Computación Cuántica versus MTPs

Juan Carlos Agudelo Agudelo

Grupo de Lógica y Computación
Universidad EAFIT

12 de febrero de 2010

Contenido

Contenido

Computación Cuántica

Generalización de modelos de computación a través de los principios de la mecánica cuántica.

- Richard Feynman (1981): sistemas cuánticos no pueden ser simulados eficientemente a través de los computadores actuales, tal vez puedan ser simulados eficientemente por computadores cuánticos.
- David Deutsch (1985): propone el modelo de máquinas de Turing cuánticas (MTCs).
- David Deutsch (1989): propone el modelo de circuitos cuánticos (CCs).
- Andrew Yao (1993): demuestra la equivalencia, en cuanto a complejidad algorítmica, entre MTCs e CCs.
- Peter Shor (1994): define un algoritmo cuántico para factorizar enteros en tiempo polinomial.

Postulados de la mecánica cuántica

Postulado

A todo sistema físico se asocia un espacio de Hilbert, conocido como espacio de estados del sistema. El estado del sistema es completamente descrito por un vector unitario en el espacio de estados del sistema.

Ejemplo (Qubit o bit cuántico)

Vector unitario en un espacio de estados bidimensional.

Estado general de un qubit: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (donde $\alpha, \beta \in \mathbb{C}$),

Usualmente: $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

Condición de normalización: $|\alpha|^2 + |\beta|^2 = 1$.

Postulados de la mecánica cuántica

Postulado

La evolución de un sistema cuántico es descrita por un operador unitario U (U es unitario si $U^\dagger U = I$):

$$|\psi'\rangle = U|\psi\rangle.$$

Reversibilidad: $U^{-1} = U^\dagger$.
Linealidad: $U(\alpha|0\rangle + \beta|1\rangle) = \alpha U(|0\rangle) + \beta U(|1\rangle)$.

Ejemplo (operador de Hadamard)

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad H(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Interferencia cuántica:

$$
\begin{aligned}
H(H(|0\rangle)) &= H(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) \\
&= \frac{1}{\sqrt{2}}(H|0\rangle + H|1\rangle) \\
&= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) \\
&= \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle + \frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle \\
&= |0\rangle.
\end{aligned}
$$

Postulados de la mecánica cuántica

Postulado

El espacio de estados de un sistema físico compuesto es el producto tensorial de los espacios de estados de los sistemas físicos que lo componen. Si se tienen los subsistemas enumerados de 1 a n, y el sistema i se encuentra en el estado $|\psi_i\rangle$, entonces, el estado del sistema total es $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$.

Ejemplo (2-qubit)

Espacio de estados $H_4 = H_2 \otimes H_2$.
Base entandar: $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.
Estado general: $|\psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$.
Condición de normalización: $|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1$.

Definición (Estado enredado)

Sistema compuesto cuyo estado no puede expresarse como producto tensorial de los sistemas que los componen.

Ejemplo

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{1}$$

Postulados de la mecánica cuántica

Postulado

En la mecánica cuántica un observable M es un operador auto-adjunto ($M = M^\dagger$). La salida numérica de una medición, de un estado $|\psi\rangle$ con respecto a M, es uno de los autovalores de M. En la medida, el autovalor λ_i es obtenido con probabilidad $Pr(\lambda_i) = \langle\psi|P_i|\psi\rangle$. El efecto colateral de tal medición es el colapso de $|\psi\rangle$ al autoestado correspondiente al autovalor obtenido en la medición.

Ejemplo

Estado: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
Para el 'observable estándar': $Pr(0) = |\alpha|^2$ y $Pr(1) = |\beta|^2$.
Si en la medición se obtiene 0 el estado colapsa a $|0\rangle$, en caso contrario colapsa al estado $|1\rangle$.

Máquinas de Turing Cuánticas

Una Máquinas de Turing Cuántica (MTC) is definida considerando los elementos de una MT como siendo propiedades (observables) de un sistema cuántico:

- Una MTC puede estar en un estado superpuesto (en múltiples configuraciones clásicas simultáneamente).
- Las operaciones son definidas a través de operadores unitarios. Los operadores unitarios son lineales, lo que permite procesamiento en paralelo (paralelismo cuántico).
- Al final de la computación debe ser realizada una medición, obteniendo como resultado un único elemento de la superposición.
- En el proceso de computación, la interferencia cuántica incrementa o decrementa las probabilidades de obtener una cierta configuración.

Circuitos Cuánticos

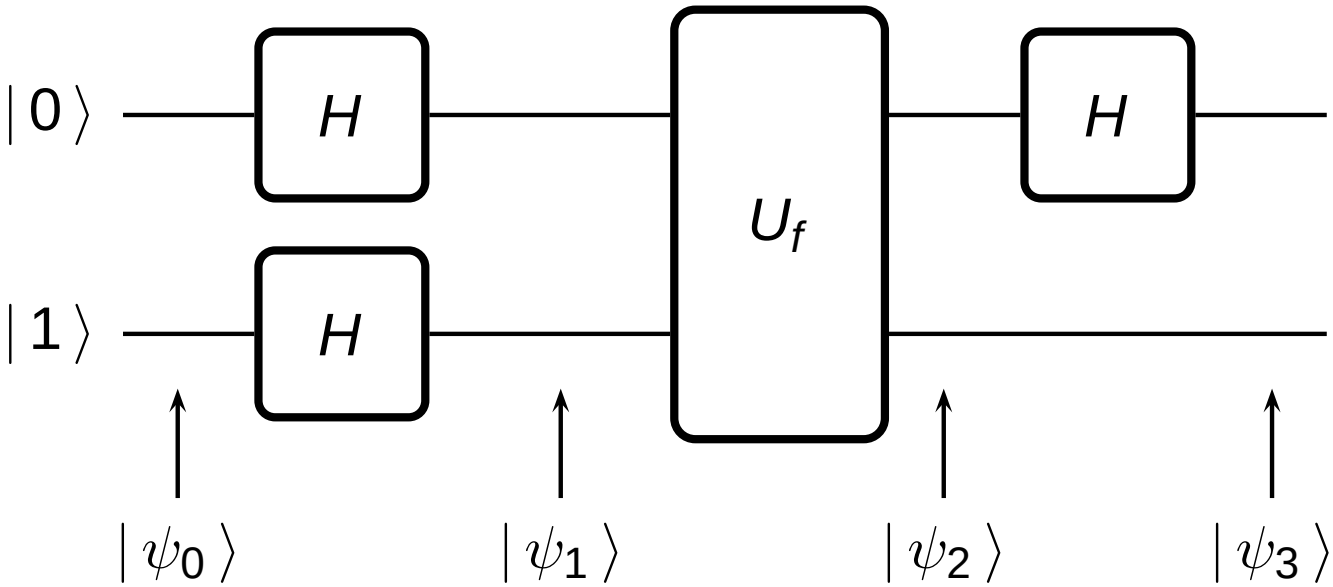
Un Circuito Cuántico (CC) es una generalización de los circuitos booleanos a través de los postulados de la mecánica cuántica:

- Las entradas/salidas de las puertas lógicas son n-qubits.
- Las puertas lógicas son operadores unitarios.
- Al final del circuito debe ser realizada una medición, obteniendo como resultado un único elemento de la superposición (de acuerdo con el postulado de la medición).
- En el proceso de computación, la interferencia cuántica incrementa o decrementa las probabilidades de obtener una cierta configuración.

Problema de Deutsch

Problema de Deutsch: dada una función $f: \{0,1\} \to \{0,1\}$ determinar si f es constante o balanceada consultando solamente una vez un 'oráculo' que computa f.

Circuito cuántico para solucionar o problema de Deutsch:



Problema de Deutsch

$$|\psi_0\rangle = |01\rangle$$

$$|\psi_1\rangle = \frac{1}{2}[|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle)]$$

$$|\psi_2\rangle = U_f\left(\frac{1}{2}[|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle)]\right)$$

$$= \frac{1}{2}[|0\rangle(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)]$$

$$= \begin{cases} \pm\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right] \otimes \left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] & se\ f(0) = f(1), \\ \pm\left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] \otimes \left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] & se\ f(0) \neq f(1). \end{cases}$$

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] & se\ f(0) = f(1), \\ \pm|1\rangle\left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] & se\ f(0) \neq f(1). \end{cases}$$

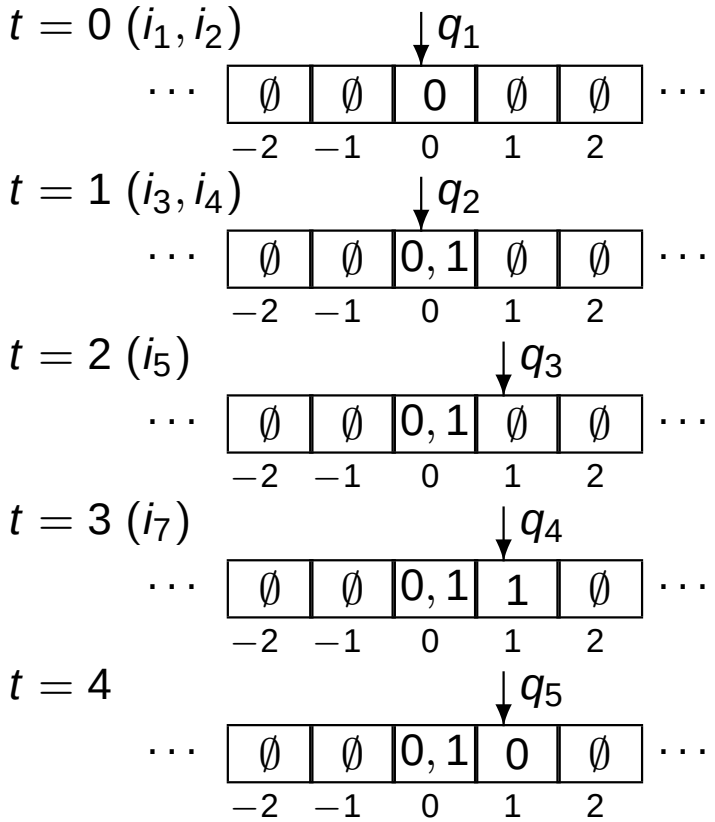
Contenido

Relaciones entre MTPs y MTCs

- Toda configuración de una MTP puede ser vista como una superposición uniforme de configuraciones de una MT clásica: estados superpuestos corresponden a estados contradictorios.
- Las MTPs no permiten una representación directa de Estados enredados (ej. $|\psi\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)$).
- Las MTPs no permiten una representación directa de la noción de fase relativa, por lo tanto, no permiten representar la interferencia cuántica (las condiciones de inconsistencia en las MTPs son un mecanismo diferente a la interferencia cuántica).

Solución del problema de Deutsch a través de MTPs

Solución a través de MTPs (para $f(0) = f(1) = 1$): sea $\mathcal{M}$ una MTP con instrucciones: $i_1 : q_1 00 q_2$, $i_2 : q_1 01 q_2$, $i_3 : q_2 0 R q_3$, $i_4 : q_2 1 R q_3$, $i_5 : q_3 \emptyset 1 q_4$, $i_6 : q_4 00 q_5$, $i_7 : q_4 10 q_5$, $i_8 : q_4 1^{\bullet} * q_5$, $i_9 : q_5 * 1 q_5$.



Solución del problema de Deutsch a través de MTPs

- Instrucciones i_1 y i_2 simulan la generación del estado superpuesto.
- Instrucciones i_3 a i_5 computan la función constante 1 sobre el estado superpuesto, calculando $f(0)$ y $f(1)$ en paralelo y escribiendo el resultado en la posición 1 (pueden ser consideradas como el oráculo, que puede ser cambiado por otro).
- Instrucciones i_6 a i_9 chequean si f es constante ($f(0) = f(1)$) o balanceada ($f(0) = f(1)$), usando una instrucción con condición de inconsistencia (i_8), escribiendo 0 en la posición 1 si f es constante o 1 en caso contrario (sustituyendo la interferencia cuántica).

Relaciones entre MTPNSs y MTCs

- MTPNSs permiten representar estados enredados uniformes:
  - Considere $|\psi\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)$ representando los símbolos en las posiciones 0 y 1 de una MTC $\mathcal{M}$.
  - El estado de $\mathcal{M}$ es equivalente a el estado de una MTPNS $\mathcal{M}'$ dividida en dos copias: una con 0 en las posiciones 0 y 1 y otra con 1 en las posiciones 0 y 1.
  - La teoría $\Delta^{\star}_{S5}(\mathcal{M}'(\alpha))$ puede deducir $S_0(\bar{t},0) \wedge_{\diamond} S_0(\bar{t},1)$ y $S_1(\bar{t},0) \wedge_{\diamond} S_1(\bar{t},1)$, y no deducir $S_0(\bar{t},0) \wedge_{\diamond} S_1(\bar{t},1)$ ni $S_1(\bar{t},0) \wedge_{\diamond} S_0(\bar{t},1)$. Consecuentemente, estados enredados corresponden a conjunciones no separables.
- Las MTPNSs tampoco permiten una representación directa de la noción de fase relativa, por lo tanto, no permiten representar la interferencia cuántica (las condiciones de inconsistencia en las MTPNSs parecen ser un mecanismo mas potente que la interferencia cuántica).