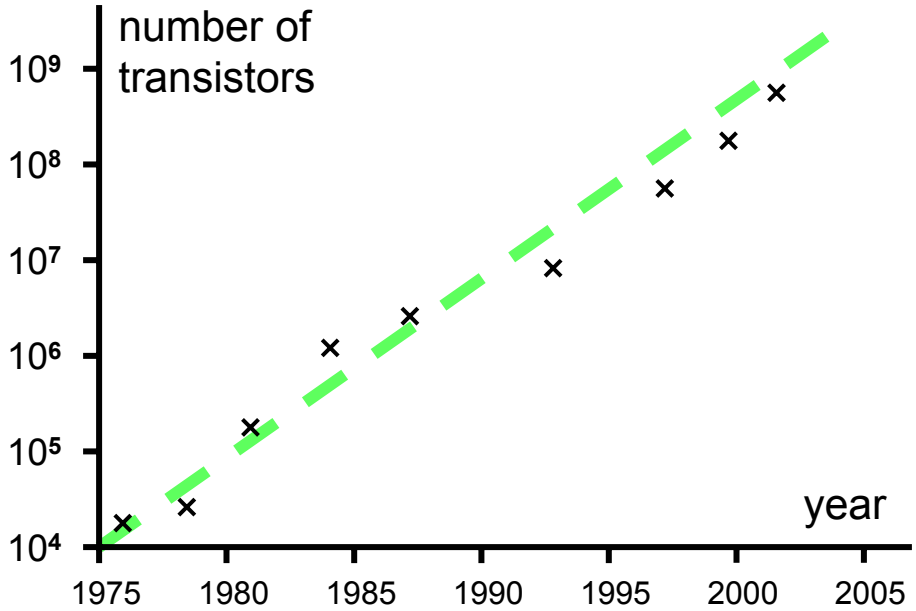
Introduction to Quantum Information Processing

CS 467 / CS 667
Phys 667 / Phys 767
C&O 481 / C&O 681

Lecture 1 (2008)

Richard Cleve
DC 2117
cleve@cs.uwaterloo.ca

Moore's Law



Following trend … atomic scale in 15-20 years

Quantum mechanical effects occur at this scale:

- Measuring a state (e.g. position) disturbs it
- Quantum systems sometimes seem to behave as if they are in several states at once
- Different evolutions can interfere with each other

Quantum mechanical effects

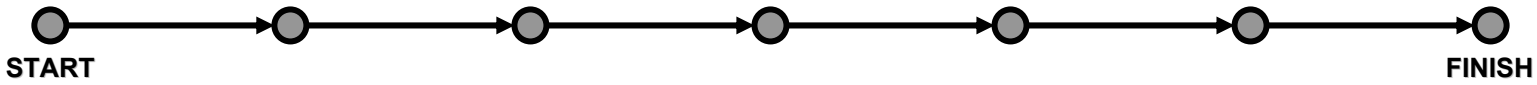
Additional nuisances to overcome?
or
New types of behavior to make use of?

[Shor, 1994]: polynomial-time algorithm for factoring integers on a ***quantum computer***

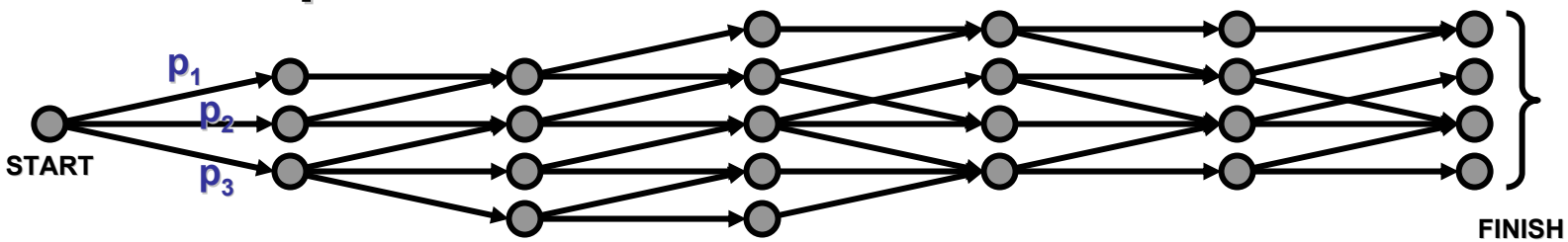
This could be used to break most of the existing public-key cryptosystems on the internet, such as RSA

Quantum algorithms

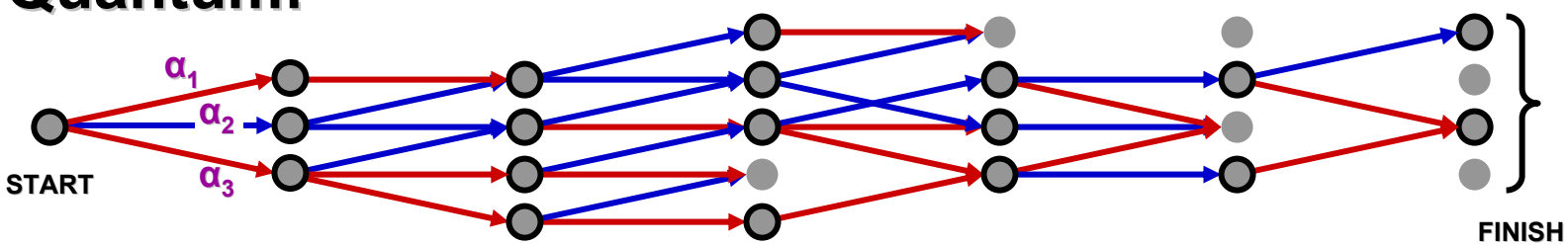
Classical deterministic:



Classical probabilistic:



Quantum:

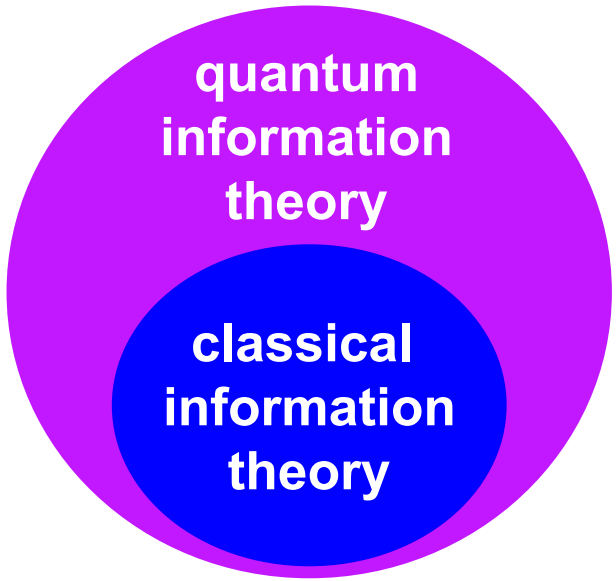


Also with quantum information:

- Fast***er*** algorithms for combinatorial search [Grover '96]
- Unbreakable codes with short keys [Bennett, Brassard '84]
- Communication savings in distributed systems [C, Buhrman '97]
- More efficient "proof systems" [Watrous '99]

… and an extensive quantum information theory arises, which generalizes classical information theory

For example: a theory of quantum error-correcting codes



This course covers the basics of quantum information processing

Topics include:

- Quantum algorithms and complexity theory
- Quantum information theory
- Quantum error-correcting codes
- Physical implementations*
- Quantum cryptography
- Quantum nonlocality and communication complexity

General course information

Background:

- classical algorithms and complexity
- linear algebra
- probability theory

Evaluation:

- 5 assignments (12% each)
- project presentation (40%)

Recommended texts:

An Introduction to Quantum Computation, P. Kaye, R. Laflamme, M. Mosca (Oxford University Press, 2007). Primary reference.

Quantum Computation and Quantum Information, Michael A. Nielsen and Isaac L. Chuang (Cambridge University Press, 2000). Secondary reference.

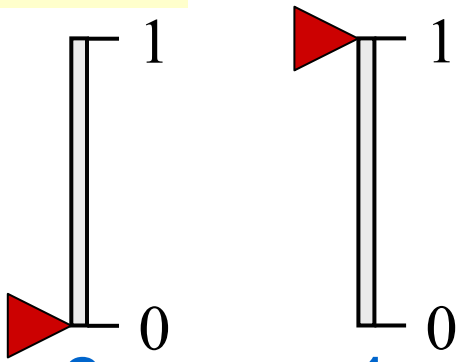
Basic framework of quantum information

Types of information

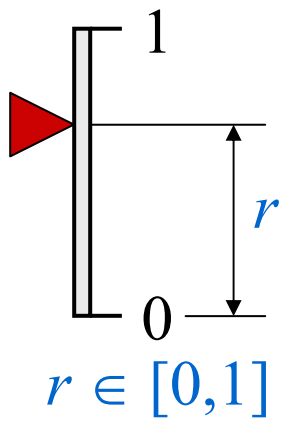
is quantum information digital or analog?

probabilistic

digital:



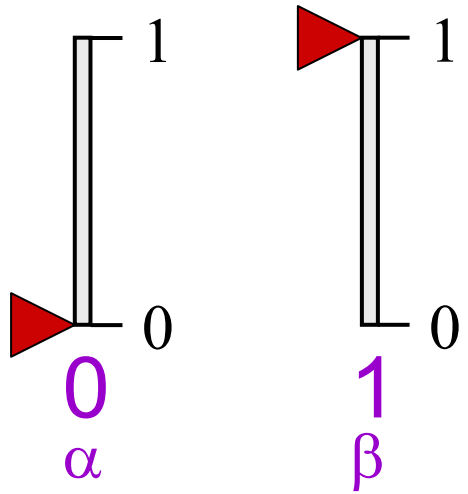
analog:



- Probabilities $p,\ q \geq 0,\ \ p + q = 1$
- *Cannot* explicitly extract p and q (only statistical inference)
- In any concrete setting, explicit state is 0 or 1
- Issue of precision (imperfect ok)

- Can explicitly extract r
- Issue of precision for setting & reading state
- Precision need not be perfect to be useful

Quantum (digital) information



- Amplitudes $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$
- Explicit state is $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$
- *Cannot* explicitly extract α and β (only statistical inference)
- Issue of precision (imperfect ok)

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

Bra: $\langle\psi|$ always denotes a row vector that is the conjugate transpose of $|\psi\rangle$, e.g. $\begin{bmatrix} \alpha^*_1 & \alpha^*_2 & \dots & \alpha^*_d \end{bmatrix}$

<u>Bra</u><u>ket</u>: $\langle\varphi|\psi\rangle$ denotes $\langle\varphi|\cdot|\psi\rangle$, the inner product of $|\varphi\rangle$ and $|\psi\rangle$

Basic operations on qubits (I)

(0) Initialize qubit to $|0\rangle$ or to $|1\rangle$

(1) Apply a unitary operation U $(U^{\dagger}U = I)$

Examples:

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

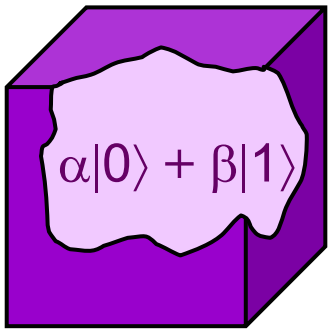
NOT (bit flip): $\sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

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

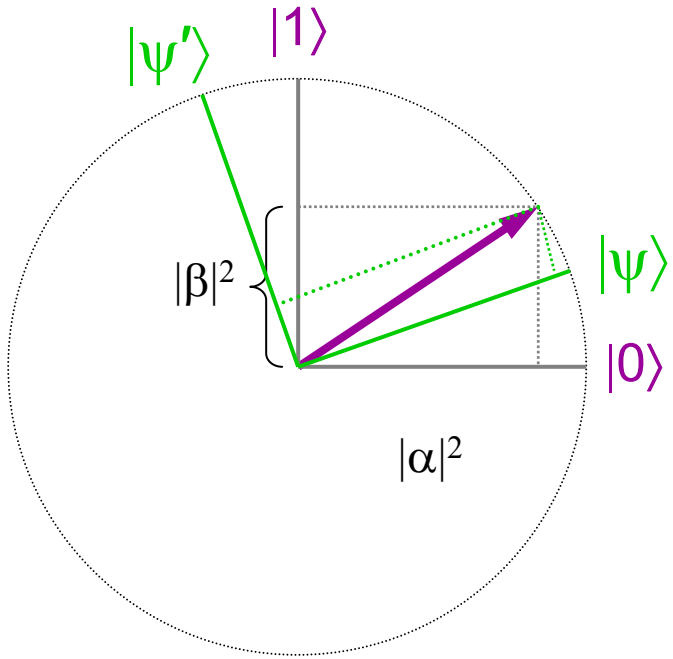
Phase flip: $\sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Basic operations on qubits (II)

(3) Apply a "standard" measurement:



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

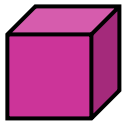


… and the quantum state collapses

(∗) 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 $|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ or $|-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$

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 …

n-qubit systems

Probabilistic states:

$$\forall x,\ p_x \geq 0$$

$$\sum_x p_x = 1$$

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

Quantum states:

$$\forall x,\ \alpha_x \in \mathbb{C}$$

$$\sum_x |\alpha_x|^2 = 1$$

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

Dirac notation: $|000\rangle$, $|001\rangle$, $|010\rangle$, …, $|111\rangle$ are basis vectors,

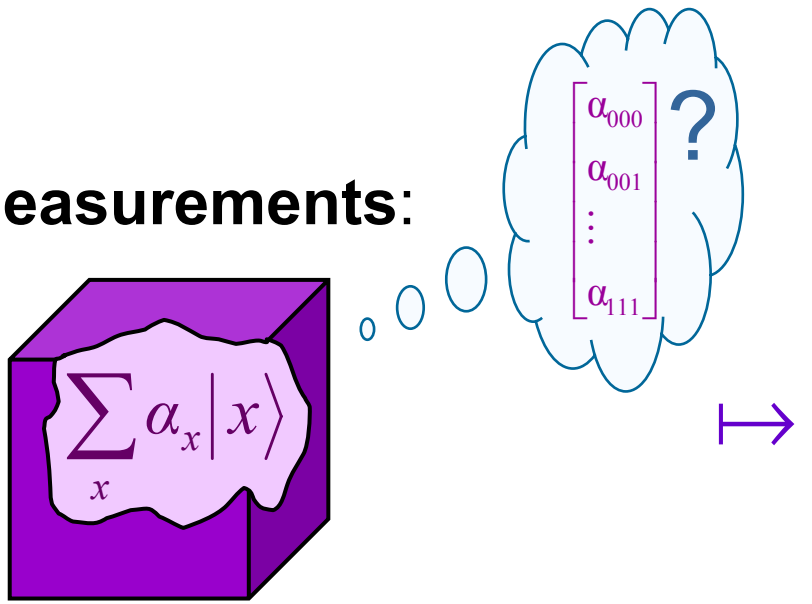
so $|\psi\rangle = \sum_x \alpha_x |x\rangle$

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:



$\mapsto$

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

… and the quantum state collapses

Entanglement

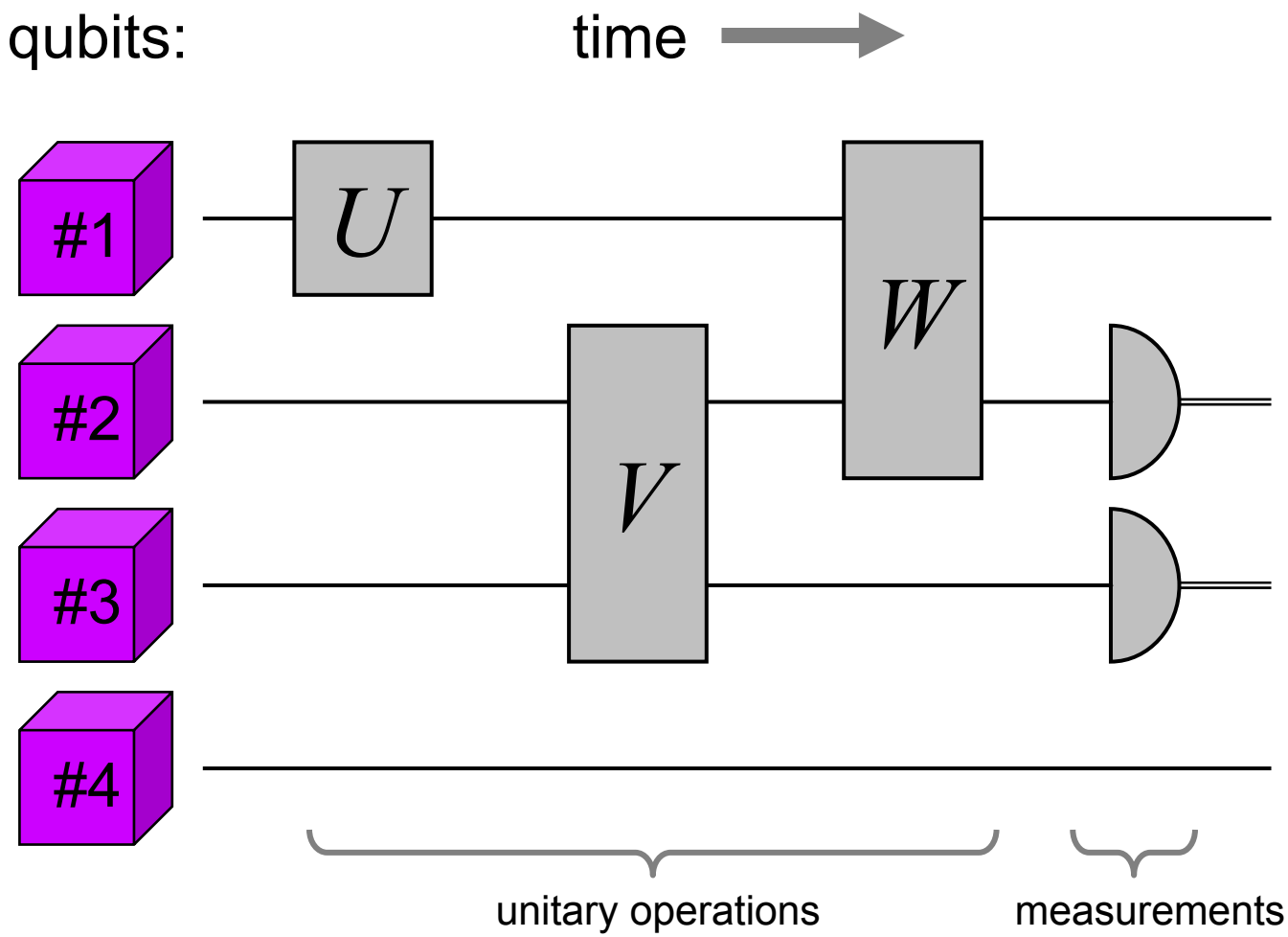
Product state (tensor/Kronecker product):

$$(\alpha|0\rangle + \beta|1\rangle)(\alpha'|0\rangle + \beta'|1\rangle) = \alpha\alpha'|00\rangle + \alpha\beta'|01\rangle + \beta\alpha'|10\rangle + \beta\beta'|11\rangle$$

Example of an ***entangled*** state: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

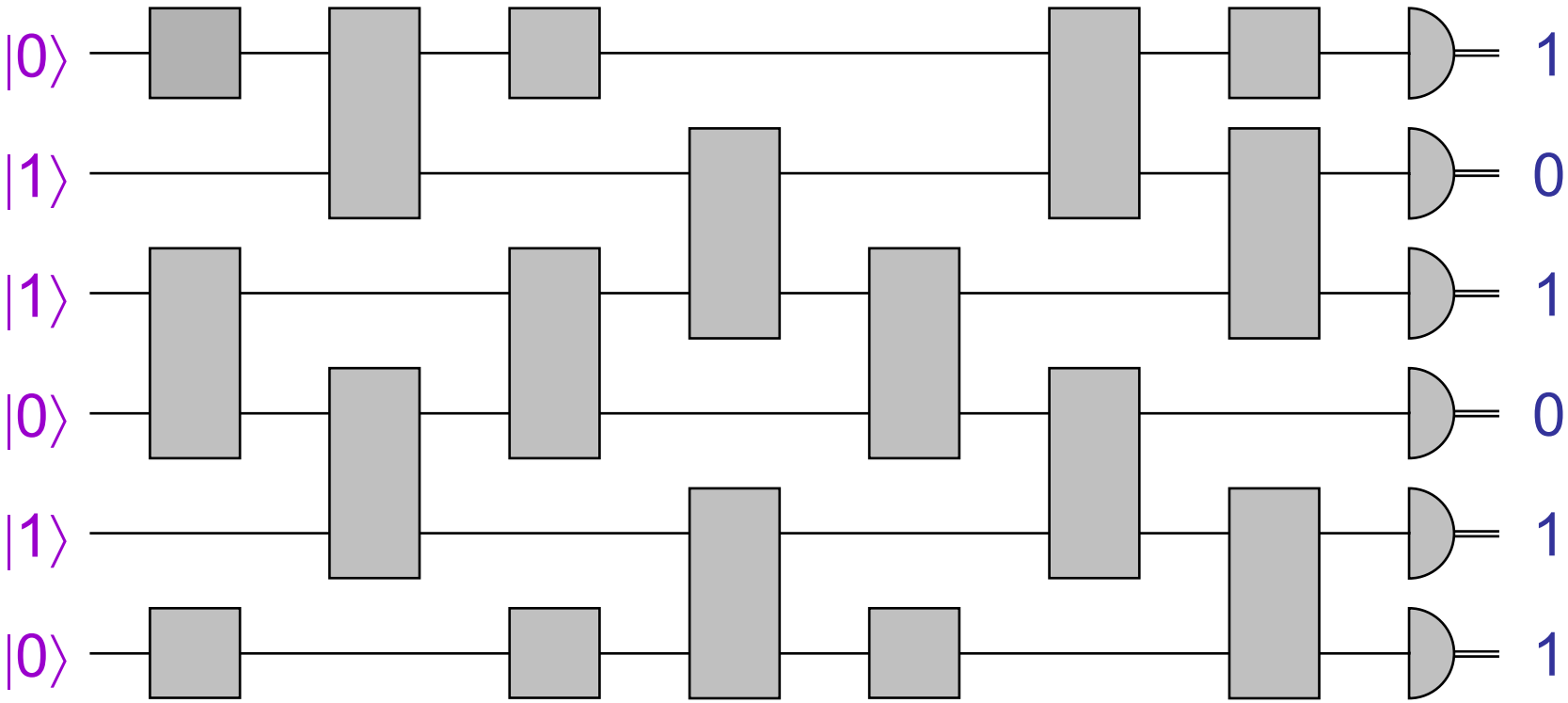
… can exhibit interesting "nonlocal" correlations:

Structure among subsystems



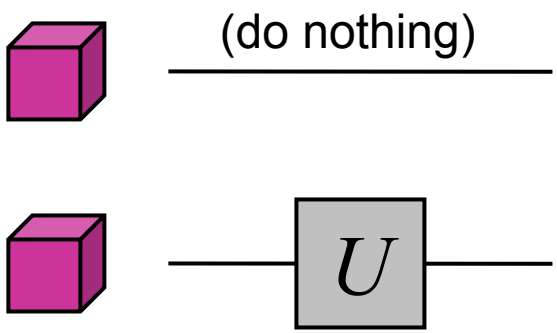
Quantum computations

Quantum circuits:



“Feasible” if circuit-size scales polynomially

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



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

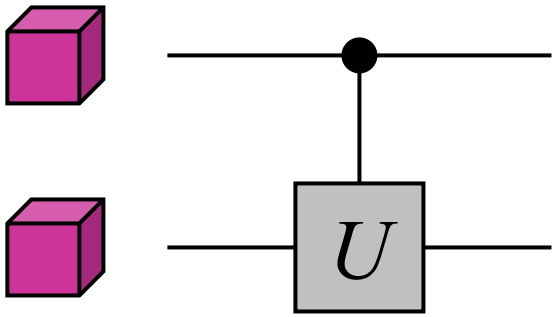
Maps basis states as:

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

The resulting 4x4 matrix is

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

Controlled-U gates



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

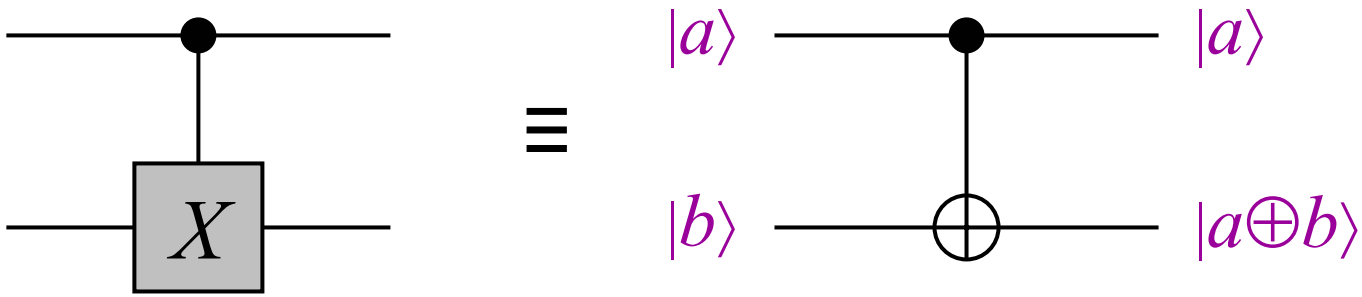
Maps basis states as:

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

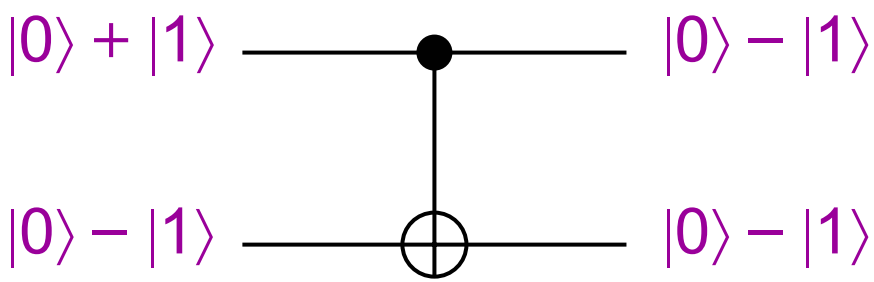
Resulting 4x4 matrix is controlled-U =

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

Controlled-NOT (CNOT)



Note: “control” qubit may change on some input states



Introduction to Quantum Information Processing

CS 467 / CS 667
Phys 667 / Phys 767
C&O 481 / C&O 681

Lecture 2 (2008)

Richard Cleve
DC 2117
cleve@cs.uwaterloo.ca

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:

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

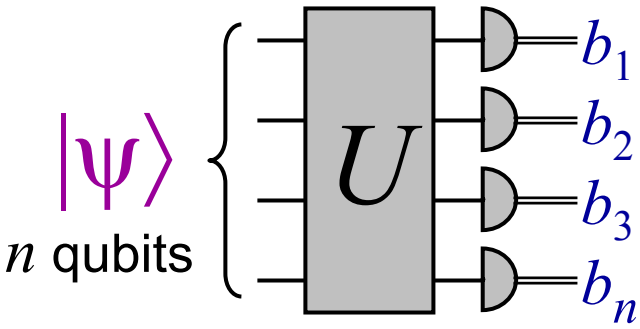
Does this mean that an exponential amount of classical information is somehow stored in n qubits?

Not in an operational sense ...

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

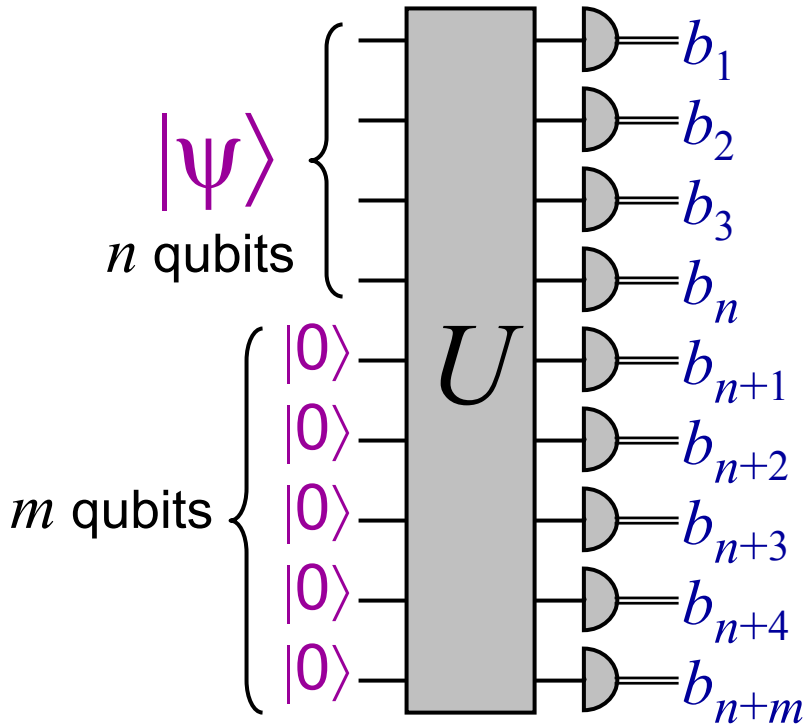
Holevo's Theorem

Easy case:



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

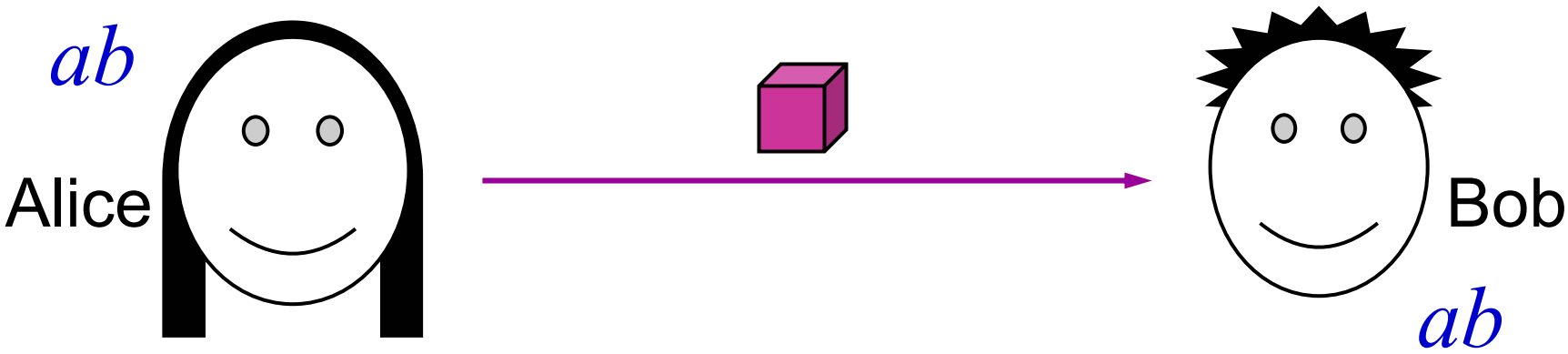
Hard case (the general case)**:**



The difficult proof is beyond the scope of this course

Superdense coding (prelude)

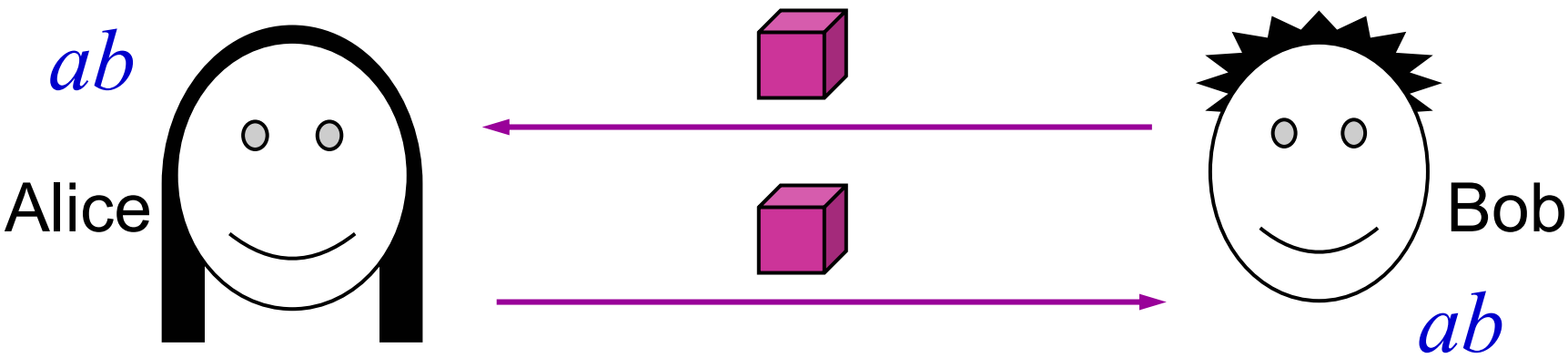
Suppose that Alice wants to convey ***two*** classical bits to Bob sending just ***one*** qubit



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

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

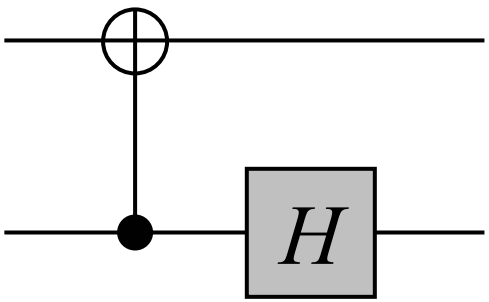
ab	state
00	$\|00\rangle + \|11\rangle$
01	$\|00\rangle - \|11\rangle$
10	$\|01\rangle + \|10\rangle$
11	$\|01\rangle - \|10\rangle$

} Bell basis

3. Bob measures the two qubits in the ***Bell basis***

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

Introduction to Quantum Information Processing

CS 467 / CS 667
Phys 667 / Phys 767
C&O 481 / C&O 681

Lecture 3 (2008)

Richard Cleve
DC 2117
cleve@cs.uwaterloo.ca

Teleportation

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

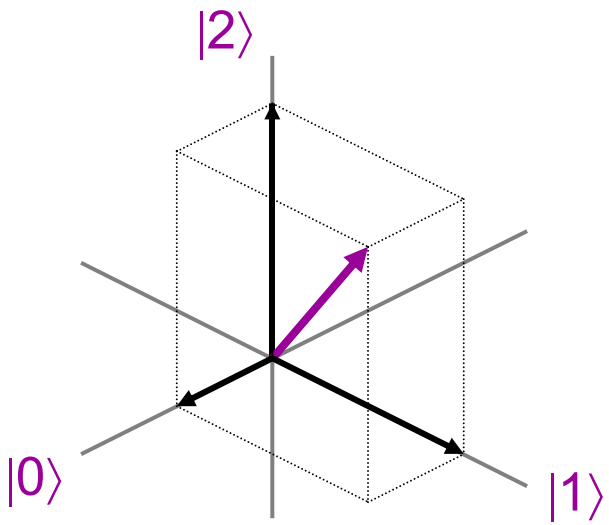
: : : : : :

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

} the columns of U are orthonormal

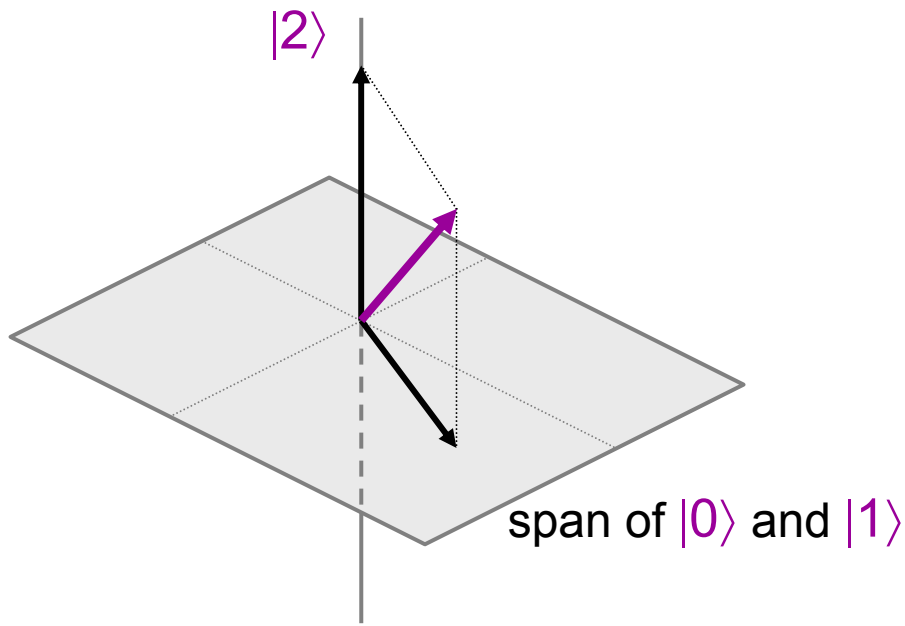
Incomplete measurements (I)

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



(qutrit)

The orthogonal subspaces can have other dimensions:



Incomplete measurements (II)

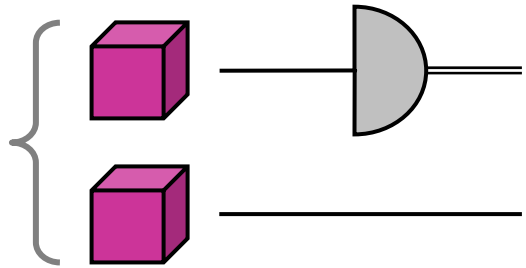
Such a measurement on $\alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle$

(renormalized)

results in $\begin{cases} \alpha_0|0\rangle + \alpha_1|1\rangle & \text{with prob } |\alpha_0|^2 + |\alpha_1|^2 \\ |2\rangle & \text{with prob } |\alpha_2|^2 \end{cases}$

Measuring the first qubit of a two-qubit system

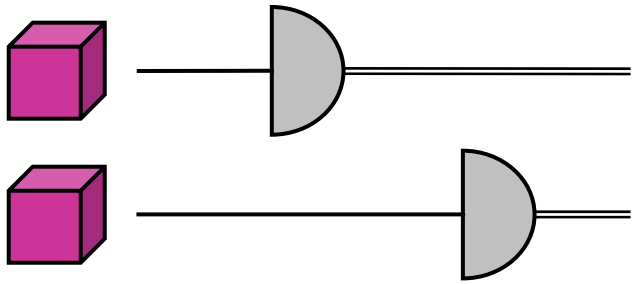
$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$



Defined as the incomplete measurement with respect to the two dimensional 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)

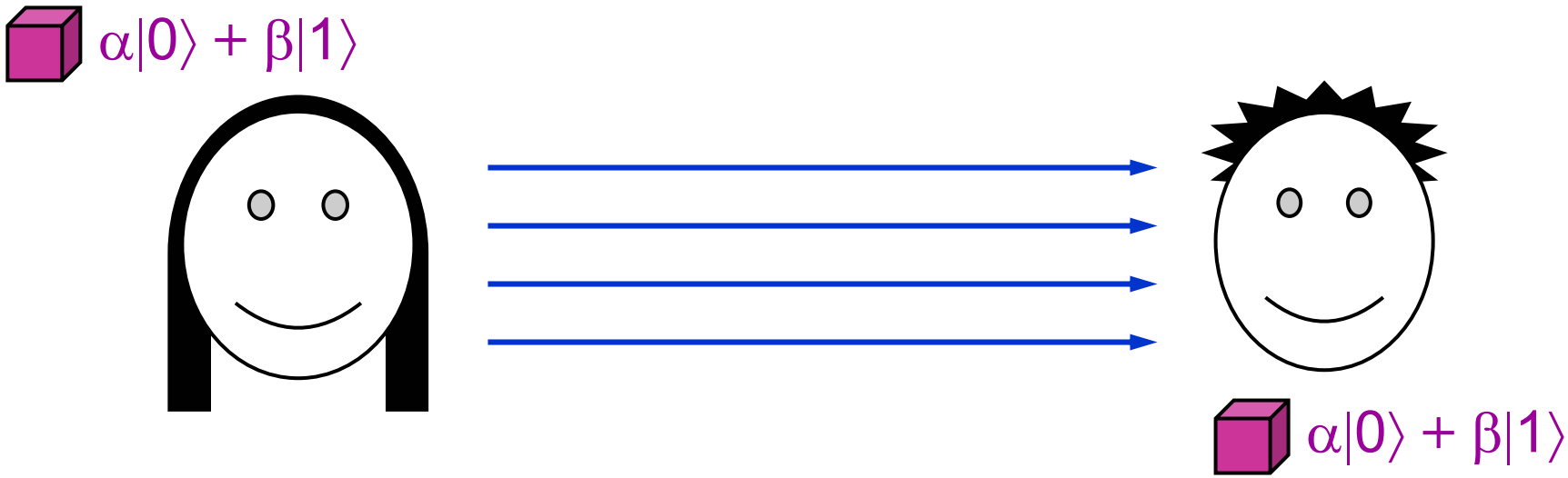
Result is the mixture $\begin{cases} \alpha_{00}|00\rangle + \alpha_{01}|01\rangle \text{ with prob } |\alpha_{00}|^2 + |\alpha_{01}|^2 \\ \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \text{ with prob } |\alpha_{10}|^2 + |\alpha_{11}|^2 \end{cases}$



Easy exercise: show that measuring the first qubit and *then* measuring the second qubit gives the same result as measuring both qubits at once

Teleportation (prelude)

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

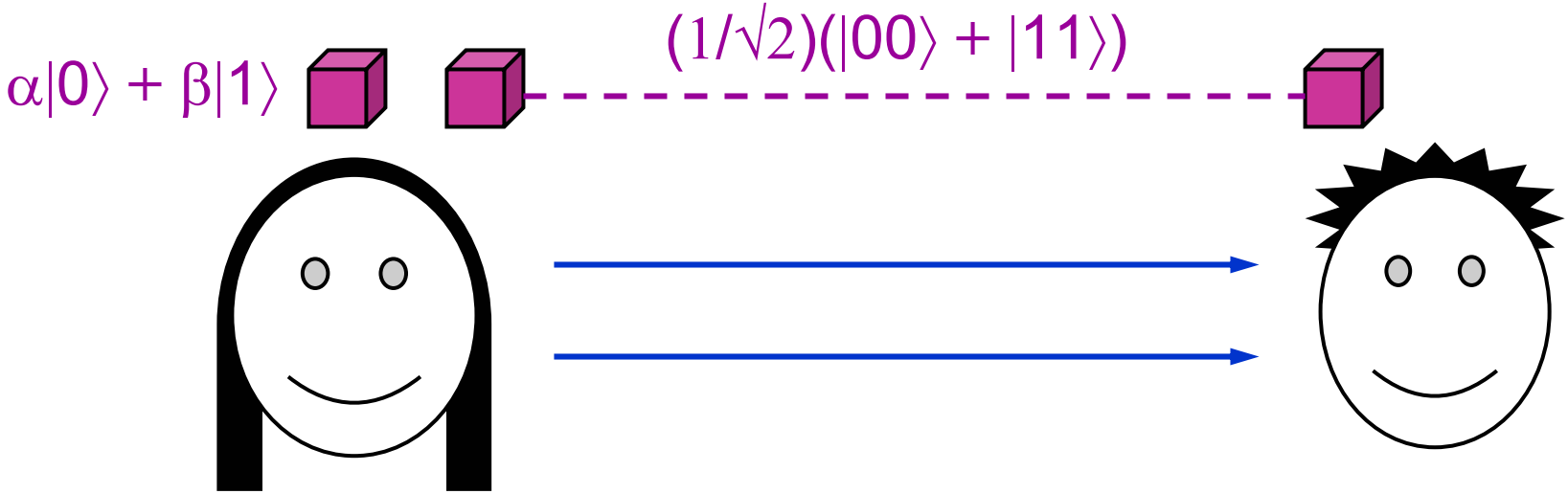


If Alice ***knows*** α and β, she can send approximations of them —but this still requires infinitely many bits for perfect precision

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

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

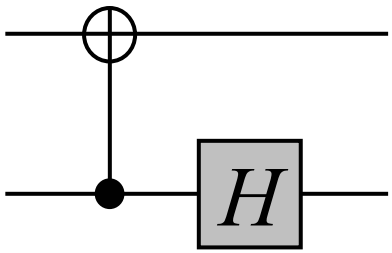
Initial state: $(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle)$ (omitting the $1/\sqrt{2}$ factor)

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

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

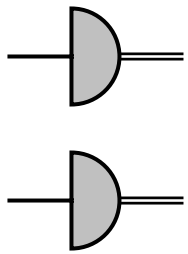
Protocol: Alice measures her two qubits ***in the Bell basis*** and sends the result to Bob (who then "corrects" his state)

What Alice does specifically

Alice applies 

to her two qubits, yielding:

$$\begin{cases} \tfrac{1}{2}|00\rangle(\alpha|0\rangle + \beta|1\rangle) \\ +\tfrac{1}{2}|01\rangle(\alpha|1\rangle + \beta|0\rangle) \\ +\tfrac{1}{2}|10\rangle(\alpha|0\rangle - \beta|1\rangle) \\ +\tfrac{1}{2}|11\rangle(\alpha|1\rangle - \beta|0\rangle) \end{cases}$$



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

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

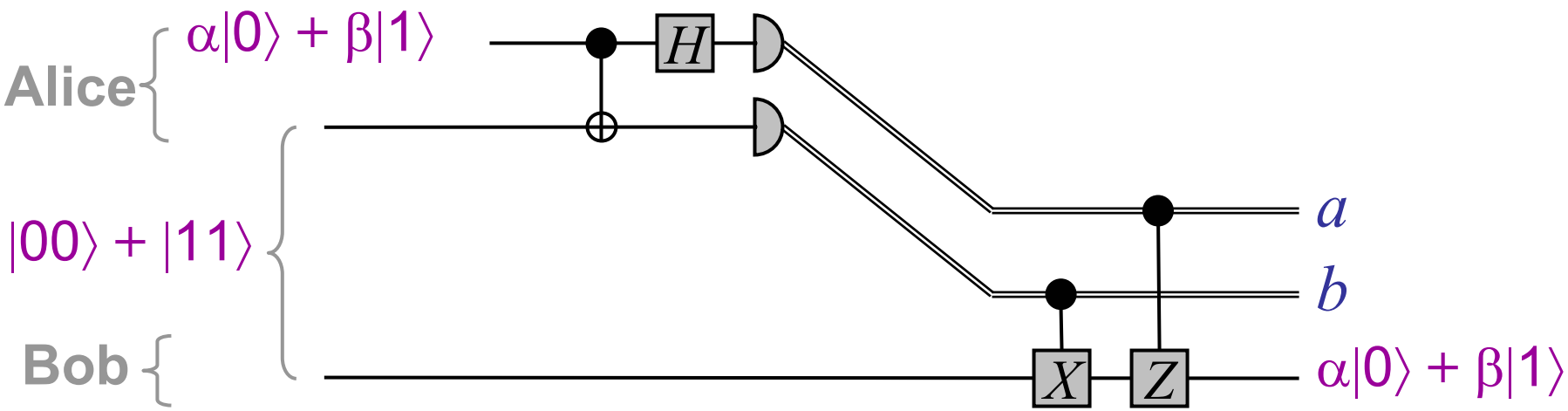
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

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

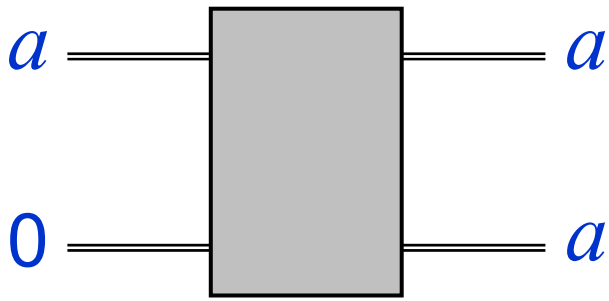
Summary of teleportation

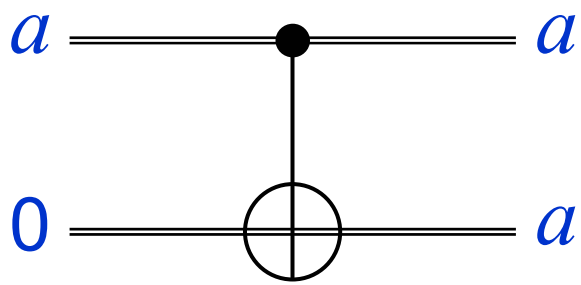


Quantum circuit exercise: try to work through the details of the analysis of this teleportation protocol

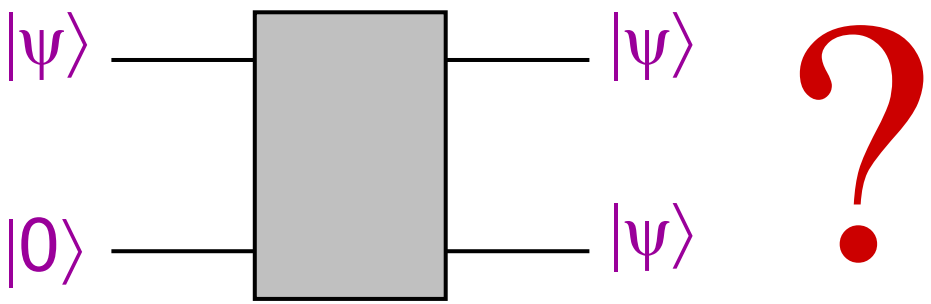
No-cloning theorem

Classical information can be copied



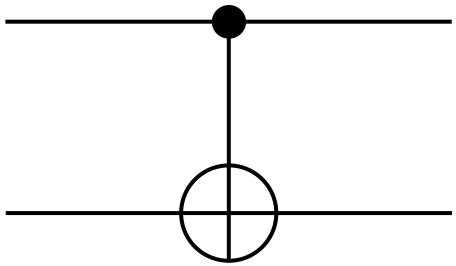


What about quantum information?



?

Candidate:



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

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

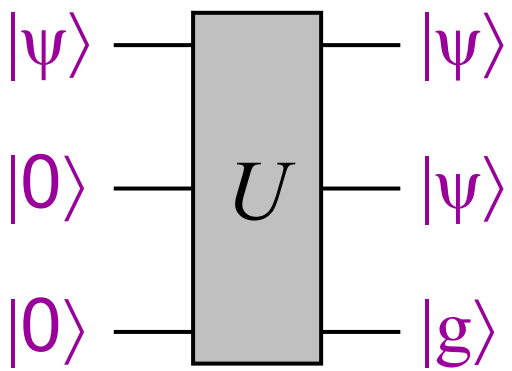
... where it yields output $(1/\sqrt{2})(|00\rangle + |11\rangle)$

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 $|\psi\rangle|\psi\rangle$

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