

Pseudo-Telepathy and Graph Colorings

Or How to Convince Your (Smart) Children of the Existence of Quantum Entanglement

Viktor Galliard ^{*} Stefan Wolf [†]

Abstract

In 1999, Brassard, Cleve, and Tapp showed that quantum entanglement allows for a phenomenon called pseudo-telepathy: Two separated parties are asked questions and respond in a way that seems possible only if they can communicate—but they cannot. The question was left open, however, for which parameters the phenomenon is impossible *without* quantum effects. We present a close connection between pseudo-telepathy and the problem of graph coloring and use this link to correct previous beliefs on the possibility of pseudo-telepathy. The studied question is of interest with respect to the design of a simple demonstration experiment showing the existence of quantum entanglement.

1 Pseudo-Telepathy and Quantum Entanglement

Consider the following game: Two parties Alice and Bob, who are not allowed or able to communicate with each other, are asked two separate questions. They win the game if they manage to respond to these questions such that the following simple condition is satisfied: Their answers have to be equal if and only if the questions were equal. Now, Alice and Bob, who are allowed to meet or exchange arbitrary information beforehand, could easily win by just repeating the questions asked. However, the game requires the answers to be shorter than the questions. More precisely, the “questions” asked to Alice and Bob are two N -bit strings v_A and v_B , respectively, for some $N = 2^n$, such that

$$d_H(v_A, v_B) \in \{0, N/2\},$$

where d_H is the Hamming distance of the two strings. The answers given by Alice and Bob are supposed to be $n (= \log N)$ -bit strings r_A and r_B with

$$r_A = r_B \iff v_A = v_B.$$

It has been shown that if N is large enough, this game cannot be won. More precisely, it was proven in [4], [6] that the amount of communication required between Alice and Bob for winning the game (with certainty) is of order $\Omega(N)$. Note, however, that this result is asymptotic and does not say anything about particular instances of the problem.

One reason why the described game of interest is the following. It was shown in [3] that if Alice and Bob are, prior to the question-and-answer phase of the game, allowed to exchange not only classical but also *quantum* information, they can win the game with certainty. More precisely, Alice and Bob need $n = \log N$ so-called EPR pairs [2]. The rest of this article does not require any knowledge in quantum mechanics or quantum information theory, so we do not have to go into detail here. An EPR pair are two possibly distant systems, for instance photons (where the property of interest is their polarization), who show a strange behavior, which cannot be explained classically, when measurements are carried out on them. Roughly spoken, the measurement results are both totally random but perfectly correlated

^{*}Untervaz, Switzerland. Email: math@galliard.ch. Supported by Canada’s NSERC and by ETH Zürich.

[†]Département d’Informatique et R.O., Université de Montréal, Montréal, QC, Canada H3C 3J7, email: wolf@iro.umontreal.ca. Supported by Canada’s NSERC.

among each other. It was shown in [2] that this behavior, often referred to as (maximal) *entanglement*, has no classical explanation (based on so-called hidden variables).

As shown in [3], the two described results together imply the price for perfectly simulating such quantum entanglement by classical communication: The amount of communication required for the classical simulation of k EPR pairs is of order $\Omega(2^k)$. For a single EPR pair for instance, 8 bits suffice. It is important to note that these results hold for the *perfect* simulation of quantum entanglement; in average, less communication is sufficient to approximate entangled states arbitrarily closely [5].

It is unsatisfactory that the lower bound on the classical communication is only asymptotic. If for instance a demonstration experiment is to be designed to convince an audience of the existence of quantum entanglement, it has to be known for which parameter N the game *cannot* be won *without* the exchange of classical information (and with which probability of failure).

This is a motivation for a further classical analysis of the pseudo-telepathy game. The questions addressed in the rest of this paper are the following: Is the pseudo-telepathy game related to another problem which is already well-studied? What is the smallest number N for which the game cannot be won without communication? The first question is addressed, and answered positively, in Section 2. The second question is, based on that, addressed in Section 3. It is shown that what was previously conjectured, namely that $N = 8$ is the smallest such game parameter, is not true.

2 Communication Complexity and Coloring Graphs

In this section we show a close relationship between the pseudo-telepathy game and the graph-coloring problem. More precisely, the question whether the game can be won or not, and if not, how much classical communication is necessary, is reduced to determining the chromatic number of certain graphs. We first define a generalized version of the game in terms of graphs.

Definition 1 Let G be an undirected graph with vertex set V and edge set $E \subseteq V^2$. (The fact that G is undirected means that $(v, v') \in E$ implies $(v', v) \in E$ for all $v, v' \in V$.) The *pseudo-telepathy game in G with answer length n and communication c* , denoted by $\text{PT}(G, n, c)$, is defined as follows. Two parties A and B are given vertices v_A and v_B (the *questions*), with respect to the condition that $v_A = v_B$ or $(v_A, v_B) \in E$. Then the parties are allowed to exchange at most c bits of communication (each bit in either direction). Then A and B are said to win the game $\text{PT}(G, n, c)$ if they can both generate an n -bit output r_A and r_B (the *answer*) with the property that $r_A = r_B$ holds if and only if $v_A = v_B$ does.

Lemma 1 Let $G = (V, E)$ be an undirected graph. Let $v, v' \in V$ with $(v, v') \notin E$. Let \overline{G} be the graph obtained from G by identifying the two (unconnected) vertices v and v' . More precisely, the vertex and edge sets of \overline{G} are

$$\begin{aligned} \overline{V} &:= (V \setminus \{v, v'\}) \cup \{\overline{v}\} \\ \overline{E} &:= (E \cap (V \setminus \{v, v'\})^2) \cup \bigcup_{\overline{v} \in V, (\tilde{v}, v) \in E \text{ or } (\tilde{v}, v') \in E} \{(\tilde{v}, \overline{v}), (\overline{v}, \tilde{v})\} \end{aligned}$$

Then $\text{PT}(\overline{G}, n, c)$ can be won if and only if $\text{PT}(G, n, c)$ can be won.

Proof. Assume first that $\text{PT}(G, n, c)$ can be won. We show that $\text{PT}(\overline{G}, n, c)$ can be won by the same protocol, where \overline{v} is treated as v . Let \overline{v}_A and \overline{v}_B be the questions asked to A and B , respectively. Clearly, the described protocol works well if $\overline{v}_A \neq \overline{v}$ and $\overline{v}_B \neq \overline{v}$. Assume $\overline{v}_A = \overline{v}_B = \overline{v}$. Then the protocol corresponds to the protocol for G with $v_A = v_B = v$, and A and B end up with the same answers. Let finally $\overline{v}_A = \overline{v}$, but $\overline{v}_B \neq \overline{v}$. Then the executed protocol corresponds to the one for G with $v_A = v$ and $v_B \neq v$, and hence ends up with different answers.

Let us now assume that $\text{PT}(\overline{G}, n, c)$ can be won. Then $\text{PT}(G, n, c)$ can be won by the same protocol, where v and v' are both treated as \overline{v} . The only critical case is $v_A \in \{v, v'\}$ and $v_B \in \{v, v'\}$. Here, A and B will end up with the same answers (since $\overline{v}_A = \overline{v}_B = \overline{v}$). This is always correct since $(v, v') \notin E$ implies $v_A = v_B$ in this case. \square

Let in the following $\chi(G)$ be the *chromatic number* of G , i.e., the minimal number of colors required for coloring the vertices of the graph in such a way that vertices which are connected by an edge have different colors.

Theorem 2 *Let $C_{\chi(G)}$ be the complete graph (i.e., every pair of vertices is connected) with $\chi(G)$ vertices. Then $\text{PT}(G, n, c)$ can be won if and only if $\text{PT}(C_{\chi(G)}, n, c)$ can be won.*

Proof. Let a coloring of G using $\chi(G)$ different colors be given. Then there exists a sequence

$$G_1, G_2, \dots, G_m$$

of graphs such that $G_1 = G$, $G_m = C_{\chi(G)}$, and G_{i+1} is obtained from G_i by identifying, in the sense of Lemma 1, two vertices of the same color (hence unconnected) for all $i = 1, \dots, m - 1$. Then Lemma 1 implies that $\text{PT}(G_i, n, c)$ can be simultaneously won for all i , or it cannot be won for all i . \square

Corollary 3 *Let G be a graph. Assume that $\text{PT}(G, n, c)$ can be won. Then*

$$c \geq \log_2 \chi(G) - n .$$

Proof. By Theorem 2, we can conclude first that $\text{PT}(C_{\chi(G)}, n, c)$ can be won. More specifically, we can assume that $\text{PT}(C_{\chi(G)}, n, c)$ can be won by a protocol which is entirely deterministic with respect to the behavior of both parties. (The reason is that the protocol must be successful with probability one, i.e., for *every single sequence of coin tosses* if it were probabilistic.) This implies that at any given point of the protocol, say after the i -th message has been sent, the space of pairs of questions (v_A, v_B) compatible with the communication is of the form $V_A^i \times V_B^i$. This can be seen by induction. Each message bit sent in one direction rules out, from the receiver's point of view, some of the questions the sender may have been asked, and is compatible with the others. Besides that, however, all combinations of questions asked to A and B remain possible.

Let $V_{\cap}^i := V_A^i \cap V_B^i$ be the overlap of the sets V_A^i and V_B^i at some point of the protocol. We now show the following two statements.

1. Assume that a single message bit is sent from one party to the other. Then, for at least one of the two possible values of this bit, we have

$$|V_{\cap}^{i+1}| \geq |V_{\cap}^i|/2 .$$

(Here, V_{\cap}^i and V_{\cap}^{i+1} are the overlap sets *before* and *after* the bit was sent, respectively.)

Proof. Assume that one message bit m is sent from A to B . Then

$$V_{\cap}^{i+1}(m = 0) \cup V_{\cap}^{i+1}(m = 1) = V_{\cap}^i ,$$

where $V_{\cap}^{i+1}(m = b)$ is the resulting overlap set, given that the bit m sent was equal to b .

2. If the set V_{\cap} is greater than 2^n after the communication between A and B , then the game cannot be won (without further communication).

Proof. Given that $|V_{\cap}| > 2^n$ at the end of the communication, there are at least two vertices $v, v' \in V_{\cap}$ with the property that A outputs the same answer for the questions $v_A = v$ and $v_A = v'$. Since $v_B = v$ and $v_B = v'$ are both possible, too, the resulting pair of answers cannot be correct in every case.

Since the initial set V_{\cap}^0 has size $\chi(G)$, we can conclude that at least

$$\log_2 \chi(G) - n$$

message bits must be sent in either direction for winning the game. \square

Corollary 4 *Let G be a graph, and let $c, n \in \mathbf{N}$ with $\log_2 \chi(G) - n \leq 0$ or*

$$c \geq \log_2 \chi(G) - n + 1 .$$

Then $\text{PT}(G, n, c)$ can be won.

Proof. Let us first assume that $n \geq \log_2 \chi(G)$. Then the game can be won by encoding the colors as n -bit strings. Here, the answer to a question, i.e., a vertex, is the encoding of its color.

Let now $c \geq \log_2 \chi(G) - n + 1$, hence also $c \geq \lceil \log_2 \chi(G) \rceil - n + 1$. Then $\text{PT}(C_{\chi(G)}, n, c)$ can be won as follows.

Assume that the vertices of the graph $C_{\chi(G)}$ are encoded as binary strings of length $\lceil \log_2 \chi(G) \rceil$. Given her question v_A , A sends the first

$$\lceil \log_2 \chi(G) \rceil - n + 1$$

bits of the encoding of v_A to B . A 's answer r_A are the last n bits of the encoding of v_A . Note that the two strings have an overlap of one bit; let b denote the value of this bit.

B on the other hand compares the first $\lceil \log_2 \chi(G) \rceil - n$ bits of his question v_B with the string received from A , but after discarding its last bit. Given that the compared strings are equal, his answer r_B are the last n bits of the encoding of his question v_B . Given that the strings are not equal however, Bob's answer is

$$r_B = (1 - b)00 \cdots 0$$

(i.e., the first bit of the string is the bit opposite to b , which is the first bit of A 's answer r_A ; hence the answers are different in this case (as they should be) since they differ in the first bit.

With this strategy, they always win the game. The corollary now follows from Theorem 2. \square

These results allow for analyzing the pseudo-telepathy game by determining the chromatic number of graphs. Unfortunately, this problem is, in its general formulation, NP-hard. The graphs that arise from the game as described in Section 1, however, are highly symmetric and, in addition, have been studied already. This will allow us to make statements about the game and, therefore, about how to design a demonstration experiment to prove the existence of quantum entanglement.

3 The Graph of Interest and its Properties

The graph corresponding to the pseudo-telepathy game as described in Section 1 is as follows.

Definition 2 Let $n \geq 1$, $N = 2^n$. The graph $G_N = (V_N, E_N)$ consists of the vertex set $V_N := \{0, 1\}^N$ and the edge set $E_N := \{(v, v') \mid v, v' \in V_N, d_H(v, v') = N/2\}$.

It is not difficult to see that for $N \geq 4$, the graph has two isomorphic connected components $V_{N,e}$ and $V_{N,o}$, consisting of the vertices with even and odd Hamming weight, respectively.

A lower bound on the chromatic number $\chi(G_N)$ of G_N can be obtained immediately from the size of a maximal clique (completely connected subgraph) of the graph. Such a clique is given by the vertices corresponding to the N codewords of a dual Hamming code.

Lemma 5 *For all $N = 2^n$, $n \geq 1$, we have*

$$\chi(G_N) \geq N . \tag{1}$$

Proof. First of all, it is clear that the size of every clique of G_N is a lower bound to its chromatic number since every vertex in this subgraph needs a different color. Secondly, the set of vertices

$$C := \{v \mid v = \bigoplus_{i=1}^{\log N} \lambda_i v_i, \lambda_i \in \{0, 1\}\} ,$$

where

$$\begin{aligned}
v_1 &= \underbrace{00 \cdots 0}_{N/2} \underbrace{11 \cdots 1}_{N/2} \\
v_2 &= \underbrace{00 \cdots 0}_{N/4} \underbrace{11 \cdots 1}_{N/4} \underbrace{00 \cdots 0}_{N/4} \underbrace{11 \cdots 1}_{N/4} \\
&\vdots \\
v_{\log N - 1} &= 001100110011 \cdots 0011 \\
v_{\log N} &= 010101010101 \cdots 0101,
\end{aligned}$$

forms a clique of size N since for all $v, v' \in C$, $v \neq v'$, we have $d_H(v, v') = N/2$. (This set of vertices, when the initial 0's are left away, corresponds to the dual Hamming code of length $N - 1$.) \square

The main question we are concerned with is for which N inequality (1) is strict; these are exactly the parameters N for which the pseudo-telepathy game cannot be won without any communication (according to Section 2). It has been previously known that for $N = 2$ and $N = 4$, equality holds in (1) (e.g., the game *can* be won); it has been believed, however, that for $N = 8$, inequality (1) is strict [3], [9]. The parallels introduced in Section 2 will allow us to show that this is wrong: For $N = 8$, the game can indeed be won.

Theorem 6 $\chi(G_8) = 8$.

Proof. Let $V_8 = V_{8,e} \cup V_{8,o}$ be the partition of the vertices into vertices with even and odd Hamming weights, respectively. Let

$$V_0 := \{0^8\} \cup \bigcup_{1 \leq i \leq 7} \{10^{i-1}10^{7-i}\}.$$

First, V_0 is an independent set since all pairs of elements have Hamming distance 2. The set

$$\overline{V_0} := \{v \in \{0, 1\}^n \mid \bar{v} \in V_0\}$$

(where \bar{v} is the bit-wise complement of the string v) is an independent set as well, and furthermore $V_0 \cup \overline{V_0} (\subseteq V_{8,e})$ is an independent set since for all $v \in V_0$, $v' \in \overline{V_0}$, $d_H(v, v') \in \{6, 8\}$. We have $|V_0 \cup \overline{V_0}| = 16$. Since $V_{8,e}$ and $V_{8,o}$ are isomorphic, we can find an independent set of the same size in $V_{8,o}$. The union C_0 of these two sets has 32 elements. We can now define 8 mutually disjoint independent sets C_0, C_1, \dots, C_7 by

$$C_{\lambda_0 + 2\lambda_1 + 4\lambda_2} := C_0 \oplus \lambda_0 \cdot 00001111 \oplus \lambda_1 \cdot 00110011 \oplus \lambda_2 \cdot 01010101$$

(where $\lambda_i \in \{0, 1\}$). These sets are mutually disjoint and each of them is an independent set (of size 32); all vertices of such a set can hence be given the same color. Thus $\chi(G_8) \leq 8$, and since we know that $\chi(G_8) \geq 8$ also holds (Lemma 5), the theorem is proven. \square

The following is now a consequence of Corollary 4 and Theorem 6.

Corollary 7 *The pseudo-telepathy game can be won (without communication) for $N = 8$.*

4 Conclusion and Open Problems

We have analyzed the so-called pseudo-telepathy game; in particular, we have shown its close relationship to the problem of coloring graphs. We have used this connection to show that what was previously believed, namely that the game cannot be won (without communication nor quantum entanglement) for the parameter $N = 8$, is not true.

Given the fact that for this parameter “pseudo-telepathy” is indeed possible (and hence unimpressive), the question arises whether $N = 16$ is the smallest number for which it is not. Investigations of this question, more precisely, on the corresponding graph, have been made in [7] based on graph-theoretical and combinatorial results generalized from [1]. The results strongly suggest (but leave the question open) that $\chi(G_{16}) > 16$. This would mean that repeated successful executions of the game for this parameter can be used as a simple demonstration of the existence of quantum entanglement (or of true telepathy).

It is important to note that the choice of a very large number for N , as may be suggested by the asymptotic result mentioned in Section 1, is not helpful in this context because the game can be won with success probability $1 - 1/N$ if both parties answer their question with a random hash value of it, using a predetermined random linear function mapping N bits to $\log N$ bits.

Acknowledgments

The authors thank Gilles Brassard, Nicolas Gisin, Chris Godsil, Penny Haxell, Mike Mosca, Renato Renner, Gordon Royle, and Alain Tapp for interesting discussions on the subject of this paper.

References

- [1] R. Ahlswede and H. Khachatrian, The complete intersection theorem for systems of finite sets, *European Journal of Combinatorics*, Vol. 18, pp. 128–136, 1997.
- [2] J. S. Bell, On the Einstein-Podolsky-Rosen paradox, *Physics*, Vol. 1, pp. 195–200, 1964.
- [3] G. Brassard, R. Cleve, and A. Tapp, The cost of exactly simulating quantum entanglement with classical communication, quant-ph/9901035, 1999.
- [4] H. Buhrman, R. Cleve, and A. Wigderson, Quantum vs. classical communication and computation, *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC 98)*, pp. 63–68, 1998.
- [5] N. Cerf, N. Gisin, and S. Massar, Classical teleportation of a quantum bit, *Phys. Rev. Lett.*, Vol. 84, No. 11, pp. 2521–2524, 2000. Also available at quant-ph/9906105, 1999.
- [6] P. Frankl and V. Rödl, Forbidden intersections, *Transactions of the American Mathematical Society*, Vol. 300, No. 1, pp. 259–286, 1987.
- [7] V. Galliard and S. Wolf, Classical pseudo-telepathy and coloring graphs, Tech. Rep., Department C&O, University of Waterloo, 2001. To appear.
- [8] S. Massar, D. Bacon, N. Cerf, and R. Cleve, Classical simulation of quantum entanglement without local hidden variables, quant-ph/0009088, 2000.
- [9] A. Tapp, personal communication, 2000.