The Impossibility of Pseudo-Telepathy Without Quantum Entanglement

Viktor Galliard *   Alain Tapp †   Stefan Wolf ‡

Abstract

Imagine that two parties Alice and Bob, unable to communicate, are both given a 16-bit string such that the strings are either equal of differ in exactly 8 positions. Both parties are then supposed to output a 4-bit string in such a way that these short strings are equal if and only if the original, longer strings given to them were equal as well. It is known that this task can be fulfilled without failure and without communication if Alice and Bob share 4 maximally entangled quantum bits. We show that, on the other hand, they *cannot* win the same game with certainty if they only share *classical* bits, even if it is an unlimited number. This means that for fulfilling this particular distributed task, quantum entanglement can completely replace communication. This phenomenon has been called pseudo-telepathy. The results of this paper complete the analysis of the first proposed game of this type between two players.

1 Introduction

1.1 Pseudo-Telepathy Games

Pseudo-telepathy is a phenomenon showing that for achieving certain well-defined distributed tasks, communication can be replaced by measuring shared quantum states proving so-called *entanglement*; this does *not* imply, however, that such quantum entanglement allows for, instantaneous, communication.

More specifically, a *two-player pseudo-telepathy game* is a game in which two separated parties who are not able to communicate are asked two *questions*, x_A and x_B, respectively, and should give *answers* y_A and y_B satisfying a certain condition defined by the game. Formally, given that the pair of questions (x_A, x_B) belongs to a certain relation $R_X \subseteq \mathcal{X}_A \times \mathcal{X}_B$, the answers have to be such that

$$(x_A, x_B, y_A, y_B) \in R_{XY} \subseteq \mathcal{X}_A \times \mathcal{X}_B \times \mathcal{Y}_A \times \mathcal{Y}_B$$

*Untervaz, Switzerland. E-mail: math@galliard.ch. Supported by Canada's NSERC and Swisscom IT Services Ltd.

†Département d'Informatique et recherche opérationnelle, Université de Montréal, C.P. 6128 succ Centre-Ville, Montréal, Québec, H3C 3J7, Canada. E-mail: tappa@iro.umontreal.ca

‡Département d'Informatique et recherche opérationnelle, Université de Montréal, C.P. 6128 succ Centre-Ville, Montréal, Québec, H3C 3J7, Canada. E-mail: wolf@iro.umontreal.ca

holds, where the game is defined by the relations R_X and R_{XY}.

Some of these games are of particular interest since they can be won by parties sharing quantum information, but *not* by parties sharing only classical information initially. A game with this property can be used for demonstrating the existence of quantum entanglement—however, this is true only if a proof is provided that there is no classical strategy for winning the game with certainty. The main result of this paper is to provide this proof for the first and most prominent example of such a game [1], for which, previously, only an asymptotic impossibility proof has been given (i.e., no concrete parameters have been known for which the game cannot be won).

1.2 The Game by Brassard, Cleve, and Tapp

In [1], the following two-party game was proposed. Let $n \geq 1$, and let $N = 2^n$. In the game with parameter n, the questions asked to the parties, Alice and Bob, are arbitrary N-bit strings x_A and x_B satisfying

$$d_H(x_A, x_B) \in \{0, N/2\} \tag{1}$$

(i.e., the questions are either equal or differ in exactly half the positions). Alice's and Bob's answers y_A and y_B have to be binary strings of length $n = \log_2 N$ satisfying the simple condition

$$y_A = y_B \longleftrightarrow x_A = x_B \ .$$

It was shown in [1] that this game can always be won if Alice and Bob share n maximally entangled quantum bits (so-called EPR pairs). On the other hand, a proof was also given that the game cannot be won without quantum entanglement if n is large enough. Unfortunately, this purely asymptotic result is not satisfactory since n has to take a particular, fixed, value, should the game be actually played (e.g., performed as an experiment demonstrating quantum entanglement). Moreover, the game *can* be won classically *with high probability* for large n if Alice and Bob agree to respond their respective questions with a random n-bit hash value thereof (using the same, predetermined, hash function).

Motivated by this, we address the question which the smallest value of n is for which the game cannot be won. In fact, for the choices $n = 1, 2$, and 3, the game can be won classically with probability 1 [1],[2]. It was conjectured that for $n = 4$ this is not the case anymore [2]. In the present paper, we prove that this conjecture is true. We will use of a connection that has been made in [2] between the game and graph colorings. In fact, the main part of the proof will be to derive a lower bound on the chromatic number of a certain graph G.

2 A Classical Impossibility Result

In this section we prove the following main result of the paper.

Theorem 1. *Classically, the described pseudo-telepathy game cannot be won with certainly for $n = 4$.*

In [2], the following connection was made between the pseudo-telepathy game and graph colorings. Let $G_N = (V_N, E_N)$ be the graph defined by

$$\begin{aligned} V_N &= \{0,1\}^N \\ E_N &= \{(u,v) \in V_N^2 \mid d_H(u,v) = N/2\} \ . \end{aligned}$$

Then the game with parameter $N = 2^n$ can be won classically if and only of

$$\chi(G_N) \le N \ , \tag{2}$$

where $\chi(G_N)$ is the chromatic number of G_N, i.e., the minimum number of different colors necessary to color the vertices of G_N in such a way that no vertices with the same color are connected by an edge. If inequality (2) is satisfied, then Alice and Bob's strategy for winning the game is to agree on a coloring of the graph beforehand and to answer a question, i.e., a vertex of the graph, by its color. If on the other hand (2) is violated, then the game cannot be won with certainty: A winning strategy *is* a corresponding coloring. All we have to prove therefore in order to obtain Theorem 1 is the following.

Proposition 2. *Let $G = G_{16}$ be the graph as defined above. Then*

$$\chi(G) > 16 \ . \tag{3}$$

In order to prove Proposition 2, we use that fact that

$$\chi(G) \ge \frac{|V(G)|}{M} \tag{4}$$

holds if M is an upper bound on the size of all independent sets of the graph. An independent set is a set of vertices which are pairwisely unconnected, and clearly, any set of vertices of the same color in a coloring is independent.

Because of (2) and (4), it is sufficient to show that no independent set of G can be larger than

$$\frac{|V(G)|}{16} - 1 = 4095 \ .$$

Lemma 3. *Let $I \subseteq V$ be an independent set of G. Then*

$$|I| \le 3912 \ .$$

Proof. Let us simplify the problem as follows. First, we observe that the graph G consists of two isomorphic connected components G_e and G_o (containing the vertices of even and odd Hamming weight, respectively). Secondly, a maximum independent set contains a vertex v if and only if it also contains its bitwise complement $\overline{v}$ since for all vertices w, we have

$$d_H(v,w) = 8 \longleftrightarrow d_H(\overline{v},w) = 8 \ .$$

Let $G_{e,<8}$ be the subgraph of G_e containing the vertices of Hamming weight less than 8, let, for $i = 0, 2, 4$, and 6 G_i be the subgraph of $G_{e,<8}$ containing the vertices of Hamming weight i, and let for a graph H $M(H)$ denote the size of a maximum independent set of H. Since

$$\begin{aligned} M(G) &= 2M(G_e) = 4M(G_{e,<8}) \\ &\leq 4(M(G_0) + M(G_2) + M(G_4) + M(G_6)) \ , \end{aligned}$$

it is sufficient to prove that

$$M(G_0) + M(G_2) + M(G_4) + M(G_6) \leq 3912/4 = 978 \tag{5}$$

holds. We will show

$$M(G_0) = 1 \tag{6}$$
$$M(G_2) = 120 \tag{7}$$
$$M(G_4) = 455 \tag{8}$$
$$M(G_6) \leq 402 \tag{9}$$

which implies (5).

Proof of (6). Trivial.

Proof of (7). We have

$$M(G_2) = |G_2| = \binom{18}{2} = 120$$

since none of the vertices are connected.

Proof of (8). The set of all vertices with a 1 in the first position is independent, and it has size 455. Its maximality follows from a result by Erdös *et. al.* [3],[4]. Let $m(n,k,t)$ be the maximum size of a subset X of all k-element subsets of $\{1, 2, \ldots, n\}$ such that for all $a, b \in X$, we have $|a \cup b| \geq t$. The mentioned result states

$$m(n,k,t) \leq \binom{n-t}{k-1}$$

whenever $n \geq (k - t + 1)(t + 1)$. We have $M(G_4) = m(16, 4, 1)$, and (8) follows.

Proof of (9). Note first that for any independent set I of G_6 such that any two vertices $u, v \in I$ satisfy $d_H(u,v) \leq 6$, we have

$$|I| \leq m(16, 6, 3) \leq 286$$

according to the result used in the proof of (8).

Let us now deal with the cases of independent sets I containing $u, v \in I$ with $d_H(u, v) \in \{10, 12\}$.

Let first $u, v \in I$ with $d_H(u,v) = 12$. Without loss of generality, we can assume

$$u = 111111 \cdot 000000 \cdot 0000 \ , \quad v = 000000 \cdot 111111 \cdot 0000 \ .$$

A third vertex $w \in I \setminus \{u,v\}$ has to be one of the following, modulo permutation of bit positions:

$$\begin{array}{lll}
000000 \cdot 111000 \cdot 1110 & 000000 \cdot 111100 \cdot 1100 & 000000 \cdot 111110 \cdot 1000 \\
100000 \cdot 100000 \cdot 1111 & 100000 \cdot 111000 \cdot 1100 & 100000 \cdot 111100 \cdot 1000 \\
100000 \cdot 111110 \cdot 0000 & 111000 \cdot 111000 \cdot 0000 &
\end{array}$$

Let now, for fixed u, v, and w, $G_{6,uvw}$ be the subgraph of G_6 arising when u, v, w, and their neighbors are removed. In order to find an upper bound on $M(G_{6,uvw})$, we decompose the graph into disjoint cliques, the number of which is such a bound. Using a simple greedy algorithm, we found decompositions for all possible vertices w (or, more precisely, "types" of vertices as listed above). The following table shows for all of the 8 types $i = 1, \ldots, 8$ the number a_i of vertices of the type and the number b_i of cliques in the decomposition of the corresponding graph.

i	1	2	3	4	5	6	7	8
a_i	80	90	24	36	720	360	36	400
b_i	394	426	495	320	370	399	425	314

Since

$$\max \left\{ \sum_{i \in \{1,2,3,4,7\}} a_i \ , \ \max_{i \in \{5,6,8\}} \{b_i\} \right\} = 399 \ ,$$

we get the bound $402 = 399 + 3$ on the size of an independent set of G_6 (including also u, v, and w). In order to see this, note that any independent set of $G_{6,uvw}$ of size larger than 399 would necessarily contain at least one vertex of one of the types 5, 6, or 8, thus the bound obtained for these types apply. The relevant clique decompositions of $G_{6,uvw}$ if w is of the types 5, 6, and 8 can be found at [5].

The case of $u, v \in I$ with $d_H(u,v) = 10$ can be treated similarly. For

$$u = 11111 \cdot 1 \cdot 00000 \cdot 00000 \ , \quad v = 00000 \cdot 1 \cdot 11111 \cdot 00000 \ ,$$

the list of types is

$$\begin{array}{lll}
00000 \cdot 0 \cdot 10000 \cdot 11111 & 00000 \cdot 0 \cdot 11100 \cdot 11100 & 00000 \cdot 0 \cdot 11110 \cdot 11000 \\
00000 \cdot 0 \cdot 11111 \cdot 10000 & 00000 \cdot 1 \cdot 00000 \cdot 11111 & 00000 \cdot 1 \cdot 11000 \cdot 11100 \\
00000 \cdot 1 \cdot 11100 \cdot 11000 & 00000 \cdot 1 \cdot 11110 \cdot 10000 & 10000 \cdot 0 \cdot 10000 \cdot 11110 \\
10000 \cdot 0 \cdot 11100 \cdot 11000 & 10000 \cdot 0 \cdot 11110 \cdot 10000 & 10000 \cdot 0 \cdot 11111 \cdot 00000 \\
11000 \cdot 1 \cdot 11000 \cdot 10000 & 11000 \cdot 1 \cdot 11100 \cdot 00000 & 11100 \cdot 0 \cdot 11100 \cdot 00000
\end{array}$$

The clique decompositions found are of size

i	1	2	3	4	5	6	7	8
a_i	5	100	50	5	1	100	100	25
b_i	318	366	394	428	260	345	365	408

i	9	10	11	12	13	14	15
a_i	125	500	125	5	500	100	100
b_i	300	346	373	405	298	313	302

We have

$$\max\left\{\sum_{i\in\{1,2,3,4,5,8,11,12\}} a_i\ ,\ \max_{i\in\{6,7,9,10,13,14,15\}}\{b_i\}\right\} = 365\ ,$$

which yields a better bound than we got for the case of Hamming distance 12. Again, the concrete decompositions can be found at [5]. □

The proof of Lemma 3 also establishes Proposition 2, and hence Theorem 1.

3 Concluding Remarks

We have shown that the first proposed two-party pseudo-telepathy game, due to Brassard, Cleve, and Tapp [1], cannot be won classically for the parameter $n = 4$ (which is hence the smallest parameter with this property). Two players on the other hand sharing four maximally entangled quantum bits can use these to completely avoid the necessary communication and win the game. A number of repeated executions of this game can, provided that Alice and Bob never fail, be seen as a convincing demonstration of the existence of quantum entanglement.

References

[1] G. Brassard, R. Cleve and A. Tapp, "The cost of exactly simulating quantum entanglement with classical communication", *Physical Review Letter*, Vol. 83, No. 9, pp. 1874–1878, 1999.

[2] V. Galliard and S. Wolf, "Pseudo-telepathy, entanglement, and graph colorings", in *Proceedings of ISIT 2002*, 2002.

[3] P. Erdös, C. Ko, and R. Rado, "Intersection theorem for systems of finite sets", *Quarterly journal of mathematics*, Vol. 2, No. 12, pp. 313–320, 1961.

[4] R. M. Wilson, "The exact bound in the Erdös-Ko-Rado theorem", *Combinatorica*, Vol. 4, pp. 247–260, 1984.

[5] http://math.galliard.ch/Quantum/pseudo-telepathy/data03/ ptp_cliques_twg03.txt. In ptp_cliques_twg03_extract.txt, initial vertices and sizes of cliques are given.