CS 294-4 Lecture 9
Notes by: Mark Pilloff April 2, 1999

Representation of Quantum Systems

A quantum system is described by specifying its *state* which is in= general an element of some complex vector space. This vector space will of= course depend on the particular system being described. For example, the= Hydrogen atom can be characterized by a vector space whose basis vectors= are states corresponding to different energies of the electron. For= simplicity we will pretend that the Hydrogen atom has only 2 such= electronic basis states: the ground state $|0\rangle$ and an excited= state $|1\rangle$. Such a 2 state system is the quantum analog of a= classical bit and is called a *qubit.*

Because this is a complex vector space the most general state can be= represented as $\alpha|0\rangle + \beta|1\rangle$, where $\alpha, = \beta \in \mathbf{C}$. Such a state is called a *superposition* of the= basis states $|0\rangle$ and $|1\rangle$ and the coefficients α and= β are the *probability amplitudes* corresponding to $|0\rangle$= and $|1\rangle$ respectively. The interpretation of such probability= amplitudes is that for a general state $|\Psi\rangle = 3D \sum_i \alpha_i = |i\rangle$, a measurement of the state of $|\Psi\rangle$ will determine= the system to be in state $|i\rangle$ with probability $|\alpha_i|^2$. = To maintain unit probabilty for the system to be in any state we thus= require that $\sum_i |\alpha_i|^2 = 3D1$ and a state satisfying this= condition is said to be properly *normalized.*

We have not yet defined what a measurement on a quantum system is or what= effect it has on such a system. In general any quantity which can be= measured is called an *observable* and is associated with a Hermitian= operator on the vector space V describing the system. (Recall that an= operator O is Hermitian if $O = 3DO^\dagger$, its conjugate transpose. = Hermiticity is required in order that measured quantities have real values,= but we shall not make explicit use of this property in these notes.) Such= an operator has a set of eigenvectors $\{|v_i\rangle\}$ with corresponding= eigenvalues $\{\lambda_i\}$ and these eigenvectors form a basis for V. = Then a mesaurement of the observable associated with operator O on state= $|\Psi\rangle = 3D \sum_i \alpha_i |v_i\rangle$ will obtain value= λ_j with probability $|\alpha_j|^2$ in accordance with the above= described interpretation of the complex coefficients as probability= amplitudes. Furthermore, the measurement irreversibly changes the state of= the system and projects it onto the subspace spanned by those eigenstates= with eigenvalue λ_j. (For the case of nondegenerate spectra there= is only one state with eigenvalue λ_j so that after a measurement= which returns the value λ_j, the state is said to have = *collapsed* to the state $|v_j\rangle$.)

The vector space V of a quantum system has an inner-product and the= inner-product of two states $|u\rangle$ and $|v\rangle$ is denoted by= $\langle u|v\rangle$. Such an inner-product allows us to conveniently= define projection operators so that the projection of state $|v\rangle$= onto $|u\rangle$ is given by $|u\rangle\langle u|v\rangle$. Thus V is in fact a Hilbert space (for infinite dimensional spaces this= means that the space is also required to be complete).

Given two quantum systems V and W with corresponding basis states= $\{|v_1\rangle, \ldots, |v_n\rangle\}$ and $\{|w_1\rangle, \ldots, = |w_m\rangle\}$ we can construct a vector space associated with the= composite system via the *tensor product* $V \otimes W$. The vector= space $V \otimes W$ has dimension nm and basis vectors of the form= $|v_i\rangle \otimes |w_j\rangle$ so that an arbitrary state may be= represented as $\sum_{i,j} \alpha_{ij} |v_i\rangle \otimes |w_j\rangle$. = The tensor product is defined to be bilinear so that, for example, $|u =\rangle \otimes |w\rangle + |v\rangle \otimes |w\rangle = 3D(|u\rangle + = |v\rangle) \otimes |w\rangle$. Furthermore it inherits an inner-product= from V and W in the natural way, $\langle v \otimes w|v' = \otimes w'\rangle = 3D\langle v|v'\rangle \cdot \langle w| = w'\rangle$.

Such a tensor product allows us to construct systems of multiple qubits by= simply taking the tensor product of two or more single qubit systems. To= return to our simple model of the Hydrogen qubit, we may imagine that we= have two such Hydrogen atoms which are tensored to form a 2-qubit system= with four states: $|00\rangle$, $|01\rangle$, $|10\rangle$, = and $|11\rangle$. Here we have adopted the conventional notation where= the tensor product state $|v_1\rangle \otimes \ldots \otimes v_k\rangle$= is abbreviated $|v_1 \ldots v_k\rangle$. Note that some states can be= factored as a single tensor product, for example,

$$\frac{1}{2}\big[= |00\rangle + |01\rangle + |10\rangle + |11\rangle\big] = 3D \frac{1}{= \sqrt{2}}\big[|0\rangle + |1\rangle\big] \otimes \frac{1}{\sqrt{2}} = \big[|0\rangle + |1\rangle\big].$$

In such a state, the 2 qubits are= independent in the sense that a measurement (and successive projection) of= one qubit does not affect the probability amplitudes corresponding to a= measurement of the second qubit.

Other states cannot be decomposed into a single tensor product, for example,=

$$\frac{1}{\sqrt{2}}\big[|00\rangle + |11\rangle\big].$$

This is an= example of one of the 4 EPR states (also known as Bell states) which have= the property of being maximally *entangled.* A measurement of the= state of one of the 2 qubits uniquely and fully determines the outcome of a= measurement on the other qubit. To see this, suppose that a measurement of= the first qubit finds it to be in state $|0\rangle$. Then the resulting= state of the system must be equal to the projection of the initial state= onto the subspace with first qubit equal to $|0\rangle$. Obviously this= means that the new state is $|00\rangle$ and thus any successive= measurement of the state of either qubit will always find it to be in state= $|0\rangle$.

Note that this outcome is consistent with our earlier description that the= effect of a measurement (with an associated Hermitian operator= corresponding to the observable being measured) is to project onto the= subspace spanned by the eigenstates of this operator with eigenvalue equal= to the measurement result. Specifically, let us denote by O_i the= operator whose eigenstates $|0\rangle$ and $|1\rangle$ describe the state= of the i^{th} qubit. Then a measurement of the first qubit is associated= with the operator $O_1 \otimes \mathbf{1}_2$ where $\mathbf{1}_2$ is the identity= operator on the second qubit. Note that the eigenstates of this operator= come in degenerate pairs, $\{|00\rangle, |01\rangle\}$ with eigenvalue= λ_0, and $\{|10\rangle, |11\rangle\}$ with eigenvalue= λ_1. Thus if we measure the first qubit to be in state $|0 =\rangle$ (that is, the result of the measurement is λ_0) we must= project onto the first of these two subspaces, and if we measure the first= qubit to be in state $|1\rangle$ we must project onto the second= subspace.

Such entangled states provoke an interesting paradox named the EPR paradox= for its inventors, Einstein, Podolsky, and Rosen. Suppose that some= experiment produces two particles which are in an entangled state such as= the EPR state shown above. (In practice, these entangled states are= readily produced. For example, the states $|0\rangle$ and $|1\rangle$ may= correspond to different directions of angular momentum. Then the EPR= states occur naturally as a result of conservation of this angular= momentum.) The seeming paradox in such an experiment is that the two= particles can travel a great distance in opposite directions, each existing= as an entangled component of the overall state, but as soon as a= measurement is made on particle 1, the state of particle 2 becomes known= instantly. According to the cherished theory of relativity, no information= can propagate faster than the speed of light and yet particle 2 seems to= instantly know that particle 1 has been measured (and even the result of= that measurement).

The resolution of this paradox (at least with respect to the theory of= relativity) is that such an effect does not allow the exchange of any= imformation. If two observers are far apart and each receives one particle= of an EPR pair, then observer 1 may choose whether or not to measure the= state of his particle, but there is no measurement which observer 2 can= perform that will give her any information about what observer 1 has done. = In particular, observer 2 will still measure a seemingly random= distribution of values for the state of her particle and it is not until= she compares her data with observer 1 that they will be able to see the= correlations between their measurements. Thus unless the two observers= compare their data via standard, slower-than-light communication, they= cannot exchange any information at all.

Of course such a paradox would not arise in the first place if we could= dispense with the idea that the most complete description of a state is= probabilisitic in nature. Perhaps the two particles are created in either= the pure state $|00\rangle$ or the pure state $|11\rangle$, each with= probability 1/2, but we simply don't have enough knowledge about our= experiment to distinguish between these two. In other words, the system is= in a definite state but our incomplete control over the experiment only= allows us to give a probability distribution for the actual state.

This issue was addressed by Bell in 1964 who showed that there is an= experimentally testable phenomenon which allows one to distinquish the two= cases where, (1) the true state of the system is a superposition (as in the= EPR states) and=20each particle's state is only determined after a= measurement of either particle, or (2) the true state of the system is a= pure, unentangled eigenstate and each particle's state is completely= determined at creation. Tests based on Bell's idea have consistently shown= that case (1) is the proper description of reality, hence outlawing the= notion that each particle has its own *local variables*—entanglement= is a fundamental feature of quantum mechanics.

Finally, we note the following very important distinction between qubits and= classical bits. Consider a pair of classical systems V and W= characterized by m and n bits respectively. Then the composite system= $V \oplus W$ has dimension $n + m$ and its state is specified by giving the= state of the $n + m$ total bits in the system. In other words, storage= capacity in classical bit systems is additive.

On the other hand, given equivalent quantum systems V and W combined to= form the composite

space $V \otimes W$, this new system has dimension $n = \cdot m$. Thus, for example, the state of n qubits is a unit vector in= the space $\mathbf{C}^2 \otimes \mathbf{C}^2 \otimes \cdots \otimes \mathbf{C}^2 =$ (n times) which has dimension 2^n. Because quantum systems allow for= the existence of *correlated,* entangled states where the state of one= particle is dependent upon the state of the others, storage capacity in a= set of qubits is multiplicative. Wouldn't it be nice if two 16Mb SIMMs= provided 256,000Gb of storage?

Operations on Quantum Systems

Before we can discuss quantum computation or quantum algorithms, we must= specify what operations can be performed on a quantum system. Recall that= a system is associated with a Hilbert space H and a state of this system= corresponds to a unit vector $|v\rangle \in H$. Frequently it will be= useful to resort to a matrix representation of this space so that, for= example, the state $\alpha|0\rangle + \beta|1\rangle$ corresponds to the= vector $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$. Similarly, an operator on this space= is represented by a 2x2 matrix.

In order to maintain unit total probability, an operator on H must= preserve inner-products and thus be unitary (recall that an operator O is= unitary if $O^\dagger = 3DO^{-1}$). We will therefore require that all= operators representing the evolution of states in H be unitary. A= general unitary operator on $\mathbf{C}^{2^n}$ has the form $U = 3DU_1 = \otimes \cdots \otimes U_n$ (or a linear combination of such terms) where= each U_i is a unitary operator on a single qubit space. Furthermore, in= order to work with operations that are physically realizable, we will= restrict our attention to those operators U where all but a small= (constant) number of the U_i operators are the identity operator $= \mathbf{1}_i$.

How do we obtain the matrix representation of an inner product of operators?= Consider a two qubit system $\mathbf{C}^2 \otimes \mathbf{C}^2$ and the unitary= operator $U_1 \otimes U_2$ where U_1 is a rotation parametrized by angle= θ,

$$U_1 = 3D \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta = & \cos\theta \end{pmatrix},$$

and U_2 is a simple reflection,

$$U_2 = 3D \begin{pmatrix} 0 = & 1 \\ 1 & 0 \end{pmatrix}.$$

Then $U_1 \otimes U_2$ is a 4x4 matrix of the form

$$U_1 \otimes U_2 = 3D \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \end{array} \\ \begin{pmatrix} 0 & \cos\theta & 0 & \sin\theta \\ \cos\theta & 0 & \sin\theta & 0 \\ 0 & -\sin\theta & 0 & \cos\theta \\ -\sin\theta & 0 & \cos\theta & 0 \end{pmatrix} \end{array}$$

obtained by multiplying each *element* of U_1 by the entire matrix= U_2. Since the form of this matrix depends on the basis chosen, in= particular, on the order in which we list the two-qubit states, we have= also explicitly indicated the basis states in the matrix representation= above. Finally, note that the outer-product $|i\rangle\langle j|$ is in= fact an operator on H whose value on the state $|v\rangle$ is given by= $|i\rangle\langle j|v\rangle$. This allows us to view the= matrix-representation of the above operator as a linear combination of 16= such outer products, each weighted by the appropriate matrix entry.

In general a computation will be described by a succession of unitary= operators, $U_{QC} = 3DU_1U_2 \ldots U_T$ where each U_J denotes a= unitary operator on the entire space of qubits. However, as noted above,= we will impose the practical constraint that each U_J is nontrivial on at= most two qubits. Thus each U_J can be thought of as an elementary= quantum gate.

It is a fact that an arbitrary unitary transformation can be= ϵ-approximated by poly(d) many such U_J operators in time= poly$(d, \log\frac{1}{\epsilon})$ where d is the dimension of the= n-qubit Hilbert space. But since $d = 3D2^n$ is exponential in the= number of qubits, we are really interested in those transformations which= can be realized in poly($\log d$) =3D poly(n) operations.

The first such transformation computable in poly($\log d$) operations is a= relabelling (or permutation) of the basis vectors. This can in fact be= done efficiently by classical computation and therefore by quantum= computation as well since Bennett has shown that P =3D reversible-P.

The Fourier transform is also computable in poly($\log d$) operations. = Observe that a qubit state $\phi \in \mathbf{C}^2$ may be regarded as a= function $f_\phi : \mathbf{Z}_2 \to \mathbf{C}$ where the value of= f_ϕ on $\{0,1\}$ is given by the complex coefficient of the respective= basis state $\{|0\rangle, |1\rangle\}$. Thus the Fourier transform $\hat{=} f_\phi : \mathbf{Z}_2 \to \mathbf{C}$ can be represented by an= appropriate transformation of the state ϕ. The necessary transformation is readily seen to be

$$H_2 = 3D \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

which correctly implies that $\hat{f}(0) = 3D\frac{1}{\sqrt{2}}[f(0) + = f(1)]$ and $\hat{f}(1) = 3D\frac{1}{\sqrt{2}}[f(0) - f(1)]$.

We may similarly associate functions $f : \mathbf{Z}_2^n \to \mathbf{C}=$ with n-qubit states $\phi \in \mathbf{C}^{2^n}$. Then the Fourier transform= $\hat{f}$ is be computed by applying to ϕ the unitary operator= H_{2^n}. It can be proven (and is easily seen to be true by example)= that H_{2^n} is the tensor product of n copies of H_2 above, =

$$H_{2^n} = 3DH_2 \otimes H_2 \otimes \cdots \otimes H_2.$$

Thus the= n-qubit Fourier transform can be computed by performing n single-qubit= operations [ref. BBCDMSSSW].