QIS KEY CONCEPTS

EXPANDED EXPLANATIONS FOR K-12 EDUCATORS

National Q-12 Education Partnership

Q12EDUCATION.ORG

QIS KEY CONCEPTS
EXPLANATIONS FOR K-12 EDUCATORS

ABOUT The purpose of this document is to provide K-12 educators with descriptions of a set of key concepts for Quantum Information Science. The set of nine key concepts described below was designed by a group of researchers and educators (*QIS Key Concepts for Future Quantum Information Science Learners workshop*) to promote future curriculum and educator development activities. The expanded descriptions in this document build on their work to provide a resource for K-12 educators to introduce and teach Quantum Information Science at a level appropriate for their students.

COMMENTS

If you have any feedback about this document, please contact us at *emily.edwards@duke.edu*

ACKNOWLEDGEMENTS

All images by Brent Yen or Jen Palmer, unless otherwise noted.

1. QUANTUM INFORMATION SCIENCE

KEY CONCEPT

Quantum information science (QIS) exploits quantum principles to transform how information is acquired, encoded, manipulated, and applied. Quantum information science encompasses quantum computing, quantum communication, and quantum sensing, and spurs other advances in science and technology.

Outline:

a. Quantum information science employs quantum mechanics, a well-tested theory that uses the mathematics of probability, vectors, algebra, trigonometry, complex numbers, and linear transformations to describe the physical world.

b. Quantum information science combines information theory and computer science, following the laws of quantum mechanics, to process information in fundamentally new ways.

c. Quantum information science has already produced and enhanced high-impact technologies such as the Global Positioning System (GPS), which depends on the extreme precision of atomic clocks. based on the quantum states of atoms.

2. QUANTUM STATE

KEY CONCEPT

A **quantum state** is a mathematical representation of a physical system, such as an atom, and provides the basis for processing quantum information.

Outline:

a. Quantum states are represented by directions or vectors in an abstract space.

b. The direction of the quantum state vector determines the probabilities of all of the possible outcomes of a set of measurements. Quantum manipulations in the physical world follow vector operations, incorporating complex numbers and negative values. This captures a behavior of physical quantum systems that cannot be described solely by the arithmetic of probability.

c. Quantum systems are fragile. For instance, measurement almost always disturbs a quantum system in a way that cannot be ignored. This fragility influences the design of computational algorithms and communication and sensing protocols.

Prerequistite Knowledge:

- Directions or vectors
- Probability

INTRODUCTION : QUANTUM STATE

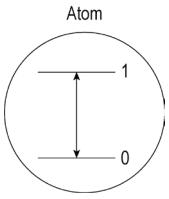
Math as a model for the world

Mathematical formulas contain symbols (like 4 and +) which we can manipulate to help us understand real-world systems. Even something as mundane as figuring out how many kids are in a classroom requires us to express our thoughts using math. Our numeral system and symbolic representations for basic math operations, like addition, are necessary for quick calculations. The alternative of counting things one by one is tedious and inaccurate in practice. Roman numerals, which were used to write numbers in Europe during the Middle Ages, are no longer used today because they were an ineffective way to perform calculations.

Beyond arithmetic, representing physical phenomena with math allows us to think about how systems (see *Glossary*) change over time and calculate predicted outcomes. For instance, mathematical models are used to predict possible storm trajectories.

Quantum states are a mathematical construct that encapsulate the quantum properties of physical systems.

Quantum systems have physical properties, such as spin, charge, temperature, position, and velocity. To understand applications of quantum information science (QIS), such as sensing, communication, and computation, it is helpful to focus on properties that are *quantized* (only take certain discrete values). For example, some properties only have two possible values, like an **atom** with two possible energy levels in its ground state. (See the *Qubits* article for more information about these types of two-state systems called **qubits**.)



The mathematical representation of a physical quantum system, like an atom or electron, is called its **quantum state**. Directions or **vectors** are the type of math used to represent quantum states.

Quantum states provide the foundation for procesing quantum information.

Quantum information science takes advantage of the features of quantum states to process and manipulate information in fundamentally new ways.

(See the first article *Quantum Information Science* for a quick overview and the later articles *Quantum Communication*, *Quantum Computing*, and *Quantum Sensing* for descriptions of QIS applications.)

In order to process quantum information, we must do something to change and control the quantum state of a system. Operations are actions that change the quantum state of a system, and this translates into changes in the physical properties of that system. For instance, you could apply an operation to change the energy state of an atom. **Quantum operations** are represented by a type of mathematical object called a **matrix**.

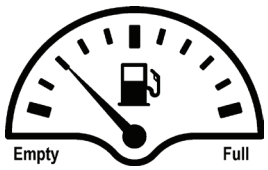
a. Quantum states are represented by directions or vectors in an abstract space.

Vectors are useful in expressing properties that have direction.

Vectors are used to express properties of a physical system that have directions associated with them. A bike's velocity is a familiar everyday example. While we are used to directions in the world around us, like when you are riding a bike or other vehicle east or west, vectors can also express directionality in an abstract space. In an *abstract space*, there is still a coordinate system, but the meaning of direction is not the same as it is on a map.

In quantum information science, quantum states are vectors.

Vectors, like the bike's velocity mentioned above, have a direction, often depicted graphically as an arrow. The information represented by a direction depends on the context. For example, a fuel gauge arrow expresses the fullness of the car's fuel tank by pointing in a particular direction between the "full" and "empty" marks.



Quantum states are vectors with a direction in an abstract space. The direction of the **quantum state vector** contains the information necesary to calculate the **probability** or chance of different outcomes of a single measurement.

b. The direction of the quantum state vector expresses the probabilities of all of the possible outcomes of a set of measurements. Quantum manipulations in the physical world follow vector operations, incorporating complex numbers and negative values. This captures a behavior of physical quantum systems that cannot be described solely by the arithmetic of probability.

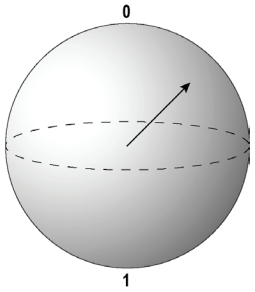
Quantum states determine the probabilities of outcomes of measurements.

The above example addresses one aspect of a quantum state: it determines the probability that the outcome of a measurement will be a certain value. For a simple measurement that only has two possible outcomes, 0 or 1, the quantum state determines the probability of measuring 0 and the probability of measuring 1. (See the next article *Measurement* to learn more about measurements of quantum systems.)

A quantum state contains all of the information about the attributes of a system. For a qubit, which is a quantum system with two available states, we store two numbers called **probability amplitudes** – these are the coefficients of the vector. The first probability amplitude relates to the probability of measuring 0, and the second relates to the probability of measuring 1. The actual probabilities are calculated from the probability amplitudes, which can be negative or complex numbers.

Quantum manipulations in the physical world follow vector operations, incorporating complex numbers and negative values.

The direction of the vector provides a mathematical representation of the quantum state. The abstract space of a **qubit** (a two-state system discussed in the *Qubits* article) is 3-dimensional and looks like a sphere or a globe – the vector runs from the center out to somewhere on the surface. Every state of the qubit can be represented as a vector on this surface.



Quantum manipulations or operations in the physical world change where the vector is pointed on the surface of this sphere. Quantum operations are represented by a type of mathematical object called a **matrix** and a type of math operation called **matrix multiplication**. These operations can involve negative and complex numbers.

c. Quantum systems are fragile. For instance, measurement almost always disturbs a quantum system in a way that cannot be ignored. This fragility influences the design of computational algorithms and communication and sensing protocols.

Quantum systems are fragile.

All quantum systems are delicate and affected by their surroundings. (See the *Decoherence* article for more details about the fragility of quantum states.)

To be useful for QIS applications, physical systems have to be isolated from disruptions.

In quantum information science, the fragile physical systems are isolated using technology, such as special refrigerators which cool the systems to very low temperatures. Perfect isolation, while also allowing perfect control for applications, is not possible. Scientists and engineers try to control both the environment and also the signals that encode and read out quantum states from the physical systems. During the COVID-19 pandemic, many researchers' quantum computers and other devices were operated entirely remotely. Scientists found that the rate of errors was dramatically reduced by not having any people in the building. Disturbances that cause errors can come from vibrations, humidity and temperature changes, changing magnetic fields, and radiation. For example, the temperature changes from human bodies being near an experiment affect equipment that control such a system.

This fragility influences the design of computational algorithms and communication and sensing protocols.

A system that is this sensitive to its surroundings has both advantages and disadvantages. In the *Measurement* section we describe how the fragility of quantum systems affects when and what you can learn from the system through measurement. Essentially, any observation or measurement of the quantum state can perturb it in meaningful ways. In some cases this can be an advantage if you want to sense incredibly small environmental disturbances, such as magnetic fluctuations, or know if another person has measured your quantum state.

Associated Glossary Terms

- **Atom**: The basic building blocks of matter. The size of an atom is about 0.1 nm, which means you could fit about 100 million atoms in one centimeter.
- **Electron**: An elementary particle that has negative electric charge and is found in all atoms.
- **Probability Amplitude**: The numbers contained in a quantum state vector. These numbers can be negative or complex.
- **Quantum Operations**: Actions that change the quantum state of a system. Quantum operations physically change the values of quantum properties.
- **System**: For quantum information science, a system is a group of objects that are connected for a particular purpose. For example, an ion trap system consisting of charged atomic particles can be used as the basis of a small-scale quantum computer.

3. QUANTUM MEASUREMENT

KEY CONCEPT

Quantum applications are designed to carefully manipulate fragile quantum systems without observation to increase the probability that the final **measurement** will provide the intended result.

Outline:

a. A measurement is an interaction with the quantum system that transforms a state with multiple possible outcomes into a "collapsed" state that now has only one outcome: the measured outcome. *(See section on qubits)*

b. A quantum state determines the probability of the outcome of a single quantum measurement, but one outcome rarely reveals complete information about the system.

c. Repeated measurements on identically prepared quantum systems are required to determine more complete information about the state.

d. Because of the limitations of quantum measurement (providing only partial information and disturbing the system), quantum states cannot be copied or duplicated.

Prerequistite Knowledge:

- *Quantum State* article
- Probability

INTRODUCTION : MEASUREMENT

One way we gather information about a system is by measuring some physical property, but measurements made on quantum systems are different from conventional measurements.

In everyday life, we often make observations of things around us. We can look with our eyes to see the color of a flower or measure the weight of a package by placing it on a scale. **Measurements** (or observations) are crucial to doing science, and therefore play a key role in quantum information science (QIS). There are some differences, though, between measurements of everyday objects and what we term '**quantum measurements**.' These usually apply to probing objects that are at the scale of atoms, very close to zero temperature, or both. Quantum measurements differ from ordinary measurements in two fundamental ways:

1. Quantum measurements, in general, alter the state of the system we are trying to measure.
2. The outcomes of quantum measurements are inherently random and not completely predictable.

We need to take these differences into consideration to properly design quantum technologies for various applications.

a. A measurement is an interaction with the quantum system that transforms a state with multiple possible outcomes into a "collapsed" state that now has only one outcome: the measured outcome.

Observations of everyday objects are predictable.

We use measurements to collect information about a physical system. To illustrate what we mean by a measurement, let's start with an example of measuring a property of an everyday object.

Example: Measuring the Length of a Table

If we want to measure the length of a table, we can place a measuring tape along the top. The table has a specific fixed length and our measurement of it will reveal this value. If the table is actually 100 cm long, we expect that the measuring tape will tell us that the table is 100 cm long. The measuring tape doesn't change the length of the table in any way – it simply reveals its length.

Quantum systems, like electrons, are different from everyday systems because observing them (performing measurements on them) affects their properties.

Now let's compare measurement of a property of an everyday object with the measurement of a quantum system. Measuring a property of a quantum system, like an electron or atom, requires the measurement device to interact with that system. Unlike the table example, though, the interaction between a quantum system and its measurement device has the possibility of changing the state of the system. This is a fundamental fact about quantum measurements and is associated with the concept of **quantum state "collapse"** described below.

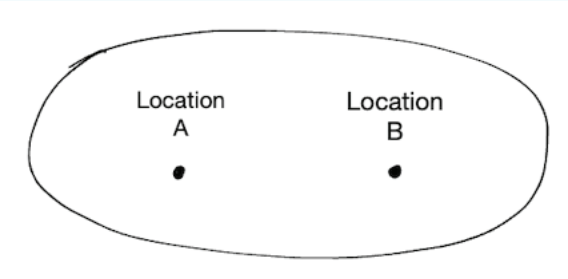
Moreover, properties of a quantum system are not determined prior to measurement. When measuring the table, its length was a certain value and was simply revealed by measurement. By contrast, a property of a quantum system does not necessarily have a fixed value prior to its measurement.

Quantum objects can be in a superposition state (a quantum state that is a superposition of different states) prior to measurement.

Before a quantum system is measured, its quantum state can describe multiple possible outcomes, any of which might reveal itself upon measurement. This multiplicity is called superposition, and is contextualized with the example below.

Example: Measuring the Position of an Electron

Let's consider measuring the position of a particle, like an electron, which in this case can be at two possible positions: Location A or Location B.



A key aspect of a quantum particle is that it can be in a **superposition** of different quantum states. It is possible for an electron to be neither definitely fixed in Location A or B before the measurement of its position at any moment in time, but equally as likely to be in one as the other.

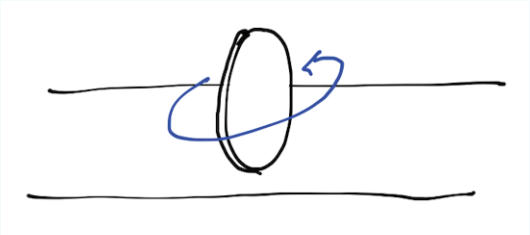
On the other hand, for an everyday object like a table, we know that the table has a certain length, like 100 cm and cannot be in a superposition of two different lengths. Atoms and electrons are quantum systems, and therefore can be in a state of having more than one possible measurement outcome.

After measurement, a superposition state "collapses" into one of the possibilities at random.

Before we measure the position of the electron, its quantum state contains multiple possible outcomes. For example, there may be a 50% chance of measuring it at Location A and a 50% chance of measuring it at Location B. *After* the first measurement, however, the quantum state now describes a 100% chance of measuring the same outcome that was measured the first time. If the measured outcome is Location A, then the new quantum state after the measurement will *only* have Location A as a possible outcome. Any further immediate measurements of the particle's location will always give Location A. Similarly, if the first measured outcome is Location B, then immediately after, the quantum state will *only* have Location B as a possible outcome. If, on the other hand, you started over again with the same quantum state that was in a superposition of Location A and B, then your measurement outcome could be either A or B, just as it was before.

Spinning Coin Analogy

If you spin a coin on the surface of a table, it has two possible outcomes while it is spinning: head or tails. If the coin lands on heads, this is like the state of the coin "collapsing" into the state of landing heads up. The landing of the coin heads up is the measurement outcome in this analogy, and after this occurs, we will always observe the coin as heads. (Of course, coins are not quantum objects, so there isn't actually quantum superposition in this system.)



The quantum state after a measurement is often called a **"collapsed" state**, because it no longer has the possibility of multiple outcomes immediately after it is measured. The collapsed state only has one possible outcome: the previously measured outcome. A quantum state collapses, or changes from having multiple possible outcomes to just one outcome, instantaneously when you make a measurement. Subsequent measurements of the same quantum system will always give the same result as the first measurement. This is true unless you perform more operations on it which change the state of the system (such as, in the case of the coin, spinning it again).

Observation and measurement affect the way we design quantum devices

The fact that observations of a quantum system can change the system's state has important implications for designing quantum applications. For example, if any aspect of the quantum system changes unintentionally while it's being used, then you might get the wrong result when you measure the outcome of a quantum application. Therefore, to do anything useful with a quantum system, great care must be taken to isolate it from accidental measurements caused by us or its environment.

Isolated quantum systems are artificial in nature.

Quantum systems exist naturally, but isolation of a system from its environment and manipulating them for quantum applications requires sophisticated engineering. For example, atoms are quantum systems, but when they are arranged into a solid, such as a piece of iron or a diamond, it can be difficult to control them for quantum applications without significant engineering. Quantum devices are designed to perform precise quantum operations that manipulate quantum states and to also avoid unintentional measurements or observations. This type of design is necessary to increase the likelihood that a quantum computer will produce the intended result from a computation, to send information securely using quantum cryptography protocols, and for quantum sensors to detect small signals, such as electromagnetic radiation.

(See the later article *Decoherence* for more about preserving fragile quantum states. See *Quantum Computing*, *Quantum Communication*, and *Quantum Sensing* for more about quantum applications.)

b. A quantum state determines the probability of each possible outcome of a single quantum measurement, but one outcome rarely reveals complete information about the system.

Quantum states determine the probability of each possible measurement outcome.

At the quantum scale, measurement outcomes are inherently random and not completely predictable. That is, we can determine the *probability* of each possible outcome from the quantum state, but not what the actual outcome will be of any single measurement. The randomness of measurement outcomes is not due to defects or inaccuracy in our measurement devices. It is also not because of any lack of skill in using these measurement devices. Randomness is simply an inherent property of nature as described by quantum physics (also called quantum mechanics).

One measurement outcome rarely reveals complete information about the system.

A single measurement only results in a single possible outcome. One quantum measurement is typically insufficient for revealing complete information about the particle's quantum state.

Example: Measuring the Position of an Electron

Using the example above, let's say the electron now has a quantum state that gives it a 75% chance of being in Location A and a 25% chance of being in Location B. This 75% / 25% probability distribution is a critical aspect of the particle's quantum state. A single measurement, however, does not reveal the probability distribution; it only reveals the particle to be in Location A or B.

c. Repeated measurements on identically prepared quantum systems are required to determine more complete information about the state.

Repeated measurements on identically prepared quantum systems give us more information about the state of a system.

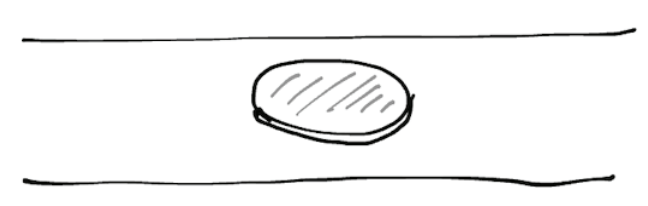
We already know that a single measurement does not reveal the probability of any outcome, just the outcome of that single measurement. However, repeated measurements on identically prepared systems can give us more information about the probabilities of each possible outcome.

Example: Weighted Coin

Imagine if your job is to determine whether a coin is "weighted" (constructed so that it is more likely to land on one side than the other). Spinning the coin and observing how it lands once will not answer this question. Instead, you would spin it many times - say 100 times - and see whether or not each side came up approximately 50 times.

Likewise, if we have placed an electron in a superposition state and calculated that it should have a 75% probability of being measured in Location A and a 25% probability of being in Location B, we would need many repeated measurements on identically prepared electrons to verify this probability distribution.

Remember that a measurement alters the state of a quantum system. So if the first measurement collapses the superposition, repeated measurements that follow will always reveal that same measured state (this assumes that nothing happens to subsequently change the state). This is like looking at a coin after it has stopped spinning. It will simply continue to show you the same result.



It is only through repeating the entire experiment on the system, *prepared in the same identical quantum state*, that we can obtain more complete information about the state. The more times we repeat this experiment, the more we will learn about the probability distribution of the measurement outcomes and the probability amplitudes that make up the quantum state vector. For the spinning coin analogy, this means that we need to pick up the coin and *spin it again and again in the same way*, and the more times we do this experiment, the more we learn about the coin.

Quantum scientists study different methods for learning about quantum states based on measurements.

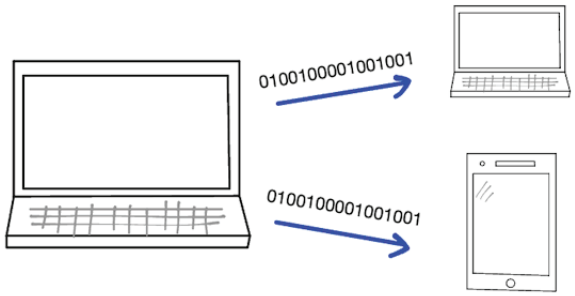
The study of using the results of measurements on identically prepared systems to reconstruct an unknown quantum state is called *quantum tomography*. Just like a CT (computed tomography) scan in medicine can use a series of virtual slices to reconstruct an image of the body, quantum scientists have developed various techniques which allow a series of measurements to reconstruct an unknown quantum state. This has applications for scientists who want to better understand the operation of their quantum devices.

d. Because of the limitations of quantum measurement (providing only partial information and disturbing the system), quantum states cannot be copied.

We can copy classical data using our computing devices.

We frequently copy or duplicate data with our personal computers. (These ordinary, non-quantum computers are referred to as **classical computers**.) For example, you might have a favorite picture that is stored on multiple devices - on your phone, your computer, and in the cloud. Or, you might want to post a picture on social media, so whenever a friend sees that post, the app makes a copy of the picture to send to their device.

Each time classical data is copied, the sequence of bits representing the data is stored in a new, different location. This can be done without destroying the original data. You can have as many copies as you want, with none of the new copies affecting the old ones. To do this, the computer measures the state of each classical bit in the original set of data and recreates them all in the new location.



It is impossible to copy quantum states.

Quantum systems are different. Making perfect new copies of unknown quantum states is impossible. This fact is known as the No-Cloning Theorem to quantum scientists.

Quantum measurements have two limitations that make copying a quantum state impossible.

- First, a single measurement does not provide all the information necessary to replicate the original copy of the state. A measurement provides a single outcome, not the probability of measuring each possible outcome (or the probability amplitudes representing a quantum state vector).
- Second, a measurement destroys ("collapses") the original copy of the state which prevents us from making subsequent measurements to obtain more information about the quantum state.

We cannot make multiple copies of quantum data, and we are limited in what we can do with a single copy of an unknown quantum state. We can physically move the quantum system around or send its quantum state to a new location by other means such as teleportation. (See the later article *Quantum Communication* for a description of teleportation and a discussion of why teleportation doesn't allow us to copy a quantum state.) But if we don't know the quantum state of our system, we can't copy it.

The impossibility of copying quantum states affects how we design quantum applications.

Why does this matter? The fact that it is impossible to copy quantum states tells us that we cannot design quantum applications the same way that we design applications for classical devices. For example, programs running on classical computers often require making multiple copies of data stored as bits during the operation of the program. Since we can't copy quantum states, we need to design programs that run on quantum computers differently than we have learned to program on classical computers.

Associated Glossary Terms

- **Classical Computer**: Classical computers (ordinary, non-quantum computers) store data represented in binary form as sequences of bits, 0s and 1s. For example, each letter, each color (associated with a certain amount of red, green, and blue), and even sounds are stored on a computer as sequences of bits
- **Superposition**: A combination of multiple quantum states. A quantum system, like an electron or photon, can have a quantum state that is a linear combination of many different mutually distinguishable states.

4. QUBITS (QUANTUM BITS)

KEY CONCEPT

The **quantum bit**, or **qubit**, is the fundamental unit of quantum information, and is encoded in a physical system, such as polarization states of light, energy states of an atom, or spin states of an electron.

Outline:

a. Unlike a classical bit, each qubit can represent information in a superposition, or vector sum that incorporates two mutually exclusive quantum states.

b. At a particular moment in time, a set of n classical bits can exist in only one of 2^n possible states, but a set of n qubits can exist in a superposition of all of these states. This capability allows quantum information to be stored and processed in ways that would be difficult or impossible to do classically. *(See section on quantum computing)*

c. Multiple qubits can also be entangled, where the measurement outcome of one qubit is correlated with the measurement outcomes of the others.

Prerequistite Knowledge:

- *Measurement* article

INTRODUCTION : QUANTUM BIT (QUBIT)

Classical computers store information in the form of bits.

The basic unit of information is the **bit** (short for **binary digit**). A single bit represents one of two possible values, 0 or 1.

One Bit : `0` or `1`

Classical computers (ordinary, non-quantum computers) store data in binary form as sequences of bits, 0s and 1s. For example, each letter, each color (associated with a certain amount of red, green, and blue), and even sounds are stored on a computer as sequences of bits.

The word "Qubit" : `01010001 01110101 01100010 01101001 01110100`

The color red : `11111111 00000000 00000000`

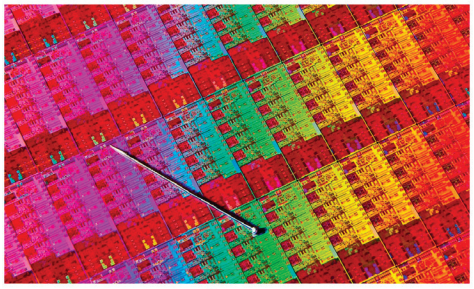
A sound file : `10110100000100111101000...`

When you use a computer for shopping, getting directions, or other everyday activities, you are usually using high-level applications that hide the details of how computers store and process binary data. You don't really need to know about bits to write an email message or to play a video on your phone. However, knowing about bits helps us understand how computers work. And a good understanding of these details is important for computer engineers or programmers who write code for controlling hardware components (such as connecting your phone to headphones).

Bits are encoded in physical systems.

The idea of a digital computer, and the representation of information in the form of bits, was a revolutionary idea in the history of computing. But to build an actual computer, you need to create it out of physical objects that can store and process bits.

In the early days of computing, devices called vacuum tubes were used to process binary data. Modern computing devices are built using a technology based on semiconductor materials. Computer processors now consist of billions of semiconductor **transistors**, the tiny electrical switches that perform binary logic operations in a computer, and binary data is stored in semiconductor memory or other types of memory such as magnetic storage devices.



Computer processor technology
(Intel Free Press, https://flic.kr/p/d8WPAo, CC BY-SA 2.0)

The fundamental unit of quantum information is the quantum bit (or qubit).

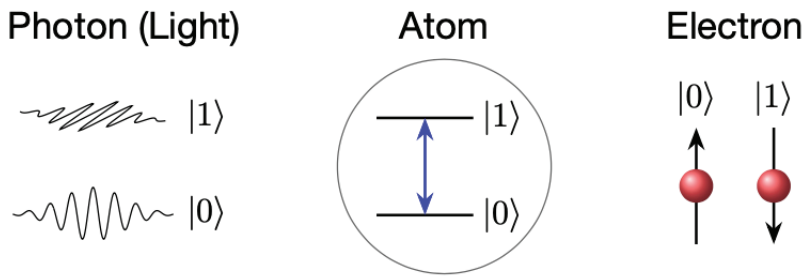
The basic unit of information for quantum computing is the **qubit** (short for **quantum bit**), and it is the quantum counterpart of the classical bit. Quantum computers store and process information in the form of qubits.

Quantum bits (qubits) are encoded in physical systems.

Any property of a quantum system that has two discrete levels or values can be used to encode a qubit. Examples of physical systems used for qubits are:

1. **Polarization** states of light: Light is composed of tiny packets of energy called photons. A photon can behave like a wave. For example, it can oscillate in a particular direction, a property called polarization. A qubit can be encoded in two different polarization directions of a photon.
2. Energy states of an atom: Electrons can have different levels of energy within an atom. Two of these energy levels can serve as a qubit.
3. **Spin** states of an electron: Electrons have a property called spin that makes them act like tiny magnets. Qubits can be encoded in two different values of an electron's spin property, analogous to the two opposite orientations of a bar magnet.

These examples are illustrated in the figure below, where the two states are written as |0› and |1›, a commonly used notation for the 0 and 1 states of a qubit.



Scientists are currently exploring a wide range of different materials and technologies for creating qubits. There is still a lot of research to be done to determine which of these systems, or which combination of these systems, will be best suited for the design of large-scale quantum information applications.

(See the *Decoherence* article for more discussion about the different types of technology used to create physical qubits.)

a. Unlike a classical bit, each qubit can represent information in a superposition, or vector sum that incorporates two mutually exclusive quantum states.

A qubit can be in a superposition, or vector sum, of two mutually exclusive quantum states.

One of the biggest differences between a classical bit and a quantum bit (or qubit) is that while a classical bit contains a single value (0 or 1), a qubit can hold any combination of 0 and 1 *at the same time*. This is called **superposition**.

Recall from the *Measurement* article that an electron, prior to measurement, is not fixed in either location A or B, but in a superposition of both locations at the same time. The state of an electron could extend to a superposition of three or more locations in an atom. A qubit is a specific type of quantum system where its quantum state can be in a superposition of only two states, 0 and 1.

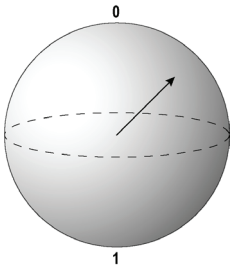
While a qubit can exist in any one of the infinite number of possible combinations of 0 and 1, we do not have direct access to all of these combinations. To extract information from a qubit, we need to measure it, and when a qubit is measured, we will only ever observe a 0 or a 1. As discussed in the *Measurement* article, the qubit will immediately "collapse" from a superposition state into the state representing the measured outcome.

Mathematically, a superposition is a combination, or a vector sum, of two mutually exclusive quantum states, one state representing a 0 and another state representing a 1. Superposition of quantum states is similar in many ways to the superposition we observe of sound and water waves.

For qubits, superposition involves combining the **probability amplitudes** of two quantum state vectors, whereas a superposition of water waves involves combining the heights of multiple water waves together. Also, for qubits, the probability amplitudes can be complex numbers (involving the imaginary number i), which is not true for the heights of water waves.

Superposition states of a qubit can be visualized on a sphere.

As mentioned in an earlier article *Quantum State*, scientists often represent the state of a qubit geometrically as a vector pointing to the surface of a sphere. Every possible superposition state of the qubit can be represented by a specific location on the surface of this sphere. Vectors that point to locations closer to the north pole of this sphere are more likely to be measured as a 0, and vectors that point closer to the south pole are more likely to be measured as a 1.



b. At a particular moment in time, a set of n classical bits can exist in only one of 2^n possible states. But, a set of n qubits can exist in a superposition of all of these states. This capability allows quantum information to be stored and processed in ways that would be difficult or impossible to do classically.

At a particular moment in time, a set of n classical bits can exist in only one of 2^n possible states.

In classical computing, a single bit can exist in only one of two possible states, 0 or 1. Two bits can represent four possible states (00, 01, 10, or 11), but at any point in time, the bits only represent one of these states. A set of three bits can exist in one of 8 possible states (000, 001, 010, 011, 100, 101, 110, or 111), and so on.

Here's a listing of all possible states from 1 bit up to 4 bits:

```
1 bit  :  0 1
2 bits  :  00 01 10 11
3 bits  :  000 001 010 011 100 101 110 111
4 bits  :  0000 0001 0010 0011 0100 0101 0110 0111
           1000 1001 1010 1011 1100 1101 1110 1111
```

Each additional bit doubles the number of possible states. In general, a set of n classical bits has 2^n possible states. If we interpret these states as **binary (or base 2) numbers**, a set of n bits can represent any number from 0 through $2^n - 1$.

A set of n qubits can be in a superposition of 2^n possible states.

Just as a single qubit can exist in a superposition of two possible states, 0 and 1, a set of n qubits can exist in a superposition of all of the 2^n possible states that n classical bits can be in.

For example, two qubits can be in a superposition of four possible states 00, 01, 10, and 11. When two qubits are measured, we will only observe one of the four possible outcomes 00, 01, 10, or 11, and the qubits will immediately "collapse" into the state representing the measured outcome.

The capability of n qubits to exist in a superposition of 2^n possible states prior to measurement allows quantum information to be stored and processed in ways that are difficult or impossible to do classically.

Superposition is one of the key features of quantum systems that is used in all three areas of QIS (computing, sensing, and communication) to store and process information in ways that are difficult or impossible to do classically.

And just like the superposition of water waves, superposition of quantum states leads to interference effects where different parts of a quantum state can be amplified or canceled. This is a feature that can be exploited in QIS applications.

Here are some examples of how superposition is used in quantum applications:

- **Quantum computation**. Quantum computers can store and process qubits that are in superpositions of quantum states. This provides them with a computational advantage over classical computers. First, even a small number of qubits in superposition can encode a large amount of information. One reason that supercomputers are incapable of solving computational problems like simulating the dynamics of molecules is that computer memory is not large enough to store the full quantum state of even 100 qubits. Quantum computers also have processing advantages. Well-designed quantum algorithms perform operations on qubits in a way that cancels certain probability amplitudes until a correct answer is likely to be measured.

  (See the later article *Quantum Computing* for more information about potential applications of quantum computing.)

- **Quantum sensing**. Superposition of quantum states can be used to create interference effects that can be used for quantum sensing. For example, quantum sensors using interference can be used to sensitively measure magnetic fields and other physical properties.

  (See the later article *Quantum Sensing* for more information.)

c. Multiple qubits can also be entangled, where the measurement outcome of one qubit is correlated with the measurement outcomes of the others.

Multiple qubits can be entangled.

Multiple qubits can share a relationship called entanglement. This is a strong relationship between qubits that can persist even when the qubits are physically separated by large distances.

When qubits are entangled, the measurement outcome of one qubit is correlated with the measurement outcomes of the others.

Qubits that are entangled with each other share a strong connection that causes their measurement outcomes to be **correlated**. Knowing the measurement outcome of one qubit can give you information about the measurement outcome of another qubit that is entangled with the first qubit.

The next article on *Entanglement* describes this in more detail and discusses applications of entanglement for QIS applications. Also, see the article *Quantum Communication* for a specific application of entanglement to **quantum teleportation**, a method for sending quantum states between distantly located quantum systems.

Associated Glossary Terms

- **Bit**: A bit (short for binary digit) is the basic unit of information. One bit represents one of two possible values, 0 or 1.
- **Interference**: Waves can experience interference effects when they are combined together. For example, parts of a water or sound wave can be amplified (constructive interference) or cancel out (destructive interference). In a similar way, a superposition of two or more quantum states can lead to different parts of a quantum state to be amplified or canceled out.
- **Polarization**: The polarization of light describes the direction that the light wave is oscillating. Most sources of light (such as light from sunlight and ordinary light bulbs) consist of a random mixture of light with different polarization states. Light with a specific polarization can be prepared using lasers or with devices called polarizers.
- **Spin**: The spin of an electron is a property that makes electrons behave like a tiny magnet. Electron spin is a quantized value and can take only one of two possible values.

5. ENTANGLEMENT

KEY CONCEPT

Entanglement, an inseparable relationship between multiple qubits, is a key property of quantum systems necessary for obtaining a quantum advantage in most QIS applications.

Outline:

a. When multiple quantum systems in superposition are entangled, their measurement outcomes are correlated. Entanglement can cause correlations that are different from what is possible in a classical system.

b. An entangled quantum system of multiple qubits cannot be described solely by specifying an individual quantum state for each qubit.

c. Quantum technologies rely on entanglement in different ways. When a fragile entangled state is maintained, a computational advantage can be realized. The extreme sensitivity of entangled states, however, can enhance sensing and communication.

Prerequistite Knowledge:

- *Qubits* article

INTRODUCTION : ENTANGLEMENT

Entanglement is an inseparable relationship between multiple qubits.

Entanglement is a feature of quantum mechanics, the theory describing the properties of tiny objects, such as atoms and electrons. Entanglement connects multiple particles such that they behave as a single combined entity, even if the individual particles themselves become separated by large distances. As we discussed in the *Qubits* article, the connection that exists among entangled particles causes their individual measurement outcomes to be correlated.

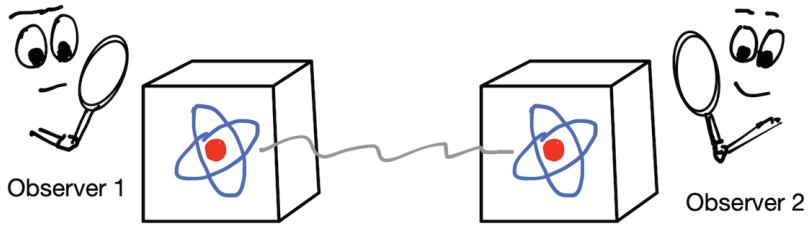
Entanglement is a key property of quantum systems necessary for obtaining a quantum advantage in most QIS applications.

Historically, quantum entanglement was a source of intense philosophical debate among the pioneers of quantum physics, including Einstein. The properties of entanglement and its apparent implications made physicists question the feasibility of the theory itself as a valid or complete description of nature. Regardless of this, the Second Quantum Revolution has demonstrated the usefulness of quantum entanglement. During the past 30 to 40 years, a wide array of initial applications have been developed, such as quantum-secure communications and powerful quantum computing algorithms, which rely on the entanglement of multiple particles for optimal operation. Many quantum scientists think of entanglement in a more practical light, as a new kind of physical resource that can be used to obtain a quantum advantage in all areas of QIS, including quantum computing, communication, and sensing. (See later articles *Quantum Computing*, *Quantum Communication*, and *Quantum Sensing* for more information about these applications.)

a. When multiple quantum systems in superposition are entangled, their measurement outcomes are correlated. Entanglement can cause correlations that are different from what is possible in a classical system.

When multiple quantum systems in superposition are entangled, their measurement outcomes are correlated.

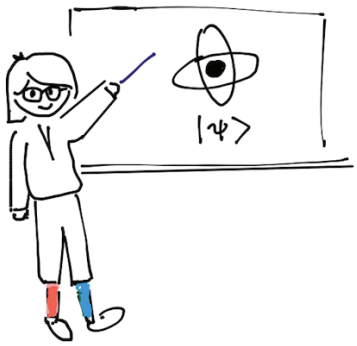
Quantum objects that are entangled with each other share a connection that causes their measurement outcomes to be highly correlated. Observations made on one part of the entangled system will be related to observations made on other parts of the system.



Entangled Quantum System

Correlations are relationships between observed values.

Correlations can be found all around us. The correlations that are produced by quantum entanglement share some similarities with the types of correlations we can find in everyday life.



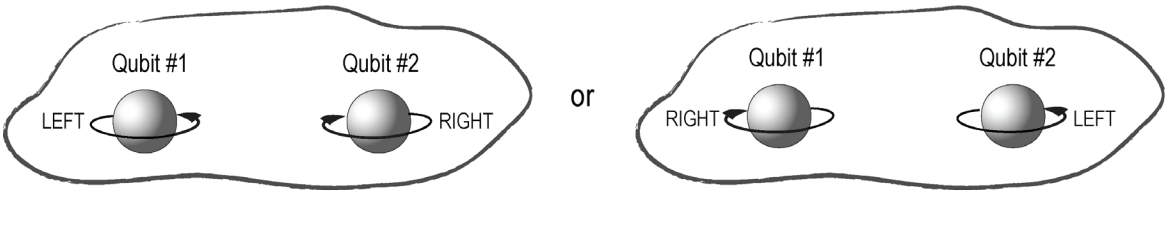
For example, let's say that your favorite teacher has a particular way of wearing socks. Based on your observations, you notice that the color of your teacher's left sock is always different from the color of their right sock. So, if you see one pink sock, you know for sure that the other sock is not pink. The colors of your teacher's socks are said to be **correlated** with each other, because there is a relationship between the colors of each sock.

Correlations can be observed when we make measurements on quantum objects.

We can also find correlations when we make observations in the quantum world. This will happen if two qubits interact with each other and become entangled. We will find correlations when we observe or measure the properties of each qubit.

Example of Correlation in the Quantum World

Suppose we have two particles that are spin-entangled. Spin is a property of quantum particles that makes them act like tiny magnets. For the entangled particles in this example, you will always observe that the particles are spinning in opposite directions. Thus, if you measure that the first particle is spinning to the left, you will immediately know that the other particle will be seen spinning to the right, and vice versa. Which one is right or left is not determined prior to measurement and the outcome is a random choice between the two. This randomness is a key feature of quantum mechanics. You can say that the spins of the entangled particles are correlated, because there is a relationship or connection between the spins of each particle.



Entanglement can cause correlations that are different from what is possible in a classical system.

So far, we have described how the correlations found in entangled quantum systems are like the correlations in classical systems. What makes quantum entanglement special is that the correlations observed cannot be explained with any non-quantum (classical) theory. In other words, entanglement, which is a purely quantum effect, is the best explanation we have for the combination of randomness and high degree of correlation observed in quantum systems, such as atoms and electrons.

For many years, scientists, like Einstein, expressed uneasiness with the implications of quantum entanglement. They wondered if the remarkably strong correlations displayed by entangled states were perhaps actually due to undiscovered "hidden variables" in the particles that predetermined what the measurement outcomes were going to be. If this were true, it would mean that all quantum particles are really classical at heart.

In 1964, a physicist named John Bell figured out a way to demonstrate that the correlations from entanglement are not due to hidden variables. He came up with a test system where the correlations arising due to hidden variables have a limit – and if instead you apply a quantum theory with entanglement, the correlations within the system surpass this limit.

J. S. BELL
1964

Experiments building on Bell's work have led to a greater understanding of entanglement and the ability to use entanglement in quantum applications.

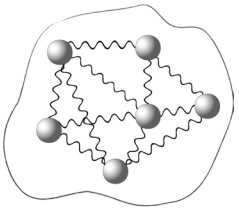
Starting in the 1970s and continuing through to today, physicists John Clauser, Alain Aspect and others have performed a series of increasingly precise experiments that have tested and confirmed Bell's predictions about quantum entanglement.

Entanglement is now the basis for a wide range of QIS applications. One such example is quantum teleportation. (See the later article *Quantum Communication* for a description of quantum teleportation.) In 1997, Anton Zeilinger's research group was the first to perform a teleportation experiment. Recently, physicists Clauser, Aspect, and Zeilinger were awarded the 2022 Nobel Prize in Physics for their efforts in understanding and manipulating quantum entanglement.

b. An entangled quantum system of multiple qubits cannot be described solely by specifying an individual quantum state for each qubit.

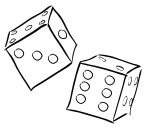
Entangled qubits act like an inseparable whole.

A set of entangled qubits acts as an inseparable combined system or entity. An overall quantum state describes the full multi-qubit system. Even when the qubits are physically separated by vast distances, we regard a set of entangled qubits as a whole rather than as individual constituent parts.



Any system consisting of independent parts can be described by considering each individual part separately.

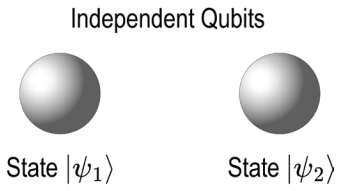
Consider an ordinary classical situation, like rolling a pair of dice. We can describe all of the possible outcomes of rolling a pair of dice in terms of what happens to each of the individual dice rolls separately.



For example, we can compute the probability of rolling two 6's by multiplying the probabilities of rolling a 6 on each dice separately. Since the probability of rolling a 6 is 1/6 for each dice, the probability of rolling two 6's is equal to the product (1/6) x (1/6) = 1/36.

Independent qubits can be described by specifying the individual quantum states.

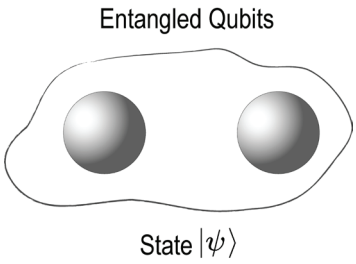
We have a similar situation when describing independent qubits. If we have two unentangled qubits, then each qubit has its own quantum state, and nothing will be missing from the description of the overall state of the whole two-qubit system if we simply specify their individual quantum states. (The figure below uses a commonly used notation, |ψ›, for a quantum state.)



An entangled quantum system of multiple qubits cannot be described solely by specifying an individual quantum state for each qubit.

On the other hand, when qubits are entangled, it is impossible to describe the whole system simply by specifying an individual quantum state for each qubit. We need to specify a quantum state for the *overall* entangled system.

Any description of the entangled qubits based only on putting together (e.g., multiplying) separate descriptions of each individual qubit will lack important information about the overall state of the system. It will crucially miss out on the correlations inherent between each of the entangled qubits. This is why we consider a set of entangled qubits as a single combined entity rather than a combination of independent parts.



c. Quantum technologies rely on entanglement in different ways. When a fragile entangled state is maintained, a computational advantage can be realized. The extreme sensitivity of entangled states, however, can enhance sensing and communication.

Quantum technologies rely on entanglement in different ways.

Quantum technologies in all three areas of QIS (computing, sensing, and communication) depend on entanglement to provide unique capabilities that classical systems cannot provide.

1. Quantum computation

Quantum algorithms that run on quantum computers can take advantage of multi-qubit entanglement to solve certain problems faster than any classical computer. Entanglement allows quantum computers to efficiently store and process a superposition of many classical states during processing. For example, a 4-qubit quantum computer can process 16 possible values in superposition. Increasing the capacity of the quantum computer to 100 qubits already surpasses the processing capacities of any classical supercomputer. However, all of the information in a quantum computer is not accessible at once. At the end of any computation, measurement yields only one bit of information. So while the processing capacity gives quantum computation a significant speed advantage, it only applies to certain problems where we have algorithms, or recipes, for processing entangled states and superpositions. For example, scientists have developed an algorithm for factoring large numbers more efficiently on a quantum computer compared to a classical computer. This has applications in current methods we use to secure private information (See the later article *Quantum Computing*.)

2. Quantum sensing

In the area of quantum sensing, scientists turn the sensitivity of fragile entangled states into a mechanism for making precise measurements. For example, we can use entangled quantum states of light or atoms to improve the precision of magnetometers for measuring tiny magnetic fields. Another example is atomic clocks that use quantum entanglement for making extremely precise time measurements. These measuring devices are so precise, they can approach the fundamental limits on measurement precision dictated by the laws of quantum mechanics. (See the later article *Quantum Sensing*.)

3. Quantum communication

Being able to create and distribute fragile entangled states is also important in the area of quantum communication and quantum networks. The ability to more entangled quantum states between different parts of a network allows users to process information in ways that are not possible in classical systems. For example, quantum teleportation is a communication protocol that uses shared entanglement as a resource to allow users to efficiently send quantum information to each other without needing to transmit any physical qubits. When there is interference with an entangled quantum state it changes due to quantum measurement. This makes eavesdropping across quantum networks highly detectable (See the later article *Quantum Communication*.)

Associated Glossary Terms

- **Correlation**: A mutual relationship or connection between two or more things. Multiple quantum particles that are entangled with each other display measurement outcomes that are highly correlated.

6. DECOHERENCE

KEY CONCEPT

For quantum information applications to be successfully completed, fragile quantum states must be preserved, or kept **coherent**.

Outline:

a. Decoherence erodes superposition and entanglement through undesired interaction with the surrounding environment. Uncontrolled radiation, including light, vibration, heat, or magnetic fields, can all cause decoherence.

b. Some types of qubits are inherently isolated, whereas others require carefully engineered materials to maintain their coherence.

c. High decoherence rates limit the length and complexity of quantum computations; implementing methods that correct errors can mitigate this issue.

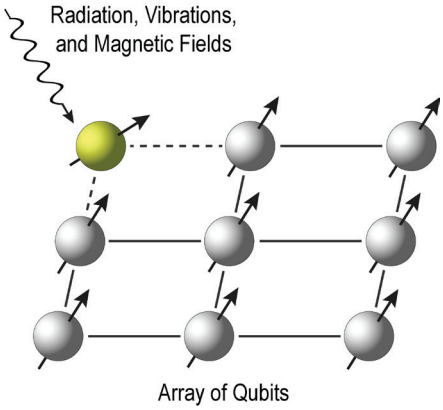
Prerequisite Knowledge:

- *Entanglement* article

INTRODUCTION : DECOHERENCE

Decoherence is an interaction with the environment that results in a loss of quantum information.

Decoherence happens when qubits experience uncontrolled interactions with their environment resulting in a loss of quantum information. Minimizing the effects of **decoherence** is one of the major challenges for creating physical devices for QIS applications, like quantum computers. It is a more general phenomenon, but here we are only talking about it in the context of qubits. Protecting quantum systems from environmental disturbances is a challenge because qubit states are very fragile. They can be easily corrupted by interactions with random elements of the environment such as heat or electromagnetic **radiation**.



Radiation can cause decoherence by changing a qubit's state. Researchers are developing better ways to protect qubits from decoherence.

For quantum information applications to operate successfully, it is necessary to maintain the fragile quantum states created in quantum systems. For this reason, researchers are working to better understand the many mechanisms of decoherence and find better ways to protect qubits from harmful environmental interactions. In addition, new methods are being developed to fix the errors caused by decoherence.

a. **Decoherence** erodes superposition and entanglement through undesired interaction with the surrounding environment. Uncontrolled radiation, including light, vibration, heat, or magnetic fields, can all cause decoherence.

Decoherence erodes superposition and entanglement through undesired interaction with the surrounding environment.

Quantum systems have two properties that are critical to obtaining an advantage over classical systems - **superposition** and **entanglement**. Decoherence can destroy both of these quantum properties. This can have detrimental effects:

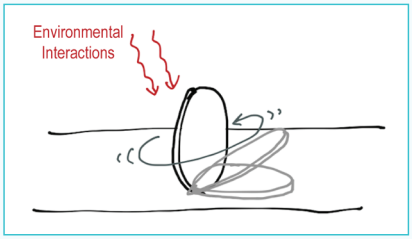
- A quantum computer that is unable to maintain qubits in superposition and multi-qubit entanglement will be no more powerful than an ordinary classical computer.
- Quantum communication protocols like teleportation also rely on entanglement. Users attempting to send qubits to each other using quantum teleportation will experience errors if the entanglement they share has been degraded by decoherence.
- Transmitting quantum information over short and long distances relies on isolation– otherwise the information can get scrambled due to decoherence.

Decoherence can change and degrade superposition states.

Let's consider the effects of decoherence on superposition and entanglement. First, decoherence changes a superposition state in unpredictable ways. As described previously in the *Measurement* article, any measurement that we perform on a qubit will "collapse" that qubit's superposition state into just one of two possible mutually distinguishable states corresponding to measurement outcomes states. Some measurements are on purpose, such as those that we engineer as part of a quantum application. Decoherence generally refers to the undesired and uncontrolled environmental interactions that can also cause a qubit's superposition state to change, or even collapse.

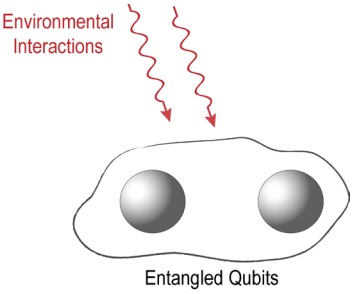
Spinning Coin Analogy

Let's consider the spinning coin analogy for a qubit from the previous *Measurement* article. The state of our qubit would be the coin spinning (perhaps a weighted coin to favor one side over the other), with some probability that it will fall as heads or tails. A small amount of decoherence might change the probability of measuring heads or tails, or alter the entanglement relationship between it and another coin. More decoherence might cause the coin to stop spinning and fall to one side, even though we did not want to measure it.



Decoherence can erode entanglement between qubits.

Similarly, decoherence can affect an entanglement relationship between multiple qubits. (The properties of entanglement are described in the previous *Entanglement* article.) With entanglement, the outcome of a measurement on one qubit can be highly correlated with a measurement on another qubit. However, decoherence can erode entanglement and cause the states of the qubits to become independent again. Entanglement is a critical feature of multi-qubit systems, so losing this relationship can drastically reduce the power of quantum computations and other quantum information applications.



Uncontrolled radiation, including light, vibration, heat, or magnetic fields, can all cause decoherence.

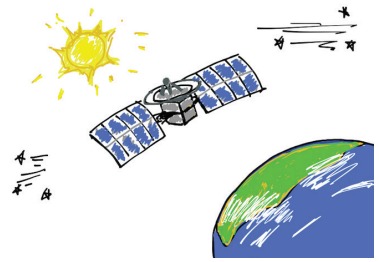
Decoherence can be caused by uncontrolled **radiation** that interacts with and degrades the qubits in a quantum system. For example, stray light of certain frequencies can disrupt qubits, and therefore a quantum computer. Heat can destroy certain types of qubits that must operate at low temperatures. Changing temperatures and humidity can interfere with classical control systems for a qubit, which is also disruptive. Changing magnetic fields can also cause decoherence. During the 2020-21 pandemic, quantum computers in a research laboratory experienced many fewer errors caused by decoherence. The ambient vibrations from the everyday activities of people in the building (e.g., walking in the rooms and hallways, body heat) caused enough errors that their absence during the pandemic improved the reliability of the quantum computers enough to be noticed by the researchers.

Decoherence can be mitigated by isolating a quantum system from its surrounding environment.

The susceptibility of a qubit to having its quantum state corrupted depends on a few things. This includes the type of physical system used to build the qubit (e.g., atoms or materials) and the way that the environment interacts with that physical system.

Classical Computing Analogy

We can make an analogy with classical computing devices that are designed to operate in extreme conditions. For example, a satellite flying in space experiences many more impacts from solar particles and cosmic rays compared to a computer system on earth. Therefore, extra engineering is required to shield the satellite equipment from exposure to radiation. In addition, engineers must design ways to detect, tolerate, and even correct the errors that inevitably occur.



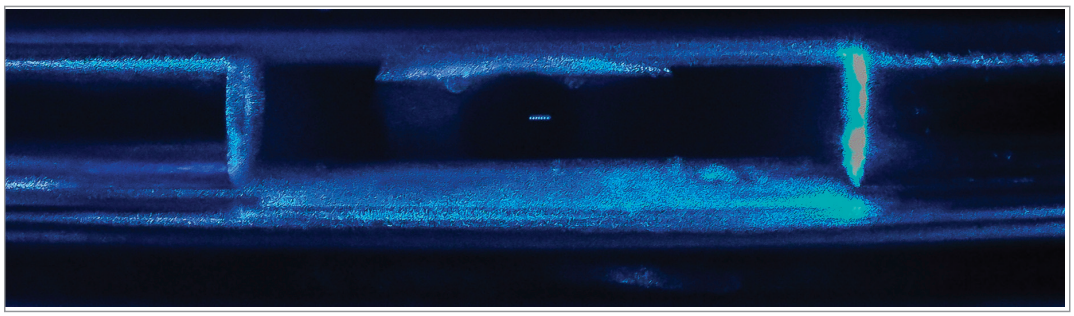
Quantum devices are much more susceptible than classical computers to the effects of minute disturbances from the environment. The qubits stored and processed in a quantum device are very fragile compared to the bits stored in a classical computer. Even a slight bump from a random particle or a tiny bit of radiation vibration can destroy the information in a qubit.

b. Some types of qubits are inherently isolated, whereas others require carefully-engineered materials to maintain their coherence.

Creating and controlling qubits is a great scientific and engineering challenge. Decoherence is a major reason why it is so difficult.

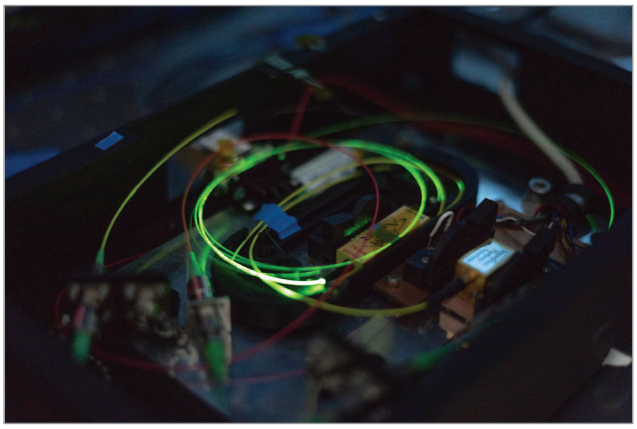
No single qubit technology is currently dominant. Instead, there are a variety of approaches and technologies being explored for building quantum computers and other types of quantum devices. Researchers are creating qubits out of particles like electrons, photons, atoms, and ions (charged atoms). In addition, new types of semiconductor and superconducting materials are being developed for building quantum technologies.

Different technologies require different approaches to preventing errors caused by decoherence.



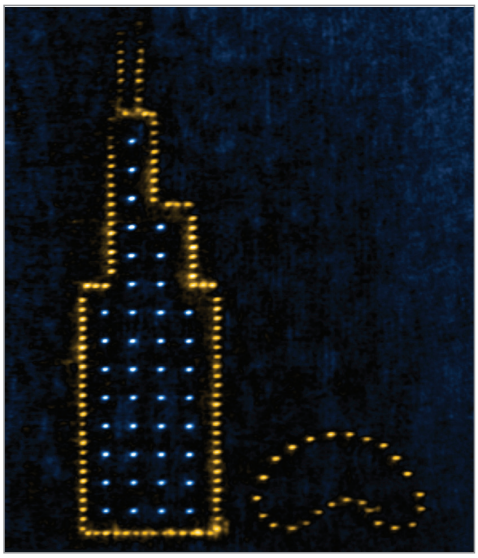
Trapped Ion System: Barium trapped ion crystal

Image Credit: AFRL Information Directorate
(https://www.quantum.gov/quantum-image-gallery/)



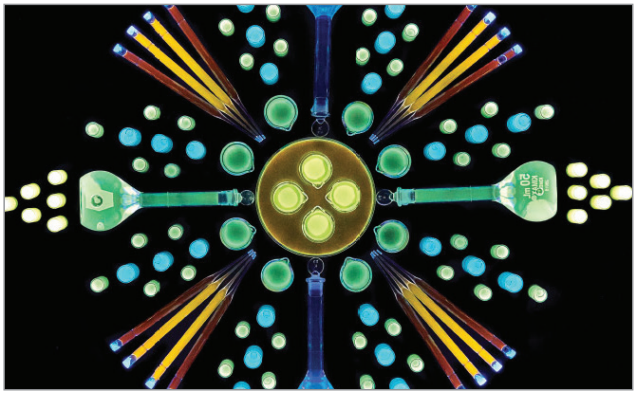
Light can be used as a qubit. Lasers can be used as a source of photons for use as qubits.

Image Credit: NASA (https://www.quantum.gov/quantum-image-gallery/)



A neutral atom qubit array configured to show the Willis Tower and the Cloud Gate sculpture in Chicago.

Image Credit: Hannes Bernier, University of Chicago (https://www.quantum.gov/quantum-image-gallery/)



Tubes filled with Quantum Dots.

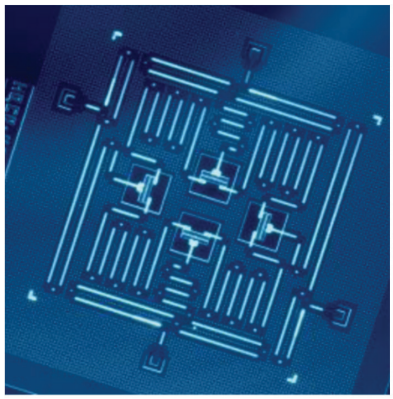
Image Credit: Photo by Christa Neu, Lehigh University Communications and Public Affairs (https://www.quantum.gov/quantum-image-gallery/)

Some types of qubits are inherently better isolated.

Qubits represented by ions and held by electromagnetic fields have internal energy levels that are inherently more isolated from typical disruptions like magnetic fields and radiation. This means we can preserve their coherence for relatively long periods of time. Qubits can also be made out of photons, which are elementary particles of light. Photons do not interact easily, so these types of qubits are also relatively isolated from certain decoherence mechanisms.

Other types of qubits require carefully-engineered materials to maintain their coherence.

For example, some researchers are creating what are called **superconducting qubits**. These qubits are built out of electrical circuits in superconducting material that is cooled down to extremely low temperatures. A superconducting qubit is macroscopic in size and can easily lose its quantum properties if there are defects in any of its electrical components. Preserving and improving the coherence of superconducting qubits requires extensive research in designing new materials and improving the fabrication process of the quantum circuits.



Superconducting qubits

(J. M. Gambetta et al., CC BY 4.0)

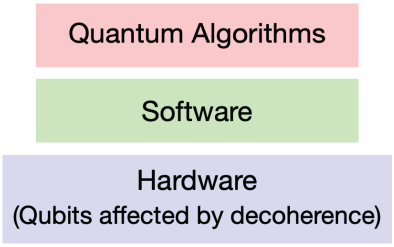
https://www.nature.com/articles/s41534-016-0004-0

c. High decoherence rates limit the length and complexity of quantum computations; implementing methods that correct errors can mitigate this issue.

High decoherence rates limit the length and complexity of quantum computations.

In classical computing, computer hardware and software are optimized so that errors are not noticeable to computer users; you can keep your computer on for days without restarting it, and you will probably not notice any errors due to the outside environment. In quantum computers, though, errors due to decoherence are so frequent that they are a major factor in preventing current quantum computers from performing useful work compared to classical computers.

The high rate of errors experienced by qubits has a large effect on all aspects of building a quantum computer - from writing the algorithms, to optimizing the resulting code, to designing the hardware. Improvements made to each layer of the process help us to get the most out of the qubits we can currently build. However, without robust hardware, quantum programs are significantly limited in how long they can run and how many quantum operations they can perform.



To help mitigate the issue of high decoherence rates in quantum computers, researchers are developing a technique for protecting qubits called quantum error correction.

Error correction is a technique that is widely used in many areas of modern digital technology, from data storage, to wireless communication networks, to satellite communications. Error correction of classical information typically works by adding extra redundancy to a system in a way that allows information to be restored if errors occur.

Classical error correction algorithms require the ability to freely measure and copy information. However, in the quantum world, this is not possible. Measurements alter qubit states, and qubit states cannot be copied. (See the earlier *Measurement* article.) This makes it difficult to translate classical error correction methods into the quantum world.

However, researchers have figured out ways to encode information across multiple qubits, which helps to protect it from being destroyed by the environment. Quantum computers that use quantum error correction are able to run longer and more complex quantum computations. The downside is that **quantum error correction** has a cost. It requires considerably more physical qubits, and adding qubits to a system is not easy. Many of the most promising applications may require thousands or even millions of extra qubits.

Associated Glossary Terms

- **Ion**: An electrically charged atom. Quantum computers based on trapped ions use atoms, like ytterbium, barium, orcalcium, with a net positive charge.
- **Photon**: An elementary particle of light. Photons travel at the speed of light and can act as both a particle and a wave.
- **Radiation**: A form of energy that can be transmitted through space or some material. Examples include light, vibration, heat, and magnetic fields.
- **Superconductor**: A material that allows an electric current to flow without resistance.

7. QUANTUM COMPUTING

KEY CONCEPT

Quantum computers, which use qubits and quantum operations, will solve certain complex computational problems more efficiently than classical computers.

Outline:

a. Qubits can represent information compactly; more information can be stored and processed using 100 qubits than with the largest conceivable classical supercomputer.

b. Quantum data can be kept in a superposition of exponentially many classical states during processing, giving quantum computers a significant speed advantage for certain computations such as factoring large numbers (exponential speed-up) and performing searches (quadratic speed-up). However, there is no speed advantage for many other types of computations.

c. A fault-tolerant quantum computer corrects all errors that occur during quantum computation, including those arising from decoherence, but error correction requires significantly more resources than the original computation.

Prerequistite Knowledge:

- *Entanglement* article
- *Decoherence* article

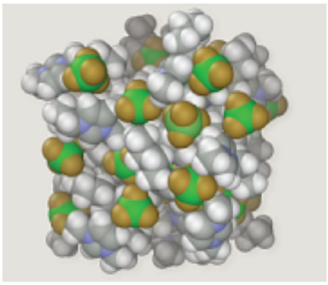
INTRODUCTION : QUANTUM COMPUTERS

Computers are used everywhere in our modern day world.

Computing devices
(Matthieu Riegler, CC-BY, Wikimedia Commons)
(Acabashi CC-BY-SA 4.0)

Computers were originally invented to automate and accelerate repetitive mathematical calculations that humans previously performed by hand. For example, in 1642, Blaise Pascal invented a mechanical calculator to reduce the effort required to calculate taxes. Likewise, in the 1930s and 40s, computers were built to perform the calculations required to aim weapons and assist codebreaking efforts in World War II. In the 19th-century, computer science pioneer Ada Lovelace imagined applications far beyond what the original inventors intended. Improvements to digital computer technology during the 20th century led to the modern information age, where computers now play a role in everything from science and technology, medicine, to music and the arts. We use computing devices at home, at school, and at work, and we depend on them for almost every aspect of our daily lives.

Classical computers have limits to their computational power.



Molecular simulation
(P99am, Wikimedia Commons)

The computing power of classical computers has dramatically changed the world we live in. But classical computers, the usual type of computers that store information as bits, have their limits. For example, scientists found that accurately simulating even simple molecular systems was too difficult for computers to handle.

Quantum computers are a new kind of computer-based on using qubits and quantum operations.

In the early 1980s, people started to imagine that some of these difficult calculations might be more efficiently performed on computers that operate based on the principles of quantum mechanics, the theory describing the properties of particles. Those initial ideas have since evolved into a thriving new area of scientific research centered around a device called a quantum computer. **Quantum computers** are a new kind of computer that is based on storing information in the form of **qubits** and doing computations with quantum operations. (See the earlier article *Qubits*.)

Quantum computers will solve certain complex computational problems more efficiently than classical computers.

Quantum computers will be able to solve *certain* computational problems significantly faster than any classical computer, even the most powerful supercomputers. Scientists are currently researching future potential applications of quantum computers, which may include more efficient molecular simulations for drug design or the ability to find more efficient delivery truck routes. Breaking a commonly used type of encryption called RSA is another application that has driven much of the investment in quantum computing over the past two decades. Potential applications in data security have also motivated researchers to search for alternative encryption methods and *standards* that are secure even against someone with a quantum computer.

Scientists don't expect quantum computers to completely replace classical computers, because this new technology is only useful for applications that can take advantage of the unique features of quantum systems, such as superposition and entanglement. Therefore, although important uses of quantum computers have already been discovered, quantum computing is currently like a hammer in search of a nail. Quantum programmers are working on identifying additional types of problems that can be solved more quickly with quantum computers compared to tackling them with classical computers.

a. Qubits can represent information compactly; more information can be stored and processed using 100 qubits than with the largest conceivable classical supercomputer.

Classical computers store information as bits.

Classical and quantum computers differ in the way they store information. As discussed in the earlier *Qubits* article, classical computers store information in the form of bits. A classical bit holds either a 0 or a 1, which can be physically stored either within a computer chip or on a hard drive. Every computing device that you own stores information as sequences of bits. For example, the number 72 is represented on your device as the 8-bit binary number sequence 01001000 and the character 'A' as the 8-bit sequence 01000001.

Qubits can represent information compactly.

Quantum bits (or **qubits**) can store information much more compactly than bits. As discussed in the *Qubits* article, there is a big difference between bits and qubits. A set of n classical bits can be in only one of 2^n possible states, while a set of n qubits can exist in a ***superposition*** of all 2^n possible states. To describe a superposition of this complexity requires us to store the values of 2^n probability amplitudes (or coefficients).

In the simplest case of representing a single qubit (n = 1), this requires us to store two probability amplitudes. This translates to a total of 256 bits on a classical computer if each amplitude is represented by 128 bits.

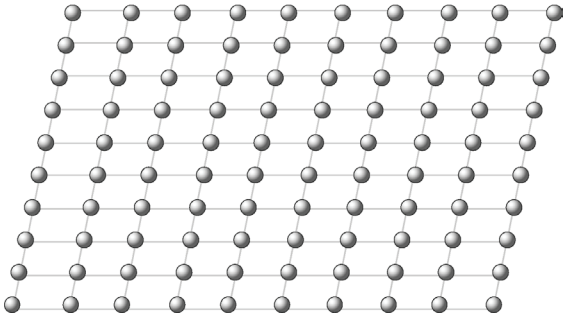
1 Qubit
(Described by 256 bits)

More information can be stored and processed using 100 qubits than with the largest conceivable classical supercomputer. There is a caveat to this.

Because we have to store so many values (probability amplitudes) when describing a qubit, classical computers quickly run out of storage when attempting to fully represent a modest number of qubits. In other words, as the number of qubits grows, the storage requirements on a classical computer increase exponentially. The total amount of data quickly goes far beyond the memory capacity of any classical supercomputer that could ever be built.

Consider trying to store and process the information contained in a set of 100 qubits, shown below as a 10 x 10 array, on a classical computer. We would need to keep track of 2^{100} probability amplitudes to process this much quantum information. Assuming each probability amplitude takes 128 bits to describe, a classical computer would need a memory capacity of at least 2^{107} bits to store all of this data. This is simply a staggering number of bits. It is more than 100,000,000,000,000,000,000,000,000,000,000, which is the number 1 followed by 32 zeros! This is far more data than can be supported by any conceivable form of classical technology.

Array of 100 Qubits
(Described by more than 2^{107} bits)

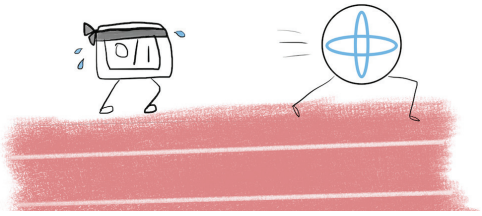


While a quantum computer can manipulate this number of qubits, and even more, the end of the quantum calculation results in only a single value. This is a limitation and major difference of quantum computing compared to parallel classical computation.

b. Quantum data can be kept in a superposition of exponentially many classical states during processing, giving quantum computers a significant speed advantage for certain computations such as factoring large numbers (exponential speed-up) and performing searches (quadratic speed-up). However, there is no speed advantage for many other types of computations.

Quantum data can be kept in a superposition of exponentially many classical states during processing, giving quantum computers a significant speed advantage for certain computations.

Quantum computers use superposition and entanglement to process information. The combination of having a storage capacity of exponentially many classical states, the ability to operate on all of these values in superposition at once, and entanglement (qubits interacting with each other quantum mechanically) results in a significant speed advantage for specific computational applications. However, as mentioned above, this is not the same as parallel processing. Quantum measurement at the end of a quantum computation still only gives you one single answer or outcome. The possible outcomes are captured by the quantum state. See the description of *Quantum Measurement.*



Quantum computers give an exponential speed-up for factoring large numbers.

As we mentioned in the introduction, perhaps the most prominent application for quantum computers is for breaking an encryption system called RSA. This type of encryption is widely used for sending private information over the Internet, for instance, to look up banking information or to send credit card information to purchase items on a store's website.

Prime Factorization of Large Numbers

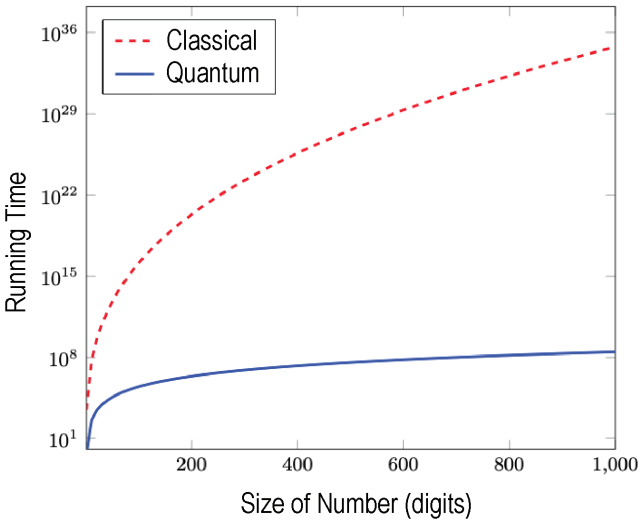
15226050279225333605356183781326374297180681149613
80688657908494580122963258952897654000350692006139
= 37975227936943673922808872755445627854565536638199
× 40094690950920881030683735292761468389214899724061

The security of RSA depends on the difficulty of factoring very large numbers. An example of factoring a number is finding the prime factors 2, 3, and 13 of the number 78. A computer can handle the factorization of relatively small numbers, like 78, without any problem. However, for finding the factors of very large numbers, programs that run on classical computers are incredibly slow. Discovering a fast method to factor numbers would make RSA encryption unsafe to use.

Classical computers struggle with factoring large numbers, because the time it takes to factor a number grows exponentially with the size of the number. If you wanted to factor a number with less than 100 digits, you could do it on a computer in less than an hour. But if you doubled the size of that number to around 200 digits, then it would be basically hopeless for you. A number that size takes huge resources to factor. In 2020, researchers using tens of thousands of computers around the world took months to find the prime factors of a 250-digit number using the most efficient classical factoring algorithm known to mathematicians.

Now consider trying to break RSA encryption. Someone attempting to break RSA encryption would need the ability to factor a number with over 600 digits. This task is completely infeasible with current technology. That's why we feel confident using RSA encryption to keep our private messages safe on the Internet.

In 1994, mathematician Peter Shor discovered a fast method for factoring large numbers (now called **Shor's algorithm**) that runs on a quantum computer. He showed that quantum computers can factor numbers in an amount of time that grows like the cube (the third power) of the size of the number. This gives quantum computers a huge speed advantage over classical computers. The following graph gives you an idea of how much faster exponential growth (red curve) is compared to polynomial growth (blue curve) like Shor's algorithm.



Quantum computers give a quadratic speed-up for performing searches.

Quantum computers also offer the potential for computational speed-ups for certain other applications. For example, problems that require searching through a large set of potential solutions, such as combing through a large database, can be solved faster on quantum computers.

Computer scientist Lov Grover showed in 1996 that a quantum computer takes about the square root of the time it would take a classical computer to solve this type of problem. This is referred to as a quadratic speed-up. Performing a search on a quantum computer only provides a more moderate **quadratic speed-up**, as opposed to the exponential speed-up for factoring, but this would offer benefits for a wide range of important applications.

Another example where they may be some level of improvement with quantum computing is optimization. Delivery companies spend millions of dollars a day on gasoline, and making optimal decisions about which packages to put on which truck and in what order to deliver the packages would save billions of dollars a year and decrease carbon emissions. Classical computers are limited in their ability to solve this problem because trying every possible combination is intractable and using heuristics (approximate decisions) leads to non-optimal solutions. However, quantum computers may be able to find more efficient solutions to such problems in a reasonable amount of time. Scientists are still doing research on how to program quantum computers for more applications.

However, there is no speed advantage for many other types of computations.

We have discussed how quantum computers provide a speed advantage for certain problems, like factoring large numbers and performing searches. One might wonder if quantum computers can help speed up every type of computation compared to a classical computer. Interestingly, the answer is no. For some problems, they simply don't help much at all.

Suppose you want to know whether a sequence of 0s and 1s contains an even or odd number of 1s. For example, 10110 has an odd number of 1s and 11011 has an even number of 1s. If you had a really long sequence, like a binary sequence with many millions of bits, you might hope that having a quantum computer could speed up this task. But it turns out that despite having access to the properties of superposition and entanglement, a quantum computer cannot solve this problem that much faster than a classical computer.

Quantum scientists have discovered that there are many other problems like this for which quantum computers have no speed advantage over classical computers. Knowing that quantum computers can help with certain types of problems, but not others, is useful for scientists who are trying to program quantum computers to gain a better understanding of the circumstances under which quantum computers can provide a speed advantage over classical computers.

c. A fault-tolerant quantum computer corrects all errors that occur during quantum computation, including those arising from decoherence, but error correction requires significantly more resources than the original computation.

A fault-tolerant quantum computer corrects all errors that occur during quantum computation, including those arising from decoherence.

While quantum computers have advantages over classical computers in terms of storage density and computational speed for particular problems, it is challenging to build a quantum computer that is reliable enough to solve problems that we are interested in. One of the main obstacles is **decoherence**. Quantum states are fragile and difficult to maintain accurately due to undesired interactions with the surrounding environment. (See the *Decoherence* article for more information about the fragility of quantum states.) In addition, errors that occur during quantum operations can easily spread and multiply, ruining the computation if they are not controlled somehow.

To solve these problems, complex error correction schemes have been invented. The ultimate goal is to create what is called a **fault-tolerant quantum computer**, a quantum computer that is able to detect and contain the spread of errors during long, complex quantum computations. Current quantum computers suffer from high decoherence rates and have limited computing power. It is believed that we will need to learn how to build large-scale fault-tolerant quantum computers to run quantum algorithms on problems of practical interest.

But error correction requires significantly more resources than the original computation.

As mentioned earlier in the *Decoherence* article, protecting quantum computers from decoherence with quantum error correction has a cost. Building a quantum computer with error correction requires considerably more resources and additional complexity in the system.

Quantum error-correction schemes involve adding redundancy, by spreading out the quantum information contained within a single qubit across many other qubits. Each of these physical qubits carries a small amount of information about the protected qubit (called a **logical qubit**), allowing for a certain level of protection from noise sources. The fault-tolerant quantum computer will then be able to perform long quantum computations on a set of nearly ideal, low-error, logical qubits.

Depending on the error rates of the original physical qubits in the system, achieving fault-tolerance for the quantum computer may require that the error-correction scheme supply thousands of physical qubits per logical qubit. For a particular quantum application, like Shor's algorithm, that needs a few thousand logical qubits to operate on, this translates to millions of physical qubits to ensure a fault-tolerant computation. This is the challenge facing researchers who are racing to build better and more powerful quantum computers.

Associated Glossary Terms

- **Fault-Tolerant Quantum Computer**: A quantum computer that is able to detect and contain the spread of errors during long, complex quantum computations.
- **RSA Encryption**: A type of encryption that is commonly used to send private information over the Internet, for example, to look up banking information or to send credit card information to purchase items on a store's website.

8. QUANTUM COMMUNICATION

KEY CONCEPT

Quantum communication uses entanglement or a transmission channel, such as optical fiber, to transfer quantum information between different locations.

Outline:

a. Quantum teleportation is a protocol that uses entanglement to destroy quantum information at one location and recreate it at a second site, without transferring physical qubits.

b. Quantum cryptography enhances privacy based on quantum physics principles and cannot be circumvented. Due to the fragility of quantum systems, an eavesdropper's interloping measurement will almost always be detected.

Prerequistite Knowledge:

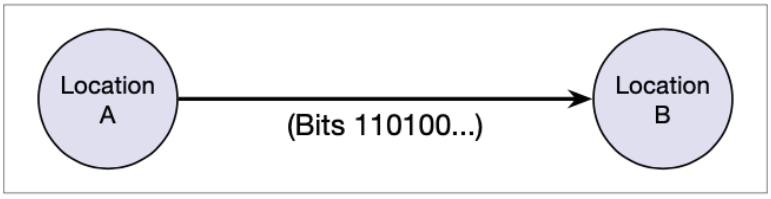
- *Entanglement* article
- *Decoherence* article

INTRODUCTION : QUANTUM COMMUNICATION

Classical (electronic) communication is the sending and receiving of information in the form of bits.

Communication is the exchange of information between different locations. With classical communication, we send digital information stored in the form of bits, 0s and 1s. This includes sending texts, emojis, photos, or other messages over Wi-Fi at home or at a public place like a library or a coffee shop.

Classical Communication



A **transmission channel** is the path or the physical medium through which the message is sent from the sender to the receiver. There are a variety of channels that are capable of sending binary data, like optical fiber cable for high-speed data transmission or a wireless connection with radio waves (like the previous Wi-Fi example).

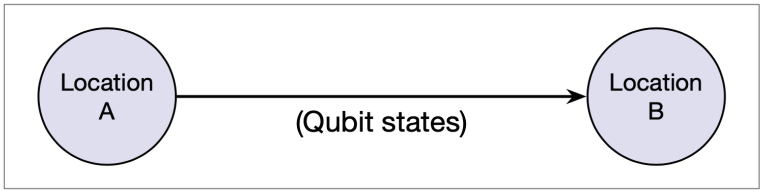
Quantum communication is the sending and receiving of information in the form of qubits, using either entanglement or a transmission channel.

Quantum communication refers to methods for sending **quantum information** from one place to another. A quantum network refers to a set of connected quantum devices. Together these are the quantum counterpart to classical communication networks: quantum communication is about sending information carried by *qubits* rather than bits.

Here are some ways we can perform quantum communication:

1. We can use a physical **transmission channel** to send qubit states over long distances. For example, we can send quantum states of light over an optical fiber cable.
2. Qubit states can also be sent between different locations through the use of entanglement by using **quantum teleportation** (which is described below). In this case, matter does not move, only information.

Quantum Communication



a. Quantum teleportation is a protocol that uses entanglement to destroy quantum information at one location and recreate it at a second site, without transferring physical qubits.

The very nature of quantum information makes quantum communication a challenge.

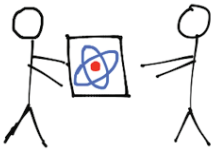
If you want to send some classical data from one place to another, your phone or computer is able to determine which bits need to be sent and then sends that information over to the other device. It would be nice if this straightforward strategy would work for quantum communication. But you can't do this with qubits!

If you have a qubit in some unknown state and you want to send it to someone else, you can't just measure it to completely determine what state you have and then send the quantum information (or state) over to the other party intact. (You can call your friend and share the result of your measurements though). The fundamental properties of quantum states and quantum measurements make this impossible. A single measurement of a qubit cannot give complete information about its state, and the measurement changes the state of the qubit in the process. Furthermore, you cannot make multiple copies of your unknown quantum state to get around this problem.

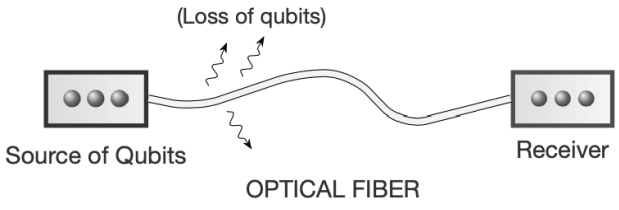
(See the earlier article *Measurement* for a discussion about measurements and the impossibility of making copies of quantum states.)

Qubits can be physically sent over a transmission channel.

If I have a qubit stored in a quantum system, like an electron or an atom, I can simply give you the electron or the atom. Therefore, the most straightforward way to transmit quantum information is to send the actual physical system containing the qubits over a transmission channel.



However, most of the time physically sending qubits to someone in this way has limitations, especially if the qubits are difficult to move or when we need to send these qubits over long distances. For example, we can send quantum states encoded onto light using optical fiber as a transmission channel. But optical fibers can be lossy for many colors of light, which can cause the information to be corrupted or lost. It is far less feasible to move physical qubits around that are made with atoms or materials.



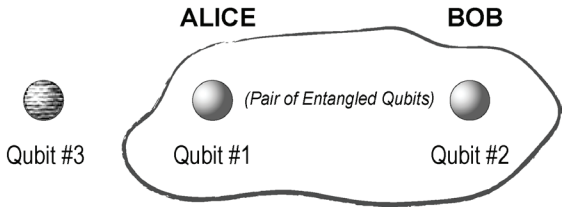
Quantum teleportation is a method for transferring quantum information between different locations that makes use of entanglement.

Fortunately, entanglement offers an alternative. **Quantum teleportation** is a communication protocol for sending quantum information from one place to another without physically moving any qubits. The protocol achieves this by utilizing entanglement, a quantum connection that can exist between two qubits located in separate locations. (See the earlier article *Entanglement* for a discussion about entanglement.)

QUANTUM TELEPORTATION PROTOCOL

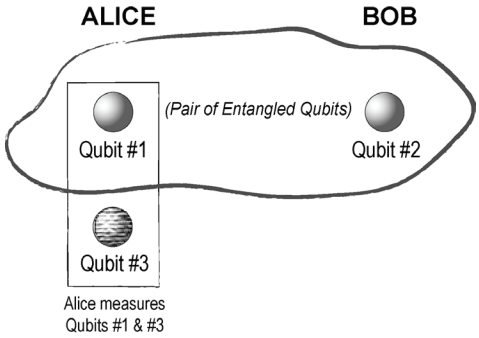
Step 1: The setup - Alice and Bob start with two entangled qubits and Alice has a message state to send

Suppose two users, Alice and Bob, are located in different locations and have qubits that are entangled with each other (the qubits labeled Qubit #1 and Qubit #2 in the figure on the right).



Alice also has a message state (represented by the striped pattern on Qubit #3) that she wants to send to Bob. Teleportation allows Alice to move the message state from Qubit #3 to Qubit #2 without ever needing to physically send Qubit #3. This works even though it is possible that Alice has no idea what the message state is.

Step 2: Alice's measurement

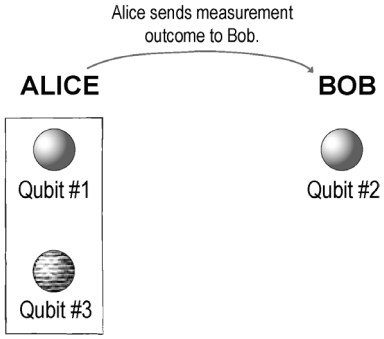


Alice begins the teleportation protocol by combining both of her qubits together (her half of the entangled pair and the message qubit) and then making a measurement. Alice will observe one out of four possible outcomes from this measurement.

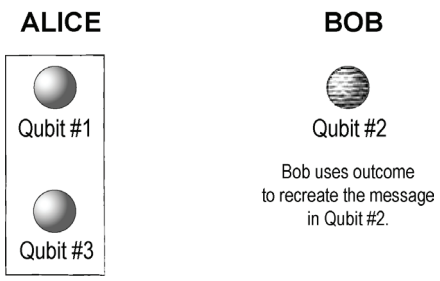
Alice's measurement also causes Bob's Qubit #2 to change because of the connection it shares with Alice's Qubit #1 through entanglement.

Step 3: Alice sends the result of the measurement

Alice uses a classical communication channel to tell Bob the result of her measurement. At this point, Bob's Qubit #2 is equally likely to be in one of four possible states.



Step 4: Bob recreates the message state



Bob uses Alice's measurement result to adjust his own Qubit #2 to recreate the state of the message qubit at his location. Once this happens, Bob will end up with the only copy of the message state. (Alice's Qubit #3 has no trace of the original message state.)

Summary:

In summary, quantum teleportation allows two users to use the entanglement that they originally shared to destroy the sender's copy of a message state and recreate it at the receiver's location. The sender can achieve this without actually physically moving any qubits to the other location.

Common misconceptions about quantum teleportation

There are some common misconceptions about quantum teleportation, so we should clarify what teleportation can and cannot do.

1. First, we cannot teleport physical objects from one place to another like in science fiction stories. No physical objects are destroyed or created. We can only teleport the quantum states of particles (e.g., information), not the particles themselves.
2. As discussed in the *Measurement* article, it is impossible to copy a quantum state. Therefore, it is not possible for both the sender and the receiver to have a copy of the message state. Teleportation causes the sender's copy of the message to be destroyed, so at the end of the teleportation protocol, only the receiver will have a copy of the message state.
3. The teleportation process does not involve faster-than-light communication. The receiver does not receive the message state from the sender until she sends him the result of her measurement (in Step 3 of the quantum teleportation protocol above). This part of the protocol cannot go faster than the speed of light.

Teleportation sounds like something from science fiction, but it's more like sending a quantum text message.

(Quantum Atlas: https://quantumatlas.umd.edu/entry/teleportation/)

Quantum teleportation has been demonstrated by researchers in a variety of settings.

Quantum teleportation has been experimentally achieved using different types of qubits, including photons, atoms, and electrons. Teleportation for applications in long-distance quantum communication is an active area of research. In one notable teleportation experiment in 2017, quantum states of photons were sent through space up to 1400 km from a ground observatory to a low-Earth-orbit satellite.

b. Quantum cryptography enhances privacy based on quantum physics principles and cannot be circumvented. Due to the fragility of quantum systems, an eavesdropper's interloping measurement will almost always be detected.

Cryptography plays an important role in modern society. Encryption techniques based on unproven mathematical assumptions have the potential to be broken.

Cryptography is the study and practice of encrypting our data to keep our information secret from others. The availability of secure communication is an important part of modern society. For instance, every day we rely on encryption techniques when we send information over the Internet or use passwords to protect files on our computers.

However, the security of much of modern day encryption is based on unproven mathematical assumptions. For example, there is a common type of encryption (called **RSA**) that is based on the assumption that it is difficult for computers to find the prime factors of very large numbers. (See *Quantum Computing*)

Prime Factorization of Large Numbers

15226050279225333605356183781326374297180681149613
80688657908494580122963258952897654000350692006139
= 37975227936943673922808872755445627854565536638199
× 40094690950920881030683735292761468389214899724061

Quantum cryptography enhances privacy based on quantum physics principles and cannot be circumvented.

Quantum cryptography is an area of quantum information science that offers us new ways to enhance privacy. Since it is based on quantum physics principles which cannot be circumvented, it has the potential to add an additional layer of security to computer networks beyond what is possible with classical cryptography.

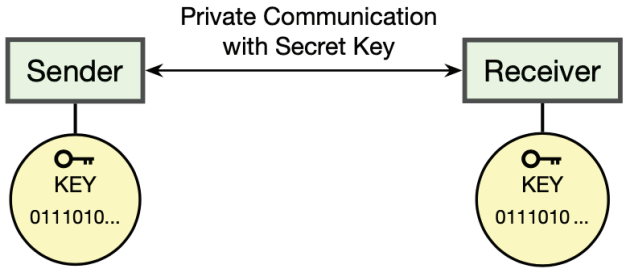
Quantum cryptography can protect against eavesdroppers. Due to the fragility of quantum systems, an eavesdropper's interloping measurement will almost always be detected.

To ensure that a communication network is secure, we want the ability to detect eavesdroppers. Consider sending mail using the postal service. With paper mail, someone can open the envelope, read our message, and then reseal the envelope. If they are careful enough, we may never know that our message has been read before reaching the intended receiver. Likewise, it is challenging to design classical computer networks in a way that eavesdroppers can be reliably detected.

The laws of quantum physics offer us a new approach for detecting eavesdroppers. The idea behind quantum cryptography is an example of making lemonade from lemons. We take a seemingly undesirable property - the fact that reading (measuring) the state of a quantum system also changes it - and turn it into a desirable property. Quantum cryptography encodes our information using qubits and takes advantage of the fact that any measurement of a qubit collapses the state and changes it in a way that is detectable. (See the *Measurement* article for a description of state "collapse.") It ensures that if someone is trying to read the messages sent over a communication network, the eavesdropper's interloping measurements will almost always be detected.

Quantum key distribution (QKD) allows users to share a secret key. Two parties that share a secret key can send private messages to each other.

One major application of quantum cryptography is called quantum key distribution (QKD). The purpose of QKD is to help users share a secret string of bits called a key. Two parties with a secret key can use their key to encrypt and decrypt private messages with each other.



Example: How two people can encrypt and decrypt a message with a shared key

There are many encryption techniques that use a shared key for secure communication. One of these encryption techniques is called a **one-time pad**. Suppose two people share a secret key, 10001011 11101100. The sender can represent the message "HI" in binary form as 01001000 01001001 (the original message is called the plaintext) using a standard encoding format called ASCII , and encrypt it using the one-time pad method by adding the plaintext message to the key to produce the encrypted code or *ciphertext*, 11000011 10100101.

The receiver can decode the message by adding the code and the key together to reveal the original message "HI". Anyone without the key will not be able to easily decode the message.

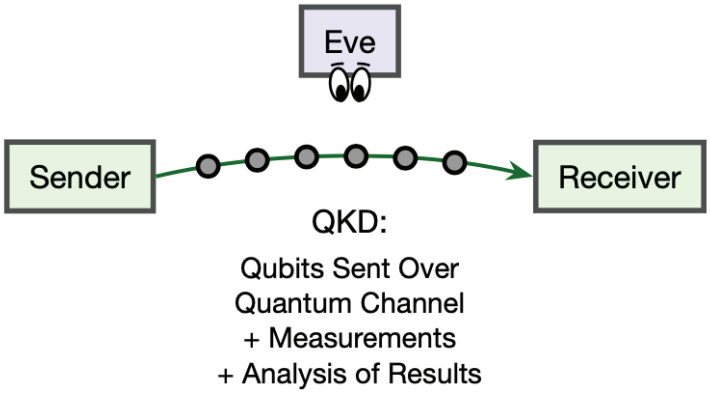
One-Time Pad Example

Plaintext:	01001000 01001001
+ Key:	10001011 11101100
Ciphertext:	11000011 10100101

The benefit of using quantum key distribution (QKD) to create the secret key is that it helps the users detect if eavesdroppers are trying to invade their privacy while they are trying to set up their key.

A brief description of the QKD protocol

If two users, a sender and a receiver, want to communicate securely, they can begin by going through a QKD protocol to generate a shared secret key. QKD involves having the sender send qubits to the receiver over a quantum channel. After the two parties exchange and analyze some measurements of these qubits, they will be able to produce a secret key.



During this process, it's possible that an eavesdropper Eve will attempt to measure some of these qubits to learn a portion of the secret key. However, Eve will collapse the quantum state of qubits she measures, unavoidably changing some of the qubits that were sent to the receiver. As a consequence, the sender and the receiver can figure out that an eavesdropper is present and that the privacy of their key has been compromised. If this happens, they can then discard their compromised key and start over again. If no eavesdropper is detected, then they can feel confident that no one else knows what their key is.

Associated Glossary Terms

- **Classical Communication**: The exchange of classical information (bits) between different locations. This is in contrast to quantum communication, which is about the sharing of quantum information, which is the information carried by qubits.
- **Cryptography**: The study and practice of encrypting our data to keep our information secret from others.
- **Quantum Information**: Quantum information is the information contained within the quantum states of qubits. Quantum information is encoded and manipulated in quantum devices and possesses features such as superposition and entanglement which allow it to be processed in fundamentally new ways.
- **Transmission Channel**: The physical medium through which a message is sent from the sender to the receiver.

9. QUANTUM SENSING

KEY CONCEPT

Quantum sensing uses quantum states to detect and measure physical properties with the highest precision allowed by quantum mechanics.

Outline:

a. The Heisenberg uncertainty principle describes a fundamental limit in simultaneously measuring two specific, separate attributes. “Squeezing” deliberately sacrifices the certainty of measuring one attribute in order to achieve higher precision in measuring the other attribute; for example, squeezing is used in LIGO to improve sensitivity to gravitational waves.

b. Quantum sensors take advantage of the fact that physical qubits are extremely sensitive to their surroundings. The same fragility that leads to rapid decoherence enables precise sensors. Examples include magnetometers, single-photon detectors, and atomic clocks for improvements in medical imaging and navigation, position, and timing.

c. Quantum sensing has vastly improved the precision and accuracy of measurements of fundamental constants, freeing the International System of Units from its dependence on one-of-a-kind artifacts. Measurement units are now defined through these fundamental constants, like the speed of light and Planck’s constant.

Prerequistite Knowledge:

- *Entanglement* article
- *Decoherence* article
- *Quantum State* article

INTRODUCTION : QUANTUM SENSING

Quantum sensing uses quantum states to detect and measure physical properties with the highest precision allowed by quantum mechanics.

Sensors are devices that detect and measure physical properties. This includes light, temperature, and pressure sensors, which allow us to obtain reliable information for applications in science, medicine, transportation, and industry. Sensors are also part of many everyday objects.

High-precision sensors, whether they are optical interferometers or atomic clocks, inevitably have some amount of error that limits their accuracy or resolution. The laws of quantum mechanics determine the fundamental limits for all high-precision measurement instruments.

Quantum sensors are devices that use the particular features of quantum states, such as quantum coherence, quantum phases of matter, and entanglement (see the *Entanglement* article), to enhance the precision and resolution of a measurement beyond what is possible with classical devices and is only limited by quantum mechanics of the particular system.

a. The Heisenberg uncertainty principle describes a fundamental limit in simultaneously measuring two specific, separate attributes. “Squeezing” deliberately sacrifices the certainty of measuring one attribute in order to achieve higher precision in measuring the other attribute; for example, squeezing is used in LIGO to improve sensitivity to gravitational waves.

The Heisenberg uncertainty principle describes a fundamental limit in simultaneously measuring two specific, separate attributes.

The Heisenberg uncertainty principle is a relationship between the measurement uncertainties of two properties. It does not apply to all properties in a physical system. The most common example is position and momentum. Due to the principle, you cannot measure both the **position** (where the object is located) and **momentum** (a physical quantity that describes the object’s motion) of an object with infinite precision. In other words, quantum mechanics says that nature has some inherent fuzziness to it.

However, the principle is more than that. First, it applies not only to position and momentum, but to any two **complementary properties** of the same entity. In this article, we will mostly focus on describing the uncertainty principle for position and momentum. However, other versions of the uncertainty principle based on other complementary properties are also important for applications. For example, there is also a version of the Heisenberg uncertainty principle involving time and energy that is relevant to time-keeping devices, like atomic clocks.

Second, it is not merely that one cannot precisely measure both properties. The uncertainty principle describes a *mathematical relationship* between the uncertainties of two complementary properties that is fundamental.

The Heisenberg uncertainty principle says how small we can make the product of the uncertainties for two complementary properties.

Suppose there is a particle freely moving around– it could be through space or an electron in an orbital around the nucleus of an atom.

As described in the *Measurement* article, there is some element of randomness in measurement outcomes. If we measure the position or momentum of the particle, there will be a spread of possible outcomes around the most likely values. This uncertainty or spread in the possible values is measured statistically by the *standard deviation*:

- Δx - Uncertainty in position (defined as the standard deviation or the spread in the possible outcomes for the measurement of position x)
- Δp - Uncertainty in momentum (defined as the standard deviation or the spread in the possible outcomes for the measurement of momentum p)

The **Heisenberg uncertainty principle** says: The more accurately we know the position of the particle, the less certain we are about the momentum of the particle, and vice versa.

More specifically, it states that multiplying two numbers, the uncertainties in the position and momentum, always results in a product that is bigger than a certain (very small) fixed number:

uncertainty in one property × uncertainty in another property ≥ $\frac{1}{4\pi}$ × Planck's constant

or, stated with the numerical value of the fixed number and measurement units:

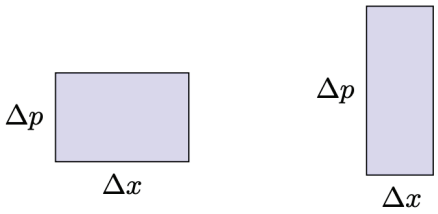
Heisenberg Uncertainty Principle

$$\Delta x \cdot \Delta p \geq 5.27 \times 10^{-35} \text{ J} \cdot \text{s}$$

The Heisenberg uncertainty principle can be described in terms of the area of a rectangle.

Another way to think about this is to imagine we have a rectangle, where the width and height represent the uncertainty in position and the uncertainty in momentum. Then the Heisenberg uncertainty principle tells us that this rectangle can be as wide or skinny as you like, but the ***area of the rectangle*** cannot be smaller than that very small fixed number in the inequality above.

In terms of the rectangles pictured below, we can make the rectangle skinnier in one direction as long as the other direction grows to keep the area of the rectangle above the specified limit. In particular, one thing you cannot do is make the width and height arbitrarily small at the same time! The Heisenberg uncertainty principle prevents us from knowing both the position and momentum of the particle with any desired precision.



Δx : Uncertainty in position

Δp : Uncertainty in momentum

This is how the Heisenberg uncertainty principle works with position and momentum, but it works the same way for other pairs of complementary properties. The only difference is that the (very small) fixed number that appears in the inequality will be different for each case.

The Heisenberg uncertainty principle is not discernible on everyday objects.

One thing to note is that the fixed number that appears on the right side of the inequality above is incredibly small, so the effect of the uncertainty principle is only noticeable for the tiny particles of the quantum world, like electrons, not for objects that we observe in everyday life.

For example, if you knew the position of a baseball extremely precisely, say to within the width of a hair, then the uncertainty in the speed of the baseball would be as small as 10^{-25}mph, which is negligible compared to the speed of a baseball thrown at 60 mph.

Another way to consider this is in terms of waves. Quantum objects are described by waves, and this gives rise to the uncertainty principle. Everyday objects are too large and hot to have quantum wave properties–therefore the implications of the uncertainty principle are negligible unless you are trying to measure wave properties of a system with ultra-high precision.

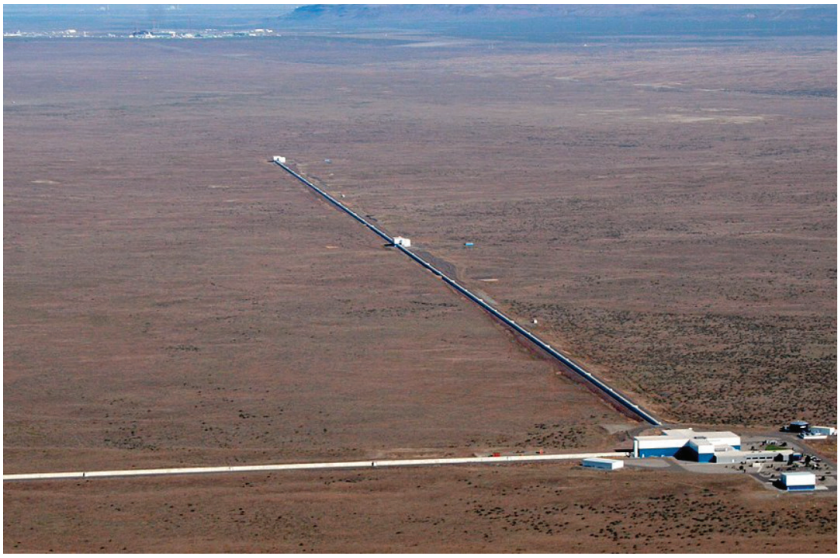
"Squeezing" deliberately sacrifices the certainty of measuring one attribute in order to achieve higher precision in measuring the other attribute.

The fact that the Heisenberg uncertainty principle only gives a limit on the *product of the uncertainties* of complementary properties means that it's possible to make the uncertainty of one attribute to be as small as you wish. The only catch is that the uncertainty of the other attribute must be larger to compensate. This is called "**squeezing**."

Squeezing is used in LIGO to improve sensitivity to gravitational waves.

One important experiment that uses squeezing is the **LIGO (Laser Interferometer Gravitational-Wave Observatory)** experiment. Scientists running this experiment use interferometers, consisting of lasers and mirrors separated by large distances, to detect gravitational waves coming from events in space.

Part of LIGO's interferometer is designed to use a specially prepared type of light that has been squeezed to reduce the uncertainty in one of its two complementary properties. This type of "squeezed light" can make it easier for the scientists working on the LIGO experiment to make the highly sensitive measurements needed to help detect gravitational waves from space.



LIGO Hanford Observatory, Washington
(LIGO Laboratory, Wikimedia Commons)

LIGO Hanford Observatory, Washington
(LIGO Laboratory, Wikimedia Commons)

b. Quantum sensors take advantage of the fact that physical qubits are extremely sensitive to their surroundings. The same fragility that leads to rapid decoherence enables precise sensors. Examples include magnetometers, single-photon detectors, and atomic clocks for improvements in medical imaging and navigation, position, and timing.

Quantum sensors take advantage of the fact that physical qubits are extremely sensitive to their surroundings. The same fragility that leads to rapid decoherence enables precise sensors.

The *Decoherence* article described how quantum states are extremely fragile and sensitive to small disruptions from the surroundings. Certain quantum phases of matter are another example of a sensitive quantum system that can sharply disappear upon tiny interactions with the outside world. Modern quantum sensors are built using these ideas and can respond to minute changes in the environment, leading to highly precise measurements.

Examples include magnetometers, atomic clocks, photon detectors, and accelerometers. Such sensors could be used in medicine, geology, and environmental data collection for position, timing, and navigation.

The following are some examples of quantum sensors that have already produced an impact on currently used technologies.

- **Magnetometers** are devices that measure the magnetic field. They are widely used in research and industry, with applications in biology, medicine, earth science, and navigation. Superconducting quantum sensors, called SQUIDs, use interference between quantum states in a superconducting loop to sensitively measure magnetic fields. (Superconductors are materials that can conduct electricity with no resistance at very low temperatures.)
- **Single-photon detectors** are high-resolution devices that are able to detect individual photons, the smallest quantity of light possible. These quantum sensors have applications in quantum technologies and the associated research, as well as biophysics (See the previous article Quantum Communication).
- **Atomic clocks** are based on the quantum states of atoms. They use stable transitions between discrete energy levels to keep time precisely, with applications in technologies such as the widely used Global Positioning System (GPS). The standard for defining how long 1 second is comes from an atomic energy transition. Commercial atomic clocks are designed to match the standard, and there are even more precise frequency standards available as well.

c. Quantum sensing has vastly improved the precision and accuracy of measurements of fundamental constants, freeing the International System of Units from its dependence on one-of-a-kind artifacts. Measurement units are now defined through these fundamental constants, like the speed of light and Planck's constant.

Quantum sensing has vastly improved the precision and accuracy of measurements of fundamental constants, freeing the International System of Units from its dependence on one-of-a-kind artifacts.

The **International System of Units** (also called **SI units**) is the system of units used for science and technology and is the most widely used system for measurements around the world. In 2019, the seven base SI units were redefined in terms of a set of fundamental constants, like the speed of light and **Planck's constant** (see the *Glossary*).

This redefinition freed the International System of Units from its dependence on artifacts such as the prototype of the kilogram displayed below. This object defined the magnitude of the kilogram until 2019. Artifacts such as this required meticulous preservation and had to be stored in fancy bell jars.

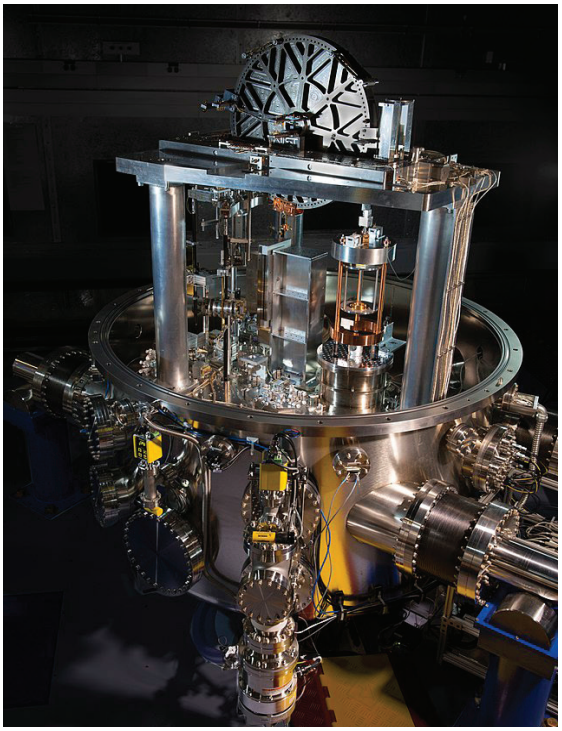
Replica of prototype kilogram standard
(NIST, Wikimedia Commons)

Replica of prototype kilogram standard
(NIST, Wikimedia Commons)

Measurement units are now defined through fundamental constants, like the speed of light and Planck's constant.

The International System of Units now defines its seven base units in terms of a set of fundamental constants. Quantum sensing devices have improved the precision of measurements of these fundamental constants.

- For example, the meter is now defined as the distance that light travels in vacuum during 9,192,631,770 transitions in a Cesium-133 atomic clock.
- The **kilogram** is now defined in terms of: Planck's constant, the speed of light, and a constant based on the transitions of a Cesium-133 atom. A complex device called a Kibble balance is used to measure Planck's constant, a fundamental constant that is important in quantum mechanics. A value for the kilogram is computed from a mathematical expression that combines these three values.

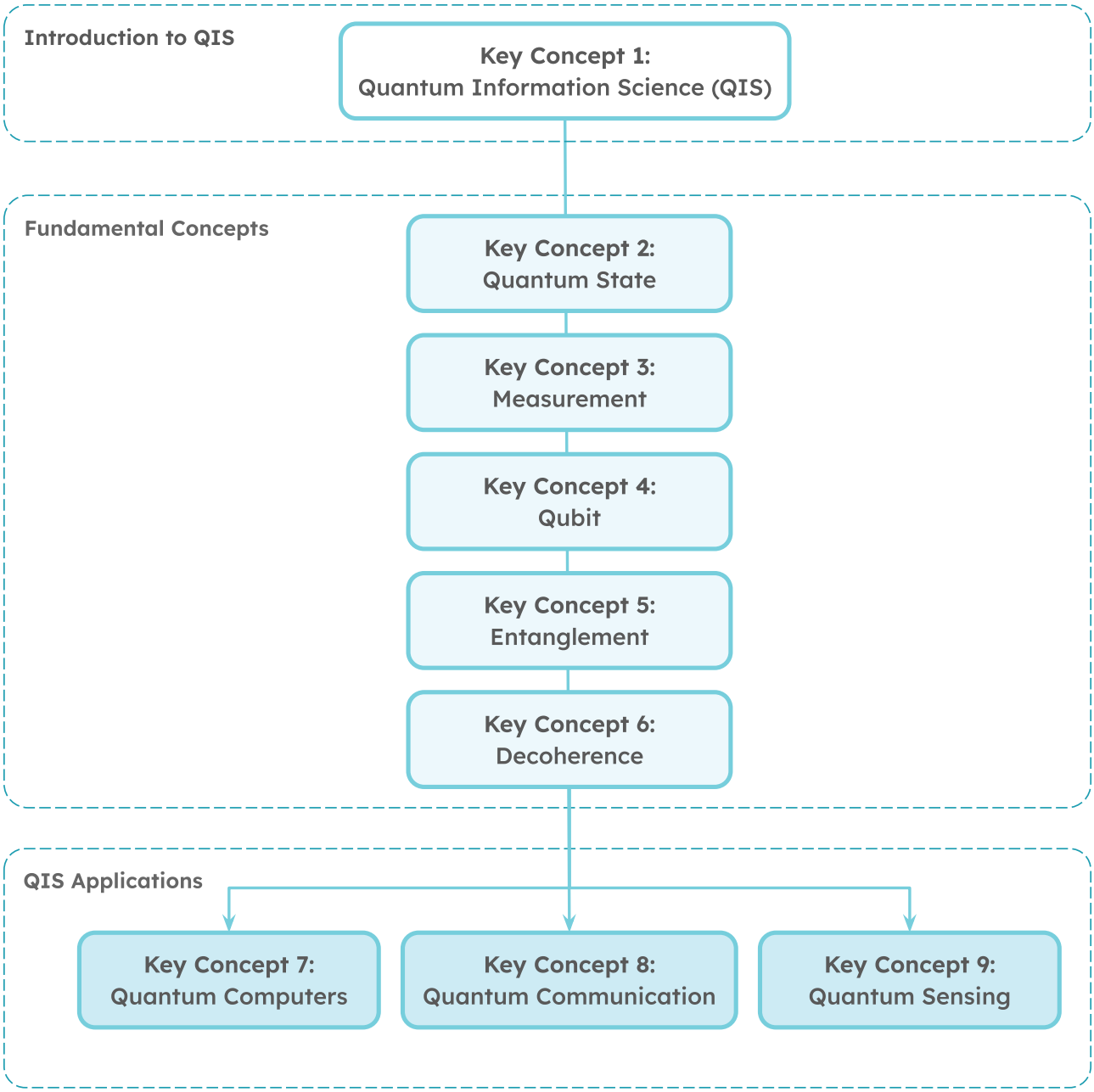


Kibble balance
(Jennifer Lauren Lee, NIST, Wikimedia Commons)

Associated Glossary Terms

- **Interferometer**: Devices that make highly-precise measurements using the interference of waves, typically electromagnetic waves, like light. Interference is the adding or canceling of waves that have been combined together.
- **Momentum**: A physical quantity that describes the motion of an object. It is defined as the product of the mass and velocity of the object, so the faster an object is moving, the greater its momentum.
- **Planck's Constant**: A fundamental physical constant that is important in quantum mechanics. It relates the energy and frequency of a photon. It is denoted by the symbol h and has the approximate value: 6.626×10^{-34} J-seconds.
- **Sensor**: A device that is used to detect and measure physical properties of its surrounding environment.

APPENDIX 1:
DEPENDENCY DIAGRAM



APPENDIX 2:
GLOSSARY OF ASSOCIATED TERMS

2. Quantum State

Atom: The basic building blocks of matter. The size of an atom is about 0.1 nm, which means you could fit about 100 million atoms in one centimeter.

Electron: An elementary particle that has negative electric charge and is found in all atoms.

Probability Amplitude: The numbers contained in a quantum state vector. These numbers can be negative or complex.

Quantum Operations: Actions that change the quantum state of a system. Quantum operations physically change the values of quantum properties.

System: For quantum information science, a system is a group of objects that are connected for a particular purpose. For example, an ion trap system consisting of charged atomic particles can be used as the basis of a small-scale quantum computer.

3. Measurement

Classical Computer: Classical computers (ordinary, non-quantum computers) store data represented in binary form as sequences of bits, 0s and 1s. For example, each letter, each color (associated with a certain amount of red, green, and blue), and even sounds are stored on a computer as sequences of bits.

Superposition: A quantum state that is a combination of multiple quantum states. A quantum system, like an electron or photon, can have a quantum state that is a superposition or combination of many different states.

4. Qubit

Bit: A bit (short for binary digit) is the basic unit of information. One bit represents one of two possible values, 0 or 1.

Interference: Waves can experience interference effects when they are combined together. For example, parts of a water or sound wave can be amplified (constructive interference) or cancel out (destructive interference). In a similar way, a superposition of two or more quantum states can lead to different parts of a quantum state to be amplified or canceled out.

Polarization: The polarization of light describes the direction that the light wave is oscillating. Most sources of light (such as light from sunlight and ordinary light bulbs) consist of a random mixture of light with different polarization states. Light with a specific polarization can be prepared using lasers or with devices called polarizers.

Spin: The spin of an electron is a property that makes electrons behave like a tiny magnet. Electron spin is a quantized value and can take only one of two possible values.

5. Entanglement

Correlation: A mutual relationship or connection between two or more things. Multiple quantum particles that are entangled with each other display measurement outcomes that are highly correlated.

6. Decoherence

Ion: An electrically charged atomic particle. Quantum computers based on trapped ions use atoms, like beryllium or calcium, with a net positive charge.

Photon: An elementary particle of light. Photons travel at the speed of light and can act as both a particle and a wave.

Radiation: A form of energy that can be transmitted through space or some material. Examples include light, vibration, heat, and magnetic fields.

Superconductor: A material that allows an electric current to flow without resistance.

7. Quantum Computers

Fault-Tolerant Quantum Computer: A quantum computer that is able to detect and contain the spread of errors during long, complex quantum computations.

RSA Encryption: A type of encryption that is commonly used to send private information over the Internet, for example, to look up banking information or to send credit card information to purchase items on a store's website.

8. Quantum Communication

Classical Communication: The exchange of classical information (bits) between different locations. This is in contrast to quantum communication, which is about the sharing of quantum information, which is the information carried by qubits.

Cryptography: The study and practice of encrypting our data to keep our information secret from others.

Quantum Information: Quantum information is the information contained within the quantum states of qubits. Quantum information is encoded and manipulated in quantum devices and possesses features such as superposition and entanglement which allow it to be processed in fundamentally new ways.

Transmission Channel: The physical medium through which a message is sent from the sender to the receiver.

9. Quantum Sensing

Interferometer: Devices that make highly-precise measurements using the interference of waves, typically electromagnetic waves, like light. Interference is the adding or canceling of waves that have been combined together.

Momentum: A physical quantity that describes the motion of an object. It is defined as the product of the mass and velocity of the object, so the faster an object is moving, the greater its momentum.

Planck's Constant: A fundamental physical constant that is important in quantum mechanics. It relates the energy and frequency of a photon. It is denoted by the symbol h and has the approximate value 6.62610-34 J/Hz.

Sensor: A device that is used to detect and measure physical properties of its surrounding environment.