Multi-party Pseudo-Telepathy

Gilles Brassard*, Anne Broadbent**, and Alain Tapp***

Département IRO, Université de Montréal, C.P. 6128, succursale centre-ville,
Montréal (Québec), Canada H3C 3J7
{brassard,broadbea,tappa}@iro.umontreal.ca

Abstract. Quantum entanglement, perhaps the most non-classical manifestation of quantum information theory, cannot be used to transmit information between remote parties. Yet, it can be used to reduce the amount of communication required to process a variety of distributed computational tasks. We speak of *pseudo-telepathy* when quantum entanglement serves to *eliminate* the classical need to communicate. In earlier examples of pseudo-telepathy, classical protocols could succeed with high probability unless the inputs were very large. Here we present a simple multi-party distributed problem for which the inputs and outputs consist of a single bit per player, and we present a perfect quantum protocol for it. We prove that no classical protocol can succeed with a probability that differs from $^1/_2$ by more than a fraction that is exponentially small in the number of players. This could be used to circumvent the detection loophole in experimental tests of nonlocality.

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 [3], through the use of either quantum communication [13] or quantum entanglement [6]. Consider for example the case of Alice and Bob, who are very busy and 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 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 [8], 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

* Supported in part by Canada's NSERC, Québec's FCAR, the Canada Research Chair Programme, and the Canadian Institute for Advanced Research.
** Supported in part by a scholarship from Canada's NSERC.
*** Supported in part by Canada's NSERC and Québec's FCAR.

F. Dehne, J.-R. Sack, M. Smid (Eds.): WADS 2003, LNCS 2748, pp. 1–11, 2003.

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 [5] and bounded-error [11] models.

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 share prior entanglement? The answer is negative if the result of the computation must become known to at least one party, but it is positive if we are satisfied with the establishment of nonlocal correlations between the parties' inputs and outputs [4].

Mathematically, consider n parties $A_1, A_2, \ldots, A_n$ and two n-ary functions f and g. In an *initialization phase*, the parties are allowed to discuss strategy and share random variables (in the classical setting) and entanglement (in the quantum setting). Then the parties move apart and they are no longer allowed any form of communication. After the parties are physically separated, each A_i is given some input x_i and is requested to produce output y_i. We say that the parties *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 protocol is *perfect* if it wins the game with certainty on all inputs that satisfy the promise, i.e. whenever $P(x_1, x_2, \ldots x_n)$ holds. A protocol 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 protocol that succeeds with probability p automatically succeeds in proportion p, but not necessarily vice versa. In particular, it is possible for a protocol that succeeds in proportion $p > 0$ to fail systematically on some inputs, whereas this would not be allowed for protocols that succeed with probability $p > 0$. Therefore, the notion of succeeding "in proportion" is meaningful for *deterministic* protocols but not the notion of succeeding "with probability".

We say of a quantum protocol that it exhibits *pseudo-telepathy* if it is perfect provided the parties share prior entanglement, whereas no perfect classical protocol can exist. The study of pseudo-telepathy was initiated in [4], but all examples known so far allowed for classical protocols that succeed with rather high probability, unless the inputs are very long. This made the prospect of experimental demonstration of pseudo-telepathy unappealing for two reasons.

- ◇ It would not be surprising for several runs of an imperfect classical protocol to succeed, so that mounting evidence of a convincingly quantum behaviour would require a large number of consecutive successful runs.
- ◇ Even a slight imperfection in the quantum implementation would be likely to result in an error probability higher than what can easily be achieved with simple classical protocols!

In Section 2, we introduce a simple multi-party distributed computational problem for which the inputs and outputs consist of a single bit per player, and we present a perfect quantum protocol for it. We prove in Sections 3 and 4 that no classical protocol can succeed with a probability that differs from $^1/_2$ by more than a fraction that is exponentially small in the number of players. More precisely, no classical protocol can succeed with a probability better than $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$, where n is the number of players. Furthermore, we show in Section 5 that the success probability of our quantum protocol would remain better than anything classically achievable, when n is sufficiently large, even if each player had imperfect apparatus that would produce the wrong answer with probability nearly 15% or no answer at all with probability 29%. This could be used to circumvent the infamous *detection loophole* in experimental proofs of the nonlocality of the world in which we live [9].

2 A Simple Game and Its Perfect Quantum Protocol

For any $n \geq 3$, game G_n consists of 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 their inputs, the players are challenged to produce a collective output that contains an even number of 1s if and only if the number of 1s in the input is divisible by 4. More formally, we require that

$$\sum_i^n y_i \;\equiv\; \tfrac{1}{2}\sum_i^n x_i \pmod 2 \tag{1}$$

provided $\sum_i^n x_i \equiv 0 \pmod 2$. We say that $x = x_1 x_2 \ldots x_n$ is the *question* and $y = y_1 y_2 \ldots y_n$ is the *answer*.

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

Proof. (In this proof, we assume that the reader is familiar with basic concepts of quantum information processing [10].) Define the following n-qubit entangled quantum states $|\Phi_n^+\rangle$ and $|\Phi_n^-\rangle$.

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

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

$$H|0\rangle \mapsto \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle$$
$$H|1\rangle \mapsto \tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle$$

and let S denote the unitary transformation defined by

$$S|0\rangle \mapsto |0\rangle$$
$$S|1\rangle \mapsto i|1\rangle\,.$$

It is easy to see that if S is applied to any two qubits of $|\Phi_n^+\rangle$, while the other qubits are left undisturbed, then the resulting state is $|\Phi_n^-\rangle$, and if S is applied to any two qubits of $|\Phi_n^-\rangle$, then the resulting state is $|\Phi_n^+\rangle$. Therefore, if the qubits of $|\Phi_n^+\rangle$ are distributed among the n players, and if exactly m of them apply S to their qubit, the resulting global state will be $|\Phi_n^+\rangle$ if $m \equiv 0 \pmod 4$ and $|\Phi_n^-\rangle$ if $m \equiv 2 \pmod 4$.

Moreover, the effect of applying the Walsh-Hadamard transform to each qubit in $|\Phi_n^+\rangle$ is to produce an equal superposition of all classical n-bit strings that contain an even number of 1s, whereas the effect of applying the Walsh-Hadamard transform to each qubit in $|\Phi_n^-\rangle$ is to produce an equal superposition of all classical n-bit strings that contain an odd number of 1s. More formally,

$$(H^{\otimes n})|\Phi_n^+\rangle = \tfrac{1}{\sqrt{2^{n-1}}} \sum_{\substack{\Delta(y)\equiv 0 \\ (\mathrm{mod}\ 2)}} |y\rangle$$
$$(H^{\otimes n})|\Phi_n^-\rangle = \tfrac{1}{\sqrt{2^{n-1}}} \sum_{\substack{\Delta(y)\equiv 1 \\ (\mathrm{mod}\ 2)}} |y\rangle\,,$$

where $\Delta(y) = \sum_i y_i$ denotes the Hamming weight of y.

The quantum winning strategy should now be obvious. In the initialization phase, state $|\Phi_n^+\rangle$ is produced and its n qubits 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. If $x_i = 1$, A_i applies transformation S to his qubit; otherwise he does nothing.
2. He applies H to his qubit.
3. He measures his qubit in order to obtain y_i.
4. He produces y_i as his output.

We know by the promise that an even number of players will apply S to their qubit. If that number is divisible by 4, which means that $\frac{1}{2}\sum_i^n x_i$ 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 $\Delta(y) \equiv 0 \pmod 2$ after step 2. It follows that $\sum_i^n y_i$, the number of players who measure and output 1, is even. On the other hand, if the number of players who apply S to their qubit is congruent to 2 modulo 4, which

means that $\frac{1}{2}\sum_i^n x_i$ 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 $\Delta(y) \equiv 1 \pmod 2$ after step 2. It follows in this case that $\sum_i^n y_i$ is odd. In either case, Equation (1) is fulfilled at the end of the protocol, as required. □

3 Optimal Proportion for Deterministic Protocols

In this section, we study the case of *deterministic* classical protocols to play game G_n. We show that no such protocol can succeed on a proportion of the allowed inputs that is significantly better than $1/2$.

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

Proof. Since no information may be communicated between players during the game, the best they can do is to agree on a strategy before the game starts. Any such deterministic strategy will be such that player A_i's answer y_i depends only on his input bit x_i. Therefore, each player has an individual strategy $s_i \in \{01, 10, 00, 11\}$, 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 $x_i = 1$. In other words, 00 and 11 denote the two constant strategies $y_i = 0$ and $y_i = 1$, respectively, 01 denotes the strategy that sets $y_i = x_i$, and 10 denotes the complementary strategy $y_i = \overline{x_i}$.

Let $s = s_1, s_2, \ldots, s_n$ be the global deterministic strategy chosen by the players. The order of the players is not important, so that we may assume without loss of generality that strategy s has the following form.

$$s = \overbrace{01, 01, \ldots, 01}^{k-\ell}, \overbrace{10, 10, \ldots, 10}^{\ell}, \overbrace{00, 00, \ldots, 00}^{n-k-m}, \overbrace{11, 11, \ldots, 11}^{m}$$

Assuming strategy s is being used, the Hamming weight $\Delta(y)$ of the answer is given by

$$\begin{aligned} \Delta(y) &= \Delta(x_1 \ldots, x_{k-\ell}) + \Delta(\overline{x_{k-\ell+1}}, \ldots, \overline{x_k}) + \Delta(\overbrace{00\ldots0}^{n-k-m}) + \Delta(\overbrace{11\ldots1}^{m}) \\ &\equiv \Delta(x_1, \ldots, x_k) + \ell + m \pmod 2 . \end{aligned}$$

Consider the following four sets, for $a, b \in \{0, 1\}$.

$$S_{a,b}^k = \{x \mid \Delta(x_1, \ldots, x_k) \equiv a \pmod 2 \text{ and } \Delta(x_1, \ldots, x_n) \equiv 2b \pmod 4\}$$

If $\ell + m$ is even then there are exactly $|S_{0,0}^k| + |S_{1,1}^k|$ questions that yield a winning answer, and otherwise if $\ell+m$ is odd then there are exactly $|S_{1,0}^k| + |S_{0,1}^k|$ questions that yield a winning answer. We also have that the four sets account for all possible questions and therefore

$$|S_{0,0}^k| + |S_{1,1}^k| \;=\; 2^{n-1} - (|S_{1,0}^k| + |S_{0,1}^k|) .$$

From here, the proof of the Theorem follows directly from Lemma 2 below. □

First we need to state a standard Lemma.

Lemma 1. [7, Eqn. 1.54]

$$\sum_{\substack{i\equiv a\\ (\mathrm{mod}\ 4)}} \binom{n}{i} = \begin{cases} 2^{n-2}+2^{\frac{n}{2}-1} & \text{if } n-2a\equiv 0 \pmod 8 \\ 2^{n-2}-2^{\frac{n}{2}-1} & \text{if } n-2a\equiv 4 \pmod 8 \\ 2^{n-2} & \text{if } n-2a\equiv 2,6 \pmod 8 \\ 2^{n-2}+2^{\frac{n-3}{2}} & \text{if } n-2a\equiv 1,7 \pmod 8 \\ 2^{n-2}-2^{\frac{n-3}{2}} & \text{if } n-2a\equiv 3,5 \pmod 8 \end{cases} \tag{2}$$

Lemma 2. *If n is odd, then*

$$|S^k_{0,0}|+|S^k_{1,1}| = \begin{cases} 2^{n-2}+2^{\frac{n-3}{2}} & \text{if } (n-1)/2+3(n-k)\equiv 0,3 \pmod 4 \\ 2^{n-2}-2^{\frac{n-3}{2}} & \text{if } (n-1)/2+3(n-k)\equiv 1,2 \pmod 4 \end{cases}$$

On the other hand, if n is even, then

$$|S^k_{0,0}|+|S^k_{1,1}| = \begin{cases} 2^{n-2} & \text{if } n/2+3(n-k)\equiv 1,3 \pmod 4 \\ 2^{n-2}+2^{\frac{n}{2}-1} & \text{if } n/2+3(n-k)\equiv 0 \pmod 4 \\ 2^{n-2}-2^{\frac{n}{2}-1} & \text{if } n/2+3(n-k)\equiv 2 \pmod 4 \end{cases}$$

Proof. From the definition of $S^k_{a,b}$, provided we consider that $\binom{0}{a}=0$ whenever $a\neq 0$ and $\binom{0}{0}=1$, we get

$$|S^k_{0,0}| = \sum_{\substack{i\equiv 0\\ (\mathrm{mod}\ 4)}} \binom{k}{i} \sum_{\substack{j\equiv 0\\ (\mathrm{mod}\ 4)}} \binom{n-k}{j} + \sum_{\substack{i\equiv 2\\ (\mathrm{mod}\ 4)}} \binom{k}{i} \sum_{\substack{j\equiv 2\\ (\mathrm{mod}\ 4)}} \binom{n-k}{j} \tag{3}$$

$$|S^k_{1,1}| = \sum_{\substack{i\equiv 1\\ (\mathrm{mod}\ 4)}} \binom{k}{i} \sum_{\substack{j\equiv 1\\ (\mathrm{mod}\ 4)}} \binom{n-k}{j} + \sum_{\substack{i\equiv 3\\ (\mathrm{mod}\ 4)}} \binom{k}{i} \sum_{\substack{j\equiv 3\\ (\mathrm{mod}\ 4)}} \binom{n-k}{j}. \tag{4}$$

Using Lemma 1, we compute (3) and (4). Since n and k are parameters for the equations, and since Lemma 1 depends on the values of n and k modulo 8, we have 8 cases to verify for n and 8 cases for k, hence 64 cases in total. These straightforward, albeit tedious, calculations are left to the reader. □

Theorem 3. *Very simple deterministic protocols achieve the bound given in Theorem 2. In particular, the players do not even have to look at their input when $n \not\equiv 2 \pmod 4$!*

Proof. The following simple strategies, which depend on $n \pmod 8$, are easily seen to succeed in proportion exactly $\frac{1}{2}+2^{-\lceil n/2\rceil}$. They are therefore optimal among all possible deterministic classical strategies. □

Table 1. Simple optimal strategies.

n (mod 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 Protocols

In this section, we consider all possible *classical* protocols to play game G_n, including probabilistic protocols. 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 protocol can succeed with a probability that is significantly better than $1/2$ on the worst-case input.

Definition 1. *A probabilistic strategy is a probability distribution over a set of deterministic strategies.*

The random variable shared by the players during the initialization phase corresponds to deciding which deterministic strategy will be used for any given run of the protocol.

Lemma 3. *Consider any multi-party game of the sort formalized in Section 1. For any probabilistic protocol that is successful with probability p, there exists a deterministic protocol that is successful in proportion at least p.*

Proof. This Lemma is a special case of a theorem proven by Andrew Yao [12], but its proof is so simple that we include it here for completeness. Consider any probabilistic strategy that is successful with probability p. Recall that this means that the protocol wins the game with probability at least p on any instance of the problem that satisfies the promise. By the pigeon hole principle, the same strategy wins the game with probability at least p if the input is chosen uniformly at random among all possible inputs that satisfy the promise. In other words, it is successful *in proportion* at least p. Consider now the deterministic strategies that enter the definition of our probabilistic strategy, according to Definition 1. Assume for a contradiction that the best among them succeeds in proportion $q < p$. Then, again by the pigeon hole principle, any probabilistic mixture of those deterministic strategies (not only the uniform mixture) would succeed in proportion no better than q. But this includes the probabilistic strategy whose existence we assumed, which does succeed in proportion at least p. This implies that $p \leq q$, a contradiction, and therefore at least one deterministic strategy must succeed in proportion at least p. □

Theorem 4. *No classical strategy for game G_n can be successful with a probability better than $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$.*

Proof. Any classical strategy for game G_n that would be successful with probability $p > \frac{1}{2} + 2^{-\lceil n/2 \rceil}$ would imply by Lemma 3 the existence of a deterministic strategy that would succeed in proportion at least p. This would contradict Theorem 2. □

Theorem 4 gives an upper bound on the best probability that can be achieved by any classical strategy in winning game G_n. However, it is still unknown if there exists a classical strategy capable of succeeding with probability $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$. We conjecture that this is the case. Consider the probabilistic strategy that chooses uniformly at random among all the deterministic strategies that are optimal according to Theorem 2. We have been able to prove with the help of Mathematica that this probabilistic strategy is successful with probability $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$ for all $3 \leq n \leq 14$. We have also proved that this probabilistic strategy is successful with probability $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$ for any odd number n of players, but only when the players all receive $x_i = 0$ as input. The general case is still open.

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

5 Imperfect Apparatus

Quantum devices are often unreliable and thus we cannot expect to witness the perfect result predicted by quantum mechanics in Theorem 1. However, the following analysis shows that a reasonably large error probability can be tolerated if we are satisfied with making experiments in which a quantum-mechanical strategy will succeed with a probability that is still better than anything classically achievable. This would be sufficient to rule out classical 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 (if the apparatus were perfect) with some probability p. With complementary probability $1 - p$, the player would output the complement of that bit. Assume furthermore that the errors are independent between players. In other words, we model this imperfection by saying that each player flips his (perfect) output bit with probability $1 - p$.

Theorem 5. *For all $p > \frac{1}{2} + \frac{\sqrt{2}}{4} \approx 85\%$ and for all sufficiently large number n of players, provided each player outputs what is predicted by quantum mechanics (according to the protocol given in the proof of Theorem 1) with probability at least p, the quantum success probability in game G_n remains strictly greater than anything classically achievable.*

Proof. In the n-player imperfect quantum protocol, the probability p_n that the game is won is given by the probability of having an even number of errors:

$$p_n \;=\; \sum_{\substack{i\equiv 0 \\ (\mathrm{mod}\ 2)}} \binom{n}{i} p^{n-i}(1-p)^i \,.$$

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. By Theorem 4, the success probability of any classical protocol 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 protocol 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 the imperfect apparatus is to assume that it gives the correct answer most of the time, but sometimes it fails to give any answer at all. This is the type of behaviour that gives rise to the infamous *detection loophole* in experimental tests of the fact that the world is not classical [9]. When the detectors fail to give an answer, the corresponding player knows that all information is lost. In this case, he has nothing better to do than output a random bit. With this strategy, either every player is lucky enough to register an answer, in which case the game is won with certainty, or at least one player outputs a random answer, in which case the game is won with probability $^1/_2$ regardless of what the other players do.

Corollary 1. *For all $q > \frac{1}{\sqrt{2}} \approx 71\%$ and for all sufficiently large number n of players, provided each player outputs what is predicted by quantum mechanics (according to the protocol given in the proof of Theorem 1) when he receives an answer from his apparatus with probability at least q, but otherwise the player outputs a random answer, the data collected in playing game G_n cannot be explained by any classical local realistic theory.*

Proof. If a player obtains the correct answer with probability q and otherwise outputs a random answer, the probability that the resulting output be correct is $p = q + \frac{1}{2}(1-q) = (1+q)/2$. Therefore, this scenario reduces to the previous one with this simple change of variables. We know from Theorem 5 that the imperfect quantum protocol is more reliable than any possible classical protocol, provided n is large enough, when $p > \frac{1}{2} + \frac{\sqrt{2}}{4}$. This translates directly to $q > \frac{1}{\sqrt{2}}$. □

6 Conclusions and Open Problems

We have demonstrated that quantum pseudo-telepathy can arise for simple multi-party problems that cannot be handled by classical protocols much better than by the toss of a coin. This could serve to design new tests for the nonlocality of the physical world in which we live.

In closing, we propose two open problems. First, can Conjecture 1 be proven or are the best possible classical probabilistic protocols for our game even worse than hinted at by Theorem 4? Second, it would be nice to find a *two*-party pseudo-telepathy problem that admits a perfect quantum solution, yet any classical protocol would have a small probability of success even for inputs of small or moderate size.

References

1. Aaronson, S., Ambainis, A.: Quantum search of spatial regions. Available as `arXiv:quant-ph/0303041` (2003).
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** (1993) 1895–1899.
3. Brassard, G.: Quantum communication complexity. *Foundations of Physics* (to appear, 2003).
4. Brassard, G., Cleve, R., Tapp, A.: Cost of exactly simulating quantum entanglement with classical communication. *Physical Review Letter* **83** (1878) 1874–1878.
5. Buhrman, H., Cleve, R., Wigderson, A.: Quantum vs. classical communication and computation. *Proceedings of 30th Annual ACM Symposium on Theory of Computing* (1998) 63–68.
6. Cleve, R., Buhrman, H.: Substituting quantum entanglement for communication. *Physical Review A* **56** (1997) 1201–1204.
7. Gould, H. W.: *Combinatorial Identities*. Morgantown (1972).

8. Kalyanasundaram, B., Schnitger, G.: The probabilistic communication complexity of set intersection. *Proceedings of 2nd Annual IEEE Conference on Structure in Complexity Theory* (1987) 41–47.
9. Massar, S.: Non locality, closing the detection loophole, and communication complexity. *Physical Review A* **65** (2002) 032121-1–032121-5.
10. Nielsen, M. A., Chuang, I. L.: *Quantum Computation and Quantum Information*. Cambridge University Press (2000).
11. Raz, R.: Exponential separation of quantum and classical communication complexity. *Proceedings of 31st Annual ACM Symposium on Theory of Computing* (1999) 358–367.
12. Yao, A. C.–C.: Probabilistic computations: Toward a unified measure of complexity. *Proceedings of 18th IEEE Symposium on Foundations of Computer Science* (1977) 222–227.
13. Yao, A. C.-C.: Quantum circuit complexity. *Proceedings of 34th Annual IEEE Symposium on Foundations of Computer Science* (1993) 352–361.