P. Universidad Católica de Chile
Facultad de Ingeniería
Tópicos en Ciencia de la Computación

Introducción a la Computación Cuántica

Gonzalo Díaz
09 de agosto de 2011

1 Introducción

Este documento presenta un resumen del mini tutorial que se dictó en el curso Tópicos en Ciencia de la Computación. Se hace una introducción a la mecánica cuántica, para luego repasar algunos conceptos básicos de información cuántica.

1.1 Mecánica clásica

La mecánica clásica se construye en torno al concepto de partícula, que corresponde a una unidad de materia puntual, que cuenta con masa, posición y velocidad definidas.

Para una partícula puntual de masa m, sea $\sum \mathbf{F}$ la suma de las fuerzas que actúan sobre ella, y $\mathbf{a}$ su aceleración. Entonces:

$$\sum \mathbf{F} = m\mathbf{a}. \tag{1}$$

La ecuación anterior (segunda ley de Newton) permite obtener el comportamiento de una partícula si se conocen las fuerzas que actúan sobre ella.

A diferencia de la mecánica clásica, donde se conoce con certeza la posición y velocidad, en la mecánica cuántica se trabajará con funciones de onda.

2 Mecánica cuántica [1]

La teoría de la mecánica cuántica postula que la única información que tenemos acerca de un sistema fśico es la función de onda, que es una función compleja del espacio y del tiempo.

2.1 Ecuación de Schrödinger

Si se modela una partícula como una onda, su ecuación de onda será la ecuación de Schrödinger:

$$i\hbar\frac{\partial\Psi}{\partial t} = -\frac{\hbar^2}{2m}\frac{\partial^2\Psi}{\partial x^2} + V\Psi. \tag{2}$$

Interpretación estadística La función de onda se interpreta estadísticamente, considerando la cantidad:

$$\int_a^b |\Psi(x,t)|^2 dx \tag{3}$$

como la probabilidad de encontrar a la partícula entre a y b, en el momento t.

Colapso de la función de onda Al hacer una medición de la posición de la partícula, la función de onda *colapsa* en el punto observado. Así, una medición inmediatamente posterior arrojará el mismo resultado.

Valor medio y varianza El valor medio de la funciíon $f(x)$, bajo una distribución de probabilidad $P(x)$ es:

$$\langle f(x)\rangle = \int_{-\infty}^{+\infty} f(x)P(x)dx. \tag{4}$$

y su varianza es $\sigma^2 \equiv \langle(\Delta x)^2\rangle = \langle x^2\rangle - \langle x\rangle^2$.

Normalización La función de onda debe cumplir:

$$\int_{-\infty}^{+\infty} |\Psi(x,t)|^2 dx = 1 \tag{5}$$

Esto equivale a afirmar que la partícula debe estar en algún punto del espacio.

2.2 Operadores

Valores de expectación El valor de expectación de la posición es:

$$\langle x\rangle = \int_{-\infty}^{+\infty} x|\Psi(x,t)|^2 dx = \int_{-\infty}^{+\infty} \Psi^* x\Psi dx, \tag{6}$$

Para el momentum, tendremos:

$$m\frac{d\langle x\rangle}{dt} = m\int_{-\infty}^{+\infty} x|\Psi(x,t)|^2 dx = m\int x\frac{\partial}{\partial t}|\Psi|^2 dx$$
$$= \int \Psi^*\left(-i\hbar\frac{\partial}{\partial x}\right)\Psi dx. \quad (7)$$

De esta forma se concluye que tanto la posición como el momentum actúan como operadores sobre la función de onda:

$$\hat{x} \to x,$$
$$\hat{p} \to -i\hbar\frac{\partial}{\partial x}. \quad (8)$$

2.3 Ecuación de Schrödinger independiente del tiempo

Si consideramos las soluciones separables de la ecuación de Schrödinger: $\Psi(x,t) = \psi(x)\varphi(t)$, obtendremos las siguientes dos ecuaciones:

$$i\hbar\frac{d\varphi}{dt} = E\varphi,$$
$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V\psi = E\psi. \quad (9)$$

La primera tiene como solución: $\varphi(t) = \exp(-iEt/\hbar)$. La segunda ecuación es la llamada ecuación de Schrödinger independiente del tiempo:

$$H\psi = E\psi, \quad (10)$$

con $H = -(\hbar^2/2m)(d^2/dx^2) + V$. Así, la solución separable será de la forma:

$$\Psi(x,t) = \psi(x)e^{-iEt/\hbar}. \quad (11)$$

Soluciones separables Las soluciones separables son *estacionarias*: $|\Psi(x,t)|^2 = |\psi(x)|^2$. Además, tienen energía definida: $\langle\hat{H}\rangle = E$ y $\sigma_{\hat{H}} = 0$.

Por último, y lo que es más importante, toda solución a la ecuación de Schrödinger puede ser escrita como superposición lineal de las soluciónes separables:

$$\Psi(x,t) = \sum_n c_n\psi_n(x)e^{-iEt/\hbar}. \quad (12)$$

2.4 Espacios de Hilbert

Las funciones de onda viven en el espacio de Hilbert, que es un espacio vectorial completo con producto interno. En la notación de Dirac, se aprovecha este hecho:

$$\Psi(x,t) \to |\Psi\rangle. \quad (13)$$

Definimos el siguiente producto interno entre dos vectores:

$$\langle f|g\rangle \equiv \int f(x)^* g(x)dx. \quad (14)$$

Los *observables* son representados por operadores hermíticos (i.e. que cumplen $\langle f|\hat{Q}f\rangle = \langle\hat{Q}f|f\rangle\ \forall f$). Cabe notar que los estados determinados de $\hat{Q}$ ($\sigma_Q = 0$) son autofunciones de $\hat{Q}$.

2.5 Operador de evolución temporal

La evolución del estado $|\Psi(x,t)\rangle$ está gobernada por la ecuación de Schrödinger:

$$i\hbar\frac{\partial}{\partial t}|\Psi(x,t)\rangle = \hat{H}|\Psi(x,t)\rangle, \quad (15)$$

donde $\hat{H}$ es el Hamiltoniano. La solución a esta ecuación es:

$$|\Psi(x,t)\rangle = \hat{U}(t)|\Psi(x,0)\rangle, \quad (16)$$

donde $\hat{U}(t)$ es el operador de evolución temporal, y es unitario (i.e. $\hat{U}^\dagger = \hat{U}^{-1}$). Resulta:

$$\hat{U}(t) = \exp\left(-i\frac{\hat{H}t}{\hbar}\right). \quad (17)$$

El operador de evolución temporal es una herramienta para transformar un estado cuántico. Posteriormente se podrá realizar una compuerta cuántica con un operador de evolución temporal (la realización física de la compuerta consiste en generar el Hamiltoniano correspondiente).

2.6 Interpretación estadística generalizada

Si medimos el observable $Q(x,p)$ de una partícula en el estado $\Psi(x,t)$, se obtendrá uno de los autovalores del operador $\hat{Q}(x, -i\hbar d/dx)$ (i.e. reemplazando el momentum por su correspondiente operador).

Además, las autofunciones de un operador observable son completas, por lo que cualquier función de

onda se puede escribir como combinación lineal de éstas:

$$\Psi(x,t) = \sum_n c_n f_n(x), \tag{18}$$

donde $c_n = \langle f_n|\Psi\rangle$. $|c_n|^2$ será la probabilidad de medir el autovalor q_n de $\hat{Q}$.

2.7 Estados mezclados

Si no conocemos el estado, pero sí la probabilidad P_n de que el sistema esté en diferentes estados (normalizados) $|\psi_n\rangle$, entonces el valor medio de un operador A será:

$$\langle A\rangle = \sum_n P_n \langle\psi_n|\hat{A}|\psi_n\rangle. \tag{19}$$

Introducimos la matriz de densidad $\hat{\rho}$:

$$\hat{\rho} = \sum_n P_n |\psi_n\rangle\langle\psi_n|. \tag{20}$$

Así, el valor medio de un operador para un estado mezclado es:

$$\langle A\rangle = Tr(\hat{\rho}\hat{A}). \tag{21}$$

Así, podemos representar un estado en su forma vectorial $|\Psi\rangle$ o con su matriz de densidad $\hat{\rho} = |\Psi\rangle\langle\Psi|$. La segunda forma permite incorporar una distribución estadística de estados.

3 Información cuántica [2]

3.1 Qubits

La unidad básica de la información cuántica es el *qubit*. Un qubit corresponde a un sistema físico que tiene dos estados ortogonales, que llamaremos $|1\rangle$ y $|0\rangle$.

La implementación física del qubit puede ser cualquier sistema de dos niveles. Por ejemplo: los estados de polarización de un fotón, la orientación del spin de una partícula de spin 1/2, dos niveles energéticos de un átomo, etc.

Como los usaremos mucho, introducimos los siguientes operadores:

$$\begin{aligned}
\hat{I} &= |0\rangle\langle 0| + |1\rangle\langle 1|,\\
\hat{\sigma}_x &= |0\rangle\langle 1| + |1\rangle\langle 0|,\\
\hat{\sigma}_y &= i|1\rangle\langle 0| - i|0\rangle\langle 1|,\\
\hat{\sigma}_z &= |0\rangle\langle 0| - |1\rangle\langle 1|.
\end{aligned} \tag{22}$$

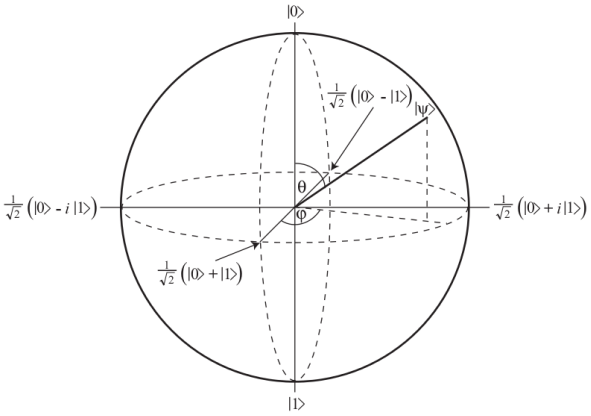
En general, un qubit puede encontrarse en una *superposición* de los estados $|1\rangle$ y $|0\rangle$:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle, \tag{23}$$

donde a_0 y a_1 son números complejos. Como $|\psi\rangle$ debe estar normalizado, podemos redefinir las constantes de la siguiente forma:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle. \tag{24}$$

Esfera de Bloch Podemos representar los parámetros θ y ϕ como las coordenadas esféricas de un punto sobre un cascarón:



Múltiples qubits Si tenemos varios sistemas físicos representando qubits, podemos escribir su función de onda con el producto tensorial:

$$|\psi\rangle = |0\rangle \otimes |1\rangle \otimes \ldots \otimes |0\rangle. \tag{25}$$

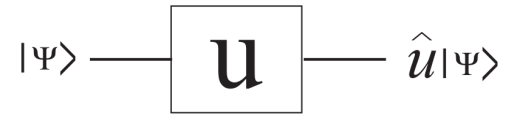
Para transformar un qubit de esta secuencia, usamos un operador definido análogamente:

$$\begin{aligned}
&(\hat{I} \otimes \ldots \otimes \hat{I} \otimes \hat{U} \otimes \hat{I} \ldots \otimes \hat{I})|\psi\rangle\\
&= |0\rangle \otimes |1\rangle \otimes \ldots \otimes (\hat{U}|0\rangle) \otimes \ldots \otimes |0\rangle.
\end{aligned} \tag{26}$$

Un estado de múltiples qubits como el anterior será el análogo de un registro de un computador clásico.

3.2 Compuertas cuánticas

Trabajamos con un sistema físico que tiene dos niveles: $|0\rangle$ y $|1\rangle$. En mecánica cuántica, podemos actuar sobre un estado $|\psi\rangle$ con una transformación unitaria $\hat{U}$. Esta transformación será el análogo a una compuerta lógica de un qubit.



Algunas de las compuertas más importantes son: Hadamard ($\hat{H}$), Pauli-X ($\hat{X}$), Pauli-Y ($\hat{Y}$), Pauli-Z ($\hat{Z}$) y Phase (S) y $\pi/8$ ($\hat{T}$).

$$\hat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad \hat{Z} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

$$\hat{X} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \qquad \hat{S} = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$$

$$\hat{Y} = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} \qquad \hat{T} = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix} \quad (27)$$

Compuerta NOT cuántica La compuerta Pauli-X es conocida también como la compuerta NOT cuántica, ya que transforma $|0\rangle \to |1\rangle$ y $|1\rangle \to |0\rangle$. Sin embargo, no es una compuerta NOT cuántica universal, ya que no transforma $|\psi\rangle \to |\psi^{\perp}\rangle$.

Una compuerta NOT óptima Consideramos los operadores:

$$\hat{A}_1 = \frac{1}{\sqrt{3}}\hat{\sigma}_x, \quad \hat{A}_2 = \frac{1}{\sqrt{3}}\hat{\sigma}_y, \quad \hat{A}_3 = \frac{1}{\sqrt{3}}\hat{\sigma}_z. \quad (28)$$

La siguiente operación:

$$\hat{\rho} \to \sum_i \hat{A}_i \hat{\rho} \hat{A}_i^{\dagger}, \quad (29)$$

produce la siguiente transformación:

$$|\psi\rangle\langle\psi| \to \frac{2}{3}|\psi^{\perp}\rangle\langle\psi^{\perp}| + \frac{1}{3}|\psi\rangle\langle\psi|, \quad (30)$$

lo cual tiene una probabilidad de éxito de un tercio.

3.3 Comunicaciones cuánticas

Alice selecciona un mensaje del conjunto $\{a_i\}$ y envía a Bob el estado correspondiente del conjunto $\{\rho_i\}$ de estados señal. Bob conoce los dos últimos conjuntos, además de las probabilidades $P(a_i)$ de que Alice seleccione un mensaje.

Así, Bob conoce de antemano la matriz de densidad del estado que recibirá:

$$\hat{\rho} = \sum_i P(a_i)\hat{\rho}_i. \quad (31)$$

Bob deberá determinar cuál de los estados ρ_i le fue enviado.

Envío de estados ortogonales Si los estados $\{\hat{\rho}_i\}$ son ortogonales (i.e. $\hat{\rho}_i\hat{\rho}_j = 0$), entonces Bob puede medir un observable cuyos autoestados sean los estados señal.

Envío de estados no-ortogonales Consideramos que Alice puede enviar uno de los estados $\{|\psi_1\rangle, |\psi_2\rangle\}$, que no son ortogonales. Reescribimos el segundo estado:

$$|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\psi_1^{\perp}\rangle, \quad (32)$$

Si Bob mide el observable $\hat{A} = |\psi_1\rangle\langle\psi_1| - |\psi_1^{\perp}\rangle\langle\psi_1^{\perp}|$, obtendrá con certeza el valor $+1$ si el estado es $|\psi_1\rangle$, pero podrá obtener tanto $+1$ como -1 si el estado es $|\psi_2\rangle$.

Las comunicaciones cuánticas se aprovecharán de este hecho ya que, si bien Bob tendrá más dificultades en recibir una señal, estas dificultades también las tendrá un posible tercero que desea interceptar la comunicación (Eve).

No-clonación El teorema de no-clonación establece que no se puede hacer una copia perfecta de un estado cuántico. Supongamos que tenemos dos registros: $|\psi\rangle$ (que queremos copiar) y $|B\rangle$ (blank). Queremos realizar la transformación

$$|\psi\rangle \otimes |B\rangle \to |\psi\rangle \otimes |\psi\rangle, \quad (33)$$

para todo estado $|\psi\rangle$. Supongamos que se cumple

$$\begin{aligned} |0\rangle \otimes |B\rangle &\to |0\rangle \otimes |0\rangle, \\ |1\rangle \otimes |B\rangle &\to |1\rangle \otimes |1\rangle. \end{aligned} \quad (34)$$

Se sigue del principio de superposición que un estado general transformará como:

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |B\rangle \rightarrow \alpha|0\rangle \otimes |0\rangle + \beta|1\rangle \otimes |1\rangle, \quad (35)$$

lo cual no es un par de copias del estado original.

3.4 Distribución cuántica de llaves

Protocolo BB84 Alice envía qubits a Bob preparados en una de dos bases. Denotamos con $\oplus$ la base $\{|0\rangle\ , |1\rangle\}$ y $\otimes$ será la base:

$$|0'\rangle \equiv \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$$
$$|1'\rangle \equiv \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \quad (36)$$

A continuación, Alice generá qubits elegidos aleatoriamente entre los cuatro anteriores. A los estados $|0\rangle$ y $|0'\rangle$ se les asocia el bit 0, mientras que a los estados $|1\rangle$ y $|1'\rangle$, el bit 1.

Los estados son enviados a Bob, quien mide cada estado con una base elegida al azar entre las dos opciones: $\oplus$ o $\otimes$. Si Bob elige la base equivocada, entonces el resultado de su medición podrá ser correcta o incorrecta.

Una vez medidos los valores, Bob comunica públicamente a Alice qué bases usó para sus mediciones (e.g. $\oplus, \oplus, \otimes, \oplus, \ldots$).

Alice responde indicando en qué ocasiones las bases coinciden. Los resultados donde las bases no coincidieron son descartados.

En ausencia de Eve (*evesdropper*), los bits resultantes serán compartidos por Alice y Bob. Si alguien está escuchando, esto introducirá errores en los bits recibidos por Bob. Alice y Bob podrán comparar un subconjunto de bits públicamente para determinar si existe un interceptor. Si es así, el procedimiento se cancela. Si no, los bits comparados públicamente se descartan y los restantes constituirán la clave privada compartida.

3.5 Principios de la computación cuántica

Para realizar una computación con estados cuánticos necesitamos:

1. Una colección finita de qubits, cuyo estado inicial corresponde al *input*. Cada qubit puede estar en uno de dos estados ortogonales, $|1\rangle$ o $|0\rangle$.

2. Un circuito de compuertas cuánticas, diseñado para ejecutar una transformación unitaria sobre el estado inicial de los qubits.

3. Finalmente, se debe realizar una medición sobre los qubits. Esta medición deberá revelar, al menos con una probabilidad suficientemente alta, el resultado.

Para acotar la notación, denotaremos, por ejemplo, el estado de cinco qubits $|1\rangle \otimes |0\rangle \otimes |0\rangle \otimes |1\rangle \otimes |1\rangle$ como $|10011\rangle$.

Idealmente, el procesador cuántico realizaría una transformación unitaria:

$$|a\rangle \rightarrow \hat{U}|a\rangle = |f(a)\rangle, \quad (37)$$

donde a es un número y $f(a)$ es cualquier función booleana. Esto no funciona, debido a que una transformación unitaria preserva los productos internos entre estados.

Introducimos una segunda secuencia de qubits $|b\rangle$ y realizaremos la siguiente transformación:

$$|a\rangle \otimes |b\rangle \rightarrow \hat{U}_f|a\rangle \otimes |b\rangle = |a\rangle \otimes |b \oplus f(a)\rangle, \quad (38)$$

donde $b \oplus f(a)$ es la adición módulo 2. Así, los estados $|a_1\rangle \otimes |b \oplus f(a_1)\rangle$ y $|a_2\rangle \otimes |b \oplus f(a_2)\rangle$ son ortogonales aunque $f(a_1) = f(a_2)$. Por último, elegimos $b = 0$.

References

[1] David J. Griffiths, *Introduction to Quantum Mechanics*. Pearson Prentice Hall, 2nd Edition 2005, cap. 1.

[2] Stephen M. Barnett, *Quantum Information*. Oxford University Press, 2009.