Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science 251 (2009) 17–26
Electronic Notes in Theoretical Computer Science
www.elsevier.com/locate/entcs

Noise and the Mermin-GHZ Game

Ivan Fialík [1,2]

Faculty of Informatics
Masaryk University
Botanická 68a, 602 00 Brno, Czech Republic

Abstract

A pseudo-telepathy game is a game for two or more players for which there is no classical winning strategy, but there is a winning strategy based on sharing quantum entanglement by the players. Since it is generally very hard to perfectly implement a quantum winning strategy for a pseudo-telepathy game, quantum players are almost certain to make errors even though they use a winning strategy. After introducing a model for pseudo-telepathy games, we investigate the impact of several basic noisy quantum channels on the quantum winning strategy for the Mermin-GHZ game. The question of how strong the noise can be so that quantum players would still be better than classical ones is also dealt with.

Keywords: Pseudo-telepathy games, Mermin-GHZ game, noisy quantum channels, quantum winning strategy.

1 Introduction

Communication complexity is an area of classical computer science which studies how much communication is necessary to solve various distributed computational problems. Since according to Holevo's theorem [6] at most n classical bits can be transmitted between two unentangled parties using n quantum bits, it may seem that quantum communication protocols cannot be better than their classical counterparts. Nevertheless, in 1998 Buhrman, Cleve and Wigderson [3] showed that this intuition is wrong. They found a problem whose quantum communication complexity is exponentially better than classical communication complexity in the error-free model. One year later, Raz proposed a problem for which this exponential separation holds also in the bounded-error model [8]. However, the existence of a promise-free distributed problem demonstrating an exponential separation between quantum communication protocols and classical communication protocols is still an open problem.

[1] This work has been supported by the research projects MSM0021622419 and 201/07/0603.

[2] Email: xfialik@fi.muni.cz

doi:10.1016/j.entcs.2009.08.025

Since quantum entanglement provides us with strong non-local correlations that cannot be achieved in the classical world, one can ask whether it can be used even to solve some distributed problems without any form of direct communication between the parties. Of course, we are interested only in such problems for which this does not hold in the classical world. On one hand, the answer is negative if we consider the standard communication complexity model [9] in which the parties compute a value of some function on their inputs and the whole result of the computation must become known to at least one party. Otherwise, faster-than-light communication would be possible which would contradict the Relativity Theory. On the other hand, if each party has its own input, computes its own output and we are interested only in non-local correlations between the inputs and the outputs, then the answer is positive. Such problems are often described using a terminology of the game theory. Therefore, they are usually called pseudo-telepathy games.

Pseudo-telepathy games also offer an alternative way to show that the physical world is not local realistic, the result which is usually proved using some form of the Bell inequality [1]. The locality property means that no action performed at a location A can have an instantenous (faster than light) effect at a remote location B. The realism property means that every characteristic about the physical system that can be measured is already determined before the actual measurement. Therefore, we can say that it exists independently of the measurement. Unfortunately, the Bell inequality is not very easy to explain because it involves nontrivial probabilistic arguments. It would be very convenient if we could demonstrate an observable behaviour which is obviously impossible in the classical world. Pseudo-telepathy games are of interest because at least some of them are very simple and one can explain that there is no classical winning strategy for them in several minutes almost to anyone.

In order to be able to describe what a pseudo-telepathy game is, we explain at first what we mean by the term two party game. A *two party game* G is a sextuple

$$G = (X, Y, A, B, P, W)$$

where X, Y are *input sets*, A, B are *output sets*, P is a subset of $X \times Y$ known as a *promise* and $W \subseteq X \times Y \times A \times B$ is a relation among the input sets and the output sets which is called a *winning condition*. Before the game begins, the parties, usually called Alice and Bob, are allowed to discuss strategy and exchange any amount of classical information, including values of random variables. They may also share an unlimited amount of quantum entanglement. Afterwards, Alice and Bob are separated from each other and they are not allowed to communicate any more till the end of the game. In one *round of the game*, Alice is given an input $x \in X$ and she is required to produce an output $a \in A$. Similarly, Bob is given an input $y \in Y$ and he is required to produce an output $b \in B$. The pairs (x, y) and (a, b) are called a *question* and an *answer*, respectively. Alice and Bob *win the round* if either $(x, y) \notin P$ or $(x, y, a, b) \in W$. Alice and Bob *win the game* if they have won all the rounds of it. A *strategy* of Alice and Bob is *winning* if it always allows them to win.

We say that a two-party game is *pseudo-telepathic* if there is no classical winning strategy, but there is a winning strategy, provided Alice and Bob share quantum entanglement. The origin of this term can be explained in the following way. Suppose that scientists who know nothing about quantum computing witness Alice and Bob playing some pseudo-telepathy game. More precisely, suppose that the players are very far from each other, they are given their inputs at the same time and have to produce their outputs in time shorter than time required by light to trave1 between them. If Alice and Bob answer correctly in a sufficiently long sequence of rounds, the scientists will conclude that Alice and Bob can communicate somehow. But according to classical physics, communication between the players is impossible. Therefore, the scientists will be made believe that Alice and Bob are able to communicate in the way unknown to classical physics. One of possible explanations will be that the players are endowed with telepathic powers. A survey of pseudo-telepathy games can be found in [2]. The definition of these games can be easily generalized to more than two players.

A classical strategy s for a pseudo-telepathy game G is *deterministic* if there are functions $s_A : X \to A$ and $s_B : Y \to B$ such that for each question $(x, y) \in X \times Y$, the only possible answer of Alice and Bob is the pair $(s_A(x), s_B(y))$. The *success of a deterministic strategy* is defined as the proportion of questions from the promise P for which it produces a correct answer. Clearly, this number can by interpreted as the probability that the strategy succeeds on a given question which is chosen uniformly and randomly. We denote with $\omega_d(G)$ the maximal success of a deterministic strategy for the game G:

$$\omega_d(G) = \max_s \frac{\{(x, y) \in P \mid (x, y, s_A(x), s_B(y)) \in W\}}{|P|}.$$

Alice and Bob can also use a randomized strategy for G. Any randomized strategy can be seen as a probability distribution over a finite set of deterministic strategies. Therefore, if questions are chosen uniformly and randomly, the probability of winning a round of the game G using a randomized strategy cannot be greater than $\omega_d(G)$ [2].

The simplest nontrivial quantum strategies for G have the following form. Alice and Bob share some entangled state $|\varphi\rangle$. After they have been given their inputs $x \in X$ and $y \in Y$, the players apply on their parts of $|\varphi\rangle$ unitary transformations U_x and U_y, respectively. Finally, the players perform measurements M_x and M_y on their parts of $|\varphi\rangle$ which give them their outputs $a \in A$ and $b \in B$, respectively.

This paper examines the impact of quantum noise on the quantum winning strategy for the Mermin-GHZ game. A general definition of this problem is given in the next section. The Mermin-GHZ game and the quantum winning strategy as well as the best classical strategy for it are described in Section 3. The remaining sections are devoted to the study of how several basic noisy quantum channels influence the quantum winning strategy for the Mermin-GHZ game.

2 Pseudo-Telepathy in the Presence of Noise

An experimental implementation of a quantum winning strategy for a pseudo-telepathy game is generally very hard to be perfect. The players may perform imperfectly the unitary transformations required by the winning strategy or they may not be able to keep the required entangled quantum state. Moreover, their measurement devices may fail to give a correct outcome or may fail to give an outcome at all.

Regarding imperfections of the shared entangled state, the players are supposed to share a quantum state $E(|\varphi\rangle\langle\varphi|)$ where E is a superoperator which realizes some noisy quantum channel. The superoperator E can be written in Kraus representation as

$$E(|\varphi\rangle\langle\varphi|) = \sum_{i=1}^{n} E_i|\varphi\rangle\langle\varphi|E_i^\dagger$$

where $\sum_{i=1}^{n} E_i E_1^\dagger = I$. After they have applied their unitary transformations, the players obtain a state

$$\rho_E = (U_x \otimes U_y)E(|\varphi\rangle\langle\varphi|)(U_x^\dagger \otimes U_y^\dagger).$$

For a question (x, y), let $P_E(x, y)$ be a probability of the event that Alice and Bob obtain after measuring ρ_E a state corresponding to a correct answer to (x, y). Furthermore, let P_E be a probability of the event that Alice and Bob obtain after measuring ρ_E a state corresponding to a correct answer to a question which is chosen uniformly and randomly from P.

3 Mermin-GHZ Game

Alice, Bob and Charles have each one bit as an input with the promise that the parity of the input bits is 0 [5]. We denote the input bits x_1, x_2 and x_3. The task for each of the players is to produce one bit so that the parity of the output bits is equal to the disjunction of the input bits. Thus, if a_1, a_2 and a_3 are the outputs, then the equation $a_1 \oplus a_2 \oplus a_3 = x_1 \vee x_2 \vee x_3$ must hold.

In the quantum winning strategy for the Mermin-GHZ game Alice, Bob and Charles share the entangled state $|\varphi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. After the players have received their inputs x_1, x_2, x_3, respectively, each of them does the following:

(i) Applies to his or her register the unitary transformation U which is defined as

$$U(|0\rangle) = |0\rangle,$$

$$U(|1\rangle) = e^{\frac{\pi \imath x_i}{2}}|1\rangle.$$

(ii) Applies to his or her register the Hadamard transformation

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}.$$

(iii) Performs a measurement in the computational basis on his or her register. Outputs the bit a_i which he or she has measured.

Now we intend to show that there is no classical winning strategy for the Mermin-GHZ game. Since no classical randomized strategy can be better than the best classical deterministic one [2], it suffices to show that there is no classical deterministic strategy. Let us admit that such a strategy exists. For this strategy let a_x be Alice's output bit if her input bit is x and let b_y and c_z be defined analogously for Bob and Charles, respectively. It follows from the winning condition that if the input bits are $x = 0$, $y = 0$ and $z = 0$, then the sum of the output bits must be even. This gives the first of the following four equations that correspond to the four possible inputs 000, 011, 101, 110 that fulfill the promise:

$$a_0 \oplus b_0 \oplus c_0 = 0$$
$$a_0 \oplus b_1 \oplus c_1 = 1$$
$$a_1 \oplus b_0 \oplus c_1 = 1$$
$$a_1 \oplus b_1 \oplus c_0 = 1$$

By adding these equations we get $0 = 1$ which is a contradiction. The best possible classical strategy satisfies three of the above equations. Therefore, it succeeds with probability $\frac{3}{4}$.

4 Depolarizing Channel

A quantum bit is with probability α replaced with the completely mixed state. The resulting state of the qubit is

$$E_\alpha(\rho) = \alpha\frac{I}{2} + (1-\alpha)\rho.$$

For a system of d qubits, the resulting state of the system is

$$E_\alpha(\rho) = \alpha\frac{I}{2^d} + (1-\alpha)\rho.$$

It holds that

$$P_\alpha(x_1, x_2, x_3) = \frac{2-\alpha}{2}$$

for any inputs x_1, x_2 and x_3 satisfying the promise. Consequently, $P_\alpha = \frac{2-\alpha}{2}$. It is not very hard to see that quantum players are better than classical ones in the presence of the depolarizing channel if $\alpha < \frac{1}{2}$.

5 Bit Flip Channel

The state of a quantum bit is flipped from $|0\rangle$ to $|1\rangle$ (and vice versa) with probability α. The resulting state of the qubit is

$$E_\alpha(\rho) = E_{\alpha_0}\rho E_{\alpha_0}^\dagger + E_{\alpha_1}\rho E_{\alpha_1}^\dagger$$

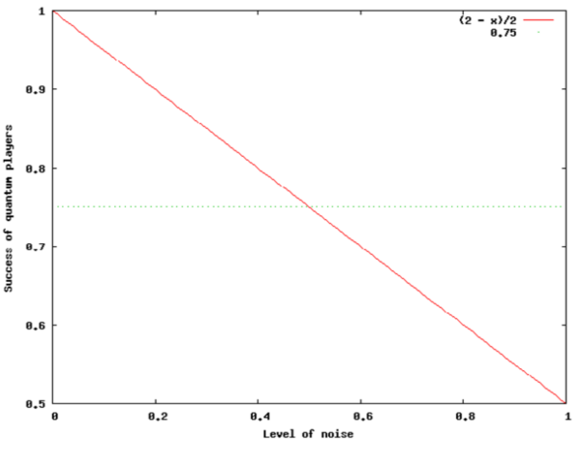

Fig. 1. Dependence of the success of quantum players on the level of noise in the presence of the depolarizing channel.

where $E_{\alpha_0} = \sqrt{1-\alpha}I$, $E_{\alpha_1} = \sqrt{\alpha}\sigma_x$ and

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

For a system of d qubits, the resulting state of the system is

$$E_\alpha(\rho) = \sum_{i=0}^{2^d-1} E_{\alpha_i}\rho E_{\alpha_i}^\dagger$$

where $E_{\alpha_{i_1\cdots i_d}} = \bigotimes_{j=1}^{d} E_{\alpha_{i_j}}$.

It holds that

$$P_\alpha(x_1, x_2, x_3) = \begin{cases} 1 & \text{if } x_1 = x_2 = x_3 = 0 \\ 2\alpha^2 - 2\alpha + 1 & \text{otherwise.} \end{cases}$$

It follows that $P_\alpha = \frac{3}{2}\alpha^2 - \frac{3}{2}\alpha + 1$. Quantum players are better than classical ones in the presence of the bit-flip channel if $\alpha \in [0, \frac{3-\sqrt{3}}{6}) \cup (\frac{3+\sqrt{3}}{6}, 1]$.

6 Phase Flip Channel

The phase of the state $|1\rangle$ is changed with probability α. The resulting state of the qubit is

$$E_\alpha(\rho) = E_{\alpha_0}\rho E_{\alpha_0}^\dagger + E_{\alpha_1}\rho E_{\alpha_1}^\dagger$$

where $E_{\alpha_0} = \sqrt{1-\alpha}I$, $E_{\alpha_1} = \sqrt{\alpha}\sigma_z$ and

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

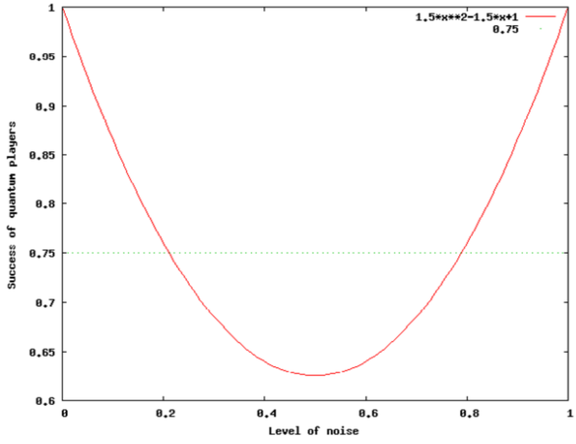

Fig. 2. Dependence of the success of quantum players on the level of noise in the presence of the bit flip channel.

For a system of d qubits, the resulting state of the system is

$$E_\alpha(\rho) = \sum_{i=0}^{2^d-1} E_{\alpha_i} \rho E_{\alpha_i}^\dagger$$

where $E_{\alpha_{i_1 \cdots i_d}} = \bigotimes_{j=1}^{d} E_{\alpha_{i_j}}$.

It holds that

$$P_\alpha(x_1, x_2, x_3) = -4\alpha^3 + 6\alpha^2 - 3\alpha + 1$$

for any inputs x_1, x_2 and x_3 satisfying the promise. Consequently, $P_\alpha = -4\alpha^3 + 6\alpha^2 - 3\alpha + 1$. Quantum players are better than classical ones in the presence of the bit-flip channel if $\alpha \in [0, -\sqrt[3]{\frac{1}{16}} + \frac{1}{2})$.

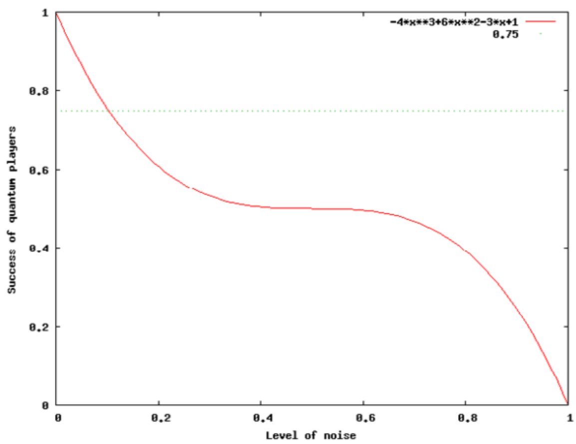

Fig. 3. Dependence of the success of quantum players on the level of noise in the presence of the phase flip channel.

7 Bit-Phase Flip Channel

The bit-phase flip channel is a combination of the two previous channels. The resulting state of the qubit is

$$E_\alpha(\rho) = E_{\alpha_0}\rho E_{\alpha_0}^\dagger + E_{\alpha_1}\rho E_{\alpha_1}^\dagger$$

where $E_{\alpha_0} = \sqrt{1-\alpha} I$, $E_{\alpha_1} = \sqrt{\alpha}\sigma_y$ and

$$\sigma_y = \begin{pmatrix} 0 & -\imath \\ \imath & 0 \end{pmatrix}.$$

For a system of d qubits, the resulting state of the system is

$$E_\alpha(\rho) = \sum_{i=0}^{2^d-1} E_{\alpha_i}\rho E_{\alpha_i}^\dagger$$

where $E_{\alpha_{i_1\cdots i_d}} = \bigotimes_{j=1}^d E_{\alpha_{i_j}}$.

It holds that

$$P_\alpha(x_1, x_2, x_3) = \begin{cases} -4\alpha^3 + 6\alpha^2 - 3\alpha + 1 & \text{if } x_1 = x_2 = x_3 = 0 \\ -\alpha + 1 & \text{otherwise.} \end{cases}$$

Consequently, $P_\alpha = -\alpha^3 + \frac{3}{2}\alpha^2 - \frac{3}{2}\alpha + 1$. Quantum players are better than classical ones in the presence of the bit-flip channel if $\alpha \in [0, -\frac{1}{4u} + u + \frac{1}{2})$ where $u = \sqrt[3]{-\frac{1}{8} + \frac{\sqrt{2}}{8}}$.

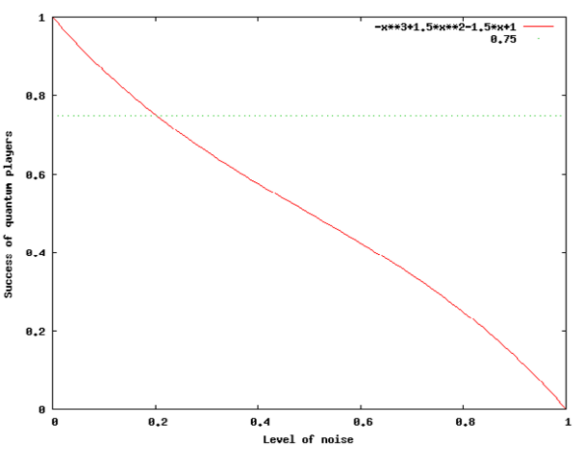

Fig. 4. Dependence of the success of quantum players on the level of noise in the presence of the bit-phase flip channel.

8 Amplitude Damping Channel

The amplitude damping channel describes effects caused by loss of energy from a quantum system. The resulting state of the qubit is

$$E_\alpha(\rho) = E_{\alpha_0}\rho E_{\alpha_0}^\dagger + E_{\alpha_1}\rho E_{\alpha_1}^\dagger$$

where

$$E_{\alpha_0} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\alpha} \end{pmatrix}, \quad E_{\alpha_1} = \begin{pmatrix} 0 & \sqrt{\alpha} \\ 0 & 0 \end{pmatrix}.$$

For a system of d qubits, the resulting state of the system is

$$E_\alpha(\rho) = \sum_{i=0}^{2^d-1} E_{\alpha_i}\rho E_{\alpha_i}^\dagger$$

where $E_{\alpha_{i_1\cdots i_d}} = \bigotimes_{j=1}^{d} E_{\alpha_{i_j}}$.

It holds that

$$P_\alpha(x_1, x_2, x_3) = \frac{1 + \sqrt{1-\alpha}^3}{2}$$

for any inputs x_1, x_2 and x_3 satisfying the promise. Consequently, $P_\alpha = \frac{1+\sqrt{1-\alpha}^3}{2}$. Quantum players are better than classical ones in the presence of the amplitude damping channel if $\alpha \in [0, 1 - \frac{1}{\sqrt[3]{4}})$.

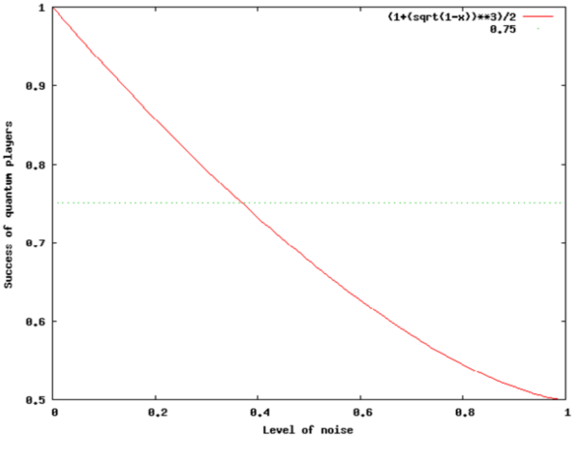

Fig. 5. Dependence of the success of quantum players on the level of noise in the presence of the amplitude damping channel.

9 Conclusions and Open Problems

We have studied the impact of several basic noisy quantum channels on the quantum winning strategy for the Mermin-GHZ game. It has turned out that all the channels are able to decrease the success probability of quantum players so that they have no advantage over classical players, provided the noise is sufficiently strong. We have also investigated how strong the noise can be so that quantum players would still be better than classical ones.

In this paper we have considered a fixed quantum strategy only. It would be certainly reasonable to investigate for various types of quantum noise whether there is a quantum strategy which is better than the winning strategy in the presence of noise and to find a bound on the success of quantum strategies. A natural direction of the future research is also to examine the impact of quantum noise on generalizations of the Mermin-GHZ game called Mermin's parity game [7] and the extended parity game [4]. Another open question of interest is how quantum noise influences other pseudo-telepathy games.

References

[1] Bell, J. S., *On the Einstein Podolsky Rosen paradox*, Physics **1** (1964), 195–200.

[2] Brassard, G., A. Broadbent and A. Tapp, *Quantum pseudo-telepathy*, Foundations of Physics **35** (2005), 1877–1907.

[3] Buhrman, H., R. Cleve and A. Wigderson, *Quantum vs. classical communication and computation*, "Proceedings of the thirtieth Annual ACM Symposium on Theory of Computing", 63–68, ACM Press, 1998.

[4] Buhrman, H., P. Hoyer, S. Massar and H. Roehrig, *Combinatorics and quantum nonlocality*, Physical Review Letters **91** (2003), 047903.

[5] Greenberger D. M., M. A. Horne, A. Shimony and A. Zeilinger, *Bell's theorem without inequalities*, American Journal of Physics **58** (1990), 1131–1143.

[6] Holevo A. S., *Bounds for the quantity of information transmitted by a quantum communication channel*, Problemy Peredachi Informatsii **9** (1973), 3–11. English translation in Problems of Information Transmission **9** (1973), 177–183.

[7] Mermin N. D., *Extreme quantum entanglement in a superposition of macroscopically distinct states*, Physical Review Letters **65** (1990), 1838–1840.

[8] Raz R., *Exponential separation of quantum and classical communication complexity*, "Proceedings of the thirty-first Annual ACM Symposium on Theory of Computing", 358–367, ACM Press, 1999.

[9] Yao A. C-C., *Some complexity questions related to distributive computing*, "Proceedings of the 11th Annual ACM Symposium on Theory of Computing", 209–213, ACM Press, 1979.