Procesamiento Cuántico de Datos

Miguel Arizmendi, Gustavo Zabaleta

10 de noviembre de 2016

Sitio web: www3.fi.mdp.edu.ar/fes/ProcQ.html

Introducción

¿Qué es una computadora?

Dispositivo físico para procesar información a través de algoritmos.

¿Algoritmo?

Procedimiento definido para procesar información realizable físicamente.

¿Complejidad?

Cantidad de recursos usados por la computadora para resolver un problema.

TIEMPO Y ESPACIO (Memoria)

Depende de la computadora

Ejemplo: $2n^2 + 3$ y $4n^3 + n + 7$ para dos computadoras distintas. (n unidades de tiempo.)

Introducción

Para abstraerse de los detalles de las máquinas ⇒ Medida gruesa

$O(n^2)$ y $O(n^3)$ cota superior del tiempo requerido. $O(n^2)$ y $O(log(n))$ están en $O(n^3)$.
Algoritmo eficiente si tiene dependencia polinomial: $O(n^k)$
$O(n)$ es lineal y $O(log(n))$ logarítmica
También eficientes.

Tiempo super polinomial o de dependencia exponencial: $O(c^n)$

El tiempo de un algoritmo no puede ser acotado por ninguna polinomial

Introducción

Esta medida gruesa de la Complejidad permite independizarse del modelo de computación.

Por ejemplo, el tiempo que lleva mover la información de un lado a otro es lineal en n y no influye en la relación polinomial versus exponencial.

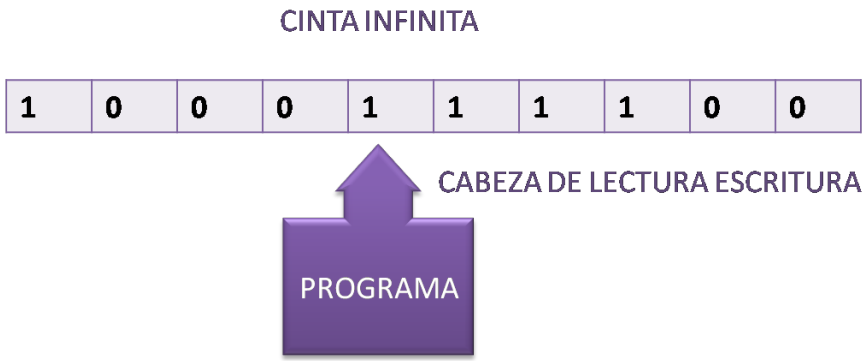
Computadoras

- Habría que dividir el problema de la eficiencia por categorías

Introducción

Tesis de Church-Turing

Todo problema que sea resuelto por una Máquina de Turing puede ser resuelto en cualquier computadora



Tesis de Church-Turing (versión fuerte)

Todo problema resoluble algorítmicamente de forma eficiente puede ser resuelto eficientemente con una Máquina de Turing

Introducción

En los primeros años parecía que las computadoras analógicas podían resolver eficientemente problemas que no tenían solución eficiente en la máquina de Turing. Pero cuando se consideró el ruido en las computadoras analógicas se vió que no eran más eficientes que la de Turing.

¿La Tesis de Turing falla?

El primer obstáculo con el que se encontró la versión fuerte de la tesis de Church Turing fue cuando Solovay y Strassen mostraron que era posible ver con cierta *probabilidad* si un entero es *primo* o no usando números aleatorios. Repitiendo el procedimiento puede acercarse a la certeza en la primalidad. Todavía no se conoce ningún test de primalidad determinístico.

Introducción

Modificación de la Tesis de Church-Turing (versión fuerte)

Todo problema resoluble algorítmicamente de forma eficiente puede ser resuelto eficientemente con una Máquina de Turing *probabilística*

Máquina de Turing *probabilística*

Sería una máquina con un generador aleatorio como una moneda.

¿Es ésto universalmente válido?

Introducción

El problema es que la formulación es clásica y con la física clásica no se puede simular la cuántica.

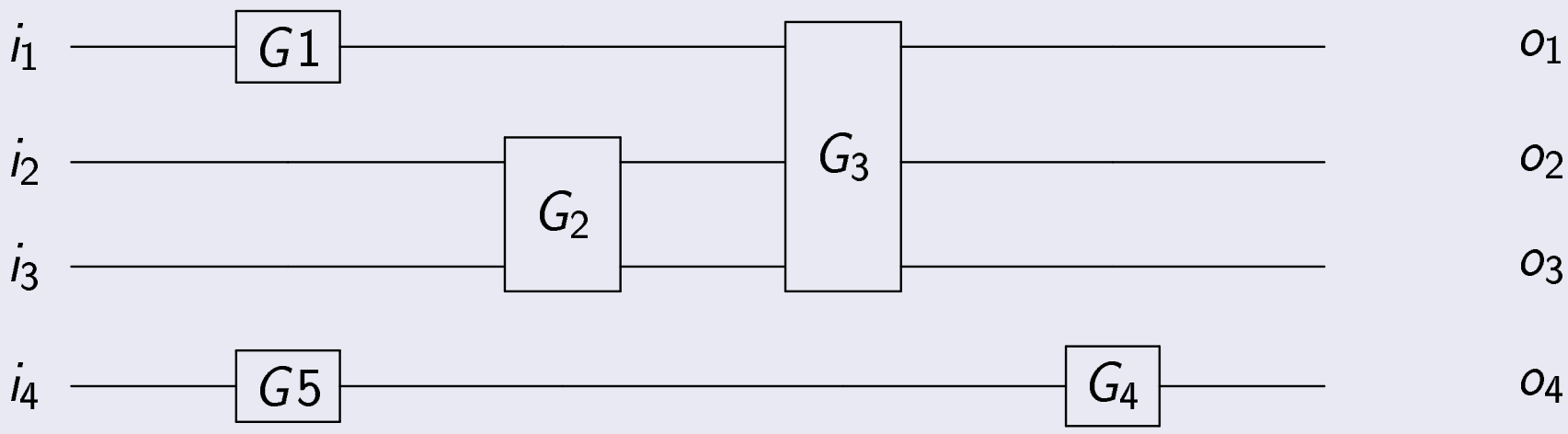
Tesis Cuántica de Church-Turing (versión fuerte)

Todo problema resoluble algorítmicamente de forma eficiente puede ser resuelto eficientemente con una Máquina de Turing cuántica

Si bien la versión clásica está aceptada, la cuántica todavía no.

Modelo de Circuitos

Circuitos de cables que llevan bits a compuertas que realizan operaciones elementales sobre ellos.



Álgebra Lineal para el Modelo de Circuitos

Sea el circuito de la figura anterior y nos dan como dato los valores de las ENTRADAS: $i_1,\ i_2,\ i_3,\ i_4$. Si nos pidieran las SALIDAS, tendríamos que ir siguiendo los bits de izquierda a derecha a medida que pasan por las compuertas en los cables.

Circuito *determinístico*

Para un circuito *determinístico* el estado en cada cable está dado por el valor del bit (0 o 1).

- Un cable con estado 0 en un circuito determinístico se representa por: $\begin{pmatrix}1\\0\end{pmatrix}$ y el de estado 1: $\begin{pmatrix}0\\1\end{pmatrix}$
- Las compuertas serán entonces representadas por *operadores* que actúan sobre los vectores de estado. Por ejemplo:

$$NOT\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix},\qquad NOT\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$$

Álgebra Lineal para el Modelo de Circuitos

La compuerta NOT

$$NOT = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Circuito *probabilístico*

Cada bit podrá estar en 0 con probabilidad p_0 y en 1 con p_1.
Vector de probabilidades:

$$\begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$$

La acción de la compuerta sobre un estado

$$NOT \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} = \begin{pmatrix} p_1 \\ p_0 \end{pmatrix}$$

Álgebra Lineal para el Modelo de Circuitos

Estado de 2 cables

El primero dado por: p_0 y p_1 y el segundo por q_0 y q_1.
Las posibilidades del estado combinado son: $\{00,\ 01,\ 10,\ 11\}$.
$Prob(i,j) = p_i q_j$. El estado combinado en ambos cables será representado por:

$$\begin{pmatrix} p_0 q_0 \\ p_0 q_1 \\ p_1 q_0 \\ p_1 q_1 \end{pmatrix} = \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \otimes \begin{pmatrix} q_0 \\ q_1 \end{pmatrix}$$

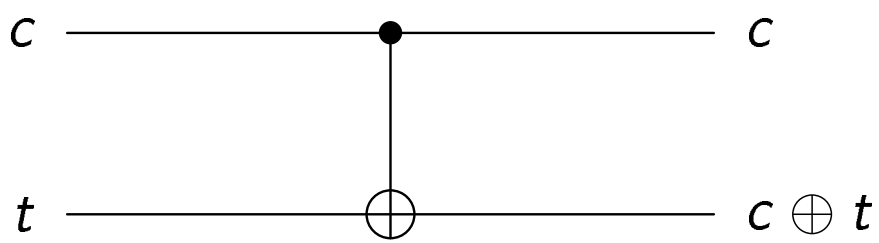
Álgebra Lineal para el Modelo de Circuitos

Compuertas que actúan sobre mas de 1 cable

Ejemplo: la **CNOT** (*controlled-NOT*) actúa sobre el bit *control* y el bit *target*. Aplica **NOT** sobre el bit *target* si el bit *control* está en 1 y lo deja igual si está en 0. El bit control queda inalterado.

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$CNOT \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$



Notación de Dirac

Espacio vectorial

- Espacios vectoriales de números complejos y de dimensión finita.
- Miembros de una clase de espacios vectoriales llamados espacios de Hilbert $\mathcal{H}$.
- Dimensión 2^n, con n entero positivo.

Base Computacional

$$\underbrace{|00\ldots00\rangle}_{n}, \quad |00\ldots01\rangle, \quad \ldots, \quad |11\ldots10\rangle, \quad |11\ldots11\rangle$$

Notación de Dirac

que se corresponden con los vectores columna:

$$|00\ldots00\rangle \Longleftrightarrow \left.\begin{pmatrix}1\\0\\0\\\vdots\\0\\0\end{pmatrix}\right\} 2^n, \qquad |00\ldots01\rangle \Longleftrightarrow \begin{pmatrix}1\\0\\0\\\vdots\\0\\0\end{pmatrix},$$

La notación de Dirac *Ahorra espacio*

En n-qubit estados los vectores columna son 2^n dimensionales mientras que en notación de Dirac son n números binarios.

Notación de Dirac

Ejemplo:

$$\sqrt{\frac{2}{3}}|01\rangle + \frac{i}{\sqrt{3}}|11\rangle = \sqrt{\frac{2}{3}}|0\rangle \otimes |1\rangle + \frac{i}{\sqrt{3}}|1\rangle \otimes |1\rangle$$

se escribe como vector columna:

$$\begin{pmatrix} 0 \\ \sqrt{\frac{2}{3}} \\ 0 \\ \frac{i}{\sqrt{3}} \end{pmatrix}$$

Notación de Dirac

Vectores Duales

Producto interno o escalar:

$$\vec{v} \cdot \vec{w} = \begin{pmatrix} v_1^* & v_2^* & \dots & v_n^* \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = \sum_{i=1}^{n} v_i^* w_i$$

En notación de Dirac el producto escalar es:

$$\langle \chi || \psi \rangle = \langle \chi | \psi \rangle$$

Notación de Dirac

Ejemplo

$$\begin{aligned} |\psi\rangle &= \sqrt{\tfrac{2}{3}}|01\rangle + \tfrac{i}{\sqrt{3}}|11\rangle \\ |\phi\rangle &= \tfrac{1}{\sqrt{2}}|10\rangle + \tfrac{1}{\sqrt{2}}|11\rangle \end{aligned}$$

como vectores columna:

$$\begin{pmatrix} 0 \\ \sqrt{\frac{2}{3}} \\ 0 \\ \frac{i}{\sqrt{3}} \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

y el producto interno es: $\langle\psi|\phi\rangle = \frac{-i}{\sqrt{6}}$

El producto interno de vectores ortogonales es 0.

Notación de Dirac

La *norma* de $|\psi\rangle$ es:

$$||\psi|| = \sqrt{\langle\psi|\psi\rangle}$$

Un conjunto ortonormal es un conjunto de vectores ortogonales de norma 1 (unitarios).

Base Ortonormal

Está formada por un conjunto de vectores $\{|b_n\rangle\}$ que cumplen:

$$\langle b_n|b_m\rangle = \delta_{n,m}$$

Notación de Dirac

Todo vector $|\psi\rangle$ se escribe

$$|\psi\rangle = \sum_n \psi_n |b_n\rangle,$$

con $\psi_n \in \mathbb{C}$

$$\psi_n = \langle b_n|\psi\rangle$$

son los coeficientes de ψ en la base $\{|b_n\rangle\}$

Vectores de la base computacional en $\mathcal{H}$

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

Notación de Dirac

Ejercicio: Escriba estos vectores de la base en formato columna y verifique ortonormalidad. Calcule el producto interno anterior

$$\langle\psi|\phi\rangle = \frac{-i}{\sqrt{6}}$$

usando notación de Dirac.
Otra base distinta de la computacional en $\mathcal{H}$ de dimensión 2 es la de *Hadamard* que en términos de la computacional se escribe:

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

Ejercicio: Verifique ortonormalidad en la base de *Hadamard*.
La base ortonormal para $\mathcal{H}^*$ es la *base dual* $\{\langle b_n|\}$

Operadores

Operador lineal

Transformación que actúa sobre vectores de $\mathcal{H}$ y produce vectores de $\mathcal{H}$.

Producto Externo $|\psi\rangle\langle\phi|$

$$(|\psi\rangle\langle\phi|)|\gamma\rangle = (\langle\phi|\gamma\rangle)|\psi\rangle.$$

Proyector ortogonal

El *proyector ortogonal* sobre $|\psi\rangle$ es el producto externo de $|\psi\rangle$ consigo mismo $|\psi\rangle\langle\psi|$ y proyecta sobre $|\psi\rangle$:

$$(|\psi\rangle\langle\psi|)|\phi\rangle = (\langle\psi|\phi\rangle)|\psi\rangle$$

O sea proyecta al vector $|\phi\rangle$ sobre el subespacio unidimensional generado por $|\psi\rangle$.

Operadores

Teorema

Sea $\{|b_n\rangle\}$ una base ortonormal de un espacio vectorial $\mathcal{H}$. Todo operador lineal T de $\mathcal{H}$ se puede escribir de la forma:

$$T = \sum_{n,m} T_{n,m} |b_n\rangle\langle b_m|$$

con $T_{n,m} = \langle b_n|T|b_m\rangle$.

El conjunto de los operadores lineales en el espacio vectorial $\mathcal{H}$ forma un nuevo espacio vectorial $\mathcal{L}(\mathcal{H})$. En este teorema se construye una base para $\mathcal{L}(\mathcal{H})$ a partir de la base de $\mathcal{H}$.
La acción de T es entonces:

$$T|\psi\rangle = \sum_{n,m} T_{n,m}|b_n\rangle \langle b_m|\psi\rangle = \sum_{n,m} T_{n,m} \langle b_m|\psi\rangle |b_n\rangle$$

$T_{n,m}$ es el elemento n, m de la matriz T.

Operadores

Ejemplo: Sea el operador Z que actúa sobre la base computacional de la forma:

$$\begin{aligned} |0\rangle &\rightarrow |0\rangle \\ |1\rangle &\rightarrow -|1\rangle. \end{aligned}$$

Z puede escribirse:

$$|0\rangle\langle 0| - |1\rangle\langle 1|$$

y en representación matricial:

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Operadores

Completitud

$$I = \sum_n |b_n\rangle\langle b_n|$$

La suma sobre todas las proyecciones de la base da la *Identidad*.

Operador Adjunto

$T^\dagger$ es el adjunto de T si:

$$(\left\langle \psi | T^\dagger | \phi \right\rangle)^* = \langle \phi | T | \psi \rangle \, , \forall |\psi\rangle, |\phi\rangle \in \mathcal{H}$$

En términos de matrices, la matriz de $T^\dagger$ es la *compleja conjugada transpuesta* de T.

Operadores

Operadores Unitarios

Los operadores asociados a la evolución temporal de estados cuánticos en sistemas cerrados son *unitarios*.
Un operador es *unitario* si $U^\dagger = U^{-1}$ con U^{-1} el inverso de U. Ésto implica que $U^\dagger U = I$.

Los operadores *unitarios* preservan la *norma* de los vectores, característica fundamental para los estados cuánticos.

Operadores Hermítico

T es *hermítico* o *auto-adjunto* si $T^\dagger = T$.

Operadores

Proyector

Un *proyector* P es un operador lineal sobre $\mathcal{H}$ que cumple $P^2 = P$. Si además es ortogonal también $P^\dagger = P$.

Autovectores y Autovalores

$|\psi\rangle$ es autovector de T si

$$T|\psi\rangle = c|\psi\rangle$$

donde c es el autovalor. Los autovalores de un operador hermítico son reales. Si $T = T^\dagger \implies T|\psi\rangle = \lambda|\psi\rangle$ con $\lambda \in \mathbb{R}$. Los autovalores de un operador hermítico son reales. Ésto se cumple para operadores asociados con magnitudes *medibles* en mecánica cuántica.

Operadores

Traza

La *traza* de A operador en un espacio de Hilbert $\mathcal{H}$ es:

$$Tr(A) = \sum_n \langle b_n | A | \ b_n \rangle$$

donde $\{|b_n\rangle\}$ es alguna base ortonormal de $\mathcal{H}$.
Se puede demostrar que $Tr(A)$ no depende de la base ortonormal elegida, estando así bien definida.

El teorema Espectral

Un operador *normal* satisface:

$$AA^\dagger = A^\dagger A$$

Tanto los operadores *hermíticos* como los *unitarios* son *normales*.

Teorema Espectral

Todo operador *normal* T se puede escribir:

$$T = \sum_i T_i |T_i\rangle\langle T_i|$$

con T_i y $|T_i\rangle$ los autovalores y autovectores de T respectivamente.

El teorema Espectral

Otra forma de expresar el Teorema Espectral

$$T = P\Lambda P^{\dagger}$$

con Λ una matriz diagonal con los autovalores de T y P una matriz unitaria con los autovectores de T como columnas de la matriz.

Ejercicio:
Encuentre P y Λ para el operador:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Funciones de Operadores

- De acuerdo al teorema espectral: $T = \sum_i T_i |T_i\rangle\langle T_i|$
- Dado que $|T_i\rangle\langle T_i|$ es un proyector, $(|T_i\rangle\langle T_i|)^m = |T_i\rangle\langle T_i|$ para cualquier entero m.
- Los autovectores son ortonormales $\Rightarrow \langle T_i| \ T_j\rangle = \delta_{i,j}$.
- $\delta_{i,j}$ la delta de Kronecker que vale 1 si $i = j$ y 0 si $i \neq j$.

Conclusión

Para elevar T a una potencia m sólo hace falta calcular las correspondientes potencias de los elementos de la diagonal en el desarrollo espectral.

$$T^m = (\sum_i T_i |T_i\rangle\langle T_i|)^m = \sum_i T_i^m |T_i\rangle\langle T_i|.$$

Funciones de Operadores

Ejemplo:

Serie de Taylor para e^x es $\sum_{m=0}^{\infty} \frac{1}{m} x^m$. Para todo x que se encuentre en el *intervalo de convergencia* la serie de Taylor converge al valor de la función.

De esta forma podemos definir la acción de funciones f sobre *operadores* sobre $\mathbb{C}$. Por ejemplo:

$$e^T = \sum_m \frac{1}{m!} T^m$$

y en general para una función f que actúa sobre T:

$$f(T) = \sum_m a_m T^m,$$

Funciones de Operadores

que usando la descomposición espectral da:

$$\begin{aligned} f(T) &= \sum_m a_m \left(\sum_i T_i |T_i\rangle\langle T_i|\right)^m \\ &= \sum_m a_m \sum_i T_i^m |T_i\rangle\langle T_i| \\ &= \sum_i \left(\sum_m a_m T_i^m\right) |T_i\rangle\langle T_i| \\ &= \sum_i f(T_i) |T_i\rangle\langle T_i|. \end{aligned}$$

O sea que con T expresada en forma diagonal, $f(T)$ se calcula aplicando f a los elementos diagonales de T.

Producto tensorial

- Supongamos que tenemos un sistema A con 8 estados posibles
- Y queremos combinar nuestro sistema con otro sistema B que también tiene sus propios 8 estados.
- El sistema A puede estar en 1 de sus posibles 8 estados.
- De forma independiente, el sistema B puede estar también en uno de sus 8 estados.
- Necesitamos dos números cuánticos independientes para especificar el estado combinado.
- Por lo tanto, la dimensión del espacio combinado de Hilbert es $8 \times 8 = 64$

Producto Tensorial

El espacio combinado de Hilbert es el PRODUCTO TENSORIAL de los dos sub-espacios de Hilbert.

Producto tensorial

El formalismo

El espacio combinado de Hilbert es el PRODUCTO TENSORIAL de los dos sub-espacios de Hilbert.

- Sean $\mathcal{H}_A$ y $\mathcal{H}_B$ dos espacios de Hilbert
- Especifiquemos dos estados, uno perteneciente a cada espacio

$$|\psi\rangle^{(A)} \in \mathcal{H}_A \qquad |\psi\rangle^{(B)} \in \mathcal{H}_B$$

- El espacio combinado es $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$
- Y el estado del nuevo espacio es $|\psi_{12}\rangle = |\psi_1\rangle^{(A)} \otimes |\psi_2\rangle^{(B)}$

Producto tensorial

Ejemplo

Supongamos que debemos elegir entre dos marcas de autos. El espacio es $M = \{$  ,  $\}$ Si los fabricantes los ofrecen en dos colores el espacio de elección crece.
El espacio de colores es $C = \{$■, ■$\}$
El espacio de elección se incrementa ahora 4 posibilidades:

$$MC = \{\text{  }, \text{  }, \text{  }, \text{  }\}$$