UNKNOWABLE MATTERS: HOW NATURE'S SPEED LIMIT ON COMMUNICATION RELATES TO QUANTUM PHYSICS

STEPHEN MCADAM

ABSTRACT. It is shown that there is no way of identifying an unknown polarization state of a photon, by proving that otherwise, faster than light communication would be possible. It is similarly argued that the 'no cloning theorem' of quantum physics must be true.

Introduction. The advent of quantum physics led to the realization that there are limits to what can be known about the real world. The most famous example is the impossibility of knowing both the position and momentum of a particle. We will concern ourselves with the polarization of a photon. If one has a single photon whose polarization is unknown, the laws of quantum physics dictate against the possibility of identifying that state. We explore why, and in particular show that if one could identify an unknown state, then faster than light communication would be possible. We also give an apparently new proof of the no cloning theorem, (which states that there is no way of making a copy of an unknown polarization state), as well as a new argument against the possibility of simultaneously taking two different measurements of the polarization state of a photon. Finally, we show that the outcome of measuring a state cannot be predicted, and discuss the relationship of that statement to Bell's Theorem.

1-QUBIT STATES

Let us use the symbol H to denote a horizontally polarized photon, and V to represent a vertically polarized photon. Consistent with that, we will use $(\cos\theta)H + (\sin\theta)V$ to represent a photon polarized at angle θ to the horizontal. We will call that expression the polarization state (or just state) of the photon. Thus, any expression of form $aH + bV$ with a and b real numbers such that $a^2 + b^2 = 1$ is the state of some photon (polarized at an appropriate angle). Now there exists photons whose angle of polarization is constantly changing. For example, circularly polarized photons have an angle of polarization that goes round and round a circle. The state of such a photon can be expressed as $\frac{1}{\sqrt{2}}H \pm \frac{i}{\sqrt{2}}V$ (the choice of sign depending on which way one goes around the circle).

In general, the polarization state of any photon can be expressed as $aH + bV$ with a and b complex numbers such that $|a|^2 + |b|^2 = aa^* + bb^* = 1$ (with x^* the complex conjugate of x). Conversely, any such expression does represent the polarization state of some photon. (Often, H and V are replaced by $|0\rangle$ and $|1\rangle$, a notation quite useful in quantum computing. However, H and V are neater, and quite adequate for our purposes.)

The above facts are easily embedded into a mathematical structure. We consider the 2-dimensional vector space over the complex numbers having basis H, V. On it, we impose the following inner product (resulting in what we call 1-qubit space).

Notation. For vectors $\alpha = aH + bV$ and $\delta = eH + fV$, let $\langle \alpha \mid \delta \rangle = a^*e + b^*f$.

Since the arbitrary vector $\alpha = aH + bV$ is a state (i.e., represents the polarization state of some photon) exactly when $1 = a^*a + b^*b = \langle \alpha \mid \alpha \rangle$, we see that the vector α is a state if and only if it is a unit vector in our inner product space.

Notation. If $\beta = cH + dV$ is a state, let $\beta^\perp = -d^*H + c^*V$.

Exercises. Show that if β is a state, so is $\beta^\perp$, and $\beta, \beta^\perp$ is an orthonormal basis of our inner product space. Show that if β represents a photon polarized at some fixed angle θ, then $\beta^\perp$ is polarized at an angle perpendicular to θ. Show that $H^\perp = V$.

Readings. Given a state β, there exists a reading device (often called a measuring device) which can reliably distinguish between the states β and $\beta^\perp$. We will denote that device by R_β. If a photon in state β encounters the device R_β, it passes through, and the device registers a 0. However, if a photon in state $\beta^\perp$ encounters the device, it reflects back, and the device registers a 1. We say that R_β reads β as 0 and reads $\beta^\perp$ as 1.

What happens if a photon in state α encounters the device R_β? Is it read as 0 or as 1 (the device having no other options available to it)? We state the answer below.

Experimentally verified facts. If a photon in state α is read with device R_β, the probability is $|\langle \beta \mid \alpha \rangle|^2$ that R_β registers 0 (and the photon passes through the device), while there is probability $|\langle \beta^\perp \mid \alpha \rangle|^2$ that R_β registers 1 (and the photon reflects back from the device).

Exercises. Show that $|\langle \beta \mid \alpha \rangle|^2 + |\langle \beta^\perp \mid \alpha \rangle|^2 = 1$, and so we either get a reading of 0, or a reading of 1. Note that since $|\langle \beta \mid \alpha \rangle|^2 = \langle \beta \mid \alpha \rangle \langle \beta \mid \alpha \rangle^*$ is real and nonnegative, $|\langle \beta \mid \alpha \rangle|^2$ and $|\langle \beta^\perp \mid \alpha \rangle|^2$ are both between 0 and 1. (That last can also be done via the Cauchy-Schwartz inequality.) Let θ be an arbitrary angle. Let $\beta = (\cos\theta)H + (\sin\theta)V$.

Let $\alpha = \frac{1}{\sqrt{2}}H \pm \frac{i}{\sqrt{2}}V$. Show that when a photon in state α is read with R_β, the probability of getting 0 is $\frac{1}{2}$, independent of θ.

Remark. In the above facts, there does not appear to be any way to predict in advance whether the device will register a 0 or a 1. It appears to be truly up to chance. That is somewhat profound, since true chance is hard to come by. A moment's thought shows that the outcome of a coin toss is pragmatically up to chance, since the relevant factors determining that outcome are very hard to measure precisely. Yet those factors do exist, and if precisely known, the outcome could be reliably predicted. Not so with our photon and reading device. Also, it is known that random number generating computer programs fail to pass sophisticated tests for randomness. The outcome of reading our photon does appear to pass such tests, and appears to be truly random, modulo the probabilistic rules stated above.

Before discussing our first unknowable matter, we must state a crucial fact.

Fact. The only way to extract information about the state of a photon is to read the photon with some R_β.

Notation. Throughout this work, we will fix $\sigma = \frac{3}{5}H + \frac{4}{5}V$ and $\rho = \frac{-3}{5}H + \frac{4}{5}V$.

Claim 1. *If a photon is in an unknown state, there is no way to identify that state.*

Claim 2. *If the state of a photon is unknown, but is known to be one of σ, ρ, H, or V, there is no way of identifying which.*

Obviously if claim 2 is true, then so is claim 1. In this work, we will concentrate on claim 2. (We could deal with claim 1 directly, but that would only add abstraction without adding wisdom.) We now give a justification for claim 2, but will then consider possible loopholes in the argument. We begin with a lemma.

Lemma. *If a photon in state χ is read with R_β, the probability of getting 0 and the probability of getting 1 are both positive unless either $\chi = f\beta$ or $\chi = f\beta^\perp$, for a complex number f such that $|f|^2 = 1$.* (Such an f is called a phase factor, and β and $f\beta$ are considered identical states. By considering our probabilistic rules for readings, the reader should have little trouble figuring out why.)

Proof. Suppose the probability of getting 0 is 0. Then $|\langle \beta \mid \chi \rangle|^2 = 0$, so that $\langle \beta \mid \chi \rangle = 0$. Also, the previous exercise shows $|\langle \beta^\perp \mid \chi \rangle|^2 = 1$. Since we know $\beta, \beta^\perp$ is an orthonormal basis, standard arguments show that $\chi = \langle \beta \mid \chi \rangle \beta + \langle \beta^\perp \mid \chi \rangle \beta^\perp = \langle \beta^\perp \mid \chi \rangle \beta^\perp = f\beta^\perp$, where $f = \langle \beta^\perp \mid \chi \rangle$ has $|f|^2 = 1$. Similarly, if the probability of getting 1 is 0, then $\chi = \langle \beta \mid \chi \rangle \beta = f\beta$, with $|f|^2 = 1$. □

Justification of Claim 2. Let $\chi \in \{\sigma, \rho, H, V\}$ be the state of our photon. The only way we can extract information about χ is to read it with some R_β, and the only information we get will be a 0 or a 1. Suppose β is not of the form $f\psi$ for any $\psi \in \{\sigma, \sigma^\perp, \rho, \rho^\perp, H, H^\perp, V, V^\perp\}$ and $|f|^2 = 1$. Then the lemma shows the reading might give 0 or it might give 1, both with positive probability, *no matter which of the four possibilities* χ *is*, and so is of no help in determining which of our four possibilities really is χ. Therefore, the only possibly useful choices for β are $f\sigma$, $f\sigma^\perp$, $f\rho$, $f\rho^\perp$, fH, $fH^\perp$, fV, and $fV^\perp$. We consider the case $\beta = f\rho$, the others being similar. If our reading is 1, then we know that $\chi \neq \rho$ (since reading ρ with R_β must give 0). However, we easily see that reading any of σ, H, or V with R_β has a positive probability of giving 1, and so those cases cannot be eliminated. In other words, a reading of 1 (with $\beta = f\rho$) only eliminates the case $\chi = \rho$, leaving σ, H, and V as possible values of χ. On the other hand, a reading of 0 (for that same β) is utterly useless, since all of σ, ρ, H, and V have positive probability of giving 0 when read by R_β. □

The argument in the above justification is sound, as far as it goes, but it does leave a few possible loopholes. We will discuss three of them, two easily closed. In order to understand the first two loopholes, it will be helpful to consider a solvable problem.

Claim 3. *Suppose we have* 201 *photons, and we know that they are either all in the state* σ*, or all in the state* ρ*, or all in the state* H*, or all in the state* V*. Then we can (almost certainly) identify what the state is.*

Proof. Read the first hundred photons, using R_σ. If the correct state is σ, each such reading will have probability $|\langle \sigma \mid \sigma \rangle|^2 = (9/25 + 16/25)^2 = 1$ of being 0 (i.e., each reading must be 0). If the correct state is ρ, each reading will have probability $\langle \sigma \mid \rho \rangle^2 = (-9/25 + 16/25)^2 = .0784$ of being 0. If the correct state is H, each such reading will have probability $\langle \sigma \mid H \rangle^2 = 9/25$ of being 0. If the correct state is V, each such reading will have probability $\langle \sigma \mid V \rangle^2 = 16/25$ of being 0. Except in the case the correct state is σ, there is a noticeable chance the reading will be 1. (For example, if the correct state is actually V, the probability the reading gives 1 is $1 - 16/25 = 9/25$.) Thus, if the correct state is one of ρ, H, or V, then within the first hundred readings, at least one reading of 1 has a very high probability of appearing. Therefore, if the first hundred readings are all 0, we conclude (with a high degree of certainty) that the correct state is σ, while if a 1 ever appears, we know it is not σ (narrowing the field to ρ, H, or V). In the latter case, we switch to R_ρ, and use it to read the second hundred photons. Arguing similarly, we see that if all hundred of them read as 0, then the correct state is (almost certainly) ρ, while if a 1 ever appears, we know it cannot be ρ (narrowing the field to either H or V). In that case, read the last photon with R_H. Getting 0 tells us the correct state is H, while getting 1 tells us it is V. □

Exercise. Suppose in the above claim, the correct state is V. Show the probability of our algorithm misidentifying it is less than 10^{-19}.

We now consider loopholes in our justification of claim 2.

Loophole 1. Why not read the photon 201 times, using the algorithm of the previous proof to find the state of the photon?

Closure 1. There is something important about reading a photon that we have not yet said. Suppose a photon in state χ is read with R_β. If the reading is 0, then the photon converts to state β, while if the reading is 1, then the photon converts to state $\beta^\perp$. (This is experimentally verified.) Suppose χ is read by R_β 100 times in a row. If the first reading is 1, then χ converts to $\beta^\perp$, and the following 99 readings automatically give 1 as well. Those last 99 readings are not reading χ at all! Multiple readings are useless. (This is part of the general fact expressed in the phrase 'an observation affects that which is observed'.)

Loophole 2. Why not make 201 copies of the photon, and read each of them once?

Closure 2. The 'no cloning theorem' says there is no way of reliably making a copy of an unknown polarization state. A simple proof based on the axioms of quantum physics can be found in [G, p.191]. We will later give a different proof of the no cloning theorem.

The fact that a reading changes the state being read, and the inability to clone an unknown state, together seem to conspire to prevent us from learning the unknown state of a photon. However, one has to consider the possibility that there is some very clever subtle way of doing it. It is often true that showing something is possible is easier than showing it is impossible, since in the latter case, you must show you have closed all loopholes. For example, the standard proof of the no cloning theorem is valid only if the axioms of quantum physics upon which it rests are valid. Lots of evidence indicates that they are, and yet there are some very smart people working hard to find a general theory encompassing both quantum theory and relativity. If they succeed, that new theory might reveal subtle ways of doing things that presently appear impossible. That leads to our third loophole.

Loophole 3. The justification given for claim 2 depends upon the alleged fact that the only way to extract information about the state of a photon is to take a reading. Is that fact actually true, or will future discoveries reveal another way to extract that information?

We are ready to state our goal.

Theorem. *If it is impossible to send messages faster than light, then claims 1 and 2 are true, and cloning must be impossible.*

Basically, our theorem transfers the burden of proof from the realm of quantum physics, to the realm of special relativity, since it is those good folks who tell us faster than light communication is impossible.

2-Qubit States

We will need to work with a pair of photons, thought of as a first photon and a second photon. We now discuss how to express the state of such a pair. Let us begin by supposing that we have four 1-qubit states, $\alpha = aH + bV$, $\beta = cH + dV$, $\gamma = eH + fV$, and $\lambda = gH + hV$. Let us suppose the first photon in our pair is in state α and is read by device R_γ, while the second photon is in state β and is read by device R_λ.

Since the first photon (in state α) is read by R_γ, we already know the probability of getting 0 is $|\langle\gamma \mid \alpha\rangle|^2$. Since the second photon (in state β) is read by R_λ, we already know the probability of getting 1 is $|\langle\lambda^\perp \mid \beta\rangle|^2$. Therefore, the probability reading 0 from the first photon and 1 from the second (which we denote $P(0,1)$) is $|\langle\gamma \mid \alpha\rangle|^2|\langle\lambda^\perp \mid \beta\rangle|^2$. The reader can easily verify the following:

$$\begin{aligned}
P(0,0) &= |\langle\gamma \mid \alpha\rangle|^2|\langle\lambda \mid \beta\rangle|^2 \;, \\
P(0,1) &= |\langle\gamma \mid \alpha\rangle|^2|\langle\lambda^\perp \mid \beta\rangle|^2 \;, \\
P(1,0) &= |\langle\gamma^\perp \mid \alpha\rangle|^2|\langle\lambda \mid \beta\rangle|^2 \;, \\
P(1,1) &= |\langle\gamma^\perp \mid \alpha\rangle|^2|\langle\lambda^\perp \mid \beta\rangle|^2 \;.
\end{aligned}$$

It is not difficult to find a mathematical structure in which those facts can be embedded. We work in a 4-dimensional vector space over the complex numbers having as a basis the four symbols $H \otimes H$, $H \otimes V$, $V \otimes H$, and $V \otimes V$. We impose the following inner product.

Notation. If $\Lambda = pH \otimes H + qH \otimes V + rV \otimes H + sV \otimes V$ and $\Delta = wH \otimes H + xH \otimes V + yV \otimes H + zV \otimes V$, then $\langle \Lambda \mid \Delta \rangle = p^*w + q^*x + r^*y + s^*z$.

Definition. A 2-qubit state is a unit vector in this inner product state.

Definition. The tensor product of $\alpha = aH + bV$ and $\beta = cH + dV$ is $\alpha \otimes \beta = acH \otimes H + adH \otimes V + bcV \otimes H + bdV \otimes V$.

Recall, the first photon of our pair is in state α, and the second is in state β. We are seeking a way of describing the state of those two photons considered as a pair. The reader might guess that the answer will turn out to be $\alpha \otimes \beta$, but of course, we need to justify why that is so. We devote the remainder of this section to that task.

Exercise. If $\alpha = aH + bV$ and $\beta = cH + dV$ are 1-qubit states, show $\alpha \otimes \beta$ is a 2-qubit state, by showing that $|ac|^2 + |ad|^2 + bc|^2 + |bd|^2 = 1$. Then read the next lemma, and use it to do this exercise another way.

Lemma. *If α, β, γ, and λ are vectors in 1-qubit space, then* $\langle \gamma \otimes \lambda \mid \alpha \otimes \beta \rangle = \langle \gamma \mid \alpha \rangle \langle \lambda \mid \beta \rangle$.

Proof. Let $\alpha = aH + bV$, $\beta = cH + dV$, $\gamma = eH + fV$, and $\lambda = gH + hV$. Then $\alpha \otimes \beta = acH \otimes H + adH \otimes V + bcV \otimes H + bdV \otimes V$ and $\gamma \otimes \lambda = egH \otimes H + ehH \otimes V + fgV \otimes H + fhV \otimes V$. Thus $\langle \gamma \otimes \lambda \mid \alpha \otimes \beta \rangle = (eg)^*(ac) + (eh)^*(ad) + (fg)^*(bc) + (fh)^*(bd) = (e^*a + f^*b)(g^*c + h^*d) = \langle \gamma \mid \alpha \rangle \langle \lambda \mid \beta \rangle$. □

Recall we are considering a pair of photons, supposing the first is read by R_γ and the second is read by R_λ. Let us denote the compound reading device consisting of those two individual reading devices used together as $R_{\gamma \otimes \lambda}$. Thus, our pair of photons (the first in state α, the second in state β) is being read by the (compound) device $R_{\gamma \otimes \lambda}$.

We earlier saw that $P(0,1) = |\langle \gamma \mid \alpha \rangle|^2 |\langle \lambda^\perp \mid \beta \rangle|^2$. In view of the lemma, we have $P(0,1) = |\langle \gamma \mid \alpha \rangle \langle \lambda^\perp \mid \beta \rangle|^2 = |\langle \gamma \otimes \lambda^\perp \mid \alpha \otimes \beta \rangle|^2$. Similarly, the reader can easily verify the following:

$$\begin{aligned}
P(0,0) &= |\langle \gamma \otimes \lambda \mid \alpha \otimes \beta \rangle|^2 , \\
P(0,1) &= |\langle \gamma \otimes \lambda^{\perp} \mid \alpha \otimes \beta \rangle|^2 , \\
P(1,0) &= |\langle \gamma^{\perp} \otimes \lambda \mid \alpha \otimes \beta \rangle|^2 , \\
P(1,1) &= |\langle \gamma^{\perp} \otimes \lambda^{\perp} \mid \alpha \otimes \beta \rangle|^2 .
\end{aligned}$$

Our goal was to find a description of the state of our pair of photons (the first in state α, the second in state β). The preceding probabilistic rules make it clear that we should take $\alpha \otimes \beta$ to be the (2-qubit) state of our pair of photons.

Entanglement

Exercise. Let $\Delta = \frac{3}{5\sqrt{2}} H \otimes H + \frac{4}{5\sqrt{2}} H \otimes V + \frac{-3}{5\sqrt{2}} V \otimes H + \frac{4}{5\sqrt{2}} V \otimes V$. Show that Δ is a unit vector (hence a 2-qubit state), but that there does not exist any pair of 1-qubit states $\alpha = aH + bV$ and $\beta = cH + dV$, such that $\alpha \otimes \beta = \Delta$.

In view of the preceding easy exercise, the reader might think that Δ cannot represent the state of any pair of photons. Somewhat surprisingly, that is not so. In fact, any 2-qubit unit vector (i.e., a 2-qubit state) can be realized as the actual polarization state of some pair of photons that can be produced — with some effort — in a lab. States of the form $\alpha \otimes \beta$ are called product states. States not of that form (such as the above Δ) are called entangled states. Entangled states are one of the most fascinating aspects of quantum physics. They are used extensively in the theory of quantum computing (it being very much a theory, since quantum computers do not yet exist except as prototypes). We will explain the most interesting aspect of entanglement.

Experimentally verified facts. If a pair of photons in the 2-qubit state Δ is read by the device $R_{\gamma \otimes \lambda}$, the following are true. (We already know these are true when $\Delta = \alpha \otimes \beta$ is a product state, and are now asserting they also hold when Δ is entangled.)

$$\begin{aligned}
P(0,0) &= |\langle \gamma \otimes \lambda \mid \Delta \rangle|^2 , \\
P(0,1) &= |\langle \gamma \otimes \lambda^{\perp} \mid \Delta \rangle|^2 , \\
P(1,0) &= |\langle \gamma^{\perp} \otimes \lambda \mid \Delta \rangle|^2 , \\
P(1,1) &= |\langle \gamma^{\perp} \otimes \lambda^{\perp} \mid \Delta \rangle|^2 .
\end{aligned}$$

Notation. In the remainder of this paper we will let $\Delta = \frac{3}{5\sqrt{2}} H \otimes H + \frac{4}{5\sqrt{2}} H \otimes V + \frac{-3}{5\sqrt{2}} V \otimes H + \frac{4}{5\sqrt{2}} V \otimes V$ (this being entangled), and we will let $\tau = \frac{1}{\sqrt{2}} H - \frac{1}{\sqrt{2}} V$. Furthermore, we will take $\beta = cH + dV$ to be an arbitrary 1-qubit state. Also, recall that $\sigma = \frac{3}{5}H + \frac{4}{5}V$, and $\rho = \frac{-3}{5}H + \frac{4}{5}V$.

Let us investigate what happens if a pair of photons in the state Δ just given is read by the compound device $R_{H\otimes\beta}$, (so that the first photon is read by R_H and the second is read by R_β). The above experimentally verified facts tell us

$$\begin{aligned} P(0,0) &= |\langle H \otimes \beta \mid \Delta\rangle|^2 \\ &= |\langle cH \otimes H + dH \otimes V | \frac{3}{5\sqrt{2}} H \otimes H + \frac{4}{5\sqrt{2}} H \otimes V + \frac{-3}{5\sqrt{2}} V \otimes H + \frac{4}{5\sqrt{2}} V \otimes V\rangle|^2 \\ &= |\frac{3c^*}{5\sqrt{2}} + \frac{4d^*}{5\sqrt{2}}|^2 = \frac{1}{50}(9|c|^2 + 12(c^*d + cd^*) + 16|d|^2) \ . \end{aligned}$$

Next, using that $H \otimes \beta^\perp = H \otimes (-d^*H + c^*V) = -d^*H \otimes H + c^*H \otimes V$, we easily see that

$$P(0,1) = |\langle H \otimes \beta^\perp \mid \Delta\rangle|^2 = \frac{1}{50}(16|c|^2 - 12(c^*d + cd^*) + 9|d|^2) \ .$$

Similarly, we see

$$P(1,0) = |\langle H^\perp \otimes \beta \mid \Delta\rangle|^2 = \frac{1}{50}(9|c|^2 - 12(c^*d + cd^*) + 16|d|^2) \ ,$$

and

$$P(1,1) = |\langle H^\perp \otimes \beta^\perp \mid \Delta\rangle|^2 = \frac{1}{50}(16|c|^2 + 12(c^*d + cd^*) + 9|d|^2) \ .$$

Exercise. Obviously the probability that the first photon is read as 0 is $P(0,0)+P(0,1)$. Show that equals $1/2$. (Use that $|c|^2 + |d|^2 = 1$.) Then argue that $P(1,0) + P(1,1)$ must also equal $1/2$, and verify that it does.

In the preceding, the second photon is read using R_β, with β arbitrary. The probability that it reads as 0 is clearly equal to

$$\begin{aligned} P(0,0) + P(1,0) &= \frac{1}{50}(9|c|^2 + 12(c^*d + cd^*) + 16|d|^2) + \frac{1}{50}(9|c|^2 - 12(c^*d + cd^*) + 16|d|^2) \\ &= \frac{1}{25}(9|c|^2 + 16|d|^2) = \frac{1}{25}(9|c|^2 + 16(1 - |c|^2)) = \frac{1}{25}(16 - 7|c|^2) \ . \end{aligned}$$

Since $0 \le |c|^2 \le 1$, that probability lies between $\frac{16-7}{25} = \frac{9}{25}$ and $\frac{16}{25}$. From that, we deduce that the second photon is not in the state β, since if it were in the state β, when read by R_β, the probability of getting 0 would be $|\langle\beta \mid \beta\rangle|^2 = 1$. Since the actual probability is at most $\frac{16}{25}$, that second photon cannot be in the state β, for any choice of β.

Remark. The preceding argument shows that entangled states are fundamentally different than product states. In the product state $\alpha \otimes \beta$, the second photon is in state β, and the first is in state α. However, in an entangled state, neither photon is in an individual state. Their state can only be described by taking both photons into account.

Exercise. Suppose the product state $\alpha \otimes \beta$ is read with $R_{\varphi\otimes\beta}$, where φ is arbitrary. Show the probability that the second photon reads as 0 is 1. (That reflects the fact that the second photon really is in the state β in this product state.)

We continue to analyze our reading of the fixed Δ with $R_{H\otimes\beta}$, (β arbitrary). The probabilistic rules given above do not depend upon the timing of the readings. The two photons can be read simultaneously, or either can be read an arbitrary amount of time after the other is read. To be explicit, let us say the second photon is read an hour later than the first one. Let us also suppose that when the first photon is read (using R_H), it gives 0. We now ask what will happen with the second photon when it is read an hour later (using R_β), specifically asking what the probability is that it will give 0?

The question we just asked requires finding the conditional probability $P(2^{\text{nd}} = 0 \mid 1^{\text{st}} = 0)$, the probability that the second photon reads as 0 given that the first one reads as 0. We know from the theory of probability that $P(2^{\text{nd}} = 0 \mid 1^{\text{st}} = 0) = \frac{P(0,0)}{P(0,0)+P(0,1)}$. As an earlier exercise shows the denominator is 1/2, we see that

$$P(2^{\text{nd}} = 0 \mid 1^{\text{st}} = 0) = 2P(0,0) = \frac{1}{25}(9|c|^2 + 12(c^*d + cd^*) + 16|d|^2) .$$

Now that is easily seen to equal $|\langle cH + dV|\frac{3}{5}H + \frac{4}{5}V\rangle|^2 = |\langle \beta \mid \sigma\rangle|^2$. However, that last is exactly the probability that when a photon in state σ is read by the device R_β, the reading is 0.

Similarly, the conditional probability $P(2^{\text{nd}} = 1 \mid 1^{\text{st}} = 0)$ (that the second photon reads as 1 given that the first photon reads as 0) is

$$\frac{P(0,1)}{P(0,0)+P(0,1)} = 2P(0,1) = \frac{1}{25}(16|c|^2 - 12(c^*d + cd^*) + 9|d|^2)$$

$$= |\langle -d^*H + c^*V \mid \frac{3}{5}H + \frac{4}{5}V\rangle|^2 = |\langle \beta^\perp \mid \sigma\rangle|^2$$

which is exactly the probability that when a photon in state σ is read by the device R_β, the reading is 1.

Let us summarize. We started with a pair of photons in state Δ, and read the first photon using R_H, getting 0 for the reading. An hour later we read the second photon using R_β. We have seen that the probability of that second reading being 0 equals the probability of getting 0 when σ is read by R_β, and the probability of getting 1 equals the probability of getting 1 when σ is read by the device R_β. In other words, when we go to read that second photon, it behaves exactly as if it were in the state σ. (This is assuming the first photon read as 0.)

Let us now suppose that when the first photon is read by R_H, it gives 1, and see what happens to the second photon when it is read by R_β. (We will show it behaves as if it were in the state ρ.) The conditional probability that the second photon will be read as 0 is

$$\begin{aligned} P(2^{\text{nd}} = 0 \mid 1^{\text{st}} = 1) &= \frac{P(1,0)}{P(1,0)+P(1,1)} = 2P(1,0) \\ &= \frac{1}{25}(9|c|^2 - 12(c^*d + cd^*) + 16|d|^2) = |\langle cH + dV \mid \frac{-3}{5}H + \frac{4}{5}V\rangle|^2 \\ &= |\langle \beta \mid \rho\rangle|^2 , \end{aligned}$$

which is exactly the probability that when a photon in state $\rho = \frac{-3}{5}H + \frac{4}{5}V$ is read by the device R_β, the reading is 0. Finally, the conditional probability that the second photon will read as 1 is

$$\begin{aligned} P(2^{\text{nd}} = 1 \mid 1^{\text{st}} = 1) &= \frac{P(1,1)}{P(1,0)+P(1,1)} = 2P(1,1) \\ &= \frac{1}{25}(16|c|^2 + 12(c^*d + cd^*) + 9|d|^2) = |\langle -d^*H + c^*V \mid \frac{-3}{5}H + \frac{4}{5}V\rangle|^2 \\ &= |\langle \beta^\perp \mid \rho\rangle|^2 , \end{aligned}$$

which is exactly the probability that when a photon in state ρ is read by the device R_β, the reading is 1.

Again we summarize. Suppose the first photon of the pair in the state Δ is read using R_H. If that reading is 0, then the second photon behaves as if it were in state σ, while if that reading is 1, the second photon behaves as if it were in state ρ. (Both of these statements hold with respect to the *arbitrary* reading device R_β.)

Pragmatic assertion. Based on the foregoing, we assert that if the first reading is 0, then the second photon becomes disentangled from the first, and goes into the state σ, while if the first reading is 1, the second photon becomes disentangled from the first and goes into the state ρ. Now a purist might disagree with our assertion, putting forth the possibility that the second photon exists in some sort of limbo until it actually is read. However, there is no way of telling which model is correct, and our pragmatic model is convenient, so we adopt it.

The fact stated in our assertion is encoded in the following fact, left as an exercise.

Exercise. Show $\Delta = \frac{1}{\sqrt{2}}H \otimes \sigma + \frac{1}{\sqrt{2}}H^{\perp} \otimes \rho$.

We earlier saw that the second photon of a pair in the entangled state Δ is not in any individual state β of its own. However, reading the first photon (with R_H) causes the second photon to go to one of the two individual states σ or ρ. (The first photon also goes into an individual state, in our case, either state H or state V. This behavior holds for any entangled state and any reading of either photon. Readings destroy entanglement.)

We are next going to give a similar argument, but this time reading Δ with $R_{\tau\otimes\beta}$ (recalling that $\tau = \frac{1}{\sqrt{2}}H - \frac{1}{\sqrt{2}}V$ and $\beta = cH + dV$ is arbitrary). Recall that means the first photon of the pair in the entangled state Δ is read using R_τ, and the second photon is read using R_β (say an hour later).

We will calculate $P(0,0)$, $P(0,1)$, $P(1,0)$, and $P(1,1)$, now understanding these are with respect to $R_{\tau\otimes\beta}$ and not $R_{H\otimes\beta}$, as previously.

We have

$$P(0,0) = |\langle \tau \otimes \beta \mid \Delta\rangle|^2 = |\langle \frac{c}{\sqrt{2}}H \otimes H + \frac{d}{\sqrt{2}}H \otimes V + \frac{-c}{\sqrt{2}}V \otimes H + \frac{-d}{\sqrt{2}}V \otimes V \mid \Delta\rangle|^2 .$$

Since $\Delta = \frac{3}{5\sqrt{2}}H \otimes H + \frac{4}{5\sqrt{2}}H \otimes V + \frac{-3}{5\sqrt{2}}V \otimes H + \frac{4}{5\sqrt{2}}V \otimes V$, we see that $P(0,0) = |6c^*/10|^2 = 36|c|^2/100$.

We leave the rest to the reader, in the following exercises.

Exercises. Show $P(0,1) = 36|d|^2/100$, $P(1,0) = 64|d|^2/100$, and $P(1,1) = 64|c|^2/100$. Show that $P(2^{\text{nd}} = 0 \mid 1^{\text{st}} = 0) = |c|^2 = |\langle cH + dV \mid H\rangle|^2 = |\langle \beta \mid H\rangle|^2$, and $P(2^{\text{nd}} = 1 \mid 1^{\text{st}} = 0) = |d|^2 = |\langle \beta^{\perp} \mid H\rangle|^2$. Conclude that if the first photon is read as 0, then the second photon goes to the state H. Also, show that $P(2^{\text{nd}} = 0 \mid 1^{\text{st}} = 1) = |d|^2 = |\langle \beta \mid V\rangle|^2$ and $P(2^{\text{nd}} = 1 \mid 1^{\text{st}} = 1) = |c|^2 = |\langle \beta^{\perp} \mid V\rangle|^2$. Conclude that if the first photon is read as 1, then the second photon goes to the state V.

Conclusions. Suppose a pair of photons is in the entangled state Δ.

If the first photon is read by R_H and gives 0, then the second photon goes to state σ.

If the first photon is read by R_H and gives 1, then the second photon goes to state ρ.

If the first photon is read by R_τ and gives 0, then the second photon goes to state H.

If the first photon is read by R_τ and gives 1, then the second photon goes to state V.

Exercise. With τ as above, show $\Delta = \frac{3}{5}\tau \otimes H + \frac{4}{5}\tau^{\perp} \otimes V$.

Remark. In general, if $\Delta = r\delta \otimes \kappa + s\delta^{\perp} \otimes \eta$ and if the first photon is read using R_δ, there is probability $|r|^2$ that it will give 0 and if so, the second photon goes to state κ, and there is probability $|s|^2$ that it gives 1, and if so, the second photon goes to state η. The interested reader can verify that. We have made use of two special cases of that fact.

We can now explain the truly fascinating aspect of entanglement. Consider our above pair of photons in the entangled state Δ. We have seen that the second photon is not in any individual 1-qubit state of its own. However, reading the first photon (with R_H for instance) causes the second photon to go into an individual 1-qubit state (either σ or ρ). Reading the first photon has an influence on the second photon. Now for the amazing part: that influence is instantaneous, and is independent of the distance between the two photons! We envisioned the second photon being read an hour after the first. We could as well have read it a nanosecond after the first, or even simultaneously with the first. The outcome would be the same, even if the two photons were light years apart.

Experiment. We describe an experiment that could be used to verify the instantaneous nature of entanglement's influence. Suppose Bob prepares a thousand pairs of photons, each pair in the entangled state Δ. Suppose Bob keeps the first photon of each pair, but sends the second photons to the distant Alice. They then both read their photons simultaneously. That is, both photons of the first pair are simultaneously read, both photons of the second pair are simultaneously read, etc.. Suppose all of Bob's readings use R_H, while all of Alice's readings use R_σ. Later, they compare notes (a slower than light process, but that is of no concern to us). They ignore all the pairs in which Bob's photons gave 1, only looking at those pairs for which it gave 0. For those pairs, we know that Alice's photons supposedly converted to state σ. That can be verified by checking that all of Alice's (non-ignored) readings are 0 (since she is using R_σ). They can then repeat the process with a new thousand entangled pairs, Bob again using R_H but Alice using R_ρ. When comparing notes, they now ignore those pairs for which Bob got 0 only considering the pairs for which he got 1. In those cases, Alice's photons should be in state ρ, which will be verified by the fact that she always gets 0 when reading them with R_ρ. (In what we discuss later, Alice will not be allowed to compare notes with Bob. She will have to try to figure out what happened at Bob's end by only reading her photons. She will find that impossible.)

The unknowable

Imagine that Bob prepares a pair of photons in the entangled state Δ, keeps the first photon, but sends the second to the far distant Alice. By reading his photon, Bob instantaneously influences Alice's photon. If Alice can detect that influence, she will know that Bob has read his photon. A piece of information ("Bob has read his photon") will have been instantaneously communicated between the two of them. If we accept that faster than light communication is impossible — and there are very strong reasons to believe that is so — then we must conclude that Alice cannot detect the influence that Bob asserts on her photon. We next explore the consequences of that conclusion, beginning with a proof of the theorem stated as our goal.

Proof of theorem. We assume faster than light communication is impossible. We previously saw that the truth of claim 2 implies the truth of claim 1, and also implies that cloning is impossible. Therefore, we must only show that claim 2 follows from the assumption just given. Thus, suppose claim 2 is false. (We will describe a way of communicating faster than light.)

Consider the situation described in the opening sentence of this section. It is agreed that at noon, Bob will read his photon, using either R_H or R_τ. A very short time after noon, Alice will try to determine which of those two reading devices Bob used. If she can, information has been transmitted from Bob to Alice faster than the speed of light.

We know that if Bob used R_H, then the state of Alice's photon is in the set $\{\sigma, \rho\}$ while if Bob used R_τ, then the state of Alice's photon in the set $\{H, V\}$. Thus the state of her photon is one of σ, ρ, H, or V. As we are assuming claim 2 is false, Alice can find the state of her photon. Thus she can determine whether it is in the set $\{\sigma, \rho\}$ (telling her Bob used R_H), or in the set $\{H, V\}$ (telling her Bob used R_τ). □

We have just seen that if faster than light communication is impossible, then it is impossible to identity the unknown state of a photon (claim 1), and also that cloning an unknown state is impossible. Other conclusions also follow. For example, loophole 1 shows that there must be some reason why multiple readings cannot be used to determine an unknown state. (Closure 1 explains what that reason is.) We consider a few other consequences of the impossibility of faster than light communication.

Let us first modify the situation described in the previous proof. Let us suppose that at noon, Bob either reads his photon with R_H, or does nothing to it.

Claim 4. *In the circumstances just described, when Alice reads her photon at one o'clock, she cannot tell if it is in a 1-qubit state, or still in an entangled state.*

Proof. If Bob did nothing with his photon, Alice's photon is still part of an entangled state, while if Bob reads his photon, then hers is in a 1-qubit state (either σ or ρ). If Alice can tell which of those is the case, she knows what option Bob chose. □

Remark. The reader familiar with special relativity will see a related reason why Alice cannot tell if her photon is still entangled or not. Suppose at noon, Bob does read his photon, causing the pair to become disentangled. At one o'clock, Alice (two light hours away) reads her already disentangled photon. Special relativity tells us there are frames of reference in which Alice's reading was done first, and Bob's was done later. To those observers, it was Alice who caused the disentanglement. To some observers, Alice's photon was disentangled when she read it, to others it was still entangled.

We are seeing that the inability to communicate faster than light forces certain restrictions on what we can know about the state of a photon. Let us look at a more subtle aspect of that fact.

Consider two collections, each consisting of a million photons. In the first collection, approximately 9/25-ths of the photons are in state H and approximately 16/25-ths of them are in state V. In the second collection, approximately half the photons are in state σ, and approximately half are in state ρ. (In both collections, the various states involved are mixed together in some unknown manner, as opposed to saying, for example, that in the second collection, the odd numbered photons are in state σ and the even numbered ones are in state ρ.)

Claim 5. *It is impossible to tell which collection is which.*

We will start with an argument from quantum physics, and then look at an esoteric loophole. Then we will give a proof using the impossibility of faster than light communication, and so show that loophole cannot exist, thus learning something of interest.

Justification. We choose a reading device R_β, with $\beta = cH + dV$ arbitrary. We read all the photons in the first collection. The probability of one of those readings being 0 is obviously approximately $(9/25)|\langle\beta \mid H\rangle|^2 + (16/25)|\langle\beta \mid V\rangle|^2 = (9/25)|c|^2 + (16/25)|d|^2$. If instead we read all the photons in the second collection, the probability of getting 0 is approximately $(1/2)|\langle\beta \mid \sigma\rangle|^2 + (1/2)|\langle\beta \mid \rho\rangle|^2$, which the reader can verify also equals $(9/25)|c|^2 + (16/25)|d|^2$. Thus, no reading can distinguish between the two collections.

Loophole. Perhaps it is possible to simultaneously read a photon using both R_σ and R_ρ. Suppose that is so. Pick a random photon in the second collection. It is either in state σ or state ρ. When we simultaneously read it with both R_σ and R_ρ, one of those two readings must give 0 (and the other may or may not give 0). Thus, each simultaneous pair of readings will involve at least one 0. On the other hand, pick a random photon from the first collection. If it is in state V, then the probability that both of the simultaneous readings will be 1 is clearly $|\langle\sigma^\perp \mid V\rangle|^2|\langle\rho^\perp \mid V\rangle|^2 = (9/25)(9/25)$. As 16/25-ths of the photons in the first collection are in state V, it is very likely that when all the photons in the first collection are dealt with, we will get some paired reading comprising two appearances of 1. Thus, *if this loophole exists*, we can almost certainly distinguish between the two collections.

Proof of Claim 5 (assuming faster than light communication is impossible). Bob and Alice take a million pairs of photons, each pair in the entangled state Δ, Bob having all the first photons, and the far distant Alice having all the second photons. At noon, Bob either reads all his first photons using R_H, or reads all his first photons using R_τ. (In either case, an hour later, Alice intends on reading all her photons with an arbitrary R_β.)

Suppose Bob uses R_H. Consider one of the entangled pairs. Since the combined reading device is $R_{H\otimes\beta}$, when Bob reads its first photon, we know that the probability he gets 0 is $P(0,0) + P(0,1) = |\langle H \otimes \beta \mid \Delta\rangle|^2 + |\langle H \otimes \beta^\perp \mid \Delta\rangle|^2$. An earlier exercise shows that equals 1/2. Thus there is a probability of 1/2 that he gets 0 (in which case we know Alice's corresponding second photon goes to state σ), and a probability of 1/2 that Bob gets 1 (in which case we known Alice's corresponding second photon goes to state ρ.) Thus, if Bob chooses the R_H option, when he is done reading all his first photons, approximately half of Alice's second photons will be in state σ, and approximately half will be in state ρ. However, that is exactly the description of the second collection of photons we are considering in claim 5.

We leave to the reader the argument that if Bob uses the R_τ option, then when he is done, Alice's collection of photons will fit the description of the first collection of claim 5.

If Alice could distinguish between those two collections, she could know (faster than light) which option Bob choose.

(Note that Alice never actually gets around to reading her photons with R_β. We just needed to mention some R_β, so as to be able to find $P(0,0) + P(0,1)$. That quantity is independent of β. After all, it is the probability of Bob getting 0, which surely cannot depend on what Alice does — or does not do — an hour later!)

We now see that the loophole mentioned above cannot exist. Actually, that fact is well known in quantum physics. The fact that you cannot read a photon with two different reading devices simultaneously, is analogous to the fact that you cannot simultaneously measure both the position and momentum of a particle. When two such measurements (or readings) cannot be simultaneously done, they are said to be complementary.

Question. Might the fact that faster than light communication is impossible be used to find some previously unknown restrictions on what can be learned by reading photons? (Probably not, since quantum physicists are pretty thorough, but it is interesting to contemplate the possibility.)

Exercise. (This exercise is harder than others in this paper.) We saw that reading the first photon of a pair in the entangled state Δ destroys that entanglement. Suppose that were false, and that the pair remains in the state Δ even after the first photon is read. (Option: Assume that reading the first photon changes the entangled state Δ to some other entangled state Δ'.) Devise a means of faster than light communication. (A personal note: when I first read a superficial account of entanglement, it did not mention that readings destroy entanglement. I did this exercise, but then began to suspect there was more to entanglement than I had been told. That was the germ which lead to this paper.)

Predictability and determinism

Let us consider flipping a coin. Although the outcome is pragmatically up to chance, the classical laws of physics tell us it is determined by variables such as the dimensions and weight of the coin, and similar variables concerning the flipping device. In fact, we accept that if we actually knew the values of all the relevant variables, we could predict the outcome of the coin flip. Let us emphasize that the prediction will be hypothetically true, even if the predictive process is applied to a hypothetical flip, and so the process can be applied to a given coin as often as we like with as many different hypothetical flipping devices as we wish.

In this section, we will use the above sense of the word 'predictable'. However, that is all we will assume about that word. Thus, we will not make any assumptions concerning the method of prediction. As an extreme example, we allow the possible existence of an oracle, capable of instantaneously tapping into knowledge from far distant parts of the universe, or the inside of black holes.

Theorem. *If faster than light communication is impossible, then the outcome of reading a photon is not predictable.*

Proof. We have already seen that if we could identify the state of a photon known to be in one of the four states σ, ρ, H or V, then we could communicate faster than light. If the outcome of reading a photon is predictable (in our sense of that word), then we could make 201 predictions, and use the algorithm in the proof of claim 3 to identify the unknown state. □

We now turn to what can be said concerning whether the outcome of reading a photon is determined.

Terminology. A determined event is locally determined if information from all the variables going into the determination can reach the location of the event prior to the completion of the event. Otherwise, the event is non-locally determined.

It might be difficult to conceive of something happening here on earth, whose outcome depends upon something which happened a nanosecond earlier in a galaxy 10 billion light years away, but the concept of non-local determinism allows that possibility.

It is also difficult to imagine that a non-locally determined event (if such exists) could be predictable, except via an oracle (if such exists). However, locally determined events could conceivably be predictable to mere humans, just as we accept the predictability of a coin flip.

Corollary. *If faster than light communication is impossible, and if locally determined events are predictable, then the outcome of reading a photon is not locally determined.*

Proof. This follows immediately from the previous theorem. □

The above theorem and corollary seem to be as far as the arguments presented in this paper allow us to go. However, we question the corollary's assumption that locally determined events are predictable. That is, we consider the possible existence of local *determining variables* that are forever hidden from us (or from the oracle), and so are *not available for predictions*. John S. Bell presented an argument more subtle than ours, which allowed him to prove the following. (The majority of physicists accept the truth of the following, although there are dissenters.)

Bell's Theorem. *If faster than light communication is impossible, then the outcome of reading a photon is not locally determined.*

Bell's argument involves a set-up in which Bob and Alice each have a choice of reading devices, Bob being able to choose between R_A and R_B, while Alice can choose between R_C and R_D (where these reading devices are cleverly specified by Bell). They make their choices at random and do their readings simultaneously. Suppose the outcome of reading a photon is determined. Then it follows from [M2, Section 8 and Remarks 1 and 2, p.809], that if Alice's two possible readings are both independent of which choice of reading device Bob uses, and vice-versa, then a contradiction exists. Thus, if we have determinism, then either a reading on Alice's end depends upon a choice made by Bob, or vice-versa, (or both), and so the determinism must be non-local. (Bob's choice is a non-local variable to Alice, since faster than light communication is impossible.)

If it could be shown that local determinism implies predictability, then our corollary would constitute an alternate proof of Bell's theorem. However, we consider that implication to be questionable. Presentations of Bell's theorem (also called Bell's inequality) often refer to local *hidden* variables. Since the word 'hidden' reminds us of the possible difference between local determinism and predictability, we consider it important.

Further Reading

This paper is a simplified version of [M1], which covers the same ground in more detail (perhaps too much detail). [M2] presents Bells' argument that the instantaneous influence of entanglement is not due to 'local hidden variables' (as Einstein believed). [G] is somewhat more sophisticated than this paper, but is highly readable, and gives an introduction to the axioms of quantum states. It introduces Dirac notation and its use in quantum computation, providing adequate background for reading [S], which is Peter Shor's groundbreaking paper on how to use entanglement to factor large numbers and solve the discrete log problem. [M3] is an accounting of Shor's work, suitable for beginners. [M4] recounts (with background information added) another quantum algorithm that can be used for factorization, introduced in [K].

References

[G] Stan Gudder, *Quantum Computation*, Amer. Math. Monthly **110** (2003), 181–201.

[K] A. Y. Kiteav, *Quantum measurements and the Abelian stabilizer problem*, arXiv:quant-ph/9511026v1, November 20, 1995.

[M1] S. McAdam, *Entanglement*, available at www.ma.utexas.edu/users/mcadam

[M2] S. McAdam, *Bell's theorem and the demise of local reality*, Amer. Math. Monthly **110** (2003), 800–811.

[M3] S. McAdam, *Shor's algorithm*, www.ma.utexas.edu/users/mcadam

[M4] S. McAdam, Kiteav's Algorithm, www.ma.utexas.edu/users/mcadam

[S] Peter Shor, *Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer*, available at `xxx.lanl.gov/abs/quant-ph/9508027`

Department of Mathematics, The University of Texas at Austin
E-mail address: `mcadam@math.utexas.edu`