Bernstein-Vazirani Algorithm

Huichen Sun

The Bernstein-Vazirani Problem

Given a function f: $\{0, 1\}^n \to \{0, 1\}$

An unknown string s $\in \{0, 1\}^n$
$f(x) = x \cdot s = (x_1 s_1 + x_2 s_2 + \ldots + x_n s_n) \bmod 2$

Find the string s

Classical Algorithm

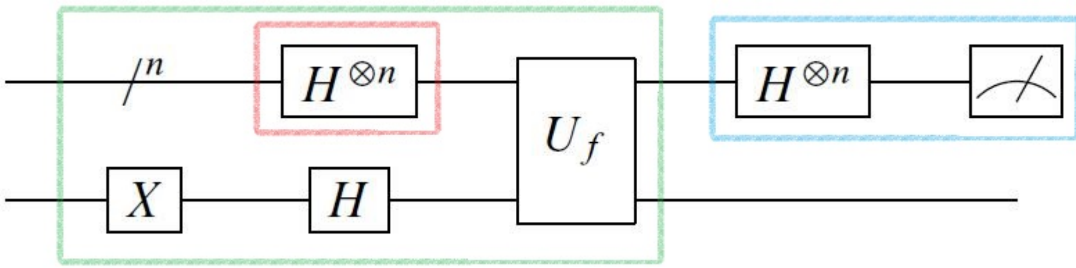
Requiring n queries to confirm s

Let $v_i = 0_1 0_2 \ldots 1_i ... 0_n$,
f(v_i) = s_i mod 2 = s_i

Intuition: string s contains n bits information, and 1 query provides 1 bit information

Quantum Algorithm

Requiring only 1 query to confirm s

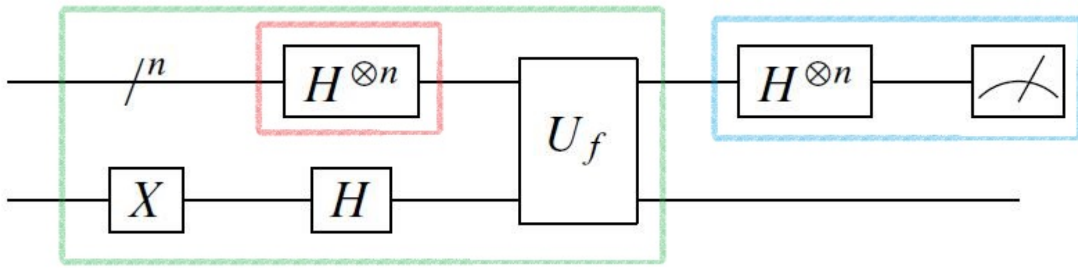


Red box: prepare superposition of computational basis
Green box: phase kickback
Blue box: measurement

State preparation and Phase kickback

Red box: uniform superposition

Green box: phase kickback



Initial state: $|0\rangle^{\otimes n}|0\rangle$

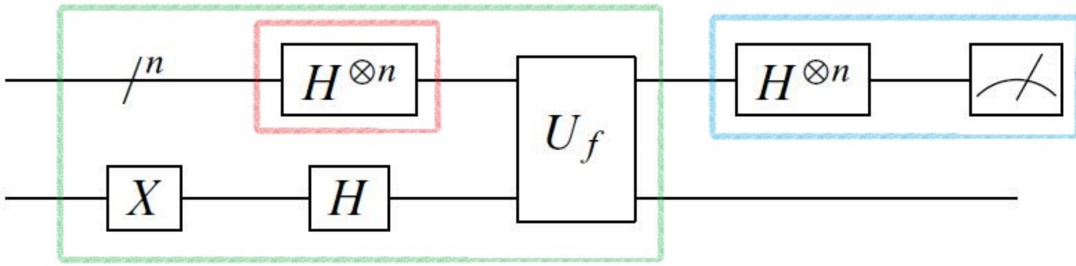
State before U_f: $\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle\text{-}|1\rangle)$

$U_f = \sum_{x\in\{0,1\}^n}\sum_{y\in\{0,1\}} |x\rangle\langle x| \otimes |y\oplus f(x)\rangle\langle y|$

State after U_f: $\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot s}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle\text{-}|1\rangle)$ ← Phase Kickback!

Define the first n-qubit state as $|\psi_s\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot s}|x\rangle$

Orthogonality of $|\psi_s\rangle$



Property of $|\psi_s\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot s}|x\rangle$

Orthogonality: $\langle\psi_s|\psi_t\rangle = \delta_{s,t}$

$\langle\psi_s|\psi_t\rangle = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot s}\langle x| \sum_{y\in\{0,1\}^n} (-1)^{y\cdot t}|y\rangle = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot s + x\cdot t}$

$(-1)^{x\cdot s+x\cdot t} = (-1)^{(x\cdot s+x\cdot t) \bmod 2}$

$(x\cdot s+x\cdot t) \bmod 2$

$= ((x_1 s_1 + x_2 s_2 + \ldots + x_n s_n) \bmod 2 + (x_1 t_1 + x_2 t_2 + \ldots + x_n t_n) \bmod 2) \bmod 2$

$= (x_1 s_1 + x_2 s_2 + \ldots + x_n s_n + x_1 t_1 + x_2 t_2 + \ldots + x_n t_n) \bmod 2$

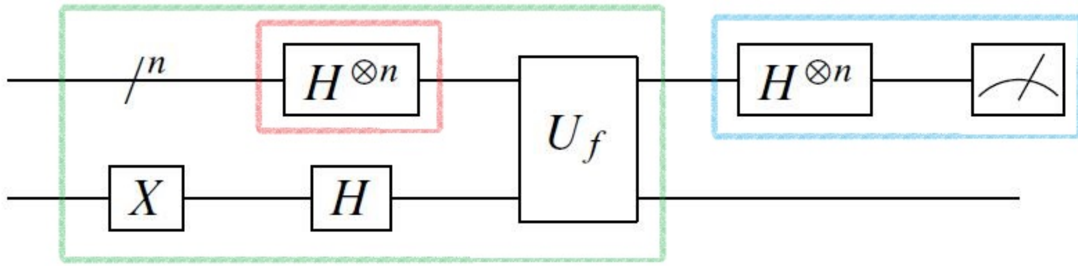
$= x \cdot (s \oplus t)$

$\langle\psi_s|\psi_t\rangle = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot(s\oplus t)}$

If s = t, $s\oplus t = 0$, $\langle\psi_s|\psi_t\rangle = 1$; $g(x) = (-1)^{x\cdot(s\oplus t)}$ is “constant” for x

If s ≠ t, $s\oplus t \neq 0$, $\langle\psi_s|\psi_t\rangle = 0$; $g(x) = (-1)^{x\cdot(s\oplus t)}$ is “balanced” for x

Measurement



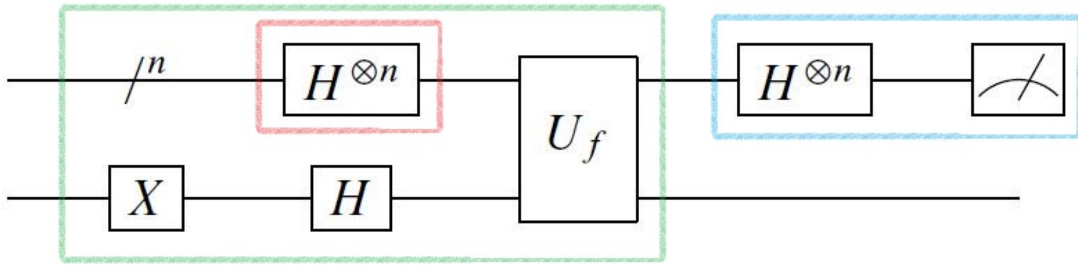
Orthogonality: $\langle \psi_s | \psi_t \rangle = \delta_{s,t}$

$\{|\psi_s\rangle | \, s \in \{0, 1\}^n\}$ is an orthogonal basis for the n-qubit system

Each s is uniquely related to a state $|\psi_s\rangle$

Measure in basis $\{|\psi_s\rangle\}$, then problem solved!

Measurement



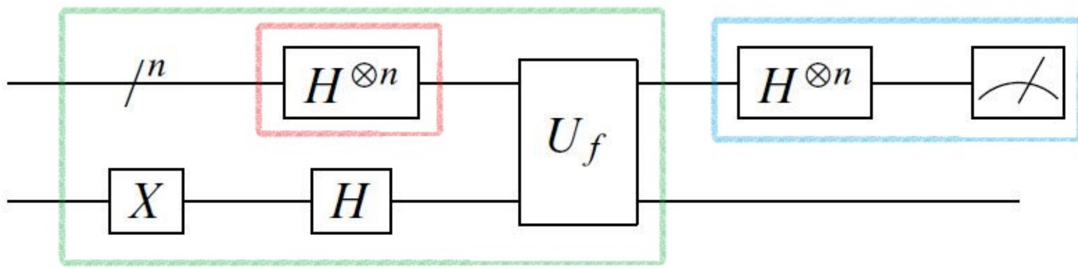
Measure in basis $\{|\psi_s\rangle\}$ = Change of Basis + Measure in computational basis

A unitary operator U changes one basis into another

$\{|\psi_s\rangle\} \overset{U}{\Longleftrightarrow} \{|x\rangle \mid x \in \{0,\ 1\}^n\}$

$H^{\otimes n}$ is just the unitary operator we need!

Measurement



$H = \frac{1}{\sqrt{2}} \sum_{x,y \in \{0,1\}} (-1)^{xy} |y\rangle\langle x|$

$H^{\otimes n} = (\frac{1}{\sqrt{2}} \sum_{x_1,y_1 \in \{0,1\}} (-1)^{x_1 y_1} |y_1\rangle\langle x_1|) \otimes \ldots \otimes (\frac{1}{\sqrt{2}} \sum_{x_n,y_n \in \{0,1\}} (-1)^{x_n y_n} |y_n\rangle\langle x_n|)$

$= \frac{1}{\sqrt{2^n}} \sum_{x,y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle\langle x| = \sum_{y \in \{0,1\}^n} (|y\rangle \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} \langle x|)$

Recall that $|\psi_s\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot s} |x\rangle$

$H^{\otimes n} = \sum_{y \in \{0,1\}^n} |y\rangle\langle \psi_y|$

$H^{\otimes n} |\psi_s\rangle = \sum_{y \in \{0,1\}^n} |y\rangle\langle \psi_y|\psi_s\rangle = |s\rangle$

Thus measure after $H^{\otimes n}$ gives the string s!

Comparison with Deutsch-Jozsa problem

DJ problem:
Classical exact: $\Omega(2^{n-1})$
Classical bounded error: O(C)
Quantum exact: O(1)

BV problem:
Classical exact: $\Omega(n)$
Classical bounded error: Ω(n)
Quantum exact: O(1)

Recursive BV problem:
Classical bounded error: $\Omega(n^{\log(n)})$
Quantum exact: O(n)

References

[1] J. D. Hidary, “Quantum Computing: An applied Approach”.
[2] D. Bacon, “The Recursive and Nonrecursive Bernstein-Vazirani Algorithm”.
[3] P. Kaye, , R. Laflamme and M. Mosca, “An Introduction to Quantum Computing”.

Thank you!