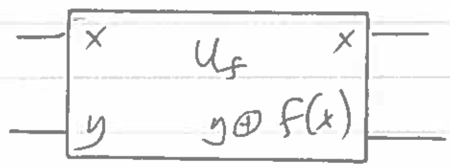
Deutsch's Algorithm
from Nielsen & Chuang

Quantum Parallelism

Consider $f(x) : \{0,1\} \rightarrow \{0,1\}$
single bit domain and range



Can we build U_f?

$\oplus$ addition modulo 2

Four possible $f(x)$

	x	$f(x)$
A	0	0
	1	0
B	0	1
	1	1
C	0	0
	1	1
D	0	1
	1	0

y	$f(x)$	$y \oplus f(x)$
0	0	0
0	1	1
1	0	1
1	1	0

U_A

$x\,y$		$x\; y \oplus f(x)$
0 0	$\rightarrow$	0 0
0 1	$\rightarrow$	0 1
1 0	$\rightarrow$	1 0
1 1	$\rightarrow$	1 1

$$U_A = I \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

U_B

x	y	x	$y \oplus f(x)$
0	0	0	1
0	1	0	0
1	0	1	1
1	1	1	0

where to send

$$U_B = \begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

U_C

x	y	x	$y \oplus f(x)$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

$$U_C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

U_D

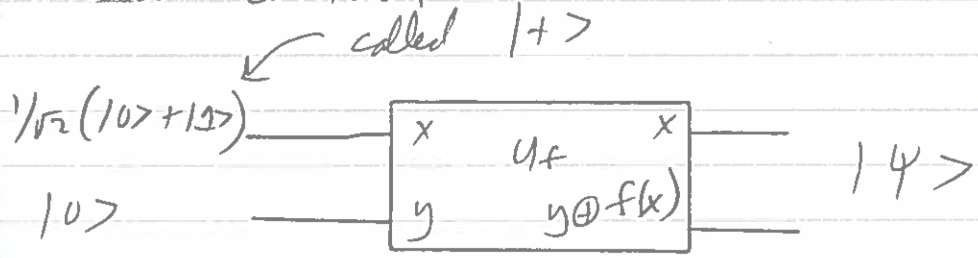
x	y	x	$y \oplus f(x)$
0	0	0	1
0	1	0	0
1	0	1	0
1	1	1	1

$$U_D = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

So we can build U_f for any of the form $f = A, B, C,$ or D, each unitary! It works classically but also quantum!

In fact, for any classical circuit that computes a function f, there is a quantum circuit of comparable efficiency that realizes U_f on a quantum computer (Fredkin gate § 3.2.5 [NC])

Now consider



where $U_f = U_A$ or U_B or U_C or U_D

The circuit has input

$$\left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right) \otimes |0\rangle$$

$$= \tfrac{1}{\sqrt{2}}\left[|00\rangle + |10\rangle\right]$$

U_f sends $|x\,y\rangle \to |x\,f(x)\rangle$

because $y = |0\rangle$

Output is

$$U_f\left(\tfrac{1}{\sqrt{2}}\left[|00\rangle + |10\rangle\right]\right)$$

$$= \tfrac{1}{\sqrt{2}}\left[U_f(|00\rangle) + U_f(|10\rangle)\right] \quad \text{linearity}$$

$$= \tfrac{1}{\sqrt{2}}\left[|0, f(0)\rangle + |1, f(1)\rangle\right]$$

For example U_c produces $\tfrac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right] = |\psi\rangle$

One evalutation of "f" using U_f on $|+\rangle$ produces information about <u>both</u> $f(0)$ and $f(1)$!

<u>Note</u> We must use U_f to get this result $|\psi\rangle$. It is NOT, as the picture suggests, the tensor product of <u>anything</u>, so it is not

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

Can we discover U_f?

Classically we need to evaluate

$$f(0) \quad \text{and} \quad f(1)$$

to discover U_f

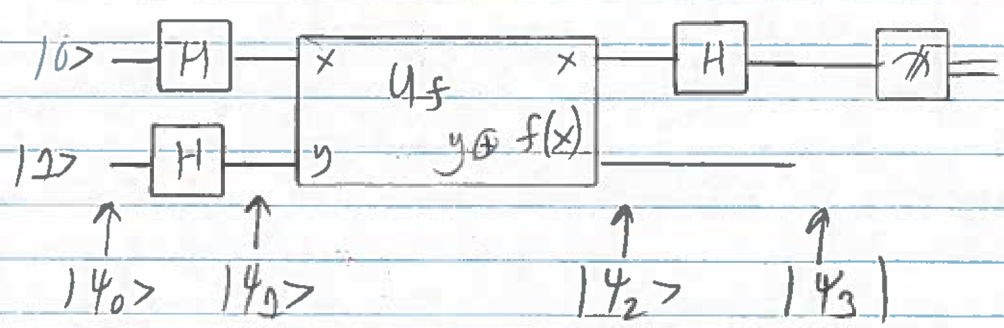
What if we want to distinguish

U_A U_B which are constant

from U_C U_D which are "balanced"

balanced: $\frac{1}{2}$ results 0
$\frac{1}{2}$ results 1

Consider same U_f, different input for y



$|\psi_0\rangle = |01\rangle$

$|\psi_1\rangle = H(|0\rangle) \otimes H(|1\rangle)$

$= \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right] \frac{1}{\sqrt{2}}\left[|0\rangle - |1\rangle\right]$

$= \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}$ Notice alternating pattern

$= \frac{1}{2}\left[|00\rangle - |01\rangle + |10\rangle - |11\rangle\right]$

y is strange - it is not $|0\rangle$ as before

If $f(x)$ is constant $f(0)=f(1) \to f(0) \oplus f(1) = 0$
is balanced $f(0) \neq f(1) \to f(0) \oplus f(1) = 1$

So we need to evaluate $f(0) \oplus f(1)$ and then we'll know

$|\psi_2\rangle = U_f\left(\frac{1}{2}\left[|00\rangle - |01\rangle + |10\rangle - |11\rangle\right]\right)$

$= \frac{1}{2}\left[U_f(|00\rangle) - U_f(|01\rangle) + U_f(|10\rangle) - U_f(|11\rangle)\right]$

$= \frac{1}{2}\left[|0, f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, f(1)\rangle - |1, 1 \oplus f(1)\rangle\right]$

Case 1 $\quad f(0) = f(1) \quad$ f is constant

$|\psi_2\rangle$ can be simplified

$$\tfrac{1}{2}\Big[\,|0, f(0)\rangle - |0, 1+f(0)\rangle$$
$$+ |1, f(0)\rangle - |1, 1+f(0)\rangle\,\Big]$$
$$= \tfrac{1}{2}\Big[\big(|0\rangle + |1\rangle\big) \otimes f(0)$$
$$- \big(|0\rangle + |1\rangle\big) \otimes \big(1 + f(0)\big)\Big]$$

$$= \underbrace{\tfrac{1}{2}\,[\,|0\rangle + |1]}_{\text{first qubit}} \otimes \underbrace{[\,f(0) - (1 + f(0))\,]}_{\text{second qubit}}$$

Recall $|+\rangle = \tfrac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$

So $\underbrace{\qquad\qquad}$ is $\frac{1}{\sqrt{2}}\,|+\rangle$

The first qubit will measure as $|+\rangle$
if $f(0) = f(1)$ at $|\psi_2\rangle$

the subsequent $\boxed{H}$ sends $|+\rangle$ to $|0\rangle$

so we see qubit 1 as $|0\rangle$
upon measurement of $|\psi_3\rangle$

Case 2 $\quad f(0) \neq f(1)$

$$\rightarrow \quad \begin{aligned} f(0) &= 1 \oplus f(1) \\ f(1) &= 1 \oplus f(0) \end{aligned}$$

then $|\psi_2\rangle$ simplifies as follows

$$\tfrac{1}{2}\left[\,|0, f(0)\rangle - |0, f(1)\rangle + |1, f(1)\rangle - |1, f(0)\rangle\,\right]$$

$$= \tfrac{1}{2}\left[\,|0\rangle - |1\rangle\,\right]\left[\,|f(0)\rangle - |f(1)\rangle\,\right]$$

$$= \underbrace{\tfrac{1}{\sqrt{2}}\,|-\rangle}_{\text{first qubit}} \otimes \underbrace{\left(|f(0)\rangle - |f(1)\rangle\right)}_{\text{second qubit}}$$

so qubit 1 measures as $|-\rangle$ at $|\psi_2\rangle$ if $f(0) \neq f(1)$

H sends $|-\rangle$ to $|1\rangle$ at $|\psi_3\rangle$

Measure at $|\psi_3\rangle$ $\quad$ $|0\rangle$ constant
$\quad\quad\quad\quad\quad\quad\quad\quad\quad$ $|1\rangle$ balanced

with just 1 eval of f !

The (old) phase kickback trick

Consider U_f on input $|x-\rangle$, $x \in \{0,1\}$

(we used $x = |+\rangle$ previously, but for now x is classic $|0\rangle$ or $|1\rangle$)

Result

Recall $U_f : |xy\rangle \to |x, y \oplus f(x)\rangle$

$$|\psi\rangle = U_f(|x-\rangle) =$$

$$= 1/\sqrt{2}\,[U_f(|x0\rangle) - U_f(|x1\rangle)]$$

$$= 1/\sqrt{2}\,[\,|x, f(x)\rangle - |x, 1 \oplus f(x)\rangle\,]$$

$$= |x\rangle \otimes 1/\sqrt{2}\,[\,|f(x)\rangle - |1 \oplus f(x)\rangle\,]$$

Two cases

$f(x) = 0$

$$|\psi\rangle = |x\rangle \otimes 1/\sqrt{2}\,(|0\rangle - |1\rangle)$$

$$= |x-\rangle$$

$f(x) = 1$

$$|\psi\rangle = |x\rangle \otimes (|1\rangle - |0\rangle)$$

$$= -|x-\rangle$$

a -1 phase factor is produced

Can summarize as

$$U_f(|x\rangle) = \underbrace{(-1)^{f(x)}}_{\text{NOT a global phase}} |x\rangle$$

$$-(a-b) = (b-a)$$

Changes the interference