Generalización del Algoritmo Cuántico de Teleportación

Alejandro Díaz Caro[1]
Departamento de Ciencias de la Computación
Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Universidad Nacional de Rosario, Argentina

Resumen

En 1993 C. Bennet, G. Brassard, C. Crepeau, R. Jozsa, A. Peres y W. Wootters[1] sugirieron un algoritmo cuántico capaz de teleportar el estado desconocido de un qubit haciendo uso de un estado de Bell. Utilizando dicho algoritmo, la teleportación de los estados de 2 o más qubits debe hacerse de a uno por vez. El problema surge cuando se quiere teleportar un estado cuántico de N-qubits que estén entangled, pues separarlos para viabilizar la teleportación implicaría perder dicha propiedad.

El objetivo del presente trabajo es realizar una generalización del algoritmo de teleportación que sea capaz de teleportar los estados de N-qubits en forma simultánea. Para ello se propone un estado entangled análogo a un estado de Bell de 2N-qubits.

Nota: Se han suprimido las demostraciones a todo lo propuesto en este trabajo por cuestiones de espacio. Esas demostraciones puodrán ser vistas en la publicación de las próximas JAIIO[2].

1. Introducción

1.1. El qubit

En el modelo cuántico de computación la unidad de información básica es el *qubit* o bit cuántico. Un qubit puede estar en dos estados distintos que se denotan $|0\rangle$ y $|1\rangle$ respectivamente o en estados intermedios, es decir, en estados que son combinación lineal de los estados $|0\rangle$ y $|1\rangle$.

Entonces un qubit es un vector de un espacio vectorial generado por los dos estados, es decir, es un vector de $\mathcal{V} = \mathcal{L}\{|0\rangle, |1\rangle\}$. Según la Mecánica Cuántica[2] $\mathcal{V}$ es un espacio de Hilbert complejo en el que $\mathcal{B} = \{|0\rangle, |1\rangle\}$ es una base ortonormal y los estados son vectores unitarios[3].

Entonces un qubit puede estar en cualquier estado $\psi = a|0\rangle + b|1\rangle$ tal que $a, b \in \mathbb{C}$ y $|a|^2 + |b|^2 = 1$. Los coeficientes a y b se denominan amplitudes.

1.2. Algoritmos cuánticos

En el modelo cuántico de computación un algoritmo es un mecanismo para manipular n-qbits. Uno de los posibles mecanismos para hacerlo es medir qubits.

Al medir un qubit $\psi = a|0\rangle + b|1\rangle$, éste toma el valor $|0\rangle$ con probabilidad $|a|^2$ y el valor $|1\rangle$ con probabilidad $|b|^2$.

El otro mecanismo consiste en transformar un estado inicial ψ_1 en su correspondiente estado final ψ_2. Si llamamos U a la función de $\mathcal{V}_n \mapsto \mathcal{V}_n$ tal que $U\psi_1 = \psi_2$ entonces el segundo mecanismo consiste en aplicar la función U. La aplicación U transforma estados en estados, es decir, conserva la norma y, según los postulados de la Mecánica Cuántica, es lineal. Por tanto, U sólo puede ser una transformación unitaria.

[1] janus@rtfm.org.ar

[2] http://www.cerider.edu.ar/jaiio34

En general se escribe una transformación como una secuencia de transformaciones unitarias elementales que se denominan *compuertas cuánticas*.

Las compuertas cuánticas más importantes, por su utilidad en el diseño de algoritmos, son las siguientes:

- La transformación H de Hadamard: $\begin{array}{c} H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array}$ donde: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

- La identidad I: $\begin{array}{c} I|0\rangle = |0\rangle \\ I|1\rangle = |1\rangle \end{array}$ donde: $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

- La negación X: $\begin{array}{c} X|0\rangle = |1\rangle \\ X|1\rangle = |0\rangle \end{array}$ donde: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

- El cambio de fase Z: $\begin{array}{c} X|0\rangle = |0\rangle \\ X|1\rangle = -|1\rangle \end{array}$ donde: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

- La *Controlled-Not* $CNOT$: $\begin{array}{c} CNOT|0x\rangle = |0x\rangle \\ CNOT|1x\rangle = |1\rangle \otimes X|x\rangle \end{array}$ donde: $CNOT = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}$

1.3. Teleportación de 1 qubit

El estado de Bell[4] $\beta_{00} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ es un estado de 2 qubits entangled[3] y se construye a partir del siguiente algoritmo

$$|00\rangle \overset{\text{H(1)}}{\longrightarrow} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \overset{\text{CNOT(1,2)}}{\longrightarrow} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

La teleportación surge de aplicarle ciertas compuertas cuánticas al qubit a teleportar (ψ) y al primero de β_{00}, para conseguir que para cada uno de los posibles resultados de la medición de los dos primeros qubits, el tercero quede en un estado que es una combinación de compuertas X y Z del estado ψ original.

Veamos un poco este algoritmo

$$\psi \otimes \beta_{00} = (\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle))$$

$$\text{CNOT(1,2)}$$

$$\longrightarrow \frac{1}{\sqrt{2}}(\alpha(|000\rangle + |011\rangle) + \beta(|110\rangle + |101\rangle))$$

[3] Enredados en forma coherente

$$\text{H(1)}$$

$$\longrightarrow \frac{1}{2}(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle))$$

$$= \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle))$$

Haciendo un pequeño abuso de notación, esta última expresión se puede escribir

$$\frac{1}{2}(|00\rangle\psi + |01\rangle X\psi + |10\rangle Z\psi + |11\rangle XZ\psi)$$

y de esta manera se puede apreciar que si el resultado de una medición sobre los dos primeros qubits es $|00\rangle$ el tercer qubit es ψ. Con un resultado de $|01\rangle$ el tercero resulta $X\psi$, con $|10\rangle$, $Z\psi$; y por último, con una medición $|11\rangle$ el tercero queda definido en $XZ\psi$. Por lo tanto, realizando una medición sobre los dos primeros qubits, el tercero queda en un estado que se puede volver a transformar en el estado ψ original por medio de compuertas X y Z.

2. Definiciones y resultados previos

2.1. Notación $\breve{k}_n$

Para generalizar la teleportación a sistemas de n-qubits es necesario construir una notación que permita manipular cualquier número de qubits en forma práctica. Entonces definimos:

$\breve{k}_n$ $\forall k \in \mathbb{N}$ es la representación binaria con n bits del número k.

2.2. El estado β_{00}^n

Primero se necesitará un estado entangled análogo al estado de Bell, sólo que con más de 2n qubits, ya que 2n son los que se llevará Bob y el resto son los que trabajará Alice[4] junto con el estado ψ a teleportar.

Prestando atención a la teleportación de un qubit, se ve que el estado de Bell β_{00} tiene todos los posibles valores de un qubit definido, repetido dos veces; esto es: $|00\rangle$, $|11\rangle$, ya que los valores posibles definidos en un qubit son 0 y 1. Esto es útil para lograr que cualquier combinación lineal de la base del espacio de Hilbert $\mathbb{C}^2$ sea teleportada puesto que sólo el último qubit es el que está en el lugar a donde se teleportará ψ. Por lo tanto, aquí se hará lo mismo: se crea un estado que sea todos los valores posibles definidos de n qubits repetidos 2 veces, o sea: $|\breve{j}_n\breve{j}_n\rangle$ $j = 1 \ldots 2^n - 1$, obteniendo así el estado:

$$\beta_{00}^n = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |\breve{i}_n\breve{i}_n\rangle$$

y se genera a partir del siguiente algoritmo:

$$|\breve{0}_n\breve{0}_n\rangle \overset{H(1,\ldots,\text{n})}{\longrightarrow} \frac{1}{\sqrt{2}} \sum_{i=0}^{2^n-1} |\breve{i}_n\breve{0}_n\rangle \overset{CNOT(\text{k,n+k})}{\underset{\text{k=1,}\ldots\text{,n}}{\longrightarrow}} \frac{1}{\sqrt{2}} \sum_{i=0}^{2^n-1} |\breve{i}_n\breve{i}_n\rangle = \beta_{00}^n$$

Lema 1 *β_{00}^n es un estado en entanglement del espacio de Hilbert $\mathbb{C}^{2^n}$*

[4]En la Teoría Cuántica "Alice" representa al que envía un mensaje y "Bob" al que lo recibe.

2.3. Delta de Iverson

2.3.1. Notación de Iverson[5]

Sea p una propiedad, entonces:

$$[p] = \begin{cases} 1 & \text{si } p \\ 0 & \text{si } \neg p \end{cases}$$

2.3.2. Delta de Iverson

Definimos con el nombre de *Delta de Iverson* a:

$$\begin{aligned} \ddot{\delta}_{i,k} &= [k \text{ tiene cantidad impar de bits en } 1 \\ &\quad \text{en los lugares de los bits en } 1 \text{ de } i] \\ &= [(k \text{ AND } i) \text{ tiene cantidad impar de bits en } 1] \end{aligned}$$

Lema 2

$$(-1)^{\ddot{\delta}_{2i+1,2k+1}} = (-1)^{\ddot{\delta}_{i,k}}(-1) \quad (1)$$

$$(-1)^{\ddot{\delta}_{2i+1,2k}} = (-1)^{\ddot{\delta}_{i,k}} \quad (2)$$

$$(-1)^{\ddot{\delta}_{2i,2k+1}} = (-1)^{\ddot{\delta}_{i,k}} \quad (3)$$

$$(-1)^{\ddot{\delta}_{2i,2k}} = (-1)^{\ddot{\delta}_{i,k}} \quad (4)$$

3. Algoritmo de teleportación

Sea el estado a teleportar:

$$\psi_n = \sum_{i=0}^{2^n-1} \alpha_i |\breve{i}_n\rangle$$

entonces

$$\psi_n \otimes \beta_{00}^n = \frac{1}{\sqrt{2^n}} \left(\sum_{i=0}^{2^n-1} \alpha_i |\breve{i}_n\rangle \right) \left(\sum_{j=0}^{2^n-1} |\breve{j}_n \breve{j}_n\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} \left(\alpha_i \sum_{j=0}^{2^n-1} |\breve{i}_n \breve{j}_n \breve{j}_n\rangle \right)$$

Teorema 1 *Sea el siguiente algoritmo:*

- *CNOT(*k*,* $n+k$*),* $k = 1, \ldots, n$
- *H(*$1, \ldots, n$*)*
- *Medición sobre los primeros* $2n$ *qubits*

Luego de esto, Bob obtiene sus n-qubits en una combinación de Xs *y* Zs *del estado* ψ_n*.*
DEMOSTRACIÓN

$$\psi_n \otimes \beta_{00}^n = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} \alpha_i |\breve{i}_n\rangle \sum_{j=0}^{2^n-1} |\breve{j}_n \breve{j}_n\rangle$$

$$\xrightarrow[k=1,\ldots,n]{\textit{CNOT(k,n+k)}}$$

$$\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} \alpha_i |\breve{i}_n\rangle \sum_{j=0}^{2^n-1} |(j \overset{\breve{}}{\text{XOR}}\ i)_n \breve{j}_n\rangle$$

$$\xrightarrow{\textit{H(}1,\ldots,n\textit{)}}$$

$$\frac{1}{\sqrt{2^n}} \left[\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} \alpha_i \sum_{k=0}^{2^n-1} (-1)^{\ddot{\delta}_{i,k}} |\breve{k}_n\rangle \sum_{j=0}^{2^n-1} |(j \overset{\breve{}}{\text{XOR}}\ i)_n \breve{j}_n\rangle \right]$$

$$= \frac{1}{2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} \sum_{k=0}^{2^n-1} |\breve{k}_n (j \overset{\breve{}}{\text{XOR}}\ i)_n\rangle (-1)^{\ddot{\delta}_{i,k}} \alpha_i |\breve{j}_n\rangle$$

Teorema 2

$$\frac{1}{2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} \sum_{k=0}^{2^n-1} |\breve{k}_n (j \overset{\breve{}}{\text{XOR}}\ i)_n\rangle (-1)^{\ddot{\delta}_{i,k}} \alpha_i |\breve{j}_n\rangle$$

$$= \frac{1}{2^n} \sum_{a_1=0}^{1} \cdots \sum_{a_{2n}=0}^{1} |a_1 \ldots a_{2n}\rangle \left(\bigotimes_{k=a_{2n}}^{a_{n+1}} X^k \right) \left(\bigotimes_{k=a_n}^{a_1} Z^k \right) \psi_n$$

Referencias

[1] Bennet, Brassard, Crepeau, Jozsa, Peres y Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. **70**, 1895-1900 (1993)

[2] Von Neuman, *Mathematical fundations of Quantum Mechanics*, Pricenton University Press, 34 (1955)

[3] Preskill, *Lecture Notes for Physics 229: Quantum Information and Computation*, California Institute of Technology, 41 (1998)

[4] Nielsen, Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 20 (2000)

[5] Graham, Knuth, Patashnik, *Concrete Mathematics*, Addison-Wesley, 24 (1990)