# **Quantum Circuits**

School on Quantum Computing @Yagami Day 1, Lesson 5 16:00-17:00, March 22, 2005 Eisuke Abe

Department of Applied Physics and Physico-Informatics, and CREST-JST, Keio University



# Bloch sphere representation $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |0\rangle$ $|\alpha|^2 + |\beta|^2 = 1$ $|\psi\rangle = \frac{e^{i\gamma}}{\cos\frac{\theta}{2}}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$ $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$ $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$

# Important single qubit gates

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

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

$$X^2 = Y^2 = Z^2 = H^2 = I$$

$$S = T^2$$
,  $S^2 = Z$ 

$$[X,Y] = 2iZ, \{X,Y\} = 0, \cdots$$

HXH = Z, HYH = -Y, HZH = X

# **Exponential operator**

$$\exp(iAx) \equiv \sum_{n=0}^{\infty} \frac{(iAx)^n}{n!}$$

$$A^2 = I \implies \exp(iAx) = \cos x \cdot I + i \sin x \cdot A$$

This operator is important because it appeared in the solution to Schrödinger equation

$$|\psi(t+\Delta t)\rangle = \exp\left[\frac{-iH\Delta t}{\hbar}\right]|\psi(t)\rangle$$

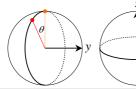
# Rotation gates

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

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

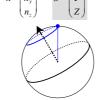
$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{bmatrix} \exp(-i\theta/2) & 0\\ 0 & \exp(i\theta/2) \end{bmatrix}$$

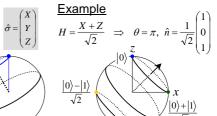




# Rotation about the $\hat{n}$ axis

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





- An arbitrary controlled-U gate can be implemented using only single qubit gates and CNOT
- 2. An arbitrary (controlled) $^{n}$ -U gate can be implemented using single qubit gates and CNOT
- 3. Two-level unitary gates are universal
- 4. Single-qubit gates and CNOT are universal
- 5. Hadamard, S, T, and CNOT are universal

# Road to universality proof

- 1. An arbitrary controlled- ${\cal U}$  gate can be implemented using only single qubit gates and CNOT
- An arbitrary (controlled)<sup>n</sup>-U gate can be implemented using single qubit gates and CNOT
- 3. Two-level unitary gates are universal
- 4. Single-qubit gates and CNOT are universal
- 5. Hadamard, S, T, and CNOT are universal

# Z-Y decomposition

For an arbitrary single qubit gate U, there exist real numbers  $\alpha$ ,  $\beta$ ,  $\gamma$ , and  $\delta$  such that

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

**Proof** 

$$\begin{split} U &= \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2} \end{bmatrix} \\ &= e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos\gamma/2 & -\sin\gamma/2 \\ \sin\gamma/2 & \cos\gamma/2 \end{bmatrix} \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix} \\ &= e^{i\alpha}R_*(\beta)R_*(\gamma)R_*(\delta) \end{split}$$

# Corollary

Set A, B, C as

$$A = R_{z}(\beta)R_{y}\left(\frac{\gamma}{2}\right)$$

$$B = R_{y}\left(-\frac{\gamma}{2}\right)R_{z}\left(-\frac{\delta + \beta}{2}\right)$$

$$C = R_{z}\left(\frac{\delta - \beta}{2}\right)$$

Then

$$ABC = I$$
,  $U = e^{i\alpha}AXBXC$ 

We will construct an arbitrary controlled-U gate using  $A,\,B,\,{\rm and}\,\,C$ 

# Corollary

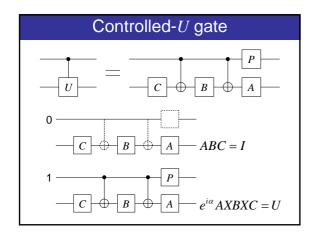
### **Proof**

$$\overline{ABC} = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(-\frac{\gamma}{2}\right)R_z\left(-\frac{\delta}{2} - \frac{\beta}{2}\right)R_z\left(\frac{\delta}{2} - \frac{\beta}{2}\right) = I$$

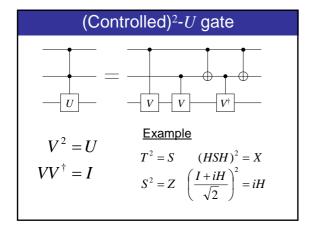
$$A = R_z(\beta)R_y\left(\frac{\gamma}{2}\right) \quad B = R_y\left(-\frac{\gamma}{2}\right)R_z\left(-\frac{\delta + \beta}{2}\right) \quad C = R_z\left(\frac{\delta - \beta}{2}\right)$$

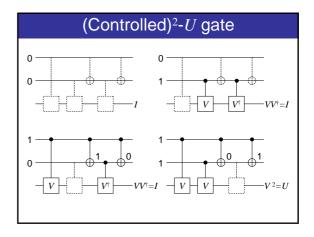
$$\begin{split} e^{i\alpha}AXBXC &= e^{i\alpha}AXR_y \bigg( -\frac{\gamma}{2} \bigg) XXR_z \bigg( -\frac{\delta+\beta}{2} \bigg) XC & XX = I \\ & XR_y(\theta)X = R_y(-\theta) \\ &= e^{i\alpha}AR_y \bigg( \frac{\gamma}{2} \bigg) R_z \bigg( \frac{\delta+\beta}{2} \bigg) C & XR_z(\theta)X = R_z(-\theta) \\ &= e^{i\alpha}R_z(\beta)R_y \bigg( \frac{\gamma}{2} \bigg) R_y \bigg( \frac{\gamma}{2} \bigg) R_z \bigg( \frac{\delta+\beta}{2} \bigg) R_z \bigg( \frac{\delta-\beta}{2} \bigg) \\ &= e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta) = U \end{split}$$

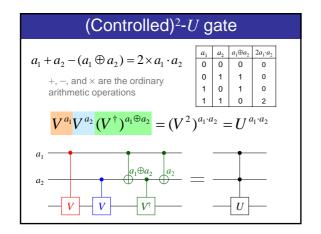
# Phase shifter $P = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix}$ $|00\rangle \rightarrow |00\rangle$ $|01\rangle \rightarrow |01\rangle$ $|10\rangle \rightarrow e^{i\alpha}|10\rangle$ $|11\rangle \rightarrow e^{i\alpha}|11\rangle$ $P \otimes I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha} & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{bmatrix}$

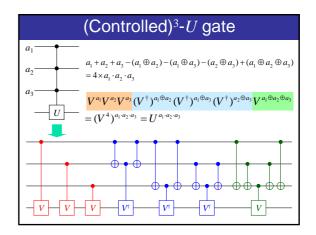


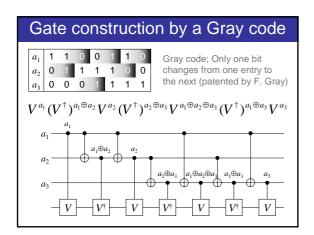
- An arbitrary controlled-U gate can be implemented using only single qubit gates and CNOT
- 2. An arbitrary (controlled) $^{n}$ -U gate can be implemented using single qubit gates and CNOT
- 3. Two-level unitary gates are universal
- 4. Single-qubit gates and CNOT are universal
- **5**. Hadamard, *S*, *T*, and CNOT are universal

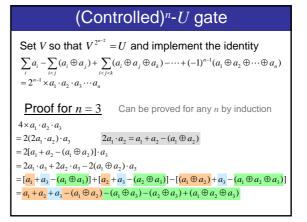


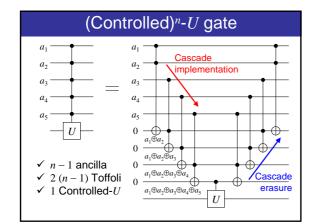




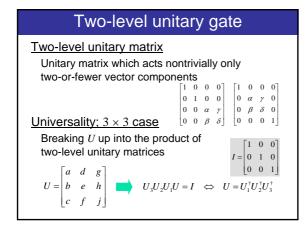








- An arbitrary controlled-U gate can be implemented using only single qubit gates and CNOT
- An arbitrary (controlled)<sup>n</sup>-U gate can be implemented using single qubit gates and CNOT
- 3. Two-level unitary gates are universal
- 4. Single-qubit gates and CNOT are universal
- 5. Hadamard, S, T, and CNOT are universal

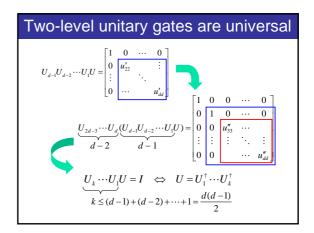


$$\begin{aligned} & U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix} & U_1 \equiv \begin{bmatrix} I & b^* \\ \frac{d}{\sqrt{|a|^2 + |b|^2}} & \frac{b^*}{\sqrt{|a|^2 + |b|^2}} & 0 \\ \frac{b}{\sqrt{|a|^2 + |b|^2}} & \frac{d}{\sqrt{|a|^2 + |b|^2}} & 0 \\ 0 & e' & h' \\ c' & f' & j' \end{bmatrix} & U_2 \equiv \begin{bmatrix} a'^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} & (c' = 0) \\ U_2 U_1 U = \begin{bmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix} & U_2 \equiv \begin{bmatrix} a'^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} & (c' \neq 0) \\ \frac{c'}{\sqrt{|a'|^2 + |c'|^2}} & 0 & \frac{c'^*}{\sqrt{|a'|^2 + |c'|^2}} \\ 0 & 1 & 0 \\ \frac{c'}{\sqrt{|a'|^2 + |c'|^2}} & 0 & \frac{-a'}{\sqrt{|a'|^2 + |c'|^2}} \end{bmatrix} & (c' \neq 0) \end{aligned}$$

Two-level unitary gates are universal 
$$U_{2}U_{1}U = \begin{bmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix}$$

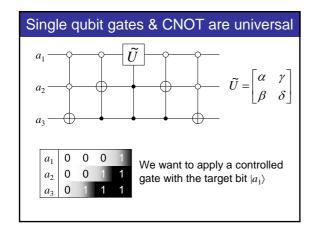
$$U_{3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e''^{*} & f''^{*} \\ 0 & h''^{*} & j''^{*} \end{bmatrix}$$

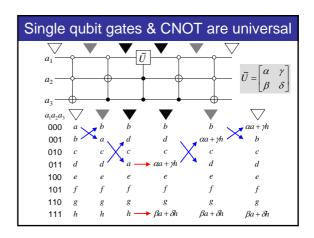
$$U_{3}U_{2}U_{1}U = I \iff U = U_{1}^{\dagger}U_{2}^{\dagger}U_{3}^{\dagger} \qquad U_{3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e''^{*} & f''^{*} \\ 0 & h''^{*} & j''^{*} \end{bmatrix}$$
For *d*-dimensional *U*, we repeat this procedure
$$U = \begin{bmatrix} u_{11} & \cdots & u_{1d} \\ \vdots & \ddots & \vdots \\ u_{d1} & \cdots & u_{dd} \end{bmatrix} \qquad U_{d-1}U_{d-2}\cdots U_{1}U = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & u'_{22} & \vdots \\ \vdots & \ddots & \vdots \\ 0 & \cdots & u'_{dd} \end{bmatrix}$$



- An arbitrary controlled-U gate can be implemented using only single qubit gates and CNOT
- 2. An arbitrary (controlled) $^{n}$ -U gate can be implemented using single qubit gates and CNOT
- 3. Two-level unitary gates are universal
- 4. Single-qubit gates and CNOT are universal
- 5. Hadamard, S, T, and CNOT are universal

### Single qubit gates & CNOT are universal Strategy To show that single qubit & CNOT gates can implement an arbitrary two-level unitary matrix $3 \times 3~U$ acting nontrivially only on $|000\rangle$ and $|111\rangle$ 0 0 0 0 0 0 7 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 d d 0 0 0 0 1 0 0 0 $0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0$ f $0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0$ g $\beta$ 0 0 0 0 0 0 $\delta$





- 1. An arbitrary controlled-U gate can be implemented using only single qubit gates
- 2. An arbitrary (controlled) $^{n}$ -U gate can be implemented using single qubit gates and
- 3. Two-level unitary gates are universal
- 4. Single-qubit gates and CNOT are universal
- 5. Hadamard, S, T, and CNOT are universal

# Discrete set of universal gates

## Why a discrete set of gates?

It can be used to perform quantum computation in an error-resistant fashion

### Problem

The set of unitary operations is continuous

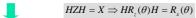
### Strategy

To show that a discrete set can be used to approximate any unitary operation to an arbitrary accuracy

# Approximation by H & T

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} = e^{i\pi/8} \begin{bmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{bmatrix} \cong R_z(\pi/4)$$

 $HTH = e^{i\pi/8}HR_z(\pi/4)H \cong R_x(\pi/4)$ 



 $R_z(\pi/4)R_x(\pi/4) = R_{\hat{n}}(\theta)$ 

 $cos(\theta/2) \equiv cos^2(\pi/8)$   $\theta$ ; irrational multiple of  $2\pi$ 

 $\sin(\theta/2) = \sqrt{1 - \cos^4(\pi/8)} = \sin(\pi/8)\sqrt{1 + \cos^2(\pi/8)}$  $\begin{bmatrix} n_x \\ n_y \end{bmatrix} = \frac{1}{\sqrt{1 + \frac{2\pi}{3}(\pi/8)}} \begin{bmatrix} \cos(\pi/8) \\ \sin(\pi/8) \end{bmatrix}$ 

 $\hat{n} = \begin{bmatrix} n_y \\ n_z \end{bmatrix} \equiv \frac{1}{\sqrt{1 + \cos^2(\pi/8)}} \begin{bmatrix} \sin(\pi/8) \\ \cos(\pi/8) \end{bmatrix}$ 

# Approximation by H & T

$$\begin{split} R_z \bigg( \frac{\pi}{4} \bigg) R_x \bigg( \frac{\pi}{4} \bigg) &= \exp \bigg( -i \frac{\pi}{8} Z \bigg) \exp \bigg( -i \frac{\pi}{8} X \bigg) \\ &= \bigg[ \cos \frac{\pi}{8} I - i \sin \frac{\pi}{8} Z \bigg] \bigg[ \cos \frac{\pi}{8} I - i \sin \frac{\pi}{8} X \bigg] \\ &= \cos^2 \frac{\pi}{8} I - i \sin \frac{\pi}{8} \bigg[ \cos \frac{\pi}{8} X + \sin \frac{\pi}{8} Y + \cos \frac{\pi}{8} Z \bigg] \\ &= \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} \bigg[ n_x X + n_y Y + n_z Z \bigg] = R_{\tilde{n}}(\theta) \end{split}$$

 $\cos(\theta/2) \equiv \cos^2(\pi/8)$  $\sin(\theta/2) = \sqrt{1 - \cos^4(\pi/8)} = \sin(\pi/8)\sqrt{1 + \cos^2(\pi/8)}$  $\begin{bmatrix} n_x \end{bmatrix}$  1  $\begin{bmatrix} \cos(\pi/8) \end{bmatrix}$  $\sin(\pi/8)$ 

# Approximation by H & T

## Weyl's theorem on uniform distribution

Let p be irrational, then the sequence  $\{p, 2p, 3p, ...\}$  is uniformly distributed modulo 1

$$\begin{array}{cccc}
\circ & \{n \ \theta/2\pi \ (\text{mod } 1)\} \\
n = 10 & \circ & \circ & \circ & \circ \\
n = 50 & \circ & \circ & \circ & \circ \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
n = 100 & \circ & \circ & \circ & \circ
\end{array}$$

0.4

0.6

0.8

n = 1

n = 500

0.2

The approximation to accuracy  $\varepsilon$  is realized through  $O(1/\varepsilon)$  times

$$R_{\hat{n}}^{O(1/\varepsilon)}(\theta) \approx R_{\hat{n}}(\alpha)$$

# H + S + T + CNOT are universal

$$HR_{\hat{n}}(\alpha)H = R_{\hat{m}}(\alpha)$$

$$U = R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\delta)$$

$$n_xHXH + n_yHYH + n_zHZH$$

$$= n_zX - n_yY + n_zZ$$

$$\int_{-\sin(\pi/8)} \cos(\pi/8)$$

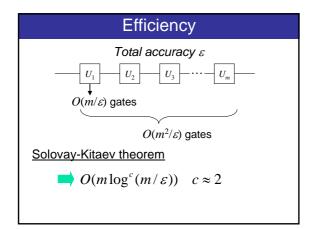
$$\cos(\pi/8)$$

$$U \approx R_{\hat{n}}^{n_1}(\theta) R_{\hat{m}}^{n_2}(\theta) R_{\hat{n}}^{n_3}(\theta)$$

 $\cos(\pi/8)$  $-\sin(\pi/8)$  $\sqrt{1+\cos^2(\pi/8)}$  $\cos(\pi/8)$ 

S has its own role in doing the approximation in a fault-tolerant fashion

Is this construction efficient?



# Discrete set of universal gates

- H, S, T, and CNOT
- H, S, CNOT, and Toffoli

