Algoritmo de Bernstein-Vazirani

Beatriz Fresno Naumova

September 23, 2024

1 Introducción

El algoritmo de Bernstein-Vazirani es un algoritmo cuántico que resuelve el problema de encontrar una cadena binaria $s \in \{0,1\}^n$ a partir de una función oculta $f(x) = s \cdot x$, donde $s \cdot x$ es el producto escalar binario entre s y x. El algoritmo resuelve el problema de forma eficiente utilizando un circuito cuántico.

Este problema puede ser visto como una versión simplificada del problema de Simon y una generalización del problema de Deutsch-Jozsa.

2 Objetivo

Dada una función $f : \{0,1\}^n \to \{0,1\}$, de la forma:

$$f(x) = s \cdot x = s_0 x_0 \oplus s_1 x_1 \oplus \cdots \oplus s_{n-1} x_{n-1},$$

donde $s = (s_0, s_1, \ldots, s_{n-1})$ es una cadena binaria fija y desconocida, el objetivo es determinar s.

3 Descripción del Algoritmo

El algoritmo de Bernstein-Vazirani se puede describir en los siguientes pasos:

1. Preparamos un registro cuántico con n qubits inicializados en el estado $|0\rangle^{\otimes n}$ y un qubit adicional en el estado $|1\rangle$. El qubit adicional será utilizado como ancilla.

2. Aplicamos la transformación de Hadamard a todos los qubits, incluyendo el ancilla, obteniendo el siguiente estado:

$$H^{\otimes n+1}|0\rangle^{\otimes n}|1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

3. Aplicamos la función f de forma cuántica a través del oráculo U_f. Esta operación cuántica afecta la amplitud del ancilla según el valor de $f(x) = s \cdot x$, cambiando la fase de los estados de x:

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

Como $f(x) = s \cdot x$, obtenemos:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{s \cdot x} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

4. Aplicamos nuevamente la transformada de Hadamard a los n primeros qubits (excluyendo el ancilla). Este paso convierte el estado en:

$$H^{\otimes n} \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{s \cdot x} |x\rangle \right) = |s\rangle.$$

De esta manera, obtenemos la cadena s.

4 El Oráculo U_f

El oráculo U_f es un elemento crucial del algoritmo. Su función es implementar la operación:

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

donde $f(x) = s \cdot x$. Dado que el valor de $f(x)$ es simplemente el producto escalar binario entre s y x, este oráculo cambia la fase del estado de x de acuerdo con la relación $(-1)^{s \cdot x}$. En el caso del algoritmo de Bernstein-Vazirani, esto se logra sin afectar el qubit ancilla al final de la ejecución, ya que su rol es garantizar que el estado de x registre correctamente la cadena secreta s.

5 Ejemplo

Consideremos un ejemplo donde $n = 3$ y la cadena secreta es $s = 101$. Los pasos del algoritmo son los siguientes:

1. Inicializamos el sistema en $|000\rangle$ para los tres qubits y $|1\rangle$ para el ancilla:

$$|000\rangle|1\rangle.$$

2. Aplicamos la transformada de Hadamard a todos los qubits, obteniendo:

$$H^{\otimes 4}|0001\rangle = \frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

3. Aplicamos la función $f(x) = 101 \cdot x$, que introduce una fase $(-1)^{f(x)}$ a los estados de x:

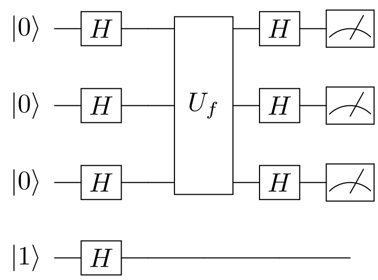
$$\frac{1}{\sqrt{8}} \sum_{x=0}^{7} (-1)^{101 \cdot x} |x\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle).$$

Esto cambia las fases de los estados de x en función de $s = 101$.

4. Finalmente, aplicamos la transformada de Hadamard a los tres primeros qubits, obteniendo el estado $|101\rangle$, que es la cadena secreta.

6 Circuito Cuántico

El circuito cuántico correspondiente al algoritmo de Bernstein-Vazirani, incluyendo el oráculo U_f, se puede representar de la siguiente manera:



En este circuito:

- Los H representan las puertas de Hadamard.
- U_f es la implementación cuántica de la función $f(x) = s \cdot x$, que introduce una fase dependiente del valor de $f(x)$.
- El qubit ancilla (última línea) se usa para auxiliar en la implementación del oráculo, pero no se mide al final.

7 Conclusión

El algoritmo de Bernstein-Vazirani ilustra cómo la computación cuántica puede resolver problemas de búsqueda de patrones con una ventaja significativa sobre los algoritmos clásicos. Con una sola evaluación de la función f, es posible determinar el valor de la cadena s, mientras que un algoritmo clásico requeriría n consultas a f. El oráculo cuántico desempeña un papel esencial al codificar la información de s en la fase de los estados cuánticos, lo que permite su extracción eficiente.