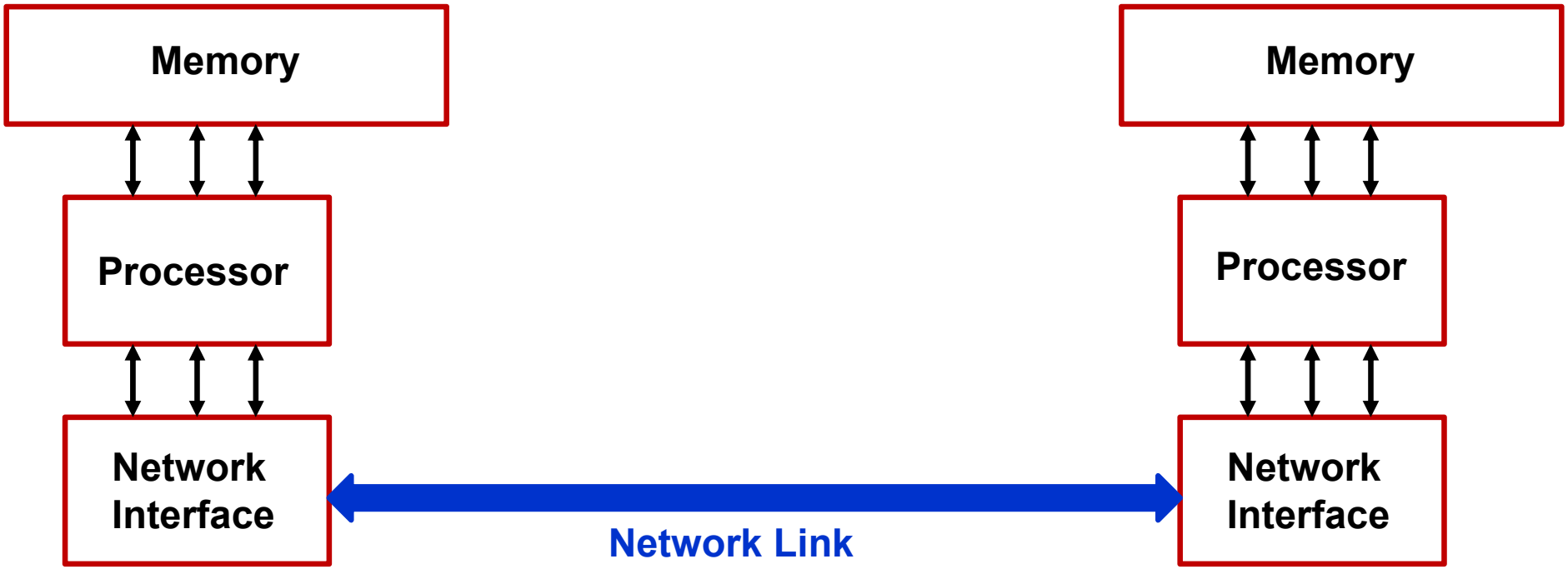
Lecture 23

Quantum Information Processing and Computation - II
Quantum No-Cloning Theorem
Quantum Networks and Quantum Teleportation
Grover's Search Algorithm
Quantum Superdense Coding
Quantum Parallelism and the Deutsch Algorithm
The Bernstein-Vazirani Algorithm

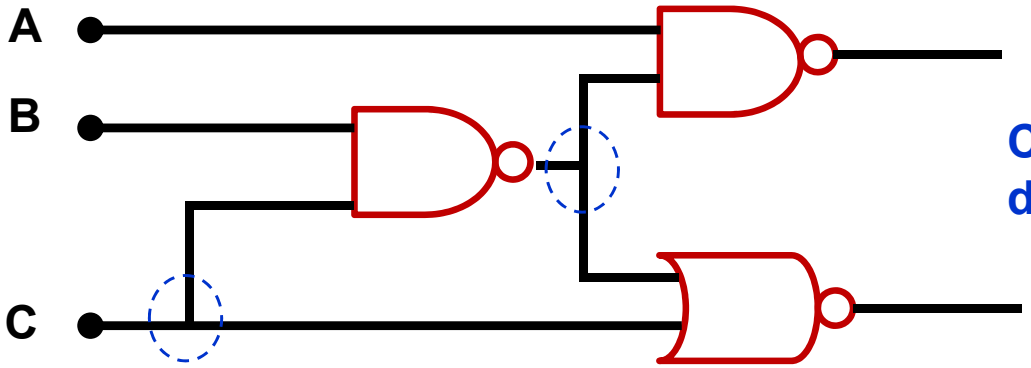
In this lecture you will learn:

- **Can one copy qubits?**
- **Quantum networks and teleportation**
- **Quantum memory search and Grover's algorithm**
- **Quantum information, coding, and superdense coding**
- **Quantum parallelism, quantum computing and the Deutsch algorithm**
- **Quantum parallelism, quantum computing and the Bernstein-Vazirani algorithm**

Classical Information Processing



Classical Digital Circuits: Bit Copying



Copying of bits is very common in digital circuits

We make copies of digital data and store it all the time every day:

Magnetic hard drive

Electronic flash drive

Cloud data storage

Can quantum bits or qubits be copied?

Qubit Copying

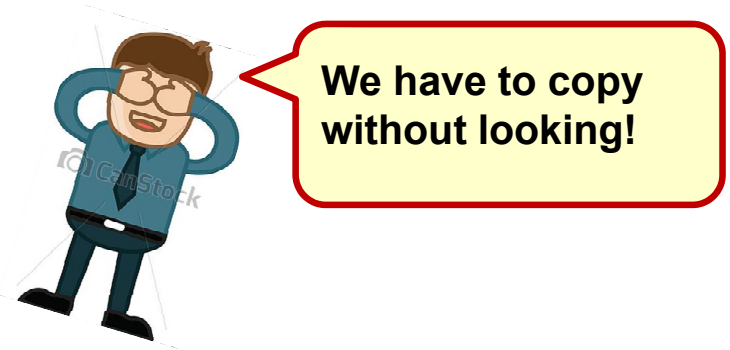
$$|\psi\rangle_A = \alpha|0\rangle_A + \beta|1\rangle_A$$

How do we make a copy of this qubit?

What we want is:

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

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

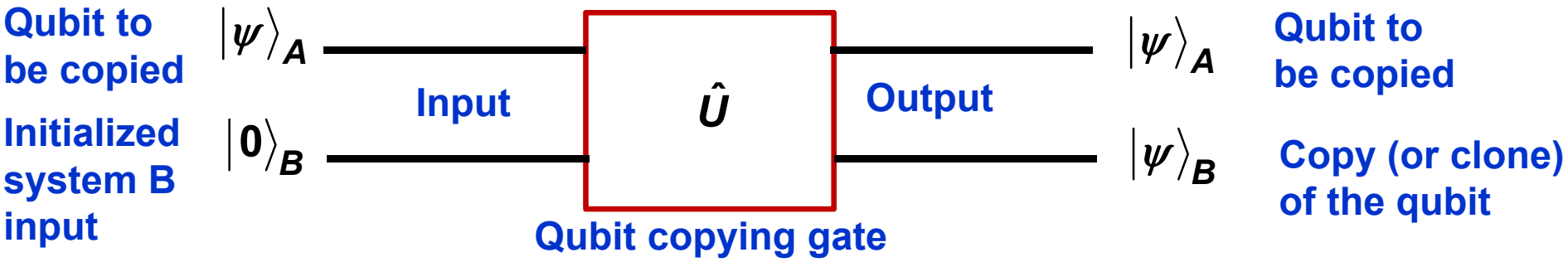


We have to make a copy without "looking" at it (or without measuring it)

If we measure it, we will collapse it !!

Copying (or Cloning) Quantum Bits (or Qubits)

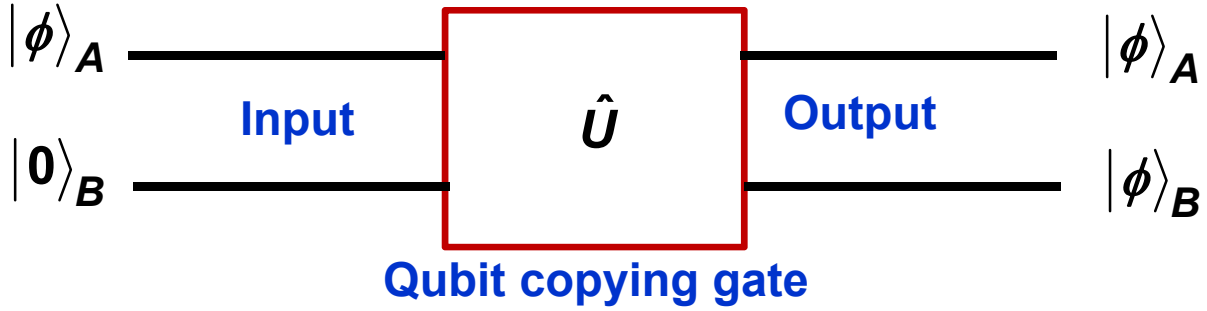
Suppose one has a qubit $|\psi\rangle_A$ of system A and one needs to make a copy of this qubit



Suppose one has realized this quantum copying or cloning device. We write its operation as:

$$|\psi\rangle_A|\psi\rangle_B = \hat{U}|\psi\rangle_A|0\rangle_B$$

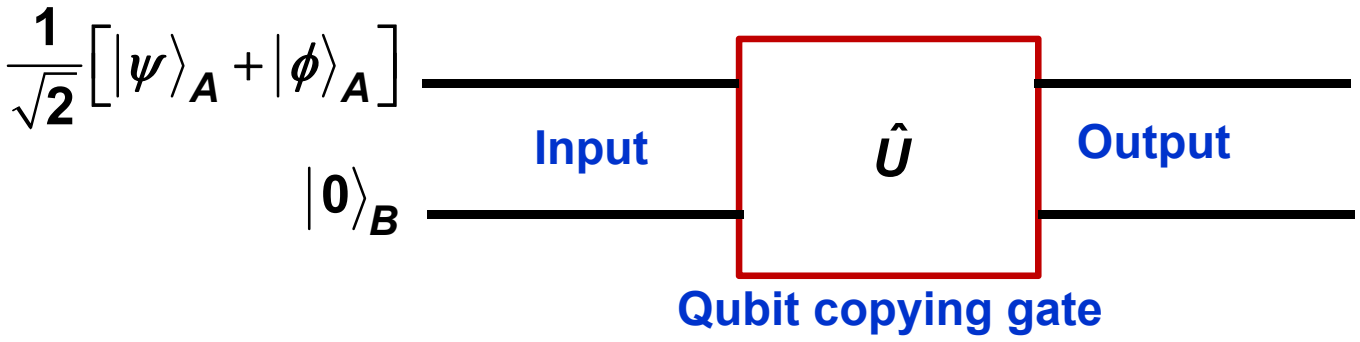
Suppose we then use this machine to clone another qubit $|\phi\rangle_A$ of system A:



$$|\phi\rangle_A|\phi\rangle_B = \hat{U}|\phi\rangle_A|0\rangle_B$$

Copying (or Cloning) Quantum Bits (or Qubits)

Satisfied with your success, you decide to make a copy of the superposition state:



We can work out the output state as follows:

$$\hat{U}\left\{\frac{1}{\sqrt{2}}\left[|\psi\rangle_A + |\phi\rangle_A\right]\otimes|0\rangle_B\right\} = \hat{U}\frac{1}{\sqrt{2}}\left[|\psi\rangle_A\otimes|0\rangle_B + |\phi\rangle_A\otimes|0\rangle_B\right]$$

$$= \hat{U}\frac{1}{\sqrt{2}}\left[|\psi\rangle_A|0\rangle_B + |\phi\rangle_A|0\rangle_B\right] = \frac{1}{\sqrt{2}}\left[\hat{U}|\psi\rangle_A|0\rangle_B + \hat{U}|\phi\rangle_A|0\rangle_B\right]$$

$$= \frac{1}{\sqrt{2}}\left[|\psi\rangle_A|\psi\rangle_B + |\phi\rangle_A|\phi\rangle_B\right] \longrightarrow \text{Entangled state!}$$

But we wanted this output:

$$\frac{1}{\sqrt{2}}\left[|\psi\rangle_A + |\phi\rangle_A\right]\otimes\frac{1}{\sqrt{2}}\left[|\psi\rangle_B + |\phi\rangle_B\right]$$

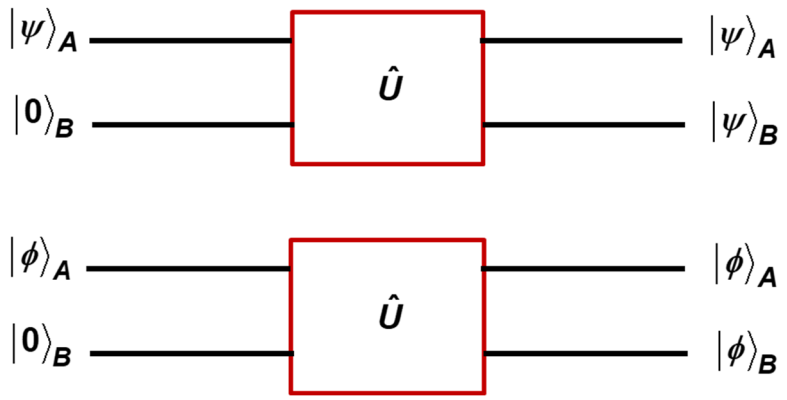
No linear quantum operation can perfectly clone any arbitrary qubit

Quantum No-Cloning Theorem: Formal Proof by Contradiction

Suppose we have a cloning machine that can clone two arbitrary states of system A: $|\psi\rangle_A$ and $|\phi\rangle_A$:

$$|\psi\rangle_A|\psi\rangle_B = \hat{U}|\psi\rangle_A|0\rangle_B$$

$$|\phi\rangle_A|\phi\rangle_B = \hat{U}|\phi\rangle_A|0\rangle_B$$



Take the inner product of the states appearing on the left and right sides of the above two equations:

$$\left({}_A\langle\psi|{}_B\langle\psi|\right)\left(|\phi\rangle_A|\phi\rangle_B\right) = \left({}_A\langle\psi|{}_B\langle 0|\hat{U}^\dagger\right)\left(\hat{U}|\phi\rangle_A|0\rangle_B\right)$$

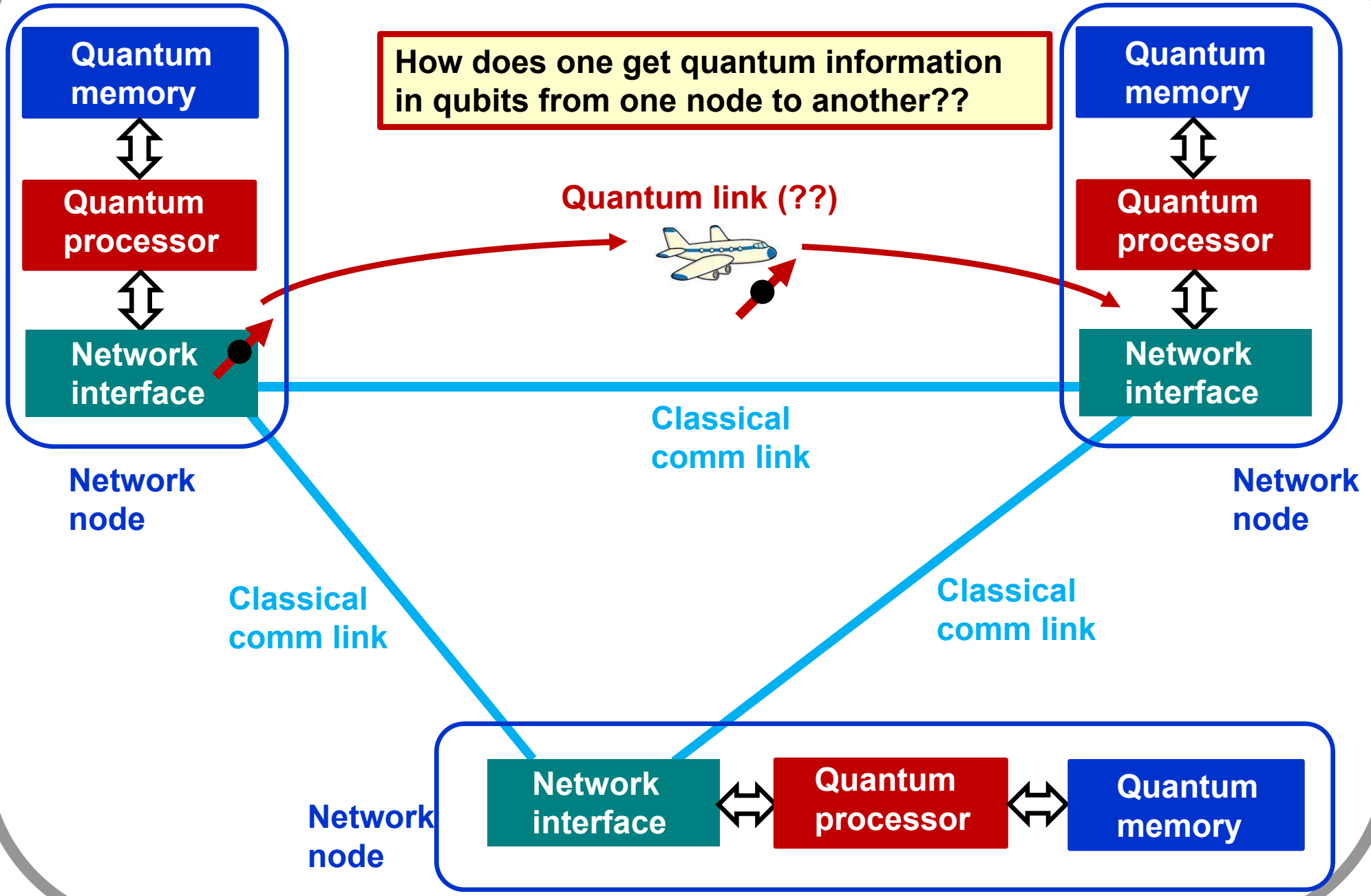
$$\Rightarrow {}_A\langle\psi|\phi\rangle_A\,{}_B\langle\psi|\phi\rangle_B = {}_A\langle\psi|{}_B\langle 0|\hat{U}^\dagger\hat{U}|\phi\rangle_A|0\rangle_B$$

$$\Rightarrow {}_A\langle\psi|\phi\rangle_A\,{}_B\langle\psi|\phi\rangle_B = {}_A\langle\psi|\phi\rangle_A\,{}_B\langle 0|0\rangle_B$$

$$\Rightarrow \langle\psi|\phi\rangle^2 = \langle\psi|\phi\rangle$$

This means that either $|\langle\psi|\phi\rangle| = 0$ or $|\langle\psi|\phi\rangle| = 1$. Which means that the two states we considered $|\psi\rangle_A$ and $|\phi\rangle_A$ cannot be arbitrary – they are either the same or orthogonal and hence our initial assumption that any arbitrary state of system A can be cloned was wrong

Quantum Information Transfer and Quantum Networks



Quantum Teleportation: The Setting

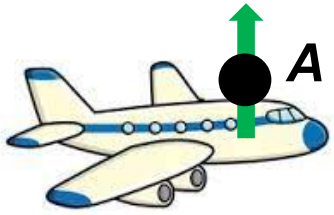
Consider the following scenario:

Alice has a qubit in some unknown state $|\psi\rangle_A$ and she wants to send it to Bob, who is sitting in Greece with his own qubit initialized in state $|0\rangle_B$. Alice and Bob want $|0\rangle_B$ to become $|\psi\rangle_B$

In the most general case: $|\psi\rangle_A = \alpha|0\rangle + \beta|1\rangle$

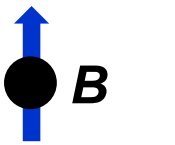
Note: Alice cannot "look" at her qubit and then convey the information to Bob over the telephone so that Bob can convert his own qubit to match that of Alice. "Looking" will collapse the qubit.

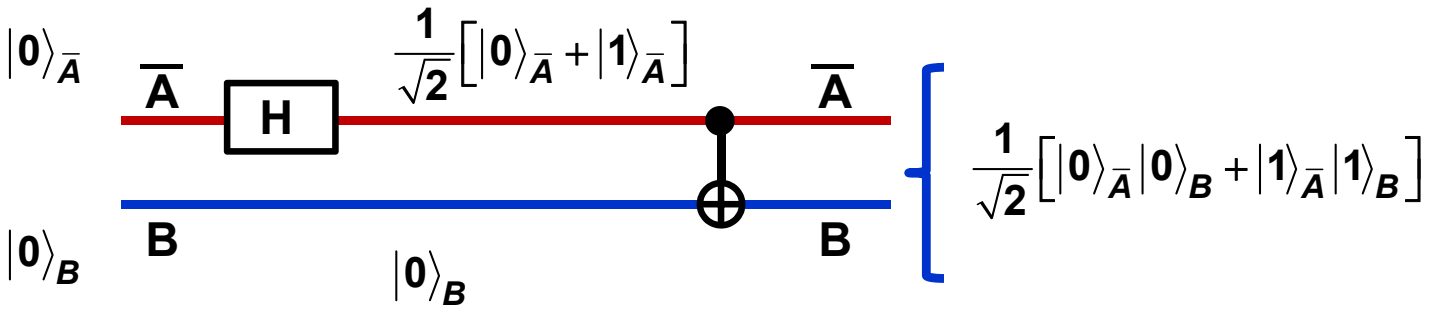
The only way, it seems, this could be possible is if Alice were to send her own qubit physically on a plane all the way to Bob …….



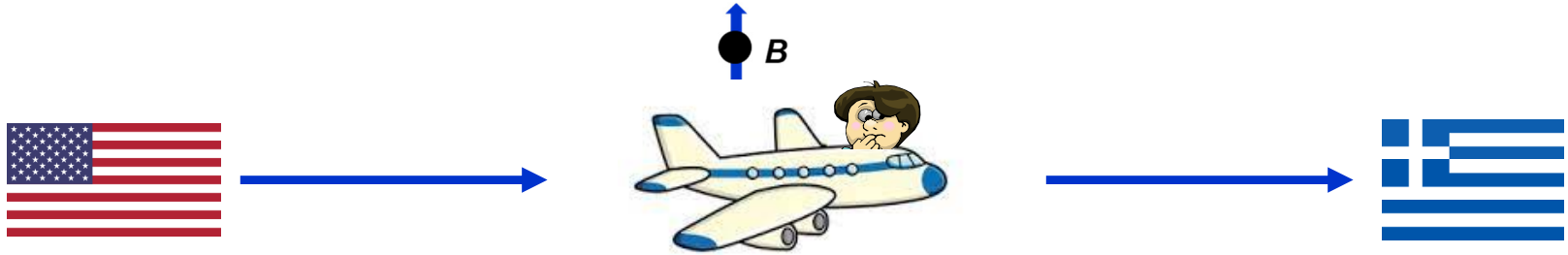
Quantum Teleportation: Entanglement as a Resource

A long long time ago, when Bob was still in USA, Alice and Bob generated an entangled qubit pair $\bar{A}$ and B …….





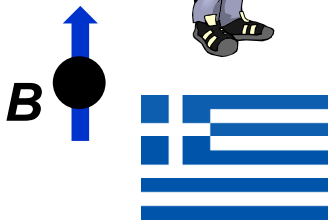
And then Bob went away to Greece and took his entangled qubit with him …….



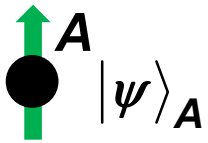
Quantum Teleportation: Entanglement as a Resource

Alice and Bob, now in different countries, share an entangled qubit pair $\overline{A}$ and B :

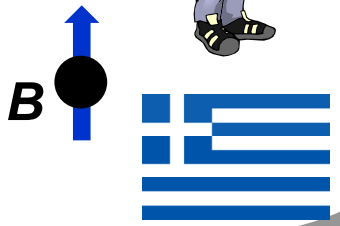
$$|S\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle_{\overline{A}}|0\rangle_B + |1\rangle_{\overline{A}}|1\rangle_B\right]$$



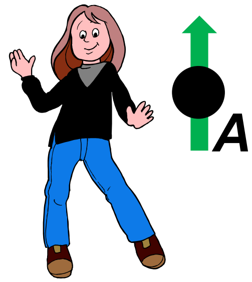
This existing shared entangled qubit pair can be used to "teleport" Alice's new qubit $|\psi\rangle_A$ onto Bob's qubit B



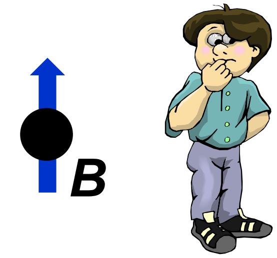
Teleportation



Quantum Teleportation: Local Operations of Alice

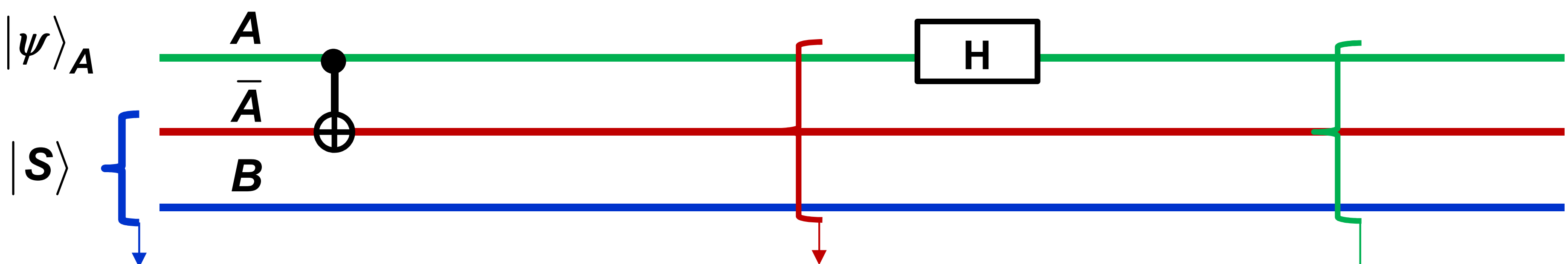


$$|\psi\rangle_A = \alpha|0\rangle + \beta|1\rangle$$



Shared entangled qubit pair

$$|S\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle_{\bar{A}}|0\rangle_B + |1\rangle_{\bar{A}}|1\rangle_B\right]$$

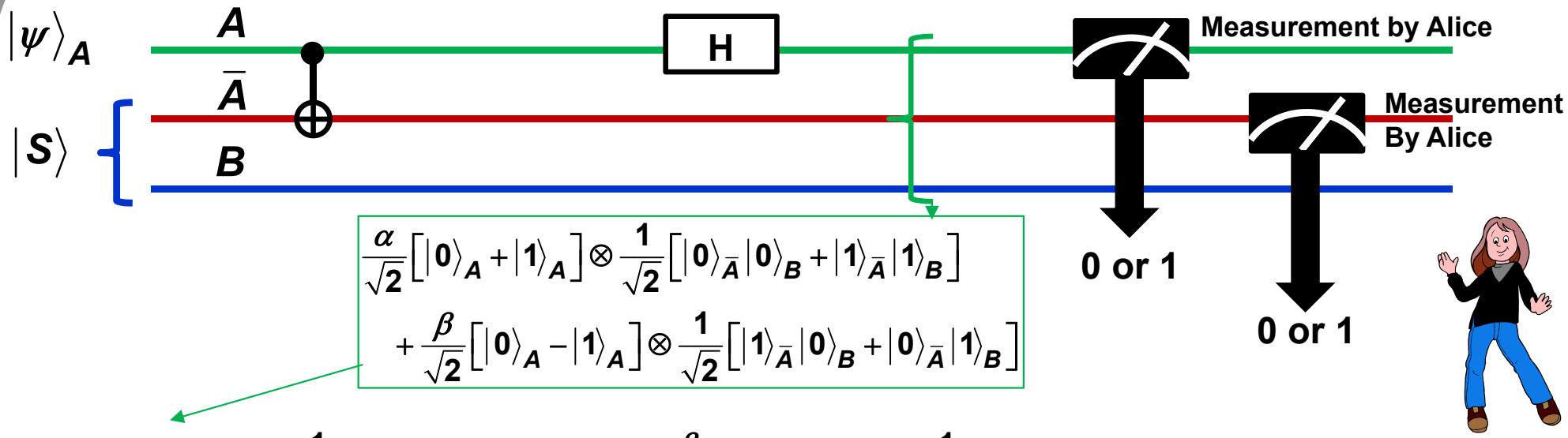


$$|\psi_{in}\rangle = |\psi\rangle_A \otimes |S\rangle$$
$$= |\psi\rangle_A \otimes \frac{1}{\sqrt{2}}\left[|0\rangle_{\bar{A}}|0\rangle_B + |1\rangle_{\bar{A}}|1\rangle_B\right]$$
$$= \alpha|0\rangle_A \otimes \frac{1}{\sqrt{2}}\left[|0\rangle_{\bar{A}}|0\rangle_B + |1\rangle_{\bar{A}}|1\rangle_B\right]$$
$$+ \beta|1\rangle_A \otimes \frac{1}{\sqrt{2}}\left[|0\rangle_{\bar{A}}|0\rangle_B + |1\rangle_{\bar{A}}|1\rangle_B\right]$$

$$\alpha|0\rangle_A \otimes \frac{1}{\sqrt{2}}\left[|0\rangle_{\bar{A}}|0\rangle_B + |1\rangle_{\bar{A}}|1\rangle_B\right]$$
$$+ \beta|1\rangle_A \otimes \frac{1}{\sqrt{2}}\left[|1\rangle_{\bar{A}}|0\rangle_B + |0\rangle_{\bar{A}}|1\rangle_B\right]$$

$$\frac{\alpha}{\sqrt{2}}\left[|0\rangle_A + |1\rangle_A\right] \otimes \frac{1}{\sqrt{2}}\left[|0\rangle_{\bar{A}}|0\rangle_B + |1\rangle_{\bar{A}}|1\rangle_B\right]$$
$$+ \frac{\beta}{\sqrt{2}}\left[|0\rangle_A - |1\rangle_A\right] \otimes \frac{1}{\sqrt{2}}\left[|1\rangle_{\bar{A}}|0\rangle_B + |0\rangle_{\bar{A}}|1\rangle_B\right]$$

Quantum Teleportation: Local Operations of Alice



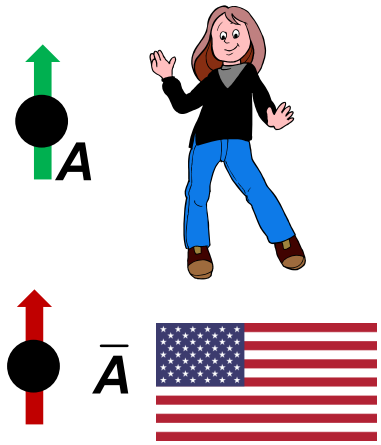
$$\frac{\alpha}{\sqrt{2}}\left[|0\rangle_A+|1\rangle_A\right]\otimes\frac{1}{\sqrt{2}}\left[|0\rangle_{\bar{A}}|0\rangle_B+|1\rangle_{\bar{A}}|1\rangle_B\right]+\frac{\beta}{\sqrt{2}}\left[|0\rangle_A-|1\rangle_A\right]\otimes\frac{1}{\sqrt{2}}\left[|1\rangle_{\bar{A}}|0\rangle_B+|0\rangle_{\bar{A}}|1\rangle_B\right]$$

$$=\frac{1}{2}|0\rangle_A|0\rangle_{\bar{A}}\otimes\left[\alpha|0\rangle_B+\beta|1\rangle_B\right]+\frac{1}{2}|0\rangle_A|1\rangle_{\bar{A}}\otimes\left[\alpha|1\rangle_B+\beta|0\rangle_B\right]$$

$$+\frac{1}{2}|1\rangle_A|0\rangle_{\bar{A}}\otimes\left[\alpha|0\rangle_B-\beta|1\rangle_B\right]+\frac{1}{2}|1\rangle_A|1\rangle_{\bar{A}}\otimes\left[\alpha|1\rangle_B-\beta|0\rangle_B\right]$$

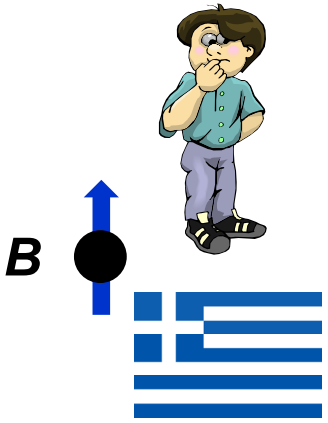
Alice's Results	Probability	Bob's Collapsed Qubit
0 and 0	0.25	$\alpha\|0\rangle_B+\beta\|1\rangle_B$
0 and 1	0.25	$\alpha\|1\rangle_B+\beta\|0\rangle_B$
1 and 0	0.25	$\alpha\|0\rangle_B-\beta\|1\rangle_B$
1 and 1	0.25	$\alpha\|1\rangle_B-\beta\|0\rangle_B$

Quantum Teleportation: Local Operations of Bob



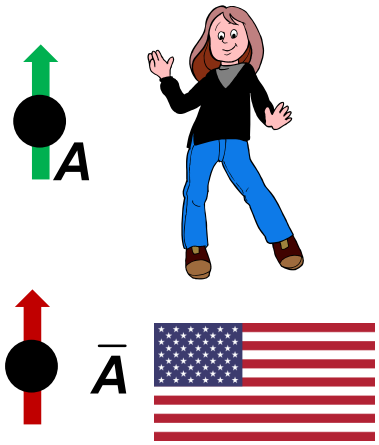
Telephone call

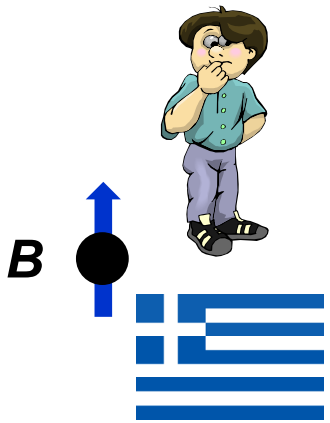
Alice provides just two bits of classical information to Bob based on her measurement results



Alice's Results	Bob's Qubit after Local Operations
0 and 0	$\left[\alpha\|0\rangle_B + \beta\|1\rangle_B\right]$
0 and 1	$\alpha\|1\rangle_B + \beta\|0\rangle_B$ — B — X — B — $\left[\alpha\|0\rangle_B + \beta\|1\rangle_B\right]$
1 and 0	$\alpha\|0\rangle_B - \beta\|1\rangle_B$ — B — Z — B — $\left[\alpha\|0\rangle_B + \beta\|1\rangle_B\right]$
1 and 1	$\alpha\|1\rangle_{\bar{B}} - \beta\|0\rangle_{\bar{B}}$ — B — iY — B — $\left[\alpha\|0\rangle_B + \beta\|1\rangle_B\right]$

Quantum Teleportation: End Result





When the dust has settled the quantum state of the three qubits is any one of the following – each with a-priori probability 1/4

$$|0\rangle_A |0\rangle_{\bar{A}} \otimes \left[\alpha|0\rangle_B + \beta|1\rangle_B\right]$$

$$|0\rangle_A |1\rangle_{\bar{A}} \otimes \left[\alpha|0\rangle_B + \beta|1\rangle_B\right]$$

$$|1\rangle_A |0\rangle_{\bar{A}} \otimes \left[\alpha|0\rangle_B + \beta|1\rangle_B\right]$$

$$|1\rangle_A |1\rangle_{\bar{A}} \otimes \left[\alpha|0\rangle_B + \beta|1\rangle_B\right]$$

Entanglement has vanished – but the initial qubit A of Alice has been "teleported" to qubit B of Bob

Quantum Networks

$$\frac{1}{\sqrt{2}}\left[|0\rangle_{\bar{A}}|0\rangle_{B}+|1\rangle_{\bar{A}}|1\rangle_{B}\right]$$

Quantum processor

Entangled pair photon source

Quantum processor

Network interface (qubit memory, photonic interface, bell measurements, etc)

Network interface

Classical comm link

Classical comm link

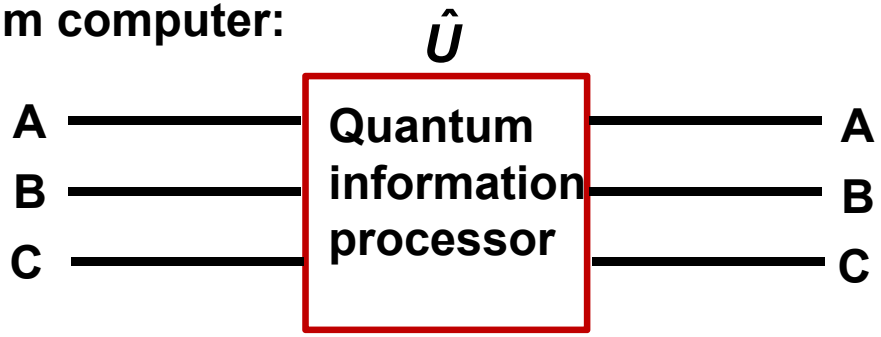
Classical comm link

Network interface

Quantum processor

Quantum Parallelism and Quantum Computing

Consider a quantum computer:



Suppose we would like to know the outputs given each of the following inputs:

$$|\psi\rangle_{in} = |0\rangle_A |0\rangle_B |1\rangle_C \quad |\psi\rangle_{in} = |0\rangle_A |1\rangle_B |0\rangle_C \quad |\psi\rangle_{in} = |0\rangle_A |1\rangle_B |1\rangle_C$$

$$|\psi\rangle_{in} = |1\rangle_A |0\rangle_B |0\rangle_C$$

What if we make a superposition input that has all the above inputs:

$$|\psi\rangle_{in} = \frac{1}{2}\left[|0\rangle_A |0\rangle_B |1\rangle_C + |0\rangle_A |1\rangle_B |0\rangle_C + |0\rangle_A |1\rangle_B |1\rangle_C + |1\rangle_A |0\rangle_B |0\rangle_C\right]$$

Then the output is:

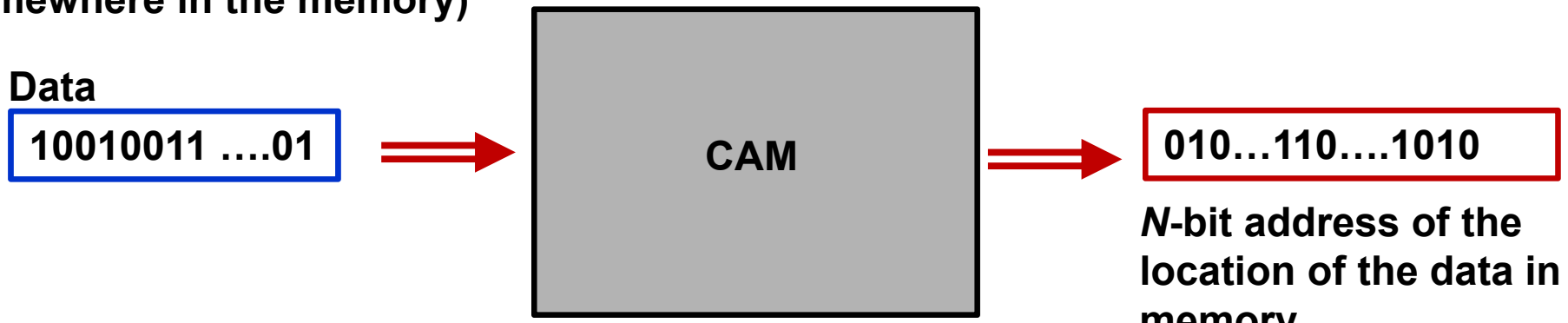
$$|\psi\rangle_{out} = \hat{U}|\psi\rangle_{in}$$

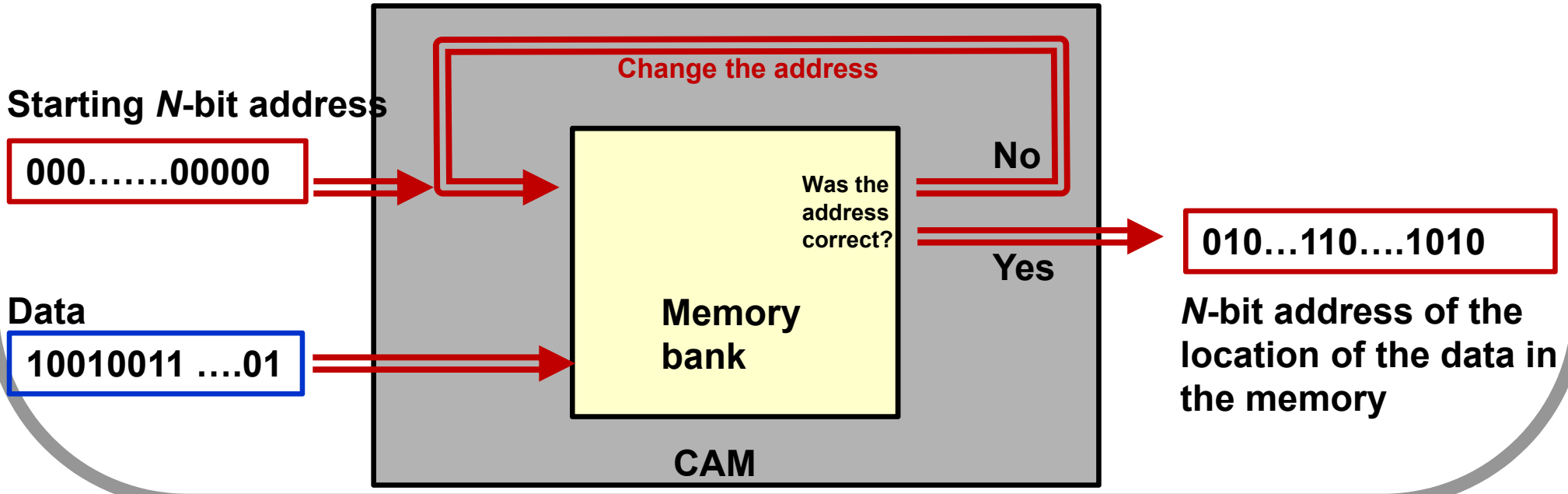
$$= \frac{1}{2}\left[\hat{U}|0\rangle_A |0\rangle_B |1\rangle_C + \hat{U}|0\rangle_A |1\rangle_B |0\rangle_C + \hat{U}|0\rangle_A |1\rangle_B |1\rangle_C + \hat{U}|1\rangle_A |0\rangle_B |0\rangle_C\right]$$

Q: Does this help speed up computation?
A: Not in any straightforward way ……

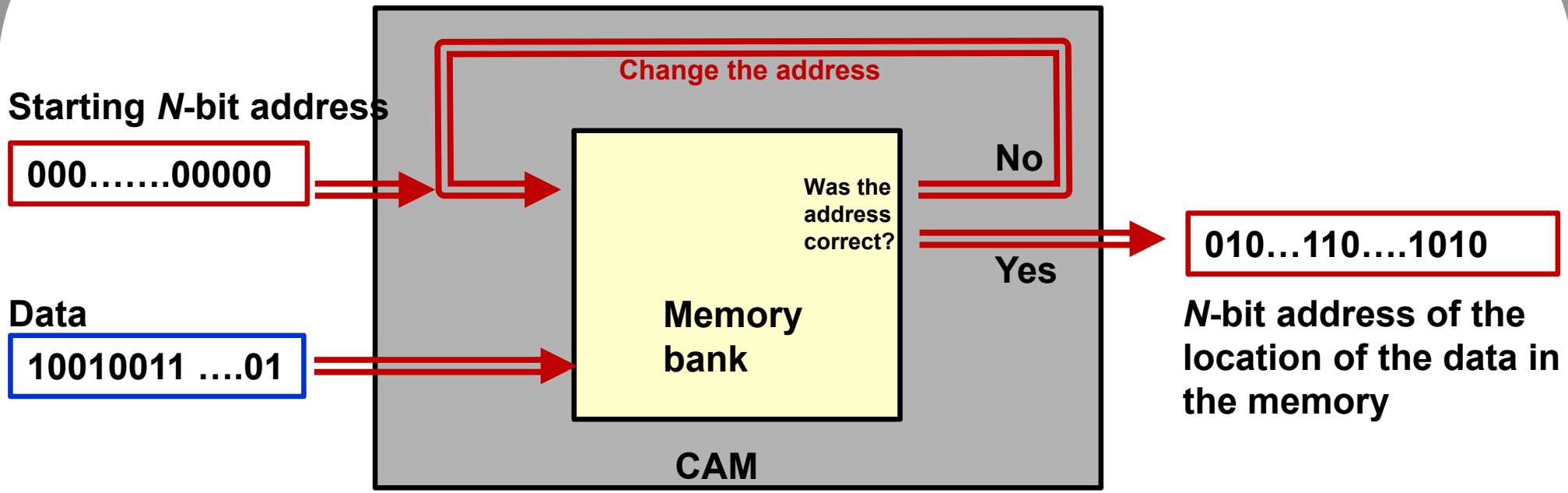
The CAM Memory Search Problem

A content addressable memory takes a data word and finds the address of the location of the data word inside the memory (we will assume the provided data word is present somewhere in the memory)





The CAM Memory Search Problem

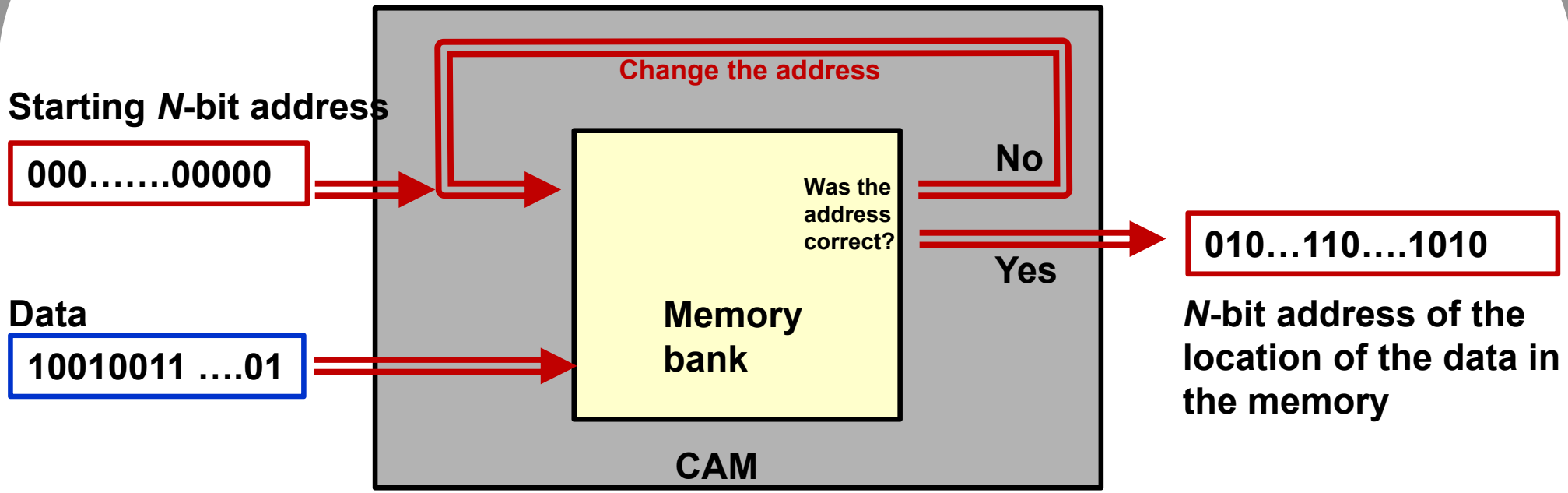


Question: How many calls to the memory bank will be required to search through the memory bank and determine the address of the data in the memory bank?

Answer:

- 2^{N-1} calls will be required on average (with random addresses) to determine the correct address

The CAM Memory Search Problem



Suppose the memory capacity is 2^N ~ 1000 Tera Words (N ~50)

Suppose one memory call takes a 1 micro-sec.

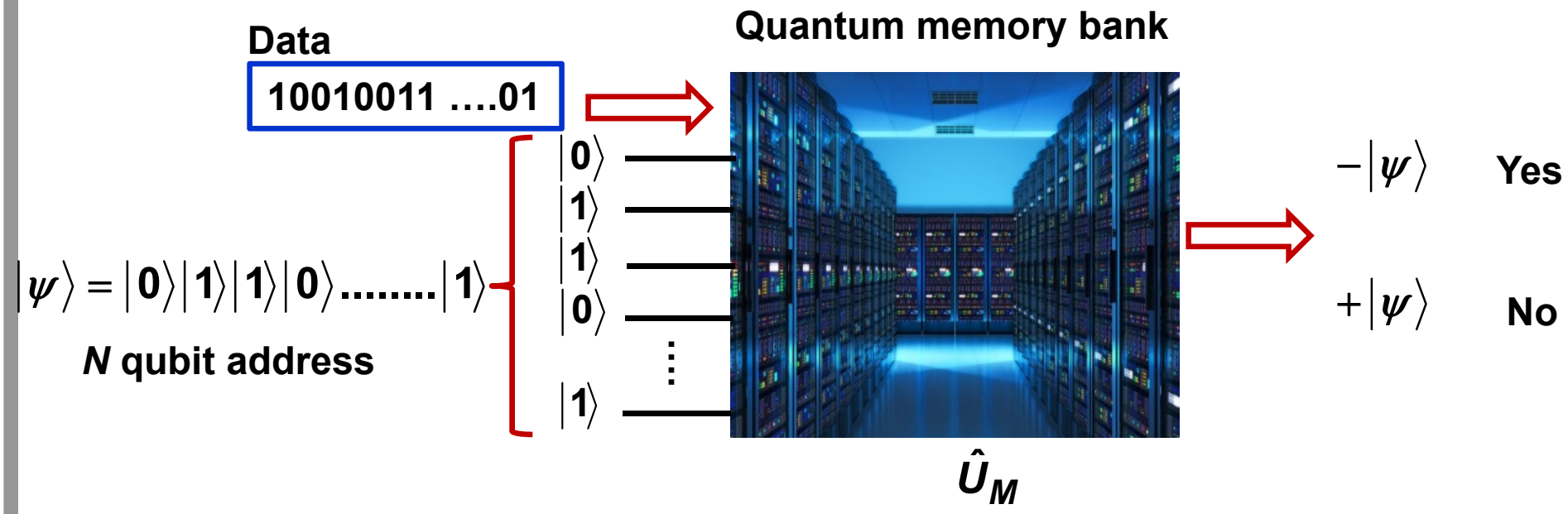
Then:

Searching through the memory bank for the correct address will require ~17 years on average (~35 years in the worst case scenario) !!

A quantum search process on a quantum memory bank may take just ~200 seconds !!

The Quantum Search Problem and Grover's Algorithm

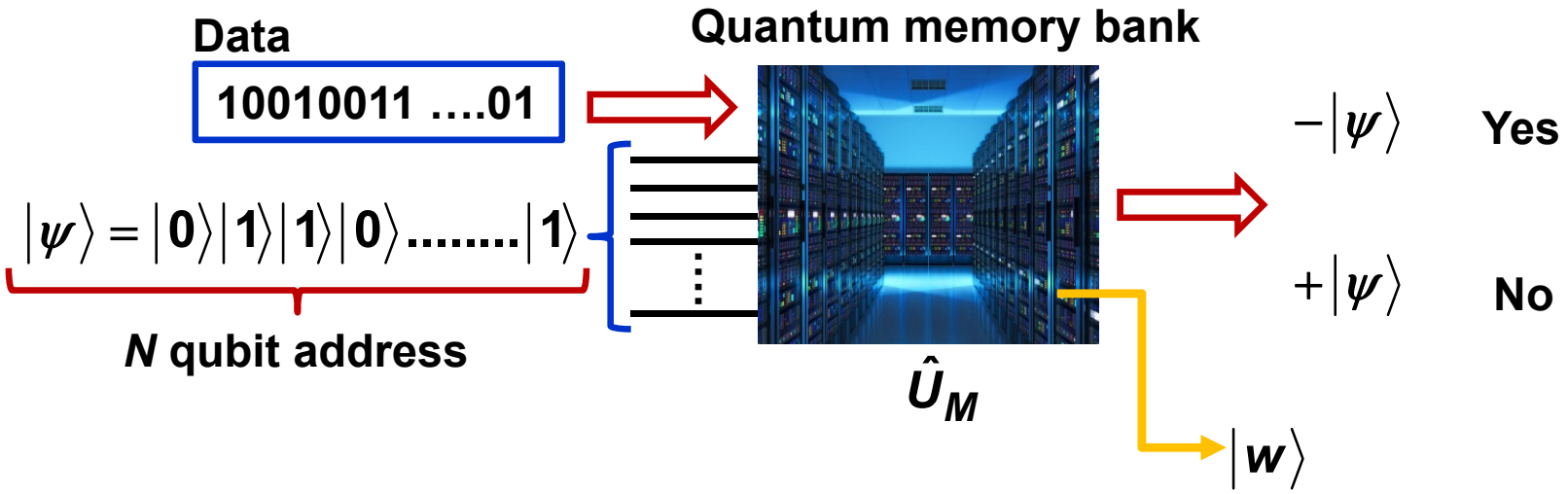
Suppose we have a quantum memory bank that takes data and an *N*-qubit address $|\psi\rangle$ and returns $-|\psi\rangle$ or $+|\psi\rangle$ as outputs if the provided data is stored or not stored in the memory at the address provided, respectively



The quantum memory bank's operation can always be modeled by a unitary operator $\hat{U}_M$

$\hat{U}_M$ is unknown but it is a unitary operator!

The Quantum Search Problem and Grover's Algorithm



Suppose the correct address is given by the *N*-qubit $|w\rangle$

Then the memory bank can be described by the following unitary operator $\hat{U}_M$:

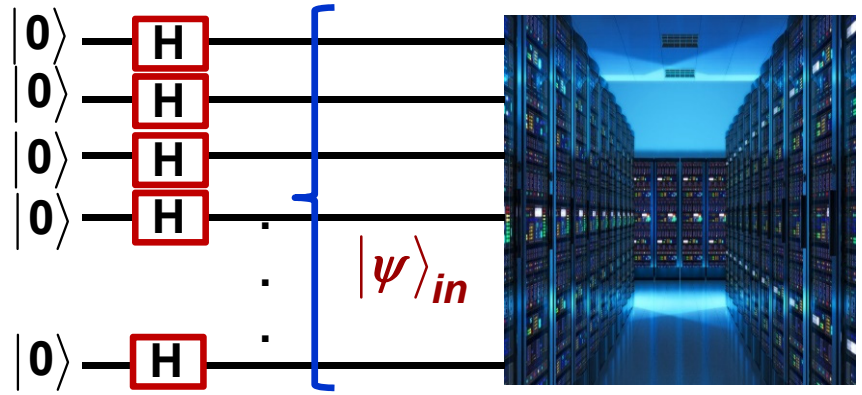
$$\hat{U}_M = \left(\hat{1} - 2|w\rangle\langle w|\right)$$

$$\hat{U}_M U_M^\dagger = U_M^\dagger \hat{U}_M = \hat{1}$$

$$\begin{cases} \hat{U}_M|\psi\rangle = -|\psi\rangle & \text{if} \quad |\psi\rangle = |w\rangle \\ \hat{U}_M|\psi\rangle = +|\psi\rangle & \text{if} \quad |\psi\rangle \neq |w\rangle \end{cases}$$

The Quantum Search Problem and Grover's Algorithm

Make the input:



For the single-qubit Hadamard gate:

$$|0\rangle \;\text{—}\boxed{H}\text{—}\; \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right]$$

$$|\psi\rangle_{in} = |s\rangle = \frac{1}{\sqrt{2^N}}\left[\begin{array}{l}|0\rangle|0\rangle|0\rangle|0\rangle.....|0\rangle|0\rangle + |0\rangle|0\rangle|0\rangle|0\rangle.....|0\rangle|1\rangle + |0\rangle|0\rangle|0\rangle|0\rangle.....|1\rangle|0\rangle + \\ ..... + |w\rangle + ... + |1\rangle|1\rangle|1\rangle|1\rangle.....|1\rangle|1\rangle\end{array}\right]$$

Superposition of all possible addresses

Let:

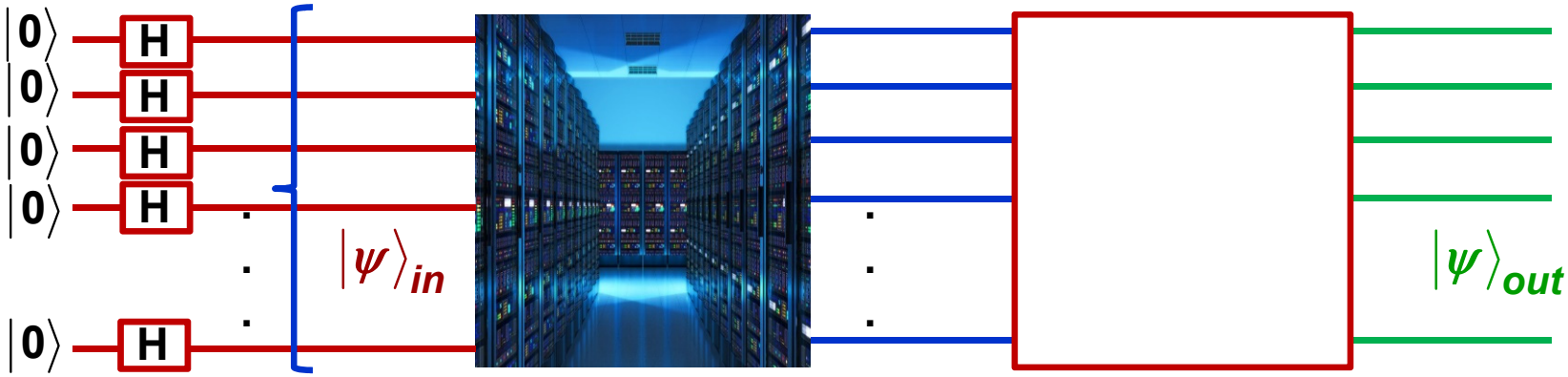
$$|s'\rangle = \frac{\sqrt{2^N}|s\rangle - |w\rangle}{\sqrt{2^N - 1}}$$

$$= \frac{1}{\sqrt{2^N - 1}}\left[\begin{array}{l}|0\rangle|0\rangle|0\rangle|0\rangle.....|0\rangle|0\rangle + |0\rangle|0\rangle|0\rangle|0\rangle.....|0\rangle|1\rangle + |0\rangle|0\rangle|0\rangle|0\rangle.....|1\rangle|0\rangle + \\ ..... + |1\rangle|1\rangle|1\rangle|1\rangle.....|1\rangle|1\rangle\end{array}\right]$$

$$\Rightarrow \langle s'|w\rangle = 0$$

Grover's Algorithm

We will need another gate:

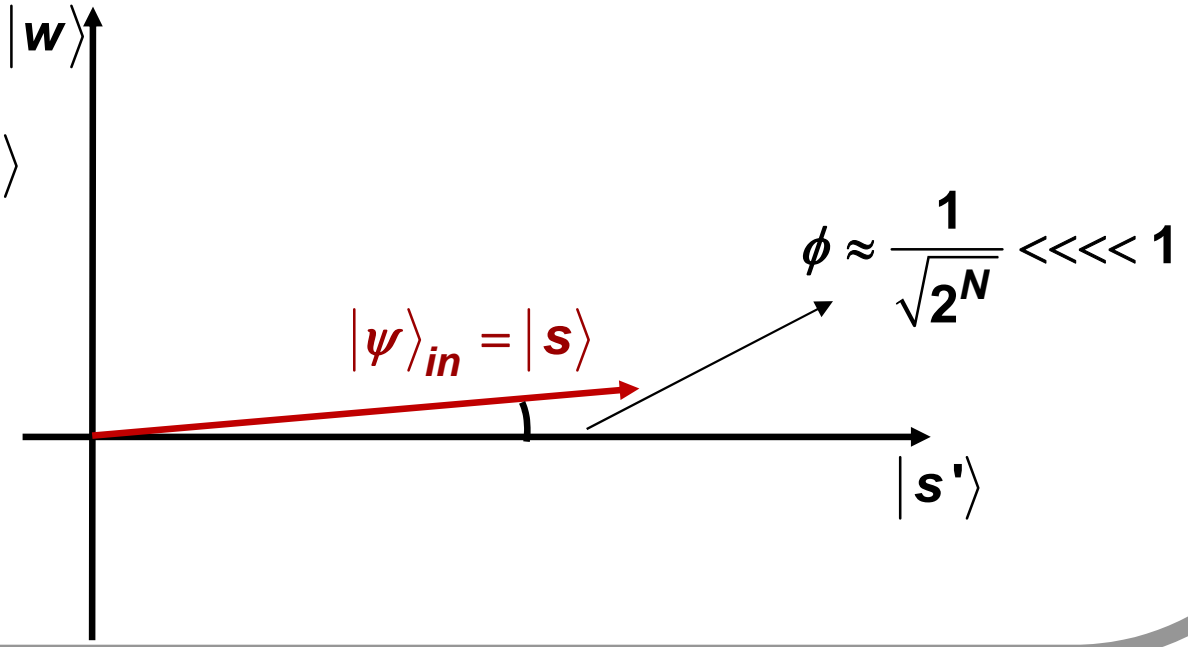


$\hat{U}_M$ $\hat{U}_G$

$$\hat{U}_M = \hat{1} - 2|w\rangle\langle w|$$

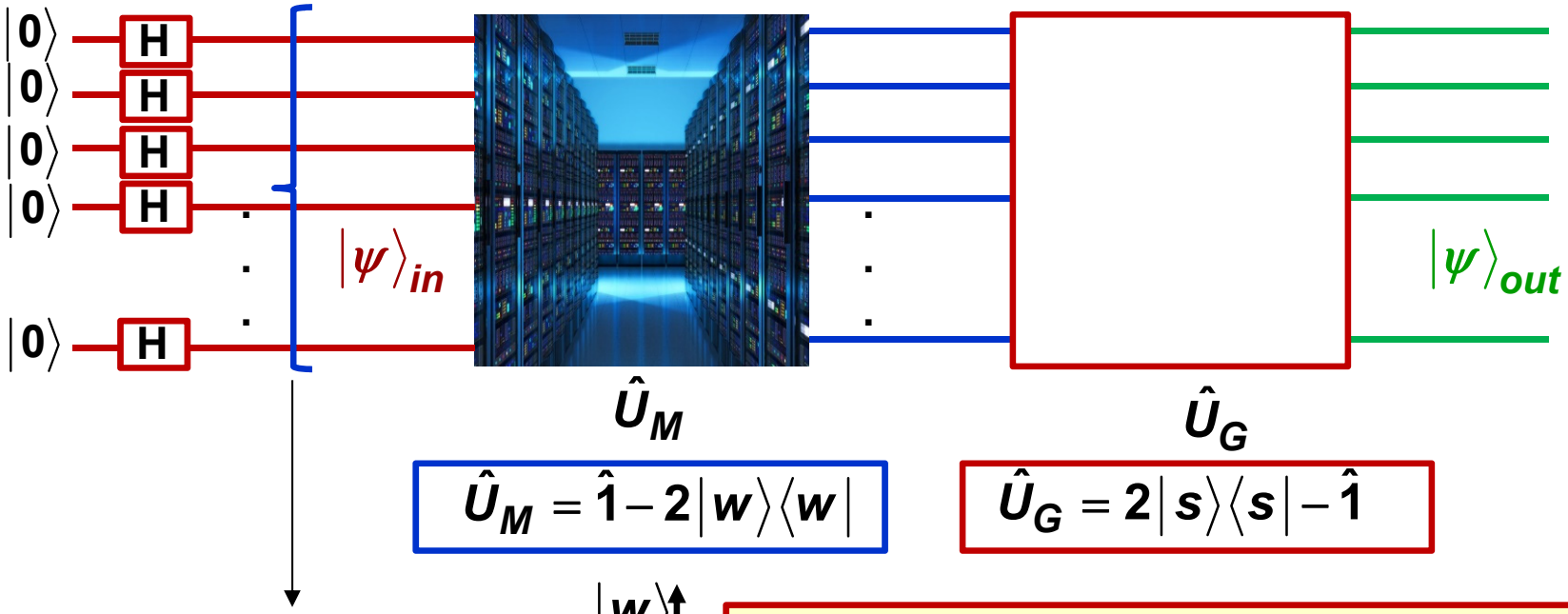
$$\hat{U}_G = 2|s\rangle\langle s| - \hat{1}$$

$$|\psi\rangle_{in} = \sqrt{\frac{2^N - 1}{2^N}}|s'\rangle + \frac{1}{\sqrt{2^N}}|w\rangle$$



Initial input state is almost orthogonal to the desired state

Grover's Algorithm



$$\hat{U}_M = \hat{1} - 2|w\rangle\langle w|$$

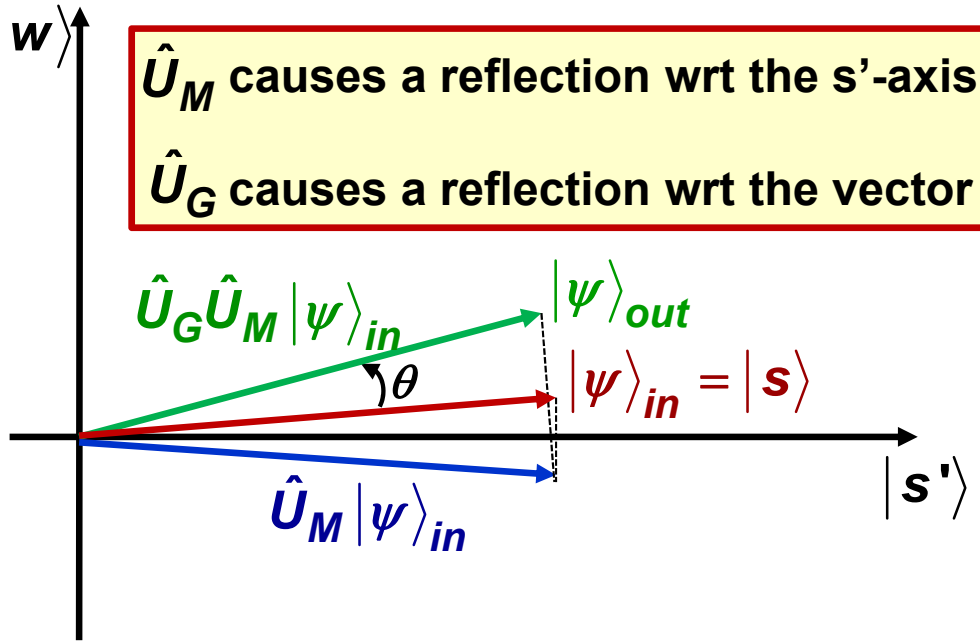
$$\hat{U}_G = 2|s\rangle\langle s| - \hat{1}$$

$\hat{U}_M$ causes a reflection wrt the s'-axis

$\hat{U}_G$ causes a reflection wrt the vector $|s\rangle$

The two operations rotate the input state towards $|w\rangle$ by an angle θ given by:

$$\sin\theta = \frac{\sqrt{2^N - 1}}{2^{N-1}} <<<< 1$$



Grover's Algorithm

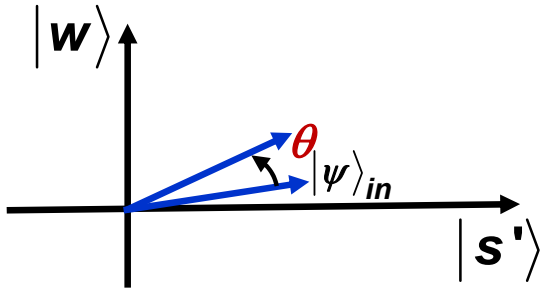
$\hat{U}_M$

$\hat{U}_M = \hat{1} - 2|w\rangle\langle w|$

$\hat{U}_G$

$\hat{U}_G = 2|s\rangle\langle s| - \hat{1}$

$$|\psi\rangle_{in} = \sqrt{\frac{2^N - 1}{2^N}}|s'\rangle + \frac{1}{\sqrt{2^N}}|w\rangle$$



$$\hat{U}_G\hat{U}_M|w\rangle = \cos\theta|w\rangle - \sin\theta|s'\rangle$$

$$\hat{U}_G\hat{U}_M|s'\rangle = \sin\theta|w\rangle + \cos\theta|s'\rangle$$

$$\sin\theta \approx \theta = \frac{\sqrt{2^N - 1}}{2^{N-1}} <<<< 1$$

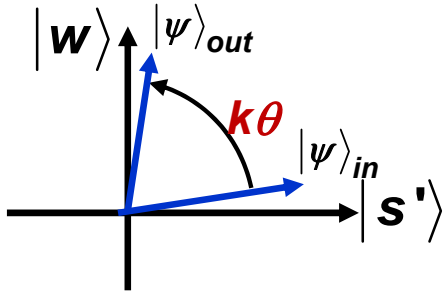
Rotation by θ

$$\hat{R}(\theta)\begin{bmatrix}0\\1\end{bmatrix} = \cos\theta\begin{bmatrix}0\\1\end{bmatrix} - \sin\theta\begin{bmatrix}1\\0\end{bmatrix}$$

$$\hat{R}(\theta)\begin{bmatrix}1\\0\end{bmatrix} = \sin\theta\begin{bmatrix}0\\1\end{bmatrix} + \cos\theta\begin{bmatrix}1\\0\end{bmatrix}$$

Grover's Algorithm

Iterate *k* times:



$$\left(\hat{U}_G\hat{U}_M\right)^k|w\rangle = \cos k\theta|w\rangle - \sin k\theta|s'\rangle$$

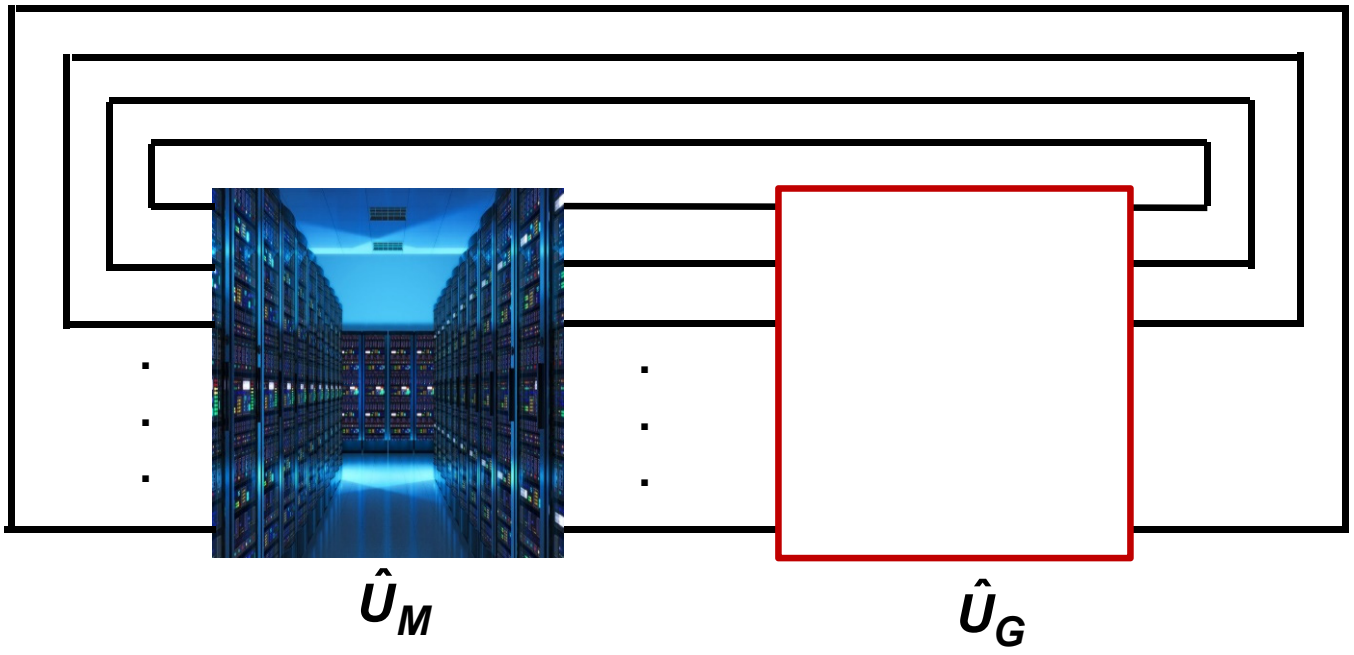
$$\left(\hat{U}_G\hat{U}_M\right)^k|s'\rangle = \sin k\theta|w\rangle + \cos k\theta|s'\rangle$$

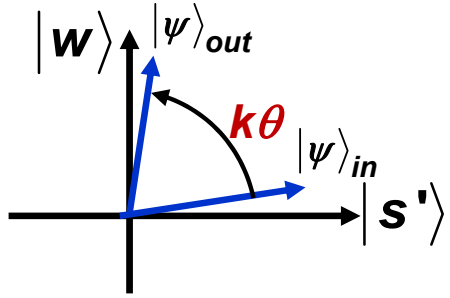
$$\left(\hat{U}_G\hat{U}_M\right)^k|\psi\rangle_{in} = \sqrt{\frac{2^N-1}{2^N}}\left(\hat{U}_G\hat{U}_M\right)^k|s'\rangle - \frac{1}{\sqrt{2^N}}\left(\hat{U}_G\hat{U}_M\right)^k|w\rangle$$

$$= \left(\sqrt{\frac{2^N-1}{2^N}}\cos k\theta + \frac{1}{\sqrt{2^N}}\sin k\theta\right)|s'\rangle + \left(\sqrt{\frac{2^N-1}{2^N}}\sin k\theta - \frac{1}{\sqrt{2^N}}\cos k\theta\right)|w\rangle$$

Grover's Algorithm

Iterate *k* times:





$$|\psi\rangle_{out} = \left(\hat{U}_G\hat{U}_M\right)^k |\psi\rangle_{in} = \left(\sqrt{\frac{2^N-1}{2^N}}\cos k\theta + \frac{1}{\sqrt{2^N}}\sin k\theta\right)|s'\rangle + \left(\sqrt{\frac{2^N-1}{2^N}}\sin k\theta - \frac{1}{\sqrt{2^N}}\cos k\theta\right)|w\rangle$$

Choose number of iteration *k* such that:

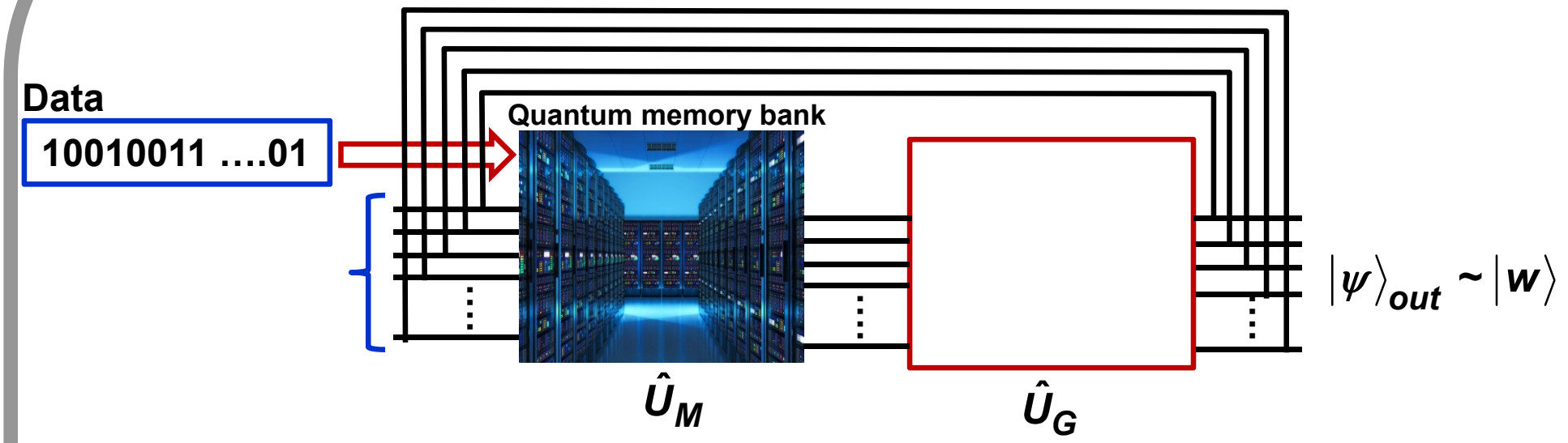
$$\sin k\theta = 1$$

$$\Rightarrow k\theta = \frac{\pi}{2}$$

$$\Rightarrow k = \pi\frac{2^{N-2}}{\sqrt{2^N-1}} \sim \pi\sqrt{2^N}$$

$$\Rightarrow |\psi\rangle_{out} \sim |w\rangle$$

Grover's Algorithm



Suppose the memory capacity is 2^N ~ 1000 Tera Words (N ~50)

Suppose it takes a 1 micro-sec for the U_M operation and 1 micro-sec for the U_G operation

Then:

Searching through the memory bank with nearly 0% probability of error will require just ~210 seconds

Classical memory search time: $\sim 2^N$

Quantum memory search time: $\sim \sqrt{2^N}$

Classical Information in Quantum States

Consider a quantum system whose states belong to a *N*-dimensional Hilbert space with the following basis states:

$$\sum_{j=1}^{N} |e_j\rangle\langle e_j| = \hat{1} \qquad \langle e_j | e_k \rangle = \delta_{jk}$$

Any quantum state of the system can be written as:

$$|\psi\rangle = \sum_{j=1}^{N} a_j |e_j\rangle$$

If Alice wants to encode classical information in bits in the quantum state $|\psi\rangle$, and then send the quantum state $|\psi\rangle$ to Bob, how much information in bits can Alice send to Bob which Bob can gain by making the best possible measurements on $|\psi\rangle$?

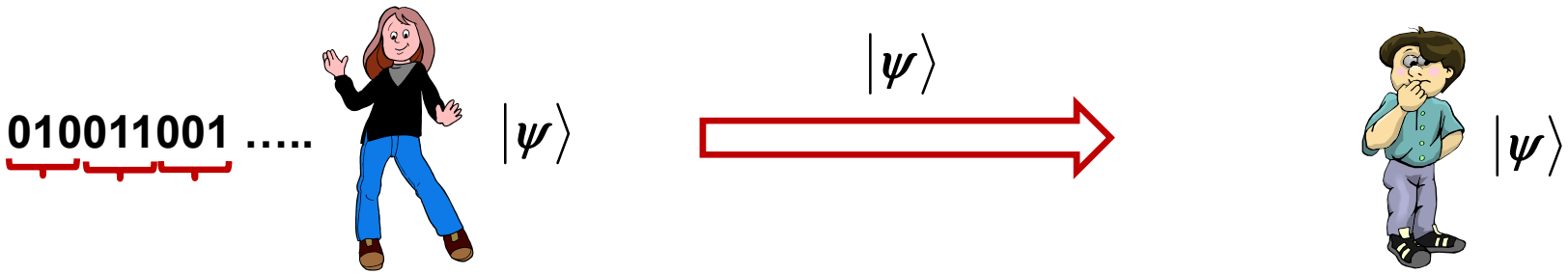
01001100 …..

$|\psi\rangle$

$|\psi\rangle$

$|\psi\rangle$

Classical Information in Quantum States: Alice's Coding



Suppose Alice chooses the following coding scheme:

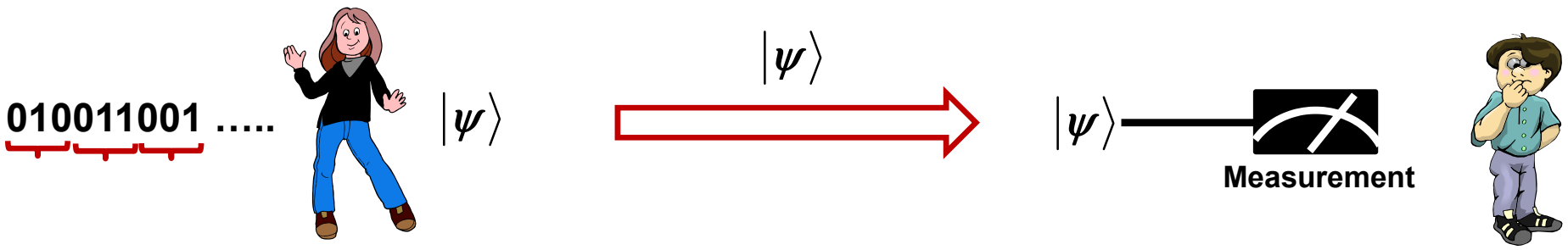
Classical Info	$\|\psi\rangle$
000	$\|e_1\rangle$
001	$\|e_2\rangle$
010	$\|e_3\rangle$
011	$\|e_4\rangle$
100	$\|e_5\rangle$
101	$\|e_6\rangle$
110	$\|e_7\rangle$
111	$\|e_8\rangle$

Hilbert space dimension: *N*=8

$$\sum_{j=1}^{8} |e_j\rangle\langle e_j| = \hat{1} \qquad \langle e_j | e_k \rangle = \delta_{jk}$$

Three classical bits are mapped to one of eight different states in the Hilbert space of the quantum system

Classical Information in Quantum States: Bob's Measurements



We assume that the quantum system has a CSCO and that each basis state $|e_j\rangle$ can be associated with a unique set of eigenvalues of the operators in the CSCO

So if each observable in the CSCO is measured for the quantum state $|\psi\rangle$ by Bob, then these measurements will let Bob figure out which one of the states $|e_j\rangle$ was sent by Alice

Result:

For each state $|\psi\rangle$ sent by Alice, Bob obtains 3 bits of classical information after making his measurements

Classical Info	$\|\psi\rangle$
000	$\|e_1\rangle$
001	$\|e_2\rangle$
010	$\|e_3\rangle$
011	$\|e_4\rangle$
100	$\|e_5\rangle$
101	$\|e_6\rangle$
110	$\|e_7\rangle$
111	$\|e_8\rangle$

Classical Information in Quantum States: Generalization

Consider a quantum system whose states belong to a *N*-dimensional Hilbert space with the following basis states:

$$\sum_{j=1}^{N} |e_j\rangle\langle e_j| = \hat{1} \qquad \langle e_j | e_k \rangle = \delta_{jk}$$

Any quantum state of the system can be written as: $|\psi\rangle = \sum_{j=1}^{N} a_j |e_j\rangle$

If Alice wants to encode classical information in bits in the quantum state $|\psi\rangle$, and then send the quantum state $|\psi\rangle$ to Bob, how much information in bits can Alice send to Bob which Bob can gain by making the best possible measurements on $|\psi\rangle$?

01001100 …..

$|\psi\rangle$

$|\psi\rangle$

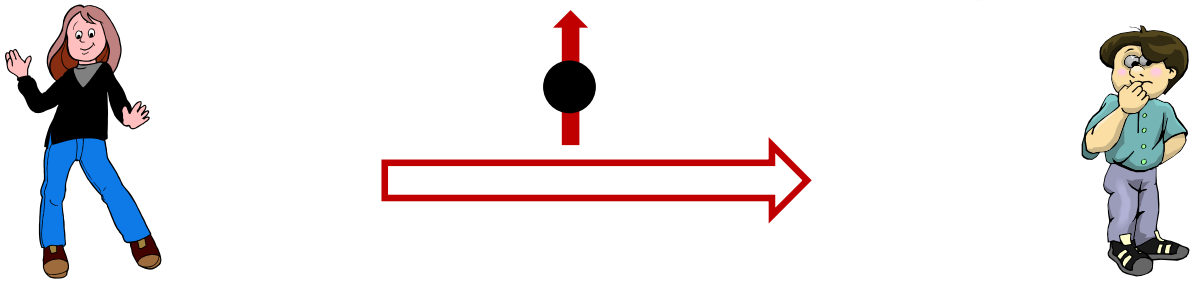
$|\psi\rangle$

Answer:

Measurements on the state $|\psi\rangle$ will give Bob $\log_2(N)$ bits of classical information

Therefore, a state in a 2-dimensional Hilbert space (i.e. a qubit) carries just one bit of classical information

Quantum Superdense Coding



Question: Can Alice send Bob more than one bit of classical information by sending just one qubit?

Quantum Superdense Coding: Alice's Local Operations

Suppose Alice and Bob, on distant planets, share an entangled qubit pair:

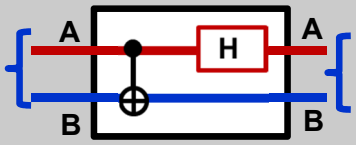
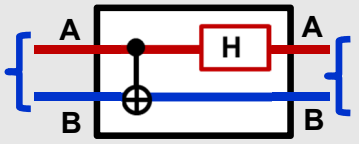
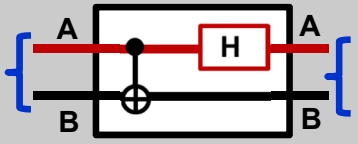
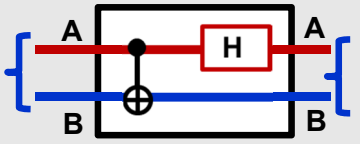
$$|S\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right]$$

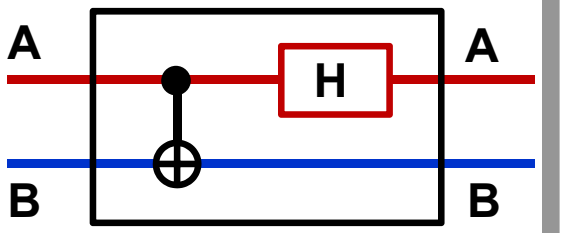
Alice's Classical Information	Alice's Local Operations
00	$\frac{1}{\sqrt{2}}\left[|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right]$ — A — $\hat{1}$ — A — $\frac{1}{\sqrt{2}}\left[|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right]$
01	$\frac{1}{\sqrt{2}}\left[|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right]$ — A — X — A — $\frac{1}{\sqrt{2}}\left[|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B\right]$
10	$\frac{1}{\sqrt{2}}\left[|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right]$ — A — Z — A — $\frac{1}{\sqrt{2}}\left[-|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right]$
11	$\frac{1}{\sqrt{2}}\left[|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right]$ — A — Y — A — $\frac{-i}{\sqrt{2}}\left[|1\rangle_A|0\rangle_B - |0\rangle_A|1\rangle_B\right]$

Quantum Superdense Coding: Bob' Local Operations

Alice then sends qubit to Bob

Bob uses a reverse Bell circuit on both the qubits

Alice's Classical Information	Bob's Local Operations
00	$\frac{1}{\sqrt{2}}\left[\|0\rangle_A\|0\rangle_B+\|1\rangle_A\|1\rangle_B\right]$  $\|0\rangle_A\|0\rangle_B$
01	$\frac{1}{\sqrt{2}}\left[\|1\rangle_A\|0\rangle_B+\|0\rangle_A\|1\rangle_B\right]$  $\|0\rangle_A\|1\rangle_B$
10	$\frac{1}{\sqrt{2}}\left[-\|0\rangle_A\|0\rangle_B+\|1\rangle_A\|1\rangle_B\right]$  $-\|1\rangle_A\|0\rangle_B$
11	$\frac{-i}{\sqrt{2}}\left[\|1\rangle_A\|0\rangle_B-\|0\rangle_A\|1\rangle_B\right]$  $i\|1\rangle_A\|1\rangle_B$

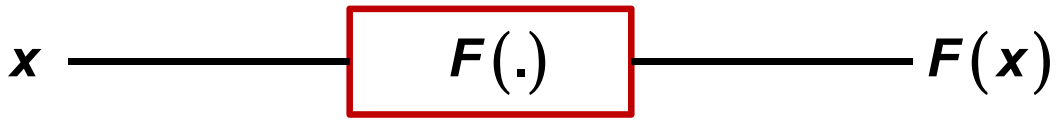


Reverse Bell Circuit

Alice is able to send two classical bits of information by sending just one qubit by using the entangled resource !!!

Quantum Parallelism and the Deutsch Algorithm

Suppose we have a classical function of one input classical bit:



There are four possibilities for the function *F*:

$F(0)=0 \quad F(1)=0$ → **Constant function**

$F(0)=0 \quad F(1)=1$ → **One-to-one function**

$F(0)=1 \quad F(1)=0$ → **One-to-one function**

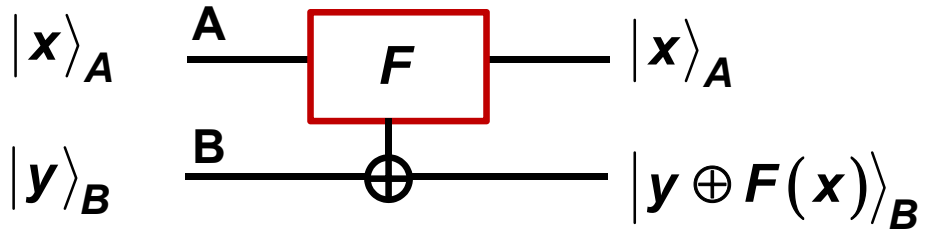
$F(0)=1 \quad F(1)=1$ → **Constant function**

Question: **Given a function black box, how many times do we need to evaluate the function *F*(.) to figure out if the function *F*(.) is a constant or a one-to-one function??**

Answer: **At least two times! Once with a "0" input and once with a "1" input.**

Quantum Parallelism and the Deutsch Algorithm

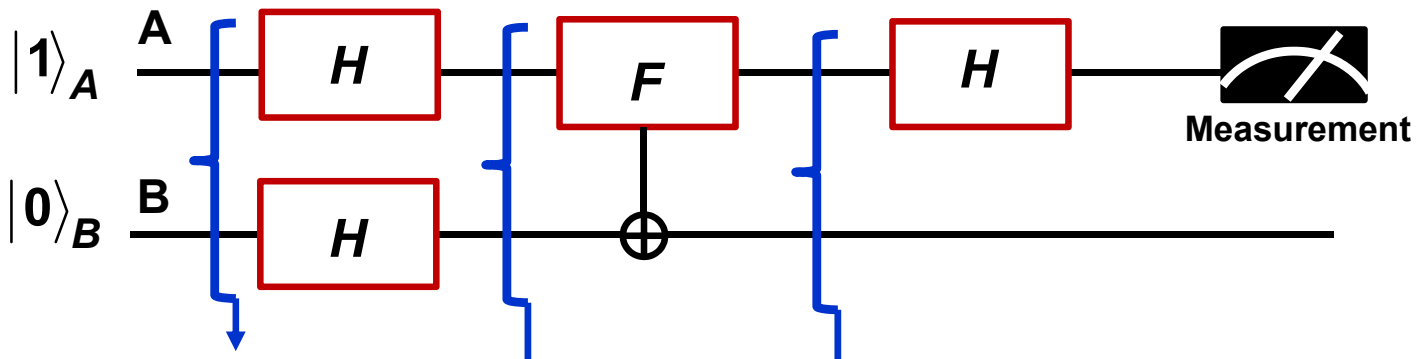
$x, y \in \{0,1\}$



Suppose we have a two-qubit unitary quantum gate that does not do anything to the A input qubit, but it changes the input B qubit such that it contains the XOR of B's original value "*y*" and the function *F*(*x*), where "*x*" is the value of A

Gate	
Input	Output
$\|0\rangle_A\|0\rangle_B$	$\|0\rangle_A\|0 \oplus F(0)\rangle_B$
$\|0\rangle_A\|1\rangle_B$	$\|0\rangle_A\|1 \oplus F(0)\rangle_B$
$\|1\rangle_A\|0\rangle_B$	$\|1\rangle_A\|0 \oplus F(1)\rangle_B$
$\|1\rangle_A\|1\rangle_B$	$\|1\rangle_A\|1 \oplus F(1)\rangle_B$

Quantum Parallelism and the Deutsch Algorithm



$$|1\rangle_A \otimes |0\rangle_B$$

$$\frac{1}{2}\left[|0\rangle_A + |1\rangle_A\right] \otimes \left[|0\rangle_B - |1\rangle_B\right]$$

$$\frac{1}{2}\left[|0\rangle_A |0 \oplus F(0)\rangle_B - |0\rangle_A |1 \oplus F(0)\rangle_B + |1\rangle_A |0 \oplus F(1)\rangle_B - |1\rangle_A |1 \oplus F(1)\rangle_B\right]$$

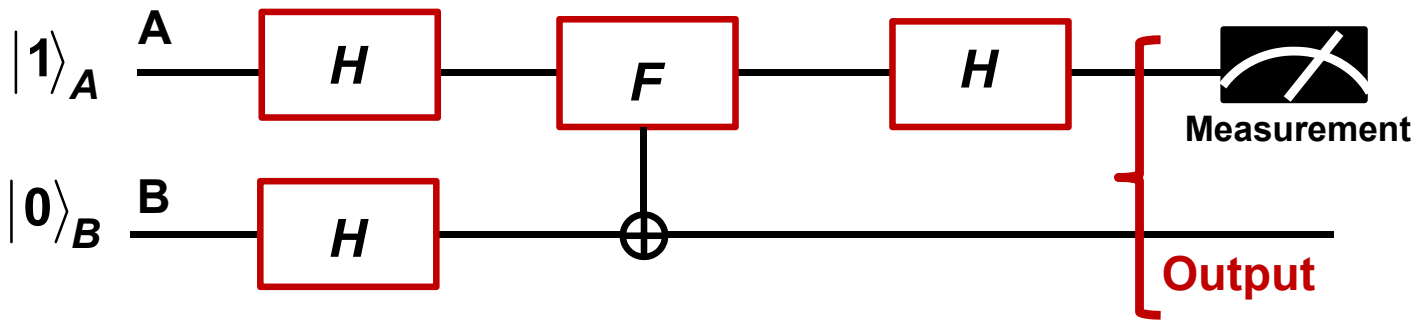
Suppose *F* is a constant then the above state is one of the following two:

$$\pm\frac{1}{2}\left[|0\rangle_A |0\rangle_B - |0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B\right]$$

Suppose *F* is a one-to-one then the above state is one of the following two:

$$\pm\frac{1}{2}\left[|0\rangle_A |0\rangle_B - |0\rangle_A |1\rangle_B + |1\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B\right]$$

Quantum Parallelism and the Deutsch Algorithm



Suppose *F* is a constant then the output is one of the following two:

$$\pm|0\rangle_A \otimes \frac{1}{\sqrt{2}}\left[|0\rangle_B - |1\rangle_B\right]$$

Suppose *F* is a one-to-one then the output is one of the following two:

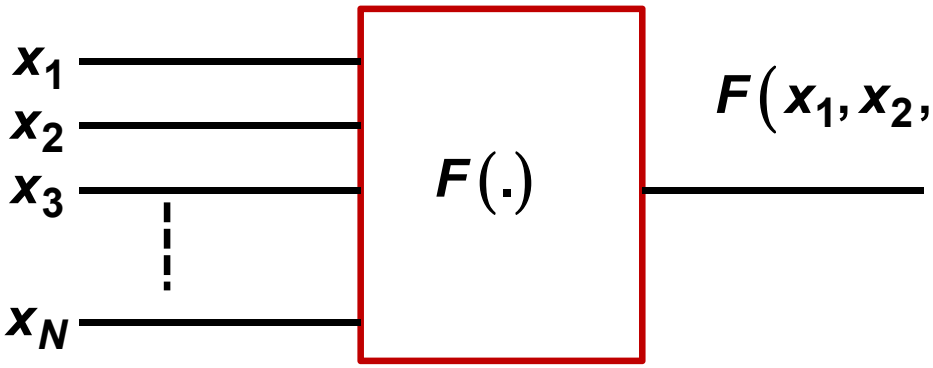
$$\pm|1\rangle_A \otimes \frac{1}{\sqrt{2}}\left[|0\rangle_B - |1\rangle_B\right]$$

Therefore, if a measurement of qubit A at the end yields "1" then *F* is one-to-one, otherwise *F* is a constant

It follows that quantum mechanics allows one to determine if a function is a constant or one-to-one using only a single evaluation of the function

Quantum Parallelism and the Bernstein-Vazirani Algorithm

Suppose we have a classical function of *N* classical input bits and one output bit:



$$F(x_1, x_2, x_3 .... x_N) = \left(\sum_{j=1}^{N} s_j x_j \right) \bmod 2$$

$$\{ s_j = 0,1$$

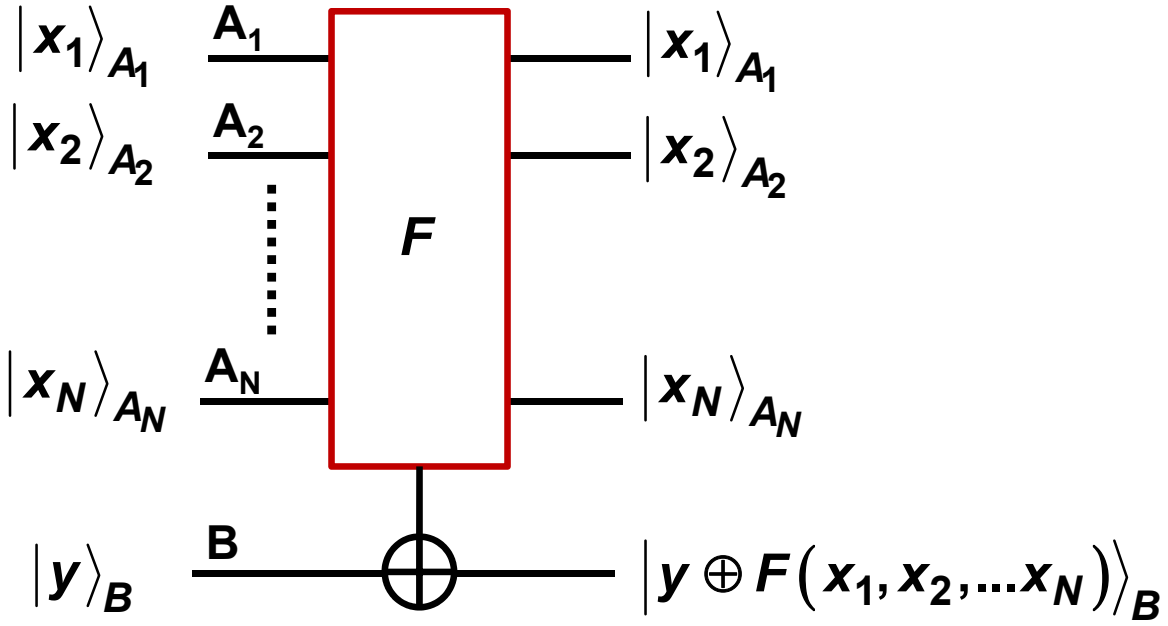
Question: Given a function black box, how many times do we need to evaluate the function *F*(.) to figure out the function (i.e. figure out the string $s_1, s_2, s_3 .... s_N$)

Answer: At least *N* times! Each time with one of the following inputs:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_N \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \quad \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_N \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \quad \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_N \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} \quad \cdots\cdots\cdots \quad \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_N \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

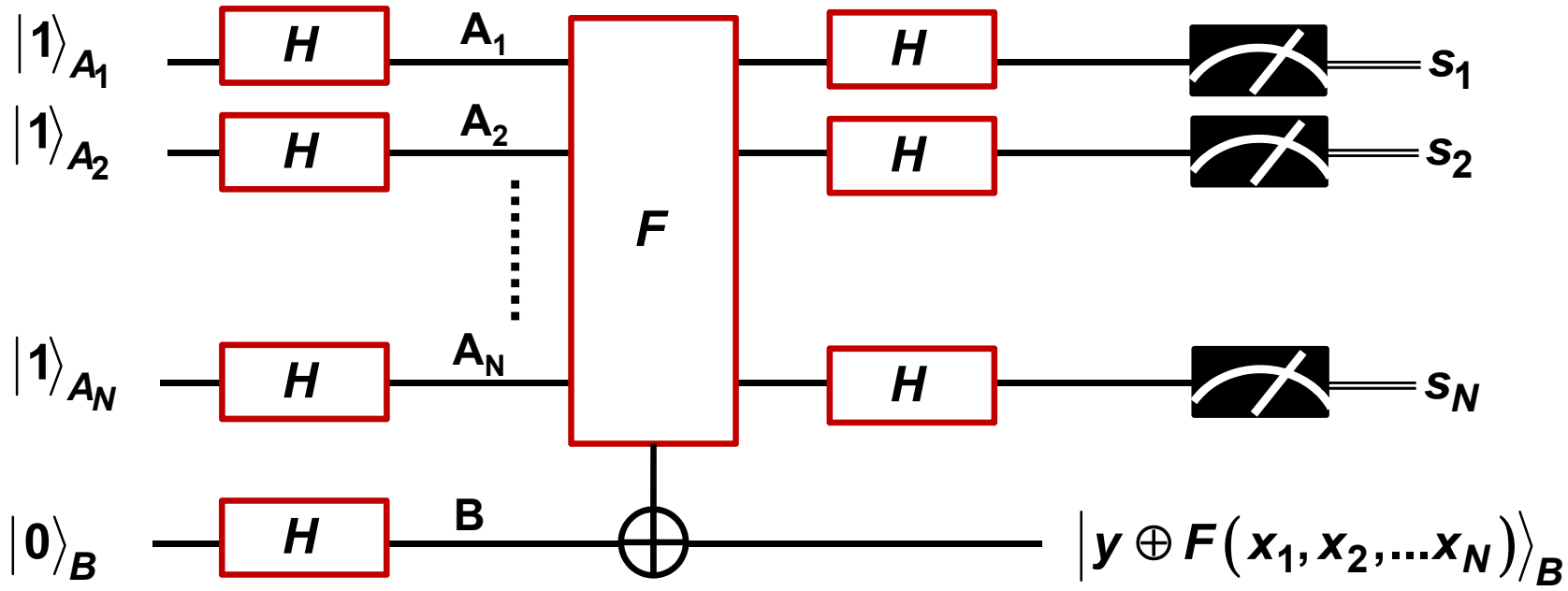
Quantum Parallelism and the Bernstein-Vazirani Algorithm

$x_j, y \in \{0,1\}$



Suppose we have a (*N*+1)-qubit unitary quantum gate that does not do anything to the input A qubits, but it changes the input B qubit such that it contains the XOR of B's original value "*y*" and the function $F(x_1, x_2, \ldots x_N)$

Quantum Parallelism and the Bernstein-Vazirani Algorithm



A measurement of all qubits A at the end yields the string $s_1, s_2, s_3 \ldots . s_N$

It follows that quantum mechanics allows one to determine the string $s_1, s_2, s_3 \ldots . s_N$ using only a single evaluation of the function !! This is *N* times faster than the best classical algorithm!