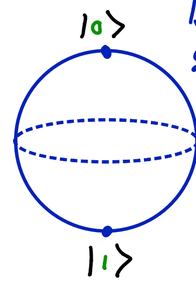
Quantum Computing

not "null"

Qubit two-state system basis $\{|0\rangle, |1\rangle\}$



Bloch Sphere

Examples: Spin 1/2 $\{|z^+\rangle, |z^-\rangle\}$

Quantum dot $\{|\text{empty}\rangle, |\text{filled}\rangle\}$

Photon polarization $\{|H\rangle, |V\rangle\}$

Josephson junction $\{|\text{flux } 0\rangle, |\text{flux } 1\rangle\}$

Coherent superposition lifetime (memory) ~ 3 hours for P-doped Si

Gates Unitary transformations $\Rightarrow$ physical processes

1-Qubit gates:

$|\psi\rangle$ — $\boxed{Z}$ — $\sigma_z|\psi\rangle$

$$\sigma_z = \begin{array}{cc} & \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ & \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{array}{c} |0\rangle \\ |1\rangle \end{array} \end{array}$$

$|\psi\rangle$ — $\boxed{R_\theta}$ — $R_\theta|\psi\rangle$

$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

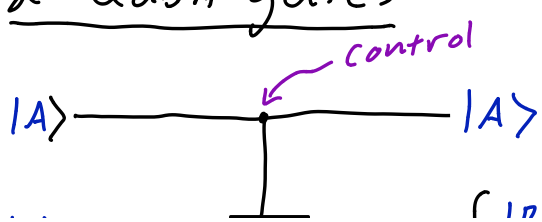
$|\psi\rangle$ — $\boxed{X}$ — $\sigma_x|\psi\rangle$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{"Not"}$$

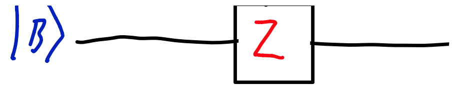
$|\psi\rangle$ — $\boxed{H}$ — $H|\psi\rangle$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{"Hadamard"}$$

2-Qubit gates

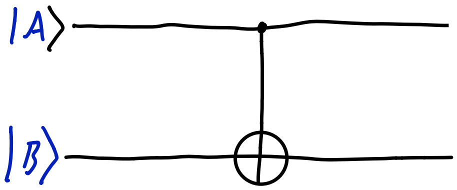


$$\begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \left(\begin{array}{cccc} \underbrace{\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}}_{I_B} & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} \end{array} \right. \end{array} \quad \text{Control-Z}$$



$$\begin{cases} |B\rangle & (A=0) \\ \sigma_z|B\rangle & (A=1) \end{cases}$$

$$\begin{pmatrix} \cdots & & & \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \leftarrow \sigma_z(B)$$



$|A\rangle$

$$\begin{cases} |B\rangle & (A=0) \\ |\neg B\rangle & (A=1) \end{cases}$$

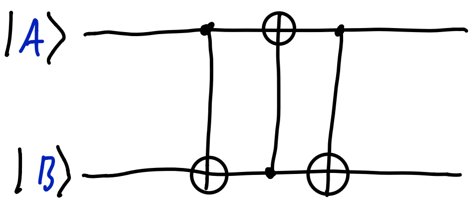
$$\parallel$$

$$|A\rangle \otimes |A \text{ xor } B\rangle$$

$$= |A\rangle \otimes |(A+B) \bmod 2\rangle$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{Control-Not}$$

$\sigma_x(B)$

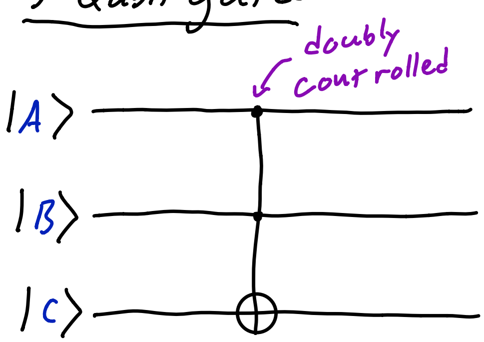


$|B\rangle$

$|A\rangle$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{swap}$$

3-Qubit gates

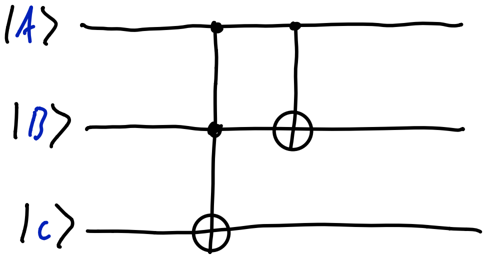


$|A\rangle$

$|B\rangle$

$$\begin{cases} |\neg C\rangle & \text{if } A \wedge B \\ |C\rangle & \text{else} \end{cases}$$

"Toffoli"



$|A\rangle$

$|(A+B) \bmod 2\rangle$ Sum

$|A \wedge B\rangle$ Carry

Quantum adder

Fourier Transform

$\{f_k : k=0,\dots,N-1\} \longrightarrow \{g_j : j=0,\cdots N-1\} \qquad g_j = \frac{1}{\sqrt{N}} \sum_k e^{2\pi i jk/N} f_k$

$\vec{f} \in \mathbb{C}^N \longrightarrow \vec{g} \in \mathbb{C}^N \qquad \vec{g} = \overleftrightarrow{F} \vec{f} \qquad F_{jk} = \frac{1}{\sqrt{N}} e^{2\pi i jk/N}$

<u>Example</u> $N=4 \qquad e^{2\pi i/4} = i \qquad F_{jk} = \frac{1}{2}(i)^{jk} \qquad \overleftrightarrow{F} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$

<u>$k=0$</u> $\quad f_k = \delta_{k0} \qquad \vec{g} = \frac{1}{2}\begin{array}{c} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \end{array}\begin{array}{l} j=0 \\ j=1 \\ j=2 \\ j=3 \end{array}$

<u>$k=1$</u> $\quad f_k = \delta_{k1} \qquad \vec{g} = \frac{1}{2}\begin{pmatrix} 1 \\ i \\ -1 \\ -i \end{pmatrix}$ etc.

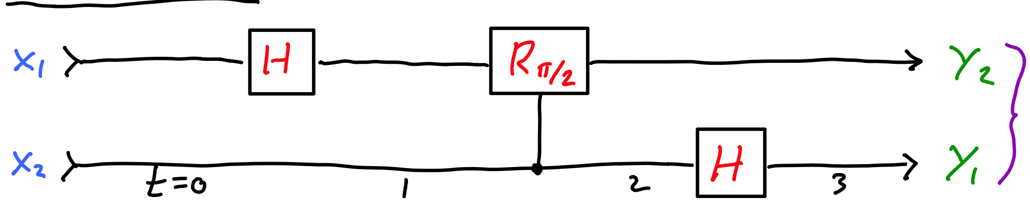
<u>Quantum FT</u> $\quad Q$ qubits $\Longrightarrow N = \dim \mathcal{H} = 2^Q$

Basis States $\quad \underbrace{|x_1 x_2 \cdots x_Q\rangle}_{\text{binary expansion of integer } k} = |x_1\rangle |x_2\rangle \cdots |x_Q\rangle \qquad x_i \in \{0,1\}$

<u>Example</u> $Q=2,\ N=4 \qquad |k=0\rangle = |00\rangle \qquad |k=1\rangle = |\underset{\uparrow}{0}1\rangle$ binary value of k

$|k\rangle = |x_1 x_2\rangle \qquad |k=2\rangle = |10\rangle \qquad |k=3\rangle = |11\rangle$

<u>QFT Circuit</u>



Note: Reverse order

Unitary evolution

basis state $|k\rangle = |x_1\rangle|x_2\rangle$

$$|\psi_0\rangle = |x_1\rangle|x_2\rangle$$

$$e^{2\pi i[0.x_1]} = \begin{cases} +1 & (x_1=0) \\ -1 & (x_1=1) \end{cases}$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_1]}|1\rangle\right)|x_2\rangle$$

$$e^{2\pi i[0.x_1x_2]} = \begin{cases} 1 & x_1x_2 = 00 \\ i & 01 \\ -1 & 10 \\ -i & 11 \end{cases}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_1x_2]}|1\rangle\right)|x_2\rangle$$

$$|\psi_3\rangle = \frac{1}{2}\left(|0\rangle + e^{2\pi i[0.x_1x_2]}|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i[0.x_2]}|1\rangle\right)$$

Example $|k=1\rangle = |01\rangle$ $\quad x_1=0 \quad x_2=1 \quad [0.x_1x_2] = 1/4 \quad e^{2\pi i[0.x_1x_2]} = i$

$$|\psi_3\rangle = \frac{1}{2}\left(|0\rangle + i|1\rangle\right)\otimes\left(|0\rangle - |1\rangle\right)$$
$$= \frac{1}{2}\left(|00\rangle + i|10\rangle - |01\rangle - i|11\rangle\right)$$

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

reverse order

Exponential speedup

FT takes $\mathcal{O}(2^Q)$ time to evaluate one FT

QFT takes $\mathcal{O}(2^Q)$ gates to evaluate $\dim \mathcal{H} = 2^Q$ FT's

Shor's algorithm

to factor large integer (break encryption)

1. Choose $a < M$
2. Find periods of $f(k) \equiv a^k \bmod M$ i.e. k s.t. $f(k+l) = f(l)$ by QFT
3. GCD $(a^{k/2} \pm 1, M)$ are factors of M