CS682: Quantum Computing	Spring 2007
Lecture 02, 03 — January 2, 4	
Lecturer: Piyush P. Kurur	*Scribe: Manu Bansal*

With that very broad overview to Quantum Computing and how it fits in the bigger picture of science and engineering, we now introduce the Dirac notation and develop the mathematical machinery for the subject, including a background in Linear Algebra.

2.1 Dirac Notation

The notation is listed here, with linear algebraic definitions in the next section, so that the linear algebra could be presented in Dirac notation itself.

$\|\psi\rangle$	Vector. Called ket-ψ.
$\langle\psi\|$	Vector dual to $\langle\psi\|$. Called bra-ψ.
$\langle\phi\|\psi\rangle$	Inner product between the vectors $\|\phi\rangle$ and $\|\psi\rangle$.
$\|\phi\rangle \otimes \|\psi\rangle$	Tensor product of $\|\phi\rangle$ and $\|\psi\rangle$.
$\|\phi\rangle\|\psi\rangle, \|\phi\psi\rangle$	Abbreviations for $\|\phi\rangle \otimes \|\psi\rangle$.
$\langle\phi\|A\|\psi\rangle$	Inner product between $\|\phi\rangle$ and $A\|\psi\rangle$.
$\|\phi\rangle\langle\psi\|$	Outer product. An operator.
$A^\dagger$	Adjoint of A.

Table 2.1. Dirac Notation

2.2 Hilbert Spaces

The basic objects of linear algebra are vector spaces. Familiarity with vector spaces is assumed. A vector space is defined over a field, which in this course will usually be the field of complex numbers $\mathbb{C}$.

2.2.1 Linear Functionals

Definition 1. *For vector spaces V and W over a field F,* a linear transformation $T : V \to W$ *is a function s.t.*

$$T(c|\alpha\rangle + |\beta\rangle) = c(T|\alpha\rangle) + T|\beta\rangle$$

for all vectors $|\alpha\rangle, |\beta\rangle \in V$ and all scalars $c \in F$. A linear transformation from V into V is a linear operator.

Definition 2. *A linear transformation T from a vector space V over F into the scalar field F is a* linear functional.

An important example of a linear functional is the trace function on a matrix, which is a linear functional on the matrix space F^{nxn}.

Definition 3. *For an nxn matrix A with entries from field F, the* trace *is*

$$trace(A) = \sum_{i=1}^{n} A_{ii},$$

Definition 4. *The* dual space *V^* of a vector space V is the collection of all linear functionals on V, which itself is a vector space in a natural way (i.e., with the natural definitions of vector addition and scalar multiplication in V^*).*

For a finite-dimensional vector space V, the dual space V^* is of the same dimension as V. Even more, the two are isomorphic. The isomorphism itself depends on the bases in the two vector spaces. An invariant isomorphism using inner products will be described ahead.

2.2.2 Inner-products

Definition 5. *An* inner product *$\langle\cdot|\cdot\rangle$ on a vector space V (over a field F) is a function mapping a pair of vectors to a scalar, satisfying the following:*

1. $\langle x|y\rangle = \overline{\langle y|x\rangle}$
2. $\langle x|\alpha y + \beta z\rangle = \alpha\langle x|y\rangle + \beta\langle x|z\rangle$
3. $\langle x|x\rangle \geq 0$ *and equality holds when $x = 0$ ((1) $\Rightarrow$ $\langle x|x\rangle$ is real. So this property is well-defined).*
4. $\langle \alpha x|y\rangle = \overline{\alpha}\langle x|y\rangle$.

The notation we adopt for inner products is the Physics notation, which is different from the Mathematics notation in that the inner product is linear in the second argument while sesqui-linear in the first argument.

2.2.3 Hilbert Spaces

Definition 6. *A vector space in which an inner product is defined is an* inner product space. *A finite-dimensional inner product space is also a* Hilbert space.

Infinite-dimensional Hilbert spaces have further properties, but we shall only deal with finite-dimensional Hilbert spaces in this course. A Hilbert space will be denoted by $\mathcal{H}$, and would generally be $\mathbb{C}$. The dual of a Hilbert space will be denoted by $\mathcal{H}^*$. Hilbert spaces are the basic objects in Quantum Computing.

With an inner product in the Hilbert space, we can know define the isomorphism between $\mathcal{H}$ and $\mathcal{H}^*$ in a bases-invariant manner: for a vector $|v\rangle$, define the dual vector $\langle v|$ (a linear functional) by

$$\langle v|(|w\rangle) \equiv \langle v|w\rangle$$

For $\mathcal{H}$ to be $\mathbb{C}^n$, we choose the standard inner product defined by

$$\langle v|w\rangle = \sum_{i=1}^{n} v_i^* w_i = \begin{bmatrix} v_1^* & \dots & v_n^* \end{bmatrix} \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}$$

which leads to a convenient matrix representation of the operator $\langle v|$, which has not yet been explicitly defined:

$$\langle v| = \begin{bmatrix} v_1^* & \dots & v_n^* \end{bmatrix}.$$

2.3 Linear Operators

2.3.1 Linear Operators over $\mathcal{H}$

Using the inner product, an *outer product* notation is defined for operators:

$$(|v\rangle\langle u|)(|w\rangle) \equiv |v\rangle\langle u|w\rangle = \langle u|w\rangle|v\rangle.$$

It is easily verified that this defines a linear transformation from the Hilbert space U containing $|u\rangle$ (and $|w\rangle$) to the Hilbert space V containing $|v\rangle$ for any $|u\rangle$ and $|v\rangle$, and a linear operator when the two spaces are same. The converse is also true, that any linear transformation can be expressed in the outer-product: if $|v_i\rangle$ is a basis of V and $|u_i\rangle$ a basis of U, then

$$A = \sum_{ij} \langle v_j|A|u_i\rangle |v_j\rangle\langle u_i|.$$

A useful interpretation of the outer-product notation is that $|b\rangle\langle a|$ is an operator that maps $|a\rangle$ to $|b\rangle$ if $|a\rangle$ is of unit norm.

2.3.2 Adjoint of an Operator

Definition 7. *In a Hilbert space $\mathcal{H}$, the* adjoint A^* *of an operator A is defined by*

$$\langle u|Av\rangle = \langle A^* u|v\rangle.$$

For the choice of standard inner product, adjoint is same as conjugate-transpose. The collection of operators over $\mathcal{H}$ is denoted by $\beta(\mathcal{H})$. For $\mathcal{H} = \mathbb{C}^n$, $\beta(\mathcal{H}) = M_{nxn}(\mathbb{C})$, the collection of all nxn matrices over $\mathbb{C}$, which is a vector space.

2.3.3 Normal, Unitary and Hermitian Operators

Definition 8. *An operator A is* normal *if $A^\dagger A = AA^\dagger$.*

Definition 9. *An operator A is* unitary *if $A^\dagger A = AA^\dagger = I$.*

Definition 10. *An operator A is* Hermitian *if $A^\dagger = A$.*

2.3.4 Eigenvectors, Eigenvalues

Definition 11. *An* eigenvector *of an operator A is a non-zero vector $|x\rangle$ such that $A|x\rangle = \lambda|x\rangle$ for a scalar λ, called the* eigen value *corresponding to the eigenvector $|x\rangle$.*

Theorem 2.1. *All eigenvalues of a Hermitian operator are real.*

Theorem 2.2. *All eigenvalues of a unitary operator have modulus 1, equivalently they lie on a unit circle.*

Theorem 2.3. *On a finite-dimensional complex inner product space V, for a normal operator A, there exists an orthonormal basis for V each vector of which is an eigenvector of A.*

2.3.5 Projections

Definition 12. *A* projection *E of vector space V is an operator on V s.t. $E^2 = E$. An* orthogonal projection *is one whose range space and null space are orthogonal.*

A projection is orthogonal iff it is Hermitian.

Lemma 2.4. *For a projection E on V with range space R and null space N, $V = R \oplus N$, the direct sum of R and N.*

Lemma 2.5. *If R and N are subspaces of V s.t. $R \oplus N = V$, then there exists a unique projection E with range space R and null space N.*

Theorem 2.6. *If $V = W_1 \oplus \ldots \oplus W_k$, then there exist k projections $E_1, \ldots, E_k$ s.t.*

$$E_i E_j = 0 \quad \text{if } i \neq j \tag{2.1}$$

$$I = E_1 + \ldots + E_k \tag{2.2}$$

$$\mathbb{R}(E_i) = W_i \tag{2.3}$$

where $\mathbb{R}(E_i)$ is the range space of E_i. By the above lemma, these projections are unique. The converse is also true, i.e., for projections satisfying 2.1-2.3, V is the direct sum of their range spaces.

Putting these together, we have the Spectral Theorem.

2.3.6 Spectral Theorem

Theorem 2.7. *Let A be a normal operator on a finite-dimensional complex inner product space V (or a self-adjoint (Hermitian) operator on a finite-dimensional real inner product space V). Let λ_i's be the distinct eigenvalues of A. Let W_i be the eigenspace associated with λ_i and E_i the orthogonal projection of V on W_i. Then W_i is orthogonal to W_j when $i \neq j$, V is the direct sum of W_i's, and*

$$A = \lambda_1 E_1 + \lambda_1 E_2 + \ldots + \lambda_1 E_k.$$

References

- Hoffman and Kunze, Linear Algebra, Second Edition, Sec. 6.2, 8.5, 6.6
- Nielsen and Chuang, Quantum Computation and Quantum Information, Sec 2.1.