Title: PSI 2016/2017 Quantum Information (Review) - Lecture 1 (Richard Cleve)

Date: Feb 21, 2017 02:00 PM

URL: http://pirsa.org/17020112

Abstract:

Lectures for

ψ Quantum Information Course

Perimeter Institute

Richard Cleve
IQC, Waterloo
cleve@uwaterloo.ca

Basic framework of quantum information

Registers (classical case)

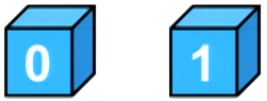
An ***n-bit register*** is an object that can contain an n-bit string

 bit (0 or 1)

 3-bit register (000, 001, 010, … or 111)

Operations on registers: **set** the state of a register
process the state of a register
read the state of a register

Can also set a register to a ***probabilistic state***



p_0 p_1

$p_0, p_1 \geq 0$

$p_0 + p_1 = 1$

 probability vector:

$$\begin{bmatrix} p_{000} \\ p_{001} \\ p_{010} \\ p_{011} \\ p_{100} \\ p_{101} \\ p_{110} \\ p_{111} \end{bmatrix}$$

Quantum registers

 qubit register

 3-qubit register

$\begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix}$ **amplitude of 0** **amplitude of 1**

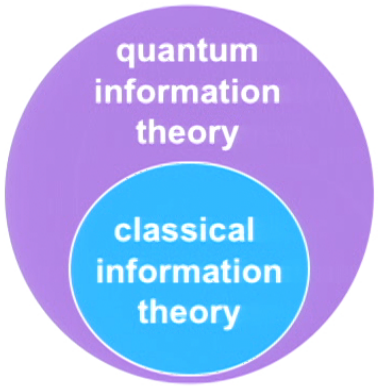
$\alpha_0, \alpha_1 \in \mathbb{C}$

$|\alpha_0|^2 + |\alpha_1|^2 = 1$

state vector: $\begin{bmatrix} \alpha_{000} \\ \alpha_{001} \\ \alpha_{010} \\ \alpha_{011} \\ \alpha_{100} \\ \alpha_{101} \\ \alpha_{110} \\ \alpha_{111} \end{bmatrix}$

The above are ***pure states***

Most general notion of a quantum state includes ***mixed states***, expressible in terms of density matrices … later



Dirac bra/ket notation

Ket: $|\psi\rangle$ always denotes a column vector, e.g. $\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_d \end{bmatrix}$

Convention: $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Bra: $\langle\psi|$ always denotes a row vector that is the conjugate transpose of $|\psi\rangle$, e.g. $[\ \alpha^*_1 \quad \alpha^*_2 \quad \ldots \quad \alpha^*_d\ ]$

Bracket: $\langle\varphi|\psi\rangle$ denotes $\langle\varphi|\cdot|\psi\rangle$, the inner product of $|\varphi\rangle$ and $|\psi\rangle$

n-qubit systems: $|000\rangle$, $|001\rangle$, $|010\rangle$, …, $|111\rangle$ are basis vectors so we can write

$$|\psi\rangle = \sum_{x=0}^{d-1} \alpha_x |x\rangle$$

Basic operations on qubits (I)

Set: a qubit register to $|0\rangle$ or to $|1\rangle$ ("computational basis" states)

Process: apply a unitary operation U (unitary means $U^\dagger U = I$)

conjugate transpose

Some examples

Rotation: $\begin{bmatrix} cos\,\theta & -sin\,\theta \\ sin\,\theta & cos\,\theta \end{bmatrix}$

NOT (bit flip): $\sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Hadamard: $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

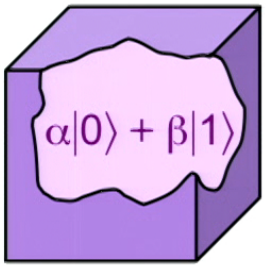
Phase flip: $\sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

$$H|0\rangle = \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle$$
$$H|1\rangle = \tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle$$

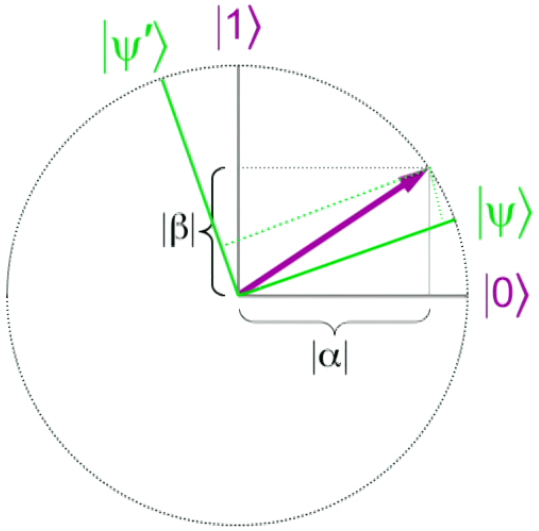
"Hadamard basis" states

Basic operations on qubits (II)

Read: apply a "standard" measurement:



$$\mapsto \begin{cases} 0 \text{ with prob } |\alpha|^2 \\ 1 \text{ with prob } |\beta|^2 \end{cases}$$



… and the quantum state collapses

*** **Note:** there exist ***other*** quantum operations, but they can all be "simulated" by the aforementioned types

Example:
measurement with respect to a different orthonormal basis $\{|\psi\rangle, |\psi'\rangle\}$

Distinguishing between two states

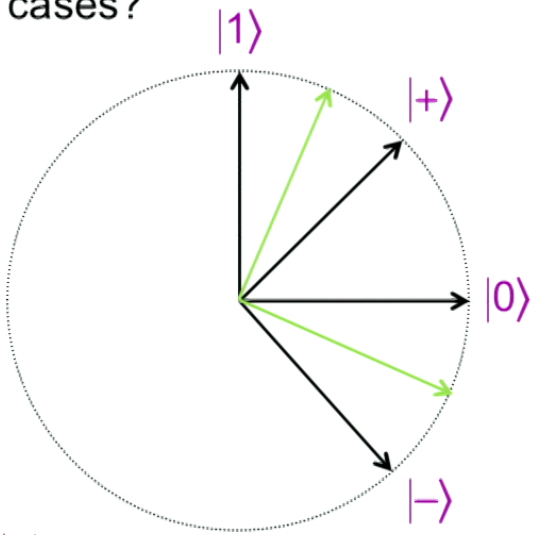
Let  be in state $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ or $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

Question 1: can we distinguish between the two cases?

Distinguishing procedure:

1. apply H
2. measure

This works because $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$



Question 2: can we distinguish between $|0\rangle$ and $|+\rangle$?

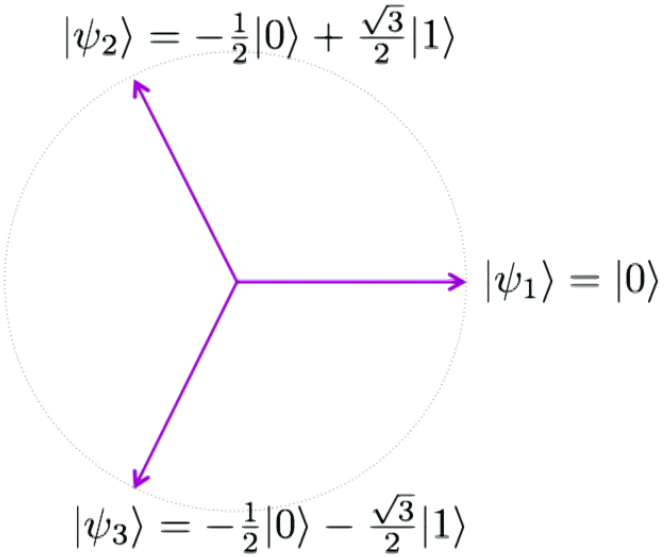
Since they're not orthogonal, they ***cannot*** be ***perfectly*** distinguished …
but what's the best possible distinguishing probability?

Distinguishing between trine states

Question 3:
what's the best distinguishing probability for the three ***trine*** states?

input: one of the three trine states
$|\psi_k\rangle$ (chosen randomly)

output: $k \in \{1, 2, 3\}$



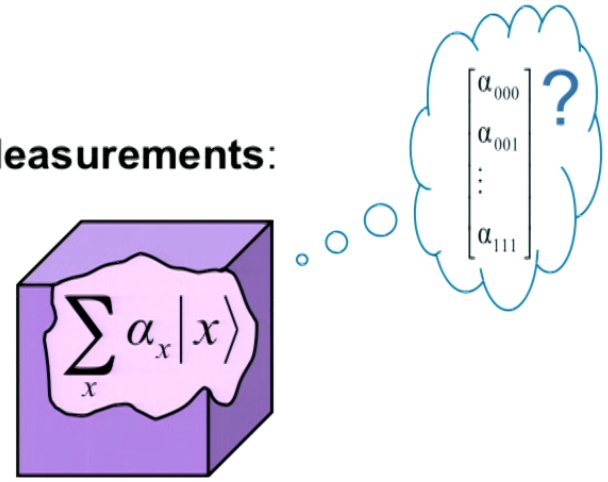
Operations on *n*-qubit states

Unitary operations:

$$\sum_x \alpha_x |x\rangle \quad \mapsto \quad U\left(\sum_x \alpha_x |x\rangle\right)$$

$$(U^\dagger U = I)$$

Measurements:



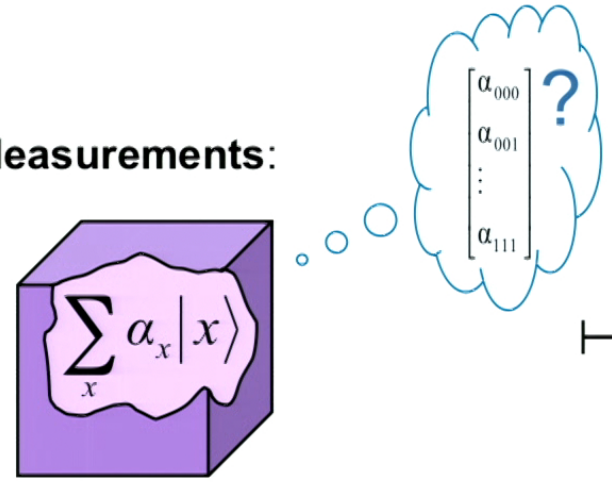
Operations on *n*-qubit states

Unitary operations:

$$\sum_x \alpha_x |x\rangle \quad \mapsto \quad U\left(\sum_x \alpha_x |x\rangle\right)$$

$(U^\dagger U = I)$

Measurements:

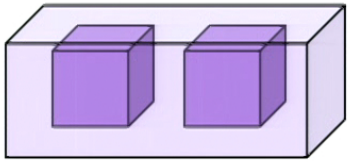


$\mapsto$

$$\begin{cases} 000 & \text{with prob } |\alpha_{000}|^2 \\ 001 & \text{with prob } |\alpha_{001}|^2 \\ \vdots & \vdots \quad \vdots \\ 111 & \text{with prob } |\alpha_{111}|^2 \end{cases}$$

… and the quantum state collapses

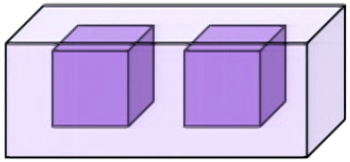
Subregisters



$$\big(\alpha|0\rangle + \beta|1\rangle\big) \otimes \big(\alpha'|0\rangle + \beta'|1\rangle\big)$$ (tensor/Kronecker product)

$$= \alpha\alpha'|00\rangle + \alpha\beta'|01\rangle + \beta\alpha'|10\rangle + \beta\beta'|11\rangle$$

Subregisters



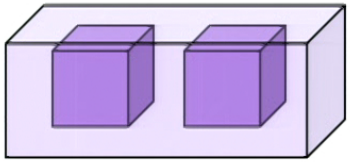
$$\big(\alpha|0\rangle + \beta|1\rangle\big) \otimes \big(\alpha'|0\rangle + \beta'|1\rangle\big)$$ (tensor/Kronecker product)

$$= \alpha\alpha'|00\rangle + \alpha\beta'|01\rangle + \beta\alpha'|10\rangle + \beta\beta'|11\rangle$$

$$\big(\quad |0\rangle + \quad |1\rangle\big) \otimes \big(\quad |0\rangle + \quad |1\rangle\big)$$

$$= \tfrac{1}{2}|00\rangle - \tfrac{1}{2}|01\rangle + \tfrac{1}{2}|10\rangle - \tfrac{1}{2}|11\rangle$$

Subregisters



$$\big(\alpha|0\rangle + \beta|1\rangle\big) \otimes \big(\alpha'|0\rangle + \beta'|1\rangle\big) \quad \text{(tensor/Kronecker product)}$$

$$= \alpha\alpha'|00\rangle + \alpha\beta'|01\rangle + \beta\alpha'|10\rangle + \beta\beta'|11\rangle$$

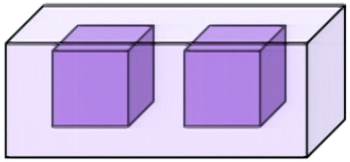
$$\big(\ |0\rangle + \ |1\rangle\big) \otimes \big(\ |0\rangle + \ |1\rangle\big)$$

$$= \tfrac{1}{2}|00\rangle - \tfrac{1}{2}|01\rangle + \tfrac{1}{2}|10\rangle - \tfrac{1}{2}|11\rangle$$

$$\big(\ |0\rangle + \ |1\rangle\big) \otimes \big(\ |0\rangle + \ |1\rangle\big)$$

$$= \tfrac{1}{2}|00\rangle + \tfrac{1}{2}|01\rangle + \tfrac{1}{2}|10\rangle - \tfrac{1}{2}|11\rangle$$

Subregisters



$$\big(\alpha|0\rangle + \beta|1\rangle\big) \otimes \big(\alpha'|0\rangle + \beta'|1\rangle\big) \quad \text{(tensor/Kronecker product)}$$

$$= \alpha\alpha'|00\rangle + \alpha\beta'|01\rangle + \beta\alpha'|10\rangle + \beta\beta'|11\rangle$$

$$\big(\ |0\rangle + \ |1\rangle\big) \otimes \big(\ |0\rangle + \ |1\rangle\big)$$

$$= \tfrac{1}{2}|00\rangle - \tfrac{1}{2}|01\rangle + \tfrac{1}{2}|10\rangle - \tfrac{1}{2}|11\rangle$$

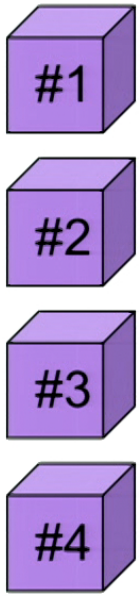
$$\big(\ |0\rangle + \ |1\rangle\big) \otimes \big(\ |0\rangle + \ |1\rangle\big)$$

$$= \tfrac{1}{2}|00\rangle + \tfrac{1}{2}|01\rangle + \tfrac{1}{2}|10\rangle - \tfrac{1}{2}|11\rangle$$

$$\big(\ |0\rangle + \ |1\rangle\big) \otimes \big(\ |0\rangle + \ |1\rangle\big) = \tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|11\rangle$$

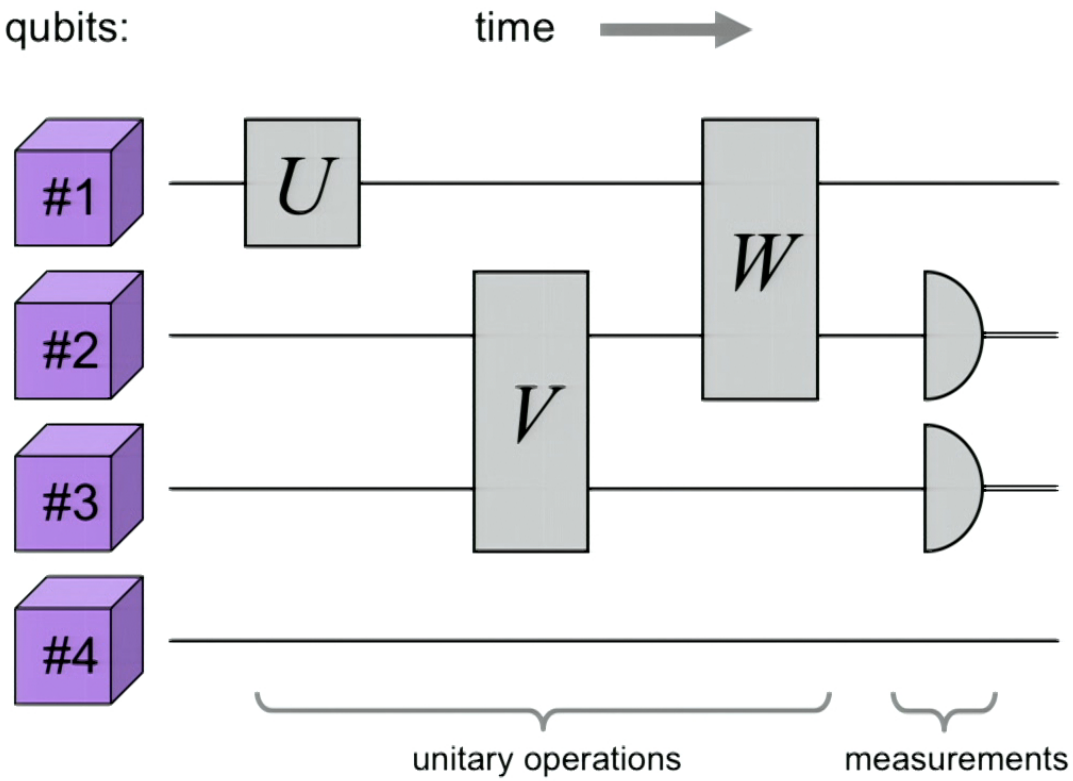
Structure among subsystems

qubits:



12

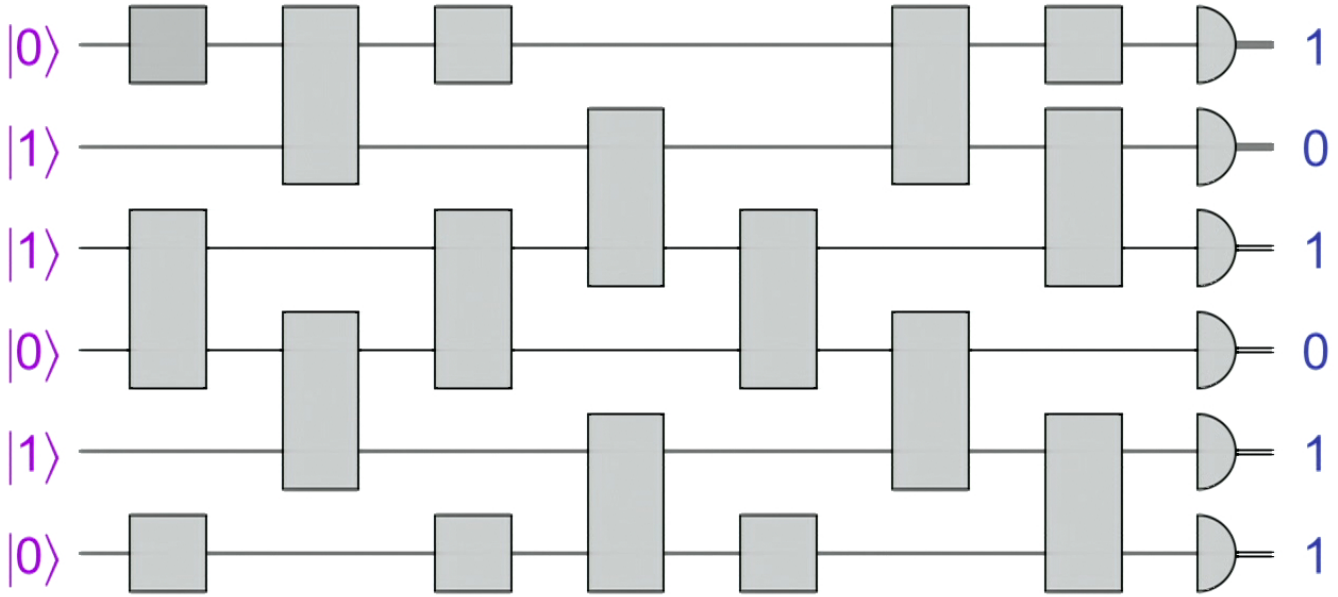
Structure among subsystems



12

Quantum computations

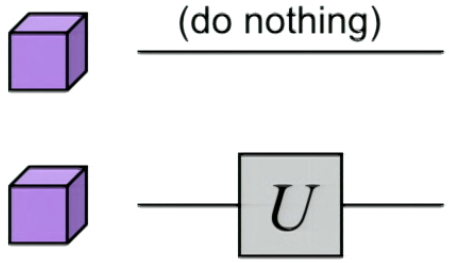
Quantum circuits:



"Feasible" if circuit-size scales polynomially

13

Example of a one-qubit gate applied to a two-qubit system



$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

Maps basis states as:

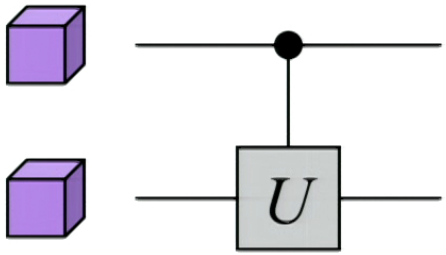
$$|0\rangle|0\rangle \rightarrow |0\rangle U|0\rangle$$
$$|0\rangle|1\rangle \rightarrow |0\rangle U|1\rangle$$
$$|1\rangle|0\rangle \rightarrow |1\rangle U|0\rangle$$
$$|1\rangle|1\rangle \rightarrow |1\rangle U|1\rangle$$

The resulting 4x4 matrix is

$$I \otimes U = \begin{bmatrix} u_{00} & u_{01} & 0 & 0 \\ u_{10} & u_{11} & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$

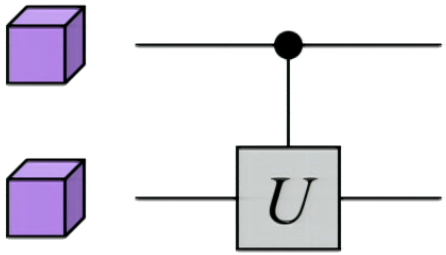
14

Controlled-U gates



$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

Controlled-U gates

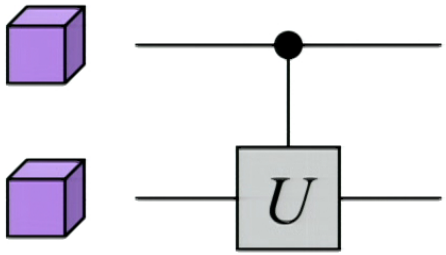


$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

Maps basis states as:

$$|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle$$
$$|0\rangle|1\rangle \rightarrow |0\rangle|1\rangle$$
$$|1\rangle|0\rangle \rightarrow |1\rangle U|0\rangle$$
$$|1\rangle|1\rangle \rightarrow |1\rangle U|1\rangle$$

Controlled-U gates



$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

Resulting 4x4 matrix is controlled-U =

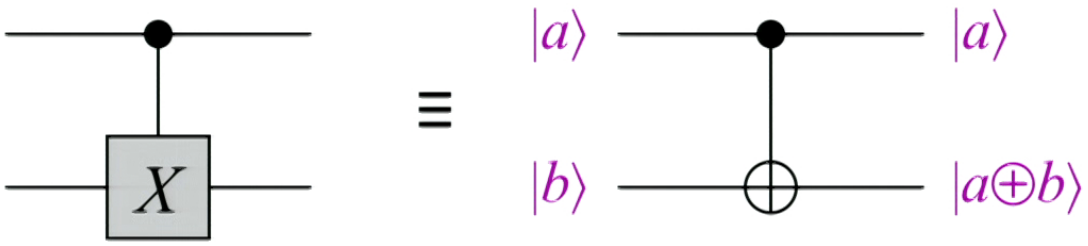
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$

Maps basis states as:

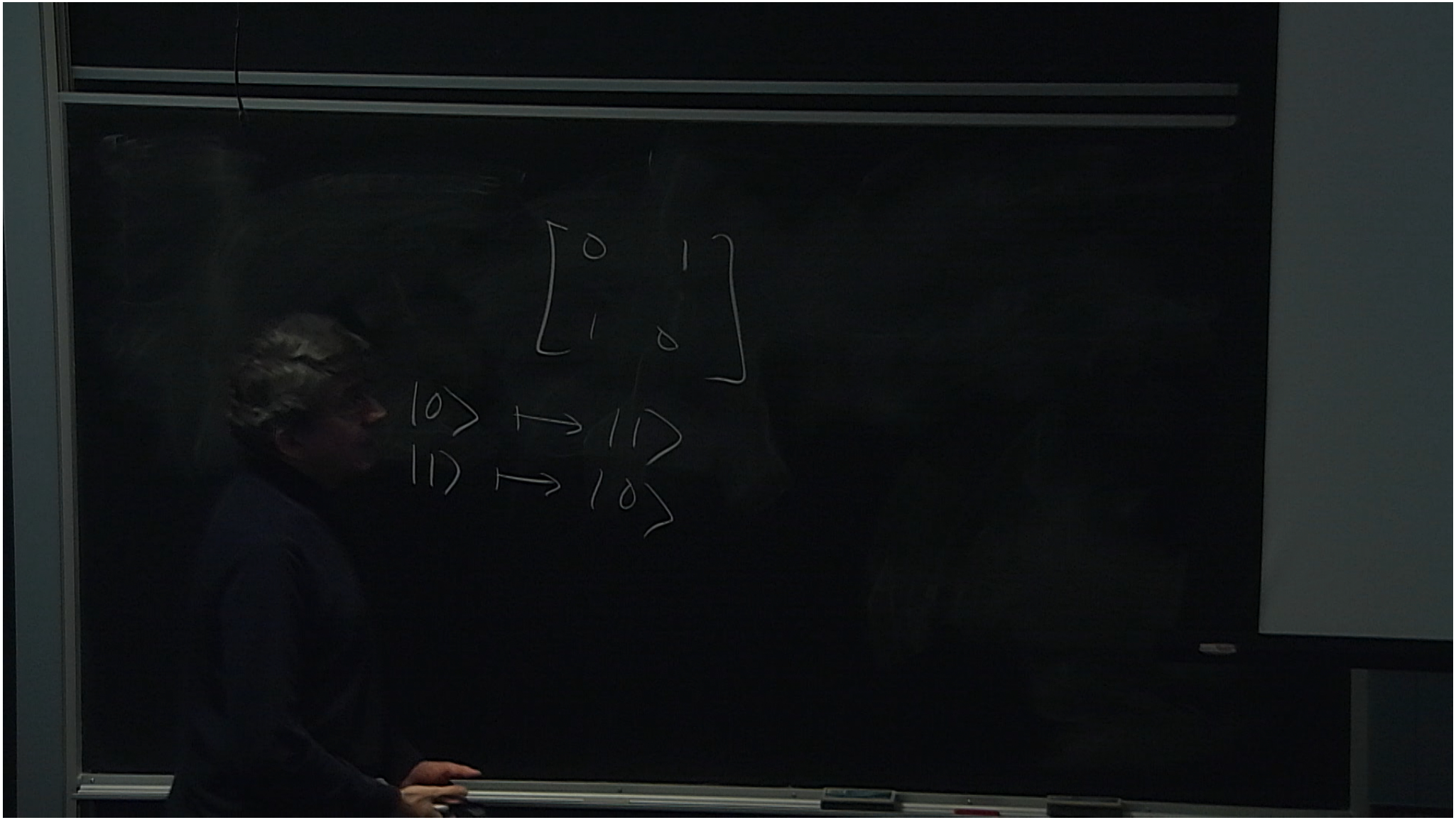
$|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle$
$|0\rangle|1\rangle \rightarrow |0\rangle|1\rangle$
$|1\rangle|0\rangle \rightarrow |1\rangle U|0\rangle$
$|1\rangle|1\rangle \rightarrow |1\rangle U|1\rangle$

15

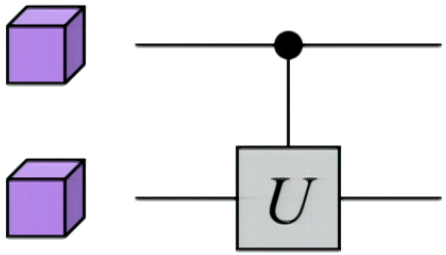
Controlled-NOT (CNOT)



16


$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
$|0\rangle \mapsto |1\rangle$
$|1\rangle \mapsto |0\rangle$

Controlled-U gates



$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

Resulting 4x4 matrix is controlled-U =

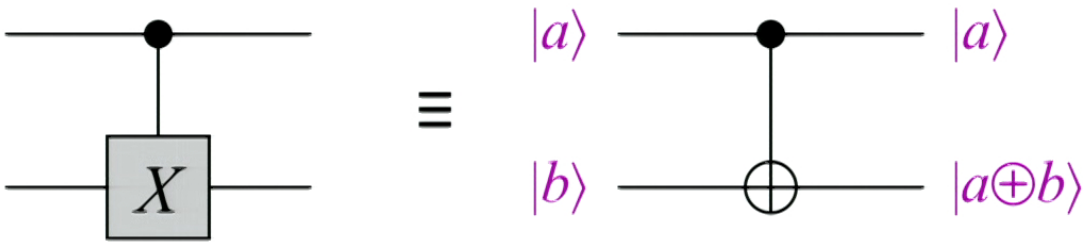
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$$

Maps basis states as:

$|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle$
$|0\rangle|1\rangle \rightarrow |0\rangle|1\rangle$
$|1\rangle|0\rangle \rightarrow |1\rangle U|0\rangle$
$|1\rangle|1\rangle \rightarrow |1\rangle U|1\rangle$

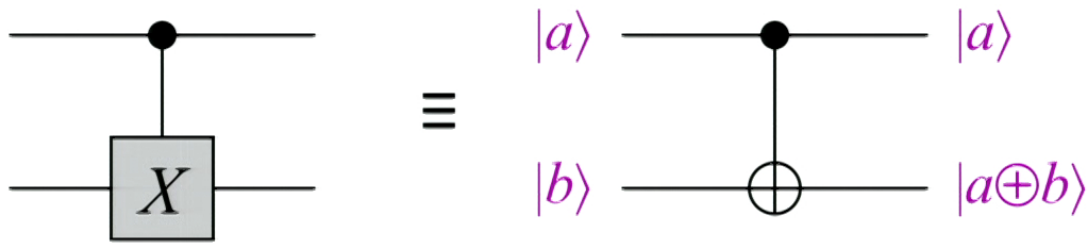
15

Controlled-NOT (CNOT)

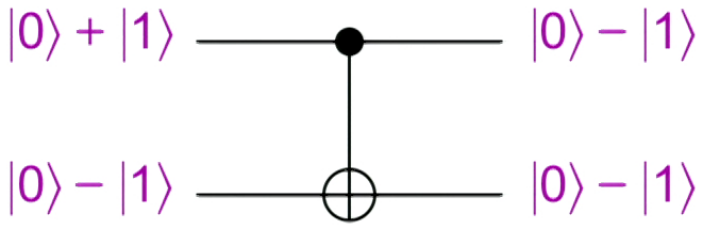


16

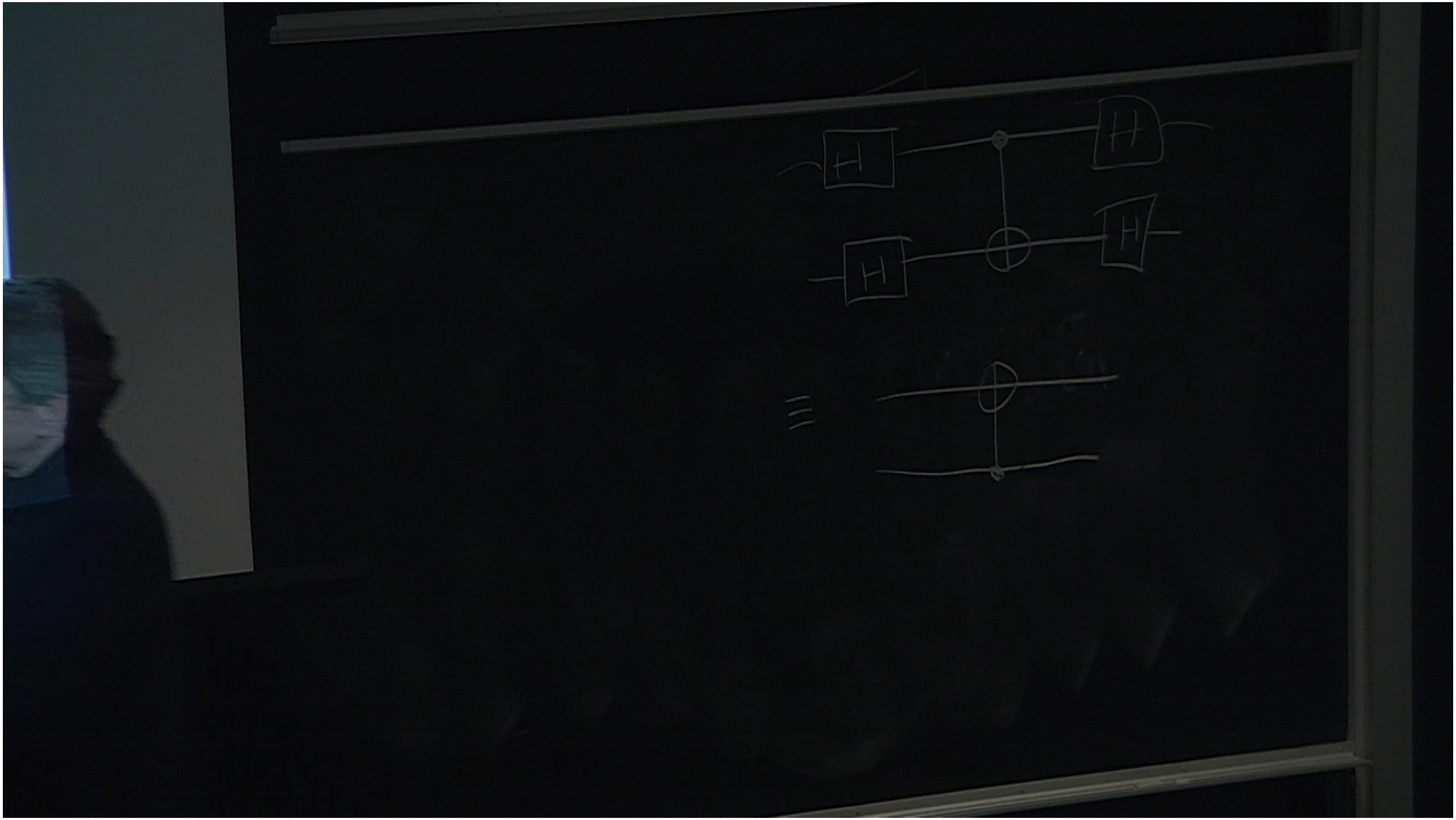
Controlled-NOT (CNOT)



Note: "control" qubit may change on some input states



16


H
H
H
H
≡

Superdense coding

How much classical information in n qubits?

$2^n - 1$ complex numbers apparently needed to describe an arbitrary n-qubit pure quantum state:

$\alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \ldots + \alpha_{111}|111\rangle$

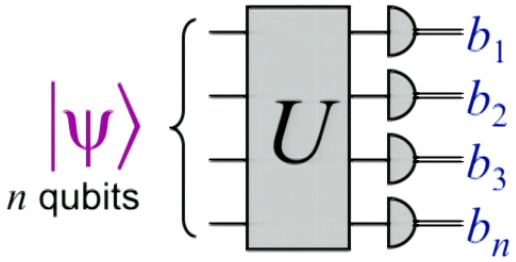
Does this mean that an exponential amount of classical information is somehow "stored" in n qubits?

Not in a direct operational sense ...

For example, ***Holevo's Theorem*** (from 1973) implies: one cannot convey more than n classical bits of information in a message of n qubits

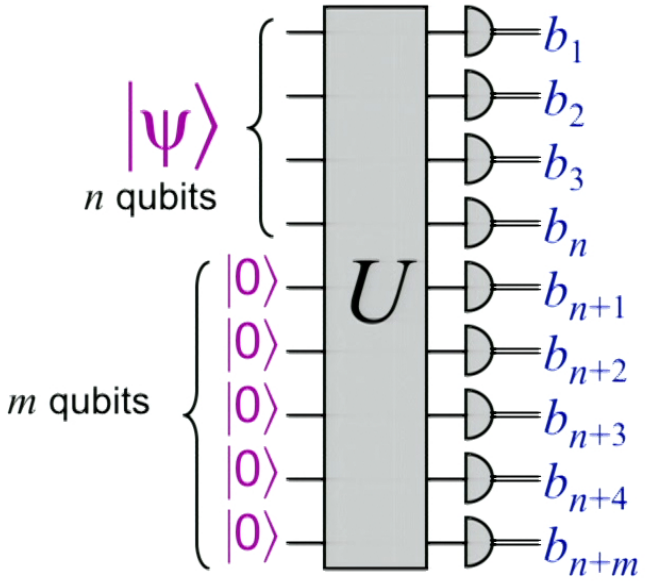
Holevo's Theorem

Easy case:



$b_1 b_2 \ldots b_n$ certainly cannot convey more than n bits!

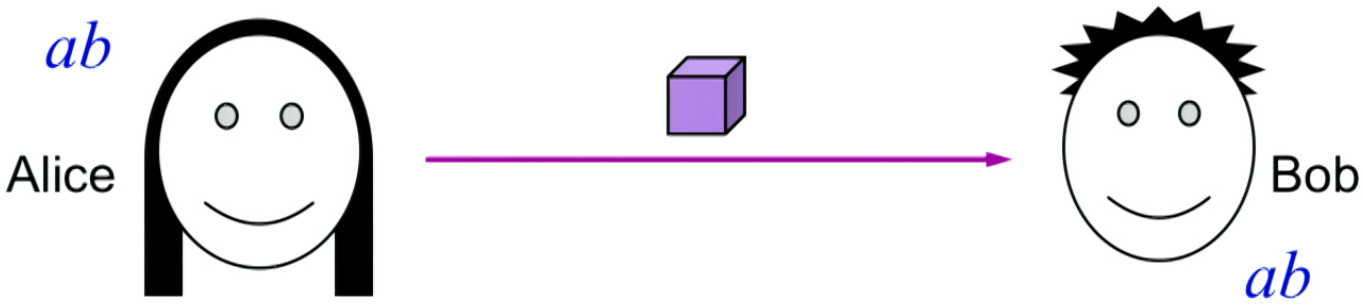
Hard case (the general case):



The proof is beyond the scope of these lectures

Superdense coding (prelude)

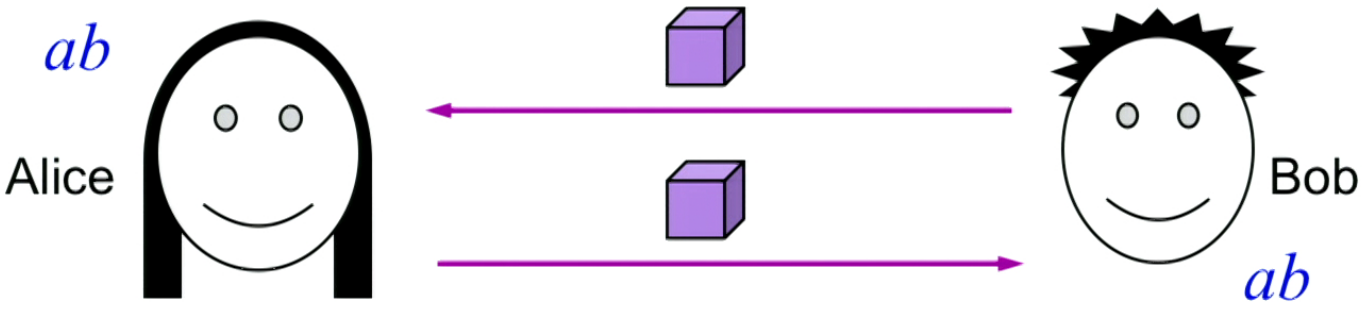
Suppose that Alice wants to convey ***two*** classical bits to Bob sending just ***one*** qubit



By Holevo's Theorem, this is ***impossible***

Superdense coding

In ***superdense coding***, Bob is allowed to send a qubit to Alice first



How can this help?

How superdense coding works

1. Bob creates the state $|00\rangle + |11\rangle$ and sends the ***first*** qubit to Alice

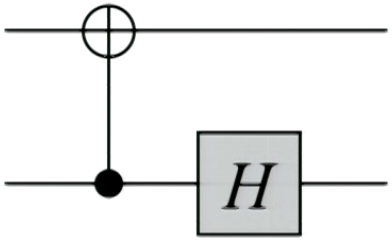
2. Alice: if $a = 1$ then apply X to qubit
   if $b = 1$ then apply Z to qubit
   send the qubit back to Bob

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

ab	state
00	$\|00\rangle + \|11\rangle$
01	$\|00\rangle - \|11\rangle$
10	$\|01\rangle + \|10\rangle$
11	$\|01\rangle - \|10\rangle$

Measurement in the Bell basis

Specifically, Bob applies



input	output
$\|00\rangle + \|11\rangle$	$\|00\rangle$
$\|01\rangle + \|10\rangle$	$\|01\rangle$
$\|00\rangle - \|11\rangle$	$\|10\rangle$
$\|01\rangle - \|10\rangle$	$-\|11\rangle$

to his two qubits ...

and then measures them, yielding ab

This concludes superdense coding

Incomplete measurements

Recap

- ***n*-qubit quantum state:** 2^n-dimensional unit vector

- **Unitary op:** $2^n \times 2^n$ linear operation U such that $U^\dagger U = I$ (where $U^\dagger$ denotes the conjugate transpose of U)

$U|0000\rangle$ = the 1st column of U

$U|0001\rangle$ = the 2nd column of U

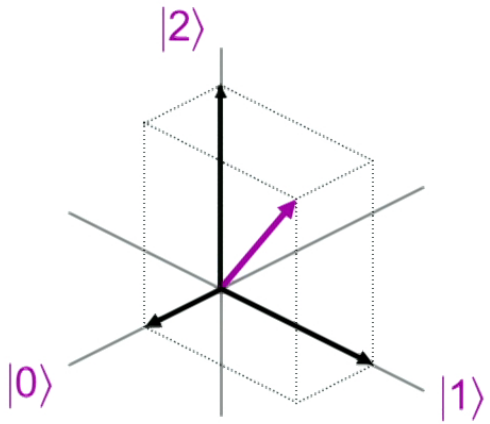
: : : : : :

$U|1111\rangle$ = the $(2^n)^{th}$ column of U

} the columns of U are orthonormal

Incomplete measurements (I)

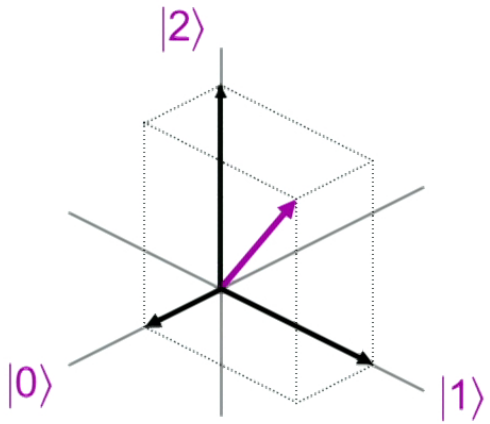
Measurements up until now are with respect to orthogonal one-dimensional subspaces:



(qutrit)

Incomplete measurements (I)

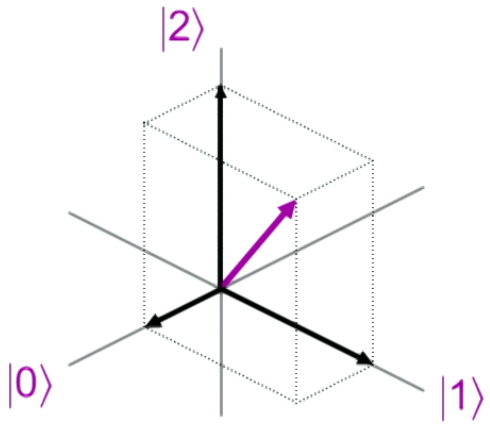
Measurements up until now are with respect to orthogonal one-dimensional subspaces:



(qutrit)

Incomplete measurements (I)

Measurements up until now are with respect to orthogonal one-dimensional subspaces:

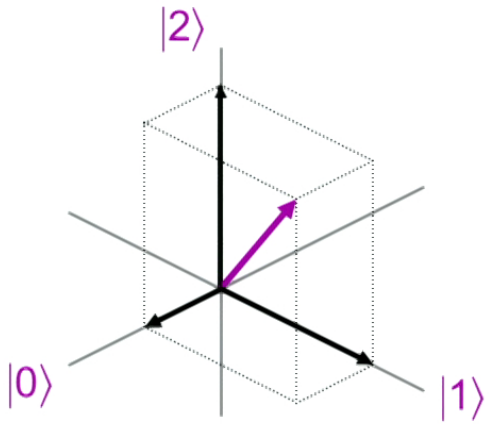


(qutrit)

The orthogonal subspaces can have other dimensions:

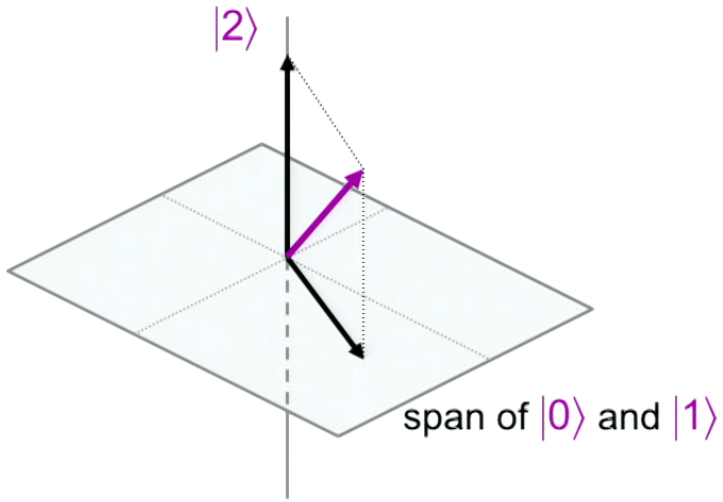
Incomplete measurements (I)

Measurements up until now are with respect to orthogonal one-dimensional subspaces:



(qutrit)

The orthogonal subspaces can have other dimensions:



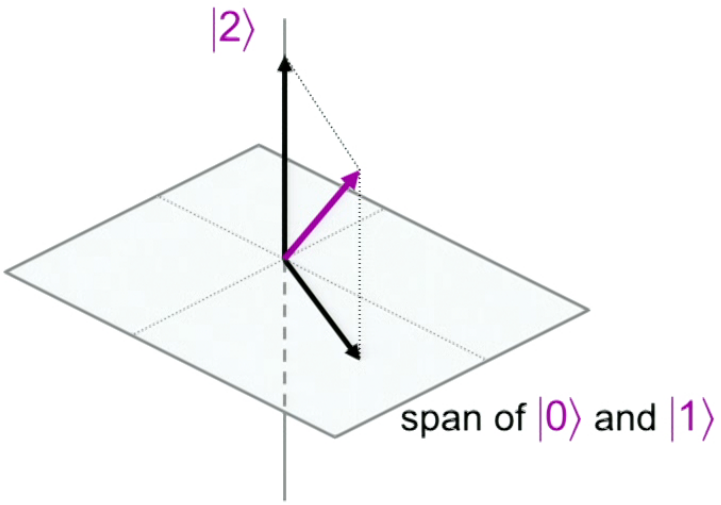
Incomplete measurements (II)

Such a measurement on $\alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle$ results in:

$$\begin{cases} \alpha_0|0\rangle + \alpha_1|1\rangle & \text{with prob } |\alpha_0|^2 + |\alpha_1|^2 \quad \text{(renormalized)} \\ \alpha_2|2\rangle & \text{with prob } |\alpha_2|^2 \quad \text{(renormalized)} \end{cases}$$

27

Incomplete measurements (II)



Such a measurement on $\alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle$ results in:

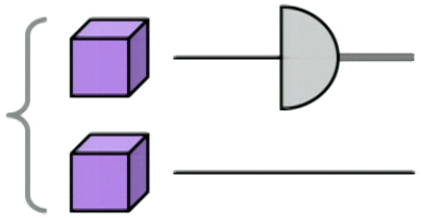
$\alpha_0|0\rangle + \alpha_1|1\rangle$ with prob $|\alpha_0|^2 + |\alpha_1|^2$ (renormalized)

$\alpha_2|2\rangle$ with prob $|\alpha_2|^2$ (renormalized)

27

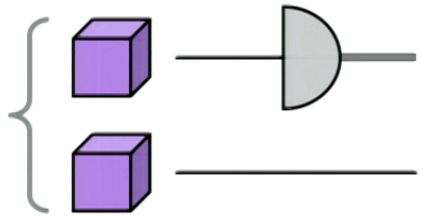
Measuring the first qubit of a two-qubit system

$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$



Measuring the first qubit of a two-qubit system

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

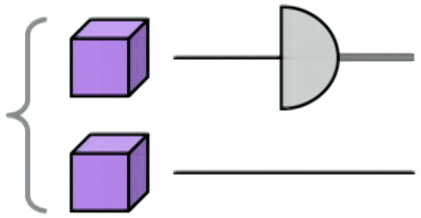


Defined as the incomplete measurement with respect to the two subspaces:

- span of $|00\rangle$ & $|01\rangle$ (all states with first qubit 0), and
- span of $|10\rangle$ & $|11\rangle$ (all states with first qubit 1)

Measuring the first qubit of a two-qubit system

$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$



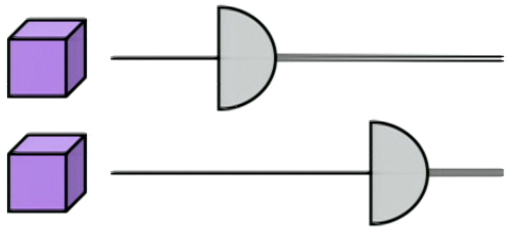
Defined as the incomplete measurement with respect to the two subspaces:

- span of $|00\rangle$ & $|01\rangle$ (all states with first qubit 0), and
- span of $|10\rangle$ & $|11\rangle$ (all states with first qubit 1)

Result is

$$\begin{cases} 0, \ \alpha_{00}|00\rangle + \alpha_{01}|01\rangle & \text{with prob } |\alpha_{00}|^2 + |\alpha_{01}|^2 \\ 1, \ \alpha_{10}|10\rangle + \alpha_{11}|11\rangle & \text{with prob } |\alpha_{10}|^2 + |\alpha_{11}|^2 \end{cases}$$

28

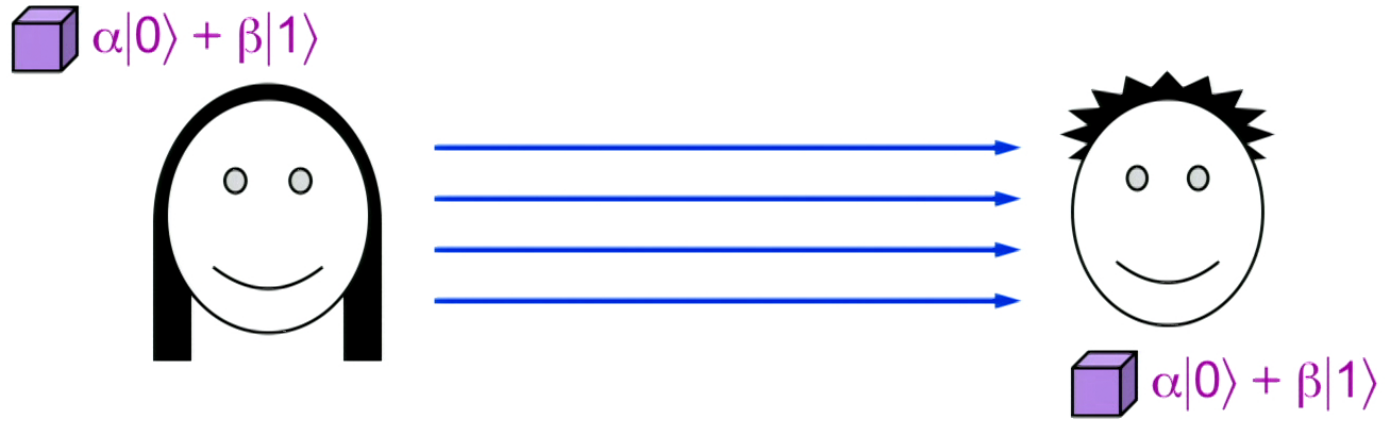


Exercise (a sanity test of the model): show that measuring the first qubit and *then* measuring the second qubit gives the same result as measuring both qubits at once

Teleportation

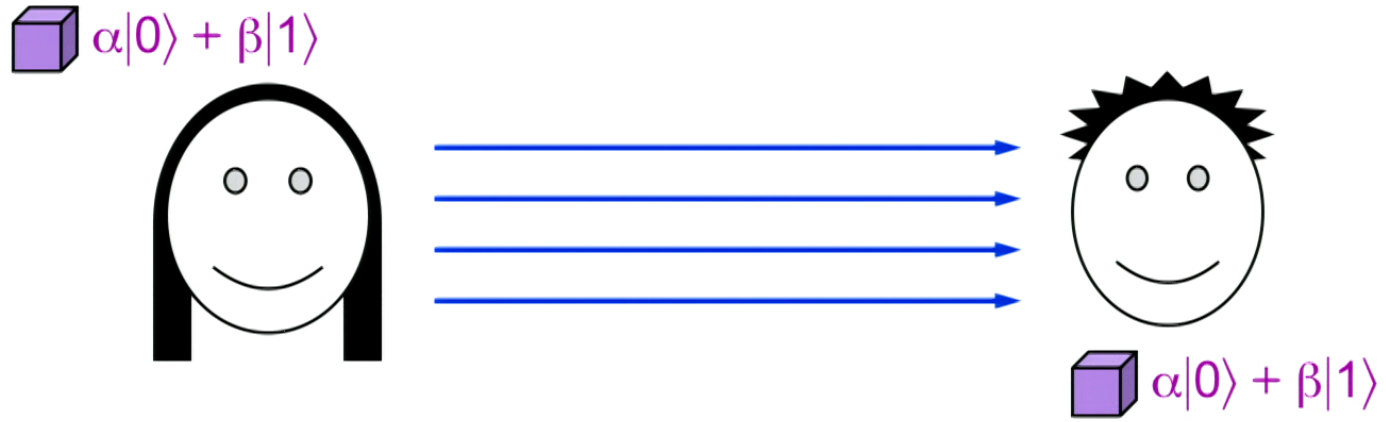
Teleportation (prelude)

Suppose Alice wishes to convey a qubit to Bob by sending just classical bits



Teleportation (prelude)

Suppose Alice wishes to convey a qubit to Bob by sending just classical bits

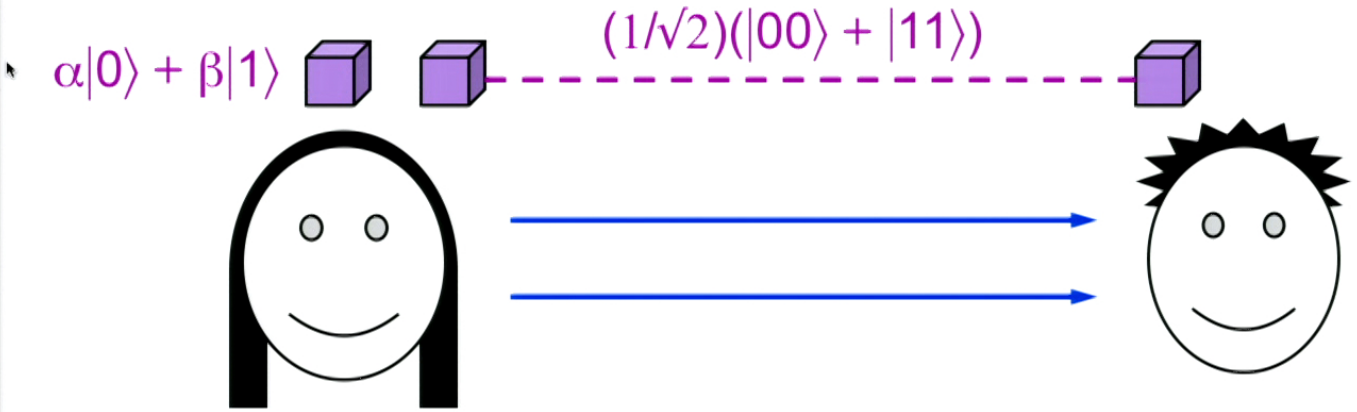


If Alice ***knows*** α and β, she can send approximations of them —but this still requires infinitely many bits for perfect precision

Moreover, if Alice does ***not*** know α or β, she can at best acquire ***one bit*** about them by a measurement

Teleportation scenario

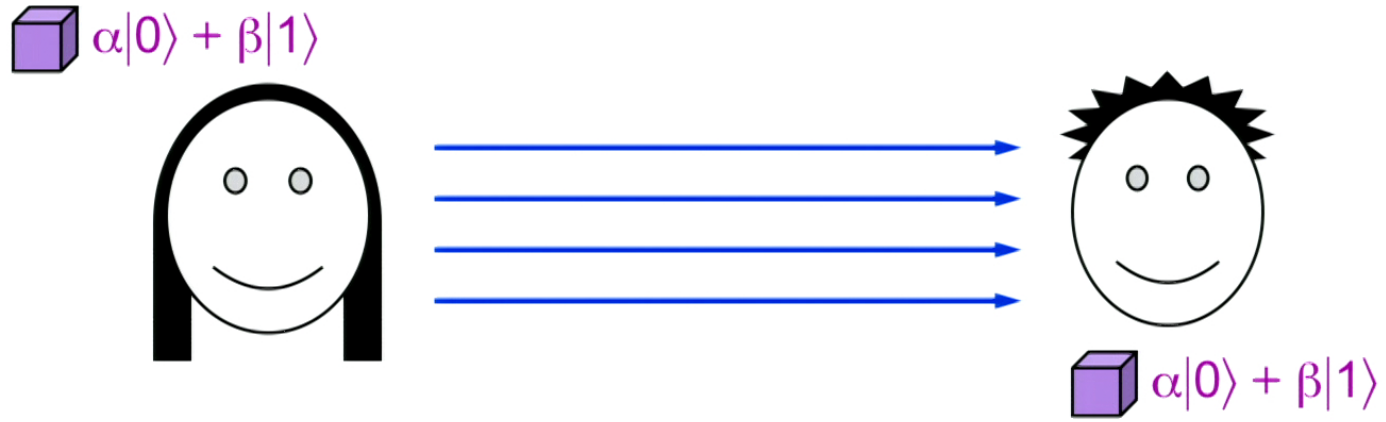
In teleportation, Alice and Bob also start with a Bell state



and Alice can send two classical bits to Bob

Teleportation (prelude)

Suppose Alice wishes to convey a qubit to Bob by sending just classical bits

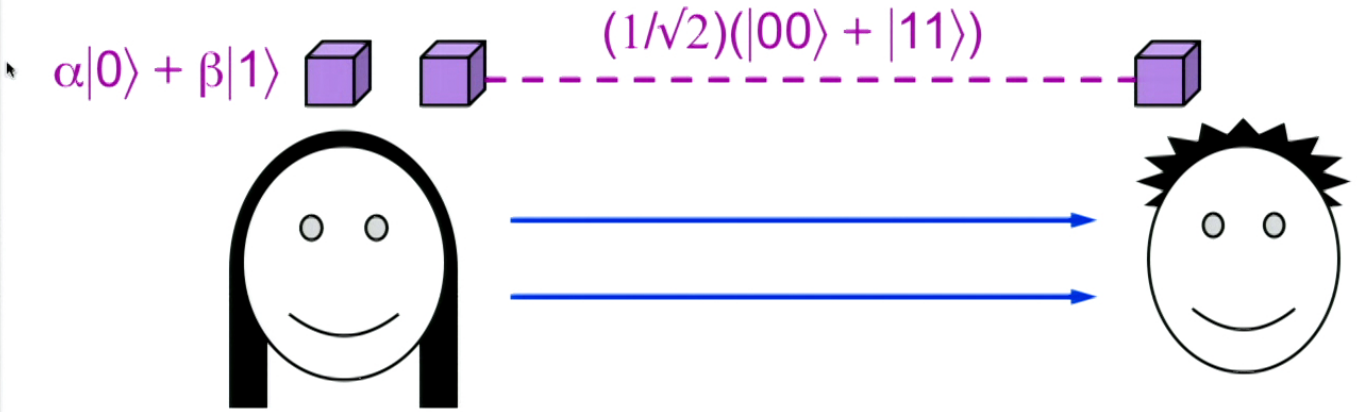


If Alice ***knows*** α and β, she can send approximations of them —but this still requires infinitely many bits for perfect precision

Moreover, if Alice does ***not*** know α or β, she can at best acquire ***one bit*** about them by a measurement

Teleportation scenario

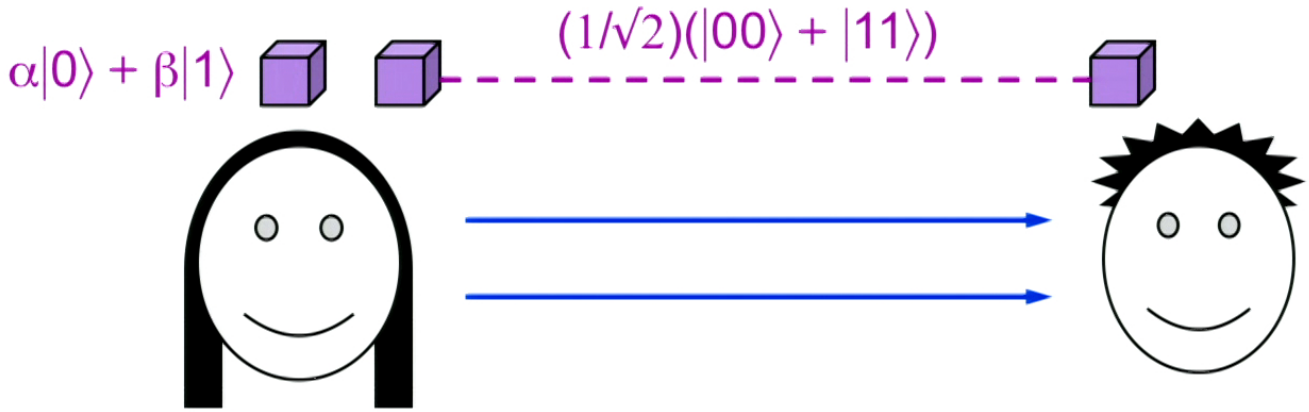
In teleportation, Alice and Bob also start with a Bell state



and Alice can send two classical bits to Bob

Teleportation scenario

In teleportation, Alice and Bob also start with a Bell state



and Alice can send two classical bits to Bob

Note that the initial state of the three qubit system is:

$(1/\sqrt{2})(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle)$

$= (1/\sqrt{2})(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$

How teleportation works

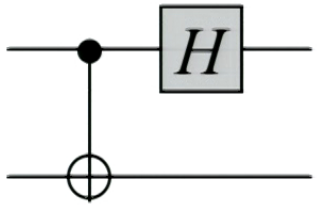
Initial state: $(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle)$ (omitting the $1/\sqrt{2}$ factor)

$= \alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle$

$= \frac{1}{2}(|00\rangle + |11\rangle)(\alpha|0\rangle + \beta|1\rangle)$
$+ \frac{1}{2}(|01\rangle + |10\rangle)(\alpha|1\rangle + \beta|0\rangle)$
$+ \frac{1}{2}(|00\rangle - |11\rangle)(\alpha|0\rangle - \beta|1\rangle)$
$+ \frac{1}{2}(|01\rangle - |10\rangle)(\alpha|1\rangle - \beta|0\rangle)$

Protocol: Alice measures her two qubits ***in the Bell basis*** and sends the result to Bob (who then "corrects" his state)

What Alice does specifically

Alice applies 

to her two qubits, yielding:

$$\begin{cases} \tfrac{1}{2}|00\rangle(\alpha|0\rangle + \beta|1\rangle) \\ +\tfrac{1}{2}|01\rangle(\alpha|1\rangle + \beta|0\rangle) \\ +\tfrac{1}{2}|10\rangle(\alpha|0\rangle - \beta|1\rangle) \\ +\tfrac{1}{2}|11\rangle(\alpha|1\rangle - \beta|0\rangle) \end{cases} \quad \begin{cases} (00, \alpha|0\rangle + \beta|1\rangle) & \text{with prob. } \tfrac{1}{4} \\ (01, \alpha|1\rangle + \beta|0\rangle) & \text{with prob. } \tfrac{1}{4} \\ (10, \alpha|0\rangle - \beta|1\rangle) & \text{with prob. } \tfrac{1}{4} \\ (11, \alpha|1\rangle - \beta|0\rangle) & \text{with prob. } \tfrac{1}{4} \end{cases}$$

Then Alice sends her two classical bits to Bob, who then adjusts his qubit to be $\alpha|0\rangle + \beta|1\rangle$ whatever case occurs

Bob's adjustment procedure

Bob receives two classical bits a, b from Alice, and:

if $b = 1$ he applies X to qubit
if $a = 1$ he applies Z to qubit

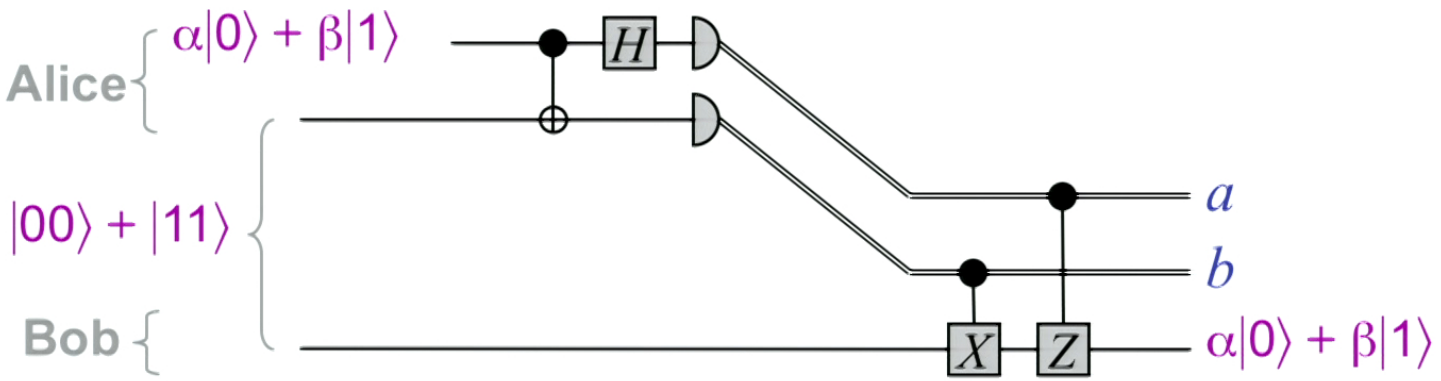
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

yielding:

$$\begin{cases} 00, & \alpha|0\rangle + \beta|1\rangle \\ 01, & X(\alpha|1\rangle + \beta|0\rangle) = \alpha|0\rangle + \beta|1\rangle \\ 10, & Z(\alpha|0\rangle - \beta|1\rangle) = \alpha|0\rangle + \beta|1\rangle \\ 11, & ZX(\alpha|1\rangle - \beta|0\rangle) = \alpha|0\rangle + \beta|1\rangle \end{cases}$$

Note that Bob acquires the correct state in each case

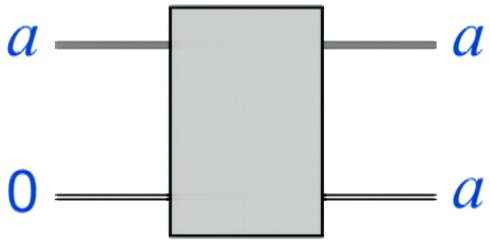
Summary of teleportation



36

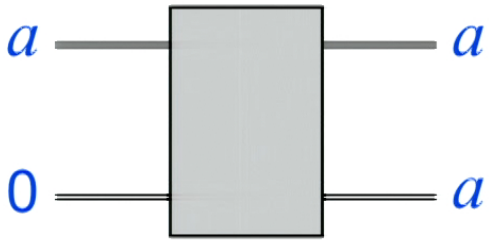
No-cloning theorem

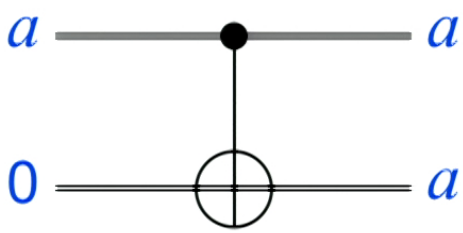
Classical information can be copied



38

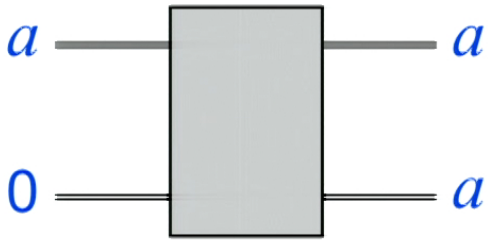
Classical information can be copied

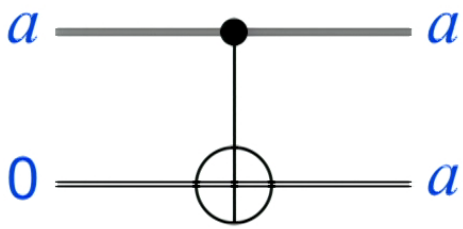




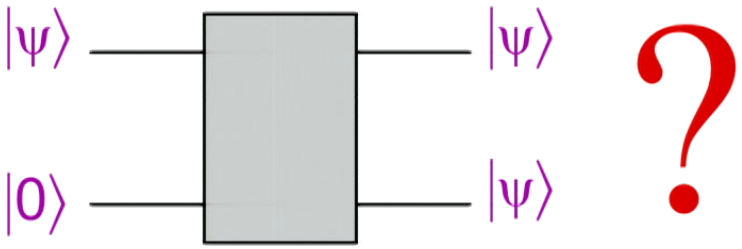
38

Classical information can be copied





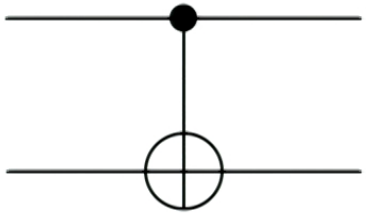
What about quantum information?



?

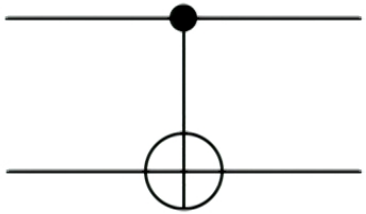
38

Candidate:



works fine for $|\psi\rangle = |0\rangle$ and $|\psi\rangle = |1\rangle$

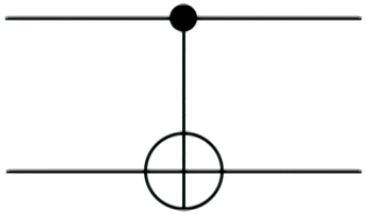
Candidate:



works fine for $|\psi\rangle = |0\rangle$ and $|\psi\rangle = |1\rangle$

... but it fails for $|\psi\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ ...

Candidate:



works fine for $|\psi\rangle = |0\rangle$ and $|\psi\rangle = |1\rangle$

... but it fails for $|\psi\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ ...

... where it yields output $(1/\sqrt{2})(|00\rangle + |11\rangle)$

instead of $|\psi\rangle|\psi\rangle = (1/4)(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

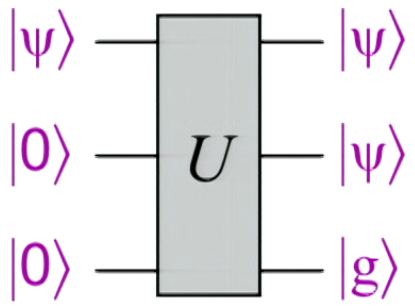
No-cloning theorem

Theorem: there is ***no*** valid quantum operation that maps an arbitrary state $|\psi\rangle$ to $|\psi\rangle|\psi\rangle$

No-cloning theorem

Theorem: there is ***no*** valid quantum operation that maps an arbitrary state $|\psi\rangle$ to $|\psi\rangle|\psi\rangle$

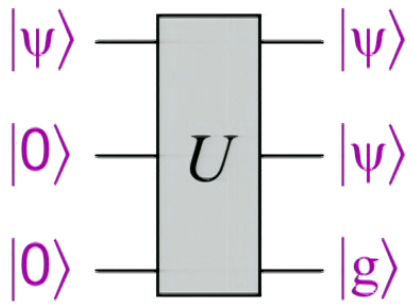
Proof:



No-cloning theorem

Theorem: there is ***no*** valid quantum operation that maps an arbitrary state $|\psi\rangle$ to $|\psi\rangle|\psi\rangle$

Proof:

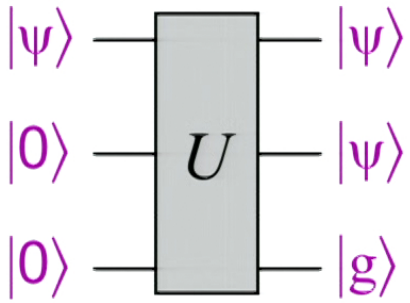


Let $|\psi\rangle$ and $|\psi'\rangle$ be two input states, yielding outputs $|\psi\rangle|\psi\rangle|g\rangle$ and $|\psi'\rangle|\psi'\rangle|g'\rangle$ respectively

No-cloning theorem

Theorem: there is ***no*** valid quantum operation that maps an arbitrary state $|\psi\rangle$ to $|\psi\rangle|\psi\rangle$

Proof:



Let $|\psi\rangle$ and $|\psi'\rangle$ be two input states, yielding outputs $|\psi\rangle|\psi\rangle|g\rangle$ and $|\psi'\rangle|\psi'\rangle|g'\rangle$ respectively

Since U preserves inner products:

$\langle\psi|\psi'\rangle = \langle\psi|\psi'\rangle\langle\psi|\psi'\rangle\langle g|g'\rangle$ so

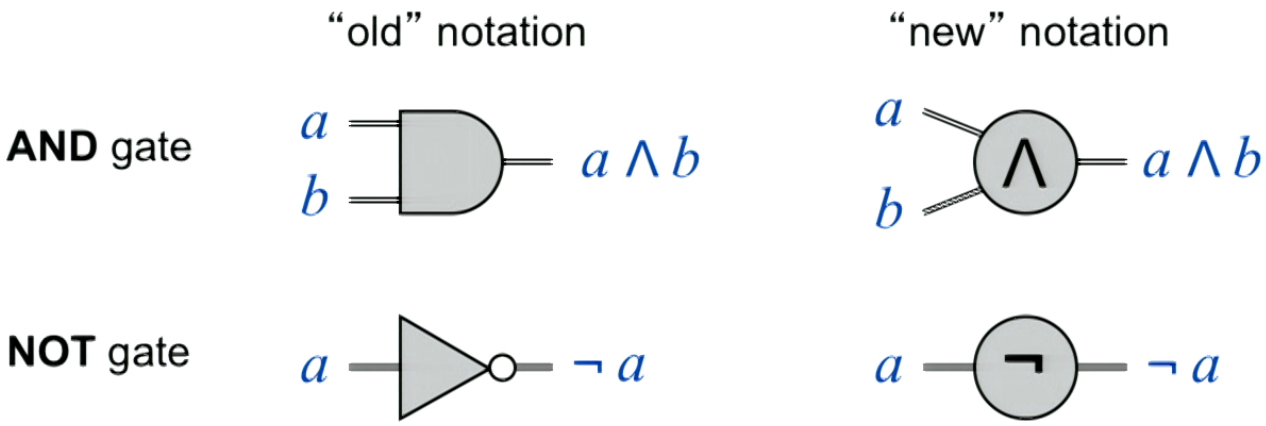
$\langle\psi|\psi'\rangle(1-\langle\psi|\psi'\rangle\langle g|g'\rangle) = 0$ so

$|\langle\psi|\psi'\rangle| = 0$ or 1

40

Classical vs. quantum circuits

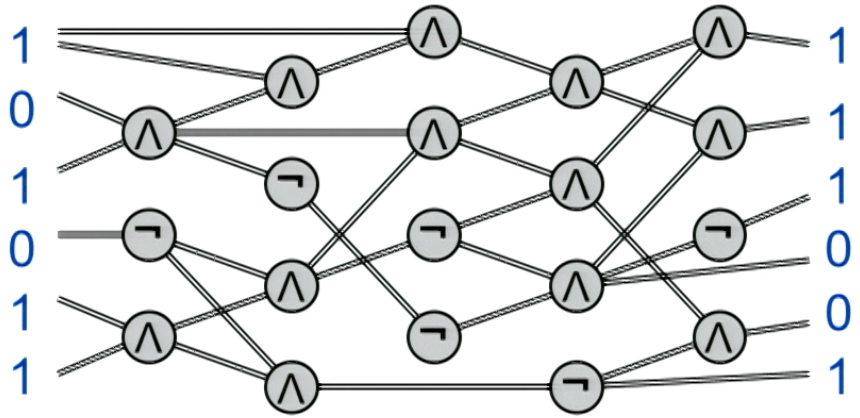
Classical (boolean logic) gates



Note: an **OR** gate can be simulated by one **AND** gate and three **NOT** gates (since $a \vee b = \neg(\neg a \wedge \neg b)$)

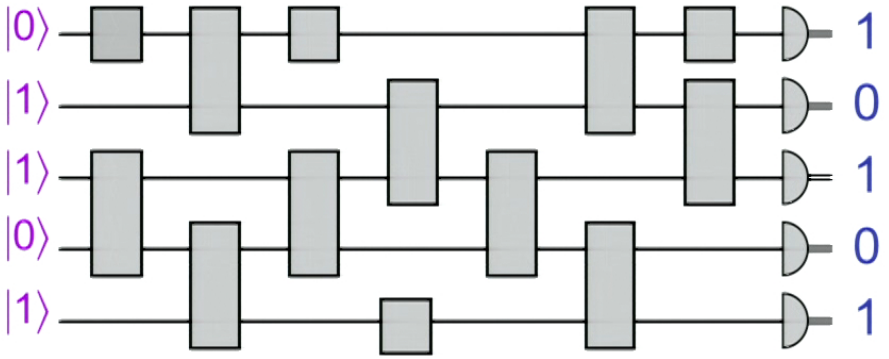
Models of computation

Classical circuits:



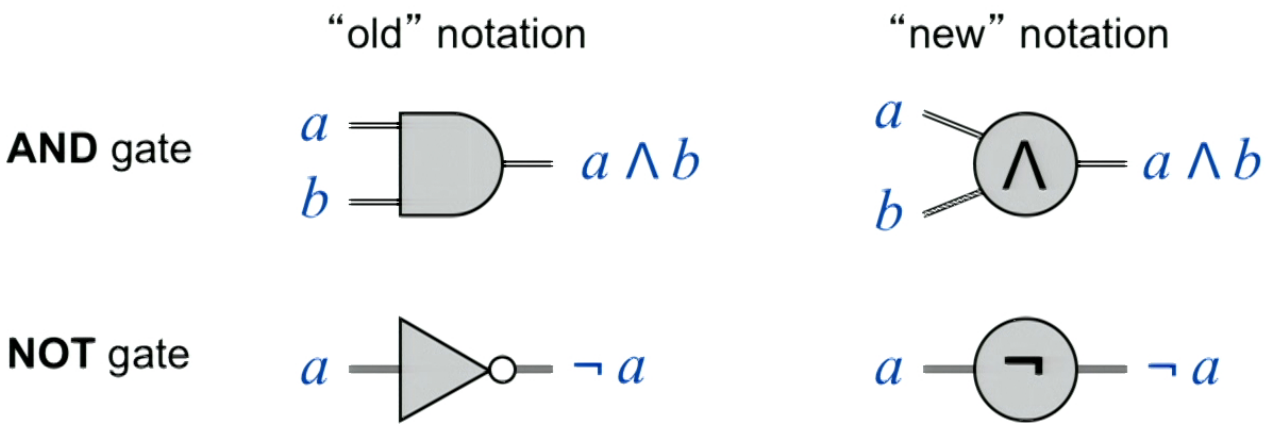
data flow →

Quantum circuits:



43

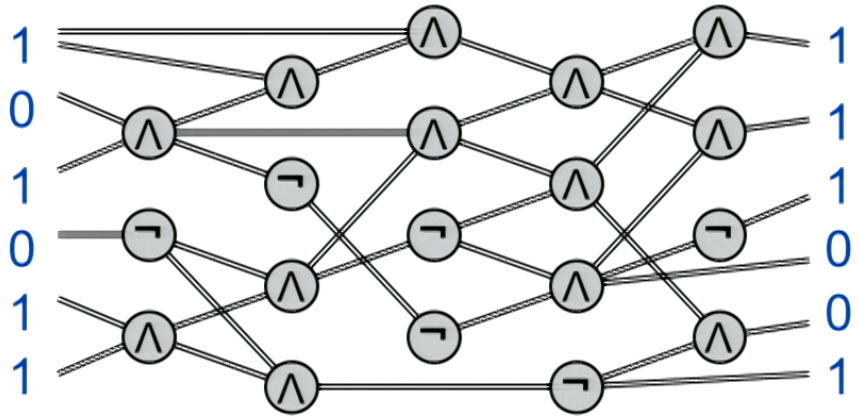
Classical (boolean logic) gates



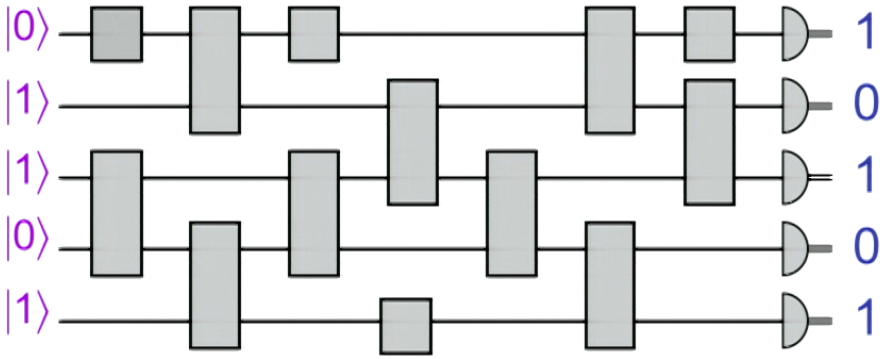
Note: an **OR** gate can be simulated by one **AND** gate and three **NOT** gates (since $a \vee b = \neg(\neg a \wedge \neg b)$)

Models of computation

Classical circuits:



Quantum circuits:



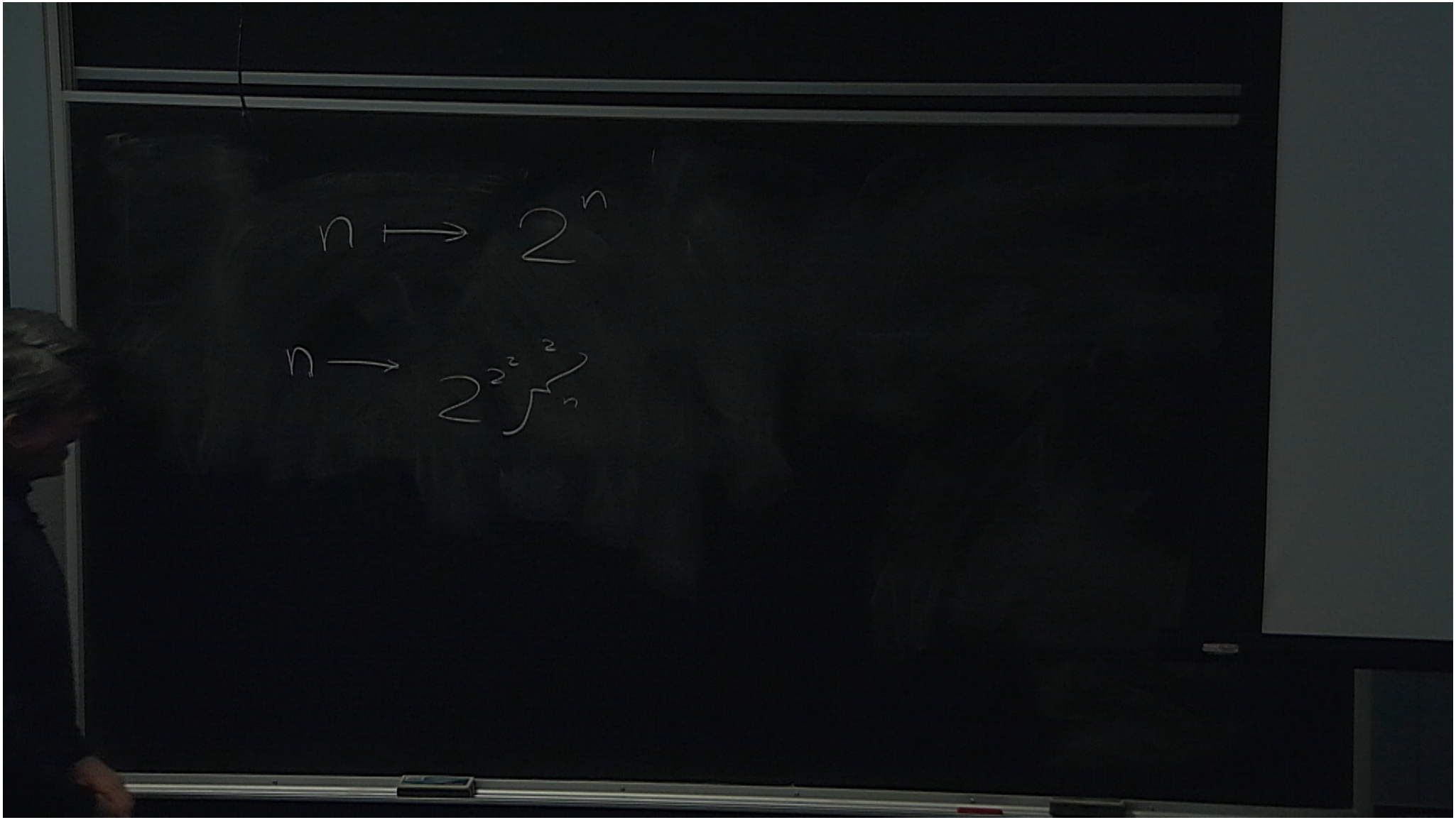
43

Multiplication problem

Input: two n-bit numbers (e.g. 101 and 111)

Output: their product (e.g. 100011)

- "Grade school" algorithm costs $O(n^2)$ [scales up *polynomially*]
- Best currently-known ***classical*** algorithm costs slightly less than $O(n \log n \ \text{loglog}\, n)$ [to be precise $O(n \log n \ 2^{\log^* n})$]
- Best currently-known ***quantum*** method: same


$n \longrightarrow 2^n$
$n \longrightarrow 2^{2^{2^{\cdots}}}$

Factoring problem

Input: an n-bit number (e.g. 100011)

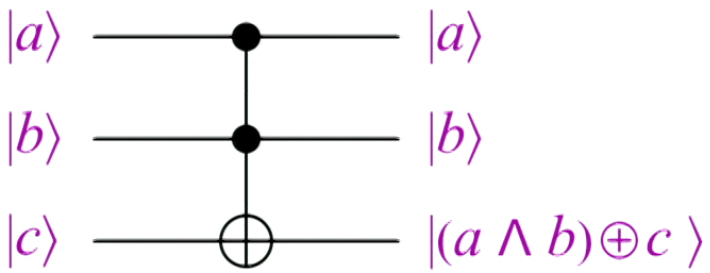
Output: their product (e.g. 101, 111)

- Trial division costs $\approx 2^{n/2}$
- Best currently-known ***classical*** algorithm costs $\approx 2^{n^{1/3}}$
  [to be more precise $2^{O(n^{1/3}\log^{2/3} n)}$ and this scaling is *not* polynomial]
- The presumed hardness of factoring is the basis of the security of many cryptosystems (e.g. RSA)
- Shors ***quantum*** algorithm costs $\approx n^2$ [less than $O(n^2 \log n \log\log n)$]
- Implementation would break RSA — and many other public-key cryptosystems

Simulating ***classical*** circuits with ***quantum*** circuits

Toffoli gate

(Sometimes called a "controlled-controlled-NOT" gate)



In the computational basis, it negates the third qubit iff the first two qubits are both $|1\rangle$

Matrix representation:

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

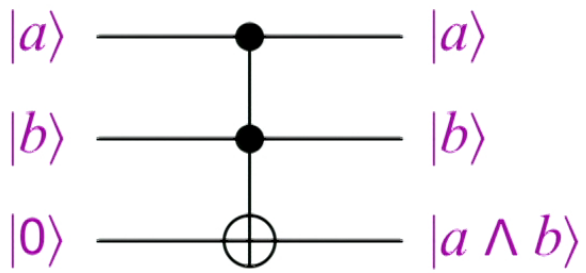
47

Quantum simulation of classical

Theorem: a classical circuit of size s can be simulated by a quantum circuit of size $O(s)$

Idea: using Toffoli gates, one can simulate:

AND gates

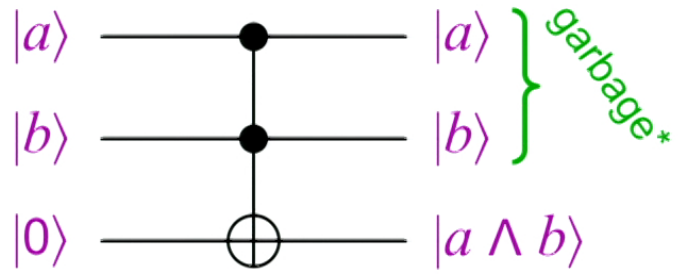


Quantum simulation of classical

Theorem: a classical circuit of size s can be simulated by a quantum circuit of size $O(s)$

Idea: using Toffoli gates, one can simulate:

AND gates



* There are mechanisms for “cleaning up” this garbage

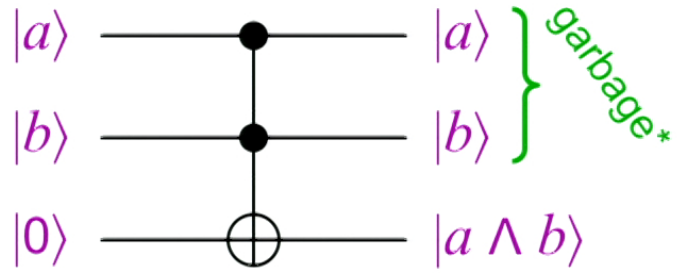
48

Quantum simulation of classical

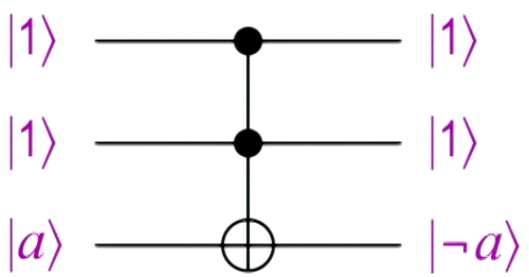
Theorem: a classical circuit of size s can be simulated by a quantum circuit of size $O(s)$

Idea: using Toffoli gates, one can simulate:

AND gates



NOT gates

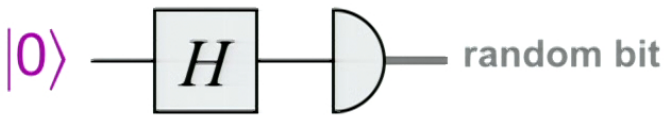


* There are mechanisms for “cleaning up” this garbage

Simulating probabilistic algorithms

Since quantum gates can simulate **AND** and **NOT**, the outstanding issue is how to simulate randomness

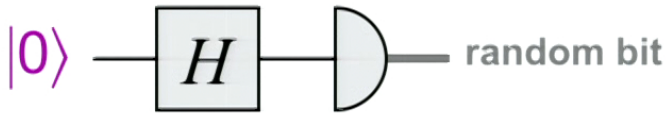
To simulate “coin flips”, one can use the circuit:



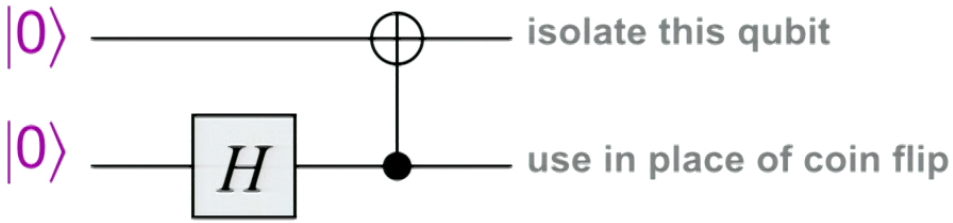
Simulating probabilistic algorithms

Since quantum gates can simulate **AND** and **NOT**, the outstanding issue is how to simulate randomness

To simulate "coin flips", one can use the circuit:



It can also be done without intermediate measurements:



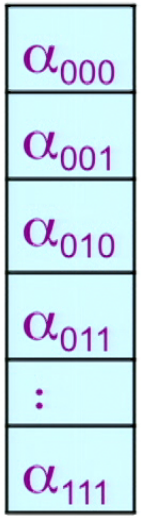
Exercise: prove that this works

Simulating ***quantum*** circuits with ***classical*** circuits

Classical simulation of quantum

Theorem: a quantum circuit of size s acting on n qubits can be simulated by a classical circuit of size $O(sn^2 2^n) = O(2^{cn})$

Idea: to simulate an n-qubit state, use an array of size 2^n containing values of all 2^n amplitudes within precision (say) 2^{-n}



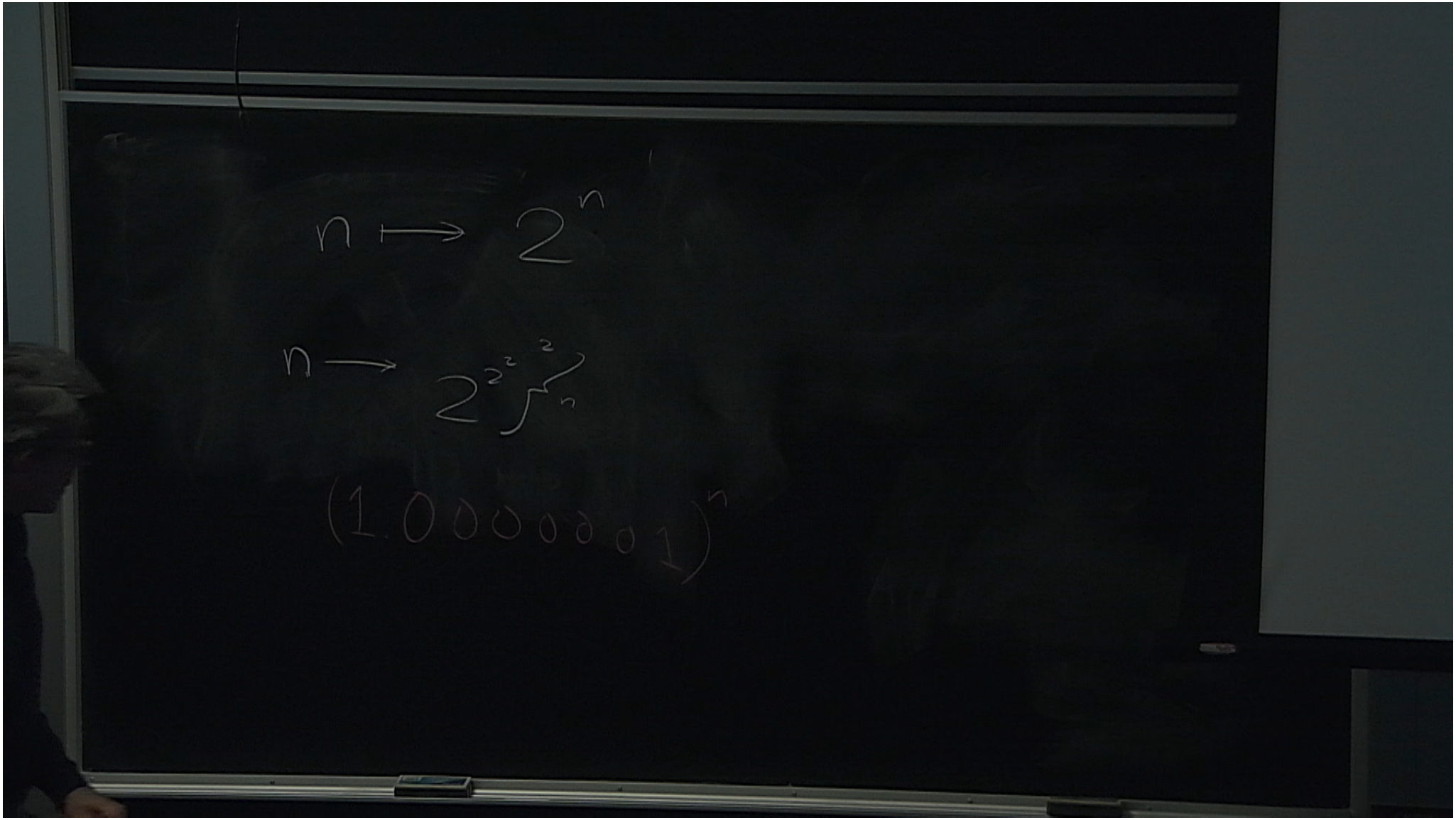
Can adjust this state vector whenever a unitary operation is performed at cost $O(n^2 2^n)$

From the final amplitudes, can determine how to set each output bit

Exercise: show how to do the simulation using only a polynomial amount of ***space*** (memory)

Some *complexity* classes

- **P (polynomial time):** the problems solved by $O(n^c)$-size classical circuits [technically, we restrict to decision problems and to "uniform circuit families"]
- **BPP (bounded error probabilistic polynomial time):** the problems solved by $O(n^c)$-size ***probabilistic*** circuits that err with probability ≤ ¼
- **BQP (bounded error quantum polynomial time):** the problems solved by $O(n^c)$-size ***quantum*** circuits that err with probability ≤ ¼
- **EXP (exponential time):**
  the problems solved by $O(2^{n^c})$-size circuits

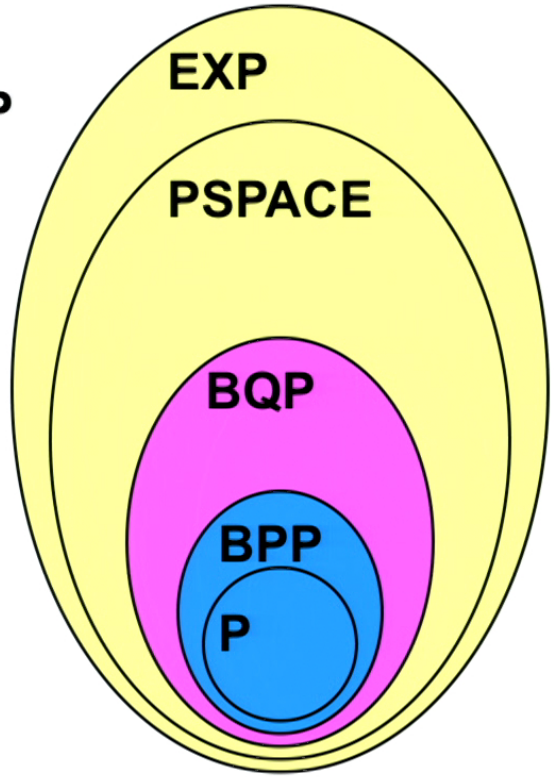

$n \longmapsto 2^n$
$n \longrightarrow 2^{2^{2^{\cdot^{\cdot^{\cdot}}}}}$ n
$(1.0000001)^n$

Some *complexity* classes

- **P (polynomial time):** the problems solved by $O(n^c)$-size classical circuits [technically, we restrict to decision problems and to "uniform circuit families"]
- **BPP (bounded error probabilistic polynomial time):** the problems solved by $O(n^c)$-size ***probabilistic*** circuits that err with probability ≤ ¼
- **BQP (bounded error quantum polynomial time):** the problems solved by $O(n^c)$-size ***quantum*** circuits that err with probability ≤ ¼
- **EXP (exponential time):**
  the problems solved by $O(2^{n^c})$-size circuits

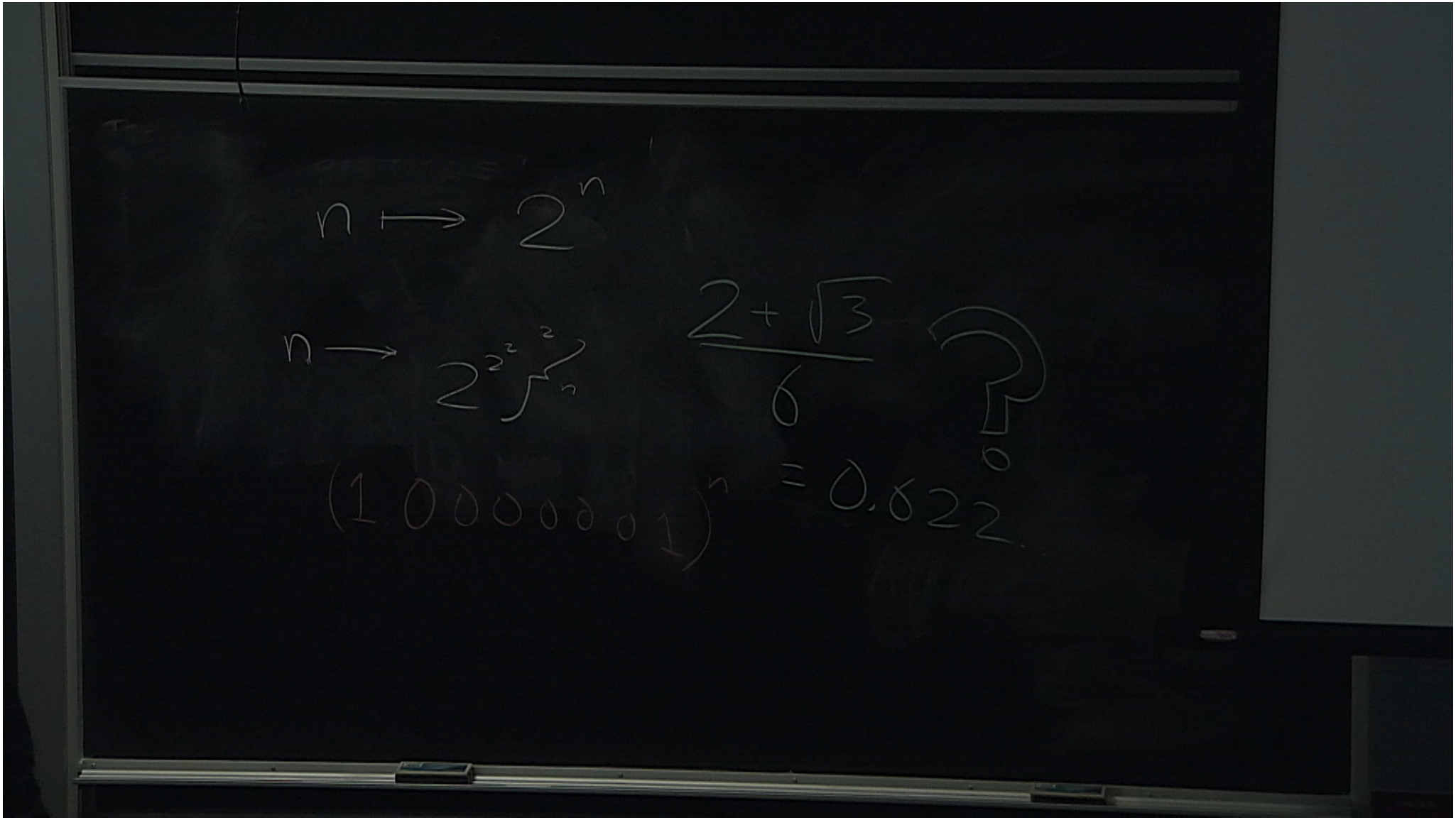
Summary of basic containments

$\mathbf{P} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXP}$



Note (for those familiar with NP):
it seems like **BQP** and **NP** are incomparable

Density matrix formalism


$n \longmapsto 2^n$
$n \longrightarrow 2^{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}$ n
$\frac{2+\sqrt{3}}{6}$?
$(1.0000001)^n = 0.622$

Density matrices (2)

A probability distribution on pure states is called a ***mixed state***:

$\left((|\psi_1\rangle, p_1), (|\psi_2\rangle, p_2), \ldots, (|\psi_d\rangle, p_d) \right)$

The ***density matrix*** associated with such a mixed state is:

$$\rho = \sum_{k=1}^{d} p_k \left| \psi_k \right\rangle \left\langle \psi_k \right|$$

Example: the density matrix for $\left((|0\rangle, \tfrac{1}{2}), (|1\rangle, \tfrac{1}{2}) \right)$ is:

$$\frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Question: what is the density matrix of

$\left((|0\rangle + |1\rangle, \tfrac{1}{2}), (|0\rangle - |1\rangle, \tfrac{1}{2}) \right)$?

Quantum channels (2)

Example 2 (decoherence): let $A_0 = |0\rangle\langle 0|$ and $A_1 = |1\rangle\langle 1|$

- This quantum op maps ρ to $|0\rangle\langle 0|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1|$

Entanglement and signaling

Recall that Entangled states, such as $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

qubit qubit

can be used to perform some intriguing feats, such as ***teleportation*** and ***superdense coding***