Une introduction aux codes correcteurs quantiques

Jean-Pierre Tillich
INRIA Rocquencourt, équipe-projet SECRET

20 mars 2008

De quoi est-il question ici ?

- Code quantique : il est possible de corriger des erreurs même en présence de mesures qui détruisent l'état.
- Code quantique stabilisateur : espace continu, mais possibilité de corriger des erreurs de manière très semblable à un code correcteur d'erreurs linéaire standard.
- Code quantiques : possibilité de corriger l'erreur sans déterminer exactement l'erreur.

1. Introduction

- (Shor, 1994) : Un ordinateur quantique peut factoriser et trouver des logarithmes discrets de manière efficace $\Longrightarrow$ casse tous les systèmes de chiffrement à clé publique utilisés actuellement.
- Construction d'un tel ordinateur : besoin de traiter le problème de decohérence. Codes correcteurs quantiques : un moyen de protéger les qubits contre ce phénomène et d'effectuer des calculs tolérants aux fautes.
- Communications quantiques dans les protocoles quantiques d'échange de clé pourraient aussi bénéficier de CCQ ($\Longrightarrow$ augmenter les distances de communication).

Quelques notions quantiques

$$\mathcal{H} \stackrel{\text{def}}{=} \{\alpha\,|0\rangle + \beta\,|1\rangle \,|\alpha, \beta \in \mathbb{C}\} \text{ avec } |0\rangle \perp |1\rangle$$

$$\mathcal{H}^{\otimes n} \stackrel{\text{def}}{=} \underbrace{\mathcal{H} \otimes \mathcal{H} \otimes \cdots \otimes \mathcal{H}}_{n} = \{ \sum_{x \in \{0,1\}^n} \alpha_x \,|x\rangle \,|\alpha_x \in \mathbb{C}\}$$

Un qubit :

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \in \mathcal{H}, \text{ avec } |\alpha|^2 + |\beta|^2 = 1.$$

Un registre de n qubits :

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x \,|x\rangle \in \mathcal{H}^{\otimes n} \text{ avec } \sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1.$$

Evolutions quantiques possibles

- transformation unitaire U,

$$|\psi\rangle \in \mathcal{H}^{\otimes n} \rightsquigarrow U|\psi\rangle \in \mathcal{H}^{\otimes n}$$

- Mesure associée à une décomposition $\mathcal{H}^{\otimes n} = E_1 \overset{\perp}{\oplus} E_2 \overset{\perp}{\oplus} \dots \overset{\perp}{\oplus} E_t$:

$$|\psi\rangle \in \mathcal{H}^{\otimes n} \rightsquigarrow \frac{1}{\| P_i |\psi\rangle \|} P_i |\psi\rangle \quad \text{avec probabilité } \| P_i |\psi\rangle \|^2.$$

où P_i est la projection orthogonale sur le sous-espace E_i et le résultat de la mesure est “on est dans le sous-espace i ”

Exemple de mesure

Mesure du 2ème qubit d'un registre quantique $|\psi\rangle = \alpha_{00}|0\rangle \otimes |0\rangle + \alpha_{01}|0\rangle \otimes |1\rangle + \alpha_{10}|1\rangle \otimes |0\rangle + \alpha_{11}|1\rangle \otimes |1\rangle$ dans $\mathcal{H}^{\otimes 2} = E_0 \overset{\perp}{\oplus} E_1$ où

$$
\begin{aligned}
E_0 &= \{\alpha|0\rangle \otimes |0\rangle + \beta|1\rangle \otimes |0\rangle \,|\alpha, \beta \in \mathbb{C}\} \\
E_1 &= \{\alpha|0\rangle \otimes |1\rangle + \beta|1\rangle \otimes |1\rangle \,|\alpha, \beta \in \mathbb{C}\}
\end{aligned}
$$

$$
\begin{aligned}
|\psi\rangle &\rightsquigarrow \frac{\alpha_{00}|0\rangle \otimes |0\rangle + \alpha_{10}|1\rangle \otimes |0\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{10}|^2}} \text{ avec prob. } |\alpha_{00}|^2 + |\alpha_{10}|^2 \\
|\psi\rangle &\rightsquigarrow \frac{\alpha_{01}|0\rangle \otimes |1\rangle + \alpha_{11}|1\rangle \otimes |1\rangle}{\sqrt{|\alpha_{01}|^2 + |\alpha_{11}|^2}} \text{ avec prob. } |\alpha_{01}|^2 + |\alpha_{11}|^2
\end{aligned}
$$

Modèle d'erreur

Beaucoup plus riche que dans le monde classique :

inversion de qubit (X)

$$\begin{aligned} |0\rangle &\rightarrow |1\rangle \\ |1\rangle &\rightarrow |0\rangle \end{aligned}$$

erreur de phase (Z)

$$\begin{aligned} |0\rangle &\rightarrow |0\rangle \\ |1\rangle &\rightarrow -|1\rangle \end{aligned}$$

les deux ! (Y)

$$
\begin{aligned}
|0\rangle &\rightarrow -i\,|1\rangle \\
|1\rangle &\rightarrow i\,|0\rangle
\end{aligned}
$$

$$
\begin{aligned}
XZ &= -ZX = -iY \\
XY &= -YX = iZ \\
YZ &= -ZY = -\,iX
\end{aligned}
$$

Le groupe de Pauli

Le groupe de Pauli sur 1 qubit $\mathcal{G}_1$:

$$\{\pm I, \pm X, \pm Y, \pm Z, \pm iI, \pm iX, \pm iY, \pm iZ\}.$$

Les éléments de ce groupe commutent ou anti-commutent.

Le groupe $\mathcal{G}_n$

Le groupe de Pauli sur n qubits $\mathcal{G}_n$:

$$\begin{aligned} \mathcal{G}_n &= \{E_1 \otimes E_2 \otimes \cdots \otimes E_n | E_i \in \mathcal{G}_1\} \\ &\equiv \{I, X, Y, Z\}^n \times \{\pm 1, \pm i\} \end{aligned}$$

- Les éléments de $\mathcal{G}_n$ commutent ou anti-commutent

Un critère simple : $E_1 \ldots E_n$ et $E'_1 \ldots E'_n$ commutent si et ssi $\#\{i : E_i E'_i = -E'_i E_i\}$ est pair.

Exemple : XXI et XYX anti-commutent et XXI et ZZZ commutent.

Un exemple

$$
\begin{aligned}
|011\rangle &\stackrel{\text{def}}{=} |0\rangle \otimes |1\rangle \otimes |1\rangle \\
X \otimes I \otimes Z\,|011\rangle &= (X \otimes I \otimes Z)(|0\rangle \otimes |1\rangle \otimes |1\rangle) \\
&= (X\,|0\rangle) \otimes (I\,|1\rangle) \otimes (Z\,|1\rangle) \\
&= -\,|1\rangle \otimes |1\rangle \otimes |1\rangle \\
&= -\,|111\rangle
\end{aligned}
$$

Le canal de dépolarisation

Sur un canal de dépolarisation de prob. p, tous les qubits subissent la transformation suivante indépendamment les uns des autres

$$
\begin{aligned}
|\psi\rangle &\rightsquigarrow |\psi\rangle \text{ avec probabilité } 1-p \\
|\psi\rangle &\rightsquigarrow X|\psi\rangle \text{ avec probabilité } \frac{p}{3} \\
|\psi\rangle &\rightsquigarrow Y|\psi\rangle \text{ avec probabilité } \frac{p}{3} \\
|\psi\rangle &\rightsquigarrow Z|\psi\rangle \text{ avec probabilité } \frac{p}{3}
\end{aligned}
$$

Exemple : Pour un registre de 5 qubits

$$\mathbf{Prob}(E = I \otimes X \otimes I \otimes I \otimes Z) = (1-p)^3 \left(\frac{p}{3}\right)^2$$

2. Codes quantiques

1. Non seulement $|0\rangle$ et $|1\rangle$ doivent être protégés, mais aussi toute superposition $\alpha|0\rangle + \beta|1\rangle$
2. Copier un qubit est impossible ("No-cloning theorem") . Pas d' U unitaire t.q. pour tout qubit $|\psi\rangle$ on a :

$$U : |\psi\rangle \otimes |0\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$$

3. La mesure peut modifier le qubit...

Codes quantiques

Un code quantique C de longueur n est un sous-espace de $\mathcal{H}^{\otimes n}$. Si de dimension 2^k, il permet d'encoder l'état d'un registre de k qubits.

Le rendement d'un code est défini comme $\frac{k}{n}$ dans ce cas et

$$\frac{\log_2(\dim C)}{n}$$

en général.

Codes stabilisateurs quantiques

- Ont beaucoup de points communs avec des codes linéaires classiques.
- Utilisent les propriétés du groupe de Pauli.

Définition

- Soit $\mathcal{S}$ un sous-groupe abélien de $\mathcal{G}_n$ où tous les éléments sont d'ordre au plus 2 et t.q. $-1 \notin \mathcal{S}$. Un tel sous-groupe est dit admissible.
- Un code stabilisateur C associé à un sous-groupe admisible $\mathcal{S}$ est un sous-espace de $\mathcal{H}^{\otimes n}$ défini par

$$C = \{|\psi\rangle \in \mathcal{H}^{\otimes n} | \forall M \in \mathcal{S}, M\,|\psi\rangle = |\psi\rangle\}$$

La propriété fondamentale

Proposition 1. *Si* $\mathcal{S}$ *est généré par* $n - k$ *générateurs indépendants, alors la dimension du code associé est* 2^k*.*

Syndrome

Pour $E, F \in \mathcal{G}_n$ nous notons

$$E \star F \stackrel{\text{def}}{=} 0 \text{ si } E \text{et } F \text{ commutent et 1 sinon.}$$

Pour un choix de $M_1, \ldots, M_{n-k}$ générateurs indépendants de $\mathcal{S}$, le syndrome associé à $E \in \mathcal{G}_n$ est

$$\sigma(E) \stackrel{\text{def}}{=} (M_i \star E)_{1 \leq i \leq n-k}$$

Syndrome (II)

Soit $s = (s_i)_{1 \leq i \leq n-k} \in \{0,1\}^{n-k}$ et C le code stabilisateur associé à $\mathcal{S} =< M_1, \ldots, M_{n-k} >$. On pose

$$C(s) \stackrel{\text{def}}{=} \{|\psi\rangle : M_i |\psi\rangle = (-1)^{s_i} |\psi\rangle\}.$$

Noter que pour $E \in \mathcal{G}_n$ de syndrome s et $|\psi\rangle \in C$ on a

$$M_i E |\psi\rangle = (-1)^{s_i} E M_i |\psi\rangle = (-1)^{s_i} E |\psi\rangle \Longrightarrow E |\psi\rangle \in C(s).$$

On peut aussi noter que

$$\mathcal{H}^{\otimes n} = \overset{\perp}{\bigoplus}_{s \in \{0,1\}^{n-k}} C(s)$$

$\Longrightarrow$ mesure associée

Un premier exemple

$$
\begin{aligned}
\mathcal{S} &= \; < ZZI, IZZ > \\
H &= \begin{pmatrix} Z & Z & I \\ I & Z & Z \end{pmatrix} \\
C &= \mathsf{Vect}(|000\rangle, |111\rangle) \\
C(01) &= \mathsf{Vect}(|001\rangle, |110\rangle) \\
C(10) &= \mathsf{Vect}(|100\rangle, |011\rangle) \\
C(11) &= \mathsf{Vect}(|010\rangle, |101\rangle)
\end{aligned}
$$

Décodage

$$
\begin{array}{cl}
|\psi\rangle \in C & \\
\Downarrow & \text{erreur } E \in \mathcal{G}_n \\
E\,|\psi\rangle \in C(\sigma(E)) & \\
\Downarrow & \text{mesure} \\
E\,|\psi\rangle & \\
\Downarrow & \text{estimation de l'erreur} \\
E_{\text{estim.}}^{-1} E\,|\psi\rangle &
\end{array}
$$

Un premier exemple(II)

$$
\begin{array}{cl}
|000\rangle \in C & \\
\Downarrow & \text{erreur } IXI \\
|010\rangle \in C(11) & \\
\Downarrow & \text{mesure : on est dans } C(11) \\
|010\rangle & \\
\Downarrow & \text{estimation de l'erreur} \\
IXI\,|010\rangle = |000\rangle &
\end{array}
$$

Un premier exemple(III)

$$|000\rangle + |111\rangle \in C$$

$\Downarrow$ erreur IZI

$$|000\rangle - |111\rangle \in C(00)$$

$\Downarrow$ mesure : on est dans $C(00)$

$$|000\rangle - |111\rangle$$

$\Downarrow$ estimation de l'erreur

$$|000\rangle - |111\rangle$$

Un deuxième exemple

$$H = \begin{pmatrix} Z & Z & I & I & I & I & I & I & I \\ I & Z & Z & I & I & I & I & I & I \\ I & I & I & Z & Z & I & I & I & I \\ I & I & I & I & Z & Z & I & I & I \\ I & I & I & I & I & I & Z & Z & I \\ I & I & I & I & I & I & I & Z & Z \\ X & X & X & X & X & X & I & I & I \\ I & I & I & X & X & X & X & X & X \end{pmatrix}$$

erreur $ZIIIIIIII \Longrightarrow$ syndrome 00000010

erreur $IZIIIIII \Longrightarrow$ syndrome 00000010

Analogies

codes linéaires	codes stabilisateurs quantiques
k bits encodés avec n bits sous-espace de dim. k	k qubits encodés avec n qubits sous-espace de dim. 2^k
matrice de parité H $n-k$ lignes, n colonnes syndrome $\in \{0,1\}^{n-k}$	générateurs de $\mathcal{S}$ $n-k$ générateurs de $\mathcal{G}_n$ qui commutent syndrome $\in \{0,1\}^{n-k}$

erreurs bénignes et problématiques

- Soit C un code stabilisateur associé à $\mathcal{S} =< S_1, \ldots, S_{n-k} >$. Deux types d'erreur ont syndrome 0
  – celles qui sont bénignes, elles appartiennent à $\mathcal{S}$ et sont de type **B** (comme **B**énignes) . Une telle erreur est sans conséquence : pour une telle erreur erreur E on a pour tout $|\psi\rangle \in C$: $E|\psi\rangle = |\psi\rangle$.
  – celles qui sont problématiques : elles n'appartiennent pas à $\mathcal{S}$. Elles sont dites de type **P** (comme **P**roblématiques). Pour une telle erreur E, il existe $|\psi\rangle \in C$ t.q. $E|\psi\rangle \neq |\psi\rangle$.

Distance minimale et capacité de correction

- Décodage réussi : $E_{\text{estimé}}^{-1} E_{\text{canal}}$ de type **B**
- Distance minimale

$$d \stackrel{\text{def}}{=} \min\{|E| : E \text{ de type } \mathbf{P}\}$$

- Capacité de correction

$$\left\lfloor \frac{d-1}{2} \right\rfloor$$

Le premier exemple revisité

$$\begin{array}{rcl} \mathcal{S} & = & < ZZI, IZZ > \\ H & = & \begin{pmatrix} Z & Z & I \\ I & Z & Z \end{pmatrix} \\ C & = & \text{Vect}(|000\rangle, |111\rangle) \end{array}$$

Erreurs bénignes : III, ZZI, IZZ, ZIZ.

Erreurs problématiques (p.ex.) ZII, ZZZ.

Distance minimale : 1.

3. codes LDPC quantiques

Pour un code stabilisateur défini par $\mathcal{S} =< M_1, M_2, \ldots, M_{n-k} >$, une "matrice de parité" associée est une matrice $(n-k) \times n$ dont les lignes sont données par les M_i.

code LDPC quantique : a une matrice de parité creuse.

Le problème : construire un code Q-LDPC de bonne distance minimale

Fait 1. *Si une colonne ne contient pas plus d'un type d'élément* $\neq I$ *alors il y a une erreur de sydrome* 0 *et de poids* 1*.*

Exemple :

$$\begin{pmatrix} X & X & X & X \\ I & Z & Z & I \\ X & I & Z & Z \end{pmatrix}$$

$XIII$ est une erreur de ce type.

Les cycles de taille 4 sont inévitables

Deux lignes de la matrice de parité s' intersectent en une colonne i en A et B, si $A, B \in \{X, Y, Z\}$ si la première ligne a A en colonne i et la seconde à B.

Distance minimale > 1

$$\Downarrow$$

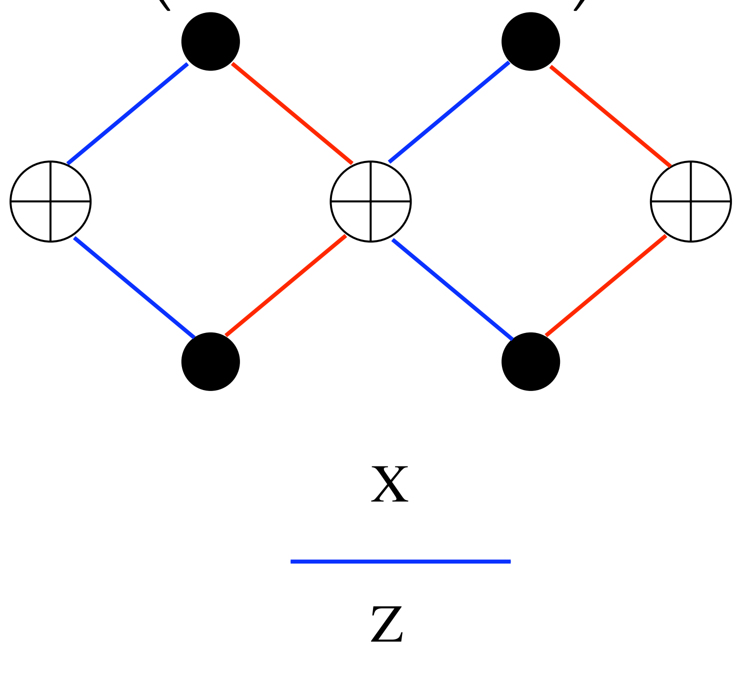
pour toute colonne i il y a une paire de lignes s'intersectant en i avec deux entrées différentes.

$$\Downarrow$$

Ces lignes doivent s'intersecter en une autre colonne pour commuter.

Un exemple de graphe de Tanner

$$\begin{pmatrix} X & X & I & I \\ I & I & Z & Z \\ Z & Z & X & X \end{pmatrix}$$



Problèmes ouverts

- Trouver une famille infinie de codes LDPC quantiques de rendement non nul et de distance minimale linéaire en la longueur.
- Trouver une famille infinie de codes LDPC quantiques de rendement non nul et de distance minimale non bornée.

4. La capacité $\mathcal{Q}$ du canal de dépolarisation

Inconnue...

Proposition 2.

$$\mathcal{Q} \geq 1 - h(p) - p \log_2 3$$

$$\begin{aligned}
\text{Nombre de syndromes} \neq \quad &\geq \quad \text{taille de l'ensemble typique des erreurs} \\
2^{n-k} \quad &\geq \quad 3^{np}\binom{n}{np} \\
1 - \frac{k}{n} \quad &\geq \quad p \log_2 3 + h(p)
\end{aligned}$$

Corollaire 1.

$$\mathcal{Q} > 0 \ \ \textit{pour } p \leq 0.18928$$

Proposition 3.

$$\mathcal{Q} > 0 \ \ \textit{pour } p \leq 0.1905$$

Proposition 4.

$$\mathcal{Q} = 0 \ \ \textit{pour } p \geq \frac{1}{4}$$

Une explication

Des erreurs de même syndrome peuvent être corrigées en même temps si elles appartiennent toutes à un même coset de $\mathcal{S}$.

$$\Longrightarrow$$

la taille de l'ensemble des erreurs typiques peut être beaucoup plus grande que le nombre de syndromes.

Le résultat de Shor

$$H = \begin{pmatrix} Z & Z & I \\ I & Z & Z \end{pmatrix}$$

$$\mathcal{S} = \{III, ZZI, IZZ, ZIZ\}.$$

Erreurs de syndrome $S=(1,0)$

$A_1=(XII).\mathcal{S}$	$A_2=(YII).\mathcal{S}$	$A_3=(IYY).\mathcal{S}$	$A_4=(IYX).\mathcal{S}$
XII	YII	IYY	IYX
YZI	XZI	IXY	ZXX
XZZ	YZZ	IXX	IXY
YIZ	XIZ	ZYX	ZYY

$$p_i(s) \stackrel{\text{def}}{=} \mathbf{Prob}(E \in A_i | S = s)$$

Le résultat de Shor

$$\begin{aligned}\bar{E} &= i \text{ si et ssi } E \in A_i \\ H_2(\bar{E}|S) &= -\sum_s \sum_{i=1}^{4} p_i(s) \log_2 p_i(s) \mathbf{Prob}(S = s)\end{aligned}$$

Théorème 1. *Si* $H_2(\bar{E}|S) < 1$ *alors* $\mathcal{Q} > 0$.