Successful Quantum Cloning Would Imply Faster-Than-Light Communication

Kirk T. McDonald
Joseph Henry Laboratories, Princeton University, Princeton, NJ 08544
(October 10, 2004)

1 Problem[1]

Show that exact cloning of an arbitrary quantum state could lead to a scheme for faster-than-light communication. In particular, consider an entangled state of two Qbits:

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|0\rangle_{\rm A}|0\rangle_{\rm B} + |1\rangle_{\rm A}|1\rangle_{\rm B}}{\sqrt{2}}, \tag{1}$$

such that after creation of this state the physical realizations of the first and second bits become separated in space. A famous example of this is the S-wave decay of an excited atom via two back-to-back photons.

Observer A (Alice) can chose to observe bit A in the basis $[|0\rangle, |1\rangle]$, or in the basis $[(|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}] \equiv [|+\rangle, |-\rangle]$ (among the infinite set of bases for a single Qbit), and the choice of which basis she uses can be delayed; *i.e.*, Alice can wait to choose her observational basis until after the bits A and B have separated in space.

The "message" that Alice wishes to send to observer B (Bob) is her choice of basis for observation of bit A, and the result of her observation.

If the state (1) cannot be cloned, Bob can make only a single observation, and must choose a single basis (either $[|0\rangle, |1\rangle]$ or $[|+\rangle, |-\rangle]$) for this.

Describe the possible correlations between the results of measurements by Alice on bit A with the results of measurements by Bob on bit B, given that both Alice and Bob can choose to use either the $[|0\rangle, |1\rangle]$ or the $[|+\rangle, |-\rangle]$ bases. Can the measurements made by Bob, in the absence of classical communication from Alice as to the nature of her measurements, be interpreted by Bob as certain knowledge by him as to which choice of basis was made by Alice? To answer this, it is helpful to re-express state (1) in the $[|+\rangle, |-\rangle]$ basis. You may or may not find it helpful to construct and apply measurement operators to the appropriate representations of the entangled state of bits A and B.

Now suppose that Bob could clone his bit B in such a manner that the clones retained the entangled structure of state (1). Describe a set of measurements on these clones that would permit Bob to know with certainty (*i.e.*, with very high probability) what choice of basis had been made by Alice. Since Alice and Bob could, in principle, be separated by arbitrarily large distances at the times that they make their measurements, successful deduction by Bob as to Alice's choice of basis would imply an "instantaneous" communication from Alice

The above scenario was presented in 1981 by Herbert [2], which appears to have been a strong motivation for the formulation of the no-cloning theorem [3]-[9].[2]

---

[1] From Prob. 6(b) of [1].

[2] To me, the statement of the no-cloning theorem in 1982 marks the end of a somewhat nonproductive era in which numerous people used variants on the Einstein-Podolsky-Rosen argument [10] to look for defects

Note: You may not be able to reproduce Herbert's logic that led to his claim that faster-than-light communication is possible, as he never wrote down the form of his quantum state including clones of bit B. He desired that all the clones of bit B be entangled with a single bit A.[3]

Consider the option that Bob makes a "copy" of bit B via a Controlled-NOT gate whose second input line, bit C, is initially $|0\rangle$.[4] The resulting entangled state of bits A, B and C is as good a copy of state (1) as possible. Show, however, that measurements by Bob of bit B in the [0,1] basis and of bit C in the $[+,-]$ basis, as proposed by Herbert [2], do not add Bob's knowledge of bit A.[5]

2 Solution

Using the relations,

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \qquad |1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}} \tag{2}$$

the entangled state (1) can be rewritten in various ways:

$$\begin{aligned}
|\psi\rangle &= \frac{|0\rangle_{\rm A}|0\rangle_{\rm B}}{\sqrt{2}} + \frac{|1\rangle_{\rm A}|1\rangle_{\rm B}}{\sqrt{2}} && (3)\\
&= \frac{(|0\rangle_{\rm A} + |1\rangle_{\rm A})(|0\rangle_{\rm B} + |1\rangle_{\rm B})}{2\sqrt{2}} + \frac{(|0\rangle_{\rm A} - |1\rangle_{\rm A})(|0\rangle_{\rm B} - |1\rangle_{\rm B})}{2\sqrt{2}} \\
&= \frac{|+\rangle_{\rm A}|+\rangle_{\rm B}}{\sqrt{2}} + \frac{|-\rangle_{\rm A}|-\rangle_{\rm B}}{\sqrt{2}} && (4)\\
&= \frac{|0\rangle_{\rm A}|+\rangle_{\rm B}}{2} + \frac{|0\rangle_{\rm A}|-\rangle_{\rm B}}{2} + \frac{|1\rangle_{\rm A}|+\rangle_{\rm B}}{2} - \frac{|1\rangle_{\rm A}|-\rangle_{\rm B}}{2} && (5)\\
&= \frac{|+\rangle_{\rm A}|0\rangle_{\rm B}}{2} + \frac{|+\rangle_{\rm A}|1\rangle_{\rm B}}{2} + \frac{|-\rangle_{\rm A}|0\rangle_{\rm B}}{2} - \frac{|-\rangle_{\rm A}|1\rangle_{\rm B}}{2}\,. && (6)
\end{aligned}$$

Thus, state $|\psi\rangle$ has the same type of entangled structure in both the $[|0\rangle, |1\rangle]$ and the $[|+\rangle, |-\rangle]$ bases, but if different bases are used to describe bits A and B the form of the state is more complicated.

---

in quantum mechanics. A popular hope was that there might exist "hidden variables" that more completely characterized a quantum state than a description such as $|\psi\rangle = \psi_0|0\rangle + \psi_1|1\rangle$. But if a more complete characterization existed, we might expect that cloning of an arbitrary quantum state would be possible. Hence, to me, the no-cloning theorem is a simple yet strong indication (much simpler than the convoluted arguments related to Bell's inequalities [11]) that the search for hidden variables is misguided. After 1982 there has been a much healthier emphasis on uses of entanglement to explore the greater richness of quantum compared to classical phenomena.

[3] It is, of course, possible to prepare numerous copies of the entire state (1), each with its own set of bits A and B. There would be no correlations between these various copies, and measurements of the various copies of bits A and B would simply build up the probability distributions underlying the measurement of just one of these copies.

[4] See, for example, Prob. 6(a) of [1].

[5] For a historical survey of debates about faster-than-light effects in quantum theory, and a somewhat simpler paradox than Herbert's, see http://kirkmcd.princeton.edu/examples/epr/epr_colloq_81.pdf
See also [9].

When a measurement is made of one of the bits in the [0,1] basis, the appropriate measurement operator is,

$$\mathsf{M}_{[0,1]} = 0 \cdot |0\rangle\langle 0| + 1 \cdot |1\rangle\langle 1|, \tag{7}$$

while when a measurement is made of one of the bits in the $[+,-]$ basis, the appropriate measurement operator is,

$$\mathsf{M}_{[+,-]} = + \cdot |+\rangle\langle +| + - \cdot |-\rangle\langle -|, \tag{8}$$

If, as appears to be the case for quantum mechanics, Alice and Bob can make only a single measurement on bits A and B, respectively, per each physical example of state $|\psi\rangle$, the results of (a repeated set of) such measurements are,

1. Bob chooses to measure in the $[|0\rangle, |1\rangle]$ basis.

   (a) Alice chooses to measure in the $[|0\rangle, |1\rangle]$ basis.
   We use eq. (3) to describe the state $|\psi\rangle$, and the appropriate measurement operator is,

$$\begin{aligned}\mathsf{M}_{[0,1]_A}\mathsf{M}_{[0,1]_B} &= (0_A \cdot |0\rangle_A\langle 0|_A + 1_A \cdot |1\rangle_A\langle 1|_A) \otimes (0_B \cdot |0\rangle_B\langle 0|_B + 1_B \cdot |1\rangle_B\langle 1|_B) \\ &= 0_A 0_B \cdot |0\rangle_A\langle 0|_A|0\rangle_B\langle 0|_B + 0_A 1_B \cdot |0\rangle_A\langle 0|_A|1\rangle_B\langle 1|_B \\ &\quad +1_A 0_B \cdot |1\rangle_A\langle 1|_A|0\rangle_B\langle 0|_B + 1_A 1_B \cdot |1\rangle_A\langle 1|_A|1\rangle_B\langle 1|_B.\end{aligned} \tag{9}$$

   Formally, the measurement yields

$$\mathsf{M}_{[0,1]_A}\mathsf{M}_{[0,1]_B}\frac{|0\rangle\mathrm{A}|0\rangle_\mathrm{B} + |1\rangle_\mathrm{A}|1\rangle_\mathrm{B}}{\sqrt{2}} = \frac{0_A 0_B}{\sqrt{2}} \cdot |0\rangle_A|0\rangle_B + \frac{1_A 1_B}{\sqrt{2}} \cdot |1\rangle_A|1\rangle_B. \tag{10}$$

   This means that,

   i. Alice observes bit A to be in the $|0\rangle$ state (with 50% probability).
   Then, Bob observes bit B to be in the $|0\rangle$ state (with 50% probability).

   ii. Alice observes bit A to be in the $|1\rangle$ state (with 50% probability).
   Then, Bob observes bit B to be in the $|1\rangle$ state (with 50% probability).

   Thus, Bob observes bit B to be $|0\rangle$ or $|1\rangle$ with 50% probability each, which is the same result that he would obtain if no measurement of bit A were made by Alice.

   (b) Alice chooses to measure in the $[|+\rangle, |-\rangle]$ basis.
   We use eq. (6) to describe the state $|\psi\rangle$, and the appropriate measurement operator is,

$$\begin{aligned}\mathsf{M}_{[+,-]_A}\mathsf{M}_{[0,1]_B} &= (+_A \cdot |+\rangle_A\langle +|_A + -_A \cdot |-\rangle_A\langle -|_A) \otimes (0_B \cdot |0\rangle_B\langle 0|_B + 1_B \cdot |1\rangle_B\langle 1|_B) \\ &= +_A 0_B \cdot |+\rangle_A\langle +|_A|0\rangle_B\langle 0|_B + +_A 1_B \cdot |+\rangle_A\langle +|_A|1\rangle_B\langle 1|_B \\ &\quad + -_A\, 0_B \cdot |-\rangle_A\langle -|_A|0\rangle_B\langle 0|_B + -_A 1_B \cdot |-\rangle_A\langle -|_A|1\rangle_B\langle 1|_B.\end{aligned} \tag{11}$$

   Formally, the measurement yields,

$$\begin{aligned}&\mathsf{M}_{[+,-]_A}\mathsf{M}_{[0,1]_B}\frac{|+\rangle_\mathrm{A}|0\rangle_\mathrm{B} + |+\rangle_\mathrm{A}|1\rangle_\mathrm{B} + |-\rangle_\mathrm{A}|0\rangle_\mathrm{B} - |-\rangle_\mathrm{A}|1\rangle_\mathrm{B}}{2} \\ &\quad = \frac{+_A 0_B}{2} \cdot |+\rangle_A|0\rangle_B + \frac{+_A 1_B}{2} \cdot |+\rangle_A|1\rangle_B \\ &\qquad + \frac{-_A 0_B}{2} \cdot |-\rangle_A|0\rangle_B + \frac{-_A 1_B}{2} \cdot |-\rangle_A|1\rangle_B.\end{aligned} \tag{12}$$

This means that,

i. Alice observes bit A to be in the $|+\rangle$ state (with 50% probability).
Then, Bob observes bit B to be in the $|0\rangle$ state (with 25% probability), or in the $|-\rangle$ state with (with 25% probability).

ii. Alice observes bit A to be in the $|-\rangle$ state (with 50% probability).
Then, Bob observes bit B to be in the $|0\rangle$ state (with 25% probability), or in the $|-\rangle$ state (with 25% probability).

Again, Bob observes bit B to be $|0\rangle$ or $|1\rangle$ with 50% probability each, which is the same result that he would obtain if no measurement of bit A were made by Alice.

Indeed, the results of Bob's measurements of bit B in the [0,1] basis (in the absence of knowledge of Alice's actions) are the same whether Alice measures bit A in the [0,1] basis, or in the $[+,-]$ basis, or if Alice makes no measurement at all.

2. Bob chooses to measure in the $[|+\rangle, |-\rangle]$ basis.

   (a) Alice chooses to measure in the $[|0\rangle, |1\rangle]$ basis.

   i. Alice observes bit A to be in the $|0\rangle$ state (with 50% probability).
   Then, Bob observes bit B to be in the $|+\rangle$ state (with 25% probability), or in the $|-\rangle$ state with (with 25% probability).

   ii. Alice observes bit A to be in the $|1\rangle$ state (with 50% probability).
   Then, Bob observes bit B to be in the $|+\rangle$ state (with 25% probability), or in the $|-\rangle$ state (with 25% probability).

   (b) Alice chooses to measure in the $[|+\rangle, |-\rangle]$ basis.

   i. Alice observes bit A to be in the $|+\rangle$ state (with 50% probability).
   Then, Bob observes bit B to be in the $|+\rangle$ state (with 50% probability).

   ii. Alice observes bit A to be in the $|-\rangle$ state (with 50% probability).
   Then, Bob observes bit B to be in the $|-\rangle$ state (with 50% probability).

By himself, Bob observes bit B to be $|0\rangle$ or $|1\rangle$ with equal probability if he measures in the $[|0\rangle, |1\rangle]$ basis, or that bit B is $|+\rangle$ or $|-\rangle$ with equal probability if he measures in the $[|+\rangle, |-\rangle]$ basis. This gives him no clue as to what Alice has done; he doesn't know whether she made measurements in the $[|0\rangle, |1\rangle]$ basis or in the $[|+\rangle, |-\rangle]$ basis, or whether she made any measurements at all.

In my view, Bob has learned nothing at all about bit A from his measurements of bit B.[6] There is no "signal" from one part of an entangled state to the other.

[6] However, starting with Einstein [10], another kind of comment has been made. Namely, that if Bob measures bit B to be, say $|0\rangle$, then he can "predict with certainty" that IF Alice measured bit A in the $[|0\rangle, |1\rangle]$ basis, then she would find bit A to be $|0\rangle$ also. Similarly, Bob can "predict with certainty" that if he measures bit B to be $|+\rangle$, then IF Alice measured bit A in the $[|+\rangle, |-\rangle]$ basis she would find bit A to be $|+\rangle$ also. Such conditional predictions are obviously unsatisfactory because they do not contain useful knowledge about bit A. Nonetheless, in a very loose usage of words they imply "certain knowledge" simultaneously about spacelike-separated quantum states in two different bases, which led Einstein to remark that they implied some kind of "spooky" action at a distance, which in turn suggested to him that quantum theory was somehow "incomplete". I subscribe to the camp of Bohr [12] that this logic does not warrant such conclusions.

Suppose, however, that Bob could make lots of copies of bit B, each having the entanglement with bit A given in eq. (3)-(6). Then he could measure half of the copies in the basis $[|0\rangle, |1\rangle]$ and the other half in the basis $[|+\rangle, |-\rangle]$. If he observes the various copies of bit B to be $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$ with equal probability, he can conclude with good assurance that Alice made no measurement of bit A. But, if he found no copies of bit B to be one of those four states (*e.g.*, no $|+\rangle$), while half of the copies to be its basis partner (*e.g.*, 50% $|-\rangle$), then he could conclude that Alice had made a measurement in that basis (*e.g.*, $[|+\rangle, |-\rangle]$), and that her result was that bit A is the same state as he found 50% of the time (*e.g.*, $|-\rangle$). He could interpret these results as a signal from Alice as to her choice of basis and of her result of a measurement, despite their measurements being spacelike-separated. This would imply faster-than-light communication!

So it is happily consistent with our trust in the theory of relativity that the needed cloning of the entangled state (1) cannot be done.[7]

Suppose Bob makes a "copy" of bit B using a Controlled-NOT gate with its second input, bit C, initially set to $|0\rangle$. He then measures bit B in the [0,1] basis and bit C in the $[+,-]$ basis. The 3-bit state $|\psi\rangle$ after the "copy" is made, but before the measurement, is,

$$|\psi\rangle = \frac{|0\rangle_{\rm A}|0\rangle_{\rm B}|0\rangle_{\rm C}}{\sqrt{2}} + \frac{|1\rangle_{\rm A}|1\rangle_{\rm B}|1\rangle_{\rm C}}{\sqrt{2}} \tag{13}$$

$$= \frac{|0\rangle_{\rm A}|0\rangle_{\rm B}|+\rangle_{\rm C}}{2} + \frac{|0\rangle_{\rm A}|0\rangle_{\rm B}|-\rangle_{\rm C}}{2} + \frac{|1\rangle_{\rm A}|1\rangle_{\rm B}|+\rangle_{\rm C}}{2} - \frac{|1\rangle_{\rm A}|1\rangle_{\rm B}|-\rangle_{\rm C}}{2} \tag{14}$$

$$\begin{aligned} = {} & \frac{|+\rangle_{\rm A}|0\rangle_{\rm B}|+\rangle_{\rm C}}{2\sqrt{2}} + \frac{|-\rangle_{\rm A}|0\rangle_{\rm B}|+\rangle_{\rm C}}{2\sqrt{2}} + \frac{|+\rangle_{\rm A}|0\rangle_{\rm B}|-\rangle_{\rm C}}{2\sqrt{2}} + \frac{|-\rangle_{\rm A}|0\rangle_{\rm B}|-\rangle_{\rm C}}{2\sqrt{2}} \\ & + \frac{|+\rangle_{\rm A}|1\rangle_{\rm B}|+\rangle_{\rm C}}{2\sqrt{2}} - \frac{|-\rangle_{\rm A}|1\rangle_{\rm B}|+\rangle_{\rm C}}{2\sqrt{2}} - \frac{|+\rangle_{\rm A}|1\rangle_{\rm B}|-\rangle_{\rm C}}{2\sqrt{2}} + \frac{|-\rangle_{\rm A}|1\rangle_{\rm B}|-\rangle_{\rm C}}{2\sqrt{2}} . \end{aligned} \tag{15}$$

If Alice makes no measurement of bit A, we read off from eq. (14) that Bob will find bits B and C in the four combinations $0_{\rm B}+_{\rm C}$, $0_{\rm B}-_{\rm C}$, $1_{\rm B}+_{\rm C}$, and $1_{\rm B}-_{\rm C}$ each with 25% probability.

Similarly, if Alice measures bit A in the [0,1] basis, she finds bit A to be 0 or 1 each with 50% probability, but Bob's measurements of bits B and C (in the absence of knowledge as to Alice's results) again yield the four combinations $0_{\rm B}+_{\rm C}$, $0_{\rm B}-_{\rm C}$, $1_{\rm B}+_{\rm C}$, and $1_{\rm B}-_{\rm C}$ each with 25% probability.

And if Alice measures bit A in the $[+,-]$ basis, she finds bit A to be $+$ or $-$ each with 50% probability, but Bob's measurements of bits B and C (in the absence of knowledge as to Alice's results) again yield the four combinations $0_{\rm B}+_{\rm C}$, $0_{\rm B}-_{\rm C}$, $1_{\rm B}+_{\rm C}$, and $1_{\rm B}-_{\rm C}$ each with 25% probability.

It appears that Bob has not increased his knowledge about bit A by making the Controlled-NOT "copy" of bit B.

One might argue that the state (13) actually includes in bit C as good a copy of bit B as possible (even if we had never heard of the no-cloning theorem). But, proper re-expression

[7] We don't need the full no-cloning theorem to conclude that we cannot make an "exact" copy of bit B if it is entangled with bit A but we have no knowledge of bit A. An exact copy of part of a system could only be made without knowledge of the rest of the system if that system could be described as a direct product of the part with the rest of the system ($|\text{system}\rangle = |\text{part}\rangle|\text{rest}\rangle$). Hence, there can be no exact copying of part of an entangled system.

of this state in the appropriate bases for measurements by Bob (and Alice) shows that the observations claimed on the top of the previous page could never occur.

References

[1] K.T. McDonald, *Ph410: Physics of Quantum Computation* (2004),
http://kirkmcd.princeton.edu/examples/ph410problems.pdf

[2] N. Herbert, *FLASH — A Superluminal Communicator Based Upon a New Kind of Quantum Measurement*, NSF-81-2003 (Jan. 1981),
http://kirkmcd.princeton.edu/examples/QM/herbert_nsf-81-2003.pdf
Found. Phys. **12**, 1171 (1982),
http://kirkmcd.princeton.edu/examples/QM/herbert_fp_12_1171_82.pdf

[3] W.K. Wootters and W.H. Zurek, *A single quantum cannot be cloned*, Nature **299**, 802 (1982), http://kirkmcd.princeton.edu/examples/QM/wootters_nature_299_802_82.pdf
It is claimed in [7] that the title was suggested by John Wheeler.

[4] D. Dieks, *Communication by EPR Devices*, Physics Letters **92A**, 271 (1982),
http://kirkmcd.princeton.edu/examples/QM/dieks_pl_a92_271_82.pdf

[5] P.W. Milonni and M.L. Hardies, *Photons Cannot Always Be Replicated*, Physics Letters **92A**, 321 (1982), http://kirkmcd.princeton.edu/examples/QM/milonni_pl_a92_321_82.pdf

[6] The essence of the no-cloning theorem had been demonstrated earlier, but was little noticed; J.L. Park, *The Concept of Transition in Quantum Mechanics*, Found. Phys. **1**, 23 (1970), http://kirkmcd.princeton.edu/examples/QM/park_fp_1_23_70.pdf

[7] A. Peres, *How the no-cloning theorem got its name*, Fort. Phys. **51**, 458 (2003),
http://kirkmcd.princeton.edu/examples/QM/peres_fp_51_458_03.pdf

[8] A quick "proof" of the no-cloning theorem is that if a quantum state, with two properties like position and momentum which obey the uncertainty principle, could be cloned, then the position could be measured precisely via one clone and the momentum measured precisely via the other, in contradiction to the uncertainty principle. See, for example, p. 229 of L. Susskind, *The Black Hole War* (Little, Brown, 2008),
http://kirkmcd.princeton.edu/examples/GR/susskind_bhw.pdf

[9] G.C. Ghirardi, *Entanglement, Nonlocality, Superluminal Signaling and Cloning*, (May 17, 2013), https://arxiv.org/abs/1305.2305
Ghirardi claimed he was the first to "prove" the no-cloning theorem, citing a letter on p. 29. But, see comments on this in [7].

[10] A. Einstein, B. Podolsky and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* Phys. Rev. **47**, 777 (1935),
http://kirkmcd.princeton.edu/examples/QM/einstein_pr_47_777_35.pdf

[11] J.S. Bell, *On the Einstein Podolsky Rosen Paradox*, Physics **1**, 195 (1964),
http://kirkmcd.princeton.edu/examples/QM/bell_physics_1_195_64.pdf

[12] N. Bohr, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* Phys. Rev. **48**, 696 (1935),
http://kirkmcd.princeton.edu/examples/QM/einstein_pr_48_696_35.pdf