# Quantum computing fundamentals

## Learning objectives

By the end of this module, you should be able to:

- Differentiate quantum computing from classical computing
- Differentiate qubits from bits
- Explain the core concepts of quantum computing
- Recognize the difference between quantum gates, quantum circuits, and quantum computers

## What quantum computing is—and what it isn’t

Can quantum computation be accomplished on classical computers? Is quantum computing just another form of AI? Katie Pizzolato, Director of IBM Quantum Theory and Computational Science at IBM Quantum, dispels several quantum computing myths in 60 seconds.

# A new way of seeing problems

There are several concepts distinct to quantum computing that will help you understand its potential applications to your organization or industry. All computing systems rely on a fundamental ability to store and manipulate information. Conventional computers store information in bits (zeros and ones) and quantum computers use **qubits** (pronounced CUE–bits). Quantum computers take advantage of the laws of quantum mechanics found in nature. They represent a fundamental change from conventional information processing.

Here is a metaphor to help you understand why quantum computing is very different from conventional computing. Consider the art and technique of photography before and after the advent of color film.

For example, consider this black-and-white photograph of a field of tulips and this color photograph of red tulips and a yellow tulip in a field.

The physical phenomena of color existed while photography was limited to grayscale. But posing the question, “Could you swap the reds and yellows?” would have been totally meaningless, as would any attempt to do so.

Once color film was invented, there was an explosion of artistic and technical options available to photographers, now that they could manipulate the physics of color.

Quantum computers exist now because we have recently figured out how to control what has been in the world this whole time: the quantum phenomena of superposition, entanglement, and interference. These new ingredients in computing expand what is possible to design into algorithms. Quantum computers offer us new ways of seeing problems, which can reveal solutions that would be invisible to classical computers.

Just as pre-color film photography was renamed “black-and-white photography” after the advent of color film, pre-quantum computing came to need a new name. The most common term for pre-quantum computing is **classical computing**. The words “classical” and “quantum” came to modify the word “computing” because this is how scientists already modified the word “physics,” as in “classical physics” and “quantum physics.”

## How quantum computing is different from classical

Today’s computers perform calculations and process information using the classical model of computation, which dates back to the work of Alan Turing and John von Neumann. In this model, all information is reducible to bits, which can take the values of either 0 or 1, and all processing can

be performed via simple logic gates (AND, OR, NOT, NAND) acting on one or two bits at a time. At any point in the computation, a classical computer's state is entirely determined by the states of all its bits, so that a computer with *n* bits can exist in one of $2^n$ possible states, ranging from 00...0 (the sequence of *n* zeros) to 11...1 (the sequence of *n* ones).

The power of the quantum model of computation, meanwhile, lies in its much richer repertoire of states. A quantum computer also has bits, but instead of 0 and 1, its quantum bits, or qubits, can represent a 0, a 1, or a combination of both, which is a property known as superposition. This on its own is no special thing, since a computer whose bits can be intermediate between 0 and 1 is just an analog computer, scarcely more powerful than an ordinary digital computer. However, a quantum computer takes advantage of a special kind of superposition that allows for exponentially many logical states at once. This is a powerful feat, and no classical computer can achieve it. The vast majority of these quantum superpositions, and the ones most useful for quantum computation, are entangled—they are states of the whole computer that do not correspond to any assignment of digital or analog states of the individual qubits.

One might think that the difficulty in understanding quantum computing lies in hard math, but mathematically, quantum concepts are only a little more complex than high school algebra. Quantum physics is hard because it requires internalizing ideas that are simple but counterintuitive.

To get a better conversational understanding of the core concepts of quantum computing, watch this video from Talia Gershon, Director of Hybrid Cloud Infrastructure at IBM Research. Gershon explains quantum computing on five levels—to a child, teen, college student, graduate student, and professional for *WIRED* magazine. Please watch up to the 06:17-minute mark; however, feel free to watch the entire video.

**Check your understanding**

Read the question below, think about your answer, then click the triangle to reveal the solution.

▶ True or false: Only people with advanced degrees in mathematics and physics can understand quantum computing concepts.

# Principles of quantum information

## Qubits

In the video below, IBM's Director of Research Darío Gil contrasts the main unit of classical information (bit) with the main unit of quantum information (qubit). He guides you to visualize the three core principles of quantum computing: superposition, entanglement, and interference. With these properties, quantum algorithms can be developed that can solve business problems that may be beyond the reach of even the world's largest supercomputers.

## Superposition

A **superposition** is a weighted sum or difference of two or more states. This mixture of states is often difficult for people to picture (like a flipped coin landing on a mixture of the two sides, heads and tails). But there are easier cases to imagine—for example, when a chord of several musical notes is played on a guitar. The vibration of the air corresponds not merely to one of the notes, but to all. The air is vibrating with a combination of frequencies corresponding to all the notes in the chord.

The "weighted sum or difference" means that some parts of the superposition are more or less prominently represented, such as when a violin is played more loudly than the other instruments in a string quartet. Ordinary, or classical, superpositions commonly occur in macroscopic phenomena involving waves. So superposition may actually be a familiar concept.

What is strange and specific to the quantum world is that, upon measuring a system in a superposition of states, the system collapses into just one of the pure states. The musical analog would be playing a chord of several notes, letting that chord propagate through the air to your ear, but hearing (measuring) only one of the several notes played. Nothing like this exists in the macroscopic world.

**How does superposition make quantum computers different from classical computers?**

A system of *n* qubits, can be measured to be in one of $2^n$ possible states. This is also true of classical computer bits, or indeed of any collection of *n* binary outcomes. To illustrate this, consider all of the possible results of flipping *n* distinguishable coins, each with two possible sides which we will call "heads" (H) and "tails" (T), respectively.

If we flip one coin, there are two possible states: H or T.

If we flip two coins, there are four possible states: HH, HT, TH, and TT.

For three coins, we find eight states: HHH, HHT, HTH, HTT, THH, THT, TTH, TTT.

The trend continues like this. Each time we add another coin, the number of possible outcomes is doubled. So the number of outcomes for a system of *n* such binary variables is $2^n$.

If this is true for both classical and quantum computers, then what makes quantum computers so special? The answer is superposition. Both classical and quantum computers can access a space of $2^n$ possible states. But a classical computer can only be in one of those states at a time, whereas a quantum computer can be in a superposition of **all** these states, at once.

To be a bit more concrete about it, suppose you are searching for the minimum cost *C* associated with some industrial process. This process depends on many input variables, which we will denote $x_i$. For now we will assume these variables to be binary, though we could generalize. On a classical computer, you would need to calculate the cost $C(x_i)$ for

each possible choice of $x_i$. That is, you would have to plug in 0000...00, 000...01, 000...10, and so on, spanning all possible inputs. A quantum computer can be in a superposition of all these states, such that operations can be performed on all the possible input states at once.

If that sounds too good to be true, there is a complication: recall that upon measuring the quantum system, we can only obtain one result, not all results from the whole space. So the task becomes to write algorithms that cause the optimal solution (lowest cost, fastest response, etc.) to be the one that ends up being measured. In other words, quantum computers don't return all possible solutions; they probe a space of many solutions simultaneously and (if the algorithm works) they return the optimal solution with high probability. For problems with very large solution spaces or very computationally expensive steps, this difference could be game-changing.

**Classical vs. quantum probability?**

Which quantum state is measured at the end of a calculation, is probabilistic. The weights described above correspond to probabilities of measuring different states. A technical note: while probabilities must be positive (or zero), the weights in a superposition can be positive, negative, or even complex numbers. The probability is the absolute value of a weight, squared: $P_i = |w_i|^2$. It is important to note that the word *probability* is sometimes used to mean different things in classical and quantum contexts. For example, if you have already flipped a set of *n* coins, but not looked at the outcome, as far as you know each coin might be heads or tails. You might call this a probabilistic mixture of $2^n$ states. But the set of coins is actually in only one of the possible states—we just don’t know which. This is not the case for quantum computers. Quantum computers can hold data corresponding to superpositions of $2^n$ distinct logical states, at once. For this reason, quantum superposition is more powerful than classical probabilism. Quantum computers capable of holding their data in superposition can solve some problems exponentially faster than any known classical algorithm.

To learn more, watch this IBM Research video about classical and quantum randomness.

## Entanglement

Imagine two friends with two very thin, sheer scarves that are almost transparent. One scarf is red, and the other is blue. When the friends lay the scarves on top of each other, together they appear purple. If the friends hold these two scarves stretched between them, the state of the two friends holding something purple is definite, even though, if separated, it is not known which friend would be holding the blue scarf and which would be holding the red scarf. Quantum **entanglement** is like this. The state of the entire system has properties that are known (like the joint color of the two scarves), but the individual pieces do not have well-defined properties (like each friend, neither of whom is holding a scarf of a clearly defined color). This metaphor is imperfect since each friend could decide ahead of time to hold one scarf more tightly than the other or to release one scarf or the other as the two friends move apart. In a quantum system, the properties of the parts are truly undefined until measurements are made.

### Interference

**Interference** is a property of quantum systems in which states with opposing phases may amplify or cancel each other. One way to imagine interference is to think about how polarized lenses in sunglasses work. If you place two polarized lenses on top of each other and begin to rotate one of them, you'll notice both constructive and deconstructive interference as more or less light is blocked.

For more intuition of how interference works, watch this video from 7:40 to 8:24.

#### Check your understanding

Read the question below, think about your answer, then click the triangle to reveal the solution.

▶ Quantum physics contains some counterintuitive ideas, such as: (a) A physical system in a definite state can still behave randomly. (b) Two systems that are too far apart to influence each other are somehow strongly correlated. (c) It is possible to have a state in a quantum system that cannot be described as the product of the independent components of the qubits that make up the state. (d) All of the above.

## Quantum circuits

### Business value of quantum circuits

Quantum circuits represent a set of instructions that allow us to manipulate qubits in order to leverage superposition, entanglement, and interference for solving complex problems. Watch the video below to see how classical and quantum circuits compare and how quantum circuits can bring value to your business.

**Check your understanding**

Read the question below, think about your answer, then click the triangle to reveal the solution.

▶ True or false: Quantum circuits are not physical devices.

## Programming a quantum circuit

What do you need to program a quantum computer? The answer is Qiskit! Learn how to pronounce this word and more in the video below.

Sign in to track your progress

Complete

Introduction to quantum computing

Quantum technology →