Chapitre II : Correction d'erreurs

II.1. Introduction :

Dans un système quantique, L'information contenue dans des états quantiques est très sensible. Cela est dû à l'interaction avec l'environnement ce qui provoque une grande perturbation des qubits et engendre des erreurs. Pour remédier à ce problème, les codes correcteurs sont largement utilisés. Ils permettent la détection et la correction de toute anomalie possible.

La correction d'erreurs quantiques est un élément essentiel du calcul de tolérance aux pannes qui doit gérer non seulement les erreurs touchant les informations stockées, mais aussi celles provoquées par l'application des portes quantiques, la préparation de nouveaux états ainsi que le processus de mesure.

Dans le cas classique, les techniques de correction d'erreurs sont basées sur l'ajout d'informations redondantes (codage) pour protéger les informations, tandis que les codes quantiques utilisent l'intrication pour délocaliser les informations codées sur plusieurs systèmes physiques.

Dans ce chapitre, nous nous intéressons à la correction d'erreurs. Comme introduction aux algorithmes quantiques, on a opté pour la présentation de l'algorithme de factorisation de Shor. Le reste du chapitre est consacré aux différentes variantes des codes stabilisateurs.

II.2. Algorithme de factorisation de Shor :

Dans les transactions importantes, les données sont souvent sécurisées via des protocoles cryptographiques puissants. Ils sont fondés principalement sur la difficulté de factoriser des nombres entiers de grandes tailles. Cette opération est très couteuse en termes de complexité algorithmiques [12].

En 1994, Peter Shor [13, 14] a publié un article qui a suscité beaucoup de réactions. Il a proposé un algorithme très intéressant permettant de factoriser les grands nombres entiers en un temps polynomial. Il est basé sur une procédure quantique dite transformée de Fourier quantique.

Algorithme :

a) Choisir a au hasard, $1< a <P$.

b) Si $PGCD\ (a, P) = 1$, continuer.
Sinon, le problème est résolu !

c) Autrement, utiliser le sous-programme de recherche de période (ci-dessous) pour trouver r, la période de la fonction suivant :

$$f_a(k) = a^k \bmod P.$$

On a alors :

$$a^r = 1 \bmod P.$$

d) Si r est pair, alors :

$$(a^{r/2}+1)\ (a^{r/2}- 1) = 0 \bmod P.$$

Si r est aussi tel que $a^{\frac{r}{2}} \neq \pm 1 \bmod P$, alors :

$$PGCD\ (a^{r/2}+1, P)$$

Et

$PGCD\ (a^{r/2}- 1, P)$ sont des facteurs de P : stop !

Sinon, retourner au pas a.

Dans cet algorithme, la partie quantique calculant la période est réalisée par le circuit suivant:

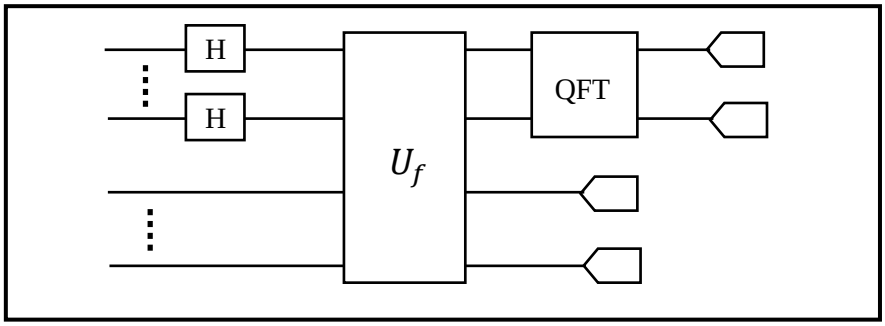

Fig.2.1 : *Le circuit quantique calculant la période.*

II.3. Particularités du cas quantique :

Les techniques utilisées pour la détection d'erreurs dans le cas classique sont basées sur l'ajout d'informations redondantes (codage). Cela permet de tester si le message codé a été perturbé et de corriger les erreurs. Parmi ces codes, le plus simple est le codage à trois bits. Il consiste à tripler chaque bit d'information :

- $0 \rightarrow 000$.
- $1 \rightarrow 111$.

On suppose que la probabilité d'erreur est suffisamment faible pour que la probabilité que deux erreurs surviennent simultanément soit négligeable. Donc après avoir traversé un canal susceptible de créer une erreur, le triplet de bits peut se retrouver avec au plus un bit inversé. La détection de l'erreur se fait en testant si tous les bits sont égaux ou non. En cas d'inégalités, on utilise la règle de la majorité pour rétablir la bonne valeur logique associée au triplet. C'est ce qu'on appelle le décodage.

Mais La transposition au cas quantique de ce code simple n'est pas immédiate pour plusieurs raisons :

- ✓ la structure du qubit est différente de celle du bit classique.
- ✓ Les erreurs quantiques possibles sont plus nombreuses que celles classiques.
- ✓ Pas de clonage: il est impossible de dupliquer des états quantiques pour obtenir le code de répétition.
- ✓ un continuum d'erreurs différentes peut se produire sur un seul qubit, déterminer quelle erreur s'est produite afin de la corriger nécessiterait une précision infinie.
- ✓ les informations quantiques sont détruites par la mesure et ne peuvent pas être récupérées.

II.4. Codes de correction à répétition :

II.4.1. Correction d'erreur de type X ou Bit-flip :

Le circuit de corriger une erreur de type X est le suivant [17]:

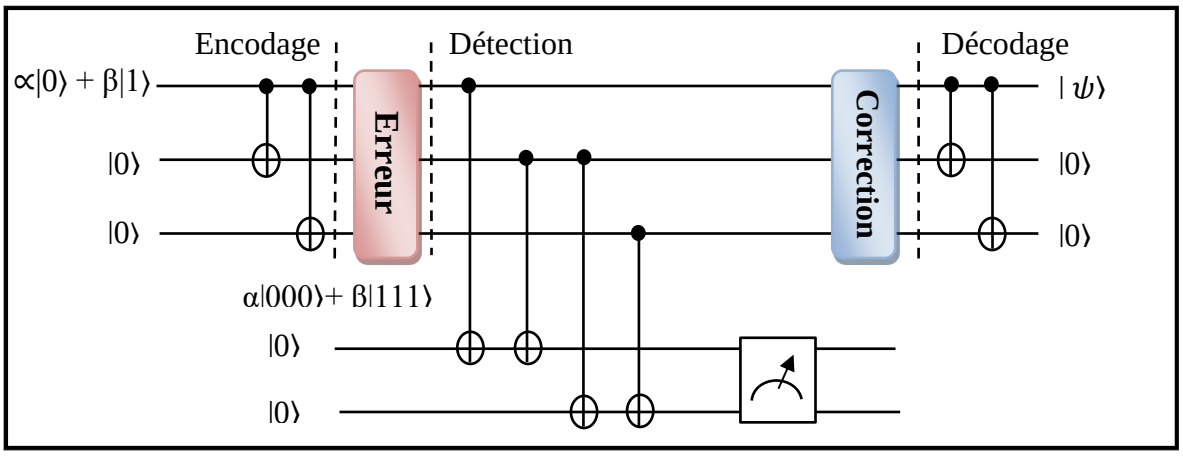

Fig.2.2 : *Circuit de correction d'erreurs de type « X ».*

❖ Encodage :

Soit le qubit $|\psi\rangle$ défini par : $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

L'étape d'encodage est basée sur une redondance spécifique. Elle consiste à l'ajout de deux qubits intriqués au qubit initial. Elle est réalisée en appliquant deux portes CNot.

- ➢ L'état initial : $|\psi_1\rangle = \alpha|000> + \beta|100>$
- ➢ L'application du CNot (1,2) donne l'état : $|\psi_2\rangle = \alpha|000> + \beta|110>$
- ➢ L'application du CNot (1,3) donne l'état : $|\psi_3\rangle = \alpha|000> + \beta|111>$

L'encodage d'un qubit : $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ donne un état quantique $|\psi_3\rangle$ de trois qubits tel que: $|\psi_3\rangle = \alpha|000\rangle + \beta|111\rangle$

❖ Détection :

La détection d'erreurs X est basée sur l'utilisation de deux qubits supplémentaires initialisés à $|0\rangle$ comme syndrome. Ce dernier est calculé par quatre portes CNot. Dans la suite, nous présentons les quatre cas possibles.

- **Cas 01 : sans erreur :**

$$|\psi_4\rangle = \alpha|000\rangle + \beta|111\rangle$$

✓ L'ajout des deux qubits du syndrome donne l'état :

$$|\psi_5\rangle = \alpha|00000\rangle + \beta|11100\rangle$$

✓ L'application des portes CNot donne les états suivants :

$$C[1,4] \Longrightarrow |\psi_6\rangle = \alpha|00000\rangle + \beta|11110\rangle$$

$$C[2,4] \Longrightarrow |\psi_7\rangle = \alpha|00000\rangle + \beta|11100\rangle$$

$$C[2,5] \Longrightarrow |\psi_8\rangle = \alpha|00000\rangle + \beta|11101\rangle$$

$$C[3,5] \Longrightarrow |\psi_9\rangle = \alpha|00000\rangle + \beta|11100\rangle$$

Dans ce cas : $|\psi_9\rangle = (\alpha|000\rangle + \beta|111\rangle)\,|00\rangle$

- **Cas 02 : Erreur X sur le 1er Qubit :**

$$|\psi_4\rangle = \alpha|100\rangle + \beta|011\rangle$$

✓ L'ajout des deux qubits du syndrome donne l'état :

$$|\psi_5\rangle = \alpha|10000\rangle + \beta|01100\rangle$$

✓ L'application des portes CNot donne les états suivants :

$$C\,[1,4] \Longrightarrow |\psi_6\rangle = \alpha|10010\rangle + \beta|01100\rangle$$

$$C\,[2,4] \Longrightarrow |\psi_7\rangle = \alpha|10010\rangle + \beta|01110\rangle$$

$$C\,[2,5] \Longrightarrow |\psi_8\rangle = \alpha|10010\rangle + \beta|01111\rangle$$

$$C\,[3,5] \Longrightarrow |\psi_9\rangle = \alpha|10010\rangle + \beta|01110\rangle$$

Dans ce cas : $|\psi_9\rangle = (\alpha|100\rangle + \beta|011\rangle)\,|10\rangle$

- **Cas 03 : Erreur X sur le 2eme Qubit :**

$$|\psi_4\rangle = \alpha|010\rangle + \beta|101\rangle$$

✓ L'ajout des deux qubits du syndrome donne l'état :

$$|\psi_5\rangle = \alpha|01000\rangle + \beta|10100\rangle$$

✓ L'application des portes CNot donne les états suivants :

$$C\,[1,4] \Longrightarrow |\psi_6\rangle = \alpha|01000\rangle + \beta|10110\rangle$$

$$C\,[2,4] \Longrightarrow |\psi_7\rangle = \alpha|01010\rangle + \beta|10110\rangle$$

$$C\,[2,5] \Longrightarrow |\psi_8\rangle = \alpha|01011\rangle + \beta|10110\rangle$$

$$C\,[3,5] \Longrightarrow |\psi_9\rangle = \alpha|01011\rangle + \beta|10111\rangle$$

Dans ce cas : $|\psi_9\rangle = (\alpha|010\rangle + \beta|101\rangle)\,|11\rangle$

- **Cas 04 : Erreur X sur le 3eme Qubit :**

$$|\psi_4\rangle = \alpha|001\rangle + \beta|110\rangle$$

✓ L'ajout des deux qubits du syndrome donne l'état :

$$|\psi_5\rangle = \alpha|00100\rangle + \beta|11000\rangle$$

✓ L'application des portes CNot donne les états suivants :

$$C\,[1,4] \Longrightarrow |\psi_6\rangle = \alpha|00100\rangle + \beta|11010\rangle$$

$$C\,[2,4] \Longrightarrow |\psi_7\rangle = \alpha|00100\rangle + \beta|11000\rangle$$

$$C\,[2,5] \Longrightarrow |\psi_8\rangle = \alpha|00100\rangle + \beta|11001\rangle$$

$$C\,[3,5] \Longrightarrow |\psi_9\rangle = \alpha|00101\rangle + \beta|11001\rangle$$

Dans ce cas : $|\psi_9\rangle = (\alpha|001\rangle + \beta|110\rangle)\,|01\rangle$

❖ Mesure :

Dans cette étape, les deux qubits du syndrome sont mesurés. Les valeurs obtenues sont suffisantes pour la correction.

❖ Correction :

On applique l'opérateur unitaire X_i^{-1}sur le qubit erroné afin de retrouver son état initial. Comme l'opérateur X est unitaire alors : $X_i^{-1} = X_i$

Cette correction est résumée dans le tableau suivant :

$\|Q_4\ Q_5\rangle$	Correction
$\|00\rangle$	Ne rein faire
$\|01\rangle$	X_3
$\|10\rangle$	X_1
$\|11\rangle$	X_2

Tab 2.1: *Correction d'erreur de type≪ X ≫.*

Ce qui permet de revenir dans tous les cas à l'état : $|\psi_9\rangle = \alpha|000\rangle + \beta|111\rangle$

❖ Décodage :

Le décodage sert à isoler le qubit initial des deux qubits d'intrication. Il est réalisé par application de l'inverse des portes utilisées dans l'étape d'encodage.

- L'état initial : $|\psi_9\rangle = \alpha|000\rangle + \beta|111\rangle$
- L'application du CNot (1,2) donne l'état : $|\psi_{10}\rangle = \alpha|000\rangle + \beta|101\rangle$
- L'application du CNot (1,3) donne l'état : $|\psi_{11}\rangle = \alpha|000\rangle + \beta|100\rangle = |\psi\rangle|00\rangle$

II.4.2. Correction d'erreur de type Z ou Phase-flip :

Comme vu dans le chapitre précédent, les portes X, Z et H sont définies par les matrices unitaires (1.13, 1.15, 1.16).

Calculant la matrice correspondante à la transformation : HZH. [17]

$$HZH \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = X \qquad (2.1)$$

Ce résultat affirme que la correction d'une erreur de type Z se ramène à celle d'une erreur de type X. Il suffit d'ajouter une transformation H à la fin de l'encodage et son inverse (H) avant la détection d'erreur. Donc, le circuit de correction est le suivant :

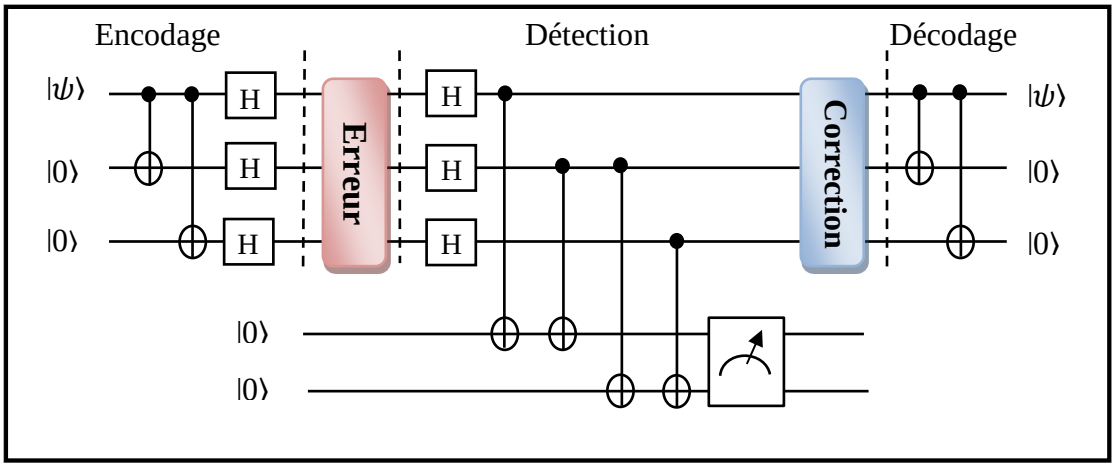

Fig.2.3 : *Circuit de transformation du code phase-flip à trois Qubits.*

Donc, Une erreur de type Z sur un qubit est transformée en une erreur de type X sur le même qubit. Alors, Les étapes suivantes sont les mêmes vues dans le traitement des erreurs X.

II.4.3. Correction d'erreur de type Y:

De même, Calculant :

$$iZX \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = Y \qquad (2.2)$$

Donc, une erreur Y peut être corrigée par application d'un correcteur d'erreurs Z suivi d'un correcteur d'erreurs X. [17]

II.5. Algorithme de Shor :

Un système quantique pourrait avoir des erreurs de type X, Y et Z. Shor a développé un code de correction universel capable de corriger ces trois types d'erreurs à la fois [17]. L'idée principale est de "concaténer" les deux codes de répétition présentés dans le paragraphe précédent :

- ✓ Un correcteur protégeant le qubit $|\psi\rangle$ des erreurs de type Z. Il utilise deux qubits supplémentaires.
- ✓ Chacun de ces trois qubits est protégé à son tour par un correcteur des erreurs de type X.
- ✓ Donc, c'est un correcteur à 9 qubits. Le schéma suivant donne l'architecture globale de cette solution

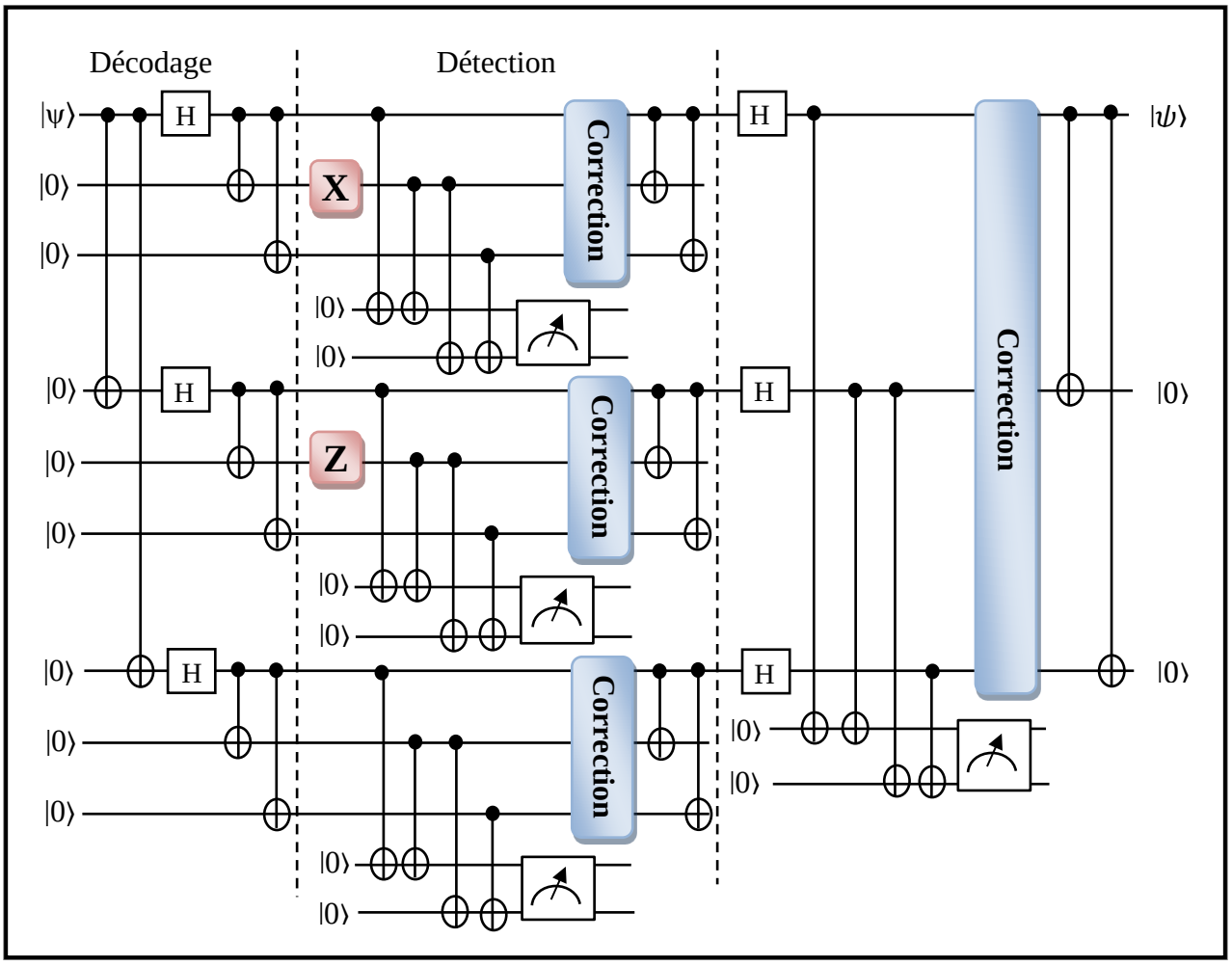

Fig.2.4: *Circuit de correction de Shor.*

II.6. Codes stabilisateurs quantiques :

Les codes stabilisateurs sont une idée originale de Daniel Gottesman, Peter Shor et Andrew Steane [15], Ils sont basés principalement sur les algèbres des opérateurs de Pauli.

II.6.1. Idée de base :

Afin d'introduire les codes stabilisateurs, prenons un cas très simple. Soit le qubit $|\psi\rangle$ défini par :

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

En premier lieu nous effectuons l'étape d'encodage en rajoutant des qubits redondants, Elle est réalisée en appliquant deux portes CNot :

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \rightarrow |\psi\rangle\,|00\rangle = \alpha\,|0\rangle\,|00\rangle + \beta\,|1\rangle\,|00\rangle \xrightarrow{\text{codage}} |\psi\rangle_c = \alpha\,|000\rangle + \beta\,|111\rangle$$

Supposons maintenant que le seul type d'erreur qui affecte le qubit $|\psi\rangle_c$ soit un bit-flip (réalisée par l'action de l'opérateur X); il y a trois possibilités :

$$X_1\ [\alpha|000\rangle + \beta|111\rangle] = \alpha|100\rangle + \beta|011\rangle$$

$$X_2\ [\alpha|000\rangle + \beta|111\rangle] = \alpha|010\rangle + \beta|101\rangle$$

$$X_3\ [\alpha|000\rangle + \beta|111\rangle] = \alpha|001\rangle + \beta|110\rangle$$

La technique basée sur les codes stabilisateurs procède de la manière suivante :

- ✓ On définit des opérateurs de syndrome qui ont la particularité d'avoir comme états propres les états erronés ainsi que l´état non perturbe.
- ✓ On mesure ces operateurs; La mesure des opérateurs de syndrome s'effectue sur le qubit auxiliaire associé. Les états, erronés ou non, ne sont pas modifiés puisqu'ils sont états propres et le résultat de la mesure (les valeurs propres) signent sans ambiguïté la position de l'erreur. Il suffit alors d'apporter la correction.

La mesure quantique de chacune des valeurs propres est mise en œuvre par le circuit suivant

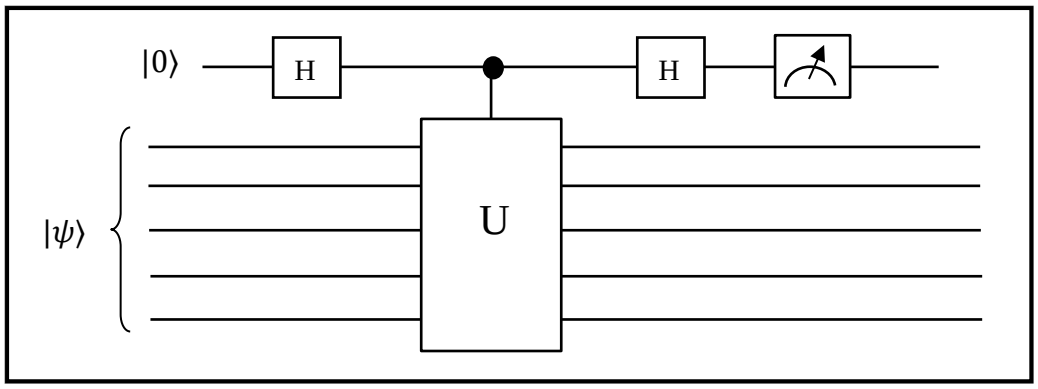

Fig.2.5: *Circuit quantique pour la mesure des syndromes.*

- On utilise un qubit auxiliaire $|0\rangle$ que l'on fait passer une porte Hadamard, l'état est alors de :

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |\psi\rangle$$

- On effectue une porte U contrôlée par le qubit auxiliaire conduisant :

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

- On effectue de nouveau une porte Hadamard sur le qubit auxiliaire ce qui donne :

$$\frac{1}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}|\psi\rangle + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\ \mathrm{U}|\psi\rangle\right) = |0\rangle\frac{|\psi\rangle + \mathrm{U}|\psi\rangle}{2} + |1\rangle\frac{|\psi\rangle\ - \mathrm{U}|\psi\rangle}{2}$$

- On mesure ensuite le qubit auxiliaire.
  - ✓ Si on obtient 0 la valeur propre est 1.
  - ✓ Par contre, si on obtient 1 la valeur propre est -1.

Dans notre cas, nous utilisons les opérateurs de syndrome : $S_1 = Z_1Z_2$ et $S_2 = Z_1Z_3$.

- ✓ Les deux opérateurs Z_1Z_2 et Z_1Z_3 forment un groupe S, appelé stabilisateur du code.
- ✓ Z_1Z_2 et Z_1Z_3 sont appelés générateurs de ce groupe.

Le tableau ci-dessous indique les valeurs propres du couple (S_1,S_2) pour chaque type d'erreur.

$|\psi_0\rangle = |\psi\rangle = \ \alpha|000\rangle + \beta|111\rangle \ \rightarrow\ (+1, +1)$

$|\psi_1\rangle = X_1|\psi\rangle = \ \alpha|100\rangle + \beta|011\rangle \ \rightarrow\ (-1, -1)$

$|\psi_2\rangle = X_2|\psi\rangle = \ \alpha|010\rangle + \beta|101\rangle \ \rightarrow\ (-1, +1)$

$|\psi_3\rangle = X_3|\psi\rangle = \ \alpha|001\rangle + \beta|110\rangle \ \rightarrow\ (+1, -1)$

Remarques :

- ➢ Les états erronés ainsi que l'état sans erreur sont des vecteurs propres des deux opérateurs de syndromes.
- ➢ les valeurs propres calculées pour chaque cas sont appelées syndromes.
- ➢ Seul le mot de code valide est un vecteur propre des opérateurs de syndromes.
- ➢ Par linéarité des opérations quantique, l'encodage d'un état : $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

  Donne : $|\psi\rangle_c = \alpha|0\rangle_c + \beta|1\rangle_c$

  Cette notation sera utilisée dans le reste de ce mémoire.

- ➢ Les opérations quantiques nécessaires dans l'étape de décodage sont les mêmes utilisées dans le processus d'encodage, mais elles doivent être appliquées dans l'ordre inverse.

II.6.2. Code à neuf Qubits :

❖ Encodage :

$|0\rangle_c = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$

$= \frac{1}{2\sqrt{2}}(|000000000\rangle + |000000111\rangle + |000111000\rangle + \ldots)$

$|1\rangle_c = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$

$= \frac{1}{2\sqrt{2}}(|000000000\rangle - |000000111\rangle - |000111000\rangle + |000111111\rangle + \cdots)$

- Le circuit d'encodage correspondant est donné dans le chapitre précèdent.

❖ Groupe stabilisateur :

	8	7	6	5	4	3	2	1	0
M0	Z	Z	I	I	I	I	I	I	I
M1	Z	I	Z	I	I	I	I	I	I
M2	I	I	I	Z	Z	I	I	I	I
M3	I	I	I	Z	I	Z	I	I	I
M4	I	I	I	I	I	I	Z	Z	I
M5	I	I	I	I	I	I	Z	I	Z
M6	X	X	X	X	X	X	I	I	I
M7	X	X	X	I	I	I	X	X	X

Tab 2.2: *Les stabilisateurs pour le code à 9 Qubits.*

❖ Calcul des syndromes :

La détection du syndrome associé à chaque type d'erreur est réalisée par le circuit suivant:

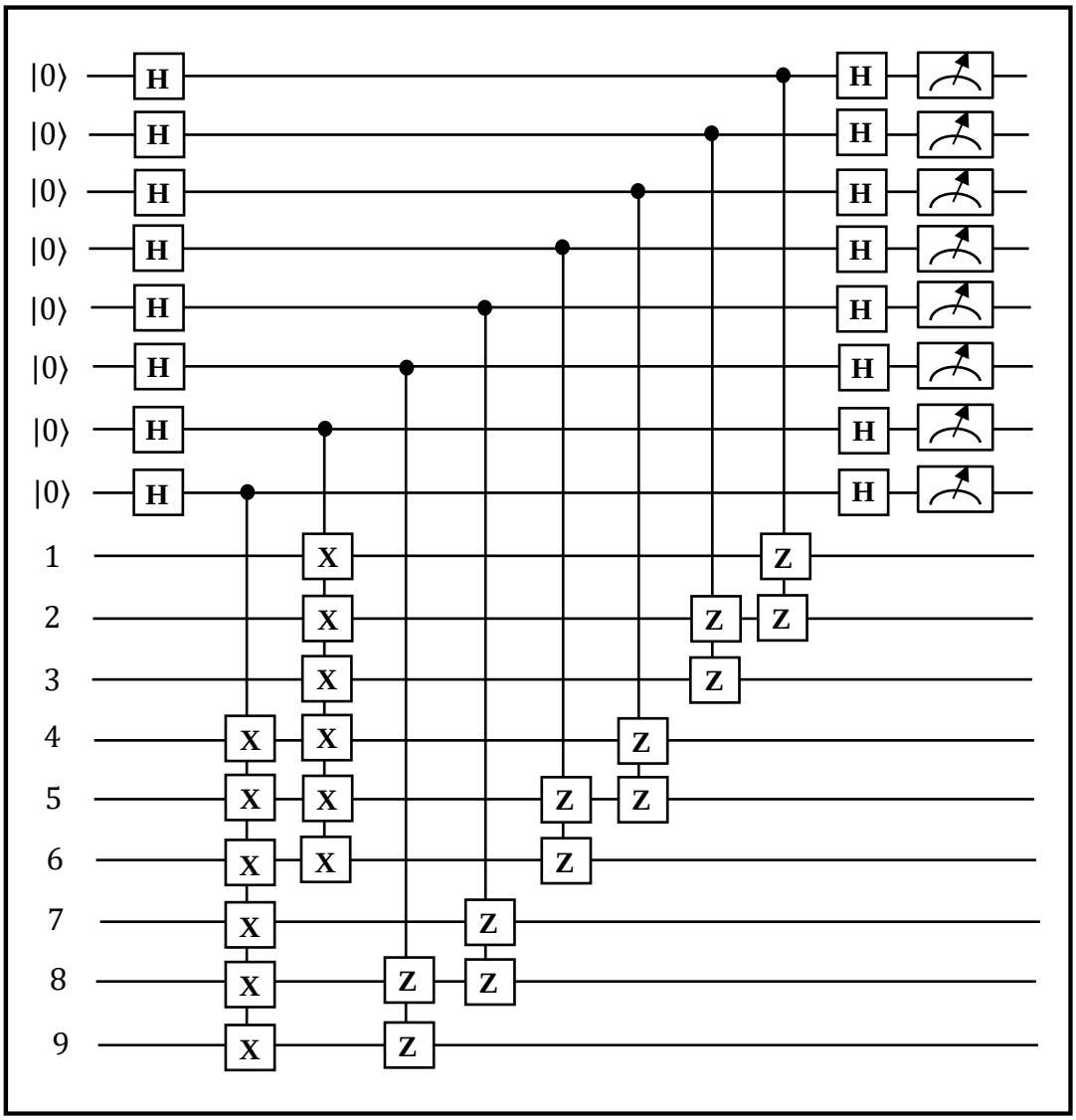

Fig.2.6: *Circuit pour la mesure du syndrome d'erreur du code correcteur à 9 Qubits.*

❖ Décodage :

De même, le circuit décodage correspondant est donné dans le chapitre précèdent.

II.6.3. Code à sept Qubits :

❖ Encodage :

$$|0\rangle_c = \frac{1}{\sqrt{8}} (1 + M_0)(1 + M_1)(1 + M_2)\,|0000000\rangle$$

$$|1\rangle_c = \frac{1}{\sqrt{8}} (1 + M_0)(1 + M_1)(1 + M_2)\,|1111111\rangle$$

Le circuit d'encodage correspondant est le suivant [16]:

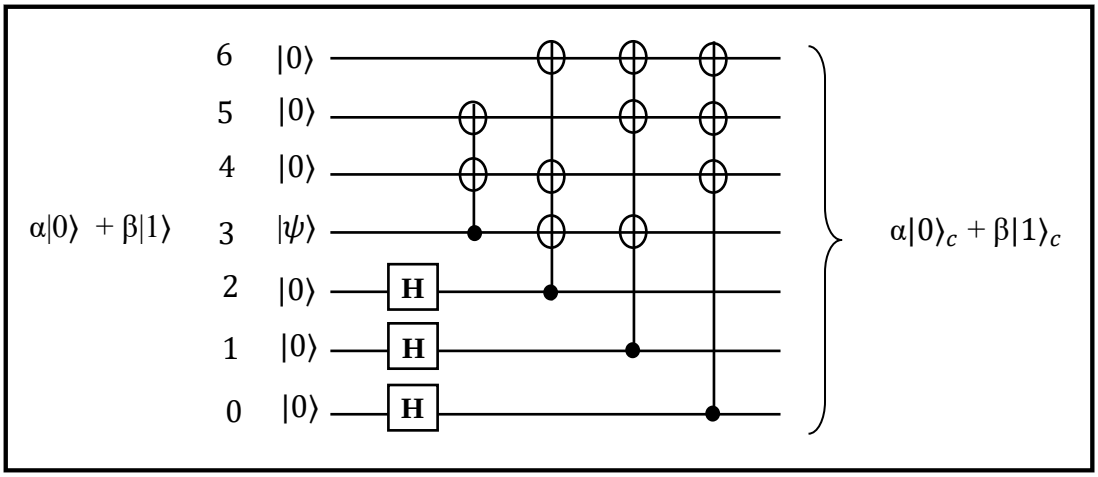

Fig.2.7: *Circuit quantique pour l'encodage d'un Qubit en 7 Qubits.*

❖ Groupe stabilisateur :

Le stabilisateur de code à sept qubits qu'on va utiliser est donné dans le tableau suivant :

	6	5	4	3	2	1	0
M_0	X	X	X	I	I	I	X
M_1	X	X	I	X	I	X	I
M_2	X	I	X	X	X	I	I
M_3	Z	Z	Z	I	I	I	Z
M_4	Z	Z	I	I	Z	I	Z
M_5	Z	I	Z	Z	Z	I	I

Tab 2.3: *Les stabilisateurs pour le code à 7 Qubits.*

❖ Calcul des syndromes :

Le circuit utilisé pour calculer les valeurs des syndromes pour sept qubits est illustré dans la page suivante [16]:

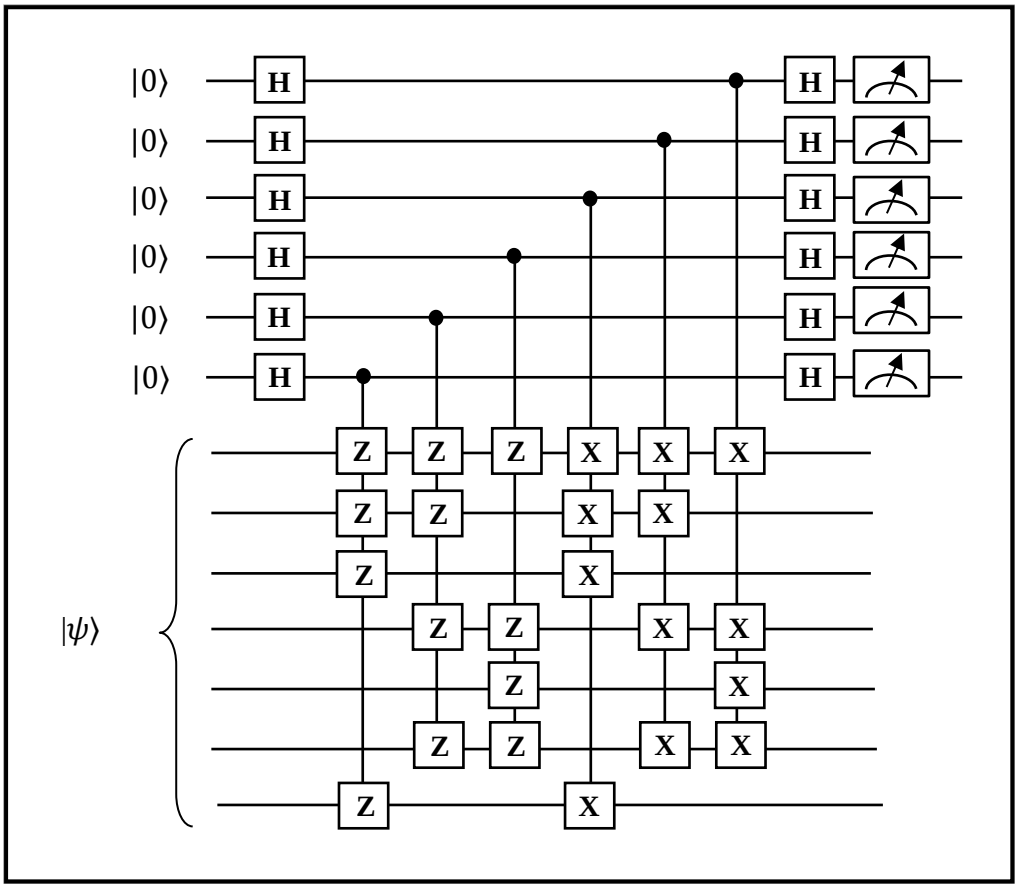

Fig.2.8: *Circuit quantique à 7 Qubits pour la détection des syndromes d'erreur.*

Les syndromes d'erreurs sont résumés dans le tableau qui suit :

	$X_0Y_0Z_0$	$X_1Y_1Z_1$	$X_2Y_2Z_2$	$X_3Y_3Z_3$	$X_4Y_4Z_4$	$X_5Y_5Z_5$	$X_6Y_6Z_6$	1
M_0	− − +	+ + +	+ + +	+ + +	− − +	− − +	− − +	+
M_1	+ + +	− − +	+ + +	− − +	+ + +	− − +	− − +	+
M_2	+ + +	+ + +	− − +	− − +	− − +	+ + +	− − +	+
M_3	+ − −	+ + +	+ + +	+ + +	+ − −	+ − −	+ − −	+
M_4	+ + +	+ − −	+ + +	+ − −	+ + +	+ − −	+ − −	+
M_5	+ + +	+ + +	+ − −	+ − −	+ − −	+ + +	+ − −	+

Tab 2.4: *Syndromes d'erreur pour le code à 7 Qubits.*

❖ Décodage :

Le circuit de décodage est représenté dans la page suivante :

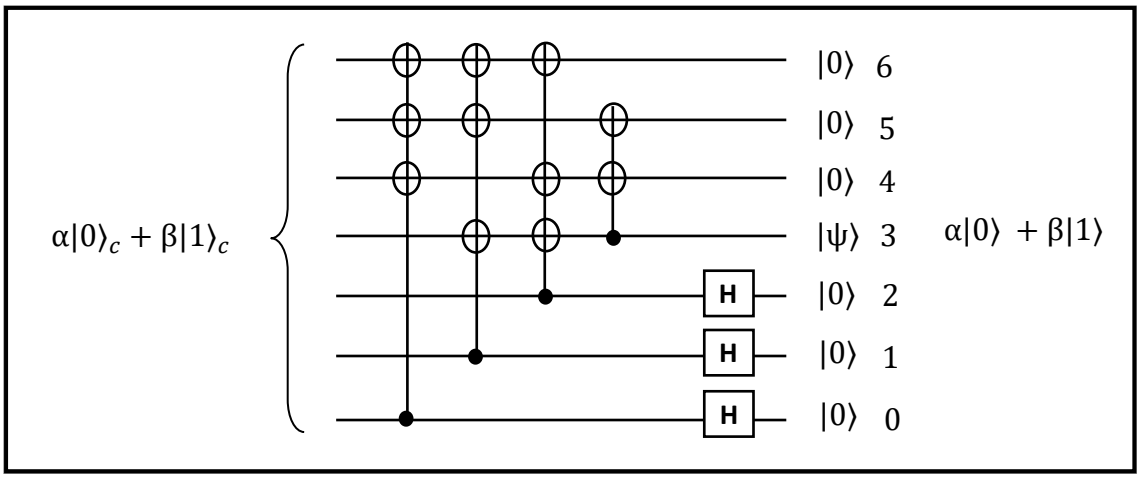

Fig.2.9**:** *Circuit quantique pour le décodage de 7 Qubits.*

II.6.4. Code à Cinq Qubits :

❖ Encodage :

$$|0\rangle_c = \frac{1}{4}(1 + M_0)(1 + M_1)(1 + M_2)(1 + M_3)|00000\rangle$$

$$|1\rangle_c = \frac{1}{4}(1 + M_0)(1 + M_1)(1 + M_2)(1 + M_3)|11111\rangle$$

Le circuit d'encodage [16] :

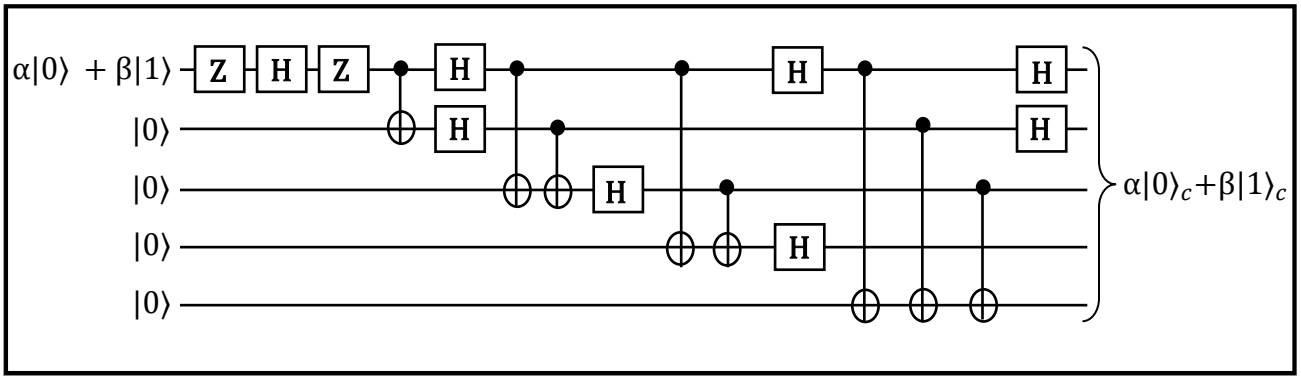

Fig.2.10 : *Circuit pour coder un Qubit sur 5 Qubits.*

❖ Groupe stabilisateur :

Le stabilisateur de code à cinq qubits utilisé est donné dans le tableau suivant [16] :

	4	3	2	1	0
M_0	Z	X	X	Z	I
M_1	X	X	Z	I	Z
M_2	X	Z	I	Z	X
M_3	Z	I	Z	X	X

Tab 2.5: *Les stabilisateurs pour le code à 5 Qubits.*

Le circuit quantique permettant de réaliser ces calculs est le suivant [16]:

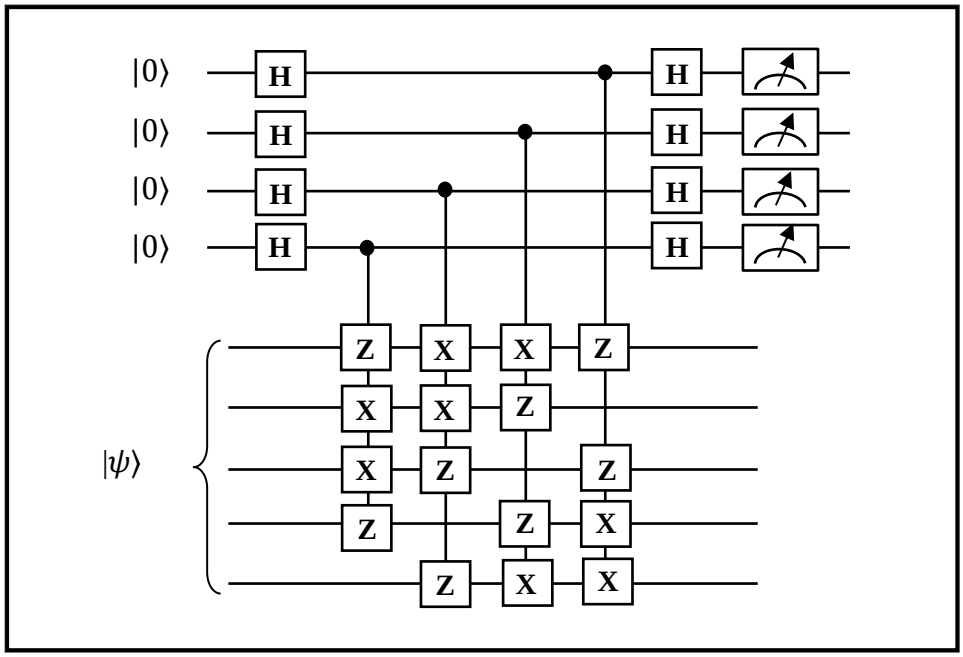

Fig.2.11 : *Circuit quantique à 5 Qubits pour la détection des syndromes d'erreur.*

❖ Calcul syndromes :

Les valeurs propres associées à chaque cas sont les suivantes :

	$X_0Y_0Z_0$	$X_1Y_1Z_1$	$X_2Y_2Z_2$	$X_3Y_3Z_3$	$X_4Y_4Z_4$	1
M_0	+ + +	− − +	+ − −	+ − −	− − +	+
M_1	− − +	+ + +	− − +	+ − −	+ − −	+
M_2	+ − −	− − +	+ + +	− − +	+ − −	+
M_3	+ − −	+ − −	− − +	+ + +	− − +	+

Tab 2.6: *Syndromes d'erreur pour le code à 5 Qubits.*

❖ Décodage :

Le circuit de décodage est le suivant :

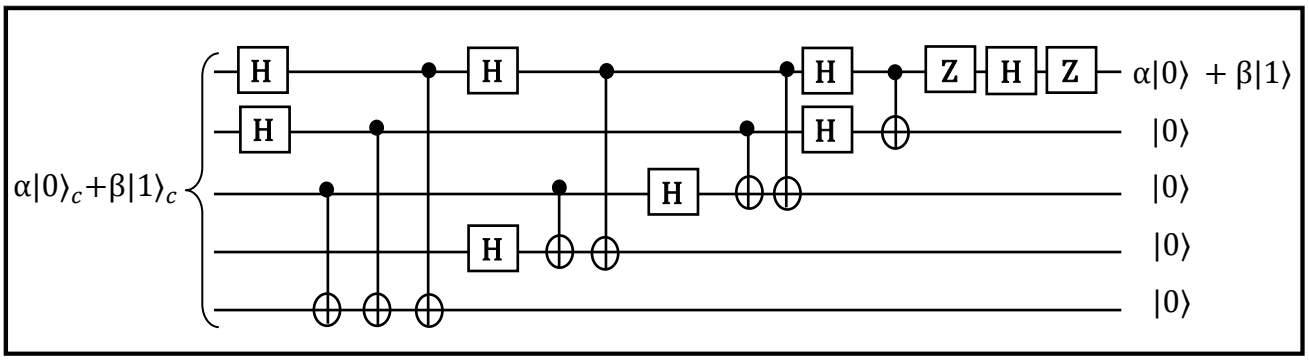

Fig.2.12 : *Circuit quantique pour le décodage de 5 Qubits.*

Remarques :

- Le code à cinq qubits est le code quantique permettant la correction d'erreurs le plus optimal. C'est le code le plus court et donc il est d'un intérêt immense [18], [8].
- $M_i^2 = I$ pour tous car : $X^2 = Y^2 = Z^2 = I$.
- $M_i M_j = M_j M_i$ donc tout couple M_i, M_j commute et M_i (1 +M_i) = (1 +M_i).
- $|0\rangle_c$ et $|1\rangle_c$ est un vecteur propre de tous les M_i.
- Il est possible de vérifier qu'en appliquant une erreur X_k (Y_k ou Z_k), les $X_k|\psi\rangle$, $Y_k|\psi\rangle$, et $Z_k|\psi\rangle$ sont également des vecteurs propres de tous les Mi , mais avec des ensembles différents d'états propres .
- La mesure de tous les M_i ne modifie pas l'état traité.
- Le résultat de la mesure signe sans ambiguïté la position de l'erreur.

II.7. Conclusion :

Les recherches affirment qu'un système quantique est très sensible aux erreurs dues à l'interaction avec l'environnement. De ce fait, la correction d'erreurs quantiques est une opération inévitable et joue un rôle très important.

Dans ce chapitre nous avons présenté quelques variantes des algorithmes de correction d'erreurs quantiques. Ils permettent la détection et la correction des erreurs de type X, Y et Z.

- L'algorithme de Shor : C'est un correcteur basé sur une redondance implémentée en s'appuyant sur le concept d'intrication. Cette solution nécessite l'utilisation de huit qubits supplémentaires.
- Les codes stabilisateurs : nous avons présenté trois techniques : Un code à 9 qubits équivalent à celui de Shor, un autre à 7 qubits et enfin un dernier à 5 qubits.

Dans le chapitre suivant, nous présentons un correcteur plus optimal. C'est un code stabilisateur à 5 Qubits mais nécessitant dix portes quantique d'encodage seulement.