Code correcteur

Vidéo ■ partie 17. Code correcteur

Lors de la transmission d'un qubit il peut y avoir des erreurs. Les codes correcteurs permettent de détecter et corriger ces erreurs.

1. Un code correcteur classique

Lorsqu'on transmet un message électronique, le message reçu peut être différent du message envoyé à cause d'erreurs (erreurs de lecture/écriture, interférences,...). Cela peut être sans conséquence, par exemple tout le monde comprend la phrase « UN PETLT PAS PQUR L'HOMNE » malgré les fautes de frappe, mais pour envoyer un code d'identification du style « 562951413 » une erreur sur un seul chiffre compromet le message.
On distingue deux tâches : détecter s'il y a eu une erreur (si c'est le cas on pourrait envoyer à nouveau le message), mais on peut aussi utiliser des techniques qui permettent de corriger directement certaines erreurs.

1.1. Répétition

L'idée la plus simple pour sécuriser la transmission est de répéter chaque partie du message. Dans toute cette section on considère que le message est composé de 0 et de 1 :

- chaque « 0 » est remplacé avant transmission par « 000 »,
- chaque « 1 » est remplacé par « 111 ».

S'il y a une erreur lors de la transmission, le décodage se fait selon le principe de la majorité :

- 000, 001, 010, 100 sont décodés en « 0 »,
- 111, 110, 101, 011 sont décodés en « 1 ».

Prenons l'exemple du message « 1.0.1 » :

- répétition de chaque bit : « 111.000.111 »,
- le message est transmis mais des erreurs surviennent,
- le message reçu est « 101.001.111 »,
- selon la règle de la majorité, le message décodé est bien le message original « 1.0.1 ».

Bien évidemment, s'il y a trop d'erreurs, par exemple « 000 » est altéré en « 101 », alors le message décodé est erroné.

1.2. Efficacité

Nous allons comparer les erreurs suivant le codage utilisé. Considérons un message de n bits, chaque bit transmis pouvant être altéré avec une probabilité p.

Proposition 1.

- *Sans utiliser de codage, le message transmis est entièrement correct avec probabilité* $(1-p)^n$.
- *En utilisant le codage de répétition triple, le message décodé est entièrement correct avec probabilité* $(1-p_3)^n$ *où* $p_3 = p^2(3-2p)$.

Les tableaux suivants présentent les probabilités qu'un message de longueur n soit transmis parfaitement correctement, selon différentes valeurs de p, avec ou sans répétition.

Cas $p = 0.1$
(10% des bits sont altérés)

n	sans répétition	avec répétition
10	35%	75%
100	0%	5%
1000	0%	0%

Cas $p = 0.01$
(1% des bits sont altérés)

n	sans répétition	avec répétition
10	90%	99.7%
100	36%	97%
1000	0%	75%

Cas $p = 0.001$
(1 bit sur mille est altéré)

n	sans répétition	avec répétition
10	99%	99.99%
100	90%	99.97%
1000	37%	99.7%

Conclusion : pour un message long, il est indispensable de mettre un place un système permettant de détecter puis de corriger les erreurs.

Démonstration de la proposition 1.

- Sans utiliser de codage, un bit est transmis correctement avec probabilité $1-p$, pour que le message reçu soit identique au message initial, il faut que les n bits soient transmis sans être altérés, ce qui arrive avec probabilité $(1-p)^n$.
- Pour le codage de répétition triple, prenons l'exemple de la transmission du bit « 0 ». Le message reçu est :
  — « 000 » avec probabilité $(1-p)^3$ (trois bits corrects),
  — « 001 », « 010 », « 100 », chacun avec probabilité $p(1-p)^2$ (un bit faux, deux bits corrects),
  — « 110 », « 101 », « 011 », chacun avec probabilité $p^2(1-p)$ (deux bits faux, un bit correct),
  — « 111 » avec probabilité p^3 (trois bits faux).
  Pour les deux premiers cas, la règle de la majorité conduit au bon décodage « 0 ». Pour les deux derniers cas, le décodage donne « 1 » et le bit est mal décodé.
  La probabilité d'erreur (deux derniers cas) est donc :
  $$p_3 = 3p^2(1-p) + p^3 = p^2(3-2p).$$
  Chaque bit est donc transmis de façon correcte avec une probabilité $1-p_3$; les n bits d'une suite sont tous transmis correctement avec probabilité $(1-p_3)^n$.

□

Exercice.
Faire les calculs de la proposition 1 dans le cas d'une répétition de longueur 5 : $0 \mapsto 00000$ et $1 \mapsto 11111$.

2. Correction d'erreurs en informatique quantique

2.1. Obstacles

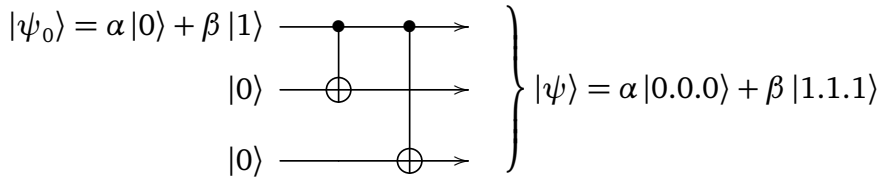
Les ordinateurs quantiques sont encore balbutiants et commettent beaucoup d'erreurs. Les codes correcteurs sont donc importants mais se confrontent à des problèmes spécifiques à l'informatique quantique :

- on ne peut pas mesurer un qubit sans le perturber irrémédiablement (effondrement du paquet d'onde),
- on ne peut pas cloner un qubit (voir le théorème de non-clonage quantique du chapitre « Portes quantiques »),
- enfin un qubit $\alpha|0\rangle + \beta|1\rangle$ peut prendre une infinité de valeurs (α, β étant des nombres complexes quelconques) à la différence du cas classique dans lequel l'information est codée par seulement deux valeurs 0 et 1.

Et pourtant, malgré toutes ces difficultés, il est possible de corriger des erreurs !
Dans toute la suite, on suppose que l'on souhaite transmettre un message formé par un qubit $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$. On commence par expliquer deux idées importantes pour la suite.

2.2. Augmentation d'un qubit

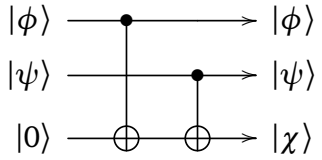
Nous avons vu que le fait de répéter un bit permet de corriger certaines erreurs. Comment faire pour nos qubits ? Nous allons généraliser une porte $FANOUT$ (voir le chapitre « Portes quantiques ») à l'aide de deux portes $CNOT$.
Le circuit suivant transforme le 1-qubit $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$ en le 3-qubit $|\psi\rangle = \alpha|0.0.0\rangle + \beta|1.1.1\rangle$.



- Pour le circuit ci-dessus si $|\psi_0\rangle = |0\rangle$ alors $|\psi\rangle = |0.0.0\rangle$ et si $|\psi_0\rangle = |1\rangle$ alors $|\psi\rangle = |1.1.1\rangle$. Par linéarité, cela donne le résultat $|\psi\rangle$ attendu pour $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$.
- Noter qu'ici nous n'avons pas dupliqué les coefficients. Le théorème de non-clonage quantique montre qu'aucun circuit ne permettrait de réaliser le 3-qubit $(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$.
- Noter aussi que si on considère le circuit inverse (de la droite vers la gauche) alors on effectue la transformation inverse : on passe de $|\psi\rangle = \alpha|0.0.0\rangle + \beta|1.1.1\rangle$ à $(\alpha|0\rangle + \beta|1\rangle)|0\rangle|0\rangle$. Ainsi après une mesure des deux derniers qubits, on obtiendrait sur la première ligne notre qubit $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$.

2.3. Décider si deux qubits de base sont égaux (sans les mesurer)

On considère ici un message composé de 1-qubits de base de la forme $|0\rangle$ ou $|1\rangle$. On souhaite vérifier sans aucune mesure si deux qubits de base sont égaux.
Pour cela on utilise un circuit à trois lignes quantiques : les deux premières sont les entrées à comparer, la troisième ligne est une ligne auxiliaire dont la sortie va répondre à la question « Les deux qubits de base sont-ils égaux ? »



Vérifier que :

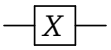
- Si $|\phi\rangle = |0\rangle$ et $|\psi\rangle = |0\rangle$ alors $|\chi\rangle = |0\rangle$.
- Si $|\phi\rangle = |1\rangle$ et $|\psi\rangle = |1\rangle$ alors $|\chi\rangle = |0\rangle$.
- Si $|\phi\rangle = |0\rangle$ et $|\psi\rangle = |1\rangle$ alors $|\chi\rangle = |1\rangle$.
- Si $|\phi\rangle = |1\rangle$ et $|\psi\rangle = |0\rangle$ alors $|\chi\rangle = |1\rangle$.

Noter que sur les deux premières lignes les qubits $|\phi\rangle$ et $|\psi\rangle$ restent inchangés. La sortie $|\chi\rangle$ vaut $|0\rangle$ si et seulement si $|\phi\rangle$ et $|\psi\rangle$ sont les mêmes qubits de base. La sortie $|\chi\rangle$ vaut $|1\rangle$ si et seulement si $|\phi\rangle$ et $|\psi\rangle$ sont des qubits de base différents.
Remarque : ce circuit permet de tester l'égalité de deux qubits de base, mais ne permet pas de comparer deux 1-qubits quelconques.

3. Code correcteur pour le flip d'un qubit

3.1. Un circuit qui corrige les erreurs ?

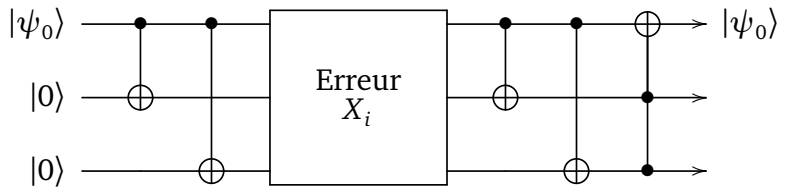
On souhaite transmettre le qubit $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$. On commence par augmenter le qubit en $|\psi\rangle = \alpha|0.0.0\rangle + \beta|1.1.1\rangle$ (on suppose que cette opération se fait sans erreur).
Lors de la transmission de ce 3-qubit il peut y avoir des erreurs. Commençons par le cas où l'erreur est un « flip » d'un des qubits. Par exemple $\alpha|0.0.0\rangle + \beta|1.1.1\rangle$ est mal transmis en $\alpha|0.0.1\rangle + \beta|1.1.0\rangle$.
Noter qu'un flip correspond à une porte X sur l'un des trois qubits, porte qui change $|0\rangle$ en $|1\rangle$ et réciproquement.



Comment détecter et corriger cette erreur ?

3.2. Circuit

Voici un circuit qui permet la transmission correct d'un qubit $|\psi_0\rangle$, même si lors de la transmission une erreur de type X se produit.



- X_i désigne l'action d'une porte X sur l'une des lignes $i \in \{1, 2, 3\}$.
- Où que soit cette erreur, la première ligne du circuit renvoie toujours le qubit original $|\psi_0\rangle$.
- Le circuit est composé de 4 portes $CNOT$ et terminé par une porte de Toffoli.
- On rappelle qu'une porte de Toffoli, est l'action d'une porte X (sur la ligne du « $\oplus$ ») à condition que les qubits des deux autres lignes soient tous les deux $|1\rangle$.

3.3. Calculs

Effectuons les calculs qui justifient que le qubit de sortie est bien le qubit original malgré l'erreur.

- Cas erreur X_1 (flip sur la première ligne).
  - — Cas $|\psi_0\rangle = |0\rangle$. Le 3-qubit avant l'erreur est $|0.0.0\rangle$. Alors le 3-qubit reçu est $|1.0.0\rangle$, les deux portes $CNOT$ le transforment en $|1.1.1\rangle$ et la porte de Toffoli renvoie $|0.1.1\rangle$. Le premier qubit est bien $|0\rangle$.
  - — Cas $|\psi_0\rangle = |1\rangle$. Le 3-qubit avant l'erreur est $|1.1.1\rangle$, mais le qubit reçu est $|0.1.1\rangle$, les deux portes $CNOT$ ne le changent pas, et la porte de Toffoli renvoie $|1.1.1\rangle$. Le premier qubit est bien $|1\rangle$.

— Cas $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$. Par linéarité, les calculs précédents donnent comme sortie $\alpha|0.1.1\rangle + \beta|1.1.1\rangle = (\alpha|0\rangle + \beta|1\rangle)|1.1\rangle$. Si on ne retient que le premier qubit on obtient $\alpha|0\rangle + \beta|1\rangle$ qui est bien notre qubit initial $|\psi_0\rangle$.

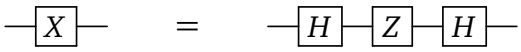
- Cas erreur X_2 (flip sur la deuxième ligne).
  — Cas $|\psi_0\rangle = |0\rangle$. Avant l'erreur le 3-qubit est $|0.0.0\rangle$, après erreur c'est $|0.1.0\rangle$, les deux portes $CNOT$ et la porte de Toffoli ne changent rien. On obtient $|0.1.0\rangle$.
  — Cas $|\psi_0\rangle = |1\rangle$. Avant l'erreur le 3-qubit est $|1.1.1\rangle$, après erreur c'est $|1.0.1\rangle$, les deux portes $CNOT$ donnent $|1.1.0\rangle$, la porte de Toffoli ne change rien. On obtient $|1.1.0\rangle$.
  — Cas $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$. Par linéarité, la sortie vaut $\alpha|0.1.0\rangle + \beta|1.1.0\rangle = (\alpha|0\rangle + \beta|1\rangle)|1.0\rangle$. Le premier qubit est encore $\alpha|0\rangle + \beta|1\rangle$ qui est bien le qubit initial $|\psi_0\rangle$.
- Cas erreur X_3 (flip sur la troisième ligne).
  Les calculs sont similaires. $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$ donne après erreur $\alpha|0.0.1\rangle + \beta|1.1.0\rangle$, et la fin du circuit renvoie $\alpha|0.0.1\rangle + \beta|1.0.1\rangle = (\alpha|0\rangle + \beta|1\rangle)|0.1\rangle$. Le premier qubit est de nouveau $|\psi_0\rangle$.

4. Code correcteur pour l'inversion de phase d'un qubit

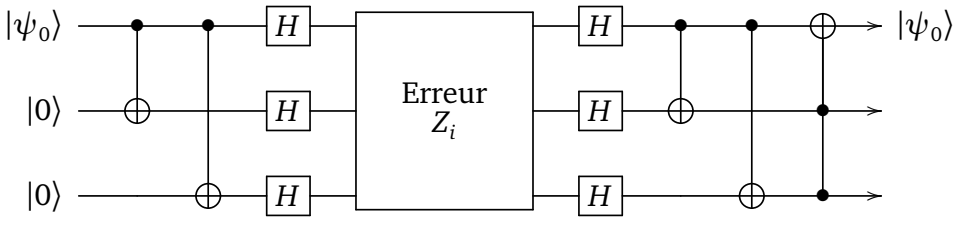
4.1. Circuit

Le flip n'est pas la seule erreur possible. Une autre erreur est l'inversion de phase qui est le changement de $\alpha|0\rangle + \beta|1\rangle$ en $\alpha|0\rangle - \beta|1\rangle$. Le changement de phase correspond à une porte Z.

On souhaite transmettre le qubit $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$. On commence par augmenter le qubit en $|\psi\rangle = \alpha|0.0.0\rangle + \beta|1.1.1\rangle$. Ensuite, lors de la transmission, on suppose que se produit un changement de phase sur l'un des trois qubits. On se ramène à la situation précédente en notant qu'une porte X est équivalente à une porte HZH, où H est une porte de Hadamard :



Voici le circuit qui détecte et corrige cette erreur.



Z_i désigne l'action d'une porte Z sur l'une des lignes $i \in \{1,2,3\}$.

4.2. Calculs

Nous n'avons pas à faire les calculs puisque ce sont les mêmes que pour le flip. En effet, on a rappelé que $HZH = X$, donc l'ensemble des portes de Hadamard et l'erreur Z_i correspondent à une erreur X_i.
Une autre façon de voir les calculs est d'utiliser la notation $|+\rangle$ et $|-\rangle$.

$$|+\rangle = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

On a aussi réciproquement $H|+\rangle = |0\rangle$ et $H|-\rangle = |1\rangle$.

Un changement de phase Z envoie $\alpha|0\rangle + \beta|1\rangle$ sur $\alpha|0\rangle - \beta|1\rangle$, et peut être simplement défini par :

$$|+\rangle \xmapsto{Z} |-\rangle \qquad |-\rangle \xmapsto{Z} |+\rangle$$

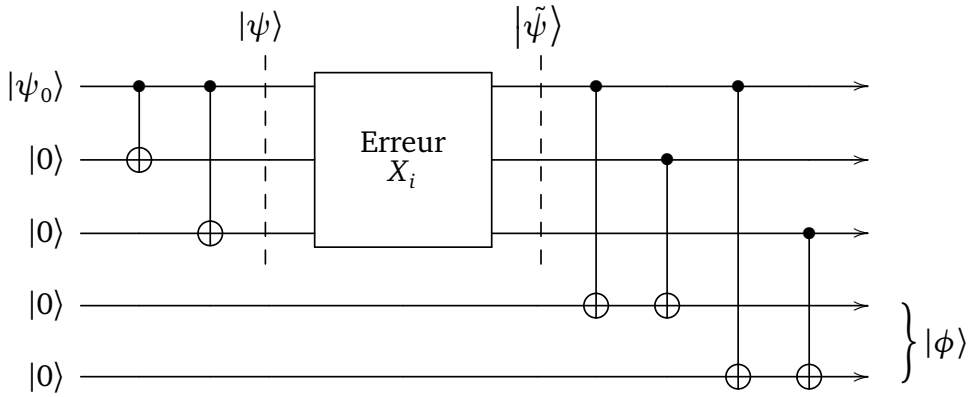
C'est donc une sorte de flip dans une autre base.
Si au départ $|\psi_0\rangle = |0\rangle$ alors, après augmentation, on a $|\psi\rangle = |0.0.0\rangle$. Puis à l'aide des portes de Hadamard le 3-qubit avant erreur est $|+\rangle|+\rangle|+\rangle$, que l'on note $|+.+.+\rangle$. L'erreur Z_i change l'un des signes, par exemple on obtient $|-.+.+\rangle$, les nouvelles portes de Hadamard le transforment en $|1.0.0\rangle$ (qui correspond bien à un flip classique de $|\psi\rangle$), qui est corrigé par la fin du circuit en $|0.1.1\rangle$ et ainsi le premier qubit est bien $|0\rangle$.

5. Détection d'un flip

Les circuits précédents font très bien leur travail : ils détectent et corrigent les erreurs. Mais ils ne sont pas très pédagogiques car les deux tâches sont effectuées en même temps. Nous allons modifier légèrement ces circuits afin qu'ils détectent les erreurs et on expliquera ensuite comment les corriger.

5.1. Un circuit qui détecte les flips

Voici un circuit qui détecte un flip.



Ce circuit se décompose en deux registres :
Premier registre. Les trois premières lignes correspondent au qubit augmenté $|000\rangle$ ou $|111\rangle$, lors de la transmission survient une erreur qui est ici un flip sur une des trois lignes.
Second registre. Les deux dernières lignes servent à détecter l'erreur. On parle de « lignes auxiliaires ».

5.2. Sortie

Notons $|\tilde{\psi}\rangle$ le 3-qubit du premier registre après transmission (juste après l'erreur éventuelle). Notons $|\phi\rangle$ le 2-qubit obtenu en sortie du second registre (à la fin du circuit).

- **Pas d'erreur.**
  Si $|\psi_0\rangle = |0\rangle$ et si $|\tilde{\psi}\rangle = |0.0.0\rangle$ alors $|\phi\rangle = |0.0\rangle$. Il n'y a pas d'erreur donc rien à corriger. De même, si $|\psi_0\rangle = |1\rangle$ et $|\tilde{\psi}\rangle = |1.1.1\rangle$ alors de nouveau $|\phi\rangle = |0.0\rangle$. Il n'y a toujours pas d'erreur donc rien à corriger. Par linéarité, si $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$ alors le 5-qubit final est $(\alpha|0.0.0\rangle + \beta|1.1.1\rangle)|0.0\rangle$.
- **Flip du premier qubit.**
  Si $|\tilde{\psi}\rangle = |1.0.0\rangle$ (alors qu'on voulait transmettre $|0.0.0\rangle$) alors $|\phi\rangle = |1.1\rangle$. Il y a une erreur et cette erreur est sur la première ligne. On corrige l'erreur en rajoutant une porte X sur la première ligne. Ainsi après correction on obtient bien un premier registre qui vaut $|0.0.0\rangle$.
  De même si $|\tilde{\psi}\rangle = |0.1.1\rangle$ (alors qu'on voulait transmettre $|1.1.1\rangle$) alors de nouveau $|\phi\rangle = |1.1\rangle$. Et on rajoute une porte X sur la première ligne.

Ainsi un qubit $|\psi\rangle = \alpha|0.0.0\rangle + \beta|1.1.1\rangle$ qui serait mal transmis en $|\tilde{\psi}\rangle = \alpha|1.0.0\rangle + \beta|0.1.1\rangle$, donnerait $|\phi\rangle = |1.1\rangle$ et serait bien corrigé en $|\psi\rangle$.

- **Flip du deuxième qubit.**
  Si $|\tilde{\psi}\rangle = \alpha|0.1.0\rangle + \beta|1.0.1\rangle$ (au lieu de $\alpha|0.0.0\rangle + \beta|1.1.1\rangle$) alors $|\phi\rangle = |1.0\rangle$ et on rajoute une porte X sur la deuxième ligne.
- **Flip du troisième qubit.** Si $|\tilde{\psi}\rangle = \alpha|0.0.1\rangle + \beta|1.1.0\rangle$ alors $|\phi\rangle = |0.1\rangle$. On corrige l'erreur en rajoutant une porte X sur la troisième.

Noter qu'on n'a jamais effectué de mesure sur le premier registre.

Bilan :

- si $|\phi\rangle = |0.0\rangle$ pas d'erreur,
- si $|\phi\rangle = |1.1\rangle$ erreur de flip sur la première ligne,
- si $|\phi\rangle = |1.0\rangle$ erreur de flip sur la deuxième ligne,
- si $|\phi\rangle = |0.1\rangle$ erreur de flip sur la troisième ligne.

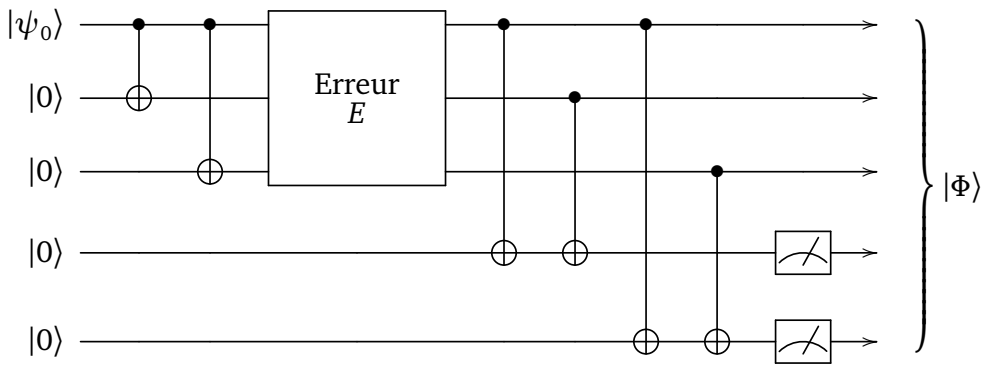
Une fois qu'on sait sur quelle ligne est l'erreur par mesure de $|\Phi\rangle$, il est facile de la corriger en ajoutant une porte X en fin de circuit sur la ligne correspondante.

5.3. Erreur par déformation

On souhaite envoyer l'information $|0\rangle$, augmentée en $|0.0.0\rangle$. On suppose que l'erreur est d'un type nouveau, le qubit est légèrement déformé. Prenons l'exemple d'une erreur qui, en sortie du premier registre, fournit :

$$|\tilde{\psi}\rangle = \sqrt{1-\epsilon^2}\,|0.0.0\rangle + \epsilon\,|0.0.1\rangle\,,$$

où $\epsilon > 0$ est un petit réel.
Le circuit suivant détecte ce type d'erreur. C'est le même que le circuit précédent avec en plus la mesure du second registre.



On a vu que juste avant la mesure, si $|\tilde{\psi}\rangle = |0.0.0\rangle$ alors le 5-qubit de sortie est $|\Phi\rangle = |0.0.0\rangle\,|0.0\rangle$; et si $|\tilde{\psi}\rangle = |0.0.1\rangle$ alors le 5-qubit de sortie est $|\Phi\rangle = |0.0.1\rangle\,|0.1\rangle$.
Donc pour le qubit $|\tilde{\psi}\rangle = \sqrt{1-\epsilon^2}\,|0.0.0\rangle + \epsilon\,|0.0.1\rangle$, la sortie est (avant mesure) :

$$|\Phi\rangle = \sqrt{1-\epsilon^2}\,|0.0.0\rangle\,|0.0\rangle + \epsilon\,|0.0.1\rangle\,|0.1\rangle\,.$$

Que se passe-t-il lorsque l'on mesure le second registre ? Deux mesures seulement sont possibles 0.0 ou bien 0.1.

- Si on obtient la mesure 0.0, alors on sait qu'il n'y a rien à corriger. Effectivement, dans ce cas le premier registre s'est effondré en $|\Psi\rangle = |0.0.0\rangle$, il n'y a pas d'erreur.
- Si on obtient la mesure 0.1, alors on sait qu'il y a une erreur qu'il faut corriger en ajoutant un flip sur la troisième ligne. Effectivement dans ce cas le premier registre s'est effondré en $|\Psi\rangle = |0.0.1\rangle$. Après correction on obtient $|0.0.0\rangle$.

Dans tous les cas on obtient, après correction éventuelle, le 3-qubit $|0.0.0\rangle$. Il s'est passé un phénomène appelé *discrétisation de l'erreur par la mesure* : même si l'erreur pouvait prendre une infinité de formes (car il y a une infinité de ϵ possibles), après mesure on se ramène à seulement deux possibilités.

Proposition 2.
Le circuit précédent détecte n'importe quelle erreur du type $E = aI + bX$.

I désigne l'identité et X un flip. Une erreur $E = aI + bX$ transforme un qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ en

$$E|\psi\rangle = (aI + bX)|\psi\rangle = a|\psi\rangle + bX|\psi\rangle .$$

Si lors de la transmission, sur une seule des trois premières lignes, un qubit subit une telle erreur, alors la sortie du second permet de savoir comment corriger cette erreur.
La preuve est la généralisation des calculs faits pour l'exemple avec les « ϵ ».

Démonstration. On note $|\psi_0\rangle = \alpha|0\rangle + \beta|1\rangle$ et $|\psi\rangle = \alpha|0.0.0\rangle + \beta|1.1.1\rangle$. Si $E = I$, alors il n'y pas d'erreur le qubit de sortie avant mesure est $|\Phi_0\rangle = |\psi\rangle|0.0\rangle$.
Si $E = X$, alors on a déjà vu que selon la ligne de l'erreur, le qubit de sortie avant mesure est l'un des $|\tilde{\psi}_1\rangle|1.1\rangle$, $|\tilde{\psi}_2\rangle|1.0\rangle$, $|\tilde{\psi}_3\rangle|0.1\rangle$.
Si l'erreur est $aI + bX$ alors, par linéarité le qubit de sortie avant mesure est par exemple

$$|\Phi\rangle = a|\psi\rangle|0.0\rangle + b|\tilde{\psi}_1\rangle|1.1\rangle$$

(ou l'une des deux autres situations).
Lors de la mesure du second registre :

- Si on obtient 0.0, alors on sait qu'il n'y a rien à corriger. Effectivement dans ce cas le premier registre s'est effondré en $|\psi\rangle$, il n'y a pas d'erreur.
- Si on obtient 1.1, alors on sait qu'il y a une erreur qu'il faut corriger en ajoutant un flip sur la première ligne. Effectivement dans ce cas le premier registre s'est effondré en $|\tilde{\psi}_1\rangle = \alpha|1.0.0\rangle + \beta|0.1.1\rangle$. Après correction on obtient $|\psi\rangle = \alpha|0.0.0\rangle + \beta|1.1.1\rangle$.
- De même pour les deux autres situations.

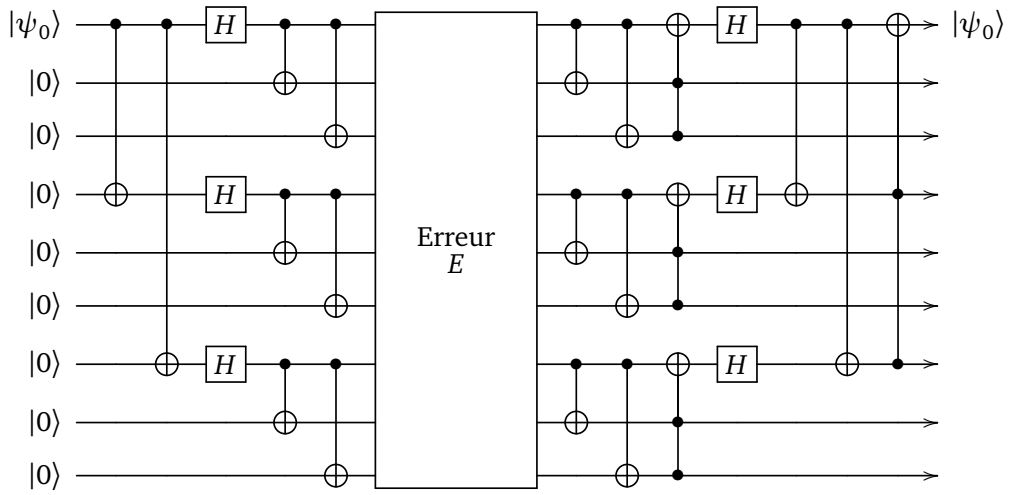
□

Exercice.
Réaliser un circuit qui détecte une inversion de phase et expliquer ensuite comment corriger l'éventuelle erreur. Montrer que votre circuit détecte n'importe quelle erreur $aI + bZ$ sur une ligne.

6. Code correcteur de Shor

6.1. Circuit

Nous terminons avec un circuit composé de 9 lignes. Ce circuit détecte et corrige une erreur de transmission qui se produirait sur une seule des 9 lignes. Cette erreur peut être un flip X, une inversion de phase Z, mais plus généralement n'importe quelle erreur sur un 1-qubit (mais toujours sur une seule ligne).



6.2. Calculs

Proposition 3.
Le circuit précédent détecte et corrige n'importe quelle erreur du type $E = aI + bX + cY + dZ$ qui arriverait sur une seule de ses lignes.

Avant de justifier ce résultat, il faut passer un peu de temps à comprendre que ce circuit est construit en regroupant le circuit qui corrige un flip et celui qui corrige une inversion de phase. Ensuite le mieux est de le programmer pour vérifier qu'il fonctionne !

Donnons maintenant des explications théoriques. Nous modélisons une erreur E comme la transformation linéaire d'un qubit en un autre qubit. Autrement dit une erreur est définie par une matrice 2×2, notée E. Rappelons la définition des matrices de Pauli auxquelles on ajoute l'identité :

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

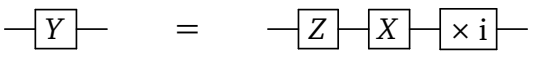
Ces quatre matrices sont linéairement indépendantes et forment donc une base de l'espace vectoriel de dimension 4, $M_2(\mathbb{C})$. Ainsi n'importe quelle $E \in M_2(\mathbb{C})$ se décompose :

$$E = aI + bX + cY + dZ$$

où $a, b, c, d \in \mathbb{C}$.
Par linéarité du circuit, on se ramène aux quatre cas $E = I$, $E = X$, $E = Y$, $E = Z$. La structure du circuit, qui regroupe la correction de flip et d'inversion de phase, fait qu'il corrige les erreurs X et Z (et aussi I).
Il ne reste plus qu'à traiter le cas de $E = Y$. Mais nous avons l'égalité :

$$Y = \mathrm{i}XZ.$$

Ceci est une égalité de matrices, qui se traduit en une équivalence de portes :



Ainsi une erreur Y est la combinaison d'un flip et d'une inversion de phase et sera bien corrigée par notre circuit.

Notes. Ce cours n'est qu'un aperçu d'un vaste domaine. La présentation adoptée ici est basée sur un cours en ligne du CERN *Introduction to quantum computing* par Elias F. Combarro. Une étude plus approfondie est faite dans le livre de Nielsen et Chuang *Quantum computation and quantum information*.