Deterministic Quantum Non-Locality and Graph Colorings

Viktor Galliard[a,d], Alain Tapp[b], Stefan Wolf[c,d]

[a] *Computer Science Department, ETH Zürich, ETH Zentrum, CH-8092 Zürich, Switzerland.*
Supported by Galliard Research & Engineering GmbH, CH-7204 Untervaz, Switzerland.
galliardv@galliard-engineering.com.
[b] *Université de Montréal, Montréal, QC, Canada H3C 3J7.*
tappa@iro.umontreal.ca.
[c] *Faculty of Informatics, University of Lugano, CH-6904 Lugano, Switzerland.*
wolfs@usi.ch.
[d] *Supported by the Swiss National Science Foundation (SNF), project no. PP002–106655.*

Abstract

One of the most fascinating consequences of quantum theory are non-local correlations: Two – possibly distant – parts of a system can have a behavior under measurements unexplainable by shared information. A manifestation thereof is so-called *pseudo-telepathy*: Tasks that can be performed by two parties who share a quantum state, whereas classically, communication would be necessary to always succeed. We show that pseudo-telepathy games can often be modeled by graphs: The classical strategy to win the game is a coloring of this graph with a given number of colors. We discuss these parallels and study the class of graphs corresponding to the first two-party pseudo-telepathy game, proposed by Brassard, Cleve, and Tapp in 1999. This leads to a proof that the game indeed has the desired property.

Key words: Entanglement, non-local correlations, communication complexity

1. Entanglement-Based Games and Graphs

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

In a two-player pseudo-telepathy game, two separated players 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, for a pair of questions (x_A, x_B), the answers (y_A, y_B) have to be such that

$$(x_A, x_B, y_A, y_B) \in R_{XY} \subseteq \mathcal{X}_A \times \mathcal{X}_B \times \mathcal{Y}_A \times \mathcal{Y}_B \tag{1}$$

holds, where the game is defined by the relation R_{XY}. (Here, $\mathcal{X}_A$, $\mathcal{X}_B$, $\mathcal{Y}_A$, and $\mathcal{Y}_B$ stand of the ranges of possible questions to and answers from Alice and Bob, respectively.)

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.

2. Special Case: The Game by Brassard, Cleve, and Tapp

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 x_A and x_B, respectively, for some $N = 2^n$, such that

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

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 y_A and y_B with

$$y_A = y_B \Longleftrightarrow x_A = x_B\,.$$

Formally, according to (1),

$$\mathcal{X}_A = \mathcal{X}_B = \{0,1\}^{2^n}, \mathcal{Y}_A = \mathcal{Y}_B = \{0,1\}^n,$$

$$R_{XY}^{BCT} := \{(x_A, x_B, y_A, y_B) : (x_A = x_B \wedge y_A = y_B) \vee (d_H(x_a, x_b) = 2^{n-1} \wedge y_A \neq y_B)\}\,. \tag{2}$$

It has been shown that if N is large enough, this game cannot be won classically. 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 is of interest is 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 [3]. More precisely, Alice and Bob need $n = \log N$ so-called EPR pairs [1]. An EPR pair describes two possibly distant systems, for instance photons (where the property of interest is their polarization), which show a strange behavior when measurements are carried out on them. It was shown in [1] that this behavior, often referred to as (maximal) *entanglement*, has no classical explanation — based on so-called *hidden variables*. The rest of this article does not require any knowledge in quantum mechanics or quantum information theory, and we do not have to go into detail here. Our goal is, rather, a full *classical* analysis of the game.

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, one bit suffices [10]. It is important to note that this result holds

for the *perfect* simulation of quantum entanglement; in average, less communication is sufficient to approximate the entangled behavior of states arbitrarily precisely [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 what 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 has been 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 3. The second question is, based on that, treated in Section 4. It is shown that $N = 16$ is the smallest such game parameter [9].

3. Relating Communication and Coloring Graphs

Here we show a close relationship between the pseudo-telepathy game and a graph-coloring problem [8]. More precisely, the question whether the game can be won classically or not — and if not, how much classical communication is necessary — is reduced to determining the chromatic number of certain graphs. The chromatic number of a graph is the minimum number of different colors needed to assign to each vertex a color in such a way that adjacent vertices have different colors. We first define a generalized version of the game in terms of graphs. These games are often referred to as Deutsch-Jozsa games.

Definition 1. Let G be an undirected graph with vertex set V and edge set $E \subseteq V^2$. The *pseudo-telepathy game in G with answer length n and communication c*, denoted by $\mathrm{PT}(G, n, c)$, is defined as follows. Two parties A and B are given vertices v_A and v_B (the *questions*) satisfying 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 $\mathrm{PT}(G, n, c)$ if they can both generate an n-bit output r_A and r_B (the *answer*) with the property that $r_A = r_B$ if and only if $v_A = v_B$.

Let $\chi(G)$ 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.

Lemma 1 and Theorem 2 reduce the corresponding graph and show the relation between a game defined by a graph and the graph's chromatic number.

Lemma 1. *Let $G = (V, E)$ be an undirected graph with some 2^n-coloring where $|V| > 2^n$. Let $v, v' \in V$ with $(v, v') \notin E$ and having the same color. Let $\tilde{G}$ be the graph obtained from G by merging the two non-adjacent vertices v and v'. More precisely, the vertex and edge sets of $\tilde{G}$ are*

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

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

Proof. Assume first that $\mathrm{PT}(G, n, c)$ can be won. We show that $\mathrm{PT}(\tilde{G}, n, c)$ can be won by the same protocol, where $\tilde{v}$ is treated as v. Let $\tilde{v}_A$ and $\tilde{v}_B$ be the questions asked to A and B, respectively. Clearly, the described protocol works well if $\tilde{v}_A \neq \tilde{v}$ and $\tilde{v}_B \neq \tilde{v}$. Assume $\tilde{v}_A = \tilde{v}_B = \tilde{v}$. 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 $\tilde{v}_A = \tilde{v}$, but $\tilde{v}_B \neq \tilde{v}$. 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 $\mathrm{PT}(\tilde{G}, n, c)$ can be won, Then $\mathrm{PT}(G, n, c)$ can be won by the same protocol, where v and v' are both treated as $\tilde{v}$. 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 $\tilde{v}_A = \tilde{v}_B = \tilde{v}$). This is always correct since $(v, v') \notin E$ implies $v_A = v_B$ in this case. □

We have seen that the identification of vertices of the graph conserves the possibility of winning the corresponding pseudo-telepathy game.

To study the amount of classical communication required to win a game defined by on an arbitrary graph G, we show that in Theorem 2 that it is sufficient to consider the complete graph $C_{\chi(G)}$.

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

Proof. Given an minimal coloring of graph G with $\chi(G)$ colors, there exists a sequence

$$G_1, G_2, \ldots, G_m$$

of graphs with $G_1 = G$, $G_m = C_{\chi(G)}$, and G_{i+1} obtained from G_i by identifying, with the construction of Lemma 1, two vertices of the same color (they are, hence, unconnected) for all $i = 1, \ldots, m-1$. Then Lemma 1 implies that $\mathrm{PT}(G_j, n, c)$ can be simultaneously won for all $j \in \{1, \ldots, m\}$, or for all j it cannot be won.

□

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

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

Proof. By Theorem 2, we can conclude first that $\mathrm{PT}(C_{\chi(G)}, n, c)$ can be won. More specifically, we can assume that $\mathrm{PT}(C_{\chi(G)}, n, c)$ 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 for winning the game. □

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 $\mathrm{PT}(G, n, c)$ 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 $\mathrm{PT}(C_{\chi(G)}, n, c)$ 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 statement now follows from Theorem 2. □

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 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.

4. Analysis of the Game By Brassard, Cleve, and Tapp

The graph corresponding to the pseudo-telepathy game described in Section 2 is the following.

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 $E_N := \{(v,v') \,|\, v, v' \in V_N\,,\, d_H(v,v') = N/2\}$.

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*

$$\chi(G_N) \geq N\,. \tag{3}$$

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

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

where

$$v_1 \quad = \quad \underbrace{00\cdots 0}_{N/2}\underbrace{11\cdots 1}_{N/2}$$

$$
\begin{aligned}
v_2 &= \underbrace{00\cdots0}_{N/4}\underbrace{11\cdots1}_{N/4}\underbrace{00\cdots0}_{N/4}\underbrace{11\cdots1}_{N/4} \\
&\vdots \\
v_{\log N-1} &= 001100110011\cdots0011 \\
v_{\log N} &= 010101010101\cdots0101\,,
\end{aligned}
$$

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 $N-1$.) □

The main question we are concerned with is for which N inequality (3) 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 is known that for $N = 2$ and $N = 4$, equality holds in (3) (e.g., the game *can* be won); it has been believed, however, that for $N = 8$, inequality (3) is strict [3]. The parallels introduced in Section 1 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

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

(where $\overline{v}$ 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 $C_0, C_1, \ldots, C_7$ 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: the vectors C_0, 00001111, 00110011 and 01010101 are linearly independent in the vector space with vectors $x \in \{0,1\}^n$ and inner product $\oplus$ of the vectors defined by the bitwise *XOR*. Therefore, any linear combination thereof is linearly independent as well. Furthermore, each of this 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 statement is proven. □

Corollary 7. *[8] The pseudo-telepathy game can be won classically without communication for $N \in \{2, 4, 8\}$.*

Proof. For G_N with $N \in \{2, 4, 8\}$, $\chi(G_N) = n$ (detail of $\chi(G_N) = N$ for $N \in \{2, 4, 8\}$ proof see [9], Section 3.). The statement is a consequence of Corollary 4 and Theorem 6. □

In [7] is has been conjectured what the structure of maximum independents sets is for G_N with $N = 2^n$, especially for more interesting cases $N > 8$. We define a maximal independent set of G in a generalized way according to [2] as follows:

Definition 3. *An independent set V_{ind} of a graph $G(V, E)$ is maximal if and only if*

$$\forall v' \in V \setminus V_{ind} : \exists v \in V_{ind} : (v, v') \in E.$$

Definition 4. *Let $\binom{[n]}{k}$ be the set of subsets of $[n] := [1, \ldots, n]$ consisting of elements with cardinality k. For even k with $t + 2i \geq 0$ and $0 \leq i \leq (n - t)/2$, let $\mathcal{F}_{t,i}^{n,k}$ be the following set:*

$$\mathcal{F}_{t,i}^{n,k} = \left\{ F \in \binom{[n]}{k} : |F \cap [t + 2i]| \geq t + i \right\}. \tag{4}$$

Moreover, let $[t + 2i] = \{1, \ldots, t + 2i\}$ denote the intersection area of size $t + 2i$.

Note that in contrast to [2], t will be negative for some sets $\mathcal{F}_{t,i}^{n,k}$. In their work, Ahlswede and Khachatrian proved that $\mathcal{F}_{t,i}^{n,k}$ is a maximal, t-intersecting subset of $\binom{[n]}{k}$ for a specific i, depending on n. We use the intersection-property to determine an independent set in $G_n(V, E)$.
First let us consider the vertices with Hamming weight less than $n/2$ (again in the subgraph with vertex set V_{even}). For $\tilde{n} \geq 3$, let

$$\begin{aligned} \mathcal{V}_{ind}^{<\frac{n}{2}} &= \mathcal{F}^{n,0}_{-\frac{n}{4}-1,\frac{n}{4}+1} \cup \mathcal{F}^{n,2}_{-\frac{n}{4}+3,\frac{n}{4}-2} \cup \ldots \\ &\quad \cup \mathcal{F}^{n,\frac{n}{2}-4}_{\frac{n}{4}-3,1} \cup \mathcal{F}^{n,\frac{n}{2}-2}_{\frac{n}{4}-1,0} \\ &= \bigcup_{l=0}^{\frac{n}{4}-1} \mathcal{F}^{n,2l}_{-c_n+2l,c_n-l} \end{aligned} \tag{5}$$

be a subset in the subgraph of $G_n(V, E)$ with vertex set $V_{even}^{<\frac{n}{2}} = \{v \in V_{even} : W_H(v) < n/2\}$, for $c_n = n/4 - 1$.

Define further the inverse set of $\mathcal{F}_{t,i}^{n,k}$ as the set $\overline{\mathcal{F}_{t,i}^{n,k}}$ with elements $\left\{A \in \binom{[n]}{n-k} : \overline{A} \in \mathcal{F}_{t,i}^{n,k}\right\}$. Now, let us determine a maximal independent set, with $\mathcal{V}_{ind}^{>\frac{n}{2}}$ analogously defined as set (5).

Theorem 8. *For $\tilde{n} \geq 3$, the set*

$$\begin{aligned} \mathcal{V}_{ind} &= \mathcal{V}_{ind}^{<\frac{n}{2}} \cup \mathcal{V}_{ind}^{>\frac{n}{2}} \\ &= \bigcup_{l=0}^{\frac{n}{4}-1} (\mathcal{F}^{n,2l}_{-c_n+2l,c_n-l} \cup \overline{\mathcal{F}^{n,2l}_{-c_n+2l,c_n-l}}) \end{aligned} \tag{6}$$

is a maximal independent set of $G_n(V_{even}, E)$ *for* $c_n = n/4 - 1$.

To prove Theorem 8, we examine first the intersection properties of its subsets in the following lemmas.

Lemma 9. *For* $0 \leq l \leq \frac{n}{4} - 1$, $\mathcal{F}^{n,2l}_{-c_n+2l,c_n-l}$ *is an independent set.*

Proof. We have to consider only sets with vertices with Hamming weight $2l \geq n/4$, since for other sets, the cardinality of the symmetric difference $(A \cup B \setminus A \cap B)$ is at most $n/2 - 2$. For the remaining cases where $A, B \in \mathcal{F}^{n,2l}_{-c_n+2l,c_n-l}$ and $l \geq n/8$, we have $|A \cap B| \geq -c_n + 2l = -n/4 + 1 + 2l$ because of Definition 4, and, the Hamming distance of the corresponding codewords is at most $2(2l - (-c_n + 2l)) = n/2 - 2$, and hence, independence follows as well. □

Lemma 10. *For all* $l, l' \in \{0, \ldots, \frac{n}{4} - 1\}$, $\mathcal{F}^{n,2l}_{-c_n+2l,c_n-l} \cup \mathcal{F}^{n,2l'}_{-c_n+2l',c_n-l'}$ *is an independent set.*

Proof. First note that in set (6), $t + 2i = (-c_n + 2l) + 2(c_n - l)$ is equal to $c_n = n/4 - 1$ and, therefore, the size of the intersection area is $n/4 - 1$ for all subsets. Consider $l, l' \in \{0, \ldots, n/4 - 1\}$, $A \in \mathcal{F}^{n,2l}_{-c_n+2l,c_n-l}$ and $B \in \mathcal{F}^{n,2l'}_{-c_n+2l',c_n-l'}$.

For $2l + 2l' < n/2$**:** Again, the cardinality of the symmetric difference is less than $n/2$, and the union of the sets is independent.

For $2l + 2l' \geq n/2$**:** We consider the intersection between A and B in the intersection area. As a consequence of Definition 4, we have $|A \cap [n/4 - 1]| \geq l$ and $|B \cap [n/4 - 1]| \geq l'$, therefore, A and B will be at least $(l + l' - (n/4 - 1))$-intersection (Inequality (7)). Since we consider the cases where $2l + 2l' \geq n/2$, we have $l + l' \geq n/4$ (Inequality (8)), and the symmetric difference between A and B is the following:

$$\begin{aligned} |A \cup B \setminus A \cap B| &\leq |A| + |B| - 2\left(l + l' - \left(\frac{n}{4} - 1\right)\right) && (7) \\ &\leq 2l + 2l' - 2\left(\frac{n}{4} - \left(\frac{n}{4} - 1\right)\right) && (8) \\ &= \frac{n}{2} - 2\ . \end{aligned}$$

Since this holds for all such A and B, the union set is independent, and the lemma follows. □

Lemma 11. *If* V_{ind} *is an independent set and* $v \in V_{ind}$*, then* $V_{ind} \cup \overline{v}$ *is an independent set as well.*

Proof. If V_{ind} is an independent set and $v \in V_{ind}$, then for all $v' \in V_{ind} \setminus \{v\}$, $D_H(v, v') \neq n/2$. Generally $\forall u, w \in \{0,1\}^n : D_H(u, w) = n - D_H(u, \overline{w})$ holds and, hence, for all $v' \in V_{ind} \setminus \{v\}$ is $D_H(\overline{v}, v') = n - D_H(v, v') \neq n/2$, and the proof is complete. □

Proof of Theorem 8. Independence follows directly from Lemmas 9, 10, and 11. We prove that the set is maximal by contradiction. Suppose V_{ind} is not maximal, then by Definition 3, there must exist a vertex $v \in V_{even} \setminus V_{ind}$, such that $V_{ind} \cup \{v\}$ is still an independent set. Since $\mathcal{F}^{n,0}_{-\frac{n}{4}-1,\frac{n}{4}-1} = \{0^n\} \subset V_{ind}$, $W_H(v) \neq n/2$. Furthermore $W_H(v) \notin \{0, 2, \ldots, n/2-2, n/2+2, \ldots, n-2, n\}$, because $\mathcal{F}^{n,2l}_{-c_n+2l,c_n-l}$ are maximal by definition. □

In order to find a lower bound on the chromatic number of such graphs, maximum independent sets allow to find such a bound. Now, we *assume* that $V^*_{ind} = V_{ind}$ as defined in Equality (6) is a maximum independent set $G_n(V_{even}, E)$. The size of V^*_{ind} for $2^{\tilde{n}} = n \geq 8$ is

$$\begin{aligned} |V^*_{ind}| &= 2\sum_{l=0}^{\frac{n}{8}-1}\sum_{m=0}^{l}\binom{\frac{n}{4}-1}{l+m}\binom{\frac{3n}{4}+1}{m} + \\ & \quad 2\sum_{l=0}^{\frac{n}{8}-1}\sum_{m=0}^{l}\binom{\frac{n}{4}-1}{\frac{n}{4}-1-l}\binom{\frac{3n}{4}-1}{\frac{n}{4}-1-l-m}. \end{aligned} \tag{9}$$

Since the chromatic number $\chi(G_n) \geq n(G_n)/\alpha(G_n)$, and we *assume* that V^*_{ind} is a maximum independent set, we have a lower bound on the chromatic number, namely for $N = 16$, $\chi(G_{16}) \geq 28$. In 2006, the conjecture (9) could be proven [17] for the case $N = 16$ and it is assumed that for the case $N = 32$ it holds too, see Section 5.

5. Pseudo-Telepathy for $N \geq 16$

In 2003, we could prove that G_{16} yields a pseudo-telepathy game [9].

Theorem 12. *For the graph G_N,*

$$\chi(G_{16}) > 16 \ .$$

In order to prove Theorem 12, we use the well-known fact that for any graph G

$$\chi(G) \geq \frac{|V(G)|}{M}$$

holds if M is an upper bound on the size of all independent sets of the graph G. An independent set is a set of vertices which are pairwise unconnected, and clearly, any set of vertices of the same color in a coloring fulfills this. We found an upper bound $M_{16} \leq 3912$ for maximum independent sets in G_{16} [3]. This yielded a lower bound 17 for the chromatic number $\chi(G_{16})$. This was the first proof that the Brassard *et al.* game for $N = 16$ is indeed a pseudo-telepathy game.

In 2005, Godsil and Newman [14] proved — by considering the Delsarte-Hoffman bound, maximum-cliques, and a recursive construction — that $\chi(G_N) > N$ with $N = 2^n$

for all $N \geq 16$. At the same time Klerk and Pasechnik could prove with semi-definite programming that for $N = 16$ our conjecture [7] is indeed true [17]. They also assume that the case $N = 32$ is true (which Newman [11] in his PhD thesis in 2004 suggested to be wrong). In the same year, Avis *et al.* [15] found a proof using quantum Fourier transform instead of Hadamard transformation as used in [3] to win the game on the graph G_{12}. They use a well-known combinatorial result by Frankl and Rödl, where they show that the game G_{12} is a pseudo-telepathy game, too. They also define the quantum chromatic number of a graph in this context.

In 2006, Cameron, Newman, Montanaro, Severini, and Winter [16] formally investigated the quantum chromatic number of a graph for different types of graphs.

6. Concluding Remarks

We have considered *pseudo-telepathy games*, which are a manifestation of non-locality in a semi-deterministic fashion: The players share quantum states, the games success probability is 1. We have shown that for a large class of games, classical strategies can be modeled by colorings of certain graphs. Proving the existence of pseudo-telepathy games can, thus, lead to well-studied problems. For instance, these parallels have led to a thorough analysis [11], [12], [13], [14], [15], [16], [17] of the class of games by Brassard, Cleve, and Tapp [3]. Crucial and central questions in the context of pseudo-telepathy games remain open: Which quantum state allow for pseudo-telepathy? For instance, it has been shown [12] that one single EPR-pair does not suffice for pseudo-telepathy. What is, for games using a given state, the minimal classical success probability that can be reached using less communication than required (i.e., the maximal separation between classical versus quantum strategies)?

References

[1] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox", *Physics*, Vol. 1, pp. 195–200, 1964.

[2] R. Ahlswede and H. Khachatrian, "The Complete Intersection Theorem for Systems of Finite Sets", *European Journal of Combinatorics*, Vol. 18, pp. 128-136, 1997

[3] 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.

[4] H. Buhrman, R. Cleve, and A. Widgerson, "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.

[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, "Classical pseudo-telepathy and coloring graphs", Diploma thesis, ETH Zurich, 2001. Available at `http://math.galliard.ch`.

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

[9] A. Tapp, V. Galliard and S. Wolf, "The Impossibility of Pseudo-Telepathy Without Quantum Entanglement", *Proceedings of ISIT 2003*, 2003.

[10] D. Bacon, B. F. Toner, "Communication Cost of Simulating Bell Correlations", *Physical Review Letter*, Vol. 91, No. 18, 1999.

[11] M. W. Newman, "Independent Sets and Eigenspaces", PhD thesis, University of Waterloo, 2004. http://etd.uwaterloo.ca/etd/mwnewman2004.pdf

[12] G. Brassard, A. A. Méthot, A. Tapp, "Minimum entangled state dimension required for pseudo-telepathy", *Quantum Information and Computation (QIC)*, Vol. 5(4,5), pp. 275-284, 2005.
[13] J. Barrett, L. Hardy, A. Kent, "No Signaling and Quantum Key Distribution", *Physical Review Letter*, Vol. 95, 010503, 2005.
[14] C. D. Godsil, M. W. Newman, "Coloring an Orthogonality Graph", *Journal on Discrete Mathematics*, Vol. 2, pp. 683-692, 2008.
[15] D. Avis, J. Hasegawa, Y. Kikuchi, Y. Sasaki, "A quantum protocol to win the graph coloring game on all Hadamard graphs", *IEICE-Tran Fund Elec, Comm & Comp Sci*, Vol. E89-A, N. 5, pp. 1378-1381, 2006.
[16] P. J. Cameron, A. Montanaro, M. W. Newman, S. Severini, A. Winter, "On the quantum chromatic number of a graph", *the electronic journal of combinatorics 14*, #R8, 2007.
[17] E. de Klerk, D. V. Pasechnik, "A note on the stability number of an orthogonality graph", *European Journal of Combinatorics*, pp. 1971-1979, 2006.