

# COL866: Quantum Computation and Information

Ragesh Jaiswal, CSE, IIT Delhi

# Quantum Computation: Basic Quantum Algorithms

# Quantum Computation

## Basic quantum algorithms

- We will see some basic quantum algorithms that were the precursor to the more popular algorithms such as Factoring. The main ideas were developed in these simple algorithms.
  - Bernstein-Vazirani
  - Simon's problem
- While discussing these algorithms we will try to argue why quantum algorithms have an advantage compared to classical ones.

# Quantum Computation

## Basic quantum algorithms: Bernstein-Vazirani

### Problem

Given a function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  such that for every  $x \in \{0, 1\}^n$ ,  $f(x) = (a \cdot x)$ , determine  $a$ . Here  $(a \cdot x)$  denotes the dot product of bit vectors  $a$  and  $x$ .

- Question: In the classical setting, how many classical queries to the function  $f$  will be needed to determine  $a$ ?

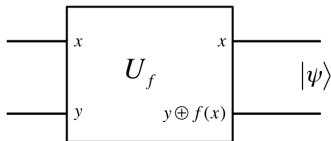
# Quantum Computation

## Basic quantum algorithms: Bernstein-Vazirani

### Problem

Given a function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  such that for every  $x \in \{0, 1\}^n$ ,  $f(x) = (a \cdot x)$ , determine  $a$ . Here  $(a \cdot x)$  denotes the dot product of bit vectors  $a$  and  $x$ .

- Question: In the classical setting, how many classical queries to the function  $f$  will be needed to determine  $a$ ?  $n$  queries
  - Since each query reveals at most one bit of  $a$ .
- Question: Suppose the unitary transformation below is available to us (as in Deutsch-Jozsa). How many invocations of this gate will be required within the quantum circuit to determine  $a$ ?



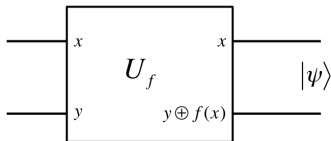
# Quantum Computation

Basic quantum algorithms: Bernstein-Vazirani

## Problem

Given a function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  such that for every  $x \in \{0, 1\}^n$ ,  $f(x) = (a \cdot x)$ , determine  $a$ . Here  $(a \cdot x)$  denotes the dot product of bit vectors  $a$  and  $x$ .

- Question: In the classical setting, how many classical queries to the function  $f$  will be needed to determine  $a$ ?  $n$  queries
  - Since each query reveals at most one bit of  $a$ .
- Question: Suppose the unitary transformation below is available to us (as in Deutsch-Jozsa). How many invocations of this gate will be required within the quantum circuit to determine  $a$ ? **One!**



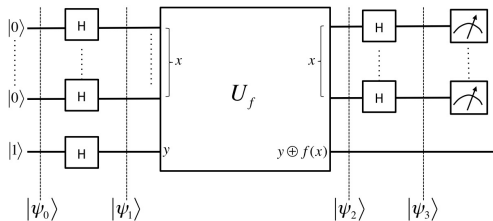
# Quantum Computation

## Basic quantum algorithms: Bernstein-Vazirani

### Problem

Given a function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  such that for every  $x \in \{0, 1\}^n$ ,  $f(x) = (a \cdot x)$ , determine  $a$ . Here  $(a \cdot x)$  denotes the dot product of bit vectors  $a$  and  $x$ .

- Question: In the classical setting, how many classical queries to the function  $f$  will be needed to determine  $a$ ?  $n$  queries
- Question: Suppose the unitary transformation below is available to us (as in Deutsch-Jozsa). How many invocations of this gate will be required within the quantum circuit to determine  $a$ ? **One!**
  - The same circuit as in Deutsch-Jozsa works!
  - Question: What will be the measurement output of the circuit below?



# Quantum Computation

Basic quantum algorithms: Bernstein-Vazirani

## Problem

Given a function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  such that for every  $x \in \{0, 1\}^n$ ,  $f(x) = (a \cdot x)$ , determine  $a$ . Here  $(a \cdot x)$  denotes the dot product of bit vectors  $a$  and  $x$ .

- Question: In the classical setting, how many classical queries to the function  $f$  will be needed to determine  $a$ ?  $n$  queries
- Question: Suppose the unitary transformation below is available to us (as in Deutsch-Jozsa). How many invocations of this gate will be required within the quantum circuit to determine  $a$ ? **One!**
- Does this really show that quantum computers are more powerful?
  - The function  $f$  is only accessible as a **black-box** in the classical setting.
  - There may be a classical algorithm that figures out  $a$  if the circuit implementing  $f$  is accessible.



# Quantum Computation

Basic quantum algorithms: Bernstein-Vazirani

## Problem

Given a function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$  such that for every  $x \in \{0, 1\}^n$ ,  $f(x) = (a \cdot x)$ , determine  $a$ . Here  $(a \cdot x)$  denotes the dot product of bit vectors  $a$  and  $x$ .

- Question: In the classical setting, how many classical queries to the function  $f$  will be needed to determine  $a$ ?  $n$  queries
- Question: Suppose the unitary transformation below is available to us (as in Deutsch-Jozsa). How many invocations of this gate will be required within the quantum circuit to determine  $a$ ? **One!**
- Does this really show that quantum computers are more powerful? **Yes and no**
- The above shows a gap factor of  $n$ . Can we design a similar problem that has **super-polynomial** gap? **Yes using a recursive extension of the above ideas.**

# Quantum Computation

## Basic quantum algorithms: Simon's problem

### Simon's problem

Given a function  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$  that satisfies the following conditions: (i)  $f(x) = f(y) \leftrightarrow x \oplus y = a$ , (ii)  $a \neq 0 \dots 0$ . The problem is to determine  $a$ .

- Such a function is called a **2-to-1** function.
- Question: How many classical queries to the function  $f$  need to be made to find  $a$ ?

# Quantum Computation

## Basic quantum algorithms: Simon's problem

### Simon's problem

Given a function  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$  that satisfies the following conditions: (i)  $f(x) = f(y) \leftrightarrow x \oplus y = a$ , (ii)  $a \neq 0 \dots 0$ . The problem is to determine  $a$ .

- Question: How many classical queries to the function  $f$  need to be made to find  $a$ ?  $\Theta(2^{n/2})$ 
  - $O(2^{n/2})$  queries are sufficient using **birthday bound**.
  - $\Omega(2^{n/2})$  queries are necessary using an information-theoretic argument.

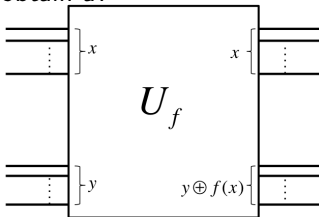
# Quantum Computation

## Basic quantum algorithms: Simon's problem

### Simon's problem

Given a function  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$  that satisfies the following conditions: (i)  $f(x) = f(y) \leftrightarrow x \oplus y = a$ , (ii)  $a \neq 0 \dots 0$ . The problem is to determine  $a$ .

- Question: How many classical queries to the function  $f$  need to be made to find  $a$ ?  $\Theta(2^{n/2})$
- Question: Suppose the following gate is available. How many invocations of this gate will be required in the quantum setting to obtain  $a$ ?



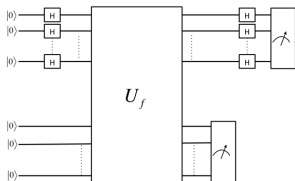
# Quantum Computation

## Basic quantum algorithms: Simon's problem

### Simon's problem

Given a function  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$  that satisfies the following conditions: (i)  $f(x) = f(y) \leftrightarrow x \oplus y = a$ , (ii)  $a \neq 0 \dots 0$ . The problem is to determine  $a$ .

- Question: How many classical queries to the function  $f$  need to be made to find  $a$ ?  $\Theta(2^{n/2})$
- Question: Suppose the following gate is available. How many invocations of this gate will be required in the quantum setting to obtain  $a$ ?  $\Theta(n)$ 
  - Running the circuit below  $\Theta(n)$  times will be sufficient to determine  $a$ .



# Quantum Computation

## Basic quantum algorithms: Simon's problem

### Simon's problem

Given a function  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$  that satisfies the following conditions: (i)  $f(x) = f(y) \leftrightarrow x \oplus y = a$ , (ii)  $a \neq 0 \dots 0$ . The problem is to determine  $a$ .

- Question: How many classical queries to the function  $f$  need to be made to find  $a$ ?  $\Theta(2^{n/2})$
- Question: Suppose the following gate is available. How many invocations of this gate will be required in the quantum setting to obtain  $a$ ?  $\Theta(n)$
- Does this really show that quantum computers are more powerful? **Yes and no**

End