Notas de las charlas introductorias a la Computación Cuántica

Alejandro Díaz-Caro
diazcaro@fceia.unr.edu.ar

Departamento de Ciencias de la Computación
Facultad de Ciencias Exactas, Ingeniería y Agrimensura
Universidad Nacional de Rosario, Argentina

Junio de 2005

a Nache

Prefacio

Estas son las notas de un pequeño curso de cuatro clases dictado en la Universidad Nacional de Rosario de introducción a la Computación Cuántica, realizado entre Mayo y Junio de 2005.

La intención de estas notas es que sirvan como una primera referencia para matemáticos y cientistas de la computación a este facinante mundo. Bajo ninguna circunstancia puede considerarse a estas notas como algo completo, sólo pretenden ayudar a dar los primeros pasos.

Índice general

Capítulo 1

1er día

1.1. Brevísima introducción

1.1.1. El porqué de la computación cuántica

La computación cuántica es un **paradigma de computación** distinto al de la computación clásica.

Se basa en el uso de **qubits** en lugar de bits, y da lugar a nuevas puertas lógicas que hacen posibles nuevos algoritmos.

Una misma tarea puede tener **diferente complejidad** en computación clásica y en computación cuántica, lo que ha dado lugar a una gran expectación, ya que algunos problemas intratables pasan a ser tratables.

1.1.2. Un poco de historia

1936 Alan Turing inventa la MT para demostrar que existían problemas matemáticos que no eran computables.

Ley de Moore ⇒ Disminución en tamaño, mayor poder de cómputo. Sin embargo, los problemas que requieren recursos exponenciales siguen causando problemas.

1982 Richard Feynman sugiere que simular sistemas cuánticos necesariamente requiere recursos exponenciales. Sin embargo la naturaleza es capaz de simularlo de manera eficiente!

1985 David Deutsch describe el primer modelo para una Quantum Turing Machine basada en la utilización de datos y control cuánticos.

1993 Charles Bennett y otros científicos de IBM diseñaron el experimento de Teleportación.

1994 Peter Shor describe un algoritmo cuántico para factorizar números que es exponencialmente más rápido que cualquier algoritmo clásico conocido. El potencial de ese algoritmo atrajo mucha inversión de entes estatales y privados.

1996 Lov K. Grover crea un algoritmo capaz de hacer búsquedas sobre datos desordenados con un orden de complejidad $O(n)$, obteniendo así una aceleración cuadrática para la búsqueda.

1998 Isaac Chuang dirige el grupo de Berkeley que desarrolla la primera computadora cuántica de 1 qubit.

2001 Un grupo de IBM desarrolla una computadora cuántica capaz de controlar 7 qubits, con ella prueban el algoritmo de Shor factorizando el número 15.

1.2. Espacio de Hilbert

1.2.1. Espacio pre-Hilbert

Definición 1 *Sea E un espacio lineal sobre $\mathbb{K}$. Un producto interno definido sobre E es una aplicación $\langle , \rangle : E \times E \to \mathbb{K}$ que verifica ser:*

- *Definida positiva:*
  $\langle x, x\rangle \geq 0, \forall x \in E \ y \ \langle x, x\rangle = 0 \Leftrightarrow x = 0_E$
- *Lineal por derecha:*
  $\langle z, \lambda x + \mu y\rangle = \lambda\langle z, x\rangle + \mu\langle z, y\rangle, \forall x, y, z \in E, \forall \lambda, \mu \in \mathbb{K}$
- *Antilineal por izquierda:*
  $\langle \lambda x + \mu y, z\rangle = \overline{\lambda}\langle x, z\rangle + \overline{\mu}\langle y, z\rangle, \forall x, y, z \in E, \forall \lambda, \mu \in \mathbb{K}$

- *Hermítica:*
  $\langle x, y\rangle = \overline{\langle y, x\rangle}, \forall x, y \in E$

Definición 2 *Un espacio pre-Hilbert es Un espacio lineal sobre $\mathbb{K}$ con producto interno.*

Nota 1 *Todo espacio pre-Hilbert es un espacio lineal normado con la norma* $\|x\| = \sqrt{\langle x, x\rangle}$

1.2.2. Espacio de Hilbert

Definición 3 *Sea X_n una sucesión de vectores del espacio V.*

Si $\|X_n - X_m\| \to 0$ cuando $n, m \to \infty$, entonces la sucesión X_n es una sucesión de Cauchy.

O lo que es lo mismo: si $\forall \varepsilon > 0, \exists N \in \mathbb{N} \not/$ si $n, m \geq N, \|X_n - X_m\| < \varepsilon$ entonces la sucesión X_n es una sucesión de Cauchy.

Nota 2 *Esto quiere decir que puedo hacer distar entre sí los términos tan poco como quiera.*

Nota 3 *Toda sucesión convergente es de Cauchy, PERO NO A LA INVERSA.*

Ejemplo 1 *"Una sucesión de Cauchy no convergente"*

Sea F el espacio vectorial de funciones reales $C[0,1]$ con producto interno definido como:

$$\langle f, g\rangle = \int_0^1 f(x)g(x)dx$$

Y sea la sucesión $\{f_n\}$ con

$$f_n(x) = \begin{cases} 1 & si\ 0 \leq x \leq \frac{1}{2} \\ 1 - (x - \frac{1}{2})n & si\ \frac{1}{2} < x < \frac{1}{2} + \frac{1}{n} \\ 0 & si\ \frac{1}{2} + \frac{1}{n} \leq x \leq 1 \end{cases}$$

$\{f_n\}$ es una sucesión de Cauchy, ya que

$$\|f_n - f_m\|^2 = \langle f_n - f_m, f_n - f_m\rangle =$$

$$= \int_0^1 |\,(f_n - f_m)(x)\,|^2 dx = \int_{\frac{1}{2}}^{\frac{1}{2}+max\{\frac{1}{n},\frac{1}{m}\}} |\,(f_n - f_m)(x)\,|^2 dx \leq \varepsilon$$

Pero $\{f_n\}$ no converge, ya que cuando $n \to \infty$, esta sucesión tiende a una función discontinua (y el espacio F es el espacio de funciones continuas en $[0,1]$).

Definición 4 *V es completo para la norma $\|\cdot\|$, si y sólo si toda sucesión de Cauchy converge.*

Definición 5 *Un espacio pre-Hilbert completo en su norma se denomina **espacio de Hilbert**.*

1.3. Productos tensoriales

Definición 6 *El producto tensorial de dos matrices, P de orden $n \times m$ y Q de orden $k \times l$, se define como la matriz*

$$P \otimes Q = \begin{pmatrix} p_{11}Q & \dots & p_{1m}Q \\ \vdots & & \vdots \\ p_{n1}Q & \dots & p_{nm}Q \end{pmatrix}$$

Definición 7 *En particular, tomando las matrices P de orden $n \times 1$ y Q de orden $k \times 1$, obtengo el producto tensorial entre vectores.*

Ejemplo 2

$$P \otimes Q = \begin{pmatrix} p_{11} \begin{pmatrix} q_{11} \\ \vdots \\ q_{1k} \end{pmatrix} \\ \vdots \\ p_{1m} \begin{pmatrix} q_{11} \\ \vdots \\ q_{1k} \end{pmatrix} \end{pmatrix}$$

Definición 8 *El producto tensorial de espacios vectoriales se define como sigue.*

Sea $B_1 = \{e_i\}, i = 1, \ldots, dim(E)$ *una base de* E, *y* $B_2 = \{f_j\}, j = 1, \ldots, dim(F)$ *una base de* F, *entonces, el producto tensorial de* B_1 *y* B_2 *es una nueva base, y el espacio generado por ella es el espacio* $E \otimes F$.

En símbolos: $B_1 \otimes B_2 = B_3$ *y* $\mathfrak{L}\{B_3\} = E \otimes F$.

por ejemplo: $B_1 = \{v_1, v_2\}$, $B_2 = \{u_1, u_1\}$ *entonces*

$B_3 = \{v_1 \otimes u_1, v_1 \otimes u_2, v_2 \otimes u_1, v_2 \otimes u_2\}$

1.3.1. Una propiedad del espacio $E \otimes F$

Existen vectores de $E \otimes F$ que no son producto tensorial entre uno de E y uno de F

Ejemplo 3

$$v = \begin{pmatrix} \alpha \\ 0 \\ 0 \\ \beta \end{pmatrix} \quad con\ \alpha, \beta \neq 0$$

Demostración:

Supongamos que existen dos vectores, tales que el producto tensorial es igual a v, *entonces:*

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \\ 0 \\ \beta \end{pmatrix} \Rightarrow \begin{cases} ac = \alpha \\ ad = 0 \\ bc = 0 \\ bd = \beta \end{cases}$$

y este es un sistema que no tiene solución.

1.4. Ejemplo de Notación de Dirac

Definamos

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Y ahora podemos considerar las combinaciones lineales de $|0\rangle$ y $|1\rangle$ de la siguiente manera:

$$\alpha\,|0\rangle + \beta\,|1\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Entonces, podemos escribir cualquier vector columna de dos dimensiones como una combinación lineal de $|0\rangle$ y $|1\rangle$

En general, puedo definir cosas como

$$|+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \qquad |-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

y como estos son dos vectores ortogonales (por ende, forman una base), ahora puedo escribir cualquier vector como combinación lineal de $|+\rangle$ y $|-\rangle$.

Por ejemplo:

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle = \frac{1}{\sqrt{2}}(\alpha+\beta)\,|+\rangle + \frac{1}{\sqrt{2}}(\alpha-\beta)\,|-\rangle$$

Capítulo 2

2do día

2.1. Notación de Dirac

Nota 4 *Consideraremos de aquí en más, excepto que se indique lo contrario, el espacio complejo de dimensión N, $\mathbb{C}^N$.*

Definición 9 *Llamamos "Ket" a un vector de la forma*

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_N \end{pmatrix}$$

y "Bra" a un vector de la forma

$$\langle\psi| = (\alpha_1^*, \ldots, \alpha_N^*)$$

donde $\alpha_i \in \mathbb{C}$ y α_i^* denota el conjugado de α_i.

Nota 5 *Además, $|\lambda_1\psi_1 + \lambda_2\psi_2\rangle = \lambda_1 |\psi_1\rangle + \lambda_2 |\psi_2\rangle$.*

A partir de esta definición, podemos llamar "braket" a la siguiente operación

$$\langle\psi|\phi\rangle = (\alpha_1^*, \ldots, \alpha_N^*) \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_N \end{pmatrix} = a \in \mathbb{C}$$

Proposición 1 *La operación braket define un producto interno en el espacio de Hilbert* $\mathbb{C}^N$

Demostración:

Definida positiva:

$$\langle\psi|\psi\rangle = \sum_{i=1}^{N} |\alpha_i|^2 \geq 0$$

Lineal por derecha:

$$\langle\psi|\lambda_1\phi_1 + \lambda_2\phi_2\rangle = \lambda_1\langle\psi|\phi_1\rangle + \lambda_2\langle\psi|\phi_2\rangle$$

Antilineal por izquierda:

$$\langle\lambda_1\psi_1 + \lambda_2\psi_2|\phi\rangle = \lambda_1^*\langle\psi_1|\phi\rangle + \lambda_2^*\langle\psi_2|\phi\rangle$$

Hermítica:

$$\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*$$

Definición 10 *Dado un conjunto* $B = \{|u_i\rangle\}_N$*, se dice que* B *es una base ortonormal de* $\mathbb{C}^N$ *sii*

$$\langle u_i|u_j\rangle = \delta_{ij}$$

Entonces, todo Ket $|\psi\rangle$ se puede expresar como

$$|\psi\rangle = \sum_{i=1}^{N} a_i\,|u_i\rangle$$

además, puedo decir que $a_i = \langle u_i|\psi\rangle \in \mathbb{C}$ ya que

$$\langle u_i|\psi\rangle = \langle u_i|\sum_{j=1}^{N} a_j\,|u_j\rangle = \sum_{j=1}^{N} a_j \underbrace{\langle u_i|u_j\rangle}_{\delta_{ij}} = a_i$$

Definición 11 *La base ortonormal* $B = \{|u_i\rangle\}_N$ *cumple con la siguiente "condición de clausura"*

$$\sum_{i=1}^{N} |u_i\rangle\,\langle u_i| = I$$

ya que

$$\left(\sum_{i=1}^{N} |u_i\rangle \langle u_i|\right) |\psi\rangle = \left(\sum_{i=1}^{N} |u_i\rangle \langle u_i|\right) \left(\sum_{j=1}^{N} a_j |u_i\rangle\right)$$

$$= \sum_{i,j=1}^{N} a_j |u_i\rangle \underbrace{\langle u_i|u_j\rangle}_{\delta_{ij}} = \sum_{i=1}^{N} a_i |u_i\rangle = |\psi\rangle$$

además, a todo Bra $\langle\phi|$ lo puedo escribir como

$$\langle\phi| = \sum_{i=1}^{N} b_i^* \langle u_i|$$

y se puede ver que $b_i^* = \langle\phi|u_i\rangle \in \mathbb{C}$ ya que

$$\langle\phi| = \langle\phi| \underbrace{\left[\sum_{i=1}^{N} |u_i\rangle \langle u_i|\right]}_{I} = \sum_{i=1}^{N} \langle\phi|u_i\rangle \langle u_i| \Rightarrow b_i^* = \langle\phi|u_i\rangle$$

De aquí en más, nos referiremos sólo a los vectores normalizados (con norma 1) de $\mathbb{C}^N$, esto es

$$1 = \|\psi\|^2 = \langle\psi|\psi\rangle = \left(\sum_{j=1}^{N} a_j^* \langle u_j|\right) \left(\sum_{i=1}^{N} a_i |u_i\rangle\right) =$$

$$\sum_{i,j=1}^{N} a_j^* a_i \underbrace{\langle u_j|u_i\rangle}_{\delta_{ij}} = \sum_{i=1}^{N} |a_i|^2 = 1$$

2.2. Representación de Operadores

Un operador A es una matriz de la forma

$$A = \left(\underbrace{\sum_{i=1}^{N} |u_i\rangle \langle u_i|}_{I}\right) A \left(\underbrace{\sum_{j=1}^{N} |u_j\rangle \langle u_j|}_{I}\right) =$$

$$\sum_{i,j=1}^{N} |u_i\rangle \underbrace{\langle u_i| \overbrace{A\,|u_j\rangle}^{|-\rangle}}_{\alpha_{ij}} \langle u_j| = \sum_{i,j=1}^{N} \alpha_{ij}\,|u_i\rangle\,\langle u_j|$$

entonces, los elementos de matriz de A son $(\alpha_{ij})_N$.
Veamos esto aplicando el operador A a un Ket $|\psi\rangle$ cualquiera

$$A\,|\psi\rangle = \left(\sum_{i,j=1}^{N} \alpha_{ij}\,|u_i\rangle\,\langle u_j|\right)\left(\sum_{k=1}^{N} a_k\,|u_k\rangle\right) =$$

$$\sum_{i,j,k=1}^{N} \alpha_{ij}a_k\,|u_i\rangle \underbrace{\langle u_j|u_k\rangle}_{\delta_{ij}} = \sum_{i,j=1}^{N} \alpha_{ij}a_j\,|u_i\rangle$$

entonces, las componentes del vector $A\,|\psi\rangle$ son

$$b_i = \sum_{j=1}^{N} \alpha_{ij}a_j$$

Viendo esto con la notación matricial (en base canónica) tendremos:

$$\begin{array}{c|c} & \begin{pmatrix} a_1 \\ \vdots \\ a_N \end{pmatrix} \\ \hline \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1N} \\ \vdots & & \vdots \\ \alpha_{N1} & \cdots & \alpha_{NN} \end{pmatrix} & \begin{pmatrix} \sum_{j=1}^{N} \alpha_{1j}a_j \\ \vdots \\ \sum_{j=1}^{N} \alpha_{Nj}a_j \end{pmatrix} \end{array}$$

Definición 12 *El "adjunto" de un operador A se nota por $A^\dagger$ y se define de la siguiente manera*

$$\langle\phi|\,A\,|\psi\rangle^* = \langle\psi|\,A^\dagger\,|\phi\rangle$$

Nota 6 *Recordando que $\alpha_{ij} = \langle u_i|\,A\,|u_j\rangle$ las componentes de $A^\dagger$ son*

$$\alpha^*_{ji} = \langle u_j|\,A\,|u_i\rangle^* = \langle u_i|\,A^\dagger\,|u_j\rangle$$

O sea: $A^\dagger = (A^*)^T$.

Propiedades 1 *Sean A y B operadores de $\mathbb{C}^N$, $\lambda \in \mathbb{C}$ y $|\phi\rangle \in \mathbb{C}^N$*

- $(A^\dagger)^\dagger = A$
- $(A+B)^\dagger = A^\dagger + B^\dagger$
- $(\lambda A)^\dagger = \lambda^* A^\dagger$
- $(AB)^\dagger = B^\dagger A^\dagger$
- $\langle A\phi| = \langle\phi| A^\dagger$

Definición 13 *Al operador $P \equiv |\phi\rangle\langle\phi|$ se le llama "proyector" ya que proyecta ortogonalmente un Ket $|\psi\rangle$ cualquiera sobre el Ket $|\phi\rangle$.*

Veamos:

$$P|\psi\rangle = |\phi\rangle \underbrace{\langle\phi|\psi\rangle}_{c_j \in \mathbb{C}} = c_j |\phi\rangle$$

Definición 14 *El operador A de dice "hermítico" si y sólo si $A = A^\dagger$*

Nota 7 *Si es hermítico, su diagonal debe ser real, ya que $\alpha_{ij} = \alpha_{ji}^* \Rightarrow \alpha_{ii} = \alpha_{ii}^*$*

Definición 15 *El operador U se dice "unitario" si y sólo si $U^\dagger U = UU^\dagger = I$, o lo que es lo mismo $A^\dagger = A^{-1}$*

Propiedades 2 *Para cualquier operador U unitario vale:*

- *U preserva el producto interno, esto es*

$$\langle U\phi|U\psi\rangle = \langle\phi|\underbrace{U^\dagger U}_{I}|\psi\rangle = \langle\phi|\psi\rangle$$

- *U^{-1} es unitario.*
- *Si $\{|\psi_i\rangle\}_N$ es base ortonormal, entonces $\{U|\psi_i\rangle\}_N$ también lo es.*

Definición 16 *Un conjunto de matrices $\{M_i\}_k$ se dice que es un "operador de medición" si satisface*

$$\sum_{i=1}^{k} M_i M_i^\dagger = I$$

Un sistema representado por un Ket $|\psi\rangle$ puede evolucionar de dos maneras:

- Por la aplicación de un operador unitario y hermítico U

$$|\phi\rangle \xrightarrow{U} |\psi\rangle$$

$$|\psi\rangle = U\,|\phi\rangle$$

- Por la aplicación de un operador de medición de la siguiente manera:

$$|\phi\rangle \xrightarrow{\{M_i\}_k} |\psi\rangle$$

$$|\psi\rangle = \frac{M_i\,|\phi\rangle}{\sqrt{\langle\phi|\,M_i^\dagger M_i\,|\phi\rangle}} \text{ para algún } 1 \leq i \leq k$$

No puedo saber qué M_i se va a aplicar, sólo su probabilidad que viene dada por la siguiente ley:

$$p(i) = \langle\phi|\,M_i^\dagger M_i\,|\phi\rangle$$

donde $p(i)$ denota la probabilidad que se aplique la matriz M_i

Ejemplo 4 *Sea el siguiente operador medición:*

$$M_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad M_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$M_0 M_0^\dagger + M_1 M_1^\dagger = M_0 + M_1 = I \quad \therefore$ *es un operador de medición.*

Sea $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, entonces, la probabilidad de que en la medición se aplique M_0 es

$$p(0) = \langle\psi|\,M_0^\dagger M_0\,|\psi\rangle = (\alpha^*\langle 0| + \beta^*|1\rangle)M_0(\alpha\,|0\rangle + \beta\,|1\rangle)$$

$$= |\alpha|^2 \underbrace{\langle 0| \overbrace{M_0 |0\rangle}^{|0\rangle}}_{1} + \alpha^*\beta \underbrace{\overbrace{\langle 0| M_0}^{\langle 0|} |1\rangle}_{0} + \alpha\beta^* \underbrace{\langle 1| \overbrace{M_0 |0\rangle}^{|0\rangle}}_{0} + |\beta|^2 \underbrace{\langle 1| \overbrace{M_0 |1\rangle}^{\overline{0}}}_{0} = |\alpha|^2$$

análogamente

$$p(1) = \langle\psi| {M_1}^\dagger M_1 |\psi\rangle = |\beta|^2$$

Notemos que dado que el vector está normalizado:

$$1 = |\alpha|^2 + |\beta|^2 = p(0) + p(1)$$

Ahora veamos a qué evoluciona el sistema. Si se aplicó M_0 obtenemos el sistema en el siguiente estado:

$$\frac{M_0 |\psi\rangle}{\sqrt{\langle\psi| {M_0}^\dagger M_0 |\psi\rangle}} = \frac{M_0 |\psi\rangle}{\sqrt{p(0)}} = \frac{\alpha}{|\alpha|} |0\rangle$$

Notemos que este estado final está normalizado, dado que

$$\left| \frac{\alpha}{|\alpha|} \right|^2 = \frac{|\alpha|^2}{|\alpha|^2} = 1$$

Análogamente si se aplicó M_1 obtenemos

$$\frac{M_1 |\psi\rangle}{\sqrt{p(1)}} = \frac{\beta}{|\beta|} |1\rangle$$

2.3. Qubit y qubits

Definición 17 *Un "qubit" o bit cuántico es un vector normalizado del espacio de Hilbert $\mathbb{C}^2$*

Si considero la base $\{|0\rangle, |1\rangle\}$ de $\mathbb{C}^2$, cualquier qubit puede escribirse

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

con $|\alpha|^2 + |\beta|^2 = 1$.

Definición 18 *Un sistema de N-qubits será un vector del espacio $\bigotimes_{i=1}^{N} \mathbb{C}^2$*

Nota 8 *La base canónica del espacio* $\bigotimes_{i=1}^{N}\mathbb{C}^2$ *es* $\{|0\ldots00\rangle, |0\ldots01\rangle, \ldots, |1\ldots11\rangle\} = \{|i\rangle\}_{i=0,\ldots,2^N-1}$

Un algoritmo cuántico consiste en la evolución de un sistema representado por N-qubits.

A los operadores unitarios hermíticos se les llama "compuertas cuánticas". Las más importantes, por su utilidad en el diseño de algoritmos, son las siguientes:

- La transformación H de Hadamard:

$$\begin{array}{l} H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array} \quad \text{donde:} \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- La identidad I:

$$\begin{array}{l} I|0\rangle = |0\rangle \\ I|1\rangle = |1\rangle \end{array} \quad \text{donde:} \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- La negación X:

$$\begin{array}{l} X|0\rangle = |1\rangle \\ X|1\rangle = |0\rangle \end{array} \quad \text{donde:} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- El cambio de fase Z:

$$\begin{array}{l} Z|0\rangle = |0\rangle \\ Z|1\rangle = -|1\rangle \end{array} \quad \text{donde:} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- La Controlled-Not $CNOT$:

$$\begin{array}{l} CNOT|0x\rangle = |0x\rangle \\ CNOT|1x\rangle = |1\rangle \otimes X|x\rangle \end{array} \quad \text{donde:} \quad CNOT = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}$$

En particular, las matrices I, X, iXZ y Z son las llamadas "matrices de Pauli"

Capítulo 3

3er día

3.1. Teorema de No-Clonning

Teorema 1 *No existe U, operador unitario y hermítico, tal que para algún $|\varphi\rangle \in \mathbb{C}^N$ y $\forall\, |\psi\rangle \in \mathbb{C}^N$ se cumpla*

$$U\,|\psi\varphi\rangle = |\psi\psi\rangle$$

Antes de proceder a demostrar este teorema, veamos una pequeña propiedad del producto interno "Bra-Ket".

$$\langle ab|cd\rangle = \sum_{i=1}^{N} a_i^* c_i \sum_{j=1}^{N} b_j^* d_j = \langle a|c\rangle\langle b|d\rangle \quad \forall a,b,c,d \in \mathbb{C}^N$$

Ahora si estamos en condición de hacer la demostración.

Supongamos que existe la operación U de la cual se habla en el teorema, entonces, dados cualesquiera $|\psi\rangle\,, |\phi\rangle \in \mathbb{C}^N$ tengo

$$U\,|\psi\varphi\rangle = |\psi\psi\rangle$$

y

$$U\,|\phi\varphi\rangle = |\phi\phi\rangle$$

esto significa que

$$\underbrace{\langle U\psi\varphi|U\phi\varphi\rangle}_{(1)} = \underbrace{\langle\psi\psi|\phi\phi\rangle}_{(2)}$$

Veamos

$$(1) = \langle\psi\varphi|\, U^\dagger U\, |\phi\varphi\rangle = \langle\psi\varphi|\phi\varphi\rangle = \langle\psi|\phi\rangle\, \underbrace{\langle\varphi|\varphi\rangle}_{1} = \langle\psi|\phi\rangle$$

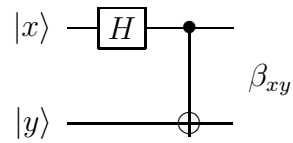
por otro lado

$$(2) = \langle\psi\psi|\phi\phi\rangle = \langle\psi|\phi\rangle\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2$$
$$\therefore \langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2 \Rightarrow \langle\psi|\phi\rangle = 0 \text{ ó} \langle\psi|\phi\rangle = 1$$

No puede ser 0 ya que $|\psi\rangle$ y $|\phi\rangle$ son dos Kets cualesquiera y si es 1 significa que son iguales.

3.2. Estados de Bell

Sea el siguiente circuito cuántico



Veamos qué sucede con cada posible entrada.

- $|00\rangle$

$$|00\rangle \overset{H(1)}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$
$$\overset{CNOT(1,2)}{\longrightarrow} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \beta_{00}$$

- $|01\rangle$

$$|01\rangle \overset{H(1)}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$$
$$\overset{CNOT(1,2)}{\longrightarrow} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \beta_{01}$$

- $|10\rangle$

$$|10\rangle \overset{H(1)}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle)$$
$$\overset{CNOT(1,2)}{\longrightarrow} \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \beta_{10}$$

- $|11\rangle$

$$|11\rangle \overset{H(1)}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|1\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle)$$
$$\overset{CNOT(1,2)}{\longrightarrow} \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \beta_{11}$$

A estos cuatro estados se les llama "Estados de Bell", los cuales son estados entangled de $\mathbb{C}^4$.

A los estados entangled también se les llama estados EPR debido a la paradoja planteada por Einstein, Podolsky y Rosen[4] la cual dice que si tengo un par entangled, por más lejano que tenga un qubit del otro, al efectuar una medición sobre uno de ellos, el otro qubit también colapsará.

Esto se puede apreciar mejor con un pequeño ejemplo.

Ejemplo 5 *Sea el conjunto de matrices* $M = \{M_0, M_1\}$ *donde*

$$M_0 = |0\rangle\langle 0|$$
$$M_1 = |1\rangle\langle 1|$$

por la condición de clausura de las bases (tomando en cuenta la base canónica de $\mathbb{C}^2$*), se cumple*

$$\sum_{i=0}^{1} M_i^\dagger M_i = \sum_{i=0}^{1} M_i = I$$

$\therefore$ *el conjunto* M *es un operador de medición.*

Apliquemos este operador al primer qubit del estado β_{00} *y veamos los resultados posibles. Si se aplica* M_0 *(el cual lo expresamos como* $M_0 \otimes I$ *para que se aplique* M_0 *al primer qubit y la identidad al segundo), el estado resultante será*

$$\frac{(M_0 \otimes I)\beta_{00}}{\sqrt{p(0)}}$$

$$= \frac{(|00\rangle\langle 00| + |01\rangle\langle 01|)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)}{\sqrt{\frac{1}{\sqrt{2}}(\langle 00| + \langle 11|)(|00\rangle\langle 00| + |01\rangle\langle 01|)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)}}$$

$$= \frac{\frac{1}{\sqrt{2}}(|00\rangle\langle 00|00\rangle)}{\sqrt{\frac{1}{2}\langle 00|00\rangle\langle 00|00\rangle}} = |00\rangle$$

Análogamente, si se aplica M_1 al primer qubit obtendré $|11\rangle$

Nota 9 *Notemos que* $\beta_{00} = (X \otimes I)\beta_{01} = (Z \otimes I)\beta_{10} = (XZ \otimes I)\beta_{11}$

3.3. Codificación Superdensa

El objetivo de esta técnica es transmitir 2 bits clásicos enviando tan sólo 1 qubit.

Los pasos a seguir por el emisor (a quien llamaremos "Alice") y el receptor (a quien llamaremos "Bob") son los siguientes.

Paso 1. Alice y Bob preparan un estado β_{00}.

Paso 2. Alice se queda con el primer qubit del par y Bob se lleva el segundo.

Paso 3. Alice aplica una transformación a su qubit, de acuerdo a los bits que quiere enviar, siguiendo la siguiente tabla

Bits a enviar	Compuerta a aplicar
00	I
01	X
10	Z
11	ZX

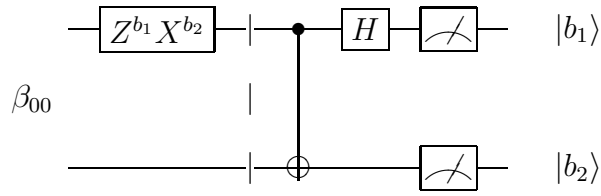
Paso 4. Alice envía su qubit a Bob.

Paso 5. Bob aplica CNOT a los dos elementos del par.

Paso 6. Bob Aplica Hadamard al primer qubit.

Paso 7. Bob realiza una medición.

El circuito completo queda de la siguiente manera



Ejemplo 6 *Supongamos que queremos enviar los bits* 11*, entonces aplicamos* $(ZX \otimes I)$ *a* β_{00}

$$(ZX \otimes I)\beta_{00} = (Z \otimes I)\left((X \otimes I)\beta_{00}\right)$$

$$= (Z \otimes I)\left((X \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)$$

$$= (Z \otimes I)\left(\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)\right) = \frac{1}{\sqrt{2}}(-|10\rangle + |01\rangle) = \beta_{11}$$

El resto del circuito (a partir de la línea punteada vertical) es el circuito inverso al de Bell, por lo tanto, al final de la medición obtendré el estado $|11\rangle$.

Para enviar cualquier otro par de bits se realiza un desarrollo análogo.

Notar que la aplicación de la compuerta $Z^{b_1}X^{b_2}$ *cambia el estado* β_{00} *a* $\beta_{b_1 b_2}$.

3.4. Teleportación Cuántica

El objetivo de esta técnica es transmitir un qubit mediante el envío de dos bits clásicos.

Los pasos a seguir por Alice y Bob son los siguientes.

Paso 1. Alice y Bob preparan un estado β_{00}.

Paso 2. Alice se queda con el primer qubit del par y Bob se lleva el segundo.

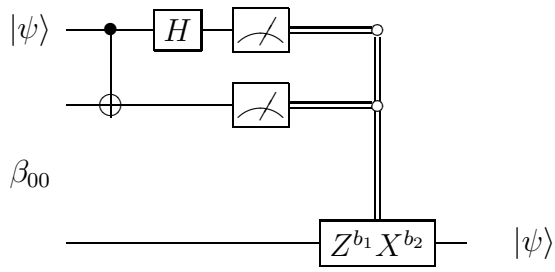
Paso 3. Alice aplica CNOT entre el qubit a transmitir y el primero del par β_{00}.

Paso 4. Alice aplica Hadamard al primero de sus dos qubits, luego realiza una medición sobre ambos y envío el resultado de la medición (2 bits clásicos) a Bob.

Paso 5. Bob aplica una transformación sobre su qubit, de acuerdo a los bits recibidos, basándose en la siguiente tabla

Bits recibidos	Compuerta a aplicar
00	I
01	X
10	Z
11	ZX

El circuito completo queda de la siguiente manera



donde $|\psi\rangle$ es el qubit a teleportar.

Veamos, sea $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, entonces

$$|\psi\rangle \otimes \beta_{00} = (\alpha|0\rangle + \beta|1\rangle)\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)$$

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

$$\xrightarrow{CNOT(1,2)} \frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle))$$

$$\xrightarrow{H(1)} \frac{1}{\sqrt{2}}\left(\alpha\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\right)$$

$$
\begin{aligned}
&= \frac{1}{2}\left[|00\rangle\left(\alpha|0\rangle + \beta|1\rangle\right)\right. \\
&\quad + |01\rangle\left(\alpha|1\rangle + \beta|0\rangle\right) \\
&\quad + |10\rangle\left(\alpha|0\rangle - \beta|1\rangle\right) \\
&\quad \left. + |11\rangle\left(\alpha|1\rangle - \beta|0\rangle\right)\right]
\end{aligned}
$$

$$
= \frac{1}{2}\sum_{b_1 b_2=0}^{1} |b_1 b_2\rangle \left(X^{b_2} Z^{b_1}\right)|\psi\rangle
$$

Por lo tanto, aplicando $Z^{b_1}X^{b_2}$ Bob obtendrá el estado original $|\psi\rangle$.

Nota 10 *Si a la compuerta* —[$Z^{b_1}X^{b_2}$]— *quiero escribirla como dos compuertas, debo hacerlo como* —[X^{b_2}]—[Z^{b_1}]—*, ya que primero se aplicará la matriz* X^{b_2} *y luego* Z^{b_1}.

3.5. Paralelismo Cuántico

Consideremos una función $f : \{0,1\} \to \{0,1\}$. Si en una computadora clásica quiero evaluar esta función. debo hacer el cálculo para todas las entradas posibles ($f(0)$ y $f(1)$, en este caso).

Consideremos ahora una compuerta cuántica U_f de $\mathbb{C}^4$ tal que

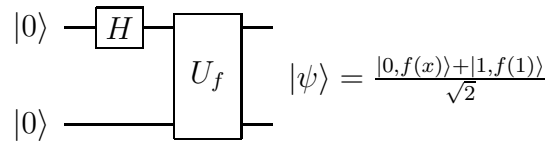
$$U_f\,|x,y\rangle = |x, y \oplus f(x)\rangle$$

donde $\oplus$ simboliza la suma módulo 2.

Por la definición anterior tenemos que

$$U_f\,|x,0\rangle = |x, f(x)\rangle$$

Ahora consideremos el siguiente circuito



Veamos

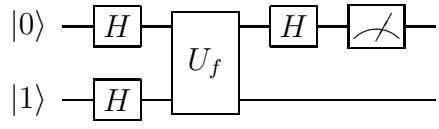
$$|00\rangle \overset{H(1)}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

$$\overset{U_f}{\longrightarrow} \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle)$$

La salida de este circuito me da un estado que es superposición de todos los resultados posibles de la aplicación de la función f. En principio esta no sería una idea muy práctica, ya que no puedo saber un valor particular de f.

3.5.1. Algoritmo de Deutsch

El objetivo de este algoritmo es saber si una función es constante.
Representamos el algoritmo con el siguiente circuito



$$|01\rangle \overset{H(1,2)}{\longrightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |x\rangle\,\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

donde $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

Veamos qué sucede con la aplicación de la compuerta U_f para cada una de las posibilidades

$$U_f\,|x, 0\rangle = \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle)$$
$$U_f\,|x, 1\rangle = \frac{1}{\sqrt{2}}(|0, 1 \oplus f(0)\rangle + |1, 1 \oplus f(1)\rangle)$$

por lo tanto

$$U_f\,|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}U_f(|x, 0\rangle - |x, 1\rangle) = \frac{1}{\sqrt{2}}\,(U_f\,|x, 0\rangle - U_f\,|x, 1\rangle)$$

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

$$= \frac{1}{2} \left(|0, f(0)\rangle + |1, f(1)\rangle - |0, 1 \oplus f(0)\rangle - |1, 1 \oplus f(1)\rangle \right)$$

Entonces, si $f(0) \neq f(1)$

$$= \pm \frac{1}{2} \left(|00\rangle + |11\rangle - |01\rangle - |10\rangle \right) = \pm \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

y si $f(0) = f(1)$

$$= \pm \frac{1}{2} \left(|00\rangle + |10\rangle - |01\rangle - |11\rangle \right) = \pm \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Luego, aplico la última compuerta Hadamard y obtengo

$$\text{Si } f(0) = f(1) \xrightarrow{H(1)} \pm |0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$
$$\text{Si } f(0) \neq f(1) \xrightarrow{H(1)} \pm |1\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

Por lo tanto, uniendo las salidas posibles tengo

$$\pm |f(0) \oplus f(1)\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

Entonces, midiendo el primer qubit puedo saber si los valores de f son iguales o distintos entre sí.

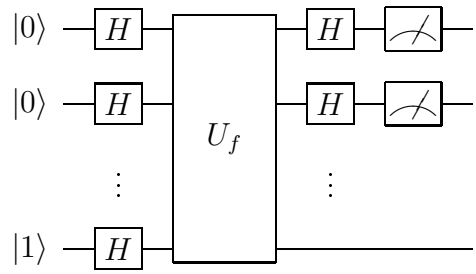
Hasta aquí no obtuve demasiada "ganancia" con respecto a un algoritmo clásico, ya que clásicamente me bastaba con 3 operaciones (evaluar la función en las 2 entradas posibles y compararlas).

Veamos una modificación a este algoritmo que nos dará la verdadera "ganancia" con respecto a su contrapartida clásica.

3.5.2. Algoritmo de Deutsch-Jotza

Este algoritmo es una generalización del anterior. Supongamos que tengo una función f que toma n bits y devuelve 0 ó 1 y quiero saber si es constante o si devuelve 0 para la mitad de las entradas posibles y 1 para la otra mitad.

Consideremos el siguiente circuito



La entrada de este algoritmo es $|0\rangle^{\otimes n}|1\rangle = |0\ldots01\rangle$. Aplicando las $n+1$ compuertas Hadamard sobre la entrada, obtengo

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)=\sum_{\overline{x}\in\{0,1\}^n}\frac{|\overline{x}\rangle}{\sqrt{2^n}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

Aquí la compuerta U_f será una generalización del caso anterior y se comportará de la siguiente manera

$$U_f|\overline{x},y\rangle = |\overline{x},y\oplus f(\overline{x})\rangle$$

entonces

$$U_f|\overline{x},0\rangle = |\overline{x},f(\overline{x})\rangle$$

y

$$U_f|\overline{x},1\rangle = |\overline{x},1\oplus f(\overline{x})\rangle$$

Por lo tanto

$$U_f\left(\sum_{\overline{x}\in\{0,1\}^n}\frac{|\overline{x}\rangle}{\sqrt{2^n}}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\right)=$$

$$\sum_{\overline{x}\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} U_f \left|\overline{x}\right\rangle \left[\frac{\left|0\right\rangle - \left|1\right\rangle}{\sqrt{2}}\right]$$

$$= \sum_{\overline{x}\in\{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}} \left(U_f \left|\overline{x}, 0\right\rangle - U_f \left|\overline{x}, 1\right\rangle\right) =$$

$$\sum_{\overline{x}\in\{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}} \left(\left|\overline{x}, f(\overline{x})\right\rangle - \left|\overline{x}, 1 \oplus f(\overline{x})\right\rangle\right)$$

$$= \sum_{\overline{x}\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} \left|\overline{x}\right\rangle \left(\frac{\left|f(\overline{x})\right\rangle - \left|1 \oplus f(\overline{x})\right\rangle}{\sqrt{2}}\right)$$

Notemos que

$$\left.\begin{array}{l} H\left|0\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle) \\ H\left|1\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) \end{array}\right\} \Rightarrow H\left|y\right\rangle = \frac{1}{\sqrt{2}} \sum_{z\in\{0,1\}} (-1)^{yz} \left|z\right\rangle$$

por lo tanto

$$H^{\otimes n} \left|\overline{x}\right\rangle = H^{\otimes n} \left|x_1 \ldots x_n\right\rangle$$

$$= \left(\frac{1}{\sqrt{2}} \sum_{z_1\in\{0,1\}} (-1)^{x_1 z_1} \left|z_1\right\rangle\right) \cdots \left(\frac{1}{\sqrt{2}} \sum_{z_n\in\{0,1\}} (-1)^{x_n z_n} \left|z_n\right\rangle\right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{\overline{z}\in\{0,1\}^n} (-1)^{\overline{x}\cdot\overline{z}} \left|\overline{z}\right\rangle$$

donde $\overline{x} \cdot \overline{z} = x_1 z_1 + \ldots + x_n z_n$.

Ahora sí, apliquemos las n compuertas Hadamard restantes

$$\begin{array}{c} H(1,\ldots,n) \\ \longrightarrow \end{array} \sum_{\overline{x}\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} \left(\frac{1}{\sqrt{2^n}} \sum_{\overline{z}\in\{0,1\}^n} (-1)^{\overline{x}\cdot\overline{z}} \left|\overline{z}\right\rangle\right) \left(\frac{\left|f(\overline{x})\right\rangle - \left|1 \oplus f(\overline{x})\right\rangle}{\sqrt{2}}\right)$$

$$= \sum_{\overline{x}\in\{0,1\}^n} \sum_{\overline{z}\in\{0,1\}^n} \frac{(-1)^{\overline{x}\cdot\overline{z}} |\overline{z}\rangle}{2^n} \left(\frac{|f(\overline{x})\rangle - |1 \oplus f(\overline{x})\rangle}{\sqrt{2}} \right)$$

Analicemos este resultado.

- Si f es constante

$$= \pm \sum_{\overline{x}\in\{0,1\}^n} \sum_{\overline{z}\in\{0,1\}^n} \frac{(-1)^{\overline{x}\cdot\overline{z}} |\overline{z}\rangle}{2^n} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

  Y en los términos en que $\overline{z} = 0$, los primeros n qubits son

$$\pm \sum_{\overline{x}\in\{0,1\}^n} \frac{|0\rangle^{\otimes n}}{2^n} = \pm \frac{2^n}{2^n} |0\rangle^{\otimes n} = \pm |0\rangle^{\otimes n}$$

  por lo tanto los términos en que $\overline{z} \neq 0$ se deberán anular por la condición de normalidad, quedando el resultado

$$\pm |0\rangle^{\otimes n} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

  lo que nos dice que si medimos los primeros n qubits obtendremos $|0\rangle^{\otimes n}$.

- Si f no es constante (50 % de las veces devuelve 0 y 50 % devuelve 1), entonces para $\overline{z} = 0$

$$\sum_{\overline{x}\in\{0,1\}^n} \frac{|0\rangle^{\otimes n}}{2^n} \left(\frac{|f(\overline{x})\rangle - |1 \oplus f(\overline{x})\rangle}{\sqrt{2}} \right) =$$

$$\sum_{\overline{x}\in\{0,1\}^n} (-1)^{\overline{x}} \frac{|0\rangle^{\otimes n}}{2^n} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = 0$$

  por lo tanto al realizar la medición de los primeros n qubits obtendré algo distinto de $|0\rangle^{\otimes n}$.

Conclusión: Si obtengo $|0\rangle^{\otimes n}$ a la salida de la medición, la función es constante, en otro caso la función es balanceada.

Capítulo 4

4to día

4.1. Algoritmo de Búsqueda de Grover

4.1.1. Oráculo

Consideremos la compuerta U_f,

$$U_f |x, b\rangle = |x, b \oplus f(x)\rangle$$

Si tomamos $b = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, entonces

$$U_f |x, b\rangle = U_f \left[|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right] = \frac{1}{\sqrt{2}} \left[U_f |x, 0\rangle - U_f |x, 1\rangle \right]$$

$$= \frac{1}{\sqrt{2}}(|x, f(x)\rangle - |x, 1 \oplus f(x)\rangle) = |x\rangle \frac{1}{\sqrt{2}}(|x, f(x)\rangle - |x, 1 \oplus f(x)\rangle)$$

$$= (-1)^{f(x)} |x, b\rangle$$

Notemos que U_f no modifica el estado b, por lo tanto podemos omitirlo y referirnos a esta transformación como

$$U |x\rangle = (-1)^{f(x)} |x\rangle$$

a la cual se le llama "Oráculo".

4.1.2. Inversión sobre el promedio

Sea el estado $|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$. Definimos la transformación "Inversión sobre el promedio" como $G = 2\,|\phi\rangle\,\langle\phi| - I$. Entonces

$$G = 2\,|\phi\rangle\,\langle\phi| - I = 2 \begin{pmatrix} \frac{1}{\sqrt{2^n}} \\ \vdots \\ \frac{1}{\sqrt{2^n}} \end{pmatrix}_{2^n} \left(\frac{1}{\sqrt{2^n}} \cdots \frac{1}{\sqrt{2^n}} \right)_{2^n} - I$$

$$= \begin{pmatrix} \frac{2}{2^n} - 1 & \frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \frac{2}{2^n} & \frac{2}{2^n} - 1 & \cdots & \frac{2}{2^n} \\ \vdots & \vdots & & \vdots \\ \frac{2}{2^n} & \frac{2}{2^n} & \cdots & \frac{2}{2^n} - 1 \end{pmatrix}_{2^n \times 2^n}$$

Veamos cómo actúa G sobre un estado cualquiera. Consideremos el estado $|\psi\rangle = \sum_{x\in\{0,1\}^n} a_x\,|x\rangle$, entonces

$G\,\lvert\psi\rangle$	$\begin{pmatrix} a_0 \\ \vdots \\ a_{2^n-1} \end{pmatrix}$
$\begin{pmatrix} \frac{2}{2^n} - 1 & \cdots & \frac{2}{2^n} \\ \vdots & & \vdots \\ \frac{2}{2^n} & \cdots & \frac{2}{2^n} - 1 \end{pmatrix}$	$\begin{pmatrix} \left(\sum_{x\in\{0,1\}^n} \frac{2a_x}{2^n} \right) - a_0 \\ \vdots \\ \left(\sum_{x\in\{0,1\}^n} \frac{2a_x}{2^n} \right) - a_{2^n-1} \end{pmatrix}$

O sea,

$$\sum_{x\in\{0,1\}^n} a_x\,|x\rangle \xrightarrow{G} \sum_{x\in\{0,1\}^n} \left[\left(\sum_{y\in\{0,1\}^n} \frac{2a_y}{2^n} \right) - a_x \right] |x\rangle$$

$$= \sum_{x\in\{0,1\}^n} (2A - a_x)\,|x\rangle$$

donde A es el promedio de los a_x.

4.1.3. El algoritmo

Partimos de una lista de tamaño N. Supondremos, incrementando la lista si es necesario, que $N = 2^n$ para algún n. Trabajaremos con los índices de los elementos de la lista, es decir con $x = 0 \dots 2^n - 1$ y queremos localizar el x_0 tal que $f(x_0) = 1$ para cierta función booleana f.

El input de nuestro circuito será $|0\rangle^{\otimes n}$.

Paso 1: Aplicamos $H^{\otimes n}$

$$|0\rangle^{\otimes n} \overset{H^{\otimes n}}{\longrightarrow} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle = |\psi_1\rangle$$

Aquí tenemos todos los registros de la lista representados. La idea es subir la probabilidad de que al medir este estado, obtengamos el elemento x_0.

Paso 2: Aplicamos el oráculo

$$|\psi_1\rangle \overset{U}{\longrightarrow} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle = |\psi_2\rangle$$

Paso 3: Hacemos una inversión sobre el promedio

$$|\psi_2\rangle = \sum_{x\in\{0,1\}^n} \underbrace{\left[\frac{(-1)^{f(x)}}{\sqrt{2^n}}\right]}_{a_x} |x\rangle \overset{G}{\longrightarrow} \sum_{x\in\{0,1\}^n} (2A - a_x) |x\rangle$$

$$= \sum_{x\in\{0,1\}^n} \left[\left(2 \sum_{y\in\{0,1\}^n} \frac{(-1)^{f(y)}}{2^n\sqrt{2^n}}\right) - \frac{(-1)^{f(x)}}{\sqrt{2^n}}\right] |x\rangle$$

$$= \sum_{x\in\{0,1\}^n} \left[\left(2 \sum_{\substack{y\in\{0,1\}^n \\ y\neq x}} \frac{(-1)^{f(y)}}{2^n\sqrt{2^n}}\right) + \frac{2(-1)^{f(x)}}{2^n\sqrt{2^n}} - \frac{(-1)^{f(x)}}{\sqrt{2^n}}\right] |x\rangle$$

$$= \sum_{x\in\{0,1\}^n} \left[\left(2 \sum_{\substack{y\in\{0,1\}^n \\ y\neq x}} \frac{(-1)^{f(y)}}{2^n\sqrt{2^n}} \right) + \frac{2-2^n}{2^n\sqrt{2^n}}(-1)^{f(x)} \right] |x\rangle$$

Analicemos este resultado, el término donde $x = x_0$ ($f(x) = 1$) queda

$$\left[\left(2 \sum_{\substack{y\in\{0,1\}^n \\ y\neq x_0}} \frac{1}{2^n\sqrt{2^n}} \right) + \frac{2^n-2}{2^n\sqrt{2^n}} \right] |x_0\rangle = \left[\frac{2}{2^n\sqrt{2^n}}(2^n-1) + \frac{2^n-2}{2^n\sqrt{2^n}} \right] |x_0\rangle$$

$$= \left[\frac{2^{n+1}+2^n-4}{2^n\sqrt{2^n}} \right] |x_0\rangle$$

y los términos donde $x \neq x_0$ quedan

$$\left[\left(2 \sum_{\substack{y\in\{0,1\}^n \\ y\neq x_0, y\neq x}} \frac{1}{2^n\sqrt{2^n}} \right) + \frac{2(-1)}{2^n\sqrt{2^n}} + \frac{2-2^n}{2^n\sqrt{2^n}} \right] |x_0\rangle$$

$$= \left[\frac{2^{n+1}-2^n-4}{2^n\sqrt{2^n}} \right] |x_0\rangle$$

Como se puede apreciar, el proceso ha cambiado las amplitudes del estado, pasando de todas las amplitudes iguales a un estado donde el resultado que nos interesa tiene mayor amplitud que el resto.

Repitiendo este proceso (pasos 2 y 3) voy levantando la amplitud del estado que queremos obtener tras la medición. Pasado cierto número de repeticiones, esa amplitud vuelve a decrecer (más adelante veremos cómo calcular el número óptimo de repeticiones). Cuando la amplitud de x_0 es máxima realizamos una medición, obteniendo el estado x_0 con la máxima probabilidad.

Ejemplo

Supongamos que tenemos una lista de 16 elementos, de los que sólo uno, al cual denominaremos x_0, verifica la propiedad $f(x_0) = 1$.

Construimos el estado $|0\rangle^{\otimes 4}$ y aplicamos $H^{\otimes 4}$ obteniendo,

$$\frac{1}{4} \sum_{x\in\{0,1\}^4} |x\rangle$$

Inicialmente todas las amplitudes son iguales a $\frac{1}{4}$. Aplicamos el oráculo y obtenemos

$$\frac{1}{4}\sum_{x\in\{0,1\}^4}(-1)^{f(x)}\,|x\rangle$$

Luego, hacemos la inversión de promedio y la nueva amplitud de x_0 será

$$\frac{2^5+2^4-4}{2^4\sqrt{2^4}}=\frac{11}{16}=0{,}6875$$

y para el resto de los x la amplitud será

$$\frac{2^5-2^4-4}{2^4\sqrt{2^4}}=\frac{3}{16}=0{,}1875$$

Si repetimos el proceso obtenemos

Repetición	Amplitud de x_0	Amplitud de $x \neq x_0$	Prob. de error
1	0.6875	0.1875	0.527
2	0.953125	0.078125	0.092
3	0.98046875	-0.05078125	0.039

Si seguimos iterando empieza a subir la probabilidad de error, por lo tanto el número óptimo de iteraciones es 3 y tengo una probabilidad de error de 0,039.

4.1.4. Cálculo del número óptimo de iteraciones

Luego de k iteraciones x_0 tendrá una amplitud b_k y el resto tendrán todos una amplitud m_k. Podemos escribir esto de la forma

$$b_k\,|x_0\rangle + m_k \sum_{\substack{x\in\{0,1\}^n\\ x\neq x_0}} |x\rangle$$

En cada iteración se aplica U, el cual cambia el signo de b_k, y luego G, por lo tanto se cumplen las siguientes ecuaciones recursivas

$$m_0 = b_0 = \frac{1}{\sqrt{2^n}}$$

$$m_{k+1} = 2A_k - m_k$$

$$b_{k+1} = 2A_k + b_k$$

donde

$$A_k = \frac{(2^n - 1)m_k - b_k}{2^n}$$

Se puede demostrar por inducción que las fórmulas cerradas para estas recursiones son

$$m_k = \frac{1}{\sqrt{2^n - 1}} cos((2k+1)\gamma)$$

$$b_k = sen((2k+1)\gamma)$$

donde

$$cos(\gamma) = \sqrt{\frac{2^n - 1}{2^n}}$$

$$sen(\gamma) = \sqrt{\frac{1}{2^n}}$$

Para conseguir la mínima probabilidad de error, debo minimizar $|m_k|$. Y

$$m_k = 0 \Leftrightarrow (2k+1)\gamma = \frac{\pi}{2} \Leftrightarrow k = \frac{\pi}{4\gamma} - \frac{1}{2}$$

Como k debe ser entero, tomamos

$$\tilde{k} = \left\lfloor \frac{\pi}{4\gamma} \right\rfloor$$

Notemos que $|k - \tilde{k}| \leq \frac{1}{2}$, entonces

$$|\frac{\pi}{2} - (2\tilde{k}+1)\gamma| = |(2k+1)\gamma - (2\tilde{k}+1)\gamma| = |2\gamma(k - \tilde{k})| \leq \gamma$$

esto nos servirá para calcular una cota de la probabilidad de error.

La probabilidad de error luego de $\tilde{k}$ iteraciones es

$$(2^n - 1)(m_k)^2 = cos^2((2\tilde{k}+1)\gamma) = sen^2(\frac{\pi}{2} - (2\tilde{k}+1)\gamma) \leq sen^2(\gamma) = \frac{1}{2^n}$$

$\therefore$ La probabilidad obtener un resultado erroneo luego de $\tilde{k}$ iteraciones será menor a $\frac{1}{2^n}$.

En el ejemplo anterior

$$\tilde{k} = \left\lfloor \frac{\pi}{4asen(\sqrt{\frac{1}{16}})} \right\rfloor = 3$$

y la probabilidad de error es $0{,}039 \leq \frac{1}{2^4} = 0{,}0625$.

4.2. Aplicaciones Criptográficas

4.2.1. One-time pad

Este es un método de criptografía clásica[5] que consiste en compartir una secuencia de bits (clave) del largo del mensaje a transmitir y aplicar la operación (reversible) XOR para cifrar y descifrar. (Ver figura 4.1)

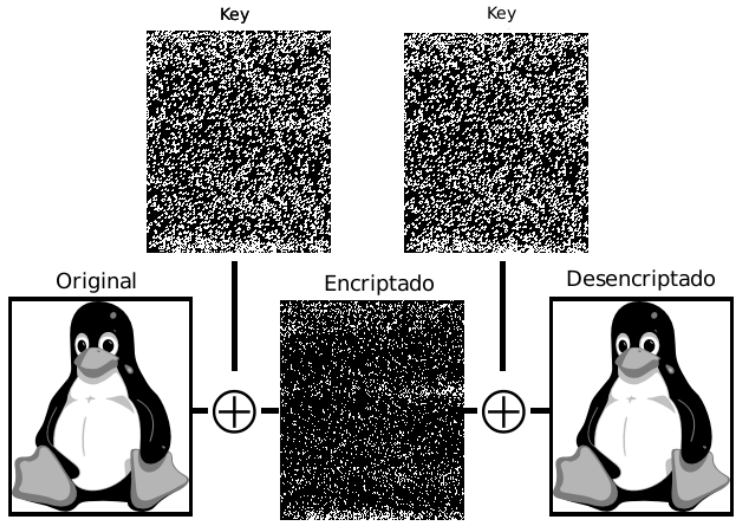


Figura 4.1: One-Time pad

Las claves deben ser 100 % secretas y no deben ser reutilizadas.

El único problema es la predistribución de claves por canales inseguros. Para esto se usa el Criptosistema Cuántico de QKD-BB84 (Quantum Key Distribution - Bennett, Brassard, 1984[6]).

4.2.2. Criptosistema Cuántico QKD-BB84

La idea es transmitir una clave binaria por un canal inseguro.

Para transmitir el bit 0, Alice (el emisor) puede elegir al azar la base $\{|0\rangle, |1\rangle\}$ (a la que llamaremos esquema $+$) y considerar $0 \equiv |0\rangle$, o la base $\{|-\rangle, |+\rangle\}$ (a la que llamaremos esquema $\times$) y considerar $0 \equiv |-\rangle$. Análogamente al bit 1 lo codificamos como $|1\rangle$ en el esquema $+$ o como $|+\rangle$ en el esquema $\times$.

Bob realizará una medición sobre el estado recibido eligiendo al azar entre el esquema $+$ y el esquema $\times$. (ver figura 4.2)

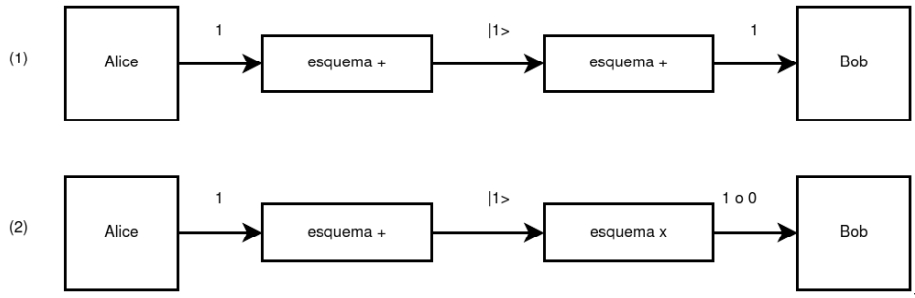


Figura 4.2: Ejemplo: (1) Alice transmite un 1 codificado mediante el esquema $+$ y Bob elije al azar el esquema $+$ obteniendo un 1 (2) si Bob elige el esquema $\times$ obtiene 0 ó 1 con la misma probabilidad.

Veamos paso a paso cómo se realiza el proceso completo de intercambio de claves.

Paso 1: Alice comienza a transmitir una secuencia aleatoria de 0 y 1 alternando los esquemas $+$ y $\times$ en forma aleatoria.

Paso 2: Bob recibe la secuencia y va alternando las mediciones entre los esquemas $+$ y $\times$ al azar.

Paso 3: Alice le transmite a Bob la sucesión de esquemas empleadas.

Paso 4: Bob le informa a Alice en qué casos adivinó el esquema de origen.

Paso 5: Usando solamente los bits de los esquemas idénticos a dos puntas, ambos han definido una sucesión aleatoria de bits que servirá como one-time pad de encriptación para transmisiones futuras por cualquier canal. (ver tabla 4.1)

Paso final: Alice y Bob intercambian hashes de las claves (en bloques) para aceptarla o descartarla.

Cuadro 4.1: Definición de la clave a partir de los esquemas utilizados.

Esquemas de Alice	$\times$	$+$	$+$	$\times$	$\times$	$+$	$\times$	$+$
Valores de Alice	$\|-\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$
Esquemas de Bob	$+$	$\times$	$+$	$\times$	$+$	$+$	$\times$	$\times$
Valores de Bob	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$
Coincidencias			$\surd$	$\surd$		$\surd$	$\surd$	
Clave			0	1		0	0	

Este protocolo es absolutamente inviolable. Supongamos que Cliff espía el canal de comunicación entre Alice y Bob e intenta recuperar la clave. Cliff está en la misma situación que Bob y no conoce cuál esquema es el correcto, $+$ o $\times$. Por lo tanto elige al azar y se equivocará, en promedio, la mitad de las veces.

En el paso 5 Alice y Bob se ponen de acuerdo en cuáles valores tomar en cuenta (las coincidencias de la secuencia de esquemas). Esta información no le sirve de nada a Cliff porque sólo en la mitad de las veces habrá usado el detector correcto, de manera que mal interpretará sus valores finales.

Además el QKD brinda el método para que Alice y Bob puedan detectar el potencial espionaje de Cliff:

Imaginemos que Alice envío un 0 con el esquema $\times$ ($|-\rangle$), Cliff usa el esquema $+$ forzando al qubit a definirse como $|0\rangle$ ó $|1\rangle$. Si Bob usa el esquema $\times$ y mide $|-\rangle$ coincide con lo enviado por Alice, pero si mide $|+\rangle$ Alice y Bob descubrirán esa discrepancia durante el intercambio de hashes, por lo tanto

descartarán el bloque.

Nota: Este método es usado actualmente mediante la polarización de fotones.

Bibliografía

[1] C. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres y W. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. **70**, 1895 (1993).

[2] G. Brassard, *Teleportation as a quantum computation*, Physica D **120**, 43 (1998).

[3] M. Nielsen y I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, (2000).

[4] A. Einstein, B. Podolsky y N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Phys. Rev. **47**, 777 (1935).

[5] G.S. Vernam, *Cipher printing telegraph systems for secret wire and radio*, IEEE, **55**, 109 (1926).

[6] C.H. Bennett y G. Brassard, *Quantum cryptography: public-key distribution and coin tossing*, En IEEE Press, editor, Proc. IEEE Int. Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175 (1984).

[7] M. Nasser-Darwish, *Computación Cuántica*, Tesis de grado, Universidad de La Laguna, España (2004).

[8] E. Rieffel y W. Polak, *An Introduction to Quantum Computing for Non-Physicists*, `e-print quant-ph/9809016` (2000).

[9] G. Blanco y A. Martínez, *Criptografía Cuántica*, En III Jornadas de Matemática Discreta y Algorítmica, Sevilla, España (2002).

[10] V. Martin, *Introducción a la Computación Cuántica*, Technical Report, Facultad de Informática, UPM, España (2000).

[11] A. García-Lopez, *Algoritmo de búsqueda de Grover*, Technical Report 18, UPM (2003).

[12] Grupo de Computación Cuántica, *Introducción al modelo cuántico de computación*, Technical Report 19, UPM (2003).

[13] G. Morales-Luna, *Un poco de computación cuántica: Algoritmos más comunes*, Technical Report, CINVESTAV-IPN, (2003).

[14] D.J. Santos, *Una breve introducción al procesado cuántico de la información*, Technical Report, Universidad de Vigo, (2003).

[15] D. Deutsch, *Quantum theory, the Church-Turing principle and the universal quantum computer*, En Proc. of the Royal Society of London A **400**, 97 (1985).

[16] D. Deutsch y R. Jozsa *Rapid solutions of problems by quantum computation*, En Proc. of the Royal Society of London, 553 (1992).

[17] L. Grover, *A fast quantum mechanical algorithm for database search*, En Proc. of the 28th ACM Symposium on the Theory of Computing, 212 (1996).