivante [19] :

— On ajoute un qubit auxiliaire initialisé à $H|0\rangle$. L'état global devient :

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|\psi_c\rangle_k$$

— On applique une opération U_i contrôlée par ce qubit auxiliaire sur les l'état $|\psi_c\rangle_k$, ce qui donne :

$$\frac{1}{\sqrt{2}}(|0\rangle\,|\psi_c\rangle_k + |1\rangle\,U_i\ |\psi_c\rangle_k)$$

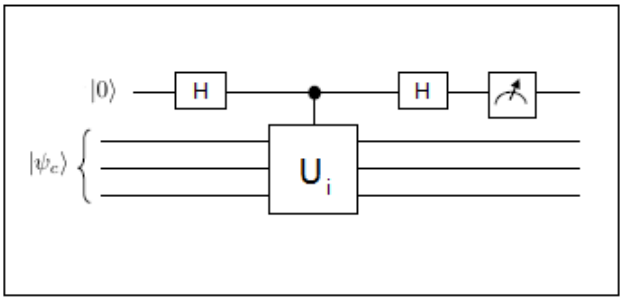
— On applique de nouveau une porte Hadamard sur le qubit auxiliaire. Le résultat est le suivant :

$$\frac{1}{2}\,|0\rangle\,(|\psi_c\rangle_k + U_i\ |\psi_c\rangle_k) + \frac{1}{2}\,|1\rangle\,(|\psi_c\rangle_k - U_i\ |\psi_c\rangle_k)$$

— Finalement, on mesure le qubit auxiliaire.

- Si le résultat de la mesure est 0, la valeur propre associée est -1.
- Par contre, Si le résultat de la mesure est 0, la valeur propre associée est +1.

Ce traitement est réalisé par le circuit quantique suivant :



4.2 Le code stabilisateur à cinq qubits

Le code stabilisateur de correction d'erreurs quantiques à cinq qubits a été proposé par Laflamme et al.[20]. Il permet de corriger les erreurs de type X,Y ou Z qui affectent un seul qubit en utilisant quatre qubits auxiliaires. Dans [21], avec les mêmes fonctionnalités, nous avons proposé un nouveau schéma plus optimisé en termes de portes quantiques utilisées. Pour plus de lisibilité, dans la suite, nous présentons d'abord les détails de cette solution. Ensuite, une illustration est donnée à travers un exemple d'application.

4.2.1 Protocole

Admettons qu'on dispose d'un un qubit $|\psi\rangle$ à protéger tel que :

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

Le circuit d'encodage proposé [21] est le suivant :

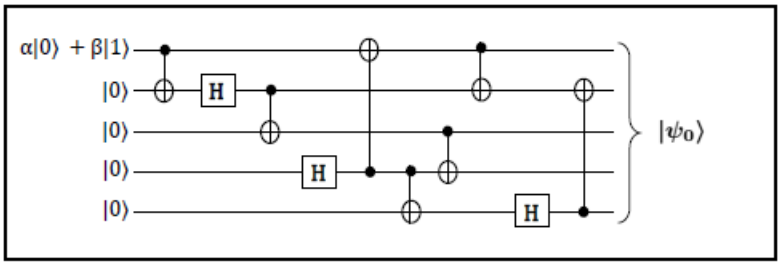


FIGURE 4.2 – Circuit d'encodage à 5 qubits

La table Tab.4.1 montre l'états du qubit encodé $|\psi\rangle_c$.

TABLE 4.1 – Encoding Results

$\|\psi_c\rangle$	$\frac{1}{2\sqrt{2}}(\alpha\,\|00000\rangle + \beta\,\|00010\rangle + \beta\,\|00101\rangle + \alpha\,\|00111\rangle + \alpha\,\|01001\rangle - \beta\,\|01011\rangle - \beta\,\|01100\rangle + \alpha\,\|01110\rangle + \beta\,\|10001\rangle - \alpha\,\|10011\rangle + \alpha\,\|10100\rangle - \beta\,\|10110\rangle + \beta\,\|11000\rangle + \alpha\,\|11010\rangle - \alpha\,\|11101\rangle - \beta\,\|11111\rangle)$

Comme opérateurs de syndrome $\{U_i\}$, on utilise :

$$U_1 = X_1\ Z_2\ X_3\ Z_4$$
$$U_2 = Z_1\ Z_2\ Z_3\ Z_5$$
$$U_3 = X_2\ Z_3\ Z_4\ X_5$$
$$U_4 = Z_1\ X_3\ X_4\ X_5$$

Les syndromes associés aux erreurs possibles sont :

0000	0101	1100	0110	1010	0100	1101	1110
No error	X_1	X_2	X_3	X_4	X_5	Y_1	Y_2

1111	1011	0111	1000	0010	1001	0001	0011
Y_3	Y_4	Y_5	Z_1	Z_2	Z_3	Z_4	Z_5

TABLE 4.2 – Table des syndromes

Le circuit de détection et de correction d'erreurs correspondant à cette solution est le suivant :

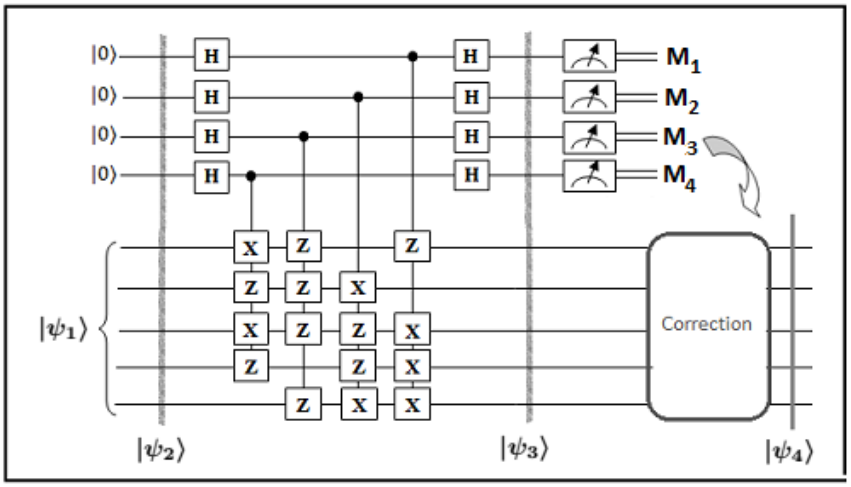


FIGURE 4.3 – Protocole de correction d'erreurs à 5 qubits

4.2.2 Exemple d'application

Une fois le qubit encodé ($|\psi_c\rangle$) comme présenté dans la table Tab.4.2, on doit vérifier son état périodiquement pour le corriger en cas d'erreurs. Supposons que l'état courant est le suivant ($|\psi_1\rangle$) :

$\|\psi_1\rangle$	$\frac{1}{2\sqrt{2}}(-i\beta\|00000\rangle+i\alpha\|00010\rangle-i\alpha\|00101\rangle+i\beta\|00111\rangle+i\beta\|01001\rangle+i\alpha\|01011\rangle-$ $i\alpha\|01100\rangle - i\beta\|01110\rangle + i\alpha\|10001\rangle + i\beta\|10011\rangle + i\beta\|10100\rangle + i\alpha\|10110\rangle -$ $i\alpha\|11000\rangle + i\beta\|11010\rangle + i\beta\|11101\rangle - i\alpha\|11111\rangle)$

TABLE 4.3 – État encodé à tester

En appliquant le circuit de détection d'erreurs (Fig.4.3), les résultats de simulation obtenus sont présentés dans les tables Tab.4.4 (($|\psi_2\rangle$), ($|\psi_3\rangle$) et ($|\psi_4\rangle$)).

$\|\psi_2\rangle$	$\frac{1}{2\sqrt{2}}(-i\beta\|000000000\rangle + i\alpha\|000000010\rangle - i\alpha\|000000101\rangle + i\beta\|000000111\rangle +$ $i\beta\|000001001\rangle + i\alpha\|000001011\rangle - i\alpha\|000001100\rangle - i\beta\|000001110\rangle +$ $i\alpha\|000010001\rangle + i\beta\|000010011\rangle + i\beta\|000010100\rangle + i\alpha\|000010110\rangle -$ $i\alpha\|000011000\rangle + i\beta\|000011010\rangle + i\beta\|000011101\rangle - i\alpha\|000011111\rangle)$
$\|\psi_3\rangle$	$\frac{1}{2\sqrt{2}}(-i\beta\|000000000\rangle + i\alpha\|000000010\rangle - i\alpha\|000000101\rangle + i\beta\|000000111\rangle +$ $i\beta\|000001001\rangle + i\alpha\|000001011\rangle - i\alpha\|000001100\rangle - i\beta\|000001110\rangle +$ $i\alpha\|000010001\rangle + i\beta\|000010011\rangle + i\beta\|000010100\rangle + i\alpha\|000010110\rangle -$ $i\alpha\|000011000\rangle + i\beta\|000011010\rangle + i\beta\|000011101\rangle - i\alpha\|000011111\rangle)$
$\|\psi_4\rangle$	$\frac{1}{2\sqrt{2}}(-i\beta\|101100000\rangle + i\alpha\|101100010\rangle - i\alpha\|101100101\rangle + i\beta\|101100111\rangle +$ $i\beta\|101101001\rangle + i\alpha\|101101011\rangle - i\alpha\|101101100\rangle - i\beta\|101101110\rangle +$ $i\alpha\|101110001\rangle + i\beta\|101110011\rangle + i\beta\|101110100\rangle + i\alpha\|101110110\rangle -$ $i\alpha\|101111000\rangle + i\beta\|101111010\rangle + i\beta\|101111101\rangle - i\alpha\|101111111\rangle)$
$M_1\,M_2\,M_3\,M_4$	1011

TABLE 4.4 – Simulation su protocole de détection d'erreur

On remarque que le résultat de l'opération de mesure sur les qubits auxiliaires est : 1011. D'après la table des syndromes (Tab.4.2), l'état courant est affecté par une l'erreur Y_4. Pour le corriger, on applique une porte Y sur le quatrième qubit. Le nouveau état quantique obtenu est présenté dans la table Tab.4.5 et les résultats montrent que l'erreur survenue a été parfaitement corrigée.

$\|\psi_4\rangle$	$\frac{1}{2\sqrt{2}}(\alpha\|00000\rangle + \beta\|00010\rangle + \beta\|00101\rangle + \alpha\|00111\rangle + \alpha\|01001\rangle - \beta\|01011\rangle -$ $\beta\|01100\rangle+\alpha\|01110\rangle+\beta\|10001\rangle-\alpha\|10011\rangle+\alpha\|10100\rangle-\beta\|10110\rangle+\beta\|11000\rangle+$ $\alpha\|11010\rangle - \alpha\|11101\rangle - \beta\|11111\rangle)$

TABLE 4.5 – Résultat de la correction

4.3 Calcul des syndromes et l'intrication quantique

Dans un protocole de correction d'erreurs quantiques basé sur les codes stabilisateurs, l'état global est constitué de deux parties :

- A = $\{Qubit_i\}$, i = 1..n : les qubits du syndrome.
- B = $|\psi_1\rangle$: l'état encodé.

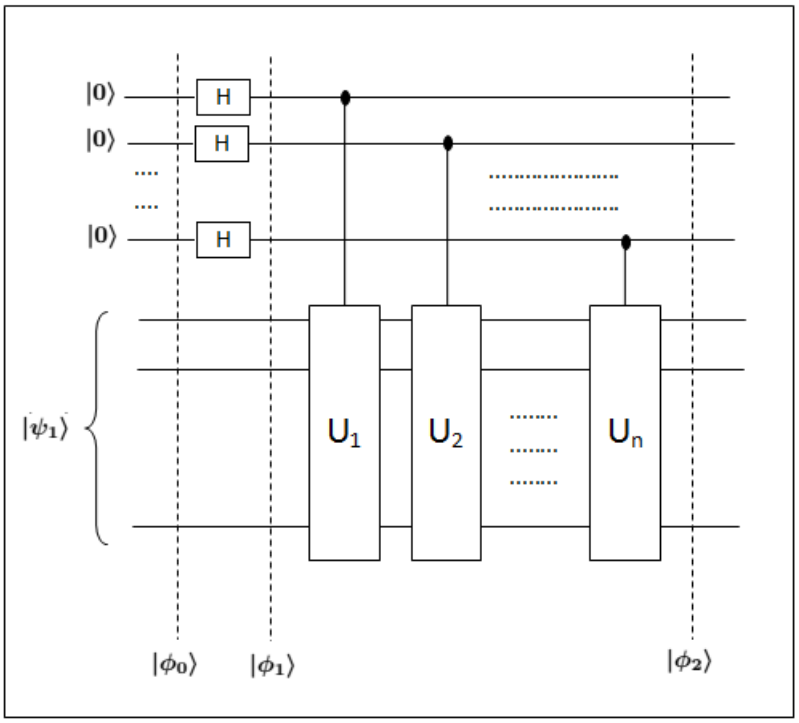


FIGURE 4.4 – Stabilizer Codes and Entanglment

Chaque qubit $Qubit_i$ est associé à un opérateur U_i tel que :

$$\begin{cases} U_i |\psi_1\rangle = \lambda_i |\psi_1\rangle \ , \ |\lambda_i| = 1 \ pour \ i = 1..n \\ U_i U_j = U_j U_i \ pour \ i, j = 1..n \end{cases} \tag{4.1}$$

En simulant le circuit présenté dans la figure Fig.4.4, on aura :

$$|\phi_0\rangle = \underbrace{|00.....0\rangle}_{n} |\psi_1\rangle \tag{4.2}$$

$$|\phi_1\rangle = \frac{1}{2^{n/2}} \sum_{\{I\}} |I\rangle \ |\psi_1\rangle \ , \ \{I\} = \{i_1, i_2, ..., i_n\} \tag{4.3}$$

A ce stade, les qubits de la partie A sont en superposition complète. L'application des opérations quantiques contrôlées U_i donne :

$$|\phi_2\rangle = \frac{1}{2^{n/2}} \sum_{\{I\}} |I\rangle \ (U)^{\delta_{\{I\};1}} \ |\psi_1\rangle \tag{4.4}$$

avec :

$$(U)^{X_{\{I\};1}} \ |\psi_1\rangle = \lambda_1^{\delta_{\{i_1\};1}} \ \lambda_2^{\delta_{\{i_2\};1}} \ ..... \ \lambda_n^{\delta_{\{i_n\};1}} \ |\psi_1\rangle \tag{4.5}$$

Notons :

$$\{\lambda\}^{\delta_{\{I\};1}} = \lambda_1^{\delta_{\{i_1\};1}} \ \lambda_2^{\delta_{\{i_2\};1}} \ ..... \ \lambda_n^{\delta_{\{i_n\};1}} \tag{4.6}$$

La matrice densité correspondante est donnée par :

$$\rho^{AB} = |\phi_2\rangle \ \langle\phi_2| \tag{4.7}$$

Calculons la trace partielle de ρ^{AB} sur les qubits de la partie A :

$$\rho^B = Tr_A(\rho^{AB}) = \frac{1}{2^n} \sum_{\{I\}} \{\lambda\}^{\delta_{\{I\};1}} \ (\{\lambda\}^{\delta_{\{I\};1}})^* \ |\psi_1\rangle \ \langle\psi_1| \tag{4.8}$$

Sachant que : $|\lambda_i| = 1 \quad \text{pour} \quad i = 1..n$, la trace partielle $Tr_A(\rho^{AB})$ est donnée par :

$$\rho^B = |\psi_1\rangle \ \langle\psi_1| \tag{4.9}$$

Ce résultat montre que malgré :

- La superposition effectuée sur les qubits de la partie A.
- L'application des opérations U_i contrôlées par les qubits de la partie A sur les qubits de la partie B.

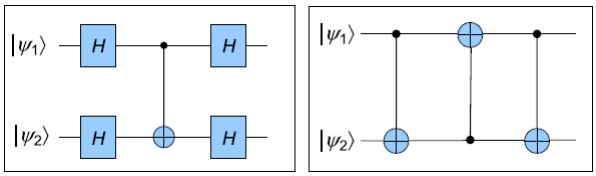
Il n'y a pas d'intrication entre les deux parties. Cela revient au fait que $|\psi_1\rangle$ est un vecteur propre des opérateurs U_i. Comme le reste des opérations quantiques sont appliquées uniquement sur les qubits de la partie A, les deux parties A et B sont toujours séparées dans ce protocole [21].

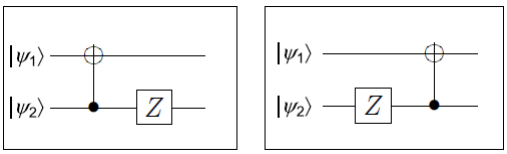
Chapitre 5

Travaux dirigés

Exercice 01 :

Soient les circuits quantiques suivants :





tels que :

$$|\psi\rangle_1 = \alpha_1 |0\rangle + \beta_1 |1\rangle$$
$$|\psi\rangle_2 = \alpha_2 |0\rangle + \beta_2 |1\rangle$$

Pour chaque circuit :

1. Calculer l'état en sortie.
2. Que peut-on déduire ?

Exercice 02 :

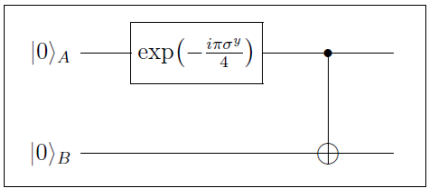
Comme présenté dans le cours, les matrices de transformation quantiques associées aux opérateurs X, Y et CNot sont les suivantes :

$$\sigma^x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma^z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, U_{CNot} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

1. Montrer que l'opération quantique M_{AB} est équivalente à une opération CNot telle que :

$$M_{AB} = \frac{1}{2}(\mathbb{I}_A + \sigma^z) \otimes \mathbb{I}_B + \frac{1}{2}(\mathbb{I}_A - \sigma^z) \otimes \sigma^x$$

2. Calculer l'état quantique en sortie du circuit quantique suivant :



tel que :

$$exp\ (-i\ \theta\ \sigma^y) = \cos(\theta)\ \mathbb{I} - i \sin(\theta)\ \sigma^y$$

- Que peut-on déduire ?

3. Considérons l'état de Bell $|\psi^+\rangle$:

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Calculer les probabilités de mesurer les états $|{+}{+}\rangle$, $|{+}{-}\rangle$, $|{-}{+}\rangle$ et $|{-}{-}\rangle$ tels que :

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

4. Calculer le résultat d'application d'une porte CNot sur les états $|{+}{+}\rangle$, $|{+}{-}\rangle$, $|{-}{+}\rangle$ et $|{-}{-}\rangle$.
- Que peut-on déduire ?

5. Pour l'état mixte $\rho^{AB} = |\psi^+\rangle \langle\psi^+|$, calculer les traces partielles :
   - $\rho^A = Tr_B(\rho^{AB})$.
   - $\rho^B = Tr_A(\rho^{AB})$.

   - Que peut-on déduire ?

Exercice 03 :

Calculer la concurrence $C_{A|B}$ pour les états quantiques suivants :

- $|\psi_1\rangle_{AB} = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$.
- $|\psi_2\rangle_{AB} = \frac{1}{\sqrt{3}}|00\rangle + \sqrt{\frac{2}{3}}|11\rangle$.
- $|\psi_2\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Exercice 04 :

Soient les états quantiques :

- $|\psi_1\rangle_{ABC} = \frac{1}{2}|000\rangle + \frac{1}{2}|001\rangle + \frac{1}{2}|110\rangle + \frac{1}{2}|111\rangle$.
- $|\psi_2\rangle_{ABC} = \frac{1}{\sqrt{2}}\sin\left(\frac{\pi}{5}\right)|000\rangle + \frac{1}{\sqrt{2}}\cos\left(\frac{\pi}{5}\right)|100\rangle + \frac{1}{\sqrt{2}}|111\rangle$.
- $|\psi_3\rangle_{ABC} = \cos\left(\frac{\pi}{8}\right)|000\rangle + \sin\left(\frac{\pi}{8}\right)|111\rangle$.
- $|\psi_4\rangle_{ABC} = \frac{1}{2}|000\rangle + \frac{1}{2}|100\rangle + \frac{1}{\sqrt{2}}|111\rangle$.

Pour chaque état, calculer :

1. $C^2_{A|BC}$, $C^2_{B/AC}$, $C^2_{C/AB}$, $C^2_{A|B}$, $C^2_{A|C}$.
2. τ_{ABC} (3-tangle).
3. $Concurrence\_Fill_{ABC}$.

Exercice 05 :

Lorsque l'on prépare deux qubits intriqués, théoriquement on peut les séparer spatialement autant que voulu tout en conservant l'intrication. En pratique, il y aura une limite de distance à cause de l'interaction avec l'environnement. La méthode étudiée dans cet exercice permet de créer de l'intrication sur des distances plus éloignées en utilisant des "répétiteurs quantiques". Admettons qu'Alice et Bob sont séparés par une distance 2L. Supposons que Charlie se trouve au milieu, donc à distance L d'Alice et à distance L de Bob. Charlie produit deux paires intriquées de Bell $|\psi^+\rangle_{12}$ et $|\psi^+\rangle_{34}$ avec :

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Il garde dans son labo les qubits 2 et 3 et envoie à Alice et Bob les qubits 1 et 4. Finalement, Charlie fait une mesure dans la base de Bell sur ses deux qubits.

1. Quels sont les résultats possibles de la mesure dans le labo de Charlie ?
2. Montrez que pour chaque résultat, les qubits 1 et 4 deviennent intriquées (sur une distance 2L).
3. Pour chaque résultat de mesure, donner les corrections locales nécessaires pour avoir $|\psi^+\rangle$ comme état intriqué partagé entre Alice et Bob.

Exercice 06 :

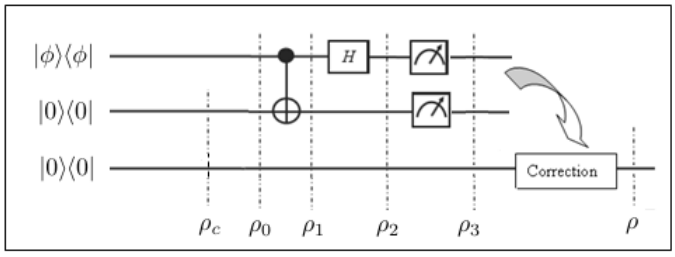
Dans le protocole de téléportation quantique original, le canal quantique partagé entre Alice te Bob est un état de Bell $|\psi^+\rangle$ avec :

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

L'objectif de cet exercice est d'étudier l'effet du bruit sur ce protocole. A titre d'exemple, admettons que le canal utilisé est le suivant :

$$\rho_c = \lambda \, |\psi^+\rangle \langle\psi^+| + \frac{1-\lambda}{4} \mathbb{I}_4$$

Dans ce cas, les états quantiques manipulés sont des états mixtes et le circuit quantique de téléportation devient :



1. Calculer les états ρ_0, ρ_1, ρ_2, ρ_3 et l'état de sortie ρ en supposant que le projecteur utilisé dans la mesure d'Alice est $|\psi^+\rangle \langle\psi^+|$.
2. Que peut-in déduire ?

Exercice 07 :

Supposons que l'interaction des qubits avec leurs environnement peut provoquer des erreurs de type phase-flip (Z). Dans cet exercice, on vous demande de proposer un protocole de correction d'erreurs basé sur les codes stabilisateurs.

Soit $|\psi\rangle$ un qubit quelconque :

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

1. Pour protéger le qubit $|\psi\rangle$ de l'erreur phase-flip, on doit d'abord procéder par une étape d'encodage. Pour ce faire, donner un circuit quantique permettant de d'intriquer le qubit $|\psi\rangle$ avec deux qubits supplémentaires. Le nouveau état encodé est noté $|\psi_c\rangle$.
2. Au cours du temps, donner les états possibles du qubit codé.
3. La détection d'erreur consiste à identifier l'état courant sans aucune ambiguïté en calculant un syndrome. Proposer deux opérateurs U_0 et U_1 de syndrome adaptés à ce problème.
4. Montrer que ces deux opérateurs commutent et que l'état $|\psi_c\rangle$ s'écrit sous la forme : $|\psi_c\rangle = \alpha\,|0\rangle_c + \beta\,|1\rangle_c$ tel que :

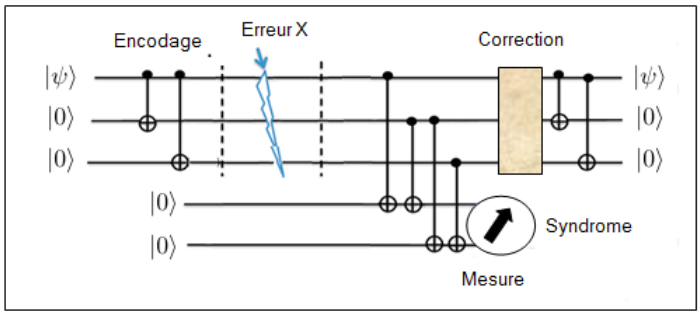
$$|0\rangle_c = \tfrac{1}{2}(1+U_1)(1+U_2)\,|000\rangle$$

$$|1\rangle_c = \tfrac{1}{2}(1+U_1)(1+U_2)\,|111\rangle$$

5. Donner la table des syndromes associés aux états possibles du qubit codé.
6. Donner le circuit quantique global.
7. Simuler ce circuit dans le cas d'une erreur sur le troisième qubit.

Exercice 08 :

L'objectif de cet exercice est de présenter un autre protocole de correction d'erreurs quantiques de type X, Y et Z proposée par Shor. Au début, commençons par le cas le plus simple en admettant que l'interaction des qubits avec leur environnement peut provoquer uniquement des erreurs de type bit-flip (X). Pour protéger un qubit quelconque $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, Shor a élaboré le circuit suivant :



Dans ce schéma, on commence d'abord par un encodage du qubit $|\psi\rangle$ en ajoutant deux qubits supplémentaires. On obtient alors un nouveau état encodé à trois qubits $|\psi_c\rangle$.

1. Calculer l'état $|\psi_c\rangle$.
2. Au cours du temps et en admettant qu'il peut y avoir une seule erreur de type bit-flip sur n'importe quel qubit, quels sont les nouveaux états possibles de $|\psi_c\rangle$?
3. La détection d'erreur est implémentée par le calcul d'un syndrome associé à l'état courant en utilisant deux qubits auxiliaires et 4 portes $CNot$. Calculer le syndrome correspondant à chaque état possible de $|\psi_c\rangle$.

Pour le cas des erreurs Bit-Phase (Z), Shor s'est basé sur le même principe en adaptant la solution précédente.

4. Sachant que : $Z = HXH$, modifier le circuit précédent afin de pouvoir corriger les erreurs Z.

Afin de corriger une erreur de type X, Y ou Z sur n'importe quel qubit, Shor à élaboré circuit quantique global utilisant un encodage à 9 qubits.

5. Imaginer le protocole de Shor.

Exercice 09 :

On veut factoriser le nombre $N = 15$ grâce à l'algorithme de Shor vu en cours. Pour cela on tire un nombre a au hasard dans $\{2, 3, ..., 15\}$. Nous supposerons que nous avons tiré $a = 7$ qui est premier avec 15.

1. Calculer l'ordre $Ord(7)$ c.à.d. le plus petit entier r tel que $7^r = 1\, mod\, 15$. Pour ce faire, il faut évaluer les premiers termes de la fonction :
$$f\ : x \rightarrow 7^x mod\, 15$$
2. Donner les étapes ultérieures de l'algorithme classique.
3. On veut maintenant simuler l'algorithme quantique pour la recherche de l'ordre en considerant que la taille du deuxième registre est m = 11.
   - Donnez l'état juste après l'application des portes de Hadamard.
   - Donnez l'état juste après l'application de l'oracle U_f.
   - Donnez l'état juste après l'application de la transformée de Fourier quantique.
   - Après la mesure du deuxième registre quantique, montrez que $Prob(y) = 1/4$ pour $y = 0$, 512, 1024 et 1536 et elle vaut 0 sinon.
   - Supposons que le résultat de la mesure est 1536. Peut-on trouver l'ordre r ?
   - Même question pour les valeurs 0, 512 et 1024.

Références bibliographiques

[01] M.A. Nielsen and I.L. Chuang, 'Quantum Computation and Quantum Information', Cambridge University Press, (2010).

[02] N.D. Mermin, 'Calculs et algorithmes quantiques : Méthodes et exemples', EDP Sciences,(2010).

[03] C.H. Bennett, G.Brassard, R. Jozsa, A. Peres, W.K. Wootters, 'Teleporting an Unkown Quantum State via Dual Classical and EPR Channels', Phys. Rev. Lett. 70, pp.1895–1899, (1993).

[04] L. Dong, X.M. Xiu, Y.J. Gao, Y.P. Ren and H.W. Liu, 'Controlled three-party communication using GHZ-like state and imperfect Bell-state measurement', Optics Communications, 284(905-908), (2011).

[05] Y.R. Sun, N. Xiang, Z. Dou, G. Xu, X.B. Chen, Y.X. Yang, 'A Universal Protocol for Controlled Bidirectional Quantum State Transmission', Quantum Inf. Process, 18(281), (2019).

[06] S. Sun, H. Zhang, 'Quantum Double-Direction Cyclic Controlled Communication via a Thirteen-Qubit Entangled State', Quantum Inf. Process, 19(120), (2020).

[07] S. Banerjee, P.K. Panigrahi, 'Quantifying parallelism of vectors is the quantication of distributed n party entanglement', J. Phys. A Math. Theor, 53, 9, (2020).

[08] R. Horodecki, M. Horodecki, P. Horodecki, 'Teleportation, Bell's inequalities and inseparability', Phys. Lett. A. 222(1–2), pp.21-25, (1996).

[09] K. Khalfaoui, E.H. Kerkouche, T. Boudjedaa, A. Chaoui, 'Optimized search

for complex protocols based on entanglement detection', Quantum Inf. Process, 21(6), 1–28 , (2022).

[10] A. Peres,'Separability Criterion for Density Matrices', Phys. Rev. Lett, 77(8) : pp.1413–1415, (1996).

[11] V.S. Bhaskara, P.K. Panigrahi, 'Generalized concurrence measure for faithful quantification of multiparticle pure state entanglement using lagrange's identity and wedge product', Quantum Inf. Process,16, 118 (2017)

[12] M. Horodecki, P. Horodecki, R. Horodecki, 'Separability of mixed states : necessary and sufficient conditions', Phys. Lett. A, 223(1–2), pp.1-8, (1996).

[13] V. Coffman , J. Kundu , W.K. Wootters, 'Distributed entanglement', Phys. Rev. A 61, 052306, (2000).

[14] S. Xie, J.H. Eberly, 'Triangle Measure of Tripartite Entanglement', Phys. Rev. Lett. 127(4), 040403, (2021).

[15] J. Zhou, G. Hou, S. Wu, Y. Zhang,'Controlled Quantum Teleportaion', https ://arxiv.org/pdf/quant-ph/0006030, (2000).

[16] R. Rivest, A. Shamir, L. Adleman, 'A method for obtaining digital signatures and public-key cryptosystems', Communications of the ACM, vol. 21, no 2, pp. 120–126, (1978)

[17] P. Shor, 'Algorithms for Quantum Computation : Discrete Logarithms and Factoring', Proceedings of the 35th Annual Symposium on Foundations of Computer Science, (1994).

[18] D. Gottesman, 'Stabilizer Codes and Quantum Error Correction', PhD thesis, California Institute of Technology, Pasadena, California, (1997).

[19] A. Y. Kitaev, 'Quantum measurements and the abelian stabilizer problem', Electronic Colloquium on Computational Complexity, 3, (1996).

[20] R. Laflamme, C. Miquel, J.P. Paz and W.H. Zurek, 'Perfect Quantum Error Correction Code', Physical Review Letters, Vol. 77, pp. 198-201, (1996).

[21] K. Khalfaoui, E.H. Kerkouche, T. Boudjedaa, A. Chaoui, 'Optimized exploration of quantum circuits space based on sub-circuits equivalences', Quantum Inf. Process, 22(71), (2023).