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

Outline

- Bloch sphere representation
- Rotation gates
- Universality proof
  - An arbitrary controlled-U gate can be implemented using only single qubit gates and CNOT
  - An arbitrary (controlled)^n-U gate can be implemented using single qubit gates and CNOT
  - Two-level unitary gates are universal
  - Single-qubit gates and CNOT are universal
  - Hadamard, S, T, and CNOT are universal

Bloch sphere representation

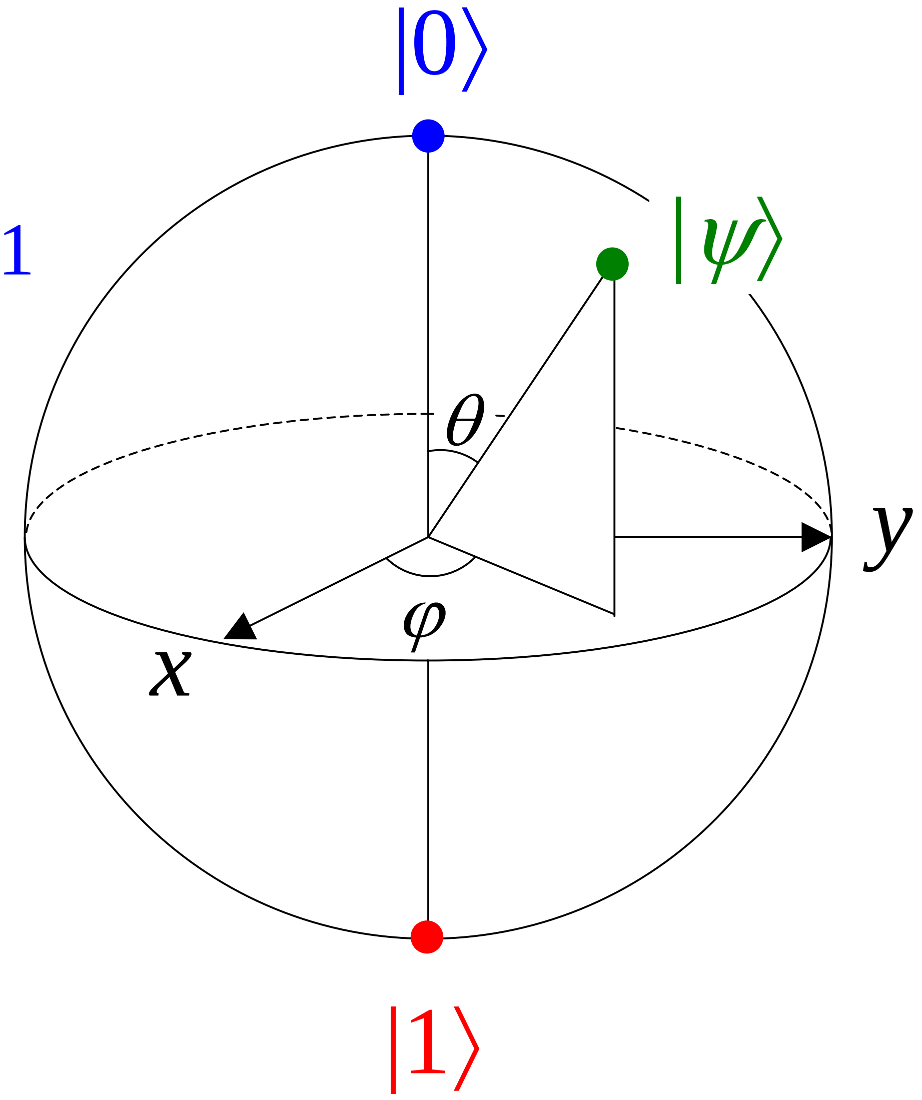
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$|\alpha|^2 + |\beta|^2 = 1$

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

No observable effect

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



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

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

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

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

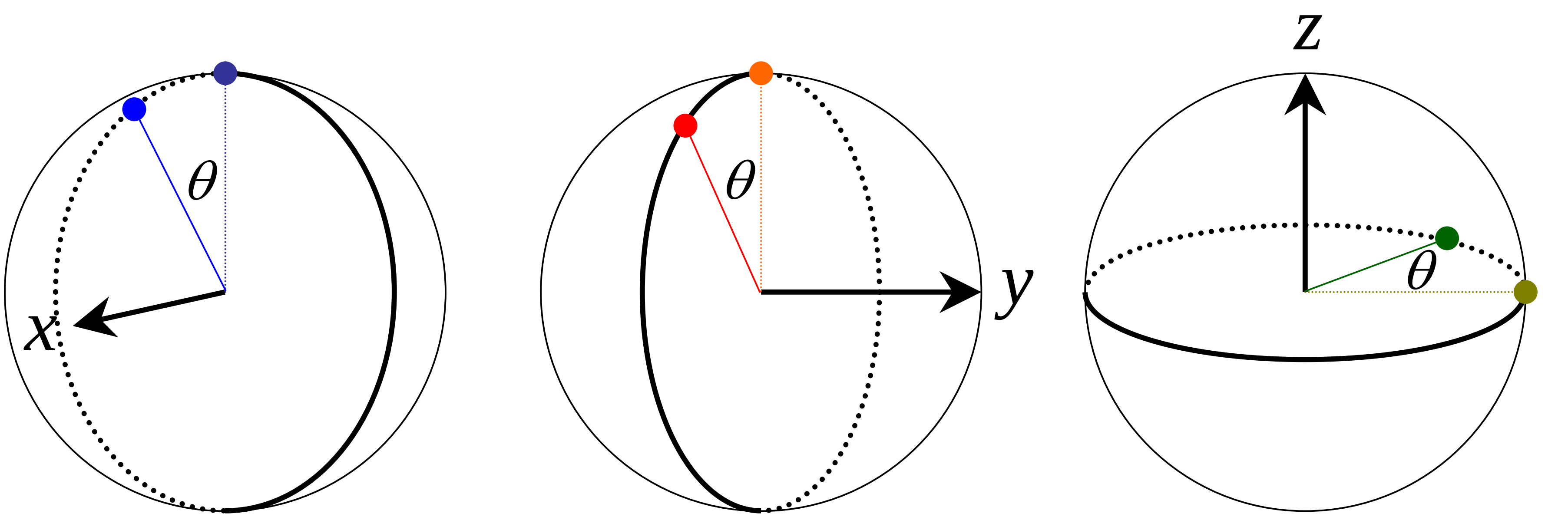
$$|\psi(t+\Delta t)\rangle = \exp\left[\frac{-iH\Delta t}{\hbar}\right]|\psi(t)\rangle$$

Rotation gates

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

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

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



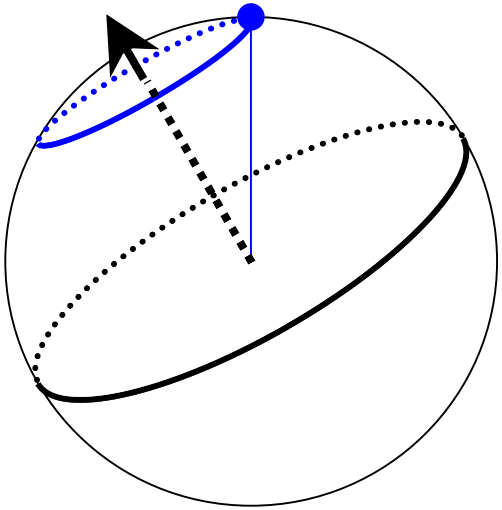
Rotation about the $\hat{n}$ axis

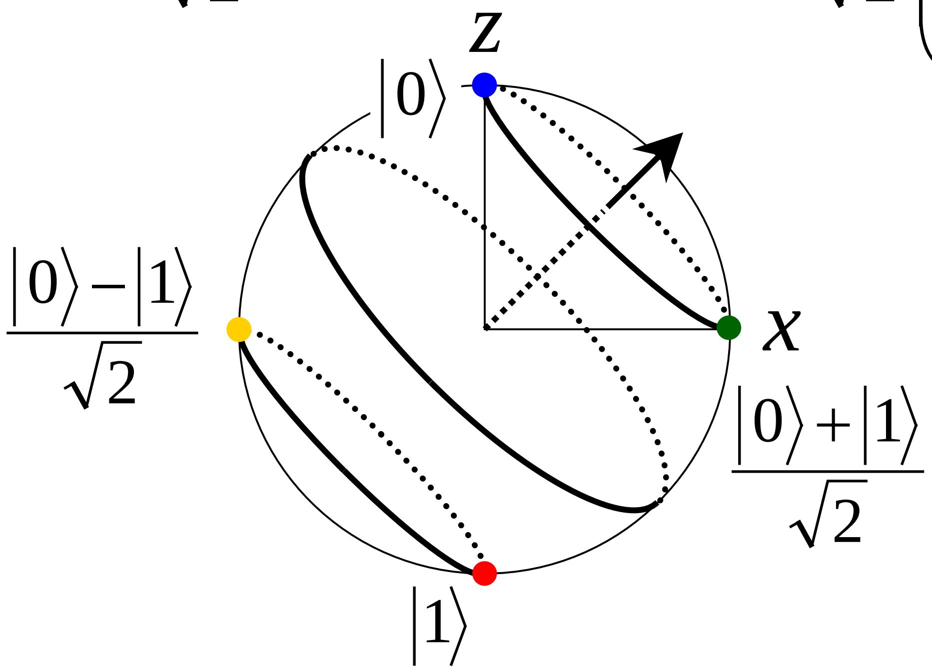
$$R_{\hat{n}}(\theta) \equiv \exp(-i\theta\, \hat{n}\cdot\hat{\sigma}/2) = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2}(n_x X + n_y Y + n_z Z)$$

$$\hat{n} = \begin{pmatrix} n_x \\ n_y \\ n_z \end{pmatrix} \qquad \hat{\sigma} = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

<ins>Example</ins>

$$H = \frac{X+Z}{\sqrt{2}} \quad \Rightarrow \quad \theta = \pi,\ \hat{n} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$





Road to universality proof

1. 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-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

Z-Y decomposition

For an arbitrary single qubit gate U, there exist real numbers α, β, γ, and δ such that

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

<u>Proof</u>

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

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

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

Corollary

Set A, B, C as

$$A \equiv R_z(\beta) R_y\left(\frac{\gamma}{2}\right)$$

$$B \equiv R_y\left(-\frac{\gamma}{2}\right) R_z\left(-\frac{\delta+\beta}{2}\right)$$

$$C \equiv R_z\left(\frac{\delta-\beta}{2}\right)$$

Then

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

We will construct an arbitrary controlled-U gate using A, B, and C

Corollary

Proof

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

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

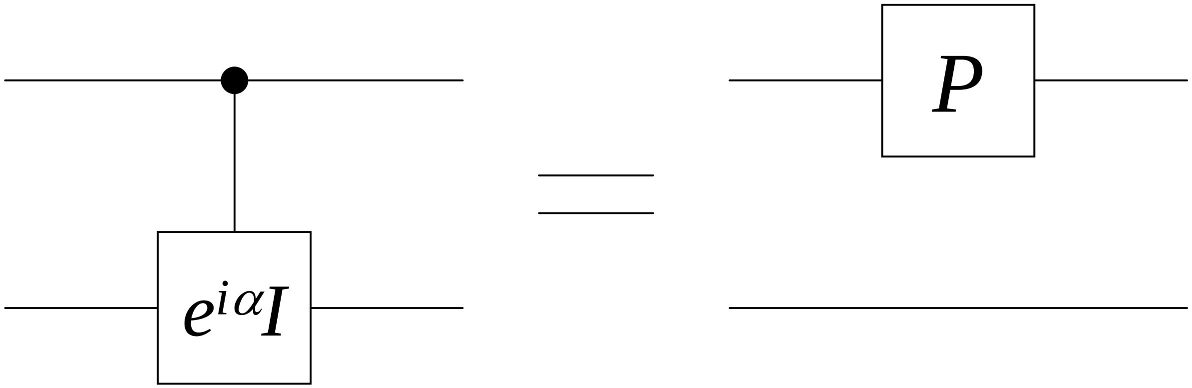
$$XX = I$$

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

$$XR_z(\theta)X = R_z(-\theta)$$

$$\begin{aligned}
e^{i\alpha}AXBXC &= e^{i\alpha}AXR_y\left(-\frac{\gamma}{2}\right)XXR_z\left(-\frac{\delta+\beta}{2}\right)XC \\
&= e^{i\alpha}AR_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right)C \\
&= e^{i\alpha}R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) \\
&= e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta) = U
\end{aligned}$$

Phase shifter



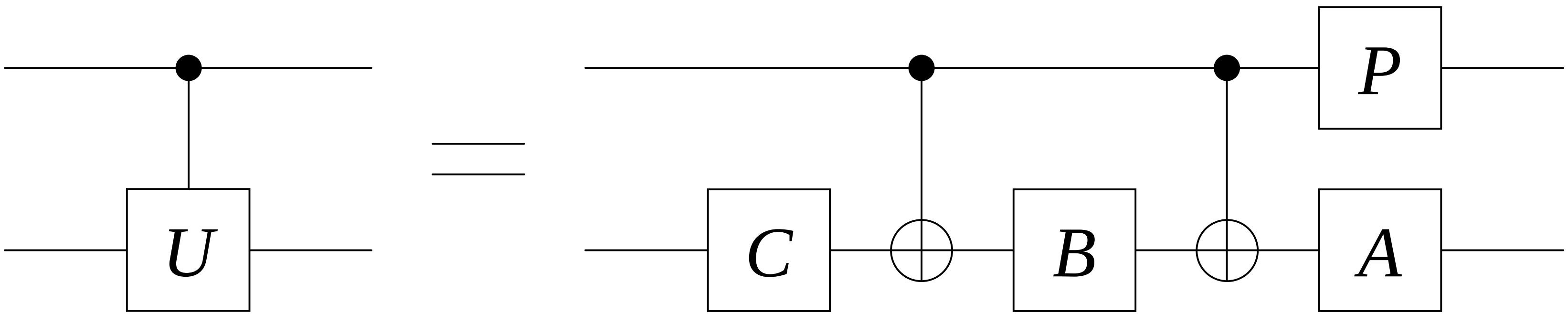
$$P = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix}$$

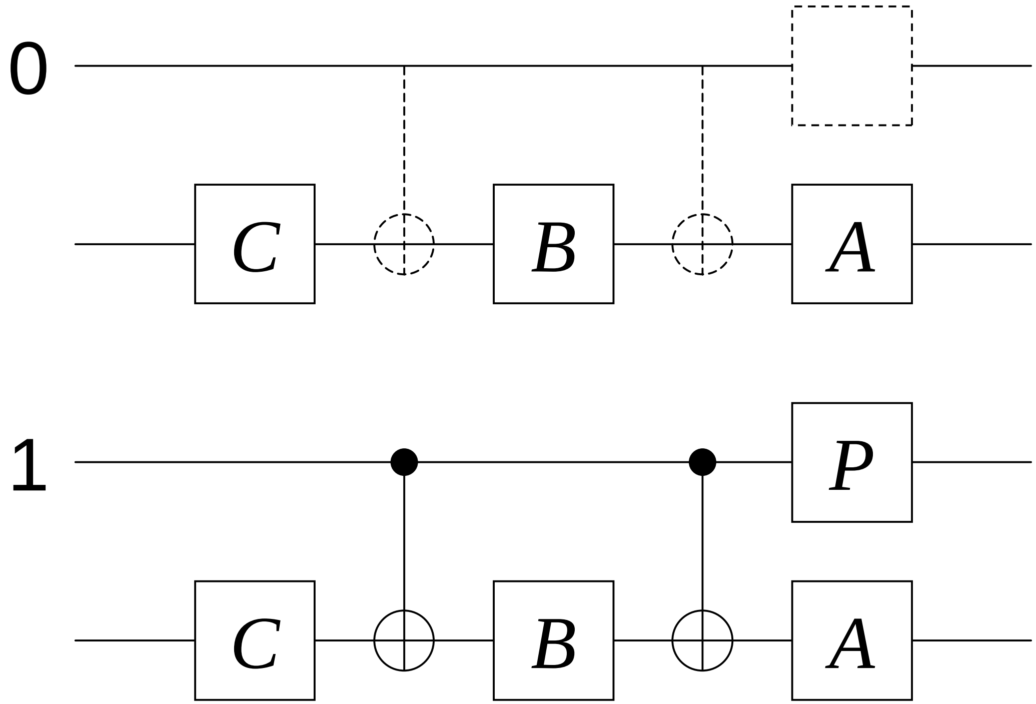
$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow e^{i\alpha}|10\rangle \\ |11\rangle &\rightarrow e^{i\alpha}|11\rangle \end{aligned}$$

$$\Leftrightarrow$$

$$P \otimes I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha} & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{bmatrix}$$

Controlled-U gate





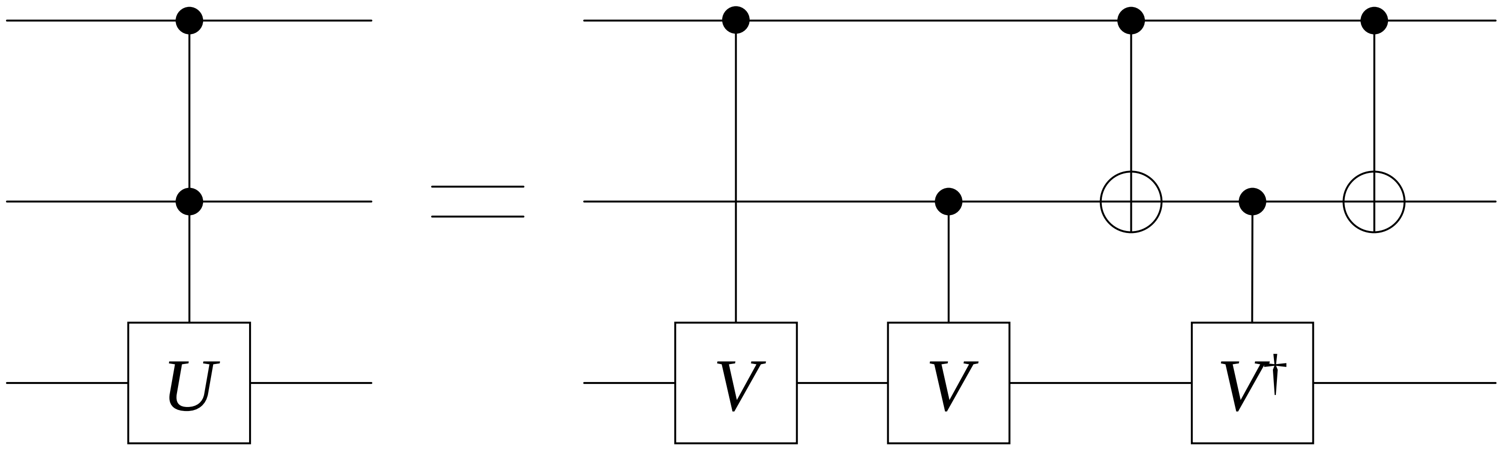
$$ABC = I$$

$$e^{i\alpha} AXBXC = U$$

Road to universality proof

1. 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

(Controlled)^2-U gate



$$V^2 = U$$

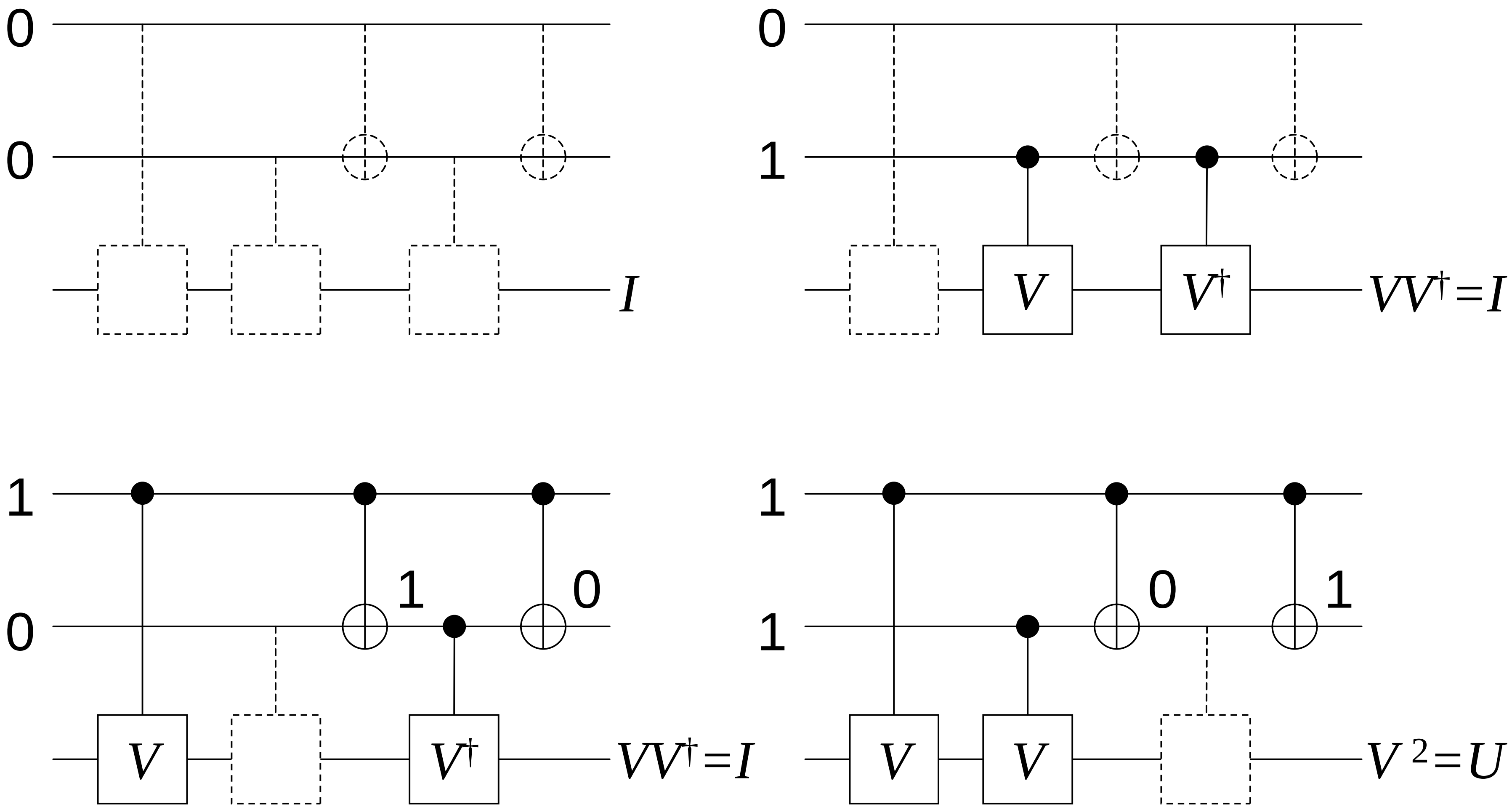
$$VV^\dagger = I$$

Example

$$T^2 = S \qquad (HSH)^2 = X$$

$$S^2 = Z \qquad \left(\frac{I + iH}{\sqrt{2}}\right)^2 = iH$$

(Controlled)^2-U gate



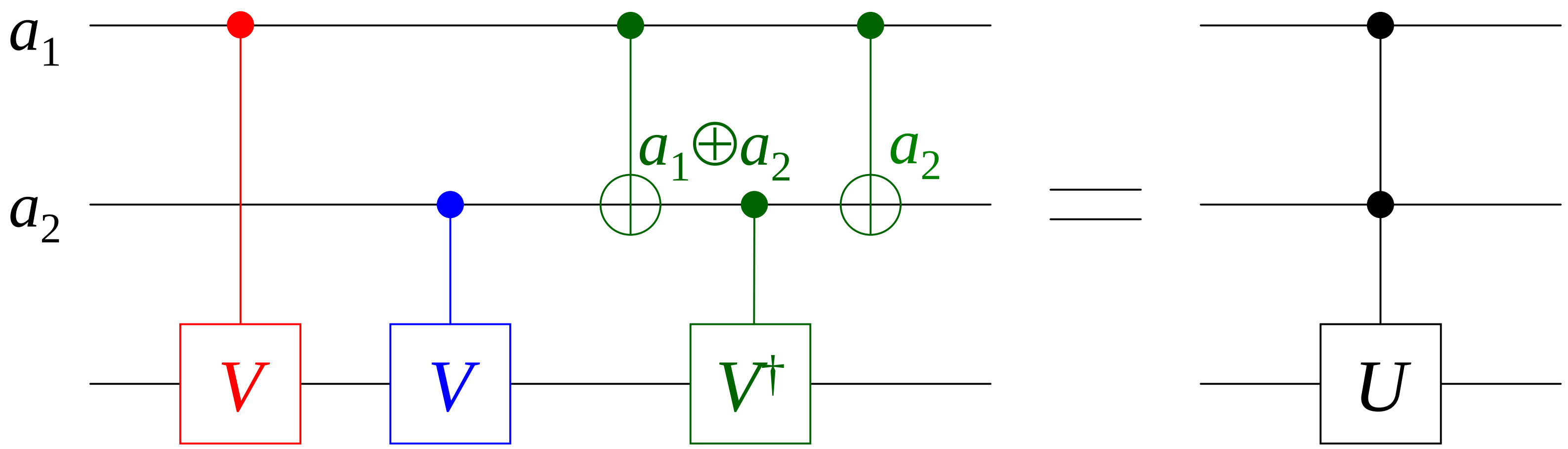
(Controlled)^2-U gate

$$a_1 + a_2 - (a_1 \oplus a_2) = 2 \times a_1 \cdot a_2$$

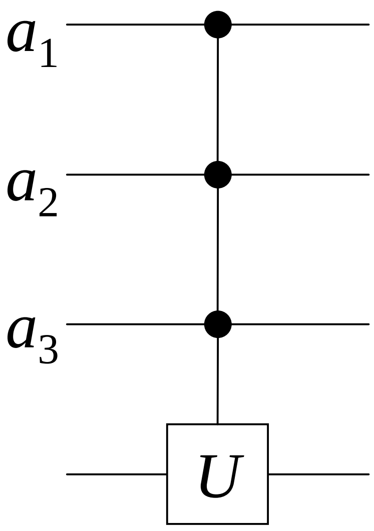
+, –, and × are the ordinary arithmetic operations

a_1	a_2	$a_1 \oplus a_2$	$2a_1 \cdot a_2$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	2

$$V^{a_1} V^{a_2} (V^\dagger)^{a_1 \oplus a_2} = (V^2)^{a_1 \cdot a_2} = U^{a_1 \cdot a_2}$$

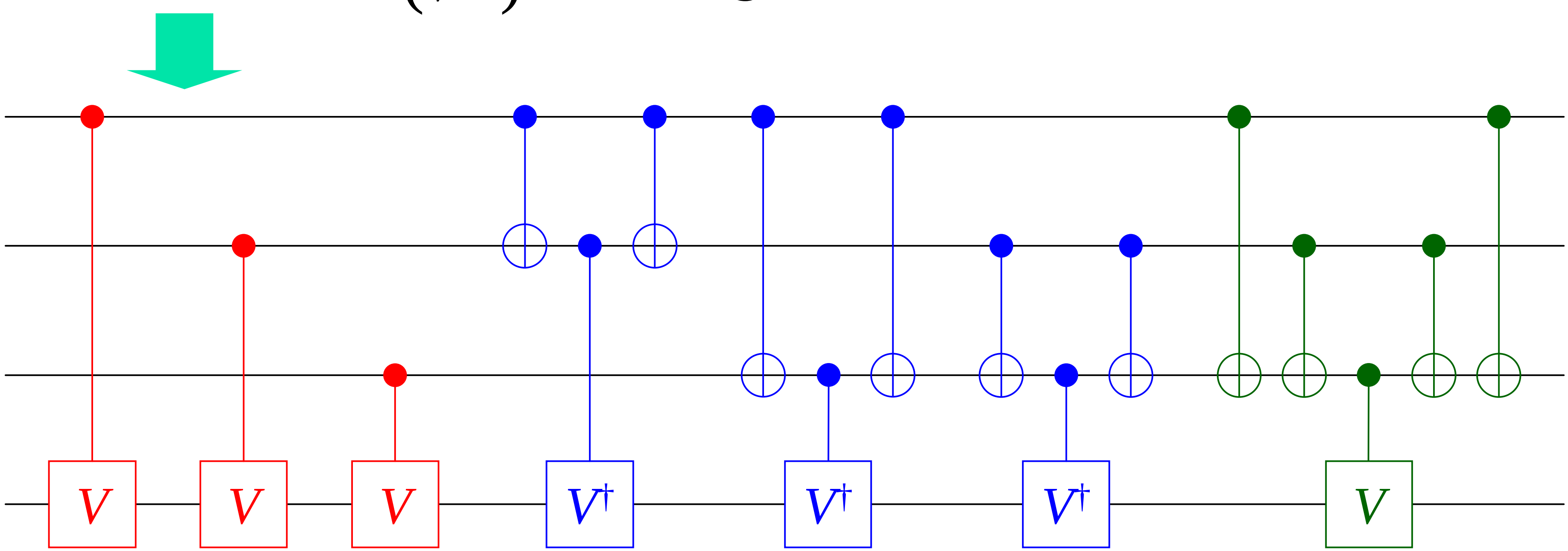


(Controlled)^3-U gate



$$a_1 + a_2 + a_3 - (a_1 \oplus a_2) - (a_1 \oplus a_3) - (a_2 \oplus a_3) + (a_1 \oplus a_2 \oplus a_3)$$
$$= 4 \times a_1 \cdot a_2 \cdot a_3$$

$$V^{a_1} V^{a_2} V^{a_3} (V^{\dagger})^{a_1 \oplus a_2} (V^{\dagger})^{a_1 \oplus a_3} (V^{\dagger})^{a_2 \oplus a_3} V^{a_1 \oplus a_2 \oplus a_3}$$
$$= (V^4)^{a_1 \cdot a_2 \cdot a_3} = U^{a_1 \cdot a_2 \cdot a_3}$$

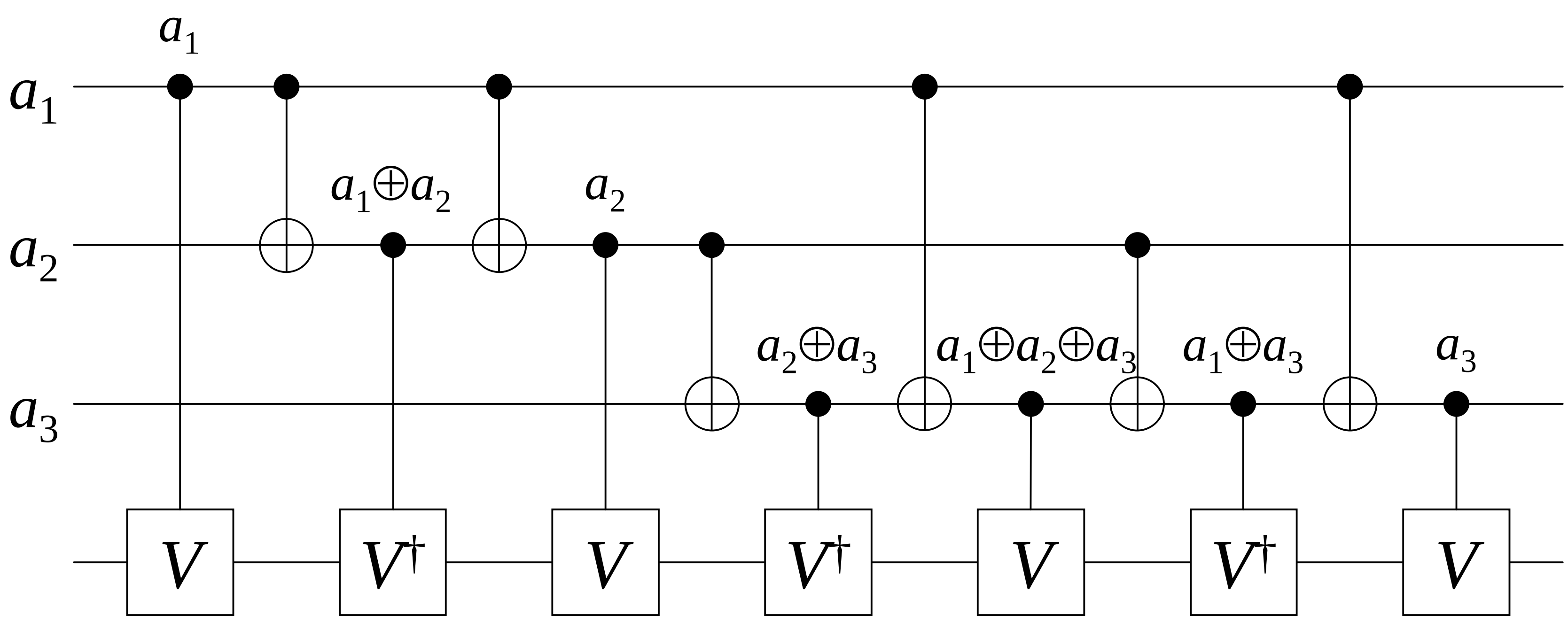


Gate construction by a Gray code

a_1	1	1	0	0	1	1	0
a_2	0	1	1	1	1	0	0
a_3	0	0	0	1	1	1	1

Gray code; Only one bit changes from one entry to the next (patented by F. Gray)

$$V^{a_1}(V^\dagger)^{a_1\oplus a_2}V^{a_2}(V^\dagger)^{a_2\oplus a_3}V^{a_1\oplus a_2\oplus a_3}(V^\dagger)^{a_1\oplus a_3}V^{a_3}$$



(Controlled)^n-U gate

Set V so that $V^{2^{n-2}} = U$ and implement the identity

$$\sum_i a_i - \sum_{i<j} (a_i \oplus a_j) + \sum_{i<j<k} (a_i \oplus a_j \oplus a_k) - \cdots + (-1)^{n-1} (a_1 \oplus a_2 \oplus \cdots \oplus a_n)$$

$$= 2^{n-1} \times a_1 \cdot a_2 \cdot a_3 \cdots a_n$$

<u>Proof for $n = 3$</u>

Can be proved for any n by induction

$$4 \times a_1 \cdot a_2 \cdot a_3$$

$$= 2(2a_1 \cdot a_2) \cdot a_3$$

$$2a_1 \cdot a_2 = a_1 + a_2 - (a_1 \oplus a_2)$$

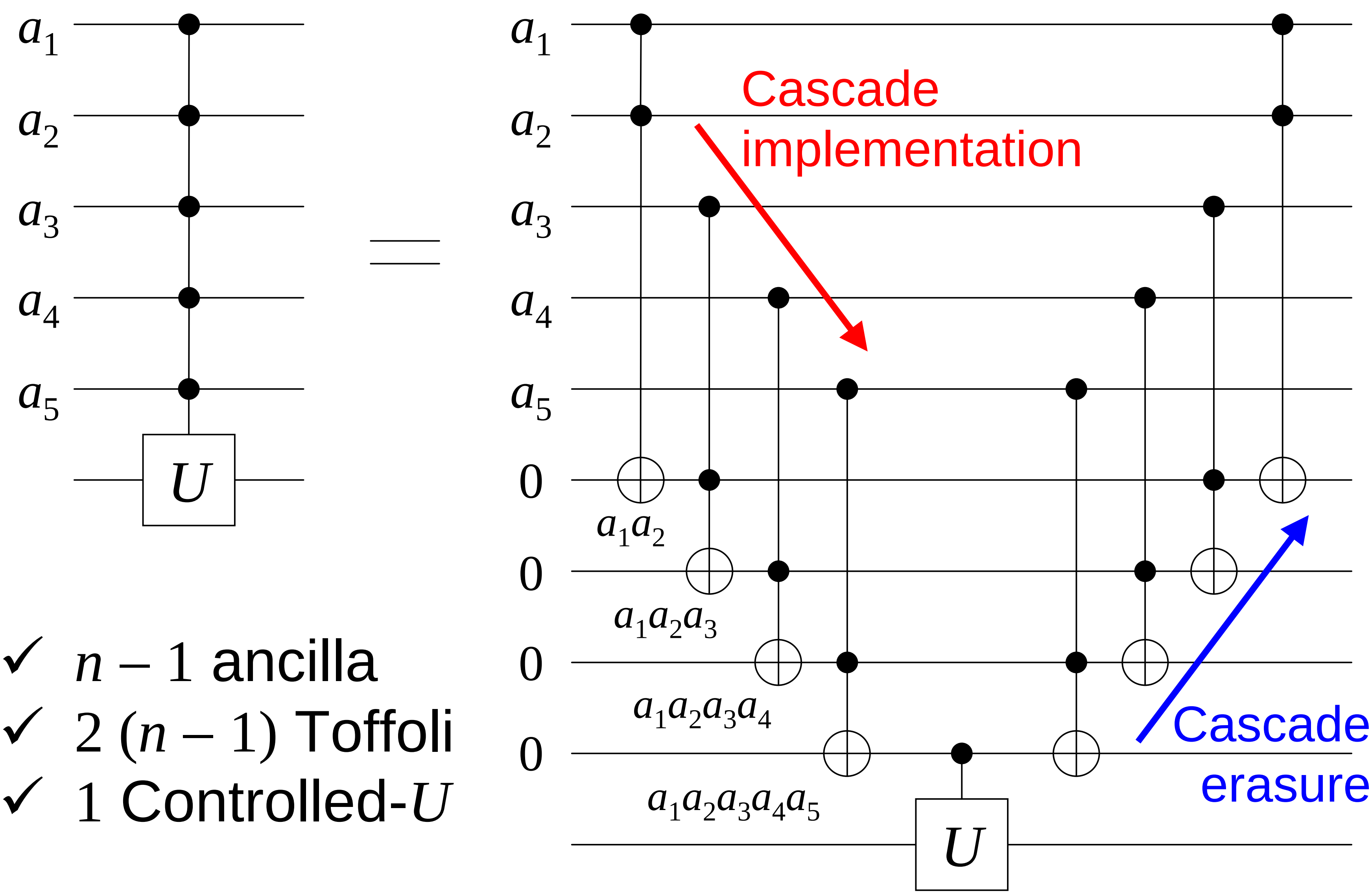
$$= 2[a_1 + a_2 - (a_1 \oplus a_2)] \cdot a_3$$

$$= 2a_1 \cdot a_3 + 2a_2 \cdot a_3 - 2(a_1 \oplus a_2) \cdot a_3$$

$$= [a_1 + a_3 - (a_1 \oplus a_3)] + [a_2 + a_3 - (a_2 \oplus a_3)] - [(a_1 \oplus a_2) + a_3 - (a_1 \oplus a_2 \oplus a_3)]$$

$$= a_1 + a_2 + a_3 - (a_1 \oplus a_2) - (a_1 \oplus a_3) - (a_2 \oplus a_3) + (a_1 \oplus a_2 \oplus a_3)$$

(Controlled)^n-U gate



- ✓ $n - 1$ ancilla
- ✓ $2\,(n - 1)$ Toffoli
- ✓ 1 Controlled-U

Road to universality proof

1. 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

Two-level unitary gate

Two-level unitary matrix

Unitary matrix which acts nontrivially only two-or-fewer vector components

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \alpha & \gamma \\ 0 & 0 & \beta & \delta \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \alpha & \gamma & 0 \\ 0 & \beta & \delta & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Universality; 3×3 case

Breaking U up into the product of two-level unitary matrices

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

$$U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix} \Rightarrow U_3 U_2 U_1 U = I \quad \Leftrightarrow \quad U = U_1^\dagger U_2^\dagger U_3^\dagger$$

Two-level unitary gates are universal

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

$$\Downarrow$$

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

$$\Downarrow$$

$$U_2 U_1 U = \begin{bmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix}$$

$$U_1 \equiv \begin{cases} I & (b = 0) \\ \begin{bmatrix} \dfrac{a^*}{\sqrt{|a|^2+|b|^2}} & \dfrac{b^*}{\sqrt{|a|^2+|b|^2}} & 0 \\ \dfrac{b}{\sqrt{|a|^2+|b|^2}} & \dfrac{-a}{\sqrt{|a|^2+|b|^2}} & 0 \\ 0 & 0 & 1 \end{bmatrix} & (b \neq 0) \end{cases}$$

$$U_2 \equiv \begin{cases} \begin{bmatrix} a'^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} & (c' = 0) \\ \begin{bmatrix} \dfrac{a'^*}{\sqrt{|a'|^2+|c'|^2}} & 0 & \dfrac{c'^*}{\sqrt{|a'|^2+|c'|^2}} \\ 0 & 1 & 0 \\ \dfrac{c'}{\sqrt{|a'|^2+|c'|^2}} & 0 & \dfrac{-a'}{\sqrt{|a'|^2+|c'|^2}} \end{bmatrix} & (c' \neq 0) \end{cases}$$

Two-level unitary gates are universal

$$U_2U_1U = \begin{bmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix}$$

$$U_3 \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & j''^* \end{bmatrix}$$

$$\Downarrow$$

$$U_3U_2U_1U = I \quad \Leftrightarrow \quad U = U_1^\dagger U_2^\dagger U_3^\dagger$$

For d-dimensional U, we repeat this procedure

$$U = \begin{bmatrix} u_{11} & \cdots & u_{1d} \\ \vdots & \ddots & \vdots \\ u_{d1} & \cdots & u_{dd} \end{bmatrix} \Rightarrow U_{d-1}U_{d-2}\cdots U_1U = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & u'_{22} & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & u'_{dd} \end{bmatrix}$$

Two-level unitary gates are universal

$$U_{d-1}U_{d-2}\cdots U_1 U = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & u'_{22} & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & & u'_{dd} \end{bmatrix}$$

$$\underbrace{U_{2d-3}\cdots U_d}_{d-2}(\underbrace{U_{d-1}U_{d-2}\cdots U_1}_{d-1}U) = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & u''_{33} & \cdots & \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & & \cdots & u''_{dd} \end{bmatrix}$$

$$\underbrace{U_k\cdots U_1}_{k \le (d-1)+(d-2)+\cdots+1 = \frac{d(d-1)}{2}} U = I \quad \Leftrightarrow \quad U = U_1^\dagger \cdots U_k^\dagger$$

Road to universality proof

1. 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

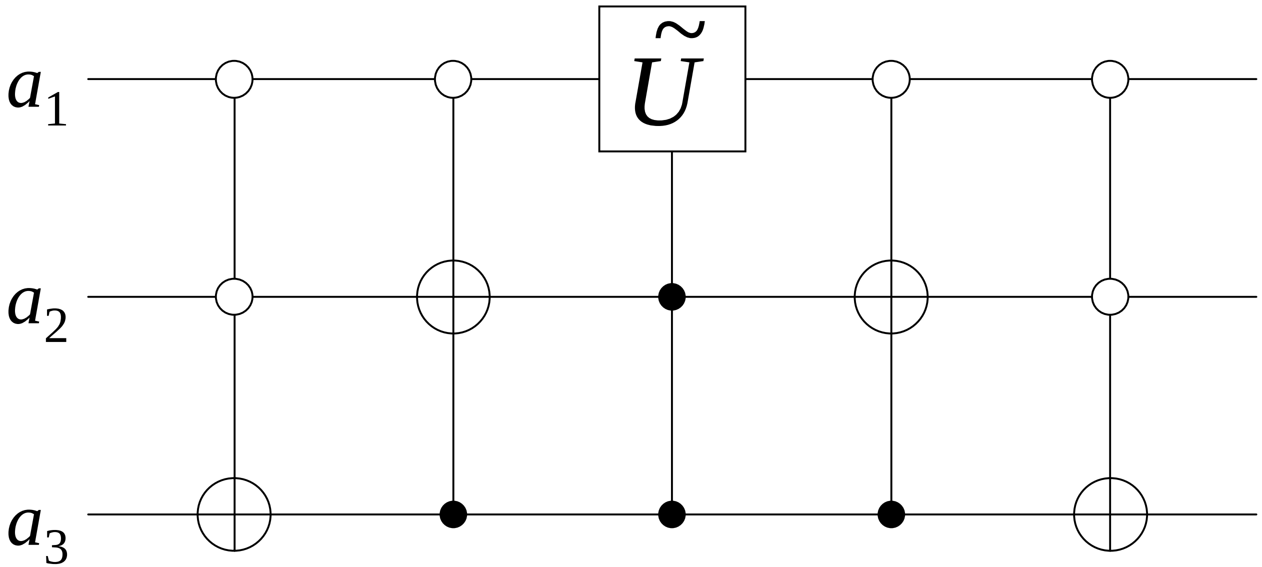
To show that single qubit & CNOT gates can implement an arbitrary two-level unitary matrix

Example

8×8 U acting nontrivially only on $|000\rangle$ and $|111\rangle$

$$U = \begin{bmatrix} \alpha & 0 & 0 & 0 & 0 & 0 & 0 & \gamma \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ \beta & 0 & 0 & 0 & 0 & 0 & 0 & \delta \end{bmatrix} \Rightarrow U \begin{bmatrix} a \\ b \\ c \\ d \\ e \\ f \\ g \\ h \end{bmatrix} = \begin{bmatrix} \alpha a + \gamma h \\ b \\ c \\ d \\ e \\ f \\ g \\ \beta a + \delta h \end{bmatrix}$$

Single qubit gates & CNOT are universal

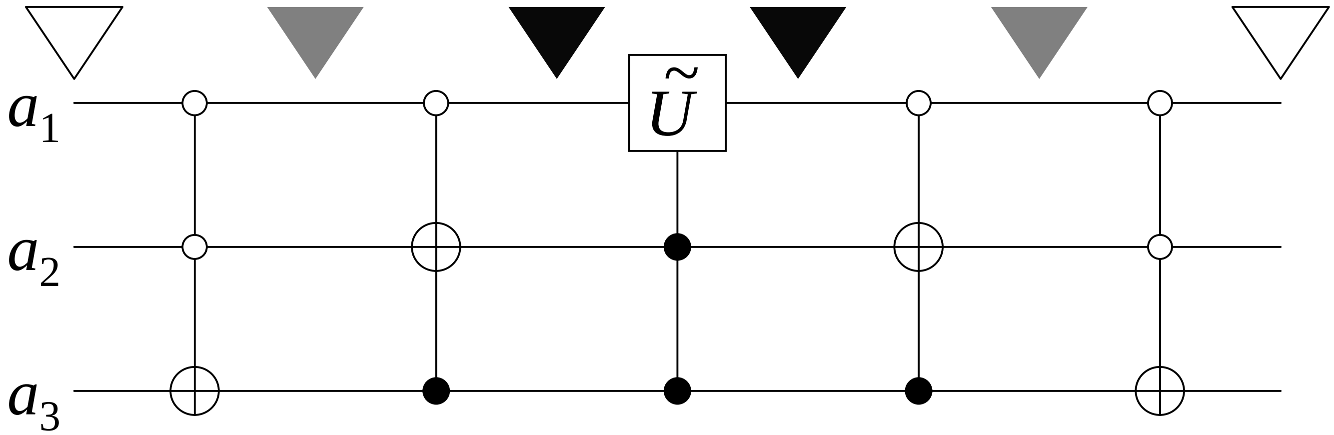


$$\tilde{U} = \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix}$$

a_1	0	0	0	1
a_2	0	0	1	1
a_3	0	1	1	1

We want to apply a controlled gate with the target bit $|a_1\rangle$

Single qubit gates & CNOT are universal



$$\tilde{U} = \begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix}$$

$a_1a_2a_3$						
000	a	b	b	b	b	$\alpha a + \gamma h$
001	b	a	d	d	$\alpha a + \gamma h$	b
010	c	c	c	c	c	c
011	d	d	a	$\alpha a + \gamma h$	d	d
100	e	e	e	e	e	e
101	f	f	f	f	f	f
110	g	g	g	g	g	g
111	h	h	h	$\beta a + \delta h$	$\beta a + \delta h$	$\beta a + \delta h$

Road to universality proof

1. 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

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

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

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

$$HZH = X \Rightarrow HR_z(\theta)H = R_x(\theta)$$

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

θ; irrational multiple of 2π

$$\cos(\theta/2) \equiv \cos^2(\pi/8)$$

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

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

Approximation by H & T

$$R_z\left(\frac{\pi}{4}\right)R_x\left(\frac{\pi}{4}\right)=\exp\left(-i\frac{\pi}{8}Z\right)\exp\left(-i\frac{\pi}{8}X\right)$$

$$\boxed{-iZX=Y}$$

$$=\left[\cos\frac{\pi}{8}I-i\sin\frac{\pi}{8}Z\right]\left[\cos\frac{\pi}{8}I-i\sin\frac{\pi}{8}X\right]$$

$$=\cos^2\frac{\pi}{8}I-i\sin\frac{\pi}{8}\left[\cos\frac{\pi}{8}X+\sin\frac{\pi}{8}Y+\cos\frac{\pi}{8}Z\right]$$

$$=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}\left[n_xX+n_yY+n_zZ\right]=R_{\hat{n}}(\theta)$$

$$\cos(\theta/2)\equiv\cos^2(\pi/8)$$

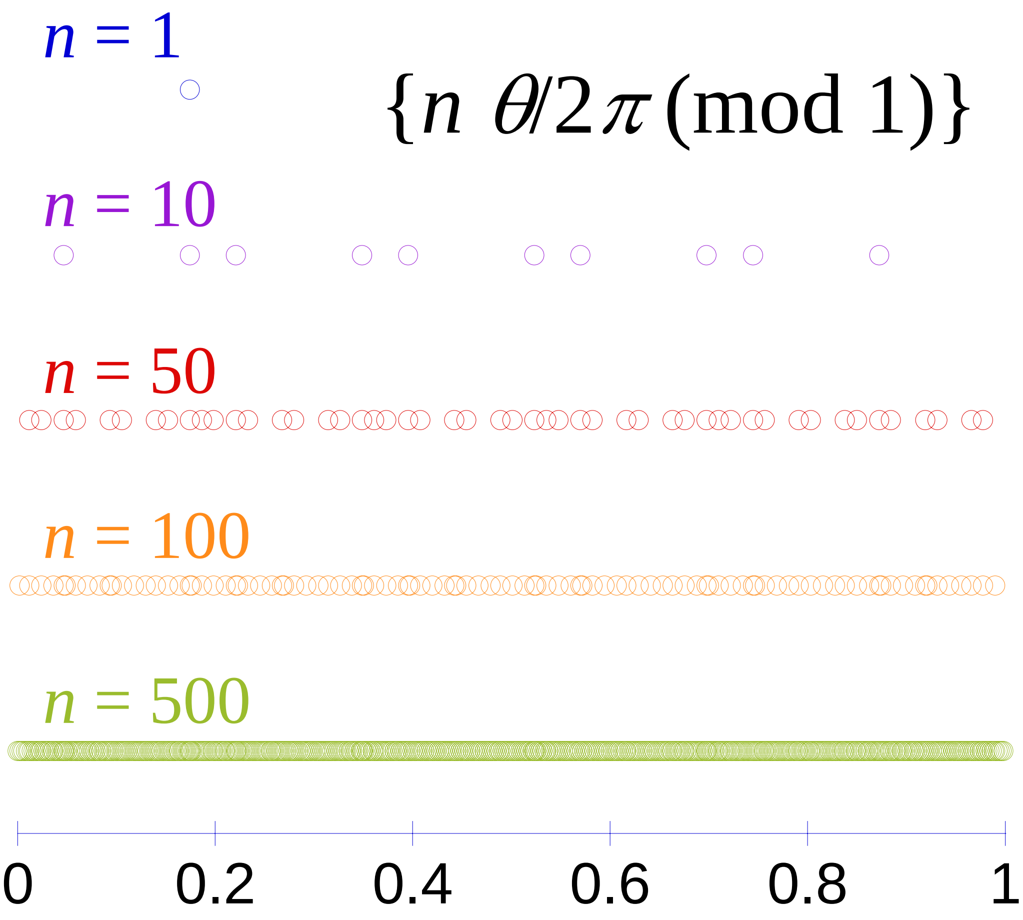
$$\sin(\theta/2)=\sqrt{1-\cos^4(\pi/8)}=\sin(\pi/8)\sqrt{1+\cos^2(\pi/8)}$$

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

Approximation by H & T

Weyl's theorem on uniform distribution

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



$$\{n\,\theta/2\pi\,(\mathrm{mod}\ 1)\}$$

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

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

$H + S + T$ + CNOT are universal

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

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

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

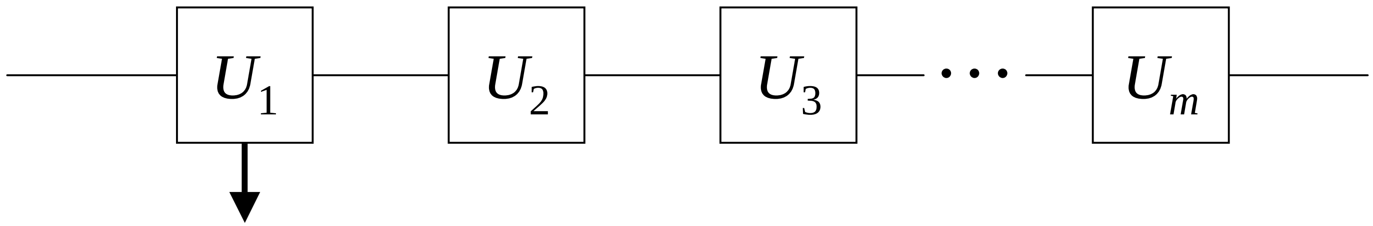
$$n_x HXH + n_y HYH + n_z HZH$$
$$= n_z X - n_y Y + n_z Z$$
$$\hat{m} \equiv \frac{1}{\sqrt{1+\cos^2(\pi/8)}} \begin{bmatrix} \cos(\pi/8) \\ -\sin(\pi/8) \\ \cos(\pi/8) \end{bmatrix}$$

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

Is this construction efficient?

Efficiency

Total accuracy ε



$O(m/\varepsilon)$ gates

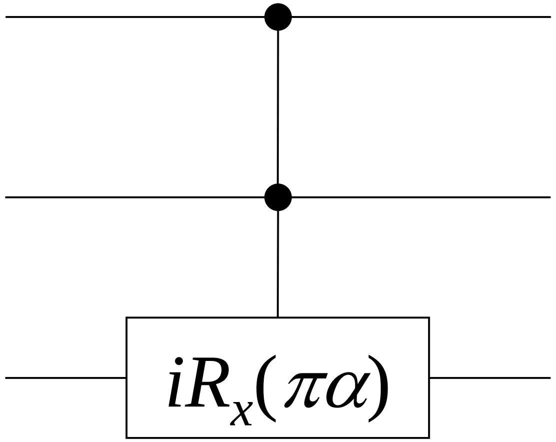
$O(m^2/\varepsilon)$ gates

<u>Solovay-Kitaev theorem</u>

$$\Rightarrow \quad O(m \log^c (m/\varepsilon)) \qquad c \approx 2$$

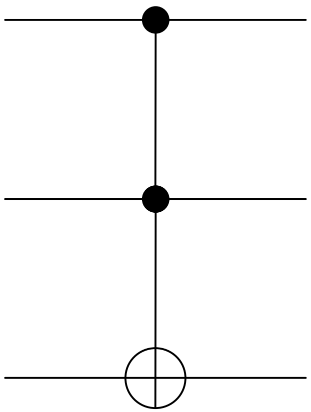
Discrete set of universal gates

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

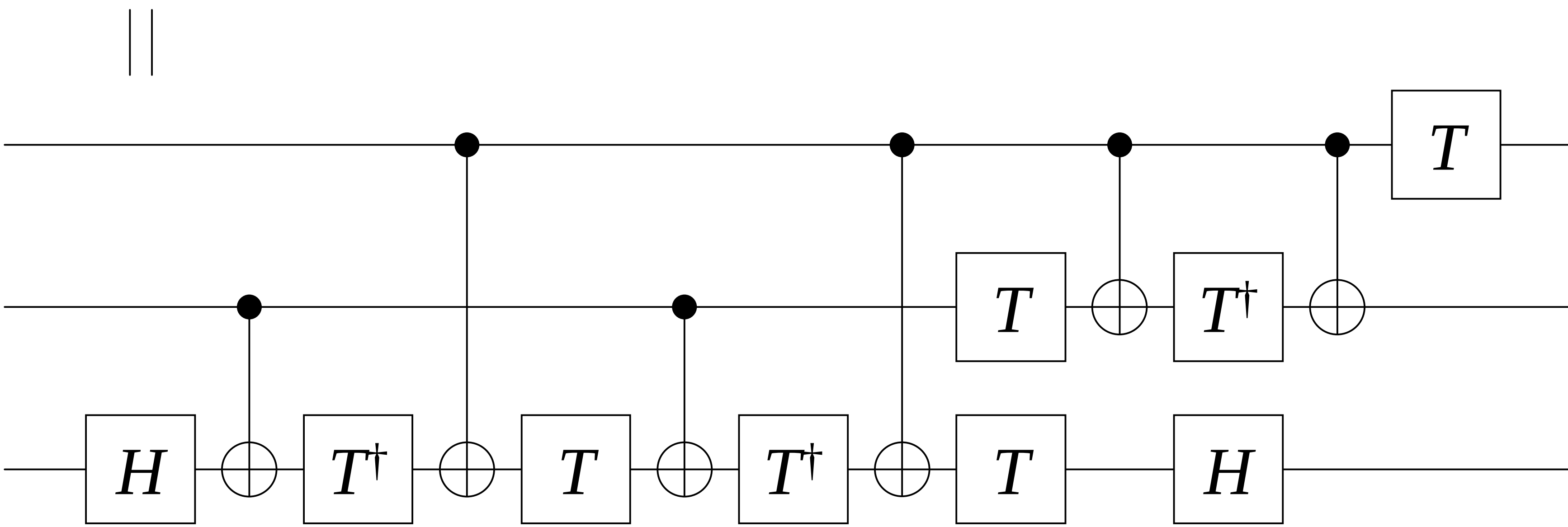


α ; irrational

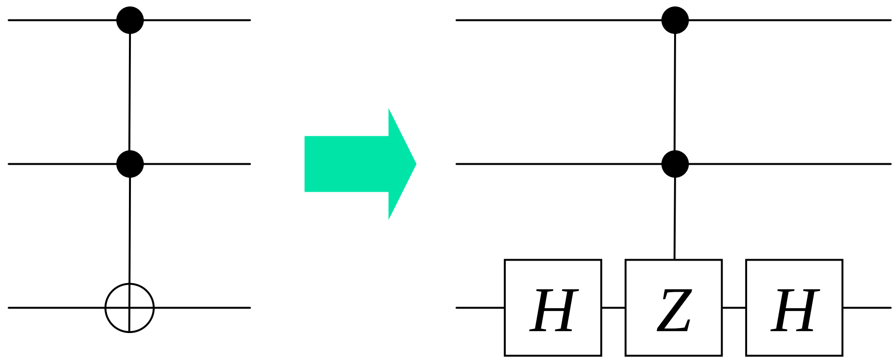
Quiz

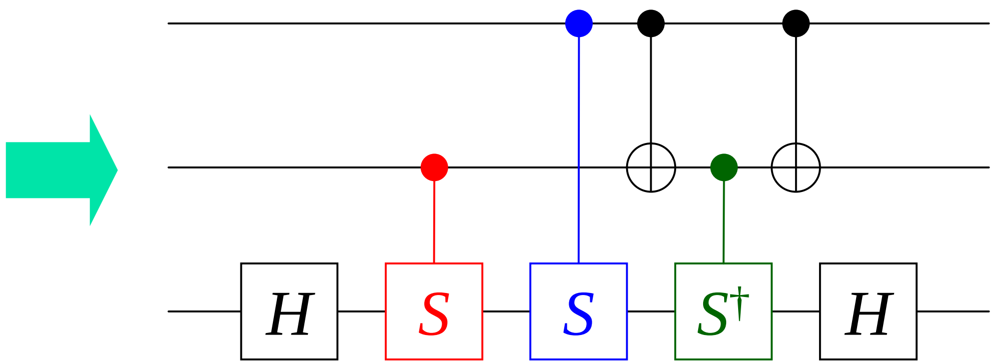


Construct Toffoli using only H, T, and CNOT



Answer

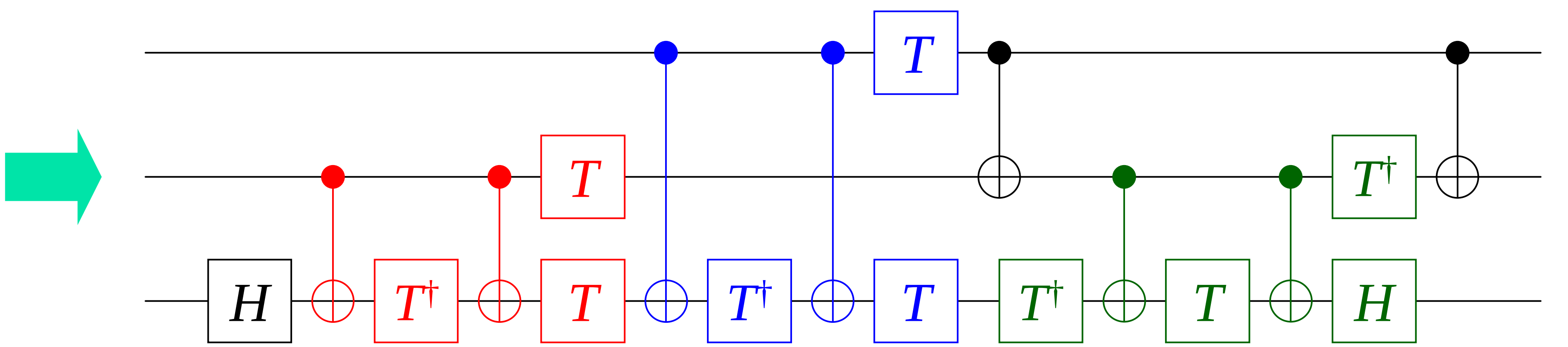




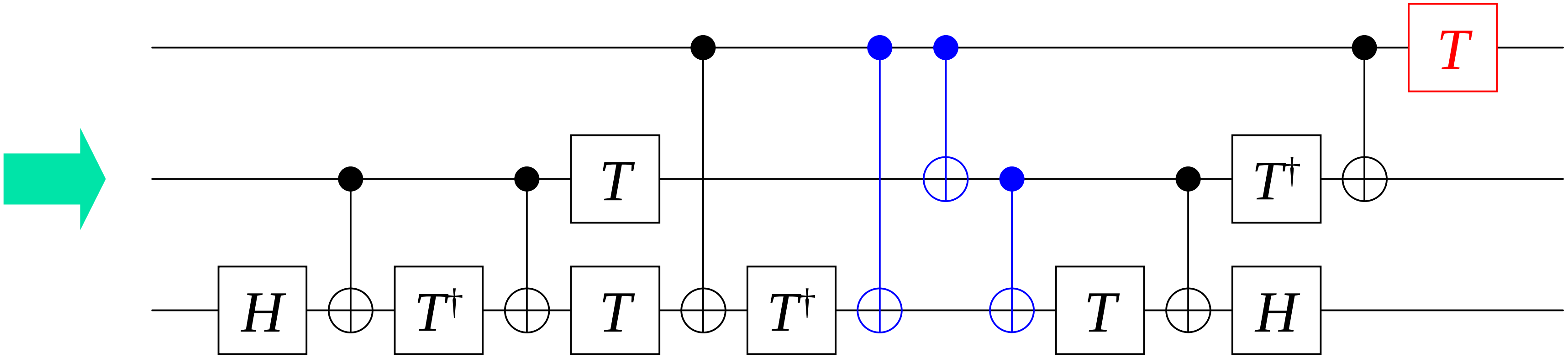
$$S^2 = Z$$

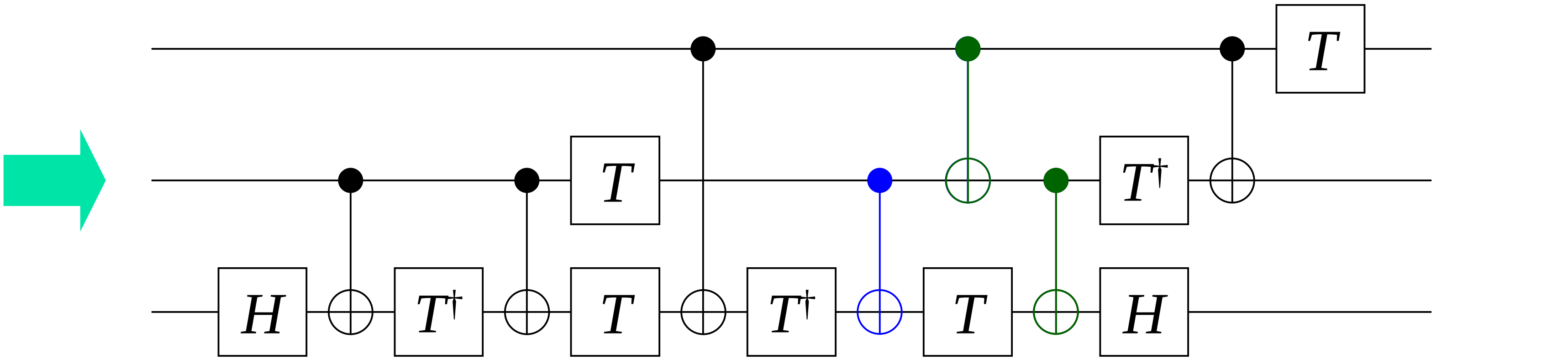
$$S = e^{i\pi/4} T X T^\dagger X$$

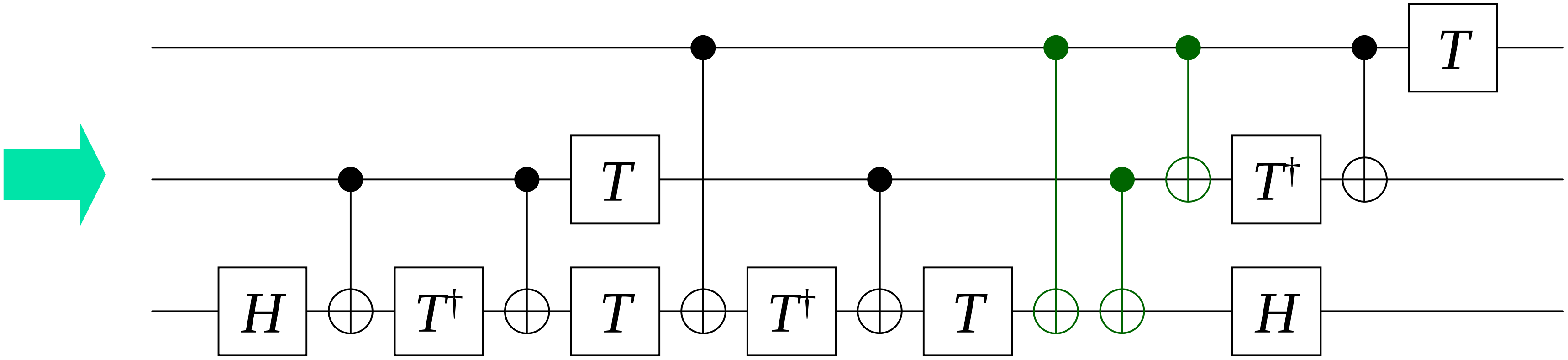
$$S^\dagger = e^{-i\pi/4} X T X T^\dagger$$



Answer







Answer