PHYC90045 Introduction to Quantum Computing

Week 4

Lecture 7

Reversible computation, One qubit adder, the Deutsch-Josza algorithm

Lecture 8

Two basic quantum algorithms: Bernstein-Vazirani and Simon's Algorithms

Lab 3

Logical statements, Reversible logic, Adder, Deutsch-Josza algorithm

1

PHYC90045 Introduction to Quantum Computing

Simple Quantum Algorithms: Simon and Bernstein-Vazirani

Physics 90045
Lecture 8

2

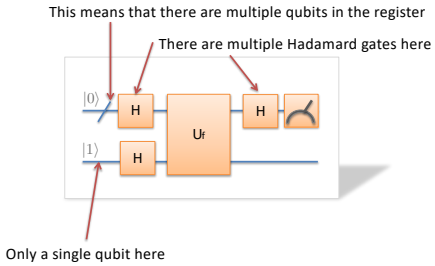
PHYC90045 Introduction to Quantum Computing

But first… Conclusion of Deutsch-Josza Algorithm

3

PHYC90045 Introduction to Quantum Computing

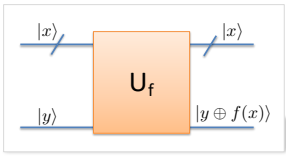
Multiple qubits: Deutsch-*Josza*



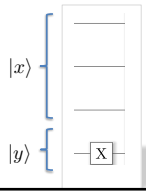
4

PHYC90045 Introduction to Quantum Computing

Example of multi-qubit constant function



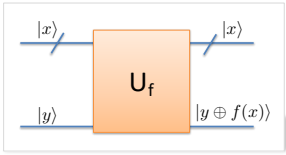
x	f(x)
000	1
001	1
010	1
011	1
100	1
101	1
110	1
111	1



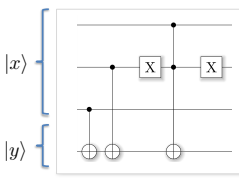
5

PHYC90045 Introduction to Quantum Computing

Example of multi-qubit balanced function



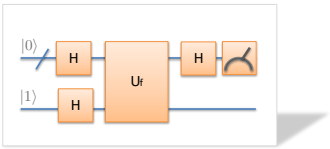
x	f(x)
000	0
001	1
010	1
011	0
100	1
101	0
110	1
111	0



6

PHYC90045 Introduction to Quantum Computing

Multiple qubits: Deutsch-*Josza*



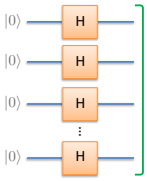
Let's walkthrough this circuit…

7

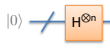
PHYC90045 Introduction to Quantum Computing

Hadamards produce equal superposition

n qubits



shorthand notation



$$|\psi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \ldots \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|\psi\rangle = \left[\frac{1}{\sqrt{2}}\right]^n (|00\ldots0\rangle + \ldots + |11\ldots1\rangle)$$

i.e. even superposition over binary rep of integers: i = 0 to $2^n - 1$

In general we use two representations in the QUI ($N = 2^n$):

"binary"

$$|\psi\rangle = a_{0\ldots00}\,|0\ldots00\rangle + a_{0\ldots01}\,|0\ldots01\rangle + a_{0\ldots10}\,|0\ldots10\rangle + \ldots + a_{1\ldots1}\,|1\ldots1\rangle$$

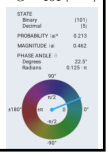
"decimal"

$$|\psi\rangle = a_0\,|0\rangle + a_1\,|1\rangle + a_2\,|2\rangle + \ldots + a_{N-1}\,|N-1\rangle$$

$$|\psi\rangle = \sum_\phi a_\phi\,|\phi\rangle$$

$$a_\phi = |a_\phi| e^{i\theta_\phi}$$

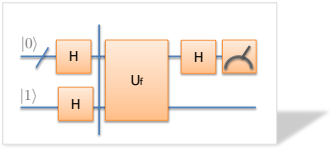
e.g. $a_{101}\,|101\rangle$



8

PHYC90045 Introduction to Quantum Computing

Deutsch-Josza Walkthrough



After the initial Hadamard gates, the state is (n qubits, N = 2^n):

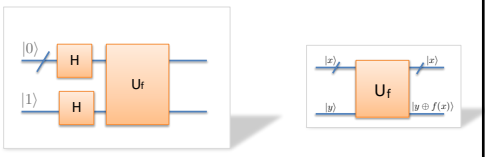
$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Equal (even) superposition of states

9

PHYC90045 Introduction to Quantum Computing

General Function Phase Kickback



Using phase kickback, after the function has been applied:

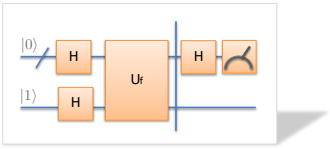
$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x (-1)^{f(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

If the function evaluates to "1" then the target qubit is flipped, and we pick up a phase. Otherwise, there is no phase applied. This is a simple way to write that.

10

PHYC90045 Introduction to Quantum Computing

Deutsch-Josza Walkthrough



Using phase kickback, after the function has been applied:

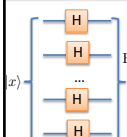
$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x (-1)^{f(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

If the function evaluates to "1" then the target qubit is flipped, and we pick up a phase. Otherwise, there is no phase applied. This is a simple way to write that.

11

PHYC90045 Introduction to Quantum Computing

Hadamard applied to a general state



$$\mathrm{H}^{\otimes n} |x\rangle = \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} a_z |z\rangle$$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Amplitude a_z -> how many times does the binary representation of z and x have 1's in the same location? $x_0 z_0 + x_1 z_1 + x_2 z_2 + \ldots + x_n z_n$

Shorthand for the bitwise dot product is: $x \cdot z = \sum_{j=0}^{n} x_j z_j$

When odd number of 1's in the same location, we get a sign change: $(-1)^{x \cdot z}$

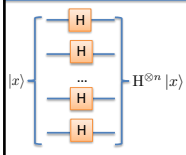
Hadamards applied to a general state (n qubits, $N = 2^n$):

$$\mathrm{H}^{\otimes n} |x\rangle = \frac{1}{\sqrt{N}} \sum_{z=0}^{N-1} (-1)^{x \cdot z} |z\rangle$$

12

PHYC90045 Introduction to Quantum Computing

e.g. Hadamard applied to a general state



$|x\rangle$ — $\mathrm{H}^{\otimes n}|x\rangle$

$$\mathrm{H}^{\otimes 3}|000\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}} \quad (x=0)$$

$$\mathrm{H}^{\otimes 3}|000\rangle = \frac{1}{\sqrt{2^3}}(\underbrace{|000\rangle}_{z=0}+\underbrace{|001\rangle}_{z=1}+\ldots+\underbrace{|111\rangle}_{z=7})$$

bitwise: $x \cdot z = 0$

$$\mathrm{H}^{\otimes 3}|x=0\rangle = \frac{1}{\sqrt{2^3}}\sum_{z=0}^{2^3-1}(-1)^{x\cdot z}|z\rangle$$

$$\mathrm{H}^{\otimes 3}|100\rangle = \frac{1}{\sqrt{2^3}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}} \quad (x=4)$$

$$\mathrm{H}^{\otimes 3}|100\rangle = \frac{1}{\sqrt{2^3}}(\underbrace{|000\rangle+|010\rangle+|001\rangle+|011\rangle}_{x\cdot z=0}-\underbrace{|100\rangle-|110\rangle-|101\rangle-|111\rangle}_{x\cdot z=1})$$

$$\mathrm{H}^{\otimes 3}|x=4\rangle = \frac{1}{\sqrt{2^3}}\sum_{z=0}^{2^3-1}(-1)^{x\cdot z}|z\rangle$$

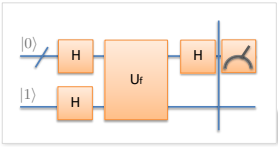
$$\boxed{\mathrm{H}^{\otimes 3}|x\rangle = \frac{1}{\sqrt{2^3}}\sum_{z=0}^{2^3-1}(-1)^{x\cdot z}|z\rangle}$$

General for n=3

13

PHYC90045 Introduction to Quantum Computing

Deutsch-Josza Walkthrough



$$\mathrm{H}^{\otimes n}|x\rangle = \frac{1}{\sqrt{N}}\sum_{z=0}^{N-1}(-1)^{x\cdot z}|z\rangle$$

Before and after the final Hadamard gates:

$$|\psi\rangle = \mathrm{H}^{\otimes n}\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}(-1)^{f(x)}|x\rangle$$

$$|\psi\rangle = \frac{1}{N}\sum_{x=0}^{N-1}(-1)^{f(x)}\sum_{z=0}^{N-1}(-1)^{x\cdot z}|z\rangle$$

14

PHYC90045 Introduction to Quantum Computing

Constant function

For a constant function (f(x) = 0 for all x, or f(x) = 1 for all x):

$$\begin{aligned}|\psi\rangle &= \frac{1}{N}\sum_{x=0}^{N-1}(-1)^{f(x)}\sum_{z=0}^{N-1}(-1)^{x\cdot z}|z\rangle \\ &= \frac{(-1)^{f(0)}}{N}\sum_{x=0}^{N-1}\sum_{z=0}^{N-1}(-1)^{x\cdot z}|z\rangle \\ &= \frac{(-1)^{f(0)}}{N}\sum_{z=0}^{N-1}\left(\sum_{x=0}^{N-1}(-1)^{x\cdot z}\right)|z\rangle \\ &= (-1)^{f(0)}|z=0\rangle\end{aligned}$$

$$\sum_{x=0}^{N-1}(-1)^{x\cdot z} = \begin{cases} N, & z=0 \\ 0, & z\neq 0 \end{cases}$$

So for a constant function "0" will always be measured (global phase is unimportant).

15

PHYC90045 Introduction to Quantum Computing

Balanced Function

$$|\psi\rangle = \mathrm{H}^{\otimes n}\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}(-1)^{f(x)}|x\rangle$$

$$|\psi\rangle = \frac{1}{N}\sum_{x=0}^{N-1}(-1)^{f(x)}\sum_{z=0}^{N-1}(-1)^{x\cdot z}|z\rangle$$

For a balanced function (equal number of f(x) = 0 and f(x) = 1):

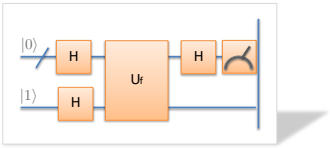
$$|\psi\rangle = \frac{1}{N}\sum_{z=0}^{N-1}\left(\sum_{x,f(x)=0}(-1)^{x\cdot z} - \sum_{x,f(x)=1}(-1)^{x\cdot z}\right)|z\rangle$$

Which has zero amplitude for the $|z=0\rangle$ state, and non-zero for other states.

16

PHYC90045 Introduction to Quantum Computing

Deutsch-Josza Walkthrough



If 0 is measured, then the function is constant.
If *any other* value is measured, then the function is balanced.

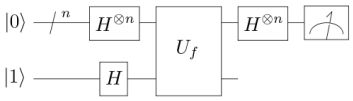
The Deutsch-Josza algorithm evaluates if a function is constant or balanced with a single query. Classically we would require $O(2^n)$ queries.

Of course, there are classical probabilistic algorithms with establish with high probability in few queries, but only with high probability of success not with certainty.

17

PHYC90045 Introduction to Quantum Computing

Deutsch-Josza algorithm



- Given a Boolean function, ***f***, determine if:
  - ***f*** is constant (always gives the same result)
  - ***f*** is balanced (gives equal numbers of 0s and 1s)

- **Classical algorithm** *(worst case) needs $2^n/2+1$ queries*
- ***Quantum algorithm*** *needs just 1 query.*

18

PHYC90045 Introduction to Quantum Computing

Overview

In this lecture we will discuss some of the early quantum algorithms,

1. Bernstein-Vazirani algorithm
2. Simon's algorithm

These algorithms can be taken as simple demonstrations of quantum computation, even if they are of limited practical use.

See:

Kaye, Chapter 6
Nielsen and Chuang, Chapters 1 & 4
Reiffel, 7.1-7.5

19

PHYC90045 Introduction to Quantum Computing

Bernstein-Vazirani Problem

Given a Boolean function, f:

$$f(x) = x \cdot s \mod 2$$

find s.

Recall, bitwise product: $x \cdot s = \sum_i x_i s_i$

20

PHYC90045 Introduction to Quantum Computing

Example: Linear Boolean function

Example:

$$f(x) = x \cdot 5 \mod 2$$

Remember, in binary, 5 = 101.

x	f(x)
000	0
001	1
010	0
011	1
100	1
101	0
110	1
111	0

Given a black-box which calculates this function, find s=5.

21

PHYC90045 Introduction to Quantum Computing

Solving BV Problem Classically

$$f(x) = x \cdot 5 \mod 2$$

x	f(x)
000	0
001	1
010	0
011	1
100	1
101	0
110	1
111	0

Input one single digit "1" at a time.

Can determine s using n queries.

22

PHYC90045 Introduction to Quantum Computing

Bernstein-Vazirani Problem

Given a Boolean function, *f*:

$$f(x) = x \cdot s \mod 2$$

find s.

Recall: bitwise product: $x \cdot s = \sum_i x_i s_i$

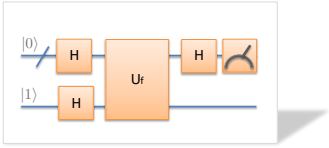
- **Classical algorithm** *needs n queries*
- ***Quantum algorithm*** *needs just 1 query.*

23

PHYC90045 Introduction to Quantum Computing

Bernstein-Vazirani algorithm

The circuit is the same as for the Deutsch-Josza algorithm:



The guarantees on f are different:

$$f(x) = x \cdot s \mod 2$$

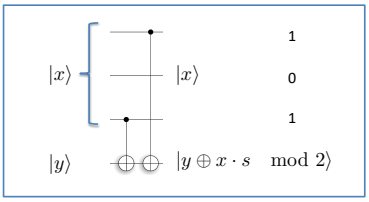
Recall: Deutsch-Josza algorithm required the function to either be constant or balanced.

24

PHYC90045 Introduction to Quantum Computing

Implementing a Linear Boolean Function

For $s = 5 = 101_2$ the function is evaluated using this circuit:



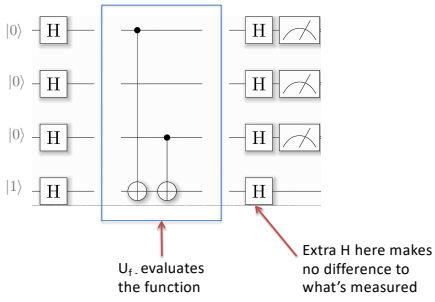
The bits of s determine the location of the CNOTs.

Every linear, Boolean function has a circuit of the same form.

25

PHYC90045 Introduction to Quantum Computing

Full BV circuit for s=5

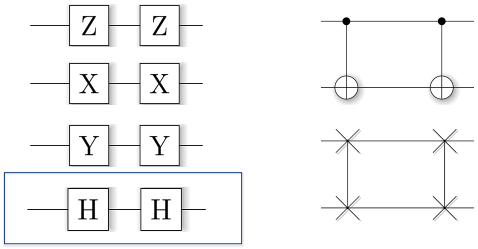


26

PHYC90045 Introduction to Quantum Computing

Many gates square to identity

Compilation tips: Most physicists looking at quantum circuit diagrams aren't multiplying matrices in their head. They're identifying common patterns.

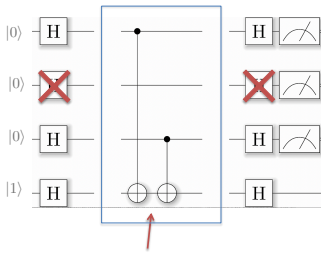


All of these combinations square to the identity (do nothing).
You can check these on the QUI.

27

PHYC90045 Introduction to Quantum Computing

BV circuit for s=5

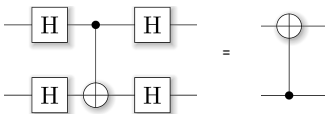


$U_{f:}$ evaluates the function

28

PHYC90045 Introduction to Quantum Computing

Circuit identity: Inverted CNOT



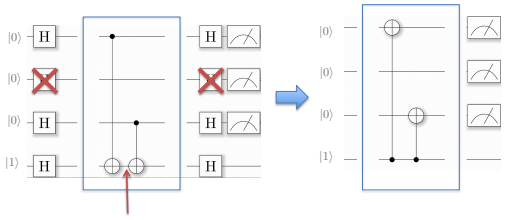
Exercise: You can verify this by writing out the matrices and multiplying!

29

PHYC90045 Introduction to Quantum Computing

Simple explanation of BV

Hadamard gates "conjugating" CNOT:



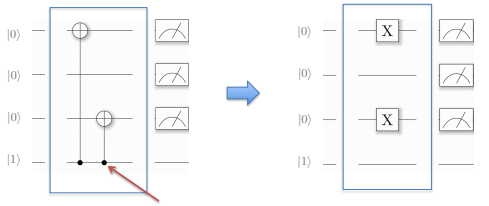
Insert H^2=I here

We can determine s with just one query, by making use of quantum superposition.

30

PHYC90045 Introduction to Quantum Computing

Simplifying circuit



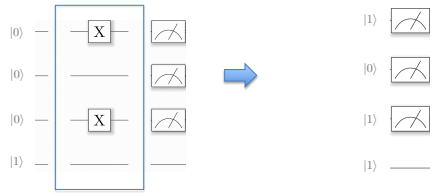
Control is a 1, so these operations always happen

If in doubt, check using QUI

31

PHYC90045 Introduction to Quantum Computing

BV Solution



This circuit will measure:
101 = 5
which is correct (s=5)

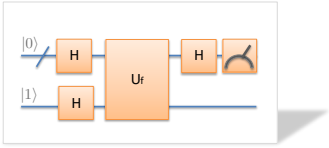
A similar reduction would work for any s, but let us prove that formally.

32

PHYC90045 Introduction to Quantum Computing

Bernstein-Vazirani algorithm

The circuit is the same as for the Deutsch-Josza algorithm:



The guarantees on f are different:

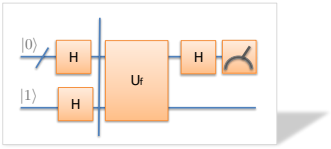
$$f(x) = x \cdot s \mod 2$$

Recall: Deutsch-Josza algorithm required the function to either be constant or balanced.

33

PHYC90045 Introduction to Quantum Computing

BV algorithm explained



State after the initial Hadamard gates:

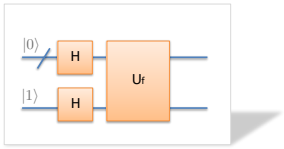
$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Sum of all computational basis states (again)

34

PHYC90045 Introduction to Quantum Computing

Recall: General Function Phase Kickback



Using phase kickback, after the function has been applied:

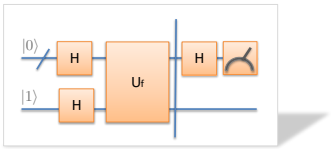
$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x (-1)^{f(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

If the function evaluates to "1" then the target qubit is flipped, and we pick up a phase. Otherwise, there is no phase applied. This is a simple way to write that.

35

PHYC90045 Introduction to Quantum Computing

BV algorithm explained



Using phase kickback, after the function has been applied:

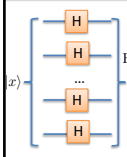
$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} (-1)^{f(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad \text{Phase kickback}$$

$$= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} (-1)^{x \cdot s} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad \text{Since } f(x) = x \cdot s \mod 2$$

36

PHYC90045 Introduction to Quantum Computing

Recall: Hadamard applied to a general state



$$\mathrm{H}^{\otimes n}|x\rangle = \frac{1}{\sqrt{N}}\sum_{z=0}^{N-1} a_z |z\rangle$$

Amplitude a_z -> how many times does the binary representation of z and x have 1's in the same location?

$$x_0 z_0 + x_1 z_1 + x_2 z_2 + \ldots + x_n z_n$$

Shorthand for the bitwise dot product is: $x \cdot z = \sum_{j=0}^{n} x_j z_j$

When 1's in the same location, we get a sign change -> $(-1)^{x\cdot z}$

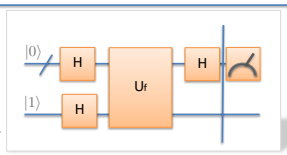
Hadamards applied to a general state (n qubits, $N = 2^n$):

$$\mathrm{H}^{\otimes n}|x\rangle = \frac{1}{\sqrt{N}}\sum_{z=0}^{N-1}(-1)^{x\cdot z}|z\rangle$$

37

PHYC90045 Introduction to Quantum Computing

BV algorithm explained



Considering the upper register only:

$$|\psi\rangle = \mathrm{H}^{\otimes n}\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}(-1)^{x\cdot s}|x\rangle$$

$$= \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}(-1)^{x\cdot s}\frac{1}{\sqrt{N}}\sum_{z=0}^{N-1}(-1)^{x\cdot z}|z\rangle$$

$$= \frac{1}{N}\sum_{x=0}^{N-1}\sum_{z=0}^{N-1}(-1)^{x\cdot(s\oplus z)}|z\rangle = \frac{1}{N}\sum_{z=0}^{N-1}\left(\sum_{x=0}^{N-1}(-1)^{x\cdot(s\oplus z)}\right)|z\rangle$$

$$\mathrm{H}^{\otimes n}|x\rangle = \frac{1}{\sqrt{N}}\sum_{z=0}^{N-1}(-1)^{x\cdot z}|z\rangle$$

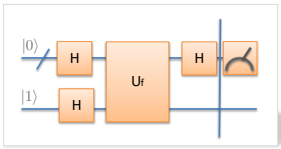
H's applied to basis state

$$x \oplus z = x_0 + z_0 \mod 2, x_1 + z_1 \mod 2, \ldots$$

38

PHYC90045 Introduction to Quantum Computing

BV algorithm explained



Simplifying the sum:

$$|\psi\rangle = \frac{1}{N}\sum_{z=0}^{N-1}\left(\sum_{x=0}^{N-1}(-1)^{x\cdot(s\oplus z)}\right)|z\rangle$$

$$= \frac{1}{N}\sum_{z=0}^{N-1}(-1)^{0}|s\rangle$$

$$= |s\rangle$$

$$\sum_{x=0}^{N-1}(-1)^{x\cdot b} = \begin{cases} N, & b = 0 \\ 0, & b \neq 0 \end{cases}$$

This sum (over x) is zero unless

$$s \oplus z = 0$$

That is, z and s are bitwise identical, ie.

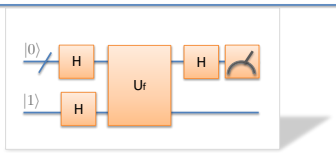
$$z = s$$

We will therefore measure s with certainty – the aim of the algorithm.

39

PHYC90045 Introduction to Quantum Computing

Bernstein-Vazirani Algorithm



Given a Boolean function, f:

$$f(x) = x \cdot s \mod 2$$

find s.

$$x \cdot s = \sum_i x_i s_i$$

- **Classical algorithm** *needs n queries*
- ***Quantum algorithm*** *needs just 1 query.*

40

PHYC90045 Introduction to Quantum Computing

Third Quantum Algorithm: Simon's algorithm

41

PHYC90045 Introduction to Quantum Computing

Simon's Problem

Given a 2-to-1 function, f, such that

$$f(x) = f(x \oplus a)$$

Find a.

Unlike the previous two examples, here the range of f(x) is Z, integers.

Simon's algorithm is an example of a "Hidden (Abelian) subgroup problem" (HSP) and was the inspiration for Shor's factoring algorithm.

42

PHYC90045 Introduction to Quantum Computing

Example of a hidden a

f(001) = f(111)

x	f(x)
000	0
001	1
010	2
011	3
100	2
101	3
110	0
111	1

We would like to find the hidden 'a' s.t.

$$f(x) = f(x \oplus a)$$

In this case:

$a = 110_2 = 6$

43

PHYC90045 Introduction to Quantum Computing

Solving Simon's problem classically

Just try different inputs until you see a collision:

f(000) = 0
f(011) = 3
f(111) = 1
f(010) = 2
f(001) = 1

Actually this is equivalent to the famous "birthday" problem, and takes fewer queries than you might expect. Probabilistically, if there are N different inputs we need

$$O(\sqrt{N})$$

Evaluations of the function before we find a collision.

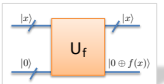
Simon's algorithm does the same with O(n) queries.

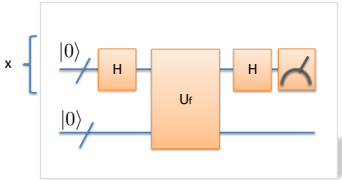
44

PHYC90045 Introduction to Quantum Computing

Simon's algorithm circuit

Randomly measure a result of the function. Collapse to a superposition of inputs which give that value. Send these through Hadamard gates, and measure:





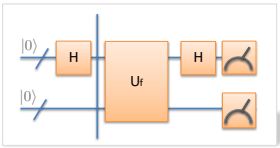
Measure to find a

$f(x_0), f(x_0 \oplus a)$

45

PHYC90045 Introduction to Quantum Computing

Simon's algorithm



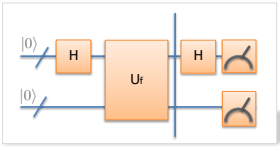
After the initial Hadamard gates:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle\,|0\rangle$$

46

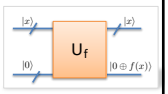
PHYC90045 Introduction to Quantum Computing

Simon's algorithm



After evaluation of the function:

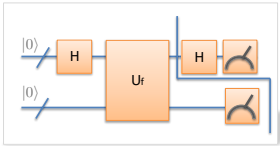
$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x U_f\,|x\rangle\,|0\rangle$$
$$= \frac{1}{\sqrt{N}} \sum_x |x\rangle\,|f(x)\rangle$$



47

PHYC90045 Introduction to Quantum Computing

Simon's algorithm



It's easiest to consider that the bottom register is measured first. Before measurement the state is:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle\,|f(x)\rangle$$

Some value, $f(x_0)$ will be measured at random, and the top register collapses to:

$$|\psi\rangle = \frac{|x_0\rangle + |x_0 \oplus a\rangle}{\sqrt{2}}$$

48

PHYC90045 Introduction to Quantum Computing

Example: Measuring function

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle |f(x)\rangle$$
$$= \frac{1}{\sqrt{8}} (|0\rangle |0\rangle + |1\rangle |1\rangle + |2\rangle |2\rangle + |3\rangle |3\rangle + |4\rangle |2\rangle + |5\rangle |3\rangle + |6\rangle |0\rangle + |7\rangle |1\rangle)$$

If we measure the second register, and measure obtain "3", the state collapses to only those states compatible with this measurement:

$$|\psi'\rangle = \frac{|3\rangle |3\rangle + |5\rangle |3\rangle}{\sqrt{2}}$$
$$= \frac{|3\rangle + |5\rangle}{\sqrt{2}} \otimes |3\rangle$$

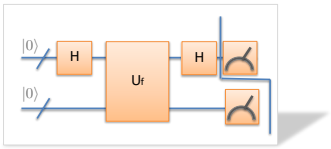
First register: $|\psi\rangle = \frac{|x_0\rangle + |x_0 \oplus a\rangle}{\sqrt{2}}$

x	f(x)
000	0
001	1
010	2
011	3
100	2
101	3
110	0
111	1

49

PHYC90045 Introduction to Quantum Computing

Simon's algorithm



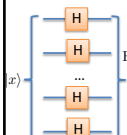
We now apply Hadamard to the top register:

$$|\psi\rangle = H^{\otimes n} \frac{|x_0\rangle + |x_0 \oplus a\rangle}{\sqrt{2}}$$

50

PHYC90045 Introduction to Quantum Computing

Hadamard applied to a general state



$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} a_y |y\rangle$$

Amplitude a_y -> how many times does the binary representation of y and x have 1's in the same location?

$$x_0 y_0 + x_1 y_1 + x_2 y_2 + \ldots + x_n y_n$$

Shorthand for the bitwise dot product is: $x \cdot y = \sum_{j=0}^{n} x_j y_j$

When 1's in the same location, we get a sign change -> $(-1)^{x \cdot y}$

Hadamards applied to a general state (n qubits, $N = 2^n$):

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} (-1)^{x \cdot y} |y\rangle$$

(changed dummy index to y)

51

PHYC90045 Introduction to Quantum Computing

Simon's algorithm

$$|\psi\rangle = H^{\otimes n}\frac{|x_0\rangle + |x_0 \oplus a\rangle}{\sqrt{2}}$$
$$= \frac{1}{\sqrt{2^{n+1}}}\sum_y \left((-1)^{x_0\cdot y} + (-1)^{(x_0\oplus a)\cdot y}\right)|y\rangle$$
$$= \frac{1}{\sqrt{2^{n+1}}}\sum_y (-1)^{x_0\cdot y}\left(1 + (-1)^{a\cdot y}\right)|y\rangle$$

The amplitude of any state, y, is zero unless:

$$a \cdot y = 0 \mod 2$$

Therefore, the state therefore becomes:

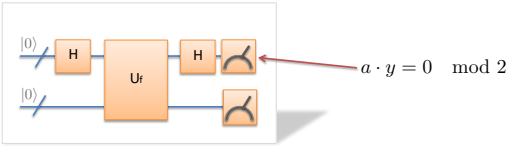
$$|\psi\rangle = \frac{1}{\sqrt{2^{n-1}}}\sum_{a\cdot y=0}(-1)^{x_0\cdot y}|y\rangle$$

52

PHYC90045 Introduction to Quantum Computing

Simon's algorithm

$$|\psi\rangle = \frac{1}{\sqrt{2^{n-1}}}\sum_{a\cdot y=0}(-1)^{x_0\cdot y}|y\rangle$$



$a \cdot y = 0 \mod 2$

Each time we measure, we randomly measure a "y" which is orthogonal to "a":

Obtain n random y's this way and **perform Gauss/Jordan elimination** to obtain "a"

53

PHYC90045 Introduction to Quantum Computing

Example of Simon's algorithm

x	f(x)
000	0
001	1
010	2
011	3
100	2
101	3
110	0
111	1

We would like to find the hidden 'a' s.t.

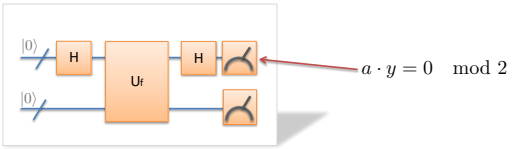
$$f(x) = f(x \oplus a)$$

In this case, $a=110_2=6$

54

PHYC90045 Introduction to Quantum Computing

Running the circuit



$$a \cdot y = 0 \mod 2$$

We run the circuit, and at random, obtain measure the results:

001
110
111

We want to find, $a=110_2=6$

55

PHYC90045 Introduction to Quantum Computing

In matrix form

We know that $a \cdot y = 0 \mod 2$

We have three values of 'y' for which this is true, so we can write a system of linear equations for the bits of 'a':

$$\mathbf{Y}\vec{a} = \vec{0}$$

001
110
111

Measured values

$$\left[\begin{array}{ccc|c} 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{array}\right] \sim \left[\begin{array}{ccc|c} 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

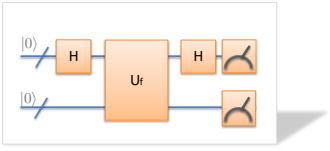
Solving for a

Solution is degenerate. a=(0,0,0) or $a_1=a_2=1$ ie. **a=(1,1,0)**

56

PHYC90045 Introduction to Quantum Computing

Simon's Algorithm



Given a 2-to-1 function, f, such that

$$f(x) = f(x \oplus a)$$

Find a.

Classical algorithm: $O(\sqrt{N})$ Queries to the oracle (probabilistically)

Quantum algorithm: $O(n)$ Queries to the oracle

57