IAS/Park City Mathematics Series
Volume 3, 1993

Quantum Computation

Ran Raz[1]

LECTURE 2
Bipartite quantum systems

2.1. The Quantum Register

A quantum register of length n qubits is a quantum system with 2^n basic states and is the analogous of a classical register of length n bits. As before, the 2^n basic states of the register are denoted by the vectors

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \cdots\cdots\cdots \quad |2^n - 1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

The general quantum state of the register is a linear combination (i.e., superposition) of the 2^n basic states and is represented by a unit vector in the vector space $H = \mathbb{C}^{2^n}$. That is, the quantum state is

$$|c\rangle = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{2^n-1} \end{pmatrix} = \sum_{i=0}^{2^n-1} c_i |i\rangle$$

[1]Faculty of Mathematics and Computer Science, The Weizmann Institute of Science, Rehovot 76100, Israel.
E-mail address: `ranraz@wisdom.weizmann.ac.il`.

July 21, 2000

Based on lecture notes taken by Yoad Lustig.

The evolution in time is given by a unitary matrix. Note that since the matrix defines a linear transformation, it can be described by describing its operation on a base for H.

When a measurement is performed (according to the standard base), we obtain each basic state $|i\rangle$ with probability $|c_i|^2$, and the quantum state then collapses to the basic state $|i\rangle$. The collapse of the quantum state is a paradoxical concept. Einstein was bothered by the fact that the collapse is probabilistic and not deterministic as he expected nature to be. As computer scientists, we are not very much bothered by the probabilistic nature of the collapse. Still, there are many other philosophical problems like: What is a measurement ? What causes the collapse ? Can we (who perform the measurement) be considered a part of the quantum system ? etcetera. In these lectures, we will not discuss these problems.

2.2. Bipartite Quantum Systems

Let A be a quantum register of length n_1 qubits, and let B be a quantum register of length n_2 qubits. A general quantum state of the register A is a unit vector in the vector space $H_A = \mathbb{C}^{2^{n_1}}$ and a general quantum state of the register B is a unit vector in the vector space $H_B = \mathbb{C}^{2^{n_2}}$. Denote the vectors of the standard base for H_A by

$$|0\rangle_A, |1\rangle_A, ..., |2^{n_1} - 1\rangle_A,$$

and the vectors of the standard base for H_B by

$$|0\rangle_B, |1\rangle_B, ..., |2^{n_2} - 1\rangle_B.$$

The combined system is a quantum register of length $n_1 + n_2$ qubits. A general quantum state of the combined register is a unit vector in the vector space $H = \mathbb{C}^{2^{n_1+n_2}}$. The dimension of the vector space H is $2^{n_1+n_2} = 2^{n_1} \cdot 2^{n_2}$. The standard base for H is

$$\{|0\rangle_A, ..., |2^{n_1} - 1\rangle_A\} \times \{|0\rangle_B, ..., |2^{n_2} - 1\rangle_B\}.$$

Denote these $2^{n_1} \cdot 2^{n_2}$ basic states by

$$|0\rangle_A|0\rangle_B, ..., |2^{n_1} - 1\rangle_A|2^{n_2} - 1\rangle_B.$$

A general quantum state of the combined register is a linear combination (i.e., superposition) of these basic states. For example,

$$(1/\sqrt{2}) \cdot |0\rangle_A|0\rangle_B + (1/\sqrt{2}) \cdot |1\rangle_A|1\rangle_B.$$

Note that $H \neq H_A \times H_B$. In order to describe a state of the combined system, it is not enough to describe a state of A and a state of B. A state of the combined system is described by $2^{n_1} \cdot 2^{n_2}$ coordinates (and not $2^{n_1} + 2^{n_2}$ coordinates). The vector space H is called the tensor product of the two vector spaces H_A and H_B and is denoted by

$$H = H_A \otimes H_B.$$

2.3. Tensor Product of Vectors

The tensor product operation is also used to describe a certain "product" of vectors and a certain "product" of matrices. Given two vectors

$$|a\rangle_A = \sum_{i=0}^{2^{n_1}-1} a_i |i\rangle_A \in H_A$$

and

$$|b\rangle_B = \sum_{j=0}^{2^{n_2}-1} b_j |j\rangle_B \in H_B,$$

their tensor product $|a\rangle_A \otimes |b\rangle_B$ is a $2^{n_1} \cdot 2^{n_2}$ dimensional vector in $H_A \otimes H_B$. The physical intuition is that $|a\rangle_A \otimes |b\rangle_B$ describes a quantum state where A is in state $|a\rangle_A$ and B is in state $|b\rangle_B$. The formal definition of $|a\rangle_A \otimes |b\rangle_B$ is

$$|a\rangle_A \otimes |b\rangle_B = \sum_{i=0}^{2^{n_1}-1} \sum_{j=0}^{2^{n_2}-1} a_i b_j |i\rangle_A |j\rangle_B.$$

Equivalently, one can define the tensor product of two vectors by defining for base elements $|i\rangle_A, |j\rangle_B$,

$$|i\rangle_A \otimes |j\rangle_B = |i\rangle_A |j\rangle_B,$$

and requiring the tensor product to be a bi-linear operation. The tensor product $|a\rangle_A \otimes |b\rangle_B$ is many times denoted also by $|a\rangle_A |b\rangle_B$.

Most vectors in $H = H_A \otimes H_B$ are not a tensor product of a vector in H_A and a vector in H_B. This is obvious since H is of dimension $2^{n_1} \cdot 2^{n_2}$, whereas $H_A \times H_B$ is of dimension $2^{n_1} + 2^{n_2}$. States in $H_A \otimes H_B$ that cannot be written as the tensor product of a state in H_A and a state in H_B are called *entangled states*. One example is the state

$$(1/\sqrt{2}) \cdot (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B).$$

Two qubits in such a state are called *EPR pair* (Einstein-Podolsky-Rosen pair), and are the base for the famous EPR paradox.

2.4. Tensor Product of Matrices

Given two matrices

$$U_A : H_A \to H_A$$

and

$$U_B : H_B \to H_B,$$

their tensor product $U_A \otimes U_B$ is a $2^{n_1} \cdot 2^{n_2}$ dimensional matrix

$$U_A \otimes U_B : H_A \otimes H_B \to H_A \otimes H_B.$$

The physical intuition is that the matrix U_A is applied on H_A and the matrix U_B is applied on H_B. For the formal definition of $U_A \otimes U_B$, it is enough to define its operation on the standard base for $H_A \otimes H_B$ (since it is a linear operation). For a base vector $|i\rangle_A |j\rangle_B$, define

$$(U_A \otimes U_B)|i\rangle_A |j\rangle_B = (U_A |i\rangle_A) \otimes (U_B |j\rangle_B).$$

Hence, for any vector

$$|c\rangle = \sum_{ij} c_{ij} |i\rangle_A |j\rangle_B \in H,$$

we have

$$(U_A \otimes U_B)|c\rangle = \sum_{ij} c_{ij} (U_A|i\rangle_A) \otimes (U_B|j\rangle_B).$$

The matrix $U_A \otimes U_B$ can be written as

$$\left(\begin{array}{c|c|c|c} (U_A)_{0,0} \cdot U_B & (U_A)_{0,1} \cdot U_B & \cdots\cdots & (U_A)_{0,2^{n_1}-1} \cdot U_B \\ \hline \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \hline (U_A)_{2^{n_1}-1,0} \cdot U_B & (U_A)_{2^{n_1}-1,1} \cdot U_B & \cdots\cdots & (U_A)_{2^{n_1}-1,2^{n_1}-1} \cdot U_B \end{array}\right)$$

(where $(U_A)_{k,l}$ is the element in row k and column l of the matrix U_A).

For example, for the Hadamard matrix

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

we have

$$H_2 \otimes H_2 = \left(\begin{array}{rr|rr} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right)$$

2.5. Partial Measurements

Suppose that we have a bipartite quantum system as above. What happens when we measure one part of the system (say, register B) and leave the other part of the system (i.e., register A) untouched ? Suppose that the combined system is in the state

$$|c\rangle = \sum_{ij} c_{ij} |i\rangle_A |j\rangle_B = \sum_{j=0}^{2^{n_2}-1} \left(\sum_{i=0}^{2^{n_1}-1} c_{ij} |i\rangle_A \right) \otimes |j\rangle_B.$$

If we measure register B (according to the standard base) we obtain each base vector $|j\rangle_B$ with probability

$$\sum_{i=0}^{2^{n_1}-1} |c_{ij}|^2 = \left\| \sum_{i=0}^{2^{n_1}-1} c_{ij} |i\rangle_A \right\|^2,$$

and the quantum state of the combined system then collapses to the state

$$\left(\sum_{i=0}^{2^{n_1}-1} c_{ij} |i\rangle_A \right) \otimes |j\rangle_B$$

(normalized). That is, the state vector collapses to its projection on the subspace generated by the base vector $|j\rangle_B$, with probability equal to the square of the length of this projection.

For example, consider the state

$$(1/2) \cdot (|0\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B).$$

If we measure the register B, we get $|0\rangle_B$ with probability 1/2 (and then the system collapses to the state $(1/\sqrt{2})\cdot(|0\rangle_A+|1\rangle_A)\otimes|0\rangle_B)$, and we get $|1\rangle_B$ with probability 1/2 (and then the system collapses to the state $(1/\sqrt{2}) \cdot (|0\rangle_A - |1\rangle_A) \otimes |1\rangle_B)$.

2.6. The EPR Paradox

Consider the entangled state

$$(1/\sqrt{2}) \cdot (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B).$$

Suppose that we send register A to the moon and we leave register B on earth. The system is still in the same entangled state. When we measure B (on earth), we get the following results. With probability 1/2, we get $|0\rangle_B$, and the quantum state of the combined system collapses to $|0\rangle_A|0\rangle_B$. With probability 1/2, we get $|1\rangle_B$, and the quantum state of the combined system collapses to $|1\rangle_A|1\rangle_B$. Suppose that after measuring B we measure the register A (on the moon). If the result of the measurement of B was $|0\rangle_B$ the state collapsed to $|0\rangle_A|0\rangle_B$ and when we measure A we get $|0\rangle_A$ (with probability 1). At the other hand, if the result of the measurement of B was $|1\rangle_B$ the state collapsed to $|1\rangle_A|1\rangle_B$ and when we measure A we get $|1\rangle_A$.

The result of the measurement of register B (on earth) somehow passed to register A (on the moon). Note that we can measure A an arbitrary short time after measuring B. Thus, the information should pass from earth to the moon immediately, and in particular, faster than the time it takes light to pass that distance. This was considered by Einstein Podolsky and Rosen to be a paradox, that is, a flaw in the theory, as it contradicts the principle of special relativity theory that information cannot pass faster than light. A possible explanation (for the paradox) that was suggested is that maybe the results of the measurements of both registers were already determined before the registers were separated. This explanation is sometimes referred to as the theory of local hidden variables.

Experiments show that the prediction of quantum theory is correct. That is, if we measure B and then we measure A we do obtain the predicted results (as described above), even if the two measurements were done almost simultaneously and the two registers were at a distance that would make information propagation impossible (unless the propagation was faster than light). Moreover, it was proved by John Bell that if one allows measurements of A and B according to different bases (i.e., bases other than the standard ones) then it is mathematically impossible to explain the obtained results by the theory of local hidden variables. This was experimented successfully as well. The explanation for the EPR paradox is that what is passed is not exactly information, in the sense that it cannot be used to form a communication channel. Still, the EPR paradox is a dramatic demonstration for the power of the quantum measurement.

2.7. Entanglement and Interference

Consider the following example for interference. Let A be a register of one qubit in the quantum state

$$(1/\sqrt{2}) \cdot (|0\rangle_A + |1\rangle_A).$$

Apply on that state the unitary matrix

$$H_A = (1/\sqrt{2}) \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The obtained state is

$$|0\rangle_A,$$

and hence if we measure A we get $|0\rangle_A$ with probability 1. That is, interference has occurred.

Suppose now that the qubit A is entangled to another qubit B, and that the quantum state of the combined system is

$$(1/\sqrt{2}) \cdot (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B).$$

Apply on that state the unitary matrix

$$H_A \otimes I_B$$

(i.e., H_A is applied on A as before, and the identity matrix I_B is applied on B). The obtained state is

$$(1/2) \cdot (|0\rangle_A|0\rangle_B + |1\rangle_A|0\rangle_B + |0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B),$$

and hence if we measure A we get with probability $1/2$ the state $|0\rangle_A$ and with probability $1/2$ the state $|1\rangle_A$. That is, no interference has occurred.

We saw that the entanglement of A to B destroys the interference of states of A, and causes A to behave classically. This phenomena gives a partial explanation for the fact that large systems (e.g., Schroedinger's cat) usually behave classically in real life. It also demonstrates the importance of isolating a quantum computer from its environment. Think of A as (a part of) a quantum computer, and think of B as its environment. Suppose that the unitary transformation applied on the combined system is of the form $U_A \otimes U_B$, that is, a unitary transformation U_A is applied on A and a unitary transformation U_B is applied on B. It is not hard to show that if the original state of the combined system is a tensor product state $|a\rangle_A \otimes |b\rangle_B$ then we can ignore B altogether when analyzing the behavior of A. At the other hand, if the combined system is in an entangled state then the entanglement to the environment (or to another register) may destroy the interference and hence the entire quantum computation.

2.8. The No-Cloning Theorem

Let us end this lecture with a short discussion on the information of a quantum state. A classical state of n bits is described by an element in $\{0,1\}^n$, that is, by n bits of information. A quantum state of n qubits is described by an element of $\mathbb{C}^{2^n}$, that is, by 2^n elements of $\mathbb{C}$, and hence it contains an infinite amount of information. Even if we restrict the precision of each element of $\mathbb{C}$ to some limited (even constant) precision, the quantum state still contains an exponential amount of information. This is the reason that there is probably no efficient way to simulate quantum systems by classical computers. Such a simulation can be done in exponential time, but (as is evident by Shor's quantum factoring algorithm) probably cannot be done in polynomial time.

Thus, the quantum state contains an exponential amount of information (even if the state is given up to some limited precision). However, if we measure the quantum state it collapses to one of 2^n base states, and hence we obtain only n

bits of information about the original quantum state. The original quantum state is lost forever (as it collapsed), and we don't know what would have happen if we had measured that original state according to a different orthonormal base (this is the famous *uncertainty principle*). It can be proved, in a very strong sense, that although the quantum state contains an exponential amount of information, the total information that one can obtain about a given quantum state is at most n bits.

It could be suggested to duplicate a quantum state before measuring it, and then to measure it according to two different bases (and hence to obtain more than n bits of information about the original state). Given a quantum state $|c\rangle_A$ in register A and a fixed state (say, $|0\rangle_B$) in register B, one could hope to apply a (unitary) transformation U that duplicates $|c\rangle_A$ to register B and generates the state $|c\rangle_A \otimes |c\rangle_B$. That is, for any $|c\rangle_A$, the operator U should satisfy

$$U(|c\rangle_A|0\rangle_B) = |c\rangle_A|c\rangle_B.$$

The no-cloning theorem states that this cannot be done because such an operator U is not linear. The proof is very easy. Assume for a contradiction that such a linear operator exists. Then,

$$U(|0\rangle_A|0\rangle_B) = |0\rangle_A|0\rangle_B,$$

and similarly,

$$U(|1\rangle_A|0\rangle_B) = |1\rangle_A|1\rangle_B.$$

Therefore, by linearity,

$$U((|0\rangle_A + |1\rangle_A)|0\rangle_B) = (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \neq (|0\rangle_A + |1\rangle_A)(|0\rangle_B + |1\rangle_B)$$

(in contradiction to the requirement from U).