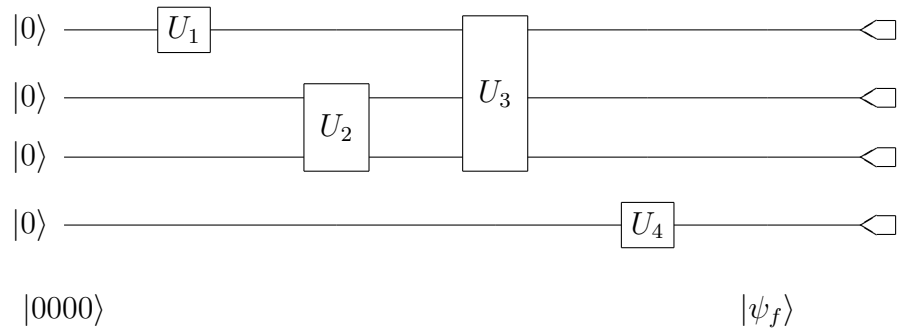
Un Modelo Cuántico de Computación

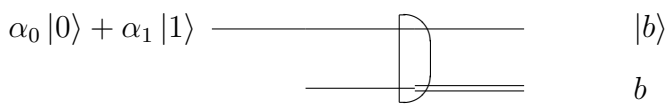
A. El Modelo de Circuitos Cuánticos

El modelo de computación (clásica) de circuitos puede ser generalizado a un modelo de *circuitos cuánticos*. En este modelo los qubits son transportados por cables y en su recorrido se encuentran con compuertas cuánticas que actúan sobre ellos. Un ejemplo se ve en la Figura. Los cables son las líneas horizontales y los qubits se propagan de izquierda a derecha en el tiempo.



En este ejemplo el estado de 4 qubits $|\psi_i\rangle = |0000\rangle$ entra en el circuito para ser procesado por las compuertas U_1, U_2, U_3, U_4. Como salida del circuito tenemos el estado de 4 qubits (posiblemente entangled) $|\psi_f\rangle$. Se realiza una medición qubit por qubit en la base computacional.

En muchos casos no importa el estado de salida cuántico y sólo se está interesado en la información clásica que indica qué salida resultó. En el circuito de la Figura, se mide el estado cuántico $\alpha_0 |0\rangle + \alpha_1 |1\rangle$ resultando el estado cuántico $|b\rangle$ ($b \in \{0, 1\}$), junto con la salida clásica b (0 o 1) que indica la salida.



B. Compuertas Cuánticas

Compuertas de 1-Qubit

Dado que todo estado $|\psi\rangle$ de 1-qubit puede ser representado como un punto en la superficie de la esfera de Bloch, la acción de una compuerta cuántica unitaria U sobre $|\psi\rangle$ puede ser pensada como una rotación sobre la esfera de Bloch del vector $|\psi\rangle$ al vector $U|\psi\rangle$. Por ejemplo, la compuerta NOT transforma el estado $|0\rangle$ en el estado $|1\rangle$. En la esfera de Bloch esta transformación es una rotación en un ángulo π alrededor del eje x.
Una clase muy importante de compuertas de 1-qubit son las *compuertas de rotación*, que corresponden a rotaciones sobre los ejes x, y y z de la esfera de Bloch:

$$\begin{aligned} R_x(\theta) &= e^{\frac{-i\theta X}{2}} \\ R_y(\theta) &= e^{\frac{-i\theta Y}{2}} \\ R_z(\theta) &= e^{\frac{-i\theta Z}{2}}, \end{aligned}$$

donde X, Y y Z son las matrices (o compuertas) de Pauli.

Ejercicio
Sea x un número real y A una matriz tal que $A^2 = I$. Muestre que

$$e^{iAx} = cos(x)I + isen(x)A.$$

Hint: Aplique el desarrollo en serie de Taylor.

Es fácil verificar que $X^2 = I$, $Y^2 = I$ y $Z^2 = I$ y por lo tanto las compuertas de rotación se pueden escribir:

$$\begin{aligned} R_x(\theta) &= e^{\frac{-i\theta X}{2}} &= cos(\tfrac{\theta}{2})I - isen(\tfrac{\theta}{2})X \\ R_y(\theta) &= e^{\frac{-i\theta Y}{2}} &= cos(\tfrac{\theta}{2})I - isen(\tfrac{\theta}{2})Y \\ R_z(\theta) &= e^{\frac{-i\theta Z}{2}} &= cos(\tfrac{\theta}{2})I - isen(\tfrac{\theta}{2})Z. \end{aligned}$$

y en forma matricial en la base computacional:

$$
\begin{aligned}
R_x(\theta) &= \begin{bmatrix} cos(\frac{\theta}{2}) & -isen(\frac{\theta}{2}) \\ -isen(\frac{\theta}{2}) & cos(\frac{\theta}{2}) \end{bmatrix} \\
R_y(\theta) &= \begin{bmatrix} cos(\frac{\theta}{2}) & sen(\frac{\theta}{2}) \\ sen(\frac{\theta}{2}) & cos(\frac{\theta}{2}) \end{bmatrix} \\
R_z(\theta) &= \begin{bmatrix} e^{\frac{-i\theta}{2}} & 0 \\ 0 & e^{\frac{i\theta}{2}} \end{bmatrix}.
\end{aligned}
$$

Considere un estado arbitrario de 1-qubit escrito en términos de sus ángulos del vector de Bloch σ y τ:

$$
cos(\frac{\sigma}{2})\,|0\rangle + e^{i\tau} sen(\frac{\sigma}{2})\,|1\rangle\,.
$$

En la base computacional será el vector columna

$$
\begin{pmatrix} cos(\frac{\sigma}{2}) \\ e^{i\tau} sen(\frac{\sigma}{2}) \end{pmatrix}
$$

El efecto de aplicar $R_z(\theta)$ a este estado será:

$$
\begin{aligned}
\begin{bmatrix} e^{\frac{-i\theta}{2}} & 0 \\ 0 & e^{\frac{i\theta}{2}} \end{bmatrix} \begin{pmatrix} cos(\frac{\sigma}{2}) \\ e^{i\tau} sen(\frac{\sigma}{2}) \end{pmatrix} &= \begin{pmatrix} e^{-i\frac{\theta}{2}} cos(\frac{\sigma}{2}) \\ e^{i\frac{\theta}{2}} e^{i\tau} sen(\frac{\sigma}{2}) \end{pmatrix} \\
&= e^{-i\frac{\theta}{2}} \begin{pmatrix} cos(\frac{\sigma}{2}) \\ e^{i\theta} e^{i\tau} sen(\frac{\sigma}{2}) \end{pmatrix} \\
&= e^{-i\frac{\theta}{2}} (cos(\tfrac{\sigma}{2})\,|0\rangle + e^{i(\tau+\theta)} sen(\tfrac{\sigma}{2})\,|1\rangle).
\end{aligned}
$$

Eliminando la fase global, el estado resultante de aplicar $R_z(\theta)$ es:

$$
cos(\frac{\sigma}{2})\,|0\rangle + e^{i(\tau+\theta)} sen(\frac{\sigma}{2})\,|1\rangle\,.
$$

O sea que ha cambiado el ángulo τ a $\tau + \theta$ lo que representa una rotación de θ alrededor del eje z de la esfera de Bloch.

Teorema

Toda compuerta unitaria U de 1-qubit admite la descomposición:

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta),$$

con α, β, γ y δ números reales.

Este teorema se cumple por la relación entre compuertas unitarias y rotaciones en la esfera de Bloch vista antes.

Como no hay nada especial en los ejes y y z de la esfera de Bloch se puede reformular el teorema:

Teorema

Toda compuerta unitaria U de 1-qubit admite la descomposición:

$$U = e^{i\alpha} R_l(\beta) R_m(\gamma) R_l(\delta),$$

con α, β, γ y δ números reales y l y m dos ejes no paralelos de la esfera de Bloch.

Corolario

Toda compuerta unitaria U de 1-qubit se puede escribir en la forma:

$$U = e^{i\alpha} AXBXC,$$

dondes A, B y C son operadores unitarios que cumplen $ABC = I$.

Ejercicio

a) Pruebe que $XR_y(\theta)X = R_y(-\theta)$ y $XR_z(\theta)X = R_z(-\theta)$.

b) Pruebe el Corolario.

Hint: De acuerdo al primer teorema se puede escribir:

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta).$$

Tome $A = R_z(\beta)R_y(\gamma/2)$, $B = R_y(-\gamma/2)R_z(-(\delta+\beta)/2)$, y $C = R_z((\delta-\beta)/2)$.

Compuertas Control-U

Ya se vió anteriormente la compuerta Control-NOT (*CNOT*). Ésta es una compuerta

cuántica de 2-qubits que aplica condicionalmente la compuerta NOT en el segundo qubit (*target*) cuando el primer qubit (*control*) está en el estado $|1\rangle$.

Ejercicio

Obtenga el resultado de la acción de la compuerta *CNOT* sobre las bases siguientes:

a) $B_1 = \left\{ |0\rangle \ (\frac{|0\rangle+|1\rangle}{\sqrt{2}}),\ |0\rangle \ (\frac{|0\rangle-|1\rangle}{\sqrt{2}}),\ |1\rangle \ (\frac{|0\rangle+|1\rangle}{\sqrt{2}}),\ |1\rangle \ (\frac{|0\rangle-|1\rangle}{\sqrt{2}}) \right\},$

b) $B_2 = \left\{ (\frac{|0\rangle+|1\rangle}{\sqrt{2}})\,(\frac{|0\rangle+|1\rangle}{\sqrt{2}}),\ (\frac{|0\rangle+|1\rangle}{\sqrt{2}})\,(\frac{|0\rangle-|1\rangle}{\sqrt{2}}),\ (\frac{|0\rangle-|1\rangle}{\sqrt{2}})\,(\frac{|0\rangle+|1\rangle}{\sqrt{2}}),\ (\frac{|0\rangle-|1\rangle}{\sqrt{2}})\,(\frac{|0\rangle-|1\rangle}{\sqrt{2}}) \right\}.$

De la misma forma que la *CNOT* se puede definir la compuerta *Control-U* ($c-U$) para cualquier compuerta de 1-qubit U que será una compuerta de 1-qubit que cumple con:

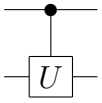
$$\begin{aligned} c-U\,|0\rangle\,|\psi\rangle &= |0\rangle\,|\psi\rangle \\ c-U\,|1\rangle\,|\psi\rangle &= |1\rangle\,U\,|\psi\rangle\,. \end{aligned}$$

Ejercicio

Pruebe que la compuerta $c-U$ corresponde al operador

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U.$$

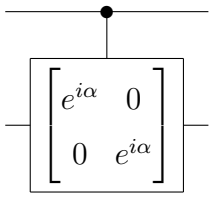
El símbolo de la compuerta $c-U$ es el de la figura.



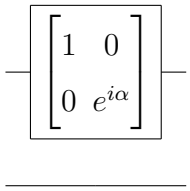
Vamos a ver ahora cómo hacer un circuito equivalente a la compuerta $c-U$ usando compuertas de 1-qubit y compuertas *CNOT*. Para ello usaremos la descomposición $U = e^{i\alpha}AXBXC$ del corolario demostrado anteriormente.

Primero veremos cómo aplicar $e^{i\alpha}$ sobre el bit target en forma controlada por el bit control. O sea que si el bit control es $|1\rangle$ se aplica, mientras que si el bit control es $|0\rangle$ no se aplica.

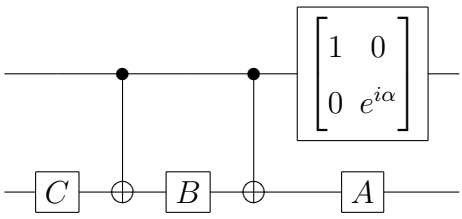
Entonces la compuerta *desfasaje controlado*



será equivalente a



Ahora es fácil darse cuenta que el circuito equivalente a la compuerta $c-U$ es el de la Figura:



Supongamos que el qubit de control es $|1\rangle$. Entonces la operación $U = e^{i\alpha}AXBXC$ se aplica al segundo qubit. Si por el contrario, el qubit control es $|0\rangle$ la operación $ABC = I$ es aplicada al segundo qubit, lo que implica que permanece igual. O sea que este circuito realiza la operación control-U.

C. Conjuntos Universales de Compuertas Cuánticas

La compuerta de *Hadamard* transforma la base computacional de la siguiente forma:

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

La representación matricial de la compuerta de *Hadamard* (en base computacional) es:

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Además es su auto-inversa, ya que $H = H^{-1}$, porque

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

Otra compuerta de 1-qubit importante es la compuerta T o de fase $\frac{\pi}{8}$:

$$\begin{aligned} T|0\rangle &= |0\rangle \\ T|1\rangle &= e^{i\frac{\pi}{4}}|1\rangle . \end{aligned}$$

con representación matricial:

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$$

que es equivalente (por medio de una fase global) a:

$$T = \begin{bmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{bmatrix}$$

y de ahí el nombre compuerta-$\frac{\pi}{8}$.

Definición

Un conjunto de compuertas se dice *universal* si todo operador unitario de n-qubits puede

ser reemplazado por un circuito cuántico que use solamente compuertas de ese conjunto.

Definición

Una compuerta de 2-qubits se conoce como *entangling* si para algún vector entrada producto $|\psi\rangle |\phi\rangle$ la salida de la compuerta no es un estado producto, o dicho de otra manera es *entangled*.

Teorema

El conjunto formado por alguna compuerta entangling de 2-qubits y *todas* las compuertas de 1-qubit es universal.

Este teorema implica que, por ejemplo, la compuerta *CNOT* junto con todas las compuertas de 1-qubit es universal. El problema es que este conjunto universal es *infinito*. De cualquier forma si se encuentra un conjunto de compuertas finito que sea universal para las compuertas de 1-qubit se puede reemplazar a *todas* ellas por ese conjunto finito.

Teorema

El conjunto $\{H, T\}$ es universal para compuertas de 1-qubit.

Teorema

El conjunto $\{CNOT, H, T\}$ es un *conjunto universal de compuertas*.

D. Mediciones con Circuitos Cuánticos

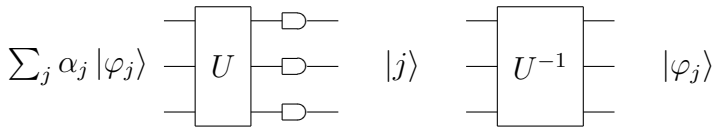
Las mediciones proyectivas completas son muy usadas en computación y comunicación cuánticas. En particular, los protocolos de codificación superdensa y teleportación cuántica están basados en mediciones de Von Neumann.
Sea un estado $|\psi\rangle$ que expresado en la base ortonormal $|\varphi_j\rangle$ tiene el desarrollo:

$$|\psi\rangle = \sum_j \alpha_j |\varphi_j\rangle .$$

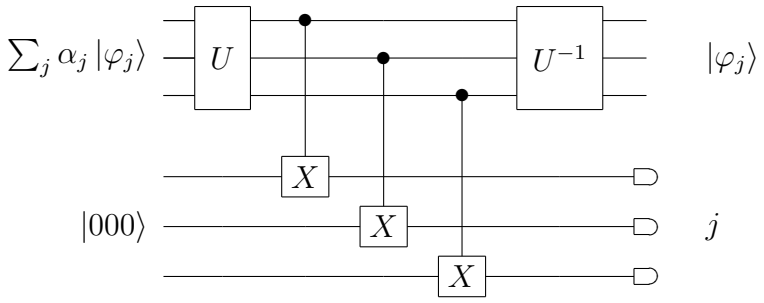
Una medición de Von Neumann de $|\psi\rangle$ con respecto a la base $\{|\varphi_j\rangle\}$ dará como resultado 'j' y el estado quedará en $|\varphi_j\rangle$ con probabilidad $|\alpha_j|^2$.
Se puede usar un circuito cuántico para registrar la medición de Von Neumann descripta: Primero se construye un circuito que realiza la transformación unitaria:

$$U\,|\varphi_j\rangle = |j\rangle$$

el índice j se supone en n-bit binario y $|j\rangle$ es el estado de la base computacional correspondiente de n-qubits. El operador U hace el cambio de base de la $\{|\varphi_j\rangle\}$ a la computacional. Después del cambio de base se mide el registro $|j\rangle$ en la base computacional. Finalmente se aplica U^{-1} (recorriendo el circuito de U hacia atrás y reemplazando cada compuerta por su inversa). El circuito completo se muestra en la figura



Una alternativa posible en la que no se mide el estado intermedio en la base computacional es la del circuito:

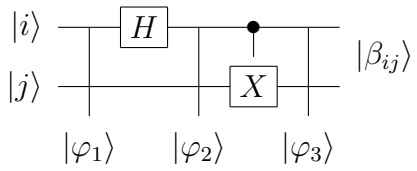


En este circuito se registran los qubits en los cables inferiores que son medidos luego en la base computacional.

Como ejemplo de cambio de base U vamos a considerar la base de 2-qubits:

$$|\beta_{00}\rangle = \tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|11\rangle \qquad |\beta_{01}\rangle = \tfrac{1}{\sqrt{2}}|01\rangle + \tfrac{1}{\sqrt{2}}|10\rangle$$
$$|\beta_{10}\rangle = \tfrac{1}{\sqrt{2}}|00\rangle - \tfrac{1}{\sqrt{2}}|11\rangle \qquad |\beta_{11}\rangle = \tfrac{1}{\sqrt{2}}|01\rangle - \tfrac{1}{\sqrt{2}}|10\rangle$$

Esta base se conoce como *base de Bell* y sus estados como *estados de Bell* (tambien llamados *pares EPR*). Son muy usados en computación cuántica. Un circuito que realiza el cambio de base de la base computacional a la de Bell se muestra en la figura:



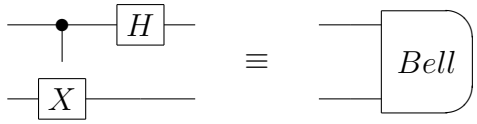
Para verificar ésto supongamos que la entrada sea el estado de la base computacional $|\varphi_1\rangle = |00\rangle$. Despues de la compuerta de Hadamard, el estado es:

$$\begin{aligned} |\varphi_2\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle \\ &= \tfrac{1}{\sqrt{2}}(|00\rangle + |01\rangle). \end{aligned}$$

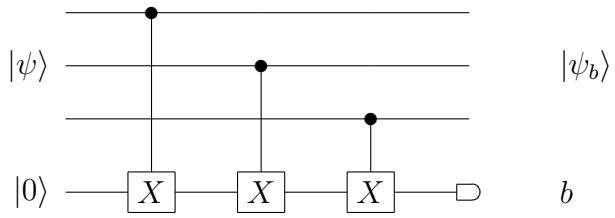
Note que el orden de los qubits se ha mantenido. Luego la compuerta control-NOT transforma este estado en:

$$|\varphi_3\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

O sea que $|\varphi_3\rangle = |\beta_{00}\rangle$. Se puede verificar de la misma forma que los otros estados de la base computacional $|01\rangle$, $|10\rangle$ y $|11\rangle$ son transformados en $|\beta_{01}\rangle$, $|\beta_{10}\rangle$ y $|\beta_{11}\rangle$ respectivamente.
Para realizar una *medición de Bell* (medición de Von Neumann respecto a la base de Bell), se puede aplicar el circuito de la Figura anterior en sentido inverso, medir en la base computacional y luego aplicar el mismo circuito en directa. Si sólo importa la salida clásica de la medición, indicada por 2 bits 00, 10, 01 o 11, entonces no hay necesidad de hacer el cambio de base a la de Bell despues de la medición y con el circuito siguiente alcanza



Finalmente veremos un ejemplo de una medición proyectiva incompleta, la medición de paridad. Los proyectores de paridad P_0 y P_1 ya fueron definidos antes. Cualquier estado de entrada $|\psi\rangle = \sum_x \beta_x |x\rangle$ se puede expresar como $|\psi\rangle = \alpha_0 |\psi_0\rangle + \alpha_1 |\psi_1\rangle$, donde $\alpha_i = \sqrt{\langle\psi|P_i|\psi\rangle}$ y $|\psi_i\rangle = \frac{P_i|\psi\rangle}{\alpha_i}$. Una medición de paridad resultará 0 y el estado $|\psi_0\rangle$ con probabilidad $|\alpha_0|^2$ o 1 y el estado $|\psi_1\rangle$ con probabilidad $|\alpha_1|^2$.
Un circuito que calcula la paridad de estados de 3 qubits es



La medición de cada uno de los 3 qubits por medio de las compuertas Control-NOT producirá el estado $|\psi_b\rangle$ como estado de salida con probabilidad $|\alpha_b|^2$ con $b = 0, 1$.
Es importante señalar la diferencia con una medición completa de Von Neumann seguida por una medición de paridad. La medición proyectiva de paridad mide *solamente* la paridad de las secuencias de bits del estado, dejando el sistema en $|\psi_0\rangle$ o $|\psi_1\rangle$. Una medición de Von Neumann permite obtener otra información y el sistema quedará en uno de los estados de la base de una determinada paridad en lugar de una superposición de todas las cadenas de caracteres de la misma paridad.