Yale University

Quantum Compiling

PART B

CPSC 4470/5470

Introduction to Quantum Computing

Instructor: Prof. **Yongshan Ding**

Computer Science, Applied Physics, Yale Quantum Institute

Outline

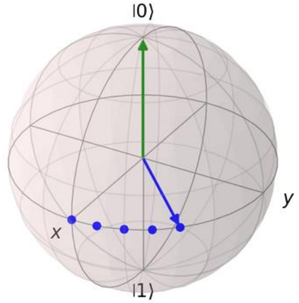
1. **Single-Qubit Unitary**: H, T gates are universal. Visual evidence.

2. **Multi-Qubit Unitary**: $H, T, CNOT$ gates are universal. Simple linear-algebraic proof.

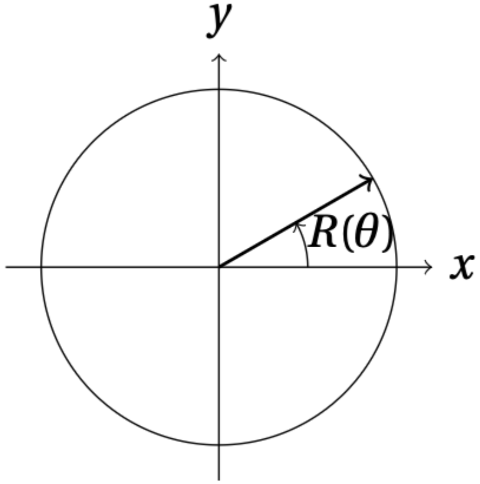
Single-Qubit Unitary Gates

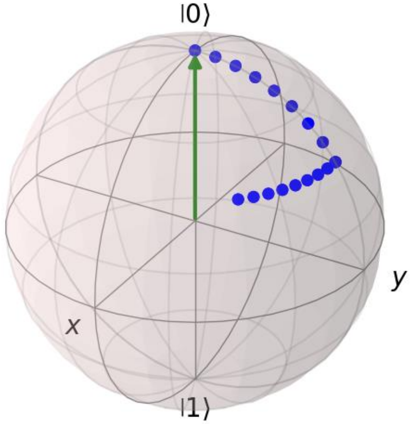
$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \qquad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{bmatrix}$$

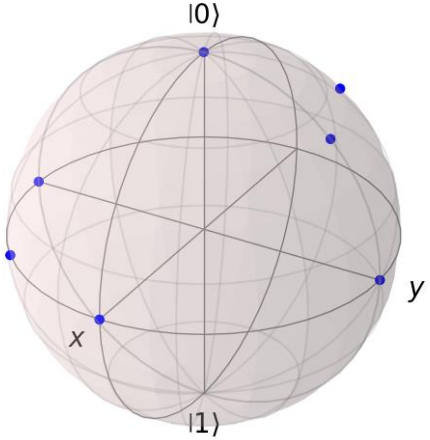
$T = R_Z(\pi/4)$



2D Rotation	**3D Rotation**	**Discrete Gates**
$R(\theta)$	$R_Z(\beta)\ R_x(\alpha)$	After H,S,H,T,H,T gates.







Universal: $R(\theta)$ by irrational angle; $H, R_Z(\theta)$; H, T

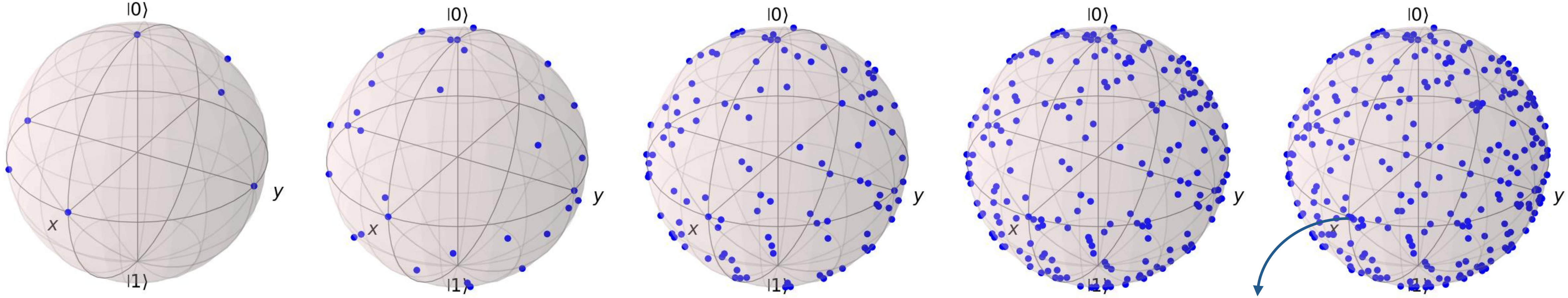
H, T gates are universal!

Single-Qubit Unitary

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

Synthesizing arbitrary z rotations using H, S, and T:

- Solovay-Kitaev: $\#T = O(\log^c(1/\epsilon)), c \approx 3$
- Ross-Selinger: $\#T = O(\log(1/\epsilon) + \log\log(1/\epsilon))$



After H,S,H,T,H,T gates.

$R_z(\pi/128)|+\rangle$
(up to $\epsilon = 10^{-10}$)

Gate sequence: H,S,H,T,H,T, (states in Fig (a)) H,T,H,T,H,T,H,T,H,T,S,H,T,H,T,H,T,H,T,S,H,T,H,T,H, (states in Fig (b))
T,H,T,H,T,S,H,T,S,H,T,H,T,H,T,H,T,H,T,S,H,T,H,T,H,T,S,H,T,S,H,T,H,T,S,H,T,S,H,T,S,H,T,H,T,H,T,H,T,S,H,T,H,T,H,T,H,T,H,T,S,H,T,S,H,T,H,T,S,H,T,H,T,S,H,T,S,H, (states in Fig (c))
T,S,H,T,S,H,T,H,T,S,H,T,S,H,T,S,H,T,S,H,T,H,T,H,T,S,H,T,S,H,T,S,H,T,H,T,H,T,H,T,S,H,T,H,T,S,H,T,H,T,H,T,S,H,T,H,T,H,T,H,T,S,H,T,H,T,S,H,T,H,T,S,H,T,S,H,T,S,H,T,H,T, (states in Fig (d))
H,T,H,T,H,T,H,T,H,T,S,H,T,H,T,S,H,T,H,T,H,T,S,H,T,S,H,T,H,T,H,T,S,H,T,S,H,T,S,H,T,H,T,S,H,T,H,T,H,T,H,T,S,H,T,S,H,T,S,H,S,S,S (states in Fig (e))

Hadamard Gate

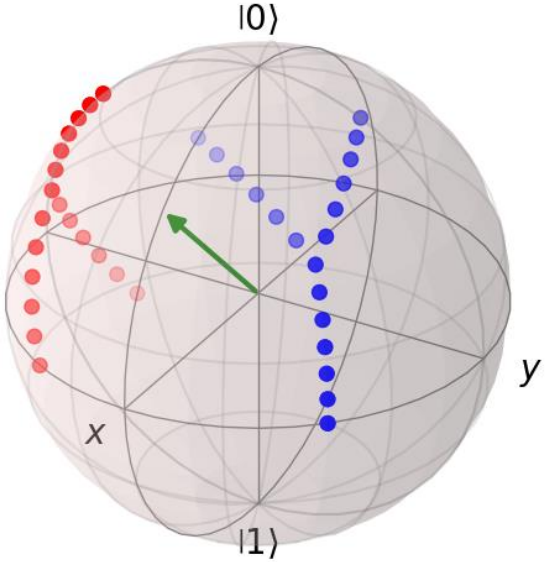
Example: $H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = \frac{X+Z}{\sqrt{2}}$

Reflection about $|h\rangle = \cos\pi/8\,|0\rangle + \sin\pi/8\,|1\rangle$

$$2|h\rangle\langle h| - I = H$$

Rotation about axis $|h\rangle$ by 180°: $R_{\hat{n}}(\pi)$, where $\hat{n} = \frac{\hat{x}+\hat{z}}{\sqrt{2}}$

$$R_{\hat{n}}(\pi) = e^{-\frac{i\pi}{2}\left(\frac{X+Z}{\sqrt{2}}\right)} = -iH$$ (Up to global phase.)

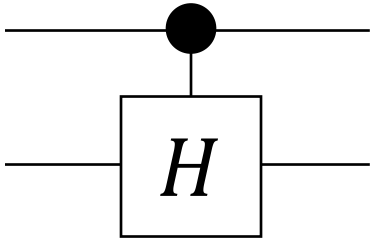


Yale

Two-Qubit Unitary: Controlled-H Gate

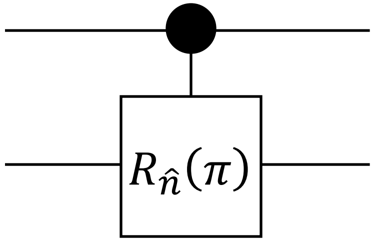
Recall: $R_{\hat{n}}(\pi) = -iH$ (same up to global phase)

What about c-H v.s. c-$R_{\hat{n}}(\pi)$ where $\hat{n} = \frac{\hat{x}+\hat{z}}{\sqrt{2}}$?



$$\text{c-H} = \begin{bmatrix} I & 0 \\ 0 & H \end{bmatrix}.$$

$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes H$

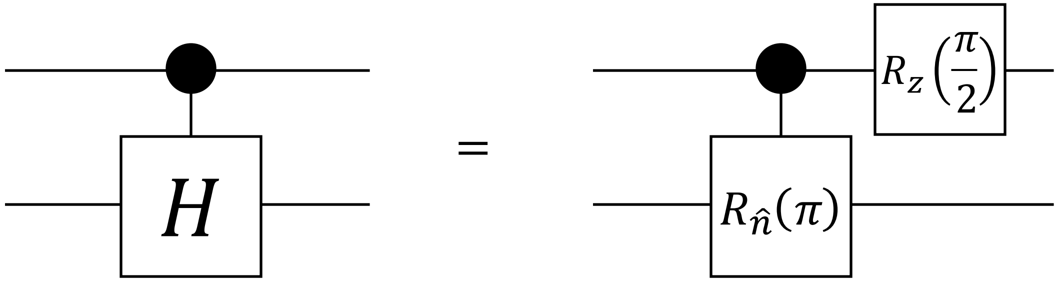


$$\text{c-}R_{\hat{n}}(\pi) = \begin{bmatrix} I & 0 \\ 0 & -iH \end{bmatrix}.$$

$|0\rangle\langle 0| \otimes I - i|1\rangle\langle 1| \otimes H$

Differ by a relative phase!

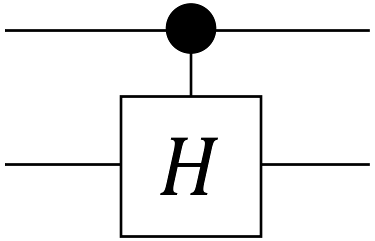
How to fix this? How to implement c-H using c-$R_{\hat{n}}(\pi)$?



$$\begin{bmatrix} I & 0 \\ 0 & H \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & iI \end{bmatrix} \cdot \begin{bmatrix} I & 0 \\ 0 & -iH \end{bmatrix}$$

Controlled-H Gate from Single-Qubit Gates and CNOT

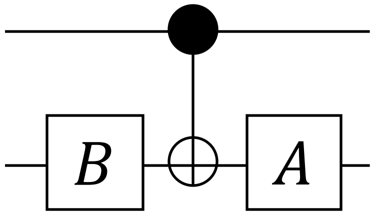
Example: controlled Hadamard (c-H) gate



$$\text{c-H} = \begin{bmatrix} I & 0 \\ 0 & H \end{bmatrix}.$$

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes H$$

Implement **c-H** with CX and single-qubit gates?



- If control==0:
  - AB is applied
- If control==1:
  - AXB is applied

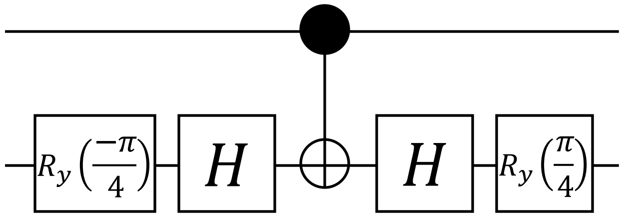
We want to find A, B such that:

- $AB = I$
- $AXB = H$

What are A and B?

$$H = R_y\left(\frac{\pi}{4}\right) Z R_y\left(-\frac{\pi}{4}\right)$$

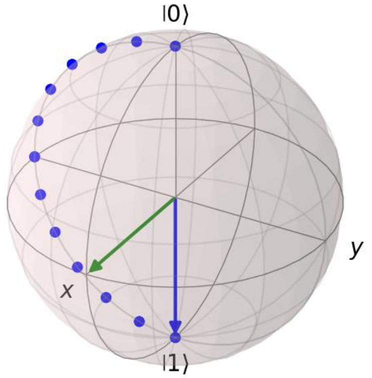
$$H = R_y\left(\frac{\pi}{4}\right) HXH R_y\left(-\frac{\pi}{4}\right)$$



Changing Rotation Axis

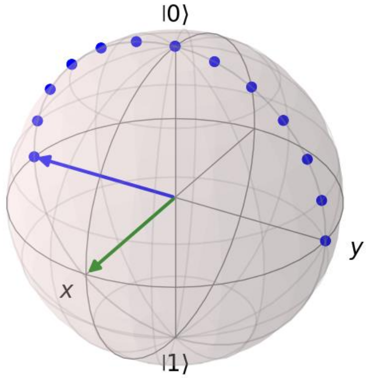
$$XR_z(\theta)X = R_z(-\theta)$$

$$\hat{z} \xrightarrow{\text{X}} -\hat{z}$$



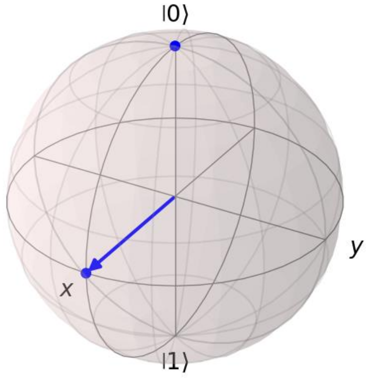
$$XR_y(\theta)X = R_y(-\theta)$$

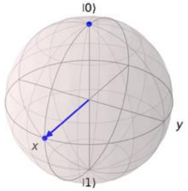
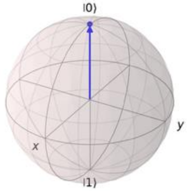
$$\hat{y} \xrightarrow{\text{X}} -\hat{y}$$



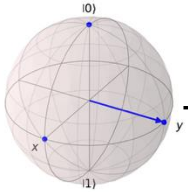
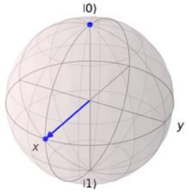
$$XR_x(\theta)X = R_x(\theta)$$

$$\hat{x} \xrightarrow{\text{X}} \hat{x}$$

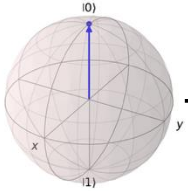
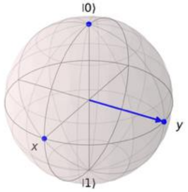



X axis $\xrightarrow{H}$ 
Z axis

$$HXH = Z$$


Y axis $\xrightarrow{S^\dagger}$ 
X axis

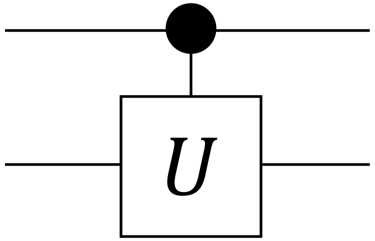
$$S^\dagger YS = X$$


Z axis $\xrightarrow{SH}$ 
Y axis

$$SHZHS^\dagger = Y$$

Controlled-U Gate from Single-Qubit Gates and CNOT

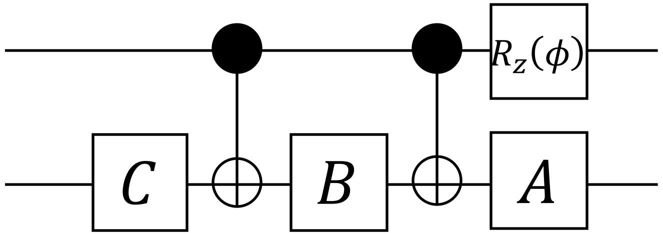
Controlled-U Gate (“quantum if-else”):



$$\text{C-U} = \begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix}.$$

$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

Implement c-U with CX and single-qubit gates?



Recipe: We can always find A, B, C such that:

- $ABC = I$
- $AXBXC = e^{-i\phi} U$

Take any single-qubit unitary:

$$e^{-i\phi} U = R_z(\gamma)\, R_x(\beta)\, R_z(\alpha)$$

Let $\theta_1 = \alpha + \frac{\pi}{2}, \theta_2 = \beta, \theta_3 = \gamma - \frac{\pi}{2},$

$$e^{-i\phi} U = R_z(\theta_3)\, R_y(\theta_2)\, R_z(\theta_1)$$

<u>Derive on board:</u>

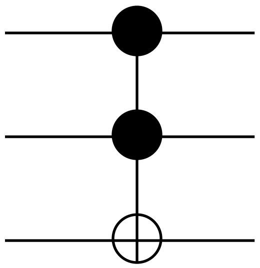
$$e^{-i\phi} U$$

$$= \underbrace{R_z(\theta_3) R_y\left(\frac{\theta_2}{2}\right)}_{A} X \underbrace{R_y\left(\frac{-\theta_2}{2}\right) R_z\left(\frac{-\theta_1}{2}\right) R_z\left(\frac{-\theta_3}{2}\right)}_{B} X \underbrace{R_z\left(\frac{-\theta_3}{2}\right) R_z\left(\frac{\theta_1}{2}\right)}_{C}$$

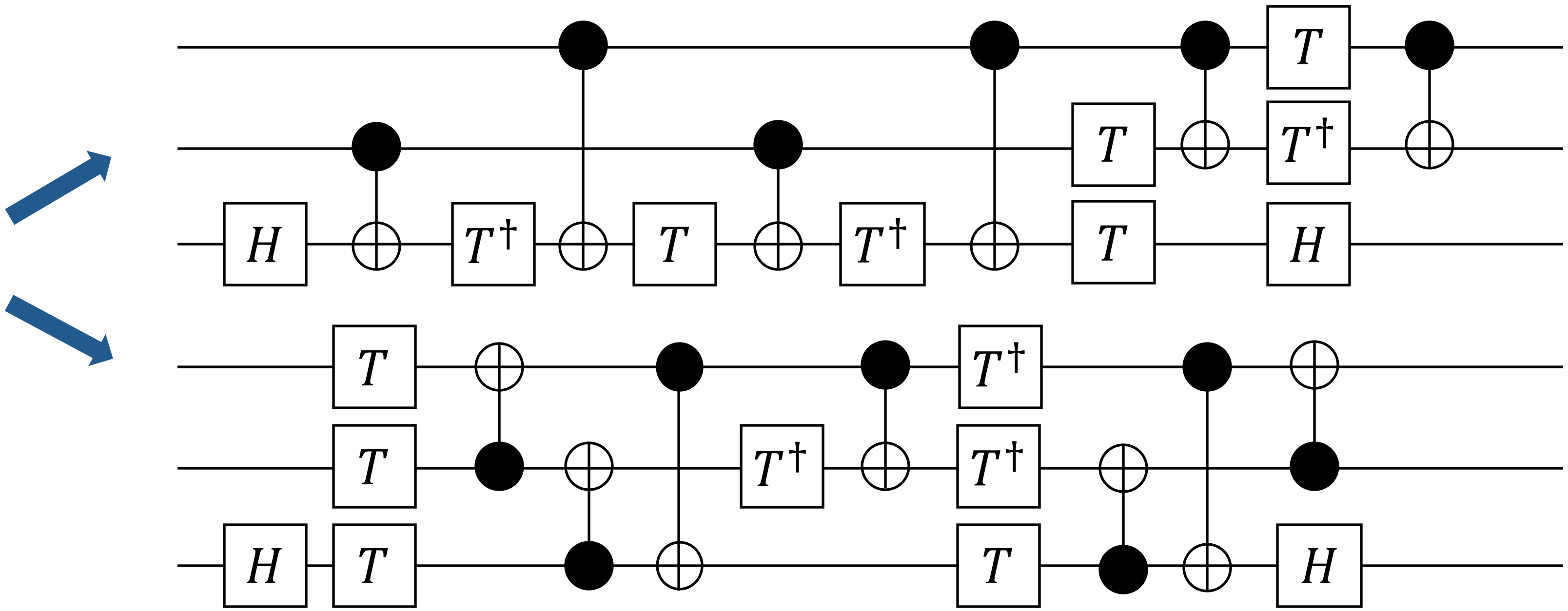
Multi-Qubit Unitary Synthesis

Computational Universality Theorem:
Any n-qubit unitary can be synthesized by single-qubit and two-qubit gates.

Example: Universal instruction set $\{H, T, CX\}$.



Toffoli gate
(controlled-CX)



Minimal in CX count.
[N&C. 2000]

Minimal in T count
and in T depth.
[Amy et. al. 2013]

Proof Sketch for the Universality Theorem

Computational Universality Theorem:
Any n-qubit unitary can be synthesized by **single-qubit** and **two-qubit gates**.

Proof outline:

- Two-qubit gates are *necessary*. Why?
- Two-qubit gates are *sufficient*:
  - Any $\boldsymbol{n}$**-qubit unitary** can be decomposed into a product of block-diagonal matrices.
  - Each **block-diagonal matrices** can be decomposed into a product of two-qubit gates.

I_{j-1}: $(j-1) \times (j-1)$ identity matrix

V: 2×2 unitary matrix

Block-diagonal matrix: $\Gamma_j(V) = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & v_{00} & v_{01} & & \\ & & & v_{10} & v_{11} & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{bmatrix}$

$(1 \leq j \leq d-1)$

I_{d-j+1}: $(d-j+1) \times (d-j+1)$ identity matrix

Proof Outline

- Any $\boldsymbol{n}$**-qubit unitary** can be decomposed into a product of $O(2^{2n})$ block-diagonal matrices.

Want to find:

$$U = W_{2^n} \cdot W_{2^n} \cdot \cdots \cdot W_2 \cdot W_1$$

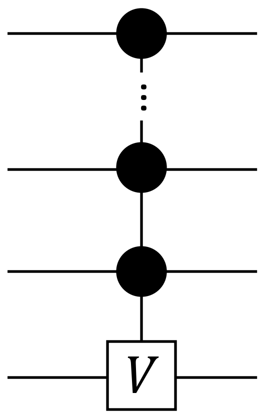
where W_i as a product of $O(2^n)$ block-diagonal matrices.

$$\Rightarrow \; W_{2^n} \cdot W_{2^n} \cdot \cdots \cdot W_2 \cdot W_1 U^{-1} = I$$

Derive on board: Multiply U^{-1} by W matrices to obtain identity I column by column.

Proof Outline

$\Lambda^{n-1}(V)$ gate



- Each **block-diagonal matrices** can be decomposed into a product of two-qubit gates.

Want to find (<u>Derive on board</u>)**:**

- $\Gamma_i(V)$ as a product of **permutations**, and **multi-controlled-V** ($\Lambda^{n-1}(V)$) gate.
- Permutations and $\Lambda^{n-1}(V)$ gates with two-qubit gates.

V: 2 × 2 unitary matrix

$$\Gamma_j(V) = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & v_{00} & v_{01} & & \\ & & & v_{10} & v_{11} & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{bmatrix}$$

$(1 \leq j \leq d-1)$

$$\Lambda^{n-1}(V) = \begin{bmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & \ddots & & & \\ & & & & & 1 & & \\ & & & & & & v_{00} & v_{01} \\ & & & & & & v_{10} & v_{11} \end{bmatrix}$$