Communication tasks with infinite quantum-classical separation

Christopher Perry, Rahul Jain, and Jonathan Oppenheim

How much of an advantage can be gained from using quantum strategies over classical ones? Here we consider a two player task where quantum resources are infinitely more powerful. Suppose Alice is given a string of length n, and Bob's task is to exclude certain combinations of bits that Alice might have. If Alice must send classical messages, then she must reveal nearly n bits of information to Bob, but if she is allowed to send quantum bits, the amount of information she must divulge goes to zero with increasing n. Next, we consider a version of the task where the parties may have access to entanglement. With this assistance, Alice only needs to send a constant number of bits, while without entanglement, the number of bits Alice must send grows linearly with n. Our task is related to the PBR theorem which arises in the foundations of quantum theory.

Below, we briefly outline the present work. For a full version of the proofs, please see [1].

For a given communication task, what advantages are there in using quantum resources? The standard measure used to investigate this question is the communication complexity [2], the minimum amount of bits or qubits the players must exchange to succeed. Tasks exist for which there is an exponential separation between the quantum and classical communication complexities [3–6] and in the absence of shared entanglement, it is known that such a separation is maximal in the bounded error model [7].

Here we consider a particular game between Alice and Bob and two alternative figures of merit: how much information must the players reveal about their inputs and what is the entanglement assisted communication complexity? With respect to both of these measures we find that there is an infinite separation between what is possible with purely classical strategies and what can be achieved with access to quantum resources. In order to win the game with certainty, Alice must disclose nearly everything about her input to Bob if her communication is classical, while there exists a quantum strategy in which the information she divulges to Bob goes to zero. Similarly, while a classical strategy for the game will require sending nearly all of Alice's input bits to Bob, allowing the players to share some entanglement can reduce the communication complexity to a constant, independent of the size of the inputs. Both of these gaps are larger than the at most exponential separation that can be achieved with respect to the unentangled communication complexity for any task.

The quantum strategies we develop are based upon the Pusey, Barrett, Rudolph (PBR) theorem regarding the reality of the quantum state [8]. Investigating the nature of the wave function has been a subject of much recent interest in the foundations community [9–15] and our separations serve to derive information theoretic implications from this debate. Even though a quantum message may convey a vanishingly small amount of information, to reproduce this information using purely classical means can require an infinitely large amount of information to be sent.

Our game, which we refer to as the exclusion game, involves Alice and Bob, together with a referee to mediate the task. It runs as follows. First, the referee gives Alice an n-bit string, $\vec{x} \in \{0,1\}^n$, with each of the 2^n strings being equally likely. Alice is then allowed to send a single message regarding her input to Bob. Next, the referee chooses at random a subset, $y \subseteq [n]$ of size m, of locations in Alice's bit string and gives this to Bob. There are $\binom{n}{m}$ possible subsets and they are all equally likely. If $\mathcal{M}_y\left(\vec{x}\right)$ denotes the m-bit string formed by restricting $\vec{x}$ to the bits specified by y, Bob's task is to produce a string $\vec{z}_y \in \{0,1\}^m$ such that $\mathcal{M}_y\left(\vec{x}\right) \neq \vec{z}_y$.

As an illustration, consider a game where $n = 3$, $m = 2$ and the inputs given to Alice and Bob are $\vec{x} = 001$ and $y = \{1,3\}$ respectively. Winning answers that Bob can give would then be $\vec{z}_y \in \{00, 10, 11\}$ as the only losing answer is $\vec{z}_y = \mathcal{M}_y\left(\vec{x}\right) = \mathcal{M}_{\{1,3\}}\left(001\right) = 01$.

More formally, the amount of information that the players reveal to one another about their inputs is called the internal information cost of the protocol [37]. The information cost is an interesting quantity as it lower bounds a protocol's communication complexity [16, 17] and in classical information theory, it has found use in proving direct sum theorems [16–19]. While for quantum protocols involving multiple rounds there is not a unique definition (see for example [20–23]), it is well defined for single round schemes as we consider here. If one is concerned with lowering the information cost and keeping information private, it is natural to ask if an advantage can be gained in using quantum protocols instead of classical ones and there are known exponential separations [24]. In the exclusion game, we find that, for certain choices of m, classical strategies must reveal greater than $n - o(n)$ bits of information. We will see however, that quantum mechanics admits a strategy for which the amount of information revealed tends to zero in the limit of large n.

For our second result, we consider how the communication complexity changes when the players are allowed to preshare some entanglement. This scenario was originally formulated in [25] where a task was found for which sharing an entangled state reduces the communication complexity by a single bit. Further developments on this work are found in [26] and [27] which show a similar saving and extend the scenario to k parties. Exponential separations between what is possible with entanglement assisted and purely classical strategies have also been found [28, 29] but in general, it is known that almost all Boolean functions have linear communication complexity even with this additional resource [30–32]. By modifying the exclusion game to allow Alice to decline to play with probability δ, it is possible to find an entanglement assisted scheme for which the communication complexity is less than a constant (that depends on δ) for all n. On the other hand, for totally classical strategies, the communication complexity is $\Omega(n)$. This represents a beyond exponential, infinite separation.

Both of these scenarios exhibit a larger than exponential gap between what is possible with quantum and classical strategies, and to our knowledge it is the first of its kind in the field of communication protocols. The size of the gap, near maximal for the information cost, is comparable to that found in the Deutsch-Jozsa algorithm with respect to the number of oracle calls [33], non-deterministic query complexity problems [5] and space complexity theory, the size of writable memory need for computation [34].

A. Information Cost

In the exclusion task focused on here, Alice and Bob's inputs are uniform and independent of one another and a protocol consists of sending a single classical or quantum message (M_C or M_Q) from Alice to Bob. This allows the following expressions for the classical and quantum information cost to be used:

$$IC\left(M_C\right) = n - H(X|M_C), \quad \text{and} \quad IC\left(M_Q\right) \leq 2S(M_Q),$$

To devise a quantum strategy, we consider the measurement used in the proof of the PBR theorem [8]. Suppose r systems are each prepared in one of two states, $|\psi_0\left(\theta\right)\rangle$ or $|\psi_1\left(\theta\right)\rangle$, separated by an angle θ. In total there are 2^r possible global preparations. If θ is chosen to be $\theta_r := 2\arctan\left(2^{1/r} - 1\right)$, it is possible to perform a global measurement across the r systems such that the outcome enables one to deduce a preparation that has not taken place [35]. In other words, if the global preparation resulted in $|\Psi_{\vec{x}}\rangle$, after the measurement it is possible to produce a $\vec{z}$ such that $\vec{z} \neq \vec{x}$ with certainty.

A quantum strategy for the exclusion game then involves Alice sending $|\psi_{x_i}\left(\theta_m\right)\rangle$ to Bob for each of the n bits in $\vec{x}$. If Bob performs the PBR measurement on the m locations specified by y, the outcome will enable him to win the game with certainty. As m increases, θ_m can be made smaller reducing the entropy of each individual message sent and hence the amount of information revealed. Choosing m appropriately leads to:

Theorem 1. *Suppose m depends on n in such a way that it dominates $\sqrt{n}$ asymptotically. Then there exists a quantum strategy for the exclusion game such that Bob wins the game with certainty whilst the amount of information Alice reveals to Bob regarding $\vec{x}$ tends to zero in the limit of large n.*

In comparison, how much information must Alice reveal to Bob in a classical strategy? For him to succeed with certainty, the message that Alice sends needs to allow him to produce a correct answer for each of the $\binom{n}{m}$ sets he can be asked about by the referee. Being able to answer a question correctly enables Bob to deduce some information about the input given to Alice. In particular, for each question, a winning answer enables him to exclude 2^{n-m} possible strings that could be held by Alice. As there will be some overlap between the sets of strings different answers exclude, to lower bound the information cost we need to find the set of answers that allows Bob to exclude the fewest possible $\vec{x}$. Doing so leads to the following results:

Theorem 2. *Suppose Alice and Bob are restricted to classical strategies in the exclusion game. For any winning strategy, the message that Alice sends to Bob, M_C, is such that:*

$$IC\left(M_C\right) \geq n - \log_2\left(\sum_{i=0}^{m-1}\binom{n}{i}\right).$$

Corollary 1. *If m depends on n in such a way that it dominates $\sqrt{n}$ but is dominated by n asymptotically, then $IC\left(M_C\right) \geq n - o(n)$.*

From Theorem 1 and Corollary 1, we obtain our first infinite separation between quantum and classical mechanics. For the exclusion game, there exists a quantum strategy such that for certain choices of m, the amount of information Alice must reveal to Bob tends to 0 in the limit of large n. On the other hand, for the same scaling of m all classical strategies must reveal nearly n bits of information about $\vec{x}$ to Bob. Quantum mechanics allows Alice to reveal almost nothing about her input while classically she must reveal close to everything.

Note the fact that Bob is required to output a winning answer with certainty. If Alice were to choose not to send a message to Bob, forcing him to guess at random, the probability that he would make an error is 2^{-m}. As m depends on n, this error probability will tend to zero as n increases. In spite of this, the infinite separation does persist if we consider a Las Vegas error model and allow Alice to decline to play with some probability. This is utilized in the next section.

B. Entanglement Assisted Communication Complexity

The quantum strategy given requires exactly n qubits to be sent from Alice to Bob whilst an optimal classical strategy may require $n - o(n)$ bits. To obtain a result with regards to the communication complexity, the number of sent bits, we modify the game slightly. In what follows, Alice may choose to abort the game with probability δ. When she does not abort however, Bob's answer must be correct.

To bound the classical communication complexity from below, we again consider the information cost, denoting it by IC_δ, and find:

Theorem 3. *Suppose Alice and Bob are restricted to classical strategies in the exclusion game but Alice is allowed to abort the game with probability δ. When she does not abort, Bob must answer correctly. For any winning strategy, the message that Alice sends to Bob, M_C, is such that if $m = \alpha n$ for some constant α with $0 < \alpha < \frac{1}{2}$, then $IC_\delta\left(M_C\right) \in \Omega\left(n\right)$.*

As the information cost lower bounds the communication complexity, this result also applies to the latter quantity.

With access to entangled states, rather than sending $|\Psi_{\vec{x}}\left(\theta_m\right)\rangle$ to Bob directly, Alice could instead attempt to steer Bob's side of the entanglement to the desired state by performing an appropriate measurement on her own system. Making use of a scheme from [36], suppose they share an entangled state, $|\Phi\rangle_{AB}$, for each bit x_i in $\vec{x}$ and Alice performs one of two, two outcome, measurements depending on the value of x_i. With some probability Bob's state is steered to $|\psi_{x_i}\left(\theta_m\right)\rangle$, otherwise it is steered to $|\mp\rangle$. For $m = \alpha n$, Bob's global system is steered to $|\Psi_{\vec{x}}\left(\theta_m\right)\rangle$ with probability greater than $4^{-\frac{1}{\alpha}}$ and Alice can send a single bit to Bob indicating whether this has happened or if she has aborted as one of the steering attempts has failed. Repeating this strategy k times while giving the players k sets of n copies of $|\Phi\rangle_{AB}$ and allowing Alice to occasionally abort gives the following result:

Theorem 4. *Suppose $m = \alpha n$, Alice and Bob can share entangled states and Alice is allowed to abort the game with probability δ. Then for all n and fixed $\delta > 0$, there exists a quantum strategy that uses at most k bits of classical communication where k is some constant that depends on δ but not on n.*

From Theorem 3 and Theorem 4 we obtain our second result. By allowing Alice to occasionally abort, there exist choices of m such that in the exclusion game, with access to entanglement, only a constant amount of communication is required. For classical strategies on the other hand, Alice needs to send $\Omega(n)$ bits of communication.

[1] C. Perry, R. Jain, and J. Oppenheim, arXiv preprint arXiv:1407.8217 (2014).

[2] A. C.-C. Yao, in *Proceedings of the eleventh annual ACM symposium on Theory of computing* (ACM, 1979) pp. 209–213.

[3] R. Raz, in *Proceedings of the thirty-first annual ACM symposium on Theory of computing* (ACM, 1999) pp. 358–367.

[4] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Physical Review Letters **87**, 167902 (2001).

[5] R. de Wolf, SIAM Journal on Computing **32**, 681 (2003).

[6] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf, in *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing* (ACM, 2007) pp. 516–525.

[7] I. Kremer, *Quantum Communication*, Master's thesis, The Hebrew University of Jerusalem (1995).

[8] M. F. Pusey, J. Barrett, and T. Rudolph, Nature Physics **8**, 475 (2012).

[9] R. Colbeck and R. Renner, Nature communications **2**, 411 (2011).

[10] R. Colbeck and R. Renner, Physical review letters **108**, 150402 (2012).

[11] P. G. Lewis, D. Jennings, J. Barrett, and T. Rudolph, Physical review letters **109**, 150404 (2012).

[12] L. Hardy, International Journal of Modern Physics B **27** (2013).

[13] S. Aaronson, A. Bouland, L. Chua, and G. Lowther, arXiv preprint arXiv:1303.2834 (2013).

[14] J. Barrett, E. G. Cavalcanti, R. Lal, and O. J. Maroney, arXiv preprint arXiv:1310.8302 (2013).

[15] R. Colbeck and R. Renner, arXiv preprint arXiv:1312.7353 (2013).

[16] A. Chakrabarti, Y. Shi, A. Wirth, and A. Yao, in *Foundations of Computer Science, 2001. Proceedings. 42nd IEEE Symposium on* (IEEE, 2001) pp. 270–278.

[17] Z. Bar-Yossef, T. Jayram, R. Kumar, and D. Sivakumar, in *Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on* (IEEE, 2002) pp. 209–218.

[18] R. Jain, J. Radhakrishnan, and P. Sen, Lecture notes in computer science **2719**, 300 (2003).

[19] B. Barak, M. Braverman, X. Chen, and A. Rao, SIAM Journal on Computing **42**, 1327 (2013).

[20] R. Jain, J. Radhakrishnan, and P. Sen, in *Proceedings-Annual Symposium on Foundations of Computer Science* (IEEE, 2003) pp. 220–229.

[21] R. Jain and A. Nayak, arXiv preprint arXiv:1004.3165 (2010).

[22] M. Braverman, in *Proceedings of the 44th symposium on Theory of Computing* (ACM, 2012) pp. 505–524.

[23] D. Touchette, arXiv preprint arXiv:1404.3733 (2014).

[24] I. Kerenidis, S. Laplante, V. Lerays, J. Roland, and D. Xiao, in *Foundations of Computer Science (FOCS), 2012 IEEE 53rd Annual Symposium on* (IEEE, 2012) pp. 500–509.

[25] R. Cleve and H. Buhrman, Physical Review A **56**, 1201 (1997).

[26] H. Buhrman, R. Cleve, and W. Van Dam, SIAM Journal on Computing **30**, 1829 (2001).

[27] H. Buhrman, W. van Dam, P. Høyer, and A. Tapp, Physical Review A **60**, 2737 (1999).

[28] D. Gavinsky, arXiv preprint arXiv:0901.0956 (2009).

[29] D. Gavinsky, J. Kempe, O. Regev, and R. de Wolf, SIAM Journal on Computing **39**, 1 (2009).

[30] H. Buhrman and R. de Wolf, in *Computational Complexity, 16th Annual IEEE Conference on, 2001.* (IEEE, 2001) pp. 120–130.

[31] D. Gavinsky, J. Kempe, and R. de Wolf, in *Computational Complexity, 2006. CCC 2006. Twenty-First Annual IEEE Conference on* (IEEE, 2006) pp. 8–pp.

[32] A. Montanaro and A. Winter, in *Automata, Languages and Programming* (Springer, 2007) pp. 122–133.

[33] D. Deutsch and R. Jozsa, Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences **439**, 553 (1992).

[34] E. F. Galvao and L. Hardy, Physical review letters **90**, 087902 (2003).

[35] S. Bandyopadhyay, R. Jain, J. Oppenheim, and C. Perry, Physical Review A **89**, 022336 (2014).

[36] T. Rudolph and R. W. Spekkens, Physical Review A **70**, 052306 (2004).

[37] Note that in the exclusion game the inputs are taken from a product distribution so the internal information cost is equivalent to the external information cost, the amount the players reveal about their inputs to an external observer.