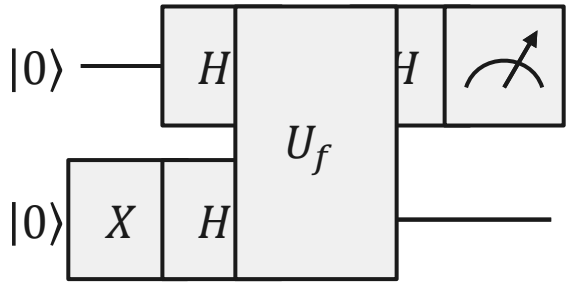
SAJID Lab
Smart & Advanced Junction of Intelligent Devices

EEE 6516 · QUANTUM COMPUTING

Oracles and Phase Kickback

Deutsch, Deutsch–Jozsa and Bernstein–Vazirani

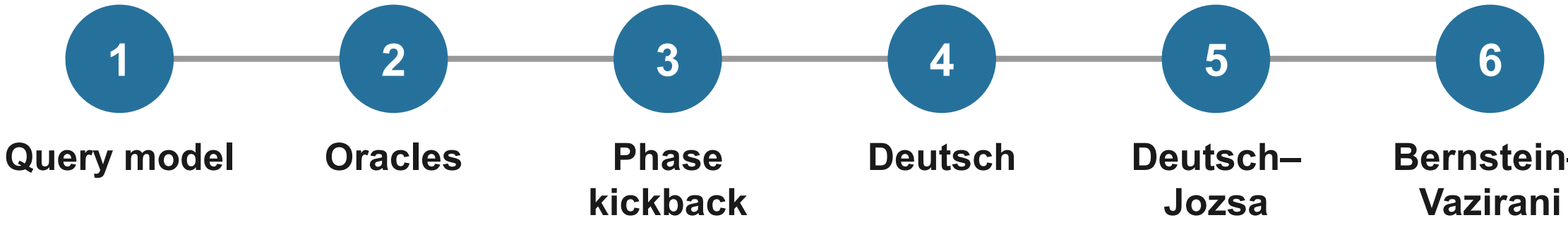


Chapter 5 · Lecture 10

Sajid Muhaimin Choudhury

Copyright © 2026 Sajid Muhaimin Choudhury. All rights reserved.

Today

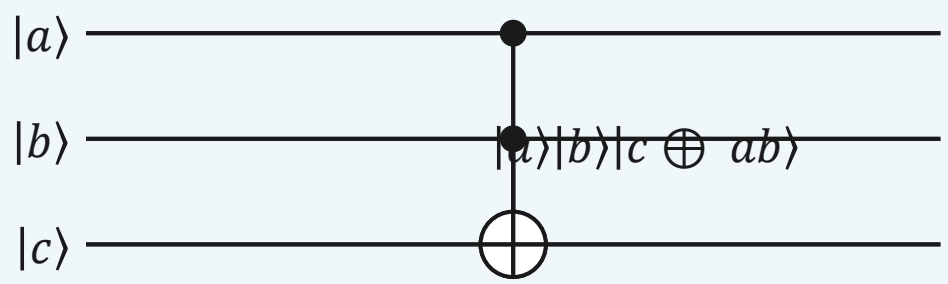


By the end of this lecture you can

- state the query model and build reversible oracles from X, CNOT and Toffoli gates
- derive phase kickback and explain why the ancilla is prepared in $|-\rangle$
- derive the outputs of Deutsch, Deutsch–Jozsa and Bernstein–Vazirani
- compare the query counts honestly with deterministic and randomised classical algorithms

Two tools from Chapter 3

Toffoli: a reversible AND (Ch. 3)



CNOT in the ± basis (Ch. 3)

$$(H \otimes H)\,\mathrm{CNOT}_{01}\,(H \otimes H) = \mathrm{CNOT}_{10}$$

control and target exchange roles

Toffoli keeps its inputs: with c = 0 the target becomes ab.

Keeping the inputs is how any Boolean function becomes reversible.

In the ± basis a CNOT can change its control: the seed of today's main trick.

YOUR TURN · PREDICT

Warm-up: how many classical queries?

Think · 1 minute

A black box computes $f: \{0,1\}^n \to \{0,1\}$. It is promised to be **constant** or **balanced** (0 on exactly half the inputs).

How many evaluations must a deterministic classical algorithm make, in the worst case, for n = 1 and for n = 3?

A 1 and 1

B 2 and 4

C 2 and 5

D 2 and 8

ANSWER

C: 2 for n = 1, and $2^{n-1} + 1 = 5$ for n = 3

n = 1: $f(0)$ says nothing about $f(1)$: two queries.

n = 3: an adversary answers 0 four times; constant and balanced both fit. The fifth answer decides: $2^{n-1} + 1 = 5$.

Today: one quantum query, with certainty.

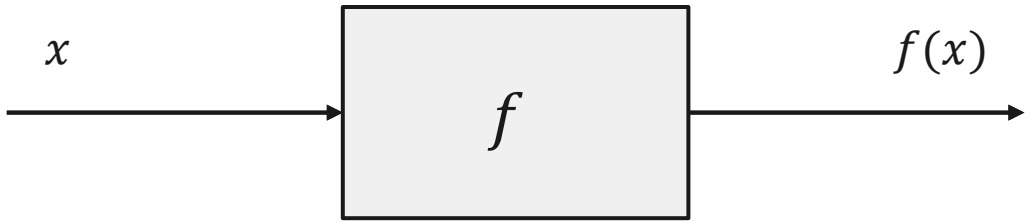
1 The query model and oracles

How do we count the cost, and how does a circuit ask f a question?

The query model: count uses of a black box

Device under test

apply input vectors, read outputs; cost = vectors applied



one use of the box = one query

Oracle: f is known only through its values.

Cost = number of queries; every other operation is free.

Deterministic: always right; worst case counts.

Randomised: may err with a small, fixed probability.

An honest comparison names its classical baseline.

DERIVATION

Reversible oracles: bit oracle and phase oracle

A unitary must be invertible; most functions are not. Keep the input, as Toffoli does.

$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ — bit oracle: keep x, add f(x) to the ancilla

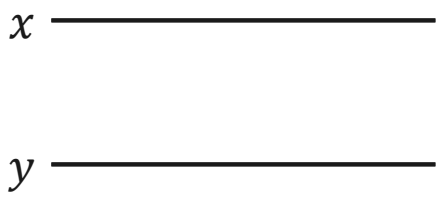
$O_f|x\rangle = (-1)^{f(x)}|x\rangle$ — phase oracle: a sign, no ancilla

$U_f U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x) \oplus f(x)\rangle$ — apply the bit oracle twice

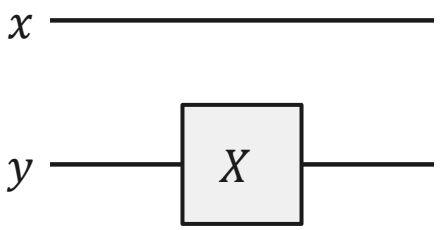
$= |x\rangle|y\rangle$ — f(x) ⊕ f(x) = 0: U_f is its own inverse

U_f permutes basis states, so it is unitary; with y = 0 it writes f(x) into the ancilla.

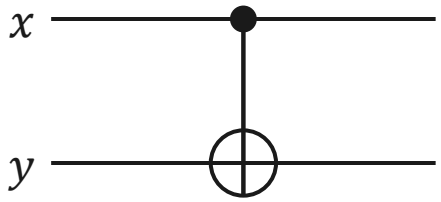
The four one-bit oracles



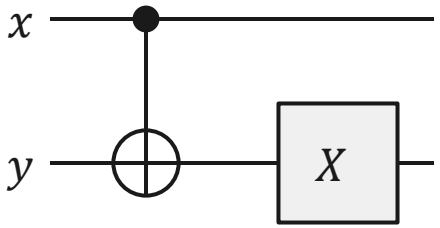
$f(x) = 0$



$f(x) = 1$



$f(x) = x$



$f(x) = \neg x$

Built from X and CNOT; qubit 0 holds x.

$$U_{\neg x} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Each matrix swaps pairs of basis states, so it squares to I.

General recipe: X-gates around a multi-controlled NOT, one per input with f(x) = 1.

COMMON MISTAKE

“A query on a superposition counts as 2^n queries”

✗ 2^n evaluations, all values readable

oracle acts on all 2^n inputs at once

so it was evaluated 2^n times

and every f(x) can be read

Confuses the state with what can be read out.

✓ One use of the box, n bits out

cost = applications of the black box: 1

measuring n qubits gives n bits

f(x) is visible only through interference

This is what the algorithms below exploit.

One application is one query. The values f(x) leave a pattern of signs, read only through interference.

2 Phase kickback

How does f(x) get out of the ancilla and into a phase?

DERIVATION

Phase kickback

Prepare the ancilla in $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.

$U_f|x\rangle|-\rangle = |x\rangle(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle)/\sqrt{2}$

the bit oracle, by linearity in the ancilla

$f(x) = 1: \quad X|-\rangle = (|1\rangle - |0\rangle)/\sqrt{2} = -|-\rangle$

f(x) = 0 changes nothing; f(x) = 1 applies X

$U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$

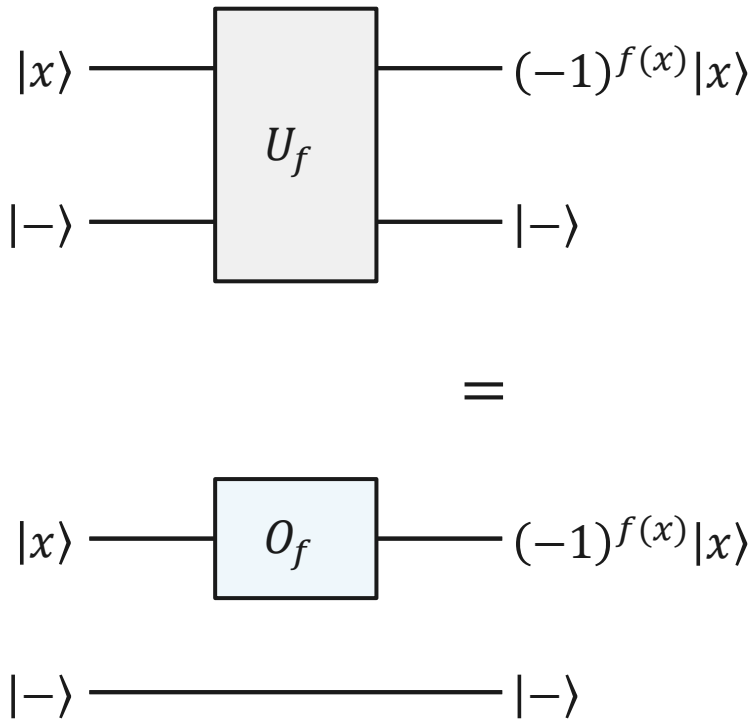
both cases in one formula

$U_f(\sum_x a_x|x\rangle)|-\rangle = \left(O_f \sum_x a_x|x\rangle\right)|-\rangle$

linearity: the phase oracle, ancilla unchanged

f(x) has moved out of the ancilla and into a sign on the input register.

Why the sign matters, and why |−⟩



ancilla untouched: it can be ignored

One basis input: $(-1)^{f(x)}$ is a global phase, invisible.

A superposition: different x get different signs, a relative phase that interference can read.

|−⟩ is the eigenvector of X with eigenvalue −1; the eigenvalue lands on the control (Ch. 3).

Ancilla in |0⟩ or |1⟩: f(x) is written into it, and it becomes entangled with x.

YOUR TURN · PREDICT

Your turn: kickback through a CNOT

Think · 45 seconds

For $f(x) = x$ the bit oracle is CNOT_{01}. What is $\mathrm{CNOT}_{01}|+\rangle|-\rangle$?

A $|+\rangle|-\rangle$ (nothing changes)

B $|-\rangle|-\rangle$

C $|-\rangle|+\rangle$

D an entangled state

ANSWER

B: the control changes, the target does not

$$\mathrm{CNOT}_{01}|+\rangle|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}|-\rangle = |-\rangle|-\rangle$$

Target in $|+\rangle$: $X|+\rangle = |+\rangle$, no kickback; $|+\rangle|+\rangle$ is unchanged.

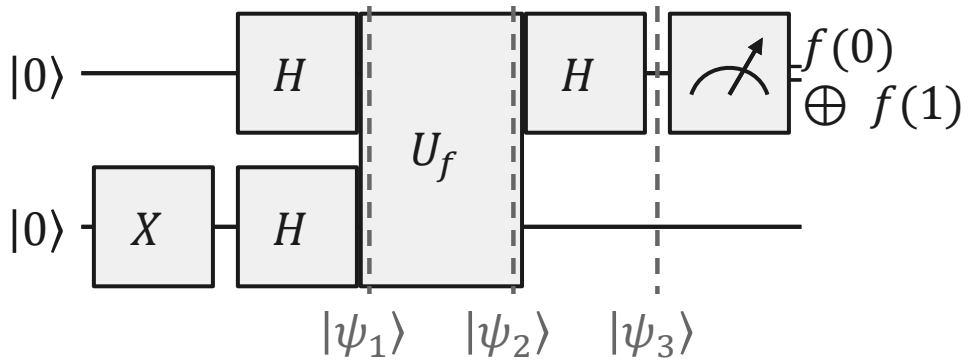
In the ± basis control and target exchange roles (Chapter 3).

Kickback needs the target in an eigenvector of X with eigenvalue −1.

3 Deutsch's algorithm

Can one query tell whether f(0) = f(1)?

Deutsch's problem and circuit



qubit 1 is the ancilla, prepared in $|-\rangle$ by X then H

Given f from one bit to one bit, decide constant or balanced: compute $f(0) \oplus f(1)$.

Classically: two queries; f(0) says nothing about f(1).

Quantum: one query, with certainty (Cleve et al.'s form, ancilla in $|-\rangle$).

DERIVATION

Deutsch's algorithm, slice by slice

$$|\psi_1\rangle = |+\rangle|-\rangle$$ after X and the Hadamards

$$|\psi_2\rangle = \Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big)/\sqrt{2}\,|-\rangle$$ one query, by kickback

$$= (-1)^{f(0)}\big(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\big)/\sqrt{2}\,|-\rangle$$ take out the global sign $(-1)^{f(0)}$

$$|\psi_3\rangle = (-1)^{f(0)}|f(0)\oplus f(1)\rangle|-\rangle$$ H: $|+\rangle \to |0\rangle$ and $|-\rangle \to |1\rangle$

The meter reads f(0) ⊕ f(1) with probability 1, after one query.

YOUR TURN · PREDICT

Predict: Deutsch for f(x) = ¬x

Think · 45 seconds

Run the circuit for $f(0) = 1$, $f(1) = 0$. What does the meter on qubit 0 show?

A 0, with certainty

B 1, with certainty

C 0 or 1, probability ½ each

D 1, but only if the global sign is +1

ANSWER

B: the meter shows 1 with certainty

$$|\psi_2\rangle = \frac{-|0\rangle + |1\rangle}{\sqrt{2}}|-\rangle = -|-\rangle|-\rangle, \qquad |\psi_3\rangle = -|1\rangle|-\rangle$$

The overall −1 = $(-1)^{f(0)}$ is a global phase: no effect on the outcome.

Simulation 5.2 (NumPy and Qiskit): Pr(0) = 1.000 for f = 0, Pr(0) = 1.000 for f = 1, Pr(0) = 0.000 for f = x, Pr(0) = 0.000 for f = ¬x

4 The Deutsch–Jozsa algorithm

What do n Hadamards do, and what can one query decide?

DERIVATION

The Hadamard transform

Bitwise inner product: $x \cdot z = x_0 z_0 \oplus x_1 z_1 \oplus \cdots \oplus x_{n-1} z_{n-1}$, the parity of the bitwise AND.

$H|x\rangle = (|0\rangle + (-1)^x |1\rangle)/\sqrt{2} = \sum_z (-1)^{xz} |z\rangle/\sqrt{2}$ — one qubit, z ∈ {0, 1}

$H^{\otimes n}|x\rangle = (H|x_0\rangle) \otimes \cdots \otimes (H|x_{n-1}\rangle)$ — n independent qubits

$= 2^{-n/2} \sum_z (-1)^{x_0 z_0 + \cdots + x_{n-1} z_{n-1}} |z\rangle$ — expand: one term per string z

$= 2^{-n/2} \sum_z (-1)^{x \cdot z} |z\rangle$ — only the parity of the exponent matters

$H^{\otimes n}|0^n\rangle = 2^{-n/2} \sum_z |z\rangle$ — x = 0^n: the uniform superposition

The Walsh–Hadamard transform

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

rows: the Walsh functions; row z holds $(-1)^{x \cdot z}$

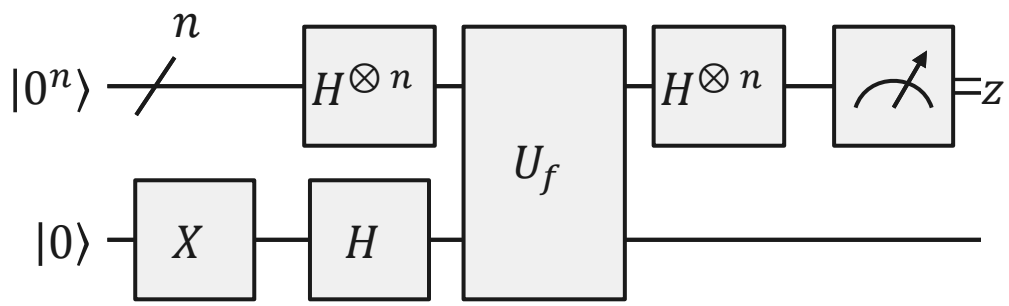
The rows of $H^{\otimes n}$ are the Walsh functions, used for example as CDMA spreading codes.

Deutsch–Jozsa reads the "DC" coefficient of the ±1 sequence $(-1)^{f(x)}$.

Bernstein–Vazirani finds the single non-zero coefficient of a linear f.

The analogy breaks at the cost: one query, one sample of |spectrum|², not the whole spectrum.

Deutsch–Jozsa: the problem and the circuit



the slashed wire carries n qubits, each measured

Promise: f is **constant** (same value on all 2^n inputs) or **balanced** (0 on exactly half).

Task: decide which.

Circuit: Deutsch's circuit with an n-qubit register.

Classical deterministic cost: $2^{n-1} + 1$ queries (the warm-up).

DERIVATION

Deutsch–Jozsa: the amplitude of 0^n

$2^{-n/2}\sum_x(-1)^{f(x)}|x\rangle$ — after $H^{\otimes n}$ and one query (kickback)

$\sum_z\left(2^{-n}\sum_x(-1)^{f(x)\oplus x\cdot z}\right)|z\rangle$ — the last Hadamards (the transform)

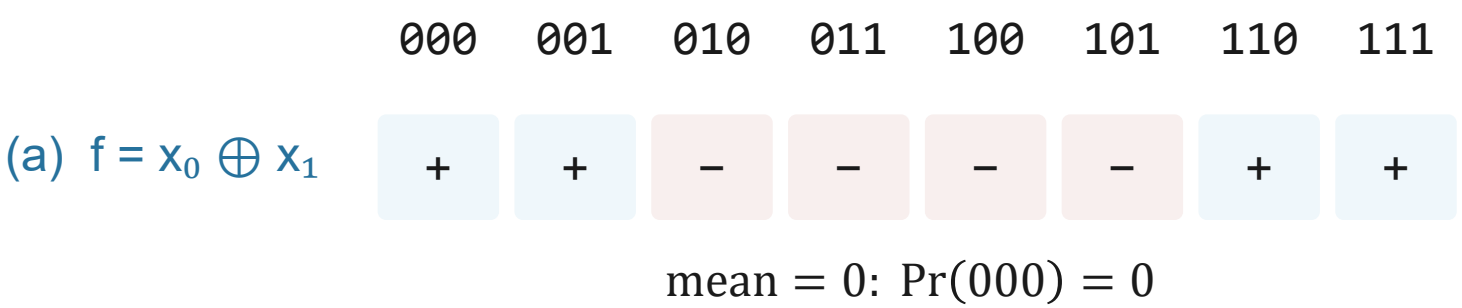
$\Pr(0^n)=\left|2^{-n}\sum_x(-1)^{f(x)}\right|^2$ — $z = 0^n$: $x\cdot z = 0$ for every x

$\text{constant: } |\pm 1|^2 = 1 \quad \text{balanced: } 0$ — the mean of the ±1 values

One query decides with certainty: 0^n means constant; any other string means balanced.

WORKED EXAMPLE · STEP 1 OF 3

Worked example: Deutsch–Jozsa for n = 3

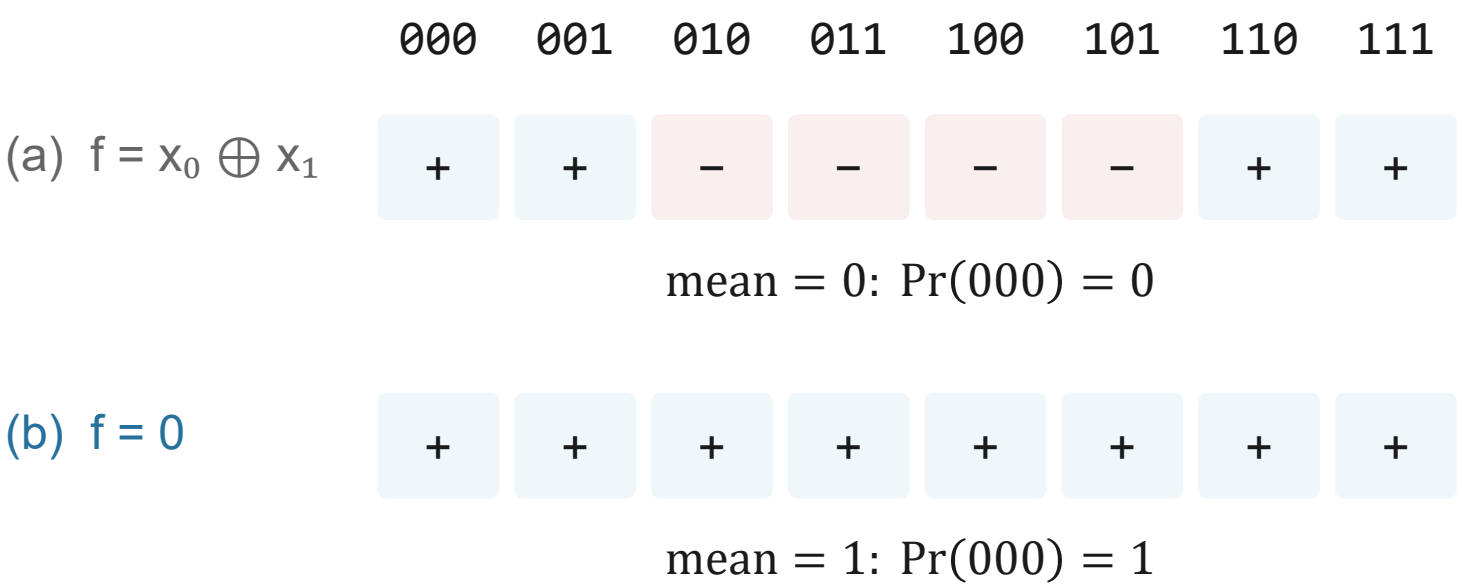


1 (a) $f = x_0 \oplus x_1 = s \cdot x$, $s = 110$: signs cancel at 000; the register ends in $|110\rangle$.

Before the next slide

What does f = 0 give?

Worked example: Deutsch–Jozsa for n = 3



1 (a) $f = x_0 \oplus x_1 = s \cdot x$, s = 110: signs cancel at 000; the register ends in $|110\rangle$.

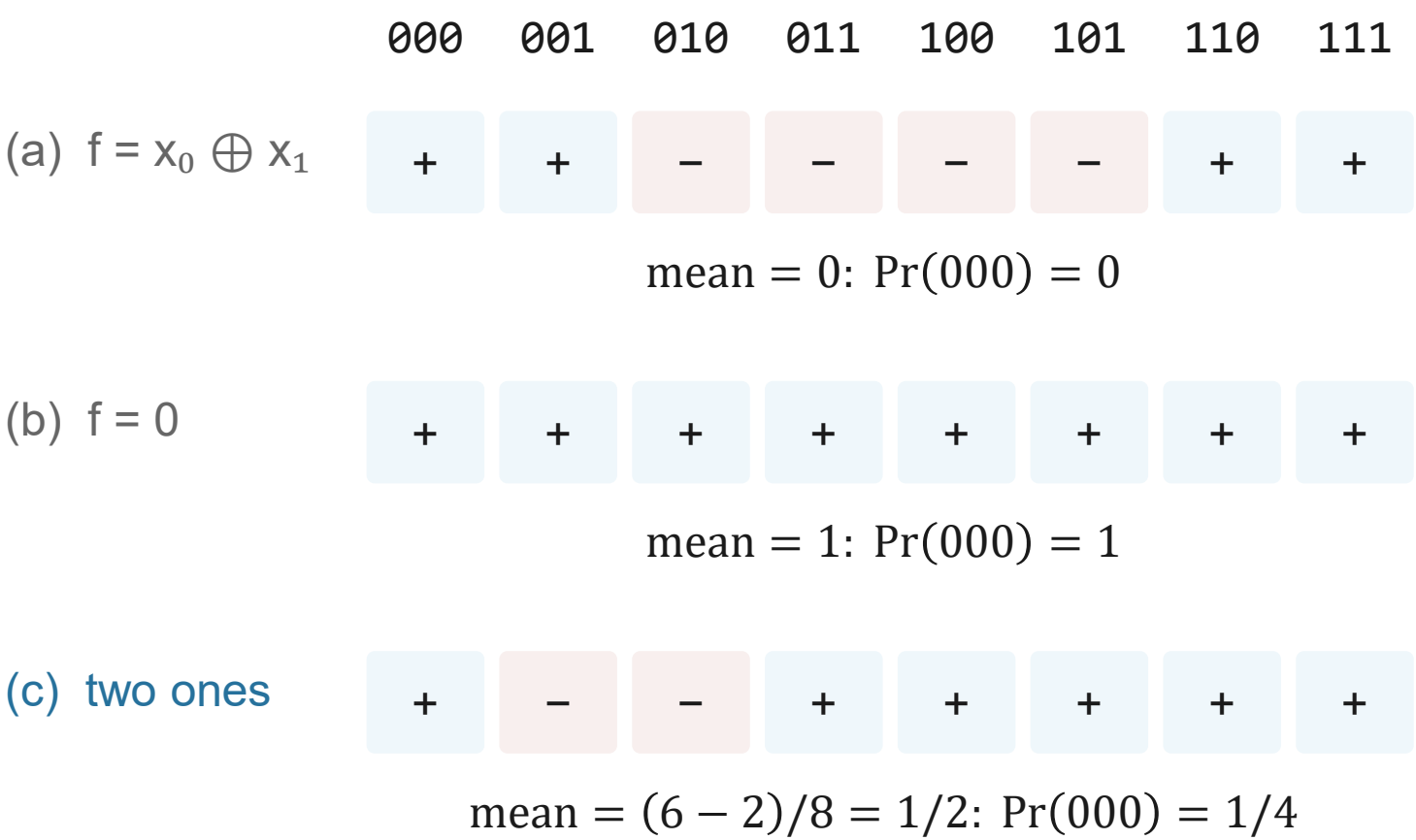
2 (b) f = 0: eight +1s, mean 1, so the output is 000 with certainty.

Before the next slide

A function with exactly two ones?

WORKED EXAMPLE · STEP 3 OF 3

Worked example: Deutsch–Jozsa for n = 3



1 (a) f = $x_0 \oplus x_1$ = s·x, s = 110: signs cancel at 000; the register ends in |110⟩.

2 (b) f = 0: eight +1s, mean 1, so the output is 000 with certainty.

3 (c) Outside the promise: mean ½, Pr(000) = ¼; the answer can be wrong.

YOUR TURN · PREDICT

Predict: a constant function f = 1, n = 3

Think · 45 seconds

Run Deutsch–Jozsa with $f(x) = 1$ for every x. Which string does the register show?

A 111

B 000

C a random string

D 000 or 111, probability ½ each

ANSWER

B: 000, for every constant function

The mean of eight −1s is −1, so Pr(000) = |−1|² = 1.

The register returns to $H^{\otimes 3}H^{\otimes 3}|000\rangle = |000\rangle$ up to the global sign $(-1)^f$.

Simulation 5.3: f = 0 and f = 1 both give 000 in 1000 of 1000 shots.

The output is not f: a constant function always gives 0^n.

Simulation 5.3: three balanced functions

function	output	counts
f = 0	000	1000
f = 1	000	1000
$x_0 \oplus x_1$	110	1000
x_2	001	1000
ones 000,011,101,110	111	1000

Balanced functions never give 000.

These three have the form $s \cdot x \oplus c$, and each returns its s with certainty: 110, 001, 111. Finding s is the next algorithm.

What the separation is, and what it is not

Deterministic classical

$$2^{n-1} + 1 \text{ queries}$$

Randomised classical, k queries

$$\text{error } 2 \cdot 2^{-k} = 2^{1-k}$$

Quantum

$$1 \text{ query, no error}$$

Randomised: query k random inputs; answer 'constant' if all agree.

Wrong only if f is balanced and all k agree: 2^{1-k}. k = 11 gives less than 10^{-3}.

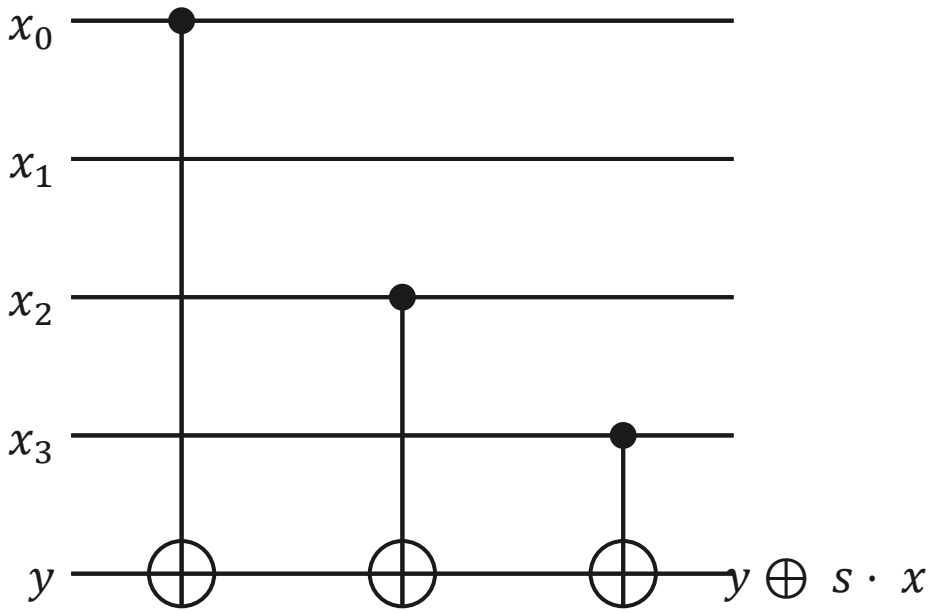
So the exponential gap is between exact algorithms; with a tiny allowed error it is a constant.

Deutsch–Jozsa matters as the cleanest demonstration of interference, not as a useful problem.

5 The Bernstein–Vazirani algorithm

Can one query find a hidden n-bit string?

Bernstein–Vazirani: find the hidden string



s = 1011: one CNOT from each qubit i with $s_i = 1$

$f(x) = s \cdot x$ for a hidden n-bit string s; find s.

Classically: one query returns one bit, so n queries (ask 10…0, 01…0, …).

The oracle is a parity of selected bits: CNOTs onto the ancilla.

Quantum: the Deutsch–Jozsa circuit, unchanged, one query.

DERIVATION

Why one query returns s

$$2^{-n/2}\sum_x (-1)^{s\cdot x}|x\rangle$$

after one query: kickback with f(x) = s·x

$$= H^{\otimes n}|s\rangle$$

the Hadamard transform, read backwards

$$H^{\otimes n}H^{\otimes n}|s\rangle = |s\rangle$$

the final Hadamards: $H^{\otimes n}$ is its own inverse

One query returns s with certainty; a classical algorithm needs n.

YOUR TURN · PREDICT

Predict: what does Qiskit print?

Think · 45 seconds

Run Bernstein–Vazirani with $s = 1011$, measuring qubit i into classical bit i. Which string does Qiskit print?

A '1011'

B '1101'

C '0100'

D '0010'

ANSWER

B: '1101', the same result written in reverse

Qiskit prints classical bit 0 **rightmost**: textbook $q_0 q_1 q_2 q_3 = 1011$ appears as '1101'.

Reading '1101' as s is the ordering error of Chapter 3: wrong for any s that is not a palindrome.

A palindrome such as 1001 would hide the error; 1011 does not. Always test with an asymmetric s.

SIMULATION · LIVE

Simulation 5.4: Bernstein–Vazirani in Qiskit

```
s = "1011"
qc.x(n)
qc.h(range(n + 1))
for i, bit in enumerate(s):
    if bit == "1":
        qc.cx(i, n)
qc.h(range(n))
qc.measure(range(n), range(n))
tb = {k[::-1]: v for k, v in raw.items()}
```

100 shots, seed 6554; qubit 4 is the ancilla.

The last line reverses each key into textbook order.

```
Qiskit counts   : {'1101': 100}
textbook order  : {'1011': 100}
```

Recap

1. **Query model**
   cost = uses of the black box; name the classical baseline

2. **Phase kickback**
   ancilla in $|-\rangle$: $U_f \rightarrow O_f$, the value becomes a sign

3. **Deutsch–Jozsa**
   one query: 0^n iff constant; exact vs randomised baseline

4. **Bernstein–Vazirani**
   one query returns s; read the bit order

Next: Lecture 11 (Week 8)

Grover search: finding a marked item in about √N queries

Read: handout 5.1–5.6; 5.9 is self-study. No lectures in Week 7.

Exit ticket

Run Deutsch–Jozsa with $n = 2$ and $f(x) = x_1$. Which string does the register show, and why?

Copyright © 2026 Sajid Muhaimin Choudhury. All rights reserved.

Rights and attributions

Copyright (c) 2026 Sajid Muhaimin Choudhury. All rights reserved.

Public edition of Lecture 10: Oracles and Phase Kickback. Release qc-2026-10-15, prepared 2026-10-15 from source revision 3df9449aa6.

This edition omits speaker notes, instructor-only material and every figure whose publication rights are not cleared for public distribution.