
Fundamentos de lenguajes de programación cuántica

Día 1:

~ Introducción a la computación cuántica ~

Alejandro Díaz-Caro

Universidad Nacional de Quilmes

22º Escuela de Verano de Ciencias Informáticas
Río Cuarto, Córdoba – 9 al 14 de febrero de 2015

Un poco de historia

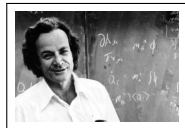
Richard Feynman

First Conference on the Physics of Computation, MIT, 1981

Simulación

- ▶ Física clásica \implies computación clásica
- ▶ Física cuántica \implies ¿computación clásica?

Necesidad de una computadora
cuántica para simular física cuántica



Un poco de historia

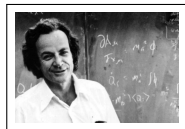
Richard Feynman

First Conference on the Physics of Computation, MIT, 1981

Simulación

- ▶ Física clásica \implies computación clásica
- ▶ Física cuántica \implies ¿computación clásica?

Necesidad de una computadora
cuántica para simular física cuántica



Entre tanto en Rusia...

R. P. Poplavskii

Uspekhi Fizicheskikh Nauk, 115:3, 465–501, 1975

- ▶ Inviabilidad computacional de simular sistemas cuánticos (debido al ppio de superposición)

Yuri I. Manin

Moscow, Sovetskoye Radio, 1980

- ▶ Uso del número exponencial de estados de base
- ▶ Propuesta de teoría de computación cuántica

Un poco de historia (continuación)

Paul Benioff

Journal of Statistical Physics 29 (3):515–546, 1982

- ▶ Primer framework teórico para computación cuántica

Charles Bennett y Gilles Brassard

Int. Conference on Computers, Systems and Signal Processing, EE.UU., 1984

- ▶ BB84: Método de distribución de claves para criptografía

David Deutsch

Proceedings of the Royal Society A 400 (1818):97–117, 1985

- ▶ Máquina de Turing Cuántica: máquina cuántica universal

... Varios hitos históricos omitidos ...

Peter Shor

35th Annual Symposium on Foundations of Computer Science, EE.UU., 1994

- ▶ Algoritmo cuántico para factorizar números primos

Lov Grover

28th Annual ACM Symposium on the Theory of Computing, EE.UU., 1996

- ▶ Algoritmo de búsqueda (con ganancia cuadrática)

Contenido del curso

Lunes y Martes: Introducción a computación cuántica

- ▶ Álgebra
- ▶ Bits cuánticos y operadores
- ▶ Teorema de no-clonado
- ▶ Estados de Bell
- ▶ Codificación superdensa y teleportación cuántica
- ▶ Paralelismo cuántico

Algoritmo de Deutsch, Deutsch-Jozsa, Grover y BB84

Miércoles: Introducción a λ -cálculo y teoría de tipos

Jueves y Viernes: Extensiones a λ -cálculo para computación cuántica

EN EL PIZARRÓN

- ▶ Espacio de Hilbert
- ▶ Producto tensorial
- ▶ Notación bra-ket

Bits cuánticos

Un qubit es. . .

(para un físico)

. . . un sistema cuántico con dos niveles de energía
y que puede ser manipulado arbitrariamente

Bits cuánticos

Un qubit es...

(para un físico)

... un sistema cuántico con dos niveles de energía
y que puede ser manipulado arbitrariamente

pero nosotros no somos físicos...

(para un matemático o informático)

... un vector normalizado del espacio de Hilbert \mathbb{C}^2

Bits cuánticos

Un qubit es...

(para un físico)

... un sistema cuántico con dos niveles de energía y que puede ser manipulado arbitrariamente

pero nosotros no somos físicos...

(para un matemático o informático)

... un vector normalizado del espacio de Hilbert \mathbb{C}^2

n-qubits: un vector de $\bigotimes_{i=1}^n \mathbb{C}^2 = \mathbb{C}^{2^n}$

EN EL PIZARRÓN

- ▶ Operador
- ▶ Adjunto y propiedades
- ▶ Proyector
- ▶ Operador hermítico
- ▶ Operador unitario
- ▶ Operador de medición
- ▶ Compuertas cuánticas
- ▶ Evolución

Compuertas más comunes y operadores de Pauli

Hadamard	$H 0\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$ $H 1\rangle = \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$ <hr/> $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	Identidad	$I 0\rangle = 0\rangle$ $I 1\rangle = 1\rangle$ <hr/> $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Negación	$X 0\rangle = 1\rangle$ $X 1\rangle = 0\rangle$ <hr/> $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	Cambio de fase	$Z 0\rangle = 0\rangle$ $Z 1\rangle = - 1\rangle$ <hr/> $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
No-controlada	$CNOT 0x\rangle = 0x\rangle$ $CNOT 1x\rangle = 1\rangle \otimes X x\rangle$ <hr/> $CNOT = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}$	Matrices de Pauli	$I \quad X$ $iXZ \quad Z$

Teorema de no-clonado

Teorema (No clonado)

No existe ninguna compuerta cuántica U tal que para algún $|\phi\rangle \in \mathbb{C}^N$ y para todo $|\psi\rangle \in \mathbb{C}^N$ se cumpla

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

Es decir...

No existe una máquina universal de clonado

Teorema de no-clonado

Teorema (No clonado)

No existe ninguna compuerta cuántica U tal que para algún $|\phi\rangle \in \mathbb{C}^N$ y para todo $|\psi\rangle \in \mathbb{C}^N$ se cumpla

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

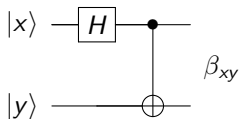
Es decir...

No existe una máquina universal de clonado

o más simplemente

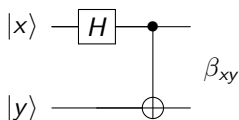
No se puede copiar un qubit desconocido

Estados de Bell



Entrada	Salida
$ 00\rangle$	$\beta_{00} = \frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
$ 01\rangle$	$\beta_{01} = \frac{1}{\sqrt{2}}(01\rangle + 10\rangle)$
$ 10\rangle$	$\beta_{10} = \frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$
$ 11\rangle$	$\beta_{11} = \frac{1}{\sqrt{2}}(01\rangle - 10\rangle)$

Estados de Bell



Entrada	Salida
$ 00\rangle$	$\beta_{00} = \frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
$ 01\rangle$	$\beta_{01} = \frac{1}{\sqrt{2}}(01\rangle + 10\rangle)$
$ 10\rangle$	$\beta_{10} = \frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$
$ 11\rangle$	$\beta_{11} = \frac{1}{\sqrt{2}}(01\rangle - 10\rangle)$

Ejemplo:

$$M = \left\{ \begin{array}{l} M_0 = |0\rangle\langle 0| \\ M_1 = |1\rangle\langle 1| \end{array} \right\}$$

Entonces

$$(M \otimes I)\beta_{00} \begin{cases} \rightarrow |00\rangle \\ \rightarrow |11\rangle \end{cases}$$

Codificación superdensa

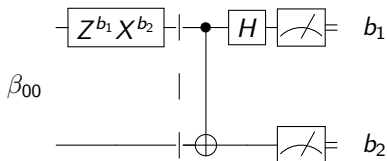
Objetivo:

Transmitir 2 bits clásicos enviando tan sólo 1 qubit

Codificación superdensa

Objetivo:

Transmitir 2 bits clásicos enviando tan sólo 1 qubit



1. A y B preparan β_{00}
2. Se llevan cada uno un qubit
3. A aplica $Z^{b_1} X^{b_2}$ a su qubit
4. A envía su qubit a B
5. B aplica $CNOT$ y H a ambos
6. B mide

Teleportación cuántica

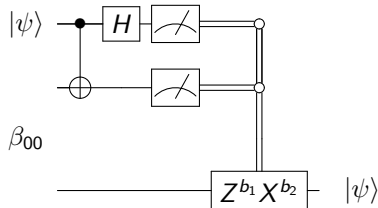
Objetivo:

Transmitir 1 qubit enviando 2 bits clásicos

Teleportación cuántica

Objetivo:

Transmitir 1 qubit enviando 2 bits clásicos



1. A y B preparan β_{00}
2. Se llevan cada uno un qubit
3. A aplica *CNOT* y *H* al qubit a transmitir y el suyo del par
4. A mide y envía el resultado a B
5. B aplica $Z^{b_1} X^{b_2}$ (b_1 y b_2 de A)

Paralelismo cuántico

Primera intuición

$$f : \{0, 1\} \rightarrow \{0, 1\}$$

Resultados posibles: 2

Cantidad de evaluaciones para obtenerlos: 2

Paralelismo cuántico

Primera intuición

$$f : \{0, 1\} \rightarrow \{0, 1\}$$

Resultados posibles: 2

Cantidad de evaluaciones para obtenerlos: 2

Supongamos que existe la siguiente compuerta:

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

Paralelismo cuántico

Primera intuición

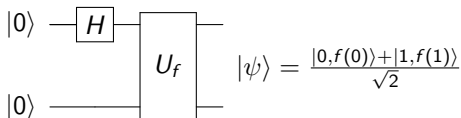
$$f : \{0, 1\} \rightarrow \{0, 1\}$$

Resultados posibles: 2

Cantidad de evaluaciones para obtenerlos: 2

Supongamos que existe la siguiente compuerta:

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



Es decir:

$$|00\rangle \xrightarrow{H(1)} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{U_f} \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle)$$

Cantidad de evaluaciones de U_f para obtener los dos resultados: 1