# Quantum Computing (Fall 2013) Instructor: Shengyu Zhang.

# Lecture 1 Basic concepts

*Anybody who is not shocked by quantum theory has not understood it*. --- Niels Bohr

 *I think I can safely say that nobody understands quantum mechanics*. --- Richard Feynman

 *On quantum theory I use up more brain grease than on relativity*. --- Albert Einstein

## About the course

* Hard math (for CS students). CSE Undergrads: If you don’t find the Algorithm course “too easy”, then you probably should consider to just *sit in* this course instead of taking it for credit.
* More from computer science perspectives, namely algorithms and complexity issues. Less from physics. Almost none about physical implementation of quantum computers.
* 4 homework assignments + 1 final: reading project.

## Starting from qubits

**One qubit**: , where are complex numbers satisfying
Some examples: , , ,

Dirac notation: for column vector, for raw vector, for inner product.

**Measurement in computational basis**: If one measures in , she observes 0 with probability , and observes 1 with probability . If 0 is observed, then the state becomes , and if 1 is observed, then the state becomes . Note that in general, measurements/observations change the system.

Note some distinctive properties: 1. Outcome of a measurement is not deterministic. 2. Measurement changes the system.

**Operation on one qubit**: One can operate on a single qubit in different ways. Some examples: the Pauli-X (NOT) gate , the Pauli-X gate , the Pauli-Z gate and the Hadamard gate are defined as follows.

Operating on a single qubit, these operators have the following effects.

**Multiple qubits**: If we have two qubits, then a state in the 2-qubit system is
where are complex numbers satisfying
For example, the following is an “EPR state”:

And it is an example of non-product state, in the sense that it cannot be written as for any coefficients .

**Measurement in computational basis**: For any Observe with probability , and the state becomes .

**Operation on two qubits**: One can also operate on a two-qubit system. An important example is Controlled-NOT (CNOT), defined as follows.

which has the effect

About the name “Controlled-NOT”: the first bit is the control bit, and conditioned on the control bit is 1, apply NOT gate to the second qubit.

**General pure states**: In general, a pure quantum state of a -qubit system corresponds to a unit vector in , the -dimensional vector space over complex numbers. Here a unit vector is a vector with -norm being 1.

**General (orthogonal) measurements**: Suppose that is a set of orthonormal basis in a -dimensional system. If we make an orthogonal measurement in basis on a pure state , then outcome occurs with probability , and if outcome occurs, the state collapses to .

If one prepares a state chosen from , and give it to you, then you can tell which state it is by the above measurement. An interesting (and sometimes annoying) fact is that if the set of states are not orthogonal, then there is no way to distinguish them perfectly.

States with different global phases cannot be distinguished. Namely, if , then no measurement can distinguish them.

## Mathematical model for quantum mechanics

The postulates of quantum mechanics.

**Postulate 1**: Associated to any isolated physical system is a complex vector space with inner product known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.

**Postulate 2**: The evolution of a closed quantum system is described by a *unitary* transformation. That is, the state of the system at time is related to the state of the system at time by a unitary operator which depends only on the times and ,

**Postulate 3**: Quantum measurements are described by a collection of *measurement operators*. These are operators acting on the state space of the system being measured. The index *m* refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is immediately before the measurement then the probability that result occurs is given by
and the state of the system after the measurement is . The measurement operators satisfy the completeness equation , which expresses the fact that probabilities sum to one.

**Postulate 4**: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through , and system number is prepared in the state , then the joint state of the total system is .

## Basic facts, protocols

**No-cloning theorem**---*One cannot make a copy of a quantum state.*

**Theorem** There isn’t a unitary operator operating on 2 qubits and mapping to for all single-qubit state .

Proof. Consider

**Teleportation**---*How to send quantum states using only classical channel (with the help of shared entanglement)*.

Alice holds a qubit . Alice and Bob share an EPR pair Here we use subscripts to indicate the registers holding the state.

Protocol: Alice applies CNOT on ( being the control bit), followed by a Hadamard gate on . Alice then measures her part , which makes Bob’s qubit to collapse to one of the four orthogonal states , , , . Alice also observes a corresponding outcome . Alice sends , the 2-bit classical information to Bob, who then knows how to revert his state back to .

For more details, see [NC00] Chapter 1.3.7. (If you don’t have the book, see the [wiki page](http://en.wikipedia.org/wiki/Quantum_teleportation#The_result) for a nice explanation.)

**Superdense coding---***Using one qubit to encode two classical bits*.

Superdense coding is something converse to teleportation. Alice and Bob share an EPR pair , and Alice wants to transfer two classical bits to Bob.

Protocol: Alice applies if , respectively. Then the shared state becomes ,, , , respectively. Alice sends her qubit to Bob, who then measures the state and gets the encoded information about .

## Entanglement and nonlocality

Recall that an EPR state is an entangled state, and it cannot be written as for any single-qubit states and . Entanglement is a key difference between classical and quantum mechanics.

**CHSH game**. Consider the following game. Alice and Bob each receive a bit, and , respectively, and they each want to output a bit, and , respectively, such that . Note that no communication between Alice and Bob is allowed.

With classical local operations and shared randomness, they can succeed with probability 3/4=75%, and that is optimal. With quantum local operations on a shared EPR pair, they can succeed with probability , higher than classical. See [BCMdW10] (Section II.B) for details.

## Reference

[NC00] Michael Nielsen and Isaac Chuang, Quantum Computation and Quantum Information, *Cambridge University Press*, 2000.

[BCMdW10] Harry Buhrman, Richard Cleve, Serge Massar, Ronald de Wolf, Nonlocality and communication complexity, *Reviews of Modern Physics*, volume 82, 2010.

## Exercise

1. We said that non-orthogonal states cannot be perfectly distinguished. Consider this on a simple example: One prepares a state chosen from , and let you guess which one it is. Show that you cannot use any measurement to identify with certainty.
2. Prove that the three Pauli matrices and the Identity matrix are orthogonal to each other with the inner product defined by . Here the superscript \* is the complex conjugate.