IQI 04, Seminar 8

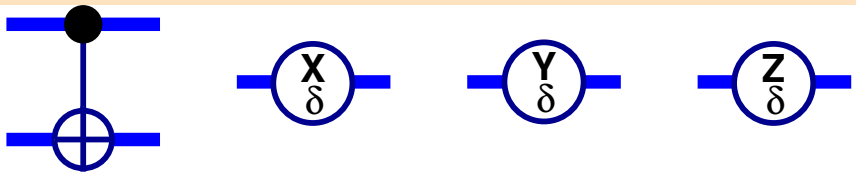
Produced with pdflatex and xfig

- Implementing the Toffoli gate.
- Multi-controlled gates.
- Universality.

E. “Manny” Knill: knill@boulder.nist.gov

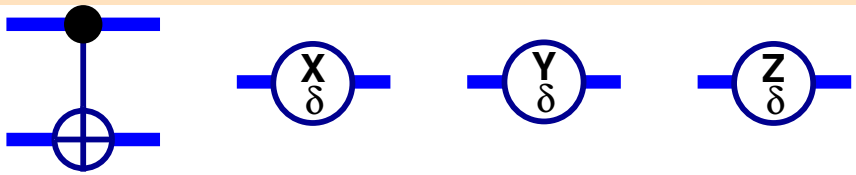
Gate Set

- Fundamental gates:

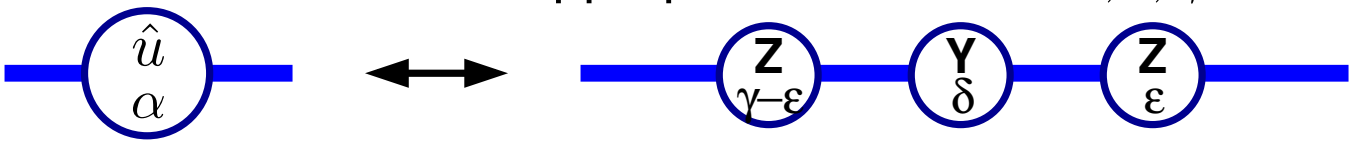


Gate Set

- Fundamental gates:

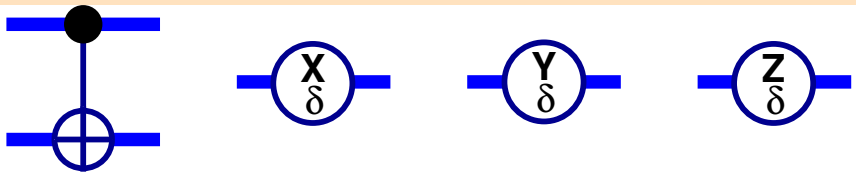


- Constructed gates.
  - α rotation around $\hat{u}$. For appropriate choices of ϵ, δ, γ:

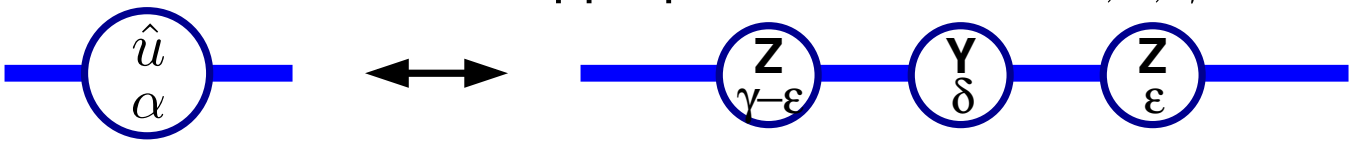


Gate Set

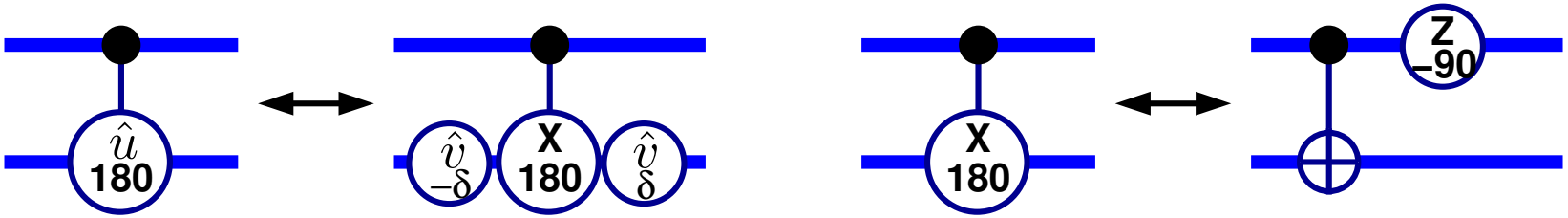
- Fundamental gates:



- Constructed gates.
  - α rotation around $\hat{u}$. For appropriate choices of ϵ, δ, γ:

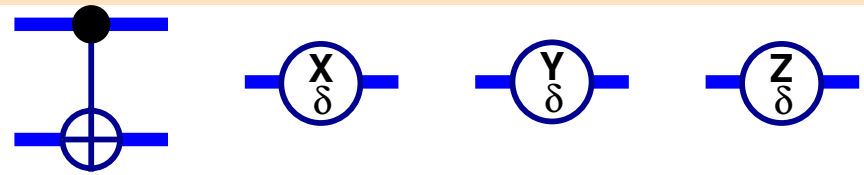


  - Controlled $180°$ rotation around $\hat{u}$. For appropriate choices of δ and $\hat{v}$:

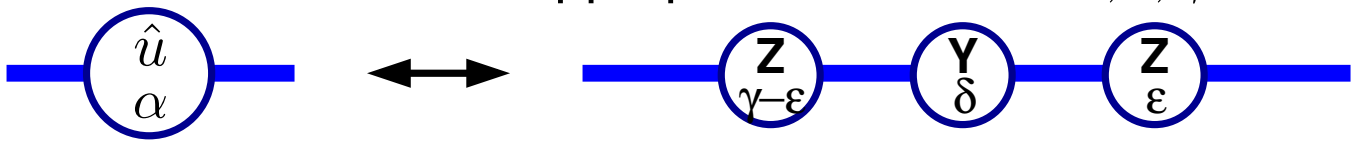


Gate Set

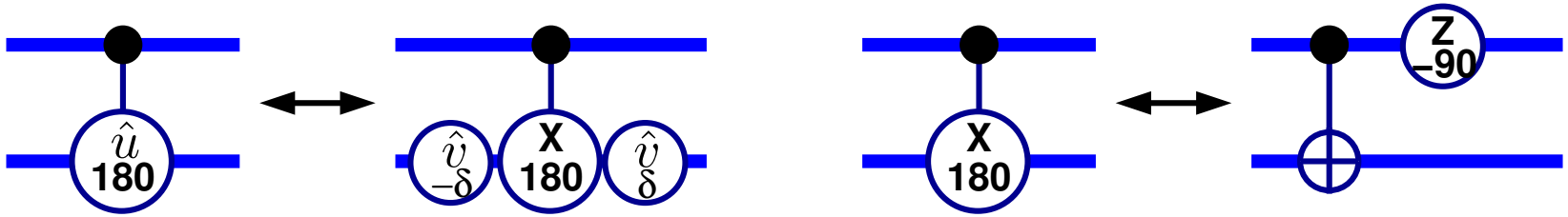
- Fundamental gates:



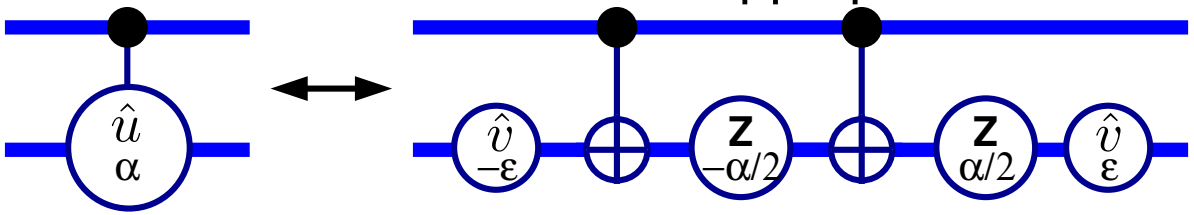
- Constructed gates.
  - α rotation around $\hat{u}$. For appropriate choices of ϵ, δ, γ:



  - Controlled $180°$ rotation around $\hat{u}$. For appropriate choices of δ and $\hat{v}$:

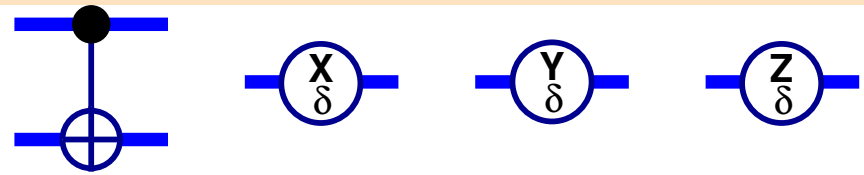


  - Controlled α rotation around $\hat{u}$. For appropriate choices of δ and $\hat{v}$:

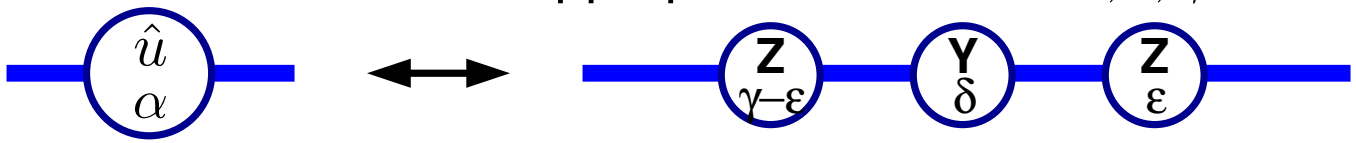


Gate Set

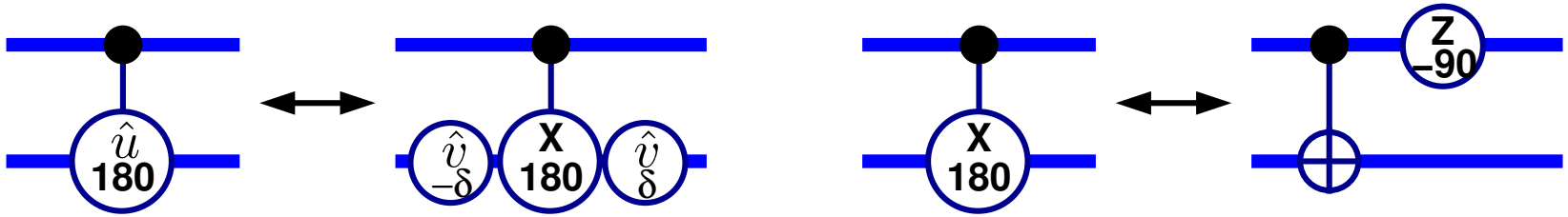
- Fundamental gates:



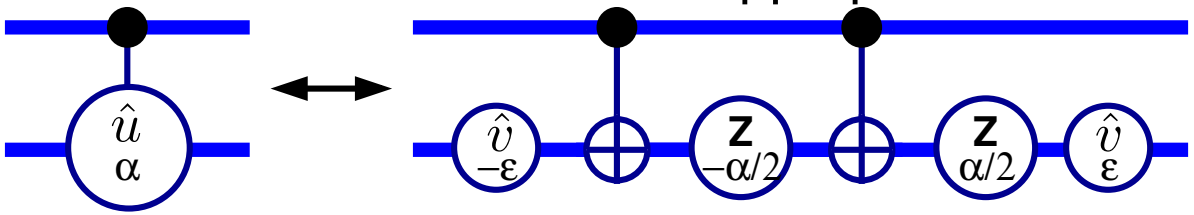
- Constructed gates.
  - α rotation around $\hat{u}$. For appropriate choices of ϵ, δ, γ:



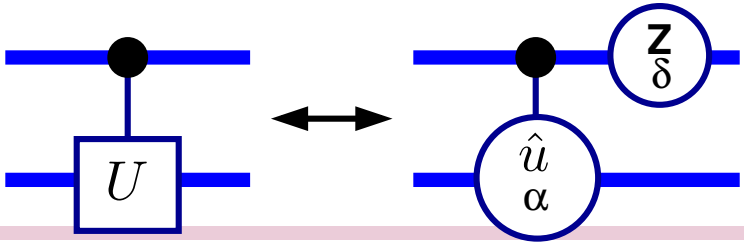
  - Controlled $180°$ rotation around $\hat{u}$. For appropriate choices of δ and $\hat{v}$:



  - Controlled α rotation around $\hat{u}$. For appropriate choices of δ and $\hat{v}$:



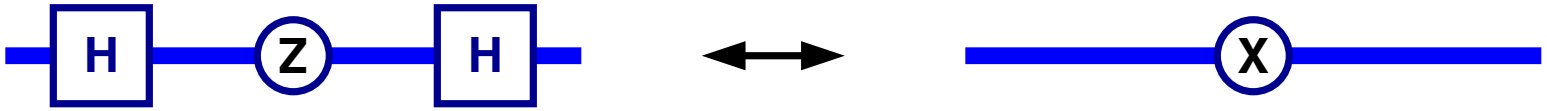
  - Controlled U. Choose α, $\hat{v}$, δ so that $e^{-i\delta}U$ is a α rotation around $\hat{u}$.



Controlled Sign Flips

- Controlled sign flips $\leftrightarrow$ controlled nots.

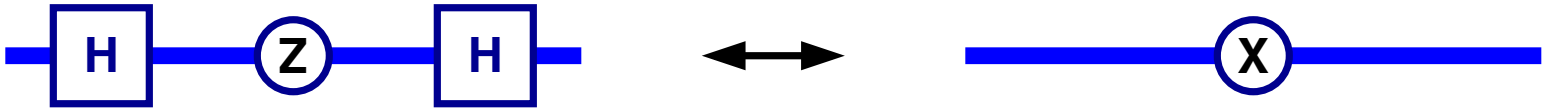
Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$



Controlled Sign Flips

- Controlled sign flips $\leftrightarrow$ controlled nots.

Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$

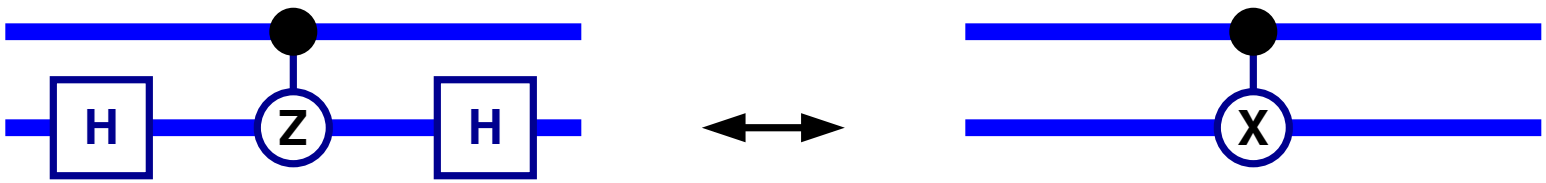


$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}.\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

Controlled Sign Flips

- Controlled sign flips $\leftrightarrow$ controlled nots.

Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$

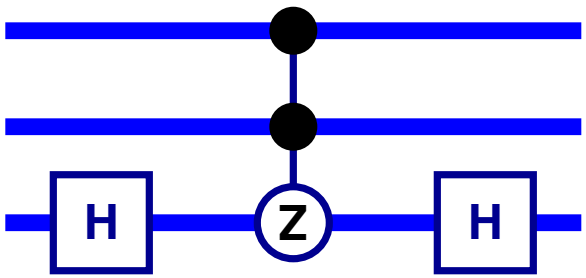


$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}.\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

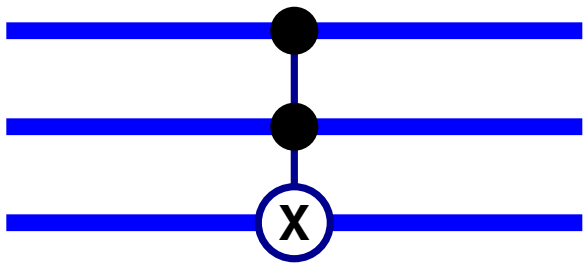
Controlled Sign Flips

- Controlled sign flips $\leftrightarrow$ controlled nots.

Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$



$\leftrightarrow$

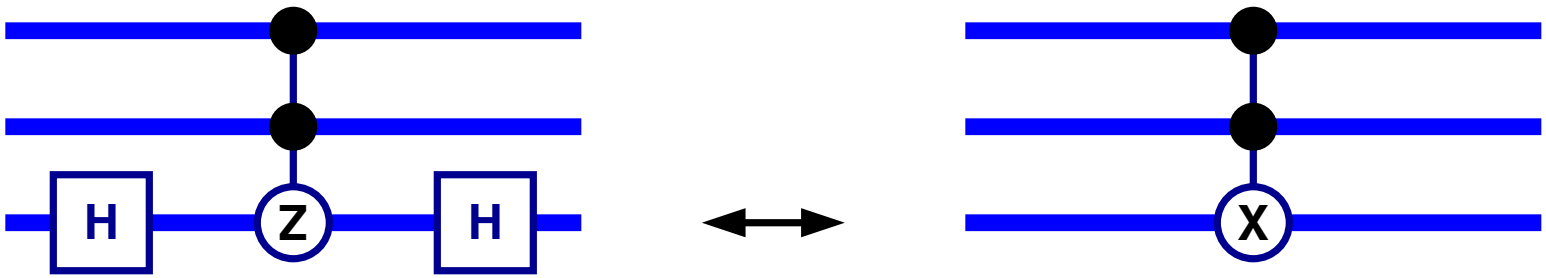


$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}.\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

Controlled Sign Flips

- Controlled sign flips $\leftrightarrow$ controlled nots.

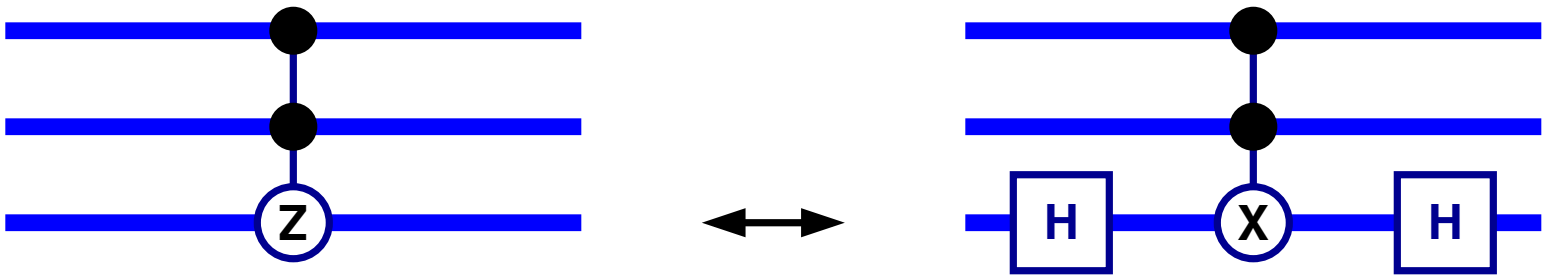
Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$



Controlled Sign Flips

- Controlled sign flips $\leftrightarrow$ controlled nots.

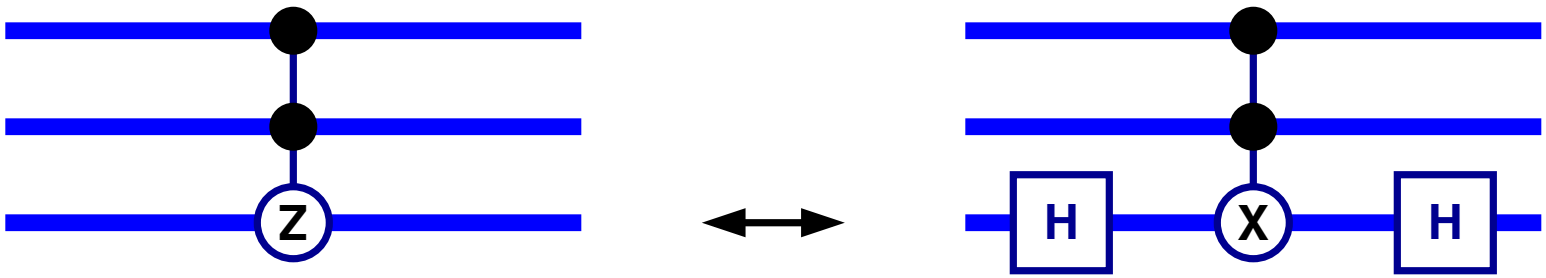
Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$



Controlled Sign Flips

- Controlled sign flips $\leftrightarrow$ controlled nots.

Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$



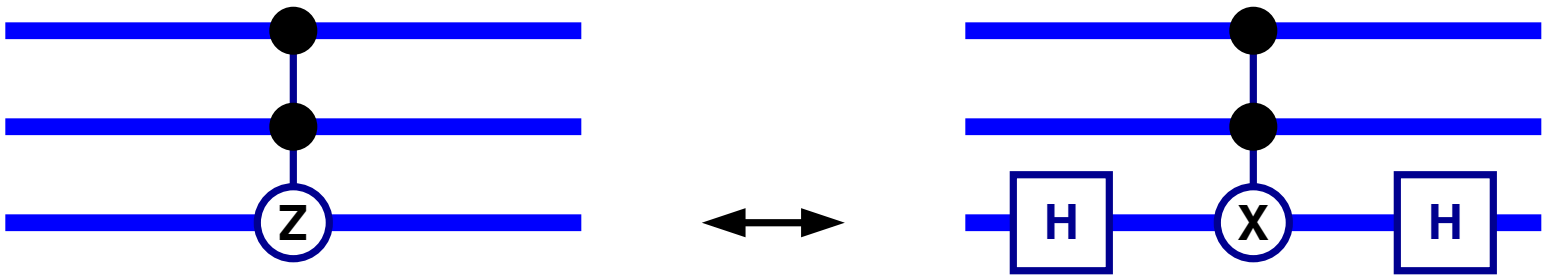
- Exponential forms for $\mathbf{sgn}, \mathbf{csgn}, \mathbf{c^2sgn}$.

$$\mathbf{sgn} = \sigma_z \quad = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Controlled Sign Flips

- Controlled sign flips $\leftrightarrow$ controlled nots.

Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$



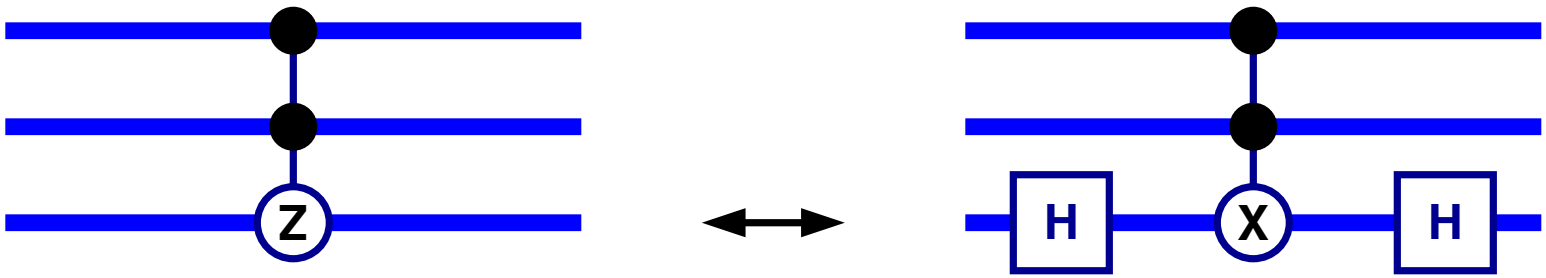
- Exponential forms for $\mathbf{sgn}, \mathbf{csgn}, \mathbf{c^2sgn}$.

$$\begin{aligned} \mathbf{sgn} = \sigma_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \exp\left(\begin{pmatrix} 0 & 0 \\ 0 & i\pi \end{pmatrix}\right) \end{aligned}$$

Controlled Sign Flips

- Controlled sign flips $\leftrightarrow$ controlled nots.

Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$



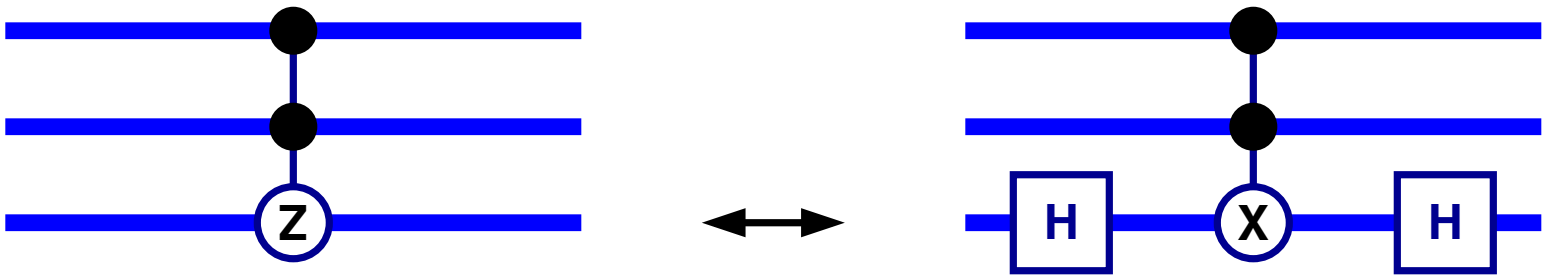
- Exponential forms for $\mathbf{sgn}, \mathbf{csgn}, \mathbf{c^2sgn}$.

$$\begin{aligned}
\mathbf{sgn} = \sigma_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
&= \exp\left(\begin{pmatrix} 0 & 0 \\ 0 & i\pi \end{pmatrix}\right) \\
&= \exp\left(\frac{i}{2}\pi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right)\right)
\end{aligned}$$

Controlled Sign Flips

- Controlled sign flips $\leftrightarrow$ controlled nots.

Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$



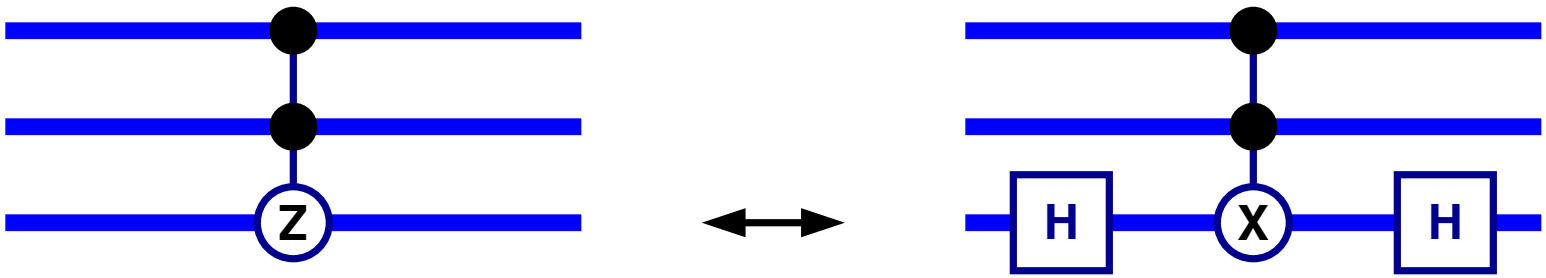
- Exponential forms for $\mathbf{sgn}, \mathbf{csgn}, \mathbf{c^2sgn}$.

$$
\begin{aligned}
\mathbf{sgn} = \sigma_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
&= \exp\left(\begin{pmatrix} 0 & 0 \\ 0 & i\pi \end{pmatrix}\right) \\
&= \exp\left(\frac{i}{2}\pi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right)\right) \\
&= e^{\frac{i}{2}(\mathbb{1}-Z)\pi}
\end{aligned}
$$

Controlled Sign Flips

- Controlled sign flips $\leftrightarrow$ controlled nots.

Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$



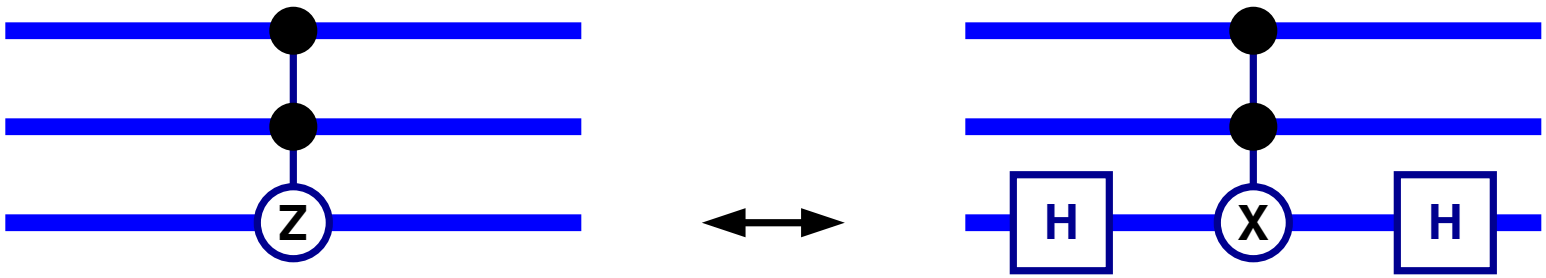
- Exponential forms for $\mathbf{sgn}, \mathbf{csgn}, \mathbf{c^2sgn}$.

$$\mathbf{sgn} = \sigma_z \quad = \quad e^{\frac{i}{2}(\mathbb{1}-Z)\pi}$$

Controlled Sign Flips

- Controlled sign flips $\leftrightarrow$ controlled nots.

Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$



- Exponential forms for $\mathbf{sgn}, \mathbf{csgn}, \mathbf{c^2sgn}$.

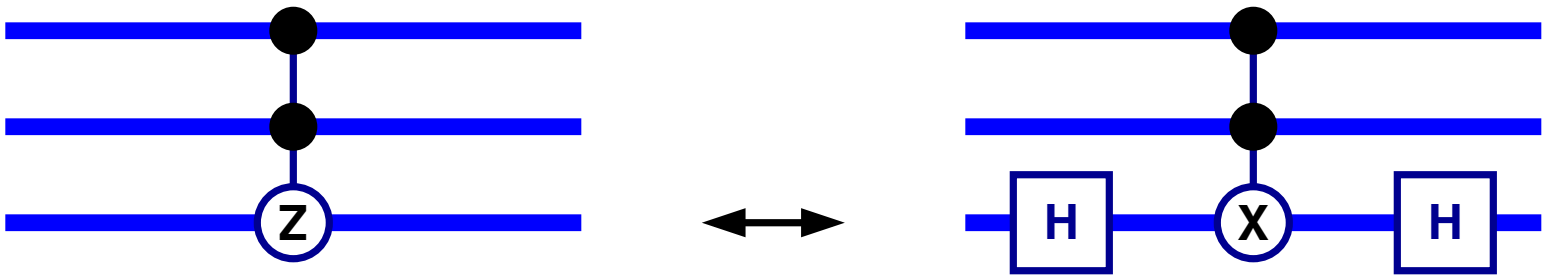
$$\mathbf{sgn} = \sigma_z \quad = \quad e^{\frac{i}{2}(\mathbb{1}-Z)\pi}$$

$$\mathbf{csgn}^{(\mathsf{AB})} \quad = \quad \exp\left(i\left(|\mathbf{1}\rangle_{\mathsf{A}}^{\mathsf{A}}\langle\mathbf{1}|\right)\left(|\mathbf{1}\rangle_{\mathsf{B}}^{\mathsf{B}}\langle\mathbf{1}|\right)\pi\right)$$

Controlled Sign Flips

- Controlled sign flips $\leftrightarrow$ controlled nots.

Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$



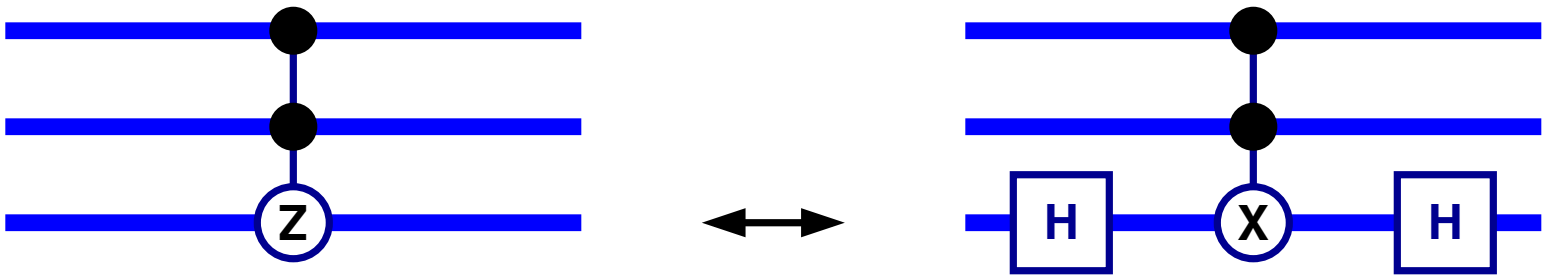
- Exponential forms for $\mathbf{sgn}, \mathbf{csgn}, \mathbf{c^2sgn}$.

$$\begin{aligned}
\mathbf{sgn} = \sigma_z &= e^{\frac{i}{2}(\mathbb{1}-Z)\pi} \\
\mathbf{csgn}^{(\mathsf{AB})} &= \exp\left(i\left(|\mathbf{1}\rangle_{\mathsf{A}}^{\mathsf{A}}\langle\mathbf{1}|\right)\left(|\mathbf{1}\rangle_{\mathsf{B}}^{\mathsf{B}}\langle\mathbf{1}|\right)\pi\right) \\
&= e^{\frac{i}{4}(\mathbb{1}-Z^{(\mathsf{A})})(\mathbb{1}-Z^{(\mathsf{B})})\pi}
\end{aligned}$$

Controlled Sign Flips

- Controlled sign flips $\leftrightarrow$ controlled nots.

Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$



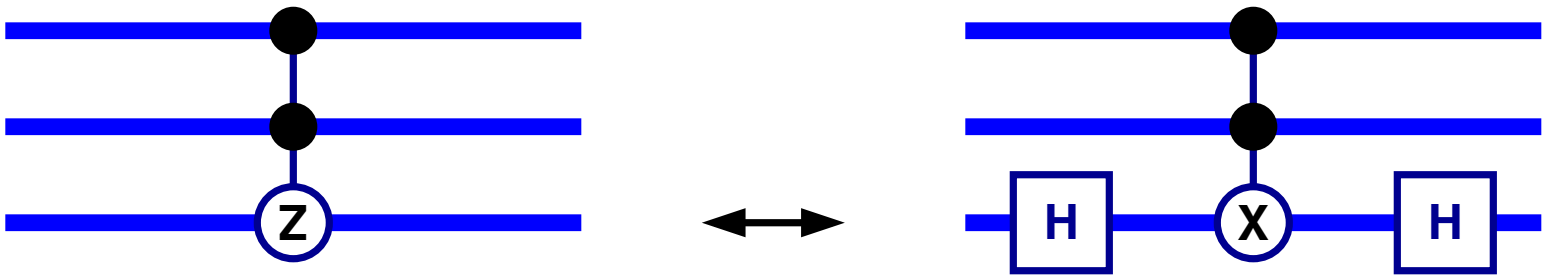
- Exponential forms for $\mathbf{sgn}, \mathbf{csgn}, \mathbf{c^2sgn}$.

$$
\begin{aligned}
\mathbf{sgn} = \sigma_z &= e^{\frac{i}{2}(\mathbb{1}-Z)\pi} \\
\mathbf{csgn}^{(\mathsf{AB})} &= \exp\left(i\left(|1\rangle_{\mathsf{A}}^{\mathsf{A}}\langle 1|\right)\left(|1\rangle_{\mathsf{B}}^{\mathsf{B}}\langle 1|\right)\pi\right) \\
&= e^{\frac{i}{4}(\mathbb{1}-Z^{(\mathsf{A})})(\mathbb{1}-Z^{(\mathsf{B})})\pi} \\
\mathbf{c^2sgn}^{(\mathsf{ABC})} &= \exp\left(i\left(|1\rangle_{\mathsf{A}}^{\mathsf{A}}\langle 1|\right)\left(|1\rangle_{\mathsf{B}}^{\mathsf{B}}\langle 1|\right)\left(|1\rangle_{\mathsf{C}}^{\mathsf{C}}\langle 1|\right)\pi\right)
\end{aligned}
$$

Controlled Sign Flips

- Controlled sign flips $\leftrightarrow$ controlled nots.

Abbreviate: $X = \sigma_x, Y = \sigma_y, Z = \sigma_z$



- Exponential forms for $\mathbf{sgn}, \mathbf{csgn}, \mathbf{c^2sgn}$.

$$
\begin{aligned}
\mathbf{sgn} = \sigma_z &= e^{\frac{i}{2}(\mathbb{1}-Z)\pi} \\
\mathbf{csgn}^{(\mathsf{AB})} &= \exp\left(i\left(|\mathbf{1}\rangle_{\mathsf{A}}^{\mathsf{A}}\langle\mathbf{1}|\right)\left(|\mathbf{1}\rangle_{\mathsf{B}}^{\mathsf{B}}\langle\mathbf{1}|\right)\pi\right) \\
&= e^{\frac{i}{4}(\mathbb{1}-Z^{(\mathsf{A})})(\mathbb{1}-Z^{(\mathsf{B})})\pi} \\
\mathbf{c^2sgn}^{(\mathsf{ABC})} &= \exp\left(i\left(|\mathbf{1}\rangle_{\mathsf{A}}^{\mathsf{A}}\langle\mathbf{1}|\right)\left(|\mathbf{1}\rangle_{\mathsf{B}}^{\mathsf{B}}\langle\mathbf{1}|\right)\left(|\mathbf{1}\rangle_{\mathsf{C}}^{\mathsf{C}}\langle\mathbf{1}|\right)\pi\right) \\
&= e^{\frac{i}{8}(\mathbb{1}-Z^{(\mathsf{A})})(\mathbb{1}-Z^{(\mathsf{B})})(\mathbb{1}-Z^{(\mathsf{C})})\pi}
\end{aligned}
$$

Controlled Sign Flip Implementations

- Decomposition of $\mathbf{csgn}$.

$$\mathbf{csgn}^{(\mathsf{AB})} = e^{\frac{i\pi}{4}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)}$$

Controlled Sign Flip Implementations

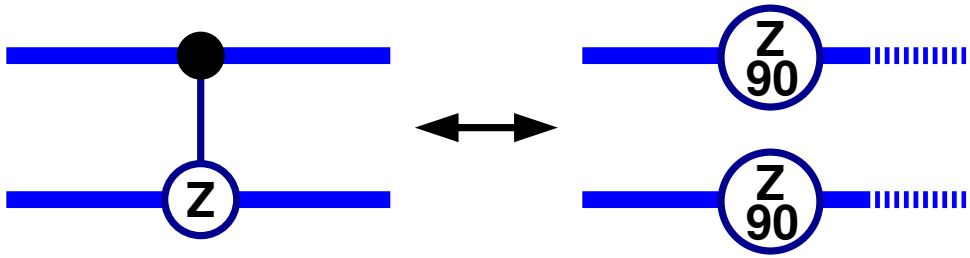
- Decomposition of $\mathbf{csgn}$.

$$\mathbf{csgn}^{(\mathsf{AB})} = e^{\frac{i\pi}{4}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)} = e^{\frac{i\pi}{4}\mathbb{1}} e^{-\frac{i\pi}{4}Z^{(\mathsf{A})}} e^{-\frac{i\pi}{4}Z^{(\mathsf{B})}} e^{\frac{i\pi}{4}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}$$

Controlled Sign Flip Implementations

- Decomposition of $\mathbf{csgn}$.

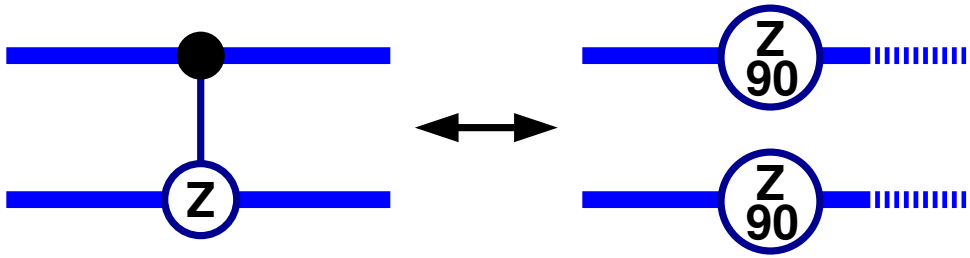
$$\mathbf{csgn}^{(\mathsf{AB})} = e^{\frac{i\pi}{4}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)} = e^{\frac{i\pi}{4}\mathbb{1}} e^{-\frac{i\pi}{4}Z^{(\mathsf{A})}} e^{-\frac{i\pi}{4}Z^{(\mathsf{B})}} e^{\frac{i\pi}{4}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}$$



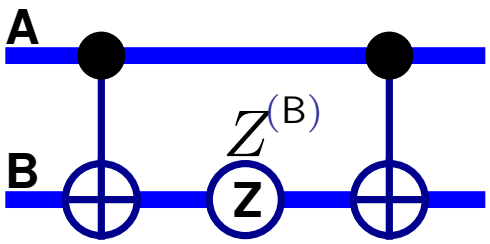
Controlled Sign Flip Implementations

- Decomposition of $\mathbf{csgn}$.

$$\mathbf{csgn}^{(\mathsf{AB})} = e^{\frac{i\pi}{4}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)} = e^{\frac{i\pi}{4}\mathbb{1}} e^{-\frac{i\pi}{4}Z^{(\mathsf{A})}} e^{-\frac{i\pi}{4}Z^{(\mathsf{B})}} e^{\frac{i\pi}{4}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}$$



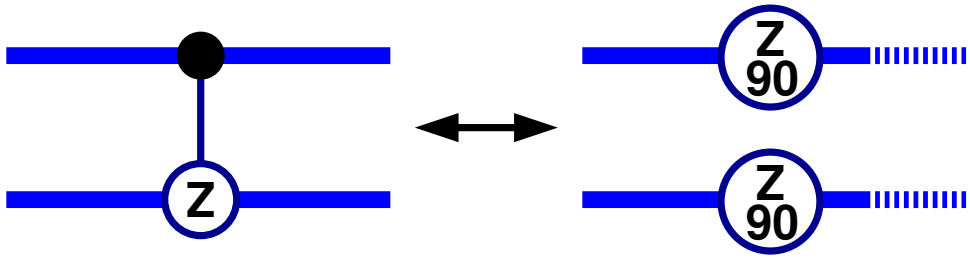
- Recall conjugation rules.



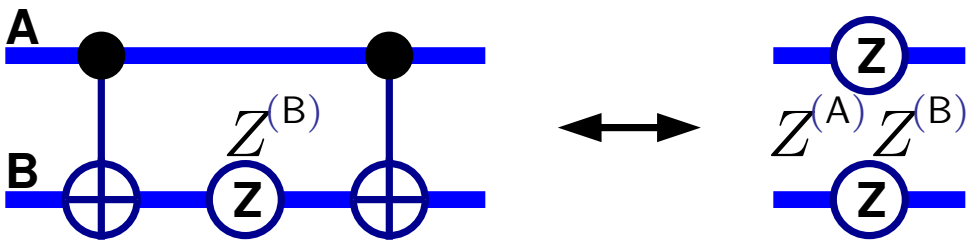
Controlled Sign Flip Implementations

- Decomposition of $\mathbf{csgn}$.

$$\mathbf{csgn}^{(\mathsf{AB})} = e^{\frac{i\pi}{4}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)} = e^{\frac{i\pi}{4}\mathbb{1}} e^{-\frac{i\pi}{4}Z^{(\mathsf{A})}} e^{-\frac{i\pi}{4}Z^{(\mathsf{B})}} e^{\frac{i\pi}{4}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}$$



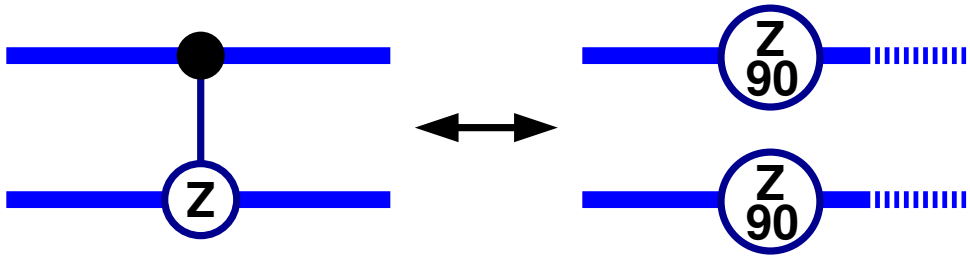
- Recall conjugation rules.



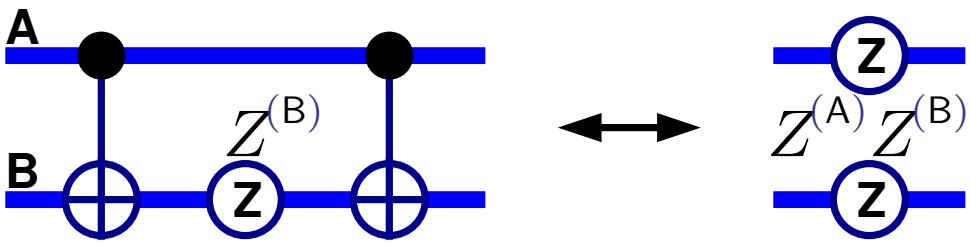
Controlled Sign Flip Implementations

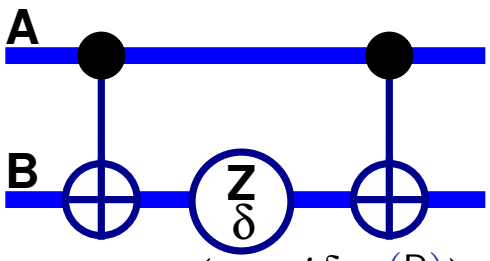
- Decomposition of $\mathbf{csgn}$.

$$\mathbf{csgn}^{(\mathsf{AB})} = e^{\frac{i\pi}{4}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)} = e^{\frac{i\pi}{4}\mathbb{1}} e^{-\frac{i\pi}{4}Z^{(\mathsf{A})}} e^{-\frac{i\pi}{4}Z^{(\mathsf{B})}} e^{\frac{i\pi}{4}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}$$



- Recall conjugation rules.



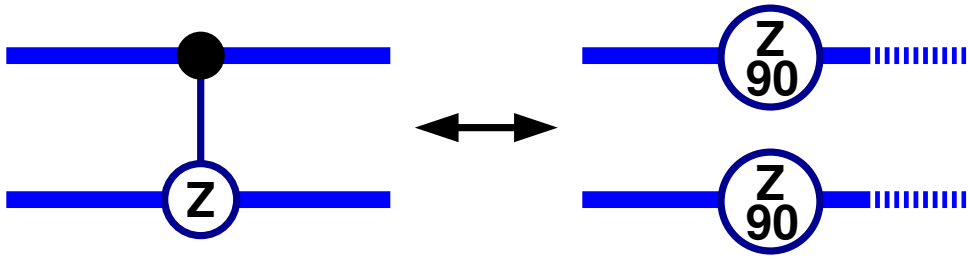


$$\exp\left(-\frac{i\delta}{2}Z^{(\mathsf{B})}\right)$$

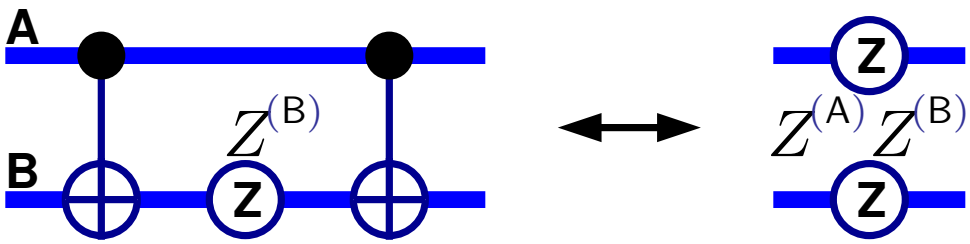
Controlled Sign Flip Implementations

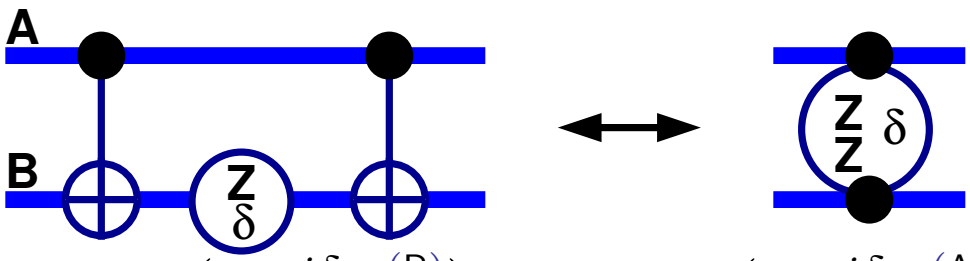
- Decomposition of $\mathbf{csgn}$.

$$\mathbf{csgn}^{(\mathsf{AB})} = e^{\frac{i\pi}{4}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)} = e^{\frac{i\pi}{4}\mathbb{1}} e^{-\frac{i\pi}{4}Z^{(\mathsf{A})}} e^{-\frac{i\pi}{4}Z^{(\mathsf{B})}} e^{\frac{i\pi}{4}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}$$



- Recall conjugation rules.



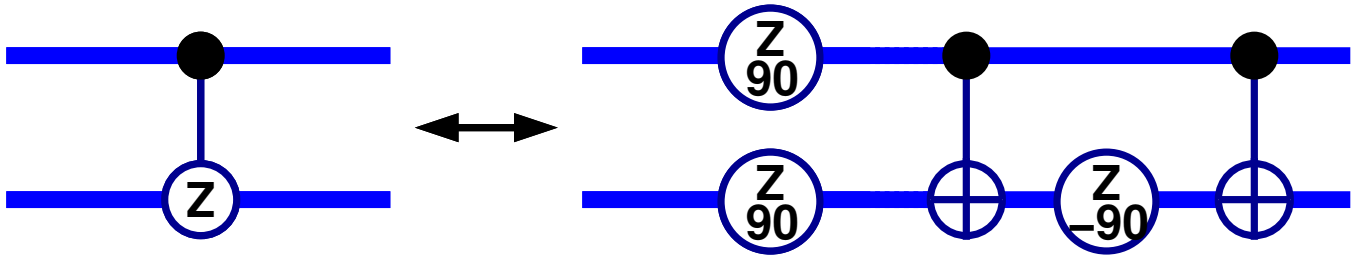


$$\exp\left(-\frac{i\delta}{2}Z^{(\mathsf{B})}\right) \qquad \exp\left(-\frac{i\delta}{2}Z^{(\mathsf{A})}Z^{(\mathsf{B})}\right)$$

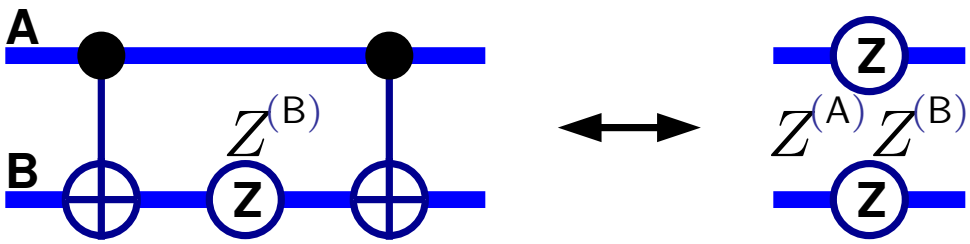
Controlled Sign Flip Implementations

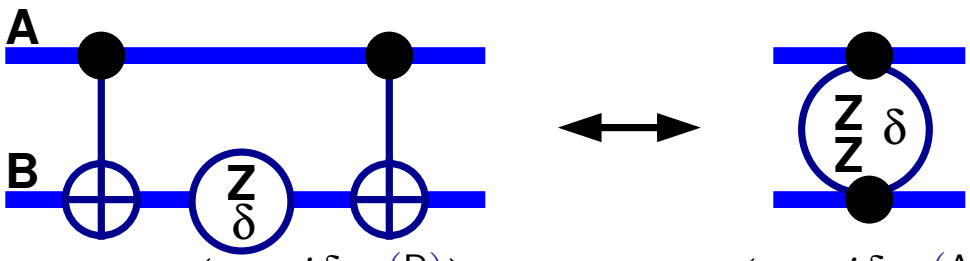
- Decomposition of $\mathbf{csgn}$.

$$\mathbf{csgn}^{(\mathsf{AB})} = e^{\frac{i\pi}{4}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)} = e^{\frac{i\pi}{4}\mathbb{1}} e^{-\frac{i\pi}{4}Z^{(\mathsf{A})}} e^{-\frac{i\pi}{4}Z^{(\mathsf{B})}} e^{\frac{i\pi}{4}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}$$



- Recall conjugation rules.





$$\exp\left(-\frac{i\delta}{2}Z^{(\mathsf{B})}\right) \qquad \exp\left(-\frac{i\delta}{2}Z^{(\mathsf{A})}Z^{(\mathsf{B})}\right)$$

Controlled Sign Flip Implementations

Controlled Sign Flip Implementations

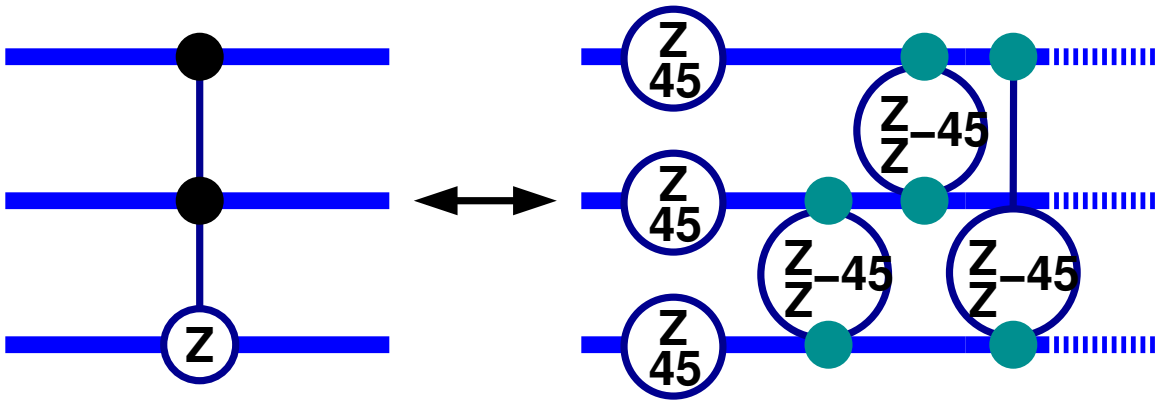
- Decomposition of $\mathbf{c^2sgn}$.

$$\mathbf{c^2sgn}^{(\mathsf{ABC})} = e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)}$$

Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

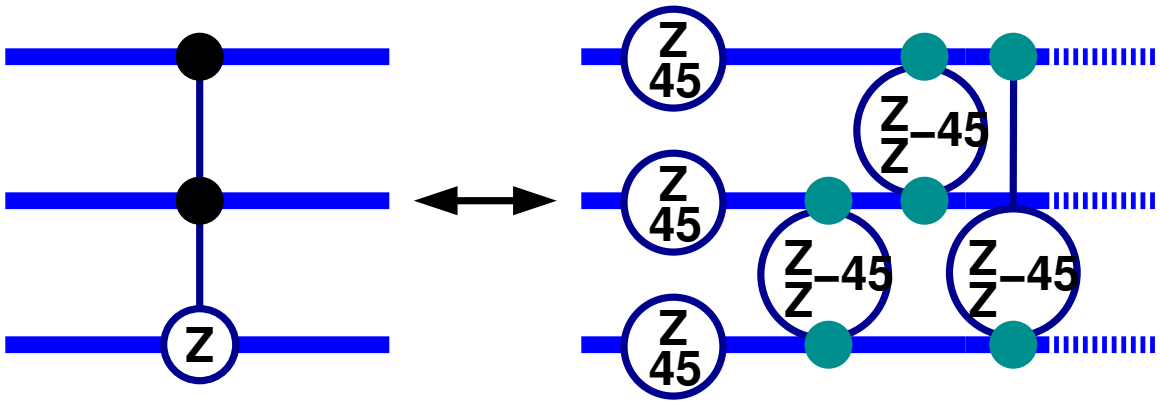
$$\begin{aligned}
\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\
&= e^{\frac{i\pi}{8}\mathbb{1}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\
&\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}}e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}
\end{aligned}$$

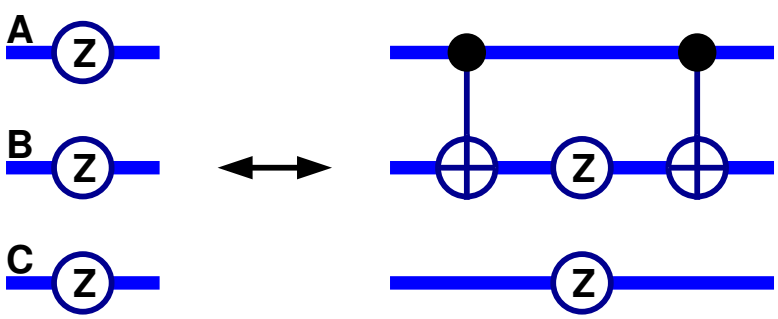


Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

$$\begin{aligned}
\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\
&= e^{\frac{i\pi}{8}\mathbb{1}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\
&\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}}e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}
\end{aligned}$$

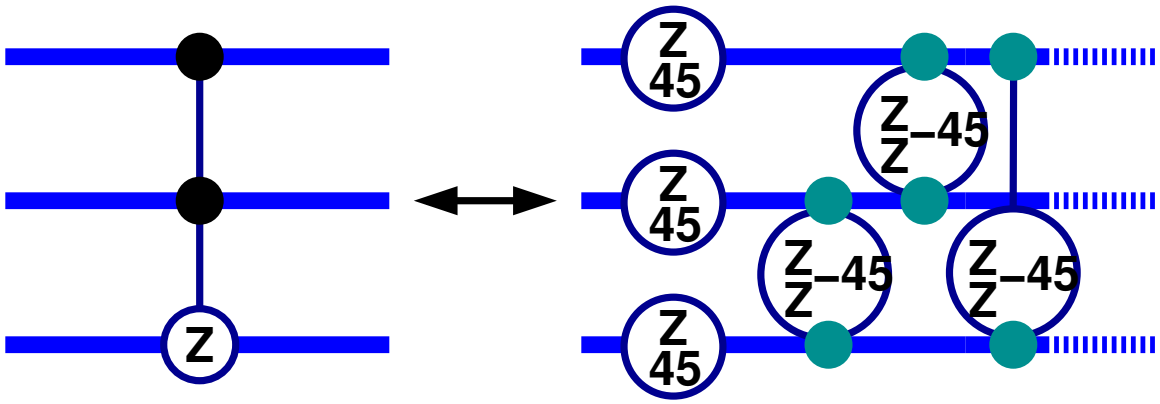


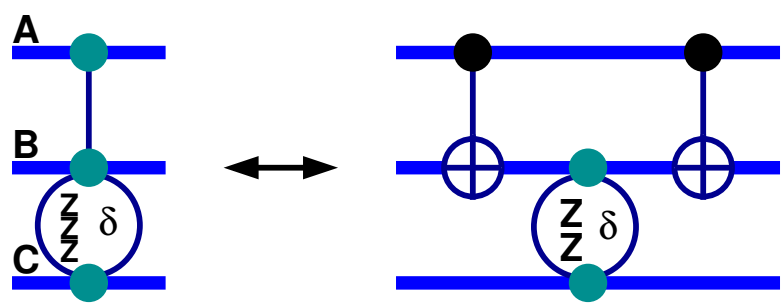


Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

$$
\begin{aligned}
\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\
&= e^{\frac{i\pi}{8}\mathbb{1}} e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}} e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}} e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\
&\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}} e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}} e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}} e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}
\end{aligned}
$$

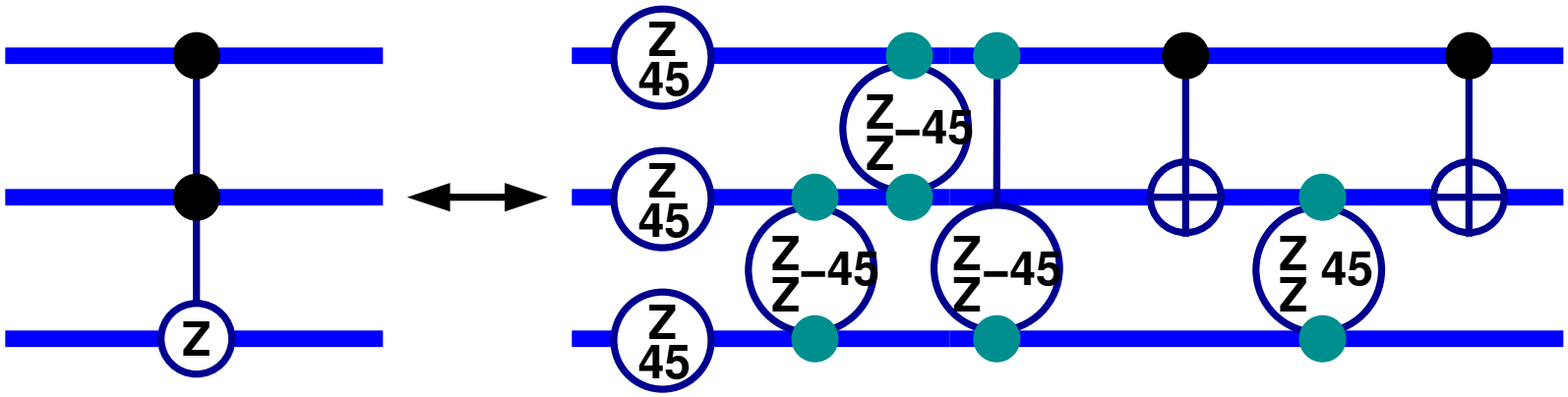


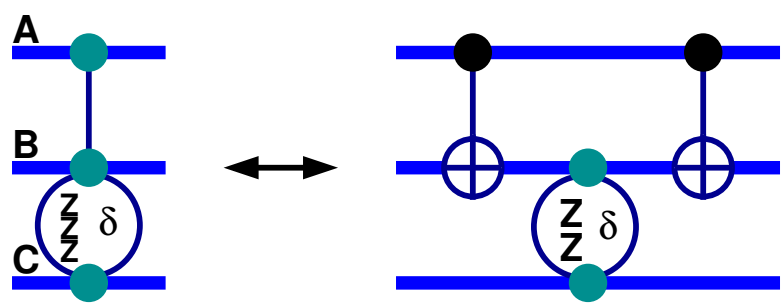


Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

$$\begin{aligned}
\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\
&= e^{\frac{i\pi}{8}\mathbb{1}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\
&\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}}e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}
\end{aligned}$$

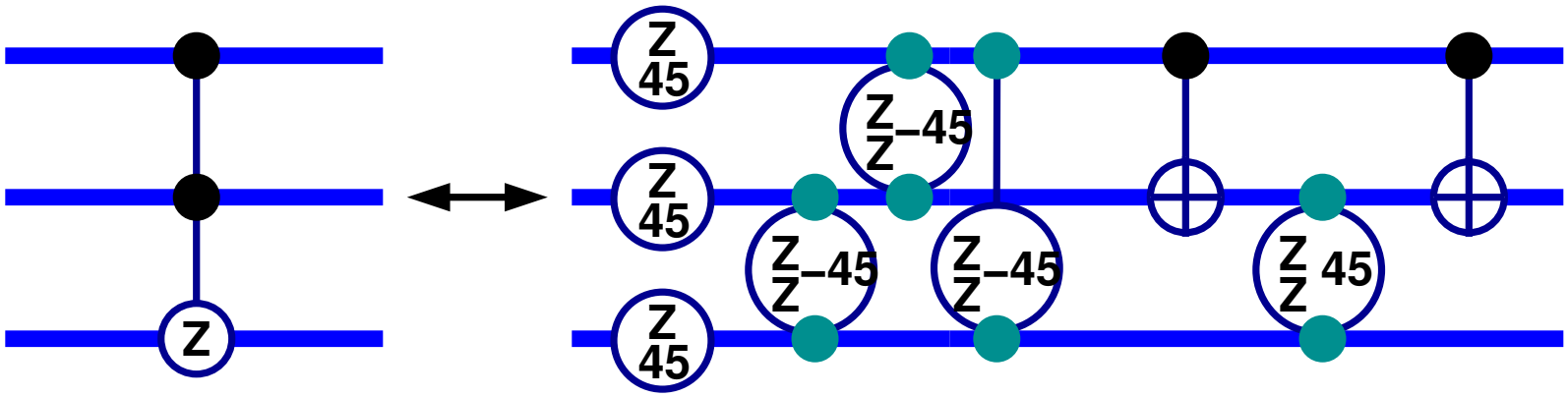




Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

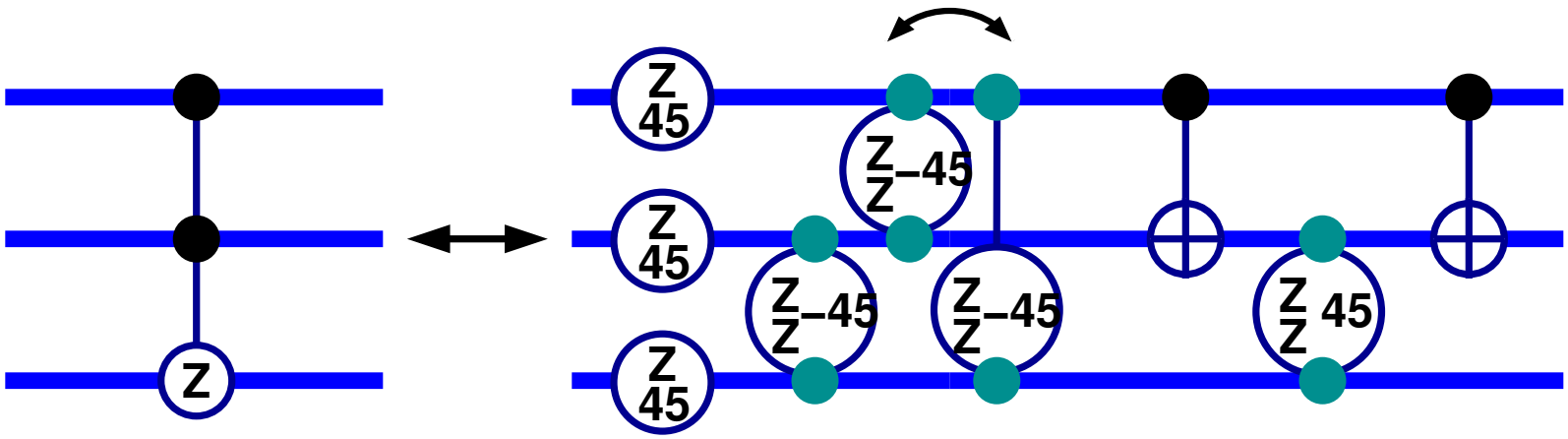
$$
\begin{aligned}
\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\
&= e^{\frac{i\pi}{8}\mathbb{1}} e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}} e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}} e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\
&\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}} e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}} e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}} e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}
\end{aligned}
$$



Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

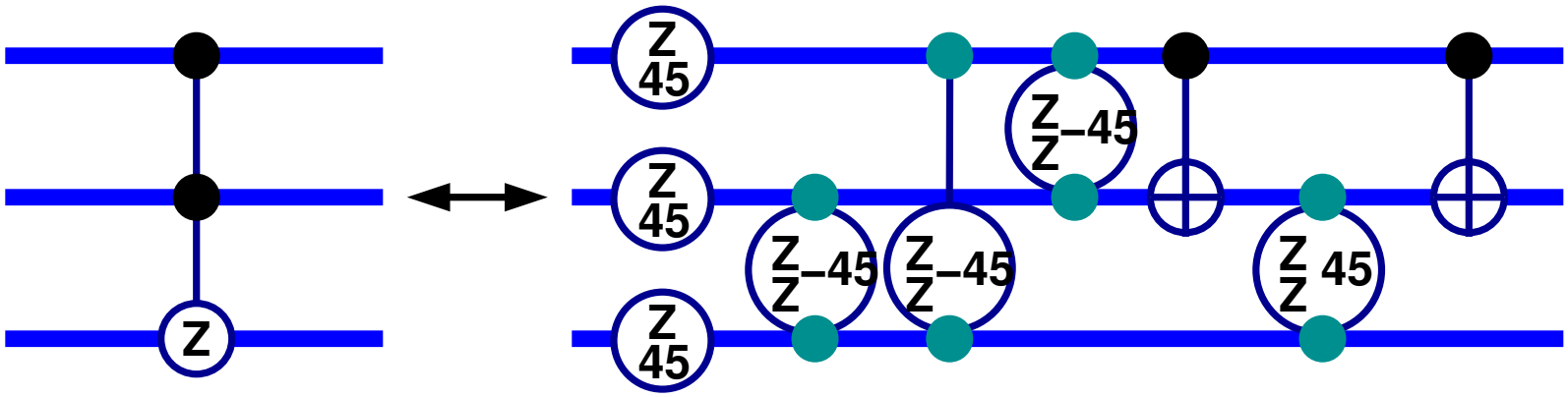
$$\begin{aligned}\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\ &= e^{\frac{i\pi}{8}\mathbb{1}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\ &\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}}e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}\end{aligned}$$



Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

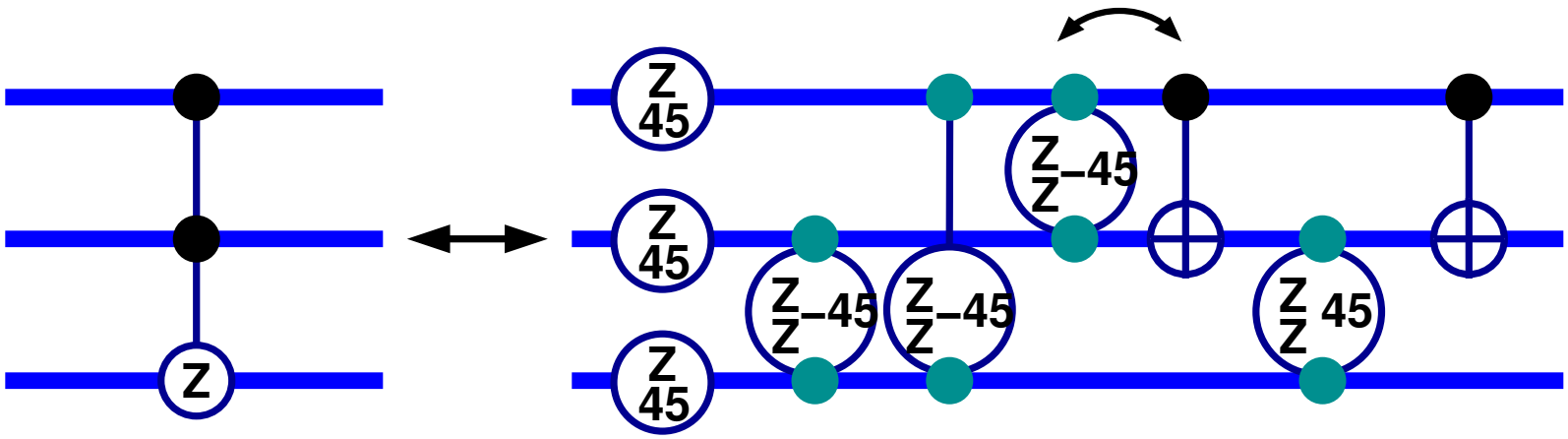
$$\begin{aligned}
\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\
&= e^{\frac{i\pi}{8}\mathbb{1}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\
&\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}}e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}
\end{aligned}$$



Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

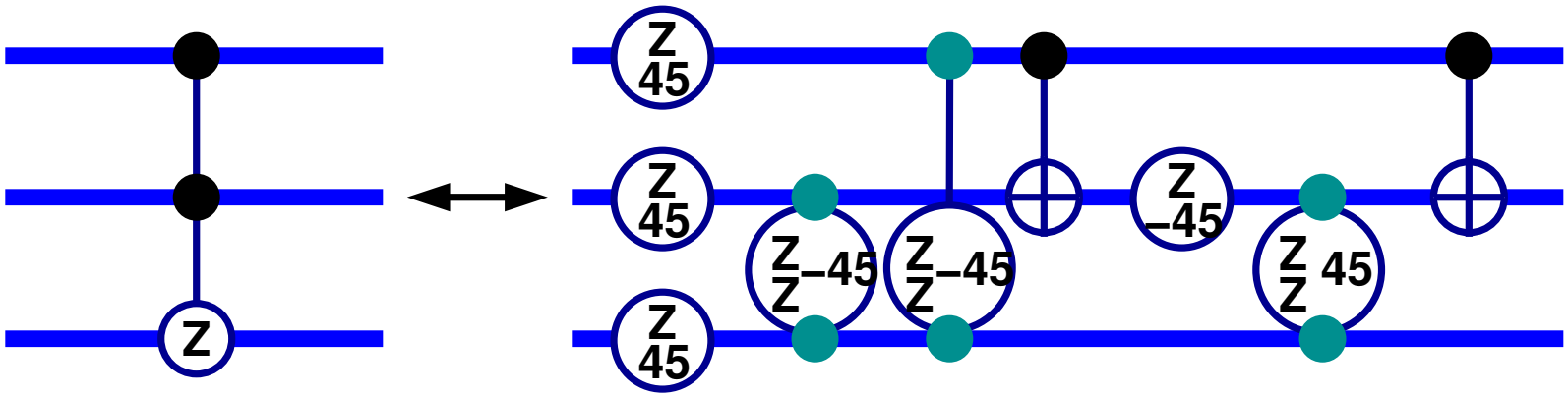
$$\begin{aligned}\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\ &= e^{\frac{i\pi}{8}\mathbb{1}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\ &\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}}e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}\end{aligned}$$



Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

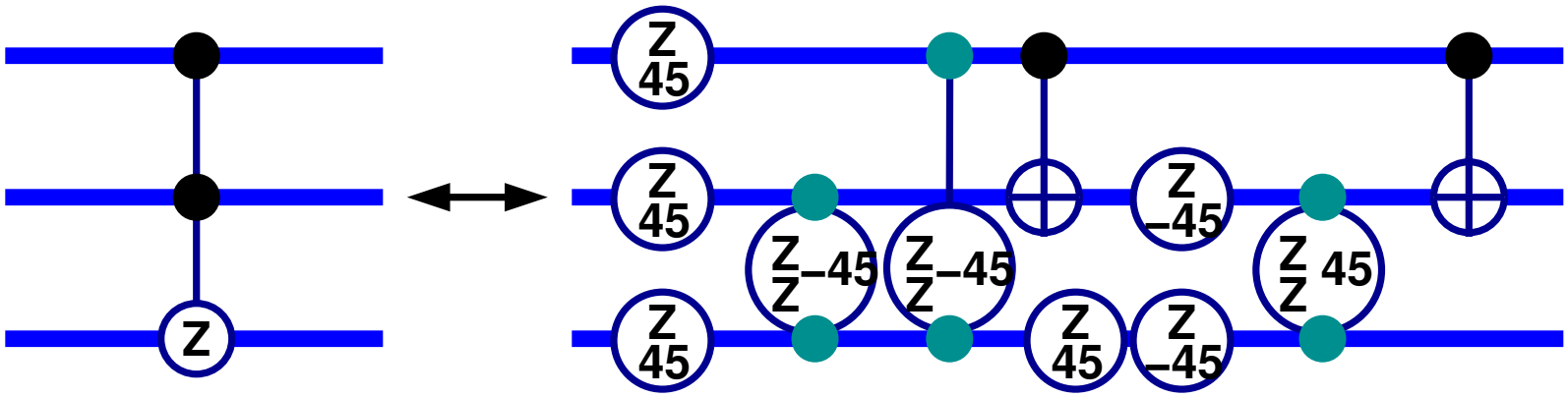
$$\begin{aligned}
\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\
&= e^{\frac{i\pi}{8}\mathbb{1}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\
&\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}}e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}
\end{aligned}$$



Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

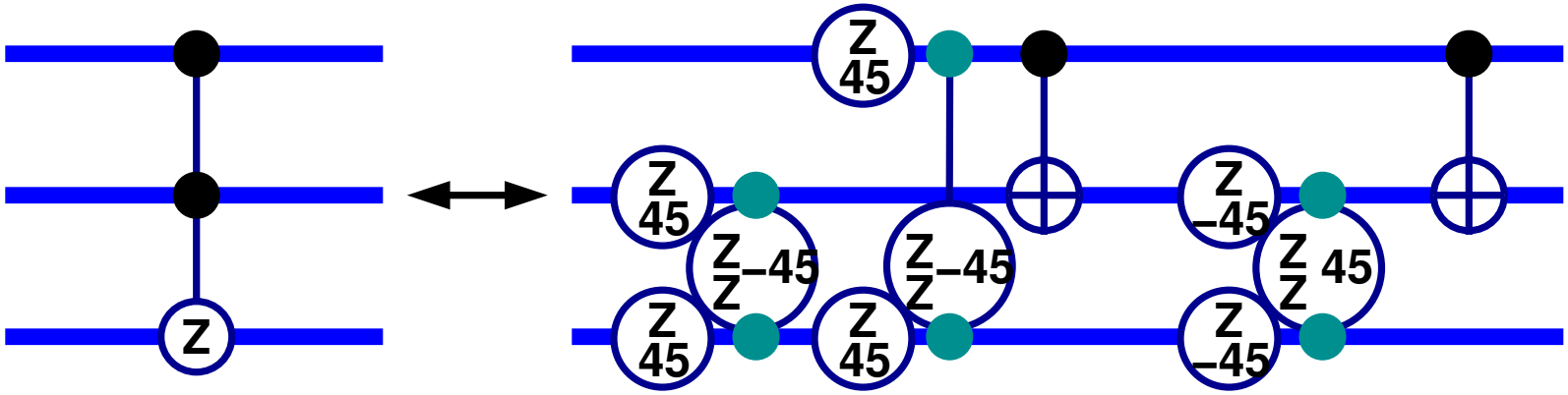
$$
\begin{aligned}
\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\
&= e^{\frac{i\pi}{8}\mathbb{1}} e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}} e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}} e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\
&\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}} e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}} e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}} e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}
\end{aligned}
$$



Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

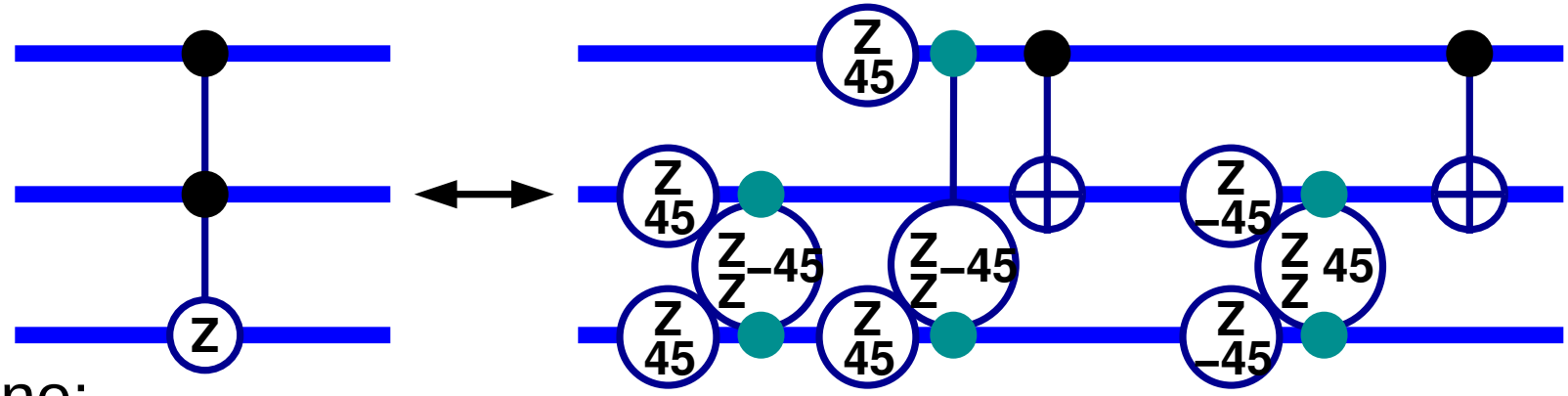
$$\begin{aligned}\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\ &= e^{\frac{i\pi}{8}\mathbb{1}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\ &\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}}e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}\end{aligned}$$



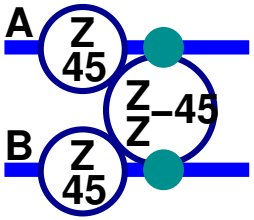
Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

$$\begin{aligned}\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\ &= e^{\frac{i\pi}{8}\mathbb{1}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\ &\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}}e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}\end{aligned}$$



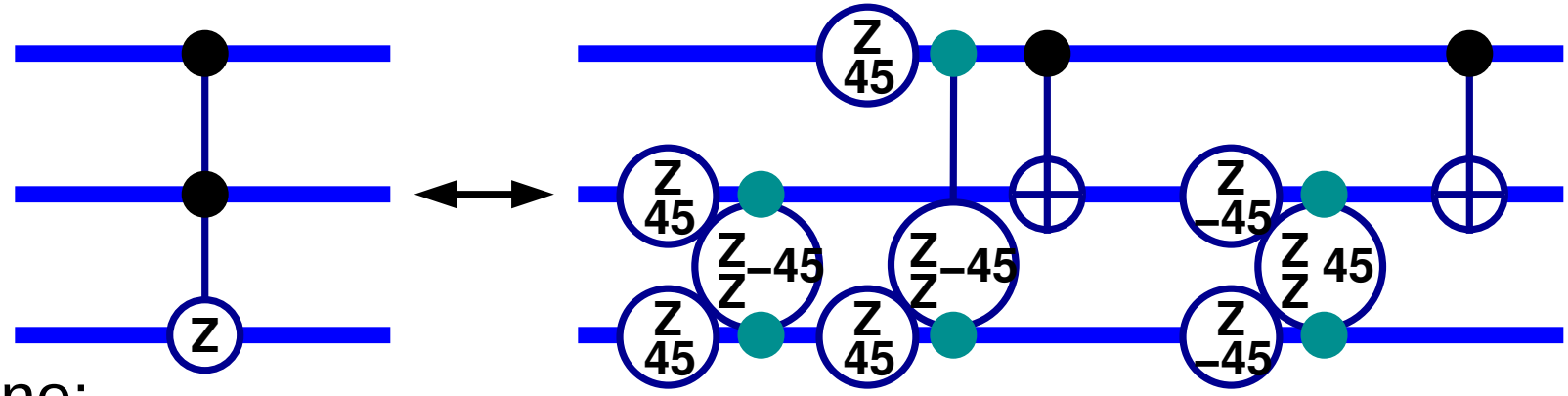
Examine:



Controlled Sign Flip Implementations

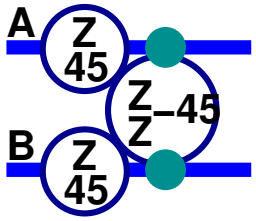
- Decomposition of $\mathbf{c^2sgn}$.

$$\begin{aligned}\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\ &= e^{\frac{i\pi}{8}\mathbb{1}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\ &\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}}e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}\end{aligned}$$



$$\exp\left(-\frac{i\pi}{8}Z^{(\mathsf{A})}-\frac{i\pi}{8}Z^{(\mathsf{B})}+\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}\right)$$

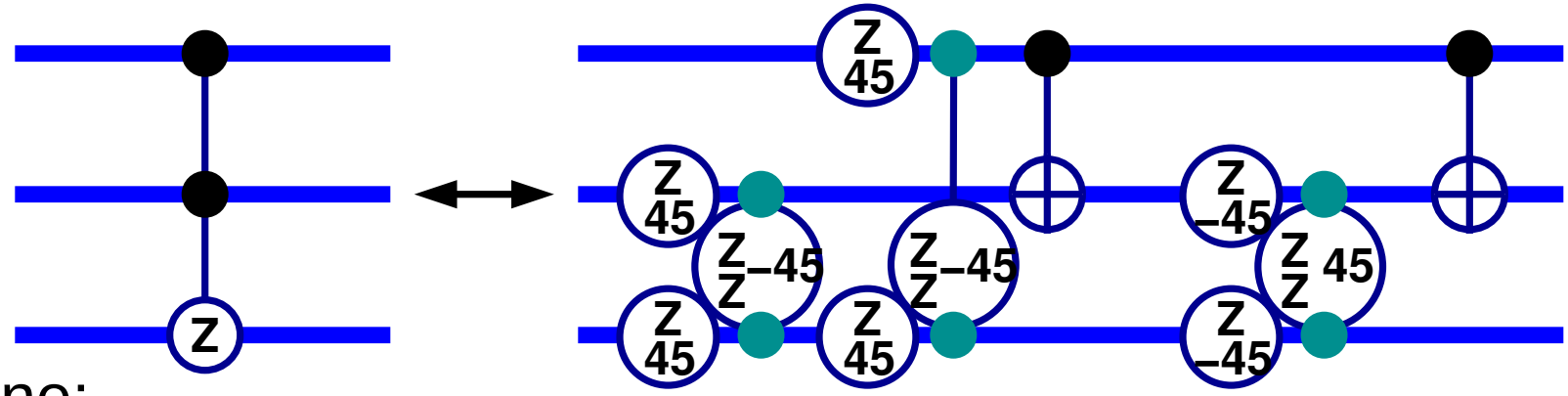
Examine:



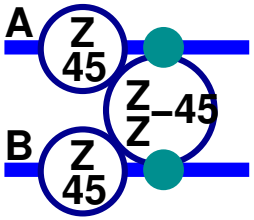
Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

$$\begin{aligned}\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\ &= e^{\frac{i\pi}{8}\mathbb{1}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\ &\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}}e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}\end{aligned}$$



Examine:

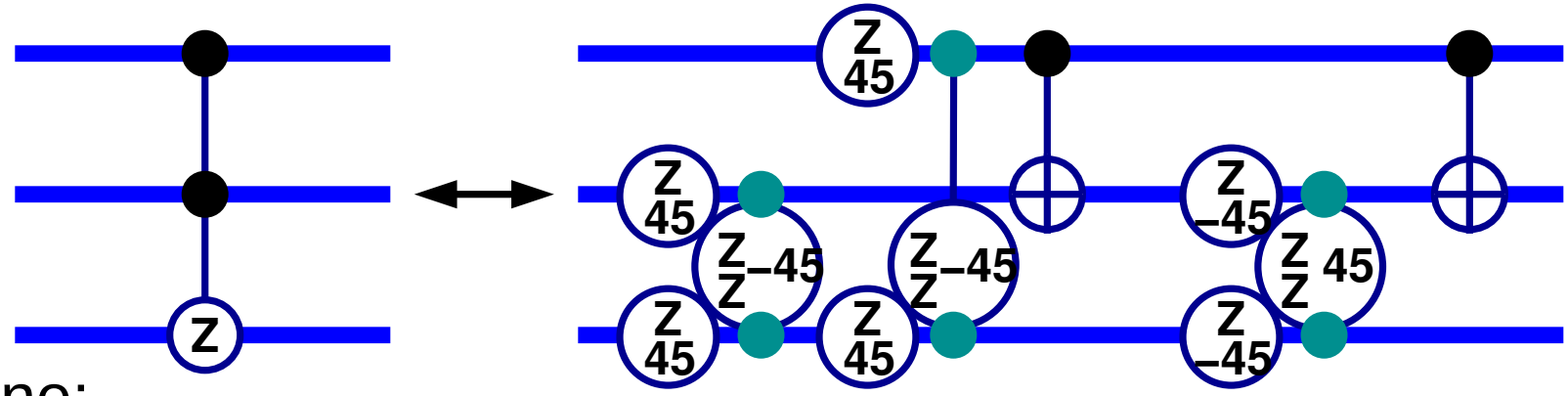


$$\begin{aligned}&\exp\left(-\frac{i\pi}{8}Z^{(\mathsf{A})}-\frac{i\pi}{8}Z^{(\mathsf{B})}+\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}\right) \\ &= \exp\left(-\frac{i\pi}{8}\right)\exp\left(\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\right)\end{aligned}$$

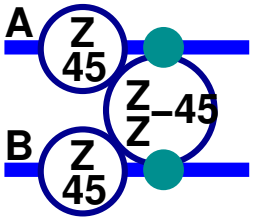
Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

$$\begin{aligned}\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\ &= e^{\frac{i\pi}{8}\mathbb{1}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\ &\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}}e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}\end{aligned}$$



Examine:

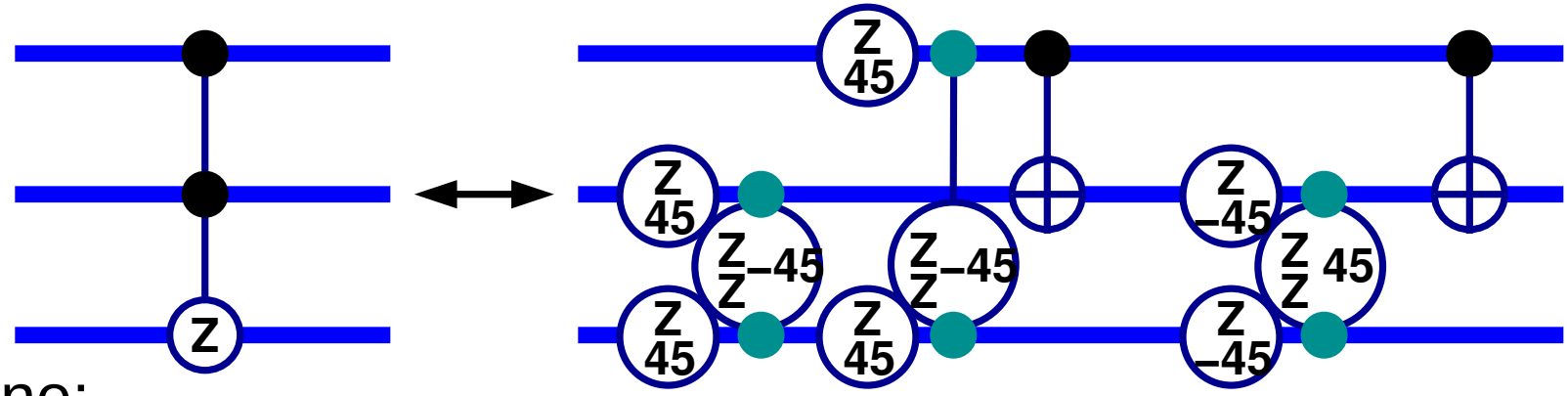


$$\begin{aligned}&\exp\left(-\frac{i\pi}{8}Z^{(\mathsf{A})}-\frac{i\pi}{8}Z^{(\mathsf{B})}+\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}\right) \\ &= \exp\left(-\frac{i\pi}{8}\right)\exp\left(\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\right) \\ &\propto |0\rangle_{\mathsf{A}}^{\mathsf{A}}\langle 0| + |1\rangle_{\mathsf{A}}^{\mathsf{A}}\langle 1|\left(|0\rangle_{\mathsf{B}}^{\mathsf{B}}\langle 0| + i|1\rangle_{\mathsf{B}}^{\mathsf{B}}\langle 1|\right)\end{aligned}$$

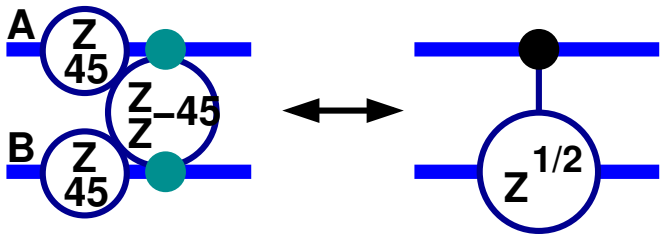
Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

$$\begin{aligned}\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\ &= e^{\frac{i\pi}{8}\mathbb{1}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\ &\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}}e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}\end{aligned}$$



Examine:

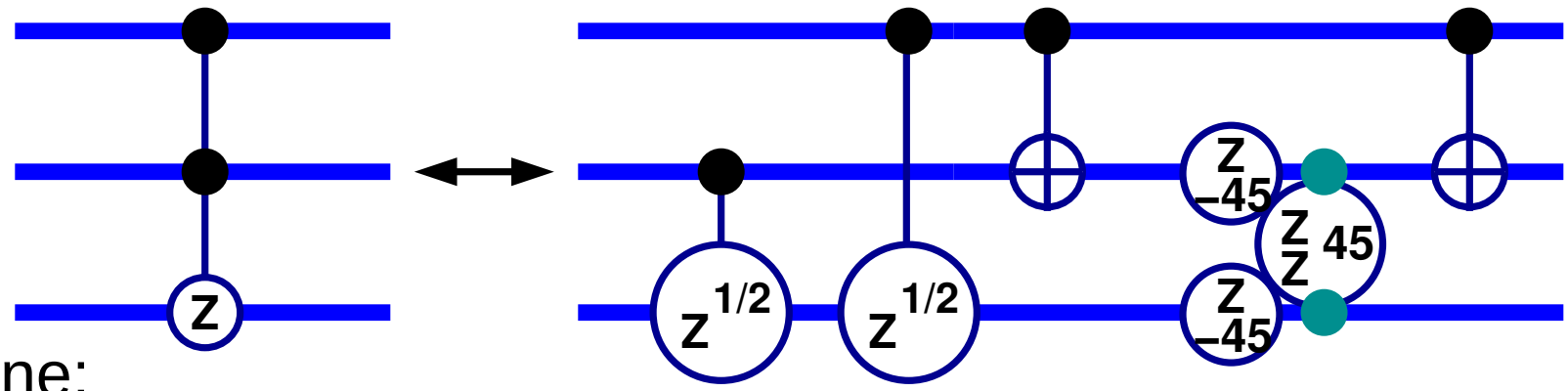


$$\begin{aligned}&\exp\left(-\frac{i\pi}{8}Z^{(\mathsf{A})}-\frac{i\pi}{8}Z^{(\mathsf{B})}+\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}\right) \\ &= \exp\left(-\frac{i\pi}{8}\right)\exp\left(\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\right) \\ &\propto |0\rangle_{\mathsf{A}}^{\mathsf{A}}\langle 0| + |1\rangle_{\mathsf{A}}^{\mathsf{A}}\langle 1|\left(|0\rangle_{\mathsf{B}}^{\mathsf{B}}\langle 0| + i|1\rangle_{\mathsf{B}}^{\mathsf{B}}\langle 1|\right)\end{aligned}$$

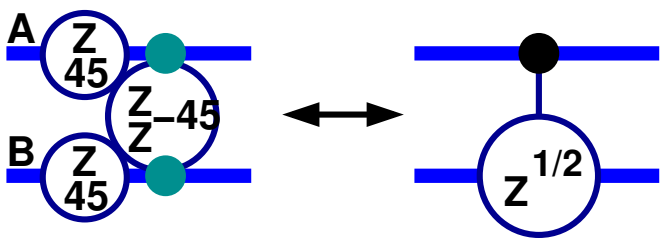
Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

$$\begin{aligned}\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\ &= e^{\frac{i\pi}{8}\mathbb{1}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\ &\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}}e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}\end{aligned}$$



Examine:

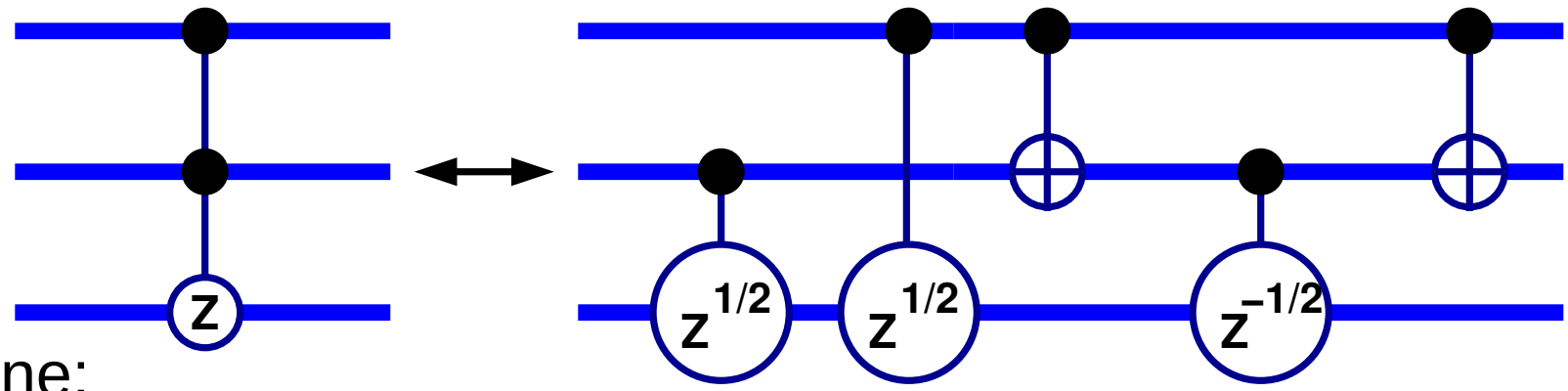


$$\begin{aligned}&\exp\left(-\frac{i\pi}{8}Z^{(\mathsf{A})}-\frac{i\pi}{8}Z^{(\mathsf{B})}+\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}\right) \\ &= \exp\left(-\frac{i\pi}{8}\right)\exp\left(\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\right) \\ &\propto |0\rangle_{\mathsf{A}}^{\mathsf{A}}\langle 0| + |1\rangle_{\mathsf{A}}^{\mathsf{A}}\langle 1|\left(|0\rangle_{\mathsf{B}}^{\mathsf{B}}\langle 0| + i|1\rangle_{\mathsf{B}}^{\mathsf{B}}\langle 1|\right)\end{aligned}$$

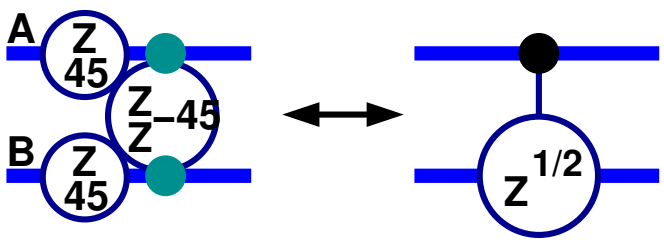
Controlled Sign Flip Implementations

- Decomposition of $\mathbf{c^2sgn}$.

$$\begin{aligned}\mathbf{c^2sgn}^{(\mathsf{ABC})} &= e^{\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\left(\mathbb{1}-Z^{(\mathsf{C})}\right)} \\ &= e^{\frac{i\pi}{8}\mathbb{1}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{B})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{C})}} \\ &\quad e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}}e^{\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{C})}}e^{\frac{i\pi}{8}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}e^{-\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}Z^{(\mathsf{C})}}\end{aligned}$$



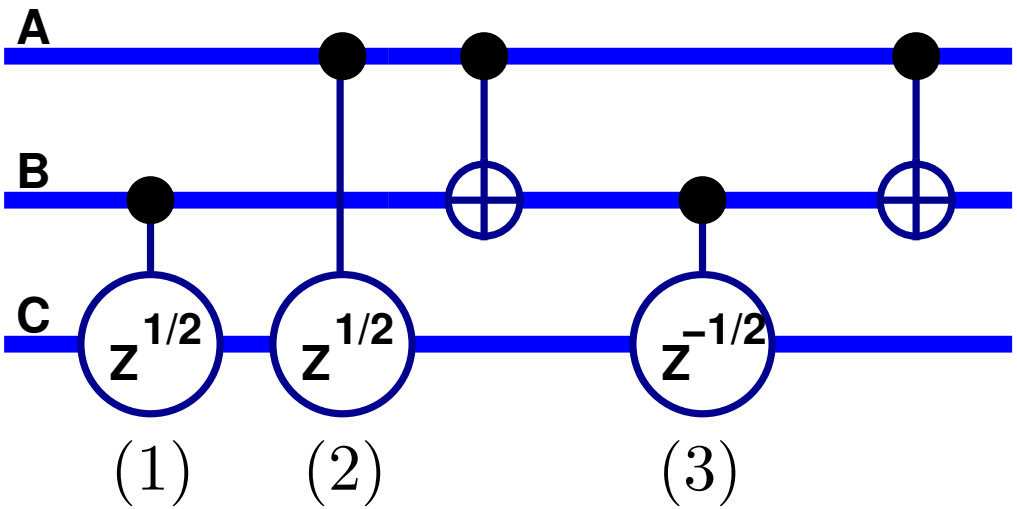
Examine:



$$\begin{aligned}&\exp\left(-\frac{i\pi}{8}Z^{(\mathsf{A})}-\frac{i\pi}{8}Z^{(\mathsf{B})}+\frac{i\pi}{8}Z^{(\mathsf{A})}Z^{(\mathsf{B})}\right) \\ &= \exp\left(-\frac{i\pi}{8}\right)\exp\left(\frac{i\pi}{8}\left(\mathbb{1}-Z^{(\mathsf{A})}\right)\left(\mathbb{1}-Z^{(\mathsf{B})}\right)\right) \\ &\propto |0\rangle_{\mathsf{A}}^{\mathsf{A}}\langle 0| + |1\rangle_{\mathsf{A}}^{\mathsf{A}}\langle 1|\left(|0\rangle_{\mathsf{B}}^{\mathsf{B}}\langle 0| + i|1\rangle_{\mathsf{B}}^{\mathsf{B}}\langle 1|\right)\end{aligned}$$

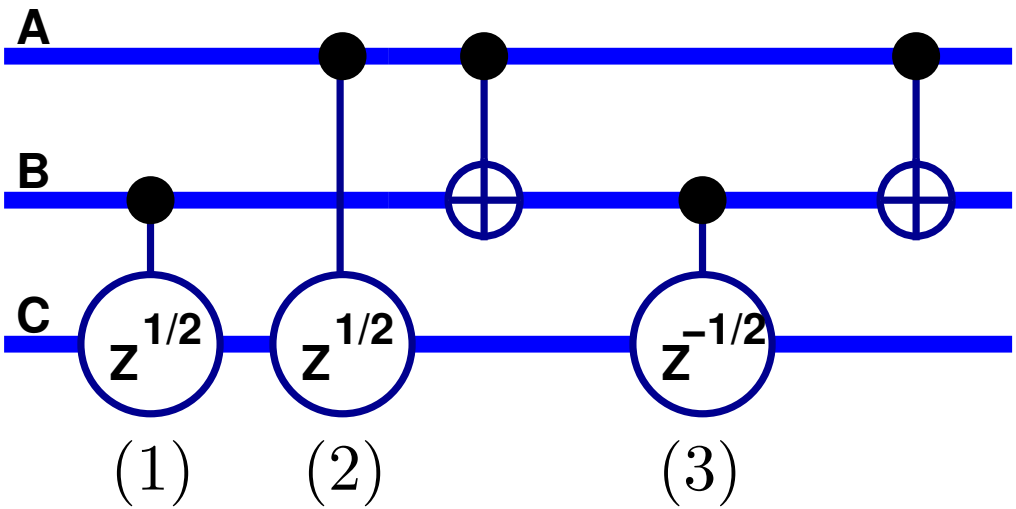
Controlled^2 Unitary

- Generalizing the controlled^2 Z implementation.



Controlled^2 Unitary

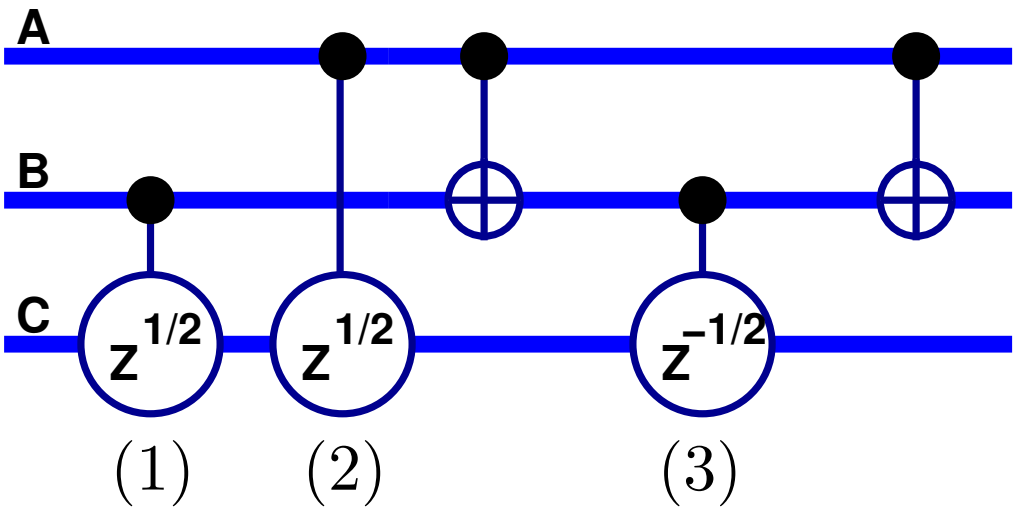
- Generalizing the controlled^2 Z implementation.



		(1)	(2)	(3)
$\lvert 00\rangle_{AB}$	:	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$

Controlled^2 Unitary

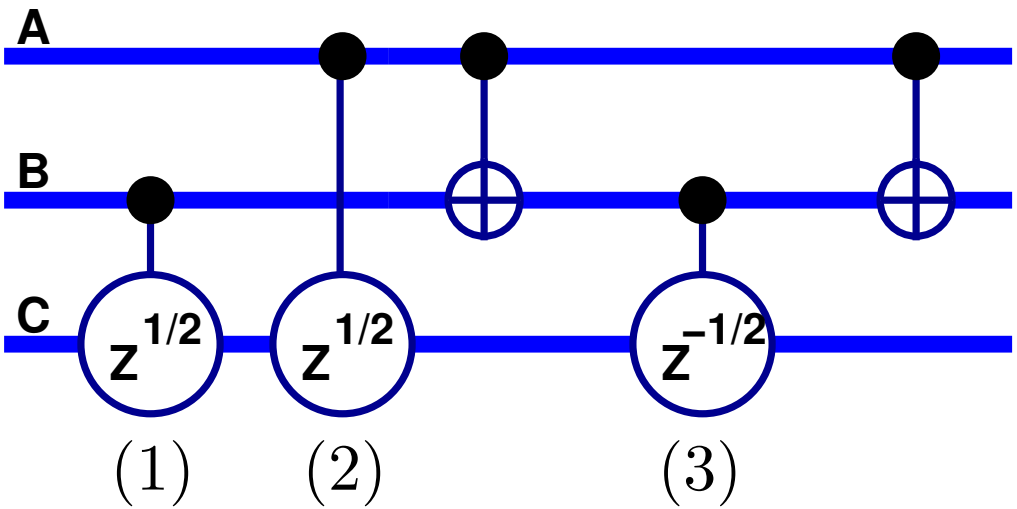
- Generalizing the controlled^2 Z implementation.



		(1)	(2)	(3)
$\lvert 00\rangle_{AB}$	:	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$
$\lvert 01\rangle_{AB}$	:	$Z^{1/2}$	$\mathbb{1}$	$Z^{-1/2}$

Controlled^2 Unitary

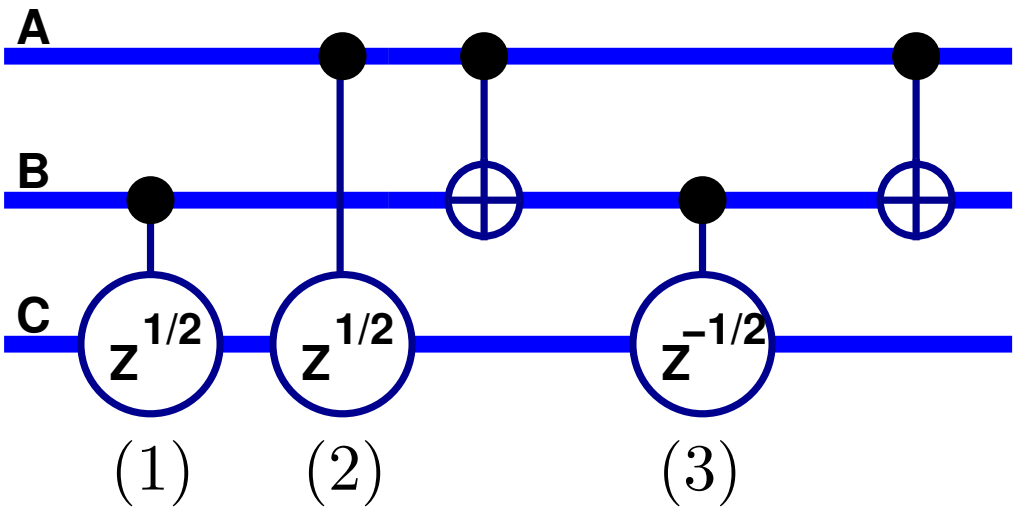
- Generalizing the controlled^2 Z implementation.



		(1)	(2)	(3)
$\lvert 00\rangle_{AB}$	:	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$
$\lvert 01\rangle_{AB}$	:	$Z^{1/2}$	$\mathbb{1}$	$Z^{-1/2}$
$\lvert 10\rangle_{AB}$	:	$\mathbb{1}$	$Z^{1/2}$	$Z^{-1/2}$

Controlled^2 Unitary

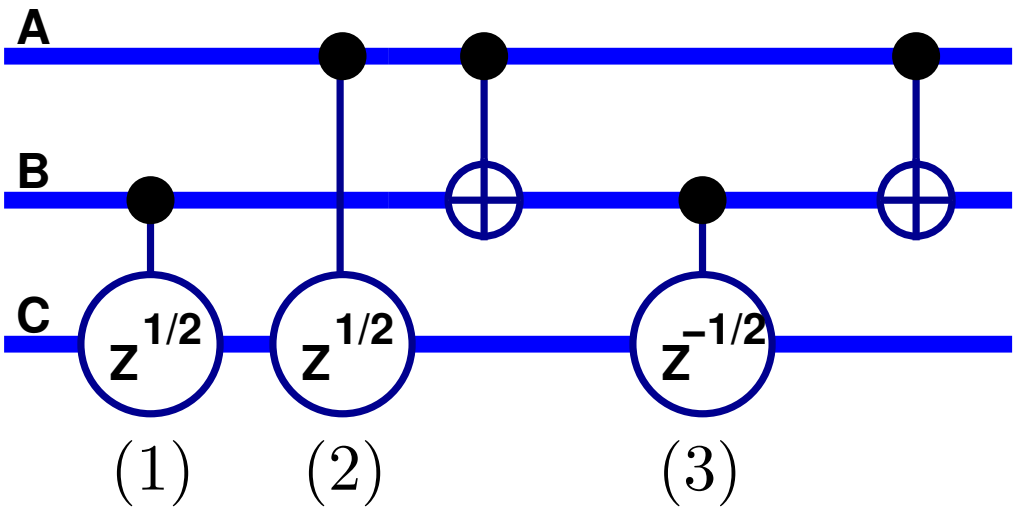
- Generalizing the controlled^2 Z implementation.



		(1)	(2)	(3)
$\lvert 00\rangle_{AB}$	:	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$
$\lvert 01\rangle_{AB}$	:	$Z^{1/2}$	$\mathbb{1}$	$Z^{-1/2}$
$\lvert 10\rangle_{AB}$	:	$\mathbb{1}$	$Z^{1/2}$	$Z^{-1/2}$
$\lvert 11\rangle_{AB}$	:	$Z^{1/2}$	$Z^{1/2}$	$\mathbb{1}$

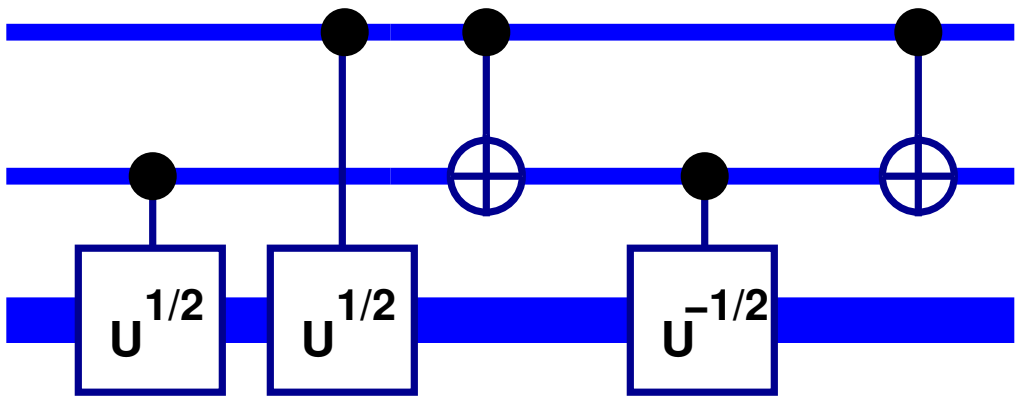
Controlled^2 Unitary

- Generalizing the controlled^2 Z implementation.



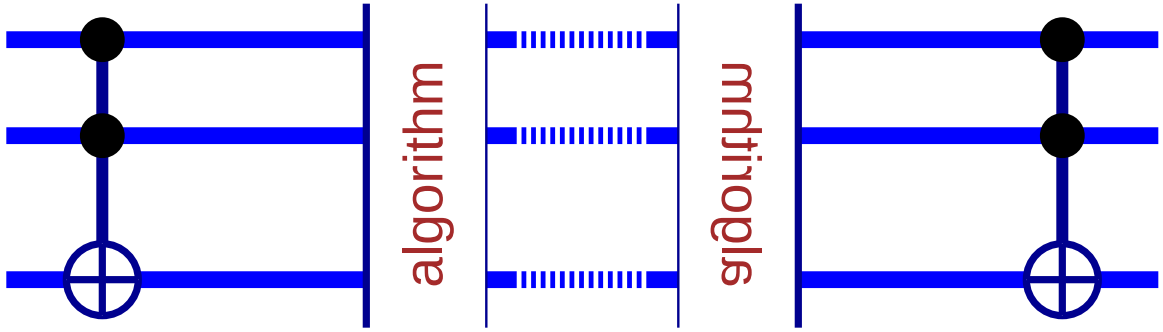
		(1)	(2)	(3)
$\lvert 00\rangle_{AB}$	:	$\mathbb{1}$	$\mathbb{1}$	$\mathbb{1}$
$\lvert 01\rangle_{AB}$	:	$Z^{1/2}$	$\mathbb{1}$	$Z^{-1/2}$
$\lvert 10\rangle_{AB}$	:	$\mathbb{1}$	$Z^{1/2}$	$Z^{-1/2}$
$\lvert 11\rangle_{AB}$	:	$Z^{1/2}$	$Z^{1/2}$	$\mathbb{1}$

- Same for a unitary U with controlled-$U^{\pm 1/2}$ implementations.



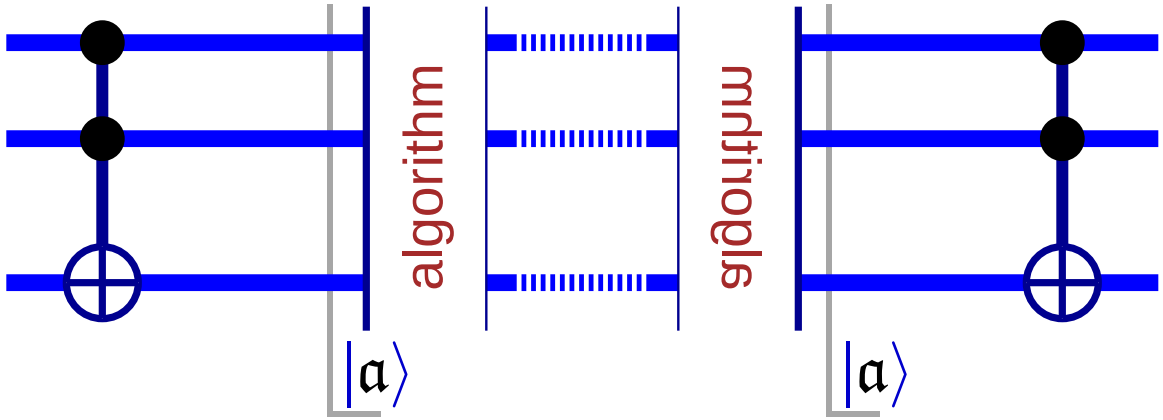
Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.



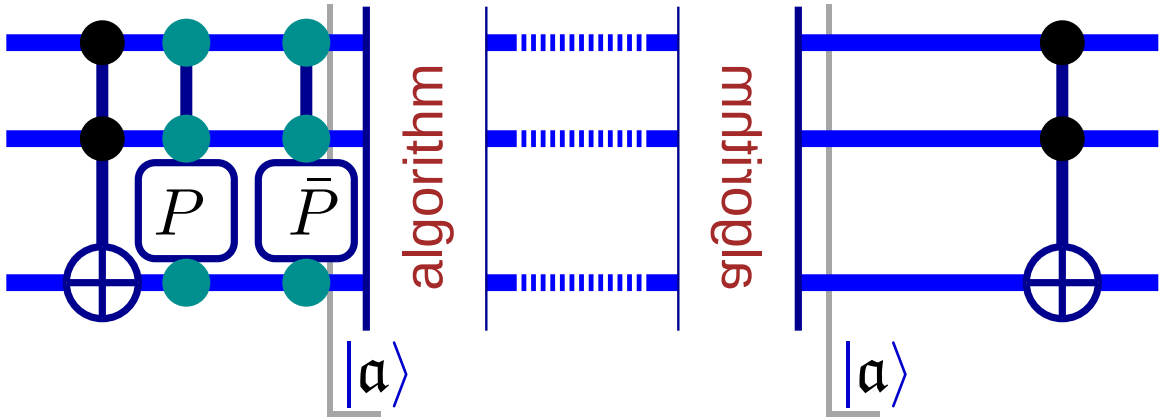
Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.



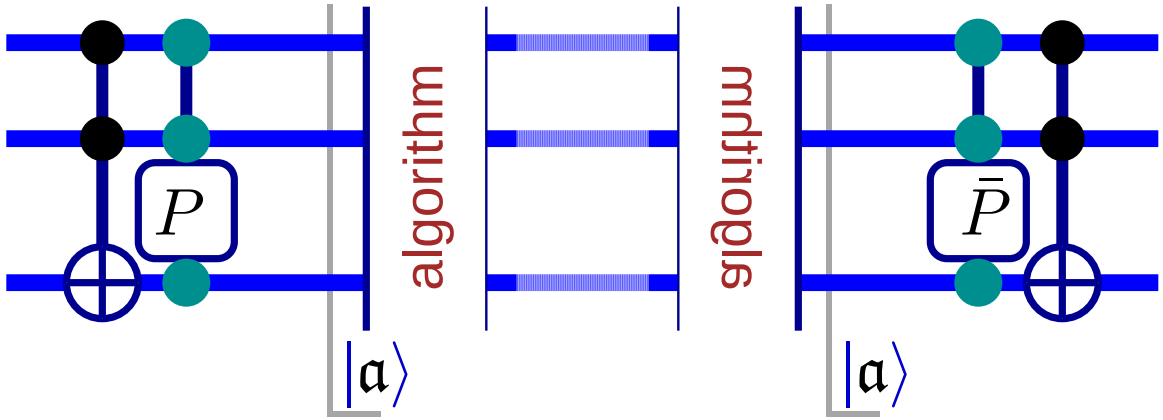
Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.



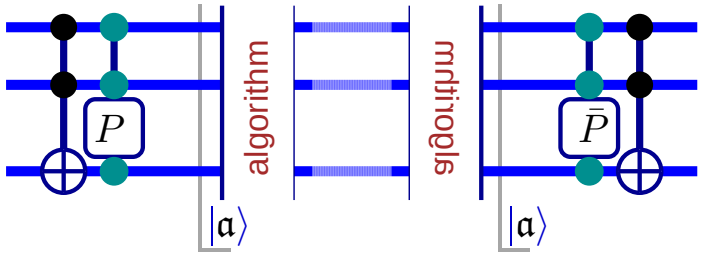
Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.



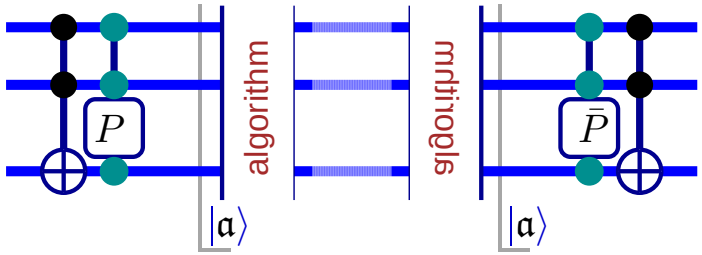
Toffoli Gate up to Control Phases

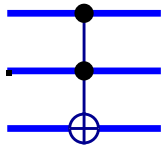
- Toffoli gates often come in reversing pairs.



Toffoli Gate up to Control Phases

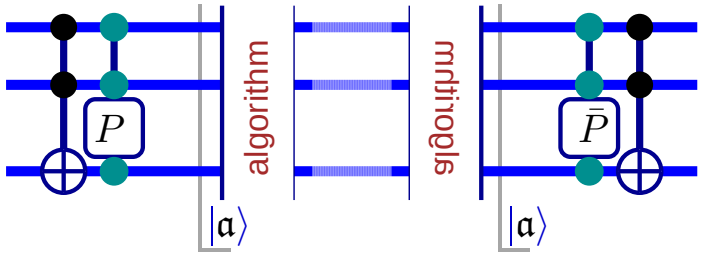
- Toffoli gates often come in reversing pairs.

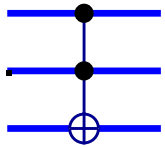


Ok to have logical phases in 

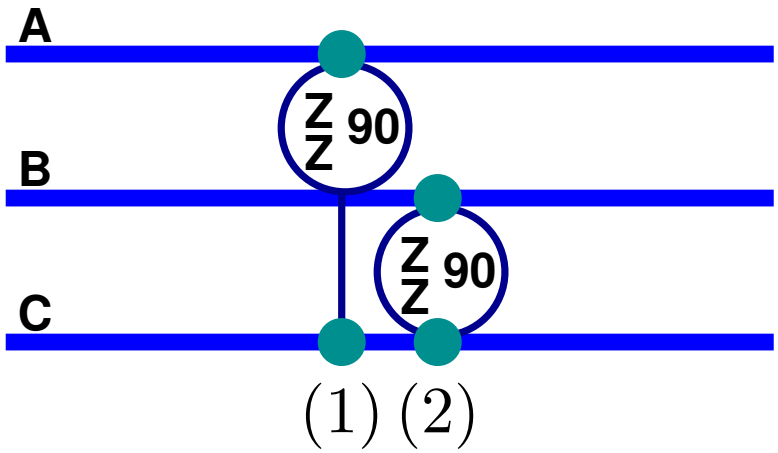
Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.



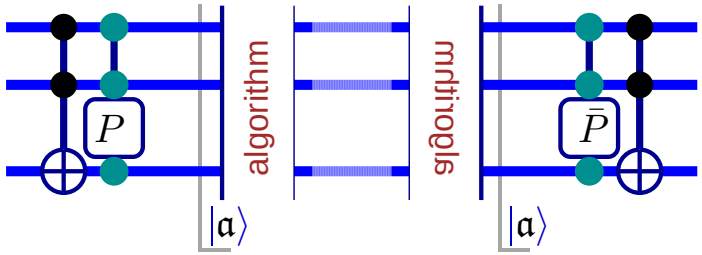
Ok to have logical phases in 

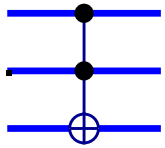
- Consider $e^{-\frac{i\pi}{8}Z^{(A)}Z^{(C)}}e^{-\frac{i\pi}{8}Z^{(B)}Z^{(C)}}$ as AB-controlled:



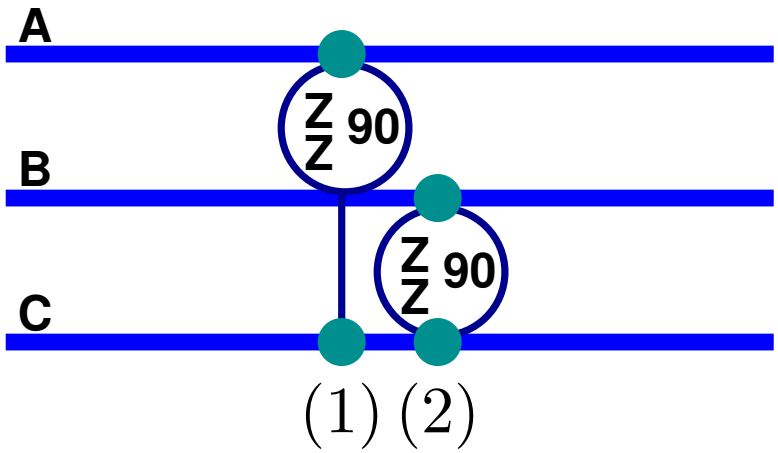
Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.

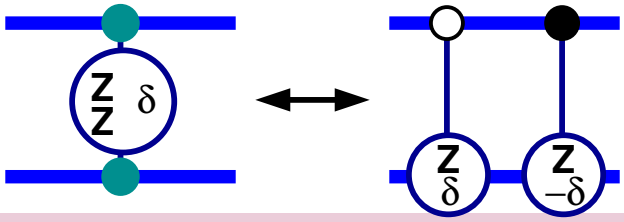


Ok to have logical phases in 

- Consider $e^{-\frac{i\pi}{8}Z^{(A)}Z^{(C)}}e^{-\frac{i\pi}{8}Z^{(B)}Z^{(C)}}$ as AB-controlled:

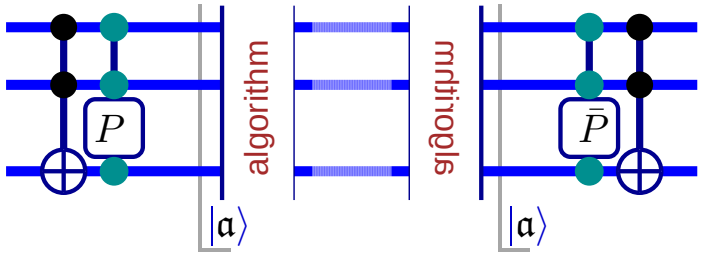


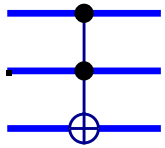
$$\left.\begin{aligned}&\exp\left(-\frac{i\delta}{2}Z^{(1)}Z^{(2)}\right)=\\&\exp\left(-\frac{i\delta}{2}\left(|0\rangle_1\langle 0|Z^{(2)}-|1\rangle_1\langle 1|Z^{(2)}\right)\right)\end{aligned}\right\}$$



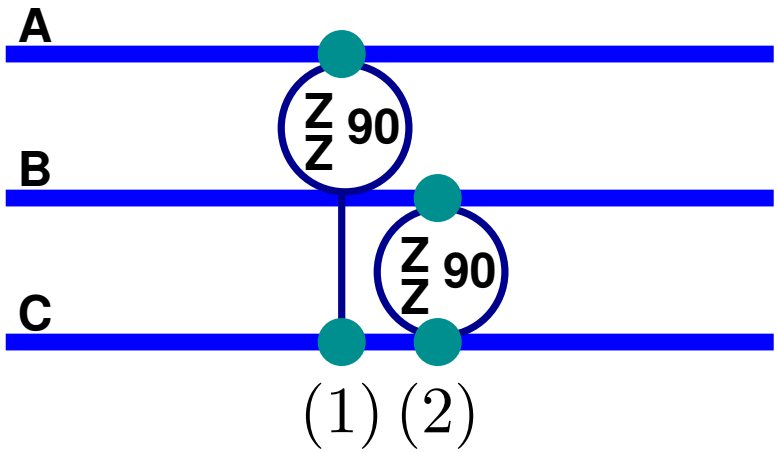
Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.



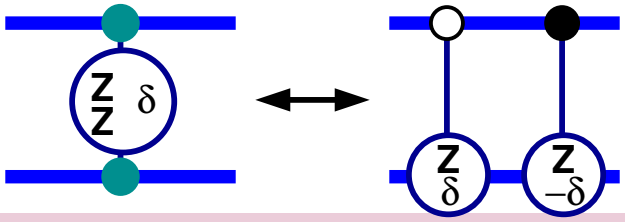
Ok to have logical phases in 

- Consider $e^{-\frac{i\pi}{8}Z^{(A)}Z^{(C)}}\,e^{-\frac{i\pi}{8}Z^{(B)}Z^{(C)}}$ as AB-controlled:



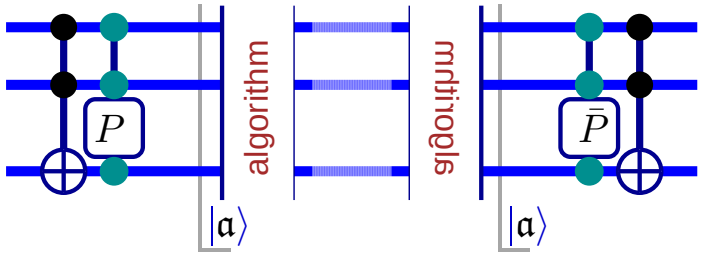
		(1)	(2)		
$\lvert 00\rangle_{AB}$	:	$\mathbf{Z}_{90^\circ}$	$\mathbf{Z}_{90^\circ}$	$=$	$\mathbf{Z}_{180^\circ}$

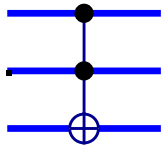
$$\left.\begin{aligned}&\exp\left(-\frac{i\delta}{2}Z^{(1)}Z^{(2)}\right)=\\&\exp\left(-\frac{i\delta}{2}\left(\lvert 0\rangle_1^1\langle 0\rvert Z^{(2)}-\lvert 1\rangle_1^1\langle 1\rvert Z^{(2)}\right)\right)\end{aligned}\right\}$$



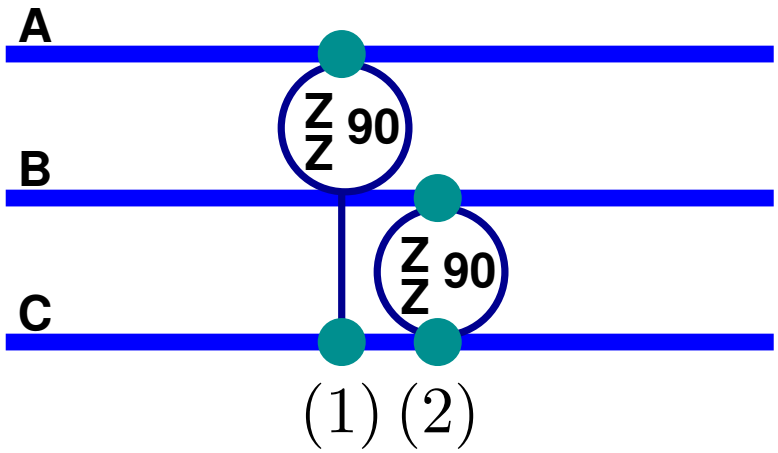
Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.



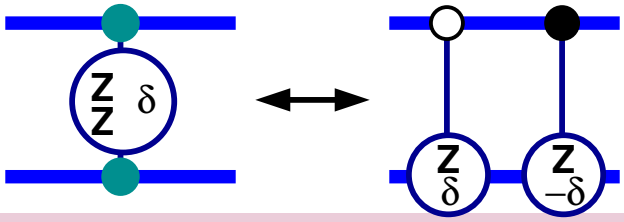
Ok to have logical phases in 

- Consider $e^{-\frac{i\pi}{8}Z^{(A)}Z^{(C)}}\,e^{-\frac{i\pi}{8}Z^{(B)}Z^{(C)}}$ as AB-controlled:



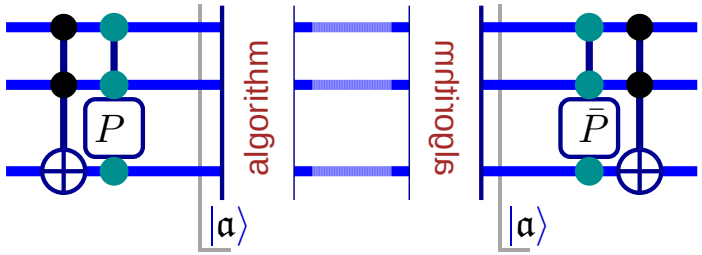
		(1)	(2)		
$\lvert 00\rangle_{AB}$	:	$\mathbf{Z}_{90^\circ}$	$\mathbf{Z}_{90^\circ}$	$=$	$\mathbf{Z}_{180^\circ}$
$\lvert 01\rangle_{AB}$	:	$\mathbf{Z}_{90^\circ}$	$\mathbf{Z}_{-90^\circ}$	$=$	$\mathbb{1}$

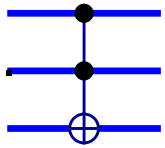
$$\left.\begin{aligned}&\exp\left(-\frac{i\delta}{2}Z^{(1)}Z^{(2)}\right)=\\&\exp\left(-\frac{i\delta}{2}\left(\lvert 0\rangle_1^1\langle 0\rvert Z^{(2)}-\lvert 1\rangle_1^1\langle 1\rvert Z^{(2)}\right)\right)\end{aligned}\right\}$$



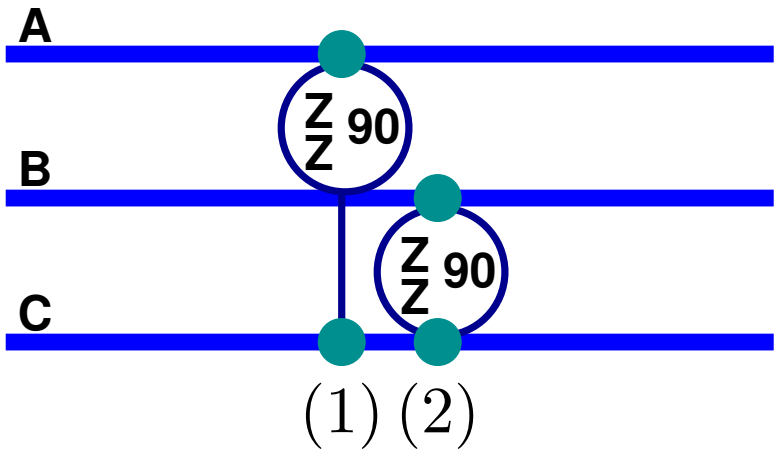
Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.



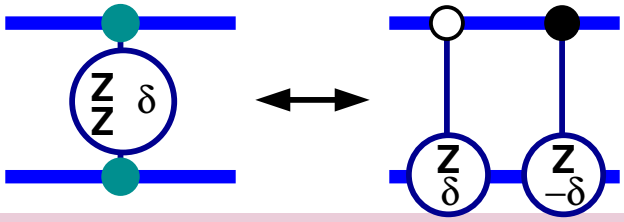
Ok to have logical phases in 

- Consider $e^{-\frac{i\pi}{8}Z^{(A)}Z^{(C)}}\,e^{-\frac{i\pi}{8}Z^{(B)}Z^{(C)}}$ as AB-controlled:



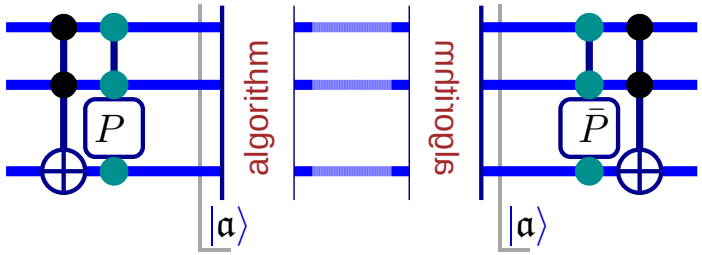
		(1)	(2)		
$\lvert 00\rangle_{AB}$	:	$\mathbf{Z}_{90^\circ}$	$\mathbf{Z}_{90^\circ}$	$=$	$\mathbf{Z}_{180^\circ}$
$\lvert 01\rangle_{AB}$	:	$\mathbf{Z}_{90^\circ}$	$\mathbf{Z}_{-90^\circ}$	$=$	$\mathbb{1}$
$\lvert 10\rangle_{AB}$	:	$\mathbf{Z}_{-90^\circ}$	$\mathbf{Z}_{90^\circ}$	$=$	$\mathbb{1}$

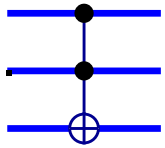
$$\left.\begin{aligned}&\exp\left(-\frac{i\delta}{2}Z^{(1)}Z^{(2)}\right)=\\&\exp\left(-\frac{i\delta}{2}\left(|0\rangle_1^1\langle 0|Z^{(2)}-|1\rangle_1^1\langle 1|Z^{(2)}\right)\right)\end{aligned}\right\}$$



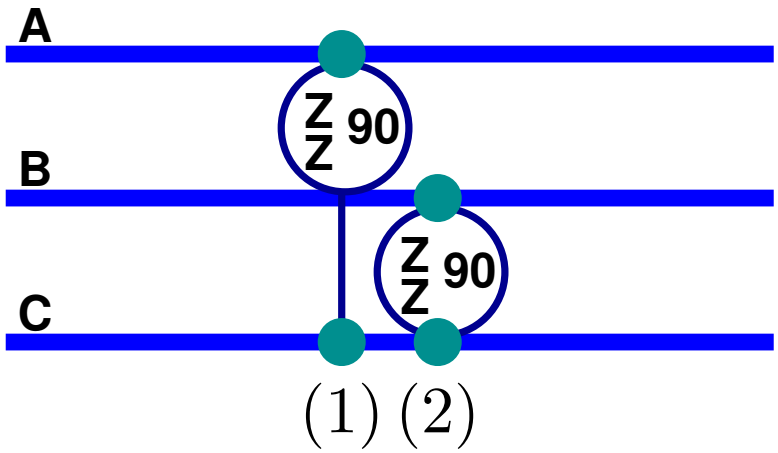
Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.



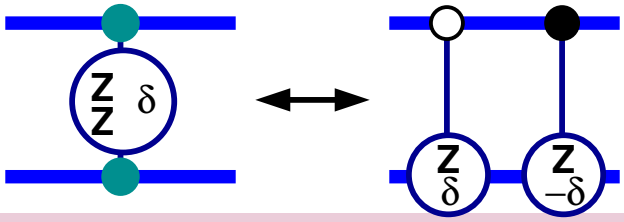
Ok to have logical phases in 

- Consider $e^{-\frac{i\pi}{8}Z^{(A)}Z^{(C)}}\,e^{-\frac{i\pi}{8}Z^{(B)}Z^{(C)}}$ as AB-controlled:



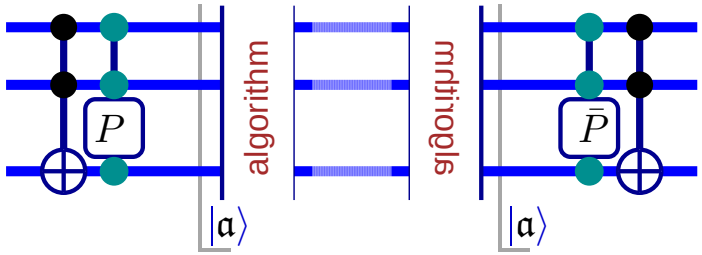
		(1)	(2)		
$\lvert 00\rangle_{AB}$	:	$\mathbf{Z}_{90^\circ}$	$\mathbf{Z}_{90^\circ}$	$=$	$\mathbf{Z}_{180^\circ}$
$\lvert 01\rangle_{AB}$	:	$\mathbf{Z}_{90^\circ}$	$\mathbf{Z}_{-90^\circ}$	$=$	$\mathbb{1}$
$\lvert 10\rangle_{AB}$	:	$\mathbf{Z}_{-90^\circ}$	$\mathbf{Z}_{90^\circ}$	$=$	$\mathbb{1}$
$\lvert 11\rangle_{AB}$	:	$\mathbf{Z}_{-90^\circ}$	$\mathbf{Z}_{-90^\circ}$	$=$	$\mathbf{Z}_{-180^\circ}$

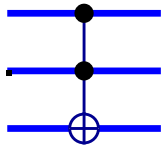
$$\left.\begin{aligned}&\exp\left(-\frac{i\delta}{2}Z^{(1)}Z^{(2)}\right)=\\&\exp\left(-\frac{i\delta}{2}\left(\lvert 0\rangle_1^1\langle 0\rvert Z^{(2)}-\lvert 1\rangle_1^1\langle 1\rvert Z^{(2)}\right)\right)\end{aligned}\right\}$$



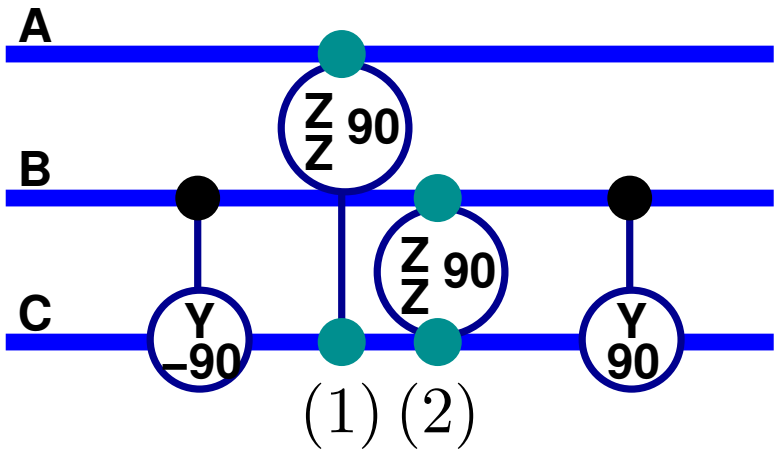
Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.



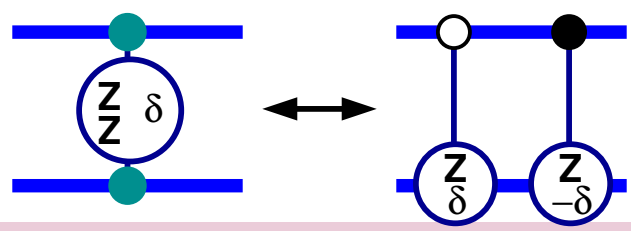
Ok to have logical phases in 

- Consider $e^{-\frac{i\pi}{8}Z^{(A)}Z^{(C)}}\,e^{-\frac{i\pi}{8}Z^{(B)}Z^{(C)}}$ as AB-controlled:



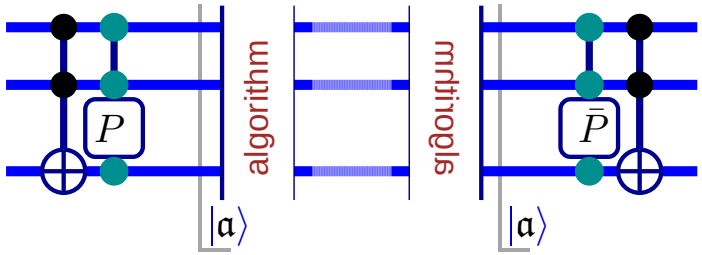
		(1)	(2)		
$\lvert 00\rangle_{AB}$	:	$\mathbf{Z}_{90^\circ}$	$\mathbf{Z}_{90^\circ}$	$\longrightarrow$	$\mathbf{Z}_{180^\circ}$
$\lvert 01\rangle_{AB}$	:	$\mathbf{Z}_{90^\circ}$	$\mathbf{Z}_{-90^\circ}$	$\longrightarrow$	$\mathbb{1}$
$\lvert 10\rangle_{AB}$	:	$\mathbf{Z}_{-90^\circ}$	$\mathbf{Z}_{90^\circ}$	$\longrightarrow$	$\mathbb{1}$
$\lvert 11\rangle_{AB}$	:	$\mathbf{Z}_{-90^\circ}$	$\mathbf{Z}_{-90^\circ}$	$\longrightarrow$	$\mathbf{X}_{-180^\circ}$

$$\left.\begin{aligned}&\exp\left(-\frac{i\delta}{2}Z^{(1)}Z^{(2)}\right)=\\&\exp\left(-\frac{i\delta}{2}\left(|0\rangle_1^1\langle 0|Z^{(2)}-|1\rangle_1^1\langle 1|Z^{(2)}\right)\right)\end{aligned}\right\}$$

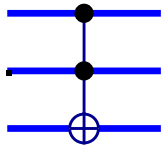


Toffoli Gate up to Control Phases

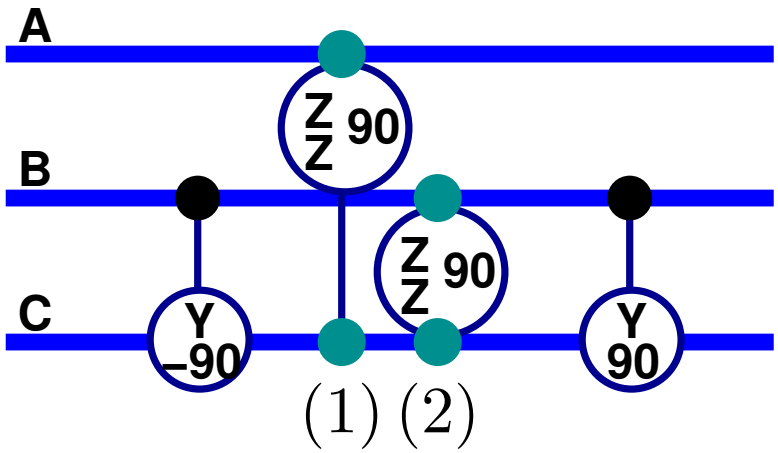
- Toffoli gates often come in reversing pairs.



Ok to have logical phases in

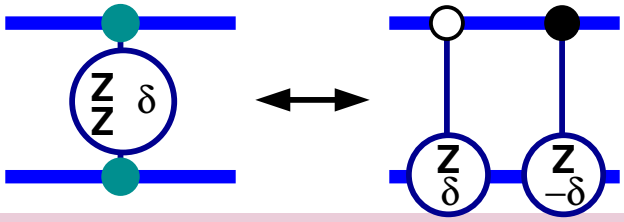


- Consider $e^{-\frac{i\pi}{8}Z^{(A)}Z^{(C)}}\,e^{-\frac{i\pi}{8}Z^{(B)}Z^{(C)}}$ as AB-controlled:



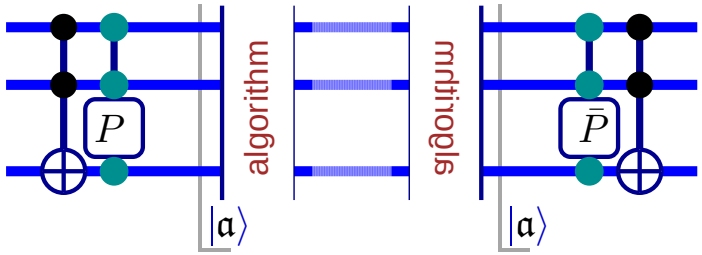
		(1)	(2)		
$\lvert 00\rangle_{AB}$	:	$\mathbf{Z}_{90^\circ}$	$\mathbf{Z}_{90^\circ}$	$\rightarrow$	$\mathbf{Z}_{180^\circ}$
$\lvert 01\rangle_{AB}$	:	$\mathbf{Z}_{90^\circ}$	$\mathbf{Z}_{-90^\circ}$	$\rightarrow$	$\mathbb{1}$
$\lvert 10\rangle_{AB}$	:	$\mathbf{Z}_{-90^\circ}$	$\mathbf{Z}_{90^\circ}$	$\rightarrow$	$\mathbb{1}$
$\lvert 11\rangle_{AB}$	:	$\mathbf{Z}_{-90^\circ}$	$\mathbf{Z}_{-90^\circ}$	$\rightarrow$	$\mathbf{X}_{-180^\circ}$

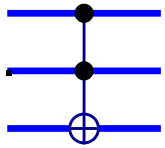
$$\left.\begin{aligned}&\exp\left(-\frac{i\delta}{2}Z^{(1)}Z^{(2)}\right)=\\&\exp\left(-\frac{i\delta}{2}\left(|0\rangle_1^1\langle 0|Z^{(2)}-|1\rangle_1^1\langle 1|Z^{(2)}\right)\right)\end{aligned}\right\}$$



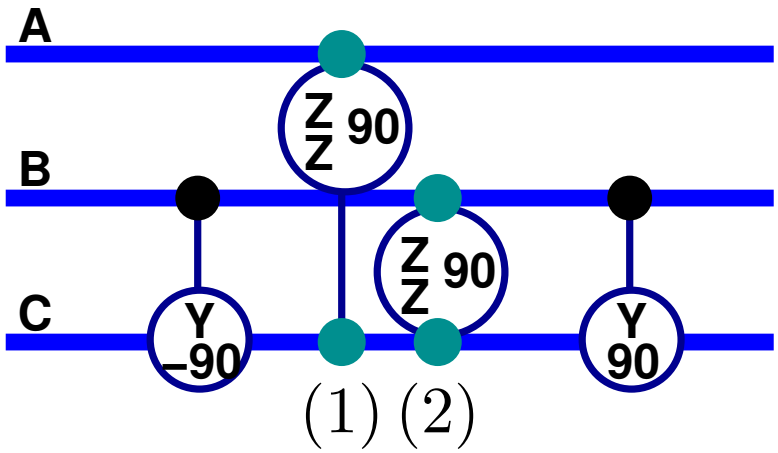
Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.

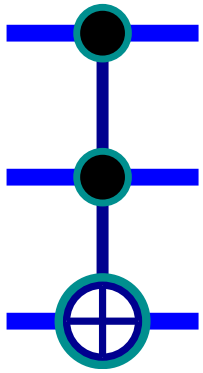


Ok to have logical phases in 

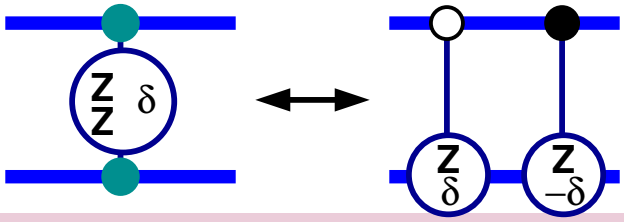
- Consider $e^{-\frac{i\pi}{8}Z^{(A)}Z^{(C)}}\,e^{-\frac{i\pi}{8}Z^{(B)}Z^{(C)}}$ as AB-controlled:



		(1)	(2)		
$\lvert 00\rangle_{AB}$	:	$\mathbf{Z}_{90^\circ}$	$\mathbf{Z}_{90^\circ}$	$\rightarrow$	$\mathbf{Z}_{180^\circ}$
$\lvert 01\rangle_{AB}$	:	$\mathbf{Z}_{90^\circ}$	$\mathbf{Z}_{-90^\circ}$	$\rightarrow$	$\mathbb{1}$
$\lvert 10\rangle_{AB}$	:	$\mathbf{Z}_{-90^\circ}$	$\mathbf{Z}_{90^\circ}$	$\rightarrow$	$\mathbb{1}$
$\lvert 11\rangle_{AB}$	:	$\mathbf{Z}_{-90^\circ}$	$\mathbf{Z}_{-90^\circ}$	$\rightarrow$	$\mathbf{X}_{-180^\circ}$

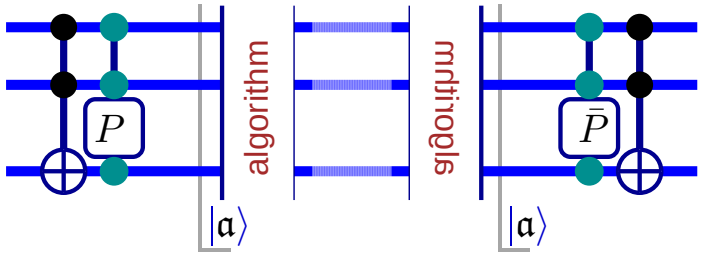


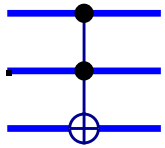
$$\left.\begin{aligned}&\exp\left(-\frac{i\delta}{2}Z^{(1)}Z^{(2)}\right)=\\&\exp\left(-\frac{i\delta}{2}\left(|0\rangle_1^1\langle 0|Z^{(2)}-|1\rangle_1^1\langle 1|Z^{(2)}\right)\right)\end{aligned}\right\}$$



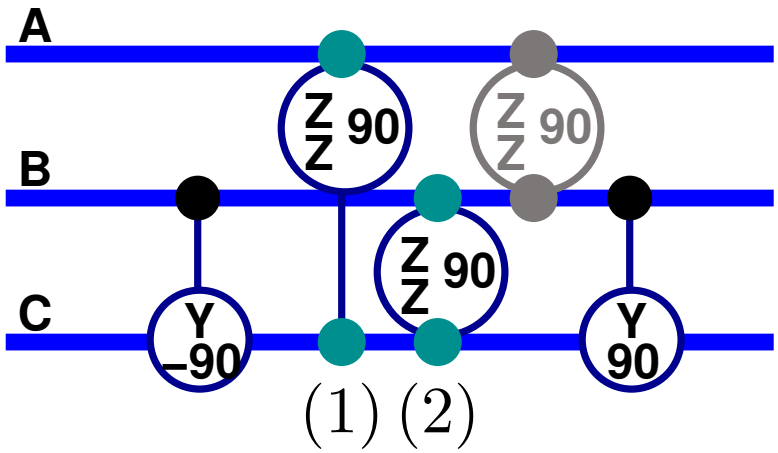
Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.

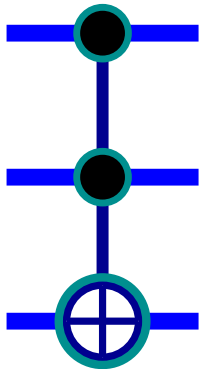


Ok to have logical phases in 

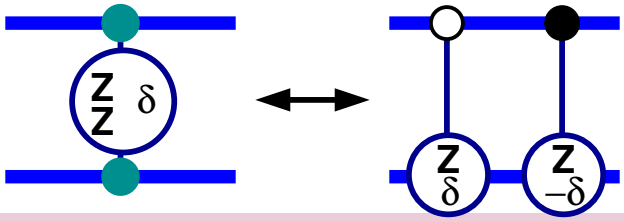
- Consider $e^{-\frac{i\pi}{8}Z^{(A)}Z^{(C)}}\,e^{-\frac{i\pi}{8}Z^{(B)}Z^{(C)}}$ as AB-controlled:



		(1)	(2)		
$\lvert 00\rangle_{AB}$	:	$\mathbf{Z}_{90^\circ}$	$\mathbf{Z}_{90^\circ}$	$\rightarrow$	$\mathbf{Z}_{180^\circ}$
$\lvert 01\rangle_{AB}$	:	$\mathbf{Z}_{90^\circ}$	$\mathbf{Z}_{-90^\circ}$	$\rightarrow$	$\mathbb{1}$
$\lvert 10\rangle_{AB}$	:	$\mathbf{Z}_{-90^\circ}$	$\mathbf{Z}_{90^\circ}$	$\rightarrow$	$\mathbb{1}$
$\lvert 11\rangle_{AB}$	:	$\mathbf{Z}_{-90^\circ}$	$\mathbf{Z}_{-90^\circ}$	$\rightarrow$	$\mathbf{X}_{-180^\circ}$

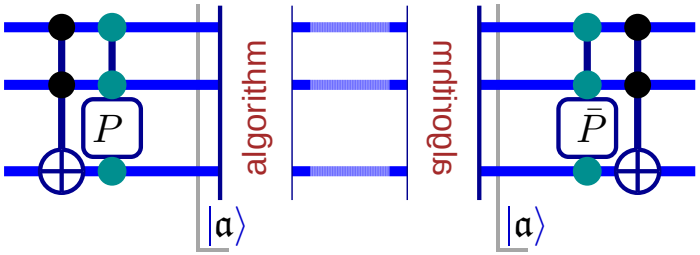


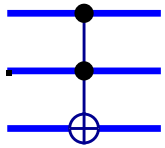
$$\left.\begin{aligned}&\exp\left(-\frac{i\delta}{2}Z^{(1)}Z^{(2)}\right)=\\&\exp\left(-\frac{i\delta}{2}\left(|0\rangle_1^1\langle 0|Z^{(2)}-|1\rangle_1^1\langle 1|Z^{(2)}\right)\right)\end{aligned}\right\}$$



Toffoli Gate up to Control Phases

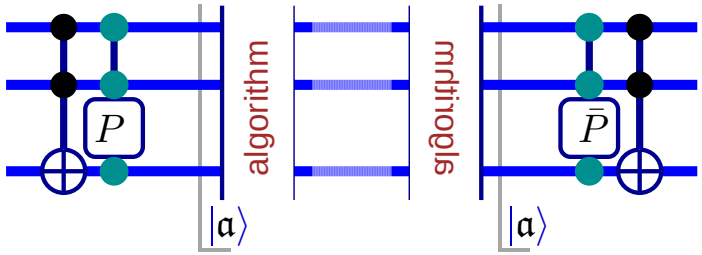
- Toffoli gates often come in reversing pairs.

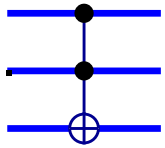


Ok to have logical phases in 

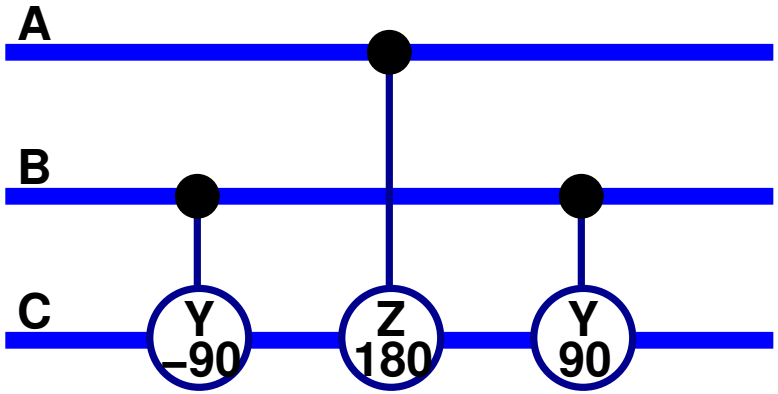
Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.



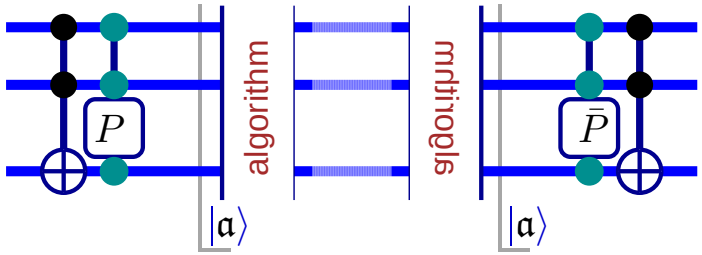
Ok to have logical phases in 

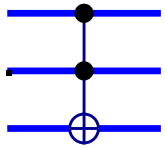
- Two more Toffolis up to logical phases.



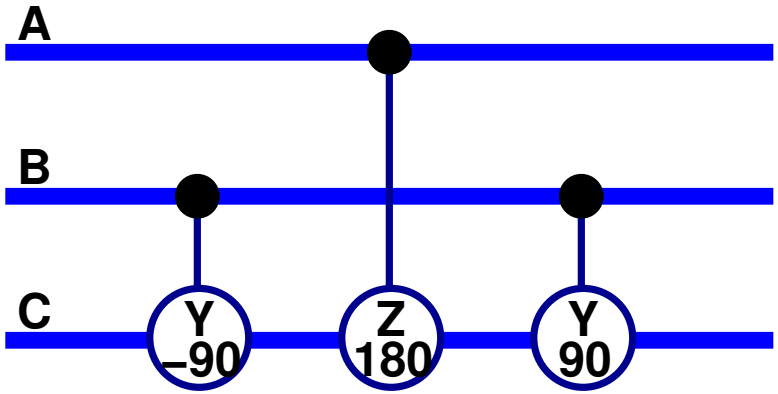
Toffoli Gate up to Control Phases

- Toffoli gates often come in reversing pairs.



Ok to have logical phases in 

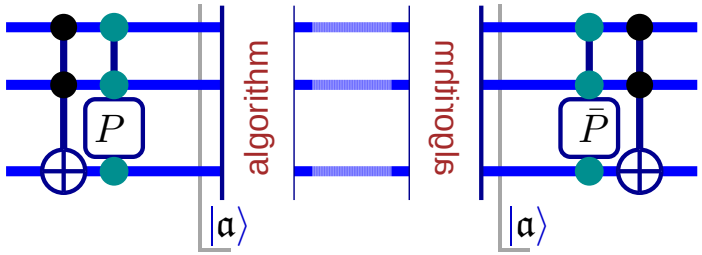
- Two more Toffolis up to logical phases.



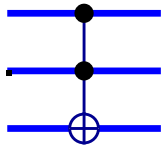
$$|0\rangle_A \quad : \quad \mathbb{1}$$
$$|10\rangle_{AB} \quad : \quad \mathbf{Z}_{180^\circ}$$
$$|11\rangle_{AB} \quad : \quad \mathbf{X}_{180^\circ}$$

Toffoli Gate up to Control Phases

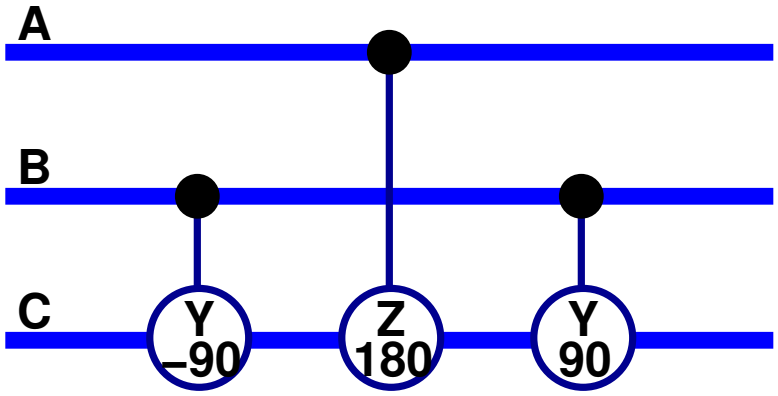
- Toffoli gates often come in reversing pairs.

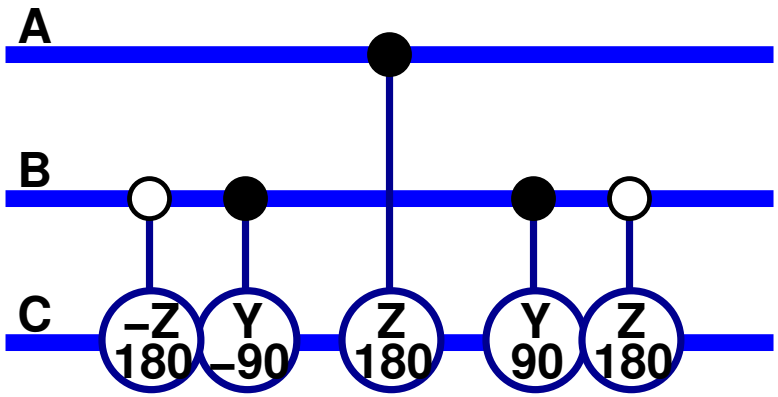


Ok to have logical phases in



- Two more Toffolis up to logical phases.

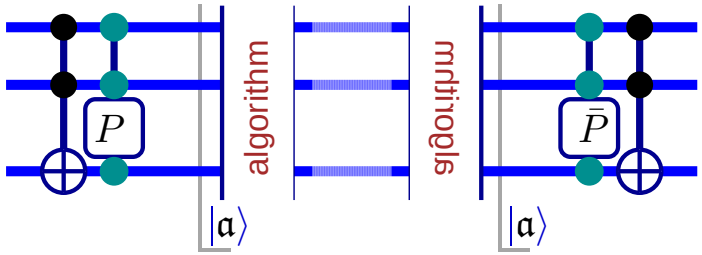




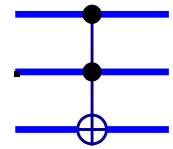
$$|0\rangle_{A} \quad : \quad \mathbb{1}$$
$$|10\rangle_{AB} \quad : \quad \mathbf{Z}_{180^\circ}$$
$$|11\rangle_{AB} \quad : \quad \mathbf{X}_{180^\circ}$$

Toffoli Gate up to Control Phases

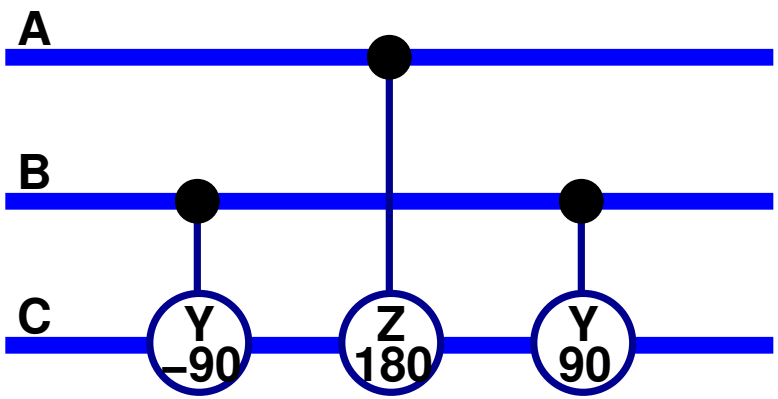
- Toffoli gates often come in reversing pairs.

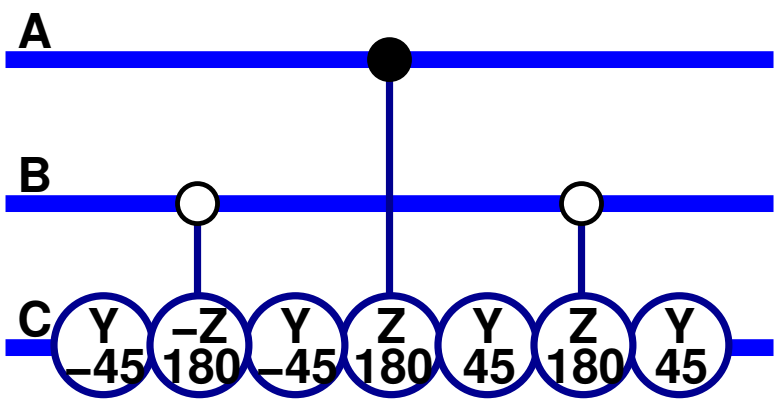


Ok to have logical phases in .



- Two more Toffolis up to logical phases.

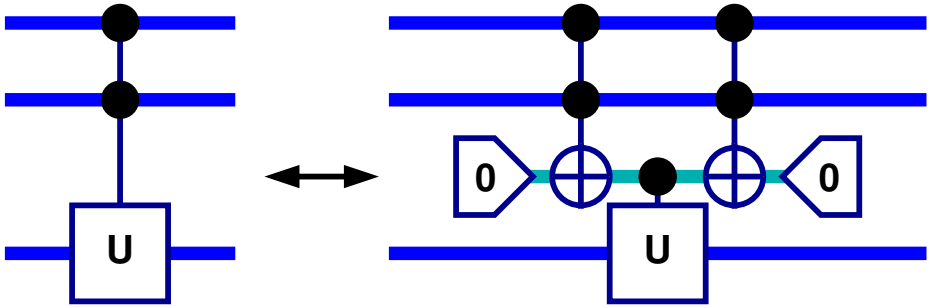




$$|0\rangle_{A} \quad : \quad \mathbb{1}$$
$$|10\rangle_{AB} \quad : \quad \mathbf{Z}_{180^\circ}$$
$$|11\rangle_{AB} \quad : \quad \mathbf{X}_{180^\circ}$$

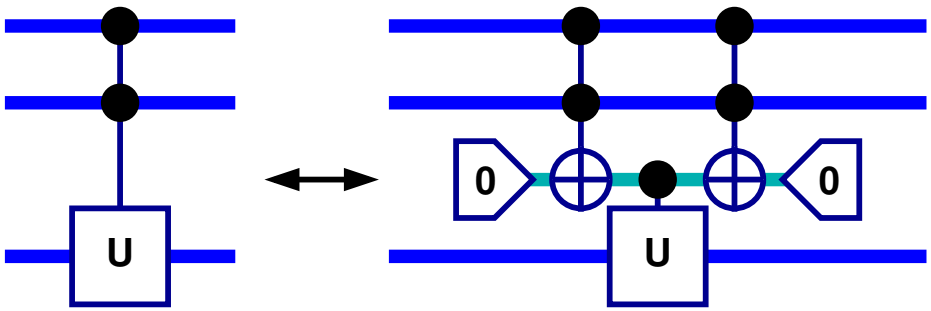
Adding Controls

- Add a control using an ancilla and two $\mathbf{c^2not}$ gates.

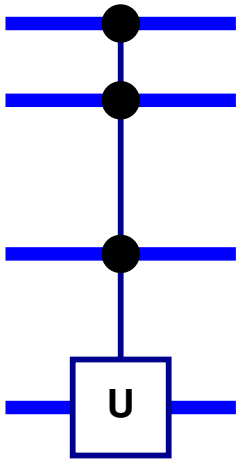


Adding Controls

- Add a control using an ancilla and two $\mathbf{c^2not}$ gates.

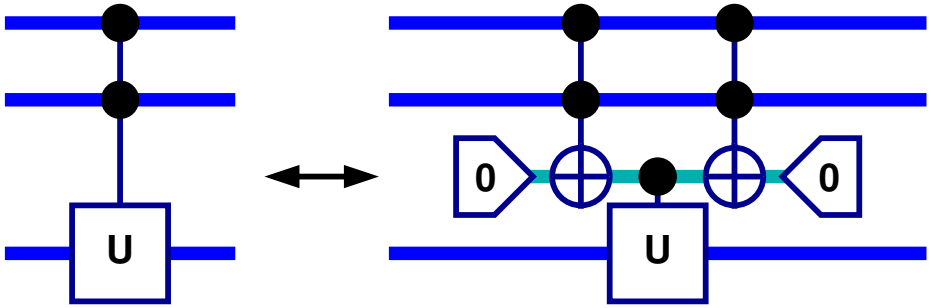


- Add multiple controls.

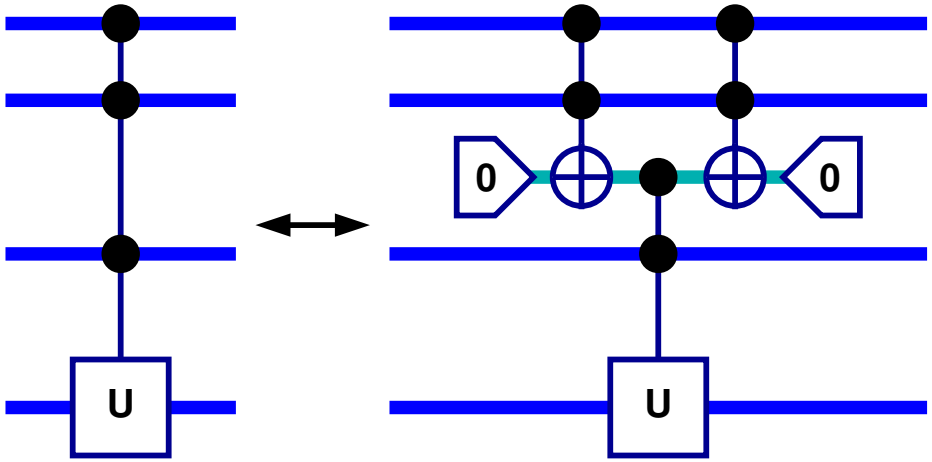


Adding Controls

- Add a control using an ancilla and two $\mathbf{c^2not}$ gates.

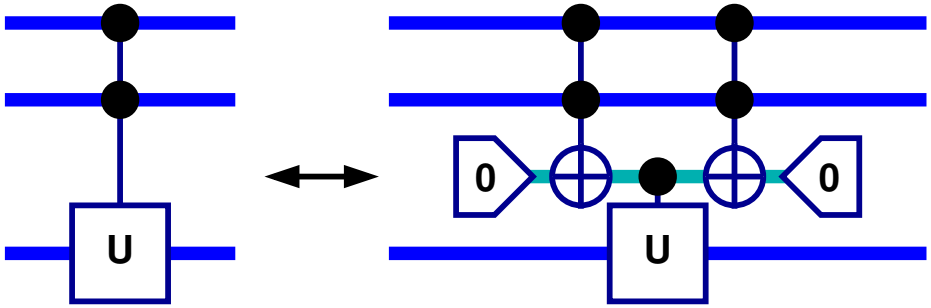


- Add multiple controls.

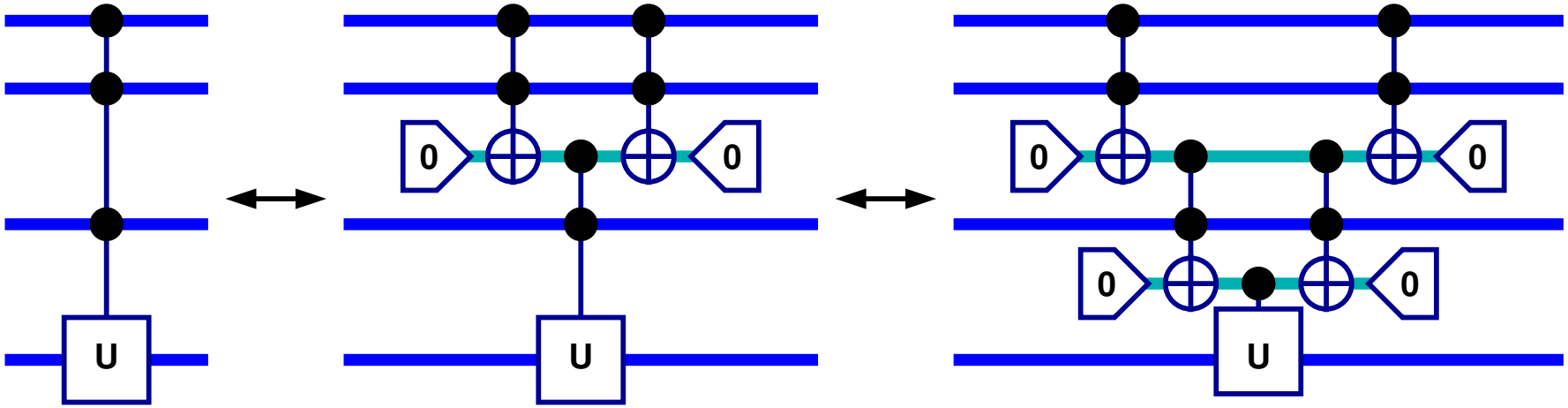


Adding Controls

- Add a control using an ancilla and two $\mathbf{c^2not}$ gates.

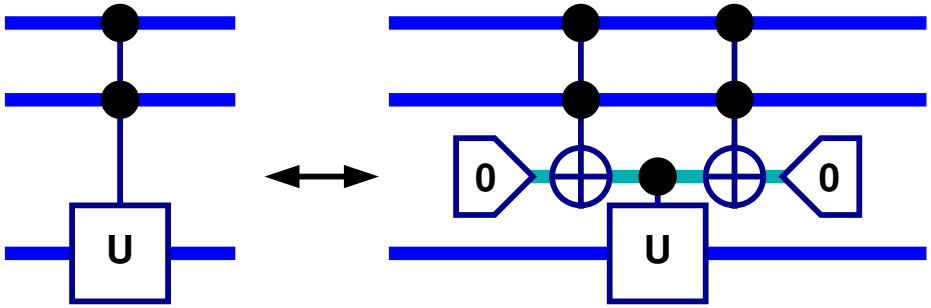


- Add multiple controls.

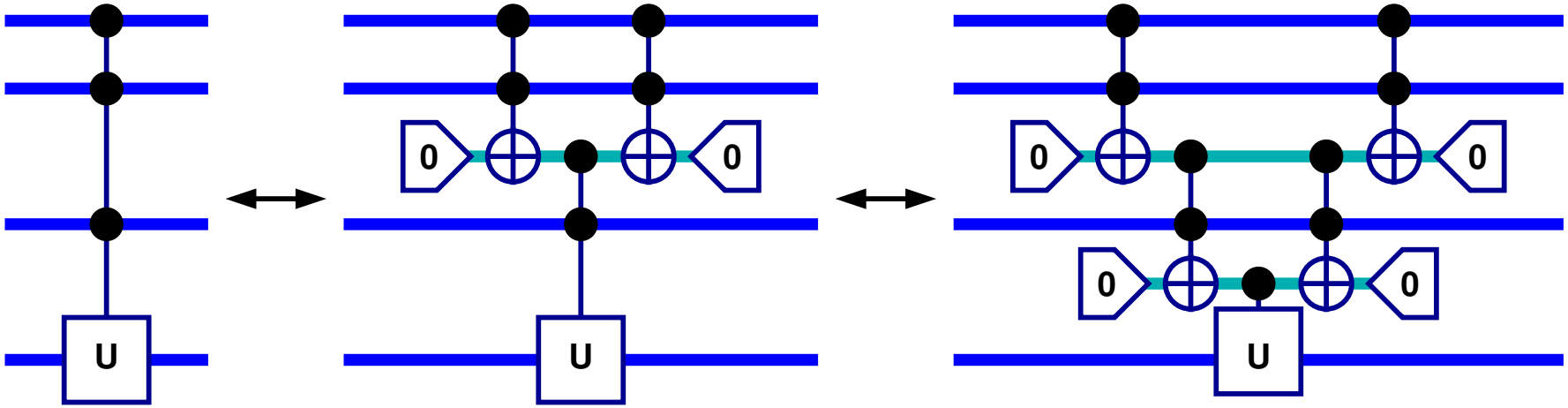


Adding Controls

- Add a control using an ancilla and two $\mathbf{c^2not}$ gates.



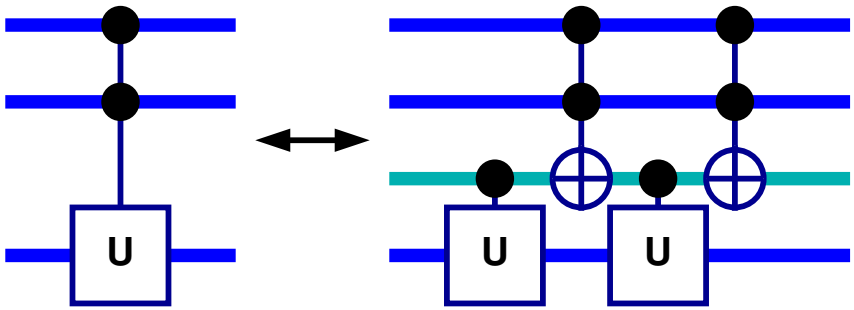
- Add multiple controls.



  - n controls: $2(n-1)$ $\mathbf{c^2not}$, $n-1$ ancillas, 1 $\mathbf{c}U$ gates.

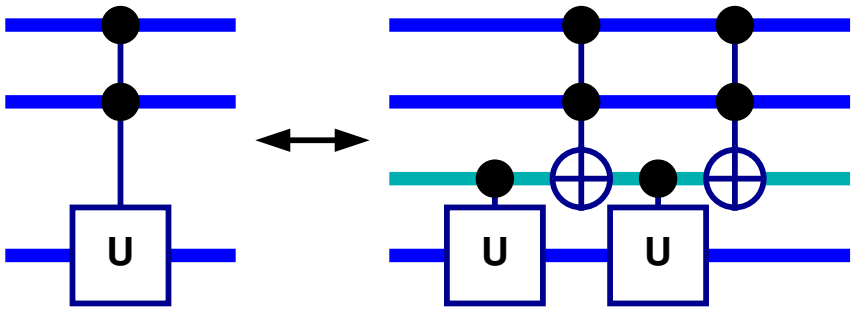
Adding Controls without Prepared Ancillas

- Suppose that $U^2 = \mathbb{1}$.

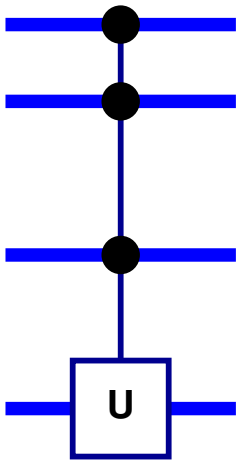


Adding Controls without Prepared Ancillas

- Suppose that $U^2 = \mathbb{1}$.

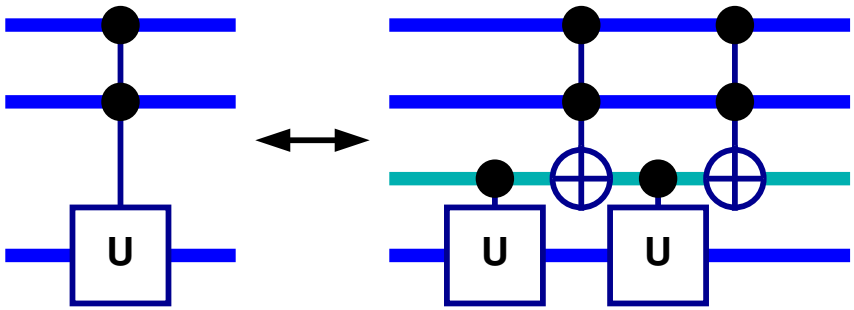


- Add multiple controls without prepared ancillas.

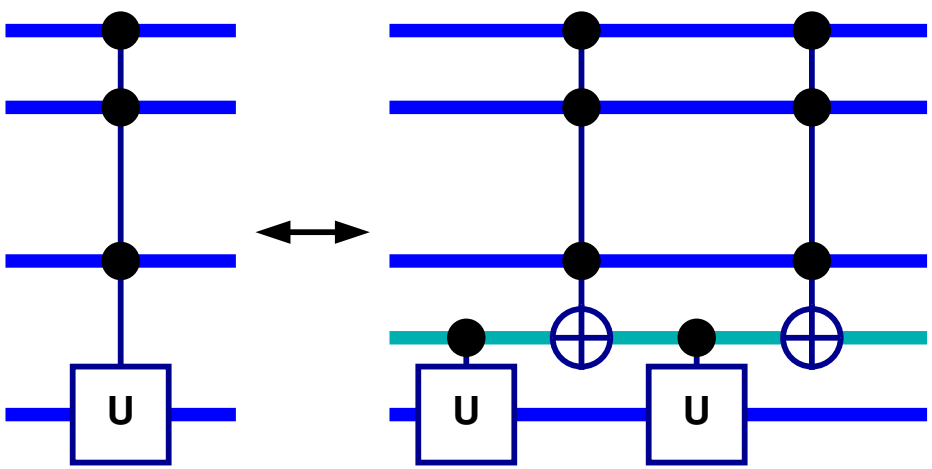


Adding Controls without Prepared Ancillas

- Suppose that $U^2 = \mathbb{1}$.

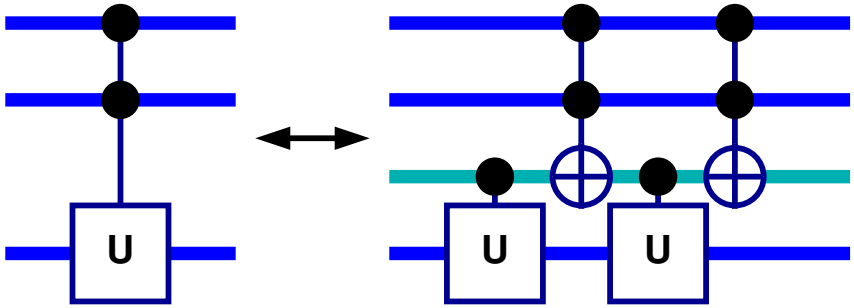


- Add multiple controls without prepared ancillas.

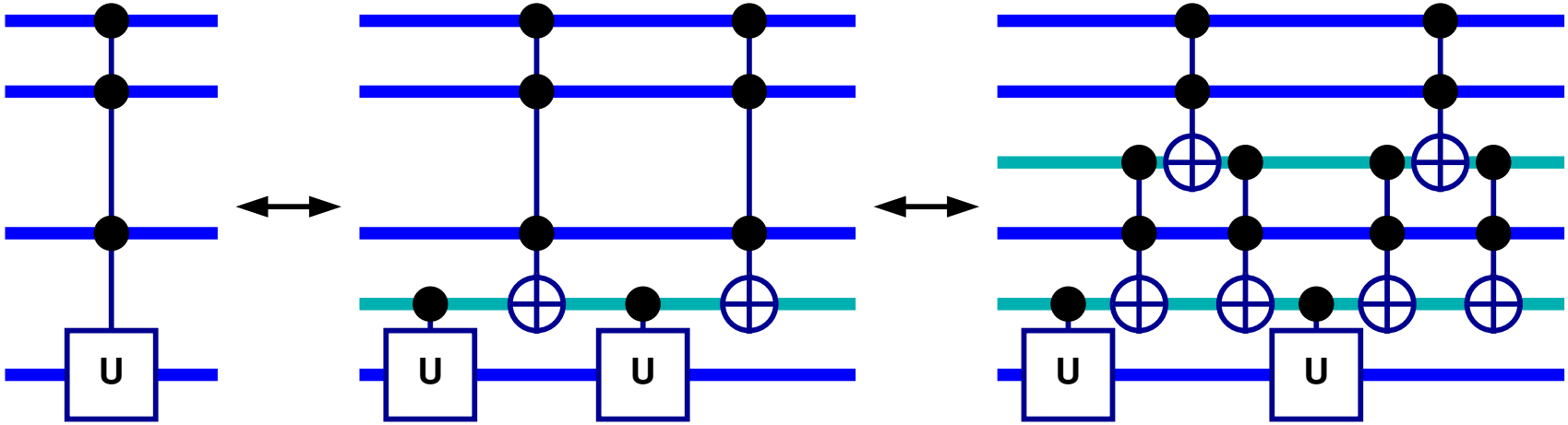


Adding Controls without Prepared Ancillas

- Suppose that $U^2 = \mathbb{1}$.

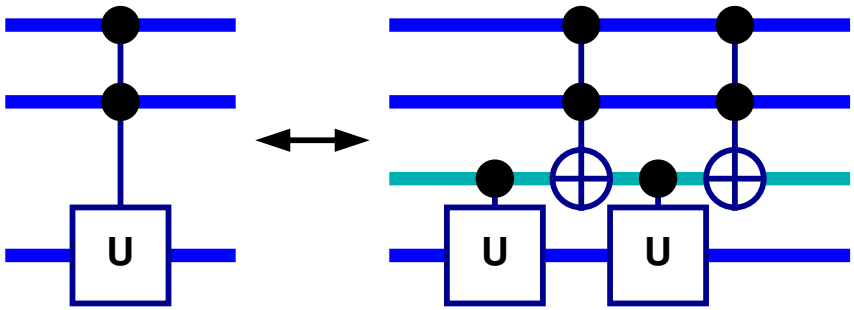


- Add multiple controls without prepared ancillas.

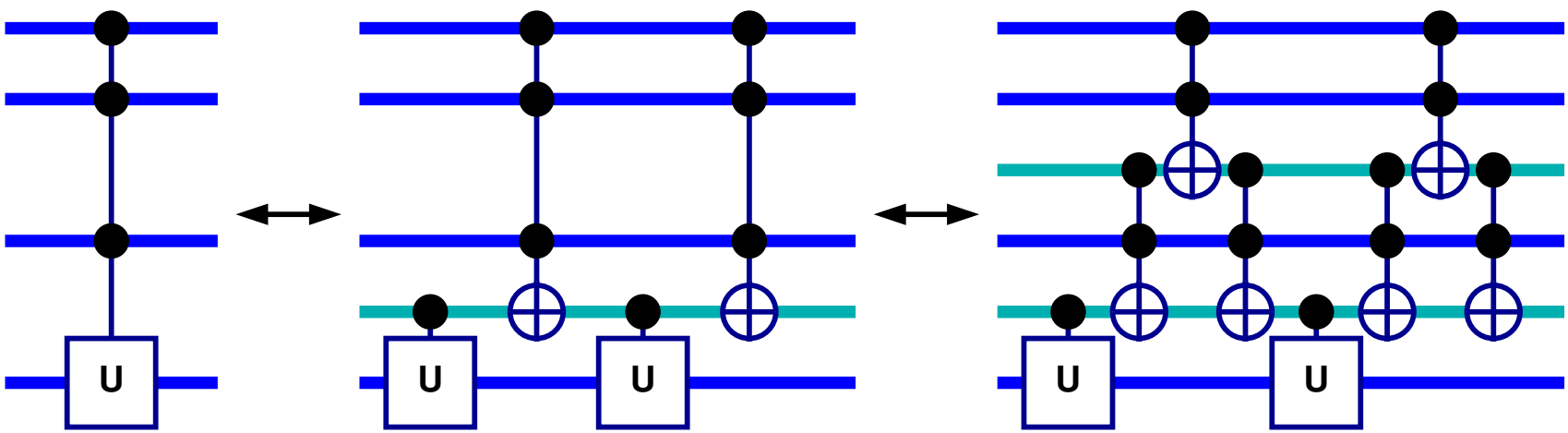


Adding Controls without Prepared Ancillas

- Suppose that $U^2 = \mathbb{1}$.



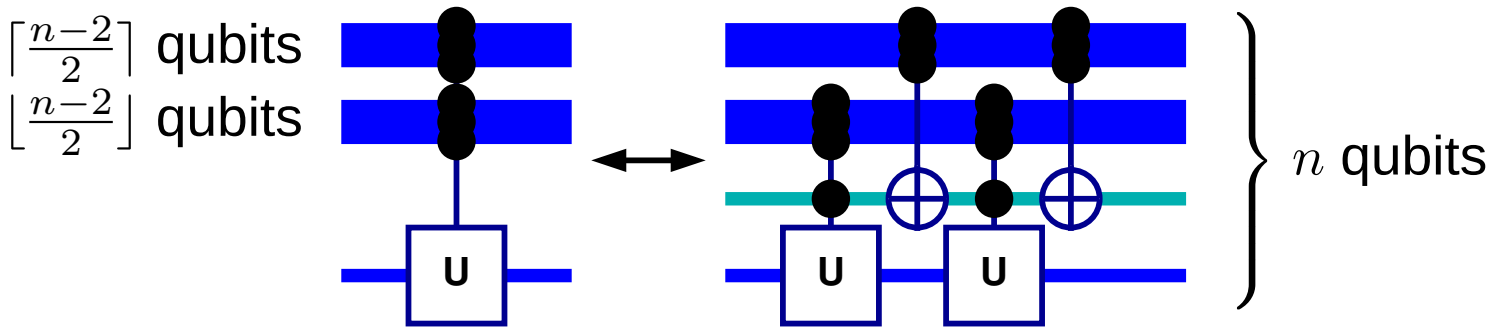
- Add multiple controls without prepared ancillas.



  - n controls: $4(n-3) + 2\ \mathbf{c^2not}$, $2n$ qubits, $2\ \mathbf{c}U$ gates.

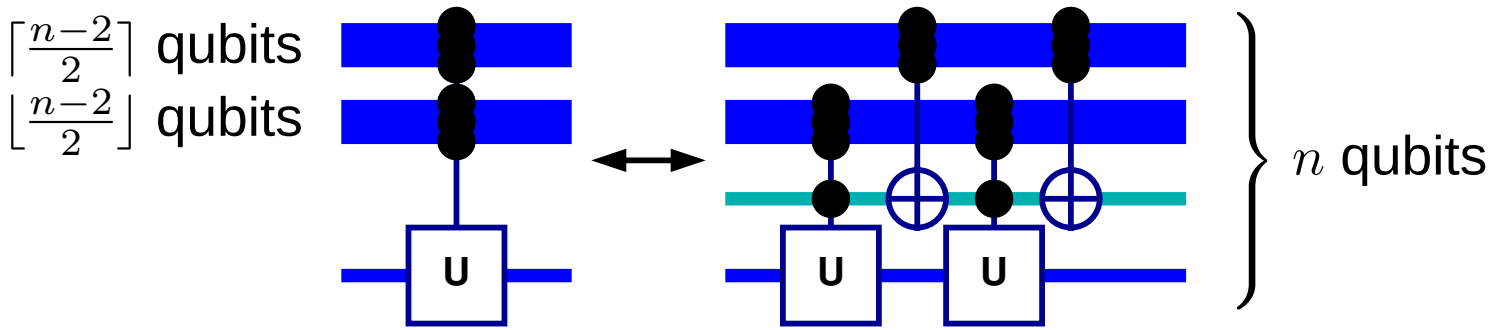
Controlled U With 0 or 1 Extra Qubit

- Halving controls for $U^2 = \mathbb{1}$, $n-2$ controls.



Controlled U With 0 or 1 Extra Qubit

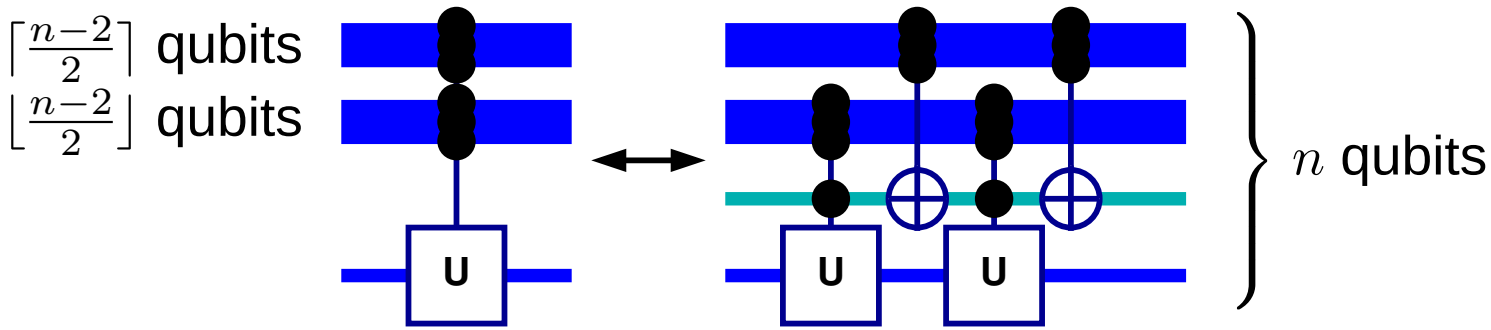
- Halving controls for $U^2 = \mathbb{1}$, $n-2$ controls.



  - $n-2$ controls: $8(n-5)$ $\mathbf{c^2not}$, n qubits, 2 $\mathbf{c}U$, 2 $\mathbf{cnot}$.

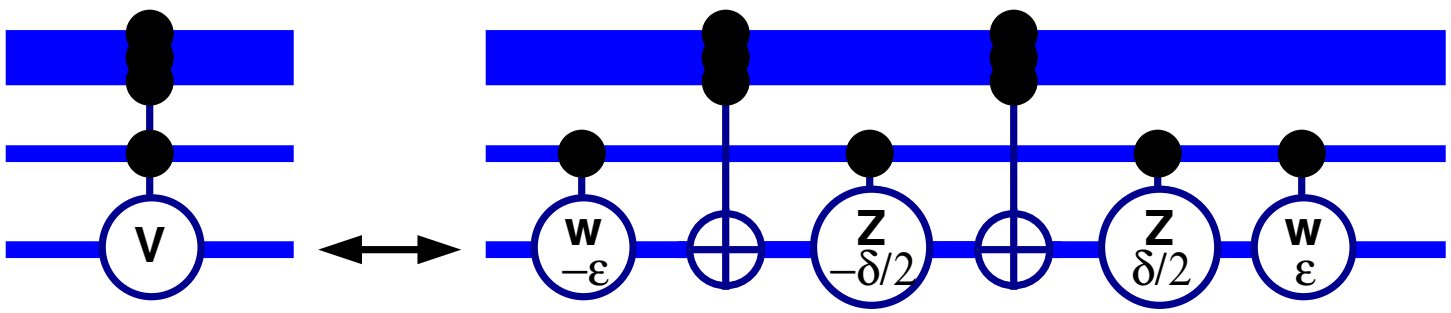
Controlled U With 0 or 1 Extra Qubit

- Halving controls for $U^2 = \mathbb{1}$, $n-2$ controls.



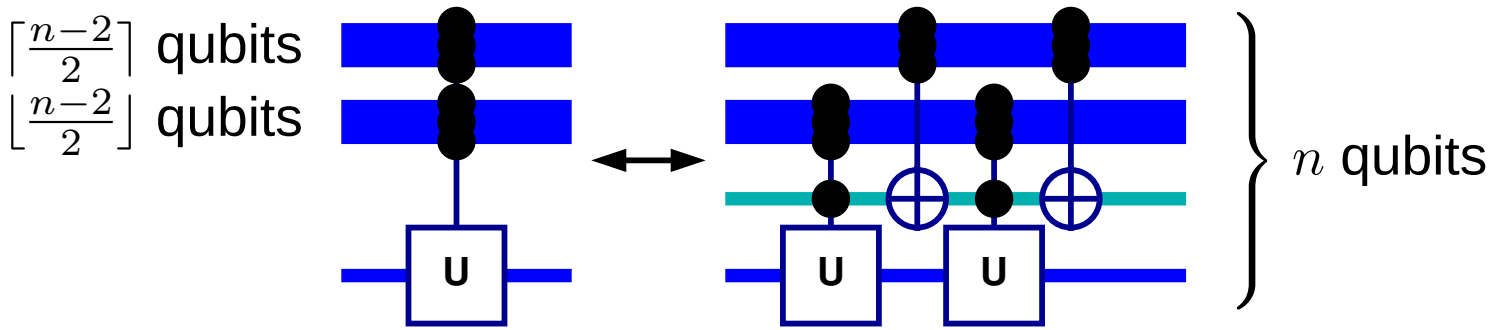
  - $n-2$ controls: $8(n-5)$ $\mathbf{c^2not}$, n qubits, 2 $\mathbf{c}U$, 2 $\mathbf{cnot}$.

- Let V be a rotation. With appropriate choice of parameters:



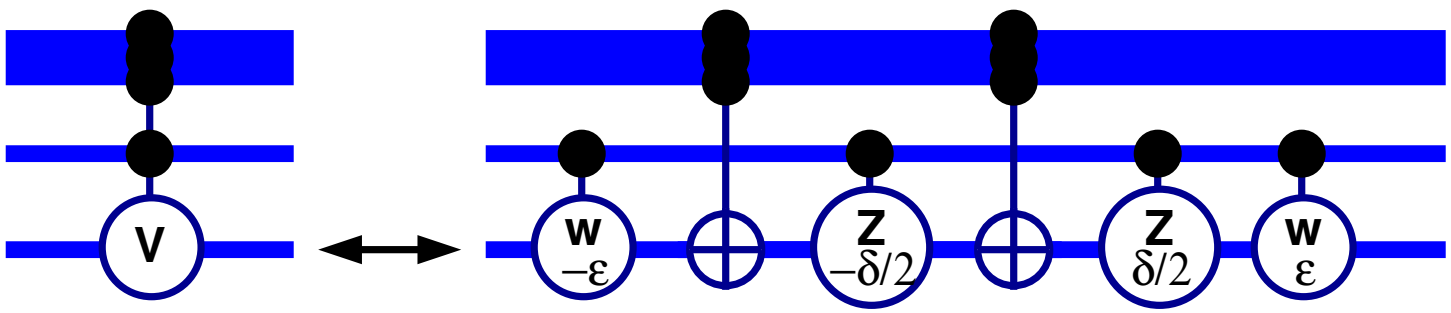
Controlled U With 0 or 1 Extra Qubit

- Halving controls for $U^2 = \mathbb{1}$, $n-2$ controls.



  - $n-2$ controls: $8(n-5)$ $\mathbf{c^2not}$, n qubits, 2 $\mathbf{c}U$, 2 $\mathbf{cnot}$.

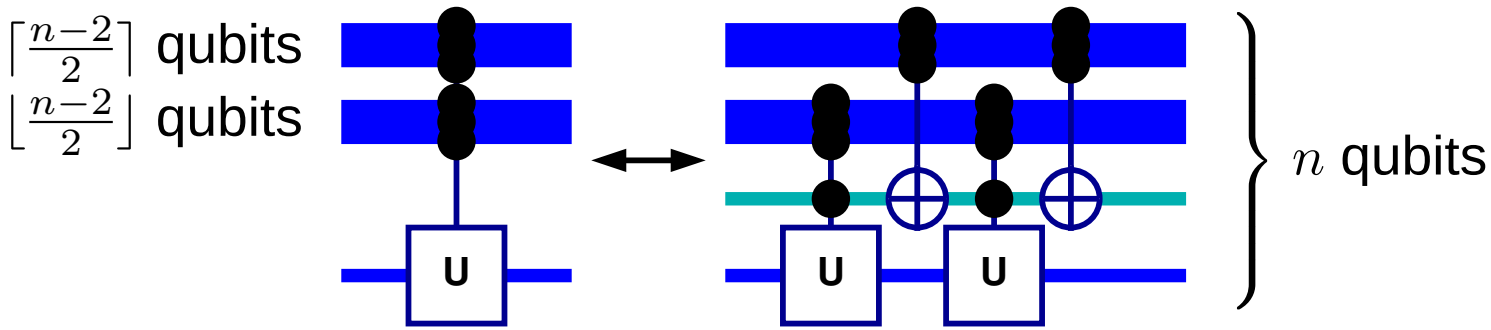
- Let V be a rotation. With appropriate choice of parameters:



  - $n-1$ controls: $16(n-5)$ $\mathbf{c^2not}$, 8 $\mathbf{cnot}$, n qubits, 4 $\mathbf{cRot}$.

Controlled U With 0 or 1 Extra Qubit

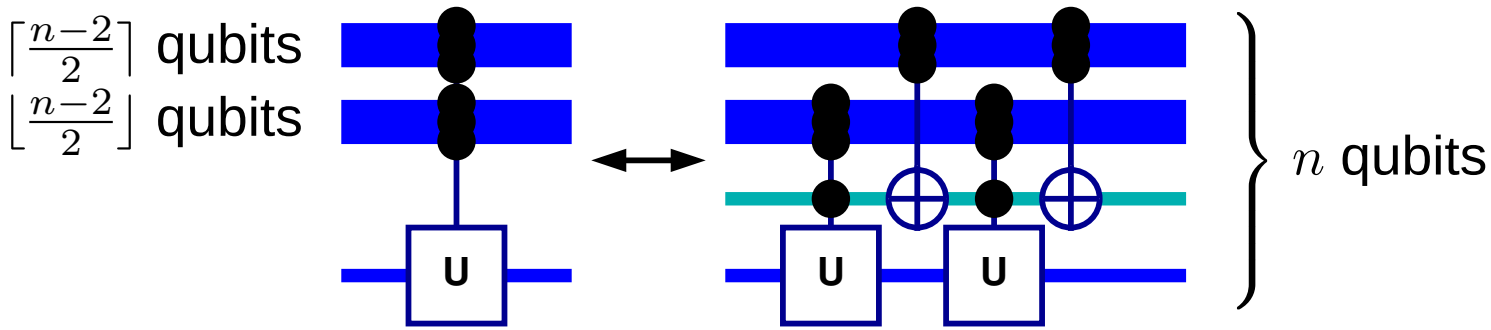
- Halving controls for $U^2 = \mathbb{1}$, $n-2$ controls.



  - $n-2$ controls: $8(n-5)$ $\mathbf{c^2not}$, n qubits, 2 $\mathbf{c}U$, 2 $\mathbf{cnot}$.

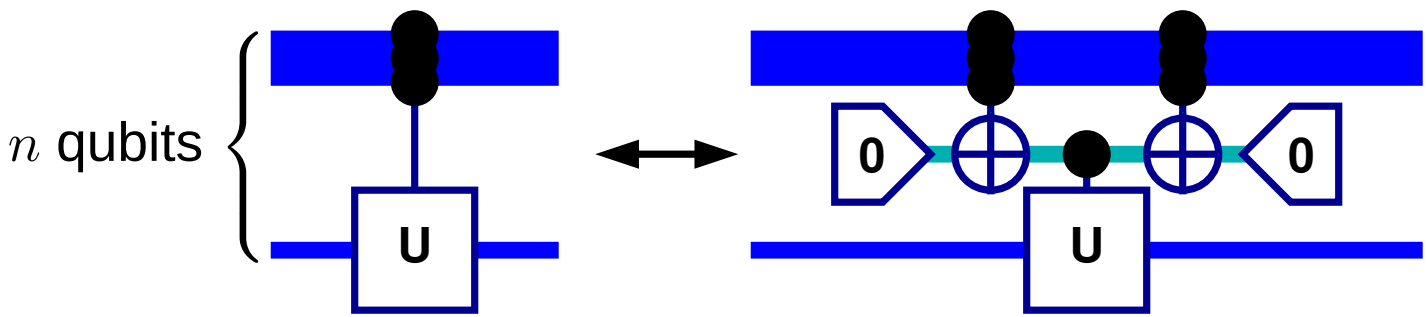
Controlled U With 0 or 1 Extra Qubit

- Halving controls for $U^2 = \mathbb{1}$, $n-2$ controls.



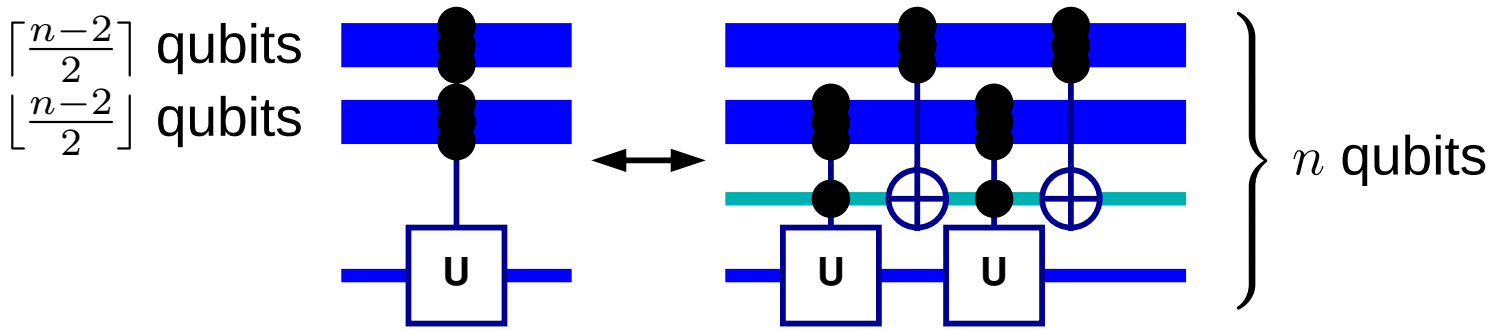
  - $n-2$ controls: $8(n-5)$ $\mathbf{c^2not}$, n qubits, 2 $\mathbf{c}U$, 2 $\mathbf{cnot}$.

- Let U be arbitrary. From before:



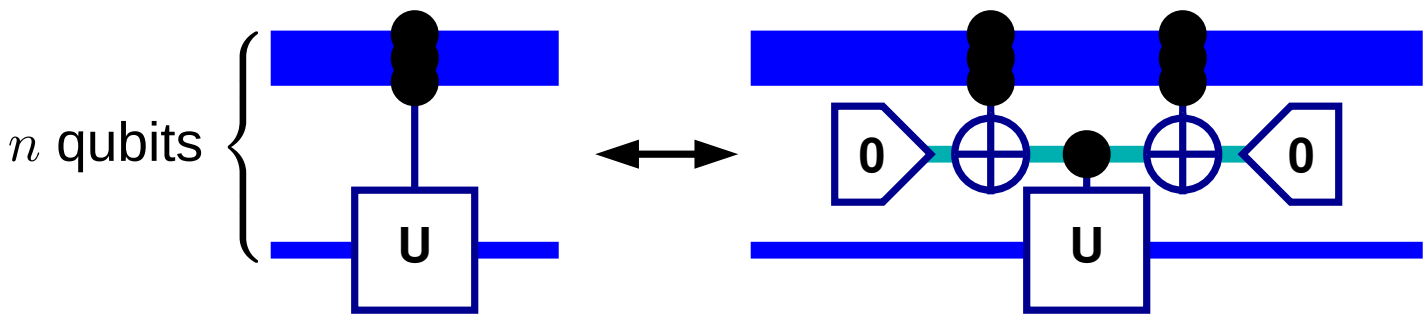
Controlled U With 0 or 1 Extra Qubit

- Halving controls for $U^2 = \mathbb{1}$, $n-2$ controls.



  - $n-2$ controls: $8(n-5)$ $\mathbf{c^2not}$, n qubits, 2 $\mathbf{c}U$, 2 $\mathbf{cnot}$.

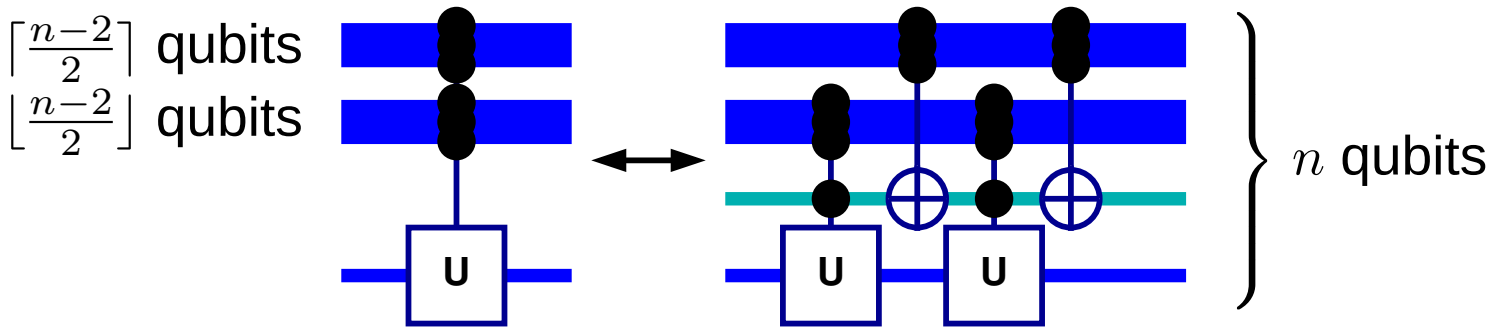
- Let U be arbitrary. From before:



  - $n-1$ controls: $8(n-4)$ $\mathbf{c^2not}$, 1 ancilla, 4 $\mathbf{cnot}$, 1 $\mathbf{c}U$.

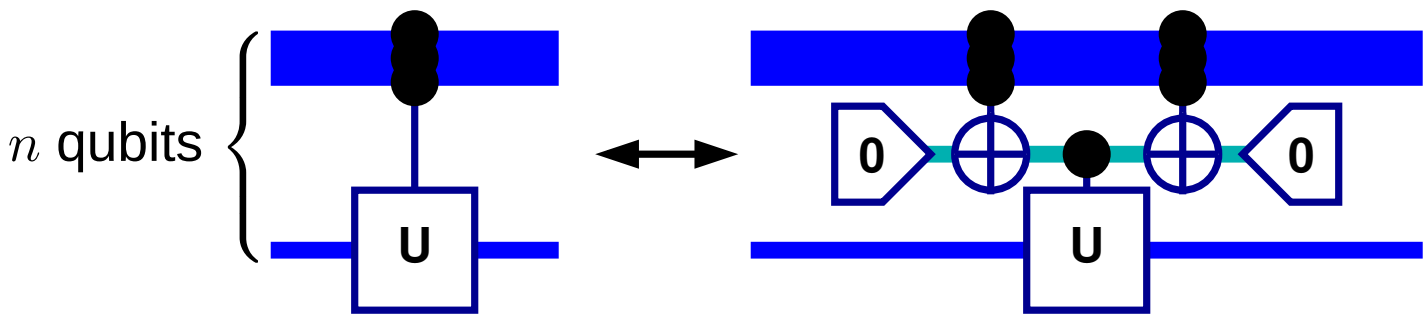
Controlled U With 0 or 1 Extra Qubit

- Halving controls for $U^2 = \mathbb{1}$, $n-2$ controls.



  - $n-2$ controls: $8(n-5)$ $\mathbf{c^2not}$, n qubits, 2 $\mathbf{c}U$, 2 $\mathbf{cnot}$.

- Let U be arbitrary. From before:



  - $n-1$ controls: $8(n-4)$ $\mathbf{c^2not}$, 1 ancilla, 4 $\mathbf{cnot}$, 1 $\mathbf{c}U$.

- Time/space tradeoff?

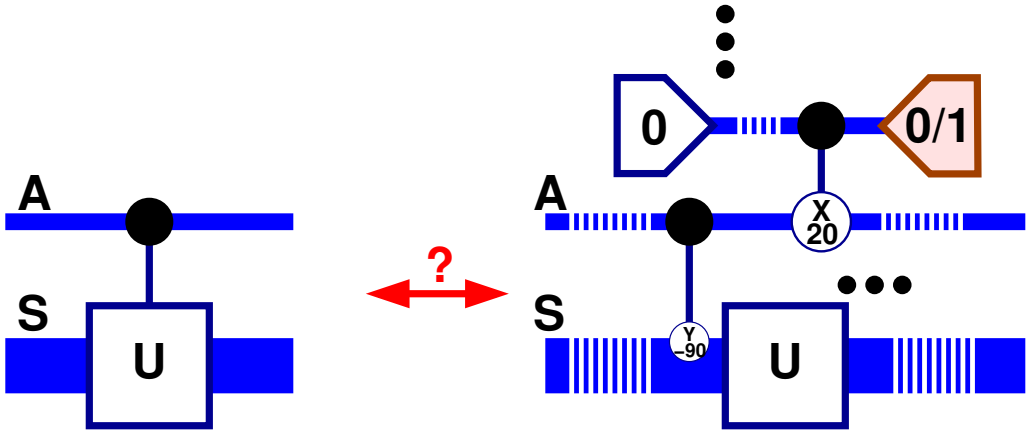
Barenco&al 1995 [1]

From U to Controlled U?

- Given that $U^{(\mathsf{S})}$ is available, can one implement $\mathbf{c}U^{(\mathsf{AS})}$?

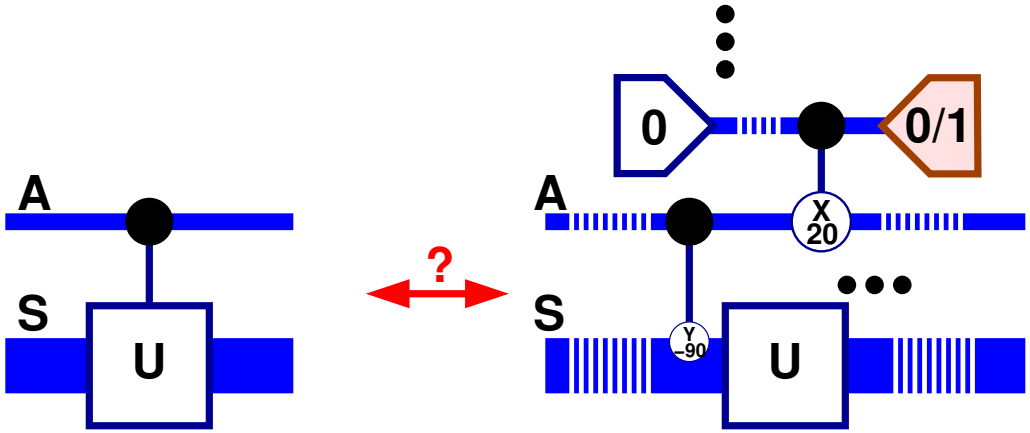
From U to Controlled U?

- Given that $U^{(\mathsf{S})}$ is available, can one implement $\mathbf{c}U^{(\mathsf{AS})}$?



From U to Controlled U?

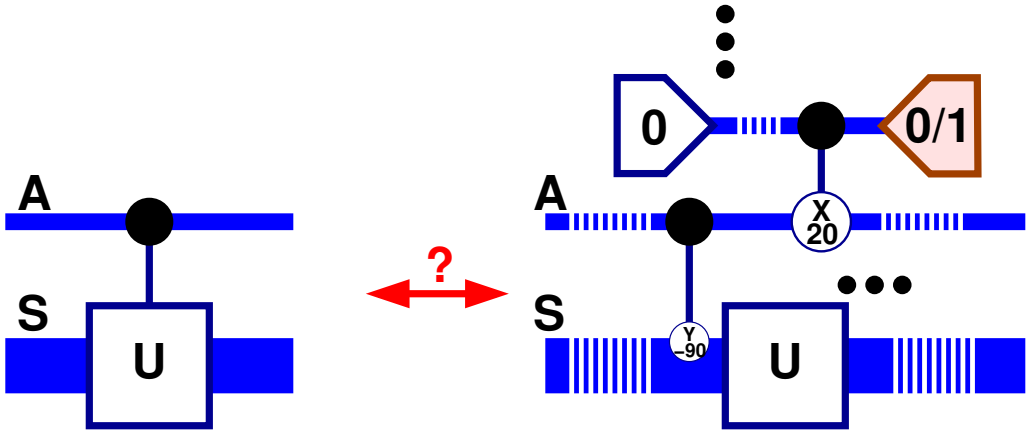
- Given that $U^{(\mathsf{S})}$ is available, can one implement $\mathbf{c}U^{(\mathsf{AS})}$?



- Yes, if $U^{(\mathsf{S})}$ is given as a quantum network using our set of fundamental gates.

From U to Controlled U?

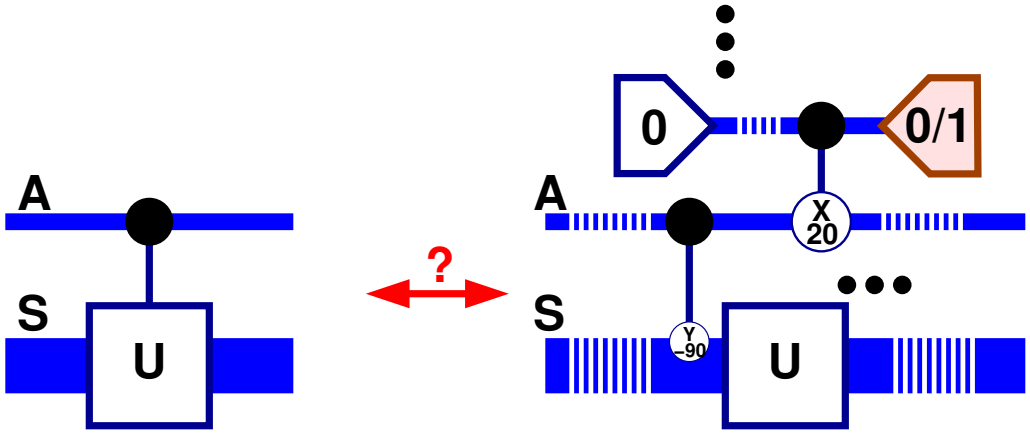
- Given that $U^{(S)}$ is available, can one implement $\mathbf{c}U^{(AS)}$?



- Yes, if $U^{(S)}$ is given as a quantum network using our set of fundamental gates.
  - Implementation: Convert each gate in $U^{(S)}$'s network to a gate controlled by qubit A.

From U to Controlled U?

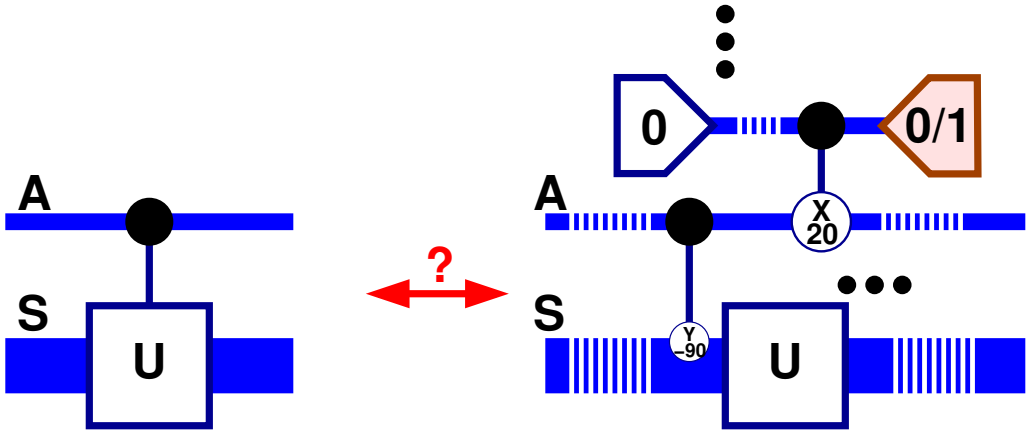
- Given that $U^{(S)}$ is available, can one implement $\mathbf{c}U^{(AS)}$?



- Yes, if $U^{(S)}$ is given as a quantum network using our set of fundamental gates.
  - Implementation: Convert each gate in $U^{(S)}$'s network to a gate controlled by qubit A.
- No, if $U^{(S)}$ is given as a black box with no promises.

From U to Controlled U?

- Given that $U^{(\mathsf{S})}$ is available, can one implement $\mathbf{c}U^{(\mathsf{AS})}$?



- Yes, if $U^{(\mathsf{S})}$ is given as a quantum network using our set of fundamental gates.
  - Implementation: Convert each gate in $U^{(\mathsf{S})}$'s network to a gate controlled by qubit A.
- No, if $U^{(\mathsf{S})}$ is given as a black box with no promises.
- Other conditions for which the answer is "yes"?

Universality: Permutations of Logical States

- $\mathbf{c}^k\mathbf{not}$ gates implement all logical state permutations.

Universality: Permutations of Logical States

- $\mathbf{c}^k\mathbf{not}$ gates implement all logical state permutations.
  Proof. Consider n qubits.

Universality: Permutations of Logical States

- $\mathbf{c}^k\mathbf{not}$ gates implement all logical state permutations.

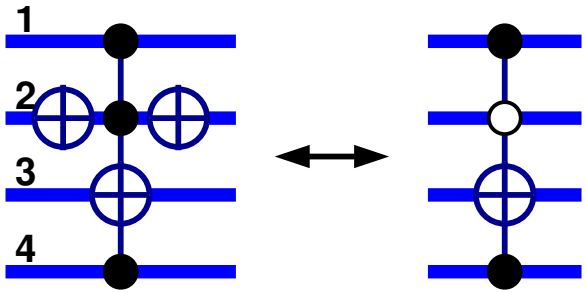
  Proof. Consider n qubits.
  - If $|\mathfrak{a} - \mathfrak{b}| = 1$, the transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.

Universality: Permutations of Logical States

- $\mathbf{c}^k\mathbf{not}$ gates implement all logical state permutations.

  Proof. Consider n qubits.
  - If $|\mathfrak{a} - \mathfrak{b}| = 1$, the transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.

    Example: $\mathfrak{a} = \mathtt{1001}$ and $\mathfrak{b} = \mathtt{1011}$:



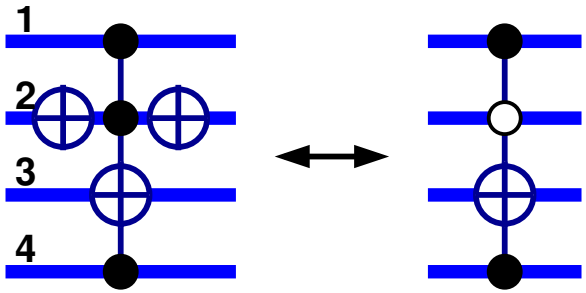
$$\begin{cases} |\mathtt{1001}\rangle & \longrightarrow & |\mathtt{1011}\rangle \\ |\mathtt{1011}\rangle & \longrightarrow & |\mathtt{1001}\rangle \\ |\mathfrak{c}\rangle & \longrightarrow & |\mathfrak{c}\rangle \quad \text{otherwise} \end{cases}$$

Universality: Permutations of Logical States

- $\mathbf{c}^k\mathbf{not}$ gates implement all logical state permutations.

  Proof. Consider n qubits.
  - If $|\mathfrak{a} - \mathfrak{b}| = 1$, the transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.

    Example: $\mathfrak{a} = \mathtt{1001}$ and $\mathfrak{b} = \mathtt{1011}$:



$$\begin{cases} |\mathtt{1001}\rangle & \longrightarrow & |\mathtt{1011}\rangle \\ |\mathtt{1011}\rangle & \longrightarrow & |\mathtt{1001}\rangle \\ |\mathfrak{c}\rangle & \longrightarrow & |\mathfrak{c}\rangle \quad \text{otherwise} \end{cases}$$

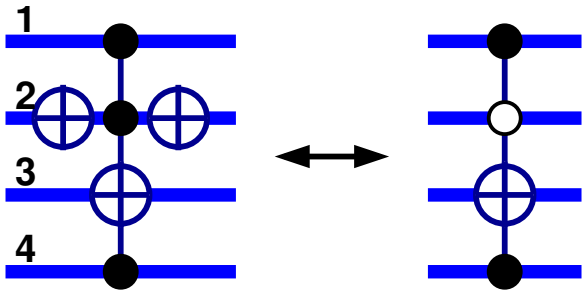
  - $\mathfrak{b}$ can be reached from $\mathfrak{a}$ by a sequence changing one bit at a time.

Universality: Permutations of Logical States

- $\mathbf{c}^k\mathbf{not}$ gates implement all logical state permutations.

  Proof. Consider n qubits.
  - If $|\mathfrak{a} - \mathfrak{b}| = 1$, the transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.

    Example: $\mathfrak{a} = \mathtt{1001}$ and $\mathfrak{b} = \mathtt{1011}$:



$$\begin{cases} |\mathtt{1001}\rangle & \longrightarrow & |\mathtt{1011}\rangle \\ |\mathtt{1011}\rangle & \longrightarrow & |\mathtt{1001}\rangle \\ |\mathfrak{c}\rangle & \longrightarrow & |\mathfrak{c}\rangle \quad \text{otherwise} \end{cases}$$

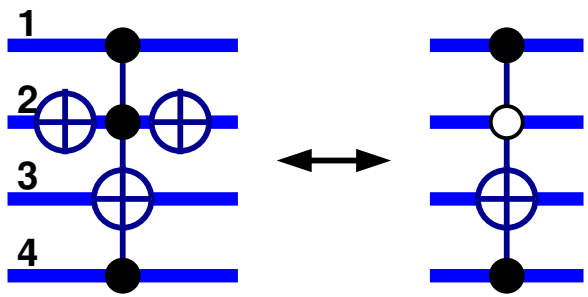
  - $\mathfrak{b}$ can be reached from $\mathfrak{a}$ by a sequence changing one bit at a time.

    Example: $\mathfrak{a} = \mathtt{0010}$ and $\mathfrak{b} = \mathtt{1001}$: $\mathtt{0010} \leftrightarrow \mathtt{1010} \leftrightarrow \mathtt{1000} \leftrightarrow \mathtt{1001}$

Universality: Permutations of Logical States

- $\mathbf{c}^k\mathbf{not}$ gates implement all logical state permutations.

  Proof. Consider n qubits.
  - If $|\mathfrak{a} - \mathfrak{b}| = 1$, the transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.
    Example: $\mathfrak{a} = \mathtt{1001}$ and $\mathfrak{b} = \mathtt{1011}$:



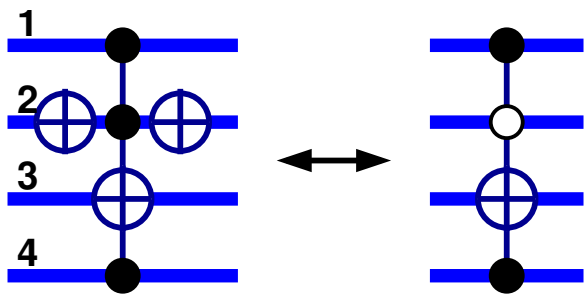
$$\begin{cases} |\mathtt{1001}\rangle & \longrightarrow & |\mathtt{1011}\rangle \\ |\mathtt{1011}\rangle & \longrightarrow & |\mathtt{1001}\rangle \\ |\mathfrak{c}\rangle & \longrightarrow & |\mathfrak{c}\rangle \quad \text{otherwise} \end{cases}$$

  - $\mathfrak{b}$ can be reached from $\mathfrak{a}$ by a sequence changing one bit at a time.
    Example: $\mathfrak{a} = \mathtt{0010}$ and $\mathfrak{b} = \mathtt{1001}$: $\mathtt{0010} \leftrightarrow \mathtt{1010} \leftrightarrow \mathtt{1000} \leftrightarrow \mathtt{1001}$
  - Every transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.

Universality: Permutations of Logical States

- $\mathbf{c}^k\mathbf{not}$ gates implement all logical state permutations.

  Proof. Consider n qubits.
  - If $|\mathfrak{a} - \mathfrak{b}| = 1$, the transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.
    Example: $\mathfrak{a} = 1001$ and $\mathfrak{b} = 1011$:



$$\begin{cases} |1001\rangle & \rightarrow & |1011\rangle \\ |1011\rangle & \rightarrow & |1001\rangle \\ |\mathfrak{c}\rangle & \rightarrow & |\mathfrak{c}\rangle \quad \text{otherwise} \end{cases}$$

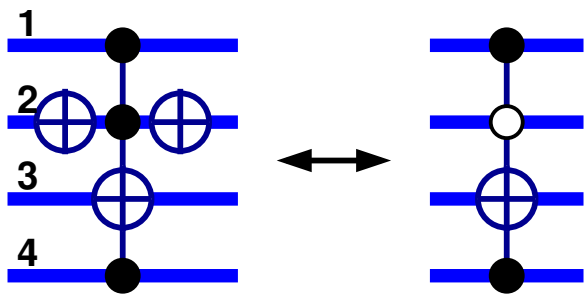
  - $\mathfrak{b}$ can be reached from $\mathfrak{a}$ by a sequence changing one bit at a time.
    Example: $\mathfrak{a} = 0010$ and $\mathfrak{b} = 1001$: $0010 \leftrightarrow 1010 \leftrightarrow 1000 \leftrightarrow 1001$
  - Every transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.
    Example: $\mathfrak{a} = 0010$ and $\mathfrak{b} = 1001$:

$1{:}|0010\rangle$
$2{:}|1010\rangle$
$3{:}|1000\rangle$
$4{:}|1001\rangle$

Universality: Permutations of Logical States

- $\mathbf{c}^k\mathbf{not}$ gates implement all logical state permutations.

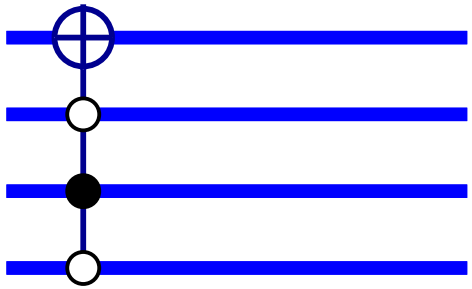
  Proof. Consider n qubits.
  - If $|\mathfrak{a} - \mathfrak{b}| = 1$, the transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.
    Example: $\mathfrak{a} = \mathtt{1001}$ and $\mathfrak{b} = \mathtt{1011}$:



$$\begin{cases} |\mathtt{1001}\rangle & \rightarrow & |\mathtt{1011}\rangle \\ |\mathtt{1011}\rangle & \rightarrow & |\mathtt{1001}\rangle \\ |\mathfrak{c}\rangle & \rightarrow & |\mathfrak{c}\rangle \quad \text{otherwise} \end{cases}$$

  - $\mathfrak{b}$ can be reached from $\mathfrak{a}$ by a sequence changing one bit at a time.
    Example: $\mathfrak{a} = \mathtt{0010}$ and $\mathfrak{b} = \mathtt{1001}$: $\mathtt{0010} \leftrightarrow \mathtt{1010} \leftrightarrow \mathtt{1000} \leftrightarrow \mathtt{1001}$
  - Every transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.
    Example: $\mathfrak{a} = \mathtt{0010}$ and $\mathfrak{b} = \mathtt{1001}$:

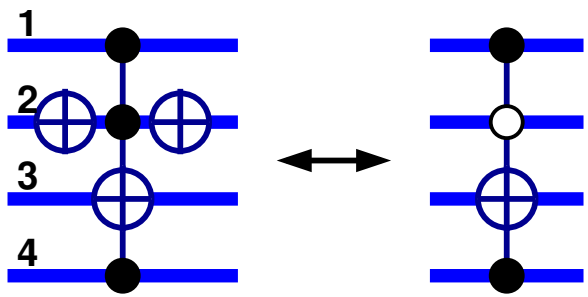
$$\begin{array}{l} 1{:}|\mathtt{0010}\rangle \\ 2{:}|\mathtt{1010}\rangle \\ 3{:}|\mathtt{1000}\rangle \\ 4{:}|\mathtt{1001}\rangle \end{array} \quad \longleftarrow \quad \begin{array}{l} 2{:}|\mathtt{1010}\rangle \\ 1{:}|\mathtt{0010}\rangle \\ 3{:}|\mathtt{1000}\rangle \\ 4{:}|\mathtt{1001}\rangle \end{array}$$



Universality: Permutations of Logical States

- $\mathbf{c}^k\mathbf{not}$ gates implement all logical state permutations.

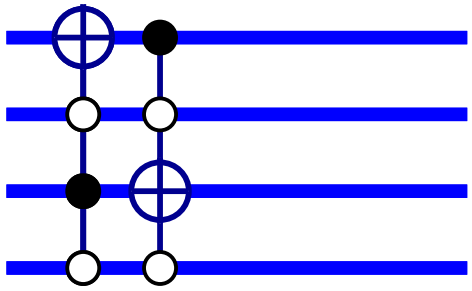
  Proof. Consider n qubits.
  - If $|\mathfrak{a} - \mathfrak{b}| = 1$, the transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.
    Example: $\mathfrak{a} = 1001$ and $\mathfrak{b} = 1011$:



$$\begin{cases} |1001\rangle & \rightarrow & |1011\rangle \\ |1011\rangle & \rightarrow & |1001\rangle \\ |\mathfrak{c}\rangle & \rightarrow & |\mathfrak{c}\rangle \quad \text{otherwise} \end{cases}$$

  - $\mathfrak{b}$ can be reached from $\mathfrak{a}$ by a sequence changing one bit at a time.
    Example: $\mathfrak{a} = 0010$ and $\mathfrak{b} = 1001$: $0010 \leftrightarrow 1010 \leftrightarrow 1000 \leftrightarrow 1001$
  - Every transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.
    Example: $\mathfrak{a} = 0010$ and $\mathfrak{b} = 1001$:

$$\begin{array}{l} 1{:}|0010\rangle \\ 2{:}|1010\rangle \\ 3{:}|1000\rangle \\ 4{:}|1001\rangle \end{array} \quad \longleftarrow \quad \begin{array}{l} 2{:}|1010\rangle \\ 3{:}|1000\rangle \\ 1{:}|0010\rangle \\ 4{:}|1001\rangle \end{array}$$

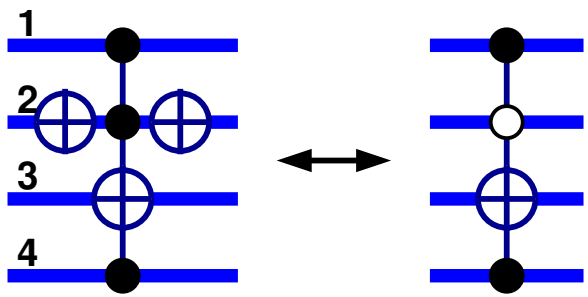


Universality: Permutations of Logical States

- $\mathbf{c}^k\mathbf{not}$ gates implement all logical state permutations.

  Proof. Consider n qubits.
  - If $|\mathfrak{a} - \mathfrak{b}| = 1$, the transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.

    Example: $\mathfrak{a} = \mathtt{1001}$ and $\mathfrak{b} = \mathtt{1011}$:



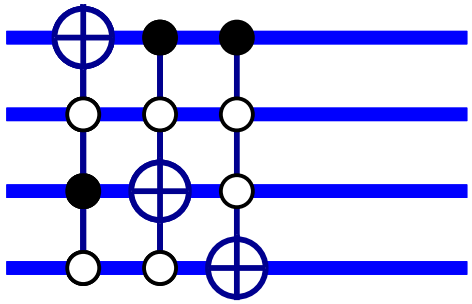
$$\begin{cases} |\mathtt{1001}\rangle & \rightarrow & |\mathtt{1011}\rangle \\ |\mathtt{1011}\rangle & \rightarrow & |\mathtt{1001}\rangle \\ |\mathfrak{c}\rangle & \rightarrow & |\mathfrak{c}\rangle \quad \text{otherwise} \end{cases}$$

  - $\mathfrak{b}$ can be reached from $\mathfrak{a}$ by a sequence changing one bit at a time.

    Example: $\mathfrak{a} = \mathtt{0010}$ and $\mathfrak{b} = \mathtt{1001}$: $\mathtt{0010} \leftrightarrow \mathtt{1010} \leftrightarrow \mathtt{1000} \leftrightarrow \mathtt{1001}$
  - Every transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.

    Example: $\mathfrak{a} = \mathtt{0010}$ and $\mathfrak{b} = \mathtt{1001}$:

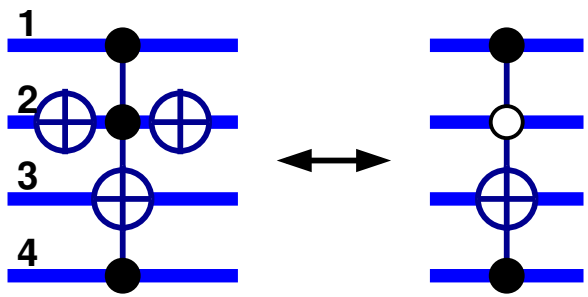
$$\begin{array}{l} 1{:}|\mathtt{0010}\rangle \\ 2{:}|\mathtt{1010}\rangle \\ 3{:}|\mathtt{1000}\rangle \\ 4{:}|\mathtt{1001}\rangle \end{array} \quad \longleftarrow \quad \begin{array}{l} 2{:}|\mathtt{1010}\rangle \\ 3{:}|\mathtt{1000}\rangle \\ 4{:}|\mathtt{1001}\rangle \\ 1{:}|\mathtt{0010}\rangle \end{array}$$



Universality: Permutations of Logical States

- $\mathbf{c}^k\mathbf{not}$ gates implement all logical state permutations.

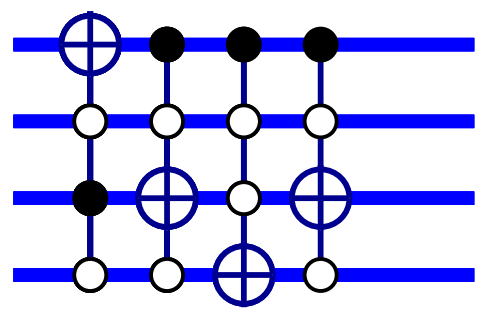
  Proof. Consider n qubits.
  - If $|\mathfrak{a} - \mathfrak{b}| = 1$, the transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.
    Example: $\mathfrak{a} = 1001$ and $\mathfrak{b} = 1011$:



$$\begin{cases} |1001\rangle & \rightarrow & |1011\rangle \\ |1011\rangle & \rightarrow & |1001\rangle \\ |\mathfrak{c}\rangle & \rightarrow & |\mathfrak{c}\rangle \quad \text{otherwise} \end{cases}$$

  - $\mathfrak{b}$ can be reached from $\mathfrak{a}$ by a sequence changing one bit at a time.
    Example: $\mathfrak{a} = 0010$ and $\mathfrak{b} = 1001$: $0010 \leftrightarrow 1010 \leftrightarrow 1000 \leftrightarrow 1001$
  - Every transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.
    Example: $\mathfrak{a} = 0010$ and $\mathfrak{b} = 1001$:

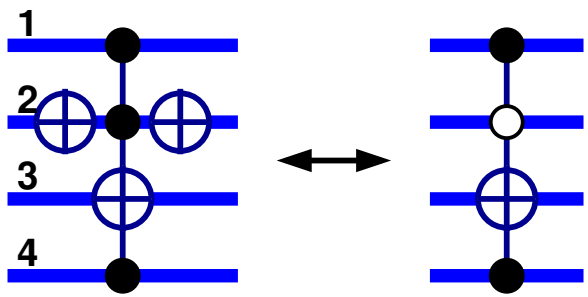
$$\begin{array}{l} 1{:}|0010\rangle \\ 2{:}|1010\rangle \\ 3{:}|1000\rangle \\ 4{:}|1001\rangle \end{array} \longleftarrow \begin{array}{l} 2{:}|1010\rangle \\ 4{:}|1001\rangle \\ 3{:}|1000\rangle \\ 1{:}|0010\rangle \end{array}$$



Universality: Permutations of Logical States

- $\mathbf{c}^k\mathbf{not}$ gates implement all logical state permutations.

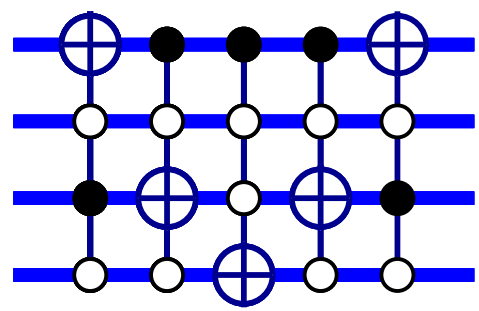
  Proof. Consider n qubits.
  - If $|\mathfrak{a} - \mathfrak{b}| = 1$, the transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.
    Example: $\mathfrak{a} = 1001$ and $\mathfrak{b} = 1011$:



$$\begin{cases} |1001\rangle & \rightarrow & |1011\rangle \\ |1011\rangle & \rightarrow & |1001\rangle \\ |\mathfrak{c}\rangle & \rightarrow & |\mathfrak{c}\rangle \quad \text{otherwise} \end{cases}$$

  - $\mathfrak{b}$ can be reached from $\mathfrak{a}$ by a sequence changing one bit at a time.
    Example: $\mathfrak{a} = 0010$ and $\mathfrak{b} = 1001$: $0010 \leftrightarrow 1010 \leftrightarrow 1000 \leftrightarrow 1001$
  - Every transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.
    Example: $\mathfrak{a} = 0010$ and $\mathfrak{b} = 1001$:

$$\begin{array}{l} 1{:}|0010\rangle \\ 2{:}|1010\rangle \\ 3{:}|1000\rangle \\ 4{:}|1001\rangle \end{array} \longleftarrow \begin{array}{l} 4{:}|1001\rangle \\ 2{:}|1010\rangle \\ 3{:}|1000\rangle \\ 1{:}|0010\rangle \end{array}$$

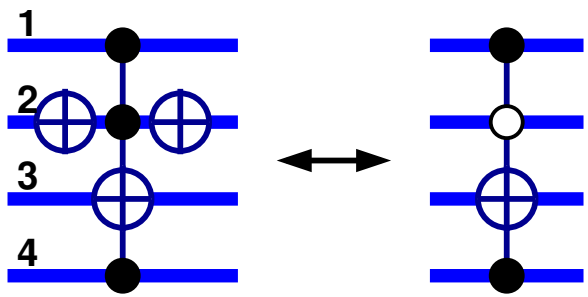


Universality: Permutations of Logical States

- $\mathbf{c}^k\mathbf{not}$ gates implement all logical state permutations.

  Proof. Consider n qubits.
  - If $|\mathfrak{a} - \mathfrak{b}| = 1$, the transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.

    Example: $\mathfrak{a} = 1001$ and $\mathfrak{b} = 1011$:



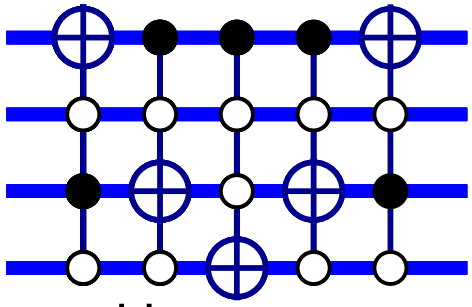
$$\begin{cases} |1001\rangle & \rightarrow & |1011\rangle \\ |1011\rangle & \rightarrow & |1001\rangle \\ |\mathfrak{c}\rangle & \rightarrow & |\mathfrak{c}\rangle \quad \text{otherwise} \end{cases}$$

  - $\mathfrak{b}$ can be reached from $\mathfrak{a}$ by a sequence changing one bit at a time.

    Example: $\mathfrak{a} = 0010$ and $\mathfrak{b} = 1001$: $0010 \leftrightarrow 1010 \leftrightarrow 1000 \leftrightarrow 1001$
  - Every transposition $|\mathfrak{a}\rangle \leftrightarrow |\mathfrak{b}\rangle$ is implementable.

    Example: $\mathfrak{a} = 0010$ and $\mathfrak{b} = 1001$:

$$\begin{array}{l} 1{:}|0010\rangle \\ 2{:}|1010\rangle \\ 3{:}|1000\rangle \\ 4{:}|1001\rangle \end{array} \longleftarrow \begin{array}{l} 4{:}|1001\rangle \\ 2{:}|1010\rangle \\ 3{:}|1000\rangle \\ 1{:}|0010\rangle \end{array}$$



  - Every permutation is a product of transpositions.

Universality: Unitary Operators

- Controlled^k one-qubit gates implement all unitary operators.

Universality: Unitary Operators

- Controlled^k one-qubit gates implement all unitary operators.

  Proof. Consider n qubits.

  For a one-qubit unitary U, define the "Givens rotation" $G(U, \mathfrak{a}, \mathfrak{b})$ by

  $$|\mathfrak{a}\rangle \to U_{00}|\mathfrak{a}\rangle + U_{10}|\mathfrak{b}\rangle,\ |\mathfrak{b}\rangle \to U_{01}|\mathfrak{a}\rangle + U_{11}|\mathfrak{b}\rangle \text{ and } |\mathfrak{c}\rangle \to |\mathfrak{c}\rangle \text{ (otherwise).}$$

Universality: Unitary Operators

- Controlled^k one-qubit gates implement all unitary operators.

  Proof. Consider n qubits.

  For a one-qubit unitary U, define the "Givens rotation" $G(U, \mathfrak{a}, \mathfrak{b})$ by

  $$|\mathfrak{a}\rangle \to U_{00}|\mathfrak{a}\rangle + U_{10}|\mathfrak{b}\rangle,\ |\mathfrak{b}\rangle \to U_{01}|\mathfrak{a}\rangle + U_{11}|\mathfrak{b}\rangle \text{ and } |\mathfrak{c}\rangle \to |\mathfrak{c}\rangle \text{ (otherwise).}$$

  - If $|\mathfrak{a} - \mathfrak{b}| = 1$ then $G(U, \mathfrak{a}, \mathfrak{b})$ is implementable.

Universality: Unitary Operators

- Controlled^k one-qubit gates implement all unitary operators.

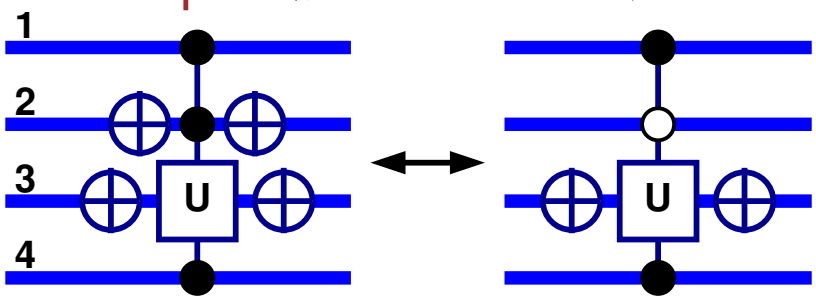
  Proof. Consider n qubits.

  For a one-qubit unitary U, define the "Givens rotation" $G(U, \mathfrak{a}, \mathfrak{b})$ by

  $$|\mathfrak{a}\rangle \to U_{00}|\mathfrak{a}\rangle + U_{10}|\mathfrak{b}\rangle,\ |\mathfrak{b}\rangle \to U_{01}|\mathfrak{a}\rangle + U_{11}|\mathfrak{b}\rangle \text{ and } |\mathfrak{c}\rangle \to |\mathfrak{c}\rangle \text{ (otherwise).}$$

  - If $|\mathfrak{a} - \mathfrak{b}| = 1$ then $G(U, \mathfrak{a}, \mathfrak{b})$ is implementable.

    Example: $\mathfrak{a} = \mathtt{1011}$ and $\mathfrak{b} = \mathtt{1001}$:



$$\begin{cases} |\mathtt{1011}\rangle & \to & U_{00}|\mathtt{1011}\rangle + U_{01}|\mathtt{1001}\rangle \\ |\mathtt{1001}\rangle & \to & U_{10}|\mathtt{1011}\rangle + U_{11}|\mathtt{1011}\rangle \\ |\mathfrak{c}\rangle & \to & |\mathfrak{c}\rangle \ \text{ otherwise} \end{cases}$$

Universality: Unitary Operators

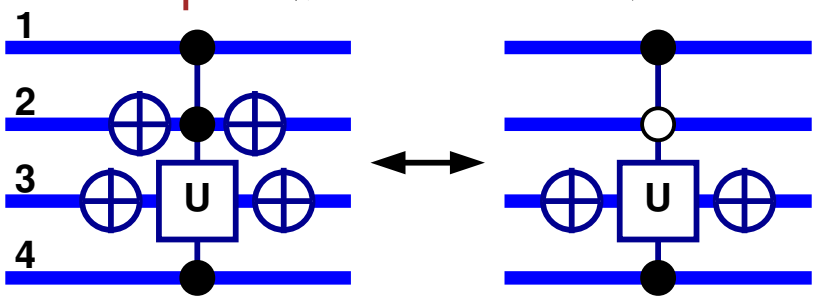
- Controlled^k one-qubit gates implement all unitary operators.

  Proof. Consider n qubits.

  For a one-qubit unitary U, define the "Givens rotation" $G(U, \mathfrak{a}, \mathfrak{b})$ by

  $$|\mathfrak{a}\rangle \to U_{00}|\mathfrak{a}\rangle + U_{10}|\mathfrak{b}\rangle,\ |\mathfrak{b}\rangle \to U_{01}|\mathfrak{a}\rangle + U_{11}|\mathfrak{b}\rangle \text{ and } |\mathfrak{c}\rangle \to |\mathfrak{c}\rangle \text{ (otherwise).}$$

  - If $|\mathfrak{a} - \mathfrak{b}| = 1$ then $G(U, \mathfrak{a}, \mathfrak{b})$ is implementable.
    Example: $\mathfrak{a} = \mathtt{1011}$ and $\mathfrak{b} = \mathtt{1001}$:



$$\begin{cases} |\mathtt{1011}\rangle & \to & U_{00}|\mathtt{1011}\rangle + U_{01}|\mathtt{1001}\rangle \\ |\mathtt{1001}\rangle & \to & U_{10}|\mathtt{1011}\rangle + U_{11}|\mathtt{1011}\rangle \\ |\mathfrak{c}\rangle & \to & |\mathfrak{c}\rangle \ \text{ otherwise} \end{cases}$$

  - Let P be a permutation that maps $\mathfrak{a} \to \mathfrak{a}'$ and $\mathfrak{b} \to \mathfrak{b}'$.
    Then $G(U, \mathfrak{a}', \mathfrak{b}') = PG(U, \mathfrak{a}, \mathfrak{b})P^\dagger$.

Universality: Unitary Operators

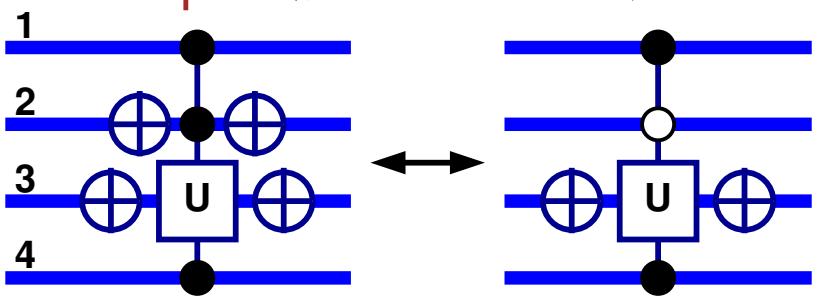
- Controlled^k one-qubit gates implement all unitary operators.

  Proof. Consider n qubits.

  For a one-qubit unitary U, define the "Givens rotation" $G(U, \mathfrak{a}, \mathfrak{b})$ by

  $$|\mathfrak{a}\rangle \to U_{00}|\mathfrak{a}\rangle + U_{10}|\mathfrak{b}\rangle,\ |\mathfrak{b}\rangle \to U_{01}|\mathfrak{a}\rangle + U_{11}|\mathfrak{b}\rangle \text{ and } |\mathfrak{c}\rangle \to |\mathfrak{c}\rangle \text{ (otherwise).}$$

  - If $|\mathfrak{a} - \mathfrak{b}| = 1$ then $G(U, \mathfrak{a}, \mathfrak{b})$ is implementable.
    Example: $\mathfrak{a} = \mathtt{1011}$ and $\mathfrak{b} = \mathtt{1001}$:



$$\left\{\begin{array}{lcl} |\mathtt{1011}\rangle & \to & U_{00}|\mathtt{1011}\rangle + U_{01}|\mathtt{1001}\rangle \\ |\mathtt{1001}\rangle & \to & U_{10}|\mathtt{1011}\rangle + U_{11}|\mathtt{1011}\rangle \\ |\mathfrak{c}\rangle & \to & |\mathfrak{c}\rangle \ \text{ otherwise} \end{array}\right.$$

  - Let P be a permutation that maps $\mathfrak{a} \to \mathfrak{a}'$ and $\mathfrak{b} \to \mathfrak{b}'$.
    Then $G(U, \mathfrak{a}', \mathfrak{b}') = PG(U, \mathfrak{a}, \mathfrak{b})P^\dagger$.

$$\left.\begin{array}{c} |\mathfrak{a}'\rangle \\ |\mathfrak{b}'\rangle \end{array}\right\} \xrightarrow{P^\dagger} \left\{\begin{array}{c} |\mathfrak{a}\rangle \\ |\mathfrak{b}\rangle \end{array}\right\}$$

Universality: Unitary Operators

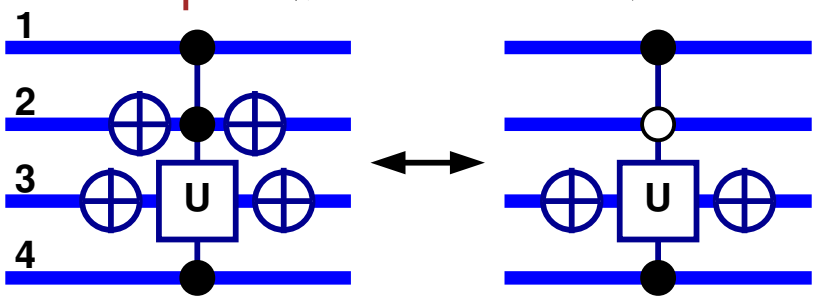
- Controlled^k one-qubit gates implement all unitary operators.

  Proof. Consider n qubits.

  For a one-qubit unitary U, define the "Givens rotation" $G(U, \mathfrak{a}, \mathfrak{b})$ by

  $$|\mathfrak{a}\rangle \to U_{00}|\mathfrak{a}\rangle + U_{10}|\mathfrak{b}\rangle,\ |\mathfrak{b}\rangle \to U_{01}|\mathfrak{a}\rangle + U_{11}|\mathfrak{b}\rangle \text{ and } |\mathfrak{c}\rangle \to |\mathfrak{c}\rangle \text{ (otherwise).}$$

  - If $|\mathfrak{a} - \mathfrak{b}| = 1$ then $G(U, \mathfrak{a}, \mathfrak{b})$ is implementable.
    Example: $\mathfrak{a} = \mathtt{1011}$ and $\mathfrak{b} = \mathtt{1001}$:



$$\left\{\begin{array}{lcl} |\mathtt{1011}\rangle & \to & U_{00}|\mathtt{1011}\rangle + U_{01}|\mathtt{1001}\rangle \\ |\mathtt{1001}\rangle & \to & U_{10}|\mathtt{1011}\rangle + U_{11}|\mathtt{1011}\rangle \\ |\mathfrak{c}\rangle & \to & |\mathfrak{c}\rangle \ \text{ otherwise} \end{array}\right.$$

  - Let P be a permutation that maps $\mathfrak{a} \to \mathfrak{a}'$ and $\mathfrak{b} \to \mathfrak{b}'$.
    Then $G(U, \mathfrak{a}', \mathfrak{b}') = PG(U, \mathfrak{a}, \mathfrak{b})P^\dagger$.

$$\left.\begin{array}{c} |\mathfrak{a}'\rangle \\ |\mathfrak{b}'\rangle \end{array}\right\} \xrightarrow{P^\dagger} \left\{\begin{array}{c} |\mathfrak{a}\rangle \\ |\mathfrak{b}\rangle \end{array}\right\} \xrightarrow{G(U,\mathfrak{a},\mathfrak{b})} \left\{\begin{array}{c} U_{00}|\mathfrak{a}\rangle + U_{10}|\mathfrak{b}\rangle \\ U_{01}|\mathfrak{a}\rangle + U_{11}|\mathfrak{b}\rangle \end{array}\right\}$$

Universality: Unitary Operators

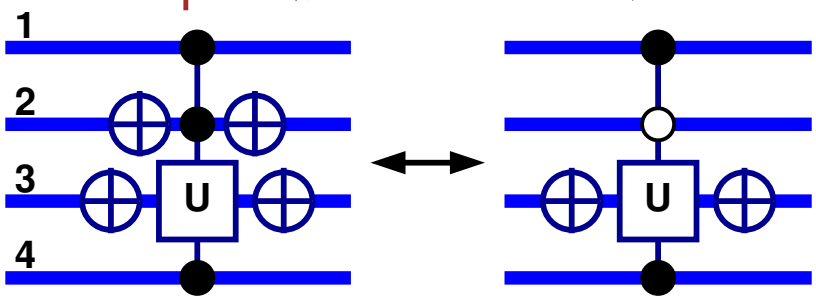
- Controlled^k one-qubit gates implement all unitary operators.

  Proof. Consider n qubits.

  For a one-qubit unitary U, define the "Givens rotation" $G(U, \mathfrak{a}, \mathfrak{b})$ by

  $$|\mathfrak{a}\rangle \to U_{00}|\mathfrak{a}\rangle + U_{10}|\mathfrak{b}\rangle,\ |\mathfrak{b}\rangle \to U_{01}|\mathfrak{a}\rangle + U_{11}|\mathfrak{b}\rangle \text{ and } |\mathfrak{c}\rangle \to |\mathfrak{c}\rangle \text{ (otherwise).}$$

  - If $|\mathfrak{a} - \mathfrak{b}| = 1$ then $G(U, \mathfrak{a}, \mathfrak{b})$ is implementable.
    Example: $\mathfrak{a} = \mathtt{1011}$ and $\mathfrak{b} = \mathtt{1001}$:



$$\left\{\begin{array}{lcl} |\mathtt{1011}\rangle & \to & U_{00}|\mathtt{1011}\rangle + U_{01}|\mathtt{1001}\rangle \\ |\mathtt{1001}\rangle & \to & U_{10}|\mathtt{1011}\rangle + U_{11}|\mathtt{1011}\rangle \\ |\mathfrak{c}\rangle & \to & |\mathfrak{c}\rangle \ \text{ otherwise} \end{array}\right.$$

  - Let P be a permutation that maps $\mathfrak{a} \to \mathfrak{a}'$ and $\mathfrak{b} \to \mathfrak{b}'$.
    Then $G(U, \mathfrak{a}', \mathfrak{b}') = PG(U, \mathfrak{a}, \mathfrak{b})P^\dagger$.

$$\left.\begin{array}{c} |\mathfrak{a}'\rangle \\ |\mathfrak{b}'\rangle \end{array}\right\} \xrightarrow{P^\dagger} \left\{\begin{array}{c} |\mathfrak{a}\rangle \\ |\mathfrak{b}\rangle \end{array}\right\} \xrightarrow{G(U,\mathfrak{a},\mathfrak{b})} \left\{\begin{array}{c} U_{00}|\mathfrak{a}\rangle + U_{10}|\mathfrak{b}\rangle \\ U_{01}|\mathfrak{a}\rangle + U_{11}|\mathfrak{b}\rangle \end{array}\right\} \xrightarrow{P} \left\{\begin{array}{c} U_{00}|\mathfrak{a}'\rangle + U_{10}|\mathfrak{b}'\rangle \\ U_{01}|\mathfrak{a}'\rangle + U_{11}|\mathfrak{b}'\rangle \end{array}\right.$$

Universality: Unitary Operators

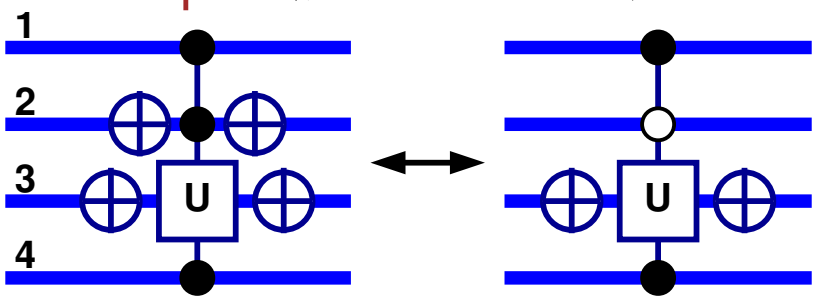
- Controlled^k one-qubit gates implement all unitary operators.

  Proof. Consider n qubits.

  For a one-qubit unitary U, define the "Givens rotation" $G(U, \mathfrak{a}, \mathfrak{b})$ by

  $$|\mathfrak{a}\rangle \to U_{00}|\mathfrak{a}\rangle + U_{10}|\mathfrak{b}\rangle,\ |\mathfrak{b}\rangle \to U_{01}|\mathfrak{a}\rangle + U_{11}|\mathfrak{b}\rangle \text{ and } |\mathfrak{c}\rangle \to |\mathfrak{c}\rangle \text{ (otherwise).}$$

  - If $|\mathfrak{a} - \mathfrak{b}| = 1$ then $G(U, \mathfrak{a}, \mathfrak{b})$ is implementable.
    Example: $\mathfrak{a} = \mathtt{1011}$ and $\mathfrak{b} = \mathtt{1001}$:



$$\left\{\begin{array}{lcl} |\mathtt{1011}\rangle & \to & U_{00}|\mathtt{1011}\rangle + U_{01}|\mathtt{1001}\rangle \\ |\mathtt{1001}\rangle & \to & U_{10}|\mathtt{1011}\rangle + U_{11}|\mathtt{1011}\rangle \\ |\mathfrak{c}\rangle & \to & |\mathfrak{c}\rangle \ \text{ otherwise} \end{array}\right.$$

  - Let P be a permutation that maps $\mathfrak{a} \to \mathfrak{a}'$ and $\mathfrak{b} \to \mathfrak{b}'$.
    Then $G(U, \mathfrak{a}', \mathfrak{b}') = PG(U, \mathfrak{a}, \mathfrak{b})P^\dagger$.

$$\left.\begin{array}{c} |\mathfrak{a}'\rangle \\ |\mathfrak{b}'\rangle \end{array}\right\} \xrightarrow{P^\dagger} \left\{\begin{array}{c} |\mathfrak{a}\rangle \\ |\mathfrak{b}\rangle \end{array}\right\} \xrightarrow{G(U,\mathfrak{a},\mathfrak{b})} \left\{\begin{array}{c} U_{00}|\mathfrak{a}\rangle + U_{10}|\mathfrak{b}\rangle \\ U_{01}|\mathfrak{a}\rangle + U_{11}|\mathfrak{b}\rangle \end{array}\right\} \xrightarrow{P} \left\{\begin{array}{c} U_{00}|\mathfrak{a}'\rangle + U_{10}|\mathfrak{b}'\rangle \\ U_{01}|\mathfrak{a}'\rangle + U_{11}|\mathfrak{b}'\rangle \end{array}\right.$$

  - Every Givens rotation is implementable.

Universality: Unitary Operators

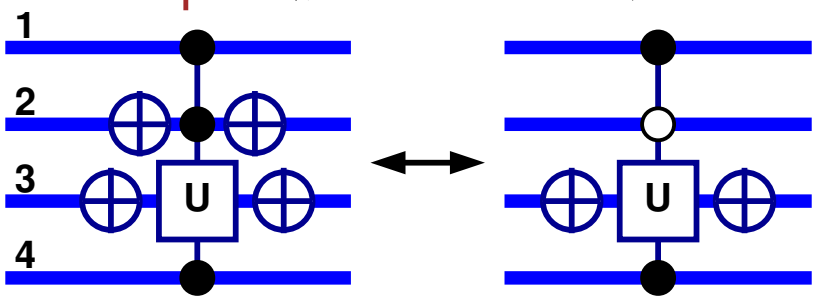
- Controlled^k one-qubit gates implement all unitary operators.

  Proof. Consider n qubits.

  For a one-qubit unitary U, define the "Givens rotation" $G(U, \mathfrak{a}, \mathfrak{b})$ by

  $$|\mathfrak{a}\rangle \to U_{00}|\mathfrak{a}\rangle + U_{10}|\mathfrak{b}\rangle,\ |\mathfrak{b}\rangle \to U_{01}|\mathfrak{a}\rangle + U_{11}|\mathfrak{b}\rangle \text{ and } |\mathfrak{c}\rangle \to |\mathfrak{c}\rangle \text{ (otherwise).}$$

  - If $|\mathfrak{a} - \mathfrak{b}| = 1$ then $G(U, \mathfrak{a}, \mathfrak{b})$ is implementable.
    Example: $\mathfrak{a} = \mathtt{1011}$ and $\mathfrak{b} = \mathtt{1001}$:



$$\left\{\begin{array}{lcl} |\mathtt{1011}\rangle & \to & U_{00}|\mathtt{1011}\rangle + U_{01}|\mathtt{1001}\rangle \\ |\mathtt{1001}\rangle & \to & U_{10}|\mathtt{1011}\rangle + U_{11}|\mathtt{1011}\rangle \\ |\mathfrak{c}\rangle & \to & |\mathfrak{c}\rangle \ \text{ otherwise} \end{array}\right.$$

  - Let P be a permutation that maps $\mathfrak{a} \to \mathfrak{a}'$ and $\mathfrak{b} \to \mathfrak{b}'$.
    Then $G(U, \mathfrak{a}', \mathfrak{b}') = PG(U, \mathfrak{a}, \mathfrak{b})P^\dagger$.

$$\left.\begin{array}{c} |\mathfrak{a}'\rangle \\ |\mathfrak{b}'\rangle \end{array}\right\} \xrightarrow{P^\dagger} \left\{\begin{array}{c} |\mathfrak{a}\rangle \\ |\mathfrak{b}\rangle \end{array}\right\} \xrightarrow{G(U,\mathfrak{a},\mathfrak{b})} \left\{\begin{array}{c} U_{00}|\mathfrak{a}\rangle + U_{10}|\mathfrak{b}\rangle \\ U_{01}|\mathfrak{a}\rangle + U_{11}|\mathfrak{b}\rangle \end{array}\right\} \xrightarrow{P} \left\{\begin{array}{c} U_{00}|\mathfrak{a}'\rangle + U_{10}|\mathfrak{b}'\rangle \\ U_{01}|\mathfrak{a}'\rangle + U_{11}|\mathfrak{b}'\rangle \end{array}\right.$$

  - Every Givens rotation is implementable.
  - Every unitary operator is a product of Givens rotations.

Givens Rotation Decomposition

- Decomposing a unitary matrix by example.

$$M$$

$$\begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}$$

$$= \begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}$$

Givens Rotation Decomposition

- Decomposing a unitary matrix by example.

$$M$$

$$\begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}$$

$$= \begin{pmatrix} \boxed{.384} & .250 & -.594 & .661 \\ \boxed{.288} & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}$$

Givens Rotation Decomposition

- Decomposing a unitary matrix by example.

$$
\underset{G_{12}}{\begin{pmatrix} .8 & .6 & .0 & .0 \\ -.6 & .8 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}}
\underset{M}{\begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}}
$$

$$
= \begin{pmatrix} \boxed{.480} & -.168 & -.166 & .845 \\ \boxed{.0} & -.640 & .768 & .024 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}
$$

Givens Rotation Decomposition

- Decomposing a unitary matrix by example.

$$
\underbrace{\begin{pmatrix} .8 & .6 & .0 & .0 \\ -.6 & .8 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}}_{G_{12}}
\underbrace{\begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}}_{M}
$$

$$
= \begin{pmatrix} \boxed{.480} & -.168 & -.166 & .845 \\ .0 & -.640 & .768 & .024 \\ \boxed{.640} & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}
$$

Givens Rotation Decomposition

- Decomposing a unitary matrix by example.

$$
\underset{G_{13}}{\begin{pmatrix} .6 & .0 & .8 & .0 \\ .0 & 1 & .0 & .0 \\ -.8 & .0 & .6 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}}
\underset{G_{12}}{\begin{pmatrix} .8 & .6 & .0 & .0 \\ -.6 & .8 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}}
\underset{M}{\begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}}
$$

$$
= \begin{pmatrix} \boxed{.800} & .360 & .288 & .384 \\ .0 & -.640 & .768 & .024 \\ \boxed{.0} & .480 & .424 & -.768 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}
$$

Givens Rotation Decomposition

- Decomposing a unitary matrix by example.

$$\underset{G_{13}}{\begin{pmatrix} .6 & .0 & .8 & .0 \\ .0 & 1 & .0 & .0 \\ -.8 & .0 & .6 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \underset{G_{12}}{\begin{pmatrix} .8 & .6 & .0 & .0 \\ -.6 & .8 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \underset{M}{\begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}}$$

$$= \begin{pmatrix} \boxed{.800} & .360 & .288 & .384 \\ .0 & -.640 & .768 & .024 \\ .0 & .480 & .424 & -.768 \\ \boxed{.600} & -.480 & -.384 & -.512 \end{pmatrix}$$

Givens Rotation Decomposition

- Decomposing a unitary matrix by example.

$$\underset{G_{14}}{\begin{pmatrix} .8 & .0 & .0 & .6 \\ .0 & 1 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .6 & .0 & .0 & -.8 \end{pmatrix}} \underset{G_{13}}{\begin{pmatrix} .6 & .0 & .8 & .0 \\ .0 & 1 & .0 & .0 \\ -.8 & .0 & .6 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \underset{G_{12}}{\begin{pmatrix} .8 & .6 & .0 & .0 \\ -.6 & .8 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \underset{M}{\begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}}$$

$$= \begin{pmatrix} \boxed{1} & .0 & .0 & .0 \\ .0 & -.640 & .768 & .024 \\ .0 & .480 & .424 & -.768 \\ \boxed{.0} & .600 & .480 & -.640 \end{pmatrix}$$

Givens Rotation Decomposition

- Decomposing a unitary matrix by example.

$$\underset{G_{14}}{\begin{pmatrix} .8 & .0 & .0 & .6 \\ .0 & 1 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .6 & .0 & .0 & -.8 \end{pmatrix}} \underset{G_{13}}{\begin{pmatrix} .6 & .0 & .8 & .0 \\ .0 & 1 & .0 & .0 \\ -.8 & .0 & .6 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \underset{G_{12}}{\begin{pmatrix} .8 & .6 & .0 & .0 \\ -.6 & .8 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \underset{M}{\begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}}$$

$$= \begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & \boxed{-.640} & .768 & .024 \\ .0 & \boxed{.480} & .424 & -.768 \\ .0 & .600 & .480 & -.640 \end{pmatrix}$$

Givens Rotation Decomposition

- Decomposing a unitary matrix by example.

$$\overset{G_{23}}{\begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & .8 & -.6 & .0 \\ .0 & .6 & .8 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \times$$

$$\overset{G_{14}}{\begin{pmatrix} .8 & .0 & .0 & .6 \\ .0 & 1 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .6 & .0 & .0 & -.8 \end{pmatrix}} \overset{G_{13}}{\begin{pmatrix} .6 & .0 & .8 & .0 \\ .0 & 1 & .0 & .0 \\ -.8 & .0 & .6 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \overset{G_{12}}{\begin{pmatrix} .8 & .6 & .0 & .0 \\ -.6 & .8 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \overset{M}{\begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}}$$

$$= \begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & \boxed{-.800} & .360 & .480 \\ .0 & \boxed{.0} & .800 & -.600 \\ .0 & .600 & .480 & .640 \end{pmatrix}$$

Givens Rotation Decomposition

- Decomposing a unitary matrix by example.

$$\overset{G_{23}}{\begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & .8 & -.6 & .0 \\ .0 & .6 & .8 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \times$$

$$\overset{G_{14}}{\begin{pmatrix} .8 & .0 & .0 & .6 \\ .0 & 1 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .6 & .0 & .0 & -.8 \end{pmatrix}} \overset{G_{13}}{\begin{pmatrix} .6 & .0 & .8 & .0 \\ .0 & 1 & .0 & .0 \\ -.8 & .0 & .6 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \overset{G_{12}}{\begin{pmatrix} .8 & .6 & .0 & .0 \\ -.6 & .8 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \overset{M}{\begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}}$$

$$= \begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & \boxed{-.800} & .360 & .480 \\ .0 & .0 & .800 & -.600 \\ .0 & \boxed{.600} & .480 & .640 \end{pmatrix}$$

Givens Rotation Decomposition

- Decomposing a unitary matrix by example.

$$\overset{G_{24}}{\begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & -.8 & .0 & .6 \\ .0 & .0 & 1 & .0 \\ .0 & .6 & .0 & .8 \end{pmatrix}} \overset{G_{23}}{\begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & .8 & -.6 & .0 \\ .0 & .6 & .8 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \times$$

$$\overset{G_{14}}{\begin{pmatrix} .8 & .0 & .0 & .6 \\ .0 & 1 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .6 & .0 & .0 & -.8 \end{pmatrix}} \overset{G_{13}}{\begin{pmatrix} .6 & .0 & .8 & .0 \\ .0 & 1 & .0 & .0 \\ -.8 & .0 & .6 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \overset{G_{12}}{\begin{pmatrix} .8 & .6 & .0 & .0 \\ -.6 & .8 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \overset{M}{\begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}}$$

$$= \begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & \boxed{1} & .0 & .0 \\ .0 & .0 & .800 & -.600 \\ .0 & \boxed{.0} & .600 & .800 \end{pmatrix}$$

Givens Rotation Decomposition

- Decomposing a unitary matrix by example.

$$\overset{G_{24}}{\begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & -.8 & .0 & .6 \\ .0 & .0 & 1 & .0 \\ .0 & .6 & .0 & .8 \end{pmatrix}} \overset{G_{23}}{\begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & .8 & -.6 & .0 \\ .0 & .6 & .8 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \times$$

$$\overset{G_{14}}{\begin{pmatrix} .8 & .0 & .0 & .6 \\ .0 & 1 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .6 & .0 & .0 & -.8 \end{pmatrix}} \overset{G_{13}}{\begin{pmatrix} .6 & .0 & .8 & .0 \\ .0 & 1 & .0 & .0 \\ -.8 & .0 & .6 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \overset{G_{12}}{\begin{pmatrix} .8 & .6 & .0 & .0 \\ -.6 & .8 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \overset{M}{\begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}}$$

$$= \begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & 1 & .0 & .0 \\ .0 & .0 & \boxed{.800} & -.600 \\ .0 & .0 & \boxed{.600} & .800 \end{pmatrix}$$

Givens Rotation Decomposition

- Decomposing a unitary matrix by example.

$$\overset{G_{34}}{\begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & 1 & .0 & .0 \\ .0 & .0 & .8 & .6 \\ .0 & .0 & -.6 & .8 \end{pmatrix}} \overset{G_{24}}{\begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & -.8 & .0 & .6 \\ .0 & .0 & 1 & .0 \\ .0 & .6 & .0 & .8 \end{pmatrix}} \overset{G_{23}}{\begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & .8 & -.6 & .0 \\ .0 & .6 & .8 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \times$$

$$\overset{G_{14}}{\begin{pmatrix} .8 & .0 & .0 & .6 \\ .0 & 1 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .6 & .0 & .0 & -.8 \end{pmatrix}} \overset{G_{13}}{\begin{pmatrix} .6 & .0 & .8 & .0 \\ .0 & 1 & .0 & .0 \\ -.8 & .0 & .6 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \overset{G_{12}}{\begin{pmatrix} .8 & .6 & .0 & .0 \\ -.6 & .8 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \overset{M}{\begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}}$$

$$= \begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & 1 & .0 & .0 \\ .0 & .0 & \boxed{1} & .0 \\ .0 & .0 & \boxed{.0} & 1 \end{pmatrix}$$

Givens Rotation Decomposition

- Decomposing a unitary matrix by example.

$$\overset{G_{34}}{\begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & 1 & .0 & .0 \\ .0 & .0 & .8 & .6 \\ .0 & .0 & -.6 & .8 \end{pmatrix}} \overset{G_{24}}{\begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & -.8 & .0 & .6 \\ .0 & .0 & 1 & .0 \\ .0 & .6 & .0 & .8 \end{pmatrix}} \overset{G_{23}}{\begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & .8 & -.6 & .0 \\ .0 & .6 & .8 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \times$$

$$\overset{G_{14}}{\begin{pmatrix} .8 & .0 & .0 & .6 \\ .0 & 1 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .6 & .0 & .0 & -.8 \end{pmatrix}} \overset{G_{13}}{\begin{pmatrix} .6 & .0 & .8 & .0 \\ .0 & 1 & .0 & .0 \\ -.8 & .0 & .6 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \overset{G_{12}}{\begin{pmatrix} .8 & .6 & .0 & .0 \\ -.6 & .8 & .0 & .0 \\ .0 & .0 & 1 & .0 \\ .0 & .0 & .0 & 1 \end{pmatrix}} \overset{M}{\begin{pmatrix} .384 & .250 & -.594 & .661 \\ .288 & -.613 & .514 & .526 \\ .640 & .576 & .485 & -.154 \\ .600 & -.480 & -.384 & -.512 \end{pmatrix}}$$

$$M = G_{12}^{\dagger} G_{13}^{\dagger} G_{14}^{\dagger} G_{23}^{\dagger} G_{24}^{\dagger} G_{34}^{\dagger} = \begin{pmatrix} 1 & .0 & .0 & .0 \\ .0 & 1 & .0 & .0 \\ .0 & .0 & \boxed{1} & .0 \\ .0 & .0 & \boxed{.0} & 1 \end{pmatrix}$$

Universality: Resources

Consider n qubit unitary operators.

- The number of $\mathbf{cnot}$ and one-qubit gates needed to implement a unitary operator U is

$$O((2^n)^2) = O(4^n)$$

Vartiainen&al 2003 [2]

*. . . except for an exponentially small fraction according to the Haar measure.

Universality: Resources

Consider n qubit unitary operators.

- The number of $\mathbf{cnot}$ and one-qubit gates needed to implement a unitary operator U is

$$O((2^n)^2) = O(4^n)$$

Vartiainen&al 2003 [2]

- There are unitary operators that require $\Omega(4^n)$ $\mathbf{cnot}$ and one-qubit gates.

Barenco&al 1995 [1]

*. . . except for an exponentially small fraction according to the Haar measure.

Universality: Resources

Consider n qubit unitary operators.

- The number of $\mathbf{cnot}$ and one-qubit gates needed to implement a unitary operator U is
$$O((2^n)^2) = O(4^n)$$

Vartiainen&al 2003 [2]

- There are unitary operators that require $\Omega(4^n)$ $\mathbf{cnot}$ and one-qubit gates.

Barenco&al 1995 [1]

- Almost all* unitary operators require $2^{\Omega(n)}$ $\mathbf{cnot}$ and one-qubit gates to approximate U with error $c - \epsilon$, where c is the average distance between unitary operators.

Knill 1995 [3, 4]

*. . . except for an exponentially small fraction according to the Haar measure.

Contents

Title: IQI 04, Seminar 8 0
Gate Set . . . . . top . . . 1
Controlled Sign Flips 2
Controlled Sign Flip Implementations I . . . . . top . . . 3
Controlled Sign Flip Implementations II 4
Controlled Sign Flip Implementations III . . . . . top . . . 5
Controlled Sign Flip Implementations IV . . . . . top . . . 6
Controlled^2 Unitary . . . . . top . . . 7
Toffoli Gate up to Control Phases I . . . . . top . . . 8
Toffoli Gate up to Control Phases II 9
Adding Controls . . . . . top . . . 10
Adding Controls without Prepared Ancillas . . . . . top . . . 11
Controlled U With 0 or 1 Extra Qubit I . . . . . top . . . 12
Controlled U With 0 or 1 Extra Qubit II 13
From U to Controlled U? . . . . . top . . . 14
Universality: Permutations of Logical States . . . . . top . . . 15
Universality: Unitary Operators . . . . . top . . . 16
Givens Rotation Decomposition . . . . . top . . . 17
Universality: Resources . . . . . top . . . 18
References 20

References

[1] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457–3467, 1995.

[2] J. J. Vartiainen, M. Möttönen, and M. M. Salomaa. Efficient decomposition of quantum gates. quant-ph/0312218, 2003.

[3] E. Knill. Approximation by quantum circuits. Technical Report LAUR-95-2225, Los Alamos National Laboratory, `knill@lanl.gov`, 1995. quant-ph/9508006.

[4] E. Knill. Bounds for approximation in total variation distance by quantum circuits. Technical Report LAUR-95-2724, Los Alamos National Laboratory, 1995. quant-ph/9508007.