



PERGAMON

Chaos, Solitons and Fractals 13 (2002) 39–41

CHAOS
SOLITONS & FRACTALS

www.elsevier.com/locate/chaos

Entanglement-based communications

Michail Zak

Jet Propulsion Laboratory, Center for Space Microelectronics Technology, California Institute of Technology, Pasadena, CA 91109, USA

Accepted 11 October 2000

Abstract

Based upon quantum entanglement, a simple algorithm for the instantaneous transmission of messages (chosen at random) to remote distances is proposed. A special class of situations when such transmissions are useful is outlined. © 2001 Elsevier Science Ltd. All rights reserved.

1. Introduction

Quantum nonlocality arising from entangled states is the most fundamental and the most mysterious phenomenon in quantum mechanics, and it is in the core of quantum information theory. Formally quantum nonlocality follows from the Schrödinger equation; however, its physical meaning is still unclear despite successful experimental confirmation [1], and applications to teleportation, cryptography and computing [2].

The most attractive aspect of quantum nonlocality is associated with instantaneous transmissions of messages. However, practical applications of this effect are restricted by the postulate adopted by many authors [3] that these messages cannot deliver any information. That is why all the quantum teleportation algorithms must include an additional (classical) channel [2].

Returning to this postulate, I would like to emphasize that it is implied that the messages cannot deliver any Shannon information. But are there, maybe, some other measures whose delivery is possible and useful? In this connection, it should be recalled that Shannon information is associated with the degree of unpredictability of the underlying event, and in the physical world that means equal probability for each outcome. However, the situation becomes more sophisticated in biological or social worlds, when the underlying system may try to hide its identity by intentionally misleading an observer [4]. Then such properties as secrecy or deception, which are the attributes of the social rather than the physical world, can represent additional measures of the usefulness of the transmitted message. In terms of unpredictability, deception can be associated with disinformation, which makes prediction even harder than in the case of maximum Shannon entropy.

2. Entanglement-based coordination

In order to illustrate my point, suppose that a sender possesses N different messages, which he can choose only at random with equal probability, and assume that any of these messages allows each receiver to achieve his goal as long as the secrecy of the message is preserved. (For instance, if a military attack can be conducted in many different ways, the most important is the secrecy of the selected strategy.) Then from

the viewpoint of Shannon information, the transmission of such a message is useless. However, if one is asked what the chance is that the message can be decoded by a wild guess, the answer will be: $1/N$. This means that the number of equally acceptable (but randomly chosen) messages is proportional to the degree of secrecy of the transmission, and that this represents the value of this transmission. Actually, the sender coordinates and synchronizes the actions of the receivers (regardless of the origin of the message itself) and preserves the secrecy of the communications by making the choice of his message random. It should be emphasized again that the whole procedure makes sense only under the condition that a receiver can use any of these messages to achieve the same objective, but nobody else must know what message has been received.

The communication paradigm described above can be implemented by a simple quantum algorithm. Let us assume that Alice (the sender) and Bob (the receiver) each possesses a set of n particles which are in a one-to-one correspondence such that each pair is entangled; and suppose that they perform a sequence of measurements: one particle per unit time-step. Each measurement performed by Alice has two equally probable outcomes. In case of electrons, these outcomes can be spin-up (+) or spin-down (-). If (+) and (-) are associated with the movements of a point along an axis to the right or to the left, respectively, the sequence of Alice's measurements can be interpreted as a symmetric random walk. Hence, by performing these measurements, Alice selected (randomly) one trajectory out of 2^n equally probable trajectories of the corresponding random walk. Due to entanglement, Bob instantaneously receives this trajectory (after performing the same type of measurements). Actually Bob's trajectory may look different, but it will be uniquely correlated with Alice's trajectory.

Thus, what has been transmitted? Even prior to the measurements, both Alice and Bob knew that there were 2^n possible trajectories; moreover, they knew how each trajectory could appear. But what they did not know was which one of the 2^n trajectories would be selected; in other words, they did not know the number of the transmitted trajectory if all the trajectories were numbered as $1, 2, 3, \dots, 2^n$. However, does this number represent new information? Obviously not, since this number has been chosen randomly. Hence, so far, no Shannon or any other measure of information has been transmitted.

Let us consider a special situation when Bob has a certain objective which can be achieved by any of the commands (trajectories) equally well, but under the condition that nobody else will know about the selected trajectory. Now we move to the world where such measures as degree of secrecy or deception may be more important than Shannon information. Indeed, the fact that the command has been chosen randomly becomes useful: it hides this command among $(2^n - 1)$ others. At the same time, the fact that the transmitted Shannon information is zero becomes irrelevant since each command is equally effective anyway.

So what has been transmitted now? The answer is: the degree of deception. Indeed, the probability that the selected trajectory can be decoded by a wild guess is 2^{-n} , i.e., vanishingly small for $n \gg 1$.

It should be noticed that the command is transmitted instantaneously regardless of the distance between Alice and Bob, and the number of receivers like Bob can be arbitrarily large as long as each receiver has a set of n particles entangled pairwise with the corresponding particles of the sender. At the same time, the secrecy of the command is preserved by the fact that the knowledge about the selected trajectory is acquired at the moment of measurement, and therefore, only the sender and the receivers possess the secret command.

3. Example

Consider a set of remote objects which communicate (classically) using a certain frequency. For security reasons, this frequency is supposed to be changed after certain time intervals. The best implementation of such changes is via entanglement-based particles. Indeed, in this case, a new frequency is chosen randomly, and it is instantaneously transmitted to all the objects. Since the knowledge about this frequency is acquired at the very moment of measurement, it is theoretically impossible for an outsider to intercept the message. Any classical imitation of this paradigm is less secure since the 'random' frequency must be assigned BEFORE the separation of the objects.

4. Discussion and conclusions

The first reaction to the proposed paradigm is to compare it with its classical implementation. Indeed, suppose there is a machine which picks one of two cards at random, rips it in half, puts each half in a separate envelope, seals the envelopes and sends it to sender A and receiver B simultaneously. Formally the effect will be the same as if A and B possess entangled particles. Indeed, in both cases, the Shannon information is transmitted from the 'external world' and shared between A and B. However, in the classical case, this transmission takes place BEFORE their separation, and it does not represent communication at a distance since there is no distance yet; actually the answer exists BEFORE the separation of A and B and that makes it less secure. The difference between the quantum and the classical cases is similar to those between real-time and pre-recorded TV programs: in the first case, the future is unpredictable, while in the second case the 'future' is fully deterministic. Hence, this paper touches several new physical and philosophical problems (such as the difference between real-time and pre-recorded samples of stochastic processes, between objective and subjective knowledge, etc.).

Thus, a simple quantum algorithm for the instantaneous transmission of randomly chosen messages to remote distances is proposed. The novelty of the algorithm is in re-interpretation of the measure of usefulness of a message. Based upon the Shannon information, transmission of randomly chosen commands is useless. However, I have introduced a special class of situations when such transmission makes sense. These situations must satisfy the following conditions: each of the randomly chosen commands is equally useful for the receiver to achieve his objective, and the transmitted command must be kept secret until its execution. Both of these conditions are usually satisfied in the military world when the deception effect of the chosen strategy is more important than the strategy itself.

One should notice that the new measure of the usefulness of a message is based on attributes of the social world such as deception, secrecy and decoding, in contradistinction to Shannon information, which is based upon the attributes of the physical world (such as entropy). It should be made clear, however, that the proposed algorithm does not violate the postulate about the impossibility of transmitting the (Shannon) information.

Acknowledgements

The research described in this paper was performed by the Jet Propulsion Laboratory, California Institute of Technology, and was sponsored by the National Aeronautics and Space Administration. The author thanks Dr. Laurence I. Gould, Dr. Jacob Barhen, Dr. Ronald E. Meyers and Dr. V. Lefebvre for fruitful discussions.

References

- [1] Bouwmeester D, Pan JW, Mattle K. *Nature* 1997;390(December 11):575–9.
- [2] Williams C, Clearwater S. *Explorations in quantum computing*. Berlin: Springer; 1997.
- [3] Mittelstaedt P. *Ann Phys Leipzig* 1998;7(7–8):710–5.
- [4] Zak M. *Chaos, Solitons & Fractals* 1999;10(10):1583–620.