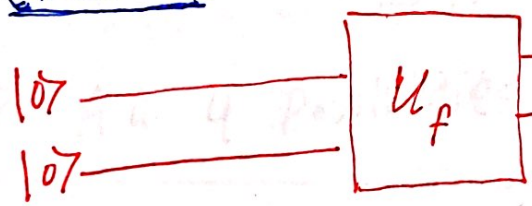
Ali Alkadhim
Quantum Computing
HW 5

1) Deutsch Algorithm

a) For each of the following circuits, we have 4 possibilities for the input & output registers, since we are using standard basis, the input and output qubits can be any of $\{|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle\}$. I shall verify each circuit using every possiblity of in/out registers.

Circuit 1

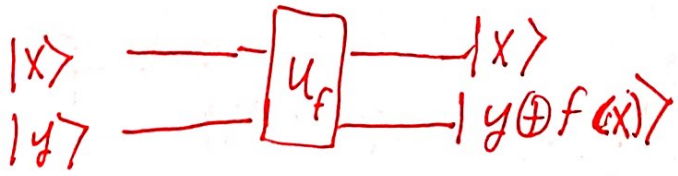
f_0



$|0\rangle = |0\rangle$

$|0 \oplus f_0(0)\rangle = |0 \oplus 0\rangle = |0\rangle$

since for any states $|x\rangle$ & $|y\rangle$



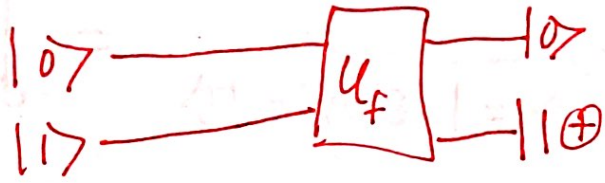
and $f_0(0) = 0$. Hence this circuit takes

$$|0\rangle|0\rangle \xrightarrow{U_f} |0\rangle|0\rangle,$$ which is

equivalent to doing nothing, i.e circuit ——— .

For the following, the same reasoning as here applies.

f_0

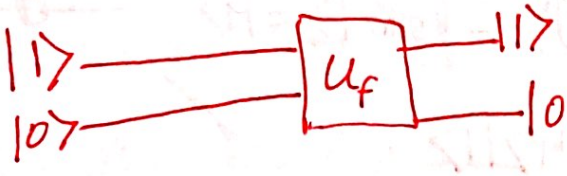


$= |1 \oplus 0\rangle = |1\rangle$

hence this takes $|0\rangle|1\rangle \xrightarrow{U_f} |0\rangle|1\rangle$,

which is equivalent to $=$ or $\mathbb{1}$.

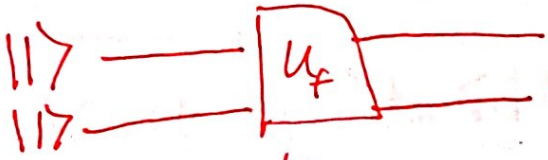
f_0



$= |0 \oplus 0\rangle = |0\rangle$

$\Rightarrow |1\rangle|0\rangle \xrightarrow{U_f} |1\rangle|0\rangle$, equivalent to $=$.

f_0



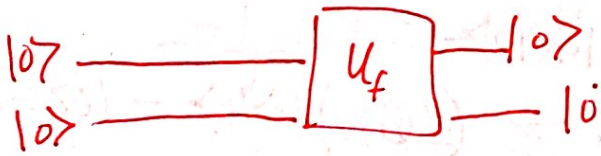
$= |1 \oplus 0\rangle = |1\rangle$

$\Rightarrow |1\rangle|1\rangle \xrightarrow{U_f} |1\rangle|1\rangle$, equivalent to $=$.

$\Rightarrow$ All 4 possibilities verified. ✓

Circuit 2

f_1



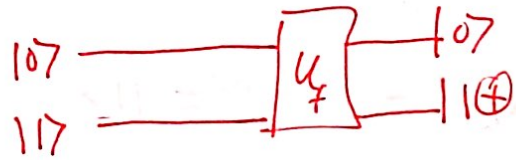
$= |0 \oplus 0\rangle = |0\rangle$

$\Rightarrow |0\rangle|0\rangle \xrightarrow{U_f} |0\rangle|0\rangle$ which is equivalent to

$= C_{NOT} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X$

Check: $C_{NOT}\,|0\rangle|0\rangle = |0\rangle|0\rangle$. ✓

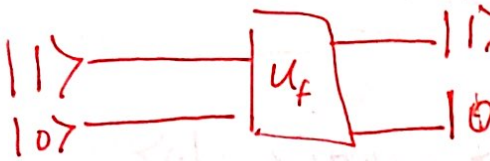
f_1



=

Check: $\text{CNOT}\,|0\rangle|1\rangle = |0\rangle|1\rangle$ ✓

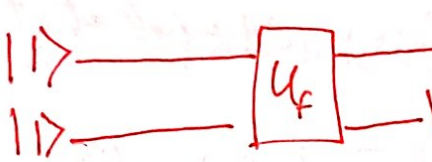
f_1



=

Check: $\text{CNOT}\,|1\rangle|0\rangle = |1\rangle|1\rangle$ ✓

f_1



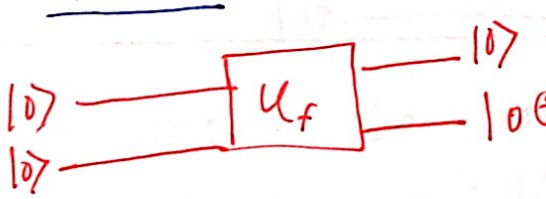
=

Check: $\text{CNOT}\,|1\rangle|1\rangle = |1\rangle|0\rangle$ ✓

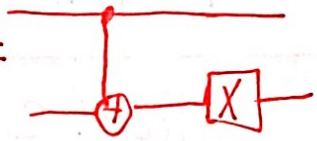
$\Rightarrow$ All 4 Possibilities Verified. ✓

Circuit 3

f_2



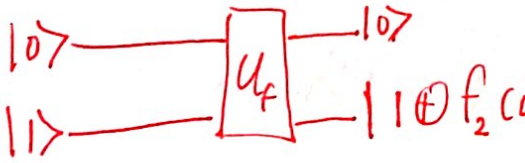
=



Check: $\text{CNOT}\,|0\rangle|0\rangle = |0\rangle|0\rangle$

$\hookrightarrow (\mathbb{1} \otimes X)|0\rangle|0\rangle = |0\rangle|1\rangle$ ✓

f_2

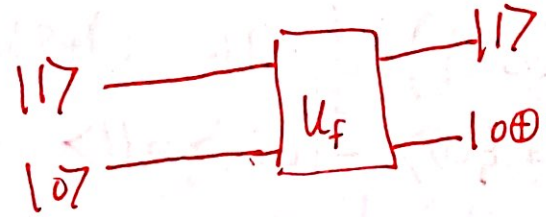


=

Check: $\text{CNOT}\,|0\rangle|1\rangle = |0\rangle|1\rangle$

$\hookrightarrow (\mathbb{1} \otimes X)|0\rangle|1\rangle = |0\rangle|0\rangle$ ✓

f_2



=

Check: CNOT $|1\rangle|0\rangle = |1\rangle|1\rangle$

$\hookrightarrow (\mathbb{1}\otimes X)|1\rangle|1\rangle = |1\rangle|0\rangle$ ✓

f_2

=

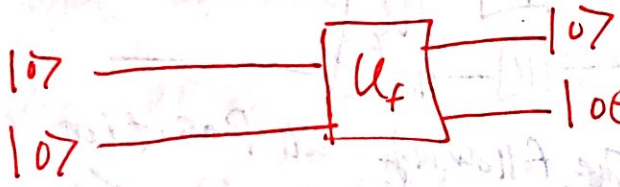
Check: CNOT $|1\rangle|1\rangle = |1\rangle|0\rangle$

$\hookrightarrow (\mathbb{1}\otimes X)|1\rangle|0\rangle = |1\rangle|1\rangle$ ✓

$\Rightarrow$ All 4 possibilities verified. ✓

Circuit 4

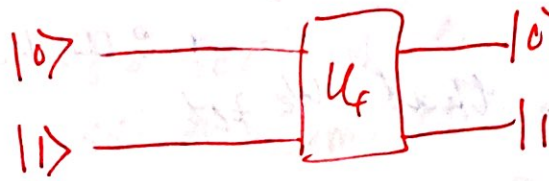
f_3



=

Clearly these are equivalent, since it takes $|0\rangle|0\rangle \xrightarrow{U_f} |0\rangle|1\rangle$, namely performs a NOT operation (X) on the second qubit.

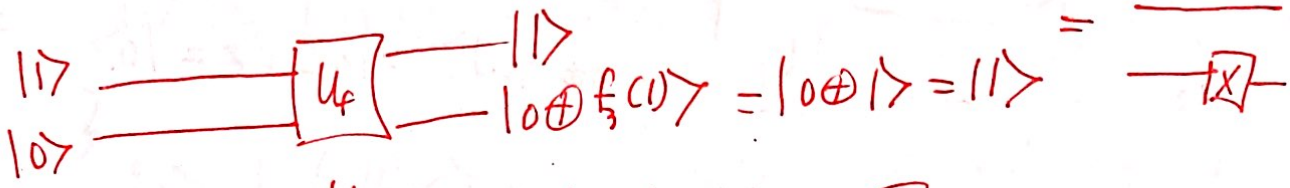
f_3



=

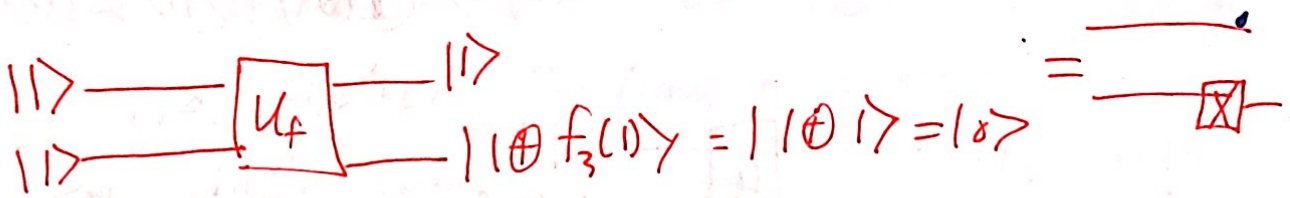
check: $|0\rangle|1\rangle \xrightarrow{U_f} |0\rangle|0\rangle$ ✓

f_3



Check: $|1\rangle|0\rangle \xrightarrow{U_f} |1\rangle|1\rangle$ ✓

f_3

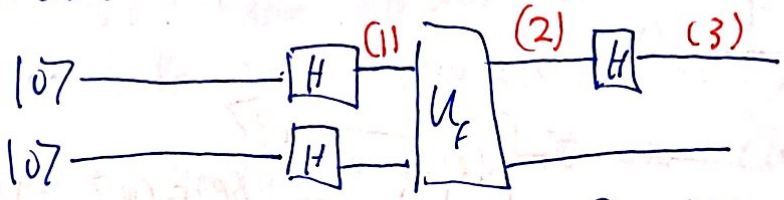


Check: $|1\rangle|1\rangle \xrightarrow{U_f} |1\rangle|0\rangle$ ✓

$\Rightarrow$ All 4 possibilities verified. ✓

---

b) As we saw in class, the Deutch algorithm applies the following circuit:



which results to the following at position (2):

$$\rightarrow \frac{1}{2}(|0\rangle - |1\rangle)(|f(0)\rangle - |\overline{f(0)}\rangle), \quad \text{if } f(0) = f(1), \text{ i.e. Balanced}$$

$$\rightarrow \frac{1}{2}(|0\rangle + |1\rangle)(|f(0)\rangle - |\overline{f(0)}\rangle), \quad \text{if } f(0) \neq f(1), \text{ i.e. unbalanced}$$

Then we apply $\boxed{H}$, so that we get

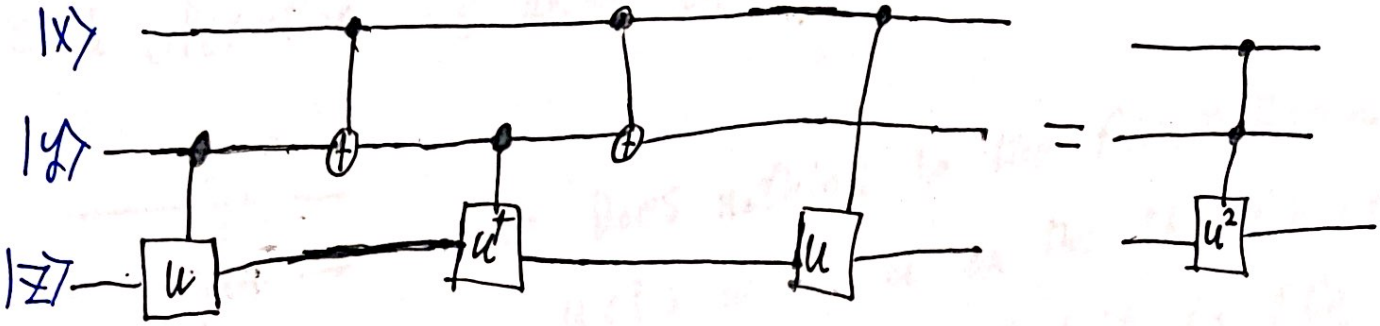
output: $\begin{cases} |1\rangle \frac{1}{\sqrt{2}}\left(|f(0)\rangle - |\overline{f(0)}\rangle\right), & \text{if } f(0)=f(1) \text{ "Balanced"} \\ |0\rangle \frac{1}{\sqrt{2}}\left(|f(0)\rangle - |\overline{f}(0)\rangle\right), & \text{if } f(0)\neq f(1) \text{ "unbalanced"} \end{cases}$

Hence, Deutch illustrated that we can know whether $f(0)=f(1)$, i.e. whether the function is balanced or not with a <u>single call</u> of U_f using a <u>quantum computer</u>. Note that this does not calculate anything regarding the actual function evaluation, just whether it's balanced or not.

On a classical computer this cannot be done. If we want to know whether the function is balanced, then we have to calculate $f(0)$, by calling U_f once (and acting it on classical bits $|0\rangle|0\rangle$ or $|0\rangle|1\rangle$), and then calling U_f <u>again</u> to calculate $f(1)$ (by acting U_f on $|1\rangle|1\rangle$ or $|1\rangle|0\rangle$), and comparing $f(0)$ to $f(1)$, to see whether they are equal. Hence a classical computer has to call U_f twice to see whether the function is balanced.

5.2

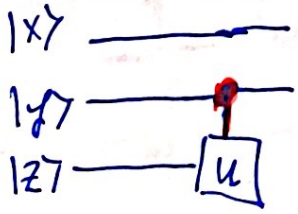
a) Verify



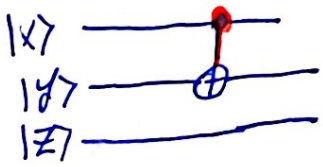
There are a few ways one can prove this. In what follows, I shall consider all possible permutations of arbitrary input states $|x\rangle|y\rangle|z\rangle$. The permutations are

$$|x\rangle|y\rangle|z\rangle = \{|0\rangle|0\rangle|0\rangle,\ |0\rangle|0\rangle|1\rangle,\ |0\rangle|1\rangle|0\rangle,\ |0\rangle|1\rangle|1\rangle,\ |1\rangle|0\rangle|0\rangle,\ |1\rangle|0\rangle|1\rangle,\ |1\rangle|1\rangle|0\rangle,\ |1\rangle|1\rangle|1\rangle\}$$

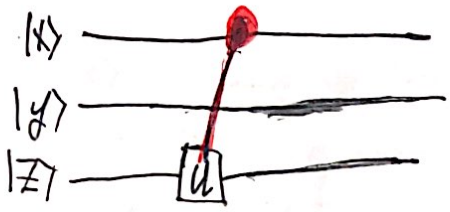
Also, in what follows, explicit calculations of the operators above can be written mathematically, for example:



$$= \Big[\mathbb{1}\otimes\underbrace{\big(|0\rangle\langle 0|\otimes\mathbb{1} + |1\rangle\langle 1|\otimes u\big)}_{\text{"Controlled-}u\text{"}}\Big]\,|x\rangle|y\rangle|z\rangle$$

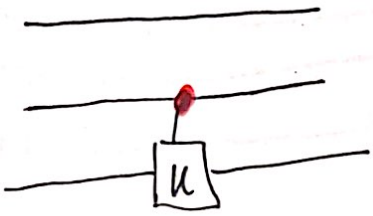


$$= \Big[\underbrace{\big(|0\rangle\langle 0|\otimes\mathbb{1} + |1\rangle\langle 1|\otimes X\big)}_{\text{CNOT}}\otimes\mathbb{1}\Big]\,|x\rangle|y\rangle|z\rangle$$

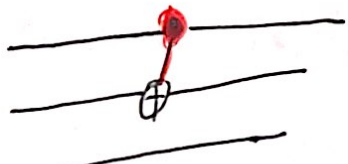


$$= \left(\left(|0\rangle\langle 0| \otimes \mathbb{1}\right) \otimes \mathbb{1} \oplus \left(|1\rangle\langle 1| \otimes U\right)\right)|x\rangle|y\rangle|z\rangle$$

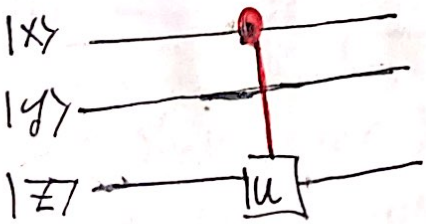
To simplify the calculations, we can also write each operation as what the operation executes in words:



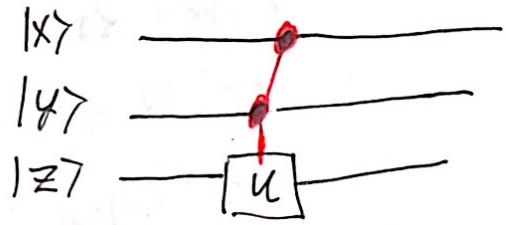
= Does nothing to the first & second bits, acts with U on the third bit only if the second bit is $|1\rangle$, otherwise it does nothing to third bit.



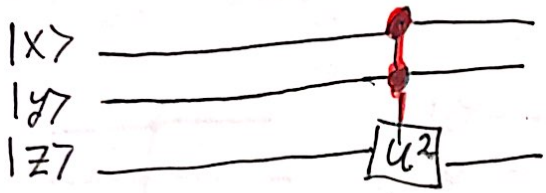
= Does nothing on first bit, acts with U on second bit only if first bit is $|1\rangle$, otherwise it does nothing to second bit, does nothing to third bit.



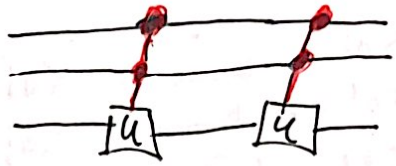
= Keeps $|x\rangle$ unchanged, keeps $|y\rangle$ unchanged, applies U to $|z\rangle$ only if $|x\rangle$ is $|1\rangle$, otherwise it keeps $|z\rangle$ unchanged.



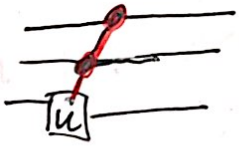
= Keeps |x> and |y> unchanged, applies U to |z> only if |x> <u>and</u> |y> are both |1>, otherwise it keeps |z> unchanged.



=



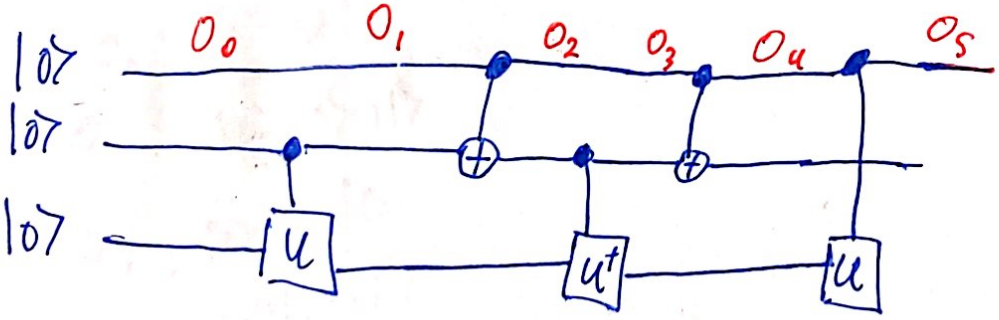
= Applies



twice

Let's Prove each of the cases:

Case 1: $|x\rangle|y\rangle|z\rangle = |0\rangle|0\rangle|0\rangle$



I shall refer back to this diagram for the proof of each case, where the states are labeled by their positions along the circuit by $O_0 \cdots O_5$.

$O_0 : |0\rangle|0\rangle|0\rangle$

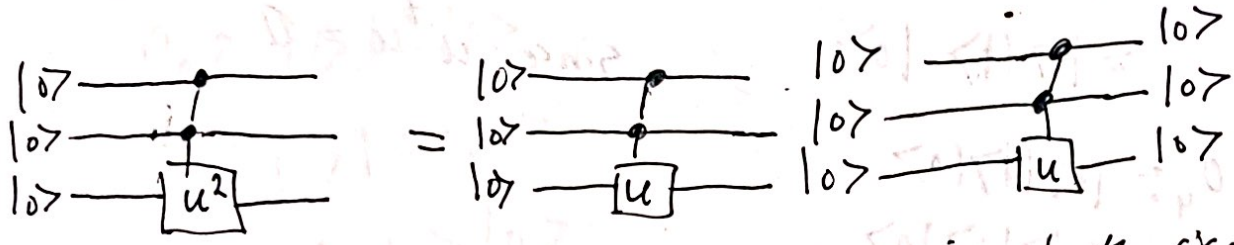
$O_1 : |0\rangle|0\rangle|0\rangle$

$O_2 : |0\rangle|0\rangle|0\rangle$

$O_3 : |0\rangle|0\rangle|0\rangle$

$O_4 : |0\rangle|0\rangle|0\rangle$

$O_5 : |0\rangle|0\rangle|0\rangle$



$\Rightarrow$ output $= |0\rangle|0\rangle|0\rangle$ in both circuits. ✓

Case 2: $|x\rangle|y\rangle|z\rangle = |0\rangle|0\rangle|1\rangle$

$O_0 : |0\rangle|0\rangle|1\rangle$

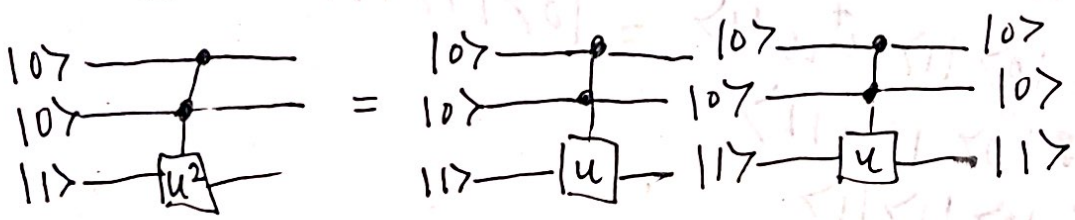
$O_1 : |0\rangle|0\rangle|1\rangle$

$O_2 : |0\rangle|0\rangle|1\rangle$

$O_3 : |0\rangle|0\rangle|1\rangle$

$O_4 : |0\rangle|0\rangle|1\rangle$

$O_5 : |0\rangle|0\rangle|1\rangle$



$\Rightarrow$ output $= |0\rangle|0\rangle|1\rangle$ in both circuits. ✓

Case 3: $|x\rangle|y\rangle|z\rangle = |0\rangle|1\rangle|0\rangle$

$O_0: |0\rangle|1\rangle|0\rangle$

$O_1: |0\rangle|1\rangle U|0\rangle$

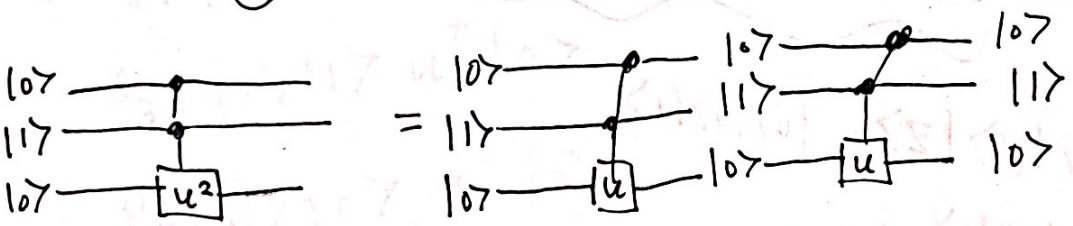
$O_2: |0\rangle|1\rangle U|0\rangle$

$O_3: |0\rangle|1\rangle U^\dagger U|0\rangle$

$= |0\rangle|1\rangle|0\rangle$, since $U^\dagger U = \mathbb{1}$

$O_4: |0\rangle|1\rangle|0\rangle$

$O_5: |0\rangle|1\rangle|0\rangle$



$\Rightarrow$ output $= |0\rangle|1\rangle|0\rangle$ in both circuits. ✓

Case 4: $|x\rangle|y\rangle|z\rangle = |0\rangle|1\rangle|1\rangle$

$O_0: |0\rangle|1\rangle|1\rangle$

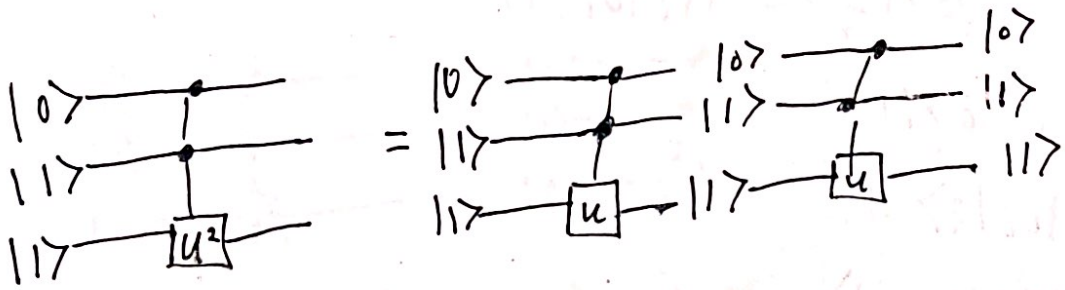
$O_1: |0\rangle|1\rangle U|1\rangle$

$O_2: |0\rangle|1\rangle U|1\rangle$

$O_3: |0\rangle|1\rangle U^\dagger U|1\rangle = |0\rangle|1\rangle|1\rangle$

$O_4: |0\rangle|1\rangle|1\rangle$

$O_5: |0\rangle|1\rangle|1\rangle$



$\Rightarrow$ output $= |0\rangle|1\rangle|1\rangle$ in both circuits. ✓

Case 5: $|x\rangle|y\rangle|z\rangle = |1\rangle|0\rangle|0\rangle$

O_0 : $|1\rangle|0\rangle|0\rangle$

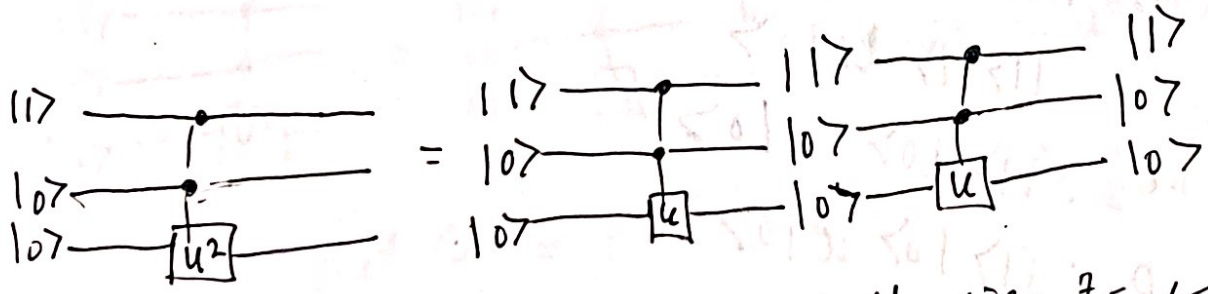
O_1 : $|1\rangle|0\rangle|0\rangle$

O_2 : $|1\rangle|1\rangle|0\rangle$

O_3 : $|1\rangle|1\rangle U^{+}|0\rangle$

O_4 : $|1\rangle|0\rangle U^{+}|0\rangle$

O_5 : $|1\rangle|0\rangle U^{+}U|0\rangle = |1\rangle|0\rangle|0\rangle$



$\Rightarrow$ Output $= |1\rangle|0\rangle|0\rangle$ for both circuits. ✓

Case 6: $|x\rangle|y\rangle|z\rangle = |1\rangle|0\rangle|1\rangle$

$o_0 = |1\rangle|0\rangle|1\rangle$

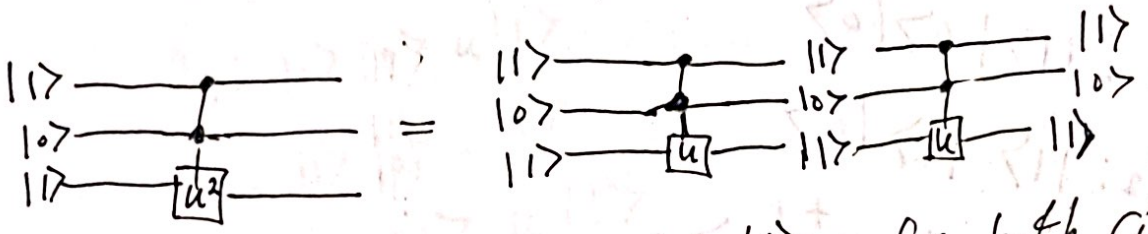
$o_1 : |1\rangle|0\rangle|1\rangle$

$o_2 : |1\rangle|1\rangle|1\rangle$

$o_3 : |1\rangle|1\rangle u^{+}|1\rangle$

$o_4 : |1\rangle|0\rangle u^{+}|1\rangle$

$o_5 : |1\rangle|0\rangle u u^{+}|1\rangle = |1\rangle|0\rangle|1\rangle$



$\Rightarrow$ output $= |1\rangle|0\rangle|1\rangle$ for both circuits. ✓

Case 7: $|x\rangle|y\rangle|z\rangle = |1\rangle|1\rangle|0\rangle$

$o_0 : |1\rangle|1\rangle|0\rangle$

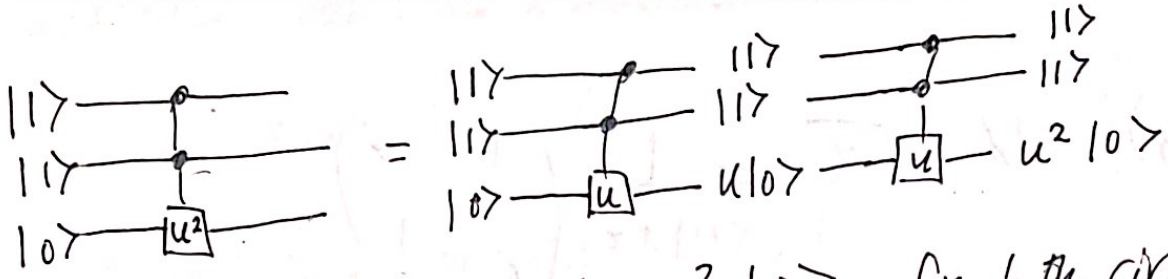
$o_1 : |1\rangle|1\rangle u|0\rangle$

$o_2 : |1\rangle|0\rangle u|0\rangle$

$o_3 : |1\rangle|0\rangle u|0\rangle$

$o_4 : |1\rangle|1\rangle u|0\rangle$

$o_5 : |1\rangle|1\rangle u u|0\rangle = |1\rangle|1\rangle u^2|0\rangle$



$\Rightarrow$ output $= |1\rangle|1\rangle U^2|0\rangle$ for both circuits.

Case 8: $|x\rangle|y\rangle|z\rangle = |1\rangle|1\rangle|1\rangle$

$O_0: |1\rangle|1\rangle|1\rangle$

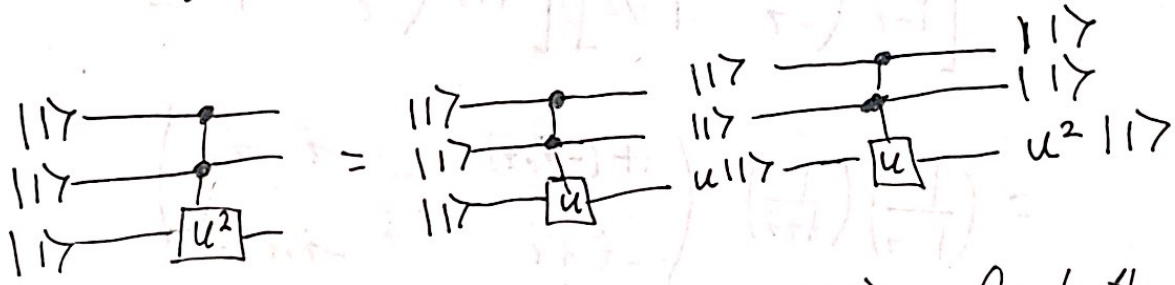
$O_1: |1\rangle|1\rangle U|1\rangle$

$O_2: |1\rangle|0\rangle U|1\rangle$

$O_3: |1\rangle|0\rangle U|1\rangle$

$O_4: |1\rangle|1\rangle U|1\rangle$

$O_5: |1\rangle|1\rangle UU|1\rangle = |1\rangle|1\rangle U^2|1\rangle$



$\Rightarrow$ out Put $= |1\rangle|1\rangle U^2|1\rangle$ for both circuits.

$\Rightarrow$ The required circuit identity is verified for all possible permutations of $|x\rangle|y\rangle|z\rangle$ in standard basis.

b) $U = \sqrt{X} = \frac{1}{1+i}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$

1) Show U is unitary

unitary definition: $U U^{+} = \mathbb{1}$, where U^{+} is the Hermitian conjugate $U^{+} = (U^{T})^{*}$

$$U^{+} = (U^{T})^{*} = \left[\frac{1}{1+i}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}\right]^{*}$$

$$= \frac{1}{1-i}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$$

$$U^{+} U = \left[\frac{1}{1-i}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}\right]\left[\frac{1}{1+i}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}\right]$$

$$= \left(\frac{1}{1-i}\right)\left(\frac{1}{1+i}\right)\begin{pmatrix} 1+(-i\cdot i) & i-i \\ -i+i & -i\cdot i+1 \end{pmatrix}$$

$$= \frac{1}{1+\cancel{i}-\cancel{i}-(i)^2}\begin{pmatrix} 1+1 & 0 \\ 0 & 1+1 \end{pmatrix}$$

$$= \frac{1}{2}\cdot 2\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{1}.$$

Hence $U^{+} U = \mathbb{1}$, namely U is unitary. ✓

2) Show that $u^2 = X$

Recall that $X = |0\rangle\langle 1| + |1\rangle\langle 0|$

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

$$u^2 = u\,u = \frac{1}{1+i}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \frac{1}{1+i}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$$

$$= \frac{1}{(1+i)(1+i)}\begin{pmatrix} 1+i^2 & i+i \\ i+i & i^2+1 \end{pmatrix}$$

$$= \frac{1}{1+2i+i^2}\begin{pmatrix} 0 & 2i \\ 2i & 0 \end{pmatrix}$$

$$= \frac{1}{2i}\begin{pmatrix} 0 & 2i \\ 2i & 0 \end{pmatrix}$$

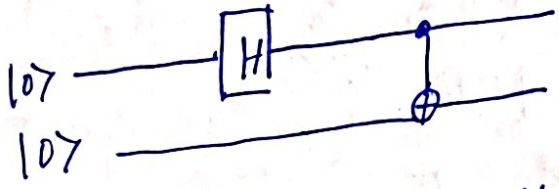
$$= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$= X$$

$$\Longrightarrow u^2 = X.$$

5.3 R&P 5.10

Recall that the Bell circuit:

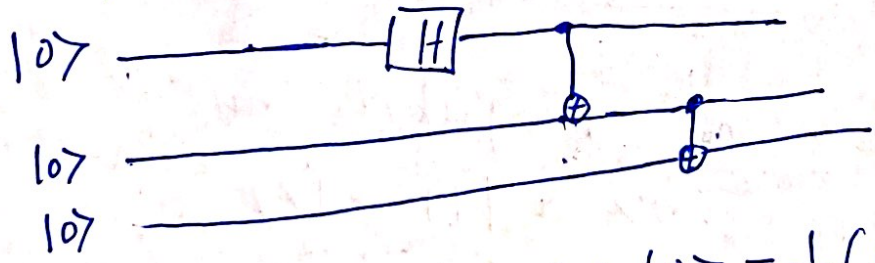


starting with input $|0\rangle|0\rangle$

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

$$\text{CNOT}\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

One can extend this by applying an extra CNOT after H for each extra qubit in state $|0\rangle$. For example, for a 3-qubit state, we have the following circuit:



Check: $(H \otimes \mathbb{1} \otimes \mathbb{1})\, |0\rangle|0\rangle|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\, |0\rangle\, |0\rangle$

$$(\text{CNOT} \otimes \mathbb{1})\, \frac{1}{\sqrt{2}}(|000\rangle + |100\rangle)$$

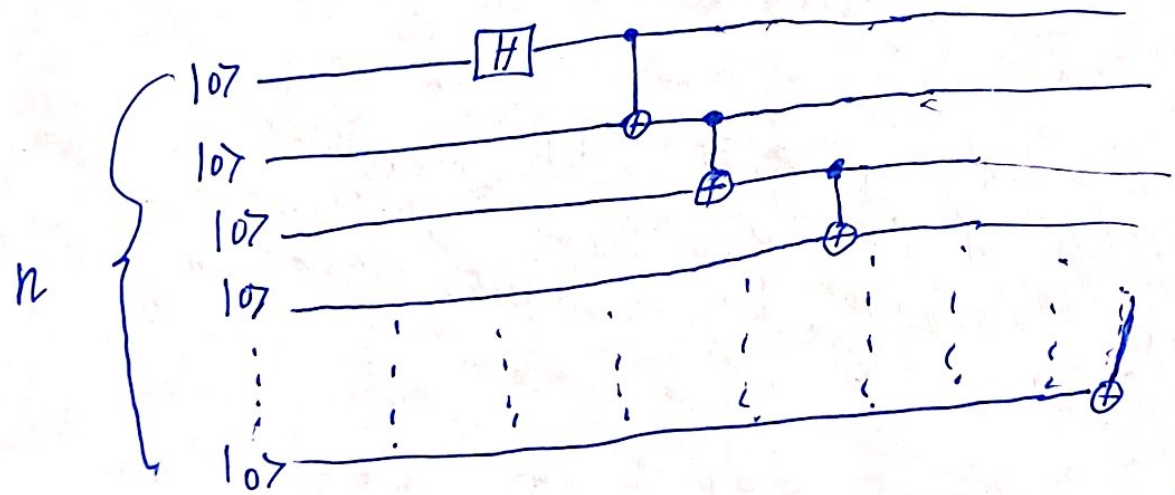
$$= \frac{1}{\sqrt{2}}(|00\rangle + |110\rangle)$$

$$\mathbb{1} \otimes \text{CNOT}\ \frac{1}{\sqrt{2}}(|000\rangle + |110\rangle) = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

✓

Hence the circuit above has taken an input state $|000\rangle$ and produced a 3-qubit cat state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.

One can recursively extend this circuit for n-qubit input state $|\underbrace{00\cdots0}_{n}\rangle$, by adding CNOT gates for each qubit after the first application of H, namely



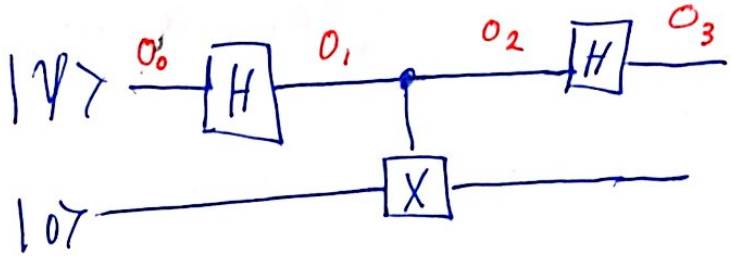
to produce an n-qubit output cat state

$$\frac{1}{\sqrt{2}}(|\underbrace{00\cdots0}_{n}\rangle + |\underbrace{11\cdots1}_{n}\rangle).$$

5.4 R&P. 5-17

on Page 8, Rieffel & Polak say that the effects of quantum circuits cannot be seen by simply looking at the circuit diagrams, and must be explicitly calculated.

Circuit 1 =



let $|\psi\rangle = a|0\rangle + b|1\rangle$

O_0: $|\psi\rangle|0\rangle = (a|0\rangle + b|1\rangle)|0\rangle$

O_1: $H \otimes \mathbb{1}\left[(a|0\rangle + b|1\rangle)|0\rangle\right] = (a|+\rangle + b|-\rangle)|0\rangle$

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

O_2: $\left[|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X\right]\left(\frac{a}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{b}{\sqrt{2}}(|0\rangle - |1\rangle)\right)|0\rangle$

$$= \frac{a}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) + \frac{b}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$$

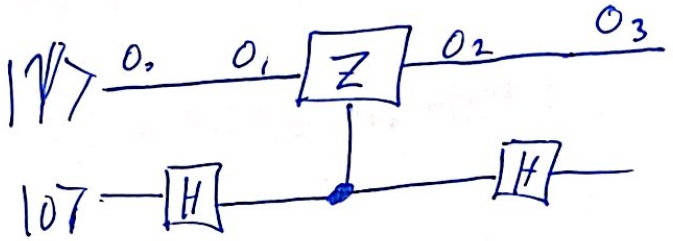
O_3: $H \otimes \mathbb{1}\left[\frac{a}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) + \frac{b}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)\right]$

$$= \frac{a}{\sqrt{2}}(|+\rangle|0\rangle + |-\rangle|1\rangle) + \frac{b}{\sqrt{2}}(|+\rangle|0\rangle - |-\rangle|1\rangle)$$

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

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

Circuit 2 =



O_0: $|\psi\rangle|0\rangle = \frac{1}{\sqrt{2}}(a|0\rangle + b|1\rangle)|0\rangle$

O_1: $(\mathbb{1}\otimes H)\frac{1}{\sqrt{2}}(a|0\rangle+b|1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(a|0\rangle+b|1\rangle)|+\rangle$

$$= \frac{1}{\sqrt{2}}(a|0\rangle+b|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$$

$$= \frac{1}{2}(a|0\rangle|0\rangle + a|0\rangle|1\rangle + b|1\rangle|0\rangle + b|1\rangle|1\rangle)$$

O_2: $\left(|0\rangle\langle 0|\otimes Z + |1\rangle\langle 1|\otimes \mathbb{1}\right)\frac{1}{2}\left(a|0\rangle|0\rangle + a|0\rangle|1\rangle + b|1\rangle|0\rangle + b|1\rangle|1\rangle\right)$

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

And recall $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$, so

$$Z|0\rangle = |0\rangle, \quad Z|1\rangle = -|1\rangle, \quad \text{so}$$

$$O_2: \frac{1}{2}\left(a|0\rangle|0\rangle + a|0\rangle|1\rangle + b|1\rangle|0\rangle - b|1\rangle|1\rangle\right)$$

$$O_3: \mathbb{1} \otimes H\left(\frac{1}{2}\left(a|0\rangle|0\rangle + a|0\rangle|1\rangle + b|1\rangle|0\rangle - b|1\rangle|1\rangle\right)\right)$$

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

$$= \frac{1}{2}\Big(a|0\rangle \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + a|0\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$+ b|1\rangle \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) - b|1\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\Big)$$

$$= \frac{1}{2\sqrt{2}}\Big[a\left(|0\rangle|0\rangle + |0\rangle|1\rangle + |0\rangle|0\rangle - |0\rangle|1\rangle\right)$$
$$+ b\left(|1\rangle|0\rangle + |1\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle\right)$$

$$= \frac{1}{2\sqrt{2}}\left[a\left(2|0\rangle|0\rangle\right) + b\left(2|1\rangle|1\rangle\right)\right]$$

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