e.g.: QRS (Quantum Recommendation System)
(Kerenidis, Prakash) (2016).
— thought to be first example of an efficient quantum algorithm that provides exponential speedup over known classical algorithms (which were polynomial).

— Ewin Tang (2018) came up with a classical algorithm with similar exponential speed up.

>>> Qubits & Bra-Ket notation

(Due to PAM Dirac).

$|0\rangle$ ket, $\langle 0|$ bra.

$\langle 0|0\rangle$ inner prod, $|0\rangle\langle 0|$ outer prod.

Qubit: 2 level quantum system,
Qudit: d level quantum system.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1.$$

$|0\rangle, |1\rangle$ are "computational basis states".

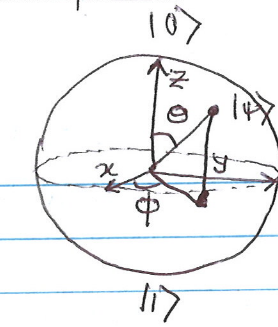
Measurement: get either $|0\rangle$ or $|1\rangle$ with prob. $|\alpha|^2$ or $|\beta|^2$.

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$$

phase irrelevant

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle.$$

Bloch sphere.



Multiple qubits.

$|0\rangle|0\rangle$ or $|00\rangle$ etc.

What happens if you measure single qubit?

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle.$$

Bell State or EPR pair.

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$ "measurement outcomes are correlated".

Single qubit gates.

X gate ("NOT" gate).

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad |0\rangle - \boxed{X} - |1\rangle \qquad |1\rangle - \boxed{X} - |0\rangle.$$

Z gate $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ $\qquad X^2 = Z^2 = H^2 = I.$

H gate $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ "Hadamard gate".

Gates are "unitary operators". (inner prod. preserving linear maps).

Work out what these gates do to $\alpha|0\rangle + \beta|1\rangle$.

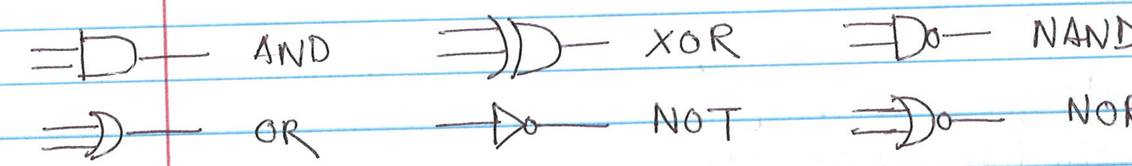
Multi-qubit gates

Again "unitary operators" on tensor prod. space.

Aside: Classical gates

AND, OR, NAND, NOR, NOT, XOR

(NAND & NOR are universal gates)

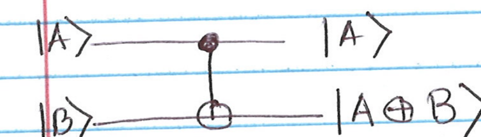


XOR truth table

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

} mod 2 addition.

CNOT (Controlled NOT gate)

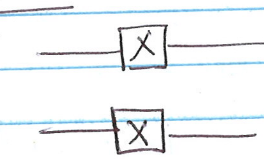


(i) Show that this is unitary

(ii) Find matrix representation.

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

$X \otimes X$



(i) Show this is unitary

(ii) Find matrix representation.

$$U_{X \otimes X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

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

Ex: Can U_{CNOT} be represented as Kronecker product of 2 2x2 matrices? [If yes this would imply that U_{CNOT} can be decomposed into 2 single qubit gates].

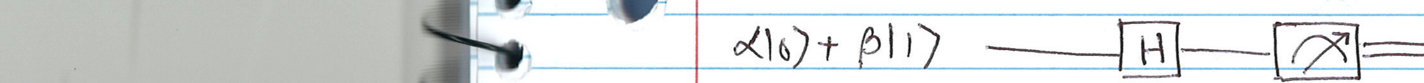
Comment: Any multiqubit gate can be synthesized from CNOT and single qubit gates.

Measurement in bases other than computational basis

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

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad = \left(\frac{\alpha+\beta}{\sqrt{2}}\right)|+\rangle + \left(\frac{\alpha-\beta}{\sqrt{2}}\right)|-\rangle.$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$\alpha|0\rangle + \beta|1\rangle$ 

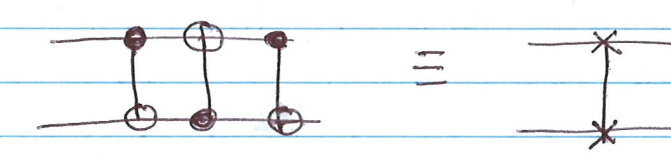
get $|0\rangle$ with prob $\frac{|\alpha+\beta|^2}{2}$,

$|1\rangle$ with prob $\frac{|\alpha-\beta|^2}{2}$.

(More on this next week).

>>> Intro to quantum circuits

SWAP GATE



$|a, b\rangle \to |b, a\rangle$

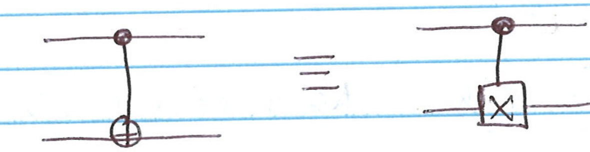
(i) Show it is unitary
(ii) Find matrix representation } HW.

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

Controlled - U

(i) Show unitary
(ii) Find matrix rep.

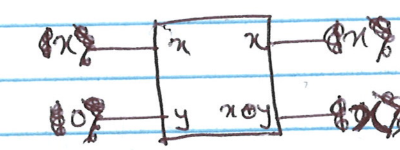
eg.



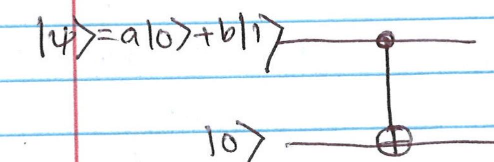
{ Show this circuit identity (Trivial example).

Does there exist a circuit to copy qubits?

Consider this circuit.



Classical bit copy.



What is the output?
$a|00\rangle + b|11\rangle$.

What does copying qubit mean? Final state must be $|\psi\rangle|\psi\rangle$.

Ex: Is this the case?

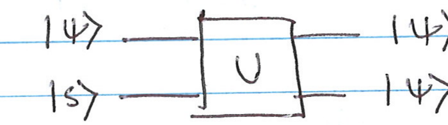
$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab\left(|01\rangle + |10\rangle\right) + b^2|11\rangle$$

For copying to be true: $a^2 = a$, $b^2 = b$
$ab = 0$

exactly one of a, b must be 1, other is 0.

Infact this cannot be done with any other circuit also.

Thm ("No-Cloning Theorem")



$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

Suppose it also works for $|\phi\rangle$

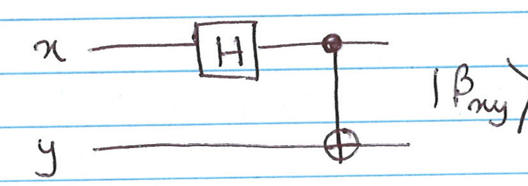
$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle.$$

Taking inner prod:

$$\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2$$ so either $|\psi\rangle = |\phi\rangle$ or $\langle\psi|\phi\rangle = 0$

Therefore general cloning is impossible.

EPR states or Bell states creation (Einstein, Podolsky, Rosen).



$$|\beta_{xy}\rangle \equiv \frac{|0,y\rangle + (-1)^x |1,\bar{y}\rangle}{\sqrt{2}}.$$

$\bar{y}$ is negation of y

$|00\rangle \to (|00\rangle + |11\rangle)/\sqrt{2}$

$|01\rangle \to (|01\rangle + |10\rangle)/\sqrt{2}$

$|10\rangle \to (|00\rangle - |11\rangle)/\sqrt{2}$

$|11\rangle \to (|01\rangle - |10\rangle)/\sqrt{2}$

Ex: Check the circuit actually does this.

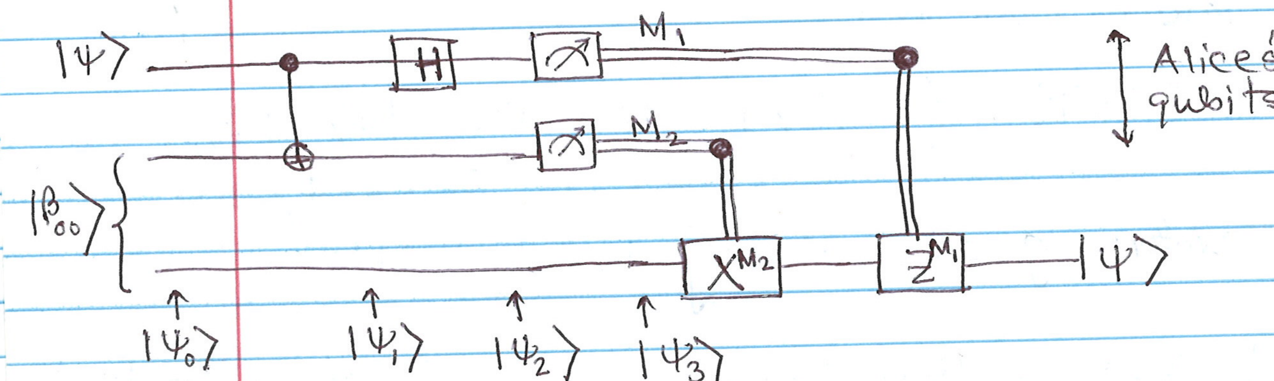
[Make class fill out table in class].

Quantum Teleportation

$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$

- Alice, Bob has EPR pair.
- Bob is in hiding many years later
- Alice's mission : Send Bob a quantum state $|\psi\rangle$.
- Alice does not know state $|\psi\rangle$.
- Alice can only send Bob classical info.

$\boxed{\text{Can she do it?}}$ [Discuss with class].



$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle$$
$$= \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\Big]$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\Big]$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left[\alpha\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)(|00\rangle + |11\rangle) + \beta\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)(|10\rangle + |01\rangle)\right]$$

$$= \frac{1}{2}\Big[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle)$$
$$+ |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\Big]$$

After Alice's measurement

Measurement outcome	Bob's state	
00	$\alpha\|0\rangle + \beta\|1\rangle$	✓
01	$\alpha\|1\rangle + \beta\|0\rangle$	X
10	$\alpha\|0\rangle - \beta\|1\rangle$	Z
11	$\alpha\|1\rangle - \beta\|0\rangle$	XZ

Then Bob fixes up the state! Cool! :)

Classical computation on a quantum computer

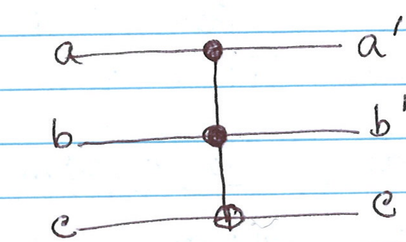
- Quantum logic gates are reversible.
- Classical logic gates are inherently irreversible. (eg. NAND)

Thm: Any classical circuit can be replaced by an equivalent circuit containing only reversible elements, by making use of a reversible gate called Toffoli gate.

Pf.

Input a	b	c	Output a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Circuit.



Toffoli gate