

Informatique quantique IFT6155

Distillation d'intrication

Motivation

L'intrication est une ressource importante. Elle permet la téléportation. Le codage dense. la résolution de problèmes en complexité de la communication. La communication secrète de bit classique et de bit quantique.

En réalité si Alice et Bob échangent des états de Bell il y aura des erreurs. La question qui occupe cette section est la suivante. Comment peut-on extraire des états de Bell presque parfait à partir d'état de Bell imparfait?

Fidélité

Définition $F(\rho, |\psi\rangle) = \langle \psi | \rho | \psi \rangle$

Théorème:

La fidélité $F(\rho, |\psi\rangle)$ est la probabilité d'obtenir $|\psi\rangle$ si on mesure dans une base contenant $|\psi\rangle$. Soit U tel que $U|0\rangle = |\psi\rangle$ alors

$$\langle 0 | U |\psi\rangle \langle \psi | U^\dagger | 0 \rangle = \langle \psi | \psi \rangle \langle \psi | \psi \rangle = 1$$

$$\langle 0 | U \rho U^\dagger | 0 \rangle = \langle \psi | \rho | \psi \rangle = F(\rho, |\psi\rangle)$$

Fidélité

Faits

$$0 \leq F(\rho, |\psi\rangle) \leq 1$$

Si $\rho = |\psi\rangle\langle\psi|$ alors $F(\rho, |\psi\rangle) = \langle\psi|\psi\rangle\langle\psi|\psi\rangle = 1$.

Si $\rho = |\phi\rangle\langle\phi|$ alors $F(\rho, |\psi\rangle) = \langle\psi|\phi\rangle\langle\phi|\psi\rangle = |\langle\psi|\phi\rangle|^2$ et en particulier si $|\psi\rangle$ et $|\phi\rangle$ sont orthogonaux alors $F(\rho, |\psi\rangle) = 0$.

SI $|\psi\rangle$ et $|\phi\rangle$ sont orthogonaux et $\rho = p|\psi\rangle\langle\psi| + (1-p)|\phi\rangle\langle\phi|$ alors $F(\rho, |\psi\rangle) = p$.

$$F\left(\frac{1}{2^n}I_{2^n}, |\psi\rangle\right) = \frac{1}{2^n}.$$

Si $F(\rho_1, |\psi\rangle) = a$ et $F(\rho_2, |\psi\rangle) = b$ alors $F(p\rho_1 + (1-p)\rho_2, |\psi\rangle) = pa + (1-p)b$.

Fidélité

Soit

$$E(\theta) = R_y(2\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

Si on applique $R_y(\theta)$ à l'état $|0\rangle$ on obtient

$$|\psi_\theta\rangle = \cos(\theta)|0\rangle + \sin(\theta)|1\rangle$$

et donc

$$F(|\psi_\theta\rangle \langle\psi_\theta|, |0\rangle) = \cos(\theta)^2.$$

Si θ est très petit la fidélité est proche de 1. Par exemple avec $\theta = 0.1$ on obtient une fidélité de 0.99.

Si on applique $E(\theta)^{\otimes n}$ à l'état $|0\dots 0\rangle$ on obtient

$$|\psi_\theta\rangle = \sum_{i=0}^{2^n-1} \cos(\theta)^{n-W(i)} \sin(\theta)^{W(i)} |i\rangle$$

et donc

$$F(|\psi_\theta\rangle \langle\psi_\theta|, |0\rangle) = \cos(\theta)^{2n}.$$

Même si θ est très petit la fidélité se détériore rapidement quand n grandit. Par exemple avec $\theta = 0.1$ et $n = 200$ on obtient une fidélité de 0.13.

Fidélité

$$|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad |\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\varphi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Définition

On définit l'état de Werner de paramètre f par

$$|\rho_f\rangle = f |\psi^-\rangle \langle\psi^-| + \frac{1-f}{3} (|\psi^+\rangle \langle\psi^+| + |\varphi^+\rangle \langle\varphi^+| + |\varphi^-\rangle \langle\varphi^-|).$$

Clairement $F(\rho_f, |\psi^-\rangle) = f$.

Théorème

Si Alice et Bob partagent un état à deux qubits ρ tel que $F(\rho, |\psi^-\rangle) = f$ alors ρ est localement équivalent à ρ_f .

Par localement on entend qu'Alice et Bob peuvent communiquer classiquement et effectuer des opérations unitaires locales sur leurs qubits. Ils ne peuvent pas échanger de l'information quantique ce qui rendrait le théorème totalement trivial. Nous appellerons cette transformation la Wernerisation d'un état ρ .

Fidélité

Voici une liste de 12 transformations unitaires

$$w_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad w_2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad w_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad w_4 = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

$$w_5 = \frac{1}{2} \begin{pmatrix} 1+i & -1+i \\ 1+i & 1-i \end{pmatrix} \quad w_6 = \frac{1}{2} \begin{pmatrix} 1-i & -1-i \\ 1-i & 1+i \end{pmatrix}$$

$$w_7 = \frac{1}{2} \begin{pmatrix} 1-i & 1+i \\ -1+i & 1+i \end{pmatrix} \quad w_8 = \frac{1}{2} \begin{pmatrix} 1-i & -1+i \\ 1+i & 1+i \end{pmatrix}$$

$$w_9 = \frac{1}{2} \begin{pmatrix} -1+i & -1+i \\ 1+i & -1-i \end{pmatrix} \quad w_{10} = \frac{1}{2} \begin{pmatrix} -1-i & -1-i \\ 1-i & -1+i \end{pmatrix}$$

$$w_{11} = \frac{1}{2} \begin{pmatrix} -1-i & 1+i \\ -1+i & -1+i \end{pmatrix} \quad w_{12} = \frac{1}{2} \begin{pmatrix} -1-i & -1+i \\ 1+i & -1+i \end{pmatrix}$$

Par de longs et fastidieux calculs, on obtient que si $F(\rho, |\psi^-\rangle) = f$ alors

$$\sum_{i=1}^{12} \frac{1}{12} (w_i \otimes w_i) \rho (w_i \otimes w_i)^\dagger = f |\psi^-\rangle \langle \psi^-| + \frac{1-f}{3} (|\psi^+\rangle \langle \psi^+| + |\varphi^+\rangle \langle \varphi^+| + |\varphi^-\rangle \langle \varphi^-|) = |w_f\rangle$$

Purification

La procédure de purification fonctionne de la façon suivante.

On choisit deux paires ayant fidélité f .

Alice applique $Y = XZ$ sur chaque qubit.

Alice et Bob applique C sur les deux qubit.

Alice et Bob mesurent le qubit cible.

Si les résultats sont identiques alors la paires restante est conservé sinon le protocole a échoué.

Alice applique Y sur la paire restante.

Alice et Bob effectuent une Wernerisation de la paire restante.

Purification

Théorème

La procédure de purification appliquée sur deux paires de fidélité $f > 1/2$ réussit avec probabilité au moins $1/4$ dans le quel cas la fidélité de la pair restante est

$$f' = \frac{f^2 + (1/9)(1-f)^2}{f^2 + (2/3)f(1-f) + (5/9)(1-f)^2} > f.$$

Preuve

Nous avons que

$$(Y \otimes I)|\psi^-\rangle = |\varphi^+\rangle \quad (Y \otimes I)|\varphi^+\rangle = |\psi^-\rangle \quad (Y \otimes I)|\psi^+\rangle = |\varphi^-\rangle \quad (Y \otimes I)|\varphi^-\rangle = |\psi^+\rangle$$

Après l'application de Y par Alice les deux paires sont dans l'état

$$f |\varphi^+\rangle \langle \varphi^+| + \frac{1-f}{3} (|\psi^+\rangle \langle \psi^+| + |\psi^-\rangle \langle \psi^-| + |\varphi^-\rangle \langle \varphi^-|)$$

On peut donc voir les deux paires comme un mélange des 16 possibilités avec les probabilités correspondantes.

Purification

Par exemple avec probabilité f^2 Alice et Bob partagent

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)$$

Notez que la première paire est dans l'état recherché. Après l'application de C par Alice et Bob (i.e. $C_{[1,3]} \otimes c_{[2,4]}$) on obtient l'état

$$\frac{1}{2}(|0000\rangle + |0011\rangle + |1111\rangle + |1100\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Les qubits 2 et 4 ne sont pas intriqué avec les deux autres on peut donc les mesurer sans affecter le qubit 1 et 3, il y a deux possibilités: Alice et Bob observent $|00\rangle$ ou $|11\rangle$ avec probabilité égale. Dans les deux cas, ils gardent la paire restante qui est dans l'état $|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ et c'est exactement ce que l'on désire.

Purification

Avec probabilité $\frac{(1-f)f}{3}$ Alice et Bob partagent

$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{2}(|0100\rangle + |0111\rangle + |1000\rangle + |1011\rangle)$$

Notez que la première paire n'est pas dans l'état cherché. Après l'application de C par Alice et Bob (i.e. $C_{[1,3]} \otimes c_{[2,4]}$) on obtient l'état

$$\frac{1}{2}(|0101\rangle + |0110\rangle + |1010\rangle + |1001\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

Le qubit 2 et 4 ne sont pas intriqués avec les deux autres on peut donc les mesurer sans affecter le qubit 1 et 3, il y a deux possibilités: Alice et Bob observent $|01\rangle$ ou $|10\rangle$ avec probabilité égale. Dans les deux cas il rejette la paire ce qui est une bonne décision.

Purification

Avec probabilité $\frac{f(1-f)}{3}$ Alice et Bob partagent

$$\frac{1}{\sqrt{2}}(|00\rangle + |00\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{2}(|0001\rangle + |0010\rangle + |1101\rangle + |1110\rangle)$$

Notez que la première paire est dans l'état recherché. Après l'application de C par Alice et Bob (i.e. $C_{[1,3]} \otimes c_{[2,4]}$) on obtient l'état

$$\frac{1}{2}(|0001\rangle + |0010\rangle + |1110\rangle + |1101\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

Les qubits 2 et 4 ne sont pas intriqués avec les deux autres on peut donc les mesurer sans affecter le qubit 1 et 3, il y a deux possibilités: Alice et Bob observent $|01\rangle$ ou $|10\rangle$ avec probabilité égale. Dans les deux cas il rejette la paire ce qui est une mauvaise décision.

Purification

Avec probabilité $\frac{(1-f)^2}{9}$ Alice et Bob partagent

$$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{2}(|0000\rangle - |0011\rangle - |1100\rangle + |1111\rangle)$$

Notez que la première paire n'est pas dans l'état recherché. Après l'application de C par Alice et Bob (i.e. $C_{[1,3]} \otimes c_{[2,4]}$) on obtient l'état

$$\frac{1}{2}(|0000\rangle - |0011\rangle - |1111\rangle + |1100\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Les qubits 2 et 4 ne sont pas intriqués avec les deux autres on peut donc les mesurer sans affecter le qubit 1 et 3, il y a deux possibilités: Alice et Bob observent $|00\rangle$ ou $|11\rangle$ avec probabilité égale. Dans les deux cas ils gardent la paire ce qui est une bonne décision.

Purification

Voici un tableau des différentes possibilités. Les lignes du tableau correspondent à la première paire et les colonnes à la deuxième paire. Dans une position du tableau on trouve l'état restant si on le garde.

	$ \varphi^+\rangle$	$ \psi^+\rangle$	$ \varphi^-\rangle$	$ \psi^-\rangle$
$ \varphi^+\rangle$	$ \varphi^+\rangle$	\neq	$ \varphi^-\rangle$	\neq
$ \psi^+\rangle$	\neq	$ \psi^+\rangle$	\neq	$ \psi^-\rangle$
$ \varphi^-\rangle$	$ \varphi^-\rangle$	\neq	$ \varphi^+\rangle$	\neq
$ \psi^-\rangle$	\neq	$ \psi^-\rangle$	\neq	$ \psi^+\rangle$

En combinant les différentes probabilités on obtient que la probabilité de garder la paire est

$$f^2 + 2f \frac{(1-f)}{3} + 5 \left(\frac{1-f}{3} \right)^2 \geq \frac{5}{9}$$

quand $f \geq 1/2$ et la probabilité associée à $|\varphi^+\rangle$ est de

$$\frac{f^2 + \left(\frac{1-f}{3} \right)^2}{f^2 + 2f \frac{(1-f)}{3} + 5 \left(\frac{1-f}{3} \right)^2} \geq f$$

quand $f > 1/2$.

Alice applique Y , Alice et Bob Wernerise et ils recommence...