

Codificação densa e compartilhamento quântico de segredos

1

- Vemos 2 aplicações de matrizes-densidade reduzida em informação quântica:
 - codificação quântica densa ["quantum dense coding"]
 - compartilhamento q. de segredos ["quantum secret sharing"]
- Considere o estado emaranhado $|B_{00}\rangle = \frac{1}{\sqrt{2}} (|100\rangle_{AB} + |111\rangle_{AB})$ de 2 qubits. O 1º está com Alice (A), e o 2º com Bob (B).
- Calculando o $\text{tr}_B(\rho_{AB}) = \rho_A$, onde $\rho_{AB} = |B_{00}\rangle\langle B_{00}|$, achamos que $\rho_A^{(00)} = \frac{1}{2}$. Além disso, $\rho_B^{(00)} = \text{tr}_A(\rho_{AB}) = \frac{1}{2}$ também. O estado global é puro ("bem definido") mas os estados locais dos qubits de A e B são maximamente mistos (mistura estatística cl. menos informação possível).
- Fazendo o mesmo pl. $|B_{01}\rangle = \frac{1}{\sqrt{2}} [|10\rangle + |01\rangle]$, também encontramos $\rho_A^{(01)} = \rho_B^{(01)} = \frac{1}{2}$.
- $\Rightarrow$ Localmente, A e B não conseguem distinguir $|B_{00}\rangle$ de $|B_{01}\rangle$. Mas como $\langle B_{00} | B_{01} \rangle = 0$, existem observáveis (que necessitam de interac. entre qubits A e B para sua implementação) que conseguem distinguir $|B_{00}\rangle$ de $|B_{01}\rangle$ perfeitamente. Por exemplo: $\hat{O} = \sigma_{00} |B_{00}\rangle\langle B_{00}| + \sigma_{01} |B_{01}\rangle\langle B_{01}|$

COMPARTILHAMENTO QUÂNTICO DE SEGREDO

- A e B compartilham $|B_{00}\rangle$ ou $|B_{01}\rangle$, codificando 1 bit (2 escolhas). O segredo está perfeitamente seguro se as partes não colaborarem; para descobrir o bit secreto, A e B precisam tomar os 2 qubits juntos, ou colaborar um com o outro.

Existem esquemas + sofisticados com + partes, e exigindo colaborações de formas diferentes do 1º.

Codificação densa

- Outros 2 estados de 2 qbits têm propriedades parecidas com $|B_{00}\rangle$ e $|B_{01}\rangle$:

$$|B_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad \text{e} \quad |B_{11}\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$$

- $\{|B_{00}\rangle, |B_{01}\rangle, |B_{10}\rangle, |B_{11}\rangle\}$ formam a base de Bell. São ortogonais entre si, e para todos eles vale $P_A = P_B = \frac{11}{2}$.

- Sejam X, Z as matrizes de Pauli. São operadores unitários ^{de 1 qbit} $\Rightarrow$ representam uma dinâmica local possível no qbit A (ou B). Verifique que vale:

$$Z_A \otimes I_B |B_{00}\rangle = |B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$X_A \otimes I_B |B_{00}\rangle = |B_{01}\rangle$$

$$(Z_A \otimes I_B)(X_A \otimes I_B) |B_{00}\rangle = |B_{11}\rangle$$

$\Rightarrow$ ou seja, localmente Alice consegue converter $|B_{ij}\rangle$ uns nos outros, é verdade.

Codificação densa

- Alice prepara $|B_{00}\rangle$, manda qbit B para Bob.
 - Agora Alice recebe a tarefa de mandar 2 bits p/ Bob, usando somente a comunicação de 1 qbit.
 - Ela codifica uma das 4 possibilidades no estado de Bell, localmente, como mostrado acima.
 - Manda seu qbit p/ Bob, que discrimina a base de Bell e lê os 2 bits.
- $\Rightarrow$ resultado: 1 ~~para~~ emaranhado (distribuído anteriormente) + 1 qbit de comunicação = 2 bits de comunicação.

Distinguindo preparações de matriz densidade e comunicação superluminal

$|\psi\rangle = \frac{1}{\sqrt{2}} (|11\rangle + |22\rangle)$. Agora qbits A e B são apartados.

• Alice ~~se tenta~~ ^{mandar} ~~se comunica~~ ^{1 bit} com Bob.

$$1 \cdot |1 \times 1| + 2 \cdot |2 \times 2|$$

• Se quer mandar 0: Mede $A_0 = |10\rangle + |20\rangle$

e acha $d=1$ com prob. $P_1 = \text{tr}(|1 \times 1\rangle \rho_A) = \frac{1}{2} \Rightarrow$ estado ~~pr-~~ ^{pr-} ~~medida~~ ^{medida}

$|22\rangle$ com prob. $\frac{1}{2} \Rightarrow$ estado $|22\rangle = |2 \times 1\rangle + |1 \times 2\rangle$

$\approx |11\rangle$

• Se quer mandar 1:

Mede $A_1 = |1+X+1\rangle + |2-X-1\rangle$ onde $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$

$P_+ = \frac{1}{2} \Rightarrow$ estado $|++\rangle$

$P_- = \frac{1}{2} \Rightarrow$ estado $|--\rangle$

• Qual o estado de Bob depois da medida?

Alice 0: $\rho_0 = \frac{1}{2} |0 \times 0\rangle + \frac{1}{2} |1 \times 1\rangle$

Alice 1: $\rho_1 = \frac{1}{2} |1+X+1\rangle + \frac{1}{2} |2-X-1\rangle$

$\left. \begin{array}{l} \text{não ignora} \Rightarrow \rho_B \text{ não} \\ \text{depende de qual medida Alice} \\ \text{fez.} \end{array} \right\}$

MAS se Bob conseguisse discriminar as 2 preparações, conseguiria ler a mensagem de Alice — mesmo a anos-luz de distância!

$\Rightarrow$ comunicação superluminal

$\Rightarrow$ mensagem por o parado.

$\left. \begin{array}{l} \text{VIOLARIA a Teoria da} \\ \text{relatividade especial.} \end{array} \right\}$