Principles of Quantum Mechanics

Raimondas Čiegis

Department of Mathematical Modelling, email: rc@vgtu.lt

September 3, 2026

States in Quantum Mechanics are mathematically described as vectors in a Hilbert linear vector space.

Physical observables are objects that we can measure. They are also described by linear operators. Some specific properties of these operators will be formulated.

Note that observables are also associated with a vector space, but they are not state-vectors (they are represented by linear operators).

Eigenvectors and Eigenvalues

The definition of an eigenvector of linear operator M (here it is written in a matrix form) is a *ket*-vector $|\lambda\rangle$ such that

$$M\,|\lambda\rangle = \lambda\,|\lambda\rangle\,.$$

Here λ (as opposed to *ket*-vector $|\lambda\rangle$) is a number – generally a complex one. It is called an eigenvalue.

Eigenvectors and Eigenvalues

The definition of an eigenvector of linear operator M (here it is written in a matrix form) is a *ket*-vector $|\lambda\rangle$ such that

$$M|\lambda\rangle = \lambda|\lambda\rangle .$$

Here λ (as opposed to *ket*-vector $|\lambda\rangle$) is a number – generally a complex one. It is called an eigenvalue.

When M acts on its eigenvector $|\lambda\rangle$ all that happens the eigenvector gets multiplied by the eigenvalue λ.

Hermitian Conjugation

Let's consider a linear operator $\mathcal{M}$.

Hermitian conjugate operator $M^\dagger$ is defined as

$$\langle\psi|\,\mathcal{M}\,|\phi\rangle = \langle\phi|\,\mathcal{M}^\dagger\,|\psi\rangle^*.$$

It is very convenient to consider matrix forms of both operators, then we get the equality

$$M^\dagger = [M^T]^*.$$

here T is used in transpostion and $*$ is used in complex conjugation.

If M acts on the ket $|A\rangle$ to give $|B\rangle$

$$M\,|A\rangle = |B\rangle$$

then

$$\langle A|\,M^{\dagger} = \langle B|\,.$$

If M acts on the ket $|A\rangle$ to give $|B\rangle$

$$M |A\rangle = |B\rangle$$

then

$$\langle A| M^\dagger = \langle B| .$$

Hermitian operators have some special properties.

1. The eigenvalues of Hermitian operators (and their matrices) are all real.

If M acts on the ket $|A\rangle$ to give $|B\rangle$

$$M|A\rangle = |B\rangle$$

then

$$\langle A| M^\dagger = \langle B| .$$

Hermitian operators have some special properties.

1. The eigenvalues of Hermitian operators (and their matrices) are all real.

2. The eigenvalues of Hermitian operator (matrix) L make a complete set of vectors

$$L|\lambda_j\rangle = \lambda_j |\lambda_j\rangle , \quad j = 1, \ldots, N.$$

Then any vector $|A\rangle$ can be expanded as a sum

$$|A\rangle = \sum_{j=1}^{N} \alpha_j |\lambda_j\rangle .$$

If λ_1 and λ_2 are two unequal eiegenvalues of a Hermitian operator, then the corresponding eigenvectors are orthogonal

$$\langle \lambda_1 | \lambda_2 \rangle = 0.$$

Thus eigenvectors make an orthonormal basis system.

If λ_1 and λ_2 are two unequal eiegenvalues of a Hermitian operator, then the corresponding eigenvectors are orthogonal

$$\langle \lambda_1 | \lambda_2 \rangle = 0.$$

Thus eigenvectors make an orthonormal basis system.

Unitary operators

All transformations of quantum algorithms are defined by unitary operators. The operator (matrix) U is unitary if it satisfies this rule

$$UU^\dagger = U^\dagger U = I.$$

Then for Hermitian unitary operators we have

$$U^{-1} = U.$$

The Axioms of Quantum Mechanics

Now we can state the principles of quantum mechanics.

First, it is important to understand that quantum systems evolve in two different ways

a) by unitary (deterministic) evolution between measurements,

b) and by wave function collapse when measurements take place (probabilistic evolution).

Principle 1:

The observable (or measurable) quantities of quantum mechanics are represented by linear operators L.

Principle 2:

The possible results of a measurement are the eigenvalues of the operator L that represents the observable.

Principle 3:

Unambiguously distinguishable states are represented by orthogonal vectors.

For state defined as an eigenvector $|\lambda_i\rangle$ of L the result of measurement is unambiguously λ_i.

Principle 4:

If $|A\rangle$ is the state-vector of a system, and the observable L is measured, the probability to observe value λ_i is

$$P(\lambda_i) = \langle A|\lambda_i\rangle \langle\lambda_i|A\rangle = |\langle A|\lambda_i\rangle|^2.$$

No way to tell for certain which of these values will be observed.

Principle 5:

The evolution of state-vectors with time is unitary

$$|\Psi(t)\rangle = U(t)\,|\Psi(0)\rangle\,.$$

The operation U is called the *time-development operator* for the system

$$U^\dagger U = I.$$

Quantum logic gates

In quantum computing and specifically the quantum circuit model of computation, a quantum logic gate (or simply quantum gate) is a basic quantum circuit operating on a small number of qubits.

Quantum logic gates are unitary operators (matrices) and they are the building blocks of quantum circuits, like classical logic gates are for conventional digital circuits.

We start with popular quantum gates on a single qubit.

Pauli gates (X, Y, Z)

$\mathcal{X}$ (or NOT) operator:

$$\mathcal{X}: \qquad \begin{aligned} |0\rangle &\rightarrow |1\rangle \\ |1\rangle &\rightarrow |0\rangle \end{aligned}$$

matrix form of $\mathcal{X}$ gate:

$$X = \begin{pmatrix} m_{00} & m_{01} \\ m_{10} & m_{11} \end{pmatrix} \quad \rightarrow \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

where e.g. $m_{01} = \langle 0| \mathcal{X} |1\rangle = \langle 0|0\rangle = 1.$

Check that X is an unitary matrix.

Operator $\mathcal{Y}$:

$$\mathcal{Y}: \qquad \begin{aligned} |0\rangle &\to \ \ i\,|1\rangle\,, \\ |1\rangle &\to -i\,|0\rangle\,, \end{aligned}$$

matrix form of Y:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

Operator $\mathcal{Y}$:

$$\mathcal{Y}: \qquad \begin{aligned} |0\rangle &\to \ \ i\,|1\rangle\,, \\ |1\rangle &\to -i\,|0\rangle\,, \end{aligned}$$

matrix form of Y:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

Complex conjugate operator $\mathcal{Z}$:

$$\mathcal{Z}: \qquad \begin{aligned} |0\rangle &\to \ \ |0\rangle\,, \\ |1\rangle &\to -\,|1\rangle\,, \end{aligned}$$

matrix form:

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

Hadamard (H) gate:

$$\mathcal{H}: \qquad |0\rangle \to \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)$$
$$|1\rangle \to \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big),$$

matrix form:

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

Controlled NOT operator ($CNOT$ or CX) for two qubits system:

$$
\begin{aligned}
CNOT: \qquad & |00\rangle \to |00\rangle \\
& |01\rangle \to |01\rangle \\
& |10\rangle \to |11\rangle \\
& |11\rangle \to |10\rangle ,
\end{aligned}
$$

matrix form:

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

Next we define the 3-qubit Toffoli gate, also called controlled-controlled-not (CCNOT) gate.

If we limit ourselves to only accepting input qubits that are $|0\rangle$ and $|1\rangle$, then if the first two bits are in the state $|1\rangle$ it applies a X gate on the third bit, else it does nothing.

$$\begin{aligned} CCNOT: \quad & |000\rangle \to |000\rangle\,, \qquad & |100\rangle \to |100\rangle\,, \\ & |001\rangle \to |001\rangle\,, \qquad & |101\rangle \to |101\rangle\,, \\ & |010\rangle \to |010\rangle\,, \qquad & |110\rangle \to |111\rangle\,, \\ & |011\rangle \to |011\rangle\,, \qquad & |111\rangle \to |110\rangle\,. \end{aligned}$$

We ask You to define also the matrix form of this 3-qubit gate.

Toffoli gate is important because it is complete for classical (also nonreversible) computation: any classical computation can be implemented by a circuit of reversible Toffoli gates.

Toffoli gate is important because it is complete for classical (also nonreversible) computation: any classical computation can be implemented by a circuit of reversible Toffoli gates.

The set of Hadamard (H) and Toffoli ($CCNOT$) is universal for all unitaries with real entries in the sense of approximation, meaning that any unitary with only real entries can be arbitrarily well approximated using circuits of only these gates.

Quantum parallelism

One uniquely quantum-mechanical effect that we can use for building quantum algorithms is quantum parallelism.

First we start from a simple example. Let's U be a linear operator and apply it for a n-qubit vector

$$|\psi\rangle = \sum_{j=1}^{2^n} \alpha_j \, |j\rangle \, ,$$

then we get

$$U \, |\psi\rangle = \sum_{j=1}^{2^n} \alpha_j \, U \, |j\rangle \, .$$

In one step, we compute the images of operator U with all 2^n basis vectors.

We compute the linear combination of the images of the basis vectors, not the image of the linear combination.

We compute the linear combination of the images of the basis vectors, not the image of the linear combination.

Second, suppose we have a classical algorithm that computes some function $f : \{0,1\}^n \to \{0,1\}^m$.

Then we can build a quantum circuit U (e.g. consisting only of Toffoli gates) that maps

$$|z\,0\rangle \to |z\,f(z)\rangle\,, \quad \forall z \in \{0,1\}^n.$$

Now suppose we apply U to a superposition of all inputs $|z\rangle$ (which is easy to build using n Hadamard transforms):

$$U\left(\frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}|z\rangle\,|0\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}|z\rangle\,|f(z)\rangle\,.$$

Again we see that we applied U just once, but the final superposition contains $f(z)$ for all $2n$ input values z.

However, by itself this is not very useful and does not give more than classical randomization, since observing the final superposition will give just one uniformly random $|z\rangle\ |f(z)\rangle$ and all other information will be lost.

Again we see that we applied U just once, but the final superposition contains $f(z)$ for all $2n$ input values z.

However, by itself this is not very useful and does not give more than classical randomization, since observing the final superposition will give just one uniformly random $|z\rangle\ |f(z)\rangle$ and all other information will be lost.

Thus quantum parallelism needs to be combined with the effects of interference and entanglement in order to get something that is better than classical.

Entaglement

Let's consider a state $|\psi\rangle$ of two qubits

$$|\psi\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle + |01\rangle\,\big).$$

It can be written as tensor product of two independent qubits

$$|\psi\rangle = |0\rangle \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big).$$

Entaglement

Let's consider a state $|\psi\rangle$ of two qubits

$$|\psi\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle + |01\rangle\,\big).$$

It can be written as tensor product of two independent qubits

$$|\psi\rangle = |0\rangle \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big).$$

Both qubits are independent and the measurement of value of one qubit is not changing a state of the other qubit.

The state $|\psi\rangle$ is called an entangled if it cannot be written as the tensor product of two separate qubits.

The state $|\psi\rangle$ is called an entangled if it cannot be written as the tensor product of two separate qubits.

Let's consider the EPR state (Einstein, Podolsky and Rosen):

$$|\psi\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big).$$

It is clear that if we measure one qubit then instantly we get the value of the second qubit.

For example, if we measure the value of the first qubit and get 0 then the wave $|\psi\rangle$ instantly collapse into state

$$|\psi\rangle = |00\rangle$$

and we also know the value of the second qubit.

Exercises 2.

1.

(a) What is the dot product between the real vectors $(0, 1, 0, 1)$ and $(0, 1, 1, 1)$?

(b) What is the inner product between the quantum states $|0101\rangle$ and $|0111\rangle$?

2. Show that

$$H\,X\,H = Z.$$

3. Eplain the role of the resulting 2-qubit gate:

$$(H \otimes H)\, CNOT\, (H \otimes H).$$

4.

Prove that an EPR-pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is an entangled state, i.e., that it cannot be written as the tensor product of two separate qubits.