Lecture 3: Operators in quantum computing

Rajat Mittal

IIT Kanpur

We saw that the states of a quantum system can be described as a vector. We also looked at linear operators on these vectors. This lecture will extend our understanding of these linear operators and mention postulate which specifies the operators allowed in quantum computing.

Let us consider a toy problem, called *Deutsch's Problem*. Suppose you are given a subroutine to compute a one-bit function $f : \{0,1\} \to \{0,1\}$. We need to find whether $f(0) = f(1)$ using minimum number of queries to the subroutine. It is easy to find the solution if we can query the subroutine twice, once for $f(0)$ and once for $f(1)$. The question is, can we do it with just one query?

Using the property of superposition, it might seem like we can do it with one query on a quantum computer. Just create $|+\rangle$ state, apply subroutine on it (linearly) and then we will have both $f(0)$ as well as $f(1)$. The idea doesn't work directly, but still we can find whether $f(0) = f(1)$ in just one query on a quantum computer!

To understand why the simple idea doesn't work and how to modify it, we need to learn the 2nd and 3rd postulate (how to operate on state and how to get output from them). Though, even before that, we need to look at some linear algebra concepts.

1 Eigenvalues and eigenvectors

You must have seen the content of this section in previous courses. The content given here is meant as a refresher. If you do not feel comfortable with this material, please refer to any standard textbook on linear algebra (e.g. [1]).

Let V, W be two vectors spaces over complex numbers. For simplicity, you can assume them to be $\mathbb{C}^n$ and $\mathbb{C}^m$. A matrix $M \in L(V,W)$ is square if $dim(V) = dim(W)(m = n)$. In particular, a matrix $M \in L(V)$ is always square. For a matrix $M \in L(V)$, a vector $v \in V$ satisfying,

$$Mv = \lambda v \text{ for some } \lambda \in \mathbb{C},$$

is called the *eigenvector* of matrix M with *eigenvalue* λ.

Exercise 1. Given two eigenvectors v, w, when is their linear combination an eigenvector itself?

The previous exercise can be used to show that all the eigenvectors corresponding to a particular eigenvalue form a subspace. This subspace is called the *eigenspace* of the corresponding eigenvalue.

An eigenvalue λ of an $n \times n$ matrix M satisfies the equation

$$Det(\lambda I - M) = 0,$$

where $Det(M)$ denotes the determinant of the matrix M. The polynomial $Det(\lambda I - M) = 0$, in λ, is called the *characteristic polynomial* of M. The characteristic polynomial has degree n and will have n roots in the field of complex numbers. Though, these roots might not be real.

Exercise 2. Give an example of a matrix with no real eigenvalue.

The next theorem shows that the eigenvalues are preserved under the action of a full rank matrix.

Theorem 1. *Given a matrix P of full rank, matrix M and matrix $P^{-1}MP$ have the same set of eigenvalues.*

Proof (Extra reading). Suppose λ is an eigenvalue of $P^{-1}MP$, we need to show that it is an eigenvalue for M too. Say λ is an eigenvalue with eigenvector v. Then,

$$P^{-1}MPv = \lambda v \Rightarrow M(Pv) = \lambda Pv.$$

Hence Pv is an eigenvector with eigenvalue λ.

The opposite direction follows similarly. Given an eigenvector v of M, it can be shown that $P^{-1}v$ is an eigenvector of $P^{-1}MP$.

$$P^{-1}MP(P^{-1}v) = P^{-1}Mv = \lambda P^{-1}v$$

Hence proved. □

Exercise 3. Where did we use the fact that P is a full rank matrix?

Exercise 4. Consider the matrix representation of the operator which takes $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ to $|0\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ to $|1\rangle$. What are its eigenvalues and eigenvectors?

Pauli matrices are used widely in quantum computing. They are defined as,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Exercise 5. What is the action of X gate on standard basis?

Notice that $|u\rangle\langle v|$ is uv^* and is a matrix. On the other hand $\langle u||v\rangle$ is u^*v, giving a scalar; we write it succinctly as $\langle u|v\rangle$.

Exercise 6. Show that any matrix can be written as $\sum_i |u_i\rangle\langle v_i|$, for any orthogonal basis u_i's by choosing v_i's carefully.

Notice that Pauli X can be written as $|0\rangle\langle 1| + |1\rangle\langle 0|$. Dirac notation allows us to compute the action of X easily.

$$(|0\rangle\langle 1| + |1\rangle\langle 0|)|0\rangle = |0\rangle\langle 1|0\rangle + |1\rangle\langle 0|0\rangle = |1\rangle.$$

Where we get the last step because $\langle 1|0\rangle = 0$ and $\langle 0|0\rangle = 1$. You can similarly see that $X|1\rangle = |0\rangle$; X is known as the quantum NOT gate.

Exercise 7. Show that $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$.

Z is known as the phase gate as it puts a phase of -1 in front of state $|1\rangle$.

Before we go further, let us look at another useful notation. Given a square $n \times n$ matrix M and two vectors $u, v \in \mathbb{C}^n$,

$$\langle u|M|v\rangle := u^*Mv = \langle u|Mv\rangle = \langle M^*u|v\rangle.$$

Exercise 8. Show that $\langle u|M|v\rangle = M \bullet |u\rangle\langle v|$, where $\bullet$ is the sum of the entry-wise product of the matrices.

1.1 Spectral decomposition

Exercise 9. Let v_1, v_2 be two eigenvectors of a matrix M with distinct eigenvalues. Show that these two eigenvectors are linearly independent.

Given an $n \times n$ matrix M, it need not have n linearly independent eigenvectors. Can it have more than n linearly independent eigenvectors? The matrix M is called *diagonalizable* iff the set of eigenvectors of M span the complete space $\mathbb{C}^n$. Let P be the matrix whose columns are n linearly independent eigenvectors, then $P^{-1}MP$ will be a diagonal matrix. By Theorem 1, our original matrix and this diagonal matrix will have same eigenvalues.

Exercise 10. What are the eigenvalues and eigenvectors of a diagonal matrix?

For a diagonalizable matrix, the basis of eigenvectors need not be an orthonormal basis. We will show a characterization of matrices whose eigenvectors can form an orthonormal basis. Fortunately, these matrices are of great importance in quantum computing, and are called *normal* matrices.

A *normal* matrix is defined to be a matrix M, s.t., $MM^* = M^*M$. Spectral theorem shows that we can form an orthonormal basis of $\mathbb{C}^n$ using the eigenvectors of a normal matrix. *Spectral theorem* allows us to view a normal matrix in terms of its eigenvalues and eigenvectors.

Theorem 2 (Spectral theorem). *For a normal matrix $M \in L(\mathbb{C}^k)$, there exists an orthonormal basis $\{|x_1\rangle, \cdots, |x_k\rangle\}$ of $\mathbb{C}^k$ and $\lambda_i \in \mathbb{C}$ $(\forall i \in [k])$ such that*

$$M = \sum_{i=1}^{n} \lambda_i |x_i\rangle\langle x_i|.$$

Exercise 11. Show that $|x_i\rangle$ is an eigenvector of M with eigenvalue λ_i.

Before the proof, let us discuss implications of Spectral theorem. It means that any normal matrix $M = U^*DU$ for a diagonal matrix D with entries λ_i and the matrix U with $|x_i\rangle$ as columns. So, under a basis change (columns of U are orthonormal), a normal matrix is similar to a diagonal matrix. Since diagonal matrices are simple and easier to deal with, many properties of diagonal matrices can be *lifted* to normal matrices.

Note 1. $\langle y|x\rangle$ is a scalar, but $|y\rangle\langle x|$ is a matrix. Also, the λ_i's need not be different. If we collect all the $|x_i\rangle$'s corresponding to a particular eigenvalue λ, the space spanned by those $|x_i\rangle$'s is the eigenspace of λ.

Proof idea (Extra reading). The proof of spectral theorem essentially hinges on the following lemma.

Lemma 1. *Given an eigenspace S (of eigenvalue λ) for a normal matrix M, then M acts on the space S and $S^\perp$ separately. In other words, $M|v\rangle \in S$ if $|v\rangle \in S$ and $M|v\rangle \in S^\perp$ if $|v\rangle \in S^\perp$.*

Proof of lemma. Since S is an eigenspace, $M|v\rangle \in S$ if $|v\rangle \in S$. For a vector $|v\rangle \in S$,

$$MM^*|v\rangle = M^*M|v\rangle = \lambda M^*|v\rangle.$$

This shows that M^* preserves the subspace S. Suppose $|v_1\rangle \in S^\perp$ and $|v_2\rangle \in S$, then $M^*|v_2\rangle \in S$. So,

$$0 = \langle v_1|M^*|v_2\rangle = \langle Mv_1|v_2\rangle.$$

Above equation implies $M|v_1\rangle \in S^\perp$. Hence, matrix M acts separately on S and $S^\perp$. □

The lemma implies that M is a linear operator on $S^\perp$, i.e., it moves every element of $S^\perp$ to an element in $S^\perp$ linearly. It can be easily shown that this linear operator (the action of M on $S^\perp$) is also normal. The proof of spectral theorem follows by using induction and is given below.

From the fundamental theorem of Algebra, there is at least one root λ_0 of $det(\lambda I - M) = 0$. Start with the eigenspace of the eigenvalue λ_0. Using Lem. 1, we can restrict the matrix to orthogonal subspace (which is of smaller dimension). We can divide the entire space into orthogonal eigenspaces by induction.

Exercise 12. Show that if we take the orthonormal basis of all these eigenspaces, then we get the required decomposition.

Exercise 13. Given the spectral decomposition of M, what is the spectral decomposition of M^*?

□

Exercise 14. What is the spectral decomposition of Identity matrix?

Exercise 15. If M is normal, prove that the rank of M is the sum of the dimension of the non-zero eigenspaces.

Exercise 16. Let spectral decomposition of M be $\sum_i \lambda_i |x_i\rangle\langle x_i|$ and $v = \sum_i \alpha_i |x_i\rangle$. Find $\langle u|M|v\rangle$ in terms of λ_i, x_i, α_i.

It is easy to show that any matrix with orthonormal set of eigenvectors is a normal matrix. Hence, spectral decomposition provides another characterization of normal matrices.

Clearly the spectral decomposition is not unique (essentially because of the multiplicity of eigenvalues). But the eigenspaces corresponding to each eigenvalue are fixed. So there is a unique decomposition in terms of eigenspaces and then any orthonormal basis of these eigenspaces can be chosen.

Note 2. It is also true that if an eigenvalue is a root of characteristic polynomial with multiplicity k, then its eigenspace is of dimension k.

Spectral decomposition allows us to define functions over normal matrices.

1.2 Functions on operators

Operator functions: The first notion is of applying a function on a linear operator. We will assume that the linear operators given to us belong to the set of normal operators or some subset of it. Suppose we have a function, $f : \mathbb{C} \to \mathbb{C}$, from complex numbers to complex numbers. It can naturally extended to be a function on a normal linear operator in $L(\mathbb{C}^n)$. By definition of operator function, we apply the function on all the eigenvalues of the operator. So, if

$$A = \lambda_1 |x_1\rangle\langle x_1| + \cdots + \lambda_n |x_n\rangle\langle x_n|.$$

then

$$f(A) = f(\lambda_1)|x_n\rangle\langle x_n| + \cdots + f(\lambda_n)|x_n\rangle\langle x_n|.$$

In particular, we can now define the square-root, exponential and logarithm of an operator.

Exercise 17. Find e^{iX}, e^{iY}, e^{iZ}; where X, Y, Z are Pauli matrices.

Extra reading: Trace Another very important function on operators introduced before is *trace*. We defined trace to be $Tr(A) = \sum_i A_{ii}$. At this point, it is a function on matrices and not linear operators.

Exercise 18. What is the problem?

For a linear operator, trace might be different for different bases. In other words, there is no guarantee that it is independent of the basis (from the definition given above).

Exercise 19. Show that the trace is cyclic, i.e., $tr(AB) = tr(BA)$.

This exercise implies that $tr(U^*AU) = tr(A)$. Hence, trace is independent of the representation.

Exercise 20. Show that $tr(|u\rangle\langle v|) = \langle u|v\rangle$.

If $M = \sum_{i=1}^n \lambda_i |x_i\rangle\langle x_i|$, the previous exercise shows that $tr(M) = \sum_i \lambda_i$. Since λ_i's do not depend on the basis chosen, this gives us a basis independent definition of trace. This definition allows us to define trace of a linear operator (and not just a matrix).

We also know that $\langle v|A|w\rangle = \sum_{ij} A_{ij} v_i^* w_j$.

Exercise 21. Show that $A_{ij} = \langle i|A|j\rangle$, where matrix A is represented in the standard basis $|1\rangle, \cdots, |n\rangle$.

From the previous exercise, $tr(A) = \sum_i \langle i|A|i\rangle$. In fact, for any orthonormal basis $v_1, \cdots, v_n$,

$$tr(A) = \sum_i \langle v_i|A|v_i\rangle,$$

(trace is indepedent of the basis).

If we take v_i to be the eigenvectors, we get the same equation

$$tr(A) = \sum_i \lambda_i.$$

Here, λ_i are the eigenvalues of the operator A.

2 Special class of matrices

We know that all eigenvalues of a normal matrix are complex numbers. We can pick any set of complex numbers and an orthonormal basis, that will give us a normal matrix. Why?

If we impose more constraints on the eigenvalues, it give us specific classes of normal matrices (some of them are very important for quantum computing).

2.1 Hermitian matrix

A matrix M is said to be *Hermitian* if $M = M^*$ (analog of symmetric matrices). It is easy to check that any Hermitian matrix is normal. You can also show that all the eigenvalues of a Hermitian matrix are real (given as an exercise).

Conversely if all the eigenvalues are real for a normal matrix then the matrix is Hermitian (from spectral theorem).

Note 3. In quantum meachanics, we use eigenvalues to denote the physical properties of a system. Since these quantities should be real, we use Hermitian operators.

For any matrix B, a matrix of the form B^*B or $B + B^*$ is always Hermitian. The sum of two Hermitian matrices is Hermitian, but the multiplication of two Hermitian matrices need not be Hermitian.

Exercise 22. Give an example of two Hermitian matrices whose multiplication is not Hermitian.

2.2 Unitary matrix

A matrix M is unitary if $MM^* = M^*M = I$ (analog of orthogonal matrices). In other words, the columns of M form an orthonormal basis of the whole space. Unitary matrices need not be Hermitian, so their eigenvalues can be complex. For a unitary matrix, $M^{-1} = M^*$.

Exercise 23. Give an example of a unitary matrix which is not Hermitian.

Unitary matrices can be viewed as matrices which implement a change of basis. Hence they preserve the angle (inner product) between the vectors. So for a unitary M,

$$\langle u|v\rangle = \langle Mu|Mv\rangle.$$

Exercise 24. Prove the above equation.

That means unitary matrix preserves the norm of a vector and angle between vectors. Another way to characterize a unitary matrix is, they move any orthonormal basis to another orthonormal basis.

If two matrices A, B are related by $A = M^{-1}BM$, where M is unitary, then they are unitarily equivalent. If two matrices are unitarily equivalent then they are similar. Spectral theorem can be stated as the fact that normal matrices are unitarily equivalent to a diagonal matrix. The diagonal of a diagonal matrix contains its eigenvalues.

Exercise 25. What is the rank of a unitary matrix?

Note 4. Since unitary matrices preserve the norm, they will be used as operators in the postulates of quantum mechanics.

Exercise 26. Show that the Pauli matrices are Hermitian as well as Unitary by calculating their eigenvalue.

Exercise 27. Show that the Pauli matrices (with identity) form a basis of all Hermitian 2×2 operators.

One of the important Unitary matrix is called the Hadamard matrix, it takes $|0\rangle$ to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1\rangle$ to $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The matrix representation is

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Exercise 28. Show that H is a unitary matrix, can you show directly that it is a unitary matrix (without computing its matrix representation)?

3 Evolution of a quantum system

The next postulate specifies, how a *closed* quantum system evolves. You might already know this postulate in terms of the very famous *Schrödinger's equation*. It is a partial differential equation which describes how a quantum state evolves with time.

The evolution is described by a *Hamiltonian* H which depends on the system being observed. For us, as computer scientists, it is just some Hermitian matrix H. Given the Hamiltonian H, the equation

$$i\frac{d|\psi\rangle}{dt} = H|\psi\rangle,$$

describes how the quantum system will change its state with time. For readers who are already familiar with this equation, we have assumed that Planck's constant can be absorbed in the Hamiltonian.

This equation can be considered as the second postulate of quantum mechanics. But, we will modify it a little bit to get rid of the partial differential equation and write it in terms of unitary operators.

Exercise 29. Read about Schrödinger's equation.

Suppose the quantum system is in state $|\psi(t_1)\rangle$ at time t_1. Then, using the Schrödinger's equation, the state at time t_2 is

$$|\psi(t_2)\rangle = e^{-iH(t_2-t_1)}|\psi(t_1)\rangle.$$

Exercise 30. Show that the matrix $e^{-iH(t_2-t_1)}$ is unitary.

Using the previous exercise,

$$|\psi(t_2)\rangle = U(t_2,t_1)|\psi(t_1)\rangle.$$

This gives us the "working" second postulate.

Postulate 2: A closed quantum system evolves unitarily. The unitary matrix only depends on time t_1 and t_2. If the state at t_1 is $|\psi(t_1)\rangle$ then the state at time t_2 is,

$$|\psi(t_2)\rangle = U(t_2,t_1)|\psi(t_1)\rangle.$$

Note 5. Unitary operators preserve norm and inner products.

Do you remember any unitary operators considered in this course before?

Exercise 31. Show that all Pauli matrices and the Hadamard matrix H are unitary operators.

Exercise 32. "Guess" the eigenvalues and eigenvectors of H. Check, if not, find the actual ones.

Notice that it is enough to specify the action of a gate/unitary on any basis (it is a linear operator). If we pick the standard basis, then we just need to mention the action on classical inputs. For example, Pauli X negates the classical inputs, it takes $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. That means, on any state $\alpha|0\rangle + \beta|1\rangle$, Pauli X will return $\alpha|1\rangle + \beta|0\rangle$. This is one of the preferred methods of specifying action of gates (or circuits) in quantum computing.

The Hadamard operator,

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

can be thought of as a random coin toss in the quantum world. If we apply Hadamard on standard basis and measure, we get 0 and 1 with equal probability.

Exercise 33. Why is

$$H' = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

not a random coin toss in the quantum world?

Controlled operators: Another class of gates, useful in quantum computing, are the *controlled versions* of a unitary gate U. There are two inputs to these gates, one is the control part and other is the target part. The unitary U is applied to the target part if and only if the control part is in *ON (set to* 1*)* state. Mostly, if the control part is a set of qubits, setting all of them to be 1 is seen as the ON state.

The simplest and most useful of these gates is called the CNOT gate. It has one control and one target qubit.

Exercise 34. Suppose, first qubit is control and second qubit is target, write the matrix representation of CNOT gate.

The CNOT gate is drawn as,

Here the first qubit is control and second qubit is data.

Exercise 35. What is the output of CNOT gate on the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Is the state still entangled?

4 Assignment

Exercise 36. Read about singular values of a matrix, show that the matrix M and M^* have the same singular values.

Exercise 37. Find the eigenvalue and eigenvectors of Pauli operators.

Exercise 38. Prove that the eigenvalues of a Hermitian matrix are real.

Exercise 39. Prove that the absolute value of the eigenvalues of an unitary matrix is 1. Is the converse true. What condition do we need to get the converse?

Exercise 40. Prove that a matrix M is Hermitian iff $\langle v|M|v\rangle$ is real for all $|v\rangle$.

Exercise 41. Show that the set of Hermitian matrices of a fixed dimension form a vector space (over which field?). What is the dimension of this vector space?

Exercise 42. Let $\sigma = \alpha_1 X + \alpha_2 Y + \alpha_3 Z$, where α_i's are real numbers and $|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1$. Show that,

$$e^{i\theta\sigma} = \cos(\theta)I + i\sin(\theta)\sigma.$$

Exercise 43. Prove that if H is Hermitian then e^{iH} is a unitary matrix.

References

1. Gilbert Strang. *Introduction to Linear Algebra.* Wellesley-Cambridge Press, 2009.