Portland State U

F, 04/17/2020

S'20 CS 410/510

Intro to quantum computing

Fang Song

Week 3

- Quantum postulates
- Distinguishing quantum states
- Deutsch / Deutsch-Josza algorithms

Credit: based on slides by Richard Cleve

Logistics

- HW2 due Sunday

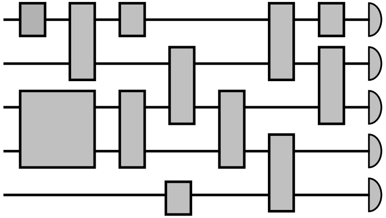
- Remarks
  - Campuswire: support markdown and LaTeX (e.g., `$$e^{iH}$$` = e^{iH});
  - Campuswire: stay informed, settings → notifications → digest messages
  - Youtube playlist: read the description (e.g., time stamps)

- Project: discussion at end of class

Postulates of quantum theory

1. States
2. Operations (dynamics)
3. Measurement
4. Composite systems

Quantum circuit model
(quantum computer)



Postulate 1: quantum states

- n-qubit system $\Leftrightarrow$ (Hilbert) state space: $\mathbb{C}^{2^n} = (\mathbb{C}^2)^{\otimes n}$
- Computational (standard) basis: $\{|x\rangle : x \in \{0,1\}^n\}$
- Quantum state: 2^n-dim. unit vector

$$\forall x \in \{0,1\}^n, \alpha_x \in \mathbb{C}, \sum_x |\alpha_x|^2 = 1$$

$$\begin{pmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{pmatrix} = \sum_{x\in\{0,1\}^3} \alpha_x |x\rangle$$

$$|000\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} |001\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} |010\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} |011\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|100\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} |101\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} |110\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} |111\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$n = 3$

Postulate 2: operations

- System evolution ⇔ Unitary transformation $|\psi_1\rangle = U|\psi_0\rangle$

- If you are really curious of the physics:

H: Hamiltonian of the system, a Hermitian matrix $(H = H^\dagger)$

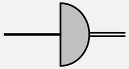
Schrodinger's equation: $i\frac{d|\psi(t)\rangle}{dt} = H|\psi(t)\rangle$

→ $|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$. $U \coloneqq e^{-iHt}$ Unitary.

$t=1: \quad U = e^{-iH}$

Postulate 3: measurements

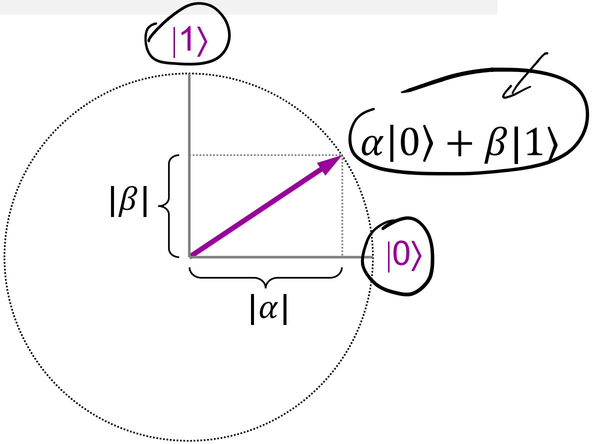
- Standard measurement (in computational basis)

$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$ 

See	w. probability	posterior state
x	$\lvert\alpha_x\rvert^2$	$\lvert x\rangle$

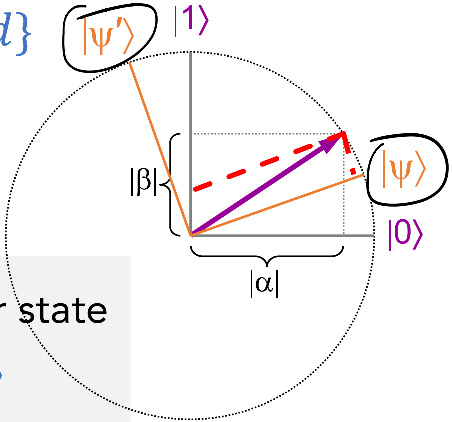
- Geometric picture: projection

$$\Pr(\text{observe } x) = |\alpha_x|^2 = |\langle x|\psi\rangle|^2$$



Measuring in an orthonormal basis

- Recall: orthonormal basis of $\mathbb{C}^d$ $\{|e_j\rangle : j = 1, \dots, d\}$
  - $\forall j, \| |e_j\rangle \| = 1$
  - $\forall i \neq j, \langle e_i | e_j \rangle = 0$ $\quad \{|0\rangle, |1\rangle\}$



	See	w/ probability	posterior state
Measure $\|\psi\rangle$ in $\{\|e_j\rangle\}$ $\mapsto$	j	$\|\langle e_j\|\psi\rangle\|^2$	$\|e_j\rangle$

j is merely a label of $|e_j\rangle$

Measuring in an orthonormal basis

	See	w/ probability	posterior state
Measure $\lvert\psi\rangle$ in $\{\lvert e_j\rangle\}$ $\mapsto$	j	$\lvert\langle e_j\lvert\psi\rangle\rvert^2$	$\lvert e_j\rangle$

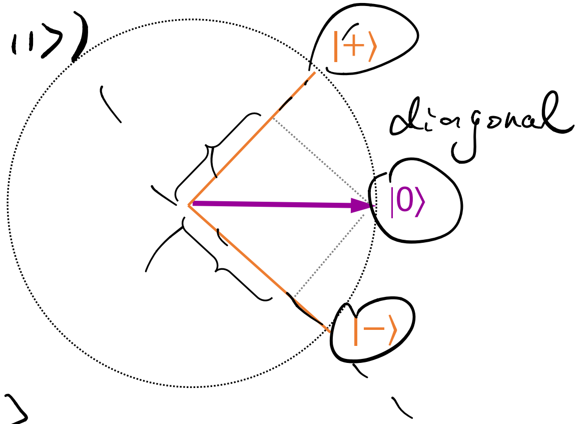
orthonormal

Ex. Measure in $\{\lvert+\rangle, \lvert-\rangle\}$

$\lvert+\rangle = \frac{1}{\sqrt{2}}(\lvert 0\rangle + \lvert 1\rangle)$ $\quad \langle +\lvert -\rangle = 0$

$\lvert-\rangle = \frac{1}{\sqrt{2}}(\lvert 0\rangle - \lvert 1\rangle)$

	See	w/ probability	posterior state
$\lvert+\rangle \mapsto$	$+$	$\lvert\langle +\lvert+\rangle\rvert^2 = 1$	$\lvert+\rangle$
	$-$	$\lvert\langle -\lvert+\rangle\rvert^2 = 0$	$\lvert-\rangle$
$\lvert 0\rangle \mapsto$	$+$	$\lvert\langle +\lvert 0\rangle\rvert^2 = 1/2$	$\lvert+\rangle$
	$-$	$\lvert\langle -\lvert 0\rangle\rvert^2 = 1/2$	$\lvert-\rangle$



$\langle +\lvert 0\rangle$

Implement measurement in arb. basis

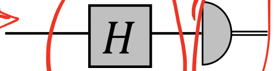
Theorem. Meas. in any $\{|e_j\rangle\}$ $\equiv$ Unitary + standard meas.

- Measure in $\{|+\rangle, |-\rangle\}$

$$|\psi\rangle = \alpha|+\rangle + \beta|-\rangle \overset{?}{\rightarrow} \alpha|0\rangle + \beta|1\rangle$$

"+" $|\alpha|^2$ "−" $|\beta|^2$

$\{|0\rangle, |1\rangle\}$ '0' '1'



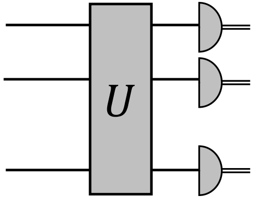
$\mathcal{U}: |+\rangle \mapsto |0\rangle$, $|-\rangle \mapsto |1\rangle$; $\mathcal{U} = H$

$|+\rangle$

$H\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) = |0\rangle$

- General case: measure in $\{|e_j\rangle\}$

$\boxed{U: |e_j\rangle \mapsto |j\rangle}$ $\quad U = \sum_j |j\rangle\langle e_j|$

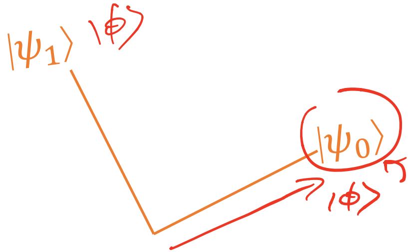


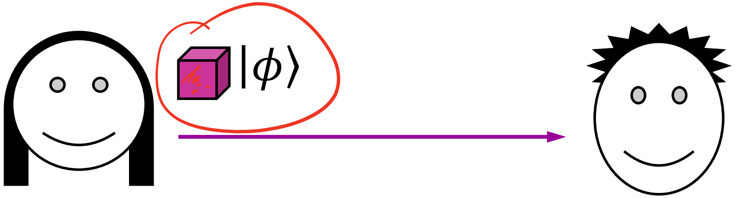
Ex: $\mathcal{U}$ is Unitary

Distinguishing quantum states

Cor. Orthogonal quantum states can be distinguished perfectly

- Given a qubit $|\phi\rangle \in \{|\psi_0\rangle, |\psi_1\rangle\}$ w. $\langle\psi_0|\psi_1\rangle = 0$





?

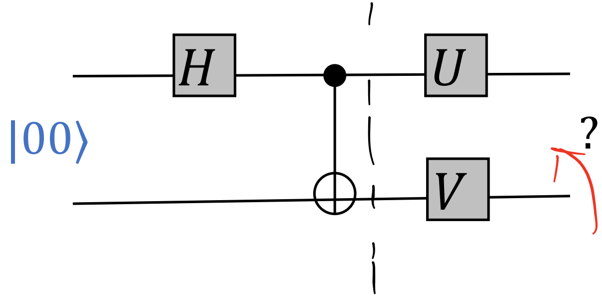
$|\psi_0\rangle$ or $|\psi_1\rangle$

! Measure in $\{|\psi_0\rangle, |\psi_1\rangle\}$

- Given $|\phi\rangle \in |\psi_1\rangle, \dots, |\psi_k\rangle \in \mathbb{C}^d, k \le d.\ \forall i \ne j, \langle\psi_j|\psi_i\rangle = 0$
  - Complete $|\psi_1\rangle, \dots, |\psi_k\rangle$ to an orthonormal basis $\{|\psi_j\rangle : j = 1, \dots, d\}$
  - Measure $|\phi\rangle$ in $\{|\psi_j\rangle : j = 1, \dots, d\}$

Exercise

1



U	V	Output
I	I	? $\vert 00\rangle + \vert 11\rangle$
X	I	? $\vert 10\rangle + \vert 01\rangle$
I	Z	? $\vert 00\rangle - \vert 11\rangle$
$\cancel{Z}$	Z	? $\vert 10\rangle - \vert 01\rangle$

Hint: you will get Bell states

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$(X \otimes I)(|00\rangle + |11\rangle)$$
$$= X \otimes I|00\rangle + X \otimes I|11\rangle$$
$$= |10\rangle + |01\rangle$$

$$X \otimes Z(|00\rangle + |11\rangle)$$
$$= X \otimes Z|00\rangle + X \otimes Z|11\rangle$$
$$= |10\rangle - |01\rangle$$

Exercise

2 Show that the 4 states form an orthonormal basis for 2 qubits

$\frac{1}{\sqrt{2}}$

$|00\rangle + |11\rangle$

$|10\rangle + |01\rangle \to |\phi\rangle$

$|00\rangle - |11\rangle \to |\psi\rangle$

$|10\rangle - |01\rangle$

- normalized
- mut. orthogonal

$\langle 10|\,00\rangle$

Goal:

$$\langle\phi|\psi\rangle = (|10\rangle + |01\rangle)^{\dagger}(|00\rangle - |11\rangle)$$

$$= (\langle 10| + \langle 01|)(|00\rangle - |11\rangle)$$

$$= \underline{(\langle 10|)(|00\rangle)}_{=0} + (\langle 10|)(-|11\rangle)_{=0}$$

$$+ (\langle 01|)(|00\rangle)_{=0} + (\langle 01|)(-|11\rangle)_{=0}$$

$$= 0$$

$(A \otimes B)(C \otimes D) = AC \otimes BD$

$\underline{\langle 10|}\,|00\rangle$

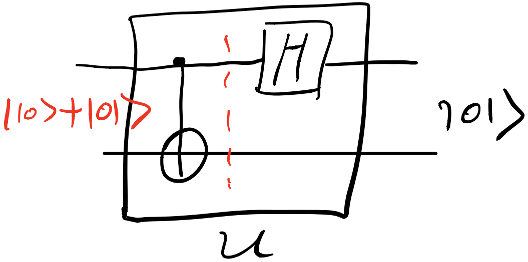
$(\langle 1| \otimes \langle 0|)(|0\rangle \otimes |0\rangle)$

$= \underbrace{\langle 1|0\rangle} \otimes \langle 0|0\rangle = 0$

Exercise

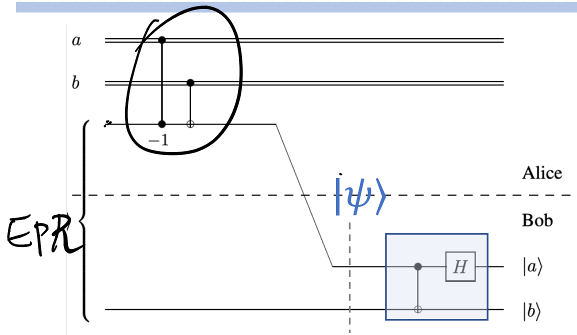
3 Design a circuit to implement the measurement in this basis

$$|00\rangle + |11\rangle \qquad |00\rangle$$
$$|10\rangle + |01\rangle \xrightarrow{U} |01\rangle$$
$$|00\rangle - |11\rangle \qquad |10\rangle$$
$$|10\rangle - |01\rangle \qquad |11\rangle$$

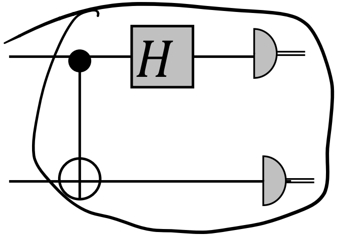


$$\mathrm{CNOT}\,(|10\rangle + |01\rangle)$$
$$= \mathrm{CNOT}\,|10\rangle + \mathrm{CNOT}\,|01\rangle$$
$$= |11\rangle + |01\rangle$$
$$= (|0\rangle + |1\rangle) \otimes |1\rangle \xrightarrow{H \otimes I} |0\rangle|1\rangle$$

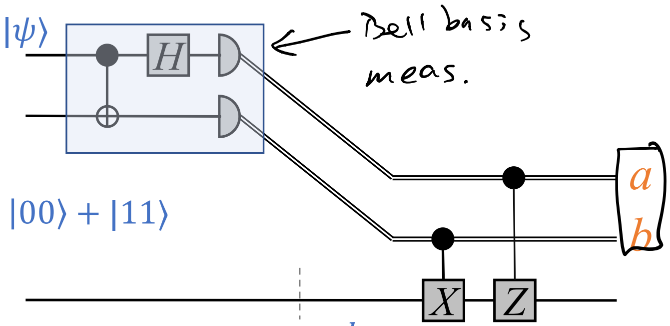
Reflection on superdense coding & teleportation



ab	$\lvert\psi\rangle$
00	$\lvert 00\rangle + \lvert 11\rangle$
01	$\lvert 10\rangle + \lvert 01\rangle$
10	$\lvert 00\rangle - \lvert 11\rangle$
11	$\lvert 10\rangle - \lvert 01\rangle$



Distinguish Bell states



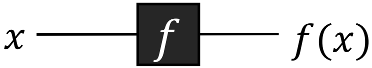
$$|\psi'\rangle = X^a Z^b |\psi\rangle$$

Ex. What is the state of the top 2 qubits after the measurement?

Deutsch's algorithm

Black-box function and query model

Given: a function f as a black box (a.k.a. oracle)



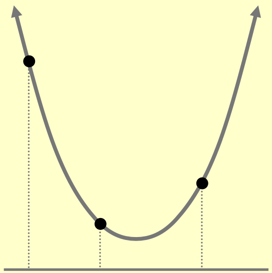
Goal: determine some property about f making as few queries to f (and other operations) as possible

Example. Polynomial interpolation

Let: $f(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_d x^d$

Goal: determine $c_0, c_1, c_2, \ldots, c_d$

Question: How many f-queries does one require for this?

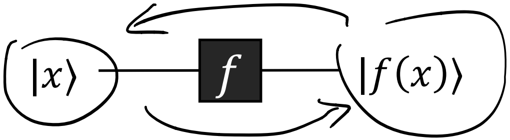


Answer: $d+1$

Quantum black-box function

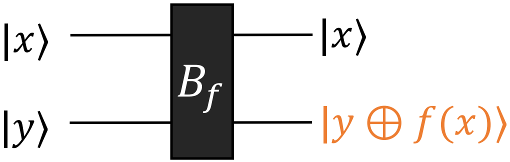
Quantum operations need to be unitary (reversible)

☹ Not reversible



$$f(x) = 1 \quad \forall x$$

☺ Unitary



$$\boxed{B_f} : \underbrace{|x\rangle|y\rangle} \longmapsto |x\rangle|\underbrace{y \oplus f(x)}\rangle \xmapsto{B_f} |x\rangle|y\rangle$$

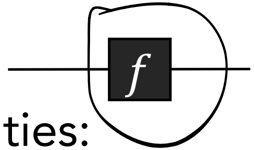
$$\oplus f(x)$$

Can query in superposition

$$\sum_{x,y} \alpha_{xy}|x\rangle|y\rangle \xmapsto{B_f} \sum_{x,y} \alpha_{x,y}|x\rangle|y \oplus f(x)\rangle$$

Deustch's problem

Let $f:\{0,1\} \to \{0,1\}$



There are four possibilities:

x	$f_1(x)$
0	0
1	0

x	$f_2(x)$
0	1
1	1

x	$f_3(x)$
0	0
1	1

x	$f_4(x)$
0	1
1	0

f_1, f_2: Constant

f_3, f_4: Balanced

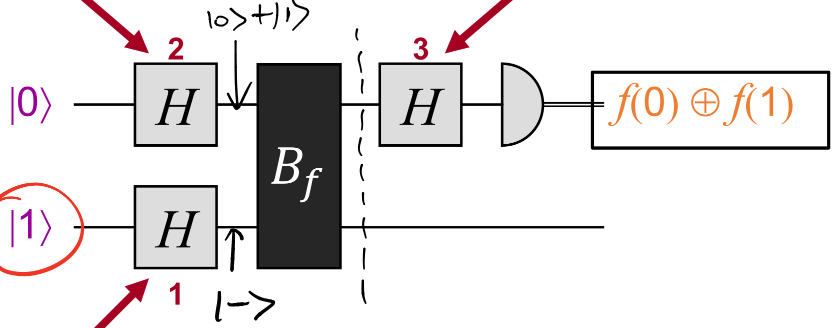
Goal: determine whether or not $f(0) = f(1)$ (i.e. $f(0) \oplus f(1)$) $= \begin{cases} 0 : \text{const} \\ 1 : \text{Bal.} \end{cases}$

- Any classical method requires ***two*** queries
- What about a quantum method?

Summary of Deutsch's algorithm

produces superpositions of inputs to f: $|0\rangle + |1\rangle$

extracts phase differences from $(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$



constructs eigenvector so f-queries induce phases: $|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$

$2 \longrightarrow 1$

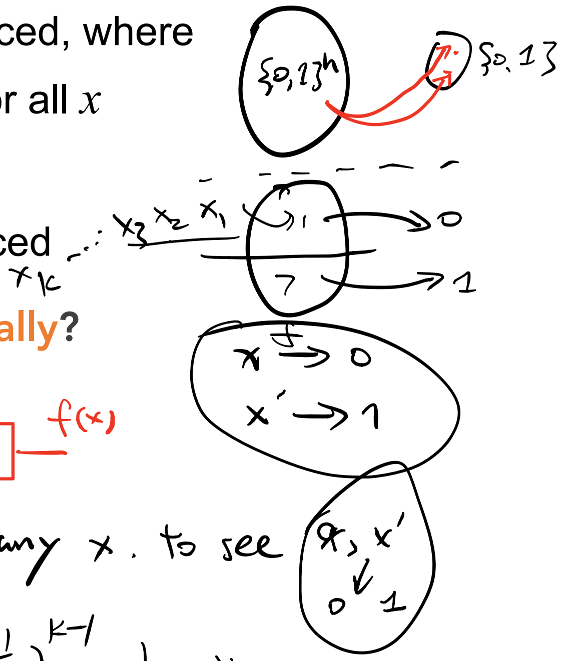
Deutsch-Josza algorithm

Deutsch-Josza problem

Let $f : \boxed{\{0,1\}^n} \to \{0,1\}$ be either constant or balanced, where

- ***constant*** means $f(x) = 0$ for all x, or $f(x) = 1$ for all x
- ***balanced*** means $\Sigma_x\ f(x) = 2^{n-1}$

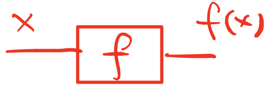
Goal: determine whether f is constant or balanced



- How many queries are there needed classically?

  Deterministic algorithms. $2^n/2+1$

  Randomized algorithms. $\Omega(n)$



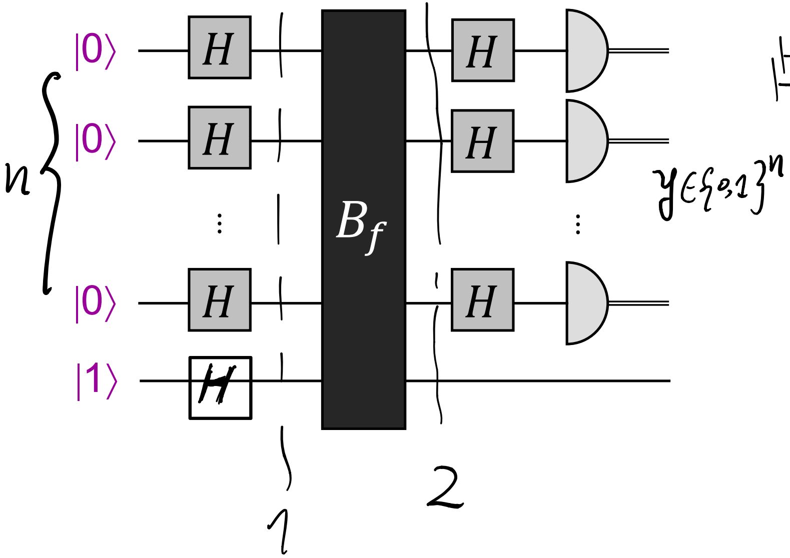
Suppose f bal: pick x at rand. how many x. to see x, x'

BAD

$\Pr[\underbrace{x_1 \cdots x_k \text{ in same half}}] = \left(\frac{1}{2}\right)^{k-1}$ when $k \sim n$

Deutsch-Josza quantum algorithm

1. Q Query suffices



$$|0^n\rangle|1\rangle$$

$$\xrightarrow{H^{\otimes n}\otimes H}\left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right)^{\otimes n}\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

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

$$=\frac{1}{\sqrt{2^{n+1}}}\left(\sum_x|x\rangle\otimes(|0\rangle-|1\rangle)\right)$$

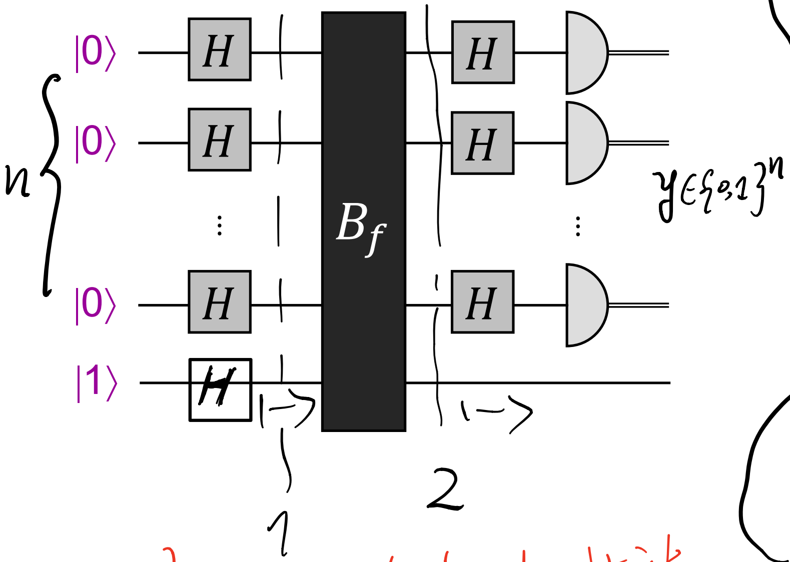
$$=\frac{1}{\sqrt{2^{n+1}}}\underbrace{\sum_x|x\rangle|0\rangle}-\underbrace{\sum_x|x\rangle|1\rangle}$$

Deutsch-Josza quantum algorithm

1. Q Query suffices

$$\xrightarrow{B_f} \frac{1}{\sqrt{2^{n+1}}}\left(\sum_x |x\rangle|0\oplus f(x)\rangle - \sum_x |x\rangle|1\oplus f(x)\rangle\right)$$

$$\overset{2}{=} \frac{1}{\sqrt{2^n}}\left(\sum_x \boxed{(-1)^{f(x)}}|x\rangle\right)\otimes \frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$$

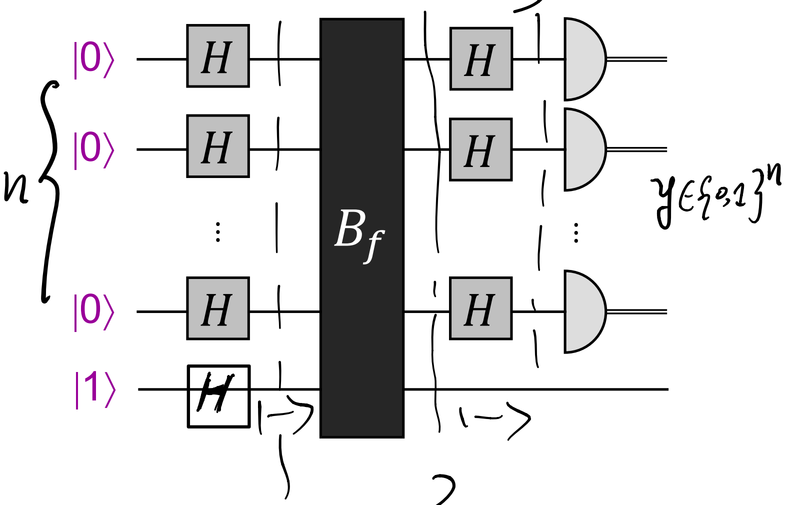


Phase-kick-back trick

$$= \frac{1}{\sqrt{2^{n+1}}} \underline{\sum_x |x\rangle|0\rangle} - \underline{\sum_x |x\rangle|1\rangle}$$

Deutsch-Josza quantum algorithm

1. Q Query Suffices



$$2 = \frac{1}{\sqrt{2^n}}\left(\sum_x \boxed{(-1)^{f(x)}}|x\rangle\right)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

$$\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}}\sum_x (-1)^{f(x)}\,\underline{H^{\otimes n}|x\rangle}$$

$$\boxed{= \frac{1}{2^n}\sum_x (-1)^{f(x)}\sum_y (-1)^{x\cdot y}|y\rangle}$$

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_y (-1)^{x\cdot y}|y\rangle$$

$x\in\{0,1\}^n$

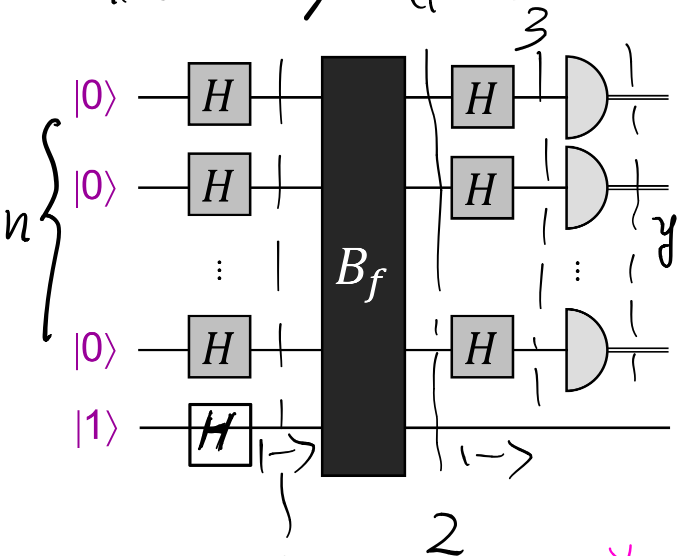
$x, y\in\{0,1\}^n$ $\quad x = x_1\cdots x_n$

$y = y_1\cdots y_n$

$x\cdot y = x_1\cdot y_1 + \cdots + x_n\cdot y_n \mod 2$

Deutsch-Josza quantum algorithm

1. Q Query suffices



$$\boxed{\stackrel{3}{=} \frac{1}{2^n} \sum_x (-1)^{f(x)} \sum_y (-1)^{x\cdot y} |y\rangle}$$

$$= \frac{1}{2^n} \sum_y \underbrace{\left(\sum_x (-1)^{f(x) + x\cdot y} \right)}_{\alpha_y} |y\rangle$$

$\xrightarrow{\text{meas.}}$ see $y \in \{0,1\}^n$

$$\Pr[y] = \left|\frac{1}{2^n} \alpha_y\right|^2$$

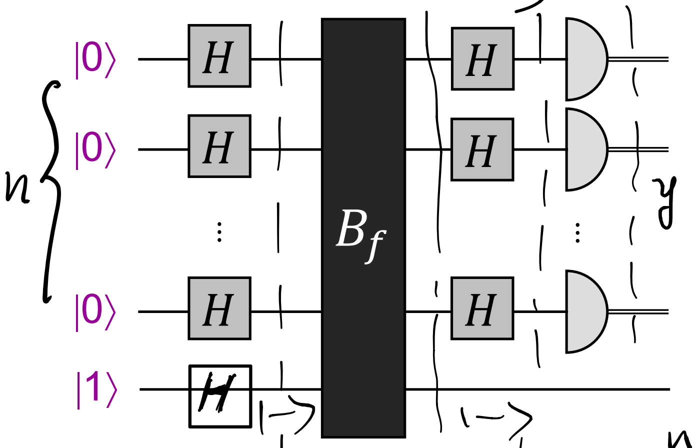
1 $x, y \in \{0,1\}^n$ $\quad x = x_1 \cdots x_n$

$y = y_1 \cdots y_n$

$x \cdot y = x_1 \cdot y_1 + \cdots + x_n \cdot y_n \mod 2$

Deutsch-Josza quantum algorithm

1. Q Query Suffices



$$= \frac{1}{2^n} \sum_y \underbrace{\left(\sum_x (-1)^{f(x)+x\cdot y}\right)}_{\alpha_y} |y\rangle$$

$\xrightarrow{\text{meas.}}$ see $y \in \{0,1\}^n$

$$\Pr[y] = \left|\frac{1}{2^n}\alpha_y\right|^2$$

$\forall x, x\cdot 0^n = 0$

$y = 0^n$: $\alpha_{0^n} = \boxed{\sum_x (-1)^{f(x)}}$

f Bal: $|f^{-1}(1)| = |f^{-1}(0)|$

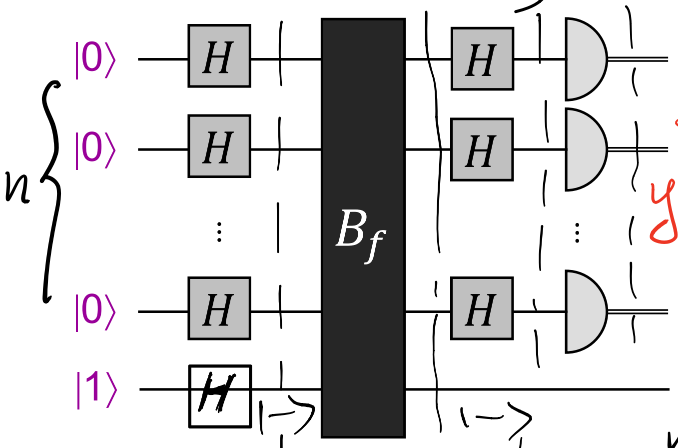
$(-1)^0 = 1$ $\quad (-1)^1 = -1$ $\quad \alpha_{0^n} = 0$

$x, y \in \{0,1\}^n$ $\quad x = x_1 \cdots x_n$, $\quad y = y_1 \cdots y_n$

$x \cdot y = x_1 \cdot y_1 + \cdots + x_n \cdot y_n \mod 2$

Deutsch-Josza quantum algorithm

1. Q Query suffices cont'd



3 $\to |0^n\rangle$

$$y = \begin{cases} 0^n : f \text{ const} \\ \text{else}: f \text{ BAL} \end{cases}$$

• f BAL: $\alpha_{0^n} = 0$

$\Pr[0^n] = 0$ i.e. Never see "0^n" in BAL.

$$\boxed{\alpha_{0^n} = \frac{1}{2^n} \sum_x (-1)^{f(x)}}$$

• f const. $\alpha_{0^n} = \frac{1}{2^n} \sum 1 = \frac{2^n}{2^n} = 1$

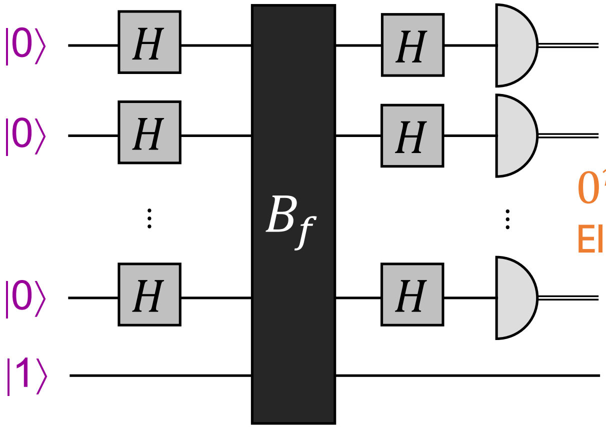
Always see "0^n"

2 $\forall x, x \cdot 0^n = 0$

1 $x, y \in \{0,1\}^n$ $x = x_1 \cdots x_n$ $y = y_1 \cdots y_n$

$x \cdot y = x_1 \cdot y_1 + \cdots + x_n \cdot y_n \bmod 2$

Summary of Deutsch-Josza algorithm



0^n: constant
Else: balanced

Det	Rand	Quantum
$2^n/2+1$	$\Omega(n)$ w.h.p	1 100% correct

Scratch