Explicación del Algoritmo Bernstein-Vazirani

Karla Sánchez Peña

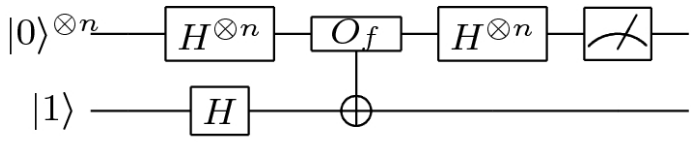

Figura 1: Circuito completo

Estado Inicial

En la primera etapa no ocurre ninguna operación:

$$|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$$

Etapa 1: Aplicación de Hadamard

Después de aplicar las compuertas Hadamard:

$$|\psi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Reescritura como Superposición Uniforme

Expresado como superposición uniforme sobre todos los estados de n bits:

$$|\psi_1\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_x |x\rangle\right) \otimes |-\rangle$$

donde $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$.

Operación del Oráculo

El oráculo U_f implementa la función $f(x) = x \cdot s$ (producto punto módulo 2):

$$f(x) = x_0 s_0 + x_1 s_1 + \cdots + x_{n-1} s_{n-1} \quad \text{mód } 2$$

Caso $f(x) = 0$

$$\begin{aligned} |0 \oplus 0\rangle &= |0\rangle \\ |1 \oplus 0\rangle &= |1\rangle \\ U_f|x\rangle|-\rangle &= |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = |x\rangle|-\rangle \end{aligned}$$

Caso $f(x) = 1$

$$\begin{aligned} |0 \oplus 1\rangle &= |1\rangle \\ |1 \oplus 1\rangle &= |0\rangle \\ U_f|x\rangle|-\rangle &= |x\rangle \left(\frac{|1\rangle - |0\rangle}{\sqrt{2}} \right) = |x\rangle \left(-\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = -|x\rangle|-\rangle \end{aligned}$$

Resultado Unificado del Oráculo

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

Estado después del Oráculo

$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_x (-1)^{x \cdot s} |x\rangle \right) \otimes |-\rangle$$

Operación del Oráculo y Estado Intermedio

Acción del Oráculo

Para estados donde $f(x) = 1$, se aplica un cambio de signo (operación Z):

- Si $f(x) = 0$: No se modifica el estado ($|\chi\rangle|-\rangle$)
- Si $f(x) = 1$: Se aplica la compuerta Z (cambio de signo)

Estado después del Oráculo ($|\psi_2\rangle$)

$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{\chi} (-1)^{f(\chi)} |\chi\rangle \right) \otimes |-\rangle$$

Para el caso específico de Bernstein-Vazirani donde $f(\chi) = \chi \cdot s$:

$$|\psi_2\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{\chi} (-1)^{\chi \cdot s} |\chi\rangle \right) \otimes |-\rangle$$

Aplicación de la Transformada de Hadamard

Aplicamos $H^{\otimes n}$ al registro principal (la ancilla no se modifica):

$$H^{\otimes n} |\chi\rangle = \frac{1}{\sqrt{2^n}} \sum_{z} (-1)^{\chi \cdot z} |z\rangle$$

El estado resultante es:

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{\chi} (-1)^{\chi \cdot s} \left(\frac{1}{\sqrt{2^n}} \sum_{z} (-1)^{\chi \cdot z} |z\rangle \right) \otimes |-\rangle$$

Página 3: Interferencia Constructiva y Estado Final

Reorganización del Estado

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{z} \sum_{\chi} (-1)^{\chi \cdot (s \oplus z)} |z\rangle \otimes |-\rangle$$

Definición de ω

Sea $\omega = s \oplus z$, entonces:

$$|\psi_3\rangle = \frac{1}{2^n} \sum_z \left(\sum_\chi (-1)^{\chi \cdot \omega} \right) |z\rangle \otimes |-\rangle$$

Propiedad Fundamental de la Suma

$$\frac{1}{2^n} \sum_\chi (-1)^{\chi \cdot \omega} = \delta_{\omega,0} = \begin{cases} 1 & \text{si } \omega = 0 \\ 0 & \text{en otro caso} \end{cases}$$

Estado Final Simplificado

$$|\psi_3\rangle = \sum_z \delta_{s,z} |z\rangle \otimes |-\rangle = |s\rangle \otimes |-\rangle$$