Quantum Complexity Theory

Ethan Bernstein and Umesh Vazirani (1997)

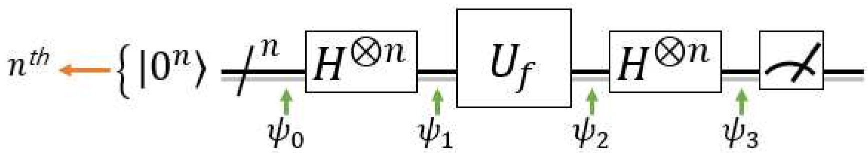
School of Air Transport, Transportation & Logistics 2018310015 Dongsin Kim

Bernstein-Vazirani's Problem

In *Bernstein-Vazirani problem*, we are given a n-bit function $f: \{0,1\}^n \rightarrow \{0,1\}$ which outputs a single bit. This function is guaranteed to be of the form $f_s(x) = x \cdot s$ where $s \in \{0,1\}^n$ and $x \cdot s = x_1 s_1 + x_2 s_2 + \cdots + x_n s_n \pmod 2$. The goal of the Bernstein-Vazirani problem is to find the unknown string s.

Bernstein-Vazirani's Algorithm

Bernstein-Vazirani algorithm can be implemented with the following quantum circuit with n-qubits initialized with, respectively, $|0\rangle$:



First, the algorithm starts with $|\psi_0\rangle = |0^n\rangle = |00\cdots 0\rangle = |0\rangle^{\otimes n}$. Analogously to the previous reports, it is clear that

$$|\psi_1\rangle = H^{\otimes n}|\psi_0\rangle = H^{\otimes n}|00\cdots 0\rangle = \frac{1}{(\sqrt{2})^n}\sum_{x\in\{0,1\}^n}(-1)^{0\times x_1+\cdots+0\times x_n}|x\rangle = \frac{1}{(\sqrt{2})^n}\sum_{x\in\{0,1\}^n}|x\rangle$$

$$\because\ H^{\otimes n}|a\rangle = \frac{1}{(\sqrt{2})^n}\textstyle\sum_{b\in\{0,1\}^n}(-1)^{a_1b_1+\cdots+a_nb_n}|b\rangle$$

Second, remembering that $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$:

$$|\psi_2\rangle = U_f|\psi_1\rangle = U_f\left(\frac{1}{(\sqrt{2})^n}\sum_{x\in\{0,1\}^n}|x\rangle\right) = \frac{1}{(\sqrt{2})^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle$$

$$= \frac{1}{(\sqrt{2})^n}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot s}|x\rangle = \frac{|0\rangle + (-1)^{s_1}|1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle + (-1)^{s_n}|1\rangle}{\sqrt{2}}$$

$$|\psi_3\rangle = H^{\otimes n}|\psi_2\rangle = H\left(\frac{|0\rangle + (-1)^{s_1}|1\rangle}{\sqrt{2}}\right) \otimes \cdots \otimes H\left(\frac{|0\rangle + (-1)^{s_n}|1\rangle}{\sqrt{2}}\right) = |s\rangle = \begin{cases}|0\rangle & \text{if } s_i = 0\ (i \in 1,\dots,n)\\ |1\rangle & \text{if } s_i = 1\ (i \in 1,\dots,n)\end{cases}$$

Conclusions

Using a quantum computer, we can solve this problem with certainty after only just a one query to the function f by measuring the n-qubits. We can see that *the result of the measurement is the binary representation (e.g. $|s\rangle$) of the unknown string s.*