Chapitre I : Calcul quantique

I.1. Introduction :

En informatique classique, les données élémentaires manipulées sont les bits dont les valeurs possibles sont 0 et 1. Les ordinateurs usuels fournissent généralement des instructions qui les manipulent pour calculer des résultats et les stocker. Mais aujourd'hui, les applications développées traitent de très grandes quantités d'informations et les calculs implémentés sont devenus de plus en plus complexes. Ces deux problèmes se heurtent à la limite des processeurs standards et à la combinaison de 0 et 1 qu'ils peuvent gérer.

Pour remédier à ce problème, l'informatique quantique introduit une nouvelle unité de données, le qubit. Contrairement au bit classique, chaque qubit a une structure plus complexe lui permettant de contenir plus d'informations. Sa manipulation offre un parallélisme parfait, ce qui augmente considérablement la vitesse de calcul. Les qubits sont soumis à de nouvelles propriétés appelées superposition et intrication [1]. Ces deux phénomènes permettent aux concepteurs et développeurs d'explorer de nouvelles façons de développer des programmes informatiques.

Dans ce chapitre, nous rappelons brièvement quelques notions de base du traitement quantique de l'information. Nous présentons d'abord les bits et les états quantiques. Ensuite, nous introduisons les opérations quantiques offertes les plus utilisées. Enfin, nous abordons la composition des circuits quantiques.

I.2. Notions de bases :

I.2.1. Bit quantique (Qubit):

Le bit quantique ou « qubit » est l'élément fondamental de l'information quantique et la plus petite unité de stockage. Qui peut se trouver dans deux états d'un système quantique qu'on note $|0\rangle$ ou $|1\rangle$.

$$\alpha|0\rangle + \beta|1\rangle$$

À la différence du bit classique qui ne peut être que dans un des deux états à la fois (0 ou 1) le qubit peut exister dans plusieurs états en même temps. Plus précisément dans une superposition de ces deux états. [2]

Tels que α et β sont deux nombres complexes appelés amplitudes et vérifiant la contrainte :

$$|\alpha|^2 + |\beta|^2 = 1$$

Il est représenté par le vecteur **:** $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

L'observation de cet état donne :

- la valeur 0 avec une probabilité $|\alpha|^2$.
- la valeur 1 avec une probabilité $|\beta|^2$.

Le tableau suivant donne une petite comparaison entre les bits classiques et les bits quantiques.

Bit Classique	Bit Quantique
Un bit a toujours une valeur définie.	Pas de valeur définie pour le qubit tant qu'on ne l'observe pas.
Un bit vaut seulement 0 ou 1.	Un qubit peut être dans une superposition de 0 et 1 simultanément.
Un bit peut être copié sans être affecté.	Un qubit dans un état inconnu ne peut être copié.
Un bit peut être lu sans affecter sa valeur.	Lire un qubit qui est initialement dans une superposition changera sa valeur.
Lire un bit n'affecte pas un autre.	La lecture d'un qubit peut avoir influence sur les autres qubits.

Tab 1.1: *Comparaison du bit quantique VS le bit classique.*

I.2.2. Etat quantique :

L'état est un registre quantique à n qubits il est considéré comme un vecteur dans un espace vectoriel complexe de dimension2^n, c'est-à-dire un vecteur avec au plus 2^n composantes complexes Un état quantique peut être donné par: [3]

$$|\psi\rangle = \sum_{x=0}^{2^n-1} c_x|x\rangle \tag{1.1}$$

Les amplitudes c_x gouvernant les probabilités des différents états doivent satisfaire la propriété suivante : [4]

$$\sum_{x=0}^{2^n-1} |c_x|^2 = 1 \tag{1.2}$$

I.2.3. Espace de Hilbert :

L'espace de Hilbert est un cadre mathématique adapté à la description des concepts de la mécanique quantique. C'est un espace vectoriel complexe équipé d'un produit scalaire. Les états purs des systèmes quantiques sont considérés comme des vecteurs d'un espace de Hilbert. Une telle réalité n'apparaît que dans le cas d'une mesure, et ce que nous savons du niveau quantique ne sont que des procédures de calcul, exprimées en termes de concepts d'espace de Hilbert.

Parmi les notations les plus efficaces sur lesquelles les spécialistes s'appuient pour exprimer l'espace de Hilbert figurent celles proposées par Dirac [5] [6].

I.2.4. Notation de Dirac :

La notation de Dirac est un moyen pratique pour décrire les vecteurs dans l'espace de Hilbert C^n.
Elle est aussi appelée notation ‘’Bra-Ket’’ Qui sont considérés comme des vecteurs [6].

On note un vecteur d’´état $|\psi\rangle$ et on l’appelle un ket. Cela correspond à une vectrice colonne [7].

$$|\psi\rangle = \sum_{i=1}^{n} a_i \, |i\rangle = \begin{pmatrix} a1 \\ a2 \\ .. \\ ai \end{pmatrix} \tag{1.3}$$

Tandis que le transposé ou vecteur ligne est appelé Bra et noté $\langle\psi|$ [7].

$$\langle\psi| = \sum_{i=1}^{n} a_i^* \, \langle i| = (a_1^*, a_2^*, \dots \, a_n^*) \tag{1.4}$$

I.2.5. Produit scalaire Bra-ket :

Etant donné les vecteurs suivants :

Un vecteur Bra :

$$\langle\phi| \; = \; \sum_{i=1}^{n} b_i^* \, \langle i| \tag{1.5}$$

Et un vecteur Ket :

$$|\psi\rangle = \; \sum_{i=1}^{n} a_i \; |i\rangle \tag{1.6}$$

Le produit scalaire Bra-Ket est un nombre complexe de deux vecteurs dans cet ordre noté

$\langle\phi \mid \psi\rangle$ et donné par l’équation suivante :

$$\langle \, \phi \mid \psi \, \rangle = \sum_{i=1}^{n} a_i \; b_i^* \, \langle i|i\rangle \tag{1.7}$$

I.2.6. Produit tensoriel :

Le produit tensoriel est un produit entre deux vecteurs, il est utilisé pour combiner deux espaces de vecteurs afin d'obtenir un nouvel espace plus large. Etant donné deux vecteurs Ket $|\psi\rangle$ et $|\phi\rangle$ tel que :

$$|\psi\rangle = \sum_{i=1}^{n} a_i \, |i\rangle$$

$$|\phi\rangle = \sum_{i=1}^{m} b_i^* \, |i\rangle$$

Le produit tensoriel de ces deux vecteurs dans cet ordre noté $|\psi\rangle \otimes |\phi\rangle$ est calculé de la façon suivante:

$$|\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} = \begin{pmatrix} a_1 \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \\ a_2 \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \\ \vdots \\ a_n \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \end{pmatrix} = \begin{pmatrix} a_1.b_1 \\ a_1.b_2 \\ \vdots \\ a_1.b_m \\ a_2.b_1 \\ \vdots \\ a_{n-1}.b_m \\ a_n.b_1 \\ \vdots \\ a_n b_m \end{pmatrix} \quad (1.8)$$

I.3. Postulats :

I.3.1. Superposition :

Un bit quantique peut être dans l'état 0 ou 1, mais également dans les deux états en même temps, alors un registre de n qubits pourra contenir 2^n composantes complexes [2]. Cette Caractéristique permet principalement un traitement parallèle de toute cette combinaison en même temps [3].

I.3.2. Intrication :

Est un phénomène dans lequel deux particules (ou groupes de particules) ont des états quantiques dépendant l'un de l'autre quelle que soit la distance qui les sépare. Deux états intriqués constituent une entité indissociable. La transformation d'un état influence l'état de l'autre.

I.3.3. Mesure :

Etant donné un état $|\psi\rangle$ tel que :

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \quad (1.9)$$

La mesure de cet état est une projection dans une base $\{|0\rangle, |1\rangle\}$.

- L'amplitude de probabilité d'obtenir l'état |0⟩ après mesure est la suivante :

$$|\alpha|^2 = |\langle 0|\psi\rangle|^2 \tag{1.10}$$

- L'amplitude de probabilité d'obtenir l'état |1⟩ après mesure est la suivante :

$$|\beta|^2 = |\langle 1|\psi\rangle|^2 \tag{1.11}$$

Dans une mesure, le point le plus important à retenir est que cette opération est irréversible. Apres la mesure, les coefficients α et β seront perdus.

I.3.4. Evolution :

Entre deux mesures le système quantique évolue avec le temps et décrite par une transformation unitaire. Cette évolution de l'état résulte de l'application d'un opérateur linéaire, nommé opérateur d'évolution on traduisant dans l'équation suivant [7], [8] :

$$|\psi(t_0)\rangle \rightarrow |\psi(t)\rangle = U(t, t_0)\,|\psi(t_0)\rangle \tag{1.12}$$

I.4. Portes quantiques :

Le traitement de l'information quantique s'effectue par l'action de portes quantiques sur le registre. Une porte quantique est une opération unitaire agissant sur un ou plusieurs qubits [9]. Dans le cas général, une porte qui agit sur n qubits est représentée par une matrice de taille $2^n \times 2^n$ [10].

I.4.1. Portes unaires :

Les portes quantiques unitaires sont des portes à un qubit qui agissent sur un seul qubit des vecteurs d'état de l'espace de Hilbert C^2 [1].

I.4.1.1. Portes de Pauli :

❖ Porte X :

Cette porte est l'équivalent quantique de la porte NOT pour les ordinateurs classiques. Sa matrice est donnée par :

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{1.13}$$

Sa table de vérité est donnée comme suit :

Entrée	Sortie
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	$\beta\|0\rangle + \alpha\|1\rangle$

Tab 1.2: *Table de vérité de la porte quantique ≪ X ≫.*

❖ Porte Y :

La porte Y échange les amplitudes de $|0\rangle$ et $|1\rangle$, multiplie chaque amplitude par i, et Change le signe du second. Cette porte est représentée par la matrice carrée suivant [6] :

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{1.14}$$

Le tableau suivant représente la table de vérité de cette porte :

Entrée	Sortie
$\|0\rangle$	$i\|1\rangle$
$\|1\rangle$	$-i\|0\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	$-\beta i\|0\rangle + \alpha i\|1\rangle$

Tab 1.3: *Table de vérité de la porte quantique ≪ Y ≫.*

❖ Porte Z :

Cette porte laisse inchangée le premier coefficient de l'entrée mais change le signe du second. Sa matrice peut s'écrit comme suit [10] :

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{1.15}$$

Le tableau suivant représente la table vérité de port Z:

Entrée	Sortie
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$-\|1\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$

Tab 1.4: *Table de vérité de la porte quantique ≪ Z ≫.*

Remarque :

Le carré d'une matrice de Pauli est la matrice d'identité :

$X^2 = Y^2 = Z^2 = I.$

I.4.1.2. Porte Hadamard :

Une autre transformation très importante à un seul qubit est la transformation de Hadamard noté H :

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \tag{1.16}$$

Cette porte est généralement utilisée pour générer des superpositions. [1]

La table de vérité de Hadamard est donnée par :

Entrée	Sortie
$\|0\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$
$\|1\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$
$\alpha\|0\rangle + \beta\|1\rangle$	$\frac{\alpha+\beta}{\sqrt{2}}\|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}\|1\rangle$

Tab 1.5: *Table de vérité de la porte quantique* $\ll Hadamard \gg$.

I.4.2. Portes multi-Qubits :

❖ Portes contrôlées :

Les portes contrôlées agissent sur 2 qubits ou plus, où un ou plusieurs qubits agissent comme un contrôle pour certaines opérations.

- N'effectue l'opération sur les qubits cibles que lorsque la valeur de qubit de contrôle est $|1\rangle$
- Sinon, rien à faire.

La représentation graphique d'une porte contrôlée est la suivante:

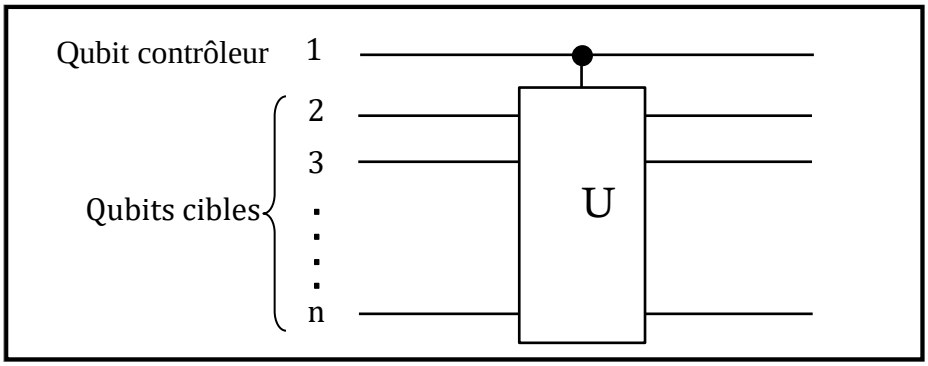


Fig.1.1: *Porte contrôlée.*

❖ Porte SWAP:

La porte SWAP (échange) comme son nom l'indique va échanger les coefficients entre les qubits [10]. Elle est donnée par la matrice suivante :

$$SWAP = S = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (1.17)$$

Entrée	Sortie
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|10\rangle$
$\|10\rangle$	$\|01\rangle$
$\|11\rangle$	$\|11\rangle$
$\alpha\|00\rangle + \beta\|01\rangle + \gamma\|10\rangle + \delta\|11\rangle$	$\alpha\|00\rangle + \gamma\|01\rangle + \beta\|10\rangle + \delta\|11\rangle$

Tab 1.6: *Table de vérité de la porte quantique ≪ Swap ≫.*

Sa représentation graphique est la suivante:

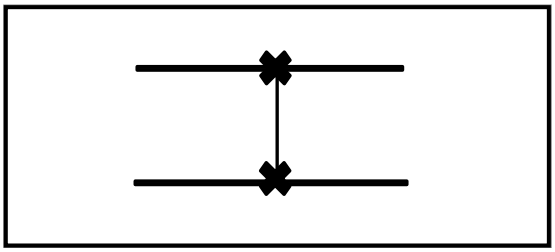


Fig.1.2: *Porte Swap.*

❖ Porte Not contrôlé (CNOT) :

Le **CNot** est un cas particulier des portes contrôlées. Il s'agit d'une transformation X contrôlée :

$$CNOT \equiv I \oplus X \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad (1.18)$$

Entrée	Sortie
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$
$\alpha\|00\rangle + \beta\|01\rangle + \gamma\|10\rangle + \delta\|11\rangle$	$\alpha\|00\rangle + \beta\|01\rangle + \delta\|10\rangle + \gamma\|11\rangle$

Tab 1.7: *Table de vérité de porte « CNOT ».*

Sa représentation graphique est la suivante:

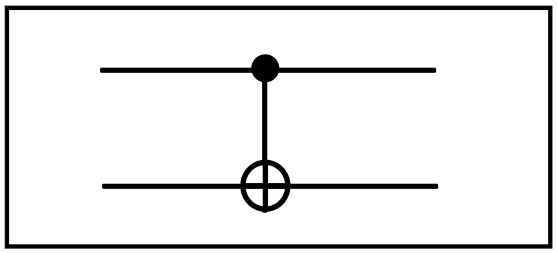


Fig.1.3: *Porte quantique « CNOT ».*

❖ Porte Toffoli :

C'est une porte qui agissent sur trois qubits, dont les deux premiers sont des qubits de contrôles et le troisième est un qubit de transformation, Qui fait la négation du dernier qubit parmi les trois si et seulement si les deux premiers sont tous les deux à 1.

$$\text{TOFFOLI} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad (1.19)$$

La table de vérité de Toffoli est présentée comme suit :

Entrée	Sortie
$\|000\rangle$	$\|000\rangle$
$\|001\rangle$	$\|001\rangle$
$\|010\rangle$	$\|010\rangle$
$\|011\rangle$	$\|011\rangle$
$\|100\rangle$	$\|100\rangle$
$\|101\rangle$	$\|101\rangle$
$\|110\rangle$	$\|111\rangle$
$\|111\rangle$	$\|110\rangle$
$a_1\|000\rangle + a_2\|001\rangle + a_3\|010\rangle + a_4\|011\rangle$ $+a_5\|100\rangle + a_6\|101\rangle + a_7\|110\rangle + a_8\|111\rangle$	$a_1\|000\rangle + a_2\|001\rangle + a_3\|010\rangle + a_4\|011\rangle$ $+a_5\|100\rangle + a_6\|101\rangle + a_7\|111\rangle + a_8\|110\rangle$

Tab 1.8: *Table de vérité de porte « $Toffoli$ ».*

Sa représentation graphique est la suivante :

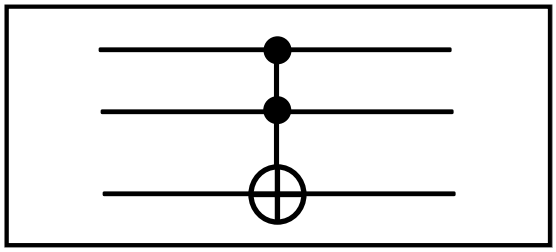


Fig.1.4: *Porte quantique «* Toffoli *».*

I.5. Circuits quantiques :

Un circuit quantique est une combinaison de deux ou plusieurs portes quantiques permettant d'effectuer un traitement plus compliqué sur un système quantique**.** [4]

Ces dernières peuvent être combinées en série ou en parallèle selon le traitement souhaité.

I.5.1. Composition en série :

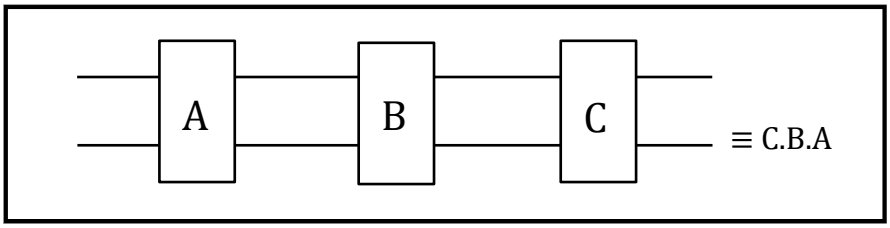
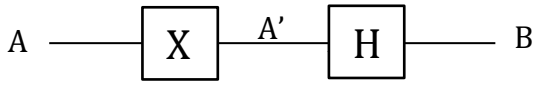


Fig.1.5: *Circuit avec composition en série.*

- La matrice globale est calculée par un produit cartésien dans le sens inverse des matrices correspondantes aux portes. [11]

Exemple :

Dans ce circuit :



$$|A'\rangle = \mathrm{X}\,|\mathrm{A}\rangle = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\beta\\ \alpha\end{pmatrix}$$

$$|\mathrm{B}\rangle = \mathrm{H}\,|A'\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}\beta\\ \alpha\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}\beta+\alpha\\ \beta-\alpha\end{pmatrix}$$

La matrice de transfert globale T est donnée par :

$$\mathrm{T} = \mathrm{H}\,.\,\mathrm{X} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}.\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}$$

Tel que :

$$|\mathrm{B}\rangle = \mathrm{T}\,|\mathrm{A}\rangle$$

$$|\mathrm{B}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}\beta+\alpha\\ \beta-\alpha\end{pmatrix}$$

I.5.2. Composition parallèle :

Ce type de composition peut être représenté par la figure suivante :

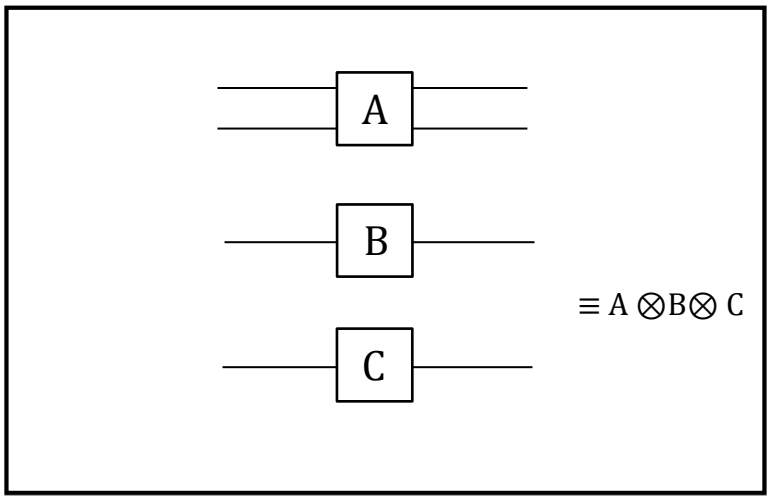
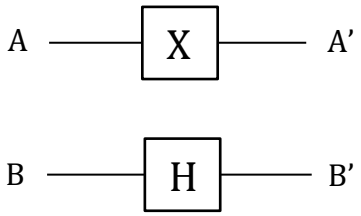


Fig.1.6: *Circuit avec composition parallèle.*

- L'obtention de la matrice globale dans cette composition est calculée par un produit tensoriel des matrices correspondantes aux portes utilisées [11].

Exemple :



On a : $|A'\rangle = X\,|A\rangle = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\beta\\ \alpha\end{pmatrix}$

$|B'\rangle = H\,|B\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}\gamma\\ \delta\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}\gamma+\delta\\ \gamma-\delta\end{pmatrix}$

Le traitement séparé de ces deux qubits donne comme résultat :

$$|A'B'\rangle = \begin{pmatrix}\beta\\ \alpha\end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix}\gamma+\delta\\ \gamma-\delta\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}\beta\gamma+\beta\delta\\ \beta\gamma-\beta\delta\\ \alpha\gamma+\alpha\delta\\ \alpha\gamma-\alpha\delta\end{pmatrix}$$

Passant maintenant au calcul de la matrice globale T, on a :

$$|A'B'\rangle = T\,|AB\rangle$$

Tel que :

$$T = X \otimes H = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\\ 1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\end{pmatrix}$$

$$|AB\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \otimes \begin{pmatrix}\gamma\\ \delta\end{pmatrix} = \begin{pmatrix}\alpha\gamma\\ \alpha\delta\\ \beta\gamma\\ \beta\delta\end{pmatrix}$$

Donc :

$$|A'B'\rangle = T\,|AB\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\\ 1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\end{pmatrix}\begin{pmatrix}\alpha\gamma\\ \alpha\delta\\ \beta\gamma\\ \beta\delta\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}\beta\gamma+\beta\delta\\ \beta\gamma-\beta\delta\\ \alpha\gamma+\alpha\delta\\ \alpha\gamma-\alpha\delta\end{pmatrix}$$

I.6. Conclusion :

Dans ce chapitre, nous avons présenté les notions les plus importantes liées au domaine de traitement quantique de l'information, On a donné un aperçu sur le formalisme mathématique utilisé ainsi que les postulats contrôlant cette théorie.

En termes de calcul, on a présenté les différentes portes quantiques en donnant les matrices de transformation correspondantes. Aussi, on a abordé les différentes compositions possibles des circuits quantiques.

Nous avons constaté que c'est un domaine spécifique caractérisé par des phénomènes très étranges par rapport au calcul classique. Les plus importants sont la superposition, l'intrication et la mesure d'états.

Le chapitre suivant sera consacré aux algorithmes de correction d'erreurs quantiques.