Quantum Information and Computation, Vol. 5, No. 7 (2005) 538–550

RECASTING MERMIN'S MULTI-PLAYER GAME INTO THE FRAMEWORK OF PSEUDO-TELEPATHY

GILLES BRASSARD[a], ANNE BROADBENT[b], ALAIN TAPP[c]
Département IRO, Université de Montréal
C.P. 6128, succursale centre-ville, Montréal (Québec), H3C 3J7, Canada
{brassard, broadbea, tappa}@iro.umontreal.ca

Received August 18, 2004
Revised June 14, 2005

Entanglement is perhaps the most non-classical manifestation of quantum mechanics. Among its many interesting applications to information processing, it can be harnessed to *reduce* the amount of communication required to process a variety of distributed computational tasks. Can it be used to *eliminate* communication altogether? Even though it cannot serve to signal information between remote parties, there are distributed tasks that can be performed without any need for communication, provided the parties share prior entanglement: this is the realm of *pseudo-telepathy*.

One of the earliest uses of multi-party entanglement was presented by Mermin in 1990. Here we recast his idea in terms of pseudo-telepathy: we provide a new computer-scientist-friendly analysis of this game. We prove an upper bound on the best possible classical strategy for attempting to play this game, as well as a novel, matching lower bound. This leads us to considerations on how well imperfect quantum-mechanical apparatus must perform in order to exhibit a behaviour that would be classically impossible to explain. Our results include improved bounds that could help vanquish the infamous detection loophole.

Keywords: Entanglement, nonlocality, pseudo-telepathy, detection loophole
Communicated by: R Cleve

1 Introduction

It is well known that quantum mechanics can be harnessed to reduce the amount of communication required to perform a variety of distributed tasks, by clever use of either quantum communication [14] (in the model of Yao [26]) or quantum entanglement [13]. Consider for example the case of Alice and Bob, two very busy scientists who would like to find a time when they are simultaneously free for lunch. They each have an engagement calendar, which we may think of as n-bit strings a and b, where $a_i = 1$ (resp. $b_i = 1$) means that Alice (resp. Bob) is free for lunch on day i. Mathematically, they want to find an index i such that $a_i = b_i = 1$ or establish that such an index does not exist. The obvious solution is for

[a] Supported in part by Canada's Natural Sciences and Engineering Research Council (NSERC), the Canada Research Chair programme and the Canadian Institute for Advanced Research (CIAR).
[b] Supported in part by a scholarship from Canada's NSERC.
[c] Supported in part by Canada's NSERC, Québec's Fonds de recherche sur la nature et les technologies (FQRNT), the CIAR and the Mathematics of Information Technology and Complex Systems Network (MITACS).

Alice, say, to communicate her entire calendar to Bob, so that he can decide on the date: this requires roughly n bits of communication. It turns out that this is optimal in the worst case, up to a constant factor, according to classical information theory [18], even when the answer is only required to be correct with probability at least $^2/_3$. Yet, this problem can be solved with arbitrarily high success probability with the exchange of a number of *quantum* bits—known as *qubits*—in the order of $\sqrt{n}$ [1]. Alternatively, a number of *classical* bits in the order of $\sqrt{n}$ suffices for this task if Alice and Bob share prior entanglement, because they can make use of quantum teleportation [2]. Other (less natural) problems demonstrate an *exponential* advantage of quantum communication, both in the error-free [11] and bounded-error [23] models. Please consult [4, 24] for surveys on the topic of quantum communication complexity.

Given that prior entanglement allows for a dramatic *reduction* in the need for classical communication in order to perform some distributed computational tasks, it is natural to wonder if it can be used to *eliminate* the need for communication altogether. In other words, are there distributed tasks that would be impossible to achieve in a classical world if the participants were not allowed to communicate, yet those tasks could be performed without *any* form of communication provided they shared prior entanglement? The answer is negative if the result of the computation must become known to at least one party—otherwise, this phenomenon could be harnessed to provide faster-than-light signalling. Nevertheless, the feat becomes possible if we are satisfied with the establishment of nonlocal *correlations* between the parties' inputs and outputs [7].

Mathematically, consider n parties A_1, A_2,..., A_n, called the *players*, and two n-ary functions f and g. In an *initialization phase*, the players are allowed to discuss strategy and share random variables (in the classical setting) and entanglement (in the quantum setting). Then the players move apart and they are no longer allowed any form of communication. After the players are physically separated, each A_i is given some input x_i and is requested to produce output y_i. We say that the players *win* this instance of the game if $g(y_1, y_2, \ldots y_n) = f(x_1, x_2, \ldots x_n)$. Given an n-ary predicate P, known as the *promise*, a strategy is *perfect* if it wins the game with certainty on all questions that satisfy the promise, i.e. whenever $P(x_1, x_2, \ldots x_n)$ holds. A strategy is *successful with probability p* if it wins *any* instance that satisfies the promise with probability at least p; it is successful in *proportion p* if it wins the game with probability at least p when the instance is chosen at random according to the uniform distribution on the set of instances that satisfy the promise. Any strategy that succeeds with probability p automatically succeeds in proportion p, but not necessarily vice versa. In particular, it is possible for a strategy that succeeds in proportion $p > 0$ to fail systematically on some questions, whereas this would not be allowed for strategies that succeed with probability $p > 0$. Therefore, the notion of succeeding in proportion is the only one that is meaningful for *deterministic* strategies, and this is indeed where the name "in proportion" comes from: it is the ratio of the number of questions on which the strategy provides a correct answer to the total number of possible questions, taking account only of questions $x_1 x_2 \cdots x_n$ for which $P(x_1, x_2, \ldots, x_n)$ holds.

We say of a quantum strategy that it exhibits *pseudo-telepathy* if it is perfect provided the players share prior entanglement, whereas no perfect classical strategy can exist. The study of pseudo-telepathy was initiated in [7], but games that fit this framework had been introduced earlier [17, 15] (but *not* [16], see [8]). Unfortunately, those earlier papers were presented in a physics jargon hardly accessible to computer scientists, even with decent background in quantum information theory. Mermin offered a refreshing but temporary relief to this physicists-writing-for-their-kind-only paradigm when he presented a very accessible three-player account [20] of the GHZ scenario [15]. This protocol was also set into the communication complexity framework in [10].

But even Mermin donned his physicist's hat when he generalized his own game to an arbitrary number of players [21] in 1990. In this article, we develop the pseudo-telepathy game thus introduced by Mermin, which involves $n \geq 3$ players. This is probably the simplest multi-player game possible because each player is given a single bit of input and is requested to produce a single bit of output. Moreover, the quantum perfect strategy requires each player to handle a single qubit. To the best of our knowledge, this 1990 game is also the first pseudo-telepathy game ever proposed that is *scalable* to an arbitrary number of players.

We recast Mermin's n-player game in terms of pseudo-telepathy in Section 2 and we give a perfect quantum strategy for it. In Sections 3 and 4, we prove that no classical strategy can succeed with a probability that differs from random guessing by more than an exponentially small fraction in the number of players. More specifically, no classical strategy can succeed in the n-player game with a probability better than $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$. Then, we match this bound with a novel explicit classical strategy that is successful with the exact same probability $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$. Finally, we show in Section 5 that the quantum success probability would remain better than anything classically achievable, when n is sufficiently large, even if each player had imperfect apparatus that would produce the wrong outcome with probability nearly 15% or no outcome at all with probability close to 50%. This could be used to circumvent the infamous *detection loophole* in experimental proofs of the nonlocality of the world in which we live [19]. We assume throughout this paper that the reader is familiar with elementary concepts of quantum information processing [22].

2 The Game and its Perfect Quantum Strategy

For any $n \geq 3$, game G_n involves n players. Each player A_i receives a single input bit x_i and is requested to produce a single output bit y_i. The players are promised that there is an even number of 1s among their inputs. Without being allowed to communicate after receiving the question, they are challenged to produce a collective answer that contains an even number of 1s if and only if the number of 1s in the inputs is divisible by 4. More formally, we require that

$$\sum_{i=1}^{n} y_i \equiv \tfrac{1}{2}\sum_{i=1}^{n} x_i \pmod 2 \qquad (1)$$

provided $\sum_i x_i$ is even. We say that $x = x_1 x_2 \cdots x_n$ is the *question* and $y = y_1 y_2 \cdots y_n$ is the *answer*, which is *even* if it contains an even number of 1s and *odd* otherwise. We say that a question is *legitimate* if it satisfies the promise and that an answer is *appropriate* if Equation 1 is satisfied. Please do not confuse the words "input" and "question": the former refers to the single bit x_i seen by one of the players whereas the latter refers to the collection x of all input bits that serves as challenge for the collectivity of players. The same distinction applies between "output" and "answer".

Theorem 1 *If the n players are allowed to share prior entanglement, then they can always win game G_n.*

Proof. Define the following n-qubit entangled quantum states $|\Phi_n^+\rangle$ and $|\Phi_n^-\rangle$:

$$\begin{aligned} |\Phi_n^+\rangle &= \tfrac{1}{\sqrt{2}}|0^n\rangle + \tfrac{1}{\sqrt{2}}|1^n\rangle \\ |\Phi_n^-\rangle &= \tfrac{1}{\sqrt{2}}|0^n\rangle - \tfrac{1}{\sqrt{2}}|1^n\rangle\,. \end{aligned}$$

Let H denote the Walsh-Hadamard transform, defined as usual by

$$H \,:\, \begin{cases} |0\rangle \mapsto \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle \\ |1\rangle \mapsto \tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle \end{cases}$$

and let P denote a phase-change unitary transformation defined by

$$P \,:\, \begin{cases} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto \imath|1\rangle\,, \end{cases}$$

where we use a dotless $\imath$ to denote $\sqrt{-1}$ in order to distinguish it from index i, which is used to identify a player. It is easy to see that if P is applied to any two qubits of $|\Phi_n^+\rangle$, while the other qubits are left undisturbed, the resulting state is $|\Phi_n^-\rangle$, and vice versa. Therefore, if P is applied to any *four* qubits of $|\Phi_n^+\rangle$ or $|\Phi_n^-\rangle$, while the other qubits are left undisturbed, the global state stays the same. Therefore, if the qubits of $|\Phi_n^+\rangle$ are distributed among the n players, and if exactly m of them apply P to their qubit, the resulting global state remains $|\Phi_n^+\rangle$ if $m \equiv 0 \pmod 4$, whereas it evolves to $|\Phi_n^-\rangle$ if $m \equiv 2 \pmod 4$.

Furthermore, the effect of applying the Walsh-Hadamard transform to each qubit in $|\Phi_n^+\rangle$ is to produce an equal superposition of all even n-bit strings, whereas the effect of applying the Walsh-Hadamard transform to each qubit in $|\Phi_n^-\rangle$ is to produce an equal superposition of all odd n-bit strings. More formally,

$$\begin{aligned} (H^{\otimes n})|\Phi_n^+\rangle &= \frac{1}{\sqrt{2^{n-1}}}\sum_{y \text{ even}} |y\rangle \\ (H^{\otimes n})|\Phi_n^-\rangle &= \frac{1}{\sqrt{2^{n-1}}}\sum_{y \text{ odd}} |y\rangle \end{aligned}$$

where y ranges over all n-bit strings.

The quantum winning strategy should now be obvious. In the initialization phase, the n qubits of state $|\Phi_n^+\rangle$ are distributed among the n players. After they have moved apart, each player A_i receives input bit x_i and does the following:

1. apply transformation P to qubit if $x_i = 1$ (skip this step otherwise);
2. apply H to qubit;
3. measure qubit in the computational basis ($|0\rangle$ versus $|1\rangle$) in order to obtain y_i ;
4. produce y_i as output.

We know by the promise that an even number of players will apply P to their qubit. If that number is divisible by 4, which happens when $\frac{1}{2}\sum_i x_i$ is even, then the global state reverts to $|\Phi_n^+\rangle$ after step 1 and therefore to a superposition of all $|y\rangle$ such that y is even after step 2. It follows that $\sum_i y_i$, the number of players who measure and output 1, is even. On the other hand, if the number of players who apply P to their qubit is congruent to 2 modulo 4, which happens when $\frac{1}{2}\sum_i x_i$ is odd, then the global state evolves to $|\Phi_n^-\rangle$ after step 1 and therefore to a superposition of all $|y\rangle$ such that y is odd after step 2. It follows in this case that $\sum_i y_i$ is odd. In either case, Equation 1 is satisfied at the end of the strategy, as required. □

3 Optimal Proportion for Deterministic Strategies

In this section, we prove matching upper and lower bounds on the success proportion achievable by deterministic strategies that play game G_n for any $n \geq 3$.

Theorem 2 *Any deterministic strategy for game G_n is successful in proportion at most $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$.*

Proof. Let S be a deterministic strategy specified by S_{ij}, where $S_{ij} = 1$ if player i's output on input j is 0 and $S_{ij} = -1$ otherwise. Notice that we can consider the sign of the product of a subset of the S_{ij}s in order to determine if the game is won: for a given question $x = x_1 x_2 \cdots x_n$, $\prod_{i=1}^n S_{ix_i} = 1$ if the players' answer $y = y_1 y_2 \cdots y_n$ is even and $\prod_{i=1}^n S_{ix_i} = -1$ if the players' answer is odd. Consider the following quantity s.

$$s = \prod_{i=1}^{n} (S_{i0} + \imath S_{i1}) \tag{2}$$

$$= \sum_{x \in \{0,1\}^n} \left(\imath^{\Delta(x)} \prod_{i=1}^{n} S_{i\,x_i} \right) \tag{3}$$

where $\Delta(x) = \sum_i x_i$ denotes the Hamming weight of x (the number of 1s in x). By expanding the product into a sum, we see that each term corresponds to an n-bit string x. If $\Delta(x)$ is odd, then the question x is not legitimate, in which case $\imath^{\Delta(x)}$ is purely imaginary. Otherwise, if x is legitimate, $\imath^{\Delta(x)}$ is real. More to the point, $\imath^{\Delta(x)} = 1$ if $\frac{1}{2}\sum_i x_i$ is even and $\imath^{\Delta(x)} = -1$ otherwise.

In order for strategy S to give an appropriate answer on question x, we must have that $\prod_i S_{i\,x_i} = 1$ if $\frac{1}{2}\sum_i x_i$ is even and $\prod_i S_{i\,x_i} = -1$ otherwise. Combining this with the previous observations, we conclude that for all legitimate questions, the corresponding term in the expansion of s (Equation 3) is 1 if the strategy gives an appropriate answer on question x, and it is -1 otherwise. It follows that $\mathrm{Re}(s)$, the real part of s, is precisely the number of appropriate answers minus the number of inappropriate answers provided by strategy S, counted on the set of all legitimate questions. To upper-bound $\mathrm{Re}(s)$, we revert to Equation 2. Consider each factor of the product that defines s: $S_{i0} + \imath S_{i1} = \sqrt{2} e^{\imath a_i \pi/4}$ for some a_i in $\{1, 3, 5, 7\}$. Thus, if n is even, we have $s \in \{2^{n/2}, \imath 2^{n/2}, -2^{n/2}, -\imath 2^{n/2}\}$ and $\mathrm{Re}(s) \leq 2^{n/2}$. If n is odd, we have $s \in \{2^{n/2}(\pm\frac{1}{\sqrt{2}} \pm \frac{1}{\sqrt{2}}\imath)\}$ and $\mathrm{Re}(s) = \pm 2^{(n-1)/2}$. In either case, $\mathrm{Re}(s) \leq 2^{\lfloor n/2 \rfloor}$.

The difference between the number of appropriate answers and the number of inappropriate answers is at most $\mathrm{Re}(s) \leq 2^{\lfloor n/2 \rfloor}$, but the sum of those two numbers is 2^{n-1}, the total number of legitimate questions. It follows—by adding these two statements and dividing by 2—that the number of appropriate answers is at most $2^{n-2} + 2^{\lfloor n/2 \rfloor - 1}$. The desired upper bound on the proportion of appropriate answers is finally obtained after a division by the number of legitimate questions:

$$\frac{2^{n-2} + 2^{\lfloor n/2 \rfloor - 1}}{2^{n-1}} = \tfrac{1}{2} + 2^{-\lceil n/2 \rceil}.$$

□

It turns out that *very* simple deterministic strategies achieve the bound given in Theorem 2. In particular, the players do not even have to look at their input when $n \not\equiv 2 \pmod 4$. Even when $n \equiv 2 \pmod 4$, it is sufficient for a single player to look at his input!

Theorem 3 *There is a classical deterministic strategy for game G_n that is successful in proportion exactly $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$.*

Proof. A tedious but straightforward case analysis suffices to establish that the following simple strategies (Table 1), which depend on $n \pmod 8$, succeed in proportion exactly $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$. We have used two bits to represent a player's strategy, where the first bit of the pair denotes the strategy's output y_i if the input bit is $x_i = 0$ and the second bit of the strategy denotes its output if the input is $x_i = 1$. (For example, player 1 would output $y_1 = 0$ on input $x_1 = 1$ if n is congruent to 6 modulo 8.) A pair of identical bits as strategy means that the corresponding player outputs that bit regardless of his input bit. □

Table 1 Simple Optimal Strategies

$n \pmod 8$	player 1	players 2 to n
0	00	00
1	00	00
2	01	00
3	11	11
4	11	00
5	00	00
6	10	00
7	11	11

4 Optimal Probability for Classical Strategies

In this section, we consider all possible *classical* strategies to play game G_n, including probabilistic strategies. We give as much power as possible to the classical model by allowing the playing parties unlimited sharing of random variables. Despite this, we prove that no classical strategy can succeed with a probability that is significantly better than $^1/_2$ on the worst-case question, and we show that our lower bound is tight by exhibiting a probabilistic classical strategy that achieves it.

Definition 1 *A probabilistic strategy $\mathcal{S}$ is a probability distribution over a finite set of deterministic strategies.*

Without loss of generality, the random variables shared by the players during the initialization phase correspond to deciding which deterministic strategy will be used for any given instance of the game.

Notation 1 *Given an arbitrary strategy $\mathcal{S}$ and legitimate question x, let $\Pr_{\mathcal{S}}(\text{win} \mid x)$ denote the probability that strategy $\mathcal{S}$ provides an appropriate answer on question x, and let*

$$\Pr_{\mathcal{S}}(\text{win}) = \frac{1}{2^{n-1}} \sum_x \Pr_{\mathcal{S}}(\text{win} \mid x)$$

denote the average success probability of strategy S when the question is chosen at random according to the uniform distribution among all legitimate questions.

Whenever S is a deterministic strategy, note that $\Pr_{\mathcal{S}}(\text{win} \mid x) \in \{0,1\}$ and $\Pr_{\mathcal{S}}(\text{win})$ is the same as what we had called the success proportion. If $\mathcal{S}$ is a probabilistic strategy, $\Pr_{\mathcal{S}}(\text{win})$ corresponds also to the success proportion, which is not to be confused with the more interesting notion of success *probability*. Indeed, the formal definition of the success probability of $\mathcal{S}$ involves taking the *minimum* rather than the average of the $\Pr_{\mathcal{S}}(\text{win} \mid x)$ over all x.

It is well known [25] that the success probability of an arbitrary classical strategy, even probabilistic, can never exceed the success proportion of the best possible deterministic strategy (for the case of pseudo-telepathy, this is proved in [6]). Even though Theorem 4 (below) follows directly from this general principle, we give it an explicit proof for the sake of completeness.

Theorem 4 *Any classical strategy for game G_n is successful with probability at most $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$.*

Proof. Consider a general probabilistic strategy $\mathcal{S}$, which is a probability distribution over deterministic strategies $\{s_1, s_2, \ldots, s_\ell\}$. Let $\Pr(s_j)$ be the probability that strategy s_j be chosen on any given instance of the game. Let p be the success probability of $\mathcal{S}$, which is the quantity of interest in this theorem. By definition, $p \leq \Pr_{\mathcal{S}}(\text{win} \mid x)$ for any legitimate question x, and therefore $p \leq \Pr_{\mathcal{S}}(\text{win})$ as well. (This simply says that the minimum can never exceed the average.) Also by definition,

$$\Pr_{\mathcal{S}}(\text{win} \mid x) = \sum_j \Pr(s_j) \Pr_{s_j}(\text{win} \mid x) \,.$$

Putting it all together,

$$\begin{aligned}
p &\leq \Pr_{\mathcal{S}}(\text{win}) \\
&= \frac{1}{2^{n-1}} \sum_x \Pr_{\mathcal{S}}(\text{win} \mid x) \\
&= \frac{1}{2^{n-1}} \sum_x \sum_j \Pr(s_j) \Pr_{s_j}(\text{win} \mid x) \\
&= \sum_j \Pr(s_j) \frac{1}{2^{n-1}} \sum_x \Pr_{s_j}(\text{win} \mid x) \\
&= \sum_j \Pr(s_j) \Pr_{s_j}(\text{win}) \\
&\leq \sum_j \Pr(s_j) \left(\tfrac{1}{2} + 2^{-\lceil n/2 \rceil}\right) \\
&= \tfrac{1}{2} + 2^{-\lceil n/2 \rceil} \,.
\end{aligned}$$

The last inequality comes from Theorem 2. □

We now proceed to prove that Theorem 4 is tight.

Definition 2 *We define an* optimal strategy *to be a deterministic strategy that is successful in proportion exactly* $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$.

We know from Theorem 3 that optimal strategies exist and from Theorem 2 that they are optimal indeed.

Definition 3 *A set O of optimal strategies is* balanced *if the number of strategies in O that answer appropriately any given legitimate question is the same for each legitimate question.*

Note that it is not *a priori* obvious that nontrivial balanced sets of optimal strategies exist at all. We shall prove this later, but let us take them for granted for now.

Lemma 1 *Consider any nonempty balanced set O of optimal strategies. Define probabilistic strategy $\mathcal{S}$ for game G_n as a uniform distribution over O. Then $\mathcal{S}$ is successful with probability* $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$.

Proof. Consider the proof of Theorem 4. Because O is balanced, $\Pr_{\mathcal{S}}(\text{win} \mid x)$ is the same for all x, and therefore the average of these values is the same as their minimum. This means that if p is the success probability of $\mathcal{S}$, then $p = \Pr_{\mathcal{S}}(\text{win})$ as well. Moreover, $\Pr_{s_j}(\text{win}) = \frac{1}{2} + 2^{-\lceil n/2 \rceil}$ for each j because each s_j is optimal. It follows that both inequalities in the proof of Theorem 4 become equalities, and therefore the success probability of $\mathcal{S}$ is $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$. □

Theorem 5 *There is a classical probabilistic strategy for game G_n that is successful with probability exactly* $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$.

Proof. Consider the probabilistic strategy $\mathcal{S}$ that is a uniform distribution over the set O of *all* optimal strategies. If we show that O is balanced, then it follows by Lemma 1 that $\mathcal{S}$ is successful with probability $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$.

Using the same notation as in Theorem 2, a deterministic strategy S is optimal if and only if

$$\mathrm{Re}\left[\prod_{i=1}^{n}(S_{i0} + \imath S_{i1})\right] = 2^{\lfloor n/2 \rfloor} .$$

We proceed to show that if we flip two bits of any legitimate question, we get another legitimate question for which there are at least as many optimal strategies that give an appropriate answer. Because it is possible to go from any legitimate question to any other legitimate question by a sequence of two-bit flips, this shows that the number of optimal strategies that give an appropriate answer is the same for all legitimate questions.

Assume without lost of generality that the two questions differ in the first two positions. Assume furthermore that $x = 00x_3 \cdots x_n$ and $x' = 11x_3 \cdots x_n$. (A similar reasoning works if the first two bits of x are 01, 10 or 11, or if the two questions differ in any other two positions.)

To each optimal strategy S that gives an appropriate answer for x, we associate a strategy S' that gives an appropriate answer for x'. The mapping that does the association between the strategies is a one-to-one correspondence defined as follows: $S'_{10} = S_{11}$, $S'_{11} = -S_{10}$, $S'_{20} = -S_{21}$, $S'_{21} = S_{20}$, and for all $i \geq 3$ and $j \in \{0,1\}$, $S'_{ij} = S_{ij}$. We have that $S'_{11}S'_{21} = -S_{10}S_{20}$, which means that the answer given by strategy S' on question x' is as appropriate as the answer given by strategy S on question x. Moreover,

$$\begin{aligned}(S'_{10}+\imath S'_{11})(S'_{20}+\imath S'_{21}) &= (S_{11}-\imath S_{10})(-S_{21}+\imath S_{20})\\ &= -S_{11}S_{21}+\imath S_{11}S_{20}+\imath S_{10}S_{21}+S_{10}S_{20}\\ &= (S_{10}+\imath S_{11})(S_{20}+\imath S_{21})\,.\end{aligned}$$

This shows that

$$\prod_{i=1}^{n}(S'_{i0}+\imath S'_{i1}) = \prod_{i=1}^{n}(S_{i0}+\imath S_{i1})\,.$$

Since these products are the same, so is their real part, which is equal to $2^{\lfloor n/2 \rfloor}$ given that S is optimal. Therefore, S' is optimal as well. This establishes that at least as many optimal strategies give the appropriate answer on x' than on x, and therefore this number of optimal strategies is the same for all legitimate questions. This concludes the proof that the set of all optimal strategies is balanced, and therefore that $\mathcal{S}$ is successful with probability $\frac{1}{2}+2^{-\lceil n/2 \rceil}$ by virtue of Lemma 1. □

5 Imperfect Apparatus

Quantum devices are often unreliable and thus we cannot expect to witness the perfect results predicted by quantum mechanics in Theorem 1. However, the following analysis shows that reasonable imperfections in the apparatus can be tolerated if we are satisfied with making experiments in which a quantum-mechanical strategy succeeds with a probability that is still better than anything classically achievable. Provided care is taken to make it impossible for the players to "cheat" by communicating after their inputs have been chosen (see [6] for a detailed discussion on this issue), this would definitively rule out any possible classical (local realistic) theories of the universe.

First consider the following model of imperfect apparatus. Assume that the classical bit y_i that is output by each player A_i corresponds to the predictions of quantum mechanics—should the apparatus be perfect—with some probability p. With complementary probability $1-p$, the player outputs the complement of that bit. Assume furthermore that the errors are independent between players. In other words, we model this imperfection as if each player would flip his (perfect) output bit with probability $1-p$. Please note that this assumption of independence does *not* model imperfections that might occur in the entanglement shared between the players.

Theorem 6 *For any $p > \frac{1}{2}+\frac{\sqrt{2}}{4} \approx 85\%$ and for any sufficiently large number n of players, the success probability of the quantum strategy given in the proof of Theorem 1 for game G_n remains strictly better than anything classically achievable, provided each player outputs what is predicted by quantum mechanics with probability at least p, independently from one another.*

Proof. In the n-player imperfect quantum strategy, the probability p_n of winning the game is given by the probability of having an even number of errors.

$$p_n = \sum_{i \text{ even}} \binom{n}{i} p^{n-i}(1-p)^i$$

It is easy to prove by mathematical induction that

$$p_n = \frac{1}{2}+\frac{(2p-1)^n}{2}\,.$$

Let's concentrate for now on the case where n is odd, in which case $\lceil n/2 \rceil = (n+1)/2$. By Theorem 4, the success probability of any classical strategy is upper-bounded by

$$p'_n = \frac{1}{2} + \frac{1}{2^{(n+1)/2}} .$$

For any fixed n, define

$$e_n = \frac{1}{2} + \frac{(\sqrt{2}\,)^{1+1/n}}{4} .$$

It follows from elementary algebra that

$$p > e_n \;\Rightarrow\; p_n > p'_n .$$

In other words, the imperfect quantum strategy on n players surpasses anything classically achievable provided $p > e_n$. For example, $e_3 \approx 89.7\%$ and $e_5 \approx 87.9\%$. Thus we see that even the game with as few as 3 players is sufficient to exhibit genuine quantum behaviour if the apparatus is at least 90% reliable. As n increases, the threshold e_n decreases. In the limit of large n, we have

$$\lim_{n\to\infty} e_n = \frac{1}{2} + \frac{\sqrt{2}}{4} \approx 85\% .$$

The same limit is obtained for the case when n is even. □

Another way of modelling an imperfect apparatus is to assume that it will never give the wrong answer, but that sometimes it fails to give an answer at all. This is the type of behaviour that gives rise to the infamous *detection loophole* in experimental tests that the world is not classical [19] because we say that the apparatus "detects" the correct answer with some probability η, whereas it fails to detect an answer with complementary probability $1-\eta$.

To formalize this model, we allow players (classical or quantum) to answer a special symbol $\perp$ instead of 0 or 1. We say that a strategy is *error-free* if, given any legitimate question, one of two things happens:

1. at least one player produces $\perp$ as output, in which case we say that the answer is a *draw*; or

2. the answer is appropriate for the given question, which can only happen when none of the players output $\perp$.

We say that a player "provides an output" whenever that output is not $\perp$. The larger the probability of obtaining an appropriate answer for the worst possible question, the better the strategy. We are concerned with the smallest possible detection threshold η that makes a quantum implementation better than any error-free classical strategy. But first, we need a Lemma.

Lemma 2 *Given any classical deterministic error-free strategy for game G_n, there are at most two legitimate questions on which the players can provide an appropriate answer.*

Proof. Let us dismiss the possibility for some player to output $\perp$ on both possible inputs because in that case there would be no questions at all on which an appropriate answer is obtained. We say of a player that he is *interesting* if he never outputs $\perp$. For any i, define $q_i = \star$ if player i is interesting, and otherwise define q_i as the one input (0 or 1) that results in a non-$\perp$ output for that player. Consider the string $q = q_1 q_2 \cdots q_n$ of symbols from $\{0, 1, \star\}$. We say that an n-bit string $x = x_1 x_2 \cdots x_n$ is *answerable* if $x_i = q_i$ whenever $q_i \neq \star$. The questions that give rise to an appropriate answer are precisely those that are both answerable and legitimate. Let ℓ denote the number of interesting players. There are 2^ℓ answerable questions and exactly half of them are legitimate provided $\ell > 0$. It follows that there are $2^{\ell-1}$ legitimate questions on which the players will provide an appropriate answer. (If $\ell = 0$, there is only one answerable question, which may be legitimate or not, and therefore there is at most one legitimate question on which the players will provide an appropriate answer.)

Consider any interesting player. We say that he is *passive* if his output does not depend on his input, and that he is *active* otherwise. Finally, we say that two players are *compatible* either if they are both active or both passive. Assume now for a contradiction that $\ell \geq 3$. Among the ℓ interesting players, there must necessarily be at least two who are compatible; call them Alice and Bob. Consider any legitimate question that is answerable for which the input to both Alice and Bob is 0. (This is always possible by using the degree of freedom provided by the input to the third interesting player.) If we flip the inputs of Alice and Bob, the new question is still legitimate and still answerable. The parity of the answer given by the players on those two questions is the same because Alice and Bob are compatible. But it should *not* be the same because there are two more 1s in the new question. We conclude from this contradiction that $\ell \leq 2$.

The Lemma follows from the fact that there are $2^{\ell-1}$ legitimate questions on which the players will provide an appropriate answer, and $2^{\ell-1} \leq 2$ given that $\ell \leq 2$. □

We now give a simple optimal error-free deterministic strategy for the game G_n: it succeeds on exactly two questions. All players output 0 on input 0 and $\perp$ on input 1, except for the first two players. Player 1 outputs 0 on both inputs and player 2 outputs 0 on input 0 and 1 on input 1. All legitimate questions lead to a draw, except questions $000 \cdots 0$ and $110 \cdots 0$, on which an appropriate answer is indeed obtained.

Theorem 7 *For all $\eta > {}^1\!/_2$ and for any sufficiently large number n of players, the probability that the quantum strategy given in the proof of Theorem 1 for game G_n will produce an appropriate answer remains strictly better than anything classically achievable by an error-free strategy, provided each player outputs what is predicted by quantum mechanics with probability at least η, independently from one another, and outputs $\perp$ otherwise. The probabilities are taken according to the uniform distribution on the set of all legitimate questions.*

Proof. There are 2^{n-1} legitimate questions and any classical deterministic error-free strategy is such that at most two questions give rise to an appropriate answer. When the questions are asked according to the uniform distribution on the set of all legitimate questions, the best a classical deterministic error-free strategy can do is to provide an appropriate answer with probability $\frac{2}{2^{n-1}}$. It is easy to see that classical *probabilistic* error-free strategies cannot fare any better.

On the other hand, if each quantum player from the proof of Theorem 1 outputs the answer predicted by quantum mechanics with probability η and answers $\perp$ with complementary probability $1 - \eta$, and if these events are independent, then the probability to obtain an appropriate answer (none of the players output $\perp$) is $p_\eta = \eta^n$. Elementary algebra suffices to show that $p_\eta > \frac{2}{2^{n-1}}$ precisely when $\eta > \frac{\sqrt[n]{4}}{2}$. The theorem follows from the fact that

$$\lim_{n\to\infty} \frac{\sqrt[n]{4}}{2} = \frac{1}{2}\,.$$

□

This result is a significant improvement over [9], which required the probability for each quantum player to provide a non-$\perp$ output to be greater than $\frac{1}{\sqrt{2}} \approx 71\%$ even in the limit of large n.

6 Conclusions and Open Problems

We have recast Mermin's n-player game into the framework of pseudo-telepathy, which makes it easier to understand for non-physicists, and in particular for computer scientists. An upper bound was known on the success proportion for any possible classical deterministic strategy, and therefore also for the probability of success for any possible classical probabilistic strategy. In this paper, we have proved that these upper bounds are tight. We have analysed the issue of when a quantum implementation based on imperfect or inefficient quantum apparatus remains better than anything classically achievable. In the case of inefficient apparatus, our analysis provides a significant improvement on what was previously known.

A lot is known about pseudo-telepathy [6] but many questions remain open. The game studied in this article has been generalized to larger inputs [27, 12] and larger outputs [3]. It would be interesting to have tight bounds for those more general games. Also, it would be interesting to know how to construct the pseudo-telepathy game that minimizes classical success probability when the dimension of the entangled quantum state is fixed. In all the pseudo-telepathy games known so far, it is sufficient for the quantum players to perform a projective von Neumann measurement. Could there be a *better* pseudo-telepathy game (in the sense of making it harder on classical players) that would make inherent use of generalized measurements (POVM)?

We have modelled imperfect apparatus in two different ways: when they produce incorrect outcomes and when they don't produce outcomes at all. It would be natural to combine those two models into a more realistic one, in which each player receives an outcome with probability η, but that outcome is only correct with probability p. Finally, we should model other types of errors in the quantum process, such as imperfections in the prior entanglement shared among the players.

Acknowledgements

We are most grateful to Serge Massar for pointing out Mermin's paper [21] after we thought we had invented this game [5]! We are also grateful to George Savvides for helping us simplify some of our proofs.

References

1. Aaronson, S., Ambainis, A., "Quantum search of spatial regions", *Proceedings of 44th Annual IEEE Symposium on Foundations of Computer Science*, pp. 200–209, 2003. Full version available as arXiv:quant-ph/0303041.
2. Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W. K., "Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels", *Physical Review Letters* **70**:1895–1899, 1993.

3. Boyer, M., "Extended GHZ n-player games with classical probability of winning tending to 0". Available as arXiv:quant-ph/0408090, 2004.
4. Brassard, G., "Quantum communication complexity", *Foundations of Physics* **33**:1593–1616, 2003.
5. Brassard, G., Broadbent, A., Tapp, A., "Multi-party pseudo-telepathy", *Proceedings of 8th International Workshop on Algorithms and Data Structures*, Volume 2748 of *Lecture Notes in Computer Science*, pp. 1–11, 2003.
6. Brassard, G., Broadbent, A., Tapp, A., "Quantum pseudo-telepathy", *Foundations of Physics* **35**(11), November 2005. Available as arXiv:quant-ph/0407221.
7. Brassard, G., Cleve, R., Tapp, A., "Cost of exactly simulating quantum entanglement with classical communication", *Physical Review Letters* **83**:1874–1878, 1999.
8. Brassard, G., Méthot, A. A., Tapp, A., "Minimum entangled state dimension required for pseudo-telepathy", *Quantum Information & Computation*, **5**:275–284, 2005.
9. Braunstein, S. L., Mann, A., "Noise in Mermin's n-particle Bell inequality", *Physical Review A* **47**:R2427–R2430, 1993.
10. Buhrman, H., Cleve, R., van Dam, W., "Quantum entanglement and communication complexity", *SIAM Journal on Computing* **30**:1829–1841, 2001.
11. Buhrman, H., Cleve, R., Wigderson, A., "Quantum vs. classical communication and computation", *Proceedings of 30th Annual ACM Symposium on Theory of Computing*, pp. 63–68, 1998.
12. Buhrman, H., Høyer, P., Massar, S., Röhrig, H., "Combinatorics and quantum nonlocality", *Physical Review Letters* **91**:047903.1–047903.4, 2003.
13. Cleve, R., Buhrman, H., "Substituting quantum entanglement for communication", *Physical Review A* **56**:1201–1204, 1997.
14. Cleve, R., van Dam, W., Nielsen, M., Tapp, A., "Quantum entanglement and the communication complexity of the inner product function", *Proceedings of First NASA International Conference on Quantum Computing and Quantum Communication (QCQC'98)*, Lecture Notes in Computer Science, Vol. 1590 (Springer, 1999), pp. 61–74.
15. Greenberger, D. M., Horne, M. A., Zeilinger, A., "Going beyond Bell's theorem", in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, M. Kafatos (editor), pp. 69–72, 1989.
16. Hardy, L., "Quantum mechanics, local realistic theories, and Lorentz-invariant realistic theories", *Physical Review Letters* **68**:2981–2984, 1992.
17. Heywood, P., Redhead, M. L. G., "Nonlocality and the Kochen-Specker paradox", *Foundations of Physics* **13**:481–499, 1983.
18. Kalyanasundaram, B., Schnitger, G., "The probabilistic communication complexity of set intersection", *Proceedings of 2nd Annual IEEE Conference on Structure in Complexity Theory*, pp. 41–47, 1987.
19. Massar, S., "Nonlocality, closing the detection loophole, and communication complexity", *Physical Review A* **65**:032121.1–032121.5, 2002.
20. Mermin, N. D., "Quantum mysteries revisited", *American Journal of Physics* **58**:731–734, 1990.
21. Mermin, N. D., "Extreme quantum entanglement in a superposition of macroscopically distinct states", *Physical Review Letters* **65**:1838–1840, 1990.
22. Nielsen, M. A., Chuang, I. L., *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
23. Raz, R., "Exponential separation of quantum and classical communication complexity", *Proceedings of 31st Annual ACM Symposium on Theory of Computing*, pp. 358–367, 1999.
24. de Wolf, R., "Quantum communication and complexity", *Theoretical Computer Science* **287**:337–353, 2002.
25. Yao, A. C.–C., "Probabilistic computations: toward a unified measure of complexity", *Proceedings of 18th Annual IEEE Symposium on Foundations of Computer Science*, pp. 222–227, 1977.
26. Yao, A. C.–C., "Quantum circuit complexity", *Proceedings of 34th Annual IEEE Symposium on Foundations of Computer Science*, pp. 352–361, 1993.
27. Żukowksi, M., "Bell theorem involving all settings of measuring apparatus", *Physics Letters A* **177**:290–296, 1993.