

Bernstein-Vazirani problem ( § 18.1 )

Setup : find  $S = (S_i)_{0 \leq i < n} \in \{0, 1\}^n$  from the function  $f: \{0, 1\}^n \rightarrow \{0, 1\}$

$$f(x) = S \cdot x = \sum_{0 \leq i < n} S_i x_i \pmod{2}.$$

Classical solution

compute  $f(100 \dots 0) = S_0$ ,  $f(010 \dots 0) = S_1, \dots$

$\Rightarrow$  need  $n$  queries

Quantum algorithm : one query (but  $\sim 2n$  gates)

use the phase query  $U_f |x\rangle \mapsto (-1)^{f(x)} |x\rangle$   
 $x \in \{0, 1\}^n$

Prop. 1  $(\underbrace{H \otimes \dots \otimes H}_{n \text{ factors}}) U_f (H \otimes \dots \otimes H) |0 \dots 0\rangle = |S\rangle$

Proof Step 1  $|\psi\rangle = (H \otimes \dots \otimes H) |0 \dots 0\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0, 1\}^n} |x\rangle$

$\therefore$  expand  $|+\rangle \otimes |+\rangle \otimes \dots \otimes |+\rangle$

Step 2  $|\varphi\rangle = U_f |\psi\rangle = \frac{1}{2^{n/2}} \sum_x (-1)^{f(x)} |x\rangle = \frac{1}{2^{n/2}} \sum_x (-1)^{x \cdot S} |x\rangle$

Step 3  $(H \otimes \dots \otimes H) |\varphi\rangle = \frac{1}{2^{n/2}} \sum_{y \in \{0, 1\}^n} (-1)^{x \cdot y} |y\rangle$

$\therefore H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2}} (|0\rangle + (-1)^{x_0} |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + (-1)^{x_1} |1\rangle) \otimes \dots$

Step 4  $H^{\otimes n} = (H^{\otimes n})^{-1}$

$\therefore H = H^\dagger = H^{-1}$ ,  $(H \otimes \dots \otimes H)^2 = H^2 \otimes \dots \otimes H^2 = I_{2^n}$

Step 5  $H^{\otimes n} |\varphi\rangle = |S\rangle$

$\therefore |\varphi\rangle = H^{\otimes n} |S\rangle$  by Steps 2 & 3  $\Rightarrow$  Step 4  $H^{\otimes n} |\varphi\rangle = |S\rangle$

Simon's problem (§ 18.2).

First exponential speedup.

cf. Deutsch's algorithm, Bernstein-Vazirani algorithm  
only give polynom. speedup like  $O(n^k)$  vs  $O(1)$

Setup Find  $S = (s_i)_{0 \leq i < n} \in \{0, 1\}^n$  from

$f: \{0, 1\}^n \rightarrow \{0, 1\}^n$  s.t.  $f(x) = f(y) \Leftrightarrow y = x \oplus S$  bitwise XOR

Classically: typically requires  $O(2^{\frac{n}{2}})$  steps.

once we can find  $x \neq y$  with  $f(x) = f(y)$

then  $S = x \oplus y$  ( $x \oplus S$ : sum of vectors in  $\mathbb{F}_2^n$ )

why? : do "birthday attack"

randomly choose  $x^0, x^1, \dots \in \{0, 1\}^n$  and

keep comparing  $f(x^0), f(x^1), \dots$

with  $k$  samples, the prob. of not

having  $x^i$  and  $x^j$  with  $f(x^i) = f(x^j)$  is

$$\underbrace{\left(1 - \frac{1}{2^n}\right)}_{f(x^1) \neq f(x^0)} \underbrace{\left(1 - \frac{2}{2^n}\right)}_{\substack{f(x^2) \neq f(x^0) \\ f(x^2) \neq f(x^1)}} \dots \underbrace{\left(1 - \frac{k}{2^n}\right)}_{\substack{f(x^k) \neq f(x^i) \\ \text{all } i < k}} \sim \exp\left(-\frac{k^2}{2^{n+1}}\right)$$

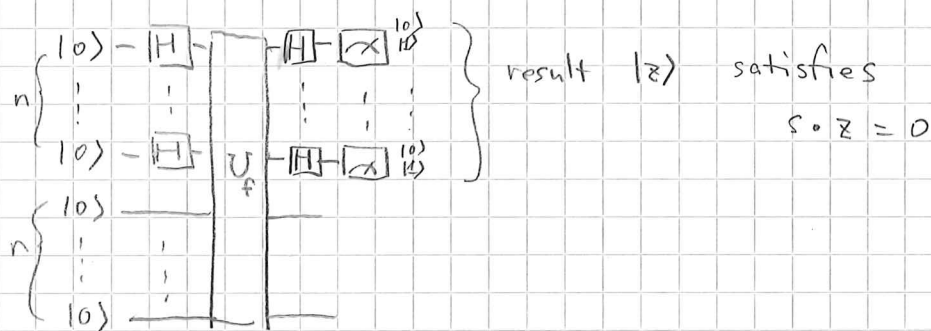
so  $k \sim 2^{\frac{n}{2}}$  is enough to get a high prob.

of finding  $f(x^i) = f(x^j)$

Quantum algorithm: typically requires  $O(n)$  steps

use the XOR query  $U_f: |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$   
 $x, y \in \{0, 1\}^n$

Prop 2



after repeating this  $k$  times, we get a system of lin. eqs  $s \cdot z^i = 0 \pmod{2}$   $0 \leq i < k$   
 $\leadsto$  enough to determine  $s$  at  $k \sim n = \dim \mathbb{F}_2^n$

Proof of Prop 2.

$$\text{Step 1. } |\psi\rangle = U_f (H^{\otimes n} \otimes I_{2^n}) |0 \dots 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

$$\therefore (H^{\otimes n} \otimes I_{2^n}) |0 \dots 0\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |0 \dots 0\rangle$$

Step 2. suppose we got  $|w\rangle$  by measuring

the  $n$ -th  $\sim (2n-1)$ -th qubits of  $|\psi\rangle$  in  $|0\rangle, |1\rangle$

then the  $0$ -th  $\sim (n-1)$ -th qubits are

$$\frac{1}{\sqrt{2}} (|x\rangle + |y\rangle) \quad \text{s.t.} \quad f(x) = f(y) = w$$

$\therefore$  partial meas. gives  $|w\rangle \leadsto$  the rest is

$$\text{normalization of } (I_{2^n} \otimes \langle w |) |\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{\substack{x \in \{0,1\}^n \\ f(x)=w}} |x\rangle$$

only two possibilities of  $x$  ( $x^0$  and  $y^0 = x^0 \oplus s$ )

$$\text{Step 3} \quad H^{\otimes n} \frac{1}{\sqrt{2}} (|x\rangle + |y\rangle) = \frac{1}{\sqrt{2^{n+1}}} \sum_{z \in \{0,1\}^n} ((-1)^{x \cdot z} + (-1)^{y \cdot z}) |z\rangle$$

Step 4  $z$  is observable in first  $n$  qubits

of  $(H^{\otimes n} \otimes \langle w |) |\psi\rangle$  normalized

$$\Leftrightarrow s \cdot z = 0 \pmod{2}$$

$$\therefore (-1)^{x \cdot z} + (-1)^{y \cdot z} \neq 0 \quad \Leftrightarrow x \cdot z = y \cdot z \pmod{2}$$

$$\text{use } x = y \oplus s \Rightarrow x \cdot z - y \cdot z = s \cdot z. \quad \square$$

