Deutsch's Problem

PHYS/CSCI 3090

Prof. Alexandra Kolla

Alexandra.Kolla@Colorado.edu
ECES 122

Prof. Graeme Smith

Graeme.Smith@Colorado.edu
JILA S326

https://home.cs.colorado.edu/~alko5368/indexCSCI3090.html

Homework

- HW 1 is out, due next Monday at noon.

Come see us!

- Alexandra Kolla/ Graeme Smith: Friday 3:00-4:00 pm, JILA X317.
- Ariel Shlosberg: Tu/Th 2:00-4:00pm, DUANG2B90 (physics help room)
- Steven Kordonowy: Th 11am-12pm, ECAE 124.

Last Class

- Unitary circuits, input and output registers
- Quantum Parallelism
- No cloning
- Uncertainty principle

Today

- Deutsch’s problem
- Simplest example of quantum tradeoff that sacrifices particular information to get relational information.
- First “Quantum supremacy” result

Inner Product test

Assume $|y\rangle$, $|x\rangle$, $|w\rangle$, $|k\rangle$ are arbitrary vectors.
What is the inner product $(|y\rangle \otimes |w\rangle, |x\rangle \otimes |k\rangle)$?

A) 0

B) $\langle x|y\rangle \cdot \langle w|k\rangle$

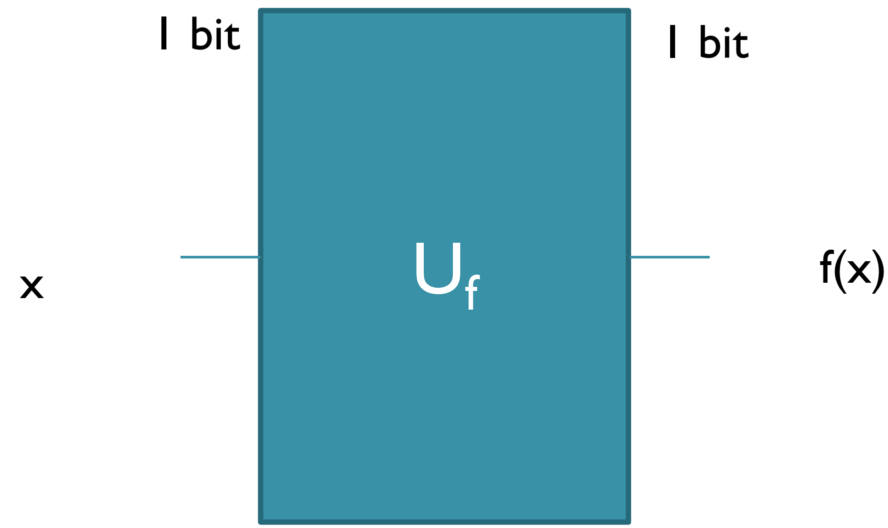
C) $\langle x|k\rangle \cdot \langle y|w\rangle$

D) $\langle x|w\rangle \cdot \langle y|k\rangle$

Is this it for Quantum?

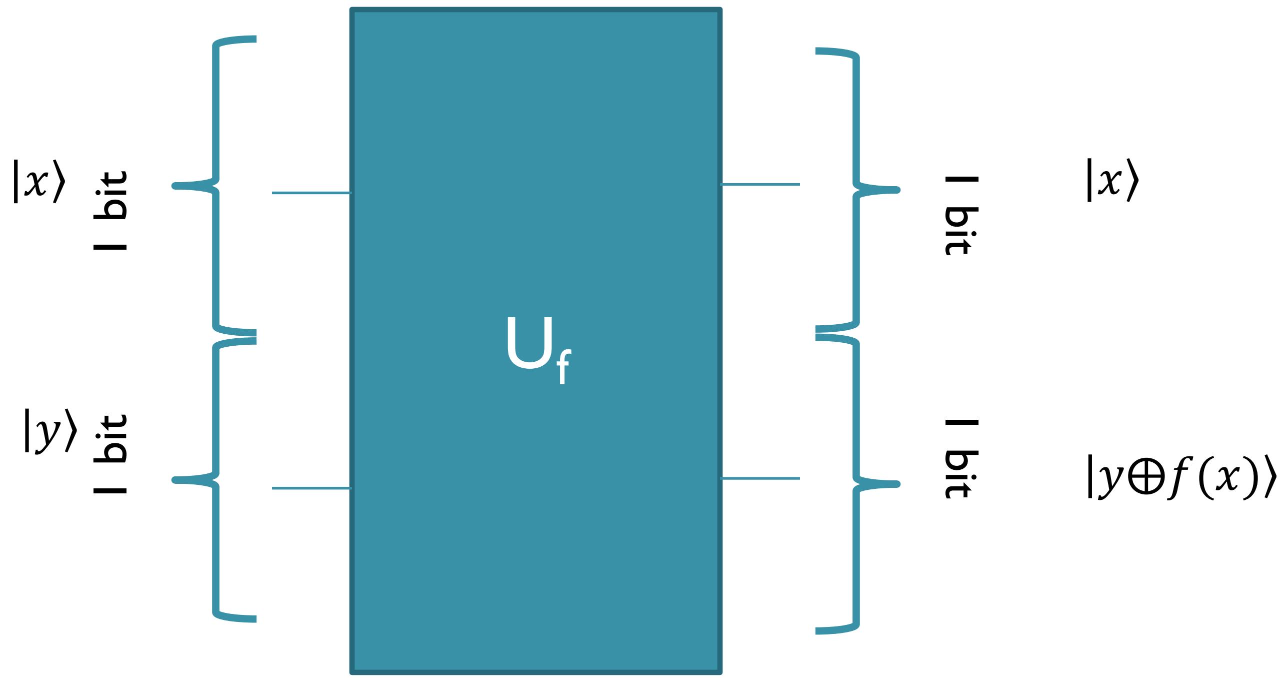
- We can be more clever, apply more unitaries to the qubits before or after applying U_f.
- We can learn something about the relations between different values of f(x).
- We lose the information of f(x)
- This tradeoff of information is typical of physics: Uncertainty principle.

The setup



- Both input and output registers contain one bit.
- Functions f that take one bit to one bit
- Two different ways to think about such f.

The setup, in quantum



How many functions?

How many different functions f: $\{0,1\}^n \rightarrow \{0,1\}$ are there that take input n bits and output one bit

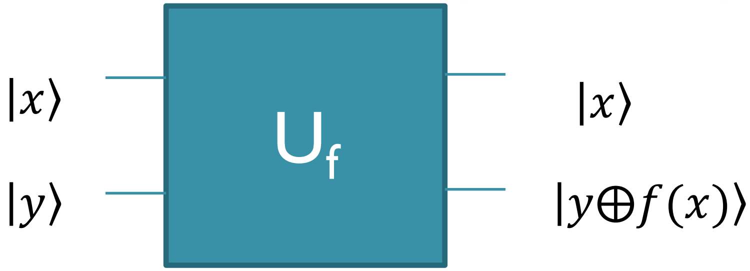
A) 2

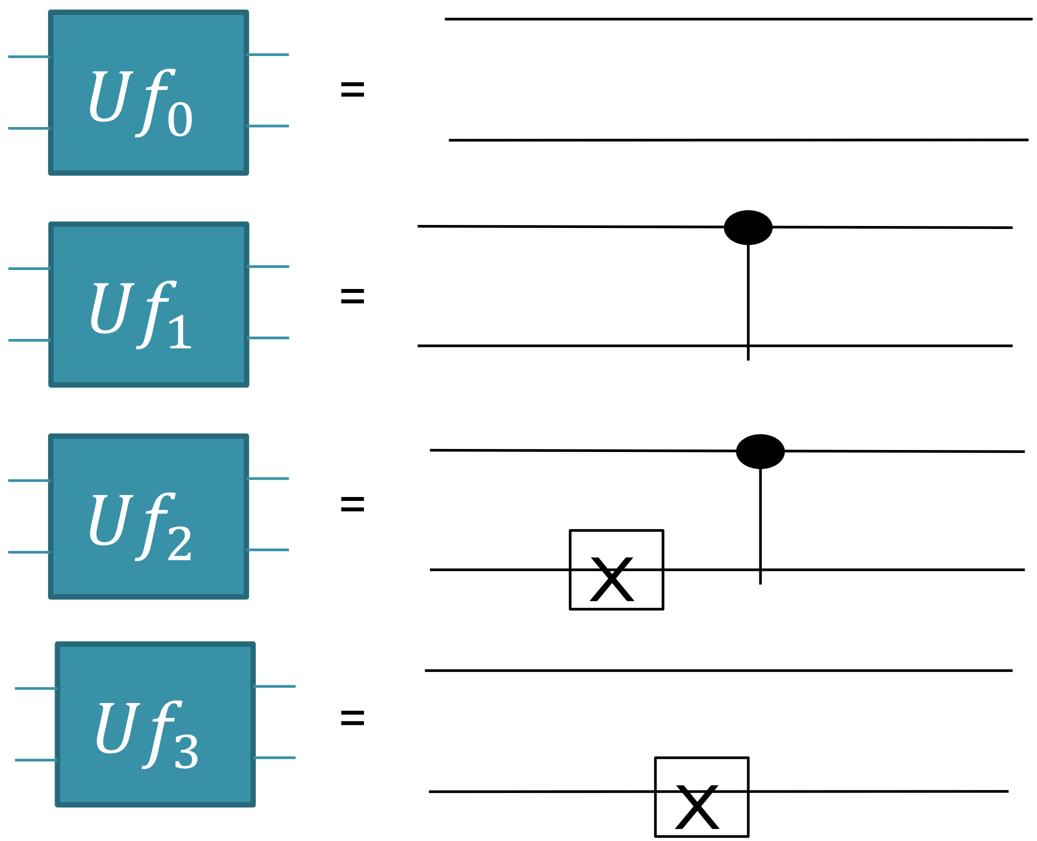
B) 2^n

C) 2^{2^n}

D) 2×2^n

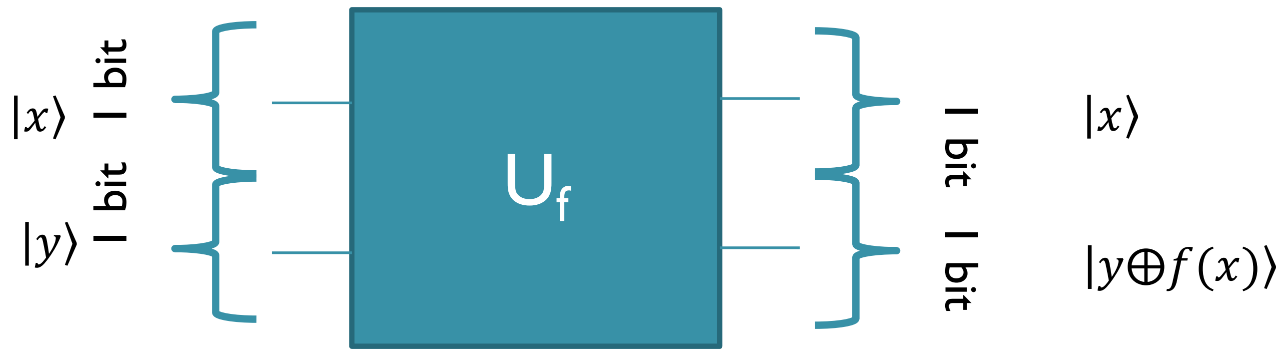
The setup, in quantum





$f(0)$	$f(1)$
0	0
0	1
1	0
1	1

The setup, in quantum

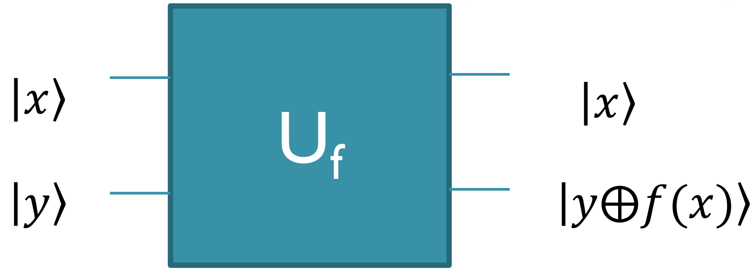


- U_f is one of 4 possibly functions (table).
- We are given a black box that calculates one of the 4 f's by performing

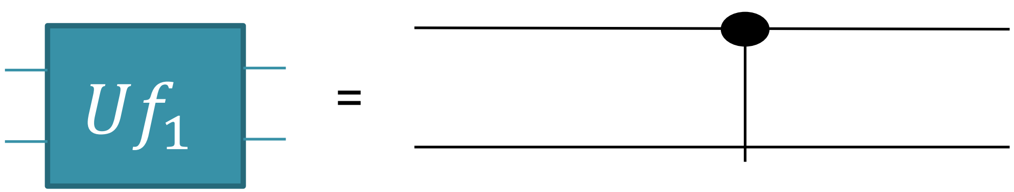
$$U_f |x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f(x)\rangle$$

- We are guaranteed that the black box performs one of the four computations, but we are not told which one.
- We are allowed to use the box only once, what can we learn about f?

The setup, in quantum

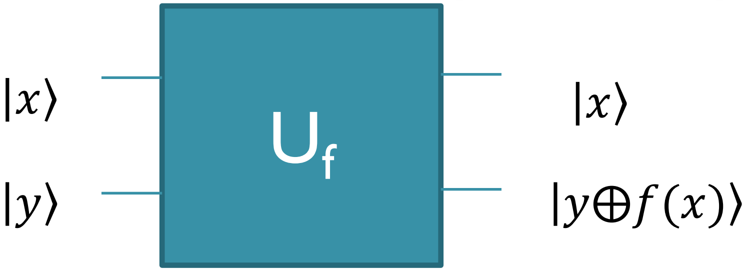


$f(0)$	$f(1)$
0	1

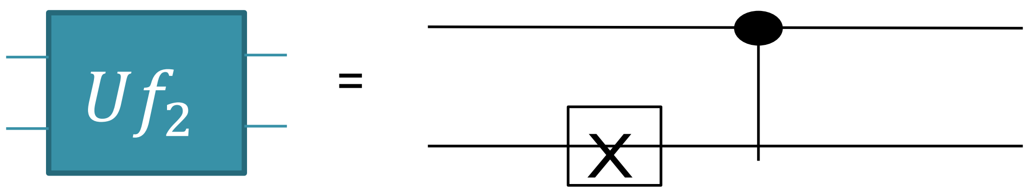


f(x) =x
(CNOT)

The setup, in quantum

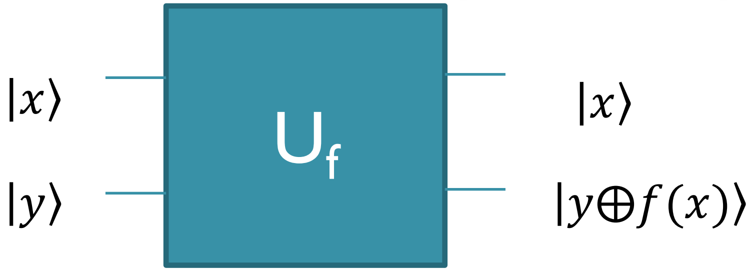


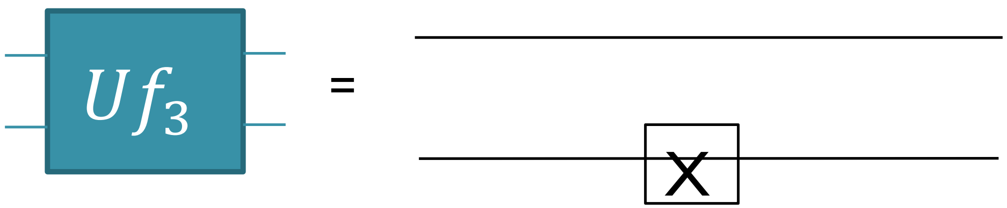
$f(0)$	$f(1)$
1	0



f(x) =NOT(x)

The setup, in quantum

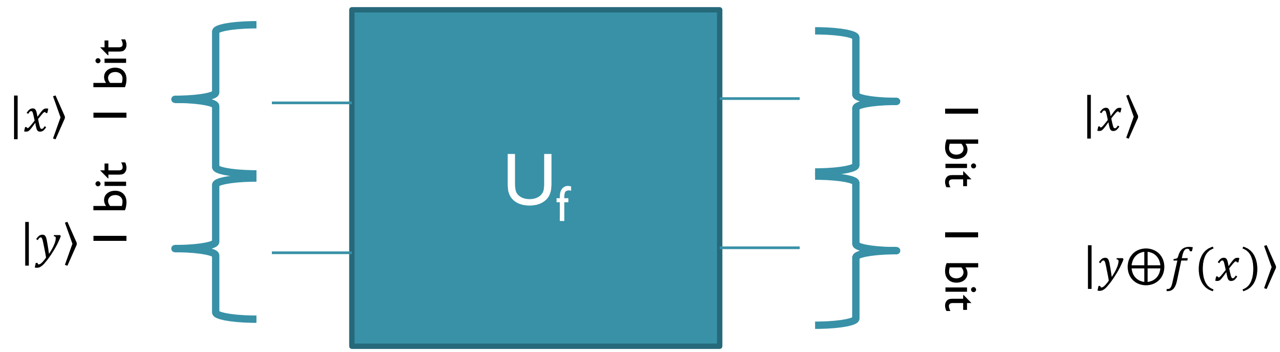




$f(0)$	$f(1)$
1	1

$f(x) = 1$

The setup, in quantum



- Deutsch's problem

We want to learn if f is constant (f(0)=f(1), satisfied by f_0 and f_3) or not, with one application of black box.

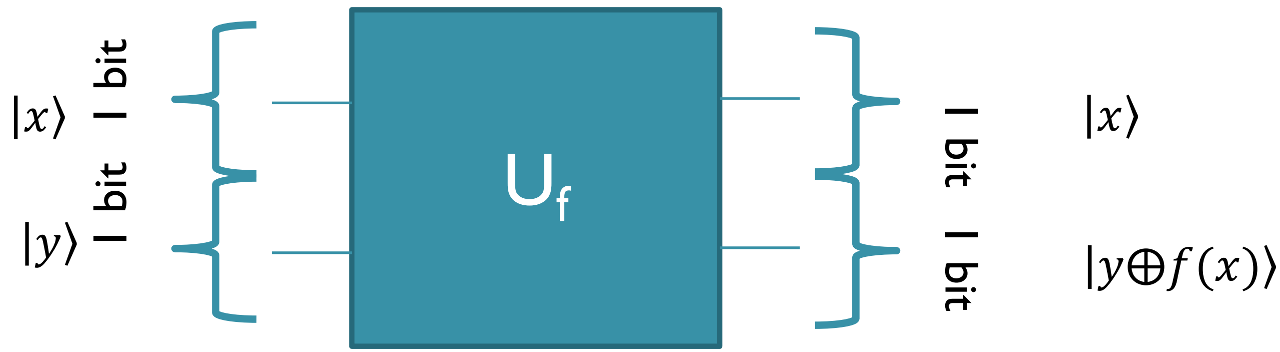
Classically

- We want to learn if f is constant (f(0)=f(1), satisfied by f_0 and f_3) or not, with one application of black box.

- With a classical computer, we can either learn the value f(0) or f(1), so we can learn whether the function is one of (f_0, f_1) with f(0)=0 or (f_2, f_3) with f(0)=1.

- A classical computer needs two queries to U_f to determine if it is constant or not!

The setup, in quantum



- With a quantum computer we can do better! Without learning any information about the values of f(0) or f(1), we can determine with one application of the black box if f is constant or not.

More on Deutsch's problem

- Second way to look at Deutsch's problem, which gives it nontrivial mathematical content.
- One can think of x as specifying a choice of two different inputs to an elaborate subroutine that requires many additional Qbits, and one can think of f (x) as characterizing a two-valued property of the output of that subroutine.
- For example f (x) might be the value of the millionth bit in the binary expansion of $\sqrt{(2 + x)}$ so that f (0) is the millionth bit in the expansion of 2 while f (1) is the millionth bit of $\sqrt{3}$.
- In this case the input register feeds data into the subroutine and the subroutine reports back to the output register.

More on Deutsch's problem

- In the course of the calculation the input and output registers will in general become entangled with the additional Qbits used by the subroutine.
- If the entanglement persists to the end of the calculation, the input and output registers will have no final states of their own, and it will be impossible to describe the computational process as the simple unitary transformation we saw earlier.
- We shall see next lecture however, that it is possible to set things up so that at the end of the computation the additional Qbits required for the subroutine are no longer entangled with the input and output registers, so that the additional Qbits can indeed be ignored.

More on Deutsch’s problem

- The simple linear transformation then correctly characterizes the net effect of the computation on those two registers.
- Under interpretation (1) of Deutsch’s problem, answering the question of whether f is or is not constant amounts to learning something about the nature of the black box that executes Uf without actually opening it up and looking inside.
- Under interpretation (2) it becomes the nontrivial question of whether the millionth bits of $\sqrt{2}$ and $\sqrt{3}$ agree or disagree. Under either interpretation, to answer the question with a classical computer we can do no better than to run the black box twice, with both 0 and 1 as inputs, and compare the two outputs.

Attempt 1: Superposition

- We could try preparing the input register in superposition of 0 and 1.

$$U_f(H\otimes 1)(|0\rangle\otimes|0\rangle)= \frac{1}{\sqrt{2}}|0\rangle|f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle|f(1)\rangle$$

We can measure, and get either 0, f(0) or 1, f(1) but no improvement over classical

Attempt 2: Superposition ++

- We can pre and post process the state to yield what we want

$$U_f(H \otimes H)(X \otimes X)(|0\rangle \otimes |0\rangle)$$

Superposition ++

- We can pre and post process the state to yield what we want

$$(\mathrm{H} \otimes H)(X \otimes X)(|0\rangle \otimes |0\rangle) = (\mathrm{H} \otimes H)(|1\rangle \otimes |1\rangle) =$$

$$\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$$

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

The Trick

- We can pre and post process the state to yield what we want

$$U_f(H \otimes H)(X \otimes X)(|0\rangle \otimes |0\rangle)$$

$$= \frac{1}{2}(U_f|0\rangle|0\rangle - U_f|1\rangle|0\rangle - U_f|0\rangle|1\rangle + U_f|1\rangle|1\rangle)$$

$$= \frac{1}{2}(|0\rangle|f(0)\rangle - |1\rangle|f(1)\rangle - |0\rangle|1 \oplus f(0)\rangle$$

$$+|1\rangle|1 \oplus f(1)\rangle)$$

The Trick

$$|0\rangle|f(0)\rangle - |1\rangle|f(1)\rangle - |0\rangle|1\oplus f(0)\rangle + |1\rangle|1\oplus f(1)\rangle$$

- Case 1: f(0)=f(1), output state is

$$|0\rangle|f(0)\rangle - |1\rangle|f(0)\rangle - |0\rangle|1\oplus f(0)\rangle + |1\rangle|1\oplus f(0)\rangle$$
$$= (|0\rangle - |1\rangle)|f(0)\rangle - (|0\rangle - |1\rangle)\,|1\oplus f(0)\rangle$$
$$= (|0\rangle - |1\rangle)(|f(0)\rangle - |1\oplus f(0)\rangle)$$

The Trick

$|0\rangle|f(0)\rangle$ - $|1\rangle|f(1)\rangle$ - $|0\rangle|1\oplus f(0)\rangle$ +$|1\rangle|1\oplus f(1)\rangle$

- Case 2: f(0)≠f(1), $f(1) = |1\oplus f(0)\rangle$

output state is

$|0\rangle|f(0)\rangle$ - $|1\rangle|1\oplus f(0)\rangle$- $|0\rangle|1\oplus f(0)\rangle$ +$|1\rangle|f(0)\rangle$

= $(|0\rangle + |1\rangle)|f(0)\rangle - (|0\rangle + |1\rangle)\, |1\oplus f(0)\rangle$

= $(|0\rangle + |1\rangle)(|f(0)\rangle - |1\oplus f(0)\rangle)$

The Trick

$$|0\rangle|f(0)\rangle - |1\rangle|f(1)\rangle - |0\rangle|1\oplus f(0)\rangle + |1\rangle|1\oplus f(1)\rangle$$

- Case 1: f(0)=f(1), output state is

$$(|0\rangle - |1\rangle)(|f(0)\rangle - |1\oplus f(0)\rangle)$$

- Case 2: f(0) $\neq$ f(1), output state is

$$(|0\rangle + |1\rangle)(|f(0)\rangle - |1\oplus f(0)\rangle)$$

The Trick

$$|0\rangle|f(0)\rangle - |1\rangle|f(1)\rangle - |0\rangle|1\oplus f(0)\rangle + |1\rangle|1\oplus f(1)\rangle$$

- Case 1: f(0)=f(1), output state is

$$(|0\rangle - |1\rangle)(|f(0)\rangle - |1\oplus f(0)\rangle)$$

- Case 2: f(0) $\neq$ f(1), output state is

$$(|0\rangle + |1\rangle)(|f(0)\rangle - |1\oplus f(0)\rangle)$$

- Apply H to the *input register*

The Trick

$$|0\rangle|f(0)\rangle - |1\rangle|f(1)\rangle - |0\rangle|1\oplus f(0)\rangle + |1\rangle|1\oplus f(1)\rangle$$

- Case 1: f(0)=f(1), output state is

$$(|0\rangle - |1\rangle)(|f(0)\rangle - |1\oplus f(0)\rangle)$$

  After applying H:

$$(H\otimes 1)(|0\rangle - |1\rangle)(|f(0)\rangle - |1\oplus f(0)\rangle)$$
$$=|1\rangle(|f(0)\rangle - |1\oplus f(0)\rangle)$$

- Apply H to the *input register*

Finally

$|0\rangle|f(0)\rangle$ - $|1\rangle|f(1)\rangle$ - $|0\rangle|1\oplus f(0)\rangle$ +$|1\rangle|1\oplus f(1)\rangle$

- Case 2: f(0) $\neq$ f(1), output state is

$$(|0\rangle + |1\rangle)(|f(0)\rangle - |1\oplus f(0)\rangle)$$

After applying H:

$$(H \otimes 1)(|0\rangle + |1\rangle)(|f(0)\rangle - |1\oplus f(0)\rangle)$$
$$=|0\rangle(|f(0)\rangle - |1\oplus f(0)\rangle)$$

- Measure the *input register* t decide if f is constant (get $|1\rangle$), or not (get $|0\rangle$),

Uncertainty principle

$$|0\rangle|f(0)\rangle - |1\rangle|f(1)\rangle - |0\rangle|1\oplus f(0)\rangle + |1\rangle|1\oplus f(1)\rangle$$

- Case 2: f(0) $\neq$ f(1), output state is

$$(|0\rangle + |1\rangle)(|f(0)\rangle - |1\oplus f(0)\rangle)$$

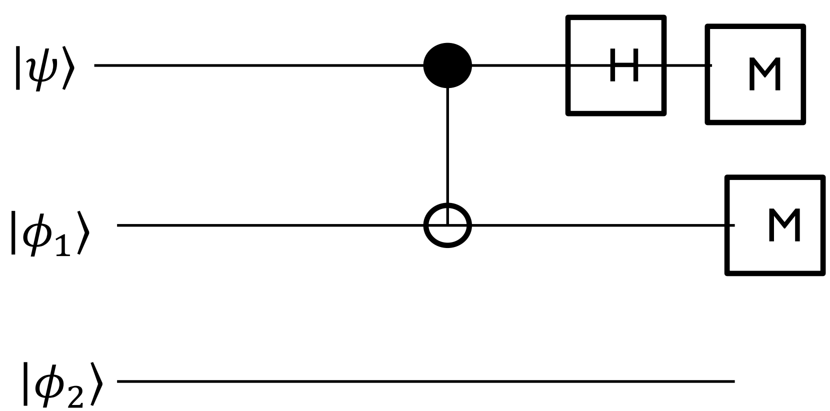
After applying H:

$$(H\otimes 1)(|0\rangle + |1\rangle)(|f(0)\rangle - |1\oplus f(0)\rangle)$$
$$=|0\rangle(|f(0)\rangle - |1\oplus f(0)\rangle)$$

- However, we learn nothing about output, since it is in uniform superposition of both values!

The whole operation

- $(\mathrm{H} \otimes 1)\, \mathrm{U_f}(\mathrm{H} \otimes H)(X \otimes X)(|0\rangle \otimes |0\rangle) =$
- Either $|1\rangle \frac{1}{\sqrt{2}}(|f(0)\rangle - |1 \oplus f(0)\rangle), \mathrm{f}(0) = \mathrm{f}(1)$
- Or $|0\rangle \frac{1}{\sqrt{2}}(|f(0)\rangle - |1 \oplus f(0)\rangle), \mathrm{f}(0) \neq \mathrm{f}(1)$
- Instead of querying the values of $f(0), f(1)$ algorithm queries the XOR $\mathrm{f}(0) \oplus f(1)$


$|\psi\rangle$
$|\phi_1\rangle$
$|\phi_2\rangle$
H
M
M