8.1 Nécessité des codes correcteurs quantiques

8.1.1 Problèmes rencontrés

Rappelons l'intérêt du calcul quantique pour calculer la table de valeurs d'une fonction agissant sur N bits, c'est-à-dire ayant 2^N arguments possibles. La méthode classique nécessite de calculer $f(x)$ 2^N fois, ce qui est impossible si N est grand. Le calcul quantique permet d'obtenir toutes les valeurs de f en un seul calcul, en utilisant le principe de "parallélisme quantique". L'opérateur calculant f est f :

$$U_f : |x\rangle \otimes |0\rangle \to |x\rangle \otimes |f(x)\rangle$$

Le registre d'entrée est initialement dans l'état :

$$(\frac{|0\rangle + |1\rangle}{\sqrt{2}})^N = \frac{1}{2^{\frac{N}{2}}} \sum_{x=0}^{2^N-1} |x\rangle$$

En appliquant une fois U_f, on obtient :

$$\frac{1}{2^{\frac{N}{2}}} \sum_{x=0}^{2^N-1} |x\rangle|f(x)\rangle$$

On obtient ainsi un état intriqué qui contient toutes les valeurs de f.

Si le système n'est pas bien isolé, il risque de s'intriquer avec l'environnement et son état va devenir :

$$\frac{1}{2^{\frac{N}{2}}} \sum_{x=0}^{2^N-1} |x\rangle|f(x)\rangle|\chi_{env}(x)\rangle$$

Les deux cas limites pour l'environnement sont :

- $|\chi_{env}(x)\rangle$ est indépendant de x, donc se factorise : alors l'information est préservée
- $|\chi_{env}(x)\rangle$ dépend de x et tous les $|\chi_{env}\rangle$ sont orthogonaux : alors la matrice densité obtenue par trace partielle sur l'environnement est un mélange statistique. Il y a décohérence, l'information est complètement perdue.

Cette apparition de corrélations non locales entre le système et l'environnement, qui sont inexploitables pour un calcul et causent la perte de l'information est la première raison d'existence des codes correcteurs. L'autre raison est que les portes quantiques ne sont pas parfaites, et peuvent progressivement fausser le calcul. Il faut donc régulièrement «remettre en forme» les bits pour se protéger des petites erreurs des portes quantiques.

8.1.2 Description d'un code correcteur

Le code correcteur classique le plus simple est le code à répétition à 3 bits :

$$0 \longrightarrow (000)$$

$$1 \longrightarrow (111)$$

Ce code permet de corriger une erreur de bit, en faisant un choix à la majorité après mesure des trois bits. Avec une probabilité p d'erreur sur un bit, et en supposant les erreurs indépendantes (on fera toujours cette hypothèse dans la suite), on obtient :

- probabilité de 3 erreurs = p^3
- probabilité de 2 erreurs = $3p^2(1-p)$
- probabilité de 1 erreur = $3p(1-p)^2$
- probabilité de 0 erreur = $(1-p)^3$

Soit une probabilité d'erreur après correction de : $p^3 + 3p^2(1-p) \ll p$. Il existe d'autres codes correcteurs plus complexes, avec des efficacités encore plus grandes.

Dans le cas d'un code quantique, la correction est plus compliquée car il y a plusieurs types d'erreurs possibles, qui peuvent se cumuler.

Définition 8.1. *Une erreur sur un code quantique est la composée de trois erreurs types :*

- *erreur de bit :* $|0\rangle \longleftrightarrow |1\rangle$
- *erreur de phase :* $\dfrac{|0\rangle + |1\rangle}{\sqrt{2}} \longleftrightarrow \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$
- *«petites» erreurs :* $(a|0\rangle + b|1\rangle) \longrightarrow (a'|0\rangle + b'|1\rangle)$

L'impossibilité de mesurer un qubit sans changer son état, et l'impossibilité de dupliquer un état viennent augmenter la difficulté de la correction d'erreur. C'est toutefois quand même possible, comme le montre les deux exemples de codes correcteurs définis dans la suite de ce polycopié.

8.2 Le code de Shor

8.2.1 Première approche

La première idée est de faire comme le code classique :

$$|0\rangle \longrightarrow |000\rangle$$

$$|1\rangle \longrightarrow |111\rangle$$

Ceci n'est pas interdit par le théorème de non-clônage, car :

$$a|0\rangle + b|1\rangle \longrightarrow a|000\rangle + b|111\rangle \neq (a|0\rangle + b|1\rangle)^3$$

Erreur de bit

Une fois ce codage fait, il faut pouvoir détecter les erreurs. Commençons par étudier les inversion de bit : on ne peut pas, comme en classique, mesurer les trois qubits séparément, car cela détruirait l'information. On ne peut donc pas connaître de manière certaine les valeurs des trois qubits, mais cela n'a pas d'importance car nous avons seulement besoin de savoir quel qubit corriger mais sa valeur réelle n'a pas d'importance.

Définition 8.2. *Un **syndrôme** d'une erreur est le résultat d'une mesure qui permet de déterminer l'erreur afin de la corriger.*

Lemme 8.3. *Pour un codage à 3 répétitions, une mesure sur 2 qubits permet d'obtenir un syndrôme de l'inversion de bit.*

Démonstration Comme on ne peut pas mesurer un qubit seul, essayons de mesurer deux qubits à la fois. Cette mesure donne les résultats suivants :

Entrée	$x \oplus z$	$y \oplus z$	Correction	Sortie
$\|000\rangle$	0	0	rien	$\|000\rangle$
$\|100\rangle$	1	0	basculer bit 1	$\|000\rangle$
$\|010\rangle$	0	1	basculer bit 2	$\|000\rangle$
$\|001\rangle$	1	1	basculer bit 3	$\|000\rangle$
$\|111\rangle$	0	0	rien	$\|111\rangle$
$\|011\rangle$	1	0	basculer bit 1	$\|111\rangle$
$\|101\rangle$	0	1	basculer bit 2	$\|111\rangle$
$\|110\rangle$	1	1	basculer bit 3	$\|111\rangle$

On constate que les résultats des mesures de $x \oplus z$ et $y \oplus z$ sont bien représentatives du bit à corriger, quelque soit la valeur réelle du bit.

Petites erreurs

Considérons maintenant les petites erreurs, dues à l'imperfection des portes quantiques, qui induisent une petite rotation de chaque qubit :

$$|000\rangle \longrightarrow |000\rangle + \epsilon_1|100\rangle + \epsilon_2|010\rangle + \epsilon_3|001\rangle$$

$$|111\rangle \longrightarrow |111\rangle + \epsilon_1|011\rangle + \epsilon_2|101\rangle + \epsilon_3|110\rangle$$

En mesurant $x \oplus z$ et $y \oplus z$:
- avec probabilité $1 - \sum_i |\epsilon_i|^2$, on obtient (0,0) et la mesure projette sur le bon état
- avec probabilité $|\epsilon_i|^2$, on obtient respectivement (1,0), (0,1) ou (1,1) : la mesure projette sur un mauvais état, mais on a le bon syndrôme de basculement et on peut corriger.

Erreurs de phase

Une erreur de phase dans la base $\{|0\rangle, |1\rangle\}$ effectue la transformation suivante :

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \longleftrightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Cette transformation est exactement une erreur de bit dans la base $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$. Pour corriger une erreur de phase, on va donc se servir de la méthode précédente pour corriger une erreur de bit dans la base auxiliaire.

8.2.2 Définition du code de Shor

Au total, il faut 9 qubits pour corriger toutes les erreurs : les erreurs de bit dans chaque bloc de 3 qubits, et les erreurs de phase entre les blocs de 3 qubits.

Définition 8.4. *Le code de Shor est défini par :*

$$|0\rangle \longrightarrow \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2^{\frac{3}{2}}}$$

$$|1\rangle \longrightarrow \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2^{\frac{3}{2}}}$$

Ce code permet la correction d'une erreur, toutefois il rend difficile l'application de portes logiques sur le bit ainsi protégé. Dans la suite nous présentons un code sur 7 qubits, sur lequel l'application de ces opérations est plus simple.