Chapitre 10

Correction d'erreur en MQ

Dans la théorie classique la facon usuelle de compenser les effets du bruit dans le stockage ou la communication des données est d'introduire de la redondance de facon suffisamment structurée. C'est ce que l'on appelle la correction d'erreurs. La correction d'erreurs est efficace dans la mesure où l'information est digitale. En effet pour des signaux analogues les perturbations sont continues ce qui rend la correction d'erreurs quasiment impossible.

On pourrait maintenant croire que dans le cas quantique la correction d'erreurs est aussi impossible (ou néanmoins difficile) car les états de l'espace d'Hilbert forment un continuum. D'autrepart le processus de mesure tend à détruire l'état quantique du système, ce qui n'est pas le cas dans le monde classique. Parfois des arguments ont été avancés pour dire que la correction d'erreur n'est pas possible pour des états quantiques, mais il s'est avéré (suite aux travaux de Shor) qu'il n'en est rien. La nature discrète de la MQ se manifeste dans la classification des perturbations possibles et on peut encore construire des codes correcteurs d'erreurs.

10.1 Bref rappel sur les codes linéaires classiques

Le code correcteur le plus simple que l'on puisse imaginer est le code de répétition. Supposons que l'on veuille transmettre un bit 0 ou 1 à travers un canal BSC qui renverse le bit avec probabilité p. On pourrait utiliser le code de répétition

$$0 \longrightarrow 000$$
$$1 \longrightarrow 111$$

Pour aucun ou un seul renversement on peut facilement détecter puis corriger l'erreur grâce á la règle de la majorité. Par exemple si 010 est recu on en conclu que très probablement le deuxiéme bit a été renversé et on décode en faisant l'opération $010 \to 000$. Ce faisant, peut-être que l'on fait une erreur de décodage car il se pourrait qu'en fait 111 était effectivement transmis et que les premier et troisième bits aient été renversés par le canal. Mais la probabilité de cet événement est très faible si p est assez petit. Sans répétition la probabilité d'erreur de décodage sera toujours égale à p alors qu'avec répétition elle est égale à $p^3 + 3p^2(1-p) = 3p^2 - 2p^3$ et est inférieure à p pour tout $0 < p < \frac{1}{2}$.

De facon générale un code binaire linéaire est obtenu par une application linéaire

$$\begin{aligned} \mathbb{F}_2^k &\to \mathbb{F}_2^n \\ \vec{u} &\mapsto G\vec{u} = \vec{x} \end{aligned}$$

où $\vec{u} = \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}$ est un vecteur colonne contenant k bits d'information et G une matrice (d'éléments 0 ou 1) $n \times k$. Le vecteur $G\vec{u}$ est le mot de code, vecteur binaire à n composantes. Toutes les opérations sont faites mod 2. Pour que l'image de $\mathbb{F}_2^k$ dans $\mathbb{F}_2^n$ soit un sous-espace vectoriel de dimension k on prend une matrice G de rang k. C'est à dire que les k colonnes de G sont linéairement indépendantes. Le code de répétition correspond à la matrice $G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ et $k = 1$. Un autre exemple correspond à $G = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$. Les mots de code sont :

$$G\begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, G\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, G\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, G\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}.$$

La matrice G s'appelle la matrice génératrice, n la longueur du code et k sa dimension (la dimension du sous-espace vectoriel dans $\mathbb{F}_2^n$). On dit que l'on a un code (n, k). Le nombre de mots de code est 2^k et son "rendement" $\frac{k}{n}$.

Une autre représentation utile du code est en terme de sa matrice de parité (celle-ci n'est pas unique). Puisqu'un code linéaire est un sous-espace vectoriel de $\mathbb{F}_2^n$, il peut être vu comme le noyau d'une matrice H, c'est à dire l'ensemble des vecteurs solutions de

$$H\vec{x} = 0 \qquad , \ H \text{ de dimension } (n-k) \times n$$

et H est duale de G, c'est à dire $HG = 0$.

Pour construire H à partir de G on peut écrire $G = [\vec{g}_1, \ldots, \vec{g}_k]$ où $\vec{g}_1, \ldots, \vec{g}_k$ sont indépendants et prendre $n-k$ vecteurs orthogonaux $\vec{h}_1, \ldots, \vec{h}_{n-k}$ au sous-espace engendré par $\vec{g}_1, \ldots, \vec{g}_k$. Alors

$$H = \begin{bmatrix} \vec{h}_1^T \\ \vdots \\ \vec{h}_{n-k}^T \end{bmatrix}$$

Ici rang $H = n-k$ et donc dim(Ker H) $= n -$ rang $H = k$. Réciproquement pour construire G à partir de H on prend les $n-k$ vecteurs lignes indépendants de H et on construit k vecteurs orthogonaux (au sous-espace engendré par les lignes de H) qui forment les k colonnes de G.

La matrice de parité permet de détecter certaines erreurs (mais pas toutes). Supposons que le mot $\vec{x}$ soit transmis à travers un canal et que $\vec{x}'$ soit recu : $\vec{x}' = \vec{x} + \vec{e}$ où $\vec{e}$ est un vecteur contenant des 1 aux composantes erronées et 0 ailleurs. On a :

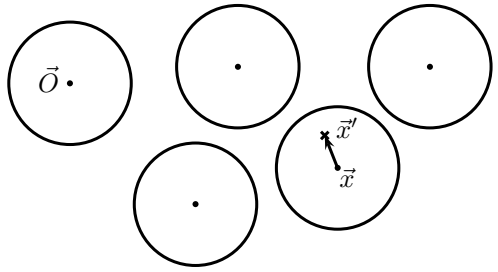
$$H\vec{x}' = H\vec{x} + H\vec{e} = H\vec{e}$$

On appelle $H\vec{e}$ le syndrome. Si celui-ci est non-nul il indique que le mot recu est erroné. Notez que s'il est nul il peut y avoir ou non erreur de transmission. Pour le canal BSC la probabilité d'avoir un vecteur d'erreur $\vec{e}$ est $p^{|\vec{e}|}(1-p)^{n-|\vec{e}|}$ et il est naturel (pour p petit) de décoder $\vec{x}'$ en déclarant que $\vec{x}$ est le vecteur qui minimise $d(\vec{x}, \vec{x}')$ (égale é $|\vec{e}|$) la distance de Hamming entre $\vec{x}$ et $\vec{x}'$. En effet $\vec{x}$ est le vecteur transmis le plus probable (qui maximise $p^{|\vec{e}|}(1-p)^{n-|\vec{e}|}$) étant donné que $\vec{x}'$ a été recu (les vecteurs transmis sont choisis uniformément). C'est le décodeur dit de "distance minimale".

Un paramètre important qui caractérise la qualité d'un code est sa distance minimale $d = \min_{x,x' \in \mathcal{C}} d(\vec{x}, \vec{x}')$. Pour un code linéaire on a aussi $d = \min_{x \neq 0 \in \mathcal{C}} d(\vec{x}, 0)$. On parle alors de code (n, k, d) : longueur n, dimension k et distance minimale d. Le théorème suivant est important (et facile à prouver).

Théoréme : Soit un code (n, k, d). On peut toujours corriger jusqu'à t erreurs avec $2t + 1 \leq d$ grâce au décodeur de la distance minimale.

Si on considére les boules de Hamming de rayon $\frac{d-1}{2}$ autour des mots de codes, celles-ci ne s'intersectent pas. De plus si le nombre d'erreur est $\leq \frac{d-1}{2}$ alors le mot recu $\vec{x}'$ est certainement dans une et une seule des boules. On déclare que le mot transmis est l'unique mot de code dans la même boule que $\vec{x}'$.



Rappel sur les codes de Hamming. Ceux-ci sont commodément décrits par leur matrice de parité. Soit $r \geq 2$ et H la matrice de parité dont les colonnes sont tous les $2^r - 1$ vecteurs binaires non nuls de longueur r. On a $n = 2^r - 1$ et $n - k = r \Rightarrow k = 2^r - r - 1$. On obtient donc un code $(n, k) = (2^r - 1, 2^r - r - 1)$ de longueur $2^r - 1$ et dimension $2^r - r - 1$. Il faut vérifier que le rang de cette matrice est bien r : cela est vrai car parmi les $2^r - 1$ vecteurs binaires non nuls, il y en a r indépendants qui engendrent tout $\mathbb{F}_2^r$.

On peut montrer que pour tout code linéaire, le nombre minimal de colonnes de H qui sont linéairement indépendantes donne exactement d (c'est é dire toute collection de $d - 1$ colonnes sont linéairement indépendantes). Pour les codes de Hamming on voit facilement que $d = 3$. Ainsi ces codes corrigent une erreur. Par exemple le code de Hamming $(7, 4, 3)$ posséde la matrice (ici $r = 3$)

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

Ici nous avons ordonné les colonnes dans l'ordre lexicographique car cela permet une correction d'erreur aisée. Supposons qu'une erreur soit produite

dans le $3^{\text{iéme}}$ bit. Alors c'est $\vec{e} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ et le syndrome vaut $H\vec{e} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$ qui est égal à la $3^{\text{iéme}}$ colonne de H. Le syndrome nous montre automatiquement quel bit est erroné et il suffit de le renverser pour effectuer la correction d'erreur. On est assuré que l'erreur est correctement détectée et corrigée, *seulement* si elle est unique.

10.2 Codes de Répétition Quantique

Par analogie avec le cas classique on peut considérer le code de répétition

$$|0\rangle \rightarrow |000\rangle$$
$$|1\rangle \rightarrow |111\rangle.$$

que nous allons utilisé sur un *canal bit-flip*.

Quel est le procédé de détection et correction dans le cas quantique ? Il faut choisir correctement la base de mesure pour ne pas détruire irrémédiablement l'information restante du canal ! Ici l'espace d'Hilbert à la sortie du canal est de dimension $2^3 = 8$ et il faut une base à 8 dimensions. Considérons les 4 projecteurs de dimension 2 chacun (8 donc au total)

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$$
$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$$
$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|.$$

P_0 projette dans le sous-espace à 0 erreurs, P_1 dans le sous-espace à une erreur sur le premier bit, P_2 dans le sous-espace à une erreur dans le deuxiéme bit, P_3 dans le sous-espace à une erreur sur le $3^{\text{iéme}}$ bit. L'entrée du canal est le ket $\alpha\,|0\rangle + \beta\,|1\rangle$ codé :

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

Notez que ce code de répétition ne viole pas le "no-cloning theorem" car on répète uniquement des états de base orthonormés. Ici on ne répète pas l'état $\alpha\,|0\rangle + \beta\,|1\rangle$, ce qui violerait le no-cloning theorem. Si une seule erreur est produite, mettons pour le deuxième bit (avec probabilité p) la sortie est

$$\alpha\,|010\rangle + \beta\,|101\rangle$$

Une mesure dans la base $\{P_0, P_1, P_2, P_3\}$ préserve l'état avec probabilité 1 car

$$P_2(\alpha\ |010\rangle + \beta\ |101\rangle) = \alpha\ |010\rangle + \beta\ |101\rangle$$

et ainsi on détecte que l'erreur est dans le deuxième bit sans détruire l'état. La correction d'erreur se fait en appliquant l'opérateur unitaire $\mathbb{1} \otimes X \otimes \mathbb{1}$ qui renverse le deuxième bit.

$$\mathbb{1} \otimes X \otimes \mathbb{1}(\alpha\ |010\rangle + \beta\ 101\rangle) = \alpha\ |000\rangle + \beta\ |111\rangle.$$

Bien sur (comme dans le cas classique) on ne détecte pas correctement des renversements de deux ou trois bits.

Il est utile de d'écrire le procédé de correction d'erreur d'un autre point de vue. Considérons un appareil de mesure qui mesure les observables

$$Z_1 \otimes Z_2 \otimes \mathbb{1} \qquad \text{et} \qquad \mathbb{1} \otimes Z_2 \otimes Z_3.$$

Notons que la mesure simultanée de ces observables (avec un seul appareil de mesure) est possible car elles commutent. La mesure de chaque observable donne les résultats (± 1) et (± 1). Ces mesures constituent l'analogue du "syndrome classique" :

$+1$	et	$+1$	$\longrightarrow$	pas d'erreur
-1	et	$+1$	$\longrightarrow$	erreur dans le 1^{er} bit
-1	et	-1	$\longrightarrow$	erreur dans le $2^{\text{éme}}$ bit
$+1$	et	-1	$\longrightarrow$	erreur dans le $3^{\text{éme}}$ bit.

Une fois l'erreur détectée on la corrige en appliquant un opérateur unitaire :

pas d'erreur	$\longrightarrow$	$\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1}$
1^{er} bit	$\longrightarrow$	$X_1 \otimes \mathbb{1} \otimes \mathbb{1}$
$2^{\text{éme}}$ bit	$\longrightarrow$	$\mathbb{1} \otimes X_2 \otimes \mathbb{1}$
$3^{\text{éme}}$ bit	$\longrightarrow$	$\mathbb{1} \otimes \mathbb{1} \otimes X_3$.

Toutes les opérations – encodage, transmission, mesure, correction – sont permises par la MQ (opérateurs unitaires ou mesures projectives).

Exercice Proposez un circuit pour réaliser l'opération d'encodage.

Ce code n'est pas efficace pour protéger létat contre les erreurs produites par un canal "phase-flip". En effet un phase-flip (sur n'importe-quel bit) produit létat

$$\alpha|000\rangle - \beta|111\rangle$$

à la sortie du canal. On voit facilement que le syndrome est $(+1,+1)$ qui est interprété comme une absence d'erreur. Un code de répétition utile pour le canal "phase-flip" (mais du coup, inutile pour le bit-flip) est obtenu en travaillant dans la base $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}; |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

Encodage :

$$|0\rangle \to |+\rangle \to |+++\rangle$$
$$|1\rangle \to |-\rangle \to |---\rangle.$$

Détection d'erreur :
Mesurer les observables (qui commutent)

$$X_1 \otimes X_2 \otimes \mathbb{1} \text{ et } \mathbb{1} \otimes X_2 \otimes X_3.$$

La mesure donne les syndromes :

$+1$	et	$+1$	$\longrightarrow$	pas d'erreur
-1	et	$+1$	$\longrightarrow$	erreur dans le 1^{er} bit
-1	et	-1	$\longrightarrow$	erreur dans le $2^{\text{éme}}$ bit
$+1$	et	-1	$\longrightarrow$	erreur dans le $3^{\text{éme}}$ bit.

Correction d'erreur :
Appliquer les opérateurs unitaire :

pas d'erreur	$\longrightarrow$	$\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1}$
1^{er} bit	$\longrightarrow$	$Z_1 \otimes \mathbb{1} \otimes \mathbb{1}$
$2^{\text{éme}}$ bit	$\longrightarrow$	$\mathbb{1} \otimes Z_2 \otimes \mathbb{1}$
$3^{\text{éme}}$ bit	$\longrightarrow$	$\mathbb{1} \otimes \mathbb{1} \otimes Z_3$.

Par exemple si on transmet $|0\rangle$, on code par $|+++\rangle$ et si le canal produit $|++-\rangle$ on mesurera $(+1,-1)$ ce qui indique que le $3^{\text{iéme}}$ bit a subi un phase-flip. On applique

$$\mathbb{1} \otimes \mathbb{1} \otimes Z_3|++-\rangle = |+++\rangle \to |0\rangle.$$

10.3 Le code de Shor

La situation du paragraphe précédent n'est pas encore satisfaisante car en MQ les deux types d'erreurs peuvent essentiellement survenir en même temps et nous aimerions un procédé qui les corrige toutes. La solution de ce problème a été présentée pour la première fois par Shor et elle se révèle être à la base des autres constructions plus élaborées qui ont suivies.

Si nous pouvons corriger à la fois les bits-flips et les phases-flips, alors nous pouvons corriger du même coup une très large classe d'erreurs à 1 qubit. En effet nous pourrons corriger toutes les erreurs produites par des canaux du type

$$\mathcal{E}(\varrho) = p_0\varrho + p_1 X\varrho X + p_2 Y\varrho Y + p_3 Z\varrho Z$$

avec $p_0+p_1+p_2+p_3 = 1$. Cette classe contient les canaux blit-flip, phase-flip, bit-phase-flip, dépolarisant, etc... Notons que cela n'inclut pas des erruers sur l'amplitude des coefficients α et β.

L'idée principale du code de Shor est de "concaténer" les deux codes de répétition. La concaténation est en fait une méthode de la théorie classique du codage. Elle permet de constuire des nouveaux codes en assemblant des codes élémentaires.

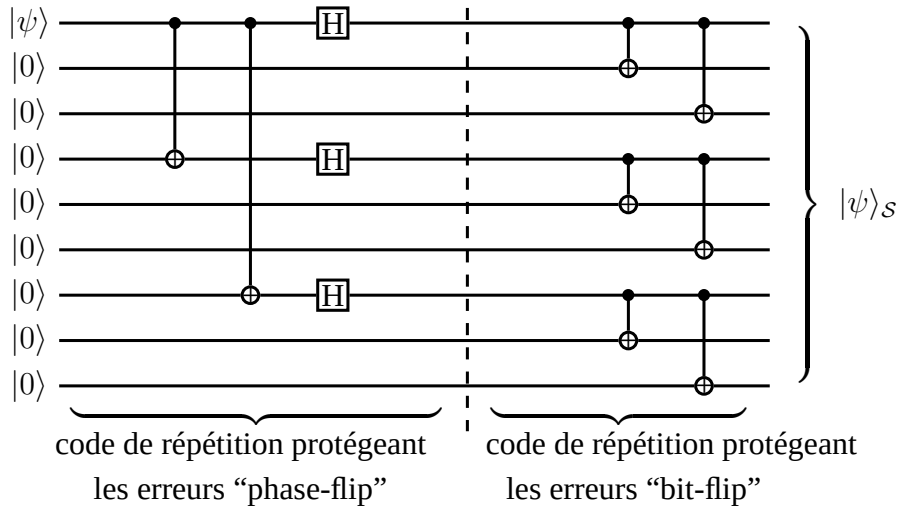
Les mots de code sont construits comme suit :

$$\begin{aligned}
|0\rangle \to |+\rangle \longrightarrow |{+}{+}{+}\rangle &= \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\
&\longrightarrow \frac{|000\rangle+|111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle+|111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle+|111\rangle}{\sqrt{2}} \equiv |0_{\mathcal{S}}\rangle. \\
|1\rangle \to |-\rangle \longrightarrow |{-}{-}{-}\rangle &= \frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&\longrightarrow \frac{|000\rangle-|111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle-|111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle-|111\rangle}{\sqrt{2}} \equiv |1_{\mathcal{S}}\rangle.
\end{aligned}$$

Ainsi chaque quibit est encodé par un état à 9 qubits. Le "rendement" de ce code est 1/9. Si nous appelons $|0\rangle_{\mathcal{S}}$ et $|1\rangle_{\mathcal{S}}$ les deux états à 9 qubits, un mot de code général est

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \to |\psi_{\mathcal{S}}\rangle = \alpha\,|0\rangle_{\mathcal{S}} + \beta\,|1\rangle_{\mathcal{S}}.$$

Le circuit suivant réalise l'opération de codage de facon unitaire :



Montrons maintenant que ce code est capable de protéger l'état contre n'importe quelle erreur sur 1 qubit engendrée par les opérateurs $\mathbb{1}$ (pas d'erreur), X (bit-flip), Z (phase-flip) et Y (bit & phase flip). En d'autres termes nous voulons montrer que si la sortie du canal est $|\psi_{\mathcal{S}}\rangle, X_1|\psi_{\mathcal{S}}\rangle, Y_1|\psi_{\mathcal{S}}\rangle, Z_1|\psi_{\mathcal{S}}\rangle$ agit sur un seul des 9 qubits, il est possible de détecter l'erreur et de reconstruire $|\psi\rangle_{\mathcal{S}}$ (et donc $|\psi\rangle$) grâce à des opérations permises en MQ.

Considérons d'abord l'action de X tout seul sur un des trois premiers qubits (bit-flip). Comme avant, la mesure simultannée des observables Z_1Z_2 et Z_2Z_3 permet de décider si un des trois premiers qubit est renversé ou non. Ensuite il est facile de le corriger en appliquant X_i (si c'est $i = 1, 2, 3$ qui est renversé). Pour pouvoir traiter tous les qubits ce cette facon il faut faire une mesure des opérateurs suivants

$$Z_1Z_2 \text{ et } Z_2Z_3; \qquad Z_4Z_5 \text{ et } Z_5Z_6; \qquad Z_7Z_8 \text{ et } Z_8Z_9.$$

Touc ces opérateurs commutent et la mesure simultannée est possible.

Considérons maintenant l'action de Z sur un seul des trois premiers qubits (phase-flip). Un phase-flip sur le deuxiéme qubit change les états de base en (l'état é la sortie du canal est $Z_2|\psi\rangle_{\mathcal{S}}$ avec probabilité p)

$$\frac{|000\rangle - |111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle + |111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

et

$$\frac{|000\rangle + |111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle - |111\rangle}{\sqrt{2}} \otimes \frac{|000\rangle - |111\rangle}{\sqrt{2}}$$

Cette erreur peut étre détectée (sans détruire ces états) gràce à une mesure des (opérateurs qui commutent entre eux)

$$(X_1X_2X_3)(X_4X_5X_6) \qquad \text{et} \qquad (X_4X_5X_6)(X_7X_8X_9)$$

Par exemple pour l'erreur ci-dessus

$$(X_1X_2X_3)(X_4X_5X_6)(Z_2|\psi_{\mathcal{S}}\rangle) = -(Z_2|\psi_{\mathcal{S}}\rangle)$$

et

$$(X_4X_5X_6)(X_7X_8X_9)(Z_2|\psi_{\mathcal{S}}\rangle) = +(Z_2|\psi_{\mathcal{S}}\rangle)$$

On conclut que l'erreur phase-flip est dans un des trois premiers qubits. Notez que l'on ne peut pas affirmer lequel des trois est erroné. Mais cela ne nous empèche pas d'effectuer la correction en appliquant l'opérateur $Z_1Z_2Z_3$ (vérifiez !)

$$Z_1Z_2Z_3(Z_2|\psi_{\mathcal{S}}\rangle) = |\psi_{\mathcal{S}}\rangle.$$

Illustrons maintenant la correction d'une erreur bit & phase-flip sur le $4^{\text{iéme}}$ bit. L'état sortant du canal est

$$X_4Z_4|\psi_{\mathcal{S}}\rangle.$$

D'abord on détecte les bit-flip comme suit :

$$\begin{aligned}
&Z_1Z_2(X_4Z_4|\psi_{\mathcal{S}}\rangle) = X_4Z_4|\psi_{\mathcal{S}}\rangle \\
&Z_2Z_3(X_4Z_4|\psi_{\mathcal{S}}\rangle) = X_4Z_4|\psi_{\mathcal{S}}\rangle \\
&Z_4Z_5(X_4Z_4|\psi_{\mathcal{S}}\rangle) = -(X_4Z_4|\psi_{\mathcal{S}}\rangle) \qquad (\text{car } Z_4X_4 = -X_4Z_4) \\
&Z_5Z_6(X_4Z_4|\psi_{\mathcal{S}}\rangle) = X_4Z_4|\psi_{\mathcal{S}}\rangle \\
&Z_7Z_8(X_4Z_4|\psi_{\mathcal{S}}\rangle) = X_4Z_4|\psi_{\mathcal{S}}\rangle \\
&Z_8Z_9(X_4Z_4|\psi_{\mathcal{S}}\rangle) = X_4Z_4|\psi_{\mathcal{S}}\rangle
\end{aligned}$$

On conclut qu'il y a un bit-flip sur le $4^{\text{iéme}}$ bit. Ensuite on détecte les phases-flips comme suit

$$\begin{aligned}
&X_1X_2X_3\ X_4X_5X_6(X_4Z_4|\psi_{\mathcal{S}}\rangle) = -X_4Z_4|\psi_{\mathcal{S}}\rangle \\
&\qquad\qquad (\text{car } X_4 \text{ et } Z_4 \text{ anti-commutent}) \\
&X_4X_5X_6\ X_7X_8X_9(X_4Z_4|\psi_{\mathcal{S}}\rangle) = -X_4Z_4|\psi_{\mathcal{S}}\rangle
\end{aligned}$$

et on conclut qu'il y a aussi un phase-flip sur le quatriéme qubit. L'état est corrigé en appliquant (X_4Z_4) sur la sortie du canal : $X_4Z_4\ (X_4Z_4)|\psi_{\mathcal{S}}\rangle = |\psi_{\mathcal{S}}\rangle$.

Correction d'erreurs générales à 1 qubit Les résultats obtenus jusqu'ici peuvent être obtenus aussi d'une facon plus unifiée qui montre leur généralité. Considérons la matrice densité décrivant la sortie d'un canal quelconque :

$$|\psi_{\mathcal{S}}\rangle\langle\psi_{\mathcal{S}}| \to \mathcal{E}(|\psi_{\mathcal{S}}\rangle\langle\psi_{\mathcal{S}}|)$$

Une mesure des observables $Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9$ et $X_1X_2X_3\ X_4X_5X_6, X_4X_5X_6\ X_7X_8X_9$ va projeter l'état $\mathcal{E}(|\psi_{\mathcal{S}}\rangle\langle\psi_{\mathcal{S}}|)$ sur un des sous-espaces propres de ces observables. Les valeurs propres sont toutes égales é ± 1. Si le bruit est faible et agit essentiellement sur un qubit au plus le syndrome sera avec une grande probabilité du type discuté dans les paragraphes précédents, c'est à dire correspondant à un bit-flip, phase-flip ou bit & phase flip. On peut l'identifier puis corriger l'erreur. Il existe une faible probabilité (si le bruit est faible) que l'erreur affecte plus qu'un qubit (comme dans le cas classique) et alors la correction d'erreur est erronée.

Pour résumer, code de Shor est de longueur 9, a dimension est 2, et il corrige 1 erreur. Plus précisément les mots de code sont de type $\alpha\,|0\rangle_{\mathcal{S}}+\beta\,|1\rangle_{\mathcal{S}}$, donc vivent dans un sous-espace de Hilbert de dimension 2^1, de l'espace à 9 qu-bits, qui est lui est de dimension 2^9. On dit que les paramètres de ce code quantique sont $[9, 1, 1]$ (longueur 9 et dim $\mathscr{H} = 2^9$; dim $\mathscr{C} = 2^1$; corrige une erreur).

10.4 Codes de Calderbank - Shor - Steane

Le code de Shor corrige seulement 1 erreur (comme les codes de Hamming). Nous donnons maintenant la construction d'une large classe de codes capables de corriger t erreurs de type bit et phase flips. Pour une longueur n donnée, il est possible de construire des codes de dimension k et corrigeant t erreurs tels que $\frac{k}{n}$ et $\frac{t}{n}$ soient $\mathrm{O}(1)$.

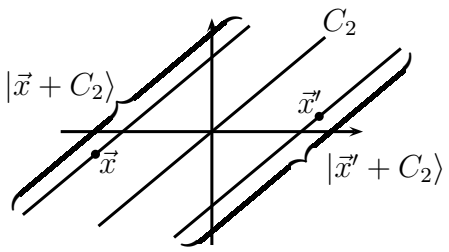
Soit C_1 et C_2 deux codes linéaires classiques tels que $C_2 \subset C_1$ de paramètres (n, k_1) et (n, k_2). Nous rappelons que C_1 est un sous-espace vectoriel de $\mathbb{F}_2^n$ de dimension k_1 et C_2 un sous-espace vectoriel de C_1 de dimension $k_2 \leq k_1$. On suppose aussi que C_1 et $C_2^\perp$ corrigent t erreurs (par exemple leur distance minimale est $d = 2t + 1$). Le code *dual* $C_2^\perp$ est le sous-espace vectoriel orthogonal à C_2 dans $\mathbb{F}_2^n$ et sa dimension est donc $n - k_2$.

En fait C_2 est aussi un sous-groupe de C_1 et on peut considérer l'ensemble des classes d'équivalences C_1/C_2. Soit $\vec{x}$ un mot de C_1, la classe d'équivalence de $\vec{x}$ est l'ensemble des mots de la forme $\{\vec{x} + \vec{y};\ \vec{y} \in C_2\}$. C'est donc l'hy-

perplan parallèle à C_2 passant par $\vec{x} \in C_1$. Posons

$$|\vec{x} + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y} \in C_2} |\vec{x} + \vec{y}\rangle$$

Ce ket ne dépend que de la classe d'équivalence associée à $\vec{x}$ et non pas du représentant spécial choisi.



Le ket $|\vec{x} + C_2\rangle$ est la superposition cohérente de tous les états dans la classe d'équivalence $\vec{x}+C_2$. Pour deux classes d'équivalence différentes $\vec{x}+C_2$ et $\vec{x}'+C_2$ (c'est à dire que $\vec{x}-\vec{x}' \notin C_2$) les kets associés sont perpendiculaires :

$$\langle \vec{x} + C_2 | \vec{x}' + C_2 \rangle = 0$$

Il y a $\frac{|C_1|}{|C_2|} = 2^{k_1-k_2}$ classes d'équivalence et donc $2^{k_1-k_2}$ vecteurs orthogonaux.

Le code $\mathrm{CSS}(C_1, C_2)$ est le sous-espace d'Hilbert engendré par ces $2^{k_1-k_2}$ vecteurs orthogonaux. C'est un sous-espace de l'espace d'Hilbert à n qubits $\underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ fois}}$ lequel est de dimension 2^n. Les paramètres du code sont $[n, k_1 - k_2]$; où $\dim \mathscr{H} = n$ et $\dim \mathrm{CSS}(C_1, C_2) = 2^{k_1-k_2}$. Nous allons montrer que si C_1 et $C_2^\perp$ corrigent t erreurs alors $\mathrm{CSS}(C_1, C_2)$ corrige t bit et phase flips.

Soit $\vec{e}_1$ et $\vec{e}_2$ les vecteurs possédants des 1 et 0 avec la coordonnée 1 aux t endroits des bit et/ou phase flips. Le vecteur corrompu par le bruit est :

$$|\psi\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y} \in C_2} (-1)^{(\vec{x}+\vec{y})\cdot\vec{e}_2} |\vec{x} + \vec{y} + \vec{e}_1\rangle$$

Pour effectuer la correction d'erreur il faut faire des opérations permises par la MQ qui reconstituent $|\vec{x} + C_2\rangle$. Comme il faudra calculer et stocker les "syndromes" du bit et phase flip on ajoute des bits auxiliaires de stockage et on travaille avec l'état

$$|\psi\rangle \otimes |0_n\rangle \otimes |0_n\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y} \in C_2} (-1)^{(\vec{x}+\vec{y})\cdot\vec{e}_2} |\vec{x} + \vec{y} + \vec{e}_1\rangle \otimes |0_n\rangle \otimes |0_n\rangle$$

Correction du bit-flip
On calcule les syndromes $H_1(\vec{x}+\vec{y}+\vec{e}_1) = H_1\vec{e}_1$ (grâce à la matrice de parité du code C_1). Ce calcul peut être implémenté de facon unitaire :

$$U_1|\vec{x}+\vec{y}+\vec{e}_1\rangle \otimes |0_n\rangle \otimes |0_n\rangle = |\vec{x}+\vec{y}+\vec{e}_1\rangle \otimes |H_1\vec{e}_1\rangle \otimes |0_n\rangle$$

si bien que

$$U_1|\psi\rangle \otimes |0_n\rangle \otimes |0_n\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y}\in C_2} (-1)^{(\vec{x}+\vec{y})\cdot\vec{e}_2} |\vec{x}+\vec{y}+\vec{e}_1\rangle \otimes |H_1\vec{e}_1\rangle \otimes |0_n\rangle$$

Une mesure du second registre dans la base computationelle donne $|H_1\vec{e}_1\rangle$ avec probabilité 1 (car le ket $|H_1\vec{e}_1\rangle$ peut être factorisé dans la dernière expression, et c'est un vecteur de la base computationelle). Donc on connait le syndrome $H_1\vec{e}_1$ et si $|\vec{e}_1| \leq t$ on peut corriger les erreurs grâce à un algorithme classique (pour le code C_1). Cela permet d'appliquer l'opérateur unitaire

$$\prod_{\text{composantes non nulles de } \vec{e}_1} X_i \equiv U_{1,\text{corr}}$$

pour corriger l'état quantique. On obtient

$$U_{1,\text{corr}}U_1|\psi\rangle \otimes |0_n\rangle \otimes |0_n\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y}\in C_2} (-1)^{(\vec{x}+\vec{y})\cdot\vec{e}_2} |\vec{x}+\vec{y}\rangle \otimes |H_1\vec{e}_1\rangle \otimes |0_n\rangle$$

Correction du phase-flip
D'abord, pour passer dans une base plus naturelle, on applique les portes de Hadamard $H^{\otimes n}$ ce qui donne

$$\begin{aligned}
&H^{\otimes n}U_{1,\text{corr}}U_1|\psi\rangle \otimes |0_n\rangle \otimes |0_n\rangle \\
&= \frac{1}{2^{n/2}} \frac{1}{\sqrt{|C_2|}} \sum_{\vec{y}\in C_2} (-1)^{(\vec{x}+\vec{y})\cdot\vec{e}_2} \sum_{\vec{z}} (-1)^{\vec{z}\cdot(\vec{x}+\vec{y})} |\vec{z}\rangle \otimes |H_1\vec{e}_1\rangle \otimes |0_n\rangle \\
&= \frac{1}{2^{n/2}} \frac{1}{\sqrt{|C_2|}} \sum_{\vec{z}} \sum_{\vec{y}\in C_2} (-1)^{(\vec{z}+\vec{e}_2)\cdot(\vec{x}+\vec{y})} |\vec{z}\rangle \otimes |H_1\vec{e}_1\rangle \otimes |0_n\rangle \\
&= \frac{1}{2^{n/2}} \frac{1}{\sqrt{|C_2|}} \sum_{\vec{z}} \sum_{\vec{y}\in C_2} (-1)^{\vec{z}\cdot(\vec{x}+\vec{y})} |\vec{z}+\vec{e}_2\rangle \otimes |H_1\vec{e}_1\rangle \otimes |0_n\rangle
\end{aligned}$$

On note que

$$\sum_{\vec{y}\in C_2} (-1)^{\vec{z}\cdot\vec{y}} = \begin{cases} |C_2| & \text{si } \vec{z} \in C_2^{\perp}, \\ 0 & \text{sinon} \end{cases}$$

ce qui donne l'état :

$$= \frac{1}{|C_2^\perp|} \sum_{\vec{z} \in C_2^\perp} (-1)^{\vec{z}\cdot\vec{x}} |\vec{z} + \vec{e}_2\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |0_n\rangle.$$

On implémente maintenant le calcul du syndrome de $C_2^\perp$ de facon unitaire en stockant le résultat dans le dernier registre

$$\begin{aligned} U_2 |\vec{z} + \vec{e}_2\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |0_n\rangle & \\ &= |\vec{z} + \vec{e}_2\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |H_2^\perp (\vec{z} + \vec{e}_2)\rangle \\ &= |\vec{z} + \vec{e}_2\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |H_2^\perp \vec{e}_2\rangle. \end{aligned}$$

où ici $H_2^\perp$ est la matrice de parité de $C_2^\perp$. L'état obtenu est :

$$\begin{aligned} U_2 H^{\otimes n} \tilde{U}_{1,\text{corr}} U_1 |\psi\rangle \otimes |0_n\rangle \otimes |0_n\rangle & \\ = \frac{1}{\sqrt{|C_2^\perp|}} \sum_{\vec{z} \in C_2^\perp} (-1)^{\vec{z}\cdot\vec{x}} |\vec{z} + \vec{e}_2\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |H_2^\perp \vec{e}_2\rangle. \end{aligned}$$

La mesure du dernier registre (dans la base computationelle) projette sur $|H_2^\perp \vec{e}_2\rangle$ lui-méme, avec probabilité 1. Donc $H_2^\perp \vec{e}_2$ est connu et $\vec{e}_2$ peut étre calculé si $C_2^\perp$ corrige t erreurs (on suppose $|\vec{e}_2| \leq t$). Cela permet alors d'appliquer l'opérateur unitaire

$$U_{2,\text{corr}} \equiv \prod_{\text{comp non nulles de } \vec{e}_2} X_i$$

pour trouver l'état :

$$\begin{aligned} U_{2,\text{corr}} U_2 H^{\otimes n} \tilde{U}_1 U_1 |\psi\rangle \otimes |0_n\rangle \otimes |0_n\rangle & \\ = \frac{1}{\sqrt{|C_2^\perp|}} \sum_{\vec{z} \in C_2^\perp} (-1)^{\vec{z}\cdot\vec{x}} |\vec{z}\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |H_2^\perp \vec{e}_2\rangle. \end{aligned}$$

La derniére étape consiste maitenant à appliquer une fois de plus $H^{\otimes n}$ pour revenir dans la base initiale. Cela donne

$$\begin{aligned} H^{\otimes n} U_{2,\text{corr}} U_2 H^{\otimes n} U_{1,\text{corr}} U_1 |\psi\rangle \otimes |0_n\rangle \otimes |0_n\rangle & \\ = \frac{1}{\sqrt{|C_2^\perp|}} \frac{1}{2^{n/2}} \sum_{\vec{z} \in C_2^\perp} \sum_{\vec{y}} (-1)^{\vec{z}\cdot(\vec{x}+\vec{y})} |\vec{y}\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |H_2^\perp \vec{e}_2\rangle & \\ = \frac{1}{\sqrt{|C_2^\perp|}} \frac{1}{2^{n/2}} \sum_{\vec{z} \in C_2^\perp} \sum_{\vec{y}} (-1)^{\vec{z}\cdot\vec{y}} |\vec{y} + \vec{x}\rangle \otimes |H_1 \vec{e}_1\rangle \otimes |H_2^\perp \vec{e}_2\rangle. \end{aligned}$$

Maintenant on note (comme avant) :

$$\sum_{\vec{z}\in C_2^\perp}(-1)^{\vec{z}\cdot\vec{y}} = \begin{cases} |C_2^\perp| & \text{si } \vec{y}\in (C_2^\perp)^\perp = C_2, \\ 0 & \text{sinon.} \end{cases}$$

L'état final obtenu est donc :

$$\left(\frac{1}{\sqrt{|C_2|}}\sum_{\vec{y}\in C_2}|\vec{x}+\vec{y}\rangle\right)\otimes|H_1\vec{e}_1\rangle\otimes|H_2^\perp\vec{e}_2\rangle.$$

Nous voyons que le mot de code initial a été reconstruit dans le premier registre !

Exemple : Le code de Steane

Le code de Steane est un code CSS(C_1, C_2) avec $C_1 =$ Hamming $(7, 4)$ et $C_2 = C_1^\perp$. On montre que ce code posséde 7 qubits, est de dimension 2 et corrige une erreur. Les mots de codes sont (voir exercices)

$$\begin{aligned}|0\rangle_{\text{Steane}} = \frac{1}{\sqrt{8}}\{&|0000000\rangle + |1001101\rangle + |0101011\rangle + |0010111\rangle \\ &+ |0111100\rangle + |1011010\rangle + |1100110\rangle + |1110001\rangle\}\end{aligned}$$

et

$$\begin{aligned}|1\rangle_{\text{Steane}} = \frac{1}{\sqrt{8}}\{&|1111111\rangle + |0110010\rangle + |1010100\rangle + |1101000\rangle \\ &+ |1000011\rangle + |0100101\rangle + |0011001\rangle + |0001110\rangle\}.\end{aligned}$$

Le mot $|0\rangle_{\text{Steane}}$ correspond à la classe d'équivalence de $(0000000) \in C_1$ et le deuxiéme mot $|1\rangle_{\text{Steane}}$ correspond à la classe d'équivalence de $(1111111) \in C_1$.