Content

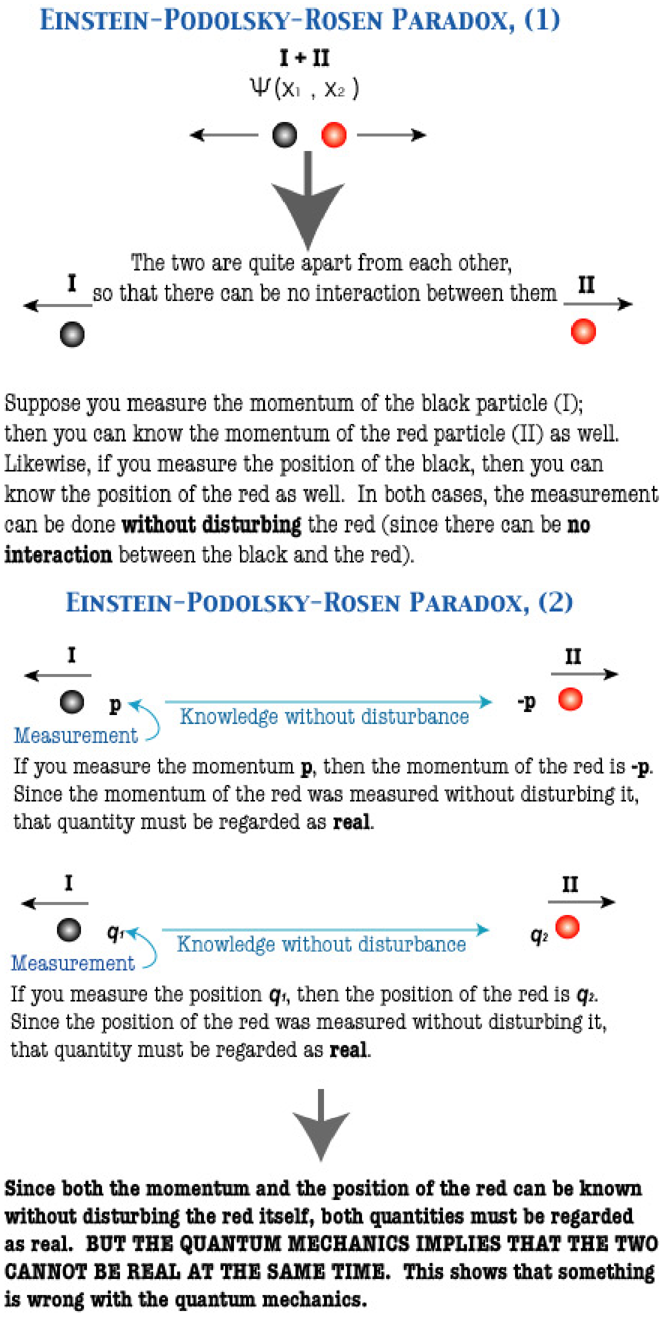
1. What is entanglement

Entanglement is a term used in quantum theory to describe the way that particles of energy/matter can become *correlated* to predictably interact with each other regardless of how far apart they are.
Particles, such as photons, electrons, or qubits that have interacted with each other retain a type of connection and can be entangled with each other in pairs, in the process known as correlation. Knowing the spin state of one entangled particle - whether the direction of the spin is up or down - allows one to know that the spin of its mate is in the opposite direction. Even more amazing is the knowledge that, due to the phenomenon of superposition, the measured particle has no single spin direction before being measured, but is simultaneously in both a spin-up and spin-down state. The spin state of the particle being measured is decided at the time of measurement and communicated to the correlated particle, which simultaneously assumes the opposite spin direction to that of the measured particle. Quantum entanglement allows qubits that are separated by incredible distances to interact with each other immediately, in a communication that is not limited to the speed of light. No matter how great the distance between the correlated particles, they will remain entangled as long as they are isolated. In some sense, we can say that superposition encompasses entanglement, since entanglement can be viewed as a special case of superposition.

2. The background of the idea

2.1 The EPR paradox

Entanglement is one of the properties of quantum mechanics which caused Einstein and others to dislike the theory. In 1935, Einstein, Podolsky and Rosen formulated the EPR paradox, demonstrating that entanglement makes quantum mechanics a non-local theory.
Initially Einstein was enthusiastic about the quantum theory. By 1935, however, his enthusiasm for the theory had given way to a sense of disappointment. Firstly, he felt the theory had abdicated the historical task of natural science to provide knowledge of significant aspects of nature that were independent of observers or their observations. Secondly, the quantum theory was essentially statistical. The probabilities built into the state function were fundamental and, unlike the situation in classical statistical mechanics, they were not understood as arising from ignorance of fine details. In this sense the theory was indeterministic. Thus Einstein began to probe how strongly the quantum theory was tied to irrealism and indeterminism.



Einstein famously derided entanglement as "spook action at a distance." It can give rise to strange phenomena that have fueled endless debates between the advocates of the theory of quantum mechanics and those trying to disprove it, the arguments exchanged by Bohr and Einstein on this subject have become history. Einstein was deeply dissatisfied with the fact that quantum mechanics allowed correlations between entangled particles to manifest themselves instantaneously over arbitrary large distances.

On the other hand, quantum mechanics has been highly successful in producing correct experimental predictions, and the strong correlations associated with the phenomenon of quantum entanglement have in fact been observed. One apparent way to explain quantum entanglement is an approach known as "hidden variable theory", in which unknown deterministic microscopic parameters would cause the correlations.

However, in 1964 Bell showed that such a theory could not be "local", the quantum entanglement predicted by quantum mechanics being experimentally distinguishable from a broad class of local hidden-variable theories.

Results of subsequent experiments have overwhelmingly supported quantum mechanics. It is known that there are a number of loopholes in these experiments, but these are generally considered to be of minor importance. Bell's inequality was only the first in a larger set of inequalities of this kind.

2.2 Bell's states

Bell's states are the subject of his famous Bell inequality. A Bell pair is a pair of qubits which jointly are in a Bell state, which is, entangled with each other. A Bell state is defined as a maximally entangled quantum state of two qubits. The qubits are usually thought to be spatially separated. Nevertheless they exhibit perfect correlations which cannot be explained without quantum mechanics. To explain, let us first look at the Bell state $|\Phi^+\rangle$:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B).$$

But quantum mechanics allows qubits to be in quantum superposition — i.e. in 0 and 1 simultaneously, e.g. in either of the states

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{or} \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

There are three other states of two qubits which lead to this maximal value of $2\sqrt{2}$ and the four are known as the four *maximally entangled two-qubit states* or *Bell states*:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B)$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B)$$
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B).$$

2.3 GHZ experiment

Another experiment was made, an experiment that would allow the clash between quantum and classical reality to be decided in one measurement, which seemed as an important achievement. The GHZ experiment is basically an extension of the EPR experiment with three correlated particles instead of two. The three-particle entanglement in the GHZ proposal provides the means to prove the contradiction without the cumbersome use of inequalities, in a much more direct and non-statistical way, as compared with Bell's original theorem. In 1999 a team of researchers at MIT produced a GHZ state using nuclear spins

instead of photon polarizations and the techniques of nuclear magnetic resonance spectroscopy to manipulate their sample. Although they were able to measure the weird quantum correlations exhibited by the GHZ state, the NMR techniques used prevented them from testing the non-local aspects of the GHZ experiment. The three qubits, embodied as nuclear spins within a molecule, were far too close together to allow for a delayed-choice experiment of the kind Aspect performed on EPR pairs. A little bit more about the GHZ experiment:
Frequently considered cases of GHZ experiments are concerned with measurements obtained by three observers, A, B, and C, who each can detect one signal at a time in one of two distinct own channels or outcomes: for instance A detecting and counting a signal either as *(A↑)* or as *(A↓)*, B detecting and counting a signal either as *(B «)* or as *(B »)*, and C detecting and counting a signal either as *(C ◊)* or as *(C ♦)*.
Signals are to be considered and counted only if A, B, and C detect them trial-by-trial together; i.e. for any one signal which has been detected by A in one particular trial, B must have detected precisely one signal in the *same* trial, and C must have detected precisely one signal in the *same* trial; and vice versa.
For any one particular trial it may be consequently distinguished and counted whether

- A detected a signal as *(A↑)* and not as *(A↓)*, with corresponding counts n_t *(A↑) =1* and n_t *(A↓) = 0*, in this particular trial *t*, or
- A detected a signal as *(A↓)* and not as *(A↑)*, with corresponding counts n_f *(A↑) = 0* and n_f *(A↓) = 1*, in this particular trial *f*, where trials *f* and *t* are evidently distinct;

similarly, it can be distinguished and counted whether

- B detected a signal as *(B «)* and not as *(B »)*, with corresponding counts n_g *(B «)* = 1 and n_g *(B »)* = 0, in this particular trial *g*, or
- B detected a signal as *(B »)* and not as *(B «)*, with corresponding counts n_h *(B «)* = 0 and n_h *(B »)* = 1, in this particular trial *h*, where trials *g* and *h* are evidently distinct;

and correspondingly, it can be distinguished and counted whether

- C detected a signal as *(C ◊)* and not as *(C ♦)*, with corresponding counts n_l*(C ◊)* = 1 and n_l*(C ♦)* = 0, in this particular trial *l*, or
- C detected a signal as *(C ♦)* and not as *(C ◊)*, with corresponding counts n_m*(C ◊)* = 0 and n_m*(C ♦)* = 1, in this particular trial *m*, where trials *l* and *m* are evidently distinct.

$p_{(A\uparrow)\,(B\,«)\,(C\,\lozenge)}(j) = (n_j\,(A\uparrow) - n_j\,(A\downarrow))\,(n_j\,(B\,«) - n_j\,(B\,»))\,(n_j\,(C\,\lozenge) - n_j\,(C\,\blacklozenge))$ can be evaluated in each trial.

Following an argument by John Stewart Bell, each trial is now characterized by particular individual *adjustable apparatus parameters*, or *settings* of the observers involved. There are (at least) two distinguishable *settings* being considered for each, namely A's settings a_1, and a_2, B's settings b_1, and b_2, and C's settings c_1, and c_2.

Trial *s* for instance would be characterized by A's setting a_2 , B's setting b_2 , and C's settings c_2 ; another trial, *r*, would be characterized by A's setting a_2 , B's setting b_2 , and C's settings c_1 , and so on. (Since C's *settings* are distinct between trials *r* and *s*, therefore these two trials are distinct.) Correspondingly, the correlation number $p_{(A\uparrow)\ (B\ «)\ (C\ \lozenge)}(\ s\ )$ is written as $p_{(A\uparrow)\ (B\ «)\ (C\ \lozenge)}(\ a_2\ ,\ b_2\ ,\ c_2\ )$, the correlation number $p_{(A\uparrow)\ (B\ «)\ (C\ \lozenge)}(\ r\ )$ is written as $p_{(A\uparrow)\ (B\ «)\ (C\ \lozenge)}(\ a_2\ ,\ b_2\ ,\ c_1\ )$ and so on.

Further, as GHZ and collaborators demonstrate in detail, the following four distinct trials, with their various separate detector counts and with suitably identified *settings*, may be considered and be found experimentally:

- trial *s* as shown above, characterized by the *settings* a_2 , b_2 , and c_2 , and with detector counts such that

$p_{(A\uparrow)\ (B\ «)\ (C\ \lozenge)}(\ s\ ) = (n_s\ (A\uparrow) - n_s\ (A\downarrow))\ (n_s\ (B\ «) - n_s\ (B\ »))\ (n_s\ (C\ \lozenge) - n_s\ (C\ \blacklozenge)) = -1$,

- trial *u* with *settings* a_2 , b_1 , and c_1 , and with detector counts such that

$p_{(A\uparrow)\ (B\ «)\ (C\ \lozenge)}(\ u\ ) = (n_u\ (A\uparrow) - n_u\ (A\downarrow))\ (n_u\ (B\ «) - n_u\ (B\ »))\ (n_u\ (C\ \lozenge) - n_u\ (C\ \blacklozenge)) = 1$,

- trial *v* with *settings* a_1 , b_2 , and c_1 , and with detector counts such that

$p_{(A\uparrow)\ (B\ «)\ (C\ \lozenge)}(\ v\ ) = (n_v\ (A\uparrow) - n_v\ (A\downarrow))\ (n_v\ (B\ «) - n_v\ (B\ »))\ (n_v\ (C\ \lozenge) - n_v\ (C\ \blacklozenge)) = 1$, and

- trial *w* with *settings* a_1 , b_1 , and c_2 , and with detector counts such that

$p_{(A\uparrow)\ (B\ «)\ (C\ \lozenge)}(\ w\ ) = (n_w\ (A\uparrow) - n_w\ (A\downarrow))\ (n_w\ (B\ «) - n_w\ (B\ »))\ (n_w\ (C\ \lozenge) - n_w\ (C\ \blacklozenge)) = 1$.

The notion of local hidden variables is now introduced by considering the following question:

Can the individual detection outcomes and corresponding counts as obtained by any one observer, e.g. the numbers $(n_j\ (A\uparrow)\ -\ n_j\ (A\downarrow))$, be expressed as a function $A(\ a_x\ ,\ \lambda\ )$ (which necessarily assumes the values +1 or -1), i.e. as a function only of the setting of this observer in this trial, and of one other *hidden* parameter λ, but without an explicit dependence on settings or outcomes concerning the other observers (who are considered *far away*)?

Therefore: can the correlation numbers such as $p_{(A\uparrow)\ (B\ «)\ (C\ \lozenge)}(\ a_x\ ,\ b_x\ ,\ c_x\ )$, be expressed as a product of such independent functions, $A(\ a_x\ ,\ \lambda\ )$, $B(\ b_x\ ,\ \lambda\ )$ and $C(\ c_x\ ,\ \lambda\ )$, for all trials and all settings, with a suitable *hidden variable* value λ?

Comparison with the product which defined $p_{(A\uparrow)\ (B\ «)\ (C\ \lozenge)}(\ j\ )$ explicitly above, readily suggests to identify

- $\lambda \rightarrow j$,
- $A(\ a_x\ ,\ j\ ) \rightarrow (n_j\ (A\uparrow) - n_j\ (A\downarrow))$,
- $B(\ b_x\ ,\ j\ ) \rightarrow (n_j\ (B\ «) - n_j\ (B\ »))$, and
- $C(\ c_x\ ,\ j\ ) \rightarrow (n_j\ (C\ \lozenge) - n_j\ (C\ \blacklozenge))$,

where *j* denotes any one trial which is characterized by the specific settings a_x , b_x , and c_x , of A, B, and of C, respectively.

However, GHZ and collaborators also require that the *hidden variable* argument to functions *A()*, *B()*, and *C()* may take the same value, λ, even in distinct trials, being characterized by distinct *settings*.

Consequently, substituting these functions into the consistent conditions on four distinct trials, *u*, *v*, *w*, and *s* shown above, they are able to obtain the following four equations concerning one and the same value λ:

1. $A(a_2 , \lambda) B(b_2 , \lambda) C(c_2 , \lambda) = -1$,
2. $A(a_2 , \lambda) B(b_1 , \lambda) C(c_1 , \lambda) = 1$,
3. $A(a_1 , \lambda) B(b_2 , \lambda) C(c_1 , \lambda) = 1$, and
4. $A(a_1 , \lambda) B(b_1 , \lambda) C(c_2 , \lambda) = 1$.

Taking the product of the last three equations, and noting that $A(a_1 , \lambda) A(a_1 , \lambda) = 1$, $B(b_1 , \lambda) B(b_1 , \lambda) = 1$, and $C(c_1 , \lambda) C(c_1 , \lambda) = 1$, yields
$A(a_2 , \lambda) B(b_2 , \lambda) C(c_2 , \lambda) = 1$
in contradiction to the first equation; $1 \neq -1$.
Given that the four trials under consideration can indeed be consistently considered and experimentally realized, the assumptions concerning *hidden variables* which lead to the indicated mathematical contradiction are therefore *collectively* unsuitable to represent all experimental results; namely the assumption of *local hidden variables* which occur *equally in distinct trials*.
It is probably worth mentioning that the assumption of *local hidden variables* which *vary* between distinct trials, such as a trial index itself, does generally not allow deriving a mathematical contradiction as indicated by GHZ. Because we have no control over the hidden variables, the contradiction derived above cannot be directly tested in an experiment.
Today, entanglement is no longer regarded as merely a quantum curiosity. People are seeing it as a physical resource that can be spent in order to solve information-processing tasks in new ways. Therefore, the question whether this “resource" really exists in Nature and can be exploited in the ways we currently believe it can, is of crucial importance for the future of quantum computation and quantum information.

3. The math behind entanglement

Consider two no interacting systems *A* and *B*, with respective Hilbert spaces H_A and H_B. The Hilbert space of the composite system is the tensor product.

$$H_A \otimes H_B$$

If the first system is in state $|\psi\rangle_A$ and the second in state $|\phi\rangle_B$, the state of the composite system is $|\psi\rangle_A \otimes |\phi\rangle_B$, which is often also written as $|\psi\rangle_A \, |\phi\rangle_B$.

States of the composite system which can be represented in this form are called separable states. Pick observables $\mathbf{\Omega_A}$ acting on $\boldsymbol{H_A}$, and $\mathbf{\Omega_B}$ acting on $\boldsymbol{H_B}$.

According to the spectral theorem, we can find a basis $\{|i\rangle_A\}$ for $\boldsymbol{H_A}$ composed of eigenvectors of $\boldsymbol{\Omega_A}$, and a basis $\{|j\rangle_B\}$ for $\boldsymbol{H_B}$ composed of eigenvectors of $\boldsymbol{\Omega_B}$. We can then write the above pure state as

$$\left(\sum_i a_i |i\rangle_A\right)\left(\sum_j b_j |j\rangle_B\right),$$

for some choice of complex coefficients a_i and b_j.

This is not the most general state of $H_A \otimes H_B$, which has the form

$$\sum_{i,j} c_{ij} |i\rangle_A \otimes |j\rangle_B.$$

If such a state is not separable, it is known as an *entangled state*.

For example, given two basis vectors $\{|0\rangle_A, |1\rangle_A\}$ of H_A and two basis vectors $\{|0\rangle_B, |1\rangle_B\}$ of H_B, the following is an entangled state:

$$\frac{1}{\sqrt{2}}\Big(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\Big).$$

If the composite system is in this state, it is impossible to attribute to either system *A* or system *B* a definite pure state. Instead, their states are superposed with one another. In this sense, the systems are "entangled".

Now suppose Alice is an observer for system *A*, and Bob is an observer for system *B*. If Alice performs the measurement Ω_A, there are two possible outcomes, occurring with equal probability:

1. Alice measures 0, and the state of the system collapses to $|0\rangle_A|1\rangle_B$
2. Alice measures 1, and the state of the system collapses to $|1\rangle_A|0\rangle_B$.

If the former occurs, any subsequent measurement of Ω_B performed by Bob always returns 1. If the latter occurs, Bob's measurement always returns 0. Thus, system *B* has been altered by Alice performing her measurement on system *A*., even if the systems *A* and *B* are spatially separated. This is the foundation of the EPR paradox.

4. Applications of entanglement

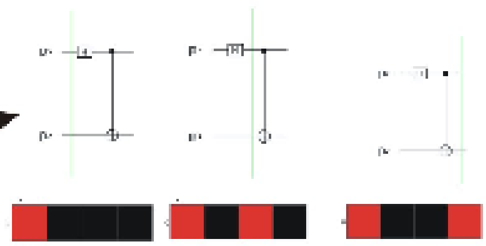
Quantum entanglement is the basis for emerging technologies such as quantum computing and quantum cryptography, and has been used for experiments in quantum teleportation. At the same time, it produces some of the more theoretically and philosophically disturbing aspects of the theory, as one can show that the correlations predicted by quantum mechanics are inconsistent with the seemingly obvious principle of local realism, which is that information about the state of a system should only be mediated by interactions in its immediate surroundings.
Quantum cryptography, or quantum key distribution (QKD), uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages. By using quantum superposition or quantum entanglement and transmitting information in quantum states, a communication system can be implemented which detects eavesdropping. If the level of eavesdropping is below a certain threshold, a key can be produced that is guaranteed to be secure (i.e. the eavesdropper has no information about), otherwise no secure key is possible and communication is aborted. Quantum cryptography is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. Quantum communication involves encoding information in quantum states, or qubits, as opposed to classical communication's use of bits. Usually, photons are used for these quantum states. Quantum cryptography exploits certain properties of these quantum states to ensure its security. There are several different approaches to quantum key distribution, one is Entanglement based protocols**.** The quantum states of two (or more) separate objects can become linked together in such a way that they must be described by a combined quantum state, not as individual objects. This is known as entanglement and means that, for example, performing a measurement on one object will affect the other. If an entangled pair of objects is shared between two parties, anyone intercepting either object will alter the overall system, allowing the presence of the third party (and the amount of information they have gained) to be determined.

5. jQuantum

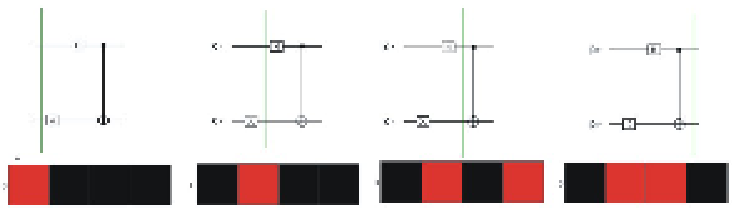
The program jQuantum is a quantum computer simulator. It simulates the implementation of quantum circuits on a small quantum register up to about 15 qubits. Its main intention is to create images—images which may help to learn and understand quantum circuits, and which perhaps will serve as building blocks for inventing new quantum algorithms.

1) Bell states - These quantum circuits construct the simplest entangled states, the Bell states or EPR states, consisting of two qubits in a superposition of two states which are not a product state. From the 8 possible states which two qubits can attain only the following four states are entangled:

the green line shows each step taken.The black box represents the possible states in which the system could be, (00,01,10,11), and the red squares represent the actual srate of the system. If the color is blue, it means that the qubit has opposite phase.

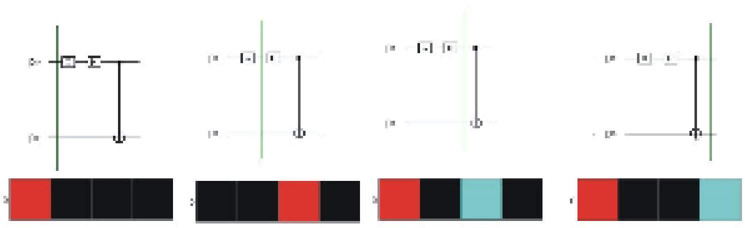


$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

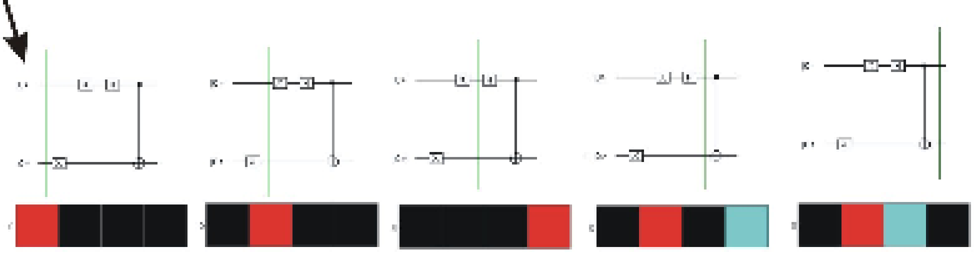


$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$



$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$



,

The relevance of entangled states stems from the case that the entangled qubits are far apart from each other. A measurement of one of them then has an *instant* impact on the entangled qubit. In this way, entanglement can be used to perform teleportation or quantum communication.

2) GHZ experiment - The *GHZ experiment*, after Greenberger, Horne and Zeilinger, is an experiment in quantum mechanics which gives opposite results depending on whether quantum mechanics or Einstein's local realism with hidden variables holds. First published in 1989, it was performed in 1999 and falsified the predictions of hidden variable theories.

Whereas the Bell inequalities, which in essence decide the same question, require a statistical evaluation of large measurement series, the GHZ experiment only needs four measurements. Its core idea is to take *three* particles, each of which is a two-state quantum system attaining the states $|0\rangle$ and $|1\rangle$, and entangle them into the *GHZ state*

$$|\psi\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

Here $|0\rangle$ and $|1\rangle$ may represent the states spin-up and spin-down, for instance, with the eigenvalue +1 for $|0\rangle$ and -1 for $|1\rangle$**.** As a quantum circuit, the GHZ state can be obtained from the initial state $|0\rangle|0\rangle|0\rangle$ by a Hadamard and two c-NOTs, $|\psi\rangle = \mathrm{cNOT}_1^3\ \mathrm{cNOT}_2^3\ H_3\ |000\rangle$**.** With the first two Pauli matrices X,Y we then construct the four measurement operators

$$\boldsymbol{A_1 = X_1Y_2Y_3}$$
$$\boldsymbol{A_2 = Y_1X_2Y_3}$$
$$\boldsymbol{A_3 = Y_1Y_2X_3}$$
$$\boldsymbol{B = X_1X_2X_3}$$

Realized as a quantum register, a measurement in the Pauli basis X may be regarded as a transformation of the quantum state in the standard computational basis by H, i.e.,

$$|0_x\rangle = H\,|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |1_x\rangle = H\,|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

or equivalently

$$|0\rangle = H\,|0_x\rangle = \frac{|0_x\rangle + |1_x\rangle}{\sqrt{2}}, \qquad |1\rangle = H\,|1_x\rangle = \frac{|0_x\rangle - |1_x\rangle}{\sqrt{2}},$$

and a subsequent measurement of the respective qubit; analogously, a measurement in the Pauli basis Y a transformation by $S^{\dagger}H$

$$|0_y\rangle = HS\,|0\rangle = \frac{|0\rangle + \mathrm{i}\,|1\rangle}{\sqrt{2}}, \qquad |1_y\rangle = HS\,|1\rangle = \frac{|0\rangle - \mathrm{i}\,|1\rangle}{\sqrt{2}},$$

or equivalently

$$|0\rangle = S^\dagger H\,|0_y\rangle = \frac{|0_y\rangle + |1_y\rangle}{\sqrt{2}}, \qquad |1\rangle = S^\dagger H\,|1_y\rangle = \frac{|0_y\rangle - |1_y\rangle}{\sqrt{2}\,\mathrm{i}},$$

and a subsequent measurement. In both cases, the measurement result is $\lambda = +1$ if and only if the qubit state is $|0_x\rangle$ or $|0_y\rangle$, respectively, and $\lambda = -1$ if and only if the qubit state is $|1_x\rangle$ or $|1_y\rangle$, respectively. As can be seen with the quantum circuits GHZ-A1,GHZ-A2,GHZ-A3 and GHZ-B (or as can be directly verified by calculation), the qubits in the A_i-bases contain an *odd*number of 1-qubits,

$$|\psi\rangle = \frac{1}{2}\left(|0_x0_y1_y\rangle + |0_x1_y0_y\rangle + |1_x0_y0_y\rangle + |1_x1_y1_y\rangle\right),$$

$$|\psi\rangle = \frac{1}{2}\left(|0_y0_x1_y\rangle + |0_y1_x0_y\rangle + |1_y0_x0_y\rangle + |1_y1_x1_y\rangle\right),$$

$$|\psi\rangle = \frac{1}{2}\left(|0_y0_y1_x\rangle + |0_y1_y0_x\rangle + |1_y0_y0_x\rangle + |1_y1_y1_x\rangle\right),$$

whereas in the *B*-basis we have only those qubits with *even* number of 1-qubits**,**

$$|\psi\rangle = \frac{1}{2}\left(|0_x0_x0_x\rangle + |0_x1_x1_x\rangle + |1_x0_x1_x\rangle + |1_x1_x0_x\rangle\right).$$

For each set up state, a measurement of two qubits suffices to determine the state of the third one uniquely. By construction, the measurement results are

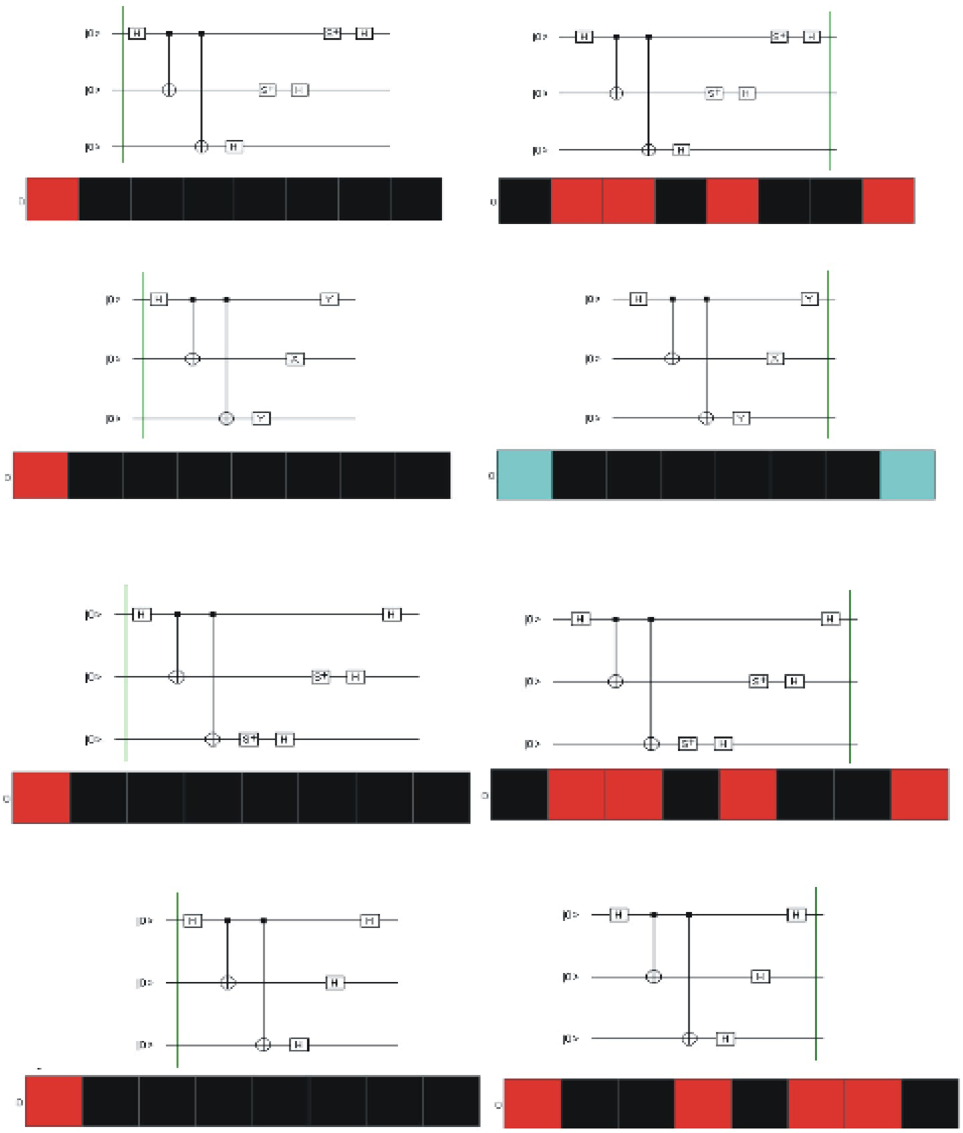
$$A_{1,2,3}|\psi\rangle = -1,$$
$$B|\psi\rangle = +1.$$

But this last measurement result for *B* leads to a contradiction to Einstein's local realism: If the GHZ state $|\psi\rangle$ was completely determined by some hidden variables and thus the same in each measurement trial, then we would have $B|\psi\rangle = -1$, since $Y_1Y_1 = Y_2Y_2 = Y_3Y_3 = +1$ and therefore $B = X_1X_1X_3$ can be expressed as the product $A_1A_2A_3$,

$$A_1 = X_1 Y_2 Y_3 = -1$$
$$A_2 = Y_1 X_2 Y_3 = -1$$
$$A_3 = Y_1 Y_2 X_3 = -1$$

$$B = X_1 X_2 X_3 = -1 \quad \textbf{(if local realism holds)}$$

However, this is a contradiction to the result $B|\psi\rangle = +1$ which quantum mechanics (without hidden variables) predicts. Realized GHZ experiments confirmed $B|\psi\rangle = +1$ and therefore falsified local realism.



The GHZ experiment, showing the first and last state of circuits GHZ-A1,GHZ-A2,GHZ-A3 and GHZ-B.

References:

Stanford Encyclopedia of Philosophy

Quantum entanglement, Wikipedia

Quantum Information Theory and The Foundations of Quantum Mechanics Christopher Gordon Timpson - The Queen's College Oxford University, Trinity Term 2004

Quantiki Portal

jQuantum - A Quantum Computer Simulator - Andreas de Vries