International Journal of Foundations of Computer Science
© World Scientific Publishing Company

SEPARATION BETWEEN CLASSICAL AND QUANTUM WINNING STRATEGIES FOR THE MATCHING GAME

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

Received (received date)
Revised (revised date)
Communicated by Editor's name

ABSTRACT

Communication complexity is an area of classical computer science which studies how much communication is necessary to solve various distributed computational problems. Quantum information processing can be used to reduce the amount of communication required to carry out some distributed problems. We speak of pseudo-telepathy when it is able to completely eliminate the need for communication. The matching game is the newest member of the family of pseudo-telepathy games. After introducing a general model for pseudo-telepathy games, we focus on the question what the smallest size of inputs is for which the matching game is a pseudo-telepathy game.

Keywords: Quantum pseudo-telepathy; classical and quantum winning strategies; the matching game; local realism.

1. Introduction

Quantum information processing allows us to solve problems that we are not able to solve in the classical world at all or at least that we are not able to solve efficiently. This is true also in the field of communication complexity. The first convincing evidence that quantum communication protocols can be more efficient than classical ones was given in 1998 by Buhrman, Cleve and Wigderson [5]. 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 [6]. Since quantum entanglement provides us with strong non-local correlations, one can ask whether it can be used even to completely eliminate the need for communication. 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 [7] in which 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 and they are usually called pseudo-telepathy games.

Apart from the fact that they can be seen as distributed problems which can be solved without any form of direct communication between the parties, there is one more reason to be interested in pseudo-telepathy games. They 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 [2]. *Locality* means that no action performed at a location A can have an instantenous (faster than light) effect at a remote location B. *Realism* 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 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 (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 able 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. We say that 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 said to be *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 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 to believe that Alice and Bob are able to communicate in the way unknown to classical physics. Now, one of possible explanations will be that the players are endowed with telepathic powers. A survey of pseudo-telepathy games can be found in [3]. 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* $\omega_s(G)$ of a deterministic strategy s is defined as the proportion of questions from the promise P for which s produces a correct answer. Clearly, this number can by interpreted as the probability that the strategy s 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:

$$\omega_d(G) = \max_s \frac{\{(x, y) \in P \mid (x, y, s_A(x), s_B(y)) \in W\}}{|P|}. \tag{1}$$

Alice and Bob can also use a classical 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 the game G using a randomized strategy cannot be greater than $\omega_d(G)$ [3].

This paper examines how successful classical players can be at the matching game. This game is described in the next section. Classical winning strategies for inputs of size 4 and for inputs of size 6 are proposed in Section 3. In Section 4, we show that there is no classical winning strategy if the input size is greater than 6.

2. The Matching Game

The matching game is the youngest member of the family of pseudo-telepathy games. It was proposed by Buhrman and Kerenidis in 2004 [4].

Definition 1
A perfect matching M on the set $\{0, \ldots, m-1\}$, where m is even, is a partition of this set into $\frac{m}{2}$ sets, each of cardinality 2. We define M_m as the set of all perfect matchings on $\{0, \ldots, m-1\}$.

2.1. The game

Alice receives a bit string $x = x_0 x_1 \cdots x_{m-1}$ and Bob receives a perfect matching $y \in M_m$. The task for Alice is to output a string $a \in \{0, 1\}^{\lceil \log m \rceil}$. The task for Bob is to output a set $\{b_{1_1}, b_{1_2}\} \in y$ and a string $b_2 \in \{0, 1\}^{\lceil \log m \rceil}$. The players win the round if and only if

$$x_{b_{1_1}} \oplus x_{b_{1_2}} = (\bar{b}_{1_1} \oplus \bar{b}_{1_2}) \cdot (a \oplus b_2) \tag{2}$$

where $u \cdot v = \bigoplus_{i=1}^{n}(u_i \wedge v_i)$ and $\bar{b}_{1_1}, \bar{b}_{1_2} \in \{0,1\}^{\lceil \log m \rceil}$. The exclusive-or operator is applied on bits on the left side of the equation and is applied bit-wise on bit strings on the right side. The bit string $\bar{b}_{1_1}$ is a binary representation of the number b_{1_1} in which the most significant bit of b_{1_1} is preceded by k_{1_1} zero bits where $k_{1_1} = \lceil \log m \rceil - \lfloor \log b_{1_1} \rfloor - 1$. Similarly, the bit string $\bar{b}_{1_2}$ is a binary representation of the number b_{1_2}.

A formal definition of the matching game is given in Table 1.

Table 1. The matching game.

X	$\{0,1\}^m$ where m is even
Y	M_m
A	$\{0,1\}^{\lceil \log m \rceil}$
B	$\{\{b_{1_1}, b_{1_2}\} \mid b_{1_1}, b_{1_2} \in \{0,1,\ldots,m-1\}\} \times \{0,1\}^{\lceil \log m \rceil}$
P	$X \times Y$
W	$x_{b_{1_1}} \oplus x_{b_{1_2}} = (\bar{b}_{1_1} \oplus \bar{b}_{1_2}) \cdot (a \oplus b_2) \wedge \{b_{1_1}, b_{1_2}\} \in y$

A quantum winning strategy for the matching game and also the proof that it always succeeds can be found in [4]. The proof of the non-existence of a classical winning strategy for the matching game is based on the exponential separation between quantum and classical one-way communication complexity of the hidden matching problem [1, 4].

3. Classical Winning Strategies for $m = 4$ and $m = 6$

The above asymptotic result tells us only that for large enough inputs, there is no classical winning strategy for the matching game. But to be able to perform practical experiments, it is important to know exactly the smallest size of inputs with this property. Obviously, there is a classical winning strategy for $m = 2$ because there is only one perfect matching on the set $\{0, 1\}$. We propose classical winning strategies both for $m = 4$ and $m = 6$. These strategies are both obtained as a straightforward consequence of the following lemma which tells us that for each input size, there is a classical strategy which is winning if we properly restrict the set of questions Alice and Bob can be given.

Definition 2 *For a positive integer m, we denote with W_m the set $\{0\} \cup \{2^i \mid i \in \{0, 1, \ldots, \lceil \log m \rceil - 1\}\}$.*

Lemma 1 *Let $m > 0$ be an even integer. Suppose that Alice is given an input $x = x_0 x_1 \cdots x_{m-1}$ and that Bob's input y contains a pair $\{w_1, w_2\} \subset W_m$. If Alice outputs the string $a = (x_0 \oplus x_{2^{\lceil \log m \rceil - 1}})(x_0 \oplus x_{2^{\lceil \log m \rceil - 2}}) \cdots (x_0 \oplus x_1)$ and Bob outputs the pair $b = (\{w_1, w_2\}, 0^{\lceil \log m \rceil})$, the players will win.*

Proof. Let $str^m(i,j)$, where $i, j \in \{0, \ldots, \lceil \log m \rceil - 1\}$, be the bit string of length $\lceil \log m \rceil$ such that

$$\begin{array}{ll} str^m(i,j)_k = 1 & \text{if } k = i \vee k = j \\ str^m(i,j)_k = 0 & \text{otherwise.} \end{array}$$

We show that for the players' inputs x and y, respectively, and their outputs a and b, respectively, the equation

$$x_{w_1} \oplus x_{w_2} = (\bar{w}_1 \oplus \bar{w}_2) \cdot (a \oplus 0^{\lceil \log m \rceil})$$

is satisfied. Without loss of generality, four distinct cases are sufficient to consider:

- If $x_0 = 0$, $w_1 = 0$ and $w_2 = 2^j$, then the right side of the equation can be transformed in the following way:

$$str^m(j,j) \cdot x_{2^{\lfloor \log m \rfloor -1}} x_{2^{\lfloor \log m \rfloor -2}} \cdots x_1 = x_{w_2} = x_{w_1} \oplus x_{w_2},$$

- if $x_0 = 0$, $w_1 = 2^i$ and $w_2 = 2^j$, then the right side of the equation can be transformed in the following way:

$$str^m(i,j) \cdot x_{2^{\lfloor \log m \rfloor -1}} x_{2^{\lfloor \log m \rfloor -2}} \cdots x_1 = x_{w_1} \oplus x_{w_2},$$

- if $x_0 = 1$, $w_1 = 0$ and $w_2 = 2^j$, then the right side of the equation can be transformed in the following way:

$$str^m(j,j) \cdot \neg x_{2^{\lfloor \log m \rfloor -1}} \neg x_{2^{\lfloor \log m \rfloor -2}} \cdots \neg x_1 = \neg x_{w_2} = x_{w_1} \oplus x_{w_2},$$

- if $x_0 = 1$, $w_1 = 2^i$ and $w_2 = 2^j$, then the right side of the equation can be transformed in the following way:

$$str^m(i,j) \cdot \neg x_{2^{\lfloor \log m \rfloor -1}} \neg x_{2^{\lfloor \log m \rfloor -2}} \cdots \neg x_1 = \neg x_{w_1} \oplus \neg x_{w_2} = x_{w_1} \oplus x_{w_2}.$$

□

Theorem 1 *There is a classical winning strategy for the matching game for $m = 4$ and also for $m = 6$.*

Proof. For $m = 4$, Lemma 1 gives us the following deterministic strategy:

1. For an input $x = x_0x_1x_2x_3$, Alice outputs a string $a = a_0a_1$ where $a_0 = x_0 \oplus x_2$ and $a_1 = x_0 \oplus x_1$,

2. for an input y, Bob outputs a pair $(\{w_1, w_2\}, 00)$ where $\{w_1, w_2\} \subset \{0, 1, 2\}$ and $\{w_1, w_2\} \in y$.

This strategy is depicted in Figure 1.

It follows from Lemma 1 that each deterministic strategy which satisfies simultaneously the following conditions succeeds for all possible inputs of size 6:

1. For an input $x = x_0x_1 \cdots x_5$, Alice outputs a string $a = a_0a_1a_2$ where $a_0 = x_0 \oplus x_4$, $a_1 = x_0 \oplus x_2$ and $a_2 = x_0 \oplus x_1$,

2. for an input y, Bob outputs a pair $(\{w_1, w_2\}, 000)$ where $\{w_1, w_2\} \subset \{0, 1, 2, 4\}$ and $\{w_1, w_2\} \in y$.

Figure 1: Classical winning strategy for $m = 4$.

x	$s_A(x)$
0000, 0001, 1110, 1111	00
0100, 0101, 1010, 1011	01
0010, 0011, 1100, 1101	10
1000, 1001, 0110, 0111	11

y	$s_B(y)$
{{0, 1}, {2, 3}}	({0, 1}, 00)
{{0, 2}, {1, 3}}	({0, 2}, 00)
{{1, 2}, {0, 3}}	({1, 2}, 00)

Figure 2: Classical winning strategy for $m = 6$.

x	$s_A(x)$
000000, 000001, 000100, 000101, 111010, 111011, 111110, 111111	000
000010, 000011, 000110, 000111, 111000, 111001, 111100, 111101	100
001000, 001001, 001100, 001101, 110010, 110011, 110110, 110111	010
001010, 001011, 001110, 001111, 110000, 110001, 110100, 110101	110
010000, 010001, 010100, 010101, 101010, 101011, 101110, 101111	001
010010, 010011, 010110, 010111, 101000, 101001, 101100, 101101	101
011000, 011001, 011100, 011101, 100010, 100011, 100110, 100111	011
011010, 011011, 011110, 011111, 100000, 100001, 100100, 100101	111

y	$s_B(y)$
{{0, 1}, {2, 3}, {4, 5}}, {{0, 1}, {2, 5}, {3, 4}}	({0, 1}, 000)
{{0, 2}, {1, 3}, {4, 5}}, {{0, 2}, {1, 5}, {3, 4}}	({0, 2}, 000)
{{0, 4}, {1, 2}, {3, 5}}, {{0, 4}, {1, 3}, {2, 5}}, {{0, 4}, {1, 5}, {2, 3}}	({0, 4}, 000)
{{0, 3}, {1, 2}, {4, 5}}, {{0, 5}, {1, 2}, {3, 4}}	({1, 2}, 000)
{{0, 2}, {1, 4}, {3, 5}}, {{0, 3}, {1, 4}, {2, 5}}, {{0, 5}, {1, 4}. {2, 3}}	({1, 4}, 000)
{{0, 1}, {2, 4}, {3, 5}}, {{0, 3}, {1, 5}, {2, 4}}, {{0, 5}, {1, 3}, {2, 4}}	({2, 4}, 000)

One possible winning strategy for inputs of size 6 is depicted in Figure 2.

□

4. Classical Winning Strategies for $m \geq 8$

This section investigates whether there is a classical winning strategy for the matching game for $m \geq 8$. The task is carried out using some pieces of knowledge from the graph theory. Therefore, we begin this section with several necessary definitions regarding graphs and their properties.

Definition 3 *A (undirected) graph G is an ordered pair $G = (V, E)$ where V is a set of vertices and E is a set of two-element sets of vertices. These sets are called edges.*

Definition 4 *Let $G = (V, E)$ be a graph. A path in G is a sequence $v_0, v_1, \ldots, v_n$, where n is a non-negative integer, of mutually different vertices such that for each $i \in \{0, \ldots, n-1\}$, it holds that $\{v_i, v_{i+1}\} \in E$.*

Definition 5 *Let $G = (V, E)$ be a graph. The distance $d_G(u, v)$ of vertices $u, v \in V$ in G is the smallest number n for which there is a path $v_0, v_1, \ldots, v_n$ in G such that $v_0 = u$ and $v_n = v$.*

Definition 6 *Let $G = (V, E)$, $G' = (V', E')$ be graphs. We say that G' is a subgraph of G if $V' \subseteq V$ and $E' \subseteq E$. Moreover, G' is said to be an induced subgraph of G if for any vertices $u, v \in V'$, it holds that $\{u, v\} \in E'$ if and only if $\{u, v\} \in E$.*

Definition 7 *Let $G = (V, E)$ be a graph and let $G' = (V', E')$ be its induced subgraph such that $V' \neq \emptyset$. We say that G' is a connected component (or only component) in G if the following two conditions hold simultaneously:*

1. *There are no vertices $u \in V'$ and $v \in V \setminus V'$ such that $\{u, v\} \in E$,*
2. *for any vertices $u, v \in V'$, there is a path $v_0, v_1, \ldots, v_n$ in G' such that $v_0 = u$ and $v_n = v$.*

Definition 8 *Let $G = (V, E)$ be a graph. We say that G has cardinality (has size) n if $|V| = n$.*

Now we will proceed in the following way. At first, we assign to each classical deterministic winning strategy s a set of bit strings of length m and a set of subsets of cardinality 2 of the set $\{0, 1, \ldots, m-1\}$. Then we examine properties of these sets and show that for $m \geq 8$ such sets cannot exist. We conclude that for $m \geq 8$, there is no classical deterministic winning strategy. Since by fixing random variables we can turn any classical randomized winning strategy into a deterministic one, this means that there is no classical winning strategy at all.

Definition 9 *Let s be any classical deterministic strategy for the matching game for some m. We define a graph $G_s = (V, E_s)$ where $V = \{0, 1, \ldots, m-1\}$ and E_s is the set of all elements of the set $W = \{\{i, j\} \mid i, j \in \{0, 1, \ldots, m-1\}\}$ which Bob produces as a part of at least one of his outputs using the strategy s.*

Lemma 2 *Let $m > 0$ be an even integer. Suppose that there is a classical deterministic winning strategy s for the matching game for m. Then there is a set R of bit strings of length m such that the following conditions hold simultaneously:*

1. *$|R| \geq \frac{2^m}{2^{\lceil log\ m \rceil}}$,*
2. *the graph G_s contains a component of cardinality greater than $\frac{m}{2}$,*
3. *for each $\{i, j\} \in E_s$, the parity of bits on positions i and j is the same for every $r \in R$.*

Proof.

1. There are 2^m possible inputs and $2^{\lceil log\ m \rceil}$ possible outputs for Alice. Therefore, there are at least $\frac{2^m}{2^{\lceil log\ m \rceil}}$ inputs for which Alice produces the same output using s. We take as the set R some set of Alice's inputs with this property whose cardinality is at least $\frac{2^m}{2^{\lceil log\ m \rceil}}$.

2. Let us admit that the graph G_s does not contain a component of cardinality greater than $\frac{m}{2}$. We show that there is at least one Bob's input for which the strategy s is not defined. In other words, we show that there is a perfect matching y on the set $\{0, 1, \ldots, m-1\}$ such that for each $\{i, j\} \in y$, i and j are in different components of G_s. This result provides us with a contradiction because the strategy s is deterministic.

   Let $C_1, \ldots, C_k$ be all the components of the graph G_s. Suppose without loss of generality that for each $i \in \{1, \ldots, k-1\}$, the component C_i has greater or equal cardinality than the component C_{i+1}. We describe a simple procedure to construct the perfect matching y. We begin with $y = \emptyset$. Then we repeat as long as possible the following step. We try to find the greatest index $j \in \{2, \ldots, k\}$ such that the component C_j contains a vertex which has not been inserted in y so far. Let us denote with $u_1, \ldots, u_l$ all the vertices from C_j with this property. Since the component C_{j-1} has greater or equal cardinality than the component C_j and we proceed from components of smaller size to components of greater size, there certainly are mutually different vertices $v_1, \ldots, v_l$ in C_{j-1} which have not been inserted in y so far. Now for each $i \in \{1, \ldots, l\}$, we insert the set $\{u_i, v_i\}$ in y. If we are not able to find the index j, two possible cases can be distinguished. If the component C_1 does not contain a vertex which has not been inserted in y so far, then there is nothing more to do. On the contrary, if C_1 contains $2i$ vertices, where i is a non-negative integer, with this property, we remove i sets of vertices from y, assign the vertices from C_1 to vertices from the removed pairs and insert the sets we have obtained in y. In both cases we get the perfect matching y which gives us the desired contradiction.

3. Let x, x' be any elements of R and let $\{b_{1_1}, b_{1_2}\}$ be any element of E_s. If Bob's input is $y \in Y$ such that $s_B(y) = (\{b_{1_1}, b_{1_2}\}, b_2)$, for some b_2, the right side of the equation (2) will be the same both for x and x'. Since s is a winning

strategy, it follows that the parity of bits on positions b_{1_1} and b_{1_2} is the same both for x and x'. Since x and x' has been arbitrarily chosen from R, the parity of bits on positions b_{1_1} and b_{1_2} has to be the same for all elements of R. This holds for all pairs of positions from E_s because the set $\{b_{1_1}, b_{1_2}\}$ has been arbitrary as well.

□

Our goal is to show that for $m \geq 8$, the sets R and E_s from Lemma 2 cannot exist. For this purpose, we slightly modify the definition of the graph colouring problem.

Definition 10 *Let $G = (V, E)$ be a graph and let $h : E \rightarrow \{0, 1\}$ be a function. We say that G is colourable according to h if there is a function $c : V \rightarrow \{0, 1\}$ such that for each $\{u, v\} \in E$ it holds that $c(u) \oplus c(v) = h(\{u, v\})$. The function c is said to be a colouring of the graph G according to h.*

Lemma 3 *The last condition from Lemma 2 holds for a set R of bit strings of length m and a set T of elements of the set $W = \{\{i, j\} \mid i, j \in \{0, 1, \ldots, m-1\}\}$ if and only if there is a function $h : T \rightarrow \{0, 1\}$ for which $|R|$ various colourings of the graph $G = (V, T)$, where $V = \{0, 1, \ldots, m-1\}$, according to h exist.*

Proof. ($\Rightarrow$) Suppose that for a set R of bit strings of length m and a set T of elements of the set W, the last condition from Lemma 2 holds. We intend to find a function $h : T \rightarrow \{0, 1\}$ for which $|R|$ various colourings of the graph G according to h exist. Let r be any element of R. The function h is defined by $h(\{u, v\}) = r_u \oplus r_v$, for each $\{u, v\} \in T$. Since every $r \in R$ can be transformed to a colouring c_r of the graph G according to h by $c_r(u) = r_u$, where $u \in V$, $|R|$ various colourings of G according to h exist.

($\Leftarrow$) Suppose that there is a function $h : T \rightarrow \{0, 1\}$ such that k various colourings of the graph $G = (V, T)$, where $V = \{0, 1, \ldots, m-1\}$, according to h exist. We intend to find a set R, where $|R| = k$, of bit strings of length m such that the last condition from Lemma 2 holds for the sets R and T. We define this set as $R = \{c(0)c(1) \cdots c(m-1) \mid c \text{ is a colouring of } G \text{ according to } h.\}$. The last condition from Lemma 2 holds because for each $\{i, j\} \in T$, $r_i \oplus r_j = h(\{i, j\})$ for every $r \in R$. □

Corollary 1 *Let $m > 0$ be an even integer. In order to show that there is no classical deterministic winning strategy for the matching game for m, it suffices to show that there are no graph $G = (V, E)$, where $|G| = m$, and no function $h : E \rightarrow \{0, 1\}$ such that the following conditions hold simultaneously.*

1. *There are at least $\frac{2^m}{2^{\lceil log\ m \rceil}}$ colourings of G according to h,*

2. *G contains a component of cardinality greater than $\frac{m}{2}$.*

In the rest of this section, the following simple statement will be useful.

Lemma 4 *Let $G = (V, E)$ be a graph and let $h : E \rightarrow \{0, 1\}$ be a function. If G is colourable according to h, then there are exactly 2^k colourings according to h where k is a number of components of G.*

Proof. Suppose that there is a colouring c of the graph G according to h. It suffices to show that for any component $C = (V', E')$ of G, there are exactly 2 colourings of C according to h. Since the events of colouring mutually different components of G according to h are independent, this gives us the desired result.

If C contains only one vertex, the statement holds trivially because we can assign either 0 or 1 to the only vertex of C. Suppose further that C contains $k > 1$ vertices. By restricting the colouring c to the component C only, we obviously obtain a colouring of C according to h. Let us denote this restricted colouring with c_r. It is straightforward to see that a function $c'_r : V' \to \{0,1\}$ defined as $c'_r(u) = \neg c_r(u)$ is also a colouring of C according to h. Now consider any colouring q of C according to h and any vertices $u, v \in V'$. Clearly, it holds that either $q(u) = c_r(u)$ or $q(u) = c'_r(u)$. Suppose without loss of generality that the first possibility has occurred. We intend to show, using induction on the distance $d_C(u,v)$ of the vertices u, v in C, that also $q(v) = c_r(v)$. This is certainly true for $d_C(u,v) = 0$ because then $u = v$. Now suppose that $d_C(u,v) = n > 0$ and that the equality holds for each vertex $w \in V'$ such that $d_C(u,v) = n-1$. There is a path $v_0, v_1, \ldots, v_n$ in C such that $v_0 = u$ and $v_n = v$. Since the equation $q(v_{n-1}) \oplus q(v) = h(\{u,v\})$ has to be satisfied, it follows with the help of the induction hypothesis that

$$q(v) = h\{u,v\} \oplus q(v_{n-1}) = h\{u,v\} \oplus c_r(v_{n-1}) = c_r(v).$$

We have shown that if the colouring q agrees with the colouring c on some vertex from C, then the two colourings agree on each vertex from C. A similar result can be obtained for the case of $q(u) = c'_r(u)$. Consequently, we can conclude that either $d = c_r$ or $d = c'_r$. □

Theorem 2 *Let $m \geq 8$ be an even integer. There are no graph $G = (V, E)$, where $|G| = m$, and no function $h : E \to \{0,1\}$ such that the following conditions hold simultaneously.*

1. *There are at least $\frac{2^m}{2^{\lceil log\ m \rceil}}$ colourings of G according to h,*
2. *G contains a component of cardinality greater than $\frac{m}{2}$.*

Proof. Let $G = (V, E)$, where $|G| = m$, be a graph and let $h : E \to \{0,1\}$ be a function. Suppose that there are at least $\frac{2^m}{2^{\lceil log\ m \rceil}}$ colourings of G according to h. We show that the other condition cannot hold.

From the previous lemma we can conclude that the graph G is composed at least of $m - \lceil log\ m \rceil$ components. Since G contains a component of cardinality greater than $\frac{m}{2}$, it contains at most $\frac{m-2}{2}$ components composed of a single vertex. This indicates that G is composed at most of $\frac{m}{2}$ components. It is easy to verify that for $m \geq 8$, $\frac{m}{2} < m - \lceil log\ m \rceil$. Therefore, if $m \geq 8$, the graph G cannot exist. □

5. Conclusions and Open Problems

In the present text, we have described a general model for pseudo-telepathy games and a pseudo-telepathy game called the matching game. We have dealt with the problem what the smallest size of inputs, denoted as m, is for which the matching game is pseudo-telepathic. We have found classical winning strategies for $m = 4$ and $m = 6$. Also, we have shown that there is no classical winning strategy for $m \geq 8$.

Since the matching game is the youngest pseudo-telepathy game, it is known very little about it so far. For example, we still do not know any nontrivial upper bound for the success of the best possible classical strategy for $m \geq 8$. This is of importance because due to erroneous measurements, it is unavoidable that Alice and Bob will not be perfect in real experiments. If they try to show that the physical world is not local realistic, it will have to be sufficient that they are significantly better than classical players could ever be. Obviously, the better Alice and Bob are than classical players, the more convincing the experiment is.

Acknowledgements

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

References

1. Z. Bar-Yossef, T. S. Jayram, I. Kerenidis. Exponential separation of quantum and classical one-way communication complexity. Proceedings of the thirty-sixth Annual ACM Symposium on Theory of Computing, pp. 128–137, ACM Press, 2004.
2. J. S. Bell: On the Einstein Podolsky Rosen paradox. Physics 1(3), pp. 195–200, 1964.
3. G. Brassard, A. Broadbent, A. Tapp. Quantum pseudo-telepathy. Foundations of Physics 35(11), pp. 1877–1907, 2005.
4. A. Broadbent. Quantum pseudo-telepathy games. M.Sc. Thesis, Université de Montréal, 2004.
   http://www.iro.umontreal.ca/˜ broadbea/Publications/AnneMemoireFinal.pdf.
5. H. Buhrman, R. Cleve, A. Wigderson. Quantum vs. classical communication and computation. Proceedings of the thirtieth Annual ACM Symposium on Theory of Computing, pp. 63–68, ACM Press, 1998.
6. R. Raz. Exponential separation of quantum and classical communication complexity. Proceedings of the thirty-first Annual ACM Symposium on Theory of Computing, pp. 358–367, ACM Press, 1999.
7. A. C-C. Yao. Some complexity questions related to distributive computing. Proceedings of the 11th Annual ACM Symposium on Theory of Computing, pp. 209–213, ACM Press, 1979.