The phase estimation problem

This section of the lesson explains the *phase estimation problem*. We'll begin with a short discussion of the *spectral theorem* from linear algebra, and then move on to a statement of the phase estimation problem itself.

Spectral theorem

The *spectral theorem* is an important fact from linear algebra that states that matrices of a certain type, called *normal matrices,* can be expressed in a simple and useful way. We'll only need this theorem for unitary matrices in this lesson, but down the road in this series we'll apply it to Hermitian matrices as well.

Normal matrices

A square matrix M with complex number entries is said to be a *normal matrix* if it commutes with its conjugate transpose: $MM^\dagger = M^\dagger M$.

Every unitary matrix U is normal because

$$UU^\dagger = \mathbb{I} = U^\dagger U.$$

Hermitian matrices, which are matrices that equal their own conjugate transpose, are another important class of normal matrices. If H is a Hermitian matrix, then

$$HH^\dagger = H^2 = H^\dagger H,$$

so H is normal.

Not every square matrix is normal. For instance, this matrix isn't normal:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

(This is a simple but great example of a matrix that's often very helpful to consider.) It isn't normal because

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^{\dagger} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

while

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^{\dagger} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Theorem statement

Now here's a statement of the spectral theorem.

Theorem
Spectral theorem: Let M be a normal $N \times N$ complex matrix. There exists an orthonormal basis of N-dimensional complex vectors $\{|\psi_1\rangle, \ldots, |\psi_N\rangle\}$ along with complex numbers $\lambda_1, \ldots, \lambda_N$ such that

$$M = \lambda_1 |\psi_1\rangle\langle\psi_1| + \cdots + \lambda_N |\psi_N\rangle\langle\psi_N|.$$

The expression of a matrix in the form

$$M = \sum_{k=1}^{N} \lambda_k |\psi_k\rangle\langle\psi_k| \tag{1}$$

is commonly called a *spectral decomposition*. Notice that if M is a normal matrix expressed in the form (1), then the equation

$$M|\psi_j\rangle = \lambda_j |\psi_j\rangle$$

must be true for every $j = 1, \ldots, N$. This is a consequence of the fact that $\{|\psi_1\rangle, \ldots, |\psi_N\rangle\}$ is orthonormal:

$$M|\psi_j\rangle = \left(\sum_{k=1}^{N} \lambda_k |\psi_k\rangle\langle\psi_k| \right) |\psi_j\rangle = \sum_{k=1}^{N} \lambda_k |\psi_k\rangle\langle\psi_k|\psi_j\rangle = \lambda_j |\psi_j\rangle$$

That is, each number λ_j is an *eigenvalue* of M and $|\psi_j\rangle$ is an *eigenvector* corresponding to that eigenvalue.

- **Example 1**. Let

$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

which is normal. The theorem implies that $\mathbb{I}$ can be written in the form (1) for some choice of λ_1, λ_2, $|\psi_1\rangle$, and $|\psi_2\rangle$. There are multiple choices that work, including

$$\lambda_1 = 1, \;\; \lambda_2 = 1, \;\; |\psi_1\rangle = |0\rangle, \;\; |\psi_2\rangle = |1\rangle.$$

Notice that the theorem does not say that the complex numbers $\lambda_1, \ldots, \lambda_N$ are distinct — we can have the same complex number repeated, which is necessary for this example. These choices work because

$$\mathbb{I} = |0\rangle\langle 0| + |1\rangle\langle 1|.$$

Indeed, we could choose $\{|\psi_1\rangle, |\psi_2\rangle\}$ to be *any* orthonormal basis and the equation will be true. For instance,

$$\mathbb{I} = |+\rangle\langle +| + |-\rangle\langle -|.$$

- **Example 2**. Consider a Hadamard operation.

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

This is a unitary matrix, so it is normal. The spectral theorem implies that H can be written in the form (1), and in particular we have

$$H = |\psi_{\pi/8}\rangle\langle\psi_{\pi/8}| - |\psi_{5\pi/8}\rangle\langle\psi_{5\pi/8}|$$

where

$$|\psi_\theta\rangle = \cos(\theta)|0\rangle + \sin(\theta)|1\rangle.$$

More explicitly,

$$|\psi_{\pi/8}\rangle = \frac{\sqrt{2+\sqrt{2}}}{2}|0\rangle + \frac{\sqrt{2-\sqrt{2}}}{2}|1\rangle,$$

$$|\psi_{5\pi/8}\rangle = -\frac{\sqrt{2-\sqrt{2}}}{2}|0\rangle + \frac{\sqrt{2+\sqrt{2}}}{2}|1\rangle.$$

We can check that this decomposition is correct by performing the required calculations:

$$|\psi_{\pi/8}\rangle\langle\psi_{\pi/8}| - |\psi_{5\pi/8}\rangle\langle\psi_{5\pi/8}| = \begin{pmatrix} \frac{2+\sqrt{2}}{4} & \frac{\sqrt{2}}{4} \\ \frac{\sqrt{2}}{4} & \frac{2-\sqrt{2}}{4} \end{pmatrix} - \begin{pmatrix} \frac{2-\sqrt{2}}{4} & \\ -\frac{\sqrt{2}}{4} & \end{pmatrix}$$

As the first example above reveals, there can be some freedom in how eigenvectors are selected. There is, however, no freedom at all in how the eigenvalues are chosen, except for their ordering: the same N complex numbers $\lambda_1, \ldots, \lambda_N$, which can include repetitions of the same complex number, will always occur in the equation (1) for a given choice of a matrix M.

Now let's focus in on unitary matrices. Suppose we have a complex number λ and a non-zero vector $|\psi\rangle$ that satisfy the equation

$$U|\psi\rangle = \lambda|\psi\rangle. \tag{2}$$

That is, λ is an eigenvalue of U and $|\psi\rangle$ is an eigenvector corresponding to this eigenvalue.

Unitary matrices preserve Euclidean norm, and so we conclude the following from (2).

$$\big\||\psi\rangle\big\| = \big\|U|\psi\rangle\big\| = \big\|\lambda|\psi\rangle\big\| = |\lambda|\big\||\psi\rangle\big\|$$

The condition that $|\psi\rangle$ is non-zero implies that $\big\||\psi\rangle\big\| \neq 0$, so we can cancel it from both sides to obtain

$$|\lambda| = 1.$$

This reveals that eigenvalues of unitary matrices must always have absolute value equal to one, so they lie on the *unit circle.*

$$\mathbb{T} = \{\alpha \in \mathbb{C} : |\alpha| = 1\}$$

(The symbol $\mathbb{T}$ is a common name for the complex unit circle. The name S^1 is also common.)

Phase estimation problem statement

In the *phase estimation problem*, we're given a quantum state $|\psi\rangle$ of n qubits, along with a unitary quantum circuit that acts on n qubits. We're

promised that $|\psi\rangle$ is an eigenvector of the unitary matrix U that describes the action of the circuit, and our goal is to compute or approximate the eigenvalue λ to which $|\psi\rangle$ corresponds. More precisely, because λ lies on the complex unit circle, we can write

$$\lambda = e^{2\pi i \theta}$$

for a unique real number θ satisfying $0 \leq \theta < 1$. The goal of the problem is to compute or approximate this real number θ.

Phase estimation problem
Input: A unitary quantum circuit for an n-qubit operation U along with an n-qubit quantum state $|\psi\rangle$
Promise: $|\psi\rangle$ is an eigenvector of U
Output: an approximation to the number $\theta \in [0, 1)$ satisfying $U|\psi\rangle = e^{2\pi i \theta}|\psi\rangle$

Here are a few remarks about this problem statement:

1. The phase estimation problem is different from other problems we've seen so far in the course in that the input includes a quantum state. Typically we focus on problems having classical inputs and outputs, but nothing prevents us from considering quantum state inputs like this. In terms of its practical relevance, the phase estimation problem is typically encountered as a *subproblem* inside of a larger computation, like we'll see in the context of integer factorization later in the lesson.

2. The statement of the phase estimation problem above isn't specific about what constitutes an approximation of θ, but we can formulate more precise problem statements depending on our needs and interests. In the context of integer factorization, we'll demand a very precise approximation to θ, but in other cases we might be satisfied with a very rough approximation. We'll discuss shortly how the precision we require affects the computational cost of a solution.

3. Notice that as we go from $\theta = 0$ toward $\theta = 1$ in the phase estimation problem, we're going all the way around the unit circle, starting from $e^{2\pi i \cdot 0} = 1$ and moving counter-clockwise toward $e^{2\pi i \cdot 1} = 1$. That is, when we reach $\theta = 1$ we're back where we started at $\theta = 0$. So, as we consider the accuracy of approximations, choices of θ near 1 should be considered as being near 0. For example, an approximation $\theta = 0.999$ should be considered as being within $1/1000$ of $\theta = 0$.

Was this page helpful?

Yes No

Report a bug, typo, or request content on GitHub ↗.

Previous page Next page