Informatique quantique IFT6155

Correction d'erreurs

Correction d'erreur classique

Définition: La distance de Hamming entre deux chaînes x et y de n bit est le nombre de positions ou elle sont différentes,

$$H(x,y) = x_1 \oplus y_1 + x_2 \oplus y_2 + \cdots + x_n \oplus y_n.$$

Le poids de Hamming de x est définit par $W(x) = H(0,x)$.

Définition: Un code $[n,k,d]$ est un une fonction injective $E : \{0,1\}^k \to \{0,1\}^n$ tel que pour tout x et y, $x \neq y \Rightarrow D(E(x),E(y)) \geq d$.

Définition: On dira qu'un code C est linéaire il existe une matrice G $(n \times k)$ tel que $E(x) = M^T.x$. On appelle G la matrice génératrice du code C.

Fait: Un code $[n,k,d]$ encode des chaînes de k bit dans des chaînes de n bit et permet de détecter jusqu'à $d-1$ erreurs et de corriger jusqu'à $\lfloor d/2 \rfloor - 1$ erreurs.

L'algorithme de décodage naïf fonctionne comme suit. Soit z le message incorrecte et x appartenant au code tel que $H(x,z) \leq \lfloor d/2 \rfloor - 1$ alors le décodage retourne $E^{-1}(x)$.

Exemple

Soit le code C définit par $E(0) = 000$ et $E(1) = 111$.
Clairement ce code est $[3, 1, 3]$ et il est linéaire.

$$G = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

$$E(x) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \cdot x$$

Ce code peut corriger une erreur et en détecter deux mais trois erreurs inversent les deux mots de code.

On peut répéter ce code pour plus de 1 bit. Par exemple pour encoder 4 bit on obtient un code $[12, 4, 3]$. Peut-on faire mieux?

Exemple

Soit C le code ayant comme matrice génératrice G,

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

$$C = \begin{bmatrix} 0000 \cdot 000 & 0100 \cdot 110 & 1000 \cdot 111 & 1100 \cdot 001 \\ 0001 \cdot 011 & 0101 \cdot 101 & 1001 \cdot 100 & 1101 \cdot 010 \\ 0010 \cdot 101 & 0110 \cdot 011 & 1010 \cdot 010 & 1110 \cdot 100 \\ 0011 \cdot 110 & 0111 \cdot 000 & 1011 \cdot 001 & 1111 \cdot 111 \end{bmatrix}$$

Nous avons donc que $n = 7$ et $k = 4$ qu'en est t'il de d? On peut vérifier que $d = 3$ ce code corrige une erreur et encode 4 bits, ceci est plus efficace que l'utilisation répétée du code précédent qui serait de la forme $[12, 4, 3]$.

Codes équivalents

Deux code C_1 et C_2 sont équivalent si si on peut obtenir C_2 a partir de C_1 en permutant les positions dans les mots de code et/ou en inversant le bit de certaines positions. Dans le cas de code linéaire, on dira que C_1 et C_2 sont équivalent si on peut obtenir G_2 a partir de G_1 en permutant les lignes de G_1 ou en ajoutant un vecteur z a chaque ligne.

Par exemple

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = G_2$$

Forme systématique

Lemme:
Tout code linéaire C, $[n, k, d]$ est équivalent à un code linéaire C' tel que

$$G' = (I_k|A).$$

On dira que le code C' est en forme systématique.

Preuve:
On utilise les règles d'équivalence pour obtenir la matrice identité dans la première partie de la matrice de G.

Définition:
Pour un code C, $[n, k, d]$ ayant comme matrice de génératrice $G = (I_k|A)$ on définit la matrice de parité $H = (A^T|I_{n-k})$.

Lemme: Pour tout w dans C, $H \cdot w = 0$.

Définition:
Pour un code C ayant comme matrice génératrice G on définit le code $C^\perp = \{w|\forall x \in Cx \cdot w = 0\}$.

Lemme:
La matrice de parité H d'un code C est la matrice génératrice du code $C^\perp$.

Définition:
Un code C tel que $C^\perp = C$ est auto-dual (self dual).

Code de Hamming

Définisions une famille de code (code de Hamming) en donnant une définition simple pour leur matrice de parité.

$$H_k = \left([1]_{bin}, [2]_{bin}, \ldots, [2^k - 1]_{bin}\right)$$

En particulier

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

et donc la matrice génératrice est

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Nous avons vu que ce code est $[7, 4, 3]$.

Lemme: Le code de Hamming de niveau k est un code $[2^k - 1, 2^k - k - 1, 3]$ et peux donc corriger une erreur.

Borne supérieure

On aimerait pour n et d donné, maximiser le nombre de mots de code.

Théorème [Hamming]:
Pour tout code (binaire) C, $[n, k, 2t+1]$ nous avons que

$$\sum_{i=0}^{t} \binom{n}{i} \leq 2^{n-k}$$

Preuve:
On compte le nombre de mots. Il y a 2^k mots de code. Il y a $2^k n$ mots a distance exactement 1 d'un mot de code. Pour $0 \leq i \leq t$, il y a $2^k \binom{n}{i}$ mots à distance exactement i d'un mots de code. On a donc

$$2^n \geq \sum_{i=0}^{t} 2^k \binom{n}{i}$$

Borne inférieure

Théorème [Gilbert-Varshamov]:
Si

$$\sum_{i=0}^{d-2} \binom{n-1}{i} < 2^{n-k}$$

alors il existe un code linéaire $[n, k, d]$.

On peut reformuler ce théorème comme suit. Soit p la probabilité d'erreur d'un canal binaire symétrique. On peut en utilisant un codage en bloc suffisamment long transmettre de façon fiable un bit par la transmission en moyenne de $\frac{1}{1-H(p)}$.

En particulier si la probabilité d'erreur est de 1% il faudra (et on peut) utiliser en moyen 1.09 bits transmit par bits de message, pour 5% 1.40, pour 25%, 5.3 et pour 45% , 138.4.

Correction d'erreur quantique

Nous avons vu qu'il est impossible de cloner un qubit. Cela signifie qu'il est impossible d'utiliser de façon évidente des techniques classiques.

L'ordinateur quantique est particulièrement sensible aux erreurs.

Les erreurs peuvent à la fois être discrète ou continue.

Un code correcteur ne doit absolument pas donner d'information sur l'état encoder ou corriger.

C'est Peter Shor qui en 1995 qui donna le premier code correcteur quantique.

Types d'erreurs

Une erreur peux toujours être vue comme une interaction (indésirable) avec l'environnement.

Concentrons-nous sur le cas d'un qubits $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

On suppose que l'environnement est dans l'état $|e\rangle$ et qu'une transformation unitaire U est appliquer sur le système conjoint, environnement plus qubit.

$$\begin{aligned}
U|e\rangle|\psi\rangle &= U|e\rangle(\alpha|0\rangle + \beta|1\rangle) \\
&= \alpha U|e\rangle|0\rangle + \beta U|e\rangle|1\rangle \\
&= \alpha(|e_{00}\rangle|0\rangle + |e_{01}\rangle|1\rangle) + \beta(|e_{10}\rangle|0\rangle + |e_{11}\rangle|1\rangle) \\
&= \frac{1}{2}(|e_{00}\rangle + |e_{10}\rangle)(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}(|e_{00}\rangle - |e_{10}\rangle)(\alpha|0\rangle - \beta|1\rangle) + \\
&\quad \frac{1}{2}(|e_{01}\rangle + |e_{11}\rangle)(\alpha|1\rangle + \beta|0\rangle) + \frac{1}{2}(|e_{01}\rangle - |e_{11}\rangle)(\alpha|1\rangle - \beta|0\rangle) \\
&= |e_{0+}\rangle|\psi\rangle + |e_{0-}\rangle(Z|\psi\rangle) + |e_{1+}\rangle(X|\psi\rangle) + |e_{1-}\rangle(XZ|\psi\rangle)
\end{aligned}$$

Si on mesure l'environnement nous aurons donc un *colapse* sur l'état $|\psi\rangle$ potentiellement une erreur X et/ou une erreur Z.

Théorème fondamental

Si on peut corriger t erreur de type X et t erreurs de type Z alors on peut corriger n'importequel erreur se produisant sur t qubits.

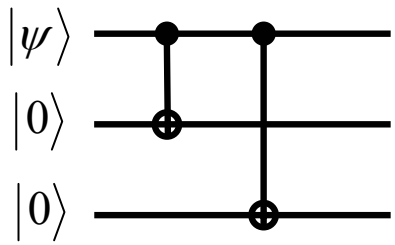
Erreurs X

Regardons premièrement comment on pourait corriger les erreurs de type X.

Utilisons le code suivant

$$|\mathbf{0}\rangle = |000\rangle \qquad |\mathbf{1}\rangle = |111\rangle$$

Nous pouvons utiliser le circuit suivant pour effectuer l'encodage.



Erreurs X

Si on encode l'état $\alpha|0\rangle + \beta|1\rangle$ on obtiendra $\alpha|000\rangle + \beta|111\rangle$.

Si nous avons au plus une erreur sur l'état encodé nous aurons un des quatre états suivants

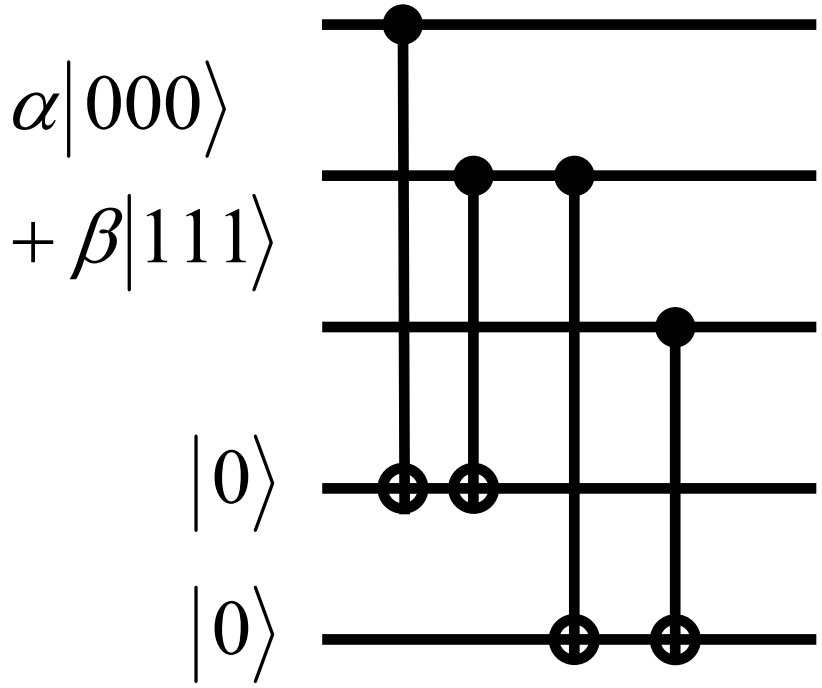
$$\alpha|000\rangle + \beta|111\rangle \quad \alpha|100\rangle + \beta|011\rangle \quad \alpha|010\rangle + \beta|101\rangle \quad \alpha|001\rangle + \beta|110\rangle$$

qui sont deux à deux orthogonaux. Essayons de détecter l'erreur sans affecter l'état. Ajoutons deux qubits ancillaires dans l'état $|0\rangle|0\rangle$. Effectuons la transformation unitaire $E = C_{[3,5]}C_{[2,5]}C_{[2,4]}C_{[1,4]}$.

Erreurs X

$$E = C_{[3,5]}C_{[2,5]}C_{[2,4]}C_{[1,4]}$$

.



Erreurs X

On peut calculer que

$$\begin{aligned}
E(\alpha|000\rangle + \beta|111\rangle)|00\rangle &= (\alpha 000 + \beta|111\rangle)|00\rangle \\
E(\alpha|100\rangle + \beta|011\rangle)|00\rangle &= (\alpha 100 + \beta|011\rangle)|10\rangle \\
E(\alpha|010\rangle + \beta|101\rangle)|00\rangle &= (\alpha 010 + \beta|101\rangle)|11\rangle \\
E(\alpha|001\rangle + \beta|110\rangle)|00\rangle &= (\alpha 001 + \beta|110\rangle)|01\rangle
\end{aligned}$$

S'il y a une erreur ou moins on peut mesurer le deuxième registre (syndrome) sans affecter le premier registre. L'information obtenue nous permet de corriger l'erreur sur le premier registre s'il y a lieu.

Notez que l'on obtient exactement le même résultat en remplaçant les $+$ par des $-$ dans les équations.

Erreurs Z

Maintenant, comment peut-on corriger une erreur de type Z. L'identité suivante nous permet de ramener ce cas a une erreur de type X.

$$HZH = X$$

Il suffit d'encoder $|\psi\rangle$ dans un état permettant la correction d'une erreur de type X pis d'appliquer H sur chaque qubit.

Le décodage commence par défaire H et procède de la même façon.

Le tout fonctionne puisque

$$HH = I \qquad HZH = X$$

$$|\mathbf{0}\rangle = H^{\otimes 3}|000\rangle = \frac{1}{2\sqrt{2}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$$

$$|\mathbf{1}\rangle = H^{\otimes 3}|111\rangle = \frac{1}{2\sqrt{2}}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$$

Le code de Shor

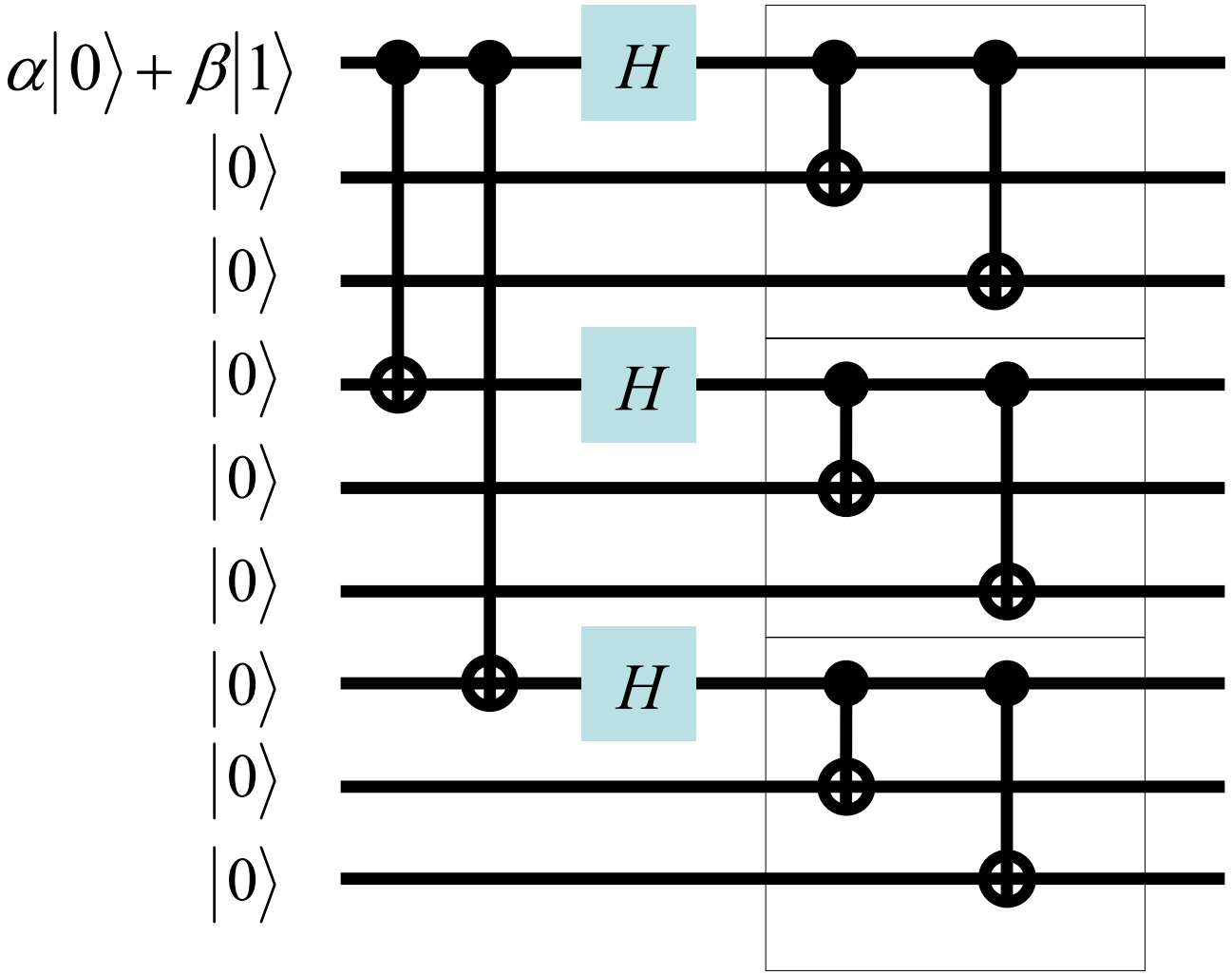
Comment peut-on corriger à la fois une erreur de type X et/ou une erreur de type Z. Ceci nous permettra en réalité de corriger n'importe quelle erreur survenant sur un seul qubit. Ce code a été découvert par Shor et ce fut une avancée véritable de l'informatique quantique.

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

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

On code d'abord pour corriger une erreur de type Z puis on code pour corriger une type X. Pour corriger on procède dans l'ordre inverse.

Encodage


$\alpha|0\rangle + \beta|1\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|0\rangle$
H
H
H

Décodage

Le décodage du code de Shor est assez simple. Supposons qu'il y a eu au plus une erreur X et au plus une erreur Z. Ces deux erreurs peuvent survenir sur le même qubit ou sur deux qubits différents.

Voyons un exemple de décodage ou une erreur de type X survient sur le deuxième qubit et une erreur de type Z surviens sur le sixième qubit. Notez qu'une erreur de type Z sur le sixième qubit est indistinguable d'une erreur de type Z sur le quatrième ou le cinquième qubit.

Le qubit encoder est $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

$$\alpha\frac{(|010\rangle + |101\rangle)(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} +$$

$$\beta\frac{(|010\rangle - |101\rangle)(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$

Décodage

Utilisons l'algorithme de correction d'erreur de type X sur chaque triplet. On ajoute deux qubit ancillaires dans l'état $|00\rangle$. On obtient

$$\alpha|00\rangle\frac{(|010\rangle+|101\rangle)(|000\rangle-|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}+$$

$$\beta|00\rangle\frac{(|010\rangle-|101\rangle)(|000\rangle+|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

Après les quatre C on obtient

$$\alpha|11\rangle\frac{(|010\rangle+|101\rangle)(|000\rangle-|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}+$$

$$\beta|11\rangle\frac{(|010\rangle-|101\rangle)(|000\rangle+|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

et donc le syndrome peut être factorisé et mesuré sans perturber l'état. On obtient $|11\rangle$ ce qui nous apprend qu'une erreur de type X est survenue sur le deuxième qubit. On applique X pour corriger l'erreur et on se débarrasse de l'ensila.

$$\alpha\frac{(|000\rangle+|111\rangle)(|000\rangle-|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}+$$

$$\beta\frac{(|000\rangle-|111\rangle)(|000\rangle+|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

Décodage

L'état obtenu semble est presque dans une forme permettant la correction d'une erreur de type Z. Décodons chaque triplet en appliquant $C_{[1,2]}, C_{[1,3]}, C_{[4,5]}, C_{[4,6]}, C_{[7,8]}, C_{[7,9]}$. On obtient l'état suivant.

$$\alpha\frac{(|000\rangle + |100\rangle)(|000\rangle - |100\rangle)(|000\rangle + |100\rangle)}{2\sqrt{2}} +$$

$$\beta\frac{(|000\rangle - |100\rangle)(|000\rangle + |100\rangle)(|000\rangle - |100\rangle)}{2\sqrt{2}}$$

les qubits $2, 3, 5, 6, 8, 9$ sont tous dans l'état $|0\rangle$ et peuvent donc être factoriser.

$$\alpha\frac{(|0\rangle + |1\rangle)|00\rangle(|0\rangle - |1\rangle)|00\rangle(|0\rangle + |1\rangle)|00\rangle}{2\sqrt{2}} +$$

$$\beta\frac{(|0\rangle - |1\rangle)|00\rangle(|0\rangle + |1\rangle)|00\rangle(|0\rangle - |1\rangle)|00\rangle}{2\sqrt{2}}$$

On peut donc s'en débarrasser et on obtient

$$\alpha\frac{(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)}{2\sqrt{2}} +$$

$$\beta\frac{(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)}{2\sqrt{2}}$$

Décodage

On obtient

$$\alpha\frac{(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)}{2\sqrt{2}}+$$

$$\beta\frac{(|0\rangle-|1\rangle)(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)}{2\sqrt{2}}$$

qui est bien l'encodage de $|\psi\rangle$ avec une erreur Z dans le code permettant la correction de ce type d'erreur. Si on applique H sur chaque qubit on obtient

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

Ce qui est bien un mot de code pour des erreurs de type X avec une erreur. On peut donc corriger cette erreur pour obtenir

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

finalement on applique $C_{[1,2]}$ et $C_{[1,3]}$ et on obtient

$$\alpha|000\rangle+\beta|100\rangle=(\alpha|0\rangle+\beta|1\rangle)|00\rangle$$

Laflamme, Miquel, Paz et Zurek

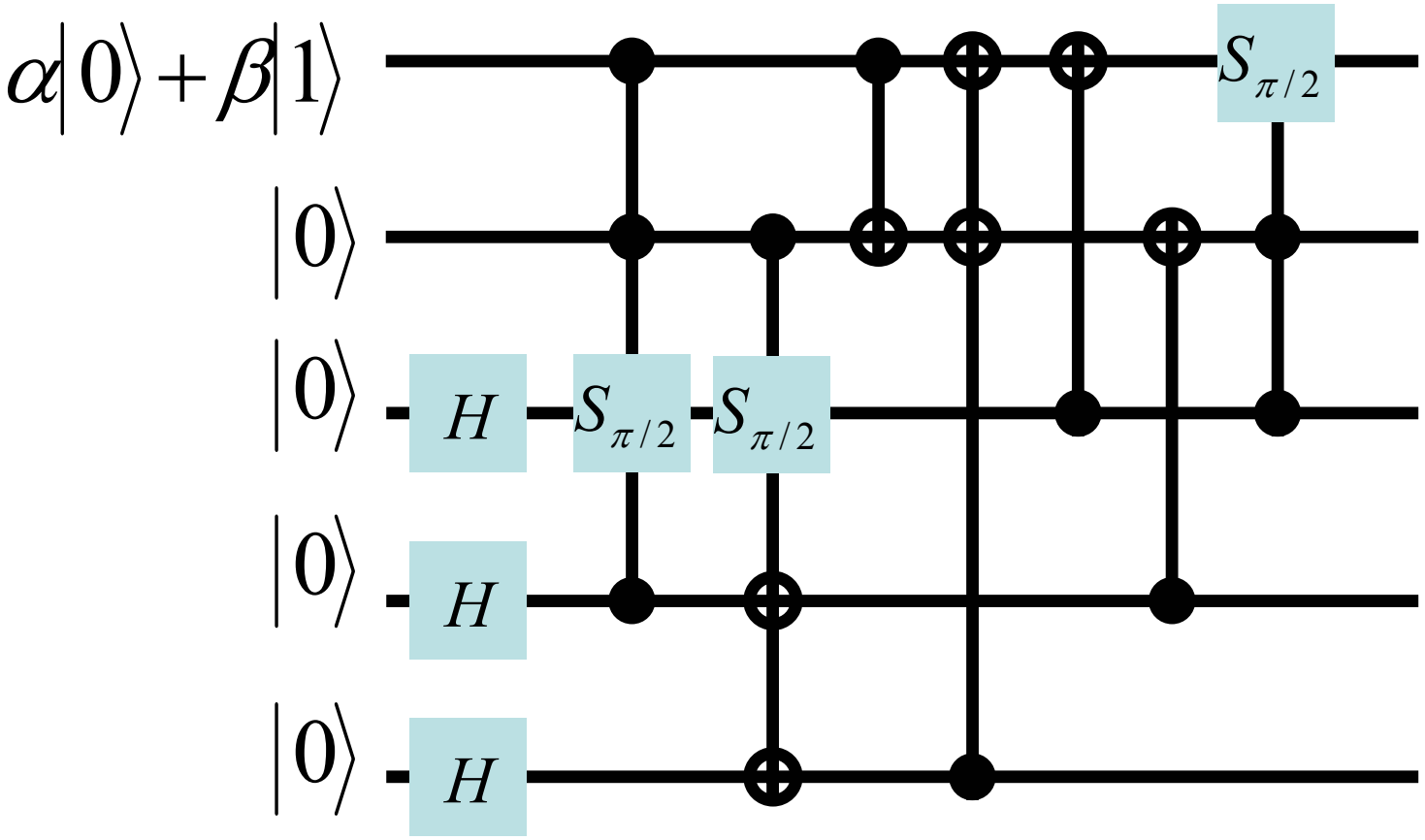
$$|\mathbf{0}\rangle = \frac{+|00000\rangle + |11100\rangle - |10011\rangle - |01111\rangle + |11010\rangle + |00110\rangle + |01001\rangle + |10101\rangle}{2\sqrt{2}}$$

$$|\mathbf{1}\rangle = \frac{+|11111\rangle - |00011\rangle + |01100\rangle - |10000\rangle - |00101\rangle + |11001\rangle + |10110\rangle - |01010\rangle}{2\sqrt{2}}$$

On peut vérifier que le codage de $\alpha|0\rangle + \beta|1\rangle$ sans erreur et chaque état obtenu en faisant une erreur de type X, Z ou XZ nous donne un état orthogonal. On peut donc distinguer ces états.

Ce code permet la correction d'une erreur et il est optimal. Il n'existe pas de code de taille 4 pour encoder un qubit qui tolère une erreur quelconque.

Codage et décodage de LMPZ



Codage et décodage de LMPZ

On utilise le circuit précédent pour encoder un qubit.

Le décodage peut se faire en inversant le circuit.

On inverse le circuit et on mesure comme syndrome les 4 qubits ancillaires.

Une fois cette information en main il est possible de récupérer le qubit original. Voici un tableau qui décrit l'état du premier qubit en fonction du syndrome obtenu en considérant qu'au plus un qubit a subit une erreur.

$\alpha\|0\rangle + \beta\|1\rangle$	0000
$-\alpha\|1\rangle + \beta\|0\rangle$	1011
$-\alpha\|0\rangle + \beta\|1\rangle$	1111
$\alpha\|0\rangle - \beta\|1\rangle$	1000 0101 0011 1010
$-\alpha\|0\rangle - \beta\|1\rangle$	1100 0001 0010 0100
$-\alpha\|1\rangle + \beta\|0\rangle$	0110 1110 1101 1001

Coder ou ne pas coder...

Est-ce que les codes sont vraiment utiles? ON peut corriger une erreur mais on utilise plusieurs qubits.

Supposont que pour un intervalle de temps donné la probabilité d'erreur est p. Si on utilise aucun codage la probabilité de n'avoir aucune erreur est donc $1-p$.

Si on utilise le code de Shor à 9 qubits cette probabilité est la somme des probabilités de n'avoir acucne erreur $(1-p)^9$ plus la probabilité de n'avoir qu'une erreur $9p(1-p)^8$.

La question maintenant est de savoir pour quel taux d'erreur il est préférable d'utiliser le code de Shor.

$$(1-p) < (1-p)^9 + 9p(1-p)^8$$

On obtient que lorsque $p < 0.032$ le codage est utile.

On peut faire le même calcul avec le code LMPZ a 5 qubit et on obtient que le codage est utile si $p < 0.13$.

Par exemple pour un taux d'erreur de 1% la probabilité de succès passe de 99% à 99.99902% avec le code LMPZ.

Codes concaténés

Peux t'ont faire mieux avec les outils que nous avons a notre disposition? Une idée simple consiste à coder récursivement. On peut coder une première fois un qubit puis coder de nouveau chaque qubit du mot de code et ainsi de suite.

En utilisant le code à 5 qubit LMPZ et en supposant que les erreurs sont uniformément distribuées on obtient une amélioration. Le seuil à partir du quel il est utile de coder augmente et la diminution de l'erreur est significative.

Une analyse complète vous sera demandée en devoir.

Attention, les codes concaténés sont bon si les erreurs sont uniformément distribué sur les qubit. Dans le pire cas le code de niveau 2 ne peut corriger 4 erreurs. Bien qu'en moyenne il peut corriger beaucoup plus.

Peut-on faire mieux dans le pire cas?

Code CSS

Les codes de Calderbank-Shor-Steane furent un progrès significatif en correction d'erreur quantique. Ils ont démontré une technique générale pour passer de bons codes classiques à de bons codes quantiques.

Supposons que nous ayons deux codes C_1 et C_2 tel que C_1 est un $[n, k_1, 2t+1]$, C_2 est une $[n, k_2, d]$ et $C_2^{\perp}$ est $[n, n-k_2, 2t+1]$ avec $C_2 \subset C_1$.

Nous allons construire un code quantique utilisant n qubit capable de coder $k_1 - k_2$ qubit et corriger t erreurs. Construisons le code $CSS(C_1, C_2)$.

Soit $x \in C_1$ alors on définit

$$|x + C_2\rangle = \frac{1}{\sqrt{2^{k_2}}} \sum_{y \in C_2} |x \oplus y\rangle$$

Si $x_1 \oplus x_2 \in C_2$ alors on peut vérifier que $|x_1 + C_2\rangle = |x_2 + C_2\rangle$ par contre si $x_1 \oplus x_2 \notin C_2$ alors $|x_1 + C_2\rangle$ et $|x_2 + C_2\rangle$ sont orthogonaux.

Les mots de code sont donc les mots de la forme $|x + C_2\rangle$ pour $x \in C_1$. Il y en a $\frac{|C_1|}{|C_2|} = 2^{k1-k2}$.

On peut corriger t erreur dans ce code quantique en utilisant les propriétés de correction d'erreurs des codes C_1 et $C_2^{\perp}$.

Supposons que les erreurs de bit soient représanté par e_1 et les erreurs de phase par le vecteur e_2. Dans les deux cas, on aura un 1 en position i si et seulement si il y a eu une erreur dans cette position. Avec un peu d'algèbre on obtient que l'état érroner est maintenant de la forme

$$\frac{1}{\sqrt{2^{k_2}}} \sum_{y \in C_2} (-1)^{(x \oplus y) \cdot e_2} |x \oplus y \oplus e_1\rangle$$

Clairement s'il n'y avait pas d'erreur de bit les états de la superposition devraient être dans l'état $|x \oplus y\rangle$, on peut donc utiliser les capacités correctrices du code C_1 pour détecter et corriger ces erreurs. Nous nous retrouverons dans l'état

$$\frac{1}{\sqrt{2^{k_2}}} \sum_{y \in C_2} (-1)^{(x \oplus y) \cdot e_2} |x \oplus y\rangle$$

Applicons maintenant H sur chaque qubit, on obtient

$$\frac{1}{\sqrt{2^{k_2} 2^n}} \sum_z \sum_{y \in C_2} (-1)^{(x \oplus y) \cdot (e_2 \oplus z)} |z\rangle$$

effectuons le changement de variable $z' = z + e_1$ on obtient

$$\frac{1}{\sqrt{2^{k_2} 2^n}} \sum_{z'} \sum_{y \in C_2} (-1)^{(x \oplus y) \cdot z'} |z' \oplus e_2\rangle$$

On peut montrer que si $z' \in C_2^{\perp}$ alors

$$\sum_{y \in C_2} (-1)^{y \cdot z'} = |C_2| = 2^{k_2}$$

et si $z' \notin C_2^{\perp}$

$$\sum_{y \in C_2} (-1)^{y \cdot z'} = 0$$

L'équation précédente peux donc se simplifier à

$$\frac{1}{\sqrt{2^{n-k_2}}} \sum_{z' \in C_2^{\perp}} (-1)^{(x \cdot z')} |z' \oplus e_2\rangle$$

Nous n'avons plus qu'a utiliser les capacités correctrice de $C_2^{\perp}$ pour corriger les erreurs e_2 on obtient

$$\frac{1}{\sqrt{2^{n-k_2}}} \sum_{z' \in C_2^{\perp}} (-1)^{(x \cdot z')} |z'\rangle$$

on applique de nouveaux H sur chaque qubit et on retrouve le mot de code

$$\frac{1}{\sqrt{2^{k_2}}} \sum_{y \in C_2} |x \oplus y\rangle = |x + C_2\rangle$$

Code CSS

En choisisant adéquatement les code C_1 et C_2 il a été possible d'obtenir des codes quantiques corrigant une erreur capable d'encoder directement plusieurs qubits. En particulier, on a obtenu un code codant 5 qubits dans 13, 6 qubits dans 14 , 7 qubits dans 17 et 9 qubit dans 20.

On a aussi obtenu le résultat général suivant qui est le pendant quantique de la borne de Gilbert-Varshamov.

Théorème
On peut sur un canal ayant une probabilité d'erreur p, en utilisant un codage en bloc suffisamment long, transmettre de façon fiable un qubit par la transmission en moyenne de $\frac{1}{1-2H(p)}$ qubits.

Calcul robuste

La correction d'erreur est suffisante pour la transmission d'information sur un canal imparfait.

Si on désire effectuer des calculs quantiques les choses se compliquent. Les erreurs peuvent se produire spontanément sur un qubit ou lors de l'application d'une porte logique. Si on doit décoder le qubit avant chaque porte on pers toute la sécurité de l'encodage.

La théorie du calcul quantique robuste solutionne ce problème. Malheureusement cette théorie nécessite des concepts en correction d'erreur hors des objectifs du cours. Nous allons voir quelques consepts élémentaires permettant tout au moins d'avoir une idée intuitive des techniques nécessaires.

Calcul robuste

Nous allons voir comment avec le code de Shor on peut implanter certaines portes de façon robuste.

La porte N.

L'aplication de $U_N = (Z \otimes I \otimes I \otimes)^{\otimes 3}$ sur le qubit encoder effectue N.

$$U_N|\mathbf{0}\rangle = U_N \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)^{\otimes 3} = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)^{\otimes 3} = |\mathbf{1}\rangle$$

$$U_N|\mathbf{1}\rangle = U_N \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)^{\otimes 3} = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)^{\otimes 3} = |\mathbf{0}\rangle$$

La porte Z.

L'aplication de $U_Z = (N \otimes N \otimes N \otimes \otimes I^{\otimes 6}$ sur le qubit encoder effectue Z.

$$U_Z|\mathbf{0}\rangle = U_N \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)^{\otimes 3} = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)^{\otimes 3} = |\mathbf{0}\rangle$$

$$U_Z|\mathbf{1}\rangle = U_N \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)^{\otimes 3} = -\frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)^{\otimes 3} = -|\mathbf{1}\rangle$$

Calcul robuste

Voyons maintenant comment implanter la porte à deux qubit C.

$U_C = (C_{[4,1]}C_{[5,2]}C_{[6,3]})^{\otimes 3}$

$$U_C|\mathbf{0}\rangle|\mathbf{0}\rangle = U_C\frac{1}{2\sqrt{2}}(|000\rangle+|111\rangle)^{\otimes 3}\otimes(|000\rangle+|111\rangle)^{\otimes 3} = \frac{1}{2\sqrt{2}}(|000\rangle+|111\rangle)^{\otimes 3}\otimes(|000\rangle+|111\rangle)^{\otimes 3} = |\mathbf{0}\rangle|\mathbf{0}\rangle$$

$$U_C|\mathbf{0}\rangle|\mathbf{1}\rangle = U_C\frac{1}{2\sqrt{2}}(|000\rangle+|111\rangle)^{\otimes 3}\otimes(|000\rangle-|111\rangle)^{\otimes 3} = \frac{1}{2\sqrt{2}}(|000\rangle+|111\rangle)^{\otimes 3}\otimes(|000\rangle-|111\rangle)^{\otimes 3} = |\mathbf{0}\rangle|\mathbf{1}\rangle$$

$$U_C|\mathbf{1}\rangle|\mathbf{0}\rangle = U_C\frac{1}{2\sqrt{2}}(|000\rangle-|111\rangle)^{\otimes 3}\otimes(|000\rangle+|111\rangle)^{\otimes 3} = \frac{1}{2\sqrt{2}}(|000\rangle-|111\rangle)^{\otimes 3}\otimes(|000\rangle-|111\rangle)^{\otimes 3} = |\mathbf{1}\rangle|\mathbf{1}\rangle$$

$$U_C|\mathbf{1}\rangle|\mathbf{1}\rangle = U_C\frac{1}{2\sqrt{2}}(|000\rangle-|111\rangle)^{\otimes 3}\otimes(|000\rangle-|111\rangle)^{\otimes 3} = \frac{1}{2\sqrt{2}}(|000\rangle-|111\rangle)^{\otimes 3}\otimes(|000\rangle+|111\rangle)^{\otimes 3} = |\mathbf{1}\rangle|\mathbf{0}\rangle$$

En général

L'implantation robuste des portes X,Z et C permettent de réaliser ces portes sans décoder le qubits. De plus si une erreur survient lors de l'application d'une des portes cette erreur n'affectera qu'un qubit et elle poura donc être corrigé.

Il est malheureusement impossible de réaliser de fa'con robuste toutes les portes à un qubits (il y en a un nombre infini).

Par contre il existe des ensembles finis de portes logiques qui sont universels dans le sens que même si il ne permette pas de faire exactement toute transformation unitaire il permettent d'aproximer avec une précision arbitraire ces transformations.

Il esiste des ensembles de portes logiques finis universelles pouvant être implantés de façon robuste.

De plus certaines techniques peuvent être utilisés pour encoder et corriger les qubits de façon robuste.

Le théorème seuil

Tout circuit contenant n portes logiques quantiques peut être simuler avec probabilité d'erreur au plus ϵ en ulisant des techniques de calculs tolérants aux erreurs utilisant

$$O(poly(\log(n/\epsilon)n)$$

portes logiques quantiques si le taux d'erreur $p \leq p_{inf}$.

Différentes analyses donnent des valeurs dirrérentes pour p_{inf} qui varie entre 10^{-4} et 10^{-6}.