Recent advances in Complexity CIS 6930/CIS 4930	December 3, 2002

Lecture 28

Lecturer: Dr. Meera Sitharam — Scribe: Hongyu Guo

Hongyu's Talk on Quantum Computing

1 The Model of Quantum Computing

Notions and Definitions

Hilbert space We discuss quantum mechanics in the context of Hilbert space over a complex field. A Hilbert space H is a linear space (can be infinite dimensional) with an inner product defined. The space is complete w.r.t. the norm induced by the inner product. By complete we mean every Cauchy sequence of points in H has a limit in H. In the context of quantum computing, usually we need only finite dimensional spaces.

Hermitian Operator A Hermitian Operator A in a Hilbert space is a linear transformation, such that $\forall \Psi, \Phi \in H, (A\Psi)^* \cdot \Phi = \Psi \cdot (A\Phi)$. Or alternatively, $A = A^\dagger$, where $A^\dagger$ is the Hermitian conjugate of A. In a finite dimensional space, an operator is represented by a matrix. The Hermitian conjugate of matrix A is defined as the complex conjugate of the tranpose of A, namely $A^\dagger = (A')^*$. We know that Hermitian operators have real eigenvalues.

Unitary Operator A unitary operator U in a Hilbert space H is a linear transformation that preserves the length of the vector, namely $\forall \Psi \in H, ||U\Psi|| = ||\Psi||$. Or equivalently, $U^{-1} = U^\dagger$.

Dirac Notation Use a ket $|\Psi>$ to denote a vector in the Hilbert space. Bra $<\Phi|$ denotes a vector in the dual space. A bra-ket denotes the inner product: $<\Phi|\Psi>$. A ket-bra $|\Psi><\Phi|$ is an operator. Notice that $I = \sum_k |k><k|$ is an identity operator, where $\{|k>\}$ is a set of complete basis. This is a very useful property.

With the notions and definitions introduced above, we state (a subset of) the axioms of quantum mechanics:

Axiom 1 The state of a physical system is represented by a vector $|\Psi>, where <\Psi|\Psi>= 1$, in a Hilbert space over complex field C.

Axiom 2 Physical quantities (observables) are represented by Hermitian operators in the Hilbert space.

Axiom 3 Let $\hat{F}$ be the Hermitian operator representing observable F. $|\Phi_n>, n = 1, 2, ...$ is a set of orthonormal eigenvectors of $\hat{F}$ with $\lambda_n, n = 1, 2, ...$ being the corresponding eigenvalues. If the system is in state $|\Psi >= \sum_n c_n|\Phi_n >$, then in the measurement, the probability F gets value λ_n is $|c_n|^2$.

Axiom 4 The time evolution of the state is described by the Shrödinger equation:

$$i\hbar\frac{\partial}{\partial t}|\Psi >= H_0|\Psi >,$$

where H_0 is the Hamiltonian operator.

The state at time $t, |\Psi(t) >$, is the result of applying a unitary operator on the initial state, $|\Psi(t) >= U(t)|\Psi(0) >$. There is always an inverse for a unitary operator U. So quantum computing is reversible while classical circuit logic computing is not reversible. We compute $a \wedge b$, then we are not able to recover a and b from the result $a \wedge b$.

Example 1 *Spin* $\frac{1}{2}$

$S_x = \frac{\hbar}{2}\sigma_x,\ S_y = \frac{\hbar}{2}\sigma_y,\ S_z = \frac{\hbar}{2}\sigma_x,$

where $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},\ \sigma_x = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, *are Pauli matrices.*

They all have eigenvalues 1 and -1.

Qubit and Tensor Product

We use "qubit" to denote quantum bit. To represent 1 qubit, we can use a system with two eigenstates, $|0>$ and $|1>$. The state space is C^2. To represent n qubits, we use n such systems and the state space is the tensor product $C^2 \otimes \cdots \otimes C^2$.

A state in this space can be written as
$|\Psi >= \sum_{x_1,\ldots,x_n} c_{x_1,\ldots,x_n}|x_1, ..., x_n >$,
where $|x_1, ..., x_n >= |x_1 > \otimes \cdots \otimes |x_n >$, and $\sum_{x_1,\ldots,x_n} |c_{x_1,\ldots,x_n}|^2 = 1$. This is a superposition of all 2^n states. By applying an operator on $|\Psi >$, we actually operate on all the 2^n strings at the same time. The strategy of quantum computing is then to take advantage of superposition, which enables us to calculate the value of a funciton at all 2^n integers simultaneously, while avoiding premature measurements which destroy the superposition.