Física Teórica 2

Guía 5: Dinámica. Computación cuántica

Mateo Koifman

14 de mayo de 2021

Problema 17

P17 **Algoritmo de Bernstein–Vazirani.** El algoritmo de Bernstein–Vazirani es uno de los ejemplos más sencillos de algoritmo cuántico y además resulta particularmente interesante en cuanto es uno de los relativamente pocos casos donde se puede realmente demostrar formalmente una ventaja respecto del escenario equivalente clásico. Supongamos que se tiene una función f que toma como input cadenas binarias $\boldsymbol{b}$ (por ejemplo $\boldsymbol{b} = (0, 1, 1, 0, 1, 1, 1, \ldots)$) de largo n y cuyo resultado es calcular el producto interno con otra cadena $\boldsymbol{s}$. Es decir, $f : \{0,1\}^n \to \{0,1\}$, tal que

$$f(\boldsymbol{b}) = \boldsymbol{b} \cdot \boldsymbol{s} = b_1 s_1 + b_2 s_2 + \cdots + b_n s_n.$$

La cadena $\boldsymbol{s}$ está fija pero es desconocida. Efectivamente, dada una caja negra que calcula f (lo que formalmente se conoce como "oráculo"), nuestro objetivo es determinar quién es $\boldsymbol{s}$.

(a) Proponga una estrategia clásica para tratar de inferir el valor de $\boldsymbol{s}$. ¿Cuantas evaluaciones de f (es decir cuantes interrogaciones al oráculo) requiere su estrategia? Se puede demostrar que clásicamente se requiere por lo menos de n evaluaciones de f.

(b) Consdiere ahora el escenario cuántico. En tal caso, la caja negra que calcula f es una unitaria U_f que actúa sobre un sistema de n qubits (sistemas de dimensión 2) de forma tal que si $\{|0\rangle, |1\rangle\}$ es una base ortonormal de cada qubit, entonces

$$U_f |\boldsymbol{b}\rangle = U_f(|b_1\rangle \otimes |b_2\rangle \otimes \ldots \otimes |b_n\rangle) = (-1)^{f(\boldsymbol{b})} |\boldsymbol{b}\rangle .$$

Luego, consideremos el siguiente algoritmo: (i) partimos con los n qubits en el estado $|\boldsymbol{0}\rangle = |0\rangle^{\otimes n}$, (ii) aplicar Hadamard a cada qubit, (iii) aplicar U_f, (iv) aplicar Hadamard a cada qubit, (v) medir cada qubit en la base computacional $\{|0\rangle, |1\rangle\}$. Muestre entonces que, con una única aplicación de U_f (es decir una única interrogación al oráculo), es posible determinar el valor de $\boldsymbol{s}$.

Recordatorio: La operación Hadamard es la unitaria sobre un qubit $H = (\sigma_z + \sigma_x)/\sqrt{2}$.

Problema 17

Nos dan una función $f : \{0,1\}^n \to \{0,1\}$

$$f(\mathbf{b}) = \mathbf{s} \cdot \mathbf{b}$$

Nos interesa hallar $\mathbf{s}$, evaluando la función f la menor cantidad de veces posible

(a) Clásicamente, una estrategia sería realizar n evaluaciones de la forma
$f(100\cdots0) = s_1$
$f(010\cdots0) = s_2$
...

(b) Vamos a ver que con el algoritmo cuántico que nos propone el enunciado, alcanza con evaluar una única vez la función f.

(i) $\left|\psi^{(i)}\right\rangle = |00\ldots0\rangle = |\mathbf{0}\rangle$

(ii) La compuerta Hadamard actua sobre de cada qubit

$$U_H\,|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad U_H\,|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Al actuar sobre los n qubits

$$U_H^{\otimes n}\,|00\ldots0\rangle = U_H\,|0\rangle \otimes U_H\,|0\rangle \otimes \cdots \otimes U_H\,|0\rangle$$

Por lo tanto[1][2]

$$\begin{aligned}\left|\psi^{(ii)}\right\rangle = U_H^{\otimes n}\,|00\ldots0\rangle &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\ldots\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{\sqrt{2^n}}\sum_{|\mathbf{x}\rangle}|\mathbf{x}\rangle\end{aligned}$$

Aplicando Hadamard al $|\mathbf{0}\rangle$ obtengo un estado que es la superposición de todos los posibles estados de los n qubits, todos con la misma fase relativa.

[1] Estamos omitiendo el $\otimes$ en la notación

[2] $\sum_{|\mathbf{x}\rangle}$ corre sobre todos los estados de los n qubits

(iii) El óraculo actua como nos dice el enunciado

$$\left|\psi^{(iii)}\right\rangle = U_f \frac{1}{\sqrt{2^n}} \sum_{|\mathbf{x}\rangle} |\mathbf{x}\rangle = \frac{1}{\sqrt{2^n}} \sum_{|\mathbf{x}\rangle} U_f |\mathbf{x}\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{|\mathbf{x}\rangle} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle$$

(iv) Volvemos a aplicar Hadamard

$$\left|\psi^{(iv)}\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{|\mathbf{x}\rangle} (-1)^{f(\mathbf{x})} U_H |\mathbf{x}\rangle$$

$$= \frac{1}{2^n} \sum_{|\mathbf{x}\rangle} (-1)^{f(\mathbf{x})} \left(\frac{|0\rangle + (-1)^{x_1} |1\rangle}{\sqrt{2}}\right) \left(\frac{|0\rangle + (-1)^{x_2} |1\rangle}{\sqrt{2}}\right) \cdots \left(\frac{|0\rangle + (-1)^{x_n} |1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{2^n} \sum_{|\mathbf{x}\rangle} (-1)^{f(\mathbf{x})} \sum_{|\mathbf{z}\rangle} (-1)^{\mathbf{x}\cdot\mathbf{z}} |\mathbf{z}\rangle$$

$$= \frac{1}{2^n} \sum_{|\mathbf{z}\rangle} \left(\sum_{|\mathbf{x}\rangle} (-1)^{\mathbf{x}\cdot(\mathbf{s}+\mathbf{z})} \right) |\mathbf{z}\rangle$$

Veamos ahora que $\left|\psi^{(iv)}\right\rangle = |\mathbf{s}\rangle$

$$\sum_{|\mathbf{x}\rangle}(-1)^{\mathbf{x}\cdot(\mathbf{s}+\mathbf{z})}$$

- Podemos reemplazar $\mathbf{s}+\mathbf{z}$ por $\mathbf{s}\oplus\mathbf{z}$, donde $\oplus$ denota la suma módulo 2.
- $s_i \oplus z_i = 0$ si $s_i = z_i$
  $s_i \oplus z_i = 1$ si $s_i \neq z_i$
- Si $\mathbf{s}\oplus\mathbf{z} = \mathbf{0}$, entonces $\sum_{|\mathbf{x}\rangle}(-1)^{\mathbf{x}\cdot(\mathbf{s}\oplus\mathbf{z})} = 2^n$
- Si $\mathbf{s}\oplus\mathbf{z}$ tiene solamente el elemento i-ésimo no nulo, $(-1)^{\mathbf{x}\cdot(\mathbf{s}\oplus\mathbf{z})} = 1$ cuando $x_i = 0$ y $(-1)^{\mathbf{x}\cdot(\mathbf{s}\oplus\mathbf{z})} = -1$ cuando $x_i = 1$. Por lo tanto $\sum_{|\mathbf{x}\rangle}(-1)^{\mathbf{x}\cdot(\mathbf{s}\oplus\mathbf{z})} = 0$
- Si $\mathbf{s}\oplus\mathbf{z}$ tiene solamente los elementos i, j no nulos, $(-1)^{\mathbf{x}\cdot(\mathbf{s}\oplus\mathbf{z})} = 1$ cuando $(x_i, x_j) = (0,0)$ o $(1,1)$ y $(-1)^{\mathbf{x}\cdot(\mathbf{s}\oplus\mathbf{z})} = -1$ cuando $(x_i, x_j) = (1,0)$ o $(0,1)$. Por lo tanto $\sum_{|\mathbf{x}\rangle}(-1)^{\mathbf{x}\cdot(\mathbf{s}\oplus\mathbf{z})} = 0$
- Por inducción, $\sum_{|\mathbf{x}\rangle}(-1)^{\mathbf{x}\cdot(\mathbf{s}+\mathbf{z})} = 2^n$ cuando $\mathbf{s}\oplus\mathbf{z} = \mathbf{0}$ (esencialmente $\mathbf{s} = \mathbf{z}$) y se anula en cualquier otro caso

$$\left|\psi^{(iv)}\right\rangle = \frac{1}{2^n}\sum_{|\mathbf{z}\rangle}\left(\sum_{|\mathbf{x}\rangle}(-1)^{\mathbf{x}\cdot(\mathbf{s}+\mathbf{z})}\right)|\mathbf{z}\rangle = |\mathbf{s}\rangle$$

(v) Al medir el qubit i-ésimo de $\left|\psi^{(iv)}\right\rangle = |\mathbf{s}\rangle$ sobre la base computacional, siempre vamos a medir s_i.