Introduction to Quantum Information Processing

QIC 710 / CS 768 / PH 767 / CO 681 / AM 871

Lecture 4 (2017)

Jon Yard
QNC 3126
jyard@uwaterloo.ca
http://math.uwaterloo.ca/~jyard/qic710

Rooms and enrollment cap

Sept. 19	QNC 1501	Sept. 21	MC 4058
Sept. 26	QNC 1501	Sept. 28	QNC 0101
Oct. 3	TBD	Oct. 5	QNC 1501
Oct. 10	QNC 0101	Oct. 12	QNC 0101
Oct. 17	QNC 0101	Oct. 19	QNC 0101
Oct. 24	QNC 0101	Oct. 26	QNC 1501
Oct. 31	QNC 0101	Nov. 2	QNC 0101
Nov. 7	QNC 0101	Nov. 9	QNC 0101
Nov. 14	QNC 0101	Nov. 16	QNC 0101
Nov. 21	QNC 0101	Nov. 23	QNC 0101
Nov. 28	QNC 0101	Nov. 30	QNC 0101

Enrollment cap raised from 50 to 60. Spaces available in CO 681 and in QIC 710.

Webpage and homework

http://math.uwaterloo.ca/~jyard/qic710

I will **not** be posting new assignments and lecture slides to LEARN. We would like to receive electronic submissions via LEARN or email if possible, though paper will be accepted in class. No poorly formatted phone pictures please!! If you discuss the homework with other classmates, please write up your own solutions and mention who you worked with in your writeup.

4. **Distinguishing nonorthogonal states (20%).** Suppose a qubit is prepared in the state $|\psi_a\rangle$ with probability $\Pr\left(|\psi_a\rangle\right)$, where $a = 0, 1$ and $\Pr\left(|\psi_0\rangle\right) + \Pr\left(|\psi_1\rangle\right) = 1$. Consider the following procedure for identifying the state: Perform a measurement in some orthogonal basis $|\phi_0\rangle$, $|\phi_1\rangle$ and declare the state to have been $|\psi_a\rangle$ if the outcome is $|\phi_a\rangle$. The average probability that this procedure succeeds in correctly identifying the state, averaged over the preparation probabilities, is

$$\begin{aligned}
\Pr(\text{correct}) &= \Pr\left(\text{correct and } |\psi_0\rangle \text{ had been prepared}\right) \\
&\quad + \Pr\left(\text{correct and } |\psi_1\rangle \text{ had been prepared}\right) \\
&= \Pr\left(\text{correct} \,\middle|\, |\psi_0\rangle \text{ had been prepared}\right) \Pr\left(|\psi_0\rangle\right) \\
&\quad + \Pr\left(\text{correct} \,\middle|\, |\psi_1\rangle \text{ had been prepared}\right) \Pr\left(|\psi_1\rangle\right) \\
&= |\langle\phi_0|\psi_0\rangle|^2 \Pr\left(|\psi_0\rangle\right) + |\langle\phi_1|\psi_1\rangle|^2 \Pr\left(|\psi_1\rangle\right).
\end{aligned}$$

   (a) Find $|\phi_0\rangle$ and $|\phi_1\rangle$ that maximize the average success probability when $|\psi_0\rangle = |0\rangle$ or $|\psi_1\rangle = |+\rangle$ are prepared with equal probabilities $\Pr\left(|\psi_0\rangle\right) = \Pr\left(|\psi_1\rangle\right) = \frac{1}{2}$. What is the optimal success probability?

   (b) Same question, but with $\Pr\left(|\psi_0\rangle\right) = \frac{3}{4}$ and $\Pr\left(|\psi_1\rangle\right) = \frac{1}{4}$.

5. **Entanglement swapping (20%).** Let $|\Psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ be the Bell state. We can express the Bell basis as

$$|\Psi_{ab}\rangle := (Z^b X^a \otimes I)|\psi\rangle = \begin{cases} \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle & ab = 00 \\ \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle & ab = 01 \\ \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle & ab = 10 \\ \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle & ab = 11. \end{cases}$$

   (a) Rewrite the tensor product of two Bell states in the form

$$|\Psi\rangle^{12}|\Psi\rangle^{34} = \frac{1}{2}|\Psi_{00}\rangle^{23}|\phi_{00}\rangle^{14} + \frac{1}{2}|\Psi_{01}\rangle^{23}|\phi_{01}\rangle^{14} + \frac{1}{2}|\Psi_{10}\rangle^{23}|\phi_{10}\rangle^{14} + \frac{1}{2}|\Psi_{11}\rangle^{23}|\phi_{11}\rangle^{14}$$

   for some states $|\phi_{ab}\rangle$, where the superscripts label the four qubits. Note that the order of the qubits is changed on the right hand side of this equation. This means that you should use the identity $|abcd\rangle^{1234} = |bcad\rangle^{2314}$ in going from the left to the right side.

   (b) If one does a Bell measurement on qubits 2 and 3, each of the four possible outcomes occurs with equal probability. What is the state of qubits 1 and 4 when the outcome of the Bell measurement is the state $|\Psi_{ab}\rangle$?

Simple quantum algorithms in the query scenario

Query scenario

Input: a function f, given as a black box (a.k.a. oracle)

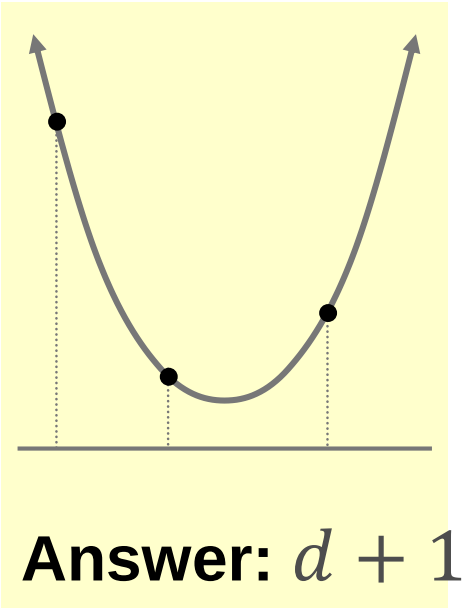
Goal: determine some information about f making as few queries to f (and other operations) as possible

Example: polynomial interpolation

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

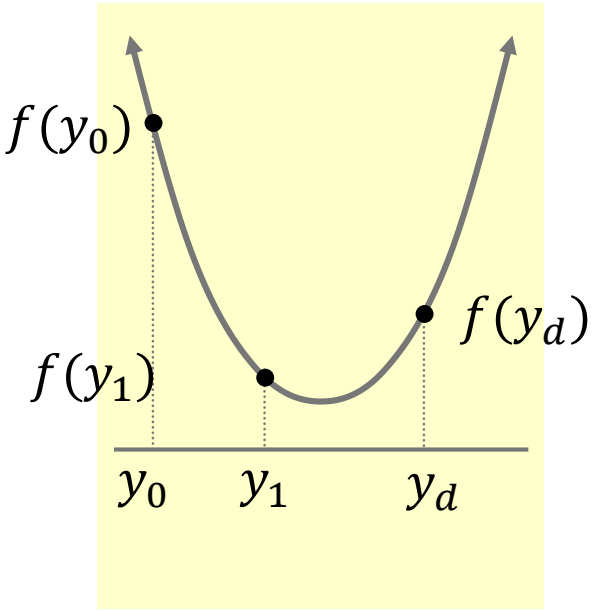
Goal: Determine $c_0, c_1, c_2, \ldots, c_d$.

Question: How many queries of f does this require?



Answer: $d + 1$

Proof



$$\begin{pmatrix} y_0^d & y_0^{d-1} & \cdots & 1 \\ y_1^d & y_1^{d-1} & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ y_d^d & y_d^{d-1} & \cdots & 1 \end{pmatrix} \begin{pmatrix} c_d \\ c_{d-1} \\ \vdots \\ c_0 \end{pmatrix} = \begin{pmatrix} f(y_0) \\ f(y_1) \\ \vdots \\ f(y_d) \end{pmatrix}$$

Vandermonde matrix

Deutsch’s problem

Deutsch'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

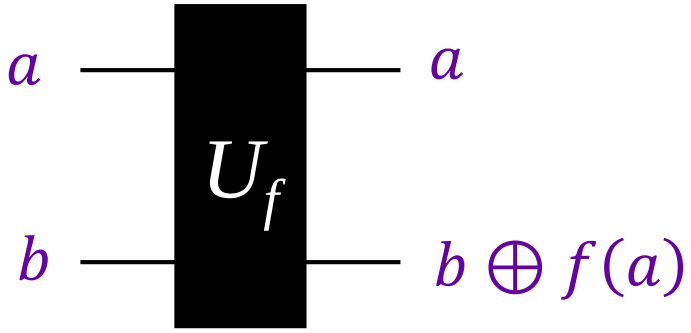
Goal:

Determine whether or not $f(0) = f(1)$ (i.e. $f(0) \oplus f(1) = 0$).
Or in other words, whether $f \in \{f_1, f_2\}$ or $f \in \{f_3, f_4\}$.

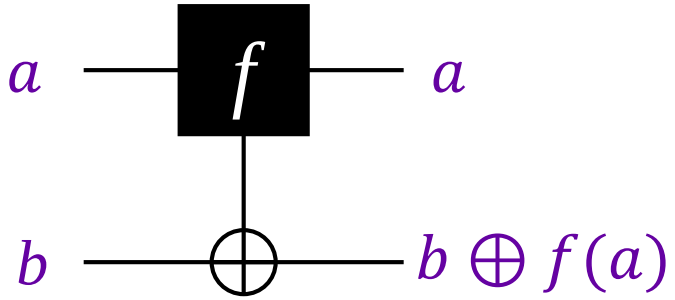
Any classical method requires ***two*** queries.

What about a quantum method?

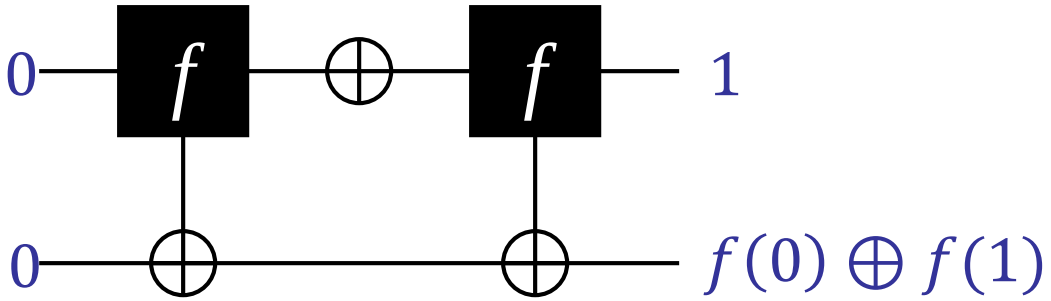
Reversible black box for f



alternate notation:

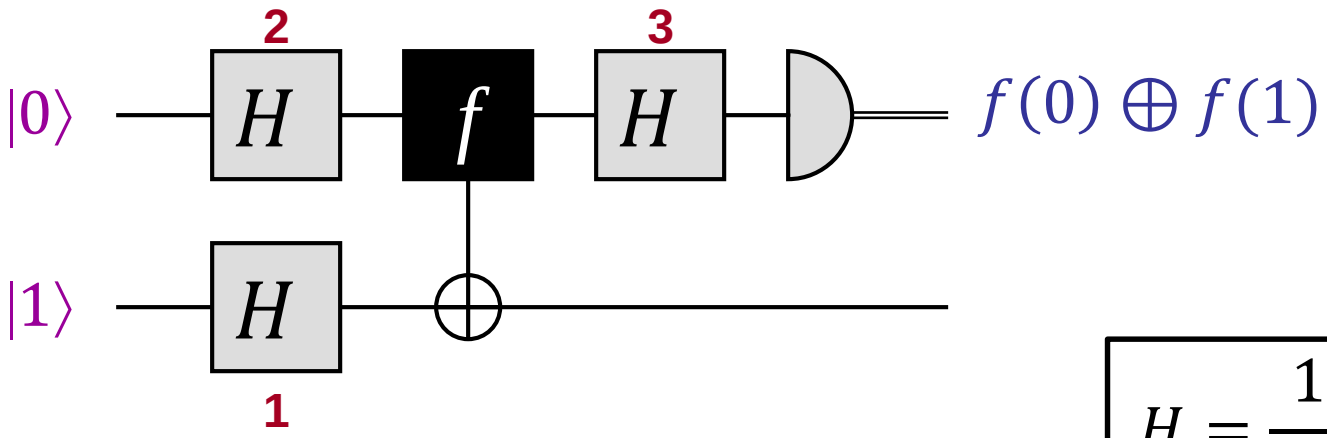


A classical algorithm:
(still requires 2 queries)



2 queries + **1** auxiliary operation

Quantum algorithm for Deutsch



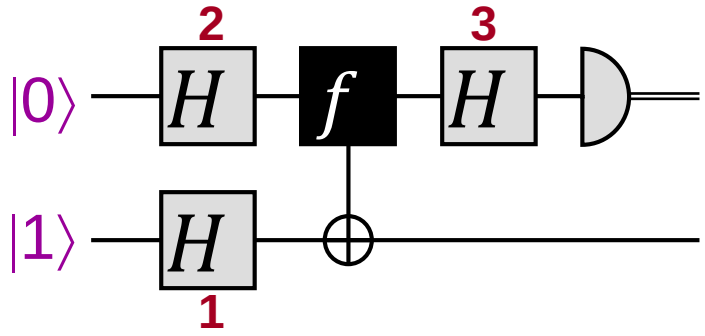
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

1 query + **4** auxiliary operations

How does this algorithm work?

Each of the three H operations can be seen as playing a different role ...

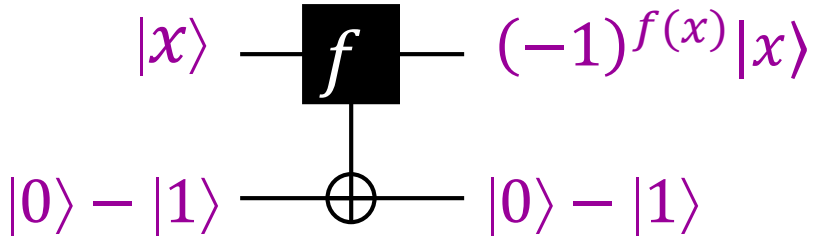
Quantum algorithm (1)



1. Creates the state $|0\rangle - |1\rangle$, which is an eigenvector of

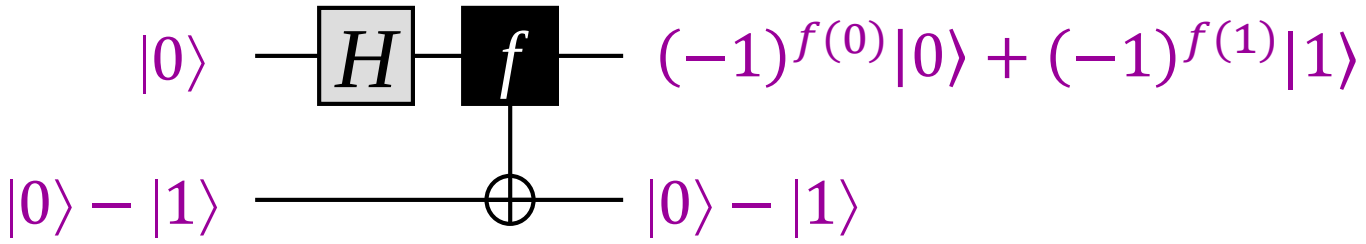
$$\begin{cases} \boldsymbol{NOT} = \boldsymbol{X} & \text{with eigenvalue } -1 \\ \boldsymbol{I} & \text{with eigenvalue } +1 \end{cases}$$

This causes f to induce a ***phase shift*** of $(-1)^{f(x)}$ to $|x\rangle$



Quantum algorithm (2)

2. Causes f to be queried ***in superposition*** (at $|0\rangle + |1\rangle$)



x	$f_1(x)$
0	0
1	0

x	$f_2(x)$
0	1
1	1

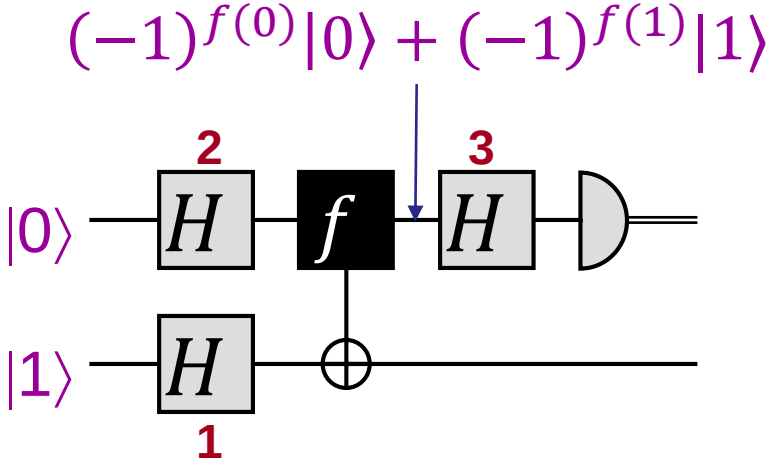
$\pm(|0\rangle + |1\rangle)$

x	$f_3(x)$
0	0
1	1

x	$f_4(x)$
0	1
1	0

$\pm(|0\rangle - |1\rangle)$

Quantum algorithm (3)



3. Distinguishes between $\pm(|0\rangle + |1\rangle)$ and $\pm(|0\rangle - |1\rangle)$

$$\pm(|0\rangle + |1\rangle) \xleftrightarrow{H} \pm|0\rangle$$

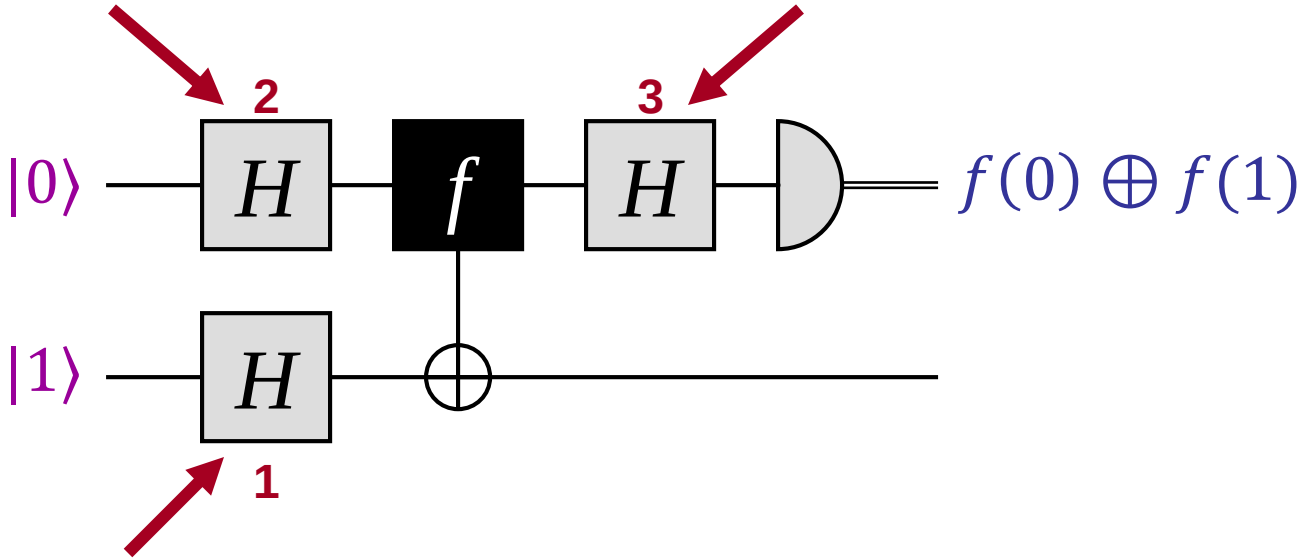
$$\pm(|0\rangle - |1\rangle) \xleftrightarrow{H} \pm|1\rangle$$

Summary of Deutsch's algorithm

Makes only one query, whereas two are needed classically

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

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



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

One-out-of-four search

One-out-of-four search

Let $f : \{0,1\}^2 \to \{0,1\}$ have the property that there is exactly one $x \in \{0,1\}^2$ with $f(x) = 1$.

4 possibilities

x	$f_{00}(x)$
00	1
01	0
10	0
11	0

x	$f_{01}(x)$
00	0
01	1
10	0
11	0

x	$f_{10}(x)$
00	0
01	0
10	1
11	0

x	$f_{11}(x)$
00	0
01	0
10	0
11	1

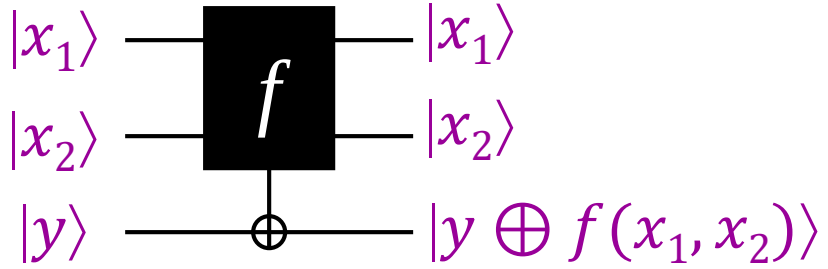
Goal: Find the $x \in \{0,1\}^2$ such that $f(x) = 1$.
In other words, determine if $f = f_{00}$, $f = f_{01}$, $f = f_{10}$ or $f = f_{11}$.

What is the minimum number of queries ***classically?*** ____

Quantumly? ____

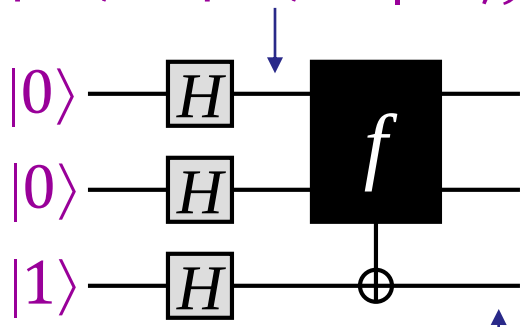
Quantum algorithm (I)

Black box for 1-4 search:



Start by creating phases in superposition of all inputs to f:

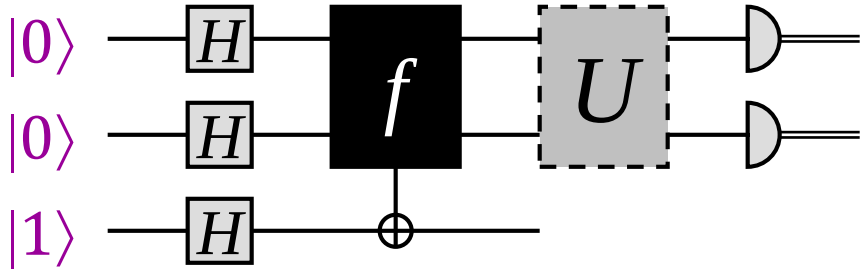
$(|00\rangle + |01\rangle + |10\rangle + |11\rangle)(|0\rangle - |1\rangle)$ ***Input*** state to query?



Output state of query?

$((-1)^{f(00)}|00\rangle + (-1)^{f(01)}|01\rangle + (-1)^{f(10)}|10\rangle + (-1)^{f(11)}|11\rangle)(|0\rangle - |1\rangle)$

Quantum algorithm (II)



← Apply the U that maps

← $|\psi_{00}\rangle$, $|\psi_{01}\rangle$, $|\psi_{10}\rangle$, $|\psi_{11}\rangle$ to

← $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ (resp.)

Output state of the first two qubits in the four cases:

Case of f_{00}? $|\psi_{00}\rangle = -|00\rangle + |01\rangle + |10\rangle + |11\rangle$

Case of f_{01}? $|\psi_{01}\rangle = +|00\rangle - |01\rangle + |10\rangle + |11\rangle$

Case of f_{10}? $|\psi_{10}\rangle = +|00\rangle + |01\rangle - |10\rangle + |11\rangle$

Case of f_{11}? $|\psi_{11}\rangle = +|00\rangle + |01\rangle + |10\rangle - |11\rangle$

What noteworthy property do these states have? **Orthogonal!**

Challenge Exercise: simulate the above U in terms of H, CNOT and NOT gates

one-out-of-N search?

Natural question: what about search problems in spaces larger than ***four*** (and without uniqueness conditions)?

For spaces of size ***eight*** (say), the previous method breaks down—the state vectors will not be orthogonal.

Later on, we'll see how to search a space of size N with $O(\sqrt{N})$ queries ...

Constant vs. balanced

Constant vs. balanced

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

- ***constant*** means $f(x) = 0$ for all x, or $f(x) = 1$ for all x.
- ***balanced*** means $\sum_x f(x) = 2^{n-1}$ (i.e. half 0s, half 1s).

Goal: Determine whether f is constant or balanced.

How many queries are needed ***classically?*** ____

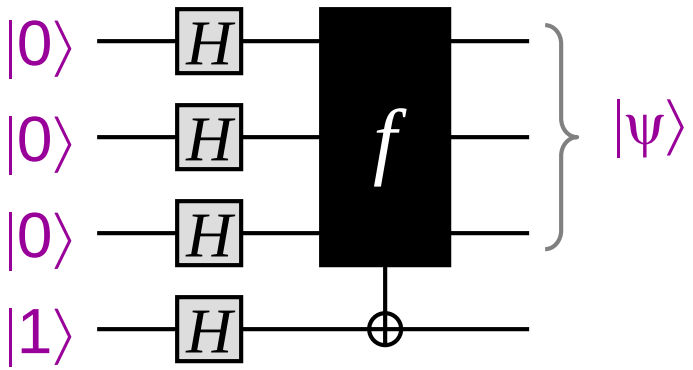
Example: It could still be either if

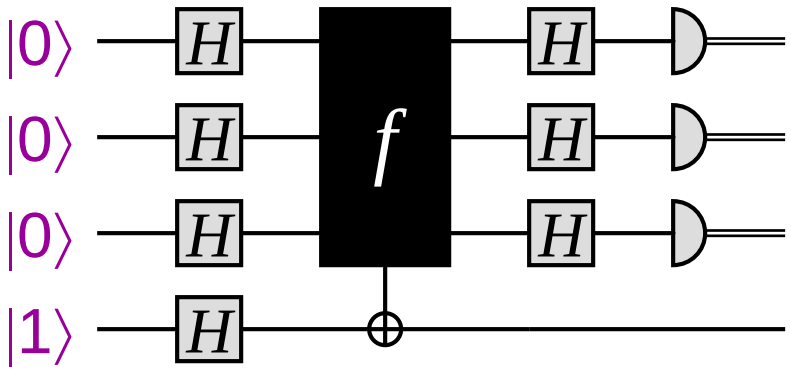
$$f(0000) = f(0001) = f(0010) = \cdots = f(0111) = 0$$

Quantumly? ____

[Deutsch & Jozsa, 1992]

Quantum algorithm





Constant case: $|\psi\rangle = \pm\sum_x |x\rangle$ ***Why?***

Balanced case: $|\psi\rangle$ is ***orthogonal*** to $\pm\sum_x |x\rangle$ ***Why?***

How to distinguish between the cases? What is $H^{\otimes n}|\psi\rangle$?

Constant case: $H^{\otimes n}|\psi\rangle = \pm|00\cdots0\rangle$

Balanced case: $H^{\otimes n}|\psi\rangle$ is orthogonal to $|0\cdots00\rangle$

Last step of the algorithm: If the measured result is 000 then output "constant", otherwise output "balanced".

Probabilistic *classical* algorithm solving constant vs balanced

But here's a classical procedure that makes only **2** queries and performs fairly well probabilistically:

1. pick $x_1, x_2 \in \{0,1\}^n$ randomly
2. **if** $f(x_1) \neq f(x_2)$ **then** output "balanced" **else** output "constant"

What happens if f is constant? The algorithm always succeeds.

What happens f if is balanced? Succeeds with probability $\frac{1}{2}$.

By repeating the above procedure k times:
$2k$ queries and one-sided error probability 2^{-k}

Therefore, for large n, we see $\ll 2^n$ queries are likely sufficient