

Re: Quantum communication might be possible?

Source: <http://sci.tech-archive.net/Archive/sci.physics.research/2006-01/msg00140.html>

- *From:* Greg Egan <gregegan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 18 Jan 2006 19:34:13 +0000 (UTC)
-

I thought I'd offer a brief summary of some matters relevant to this discussion. This is based on "Quantum Theory: Concepts and Methods" by Asher Peres. I'll try to present things in an "interpretation-neutral" and uncontroversial manner.

Bell's theorem

Suppose you have a source of two perfectly correlated photons (anti-correlations can also be analysed, but I'll follow Peres's example) that are sent to two observers. What we mean by "perfectly correlated" (regardless of any underlying physical theory) is simply that if the two observers measure polarisation *along exactly the same direction* then it is 100% certain that they will get the same outcomes.

Now suppose that Alice can *either* measure polarisation along direction A or along direction C, while Bob can *either* measure polarisation along direction B or along direction C.

If both choose C, they will find that both photons passed through their polarisation filters, or both did not. If they choose different directions, any correlations between their results will depend on the assumptions being made.

Now, Bell's theorem asks us to imagine that each photon carries with it some local properties that determine what the result *would be* for *any* choice of orientation of the filters. Under that assumption, it makes sense to talk about all three results for each photon pair (would the photon pass through the filters with directions A, B and C?) even though only two measurements can actually be made. If we call the results (whether actually measured, or merely guaranteed by the photon's properties) a, b and c, with values +1 for passing through the filter and -1 for being rejected, then for each pair we have:

$$a(b-c) = +/- (1-bc)$$

Why? Well if b and c happened to be equal, both sides give zero. If b is not equal to c, both sides have magnitude 2.

Re: Quantum communication might be possible?

If we take averages over many pairs of photons, it follows that:

$$|\langle ab \rangle - \langle ac \rangle| + \langle bc \rangle \leq 1$$

where $\langle ab \rangle$, $\langle ac \rangle$, $\langle bc \rangle$ are the correlations between the results. This is Bell's inequality.

Now, QM can't predict individual results, but it can predict values for the pairwise correlations, if the photons are prepared in a particular entangled state:

$$(x_1 x_2 + y_1 y_2)/\sqrt{2}$$

where x_1 is the state in which the first photon's polarisation is aligned with the x axis, etc.

What QM predicts is that

$$\langle ab \rangle = \cos 2(A-B)$$

$$\langle ac \rangle = \cos 2(A-C)$$

$$\langle bc \rangle = \cos 2(B-C)$$

If we put $A=0$, $B=\pi/6$, $C=\pi/3$, this becomes:

$$\langle ab \rangle = \cos(-\pi/3) = 1/2$$

$$\langle ac \rangle = \cos(-2\pi/3) = -1/2$$

$$\langle bc \rangle = \cos(-\pi/3) = 1/2$$

Then the LHS of Bell's inequality is $3/2$, so the predictions of QM violate the inequality.

Peres says that Aspect's experiment (in which the choices of direction occurred at events with spacelike separation, i.e. they were causally isolated from each other according to special relativity) violated a related inequality by five standard deviations.

Quantum communication

This is a big subject, but to summarise the basics without going into any of the sophisticated refinements or detailed practicalities:

Alice and Bob receive sequences of photons which are correlated as above. Alice and Bob randomly choose between two directions, V and W, which are 45 degrees from each other. After they have collected a large number of measurements, they publish their choices of directions; this allows them then to know when they made measurements along the same direction. Their polarisation results when their directions coincided are known only by them, and will agree, so they can use this sequence of bits as a secure key.

Re: Quantum communication might be possible?

Any eavesdropper/data–corrupter will not know the choices of direction made by Alice and Bob, and so will be forced to make his own choices. If Alice and Bob publish some further statistics about the data, it's possible for them to verify that no eavesdropping or corruption of the data has taken place.

-
- Prev by Date: [*a new discrete model of quantum mechanics*](#)
 - Next by Date: [*CFP: The 2006 IAENG International Workshop on Scientific Computing and Computational Statistics*](#)
 - Previous by thread: [*Re: Quantum communication might be possible?*](#)
 - Next by thread: [*Re: Quantum communication might be possible?*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)