Lecture 11

Time to develop the quantum circuit model of computation

Important single-qubit operations

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad T \equiv \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi \end{bmatrix}$$

phase gate

T gate

Can show that $H = \dfrac{X+Z}{\sqrt{2}}$, $S = T^2$

useful to define rotation operators

$R_x(\theta) = e^{-i\theta X/2}$ $R_y(\theta)$ + $R_z(\theta)$ defined similarly

represents a rotation about x axis in Bloch sphere

will take basis gate set to be $\{CNOT, H, T\}$

First important theorem:

Any single qubit unitary operator can be decomposed as

$$e^{i\delta} \begin{bmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{bmatrix} \begin{bmatrix} \cos\theta/2 & \sin\theta/2 \\ -\sin\theta/2 & \cos\theta/2 \end{bmatrix} \begin{bmatrix} e^{i\beta/2} & 0 \\ 0 & e^{-i\beta/2} \end{bmatrix}$$

plausible: any 2x2 ~~unitary~~ matrix has 8 parameters, but unitarity introduces 4 constraints, leaving 4 parameters

can express any 2x2 unitary as

$$\begin{bmatrix} e^{i(\delta+\alpha/2+\beta/2)}\cos\theta/2 & e^{i(\delta+\alpha/2-\beta/2)}\sin\theta/2 \\ -e^{i(\delta-\alpha/2+\beta/2)}\sin\theta/2 & e^{i(\delta-\alpha/2-\beta/2)}\cos\theta/2 \end{bmatrix}$$

we then get the factorization above

can rewrite the factorization above as

$$e^{i\delta}\, R_z(\alpha)\, R_y(\theta)\, R_z(\beta)$$

Useful corollary:

Let U be a single-qubit unitary gate.

Then $\exists\ A, B, C$ (all unitary) such that $ABC = I$ &

$$U = e^{i\delta} A X B X C$$

Take $A = R_z(\alpha) R_y(\theta/2)$

$$B = R_y\left(-\frac{\theta}{2}\right) R_z\left(-\left(\frac{\beta+\alpha}{2}\right)\right)$$

$$C = R_z\left(\left(\frac{\beta-\alpha}{2}\right)\right)$$

So $ABC = I$ (by inspection)

$$A \underline{XBX} C$$

$$XBX = X R_y\left(-\frac{\theta}{2}\right) X X R_z\left(-\left(\frac{\beta+\alpha}{2}\right)\right) X$$

$$= R_y\left(\frac{\theta}{2}\right) R_z\left(\frac{\beta+\alpha}{2}\right)$$

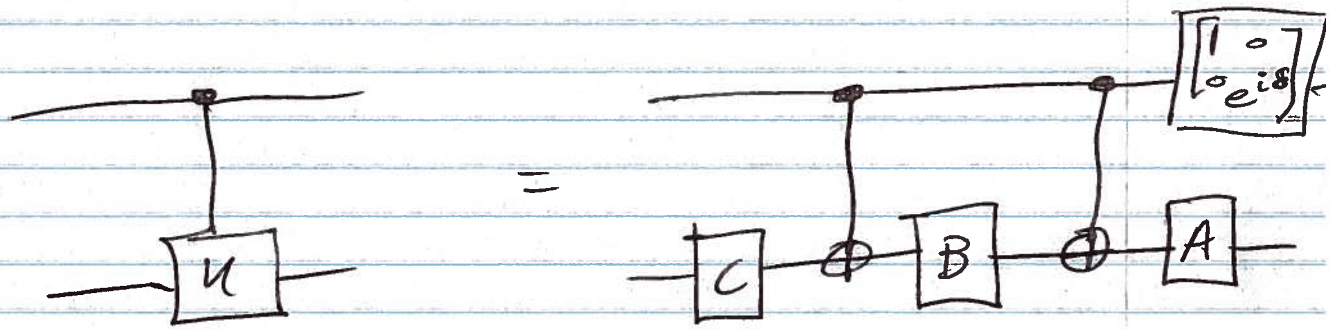
then $\underbrace{R_z(\alpha) R_y\left(\frac{\theta}{2}\right)}_{A} \underbrace{R_y\left(\frac{\theta}{2}\right) R_z\left(\frac{\beta+\alpha}{2}\right)}_{B} \underbrace{R_z\left(\frac{\beta-\alpha}{2}\right)}_{C}$

$$= R_z(\alpha) R_y(\theta) R_z(\beta)$$

utility of this decomposition is in promoting a single qubit unitary to a controlled one :

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

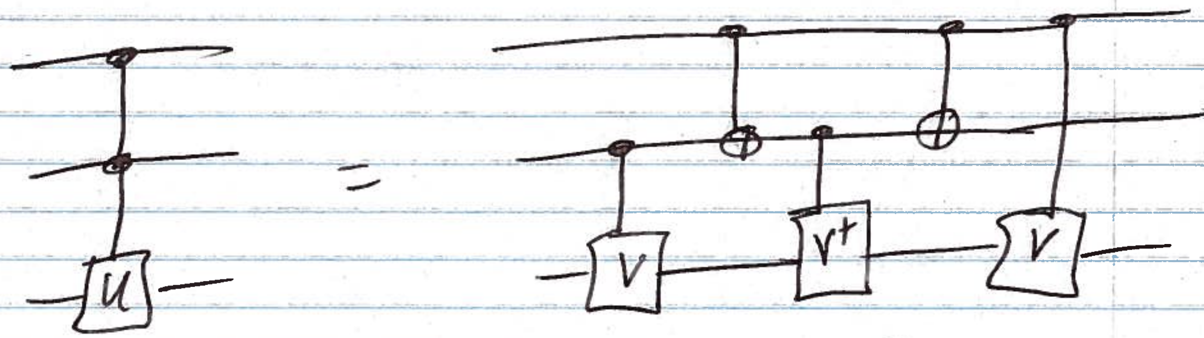
$$|ij\rangle \to (I \otimes U^{i})\,|ij\rangle$$



so if we have CNOTs + arbitrary single-qubit unitaries, then we can implement an arbitrary 2-qubit controlled-unitary controlling on multiple qubits

$$C^n(U)\,|x_1\cdots x_n\rangle|\psi\rangle = |x_1\cdots x_n\rangle\, U^{x_1\cdots x_n}|\psi\rangle$$

example:



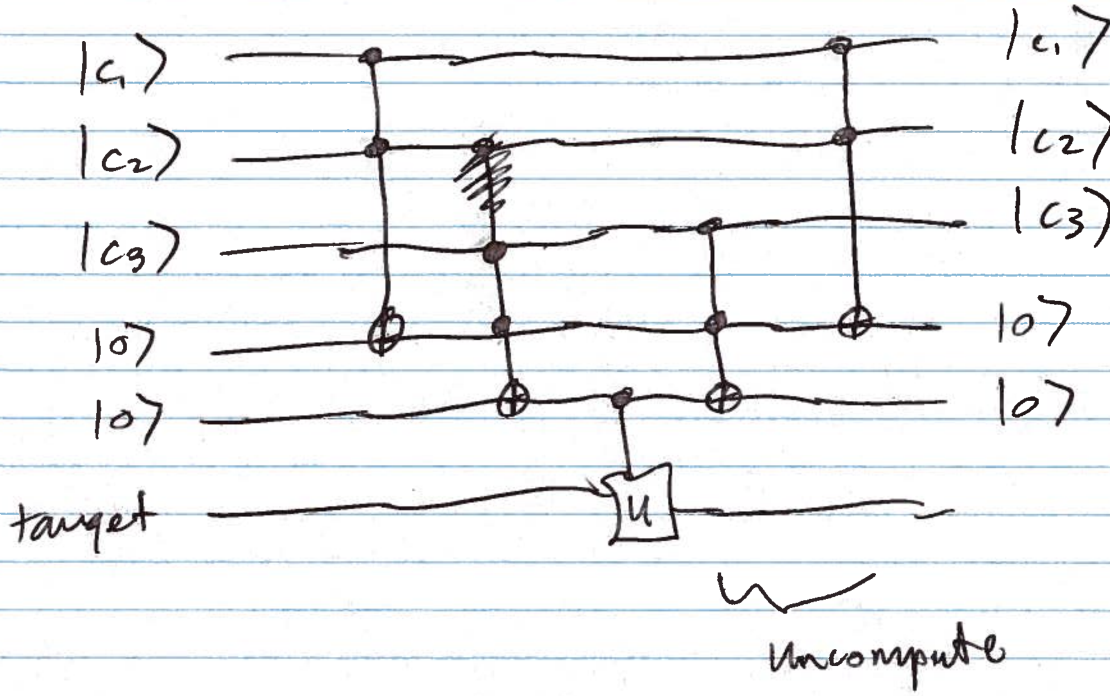
where $V^2=U$

need Toffoli gate as well

controlled-controlled-NOT

rather complicated implementation

To implement controlled-U, we do



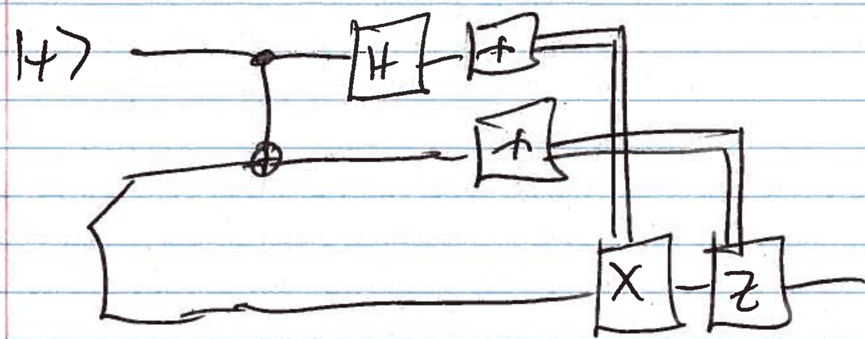
only linear overhead

regarding measurements, we will only mention the "principle of deferred measurement"

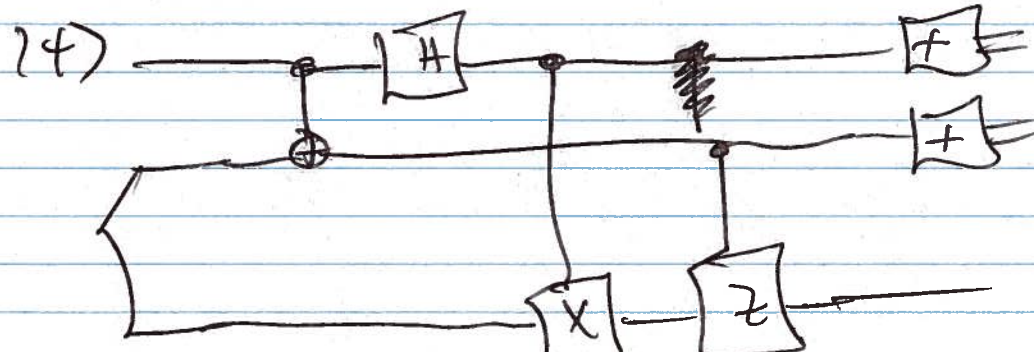
can always move measurements to the end of the computation w/o changing the operation of circuit. replace conditional operations w/ controlled operations

$\Rightarrow$ adaptive strategies do not increase computational power

Example: teleportation



=



universality of quantum gates:
would like to prove that a discrete gate set can simulate any n-qubit unitary to any desired accuracy:

I.e. $\forall U$ & $\varepsilon > 0$ $\exists V_1, \ldots, V_M$ such that

$$\max_{|\psi\rangle} \| U|\psi\rangle - V_M \cdots V_1 |\psi\rangle \|_2 \leq \varepsilon$$

Then the unitary of circuit will be indistinguishable up to an ε-error probab.

Important question: What is the overhead in the simulation?

Begin by showing that any unitary on n qubits can be implemented by CNOTs + single-qubit unitaries.

1st understand how to decompose unitaries using two-level unitaries

$$U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix}$$

want to find 2-level unitaries such that

$$U_3 U_2 U_1 U = I$$

if $b = 0$ then $U_1 = I$

if $b \neq 0$ then $U_1 = \frac{1}{\|(a,b)\|_2} \begin{bmatrix} a^* & b^* & 0 \\ b & -a & 0 \\ 0 & 0 & 1 \end{bmatrix}$

So $U_1 U = \begin{bmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{bmatrix}$

Now if $c'=0$ set

$$U_2 = \begin{bmatrix} a'^* & & \\ & 1 & \\ & & 1 \end{bmatrix}$$

if $c' \neq 0$ set

$$U_2 = \frac{1}{\|(a';c')\|_2} \begin{bmatrix} a'^* & & c'^* \\ & 1 & \\ c' & & -a' \end{bmatrix}$$

then $U_2 U_1 U =$

$$\begin{bmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix}$$

from unitarity, $d'', g'' = 0$

So then set $U_3 = \begin{bmatrix} 1 & & \\ & e''^* & f''^* \\ & h''^* & j''^* \end{bmatrix}$

can do a similar kind of thing for larger dimensional unitaries

Now show that we can use CNOTs ~~as well~~ & single-qubit unitaries

Before we showed that we can decompose U in terms of two-level matrices that act nontrivially on a 2D subspace & trivially on ~~the~~ complementary subspace.

Suppose the basis for the subspace is

$\{|s\rangle, |t\rangle\}$ where $|s\rangle = |s_1 \ldots s_n\rangle$
$|t\rangle = |t_1 \ldots t_n\rangle$

We use the classical idea of Gray codes to effect each two-level transformation.

Example: Suppose 2-level unitary is

$$\begin{bmatrix} a & & & & & & & c \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ b & & & & & & & d \end{bmatrix}$$

The unitary acts nontrivially on the space ~~spanned by~~ span$\{|000\rangle, |111\rangle\}$

So we find a Gray code connecting these states

would like a way to ~~change~~ permute this basis to $\{|011\rangle, |111\rangle\}$ & then act w/

to effect transformation

000

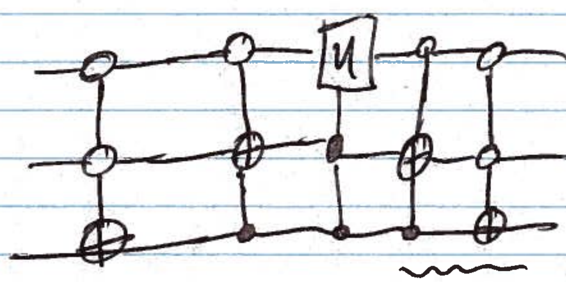
001

011

111

at most 1 bit changes in each transition

So we perform



uncompute

controlled on 00, flip the third takes

000 → 001 → 011

since the Toffoli can be realized w/ single-qubit unitaries + CNOTs, (and same for C-U) we have achieved the goal.