Towards Characterizing the Non-Locality of Entangled Quantum States

Renato Renner and Stefan Wolf

October, 2002

Abstract

The behavior of entangled quantum systems can generally not be explained as being determined by purely classical shared randomness. In the first part of this paper, we propose a simple game for n players demonstrating this non-local property of quantum mechanics: While, on the one hand, it is immediately clear that classical players will lose the game with substantial probability, it can, on the other hand, always be won by players sharing an entangled quantum state. The simplicity of the classical analysis of our game contrasts the often quite involved analysis of previously proposed examples of this type.

In the second part, aiming at a quantitative characterization of the non-locality of an n-partite quantum state $|\Psi\rangle$, we consider a general class of n-player games, where the amount of communication between certain (randomly chosen) groups of players is measured. Comparing the communication needed for both classical players and quantum players (initially sharing a state $|\Psi\rangle$) to win such a game, a new type of separation result is obtained. In particular, we show that, in order to simulate two separated qubits of an n-partite GHZ state, at least $\Omega(\log \log n)$ bits of information are required.

1 Introduction

1.1 Quantum Entanglement vs. Classical Correlation

Consider an entangled quantum state shared between n parties, each belonging to a separate, dynamically isolated system.[1] It is a known fact of quantum mechanics that entanglement can not be used to achieve communication, i.e., no information can be exchanged between these parties. Nevertheless, according to Bell's well known theorem [2], the outcomes of local measurements in the systems are generally correlated in a non-classical way. This means that the (classical) measurement outcomes can *not* be simulated by parties only sharing classical information instead of quantum entanglement. Consequently, albeit not allowing for communication, a shared quantum state might help the n parties to accomplish certain tasks.

Aiming at understanding the nature of quantum entanglement, it is instructive to study simple examples of such tasks. To this end, we will consider *games* between n collaborating *players* which, in order to win, must generate certain outputs (possibly depending on a query). The game is *won* if their outputs satisfy a given condition. To generate their answers, the players are allowed to perform arbitrary local (quantum) computations (in particular, they are computationally unbounded) while the communication between them is subject to restrictions.

It turns out that there are games which can always be won by players sharing an entangled quantum state, while any classical strategy to win fails with some positive probability. They are

[1] One often considers systems which are spatially separated (after the common quantum state has been prepared), such that, according to the theory of relativity, there is no causal connection between any two events of interest belonging to different systems.

often called *pseudo-telepathy games* since the behavior of successful players can not be explained classically without assuming some hidden extra communication between them. A nice example for such a game has been presented in [3] where two collaborating players must answer a query in a somehow correlated way without being allowed to communicate.

In Section 2, we propose another particularly simple game of this type involving $n \geq 5$ collaborating players: Two randomly picked players receive a bit b (being chosen by the remaining $n-2$ players) which they can either flip or leave unchanged. The game is won if the two players, without being allowed to communicate (in particular, none of them knows who the other one is), behave differently, meaning that *exactly* one of them flips the bit b. Obviously, there is no classical strategy for winning the game with certainty. Indeed, a simple argument (see Section 2.2) shows that the probability to lose is substantial (roughly $1/4$ for n large). This stands in contrast to other similar games, where the classical analysis is often quite involved or where only asymptotic results are proven.[2] On the other hand, our game can be won with certainty by players initially sharing a GHZ state (Section 2.3).

1.2 Non-Local Information

An n-partite quantum state $|\Psi\rangle$ can be seen as a resource consisting of n components, each of them taking a classical input (the measurement basis) and generating a classical output (the outcome of the measurement performed on the respective part part of $|\Psi\rangle$). As described above, such a resource might be more powerful than its classical counterpart, i.e., n separated components sharing purely classical information. This non-classical property of quantum states is often called *non-locality* or *non-local information* of $|\Psi\rangle$.

The non-local information of an n-partite quantum state $|\Psi\rangle$ over n subsystems can be characterized by the minimal amount of communication between n separated classical systems needed for simulating the behavior of the quantum subsystems. While, in general, it is not clear how to determine this communication, it turns out that the games mentioned in the previous section are useful to find certain bounds: Consider a game which can always be won by players sharing the quantum state $|\Psi\rangle$. The non-local information of $|\Psi\rangle$ is then lower bounded by the minimal *additional* communication being necessary for classical players to win this game.

To obtain a *real-valued measure* for the non-local information of in a state $|\Psi\rangle$, the communication needed for its simulation has to be quantified. This can be done in several ways, but any concrete measure only exhibits certain aspects of this communication, and, consequently, does not fully characterize the non-local information contained in $|\Psi\rangle$. It thus seems that, in order to understand the nature of non-locality, it is worth considering different types of such measures.

One possibility is to rely on the definition of communication complexity introduced by Yao [14]. In this setting, the communication between *two* parties is simply characterized by the number of bits exchanged between them. In a generalization to $n > 2$ parties, any message sent by a player is considered as being broadcasted, i.e., a bit sent to all players only counts once. Cleve and Buhrman [8] were the first to propose an analysis of entanglement based on this communication model. It could be shown [7] that the *communication complexity of functions* (which can be seen as the communication necessary to win a certain game[3]) is generally larger for purely classical players than for players sharing entangled quantum states. In a variety of papers, e.g., [1, 5, 6, 13, 7] (see [7] or [4] for a survey), the communication complexity for both the quantum and the classical case, and in particular the gap between them, has been studied extensively.

[2] E.g., for the mentioned two-player game from [3], the probability to lose has been shown (based on graph-theoretical results) to be positive, but no lower bound for this probability is known yet (cf. [10, 9]).

[3] Let f be a function of n variables. The communication complexity of f is defined as the minimal amount of communication necessary for n players, each holding one input variable, to compute the value of f. The setting thus corresponds to a game which is won if each player outputs the correct value of f.

In this paper, we derive a slightly different type of separation results. The idea is to not only consider the overall entanglement of a quantum state, but also the non-local information contained in certain of its parts. For instance, given a state $|\Psi\rangle$ defined on n subsystems, one might be interested in the non-local correlation between any two of the subsystems and, additionally, the dependence between this correlation from the information contained in the other $n-2$ subsystems.[4]

Our results are, similar to the mentioned results based on Yao's model, derived from an analysis of the communication necessary to win certain games. This communication is however quantified in a different way: Instead of considering all messages exchanged between the players, only bits transmitted between certain groups of players are counted (ignoring all communication within these groups).

This concept is introduced more formally in Section 3. As an example, we show that, in order to win the n-player game from Section 2 classically, the amount of information that the two chosen players must receive is at least $\Omega(\log\log n)$ bits (Section 3.2). This is in contrast to the quantum case where one bit always suffices, given that the n players share a GHZ state. Consequently, to simulate local measurements on each of two arbitrary qubits of an n-partite GHZ state, $\Omega(\log\log n)$ bits of additional information are needed. Note that this amount can be arbitrarily large (for large n), while the two simulated systems are both two-dimensional.

To obtain even stronger separation results, we propose a generalized version of the game from Section 2. It is shown (Section 3.4) that the number of bits which has to be exchanged between n classical players in order to win this generalized game is at least $\Omega(\log n)$. On the other hand, if the players are allowed to share a GHZ state, one bit of communication still suffices.

2 A Simple Pseudo-Telepathy Game

2.1 The Game and Its Rules

Consider the following game $\mathcal{G}_n^s$ involving $n \geq 5$ collaborating players $P_1, \ldots, P_n$. First, two of the players are chosen randomly in such a way that neither of them knows who the other one is. (The non-chosen, remaining, $n-2$ players can be allowed to know which pair of players was chosen.) In the following, we will (without loss of generality) call the two chosen players P_1 and P_2.

The remaining players are now allowed to communicate and generate one "hint" bit b, which they say out loud (in particular, P_1 and P_2 can hear the bit). The chosen players P_1 and P_2 must then independently (i.e., no communication between them is allowed) generate a bit b_1 and b_2, respectively. The game is won simply if $b_1 \neq b_2$.

We will show that this game can be won with probability at most (roughly) 75% classically (if n is large enough), but with probability 1 (for any value of n) if the players can share quantum information.

2.2 Classical Analysis

Let us first consider a classical setting where the players rely on arbitrary *classical* (but no quantum) information which might have been shared during an initialization phase (before the start of the game).

Each player has a fixed strategy defining his behavior for the case he is chosen. While this strategy might in general be probabilistic, i.e., depend on some randomness, we can, without loss

[4]This is motivated by classical information-theoretic measures: Given n random variables $X_1, \ldots, X_n$, one usually is not only interested in the overall correlation between them, but also in the correlation between two random variables (the mutual information $I(X_i; X_j)$), possibly conditioned on a third one (the conditional mutual information $I(X_i; X_j | X_k)$).

of generality, assume that this randomness is fixed before the game starts. This means that by the time the player is chosen, his strategy is deterministic.

Once a player is chosen, the only information he gets is the hint bit b. For any given (deterministic) strategy, this bit b thus completely determines his output. Obviously, there exist exactly *four* possible strategies, namely to output 0, 1, b, or $\overline{b}$ (where $\overline{b}$ denotes the complement of b).

If the strategies of the chosen players are the same, they will clearly output the same bit and the game is lost. (Otherwise, if their strategies are different and if the remaining players know these strategies, they can always win.) Finding the minimal probability of losing the game thus amounts to determining the minimal probability of the event that two players with the *same* strategy (where four strategies are possible) are picked.

For $n = 4k + r$ players (where k, r are integers, $0 < k$, and $0 \leq r < 4$), the probability of this event is at least

$$p(n) = (4 - r) \cdot \frac{k}{n} \cdot \frac{k-1}{n-1} + r \cdot \frac{k+1}{n} \cdot \frac{k}{n-1} \ .$$

We have for instance $p(5) = 1/10$, $p(8) = 1/7$, and $p(n) \to 1/4$ for $n \to \infty$.

2.3 A Winning Strategy for Quantum Players

We will now show that the game can be won *with certainty* if the players can not only share classical information, but are additionally allowed to store a quantum state which is generated and shared before the game starts. (During the game, the players are only allowed to process the quantum information locally, i.e., an external observer would not be able to detect that the players follow a quantum strategy.)

Assume that each player P_i (for $i = 1, \ldots, n$) controls a two-dimensional subspace $\mathcal{H}_i$ of a quantum system $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$. Let $\{|e_0\rangle, |e_1\rangle\}$ be an orthonormal basis of $\mathcal{H}_i$ (for $i = 1, \ldots, n$). The diagonal and the circular basis of $\mathcal{H}_i$ are then given by the vectors

$$|f_0\rangle := \frac{1}{\sqrt{2}}(|e_0\rangle + |e_1\rangle) \qquad\qquad |f_1\rangle := \frac{1}{\sqrt{2}}(|e_0\rangle - |e_1\rangle) \tag{1}$$

and

$$|g_0\rangle := \frac{1}{\sqrt{2}}(|e_0\rangle + i|e_1\rangle) \qquad\qquad |g_1\rangle := \frac{1}{\sqrt{2}}(|e_0\rangle - i|e_1\rangle), \tag{2}$$

respectively.

The quantum strategy to win the game is the following: The players start with a so called GHZ state (see [11, 12])

$$|\Phi\rangle := \frac{1}{\sqrt{2}}(\underbrace{|e_0\rangle \otimes \cdots \otimes |e_0\rangle}_{n \text{ times}} + \underbrace{|e_1\rangle \otimes \cdots \otimes |e_1\rangle}_{n \text{ times}}) \tag{3}$$

(being prepared before the start of the game). During the game, after the two players have been randomly chosen, the remaining players first measure their subsystems with respect to the diagonal basis $\{|f_0\rangle, |f_1\rangle\}$ and determine the number k of players having the measurement outcome $|f_1\rangle$. The parity of k is then announced to the chosen players as hint bit b, i.e., $b \equiv k \pmod 2$.

Depending on this hint b, each of the chosen players measures his subsystem in either the diagonal basis $\{|f_0\rangle, |f_1\rangle\}$ (if $b = 1$) or the circular basis $\{|g_0\rangle, |g_1\rangle\}$ (if $b = 0$). His output is then a bit indicating his measurement result (e.g., 0 for $|f_0\rangle$ or $|g_0\rangle$, and 1 otherwise).

In order to prove that, following this strategy, the players always win the game, it suffices to verify that the measurement outcomes of the chosen players (let them again be called P_1 and P_2) are always different. Using the diagonal basis for the subsystems $\mathcal{H}_3, \ldots, \mathcal{H}_n$, the players' initial state $|\Phi\rangle$ can be written as

$$|\Phi\rangle = 2^{-\frac{n-1}{2}} \Big(|e_0\rangle \otimes |e_0\rangle \otimes (|f_0\rangle + |f_1\rangle) \otimes \cdots \otimes (|f_0\rangle + |f_1\rangle) + \underbrace{|e_1\rangle \otimes |e_1\rangle}_{\in \mathcal{H}_1 \otimes \mathcal{H}_2} \otimes \underbrace{(|f_0\rangle - |f_1\rangle) \otimes \cdots \otimes (|f_0\rangle - |f_1\rangle)}_{\in \mathcal{H}_3 \otimes \cdots \otimes \mathcal{H}_n} \Big).$$

Thus, obviously, the measurements performed by the remaining players $P_3, \ldots, P_n$, getting outcomes $|f_{m_3}\rangle, \ldots, |f_{m_n}\rangle$, respectively, project the state $|\Phi\rangle$ to

$$|\Phi_{m_3,\ldots,m_n}\rangle = \frac{1}{\sqrt{2}} \Big(|e_0\rangle \otimes |e_0\rangle + (-1)^{\sum_{i=3}^n m_i} |e_1\rangle \otimes |e_1\rangle \Big) \otimes |f_{m_3}\rangle \otimes \cdots \otimes |f_{m_n}\rangle.$$

Note that the exponent $\sum_{i=3}^n m_i$ can be replaced by the hint bit b. We are thus in one of the following situations:

(a) The subsystem $\mathcal{H}_1 \otimes \mathcal{H}_2$ of P_1 and P_2 is in the state

$$|\phi^+\rangle = \frac{1}{\sqrt{2}} (|e_0\rangle \otimes |e_0\rangle + |e_1\rangle \otimes |e_1\rangle) \in \mathcal{H}_1 \otimes \mathcal{H}_2$$

and the hint bit is $b = 0$.

(b) The subsystem $\mathcal{H}_1 \otimes \mathcal{H}_2$ is in the state

$$|\phi^-\rangle = \frac{1}{\sqrt{2}} (|e_0\rangle \otimes |e_0\rangle - |e_1\rangle \otimes |e_1\rangle) \in \mathcal{H}_1 \otimes \mathcal{H}_2.$$

and $b = 1$.

Rewriting these states in terms of the measurement bases of P_1 and P_2 (which according to the described strategy depend on b) we get

$$\begin{aligned} |\phi^+\rangle &= \frac{1}{\sqrt{2}} (|g_0\rangle \otimes |g_1\rangle + |g_1\rangle \otimes |g_0\rangle) \\ |\phi^-\rangle &= \frac{1}{\sqrt{2}} (|f_0\rangle \otimes |f_1\rangle + |f_1\rangle \otimes |f_0\rangle). \end{aligned}$$

Consequently, in both cases, the measurement outcomes of P_1 and P_2 are always different, which concludes the proof.

3 Quantifying Non-Local Information

As described in Section 1.2, in order to characterize the non-local information of an n-partite quantum state $|\Psi\rangle$ in terms of communication complexity, a measure to quantify the communication between n systems is required. We will introduce a notion of communication complexity with respect to certain partitionings of the systems into groups, where only the communication between these groups is counted.

This is formalized in terms of games between n players. A game is a specification of both the partitioning of the players into groups, and a task which has to be accomplished by the players (Section 3.1). The group broadcast complexity of a game is then defined as the minimal amount of inter-group communication needed for the players to win the game (Section 3.2). The comparison of the group broadcast complexity of a game for classical and for quantum players will finally lead to a new type of separation results (Section 3.3 and 3.4).

3.1 Games and Players

A *game $\mathcal{G}_n$ for n players* is defined by a probability distribution over triples (σ, q, W) where σ describes a *partitioning of the players* into groups, q a *query* to be given as input to the players, and W a *set of allowed answers*. Formally, σ is an m-tuple $(G_1, \ldots, G_m)$ (where $m \in \mathbb{N}$ is the number of groups) of disjoint sets $G_k \subseteq \{1, \ldots, n\}$ such that $\cup_k G_k = \{1, \ldots, n\}$, q is an m-tuple of bitstrings, and W is a set of m-tuples of bitstrings.

The *players* $P_1, \ldots, P_n$ are arbitrary, possibly probabilistic, information-processing systems having an internal state. On each new input, a player generates an output depending on this input (and possibly all previous inputs) and his internal state.

We will distinguish between two different settings: In the *classical* setting, the players are completely classical systems. In this case, the initial values of their internal states $R_1, \ldots, R_n$ (when the game starts) are given by a joint probability distribution $P_{R_1 \cdots R_n}$ (in particular, the internal states of the players might initially be correlated). An n-tuple of players together with the probability distribution is called *classical strategy* τ_{cl}.

In the *quantum* setting, the internal state of a player P_i additionally contains quantum information specified by the state of a quantum system $\mathcal{H}_i$. The player's inputs and outputs are still classical, whereby the latter might depend on the (classical) outcomes of measurements performed on $\mathcal{H}_i$. Before the start of the game, the quantum systems $\mathcal{H}_i$ are initialized with a quantum state $|\Psi\rangle \in \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ (such that, in general, there is entanglement between the players' internal states). An n-tuple of quantum players together with an initial state $|\Psi\rangle$ (and, possibly an additional classical probability distribution) defines a *quantum strategy* τ_{qm} *(based on the state* $|\Psi\rangle$*)*.

Let us now describe the rules of a game $\mathcal{G}_n$: First, an instance (σ, q, W) is sampled according to the probability distribution specified by $\mathcal{G}_n$. The players are then subdivided into groups defined by σ, i.e., a player P_i is said to *belong to the group* G_k if $i \in G_k$. Let us assume that there are m such groups.

The game consists of steps, where, in each step, each player takes some input (which is identical for all players belonging to the same group) and generates an output.

In the first step, the players' inputs are specified by the query $q = (q_1, \ldots, q_m)$ (where the bitstring q_k is given to all players in the group G_k). Then, the players communicate by generating outputs (in step t) which are then (in the next step $t+1$) given as input to certain other players. In our model, a player can (in each step) choose between two possibilities: his output is either sent to all players within his group or it is broadcasted to all n players.[5]

The game runs until, after a certain number of steps, all n players are in a so-called halting state, indicated by a special output, where additionally, at most one player in each group G_k specifies a *final output string* a_k. (If there is no such player, we set $a_k = \emptyset$ where $\emptyset$ is the empty string.) The game is won iff $(a_1, \ldots, a_m) \in W$.

As an example, consider the game $\mathcal{G}_n^s$ for n players from Section 2 (where we first omit the restriction that the hint sent by the remaining players is limited to one bit). The two chosen players (P_i and P_j, for two different indices i and j) each form a group, while the remaining players are collected in a third group. Therefore, the partitioning of the n players is determined by the triple $\sigma_{ij} = (\{i\}, \{j\}, \{1, \ldots, n\} \backslash \{i, j\})$.

The query q describes the information which is given to the players when they are separated into groups. In our game, each player merely learns whether he is among the chosen or the remaining ones. This can be indicated by a bit, e.g., $q = (0, 0, 1)$. The game is won iff the outputs of the chosen players are different, i.e., the set of allowed answers is $W = \{(0, 1, \emptyset), (1, 0, \emptyset)\}$.

The choice of the two players P_i and P_j is random, while the query q and the set of allowed answers W is always the same. The game $\mathcal{G}^s$ is thus defined as the uniform distribution over all

[5] Technically, this choice can for instance be indicated by a certain bit in the player's output.

triples (σ_{ij}, q, W) where $1 \leq i < j \leq n$.

3.2 Broadcast Complexity

In order to win a game $\mathcal{G}_n$, the players, being separated in different groups, must generally communicate both with players within their own group and with players in other groups. According to the model described in the previous subsection, a player can (in each step) choose whether he wants to send information to the players in his group or broadcast information to all players. Note that, since the players are collaborating (and thus, privacy is no issue), this includes any type of communication among the players. For instance, to send a certain message to *one* specific player, the sender simply includes the address of the receiver (and possibly his own address) into the broadcasted message.

We will be interested in the total amount of information flowing from inside each group to the players outside the group, i.e., the information passing the "boundary" of each group (outwards). Therefore, to quantify this information, we have to consider the messages *broadcasted* by each player (to all players).

Let $\mathcal{G}_n$ be a game and $P_1, \ldots, P_n$ a set of players. Assume that the information being broadcasted by player P_i in step t is a bitstring $b_{t,i}$ (where $b_{t,i} = \emptyset$ if P_i does not broadcast anything in this step). Furthermore, assume (without loss of generality) that, in the next step $t+1$, this information is given as input to all players in the form of a string $\bar{b}_t = b_{t,1} \| \cdots \| b_{t,n}$ being the concatenation of the strings $b_{t,i}$ broadcasted in step t. These bitstrings $\bar{b}_t$ must fulfill the requirement that any player, reading $\bar{b}_t$ bitwise, is able to detect when the string terminates.[6] This technical point is important when quantifying the amount of broadcasted bits since it prevents information from being encoded into the length of $\bar{b}_t$.[7]

Note that the strings $\bar{b}_t$ generally depend on the randomness of the players as well as the randomness in the choice of the instance (σ, q, W) of the game $\mathcal{G}_n$. The *(worst case) group broadcast complexity* for a given strategy τ for n players is thus defined as

$$B(\mathcal{G}_n, \tau) := \max \sum_t \bar{b}_t.$$

where the maximum is taken over their whole randomness.[8]

In the following section, we will see that the minimal amount of information which has to be exchanged between the groups in order to win a certain game $\mathcal{G}_n$ (for n players) depends on the quantum state $|\Psi\rangle$ (defined on n subsystems) initially shared by the players. This motivates the following definition.

Definition 1. The *classical group broadcast complexity of a game $\mathcal{G}_n$ for n players*, $B^{\mathrm{cl}}(\mathcal{G}_n)$, is given by the minimal value of $B(\mathcal{G}_n, \tau)$ where the minimum is taken over all classical strategies τ to win $\mathcal{G}_n$ with certainty.

The *quantum group broadcast complexity of $\mathcal{G}_n$ with respect to an n-partite quantum state $|\Psi\rangle$*, $B^{\mathrm{qm}}_{|\Psi\rangle}(\mathcal{G}_n)$ is defined similarly, but the minimum is taken over all winning quantum strategies for n players sharing the quantum state $|\Psi\rangle$.

Note that, in the special case where the only partitioning specified by the game is the trivial partitioning $(\{1\}, \ldots, \{n\})$ (consisting of n singleton sets), the group broadcast complexity corresponds to Yao's definition of communication complexity.

[6] The length of any broadcasted string $\bar{b}_t$ must thus either be fixed or be encoded into the string itself.

[7] Similarly, the input for the players might be considered as the concatenation $\bar{b}_t \| \bar{r}$ of the message $\bar{b}_t$ and a random bitstring $\bar{r}$.

[8] Note that this definition is independent of the probability distribution over the triples (σ, q, W), but only depends on the set of possible triples.

3.3 A Separation Result

Let us again consider the example game $\mathcal{G}_n^s$ from Section 2. It can not be won classically if the information a chosen player gets from the other players is restricted to one bit (see Section 2.2). On the other hand, the quantum strategy introduced in Section 2.3 allows to always win the game with one hint bit using a GHZ state $|\Phi\rangle$.

This is summarized by the following lemma, which additionally gives a lower bound for the classical broadcast complexity.

Lemma 2. *The classical and the quantum group broadcast complexity satisfy*

$$B^{\mathrm{cl}}(\mathcal{G}_n^s) \geq \log_2 \log_2 n \quad \textit{and} \quad B^{\mathrm{qm}}(|\Phi\rangle, \mathcal{G}_n^s) \leq 1,$$

respectively, where $|\Phi\rangle$ is the GHZ state of n qubits.

Proof. The only missing part is the proof of the lower bound on the classical broadcast complexity $B^{\mathrm{cl}}(\mathcal{G}_n^s)$, i.e., it has to be shown that for any set of classical players $P_1, \ldots, P_n$,

$$B(\mathcal{G}_n^s, (P_1, \ldots, P_n)) \geq \log_2 \log_2 n.$$

Since the group broadcast complexity $B(\mathcal{G}^s, (P_1, \ldots, P_n))$ is defined as a maximum taken over the randomness of the players, it suffices to prove this inequality to hold for any set of deterministic players (where each player's output is completely determined by his input).

Therefore, let $P_1, \ldots, P_n$ be a fixed set of deterministic players winning the game $\mathcal{G}_n^s$ with certainty. For any two indices $i, j \in \{1, \ldots, n\}$, define m_{ij} to be the sequence of strings $(\bar{b}_t)_{t \in \mathbb{N}}$ broadcasted by all players during the game when the instance $\sigma_{ij} = (\{i\}, \{j\}, \{1, \ldots, n\} \backslash \{i, j\})$ has been chosen. Note that each of the chosen players P_i and P_j forms a 1-player group, i.e., there is no communication within these groups. Therefore, the only inputs of a chosen player are (in the first step) the query, which is always the bit 0, and (in the subsequent steps) the broadcasted messages m_{ij}.

Let M be the set of sequences m_{ij} for all possible instances of the game $\mathcal{G}_n^s$, i.e.,

$$M := \{m_{ij} : i, j \in \{1, \ldots, n\}\}.$$

Clearly, the set M must contain at least one string m_{ij} of length at least $\log_2 |M|$. Since the length of the strings m_{ij} is a lower bound for the group broadcast complexity $B(\mathcal{G}^s, (P_1, \ldots, P_n))$, it suffices to prove that

$$\log_2 |M| \geq \log_2 \log_2 n. \tag{4}$$

Note that the final output bit of any (deterministic) player P_i, when he is chosen, is fully determined by the sequence $m \in M$ of broadcasted messages. Let $m_1, \ldots, m_l$ be the $l := |M|$ elements of M. Furthermore, for each $i = 1, \ldots, n$, let $b^{(i)}$ be a bitstring of length l where the rth bit $b_r^{(i)}$ (for $r = 1, \ldots, l$) is the output bit (or an arbitrary bit, if there is no such output) of P_i given that the sequence of broadcasted messages is m_j.

By assumption, the players $P_1, \ldots, P_n$ always win the game $\mathcal{G}_n^s$. This means that for any allowed $i, j \in \{1, \ldots, n\}$ defining an instance $\sigma_{ij} = (\{i\}, \{j\}, \{1, \ldots, n\} \backslash \{i, j\})$, there must be a sequence of broadcasted messages $m \in M$ such that the output bits of the chosen players P_i and P_j are different.

This is equivalent to say that the bitstrings $b^{(1)}, \ldots, b^{(n)}$ must all be different. Their length $l = |M|$ is thus lower bounded by $\log_2 n$, from which inequality (4) immediately follows. $\square$

3.4 A Generalized Pseudo-Telepathy Game and a Stronger Separation Result

We will now consider a game $\mathcal{G}^g$ for which the gap between the classical and the quantum broadcast complexity is even larger.

For any subset $C \subseteq \{1, \ldots, n\}$, $C = \{c_1, \ldots, c_k\}$ (where $k = |C|$), let σ_C be the $k+1$-tuple $(\{c_1\}, \ldots, \{c_k\}, \{1, \ldots, n\} \backslash C\})$. Furthermore, set

$$q_k = (\underbrace{0, \ldots, 0}_{k \text{ times}}, 1) \quad \text{and} \quad W_k = \{(\underbrace{b_1, \ldots, b_k}_{k \text{ times}}, \emptyset) : \; b_i \in \{0,1\}; \; b_1 \oplus \cdots \oplus b_k = 1\}.$$

The n-player game $\mathcal{G}_n^g$ (for $n \in \mathbb{N}$) is then defined by the uniform distribution over all triples $(\sigma_C, q_{|C|}, W_{|C|})$ with $C \subseteq \{1, \ldots, n\}$ and $|C| \equiv 2 \pmod 4$.

Note that this game is very similar to the game $\mathcal{G}_n^s$ from Section 2: First, $k = 4t+2$ players (for some random integer t) are randomly chosen. (The query bit is used to indicate whether the player belongs to the chosen or the remaining ones.) Each of the chosen players must then generate an output bit b_i such that the parity of all these bits is odd (in particular, for $k = 2$, the two bits must be different).

The k chosen players each form a 1-player group, while another group consists of the $n - k$ remaining players. Therefore, if for instance the remaining players send a hint string b to the chosen players, this is inter-group communication which has to be included in the group broadcast complexity. We will show that for players sharing a GHZ state, a hint string of length 1 always suffices to win $\mathcal{G}_n^g$, while, in the classical setting, the group broadcast complexity is at least $\frac{1}{2}\log_2 n - 2$ bits for any winning strategy.

3.4.1 Classical Analysis

The game $\mathcal{G}_n^g$ can always be won classically with $\lceil \log_2 n \rceil$ bits of inter-group communication. To see this, consider the following strategy: A unique labeling bitstring m_i of length $\lceil \log_2 n \rceil$ is assigned to each player P_i (for $i = 1, \ldots, n$). During the game, the remaining players first communicate within their group in order to find out the label m_s of an arbitrary player P_s not belonging to their group (m_s is thus the label of a chosen player), and then broadcast m_s. Each of the chosen players P_i compares this message m_s with his label m_i and then generates his final output bit b_i such that $b_i = 1$ iff $m_i = m_s$.[9] Then, obviously, only player P_s outputs 1, i.e., the game is won.

The classical broadcast complexity of $\mathcal{G}_n^g$ is thus at most $\lceil \log_2 n \rceil$ bits. It turns out that, with any classical strategy using less than (roughly) one half of this amount of inter-group communication, there is a nonzero probability to lose the game.

Lemma 3. *In order to win the game $\mathcal{G}_n^g$ classically with certainty, at least $\frac{1}{2}\log_2 n - 2$ bits of information have to be exchanged between the groups, i.e., $B^{\mathrm{cl}}(\mathcal{G}_n^g) \geq \frac{1}{2}\log_2 n - 2$.*

Proof. The proof is analog to the proof of Lemma 3. The instances of the game $\mathcal{G}_n^g$ are parameterized by subsets $C \subseteq \{1, \ldots, n\}$ with $|C| \equiv 2 \pmod 4$. For a fixed set of deterministic players $P_1, \ldots, P_n$, the set of possible sequences of messages is thus given by

$$M := \{m(C) : C \subseteq \{1, \ldots, n\}; \; |C| \equiv 2 \pmod 4\},$$

where $m(C)$ is the sequence of strings $(b_t)_{t \in \mathbb{N}}$ broadcasted by the players given that the instance $(\sigma_C, q_{|C|}, W_{|C|})$ has been chosen. Since $\log_2 |M|$ is a lower bound for the group broadcast complexity, it remains to be proven that

$$\log_2 |M| \geq \frac{1}{2}\log_2 n - 2. \tag{5}$$

[9] If $k = n$, there are no remaining players sending a bitstring to the chosen players. One possibility to overcome this problem is to consider a slightly different variant of the game, where an additional player is introduced, who always belongs to the group of remaining players. His only task is to broadcast m_s.

Let $m_1, \ldots, m_l$ be the $l := |M|$ elements of M. Furthermore, define the l-bit strings $b^{(i)}$ (for $i = 1, \ldots, n$) as in the proof of Lemma 3: The jth bit $b_j^{(i)}$ (for $j = 1, \ldots, l$) is the output bit of player P_i given that the sequence of broadcasted messages is m_j.

If the players $P_1, \ldots, P_n$ win the game $\mathcal{G}_n^g$ with certainty, then, for any allowed set C defining an instance $(\sigma_C, q_{|C|}, W_{|C|})$, there must be a sequence $m \in M$ of broadcasted messages such that the xor of the output bits of the chosen players P_i $(i \in C)$ equals 1.

This requirement can again be formulated as a condition on the bitstrings $b^{(1)}, \ldots, b^{(n)}$: For all sets $C \subseteq \{1, \ldots, n\}$ with $|C| \equiv 2 \pmod 4$ there must be a $r \in \{1, \ldots, l\}$ such that $\sum_{i \in C} b_r^{(i)} \equiv 1 \pmod 2$.

Lemma 5 (see appendix) states that the length $l = |M|$ of these bitstrings, which can be considered as elements of a l-dimensional vector space over GF(2), is lower bounded by $\sqrt{n} - 2$. Since $l \geq 1$, this implies inequality (5), which concludes the proof. □

3.4.2 Quantum Analysis

There is a quantum strategy to win $\mathcal{G}_n^g$ which exactly corresponds to the winning strategy for the game from Section 2. However, the game $\mathcal{G}_n^g$ allows for more possibilities on how players might be chosen. Therefore, for the proof of the following lemma, a more general analysis than the one given in Subsection 2.3 is needed.

Lemma 4. *To win the game $\mathcal{G}_n^g$ with certainty using a GHZ state $|\Phi\rangle$, only one (classical) bit has to be exchanged between the groups, i.e., $B_{|\Phi\rangle}^{\mathrm{qm}}(\mathcal{G}_n^g) \leq 1$.*

Proof. Let $P_1, \ldots, P_n$ be n players, each of them controlling a two-dimensional quantum system $\mathcal{H}_1, \ldots, \mathcal{H}_n$, respectively. Furthermore, let $\{|e_0\rangle, |e_1\rangle\}$ be an orthonormal basis of $\mathcal{H}_i$ (for all $i = 1, \ldots, n$) and define the diagonal basis $\{|f_0\rangle, |f_1\rangle\}$ and the circular basis $\{|g_0\rangle, |g_1\rangle\}$ as in Subsection 2.3. The GHZ state initially shared by the players is then given by (3).

Each player P_i follows the same strategy: If he is among the remaining players (i.e., if he gets a bit 1 as query input in the first step), he measures his quantum system $\mathcal{H}_i$ with respect to the diagonal basis $\{|f_0\rangle, |f_1\rangle\}$ and sends the result of this measurement to the other players within his group (i.e., to the other remaining players). One of the remaining players then broadcasts a bit b depending on whether an even ($b = 0$) or an odd ($b = 1$) number of them got the measurement outcome $|f_1\rangle$.

On the other hand, if a player P_i is among the chosen players (i.e., his first input is 0), he reads the bit b broadcasted by the group of chosen players and then measures his system $\mathcal{H}_i$, depending on this bit, using either the diagonal basis $\{|f_0\rangle, |f_1\rangle\}$ (if $b = 1$) or the circular basis $\{|g_0\rangle, |g_1\rangle\}$ (if $b = 0$). He then simply outputs the bit indicating the outcome of this measurement.

It has to be shown that for all instances (σ, q, W) of $\mathcal{G}_n^g$, the players $P_1, \ldots, P_n$ win with certainty. By the symmetry of the game and the described strategy, the analysis is exactly the same for all instances. We can thus, without loss of generality, restrict to one instance (for each possible k), namely (σ_C, q_k, W_k) for $C = \{1, \ldots, k\}$, i.e., $P_1, \ldots, P_k$ are the chosen players while $P_{k+1}, \ldots, P_n$ are the remaining ones.

It can easily be verified that the vectors

$$|v_{b_1,\ldots,b_n}\rangle := \begin{cases} |f_{b_1}\rangle \otimes \cdots \otimes |f_{b_k}\rangle \otimes |f_{b_{k+1}}\rangle \otimes \cdots \otimes |f_{b_n}\rangle & \text{if } b_{k+1} \oplus \cdots \oplus b_n = 1 \\ |g_{b_1}\rangle \otimes \cdots \otimes |g_{b_k}\rangle \otimes |f_{b_{k+1}}\rangle \otimes \cdots \otimes |f_{b_n}\rangle & \text{if } b_{k+1} \oplus \cdots \oplus b_n = 0 \end{cases} \tag{6}$$

(for all $(b_1, \ldots, b_n) \in \{0,1\}^n$) build an orthonormal basis of $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$. Note that these vectors are the products of the measurement bases used by the players when following the described strategy, where $b_1, \ldots, b_k$ are the final output bits of the chosen players and $b_{k+1}, \ldots, b_n$ are the measurement outcomes of the remaining players. The probability that the chosen players $P_1, \ldots, P_k$ have output $b_1, \ldots, b_k$, respectively, is thus given by

$$p_{b_1,\ldots,b_k} := \sum_{(b_{k+1},\ldots,b_n)\in\{0,1\}^{n-k}} p_{b_1,\ldots,b_n}$$

where

$$p_{b_1,\ldots,b_n} := |\langle\Phi|v_{b_1,\ldots,b_n}\rangle|^2.$$

It thus remains to be shown that the probability for the output of the chosen players not being contained in W_k is zero, i.e.,

$$b_1 \oplus \cdots \oplus b_k = 0 \quad \Longrightarrow \quad p_{b_1,\ldots,b_n} = 0. \tag{7}$$

Let us first assume that $b_{k+1} \oplus \cdots \oplus b_n = 1$. We then have

$$\begin{aligned}\langle\Phi|v_{b_1,\ldots,b_n}\rangle = 2^{-\frac{n+1}{2}} & \big(\langle e_0| \otimes \cdots \otimes \langle e_0| + \langle e_1| \otimes \cdots \otimes \langle e_1|\big) \\ & \cdot \big(|e_0\rangle + (-1)^{b_1}|e_1\rangle\big) \otimes \cdots \otimes \big(|e_0\rangle + (-1)^{b_n}|e_1\rangle\big)\end{aligned}$$

and thus

$$p_{b_1,\ldots,b_n} = 2^{-(n+1)}|1 + (-1)^{\sum_{i=1}^n b_i}|^2.$$

From the assumption on $b_{k+1}, \ldots, b_n$ it follows immediately that for $b_1, \ldots, b_k$ satisfying the left side of implication (7), the sum in the exponent becomes odd, i.e., the probability $p_{b_1,\ldots,b_n}$ is zero.

Assume now that $b_{k+1} \oplus \cdots \oplus b_n = 0$. Then

$$\begin{aligned}\langle\Phi|v_{b_1,\ldots,b_n}\rangle = 2^{-\frac{n+1}{2}} & (\langle e_0| \otimes \cdots \otimes \langle e_0| + \langle e_1| \otimes \cdots \otimes \langle e_1|) \\ & \cdot (|e_0\rangle + (-1)^{b_1} i|e_1\rangle) \otimes \cdots \otimes (|e_0\rangle + (-1)^{b_k} i|e_1\rangle) \\ & \otimes (|e_0\rangle + (-1)^{b_{k+1}}|e_1\rangle) \otimes \cdots \otimes (|e_0\rangle + (-1)^{b_n}|e_1\rangle)\end{aligned}$$

and hence

$$p_{b_1,\ldots,b_n} = 2^{-(n+1)}|1 + i^k(-1)^{\sum_{i=1}^n b_i}|^2 = 2^{-(n+1)}|1 - (-1)^{\sum_{i=1}^n b_i}|^2,$$

where the second equality follows from $k \equiv 2 \pmod 4$. Again from the assumption on $b_{k+1}, \ldots, b_n$ we can conclude that the implication (7) is satisfied. $\square$

4 Conclusion

The classical outcomes of measurements performed on an entangled quantum state can generally not be explained by local classical randomness. This non-local property of quantum mechanics is demonstrated by the pseudo-telepathy game proposed in Section 2: A simple task, which *obviously* can not be accomplished by separated classical players, is solvable by players sharing quantum entanglement.

A characterization of the nonlocality of an n-paritite quantum state is given by the amount of communication needed by n separated classical systems for simulating the outcomes of local measurements performed on the respective parts of the state. There are clearly several ways to quantify this communication, each revealing a different aspect of the non-local information contained in the state. Contrary to the approach of Cleve and Buhrman [8], we consider the information exchanged between certain groups of systems instead of counting the overall communication. This leads to an alternative quantification of non-local information and, consequently, to new separation results. They can not directly be compared with the results based on Yao's model (as for instance [7]), but rather reveal another aspect of the nature of entanglement as well as the gap between quantum and classical correlation.

The results obtained in Section 3 are formulated in terms of communication complexity with respect to a certain game. The difference between the amount of communication needed for classical and quantum players, respectively, to win certain games, directly lead to lower bounds for the communication needed to simulate quantum states. For instance, the separation stated by Lemma 2 implies that for the classical simulation of two separated quantum systems, sharing a GHZ state with $n-2$ other systems, at least $\Omega(\log \log n)$ bits of additional information is necessary.

It is one of the goals of this paper to shed some light on the nature of quantum entanglement, a phenomenon which is not yet completely understood. While separation results, as the ones presented here, can be seen as lower bounds for the amount of non-local information contained in entangled quantum states, some work has been done to determine the maximal communication being necessary for an exact simulation of such states by classical systems (see, e.g., [3]). It is however still an open problem to find the most accurate way to characterize entanglement between quantum systems in terms of classical communication.

5 Acknowledgments

The authors thank Nicolas Gisin, Ueli Maurer, and Alain Tapp for interesting discussions. The first author was partially supported by the Swiss National Science Foundation (SNF), and the second author was partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

Appendix

Lemma 5. *Let $b^{(1)}, \ldots, b^{(n)}$ be n vectors of a l-dimensional vector space over* $\mathrm{GF}(2)$*. If for all $C \subseteq \{1, \ldots, l\}$ with $|C| \equiv 2 \pmod 4$*

$$\sum_{i \in C} b^{(i)} \neq \mathbf{0} \tag{8}$$

then

$$l \geq \sqrt{n} - 2. \tag{9}$$

Proof. Each element of a d-dimensional vector space over $\mathrm{GF}(2)$ can naturally be identified with a bitstring of length d, and vice versa. In the following, we will thus alternately speak of vectors and bitstrings, always meaning the same object.

The idea is to append additional bits to the bitstrings $b^{(i)}$ (for $i = 1, \ldots, n$) in order to obtain longer bitstrings $\bar{b}^{(i)}$ and $\hat{b}^{(i)}$. These bits are chosen in such a way that the resulting bitstrings $\bar{b}^{(i)}$ or $\hat{b}^{(i)}$, considered as vectors, are linearly independent. This will lead to a lower bound on their length which finally allows to derive a lower bound on l.

Defining (for all $i = 1, \ldots, n$)

$$\bar{b}^{(i)} := 1 \| b^{(i)}$$

(where $\|$ is the concatenation of strings) we have, for any set $I \subseteq \{1, \ldots, n\}$,

$$\sum_{i \in I} \bar{b}^{(i)} = \mathbf{0} \quad \Longrightarrow \quad |I| \equiv 0 \pmod 4. \tag{10}$$

This can be seen as follows: If $|I|$ is odd, the bits in the first position of the strings $\bar{b}^{(i)}$ (which are all equal to 1) will sum up to 1. On the other hand, if $|I| \equiv 2 \pmod 4$, then, by the assumption of the lemma, the sum $\sum_{i \in I} b^{(i)}$ is again nonzero.

For a given family $\mathcal{A}$ of disjoint nonempty subsets of $\{1, \ldots, n\}$, let $\bar{A}$ be the set of elements not contained in any of these subsets, $\bar{A} := \{1, \ldots, n\} \setminus \cup_{A \in \mathcal{A}} A$, and set $\bar{\mathcal{A}} := \mathcal{A} \cup \{\bar{A}\}$. It is easy to see that it is always possible to choose a family $\mathcal{A}$ in such a way that the following condition is satisfied: For any nonempty set B with $B \subseteq A$ for some $A \in \bar{\mathcal{A}}$

$$\sum_{i \in B} \bar{b}^{(i)} = \mathbf{0} \quad \Leftrightarrow \quad B \in \mathcal{A}, \tag{11}$$

i.e., the sets $A \in \mathcal{A}$ contain a minimal number of indices such that the vectors $\bar{b}^{(i)}$ for $i \in A$ are linearly dependent. Note that, from (10), we have

$$|A| \equiv 0 \pmod 4 \tag{12}$$

for all $A \in \mathcal{A}$.

Let $\mathcal{A}$ be a family of sets satisfying condition (11). We will distinguish two cases.

First, assume that there is a set $A \in \bar{\mathcal{A}}$ such that $|A| > \sqrt{n}$. Let V be an arbitrary subset of A with $|V| = |A| - 1$. It follows directly from condition (11) that the vectors $\bar{b}^{(i)}$ for $i \in V$ form a set of $|A| - 1$ linearly independent vectors. Consequently, their length $l + 1$ must satisfy $l + 1 \geq |A| - 1$ which immediately implies (9).

Assume now that $A \leq \sqrt{n}$ for all $A \in \bar{\mathcal{A}}$. This immediately implies that $|\mathcal{A}| \geq \sqrt{n} - 1$. Set, for all $i \in \{1, \ldots, n\}$,

$$\tilde{b}^{(i)} := e_i \| \bar{b}^{(i)}$$

where e_i is the bitstring of length n which has a bit 1 at the ith position and zeros at all other positions. Furthermore, for all $A \in \mathcal{A}$, let r_A be an arbitrary element of A. Define $\hat{b}^{(i)}$ (for $i =$

$1,\ldots,n$) as the bitstring which is identical to $\tilde{b}^{(i)}$ except that the bits at positions r_A (for all $A \in \mathcal{A}$) are omitted. Since the strings $\tilde{b}^{(i)}$ have length $n+1+l$, the strings $\hat{b}^{(i)}$ obviously have length $l' = n+1+l-|\mathcal{A}| \leq n+l-\sqrt{n}+2$.

If the strings $\hat{b}^{(i)}$ (for $i=1,\ldots,n$) form a set of n linearly independent vectors, then $l' \geq n$, i.e.,

$$n \leq n+2+l-\sqrt{n}$$

which again implies (9).

It thus remains to be shown that the bitstrings $\hat{b}^{(1)},\ldots,\hat{b}^{(n)}$ are indeed linearly independent. Assume by contradiction that there is a nonempty set $I \subseteq \{1,\ldots,n\}$ such that

$$\sum_{i\in I} \hat{b}^{(i)} = \mathbf{0}. \tag{13}$$

To show that this leads to a contradiction, we will distinguish three cases.

(a) $|I| \not\equiv 0 \pmod 4$: From condition (10) the sum $\sum_{i\in I} \bar{b}^{(i)}$ is nonzero. Since the last $n+1$ bits of $\hat{b}^{(i)}$ correspond to $\bar{b}^{(i)}$, this obviously contradicts equation (13).

(b) $|I| \equiv 0 \pmod 4$ and $I \cap \bar{A} \neq \emptyset$: Let r be an element of the intersection $I \cap \bar{A}$. By definition, there is exactly one bitstring $\tilde{b}^{(i)}$ with $i \in I$ having a bit 1 at the rth position, namely $\tilde{b}^{(r)}$. Note that the bit of $\tilde{b}^{(i)}$ at position r corresponds to a bit of $\hat{b}^{(i)}$ at some position r' (in the construction of $\hat{b}^{(i)}$ from $\tilde{b}^{(i)}$ only bits with an index in sets A with $A \in \mathcal{A}$ are omitted). Consequently, the r'th bit of the sum in (13) is 1.

(c) $|I| \equiv 0 \pmod 4$ and $I \cap \bar{A} = \emptyset$: Since I is nonempty, there exists a set $A \in \mathcal{A}$ such that $I \cap A \neq \emptyset$. Assume that $|I \cap A| > 1$, i.e. there are at least two different indices r_1 and r_2 in $I \cap A$. Consequently, the sum $\sum_{i\in I} \tilde{b}^{(i)}$ has a bit 1 at position r_1 and r_2. By the construction of the strings $\hat{b}^{(i)}$, at least one of these bits corresponds to a bit in the sum in (13) which can thus not be zero.

It remains to be shown that $|I \cap A| > 1$. Using the fact that $\bar{b}^{(i)} + \bar{b}^{(i)} = \mathbf{0}$ (over GF(2)) we have

$$\sum_{i\in A/I \cup I/A} \bar{b}^{(i)} = \sum_{i\in A} \bar{b}^{(i)} + \sum_{i\in I} \bar{b}^{(i)} = \mathbf{0}$$

where the last equality follows from $A \in \mathcal{A}$ and condition (11) as well as from assumption (13). With condition (10) this implies that

$$|A/I \cup I/A| \equiv 0 \pmod 4. \tag{14}$$

On the other hand, using (12) and $|I| \equiv 0 \pmod 4$,

$$|A/I \cup I/A| = |A| + |I| - 2|A \cap I| \equiv -2|A \cap I| \pmod 4.$$

Together with (14) we conclude that $|A \cap I|$ must be even and thus, since the set $A \cap I$ is nonempty, we have $|A \cap I| > 1$.

□

References

[1] A. Ambainis, L.J. Schulman, A. Ta-Shma, U. Vazirani, and A. Widgerson. The quantum communication complexity of sampling. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, pages 342–351, 1998.

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

[3] G. Brassard, R. Cleve, and A. Tapp. Cost of exactly simulating quantum entanglement with classical communication. *Physical Review Letters*, 83(9):1874–1877, 1999, quant-ph/9901035.

[4] H. Buhrman. Quantum computing and communication complexity. *Current Trends in Theoretical Computer Science*, pages 664–679, 2001.

[5] H. Buhrman, R. Cleve, and A. Widgerson. Quantum vs. classical communication and computation. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 63–68, 1998, quant-ph/9802040.

[6] H. Buhrman, W. van Dam, P. Høyer, and A. Tapp. Multiparty quantum communication complexity. *Physical Review A*, 60:2737–2741, 1999, quant-ph/9710054.

[7] H. Burhman, R. Cleve, and W. van Dam. Quantum entanglement and communication complexity. *SIAM Journal on Computing*, 30:1829–1841, 2001, quant-ph/9705033.

[8] R. Cleve and H. Buhrman. Substituting quantum entanglement for communication. *Physical Review A*, 56:1201–1204, 1997, quant-ph/9704026.

[9] V. Galliard, A. Tapp, and S. Wolf. The impossibility of pseudo-telepathy without quantum entanglement. manuscript, 2002.

[10] V. Galliard and S. Wolf. Pseudo-telepathy, entanglement, and graph colorings. In *Proceedings of 2002 IEEE International Symposium on Information Theory*, page 101, 2002.

[11] D.M. Greenberger, M.A. Horne, and A. Zeilinger. Going beyond Bell's theorem. In M. Kafatos, editor, *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, pages 73–76. Kluwer Academic, 1989.

[12] D.M. Greensberger, M.A. Horne, A. Shimony, and A. Zeilinger. Bell's theorem without inequalities. *American Journal on Physics*, 58:1131–1143, 1990.

[13] R. Raz. Exponential separation of quantum and classical communication complexity. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing*, pages 358–367, 1999.

[14] A.C. Yao. Some complexity questions related to distributed computing. In *Proceedings of the 11th Annual ACM Symposium on Theory of Computing*, pages 209–213, 1979.

Towards Characterizing the Non-Locality of Entangled Quantum States

Renato Renner[1]
Computer Science Department
ETH Zürich
CH-8092 Zürich
Switzerland
e-mail: renner@inf.ethz.ch

Stefan Wolf[2]
Département d'Informatique et R.O.
Université de Montréal
Montréal, QC
Canada H3C 3J7
e-mail: wolf@iro.umontreal.ca

Abstract — **We propose a so called pseudo-telepathy game for n players demonstrating the non-locality of quantum information. The simplicity of the classical analysis of our game contrasts the often quite involved analysis of previously proposed pseudo-telepathy games [1]. Moreover, our game allows for a quantitative characterization of entanglement in terms of communication complexity.**

I. The Game

Consider the following game $\mathcal{G}_n^s$ involving $n \geq 5$ collaborating players $P_1, \ldots, P_n$. First, two players P_i and P_j are chosen randomly in such a way that neither of them knows who the other one is. (The non-chosen, remaining, $n-2$ players can be allowed to know which pair of players was chosen.)

The remaining players are now allowed to communicate in order to generate one "hint" bit b which they say out loud (in particular, P_i and P_j can hear the bit). The chosen players P_i and P_j must then independently (i.e., no communication between them is allowed) generate a bit b_i and b_j, respectively. The game is won simply if $b_i \neq b_j$.

We will show that this game can be won with probability at most (roughly) 75% classically (if n is large enough), but with probability 1 (for any value of n) if the players can share quantum information.

II. Classical Analysis

Let us first consider a classical setting where the players rely on arbitrary *classical* (but no quantum) information which might have been shared before the start of the game.

Each player has a fixed strategy defining his behavior for the case he is chosen. While this strategy might in general be probabilistic, i.e., depend on some randomness, we can, without loss of generality, assume that this randomness is fixed before the game starts. This means that by the time the player is chosen, his strategy is deterministic.

Once a player is chosen, the only information he gets is the hint bit b. For any given (deterministic) strategy, this bit b thus completely determines his output. Obviously, there exist exactly *four* possible strategies, namely to output 0, 1, b, or $\overline{b}$ (where $\overline{b}$ denotes the complement of b).

If the strategies of the chosen players are the same, they will clearly output the same bit and the game is lost. (Otherwise, if their strategies are different and if the remaining players know these strategies, they can always win.) Finding the minimal probability of losing the game thus amounts to determining the minimal probability of the event that two players with the *same* strategy (where four strategies are possible) are picked (out of the set of n players).

For $n = 4k + r$ players (where k, r are integers, $0 < k$, and $0 \leq r < 4$), the probability of this event is at least

$$p(n) = (4-r) \cdot \frac{k}{n} \cdot \frac{k-1}{n-1} + r \cdot \frac{k+1}{n} \cdot \frac{k}{n-1} \ .$$

We have for instance $p(5) = 1/10$, $p(8) = 1/7$, and $p(n) \to 1/4$ for $n \to \infty$.

III. A Winning Strategy for Quantum Players

If the players can not only share classical information, but are additionally allowed to store a quantum state being generated and shared before the game starts, they can win the game *with certainty.* (Note that, during the game, the players are only allowed to process the quantum information locally, i.e., an external observer would not be able to detect that the players follow a quantum strategy.)

Assume that the n players initially share a so called GHZ state, $\frac{1}{\sqrt{2}}(|0\rangle \cdots |0\rangle + |1\rangle \cdots |1\rangle)$ where each of them controls one qubit. Then, the winning quantum strategy is as follows: After the two players have been chosen, the remaining players first measure their qubits with respect to the diagonal basis $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$, and determine the number k of players having the measurement outcome $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle$. The parity of k is then announced to the chosen players as hint bit b, i.e., $b \equiv k \pmod 2$.

Depending on this hint b, each of the chosen players measures his subsystem in either the diagonal basis (if $b = 1$) or the circular basis $\{\frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)\}$ (if $b = 0$). His output is then a bit indicating his measurement result (e.g., 0 for $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ or $\frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$, and 1 otherwise).

A straightforward calculation (which is omitted in this extended abstract) then shows that the probability of the event that the two chosen players both have the same measurement outcome is zero, i.e., they will always have different outputs and thus win the game.

IV. Quantitative Results

While, for quantum players, communicating only one hint bit to the chosen players suffices to win the game $\mathcal{G}_n^s$, the number of bits $C_{\mathrm{win}}^{\mathrm{cl}}(\mathcal{G}_n^s)$ to be communicated in order to win $C_{\mathrm{win}}^{\mathrm{cl}}(\mathcal{G}_n^s)$ can be shown to be bounded by

$$C_{\mathrm{win}}^{\mathrm{cl}}(\mathcal{G}_n^s) \geq \log_2 \log_2 n \ .$$

This automatically gives a bound for the amount of communication necessary to classically simulate the classical outcomes of local measurements on two (arbitrarily chosen) 2-dimensional subsystems, being in a GHZ state with $n-2$ other subsystems (cf. [2]).

[1]Supported by the Swiss National Science Foundation.
[2]Supported by Canada's NSERC.

An even stronger result is obtained when considering a slight generalization $\mathcal{G}_n^g$ of the game $\mathcal{G}_n^s$, where not only 2, but an arbitrary number k of players might be arbitrarily chosen. It can be shown that in order to win $\mathcal{G}_n^g$, at least $C_{\mathrm{win}}^{\mathrm{cl}}(\mathcal{G}_n^g) \geq \frac{1}{2}\log_2 n - 2$ bits have to be communicated by classical players, while, for quantum players sharing a GHZ state, one bit still suffices.

Acknowledgments

The authors thank Gilles Brassard and Alain Tapp for interesting discussions.

References

[1] G. Brassard, R. Cleve, and A. Tapp. Cost of exactly simulating quantum entanglement with classical communication. *Physical Review Letters*, 83(9):1874–1877, 1999.

[2] R. Cleve and H. Buhrman. Substituting quantum entanglement for communication. *Physical Review A*, 56:1201–1204, 1997.