Quantum Information Science Lecture 1

Andy Lutomirski

Spring 2007-08

Contents

1 Intro to the class **1**

2 Quantum Error Correction **1**
2.1 Quantum operations 1
2.1.1 Density matrices 1
2.1.2 System-environment model 2

1 Intro to the class

This is 6.443J, 8.371J, 18.409, and MAS.865.

We'll discuss quantum algorithms (Shor's, Grover's, etc.), crypto (key distribution and signatures), quantum communication (superdense coding, etc.), error correction, alternative models of computation (quantum computation by teleportation or measurement), etc. We will not cover implementations (these are covered more in 8.422, 6.73? (Orlando's), Dave Cory's). We will also not cover complexity theory (covered in the fall in Scott Aaronson's class).

There will be a project (20% presentation, 40% paper) as well as four problem sets (40%).

2 Quantum Error Correction

We will cover quantum operations, the criteria for quantum error correction, the CSS codes, the stabilizer formalism, and non-additive codes using the CWS (codeword-stabilized codes) framework.

2.1 Quantum operations

2.1.1 Density matrices

This will provide to background to understand errors. We need to understand what happens when we take a quantum state, put it into a black box, and receive output. This system could be a measurement, an operation, something that throws out the state and replaces it entirely, for example. It could be an adversary or a friend. We will only describe a discrete-time model.

Using pure states is insufficient to describe such systems because they could add randomness.

Pure states are of the form $a|0\rangle + b|1\rangle$. Unitary operations act by $U|\psi\rangle = a'|0\rangle + b'|1\rangle$. If, on the other hand, we throw away qubits, we might have $|\psi_{AB}\rangle = a|00\rangle + b|01\rangle + c|10\rangle$ and throw away B's state. This results in the partial trace over B. One way to think of it is to imagine B measuring the bit.

In a simple example, if we start with $\sqrt{\frac{3}{4}}|00\rangle + \sqrt{\frac{1}{4}}|11\rangle$, then A gets $\sqrt{\frac{3}{4}}|0\rangle \overset{\text{"}or\text{"}}{\oplus} \sqrt{\frac{1}{4}}|1\rangle$. If B instead applies a Hadamard gate and measures, then the (pre-measurement) state is $\left(\sqrt{\frac{3}{8}}|0\rangle + \sqrt{\frac{1}{8}}|1\rangle\right)|0\rangle + \left(\sqrt{\frac{3}{8}}|0\rangle - \sqrt{\frac{1}{8}}|1\rangle\right)|1\rangle$. Then A has $\left(\sqrt{\frac{3}{8}}|0\rangle + \sqrt{\frac{1}{8}}|1\rangle\right) \oplus \left(\sqrt{\frac{3}{8}}|0\rangle - \sqrt{\frac{1}{8}}|1\rangle\right)$. A must not be able to tell these mixed states apart (by any means at all).

The density matrix is a tool for tracking statistical mixtures, defined by

$$\rho = \sum_k |\psi_k\rangle\langle\psi_k| \tag{1}$$

where the $|\psi_k\rangle$are unnormalized. For example,

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

and both mixtures give $\rho = \frac{1}{4}\begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}$.

A matrix ρ is a density matrix iff $Tr(\rho) = 1$ and $\rho \succeq 0$. The recipe $\rho = \sum_k p_k|\psi_k\rangle\langle\psi_k|$ always gives a density matrix (for normalized states and a probability distribution). Also, $\forall$ density matrixes $\rho.\rho = \sum_k p_k|\psi_k\rangle\langle\psi_k|$ for some $\{p_k\}, \{|\psi_k\rangle\}$ (the spectral decomposition).

Unraveling lemma Let $\rho = \sum_k p_k|\psi_k\rangle\langle\psi_k|$. Then $\rho = \rho' = \sum_k q_k|\phi_k\rangle\langle\phi_k|$ if $\sqrt{p_k}|\psi_k\rangle = \sum_j u_{kj}q_j|\phi_k\rangle$ with u unitary.

2.1.2 System-environment model

Suppose we have a system ρ and an environment $|e\rangle$. We have a black box which acts by a unitary matrix u on $|\psi\rangle$ and $|e\rangle$, producing ρ_{out} and some other output which is measured and then forgotten. Then the output can be written in terms of partial projections $\rho = \oplus_k\langle e_k|u|e\rangle|\psi\rangle$ where the $|e_k\rangle$are the possible outputs of the environment.

(In full generality,

$$\rho = \sum_k E_k\rho_{in}E_k^\dagger, \tag{2}$$

where, in this case $E_k = \langle e_k|u|e\rangle$.)

As an example, suppose the input state is controlles a rotation of the environment (with the environment written first). Then $U|00\rangle = |00\rangle$ and $U|01\rangle = \left[\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle\right]|1\rangle_{sys}$. $E_0 = |0\rangle\langle 0| + \cos\frac{\theta}{2}|1\rangle\langle 1|$ and $E_1 = \sin\frac{\theta}{2}|1\rangle\langle 1|$. Using eq. 2, $E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{p} \end{bmatrix}$ and $E_1 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{1-} \end{bmatrix}$, the operation elements. The final result is $\mathcal{E}(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = \begin{bmatrix} a & \sqrt{p}b \\ \sqrt{p}c & d \end{bmatrix}$, which is phase damping (and is dephasing as $p \to 0$).

As another example, we could put a CNOT at the end (environment controlling input), which allows energy exchange as well. The result is $\mathcal{E}(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = \begin{bmatrix} 1-pd & b\sqrt{p} \\ c\sqrt{p} & pd \end{bmatrix}$. This is called amplitude damping.