Capitulo 5

La Computación Cuántica

La computación cuántica usa fenómenos cuánticos, tal como la interferencia y el enredo, para el procesamiento de información. Feynman planteó la primera pregunta en este sentido en 1982, cuando él preguntó si el comportamiento de cada sistema mecánico cuántico puede ser eficazmente simulado por una computadora o un simulador clásico. En 1985 Deutsch propuso el primer algoritmo cuántico y también describió una computadora cuántica universal. Después de Deutsch varios algoritmos cuánticos han sido propuestos, culminando con el descubrimiento importante del algoritmo de Shor en 1994. Con este algoritmo cuántico fue mostrado que la computadora cuántica, al menos en principio, puede factorizar números grandes de tal manera que el tiempo de ejecución del algoritmo crece polinomialmente con el número de dígitos del número a ser factorizado. Es sabido que en comparación para cualquier algoritmo clásico el tiempo de ejecución crece exponencialmente. Otro algoritmo cuántico, descubierto por Grover en 1996, hace posible la búsqueda en una base de datos desordenada de un elemento y es más rápido cuando se compara con los algoritmos clásicos equivalente a la raíz cuadrada del número de elementos en la base de datos.

La teoría para una computadora cuántica esta en principio determinado, el obstáculo principal es práctico, o sea para mantener la coherencia en el sistema cuando aumentamos el número de unidades computacionales. Un método importante en combatir las impurezas en sistemas cuánticos es el método de corrección de error propuesto por Deutsch. El sugirió un procedimiento de simetrización. Esta idea ha sido mejorada paso a paso, por ejemplo por Palma quien introdujo la decoherencia de los subespacios libres, y en particular por Shor que propuso un análogo cuántico del método clásico de corrección de error. En este método es posible usar repetidamente la codificación de los qubits para detectar y corregir errores de las compuertas cuánticas debido a la interacción con el entorno. Otro método para alcanzar un cálculo cuántico coherente es usar el cálculo cuántico geométrico o topológico.

5.1 Introducción

El elemento básico para la construcción de la computación cuántica es el qubit es decir cualquier sistema mecánico cuántico de dos niveles. Si denotan la base del ortonormal para el sistema como |0› y |1› (llamados la base computacional) nosotros podemos expresar un estado arbitrario normalizado del qubit como

$$|\phi\rangle = \cos(\theta/2)\, e^{i\alpha}|0\rangle + \operatorname{sen}(\theta/2)\,|1\rangle \qquad (5.1)$$

Como que un qubit puede estar en una superposición este puede contener dos valores al mismo tiempo, por ejemplo los estados Booleanos |0› y |1›, mientras que un bit clásico está restringido solamente a solo un valor, 0 o 1. Un qubit puede ser construido con un átomo, espín nuclear, o un fotón polarizado. Si tenemos a varios qubits, la cantidad de información que pueden almacenar en un momento dado, aumenta exponencialmente con el número de qubits. Si tenemos a 2 qubits en estado $|\phi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$, entonces en un momento dado hemos almacenado 4 valores numéricos (con igual amplitud de probabilidad). En general N qubits puede contener 2^N valores numéricos (en una superposición cuántica) en cualquier momento mientras que los N bits clásicos puedan almacenar un resultado de los 2N valores numéricos. Otros fenómenos cuánticos importantes es el enredo. Dos (o muchos) qubits están enredados, no separable, si el estado total no puede ser escrita como un producto tensorial de los dos estados individuales del qubit, es decir

$$|\phi_{1,2}\rangle \quad |\phi_1\rangle\,|\phi_2\rangle$$

Si tenemos un registro, es decir una colección, de qubits en algún estado inicial, podemos realizar operaciones cuánticas sobre estos de acuerdo a algún procedimiento prescripto llamada un algoritmo cuántico. El cálculo es entonces llevado a cabo de una manera paralela con los diferentes estados de la base en la superposición. Si tenemos N qubits, entonces habrá 2^N estados base paralelos, entonces podemos realizar un calculo paralelo que requeriría 2^N cálculos en una computadora clásica. Después del cálculo del estado final de los qubits, este lleva la información resultante. Debido a que la toma de medidas destruye las superposiciones, no se logra restaurar toda información del

cálculo. Pero con interferencia cuántica podemos incrementar la amplitud de probabilidad del resultado deseado tal que la medida da el resultado correcto en mucho de los casos.

Una operación cuántica unitaria fijada desarrollada sobre una selección de qubit es llamado una compuerta lógica cuántica. Varias compuertas lógicas, sincronizadas en el tiempo, forman una red cuántica, donde el tamaño de la red es el número de compuertas que contiene.

La compuerta lógica de un qubit de Hadamard y la compuerta lógica de fase condicional de dos qubits juntas forman un conjunto universal de compuertas, es decir, cualquier operación unitaria de N-qubits puede ser simulada exactamente usando redes fuera de las dos compuertas. Este no es un conjunto único, casi cualquier compuerta de dos qubits que pueda enredar los qubits puede ser usado como una compuerta universal.

Seguidamente se describe el conjunto universal con las compuertas de Hadamard y el corrimiento de la compuerta de fase condicional. Una sola compuerta de fase es considerado que no es eficiente usar la compuerta de fase condicional para operaciones de corrimiento de fase para un qubit.

- La Compuerta de Hadamard es la compuerta de un solo qubit **H** desarrollando la transformación unitaria conocida como la transformación de Hadamard definida por

$|0\rangle \quad 1/\ 2\ (|0\rangle + |1\rangle)$, $|1\rangle \quad 1/\ 2\ (|0\rangle + |1\rangle)$, es decir creando superposiciones.

También podemos escribir la compuerta de Hadamard como

$$\left.\begin{array}{l} \mathbf{H} = (1/\sqrt{2}) \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ |x\rangle \quad \boxed{\mathbf{H}} \quad ((-1)^x |x\rangle + |1-x\rangle)/\sqrt{2} \end{array}\right\} \qquad (5.2)$$

La matriz está escrita en la bases {|0›, |1›} y el diagrama en el lado derecho provee una representación esquemática de la compuerta *H* actuando sobre un qubit en estado |x›, con

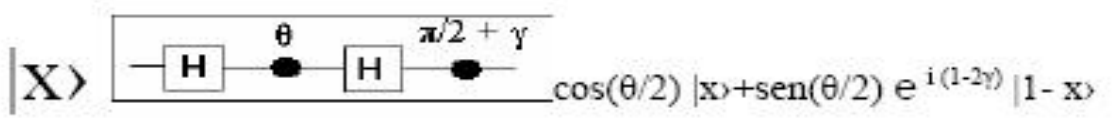
x =0, 1. Una comprensión física de una compuerta de Hadamard podría ser el desdoblamiento de un haz en un conjunto de interferometría.

• Usando la misma notación definimos la compuerta de corrimiento de fase como una única compuerta qubit tal que |0›_ |0› y |1›_ ^{i} _ |1›, para algún _ prescrito. La notación de la matriz y el diagrama de estructura están dados por

$$\left.\begin{array}{l} \Gamma = \begin{pmatrix} 1 & 0 \\ 1 & e^{i\gamma} \end{pmatrix} \\ |x\rangle \xrightarrow{\ \gamma\ } e^{i x\gamma}\,|x\rangle \end{array}\right\} \qquad (5.3)$$

Un comprensión física de una compuerta de de corrimiento de fase puede ser un corrimiento de fase en uno de los haces de un interferómetro.

Con las compuertas qubit mostradas, el Hadamard y la compuerta de corrimiento de fase, cualquier transformación de un qubit pueden ser realizado (hasta la fase global) de acuerdo a una simple red que se muestra seguidamente en una representación diagramático.



Con esta red podemos transformar a los N-qubit estados |00…0› a

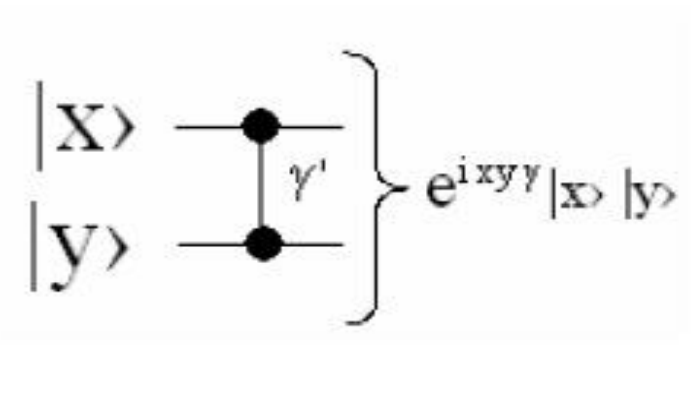
|ø$_1$ ø$_2$… ø$_N$›, dónde cada _$_i$ es una superposición arbitraria de |0› y |1›. Éstos son los llamados producto de estado o estados separables, lo cual esta restringido a un

conjunto de N-qubit estados. Para transformar a estados separables, es decir los estados enredados, nosotros la necesitamos dos compuertas qubit.

- Las compuertas de fase condicional de dos qubit está definida como:

|00› |00›,|01› |01›,|10› |10›,|11› äiã|11›, para algún ã´ dado. La notación matricial y la estructura del diagrama están dadas por (la matriz escrita en la base computacional {|00›,|01›,|10›,|11›})

$$B(\gamma) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\gamma} \end{pmatrix} \qquad (5.4)$$



Esta compuerta hace posible enredar dos (o más) qubits.

El conjunto universal de compuertas no puede ser construido de un corrimiento de fases (regular o condicional) aislados. Es necesario operaciones que combinen las bases computacionales, tal como la compuerta de Hadamard. Para implementar tales compuertas de una manera geométrica se necesita estar habilitados para construir compuertas geométricas o topológicas no Abelianas.

Ejemplos de realizaciones experimentales de compuertas han sido desarrollados usando por ejemplo resonancia magnética nuclear, trampas de iones, cavidad QED, y sistemas fotónicos.

5.2 La computación cuántica geométrica

Para lograr un cálculo cuántico tolerante podemos usar la fase geométrica, descritas en el capítulo 2, e implementar las compuertas cuánticas, así llamado cálculo cuántica geométrica. Tales fases son, como mencionamos antes, fallas tolerables para la región del espacio de estados conservando las operaciones.

Se hará un conjunto universal de compuertas basado en fases geométricas adiabáticas. La descripción de la fase geométrica adiabática fue considerada en el capítulo 2. Si un eigenestado de un sistema cuántico depende de un conjunto de parámetros externos **R** entonces una variación cíclica adiabática de estos parámetros retorna el sistema a su estado original. El vector de estado final esta relacionado con el vector de estado inicial vía el producto de un factor de fase dinámica y de un factor de fase geométrico $e^{i\gamma_g}$, lo cual depende sólo de la forma del camino en el espacio de parámetro. Si el estado $|\phi(t)\rangle$ pertenece a un subespacio degenerado que permanece en el subespacio degenerado durante una evolución adiabática. Sin embargo, el sistema regresa en general a su estado final

$|\phi(t)\rangle$ relacionado a su estado inicial $|\phi(0)\rangle$ por un operador unitario U_g

$$|\psi(\tau)\rangle = U_g |\psi(0)\rangle \exp\{-i/\hbar \int_0^\tau E(t)dt\}. \qquad (5.5)$$

Donde la U_g depende sólo de forma del camino en el parámetro espacio. La matriz U_g es una generalización de la fase geométrica (la multiplicación por el factor $i\gamma_g$) en casos no abelianos.

Para evaluar U_g elegimos un conjunto de N-pliegues de estados de referencia degenerados $[|n, (\mathbf{R})\rangle]$, perteneciente al espacio de fase local. Entonces en cualquier punto en el camino del adiabático en el espacio de parámetro $\mathbf{R}(t)$ podemos escribir.

$$|\psi_l(t)\rangle = \sum_n U_g(t)|n,\mathbf{R}(t)\rangle \quad (5.6)$$

En particular, para un circuito cerrado la condición final $|\psi_l(\tau)\rangle = \sum_n U_{g\,l\,n}(\tau)|n\rangle$ está relacionada al estado inicial, eligiendo $|l\rangle$, vía $U_{l\,n}(\hat{o})$. Estos elementos de matriz pueden ser evaluados como la integral de camino.

$$U=\mathbf{P}\exp[i\int_0^t dt' \mathbf{A}(\mathbf{R})\, d\mathbf{R}/dt] \quad (5.7)$$

con el potencial gauge definido como

$$\mathbf{A}_{ab}(\mathbf{R}) = i\langle a|\partial/\partial\mathbf{R}|b\rangle. \quad (5.8)$$

En el caso abeliano, es decir, la fase geométrica, el camino ordenando no es necesario y la integral se reduce a una integral de línea regular. Una prueba experimental de la fase geométrica no Abeliana también ha sido generalizada para evoluciones no Adiabáticas y no cíclicas.

La compuerta geométrica más sencilla es una compuerta de fase qubit. El estado de referencia $|n(\grave{e},\ddot{o})\rangle$ puede estar escrita como

$$|n(\theta,\varphi)\rangle = \cos(\theta/2)\,|0\rangle + e^{i\varphi}\,\mathrm{sen}(\theta/2)\,|1\rangle \quad (5.9)$$

donde $\mathbf{R} = \{\grave{e},\ddot{o}\}$ son los ángulos polares esféricos del vector Bloch. El potencial gauge Abeliano se escribe

$$A_\theta = i\langle n|\partial/\partial\theta|n\rangle = 0 \quad (5.10)$$

$$A_\varphi = i\langle n|\partial/\partial\varphi|n\rangle = -1/2(1-\cos\theta) \quad (5.11)$$

Consideremos un qubit, por ejemplo el spin semientero de un núcleo en un campo magnético que varía lentamente, experimenta una evolución cónica cíclica con ángulo cónico è. Entonces la integral de línea del potencial gauge da la fase

$$\gamma_g = \pm \tfrac{1}{2} \Omega = \pm \pi (1 - \cos \theta),$$

geométrica de un ciclo adiabático

donde el signo ± depende de si el sistema está alineado o no lo esta con el campo, y _ es el ángulo sólido subtendido por el circuito cónico. Así los dos estados del qubit |0› y |1› pueden

terminar con fases geométricas de signos opuestos, la cual da una compuerta de fase con un corrimiento de 2ã entre los dos estados.

Los experimentos más comunes de compuertas de corrimiento de fase geométrica es un qubit en una campo magnético estático acoplado a un campo magnético oscilante [14]. Si $ù_0$ es la frecuencia de transición del qubit en el campo, ù es la frecuencia del campo oscilante, y $ù_1$ es la amplitud del campo oscilante, entonces controlando ù y $ù_1$ uno puede efectivamente implementar un circuito cónico equivalente tal que el campo magnético varía lentamente con un ángulo è dado por

$$\cos \theta = (\omega_0 - \omega)/((\omega_0 - \omega)^2 + \omega_1^2)^{1/2} \qquad (5.12)$$

Note que para alguna deformación en el camino del spin la cual conserva este ángulo sólido mantiene la misma fase. Así la fase no es afectada por la velocidad con la cual se recorra el camino; no es muy sensitivo a fluctuaciones al azar alrededor del camino.

Para una compuerta de fase geométrica condicional podemos considerar un sistema de dos partículas de spin semientero que no interactúan S_a y S_b. En un marco de referencia alineado con el campo estático, el Hamiltoniano será

$$H_0 = \hbar\omega_a S_{az} \otimes 1_b + \hbar\omega_b 1_a \otimes S_{bz} \qquad (5.13)$$

donde las frecuencias $ù_a/2ð$ y $ù_b/2ð$ son las frecuencias de transición de los dos spines y se ha usado los operadores de Pauli $S_i = ó_i/2$. Se asume que $_a$ y $_b$ son muy diferentes con $ù_a > ù_b$. Si las dos partículsa están suficientemente próximas uno a la

otra, ellos interactuaran, creando desdoblamientos adicionales entre los niveles de energía. En el caso de dos partículas con spin semientero, el campo magnético de un spin puede directamente o indirectamente los niveles de energía del otro spin; la energía del sistema es incrementado por ð J/2 si los spines son paralelos y decrecen en ð J/2 si los spines son antiparalelos. El Hamiltoniano del sistema toma en cuenta esta interacción como

$$H = H_0 + 2\pi\hbar J\, S_{az} \otimes S_{bz} \qquad (5.14)$$

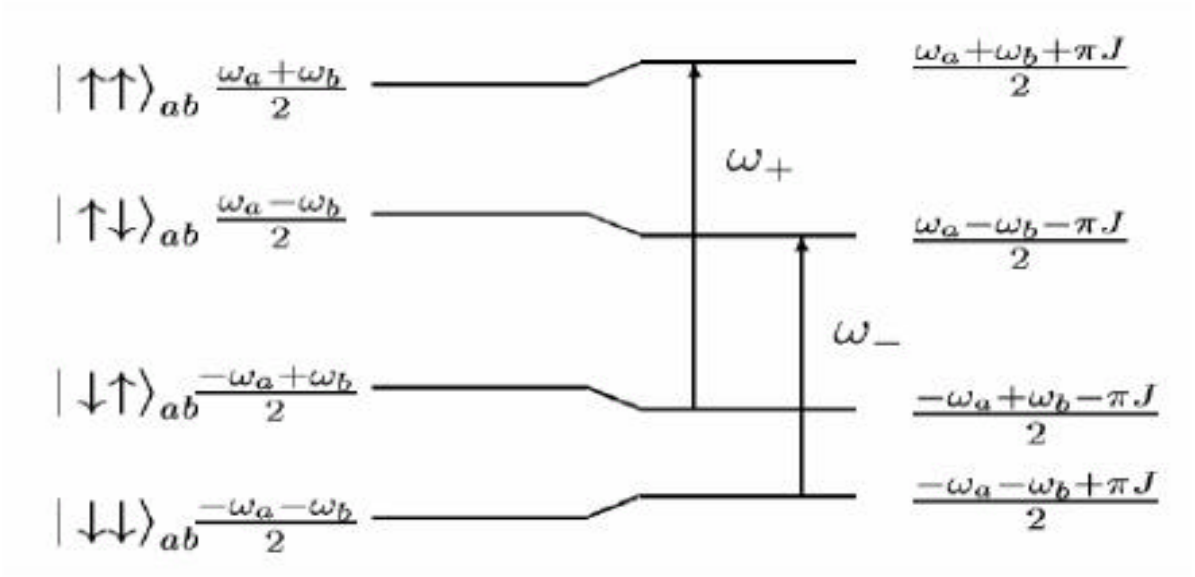


Fig. 7.- El diagrama de energía de los spines de dos núcleos en interacción. La frecuencia de transición del primer spin depende del estado del segundo spin.

Debido al campo, S_x y S_y son pequeños para ambas partículas. La Fig.7 muestra los niveles de energía del sistema. Cuando el spin S_b esta en el estado |_›, la frecuencia de transición del spin S_a es

$$\omega_+ = \omega_a + \pi J, \qquad (5.15)$$

mientras que cuando el spin S_b esta en un estado |!›, la frecuencia de transición del spin S_a es

$$\omega_{-} = \omega_a - \pi J, \tag{5.16}$$

Ahora supongamos que además del campo estático, aplicamos un campo rotante que varíe lentamente como se menciono anteriormente. Vimos que la fase de Berry adquirida por un spin depende de la frecuencia de transición como la que se presenta en la ecuación (5.12).

Por lo tanto, en el término de una evolución cíclica, la fase de Berry adquirida por el spin S_a será diferente para los dos posibles estados del spin S_b. De modo semejante, cuando la spín S_b se encuentre en un estado $|\ \rangle$, la fase de Berry adquirido por el spín S_a es

$$\gamma_{+} = \mp \pi (1 - \cos\theta_{+}),$$

con el signo negativo o positivo dependiendo de si el giro es up o down, respectivamente, y

$$\cos\theta_{+} = (\omega_{+} - \omega)/ ((\omega_{+} - \omega)^2 + \omega_1^2)^{1/2} \tag{5.17}$$

Similarmente, cuando el spin S_b esta en el estado $|!\rangle$, la fase de Berry adquirida por el spin S_a is

$$\gamma_{-} = \mp \pi (1 - \cos\theta_{-}),$$

donde

$$\cos\theta_{-} = (\omega_{-} - \omega)/ ((\omega_{-} - \omega)^2 + \omega_1^2)^{1/2} \tag{5.18}$$

La diferencia de fase geométrica $\tilde{a}_{+} - \tilde{a}_{-}$ depende de la amplitud de oscilación del campo magnético $\dot{u}_1$ de tal manera que este tiene un máximo para un valor no nulo de $\dot{u}_1$.