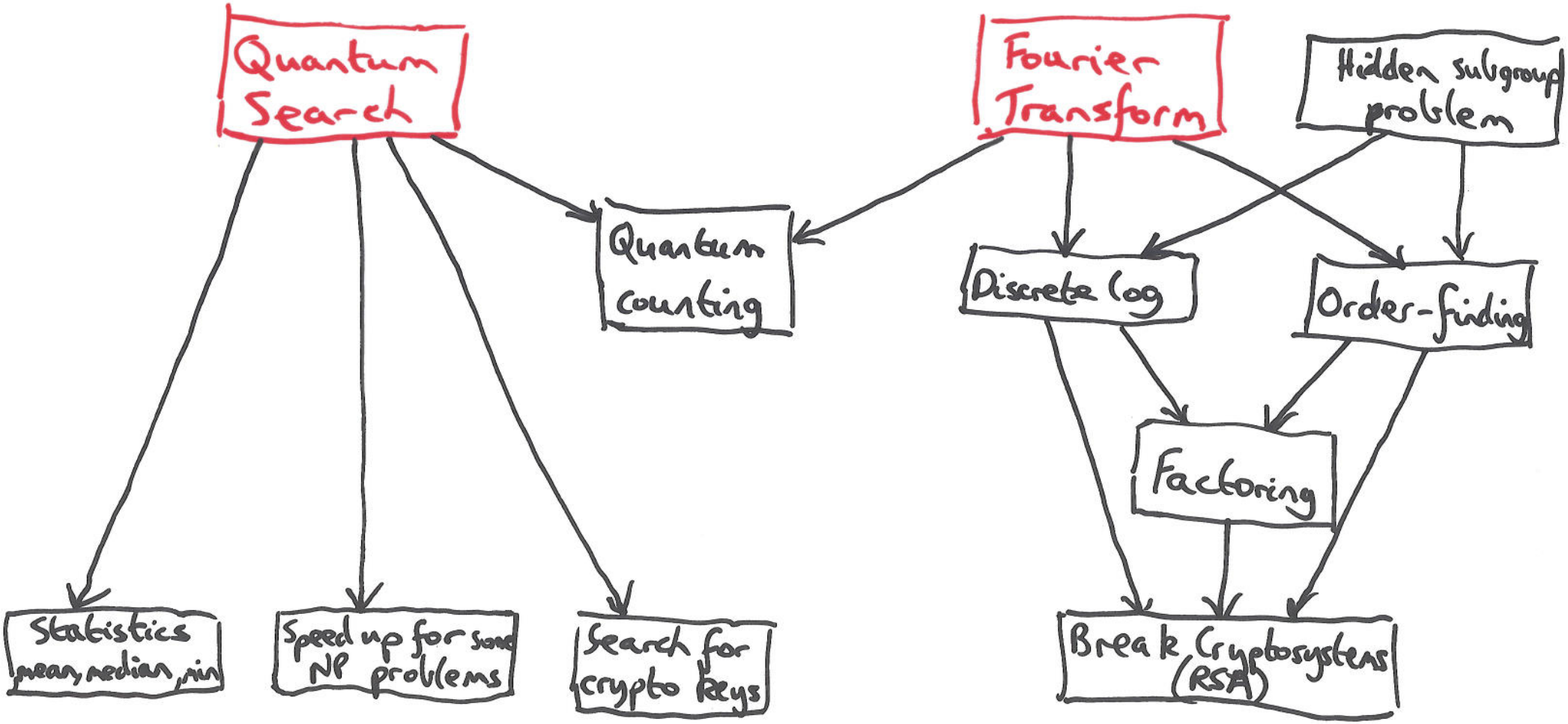
Quantum Circuits

Quantum Algorithms

Two classes:

1. Based on Shor's quantum Fourier transform
   - exponential speed-up.
2. Based on Grover's algorithm for quantum searching
   - quadratic speed-up.

Main quantum algorithms



Why so few quantum algorithms?

.... a difficult problem.

Why?

1. Algorithm design is difficult
   ... must be better than best classical.

2. Our intuitions adapted to classical world.

Single Qubit Operations

e.g.

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

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}; \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}; \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

← Sometimes called $\pi/8$ gate for silly reasons

Observe,

$$H = (X+Z)/\sqrt{2}, \qquad S = T^2.$$

A single qubit, $a|0\rangle + b|1\rangle$ can be visualized as (θ, φ) on the unit sphere, where $a = \cos(\theta/2)$, $b = e^{i\varphi}\sin(\theta/2)$.
a can be considered real up to overall phase.
Bloch vector is $(\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta)$

Exercise

Find the points on the Bloch sphere which correspond to the normalized eigenvectors of the different Pauli matrices.

e.g.

eigenvectors of $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ are $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$

$\Rightarrow$ normalised eigenvectors are $(|0\rangle + |1\rangle)/\sqrt{2}$ and $(|0\rangle - |1\rangle)/\sqrt{2}$

For $(|0\rangle + |1\rangle)/\sqrt{2}$:

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

But $a = \cos(\theta/2) \Rightarrow \theta = \frac{\pi}{2}$, $b = e^{i\varphi}\sin(\theta/2) \Rightarrow \varphi = 0$

$\therefore$ Bloch vector $= (\cos\varphi\sin\theta, \sin\varphi\sin\theta, \cos\theta) = (1, 0, 0)$.

Exponents of Pauli matrices

Rotation operators about the $\hat{x}$, $\hat{y}$ and $\hat{z}$ axes,

$$R_x(\theta) = e^{-i\theta X/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_y(\theta) = e^{-i\theta Y/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_z(\theta) = e^{-i\theta Z/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}.$$

Let x be a real number and A a matrix such that $A^2 = I$. Then,

$$e^{iAx} = \cos(x) I + i \sin(x) A$$

Proof sketch: eigenvalues of A are ± 1. e.g. if both $\lambda_0 = \lambda_1 = \pm 1$, then

$$\begin{aligned} e^{iAx} &= e^{\lambda_0 i x} |a_0\rangle\langle a_0| + e^{\lambda_1 i x} |a_1\rangle\langle a_1| \\ &= \cos(x)\left[|a_0\rangle\langle a_0| + |a_1\rangle\langle a_1|\right] + i\sin(x)\left[\lambda_0 |a_0\rangle\langle a_0| + \lambda_1 |a_1\rangle\langle a_1|\right] \\ &= \cos(x) I + i \sin(x) A. \end{aligned}$$

$\Rightarrow$ e.g. $R_x(\theta) = e^{-i\theta X/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} X$.

Similarly,

$$T = R_z\left(\tfrac{\pi}{4}\right) = \begin{bmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{bmatrix},$$

to within global phase.

Also,

$$H = \begin{bmatrix} \cos\tfrac{\pi}{4} & -\sin\tfrac{\pi}{4} \\ \sin\tfrac{\pi}{4} & \cos\tfrac{\pi}{4} \end{bmatrix} \begin{bmatrix} e^{-i\pi} & 0 \\ 0 & e^{i\pi} \end{bmatrix} \times -1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$= R_x\left(\tfrac{\pi}{2}\right) \times R_z(2\pi) \times e^{i\pi}.$$

More generally,

$$R_{\hat{n}}(\theta) = e^{-i\theta\hat{n}\cdot\vec{\sigma}/2} = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)(n_x X + n_y Y + n_z Z),$$

where $\hat{n} = (n_x, n_y, n_z)$, and $\vec{\sigma} = (X, Y, Z)$.

This can be proved by using,

$$(\hat{n}\cdot\vec{\sigma})^2 = I.$$

Bloch Sphere interpretation

Let a qubit be represented by Bloch vector, $\vec{\lambda}$.

Then $R_{\hat{n}}(\theta)$ rotates the state by angle θ about the $\hat{n}$ axis.

Observe:

$$X R_y(\theta) X = R_y(-\theta).$$

Proof:

Use $XYX = -Y$.

Single Qubit Unitary

$$U = e^{i\alpha} R_{\hat{n}}(\theta).$$

Prove?

$$H = X + Z$$

$$\Rightarrow H = e^{i\frac{\pi}{2}} R_{101}(\pi).$$

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = e^{i\pi/4} \begin{bmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} = e^{i\pi/4} R_{001}\left(\frac{\pi}{2}\right).$$

Z-Y Decomposition for a Single Qubit

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta).$$

Proof:

$$U = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2} \end{bmatrix}.$$

Remember:

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta).$$

Give a decomposition using R_x instead of R_z

.....

Another Decomposition

$$U = e^{i\alpha} R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\delta),$$

where $\hat{n}$ and $\hat{m}$ are not parallel.

Another Decomposition

$\exists$ unitaries A, B, C, such that,

$$ABC = I, \quad \text{and}$$

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

Proof:

Set $A = R_z(\beta) R_y(\gamma/2)$, $B = R_y(-\gamma/2) R_z(-(\delta+\beta)/2)$,

$C = R_z((\delta-\beta)/2)$.

Then, $ABC = I$, $XBX = R_y(\frac{\gamma}{2}) R_z(\frac{\delta+\beta}{2})$, $AXBXC = R_z(\beta) R_y(\gamma) R_z(\delta)$

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

What are A, B, and C, and α for the Hadamard gate?

Remember:

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

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

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

. . . . .

$$\ldots = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \ldots \; ??$$

Observe:

$$HXH = Z, \quad HYH = -Y, \quad HZH = X,$$

$$HTH = R_x(\pi/4), \quad \ldots \text{ to within global phase.}$$

... therefore X and Z are related by conjugacy with respect to H, and Y is self-conjugate with respect to H.

Composition of Single Qubit Operations

Rotate by β_1 about $\hat{n}_1$.

then Rotate by β_2 about $\hat{n}_2$.

Result is rotation by β_{12} about $\hat{n}_{12}$, where,

$$c_{12} = c_1 c_2 - s_1 s_2 \hat{n}_1 \cdot \hat{n}_2$$

$$s_{12}\hat{n}_{12} = s_1 c_2 \hat{n}_1 + c_1 s_2 \hat{n}_2 - s_1 s_2 \hat{n}_2 \times \hat{n}_1,$$

where $c_i = \cos(\beta_i/2)$, $s_i = \sin(\beta_i/2)$,

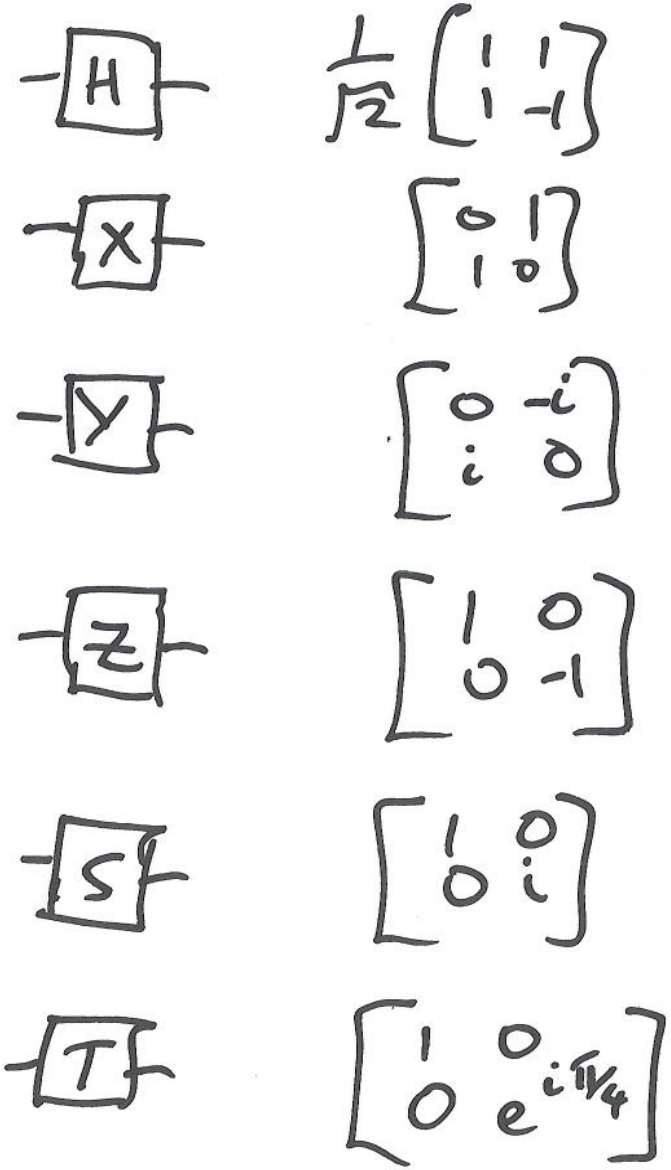
$c_{12} = \cos(\beta_{12}/2)$, $s_{12} = \sin(\beta_{12}/2)$.

If $\beta_1 = \beta_2$ and $\hat{n}_1 = \hat{z}$, then,

$$c_{12} = c^2 - s^2 \hat{z} \cdot \hat{n}_2, \qquad s_{12}\hat{n}_{12} = sc(\hat{z} + \hat{n}_2) - s^2 \hat{n}_2 \times \hat{z},$$

where $c = c_1$ and $s = s_1$.

Common Circuit Symbols



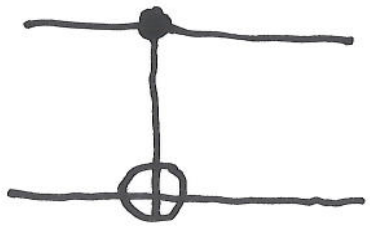
Controlled Operations

"If A is true,
then do B".

Controlled-NOT (CNOT)

$$|c\rangle|t\rangle \rightarrow |c\rangle|t \oplus c\rangle$$

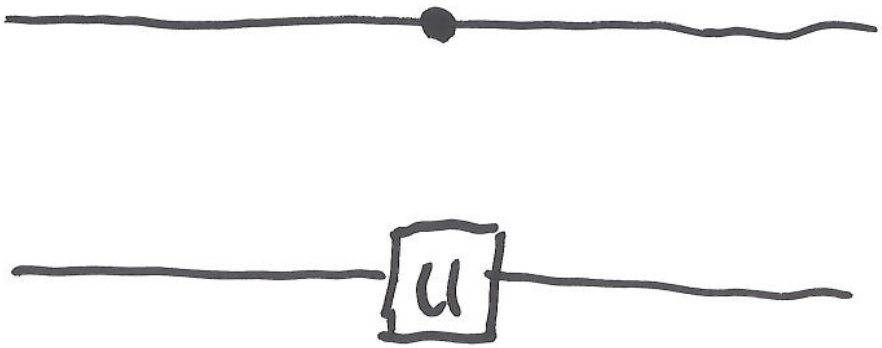
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



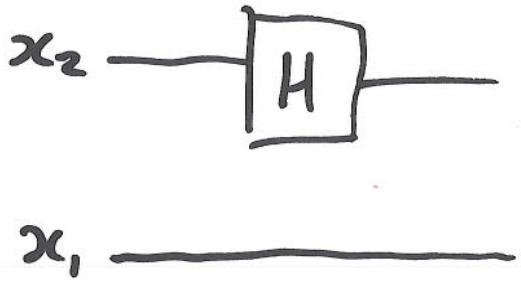
More generally.....

Controlled-U

$$|c\rangle|t\rangle \longrightarrow |c\rangle U^c|t\rangle$$

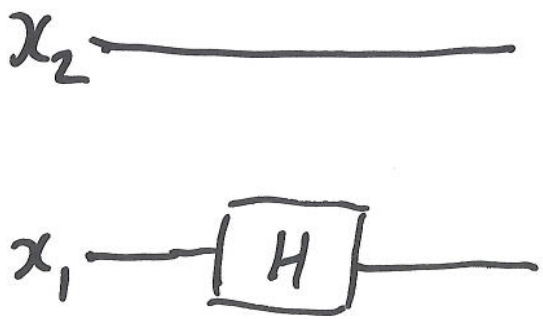


What is the 4x4 unitary matrix for



in the computational basis?

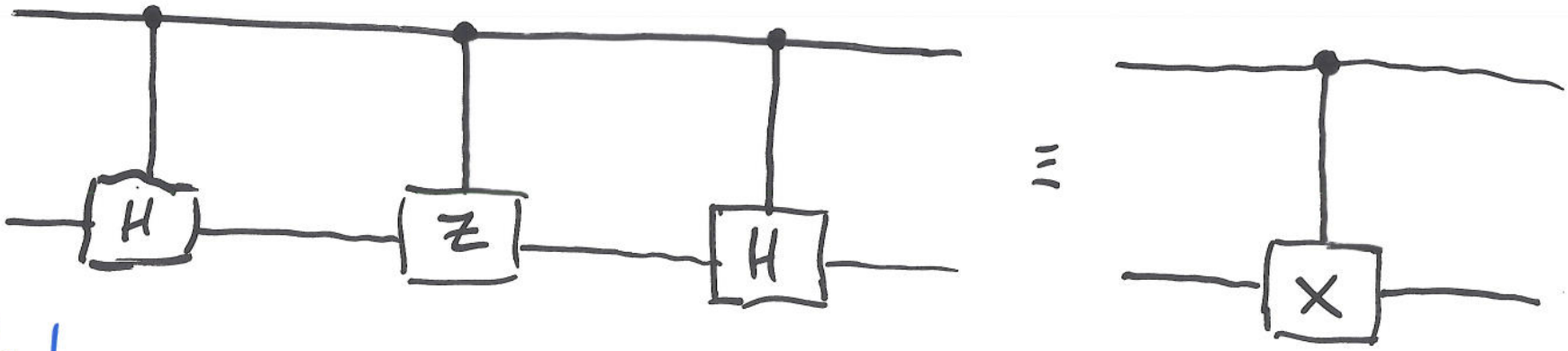
and for



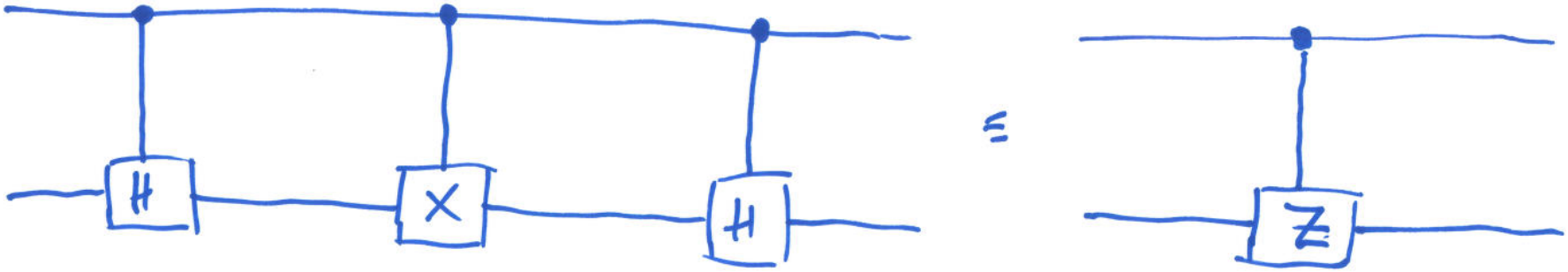
?

Controlled-Z Gate

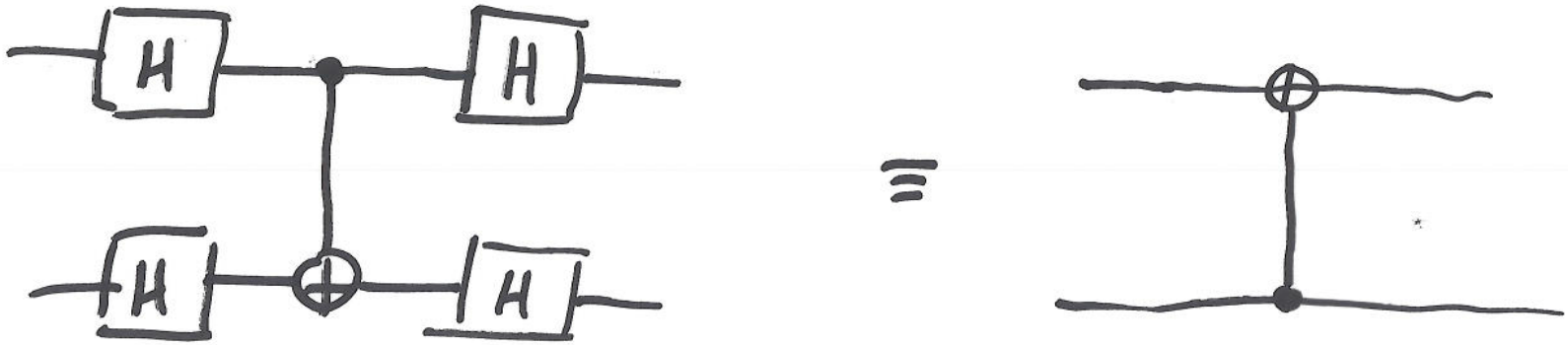
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



Similarly



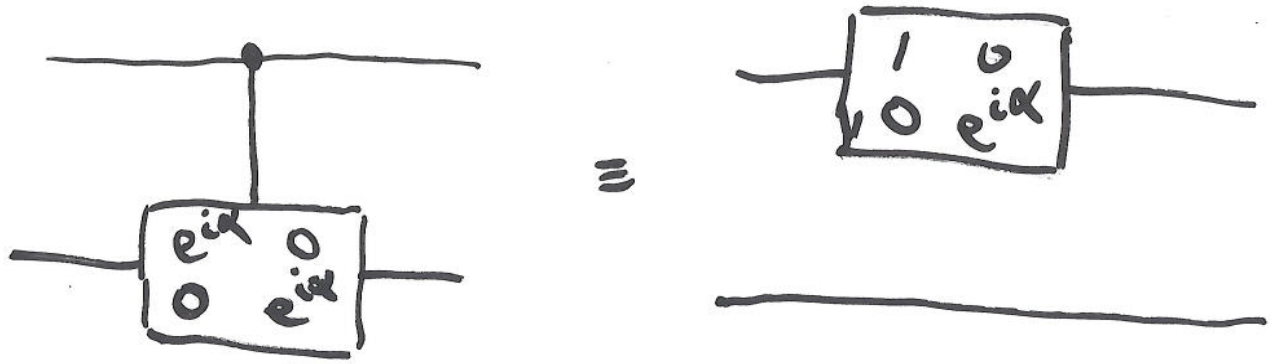
~~Basis Transformations~~ Conjugacy Relationships



Show this.

Implement Controlled-U using single qubit operations and controlled-NOT

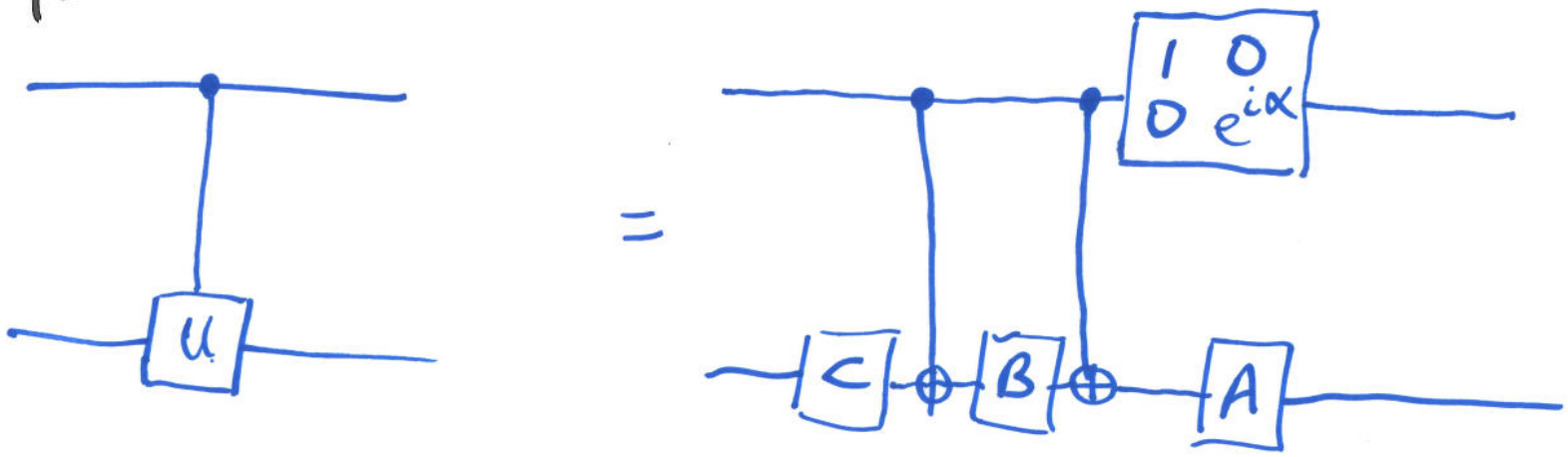
observe:



also,

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

therefore



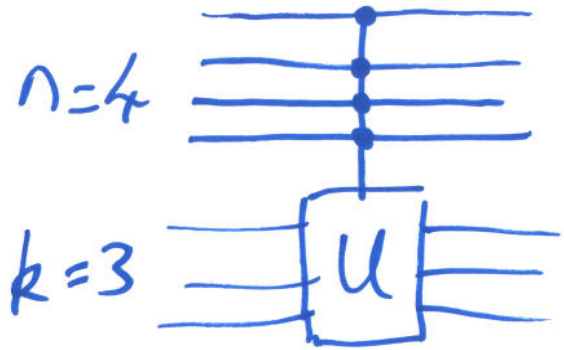
Multiple Qubit Conditioning

We have $n+k$ qubits, and U is a k qubit unitary. Then,

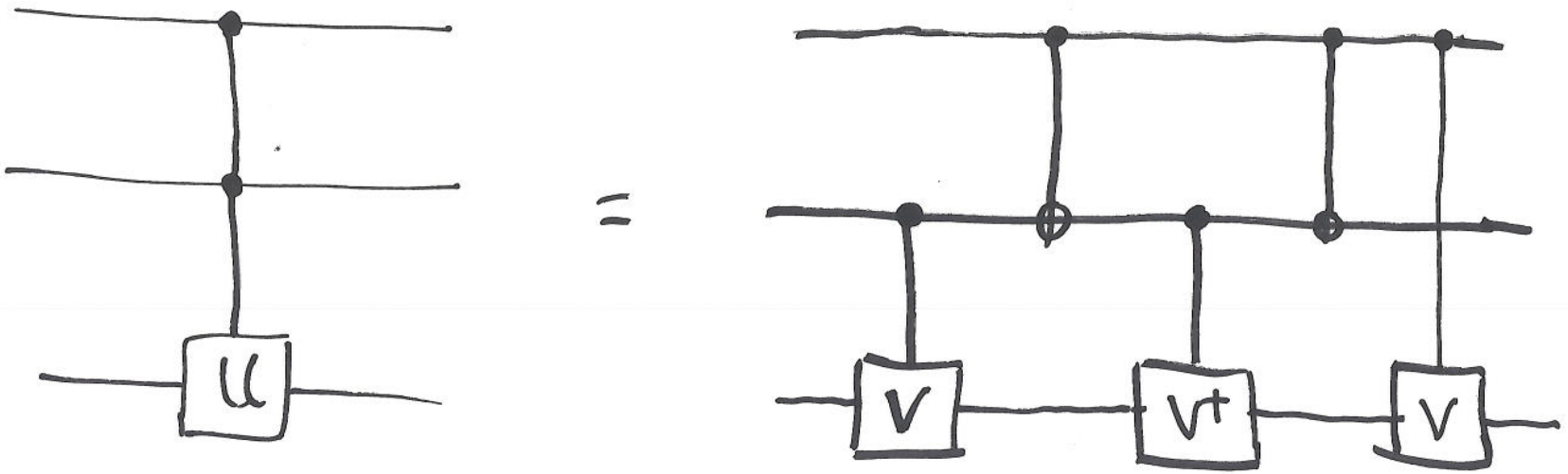
$$C^n(U)|x_1 x_2 \ldots x_n\rangle|\psi\rangle$$

$$= |x_1 x_2 \ldots x_n\rangle U^{x_1 x_2 \ldots x_n}|\psi\rangle$$

where $x_1 x_2 \ldots x_n$ is the product of bits.



Multi-Qubit Control via Single-Qubit Control



$C^2(U)$

where $V^2 = U$.

When $V = (1-i)(I+iX)/2$, then $C^2(U)$ is the Toffoli gate (i.e. $V^2 = X$).

Universal Computation

One and two qubit reversible gates are sufficient to implement the Toffoli gate,

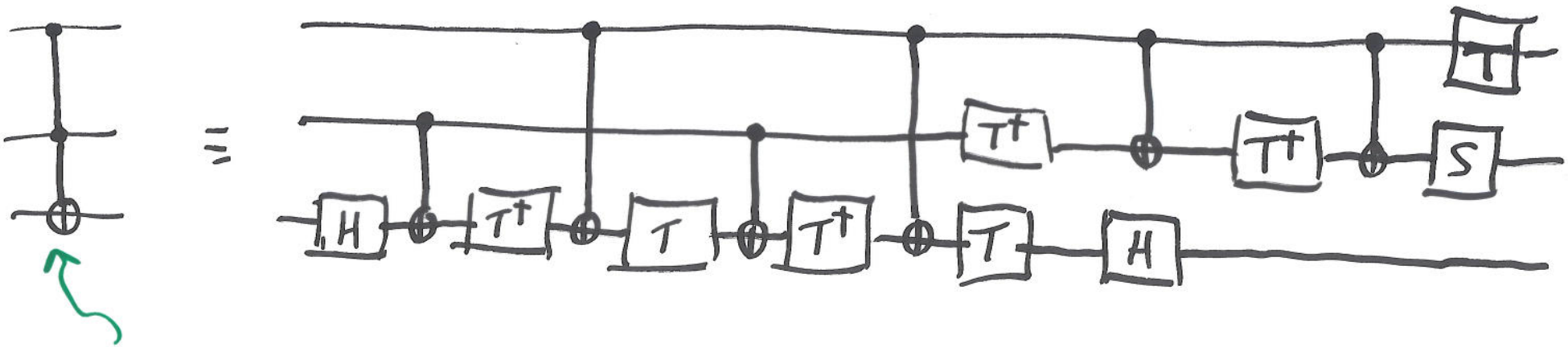
... and, more generally,

suffice for universal computation.

Even Fewer Gates are needed

Any unitary can be composed, to good approximation, from just Hadamard, phase, controlled-NOT and T gates.

e.g.



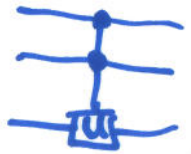
Toffoli gate

Fredkin Gate (controlled-swap)

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

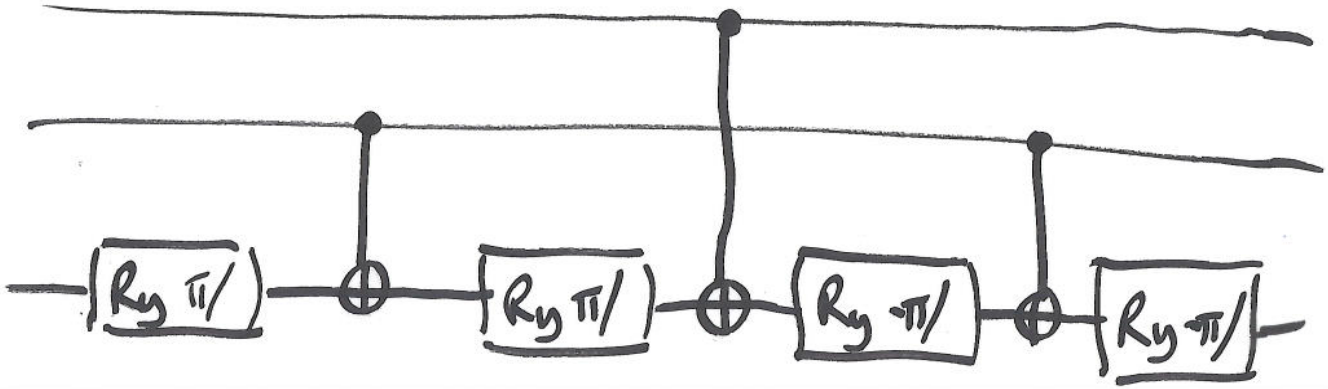
1) Fredkin gate using three Toffoli gates? - (think of swap gate)

2) Show that first and last gates can be replaced by CNOT gates.

3) Now replace middle Toffoli gate with circuit for  using two qubit gates. (Fig 4.8)

4) A simpler construction using only five two-qubit gates?

Observe:



$$|c_1, c_2, t\rangle \rightarrow e^{i\Theta(c_1,c_2,t)}|c_1, c_2, t \oplus c_1 \cdot c_2\rangle$$

$\equiv$ Toffoli up to relative phase

.... Sometimes easier to implement than Toffoli.