CMSC 657: Introduction to Quantum Information Processing
Lecture 1

Instructor: Daniel Gottesman

Fall 2024

1 Introduction to the Course

The behavior of individual atoms and objects of similar size are governed by the laws of quantum mechanics rather than the familiar rules of classical mechanics, which apply to macroscopic objects. Quantum information is the study of the properties of information encoded in quantum objects, and quantum computers can take advantage of quantum properties to solve some problems much faster than any classical computer. This course will give an overview of the major results in the field of quantum information.

1.1 Logistics

The main resource for the class is the lectures. The textbook Nielsen and Chuang is optional. It covers similar topics but I won't be following it closely.

The course web page https://www.cs.umd.edu/class/fall2024/cmsc657/ is a good resource for information about the class, including the lecture notes and problem sets. Problem sets and the final will be turned in on Gradescope. There is also a Piazza, and solution sets will be available on ELMS.

I will have office hours 11-12 on Tuesday in my office Atlantic 3251, and the TA Suchetan Dontha will have office hours Thursday 2-3 PM in Atlantic 3373.

1.2 Grading and Assignments

Your grade will be determined by the following components:

- Weekly problem sets (60%)
- Take-home final exam (40%)

Problem sets will be due on Gradescope by 5 PM on Thursdays. Late problem sets will full credit up to 24 hours late, no credit after that without an extension. You may discuss the problems with other students and even work together on them, but if you do so, you must list on your solutions the students you worked with and write up your own solution in your own words. Similarly, if you use any reference materials (e.g., books, internet, AI tools) other than lectures, the textbook Nielsen and Chuang, and any other materials suggested in class, please indicate those as well.

There will be an optional final project which is a choice:

- Term paper, 5–10 pages long, based on your reading of 1-2 research articles
- Learn a quantum programming language and implement a quantum algorithm or protocol on a cloud quantum computer and/or simulator
- Another comparable project, with instructor approval

This can be done in a group of up to 4 people, and if you do it, it replaces the lowest 2 problem set grades. Note that if you want to do it, you will need to turn in a proposal by Oct. 29.

More information about the final project and final exam will be forthcoming later in the term.

1.3 Overview of the Field of Quantum Information

I like to organize work in the field into three major themes:

- How can we build a quantum computer? (This has a theoretical and an experimental side.)
- What can we do with a quantum computer? What are the properties of quantum information?
- How can we apply quantum information ideas to other subjects in physics, CS, or other fields?

This course will mostly concentrate on the first two topics. We will also go through a variety of background material, since the course is bringing in students of very different backgrounds. You should know linear algebra, the rest is not assumed. That also means that many of you will already know some of this, and I apologize for having to go through it. The course is not intended for students who have already taken an undergrad introduction to quantum mechanics course here or elsewhere, although you may still benefit from additional material or a different perspective in this course.

Major topics include:

- Introduction to quantum mechanics: We will discuss the formalism of quantum mechanics, as used in the field of quantum information.
- Quantum circuits: Quantum algorithms are built up out of small computational units called gates. We'll discuss the main quantum gates, how to put them together into circuits, and how to represent the circuits.
- Quantum algorithms and complexity: We'll discuss some of the major quantum algorithms (e.g., Shor's algorithm, Grover's algorithm, Hamiltonian simulation), how they are useful, and the sense in which they offer an improvement over classical algorithms.
- Building quantum computers: We'll briefly discuss some of the main methods used to build quantum computers.
- Quantum error correction and fault tolerance: We'll discuss how to deal with errors in the computer through encoding in quantum error-correcting codes.
- Quantum information theory: We will discuss a variety of topics relating to quantifying and characterizing quantum information, such as quantum compression, measures of entanglement, and quantum non-locality.
- Quantum cryptography: We will primarily discuss quantum key distribution, used to establish secret keys for cryptographic purposes.

2 Introduction to Quantum Mechanics

2.1 Quantum States

When we have a quantum system, we can use math to describe what is going on in the system. Examples of quantum systems used for quantum computation are photons (individual particles of light) and atoms with a single electron which could have low energy or high energy. The mathematical description of the system at any given time is called its *state*, which is supposed to be enough information to predict what will happen to the system under various situations. However, in quantum mechanics, these predictions are statistical.

The mathematics used for quantum mechanics is just linear algebra with complex vector spaces. The states (at least the *pure states*; we will discuss *mixed states* later) are vectors. For quantum mechanics, we write vectors with a line/angle bracket combination called a *ket*. Conventionally, pure states are named after Greek letters, particularly ψ and ϕ.

$$|\psi\rangle \tag{1}$$

In this class, we will deal almost exclusively with finite-dimensional vector spaces, and we can label the basis vectors by numbers:

$$|0\rangle,\ |1\rangle,\ |2\rangle,\ \ldots. \tag{2}$$

The main unit we will use is the *qubit*, which has a 2-dimensional vector space, with basis elements $|0\rangle$, $|1\rangle$.

Other states are written as a *superposition* of the basis states:

$$\alpha|0\rangle + \beta|1\rangle \leftrightarrow \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \tag{3}$$

This represents an arbitrary state of 1 qubit when α and β are complex numbers. (However, there is a constraint on α and β which we will get to in a little bit.)

When we have multiple qubits, you can label the basis vectors by larger numbers or you can use bit strings, e.g. 00, 01, 10, 11 for 2 qubits. The general state of 2 qubits is then

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \leftrightarrow \begin{pmatrix}\alpha\\ \beta\\ \gamma\\ \delta\end{pmatrix} \tag{4}$$

If we have n qubits, the vector space has dimension 2^n, so we need bit strings of length n to label all the basis states.

This is an example of a *tensor product*. The tensor product of two finite-dimensional vector spaces A and B can be defined by taking a basis $\{|\psi_i\rangle\}_{i=1,\ldots d_A}$ of A and a basis $\{|\phi_j\rangle\}_{j=1,\ldots d_B}$ of B. Then the tensor product basis of $A \otimes B$ is

$$\{|\psi_i\rangle \otimes |\phi_j\rangle\}_{i,j}. \tag{5}$$

$A \otimes B$ thus has dimension $d_A d_B$, and the arbitrary element of $A \otimes B$ is

$$\sum_{i,j} \alpha_{ij}|\psi_i\rangle \otimes |\phi_j\rangle. \tag{6}$$

Tensor products are important, because the state space of two separate quantum systems is the tensor product of the state spaces of each one separately.

Some states are tensor product states, e.g.,

$$(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) = |00\rangle - |01\rangle + |10\rangle - |11\rangle \leftrightarrow \begin{pmatrix}1\\ -1\\ 1\\ -1\end{pmatrix}. \tag{7}$$

Pure states which cannot be factorized as a tensor product are *entangled* states, e.g.,

$$|00\rangle + |11\rangle \leftrightarrow \begin{pmatrix}1\\ 0\\ 0\\ 1\end{pmatrix}. \tag{8}$$

How about these states? Are they entangled or not?

$$|00\rangle + |10\rangle \tag{9}$$

$$|10\rangle + 2|01\rangle \tag{10}$$

Answers: no ($(|0\rangle + |1\rangle) \otimes |0\rangle$), yes.

2.2 Hilbert Space and the Inner Product

The vector spaces used in quantum mechanics are *Hilbert spaces*, which are complex vector spaces with an *inner product*. The inner product is the standard one:

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\cdot\begin{pmatrix}\gamma\\ \delta\end{pmatrix}=\alpha^*\gamma+\beta^*\delta. \tag{11}$$

Here, $*$ is complex conjugate. We usually write this inner product through the formalism of quantum mechanics by introducing *bras*, which use a left angle bracket instead of a right one. Mathematically, a bra lives in the dual space of the original Hilbert space, and there is an isomorphism between bras and kets:

$$\alpha|0\rangle+\beta|1\rangle\leftrightarrow\alpha^*\langle 0|+\beta^*\langle 1|. \tag{12}$$

This isomorphism is the adjoint. (Mathematical note: The adjoint map depends on the inner product to define it uniquely; otherwise, the isomorphism between the vector space and its dual is non-canonical.). We can think of the bras as row vectors instead of column vectors:

$$\alpha^*\langle 0|+\beta^*\langle 1|\leftrightarrow\begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}. \tag{13}$$

The inner product can then be worked out in bra-ket notation as follows:

$$\begin{aligned}|\psi\rangle =&\alpha|0\rangle+\beta|1\rangle &(14)\\ |\phi\rangle =&\gamma|0\rangle+\delta|1\rangle &(15)\\ \langle\psi|\phi\rangle =&(\alpha^*\langle 0|+\beta^*\langle 1|)(\gamma|0\rangle+\delta|1\rangle) &(16)\\ =&\alpha^*\gamma\langle 0|0\rangle+\alpha^*\delta\langle 0|1\rangle+\beta^*\gamma\langle 1|0\rangle+\beta^*\delta\langle 1|1\rangle &(17)\\ =&\alpha^*\gamma+\beta^*\delta, &(18)\end{aligned}$$

because $\langle 0|1\rangle=\langle 1|0\rangle=0$ and $\langle 0|0\rangle=\langle 1|1\rangle=1$ when we work with *orthonormal basis vectors* $|0\rangle$ and $|1\rangle$. This is the same answer you would get by multiplying the row vector bra with the column vector ket.

Note that $\langle\psi|\phi\rangle=\langle\phi|\psi\rangle^*$, which follows because of the isomorphism between the bras and kets.

When $|\psi\rangle=\sum_i\alpha_i|i\rangle$ for orthonormal basis vectors $|i\rangle$, then

$$\langle\psi|\psi\rangle=\sum_i|\alpha_i|^2. \tag{19}$$

For reasons that will become clearer later, valid quantum mechanics states are normalized states, with $\langle\psi|\psi\rangle=1$.

Actually, rather than using a Hilbert space, quantum states actually use a *projective Hilbert space*. This means that a global complex scalar has no physical effect. Because of the normalization constraint, the complex scalar has to have norm (absolute value) 1. Thus, the statement is that $|\psi\rangle$ is the same state as $e^{i\phi}|\psi\rangle$. Again, the reasons for this will become clearer next time.

Despite the normalization and projective constraints, we usually ignore these and write things like $|0\rangle+|1\rangle$ for a quantum state. This should be understand to be normalized, so

$$|0\rangle+|1\rangle\rightarrow\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle). \tag{20}$$

2.3 Unitary Operators

Physical quantum operations must preserve the linear structure of quantum mechanics and also the inner product of the Hilbert space. The states we have discussed so far are called *pure states* (we will discuss *mixed states* in the next lecture), and the possible operations that do this are *unitary operators*. They are

linear operators with the additional property that they preserve the inner product. Because a unitary map is a linear operator, it can be written as a matrix, and the unitary constraint is the statement that

$$U^\dagger U = UU^\dagger = I. \tag{21}$$

Here † is the Hermitian adjoint, which can be performed as the complex conjugate transpose. For instance, a unitary acting on a qubit is a 2×2 matrix

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{22}$$

and then the adjoint is

$$U^\dagger = \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix}. \tag{23}$$

Thus, for instance,

$$UU^\dagger = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix} = \begin{pmatrix} |a|^2 + |b|^2 & ac^* + bd^* \\ ca^* + db^* & |c|^2 + |d|^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{24}$$

Note how unitary operators preserve the inner product. That is, $U|\psi\rangle$ and $U|\phi\rangle$ have the same inner product as $|\psi\rangle$ and $|\phi\rangle$:

$$(\langle\psi|U^\dagger)(U|\phi\rangle) = \langle\psi|(U^\dagger U)|\phi\rangle = \langle\psi|\phi\rangle. \tag{25}$$

Linear operators can also be written in a bra-ket notation. Here, the bra is on the right and the ket is on the left, and then the inner product does the action of the matrix on the vector:

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \leftrightarrow U = a|0\rangle\langle 0| + b|0\rangle\langle 1| + c|1\rangle\langle 0| + d|1\rangle\langle 1|. \tag{26}$$

Thus,

$$\begin{aligned} U(\alpha|0\rangle + \beta|1\rangle) =& a\alpha|0\rangle\langle 0|0\rangle + b\alpha|0\rangle\langle 1|0\rangle + c\alpha|1\rangle\langle 0|0\rangle + d\alpha|1\rangle\langle 1|0\rangle \\ &+ a\beta|0\rangle\langle 0|1\rangle + b\beta|0\rangle\langle 1|1\rangle + c\beta|1\rangle\langle 0|1\rangle + d\beta|1\rangle\langle 1|1\rangle && (27) \\ =& a\alpha|0\rangle + c\alpha|1\rangle + b\beta|0\rangle + d\beta|1\rangle && (28) \\ =& (a\alpha + b\beta)|0\rangle + (c\alpha + d\beta)|1\rangle. && (29) \end{aligned}$$

Changing between one orthonormal basis and another is a unitary operation.

2.4 No-Cloning Theorem

Since all operations are linear maps, we get a restriction on the way quantum states can evolve:

Theorem 1 (No-Cloning Theorem)**.** *There is no quantum operation that takes one copy of an arbitrary unknown quantum state and makes two copies.*

Proof. Consider two orthogonal quantum states $|0\rangle$ and $|1\rangle$. Then $|0\rangle + |1\rangle$ (normalized appropriately) is also a quantum states. Suppose we have some map U that makes a copy of $|0\rangle$ and $|1\rangle$, perhaps using some standard *ancilla* state $|\phi\rangle$. $|\phi\rangle$ can't depend on the other state, since we only have one copy of the other state, so

$$\begin{aligned} U|0\rangle|\phi\rangle =& |0\rangle|0\rangle && (30) \\ U|1\rangle|\phi\rangle =& |1\rangle|1\rangle. && (31) \end{aligned}$$

But then it is not possible for U to also make a copy of $|0\rangle + |1\rangle$, because by linearity

$$\begin{aligned} U(|0\rangle + |1\rangle)|\phi\rangle =& |0\rangle|0\rangle + |1\rangle|1\rangle & (32)\\ \neq& (|0\rangle + |1\rangle)(|0\rangle + |1\rangle) & (33)\\ =& |0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle. & (34) \end{aligned}$$

□

Note that while it is impossible to copy arbitrary superpositions, there is no limit on copying orthogonal basis states. In a few lectures, we will see operations that do that.

The No Cloning Theorem indicates a significant difference between the behavior of quantum information and classical information: You can only have one copy, ever, of unknown quantum information, making quantum information behave more like a physical object than classical information, which has no inherent limitations on being copied. Content companies often want to limit the amount of copying of classical information, but this is inherently impossible. It may be legal under U.S. law to have copy protection, but it violates the laws of physics: Consider that if you watch a movie and remember any of it, you have made an imperfect copy of it in your brain while it is still possible to watch the original again. Even that amount of copying is not be allowed under the stronger versions of the No-Cloning Theorem that apply to quantum states.

This is an example of one of the themes of the class and of the field of quantum information: The rules of physics help to determine the properties of information. I won't be emphasizing this most of the time, but remember when we are trying to understand how quantum information is different from classical information, this is the underlying reason.