Quantum Software Development

Lecture 8: Grover’s Search Algorithm,
The Multiverse

March 13, 2024

Tufts UNIVERSITY | School of Engineering

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Grover’s Search Algorithm

Many cryptographic applications rely on the hardness of brute-force search.

Password is hashed before being sent to the server

Given the hash, the password can only be recovered via brute force

For an 8-character password, a naïve brute-force attack with 1 billion checks per second would take ~292 years.

The formal definition of unstructured search has a similar pattern to previously-discussed problems.

Suppose you're given a black-box function f that outputs a 1 for exactly one possible input and 0 for everything else.

In other words, there exists some secret string s such that $f(s) = 1$, while for all $x \neq s$, $f(x) = 0$.

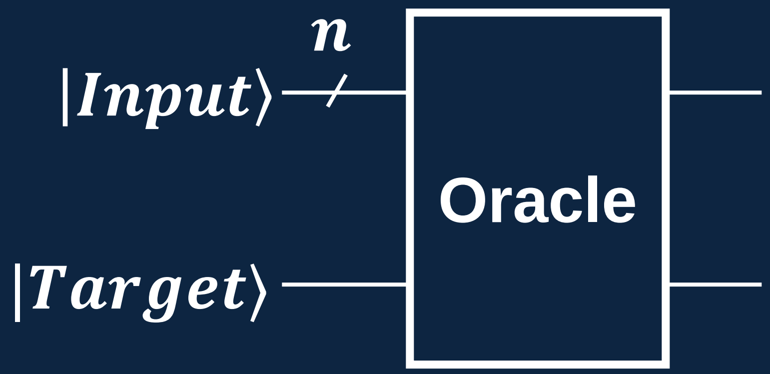
How do you find out what s is?

Check-if-all-1s, $n = 3$

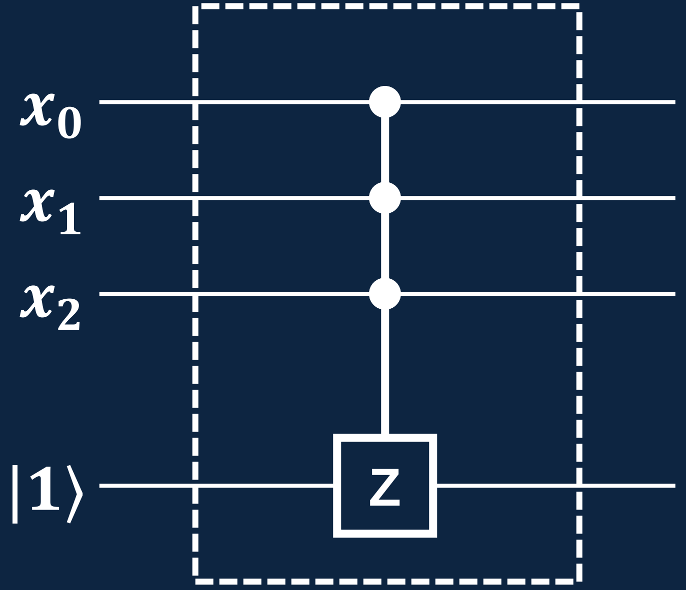
x	000	001	010	011	100	101	110	111
$f(x)$	0	0	0	0	0	0	0	1

$s = 111$

A quantum oracle defined in the typical way phase-flips the target if the input is s.



Check-if-all-1s, $n = 3$



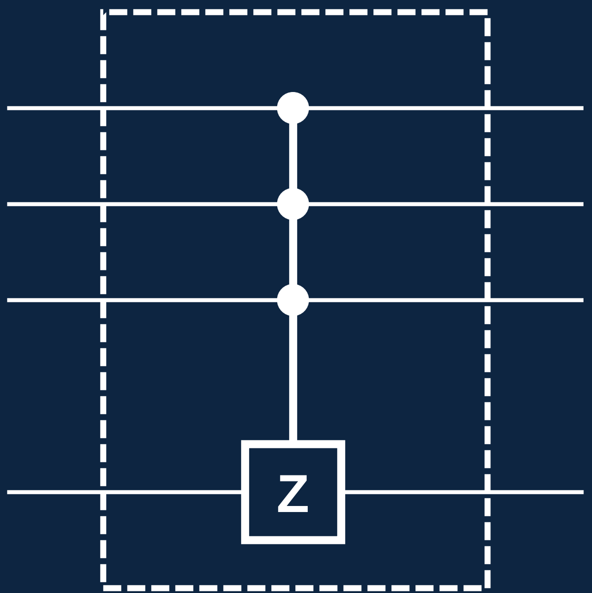
$\vert x_0 x_1 x_2\rangle$	$(-1)^{f(x)}$
$\vert 000\rangle$	1
$\vert 001\rangle$	1
$\vert 010\rangle$	1
$\vert 011\rangle$	1
$\vert 100\rangle$	1
$\vert 101\rangle$	1
$\vert 110\rangle$	1
$\vert 111\rangle$	-1

What does the typical approach of applying a Hadamard transform before and after the oracle yield?

Check-if-all-1s, $n = 3$

$$\frac{1}{\sqrt{8}}\sum_{i=1}^{7}|i\rangle$$

$|1\rangle$



$$\frac{1}{\sqrt{8}}\begin{pmatrix} |000\rangle \\ +|001\rangle \\ +|010\rangle \\ +|011\rangle \\ +|100\rangle \\ +|101\rangle \\ +|110\rangle \\ -|111\rangle \end{pmatrix}$$

$$\frac{1}{\sqrt{16}}\begin{pmatrix} 3|000\rangle + |001\rangle + |010\rangle - |011\rangle \\ +|100\rangle - |101\rangle - |110\rangle + |111\rangle \end{pmatrix}$$

$$\frac{1}{\sqrt{8}}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \end{bmatrix} \begin{array}{l} \longrightarrow 6 \\ \longrightarrow 2 \\ \longrightarrow 2 \\ \longrightarrow -2 \\ \longrightarrow 2 \\ \longrightarrow -2 \\ \longrightarrow -2 \\ \longrightarrow 2 \end{array}$$

Resulting state encodes the s^{th} column of the H transform.*

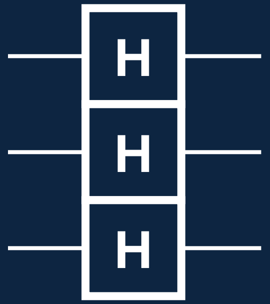
*Except for the first term.

Zero-controlled Z gets closer to desired phase pattern, then another H transform “converts” to magnitude.

$$\frac{1}{\sqrt{16}}\begin{pmatrix} 3|000\rangle \\ +|001\rangle \\ +|010\rangle \\ -|011\rangle \\ +|100\rangle \\ -|101\rangle \\ -|110\rangle \\ +|111\rangle \end{pmatrix}$$

$|1\rangle$

$$\frac{1}{\sqrt{16}}\begin{pmatrix} 3|000\rangle \\ -|001\rangle \\ -|010\rangle \\ +|011\rangle \\ -|100\rangle \\ +|101\rangle \\ +|110\rangle \\ -|111\rangle \end{pmatrix}$$



$$\frac{1}{\sqrt{32}}\begin{pmatrix} |000\rangle + |001\rangle + |010\rangle + |011\rangle + \\ |100\rangle + |101\rangle + |110\rangle + 5|111\rangle \end{pmatrix}$$

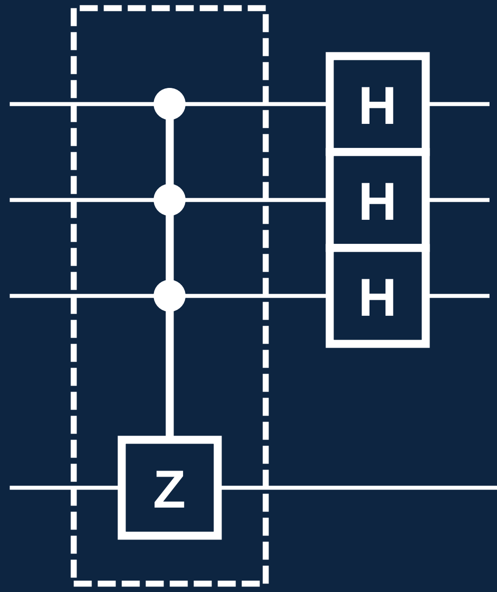
$$\frac{1}{\sqrt{8}}\begin{bmatrix} 3 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 3 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 3 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 3 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 3 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 3 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 3 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{matrix} \longrightarrow 2 \\ \longrightarrow 2 \\ \longrightarrow 2 \\ \longrightarrow 2 \\ \longrightarrow 2 \\ \longrightarrow 2 \\ \longrightarrow 2 \\ \longrightarrow 10 \end{matrix}$$

The magnitude of the s-valued term has been boosted!

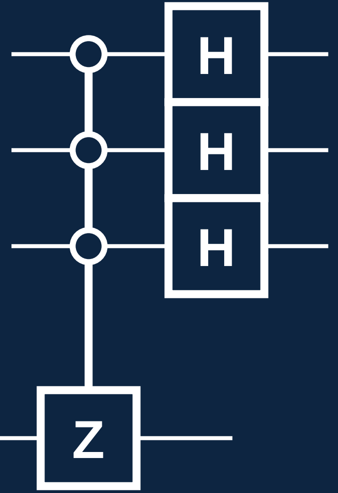
The oracle, H transform, and zero-controlled Z can be applied again to get even closer.

$$\frac{1}{\sqrt{32}}\begin{pmatrix}|000\rangle + \\ |001\rangle + \\ |010\rangle + \\ |011\rangle + \\ |100\rangle + \\ |101\rangle + \\ |110\rangle + \\ 5|111\rangle\end{pmatrix}$$

$|1\rangle$



$$\frac{1}{\sqrt{64}}\begin{pmatrix}1|000\rangle \\ +3|001\rangle \\ +3|010\rangle \\ -3|011\rangle \\ +3|100\rangle \\ -3|101\rangle \\ -3|110\rangle \\ +3|111\rangle\end{pmatrix}$$



$$\frac{1}{\sqrt{128}}\begin{pmatrix}|000\rangle + \\ |001\rangle + \\ |010\rangle + \\ |011\rangle + \\ |100\rangle + \\ |101\rangle + \\ |110\rangle - \\ 11|111\rangle\end{pmatrix}$$

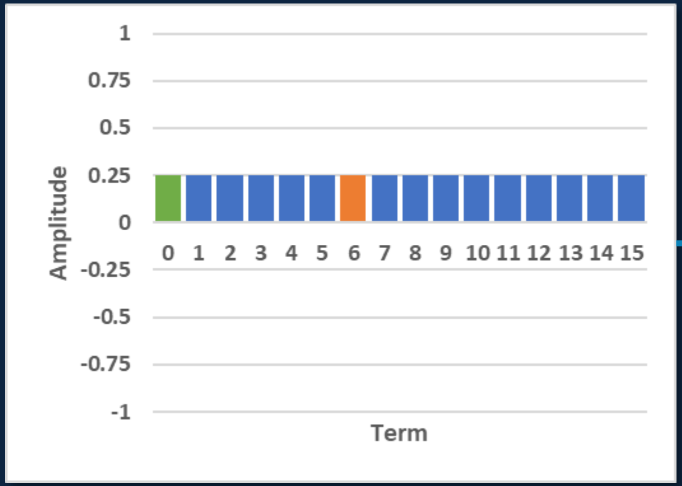
Negative phase means we can't get any closer.

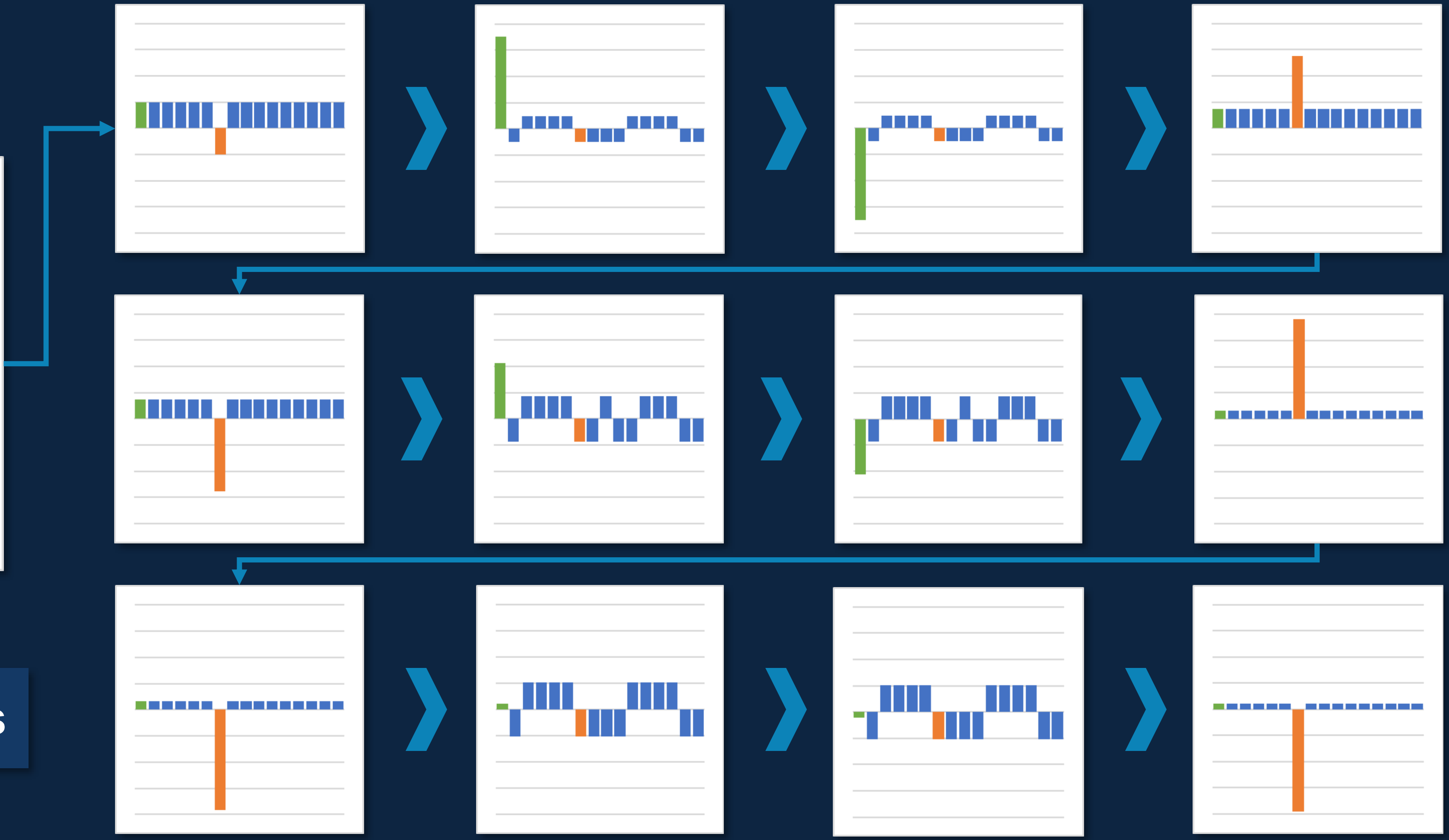
After 2 iterations, the probability of measuring $|s\rangle$ is $\frac{121}{128} = 94.5\%$

MITRE

The optimal number of iterations is $\left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$, where N is the size of the search space.

$s = 0110$ (6)



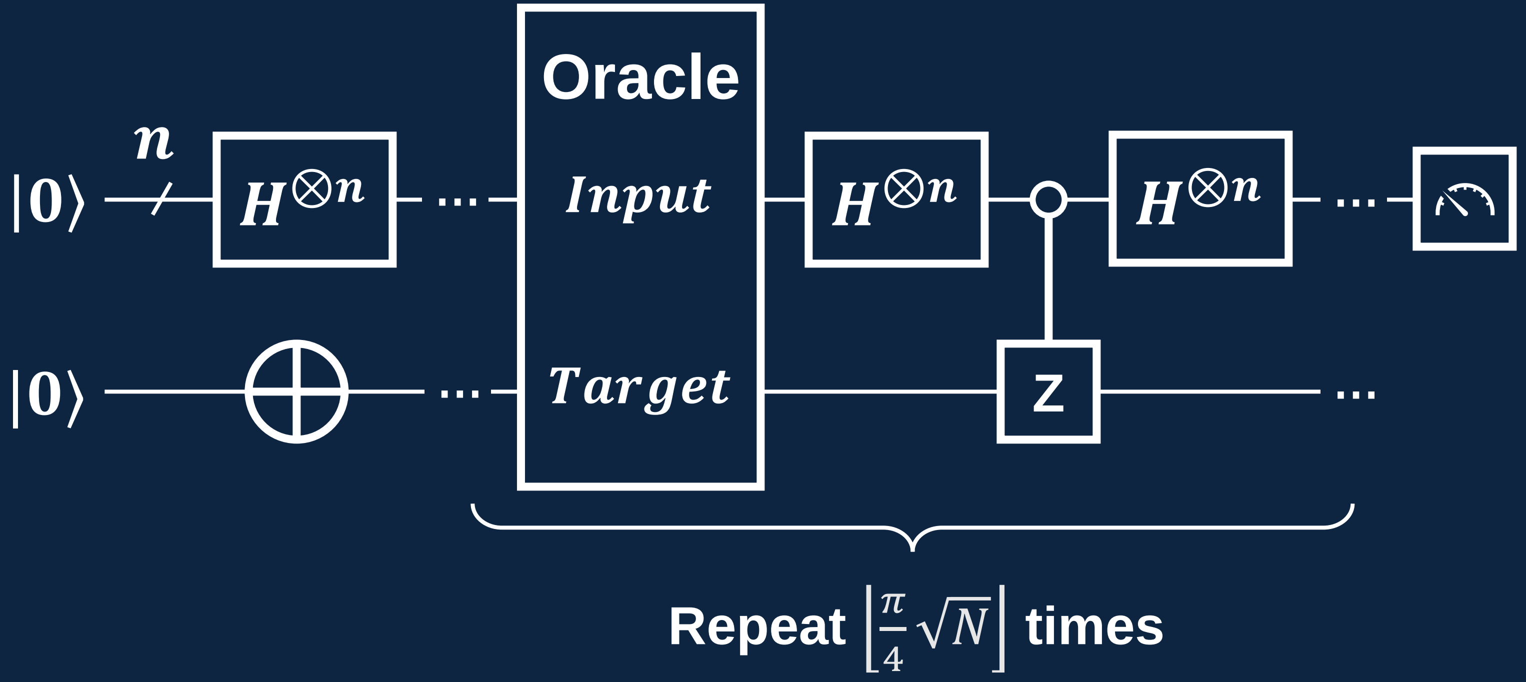


$\left\lfloor \frac{\pi}{4}\sqrt{16} \right\rfloor = \lfloor \pi \rfloor = 3$ iterations

MITRE

Grover's Algorithm

1. Prepare the input register in a uniform superposition and the target in the $|1\rangle$ state.
2. Run the amplitude amplification step $\left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$ times ($N = 2^n$):
   a. Apply the quantum oracle.
   b. Apply the Hadamard transform.
   c. Apply the zero-controlled Z.
   d. Apply the Hadamard transform.
3. Measure the input register. It will contain s with probability approaching 1 for large N.



Grover's algorithm performs unstructured search in $O(\sqrt{N})$ time, or $O\left(2^{\frac{n}{2}}\right)$, where n is the number of bits in the search space.

The Multiverse

Why does measurement seem to change the state of a quantum system?

The **Copenhagen interpretation** says (essentially) to use quantum mechanics until measurement, at which point classical mechanics takes over.

Quantum

$$|Q\rangle = a|0\rangle + b|1\rangle$$

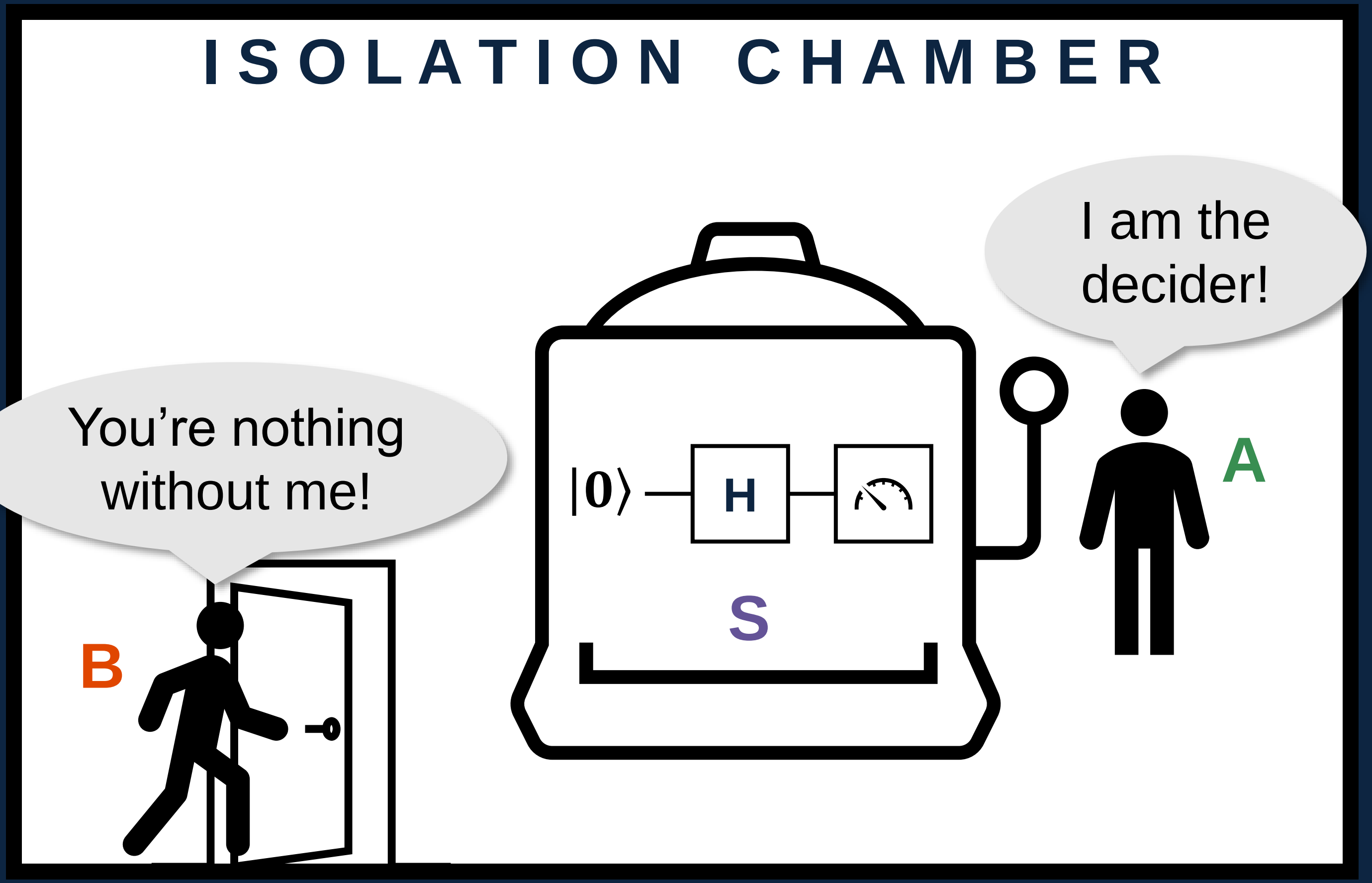
Classical

$$\mathrm{Prob}_{|0\rangle} = |a|^2 \quad |Q\rangle = |0\rangle$$

$$\mathrm{Prob}_{|1\rangle} = |b|^2 \quad |Q\rangle = |1\rangle$$

MITRE

What is measurement, anyway?



A measures a quantum state S.

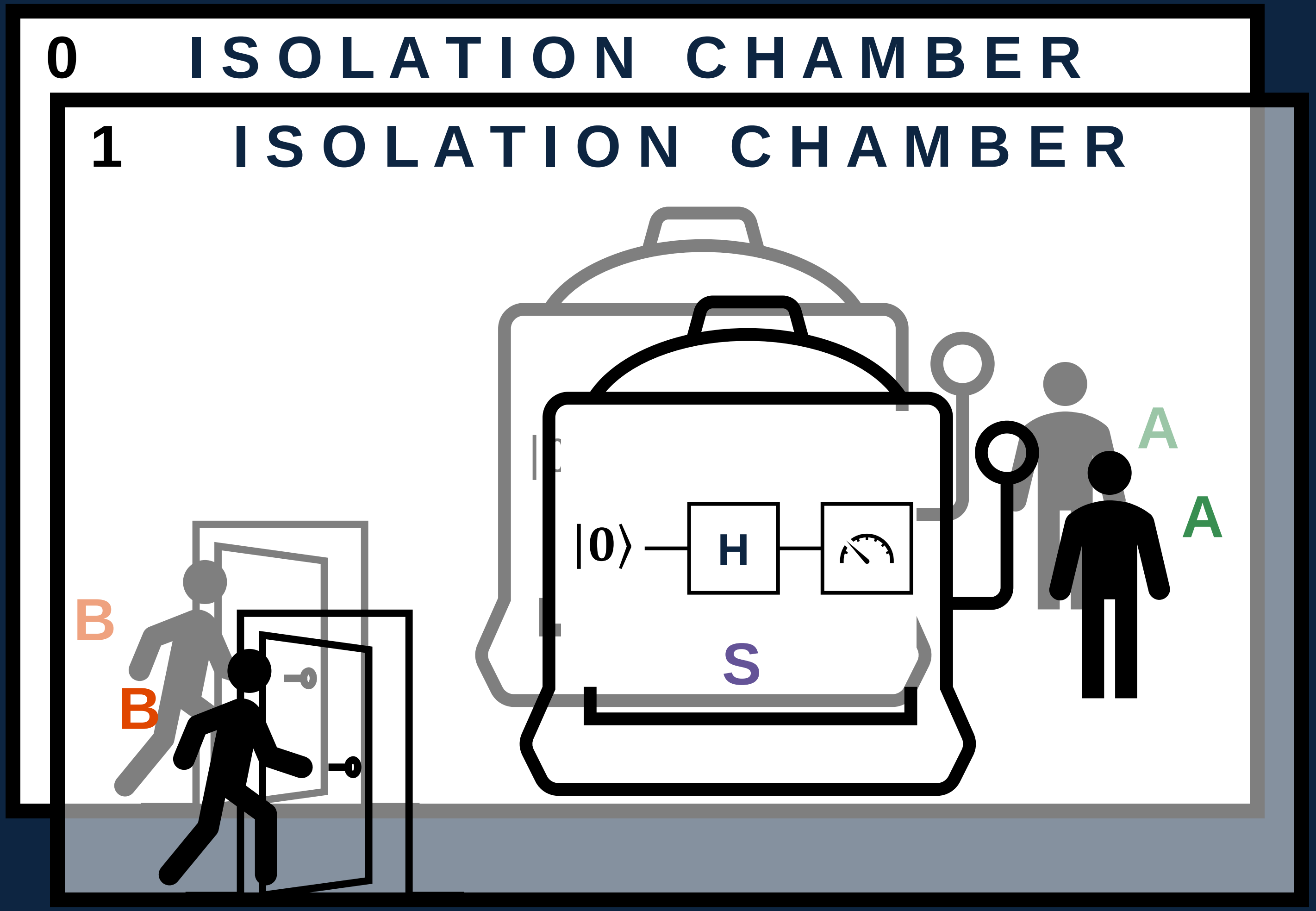
A's action decides the outcome. (Right?)

B opens the door.

Is this a measurement?
If so, is S decided then?

Is A+S a quantum or classical object before B measures?

What if measurement and entanglement are the same process?



Before A measures,

$$|S\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

After A measures,

$$|S, A\rangle = \frac{1}{\sqrt{2}}(|0, A_0\rangle + |1, A_1\rangle)$$

After B measures,

$$|S, A, B\rangle = \frac{1}{\sqrt{2}}(|0, A_0, B_0\rangle + |1, A_1, B_1\rangle)$$

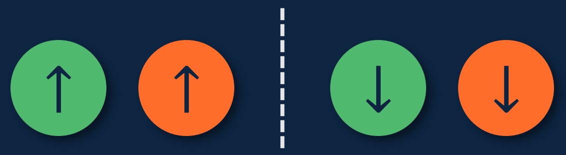
The multiverse is an emergent consequence of taking quantum mechanics seriously as a universal theory.

- **All objects, at all scales and all times, obey quantum mechanics (Schrödinger equation).**

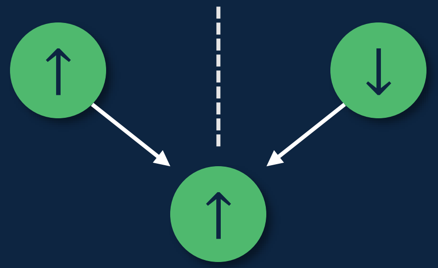
$$\boxed{i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle}$$

- **Superposition is when a physical variable has different values in different universes.**

- **Entanglement describes the relationship between physical variables in the same universe.**



- **Interference occurs when two different universes become identical through some physical process.**



The multiverse idea was first proposed in 1957 by Hugh Everett. It is still controversial.

Q: Since we cannot directly observe the other universes, isn’t this unscientific?

A: We observe their effects through interference phenomena.

Q: Ok, but we can’t communicate between universes, right?

A: Right, we can’t talk to identical copies of ourselves in other universes. (Then they would no longer be identical!)

Q: So, how do we know they exist?

A: For one thing, we can collaborate with them in a quantum computation. After all, how is it possible that a quantum algorithm provides a speedup?

Q: This is all a bit wacky; it must be wrong.

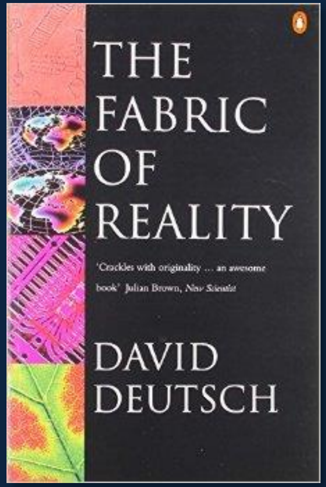
A: Do you have a better theory?

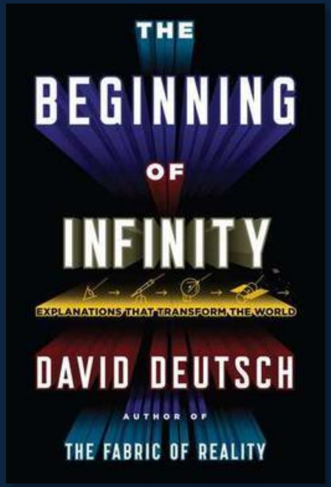
MITRE

David Deutsch (of the D-J algorithm) explores the implications of the multiverse in his books.

A few of his ideas, summarized:

- Universes are fungible, like money in your bank account. When you transact, you don't care which dollar is being used, only how many dollars.
- Counterfactual conditional statements have physical meaning. The sentence, "If I had chosen option X, then Y would have occurred" is a claim that, "In universes where I did choose X, Y did occur."
- A fundamental property of knowledge is that it is replicated across the multiverse.
- Other times (the future and past) are just other universes within the multiverse.
- **For more, read (or listen) to the books!**





MITRE