Introduction

In the following video, John Watrous steps you through the content in this lesson on entanglement in action. Alternatively, you can open the YouTube video ↗ for this lesson in a separate window. Download the slides ↗ for this lesson.

In this lesson we'll take a look at three fundamentally important examples. The first two are the *quantum teleportation* and *superdense coding* protocols, which are principally concerned with the transmission of information from a sender to a receiver. The third example is an abstract game, called the *CHSH game*, which illustrates a phenomenon in quantum information that is sometimes referred to as *nonlocality*. (The CHSH game is not always described as a game. It is often described instead as an experiment — specifically, it is an example of a *Bell test* — and is referred to as the *CHSH inequality*.)

Quantum teleportation, superdense coding, and the CHSH game are not merely examples meant to illustrate how quantum information works, although they do serve well in this regard. Rather, they are stones in the foundation of quantum information. Entanglement plays a key role in all three examples, so this lesson provides the first opportunity in this course to see entanglement in action, and to begin to explore what it is that makes entanglement such an interesting and important concept.

Before proceeding to the examples themselves, a few preliminary comments that connect to all three examples are in order.

Alice and Bob

Alice and *Bob* are names traditionally given to hypothetical entities or agents in systems, protocols, games, and other interactions that involve the exchange of information. While these are human names, it should be understood that they represent abstractions and not necessarily actual human beings — so Alice and Bob might be expected to perform complex computations, for instance.

These names were first used in this way in the 1970s in the context of cryptography, but the convention has become common more broadly since then. The idea is simply that these are common names (at least in some parts of the world) that start with the letters A and B. It is also quite convenient to refer to Alice with the pronoun "her" and Bob with the pronoun "him" for the sake of brevity.

By default, we imagine that Alice and Bob are in different locations. They may have different goals and behaviors depending on the context in which they arise. For example, in *communication,* meaning the transmission of information, we might decide to use the name Alice to refer to the sender and Bob to refer to the receiver of whatever information is transmitted. In general, it may be that Alice and Bob cooperate, which is typical of a wide range of settings — but in other settings they may be in competition, or they may have different goals that may or may not be consistent or harmonious. These things must be made clear in the situation at hand.

We can also introduce additional characters, such as *Charlie* and *Diane*, as needed. Other names that represent different personas, such as *Eve* for an eavesdropper or *Mallory* for someone behaving maliciously, are also sometimes used.

Entanglement as a resource

Recall this example of an entangled quantum state of two qubits:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle. \tag{1}$$

It is one of the four Bell states, and is often viewed as the archetypal example of an entangled quantum state.

We also previously encountered this example of a probabilistic state of two bits:

$$\frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle. \tag{2}$$

It is, in some sense, analogous to the entangled quantum state (1). It represents a probabilistic state in which two bits are correlated, but it is not entangled. Entanglement is a uniquely quantum phenomenon, essentially by definition: in simplified terms, entanglement refers to *non-classical* quantum correlations.

Unfortunately, defining entanglement as non-classical quantum correlation is somewhat unsatisfying at an intuitive level, because it's a definition of what entanglement is in terms of what it is not. This may be why it's actually rather challenging to explain precisely what entanglement is, and what makes it special, in intuitive terms.

Typical explanations of entanglement often fail to distinguish the two states (1) and (2) in a meaningful way. For example, it is sometimes said that if one of two entangled qubits is measured, then the state of the other qubit is somehow instantaneously affected; or that the state of the two qubits together cannot be described separately; or that the two qubits somehow maintain a memory of each other. These statements are not false, but why are they not also true for the (unentangled) probabilistic state (2) above? The two bits represented by this state are intimately connected: each one has a perfect memory of the other in a literal sense. But the state is nevertheless not entangled.

One way to explain what makes entanglement special, and what makes the quantum state (1) very different from the probabilistic state (2), is to explain what can be done with entanglement, or what we can see happening because of entanglement, that goes beyond the decisions we make about how to represent our knowledge of states using vectors. All three of the examples to be discussed in this lesson have this nature, in that they illustrate things that can be done with the state (1) that cannot be done with *any* classically correlated state, including the state (2).

Indeed, it is typical in the study of quantum information and computation that entanglement is viewed as a resource through which different tasks can be accomplished. When this is done, the state (1) is viewed as representing one *unit* of entanglement, which we refer to as an *e-bit*. The "e" stands for "entangled" or "entanglement." While it is true that the state (1) is a state of two qubits, the quantity of entanglement that it represents is one e-bit.

Incidentally, we can also view the probabilistic state (2) as a resource, which is one bit of *shared randomness*. It can be very useful in cryptography, for instance, to share a random bit with somebody (presuming that nobody else knows what the bit is), so that it can be used as a private key, or part of a private key, for the sake of encryption. But in this lesson the focus is on entanglement and a few things we can do with it.

As a point of clarification regarding terminology, when we say that Alice and Bob *share an e-bit*, what we mean is that Alice has a qubit named A, Bob has a qubit named B, and together the pair (A, B) is in the quantum state (1). Different names could, of course, be chosen for the qubits, but throughout this lesson we will stick with these names in the interest of clarity.

Previous page

Next page