ECE 550/650 QC
Grover Search

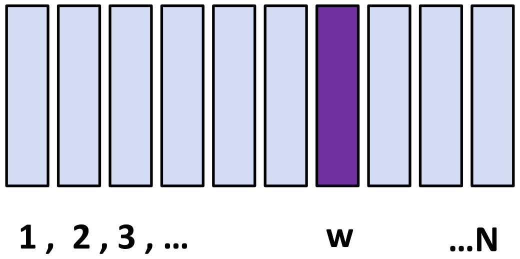
Robert Niffenegger

UMass Amherst | College of Engineering

Grover Search

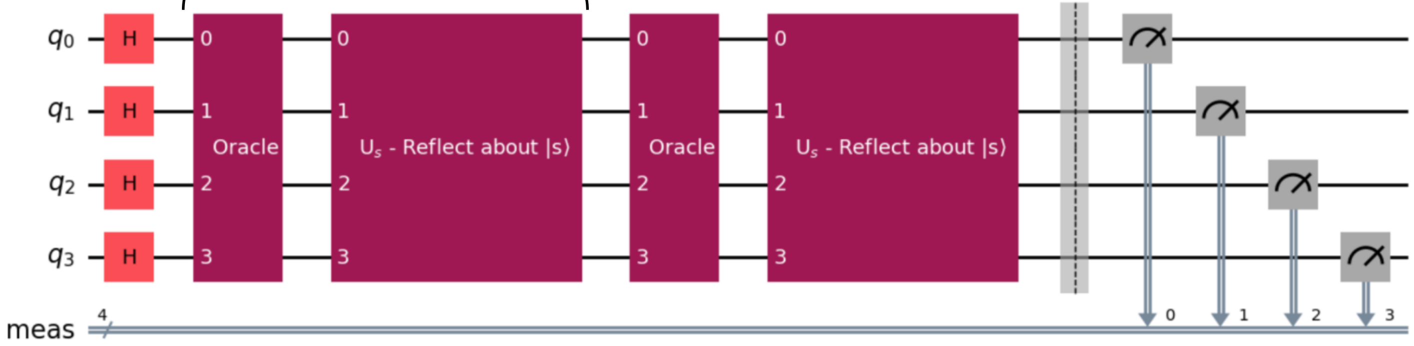
N objects
n bits in register

N = 2^n



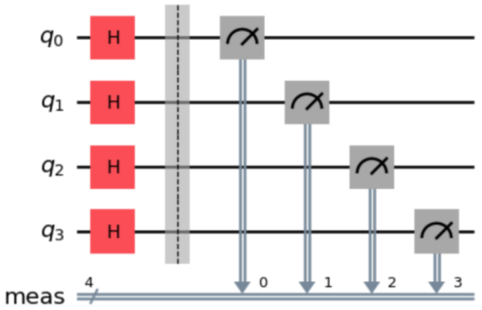
$\frac{\pi}{4}\sqrt{N}$ **iterations**

n qubits

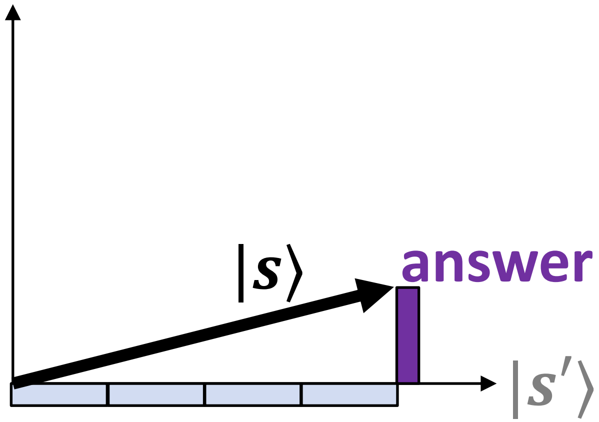


Multi-qubit superposition state $\equiv |s\rangle$

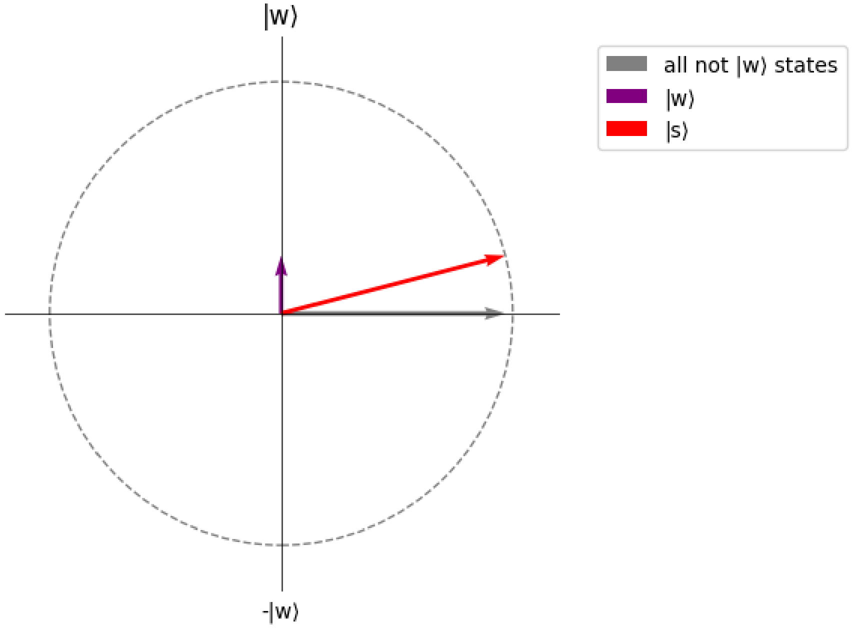
$$|s\rangle = |+\rangle\,|+\rangle\,|+\rangle\,|+\rangle\;\; = |+\rangle^{\otimes N}$$



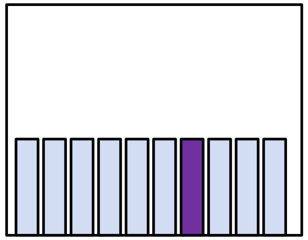
answer
'basis'
$|w\rangle$



'not answers'



$|s\rangle \equiv$ **superposition state**

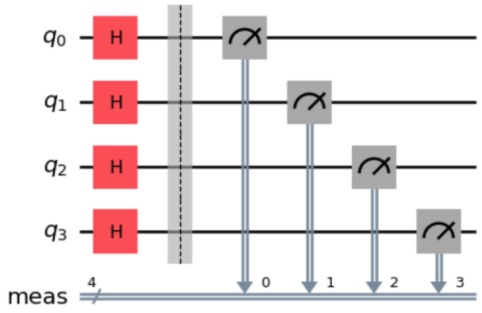


amplitudes all $1/\sqrt{N}$

Answer is equally likely as the other N-1 possibilities

The angle will be $\theta = \arcsin(1/\sqrt{N}) = \arcsin(1/4) \approx\; 15\text{deg}$

Superposition state $\equiv |s\rangle$ in the 'answer basis'

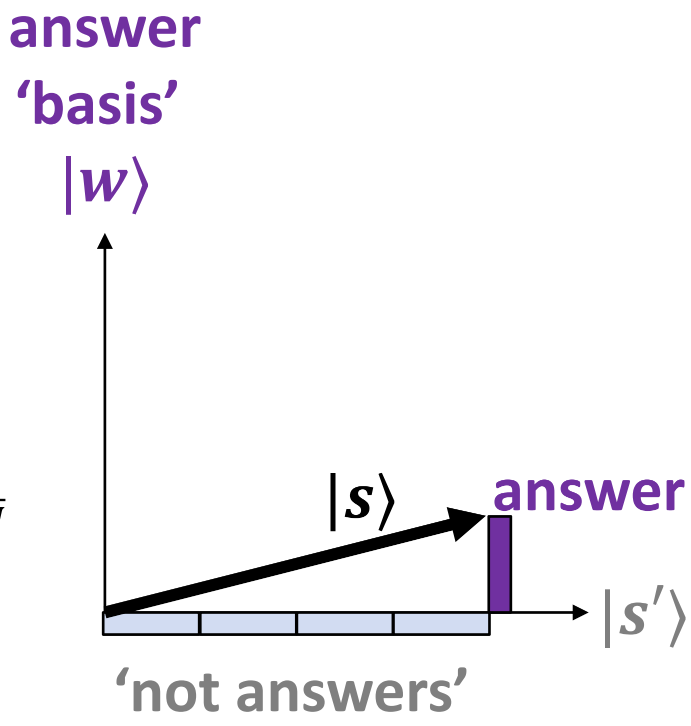


$$|s\rangle = |+\rangle\,|+\rangle\,|+\rangle\,|+\rangle \;= |+\rangle^{\otimes N}$$

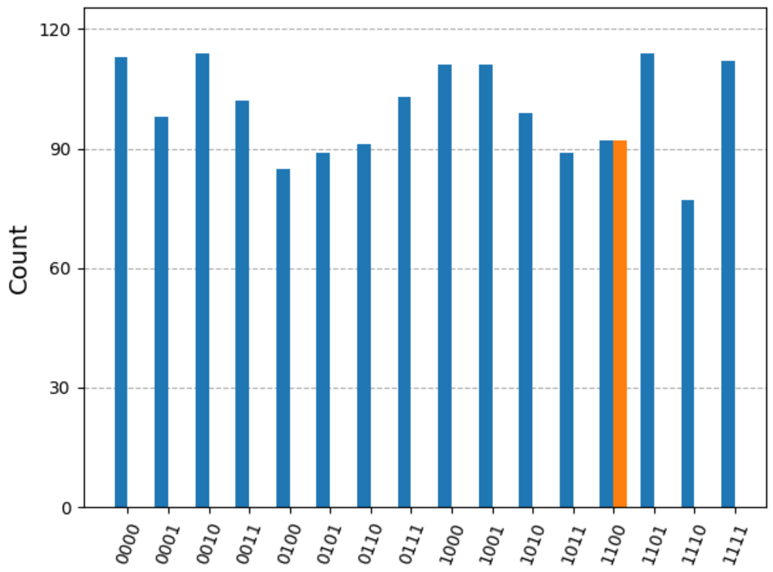
$|s\rangle \equiv$ superposition state

amplitudes all $1/\sqrt{N}$

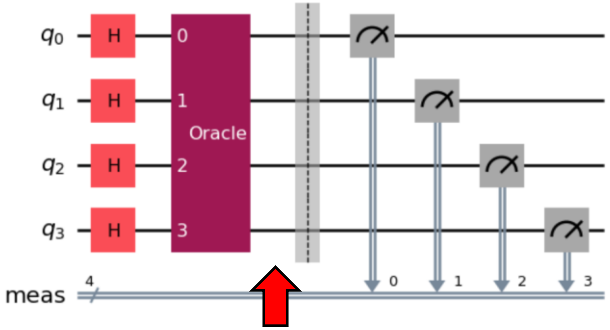
Answer is equally likely as the other N-1 possibilities



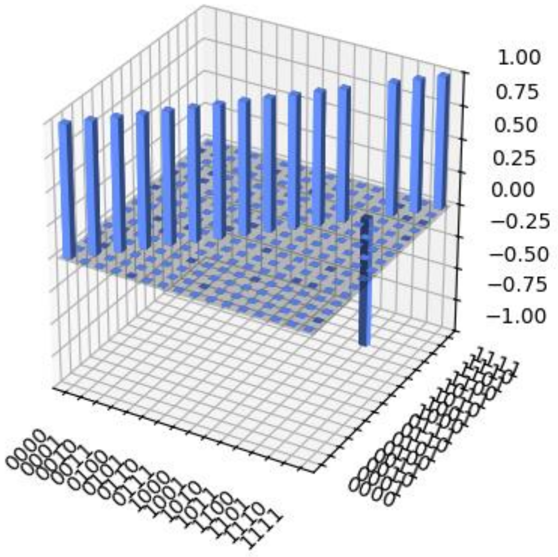
$$|s\rangle = \frac{1}{\sqrt{N}}\left((N-1)|s\rangle' + |w\rangle\right)$$

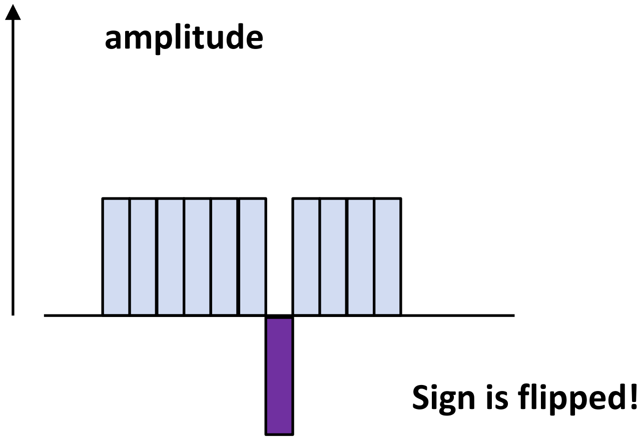


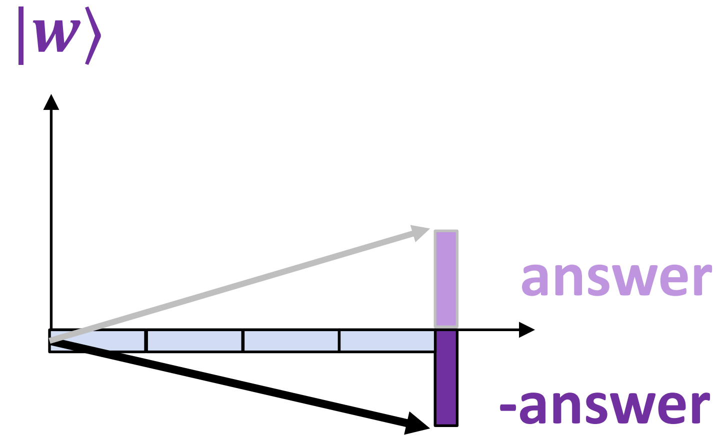
Apply the “Oracle”



Real Amplitude (ρ)

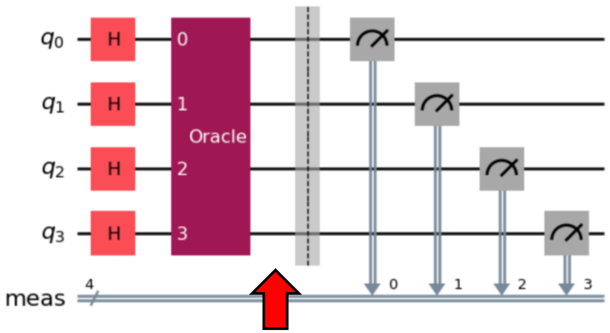


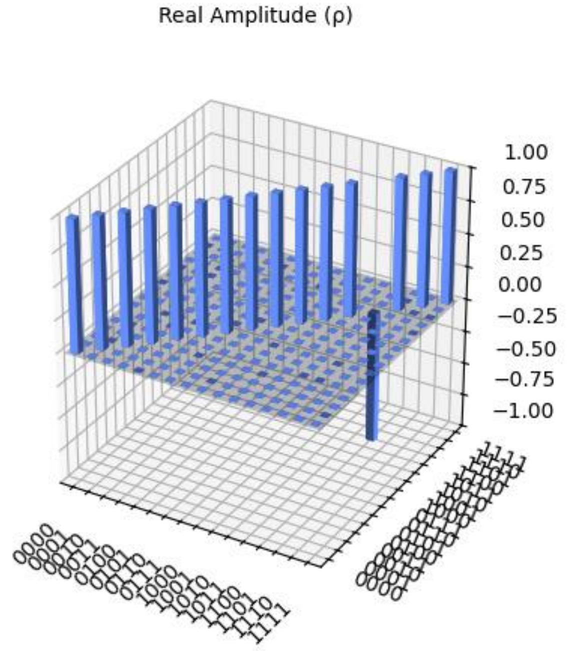


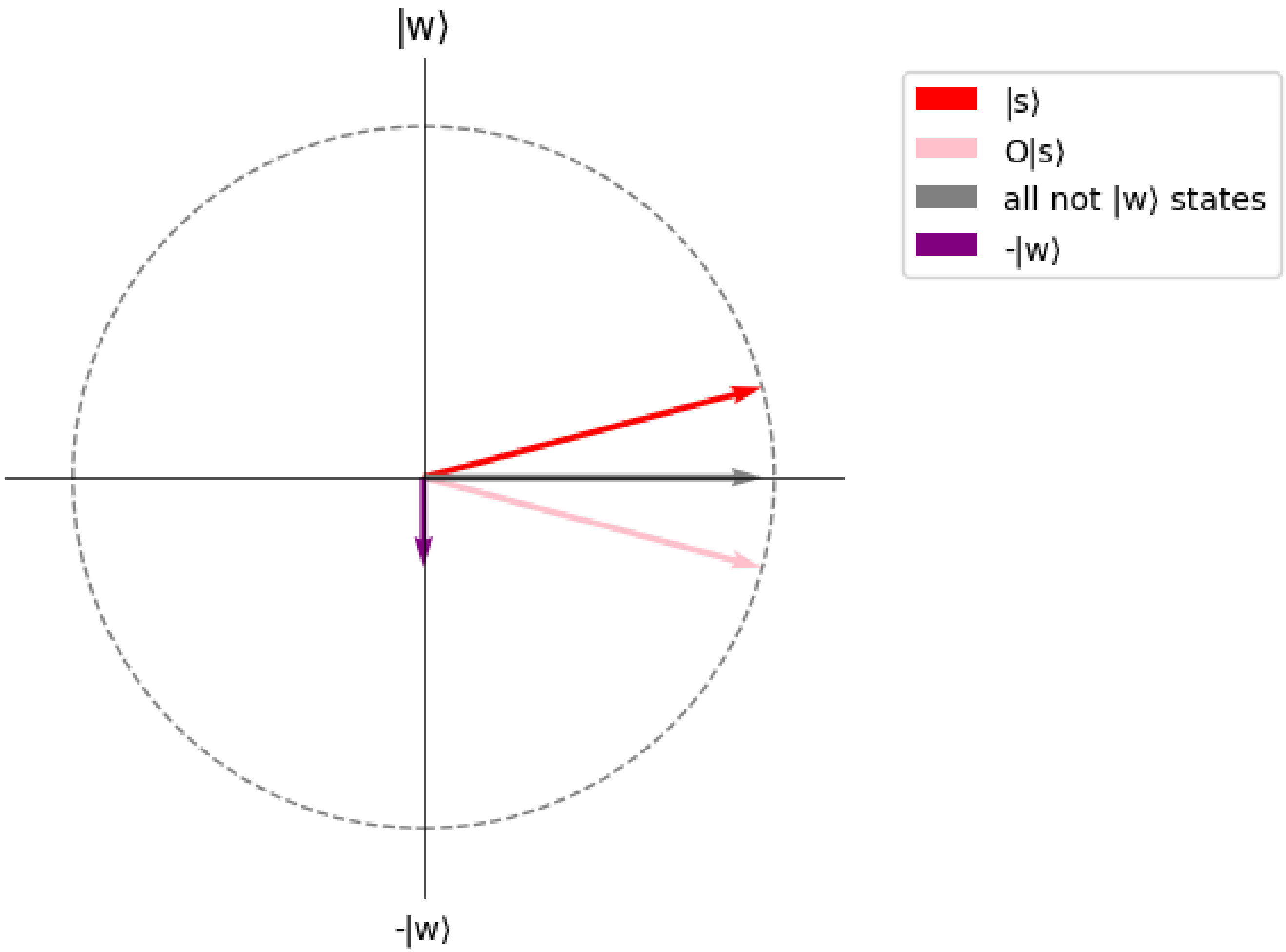


$$\Psi = 0 \cdot |s\rangle = \frac{1}{\sqrt{N}}\left((N-1)|s\rangle' - |w\rangle\right)$$

Apply the "Oracle"

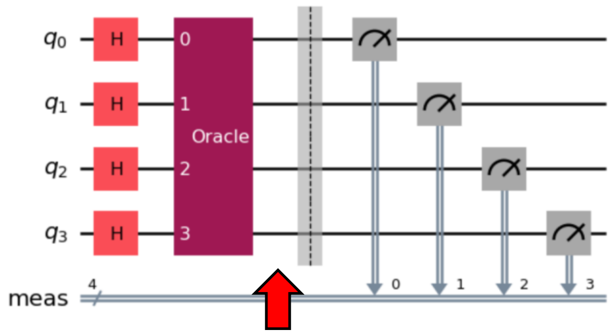






UMass Amherst College of Engineering

What do we measure?

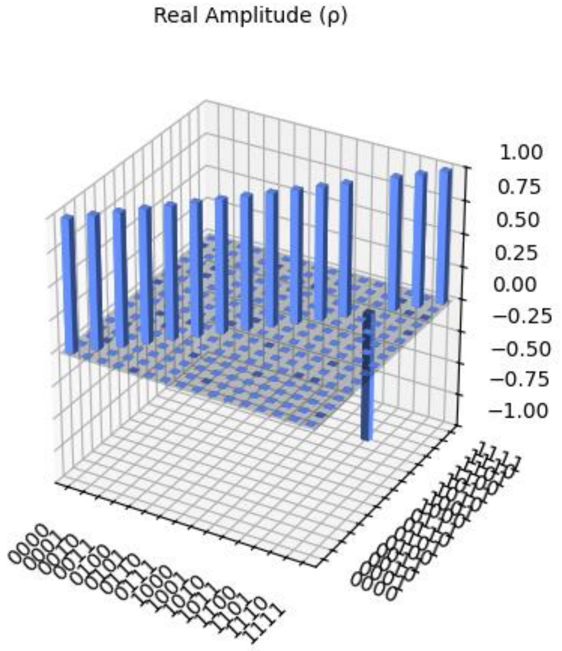


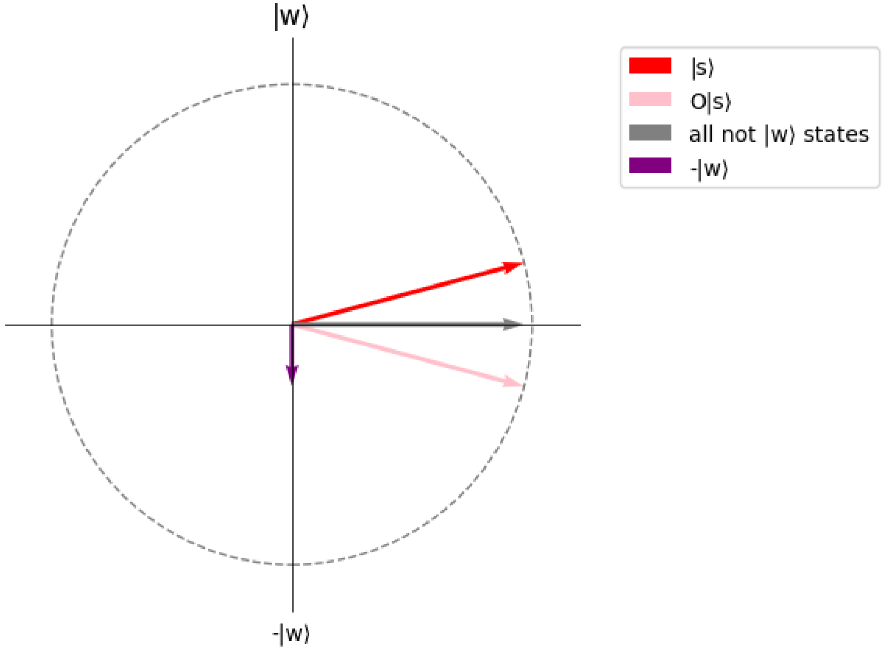

```
Max of 4 qubit register = 15
Solution= 12
Binary String of solution = 1100
```

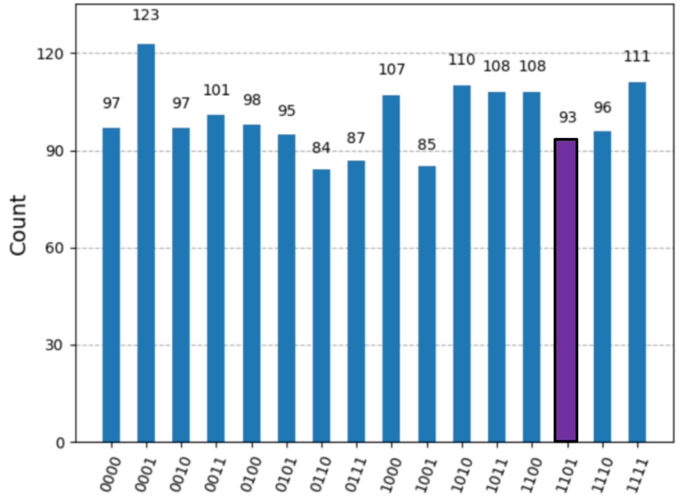
$$\frac{1}{4}|0000\rangle + \frac{1}{4}|0001\rangle + \frac{1}{4}|0010\rangle + \frac{1}{4}|0011\rangle + \frac{1}{4}|0100\rangle + \frac{1}{4}|0101\rangle + \ldots + \frac{1}{4}|1011\rangle \boxed{-\frac{1}{4}|1100\rangle} + \frac{1}{4}|1101\rangle + \frac{1}{4}|1110\rangle + \frac{1}{4}|1111\rangle$$

All measurement probabilities are still equal!

Flipping the phase of the amplitude doesn't change the measurement outcomes!

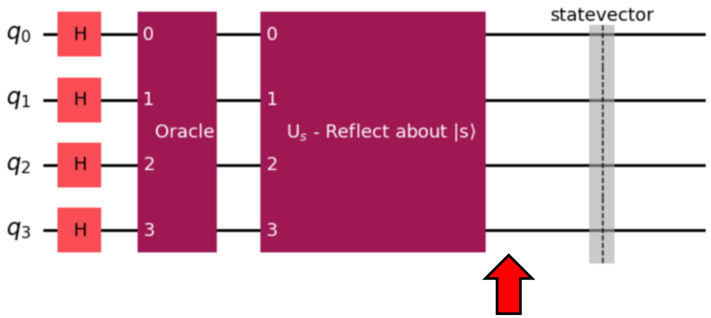






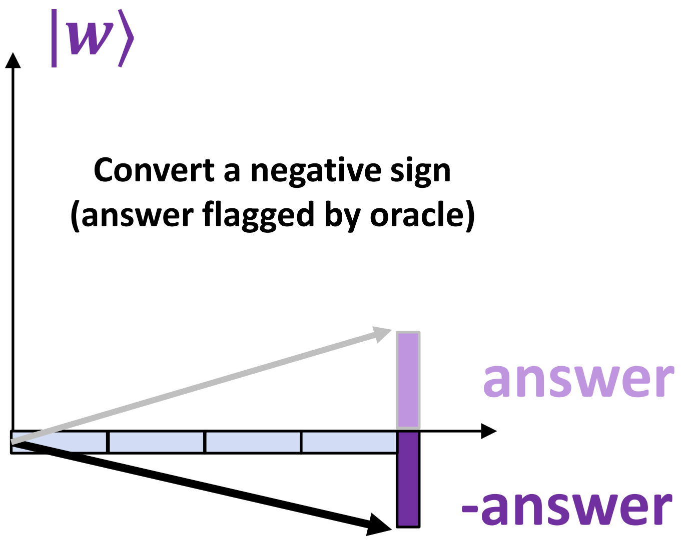
UMassAmherst College of Engineering

Amplitude Amplification

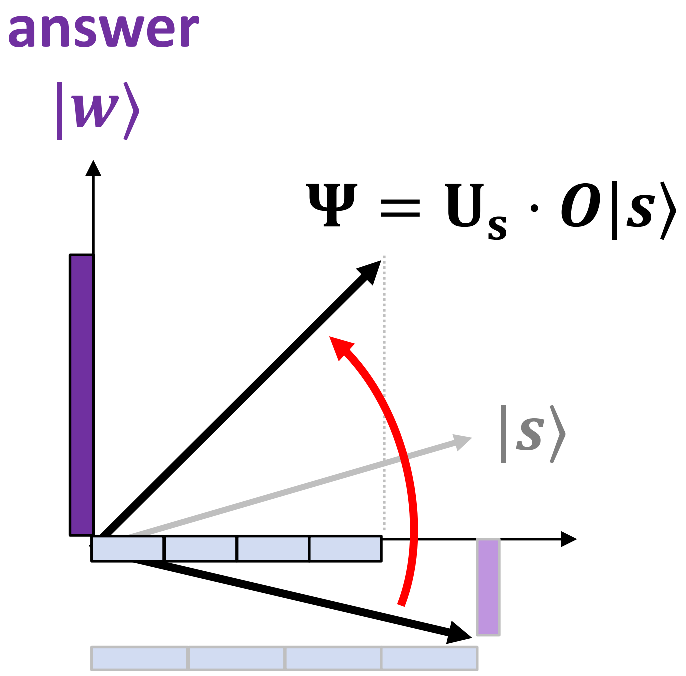


$$U_s \equiv 2|s\rangle\langle s| - \mathbb{1}$$

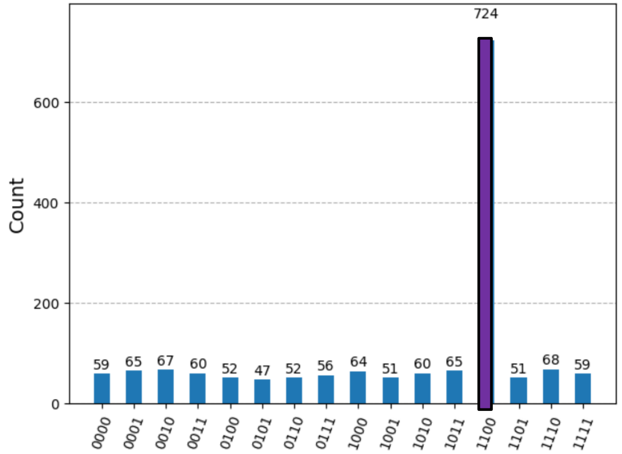
→ **Reflect about $|s\rangle$**
(everything but $|s\rangle$ flips)



$$\Psi = O|s\rangle$$



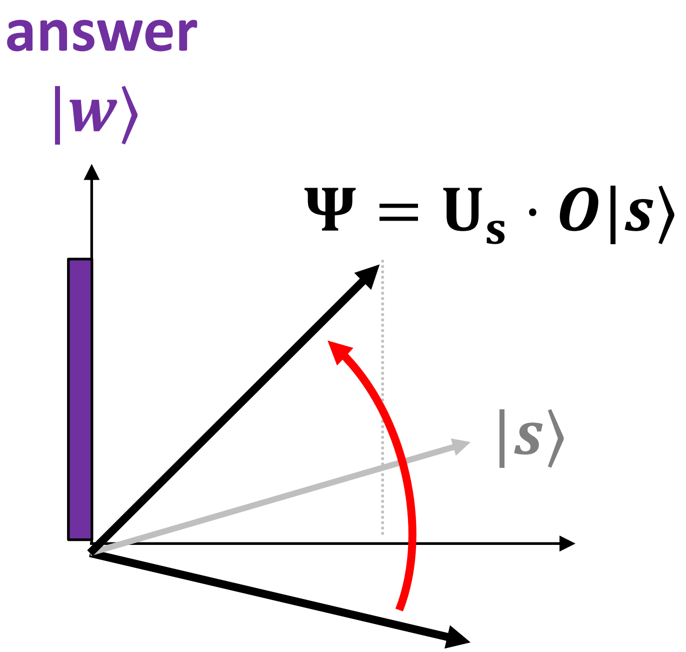
Increasing amplitude
Increases measurement
probability



UMass Amherst College of Engineering

But how do we construct $\mathrm{U_s}$ to reflect about $|s\rangle$?

$\mathrm{U_s} \equiv$ Reflect about $|s\rangle$



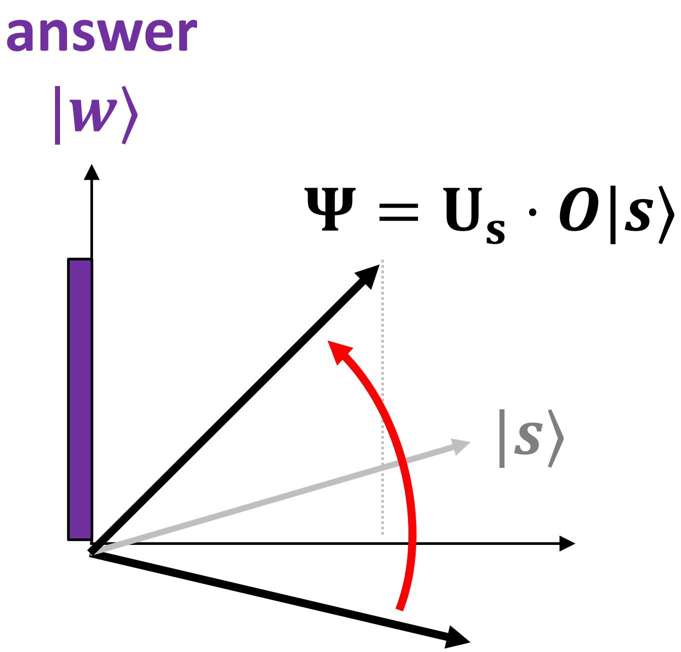
- **What gates can flip the <u>sign</u> of a state?**
- **What gates do we have?**
  - **CX**
  - **CZ**

- **CX flips the bit value but not the sign**
- **CZ flips the sign**

→ We need a CCZ

But how do we construct $\mathrm{U_s}$ to reflect about $|s\rangle$?

$\mathbf{U_s} \equiv$ **Reflect about** $|\boldsymbol{s}\rangle$



CZ flips the sign → we need a CCZ

But that flips $|111..1\rangle$ to -$|111..1\rangle$

New problem:

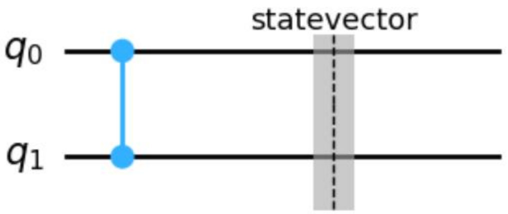
- **Use CCZ (which flips $|111\rangle$ to -$|111\rangle$) to invert about $|s\rangle$ instead**

Solution:

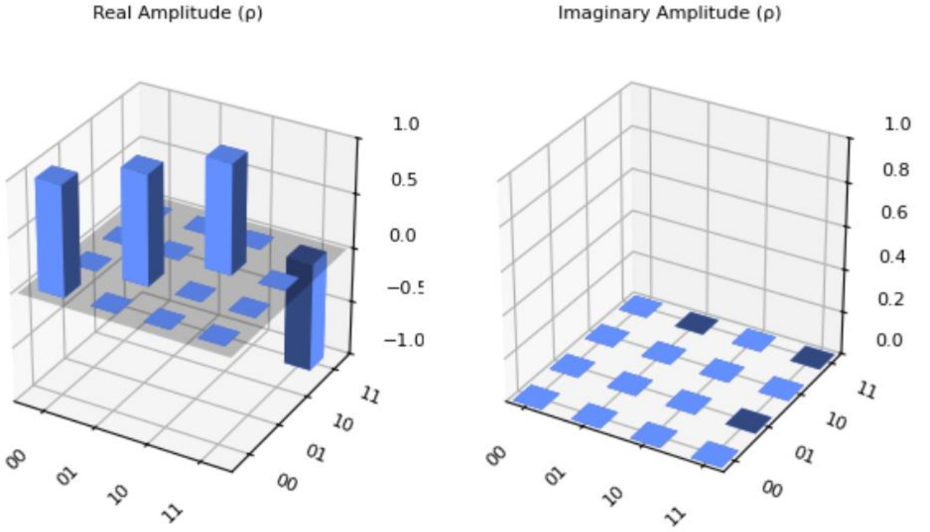
- **Convert $|111\rangle$ to $|s\rangle$ and back again as needed**
- **How?**

Control Phase Gate Review

$$\mathbf{U_s} \equiv 2|s\rangle\langle s| - \mathbb{1}$$



$$\text{Circuit} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$



$$\boldsymbol{CP} \equiv \mathbb{1} - \ \mathbf{2|11\rangle\langle 11|}$$

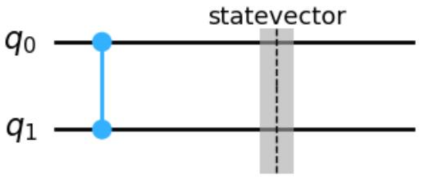
$\boldsymbol{CP}$ $\mathbb{1}$ $\mathbf{|11\rangle\langle 11|}$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} - 2 \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

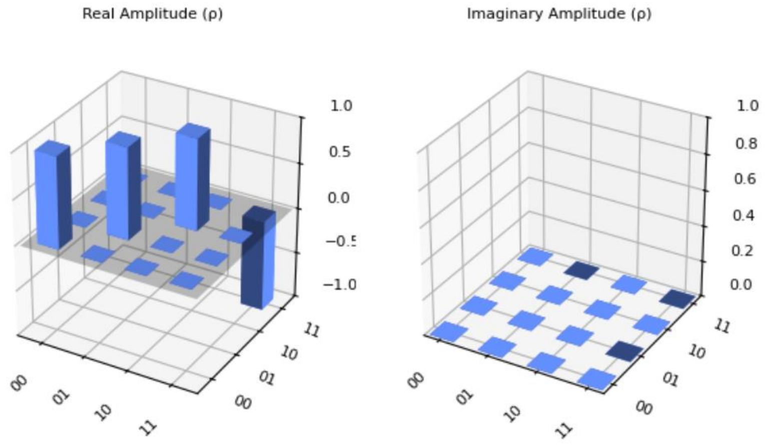
Control Phase Gate Review

$$\mathbf{U_s} \equiv 2|s\rangle\langle s| - \mathbb{1}$$

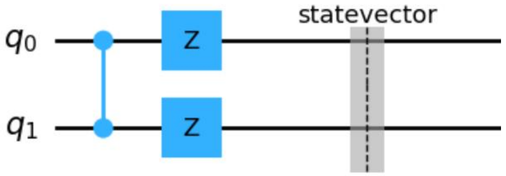
$$CP \equiv \mathbb{1} - \; 2|11\rangle\langle 11|$$



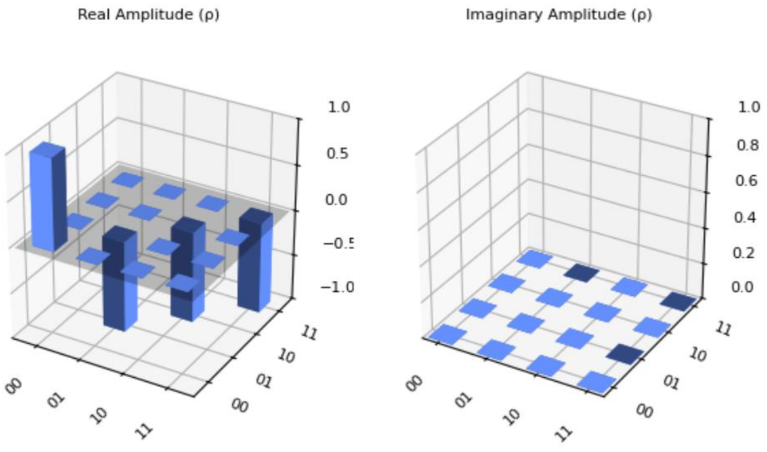
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$



$$Z^{\otimes N} \cdot CP \equiv \; 2|00\rangle\langle 00| - \mathbb{1}$$



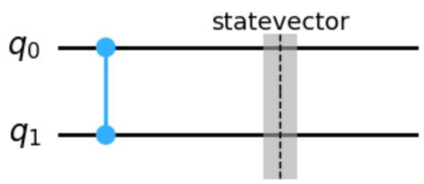
$$\text{Circuit} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$



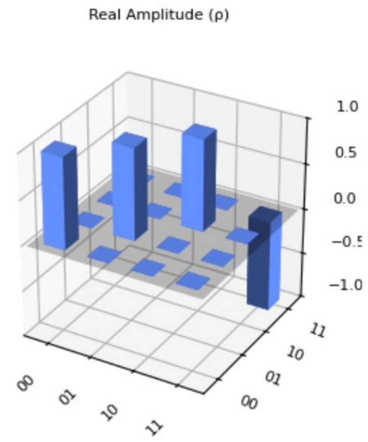
Control Phase Gate Review

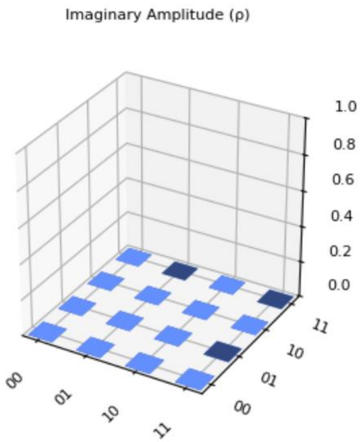
$$\mathbf{U_s} \equiv \mathbf{2|s\rangle\langle s| - \mathbb{1}}$$

$$\boldsymbol{Z^{\otimes N} \cdot CP \equiv 2|00\rangle\langle 00| - \mathbb{1}}$$

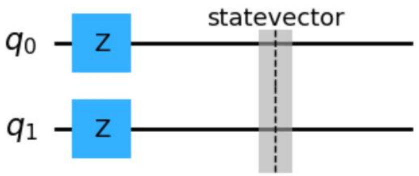


$$\text{Circuit} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

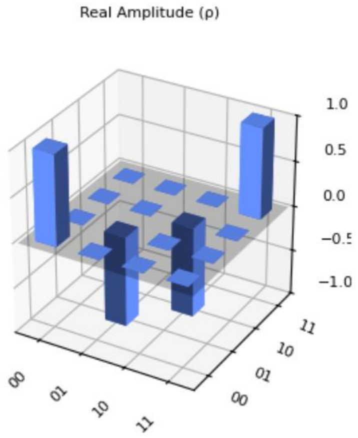


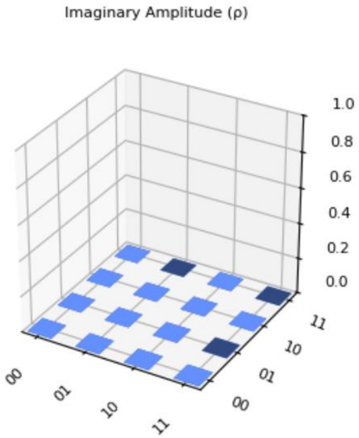


+

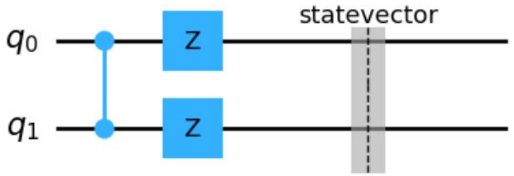


$$\text{Circuit} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

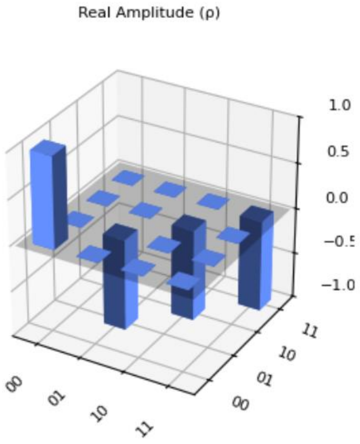


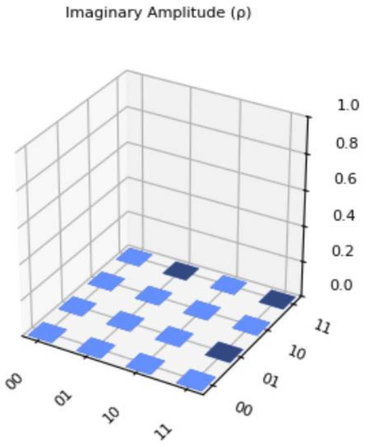


=



$$\text{Circuit} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

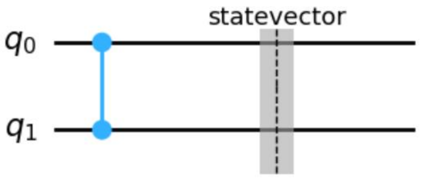




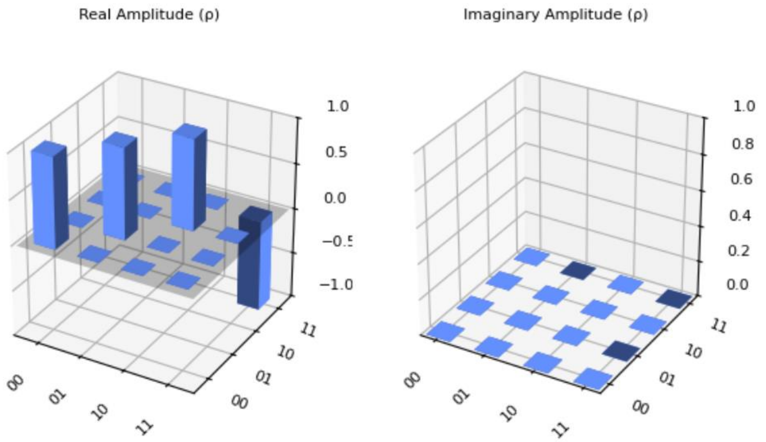
Control Phase Gate Review

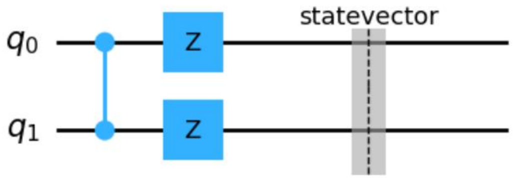
$$\mathbf{U_s} \equiv 2|s\rangle\langle s| - \mathbb{1}$$

$$\boldsymbol{Z^{\otimes N} \cdot CP \equiv 2|00\rangle\langle 00| - \mathbb{1}}$$

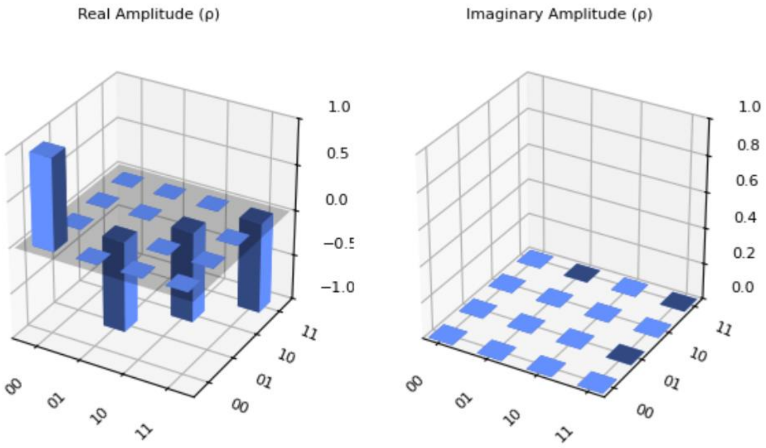


$$\text{Circuit} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$





$$\text{Circuit} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$



Altogether the CZ gate plus Z gates create:

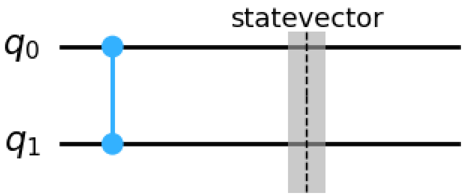
$$= 2|00\rangle\langle 00| - \mathbb{1} =$$

$$= 2 \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

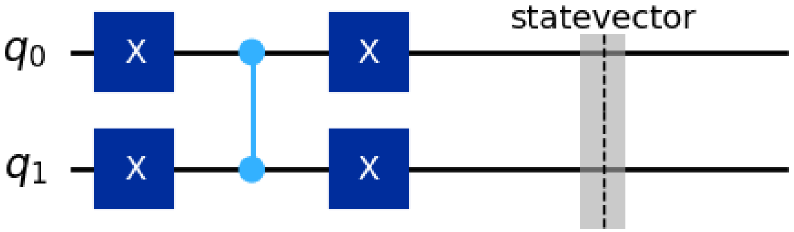
$$\boldsymbol{\equiv 2|00\rangle\langle 00| - \mathbb{1}}$$

Amplitude Amplification Circuit

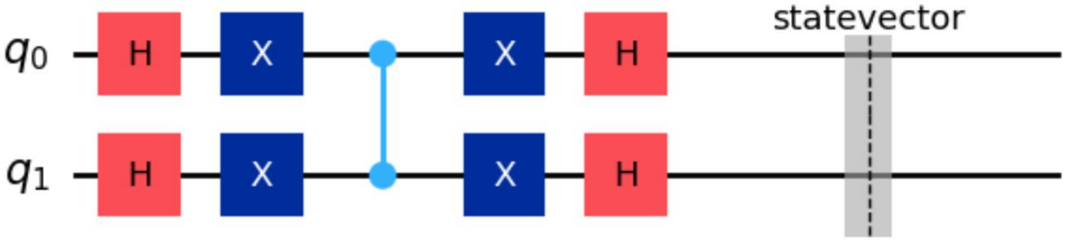
$$\mathbf{U_s} \equiv 2|s\rangle\langle s| - \mathbb{1}$$



$$CP \equiv \mathbb{1} - 2|11\rangle\langle 11|$$



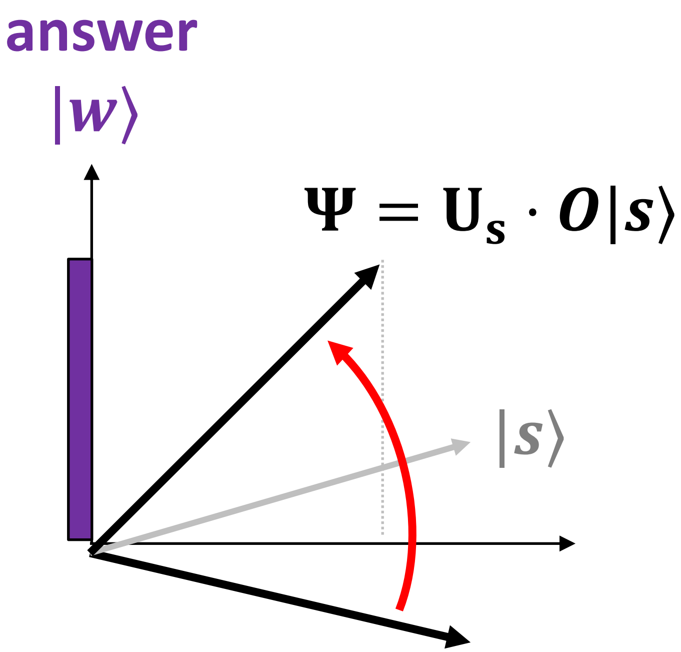
$$= \mathbf{X}^{\otimes n}(\mathbb{1} - 2|11\rangle\langle 11|)\mathbf{X}^{\otimes n}$$
$$= \mathbb{1} - 2|00\rangle\langle 00|$$



$$= \mathbf{H}^{\otimes n}(\mathbb{1} - 2|00\rangle\langle 00|)\mathbf{H}^{\otimes n}$$
$$= \mathbb{1} - 2|++\rangle\langle ++|$$
$$= \mathbb{1} - 2|s\rangle\langle s|$$

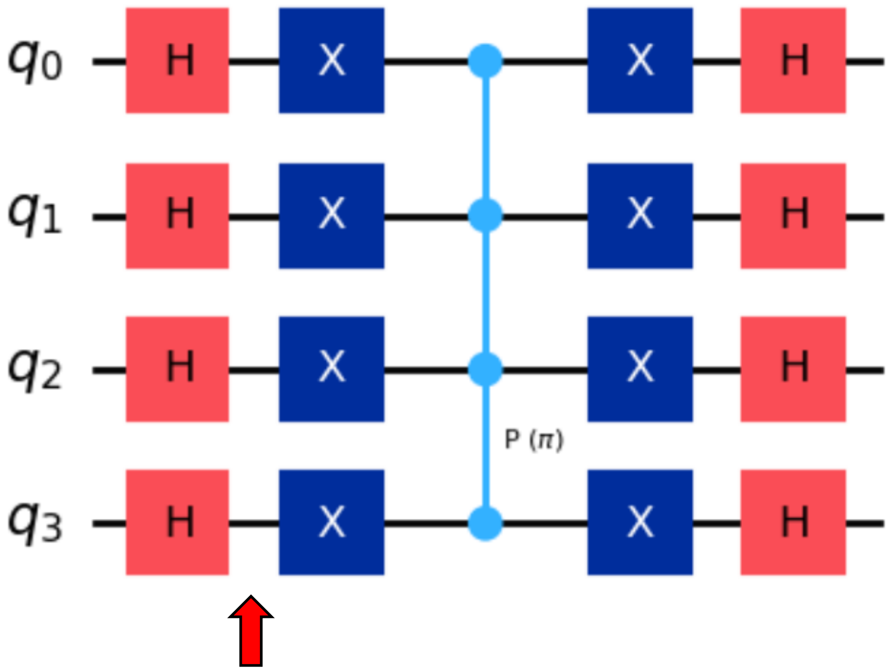
But how do we construct U_s to reflect about $|s\rangle$?

$U_s \equiv$ **Reflect about** $|s\rangle$



Convert $|1111\rangle$ to $|s\rangle$ and back again

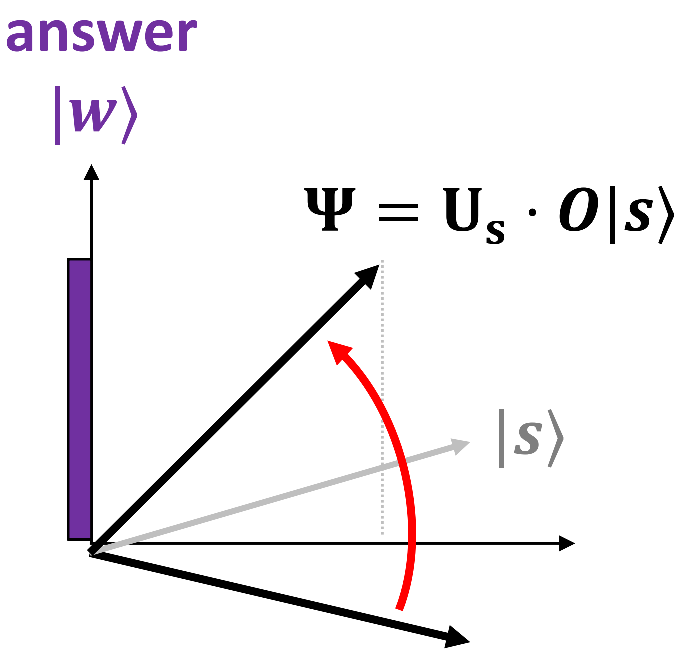
$|s\rangle \rightarrow \; |0000\rangle$



Convert
$|s\rangle$ **to** $|0000\rangle$

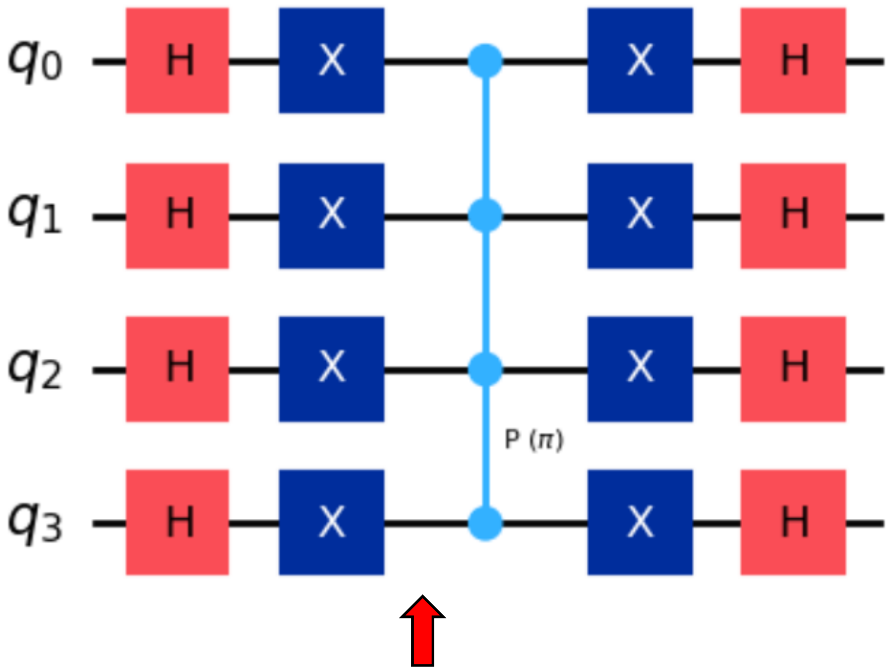
But how do we construct U_s to reflect about $|s\rangle$?

$U_s \equiv$ Reflect about $|s\rangle$



Convert $|1111\rangle$ to $|s\rangle$ and back again

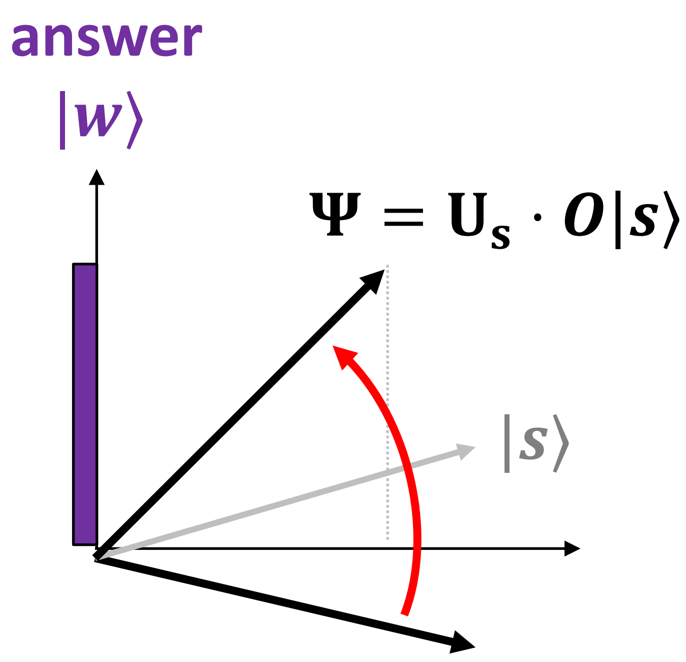
$|s\rangle \rightarrow |0000\rangle \rightarrow |1111\rangle$



Convert
$|0000\rangle \rightarrow |1111\rangle$

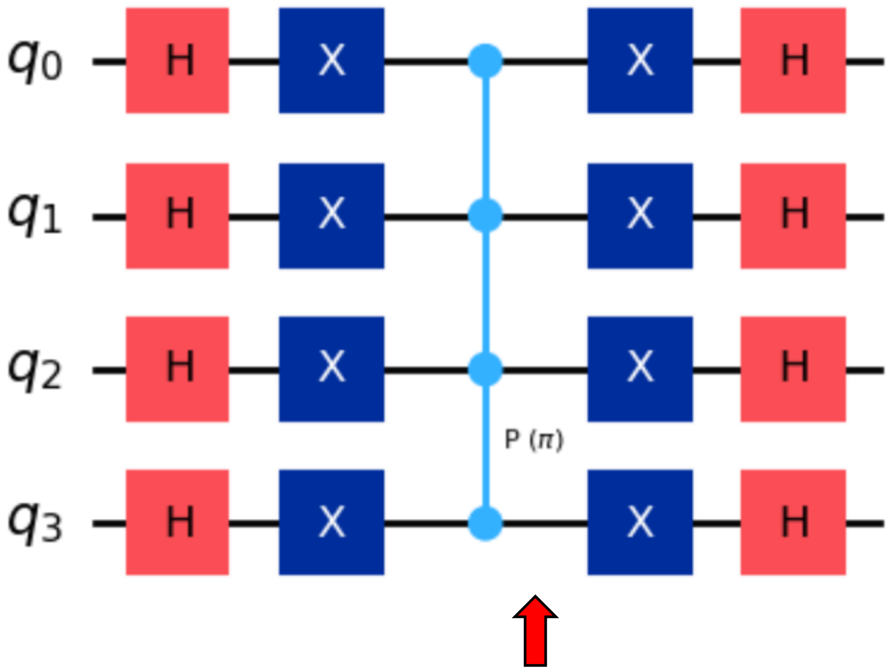
But how do we construct U_s to reflect about $|s\rangle$?

$U_s \equiv$ Reflect about $|s\rangle$



Convert $|1111\rangle$ to $|s\rangle$ and back again

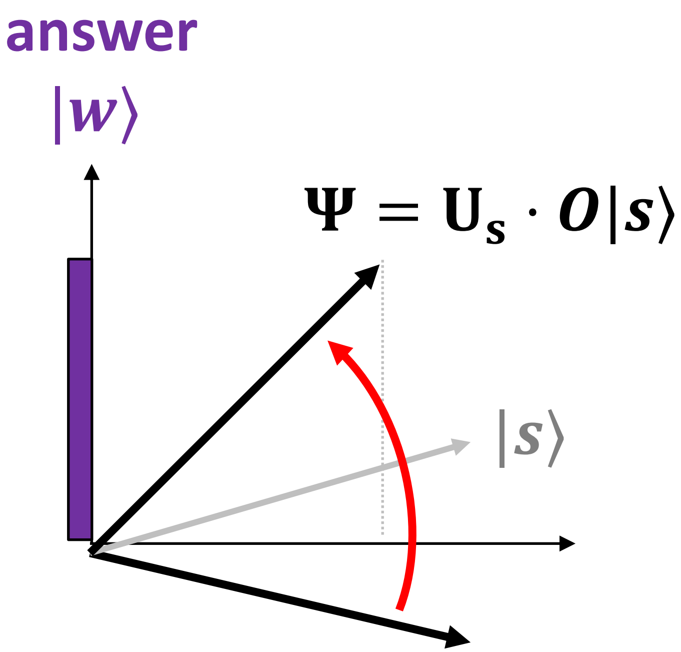
$|s\rangle \rightarrow \; |0000\rangle \rightarrow |1111\rangle \rightarrow -|1111\rangle$



Flip ONLY
$|1111\rangle \rightarrow -|1111\rangle$

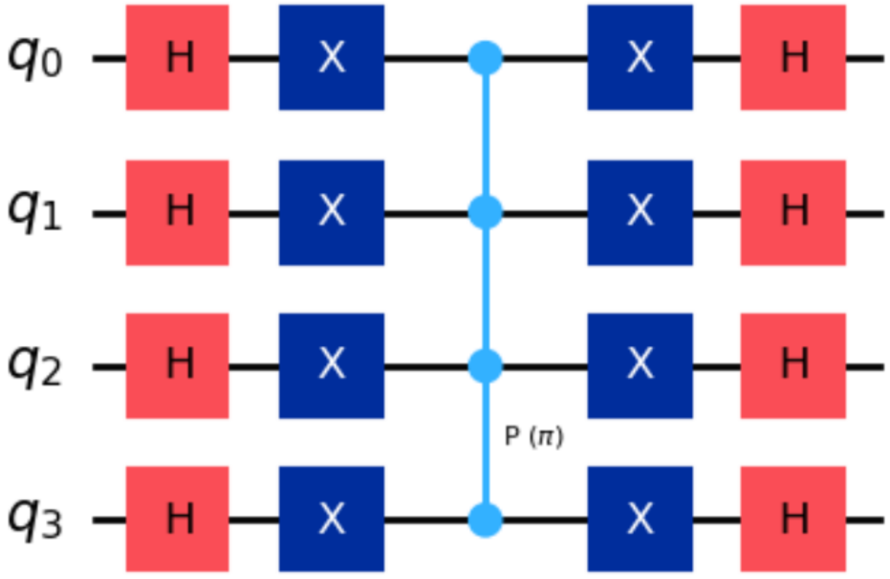
But how do we construct U_s to reflect about $|s\rangle$?

$U_s \equiv$ Reflect about $|s\rangle$



Convert $|1111\rangle$ to $|s\rangle$ and back again

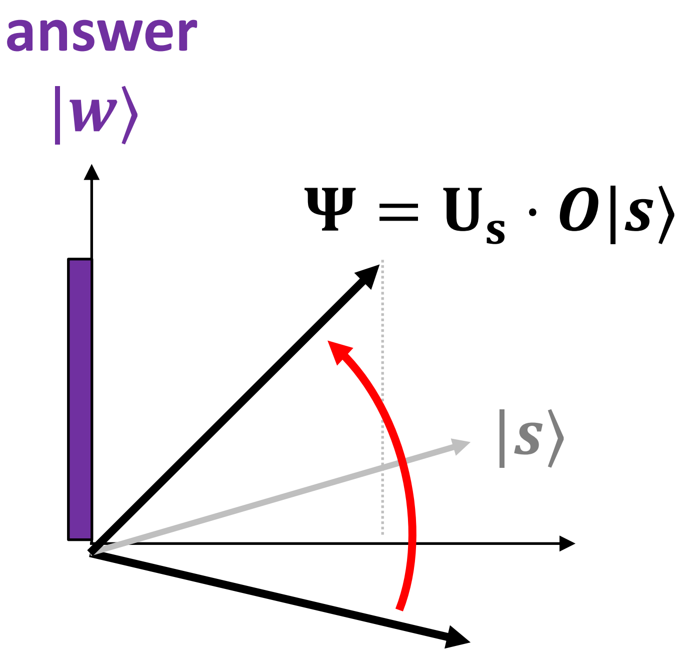
$|s\rangle \rightarrow \ |0000\rangle \rightarrow |1111\rangle \ \rightarrow -|1111\rangle \rightarrow -|0000\rangle$



Convert
$-|1111\rangle \rightarrow -|0000\rangle$

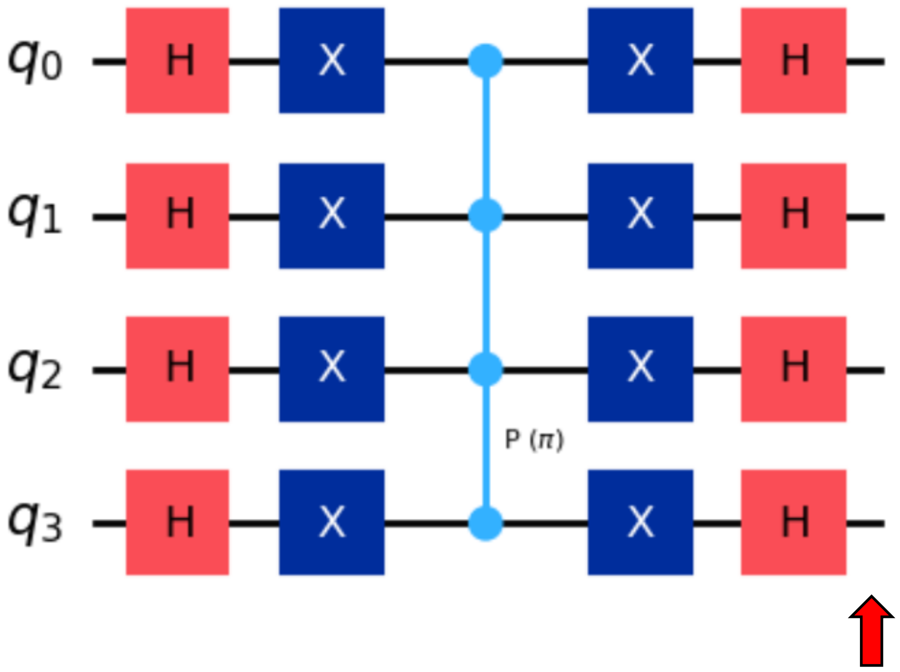
But how do we construct U_s to reflect about $|s\rangle$?

$U_s \equiv$ Reflect about $|s\rangle$



Convert $|1111\rangle$ to $|s\rangle$ and back again

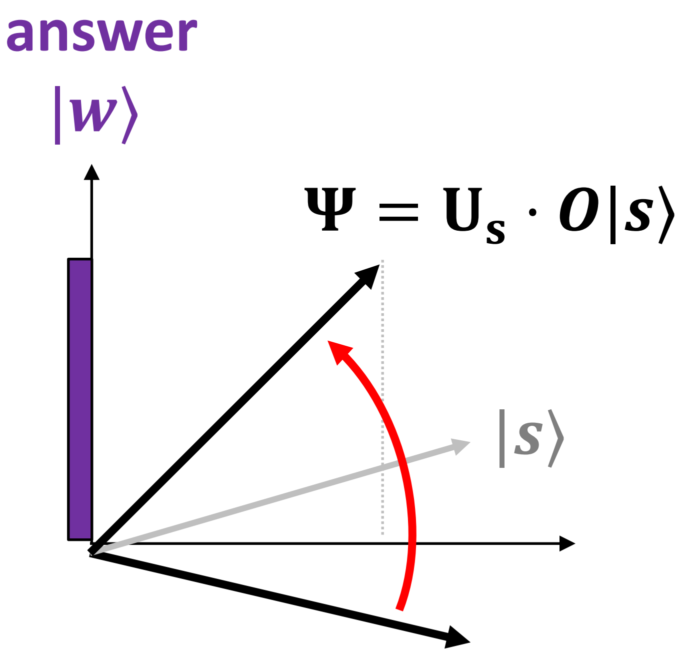
$|s\rangle \rightarrow |0000\rangle \rightarrow |1111\rangle \rightarrow -|1111\rangle \rightarrow -|0000\rangle \rightarrow -|s\rangle$



Convert
$-|0000\rangle \rightarrow -|s\rangle$

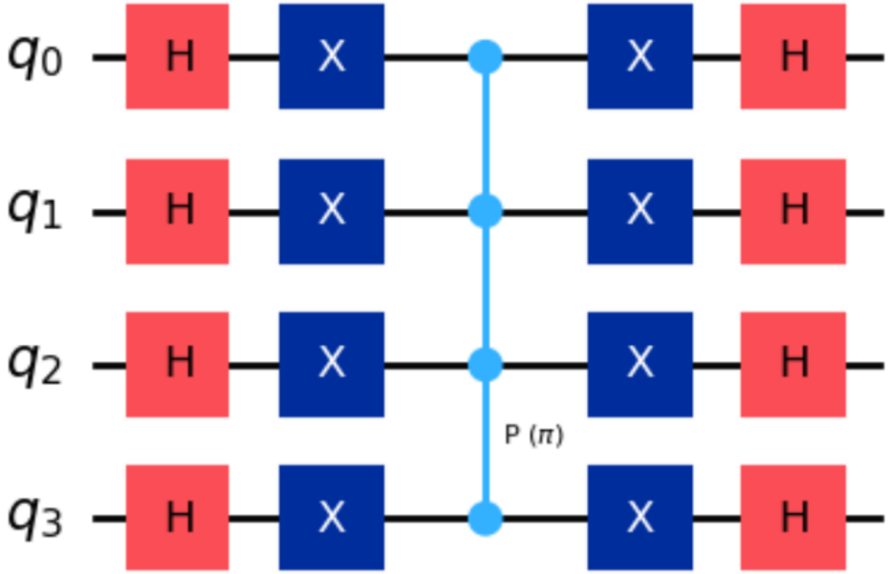
But how do we construct $\mathrm{U_s}$ to reflect about $|s\rangle$?

$\mathrm{U_s} \equiv$ **Reflect about** $|s\rangle$



Convert $|1111\rangle$ **to** $|s\rangle$ **and back again**

$|s\rangle \rightarrow |0000\rangle \rightarrow |1111\rangle \rightarrow -|1111\rangle \rightarrow -|0000\rangle \rightarrow -|s\rangle$

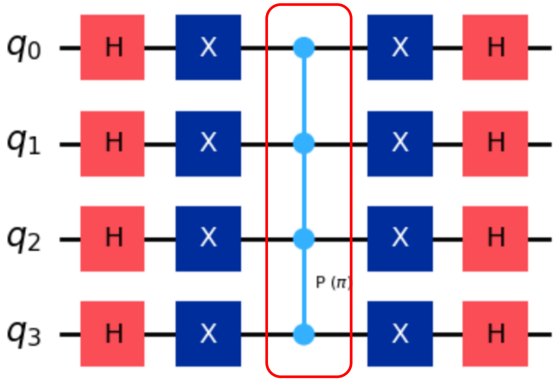


Convert
$-|0000\rangle \rightarrow -|s\rangle$

$$CCCZ \equiv 2|1111\rangle\langle 1111| - \mathbb{1}$$

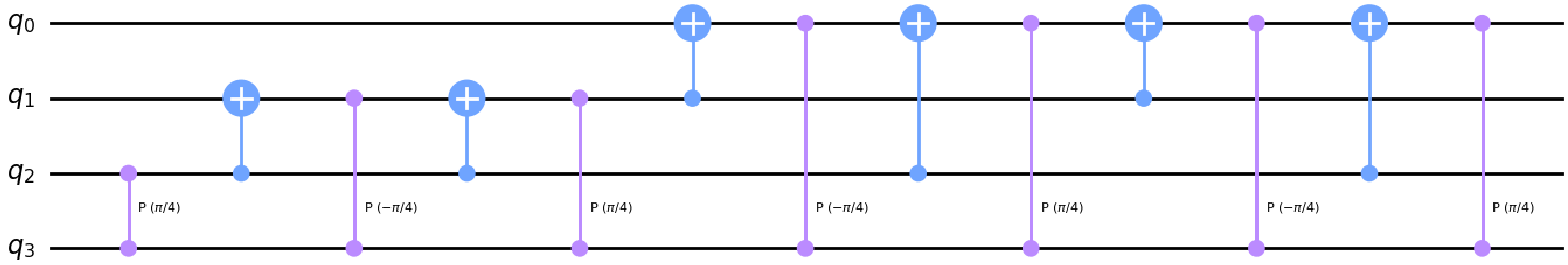
$$U_s \equiv 2|++++\rangle\langle ++++| - \mathbb{1}$$

CCCZ - decomposed

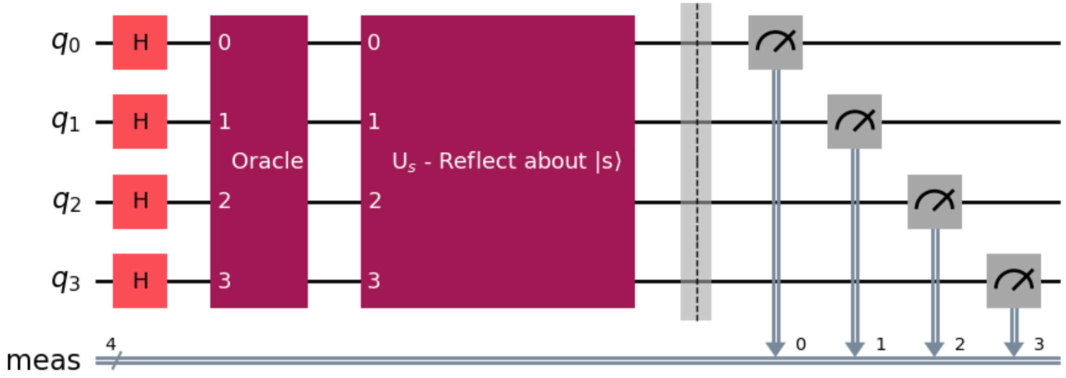


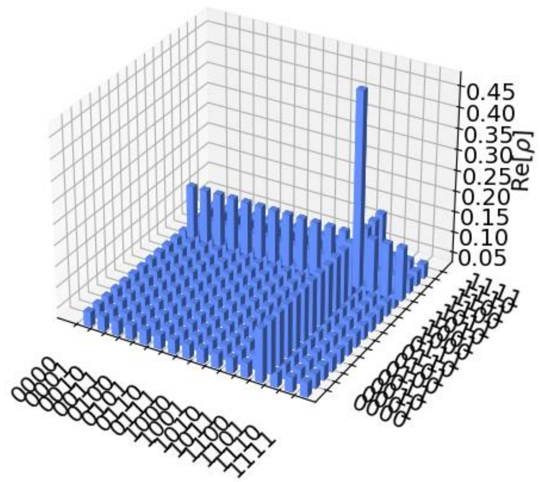
$$\boldsymbol{CCCZ \equiv 2|0000\rangle\langle 0000| - \mathbb{1}}$$

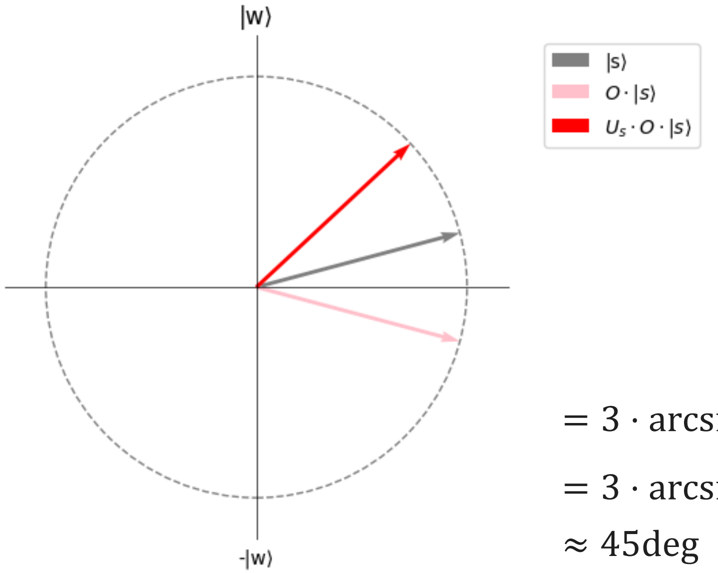
$$\boldsymbol{U_s \equiv 2|{+}{+}{+}\ {+}\rangle\langle{+}{+}{+}\ {+}| - \mathbb{1}}$$



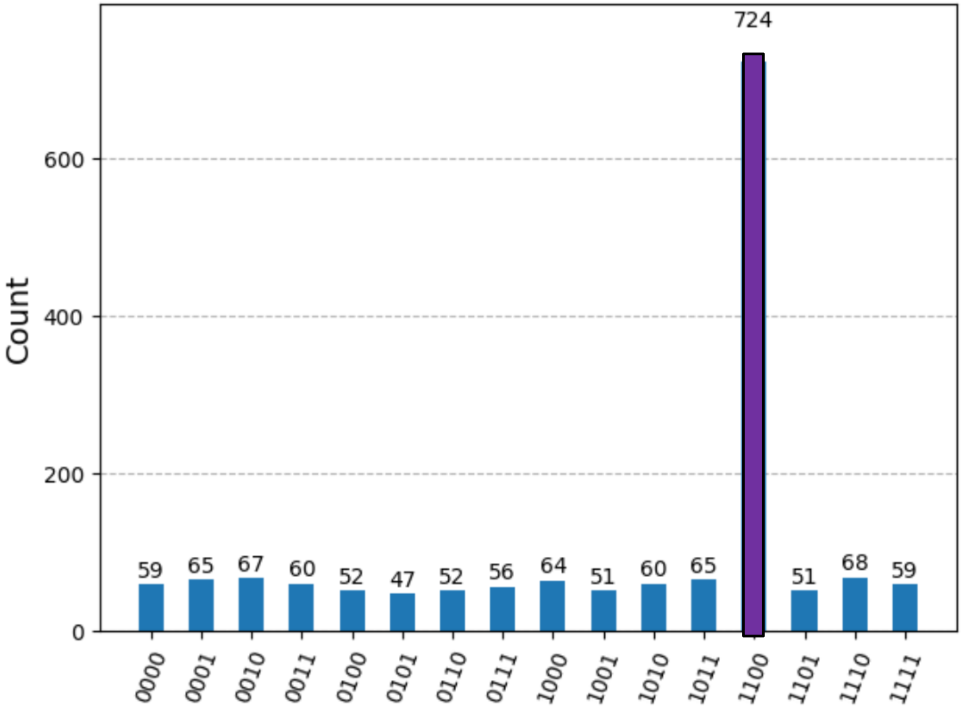
Amplify the Amplitude – First Iteration







$$= 3 \cdot \arcsin\left(\frac{1}{\sqrt{N}}\right)$$
$$= 3 \cdot \arcsin\left(\frac{1}{4}\right)$$
$$\approx 45\text{deg}$$

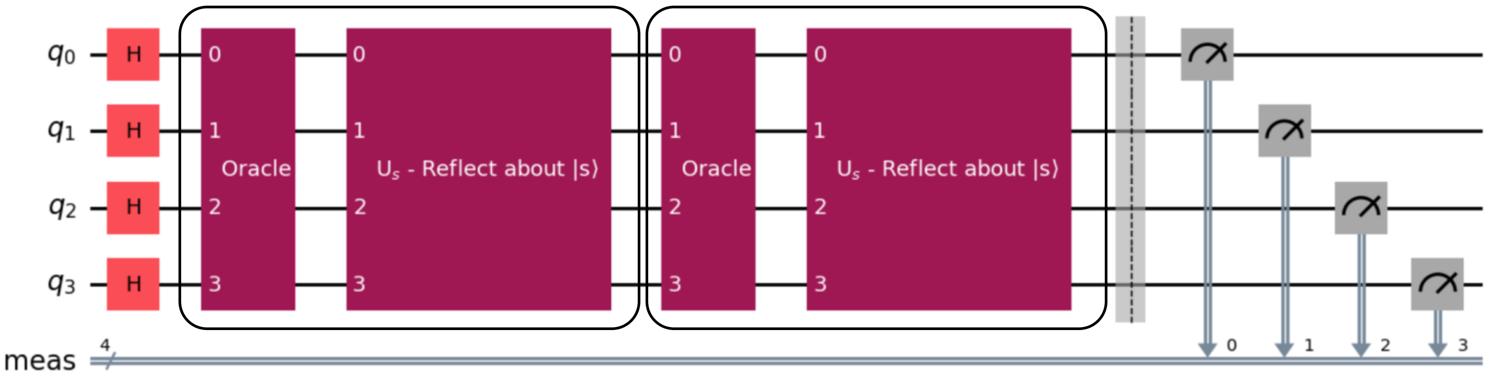


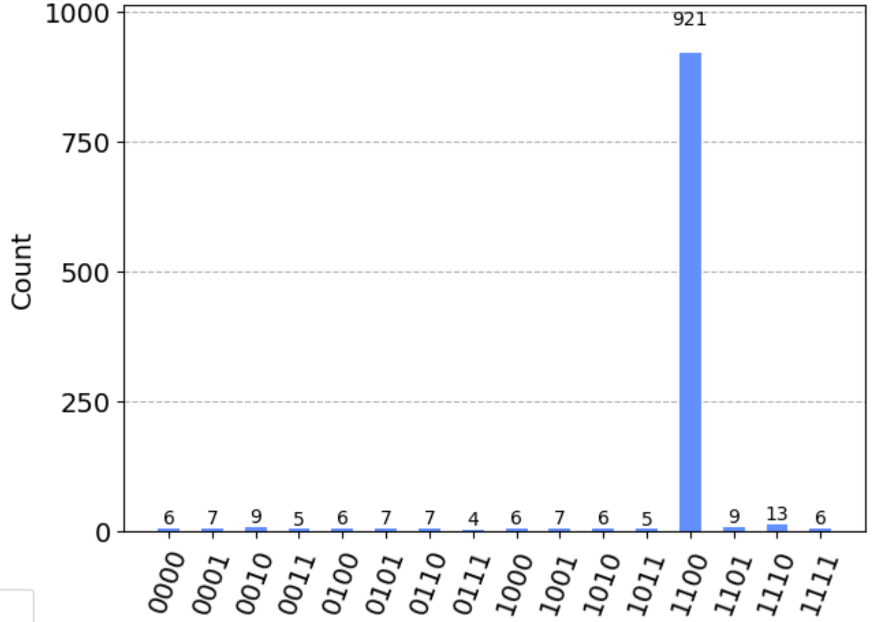
UMass Amherst College of Engineering

Repeat → Amplify the Amplitude again

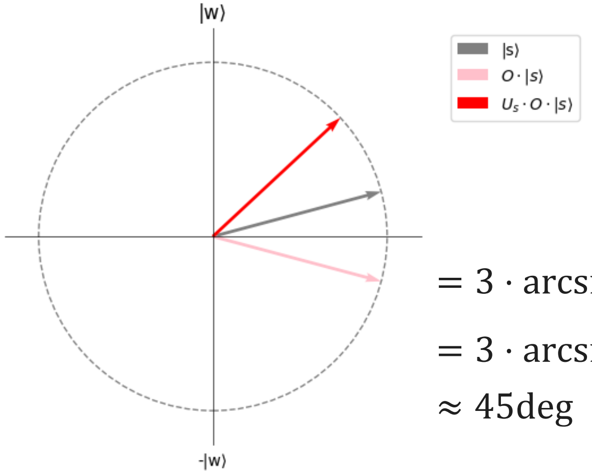
n bit register

Repeat $\frac{\pi}{4}\sqrt{N}$ times

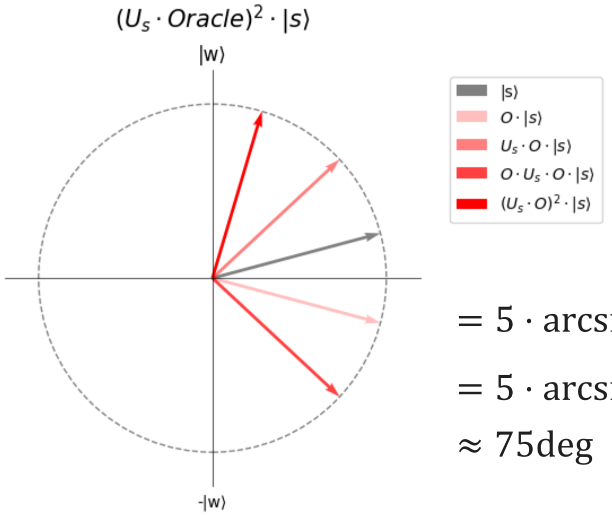




Repeat $\frac{\pi}{4}\sqrt{16}$ times (~3)



$$= 3 \cdot \arcsin\left(\frac{1}{\sqrt{N}}\right)$$
$$= 3 \cdot \arcsin\left(\frac{1}{4}\right)$$
$$\approx 45\text{deg}$$

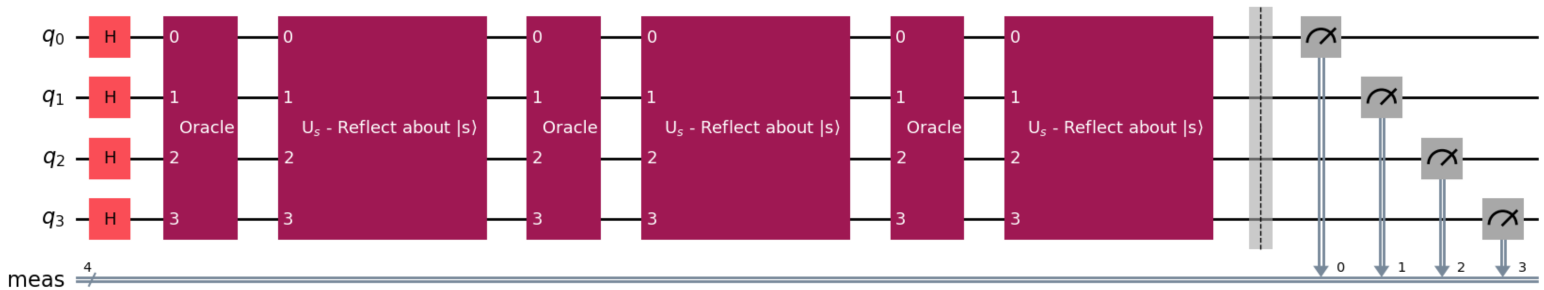


$$= 5 \cdot \arcsin\left(\frac{1}{\sqrt{N}}\right)$$
$$= 5 \cdot \arcsin\left(\frac{1}{4}\right)$$
$$\approx 75\text{deg}$$

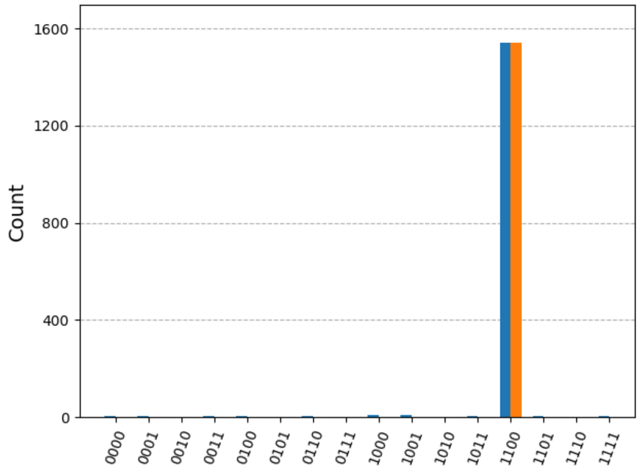
Repeat → Amplify the Amplitude again and Again!?

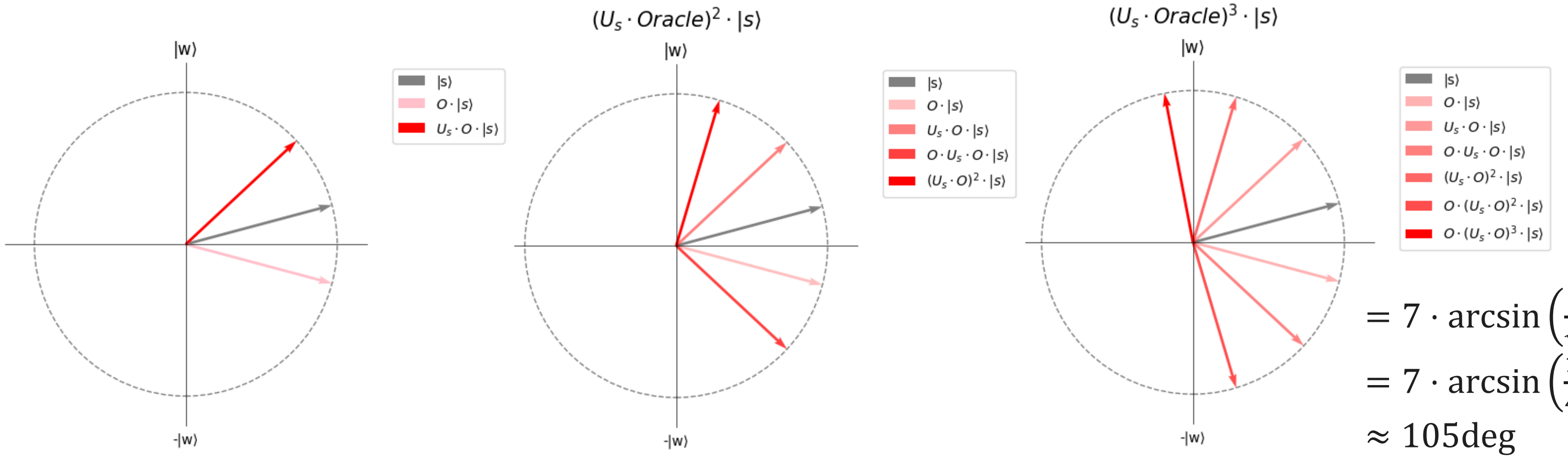
n bit register

Repeat $\frac{\pi}{4}\sqrt{N}$ times



Repeat $\frac{\pi}{4}\ \sqrt{16}$ times (~3)





$$= 7 \cdot \arcsin\left(\frac{1}{\sqrt{N}}\right)$$
$$= 7 \cdot \arcsin\left(\frac{1}{4}\right)$$
$$\approx 105\text{deg}$$

Overrotated!!

Now we see that we've actually over rotated past the optimal answer and the further interations would just continue to rotated us farther from the answer.

The angle is now $\theta = 7 \cdot \arcsin(1/\sqrt{N}) = 7 \cdot \arcsin(1/4) \approx 105$ deg

Only 3 iteractions were needed!

Turns out it can be shown that the optimal number of iterations is: $\frac{\pi}{4}\sqrt{N}$

This is because we always want a final angle of $\frac{\pi}{4}$ (90°) and the initial angle of the superposition state will always be : $\arcsin(1/\sqrt{N})$

Thus dividing them gives the optimal number of iterations.

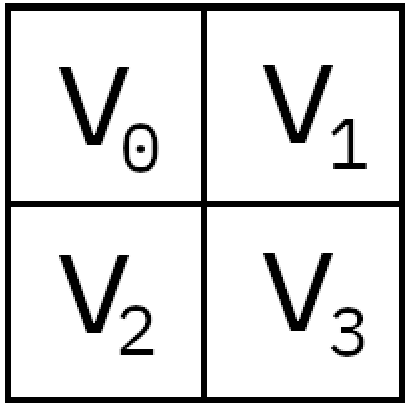
> See Thomas Wong's Textbook

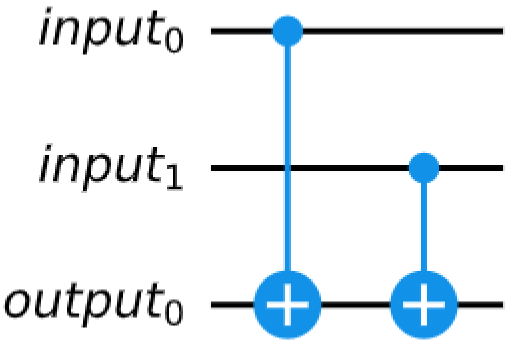
Which for n=4 and N=16 means the optimal number of iterations is : $\frac{\pi}{4}\sqrt{16} = \pi \approx 3$

Getting the Oracle to ask interesting questions

Sudoku

- Logical checks → Oracle
- Use CNOTs (CXs)





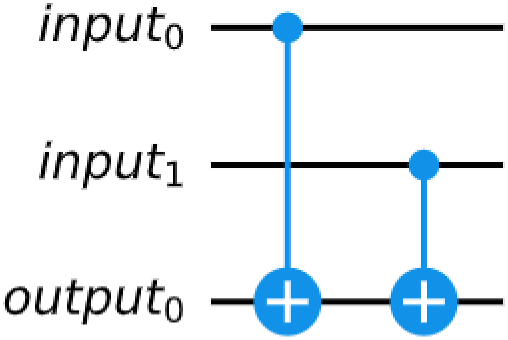
Classical		Reversible/Quantum	
NOT	A → $\overline{A}$	X-Gate	A —X— $\overline{A}$
AND	A, B → AB	Toffoli	A, B, 0 → A, B, AB
OR	A, B → $A + B$	anti-Toffoli	A, B, 1 → A, B, $A + B$
XOR	A, B → $A \oplus B$	CNOTs	A, B, 0 → A, B, $A \oplus B$
NAND	A, B → $\overline{AB}$	Toffoli	A, B, 1 → A, B, $\overline{AB}$
NOR	A, B → $\overline{A + B}$	anti-Toffoli	A, B, 0 → A, B, $\overline{A + B}$

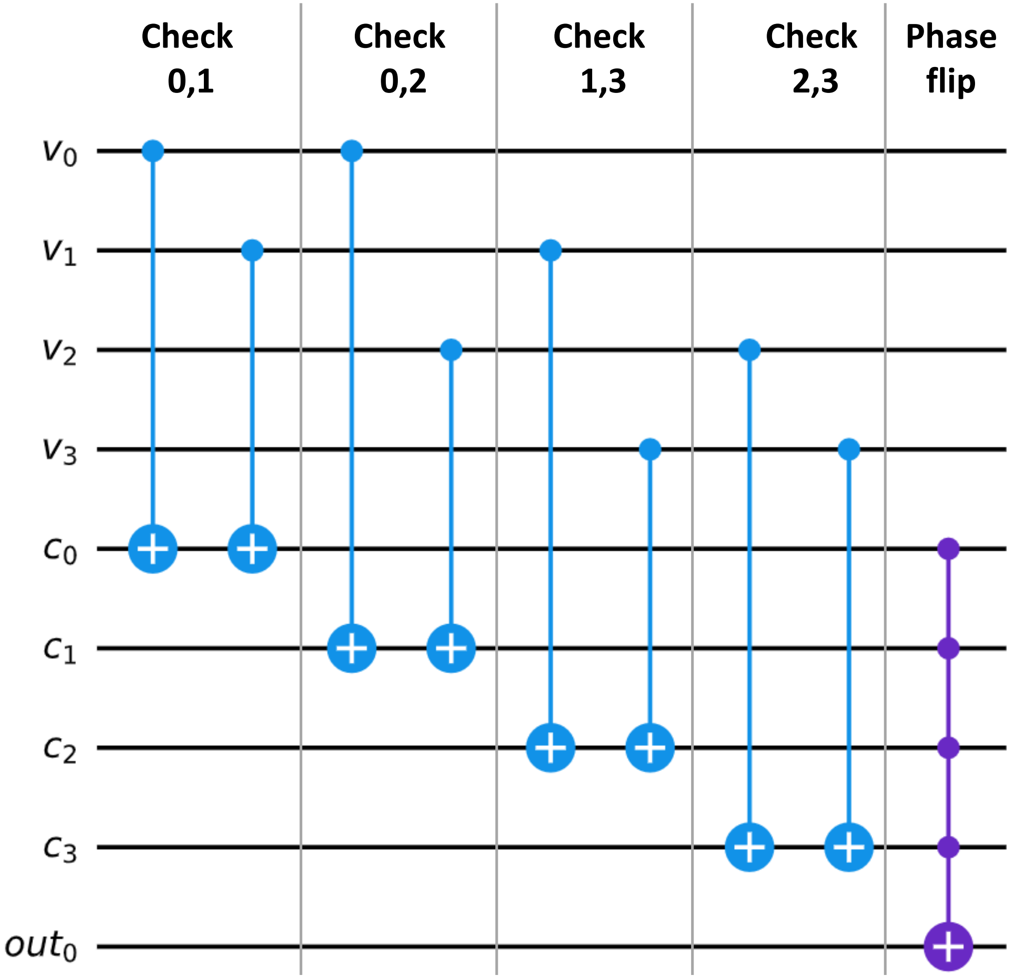
Getting the Oracle to ask interesting questions

Sudoku

- Logical checks → Oracle
- Use CNOTs (CXs)

V_0	V_1
V_2	V_3





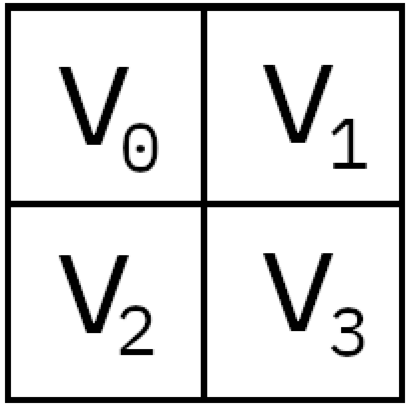
Getting the Oracle to ask interesting questions

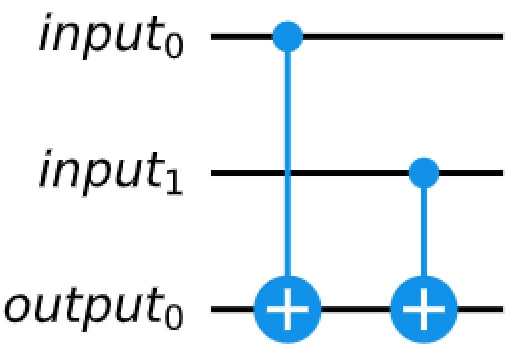
Sudoku

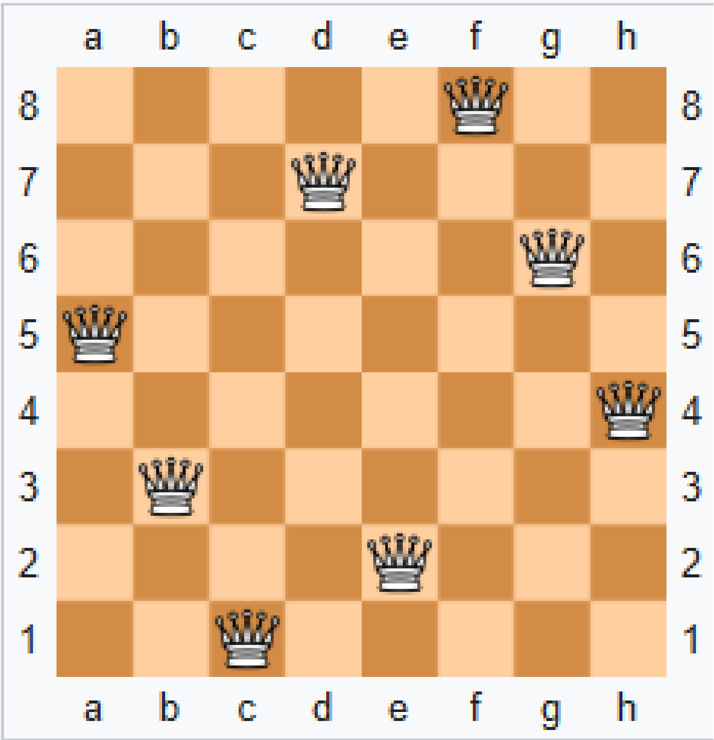
- **Logical checks → Oracle**

Queens Puzzle

- **Logical checks → Oracle**

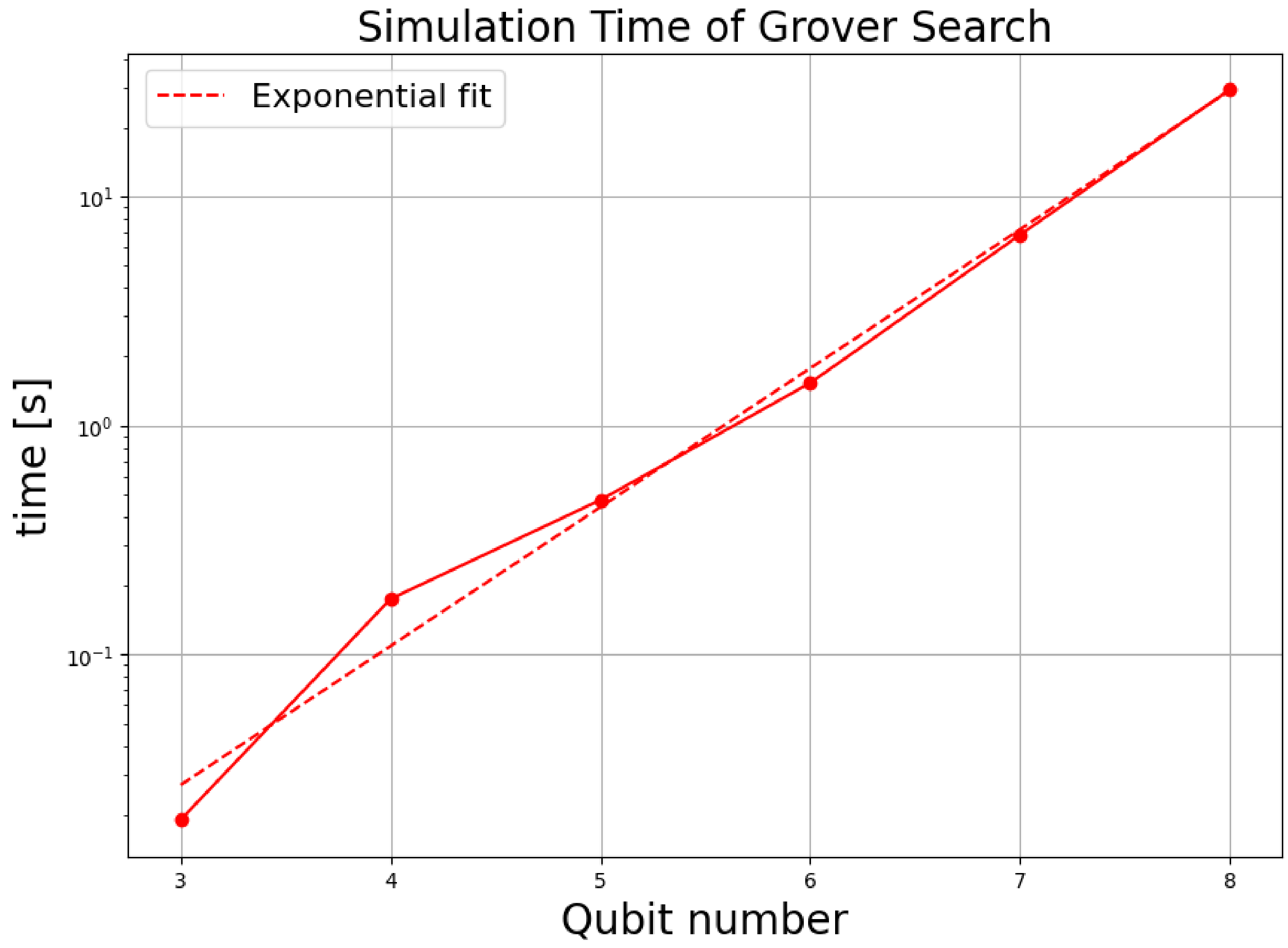






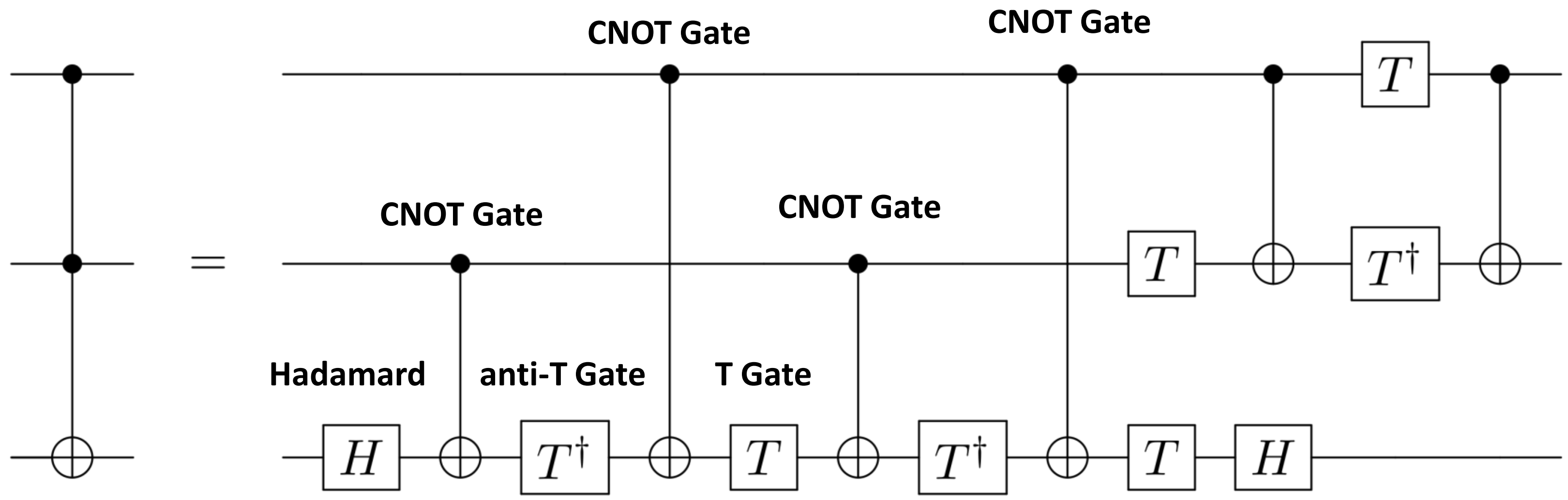
The only symmetrical solution to the eight queens puzzle (up to rotation and reflection)

Classically scales exponentially



Toffoli gate (CCNOT)

Toffoli Gate (CCNOT Gate)



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

T Gate