8.1 Code de Steane

Le code de Shor fonctionnant sur 9 qubits, il est difficile à manipuler. Par conséquent, il est normal de réfléchir à des solutions permettant de corriger les erreurs en codant sur moins de qubits.

Il a été démontré qu'un code correcteur quantique nécessite au minimum 5 qubits pour des erreurs n'affectant qu'un seul qubit. Il existe une construction de ce code correcteur à 5 qubits.

Cependant, nous allons étudier une autre version correctrice codant sur 7 qubits, le code de Steane, qui est plus simple à aborder que le code à 5 qubits.

8.1.1 Code de Hamming

Le code de Hamming est un code correcteur qui utilise 7 bits pour en encoder 4. Il permet de corriger une erreur portant sur un seul bit sans avoir d'information sur le mot codé.

Fonctionnement : Dans un premier temps, il faut associer à chaque chaine de bits de $\{0,1\}^4$ une chaine de $\{0,1\}^7$. Ces $2^4 = 16$ chaines $\{v_k\}_{k\in\{1,16\}}$ sont choisies selon la relation : $Hv_k = 0\,(mod\,2)$ avec H la matrice de $M_{3,7}(\{0,1\})$:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Lemme 8.1. *L'équation $Hv = 0$ admet 4 solutions linéairement indépendantes.*

Preuve: Si on écrit $v = \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \\ g \end{pmatrix}$ alors la résolution $Hv = 0$ est équivalente au système :

$$\begin{cases} d+e+f+g = 0 \\ b+c+f+g = 0 \\ a+c+e+g = 0 \end{cases} \quad (mod\,2)$$

Étant un système de 3 équations à 7 inconnues, il est de dimension au moins 4. En simplifiant les équations, on trouve :

$$\begin{cases} e = b + c + d \\ f = a + c + d \\ g = a + b + d \end{cases} \quad (mod\, 2)$$

Ces équations étant indépendantes, on en déduit qu'il existe 4 solutions linéairement indépendantes, qu'on peut choisir comme étant :

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \; et \; \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

□

On choisit donc les v_k comme étant les combinaisons linéaires de ces 4 matrices, avec des coefficients choisis dans $\{0, 1\}$. Dès lors, la correction d'erreur se déroule de la manière suivante :
Si on suppose qu'une erreur se produit sur le *ième* bit du mot v_k, alors il y aura une transformation de la forme $v_k \longrightarrow v_k + e_i$ (où par exemple $e_3 = \big(0010000\big)$). On a alors :

$$H(v_k + e_i) = Hv_k + He_i = He_i$$

qui correspond à la *ième* colonne de H. Toutes les colonnes de H étant distinctes, on peut alors connaître le bit erroné (ce qui revient à connaître i) et corriger le mot en inversant le *ième* bit. Cette manœuvre est possible sans connaître v_k et uniquement dans le cas d'erreur sur un seul bit.

8.1.2 Code de Steane

Définition 8.2. *Mots codes de Steane*
En considérant la parité des mots comme étant la parité de la somme de leurs bits, les mots codes de Steane sont les mots obtenus à partir du code de Hamming :

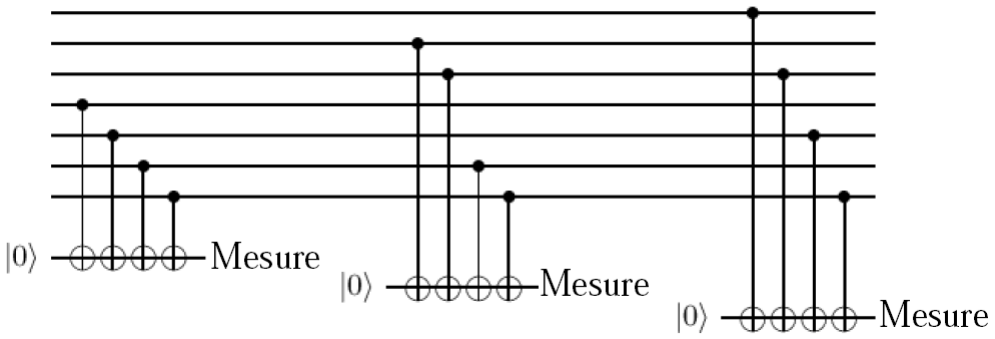
$$\begin{aligned} |\overline{0}\rangle &= \frac{1}{\sqrt{8}} \sum_{mots\, pairs} v_k = \frac{1}{\sqrt{8}} \big(|0000000\rangle + |0001111\rangle + |0110011\rangle + |0111100\rangle \\ &\quad + |1010101\rangle + |1011010\rangle + |1100110\rangle + |1101001\rangle \big) \\ |\overline{1}\rangle &= \frac{1}{\sqrt{8}} \sum_{mots\, impairs} v_k = \frac{1}{\sqrt{8}} \big(|1111111\rangle + |1110000\rangle + |1001100\rangle + |1000011\rangle \\ &\quad + |0101010\rangle + |0100101\rangle + |0011001\rangle + |0010110\rangle \big) \end{aligned}$$

Correction des erreurs de bit

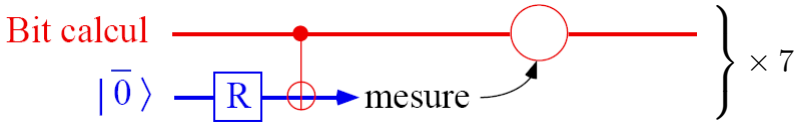
- **3 bits auxiliaires et 12 portes CNOT :**
  Afin de construire le mot Hv, on rajoute 3 qubits auxiliaires pour effectuer l'opération :

$$|v\rangle \otimes |000\rangle_{aux} \rightarrow |v\rangle \otimes |Hv\rangle_{aux}$$

  On peut alors modifier le qubit erroné sans connaître v. Pour faire cette opération, il faut 4 portes CNOT par bit auxiliaire.



- **7 bits auxiliaires, 7 portes de Hadamard et 7 portes CNOT :**
  Dans cette méthode, on "copie" chacun des qubits sur un bit auxiliaire, grâce à une porte de Hadamard par bit, appliquée au bit logique 0. On applique ensuite une porte CNOT bit à bit entre les bits logiques et les bits auxiliaires. Il suffit alors de mesurer les bits auxiliaires pour détecter une erreur (en utilisant le code classique de Hamming), et pouvoir la modifier.



Correction des erreurs de phase

Les erreurs de phase dans la base $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ correspondent aux erreurs de bits dans la base tournée par une transformation de Hadamard :

$$R = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

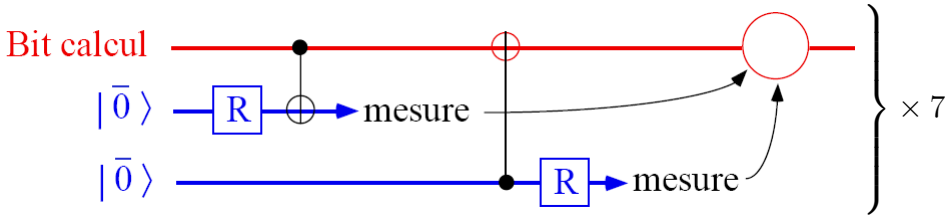
On remarque qu'en appliquant R aux 7 qubits, on obtient de nouveaux mots codes de Steane :

$$|\tilde{0}\rangle = \frac{1}{\sqrt{2}} \left(|\bar{0}\rangle + |\bar{1}\rangle\right) \qquad |\tilde{1}\rangle = \frac{1}{\sqrt{2}} \left(|\bar{0}\rangle - |\bar{1}\rangle\right)$$

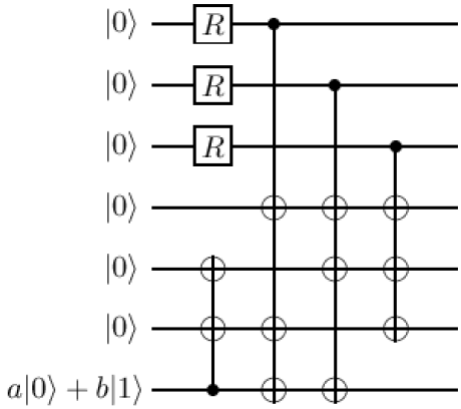
Dès lors, en mesurant $H\tilde{v}$ au lieu de Hv, on obtient les erreurs de phase.

Conclusion

Finalement, il suffit de mesurer les erreurs dans les deux bases, à l'aide de 6 qubits auxiliaires (3 pour les erreurs de bit, 3 pour les erreurs de phases), pour pouvoir corriger les erreurs du code. Il est également possible de le faire avec 14 qubits supplémentaires, de manière simple :



L'encodage se fait de la manière suivante :



8.2 Le calcul quantique « tolérant aux erreurs »

8.2.1 Fault-tolerant

Pour avoir une bonne tolérance aux erreurs en utilisant un code correcteur quantique, il faut :

- Vérifier tous les qubits auxiliaires
- Éviter la propagation d'erreurs
- Répéter les mesures des syndromes

8.2.2 Principe général des codes correcteurs

Pour corriger les erreurs, il faut aborder la stratégie suivante :

- Choisir un sous-espace de l'espace de Hilbert, qui contient les seuls mots-code valides, comme **sous-espace de codage**.
- Chaque erreur corrigeable doit alors transformer le sous-espace de codage en un autre sous-espace, tous les sous-espaces étant orthogonaux entre eux.
- Grâce à leur orthogonalité, on peut identifier le sous-espace où se trouve le système.
- On peut donc corriger l'erreur par une transformation unitaire associée.