Lec 7 24 Sep 20

$$H = \frac{1}{\sqrt{2}}(X+Z)$$

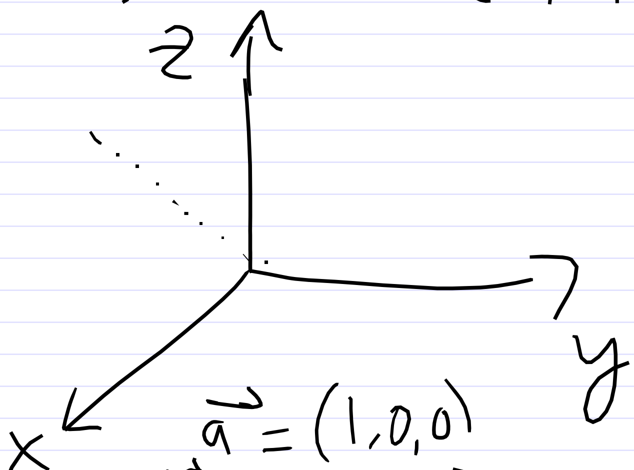
$$HXH = Z \qquad HZH = X$$

$$U(\hat{n},\theta) = \mathbb{1}\cos\frac{\theta}{2} + i\,\hat{n}\cdot\vec{\sigma}\sin\frac{\theta}{2}$$

$$iH = \frac{1}{\sqrt{2}}(i\sigma_x + i\sigma_z)$$

so $\theta = \pi$ $\quad \hat{n} = (1,0,1)/\sqrt{2}$

$$= \frac{\hat{x}+\hat{z}}{\sqrt{2}}$$



$$U\vec{a}\cdot\vec{\sigma}U^{+} = \vec{a}'\cdot\vec{\sigma}$$

$$\vec{a} = (1,0,0)$$

$$\vec{a}' = (0,0,1)$$

$$U = H,\ U^{+} = H$$

$$u \to u' = e^{i\alpha} u$$

$$u' \vec{a} \cdot \vec{\sigma} (u')^{+}$$

$$= e^{i\alpha} u (\vec{a} \cdot \vec{\sigma}) u^{+} e^{-i\alpha}$$

$$U(2)$$

$$U(2)/U(1) \simeq SU(2)/\mathbb{Z}_2$$

Deutsch problem

1 bit → 1 bit function

i.e., $m = n = 1$

	$x=0$	$x=1$	
f_0	0	0	const $f(x)=0$
f_1	0	1	identity $f(x)=x$
f_2	1	0	not $f(x)=1-x$
f_3	1	1	const $f(x)=1$

Invoke f once, can't distinguish between constant and non-constant functions (f_0, f_3) vs (f_1, f_2) classically.

But quantum mechanically can make that distinction with just one call to U_f

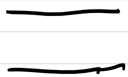
f(x) could be

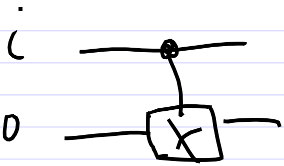
millionth bit of $\sqrt{x+2}$

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

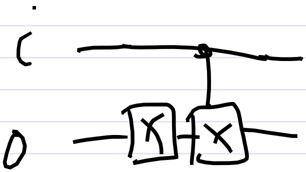
	$x=0$	$x=1$
f_0	0	0
f_1	0	1
f_2	1	0
f_3	1	1

U_f

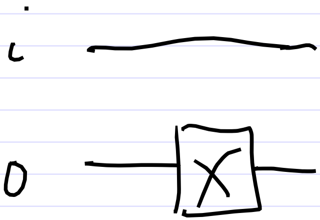
f_0  $U_f = 1$

f_1 

$U_f = C_{i0}$

f_2 

$U_f = C_{i0} X_0$

f_3 

$U_f = X_0$

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

But apply something else before U_f

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

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

$$U_f \Big| \rightarrow \; = \frac{1}{2}\left(|0\,f(0)\rangle - |0\,\bar{f}(0)\rangle - |1\,f(1)\rangle + |1\,\bar{f}(1)\rangle\right)$$

Suppose $f(0)=f(1)$ $\hookrightarrow \; = \frac{1}{2}\left(|0\rangle - |1\rangle\right)\left(|f(0)\rangle - |\bar{f}(0)\rangle\right)$

and if $f(0)\neq f(1) \rightarrow \; = \frac{1}{2}\left(|0\rangle + |1\rangle\right)\left(|f(0)\rangle - |\bar{f}(0)\rangle\right)$

apply H_i

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

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

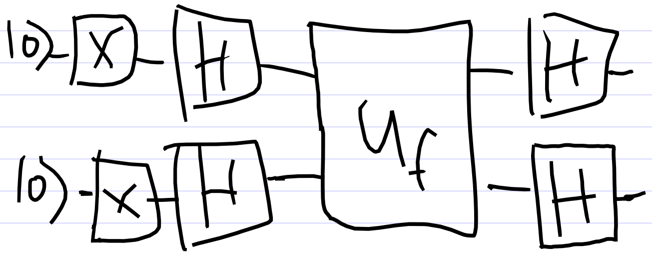
Notice ↑

Result:

Measure the input bit!

$|1\rangle$ f_0, f_3

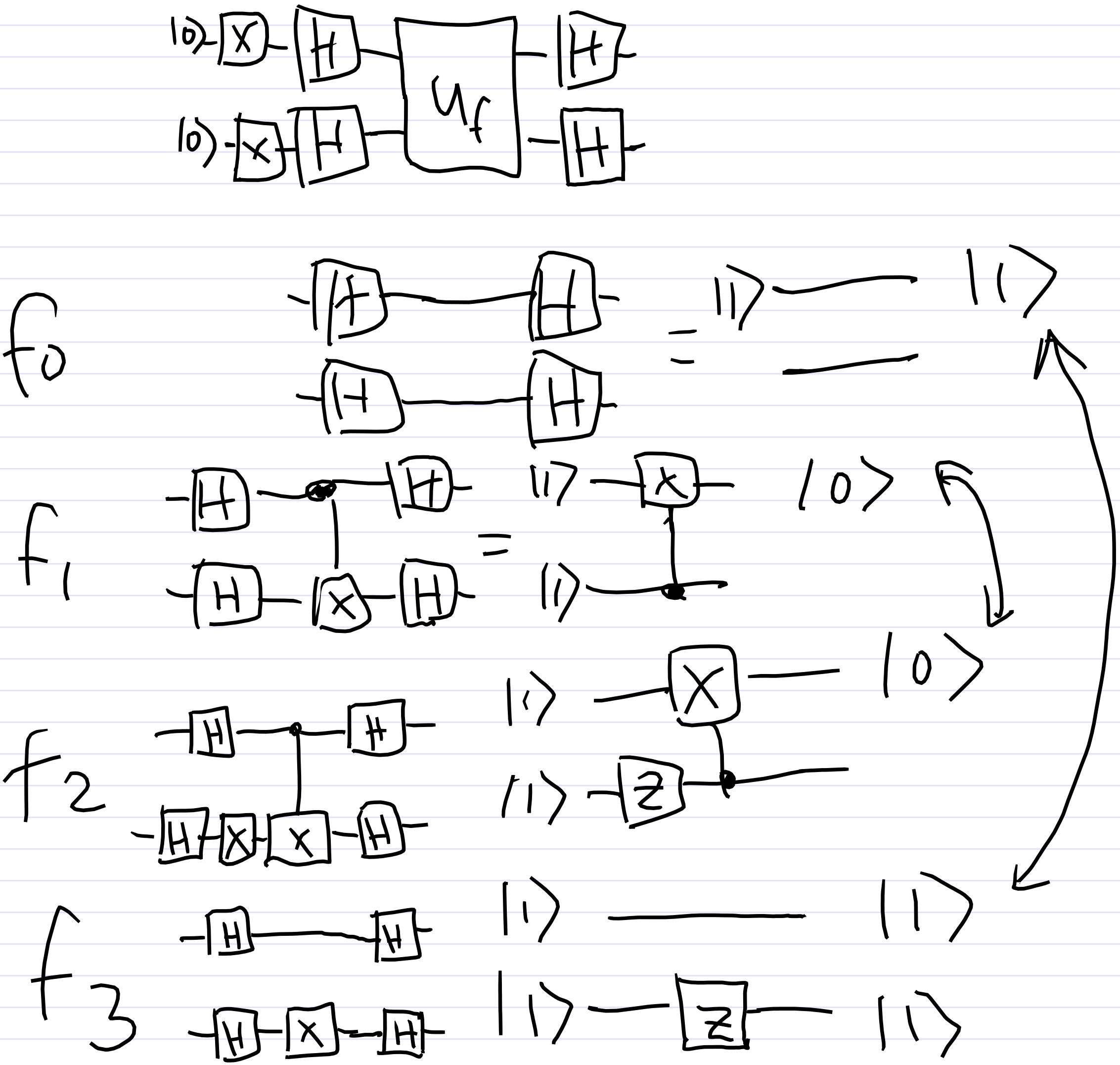
$|0\rangle$ f_1, f_2



$|0\rangle$ f_1, f_2

$|1\rangle$ f_0, f_3

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



so clear from circuit diagrams that
$H^{\otimes 2} U_f H^{\otimes 2}$ leaves $|1\rangle$ on input bit for f_0, f_3
$|0\rangle$ f_1, f_2

'93 Bernstein-Vazarani

n bit   1-bit $m=1$

artificial? but unambiguous speed-up

Choose some $a < 2^n$

$$f(x) = a \cdot x = \oplus a_i x_i$$ bitwise XOR

How many invocations of f to determine a?

Classically takes n

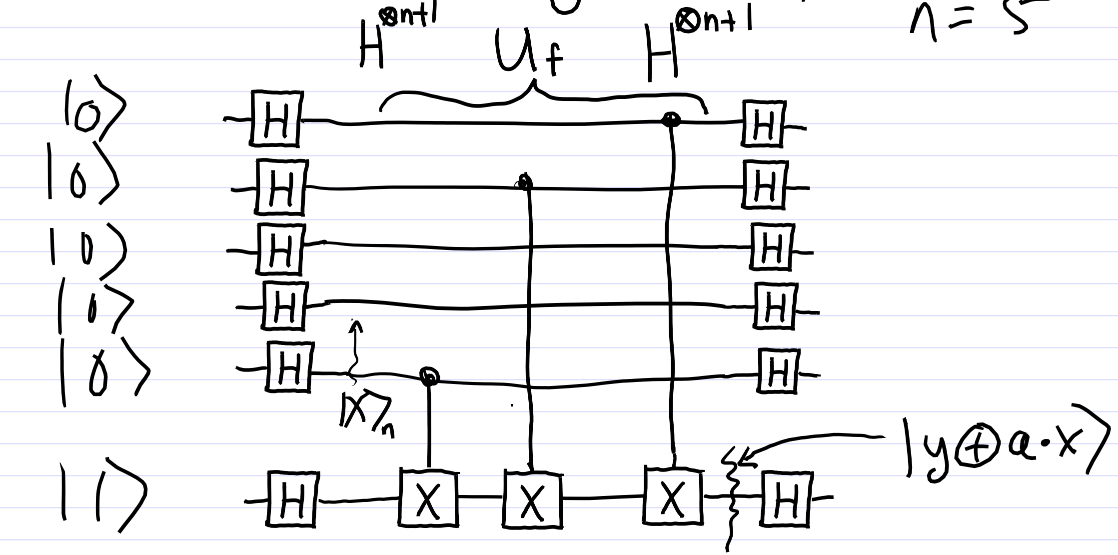
Choose $x = 2^m$ $x = (0, \ldots 0, \overset{m\text{th}}{1}, 0 \ldots 0)$

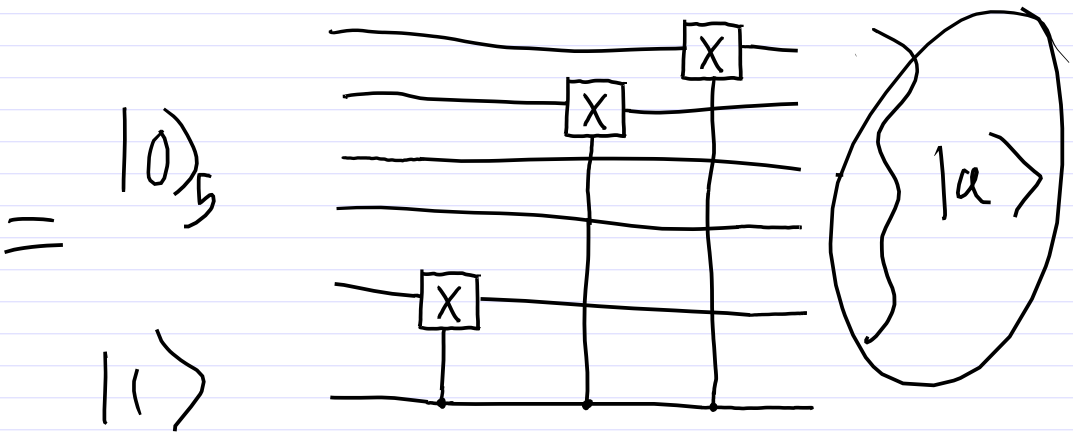
then $x \cdot a = a_m$

$m = 0, \ldots, n-1$ so n times to determine each bit of a

$U_f|x\rangle_n|y\rangle_1 = |x\rangle_n|y\oplus a\cdot x\rangle_1$, $a = 11001$

$n = 5$





measure input bits, gives $|a\rangle$!

Single invocation of U_f