PHYSICAL REVIEW A **77**, 052310 (2008)

Quantum advantages in classically defined tasks

N. Aharon and L. Vaidman
School of Physics and Astronomy, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel-Aviv University, Tel-Aviv 69978, Israel
(Received 9 October 2007; published 8 May 2008)

We analyze classically defined games for which a quantum team has an advantage over any classical team. The quantum team has a clear advantage in games in which the players of each team are separated in space and the quantum team can use unusually strong correlations of the Einstein-Podolsky-Rosen type. We present an example of a classically defined game played at *one* location for which quantum players have a real advantage.

DOI: 10.1103/PhysRevA.77.052310 PACS number(s): 03.67.−a, 03.65.Ta, 03.65.Ud, 02.50.Le

Quantum-information research shows how quantum devices can outperform devices working on the basis of classical physics for certain communication and computational tasks. One of the clear ways to compare between the strength of quantum and classical methods is to consider the advantages of a quantum team playing games against a classical team. Many papers give the impression that for nearly all games "quantum strategies" are advantageous compared to classical strategies [1–8]. Van Enk and Pike [9,10], however, have pointed out that quantized classical games differ as games from their original classical counterparts, and that in many cases quantum players cannot win against classical players as long as the rules of the game are unchanged. We find that in these games it is also important to analyze the role of decoherence resulting from actions of classical players. This decoherence frequently eliminates the advantage of quantum players.

Quantum objects and strategies can be useful in many contexts. In quantum-cryptography applications, quantum devices can replace the third trusted party needed for some games (e.g., quantum gambling [11]). In numerous cases where constraints on resources are involved, a quantum team with N qubits is much more efficient than a classical team with N bits [12,13], although it is not really a fair comparison. This raises the question: In which games, under *equal* natural conditions, does a quantum team win against a classical team?

We can define a particular game as a competition for factoring large numbers. A quantum player using Shor's algorithm [14] should win against a classical player by performing this task faster. However, it is not clear when a quantum computer that outperforms a classical computer will be built and, moreover, we do not have proof that a classical efficient algorithm does not exist.

It is even less clear that a quantum team can win in a competition on the minimum time for finding the answer to the Deutsh-Jozsa problem [15], as Meyer suggests [16]. In this game a black box is given which calculates a function for various inputs. Even if we assume unlimited technological power of the quantum team outside the black box, we cannot be sure that inside the box the coherence needed for quantum computation is preserved. We can imagine a quantum box which preserves coherence and which can also serve as a classical box for each possible input, but it is not a particularly interesting observation that a classical team cannot operate quantum devices efficiently. The question raised in this regard is whether a quantum team outperforms a classical team in classically defined tasks.

There is a well-known class of games in which a quantum team with good quantum devices can unambiguously outperform any classical team. We call them Einstein-Podolsky-Rosen (EPR) games, since the advantage of the quantum team is based on the use of entangled systems exhibiting EPR correlations, which are stronger than any possible classical correlations. Other names associated with these games are pseudotelepathy [17,18] and Bell games [19].

In EPR-type games each team has two or more players at separate locations. There is a known set of questions the players can receive, a known set of possible answers, and a payoff table for these answers. The players are not allowed to communicate once the game begins (so they do not know which questions the other team members were asked) but they are allowed to communicate beforehand and share any physical devices that might help them. The way to enforce the rule that these devices must not allow the players to communicate during the game is to have the players make their moves before light signals signifying the other players being given their questions can arrive. There are many examples of EPR games [20–23]. Conceptually, the simplest and clearest EPR game is the one based on the Greenberger-Horne-Zeilinger proof of nonlocality [24–26]. Note also games based on the Zeno-type proof of Bell inequalities [27,28].

Using a key distribution protocol [29], one can construct a (rather artificial) game with players at two separate locations in which teams equipped with quantum devices can have an advantage even without entanglement. The task is to transmit a message from one laboratory to another through an optical fiber. One team has players at two laboratories, while the second team has access to the fiber. The second team gains points for correct guesses of the transmitted messages. The first team gains points when it correctly catches the eavesdropping attempts, but loses points if it announces eavesdropping when the opponent has not touched the fiber. Teams with quantum technology will have an advantage when the allowed prior shared information is less than one time pad, but enough to run the quantum protocol [29].

The question we want to analyze here is the following: Are there games played at *one* location for which quantum players have an advantage? An important candidate for such a game is Meyer's coin flipping problem [3]. A coin is placed heads up. Alice, in her first move, can either flip or not flip the coin. Bob, in his subsequent move, can also either flip or not flip the coin, but he is not allowed to see the state of the coin. Alice gets another turn in which she can again either flip or not flip the coin without looking at its state. She wins if the final state of the coin is heads up.

Classically, each player has maximally a 50% chance of winning. Meyer claims that, using quantum mechanics, Alice can reach a 100% chance of winning. Meyer's proposal is that Alice, in her first move, should put the coin in the superposition

$$\frac{1}{\sqrt{2}}(|\text{head}\rangle + |\text{tail}\rangle). \tag{1}$$

Then, whatever Bob does, either flip or not flip, the state of the coin remains unchanged, and Alice in her last move can rotate the (quantum) state back to $|\text{head}\rangle$.

Van Enk [9] analyzed a particular realization of Meyer's proposal in which the sides of the coin were represented as photon polarization states and showed that quantum rotation to the superposition (1) is actually a classical rotation of the polarization that Alice, even without quantum capabilities, can perform. So, van Enk concluded that even classically Alice can reach a 100% chance of winning.

Discussing Meyer's proposal requires specifying its actual realization. Van Enk mentioned that, when we consider an actual coin, the classical analog of Alice's quantum action is putting the coin on its edge, which also yields a 100% chance of winning. However, this is clearly a different game because the set of allowed moves is enlarged. Note that a coin standing on its edge is not described by the state (1).

In Meyers's game with a real coin and original rules, neither the classical nor the quantum Alice can really always win. Indeed, even if Alice, equipped with unlimited quantum technology, is capable of creating the state (1), classical Bob will not leave it unchanged after his turn. He is not supposed to perform a careful, precise quantum experiment. Clearly, when Bob takes the coin in his hand, its quantum state will decohere and Alice will not be able to rotate it back to the state $|\text{head}\rangle$.

Formally, Meyer's idea, in which a quantum player puts the system in a state that moves of the classical player do not change, provides an advantage for the quantum player. However, we are not aware of any natural implementation of it as a real game in which a quantum team, even with unlimited technological power, will have an advantage over a classical team. The game involves a classical player, and he invariably causes decoherence of the quantum state, thereby eliminating the advantage of the quantum player.

We claim that there is at least one game, played at one location, in which quantum players can get better results than classical players. This is the game based on the *three-box paradox* [30]. Contrary to EPR games which do not involve quantum objects, but where the quantum player uses a quantum device to get the right advice for a classical move, in this game, as in Meyer's game, the object we play with is itself quantum. And, as in Meyer's game, Bob does not see that the object he is playing with is a quantum one. The difference is that, according to our game's rules, Bob's actions do not cause the decoherence which ultimately spoils Alice's quantum moves.

Our game is a three-stage game in which each player makes his moves privately. Alice begins the game by preparing a single particle that she places inside two boxes or any other place other than the two boxes. The particle can be prepared in any possible state chosen by Alice. Bob, who has no information about the chosen state of the system, can make one of two possible moves, either look for the particle in box A or look for the particle in box B. To avoid any possible cheating by Alice, Bob can occasionally, instead of his legitimate move, open two boxes to make sure that Alice does not use two particles. Alice is not allowed to see Bob's move, but there is a third trusted party which observes Bob's action and which can see if Bob finds the particle. Bob's objective is to leave no trace of his action, so he tries to leave the box exactly as it was before. He is not allowed to touch the box that he chooses not to open. Then Alice, in her turn, gets access to the boxes and can perform any measurement she wants. She then has the option of either canceling or accepting this trial of the game. She wins if Bob finds the particle. Alice's objective is to maximize the probability of the trials she does not cancel in which Bob finds the particle.

It is clear that if Alice can use only classical objects she cannot obtain more than a 50% chance of winning. It seems that placing the particle outside the two boxes can only reduce Bob's chances of finding the particle and consequently Alice's chances of winning. Placing the particle in one of the boxes A or B leads to a 50% chance of Bob finding the particle. Alice's last move seems useless; Bob's finding or not finding the particle does not change the system, so her allowed measurement cannot help. She gets no information about those cases when it is in her interest to cancel the game trial.

However, Alice equipped with quantum devices can reach a 100% chance of winning. She prepares the particle in a quantum state which is a superposition of being in three boxes A, B, and C. The boxes A and B are the ones Bob plays with. The third box she keeps for herself; Bob need not know about it. The state is

$$|\psi\rangle = \frac{1}{\sqrt{3}}(|A\rangle + |B\rangle + |C\rangle), \tag{2}$$

where the states $|A\rangle$, $|B\rangle$, and $|C\rangle$ denote the particle being in box A, B, and C, respectively.

Now, Bob opens either box A or box B. He has a chance of one-third to find the particle in the box. Let us assume he opens box A. (The game is symmetric with respect to the choices of A and B.) If Bob finds the particle in the box, its quantum state becomes

$$|\psi_{\text{find}}\rangle = |A\rangle. \tag{3}$$

If he does not find the particle in the box, its quantum state becomes

$$|\psi_{\text{not find}}\rangle = \frac{1}{\sqrt{2}}(|B\rangle + |C\rangle). \tag{4}$$

Since Bob is not allowed to touch the other box, i.e., box B, the final quantum state in this case is exactly (4). We assume that Alice's technological abilities are sufficient to build robust boxes which, if untouched, keep the quantum state of the particle inside them undisturbed. Bob's action with box A, even if he is not careful, will not cause a change in the state (4). Bob tries to leave no trace of his action, but if he finds the particle in A and he is not careful, he might disturb the quantum state (3).

Alice, in her turn, makes a projective measurement of the particle on the state

$$|\phi\rangle = \frac{1}{\sqrt{3}}(|A\rangle + |B\rangle - |C\rangle). \tag{5}$$

If she finds the state, she accepts the game trial, and if she does not, she cancels it.

Now we see that Alice cannot lose:

$$\langle \psi_{\text{not find}}|\phi\rangle = 0, \tag{6}$$

so the probability of Alice finding this particular state if Bob did not find the particle is zero. And this is not sensitive to Bob's action, provided he follows the rules. If Bob does find the particle and the final state is (3), we obtain

$$\langle \psi_{\text{find}}|\phi\rangle = \frac{1}{\sqrt{3}}. \tag{7}$$

Thus, Alice will accept the game with a probability of one-third. This probability becomes smaller if Bob is not careful and disturbs the state of the particle in box A. Alice declares "game on" only in the trials she wins, and never when she would lose.

We have shown that, apart from games played in separate locations, in which the EPR correlations give advantage to a quantum team, there are classically defined games in one location in which a classical player unaware of quantum mechanics should not suspect anything strange except for the unexplained fact that he loses. The essence of the quantum team's advantage here is that, whereas in classical physics during "an observation of a particle" either we find it or we do not, we do not change the state of the particle, in quantum mechanics "observation of a particle" does change its state, provided that the particle started in a superposition. (Compare this with Meyer's example in which the action always changes "classical" states, and does not change the superposition state.)

Note that it is possible to find EPR correlations in our system. Indeed, there is an entanglement between boxes. It is possible to devise local experiments at different boxes showing violation of Bell's inequality [31]. However, in our game we do not have a team of players each addressing a particular box, so this entanglement is not the source of the advantage of the quantum player. The locality aspect of our game, i.e., that the three boxes are not at the same place, is crucial for the issue of decoherence. Opening one box does not disturb the relative phase between parts of the quantum wave in other boxes.

One might gain an additional insight from viewing our game in the framework of the two-state vector approach [32]. The essence of the quantum advantage in this picture is that, while the state of a classical system at a particular time yields everything one can know about this system given a known environment, in quantum mechanics, future measurements might add information about the present of a quantum system even if everything about the past is known. This is why quantum Alice can benefit from her measurement after Bob's observation.

Although there are real experiments testing these quantum predictions [33], and there are demonstrations of other games [34], today's technology does not yet enable one to win games using quantum devices [28]. It seems, however, that we are not very far from this stage in technological development.

Finally, we hope that our analysis of transforming the three box paradox into a game in which a quantum team wins against any classical team will put an end to the controversy about the classical analogy of the three-box paradox [35–38]. In all proposed classical "analogies" of the three-box paradox, the intermediate measurement changes the state of the system, while an observation of a classical particle in a box does not.

We thank anonymous referees for helpful comments. This work has been supported in part by the European Commission under the integrated project Qubit Applications (QAP) funded by the IST directorate as Contract No. 015848 and by the Israel Science Foundation Grant No. 990/06.

[1] J. Eisert, M. Wilkens, and M. Lewenstein, Phys. Rev. Lett. **83**, 3077 (1999).
[2] S. C. Benjamin and P. M. Hayden, Phys. Rev. A **64**, 030301(R) (2001).
[3] D. A. Meyer, Phys. Rev. Lett. **82**, 1052 (1999).
[4] H. Li, J. F. Du, and S. Massar, Phys. Lett. A **306**, 73 (2002).
[5] C. F. Lee and N. F. Johnson, Phys. Rev. A **67**, 022311 (2003).
[6] A. P. Flitney and D. Abbott, Proc. R. Soc. London, Ser. A **459**, 2463 (2003).
[7] A. Iqbal and S. Weigert, J. Phys. A **37**, 5873 (2004).
[8] N. Patel, Nature (London) **445**, 144 (2007).
[9] S. J. van Enk, Phys. Rev. Lett. **84**, 789 (2000).
[10] S. J. van Enk and R. Pike, Phys. Rev. A **66**, 024306 (2002).
[11] L. Goldenberg, L. Vaidman, and S. Wiesner, Phys. Rev. Lett. **82**, 3356 (1999).
[12] E. F. Galvao and L. Hardy, Phys. Rev. Lett. **90**, 087902 (2003).
[13] L. Vaidman and Z. Mitrani, Phys. Rev. Lett. **92**, 217902 (2004).
[14] P. W. Shor, in *Proceedings of the 35th Symposium on Foundations of Computer Science, Santa Fe, 1994,* edited by S. Goldwasser (IEEE, Los Alamitos, CA, 1994), p. 124.
[15] D. Deutsch and R. Jozsa, Proc. R. Soc. London, Ser. A **439**, 553 (1992).

[16] D. A. Meyer, Phys. Rev. Lett. **84**, 790 (2000).
[17] G. Brassard, A. Broadbent, and A. Tapp, in *Proceedings of the Eighth International Workshop on Algorithms and Data Structures*, edited by F. Dehne, J. R. Sack, and M. C. Smid, Lecture Notes in Computer Science Vol. 2748 (Springer, New York, 2003), p. 1.
[18] A. Cabello, Phys. Rev. A **73**, 022302 (2006).
[19] B. Tsirelson (unpublished).
[20] D. P. DiVincenzo and A. Peres, Phys. Rev. A **55**, 4089 (1997).
[21] P. G. Kwiat and L. Hardy, Am. J. Phys. **68**, 33 (2000).
[22] A. Cabello, Phys. Rev. Lett. **86**, 1911 (2001).
[23] A. Steane and W. van Dam, Phys. Today **53** (2), 35 (2000).
[24] N. D. Mermin, Am. J. Phys. **58**, 731 (1990).
[25] L. Vaidman, Found. Phys. **29**, 615 (1999).
[26] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos (Springer, Berlin, 1988), p. 69.
[27] L. Hardy and W. van Dam, Phys. Rev. A **59**, 2635 (1999).
[28] L. Vaidman, Phys. Lett. A **286**, 241 (2001).
[29] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore* (IEEE, New York, 1984), p. 175.
[30] Y. Aharonov and L. Vaidman, J. Phys. A **24**, 2315 (1991).
[31] Y. Aharonov and L. Vaidman, Phys. Rev. A **61**, 052108 (2000).
[32] Y. Aharonov and L. Vaidman, Phys. Rev. A **41**, 11 (1990).
[33] K. J. Resch, J. S. Lundeen, and A. M. Steinberg, Phys. Lett. A **324**, 125 (2004).
[34] J. Du, H. Li, X. Xu, M. Shi, J. Wu, X. Zhou, and R. Han, Phys. Rev. Lett. **88**, 137902 (2002).
[35] K. A. Kirkpatrick, J. Phys. A **36**, 4891 (2003).
[36] M. S. Leifer and R. W. Spekkens, Phys. Rev. Lett. **95**, 200405 (2005).
[37] T. Ravon and L. Vaidman, J. Phys. A **40**, 2873 (2007).
[38] K. A. Kirkpatrick, J. Phys. A **40**, 2883 (2007).