# Infinite separation of quantum information and communication

Zi-Wen Liu[*] Dax Enshan Koh[†]

**Abstract**

We prove an infinite separation between quantum information complexity and quantum communication complexity by considering the exclusion game, first introduced by Perry, Jain and Oppenheim [1], who showed that for appropriately chosen parameters of the game, the quantum information cost vanishes as the size of the problem $n$ increases. We extend their result by showing that for those parameters, the quantum communication cost is lower bounded by $\Omega(\log n)$, thereby proving that there are protocols for which an infinite gap exists between their quantum information and communication costs. We show that this holds not only for zero-error protocols, but also for protocols that have a sufficiently small probability of error.

## 1 Introduction

The exclusion game, introduced by Perry, Jain and Oppenheim (PJO) [1], provides the first example of a communication task for which there is an infinite separation in information costs between classical and quantum strategies. The game, which involves two players Alice and Bob who have infinite computational power, may be described as follows: Alice and Bob randomly draw an $n$-bit string $x$ and some subset $y \subseteq [n]$, where $|y| = m$, respectively. They win the game if Bob is able to output a string $z$ that is different from $x$ restricted to the bits specified by $y$, subject to the constraint that the only allowed communication, whether classical or quantum, is from Alice to Bob.

There are two quantities that are relevant to the communication task, namely the information cost and the communication cost. The information cost of a protocol measures the amount of classical or quantum information exchanged, whereas the communication cost measures the number of bits or qubits exchanged in order for the protocol to succeed. In [1], the authors consider the information costs required for the exclusion game and they prove that for certain values of $m$, while the information cost of any classical protocol scales linearly with $n$, there exists a quantum protocol with an information cost that goes to zero as $n$ increases, thus giving the first example of an infinite separation between quantum and classical information costs.

The PJO protocol, however, requires that $n$ qubits be sent from Alice to Bob. Therefore, even though the information cost becomes vanishingly small with increasing $n$, the communication cost of the protocol grows with $n$. An interesting question that then arises is whether it is possible to succeed in the game with a smaller communication cost, i.e. can Alice and Bob still succeed if Alice compresses her quantum message? In particular, is it possible for the message to be compressed so that the communication cost also goes to zero with increasing $n$?

In this paper, we answer the above question in the negative, thus giving the first example of an infinite separation between the quantum information and communication costs. The significance of

[*] MIT. Email: zwliu@mit.edu.

[†] MIT. Email: daxkoh@math.mit.edu.

this result may be compared with its classical counterpart, where only an exponential separation was shown between classical information and communication costs [2].

This paper is organized as follows. In Section 2, we review the general formulation of one-way communication tasks and introduce the exclusion game. In Section 3, we review the quantum strategy employed by [1] that shows that the quantum information cost of the exclusion game goes to zero as the size of the problem increases. In Section 4, we prove a $\Omega(\log n)$ lower bound on the communication cost of any quantum protocol that wins the exclusion game; its variant, where a vanishingly small error is allowed is also discussed. Both cases lead to an infinite separation between quantum information and communication costs for certain parameters of the game.

## 2 General formulation of one-way communication tasks

A typical one-way communication task described by the function $f : \{0,1\}^a \times \{0,1\}^b \to \{0,1\}$ may be described as follows: Alice draws some string $x \in \{0,1\}^a$ and Bob draws some string $y \in \{0,1\}^b$. Alice sends a message to Bob and then Bob outputs a string $z$. They win the game if $z = f(x,y)$.

The exclusion game introduced in [1] requires a more general framework, which we introduce here. We shall describe a general one-way communication task by the function $F : \{0,1\}^a \times \{0,1\}^b \to \mathcal{P}(\{0,1\}^*)$, where $\mathcal{P}(S)$ denotes the power set of $S$. As before, Alice and Bob draw some strings $x \in \{0,1\}^a$ and $y \in \{0,1\}^b$ respectively. Then, Alice sends a message to Bob and Bob outputs a string $z$. The winning condition is made more general though. We say they win the game if $z \in F(x,y)$.

It is clear that the more general framework reduces to the typical framework when $F(x,y)$ contains exactly one element, say $f(x,y)$ . In this case, the only way in which they can win the game is if $z = f(x,y)$.

We shall now define the exclusion game. Let

$$\begin{aligned} \mathcal{M} : Y_{(n,m)} \times \{0,1\}^n &\to \{0,1\}^m \\ (y,x) &\mapsto \mathcal{M}_y(x). \end{aligned}$$

where $Y_{(n,m)}$ is the set of all subsets of $\{1,\dots,n\}$ of size $m$, and $\mathcal{M}_y(x)$ is the $m$-bit string formed by restricting the string $x$ to the bits specified by $y$. The exclusion-game function $\mathrm{EXC}_{n,m}$ is then defined as

$$\begin{aligned} \mathrm{EXC}_{n,m} : \{0,1\}^{s(m)} \times \{0,1\}^n &\to \{0,1\}^m \\ (\llcorner y \lrcorner, x) &\mapsto \{z | z \neq \mathcal{M}_y(x)\}, \end{aligned}$$

where $\llcorner y \lrcorner$ is the binary representation of $y$, and $s(m)$ is the number of bits needed to specify a subset $y$ of size $m$. The winning condition may then be stated as follows: Alice and Bob win if for given $x$ and $y$, Bob outputs a string $z$ such that $z \neq \mathcal{M}_y(x)$.

We now define two different ways to measure the complexity of one-way communication protocols, namely the communication complexity and information complexity.

For a protocol $\Pi$ that wins the game defined by the function $F$, we denote the information cost of a $\lambda$-protocol (where $\lambda = C$ (classical) or $= Q$ (quantum)) by $\lambda^F_{CC}(\Pi)$, and the corresponding communication cost by $R^F_{IC}(\Pi)$.

Then $\lambda^F_{CC}(\Pi)$ is defined to be the number of bits or qubits exchanged throughout the protocol, and $\lambda^F_{IC}(\Pi)$ is defined as follows: $\lambda^F_{IC}(\Pi) = I(X : \Pi|Y) + I(Y : \Pi|X)$, where $I(S : T|U) = H(SU) + H(TU) - H(STU) - H(U)$ measures the mutual information between $S$ and $T$ given $U$.

The $\lambda$-information complexity of a game is then defined to be $\lambda^F_{IC} = \inf_\Pi \lambda^F_{IC}(\Pi)$. The $\lambda$-communication complexity is defined similarly.

## 3 Perry-Jain-Oppenheim quantum strategy

In this section, we review the quantum strategy used by [1] that proves that the quantum information complexity of the exclusion game $\mathrm{EXC}_{n,m}$ vanishes as $n \to \infty$, when $m$ is chosen to satisfy $m \in \omega(n^{1/2+\epsilon})$.

For given strings $x$ and $\llcorner y \lrcorner$ that Alice and Bob, respectively, draw, we first describe how Alice encodes the string $x$ in her quantum message: she encodes each classical bit $x_i$ using the state $|\psi_{x_i}(\theta)\rangle = \cos(\theta/2)|0\rangle + (-1)^{x_i}\sin(\theta/2)|1\rangle$, where $\theta = 2\tan^{-1}(2^{1/r} - 1)$. Her $n$-bit string $x = x_1 \dots x_n$ is then encoded as $|\Psi_x(\theta)\rangle = \otimes_{i=1}^{r}|\psi_{x_i}(\theta)\rangle$, which she sends to Bob via the quantum channel.

Upon receiving the state from Alice, Bob now has to perform a measurement. The measurement technique used may be described as a conclusive-exclusion measurement, which was first introduced by [3] and subsequently used to prove the PBR theorem [4], a result in the field of quantum foundations that rules out a certain class of $\psi$-epistemic models of quantum mechanics. In [1, 5], it was shown that if Bob performs the projective measurement $\{|\zeta_z\rangle\}_{z\in\{0,1\}^r}$, where $|\zeta_z\rangle = \frac{1}{\sqrt{2^r}}(|0\rangle - \sum_{s\neq 0}(-1)^{z\cdot s}|s\rangle)$, then the probability that Alice's string is $x_y$ given that $z = x_y$ is zero, and hence, by outputting the result corresponding to the projection $|\zeta_z\rangle$, they win the game with certainty.

It now suffices to show that the quantum information cost of the protocol can be made vanishingly small. Indeed, the quantum information can be calculated to be given by $Q_{IC}^{\mathrm{EXC}_{n,m}}(\Pi) \leq 2S(M_Q) \in o(n^{-2\epsilon})$, where $S(M_Q)$ is the von Neumann entropy of the quantum message $M_Q$ that Alice sends to Bob. Hence, it vanishes in the large $n$ limit.

## 4 Lower bound on the quantum communication cost

Since the amount of quantum information that Alice actually reveals to Bob in the PJO quantum strategy (i.e., the information cost $Q_{IC}^{\mathrm{EXC}_{n,m}}(\mathrm{PJO})$) tends to zero in the large-$n$ limit, one might ask if the number of qubits that Alice has to send in any winning strategy could also go to zero in the limit. In this section, we show that this is not possible by proving an $\Omega(\log n)$ lower bound on the quantum communication complexity for certain parameters of the game. We consider two cases: when zero error is allowed and when a vanishingly small error is allowed. For both these cases, our proof involves simulating a quantum protocol $\Pi_Q$ by a classical protocol but with an exponential overhead, so that the existence of a quantum strategy with $Q_{CC}^{\mathrm{EXC}_{n,m}}(\Pi_Q) = o(\log n)$ would contradict the following classical communication cost lower bound:

**Lemma 1.** *Let $\omega(n^{\frac{1}{2}+\epsilon}) \leq m \leq \alpha n$, where $0 < \alpha < \frac{1}{2}$ is a constant. Any classical strategy that wins the exclusion game $\mathrm{EXC}_{n,m}$ in the large $n$ limit with certainty, requires that the number of bits sent from Alice to Bob be of order $\Omega(n)$, i.e., for all strategies $\Pi$, $C_{CC}^{\mathrm{EXC}_{n,m}}(\Pi) \in \Omega(n)$ where $m$ is within the above regime.*

*Proof.* In Theorem 2 of [1], it was shown that $C_{IC}^{\mathrm{EXC}_{n,m}}(\Pi) \geq n - \log_2\left(\sum_{i=0}^{m-1}\binom{n}{i}\right)$. For $\omega(n^{\frac{1}{2}+\epsilon}) \leq m \leq \alpha n$, where $0 < \alpha < \frac{1}{2}$, the lower bound could be simplified to $C_{IC}^{\mathrm{EXC}_{n,m}}(\Pi) \in \Omega(n)$ (see Appendix B2 of [1]). Since the amount of information revealed is bounded above by the communication cost, i.e., $C_{IC} \leq C_{CC}$ for any communication protocol, it follows that $C_{CC} \in \Omega(n)$. As Alice can always send the whole string to Bob in order to win, this bound is tight, and we obtain $C_{CC}^{\mathrm{EXC}_{n,m}}(\Pi) \in \Omega(n)$ in the specified regime of $m$, as desired. □

Before proving the main results, we state and prove the following lemma.

**Lemma 2.** *A $q$-qubit quantum state can be classically described by a set of real numbers encoding the real and imaginary parts of all amplitudes to accuracy $\epsilon$ using $O\left(2^q \log(\frac{1}{\epsilon})\right)$ bits.*

*Proof.* A general $q$-qubit pure state $|\psi_q\rangle$ can be written as $|\psi_q\rangle = \sum_{i=1}^{2^q} \alpha_i |i\rangle$, where $\alpha_i \in \mathbb{C}$, and $\{|i\rangle\}$ is a complete orthonormal basis set containing $2^q$ elements. We express all complex amplitudes as $\alpha_i = b_i + ic_i$ where $b_i, c_i \in \mathbb{R}$, satisfying $\sum_{i=1}^{2^q} |\alpha_i|^2 = \sum_{i=1}^{2^q}(b_i^2 + c_i^2) = 1$. Thus, $0 \leq |b_i|, |c_i| \leq 1$. To approximate each of these real numbers to accuracy $\epsilon = 2^{-l}$, we keep the first $l$ bits after the binary point, and we make use of one bit to indicate its sign, i.e., we can find an $(l+1)$-bit classical string that encodes an approximation $\tilde{b}_i$ of each $b_i$ such that $|\tilde{b}_i - b_i| \leq \epsilon$ (same for $c_i$). Notice that there are $2 \cdot 2^q$ such numbers in total, thus only $2^{q+1}(l+1) = O\left(2^q \log(\frac{1}{\epsilon})\right)$ bits are needed to encode $|\psi_q\rangle$ such that we have specified the real and imaginary parts of all amplitudes to accuracy $\epsilon$. □

## 4.1 Zero error

We now prove that in a specific regime of the original exclusion game where no error is allowed, $\Omega(\log n)$ qubits of communication is necessary.

**Theorem 3.** *For the exclusion game $\mathrm{EXC}_{n,m}$ where $\omega(n^{\frac{1}{2}+\epsilon}) \leq m \leq \alpha n$ in the large $n$ limit for some constant $\alpha$ s.t. $0 < \alpha < \frac{1}{2}$, $Q_{CC} \geq \Omega(\log n)$.*

*Proof.* Suppose that $Q_{CC} \in o(\log n)$. Then there exists a winning quantum strategy $\Pi_Q$ in which Alice sends a $q$-qubit state $|\psi_x\rangle$ to Bob upon receiving the $n$-bit string $x$, where $q = o(\log n)$. WLOG, the state $|\psi_q\rangle$ that Alice sends to Bob is pure. (Indeed, any mixed state can be described by a pure state on a large Hilbert space of dimension at most twice as large, and hence, the quantum communication cost can increase by at most a constant factor and does not affect the scaling asymptotically.)

Using $\Pi_Q$, we shall now construct a classical protocol $\Pi_C$ that succeeds in the game by using only $o(n)$ bits, thus contradicting the classical lower bound of Lemma 1. The reduction runs as follows: let $|\Psi_x\rangle$ be the quantum message that Alice sends in the protocol $\Pi_Q$ when she draws the string $x \in \{0, 1\}$. From $|\Psi_x\rangle$, she constructs an approximate classical description $C(\psi_x)$ of $|\Psi_x\rangle$ that has an error of at most $\epsilon$. By plugging the expression $q = o(\log n)$ into Lemma 2, it follows that this can be done using $o(n \log(1/\epsilon))$ bits. She sends the classical message $C(\psi_x)$ across the classical channel. We shall denote the state that is described by $C(\psi_x)$ by $|\tilde{\psi_x}\rangle$.

Now, let $\{P_k^y\}_k$ be the POVM used by Bob in $\Pi_Q$ to measure the state received from Alice. Bob computes all the probabilities of each of the outcomes $k$ of the POVM, by using Born's rule $p_k = \langle\tilde{\psi_x}|P_k^y|\tilde{\psi_x}\rangle$. There exists a threshold $\delta$ such that if the probability $p_k$ were below the threshold for the state $|\tilde{\psi_x}\rangle$, then if the state were $|\psi_x\rangle$, the probability would have been zero. Hence, Bob rounds down all probabilities $p_k$ that are bounded above by $\delta$ to zero. For any such $k$, the string $z$ that Bob outputs is guaranteed to be different from $x_y$. Hence, we have reached a contradiction by constructing an $o(n)$-classical protocol for the exclusion game.

□

## 4.2 Vanishingly small probability of error

Now we present a variant of the above protocol that shows that when a very tiny amount of error is allowed, a nonvanishing amount of quantum communication is still required.

**Theorem 4.** *Suppose that there exists a winning quantum strategy $\Pi_Q$ with $Q_{CC}^{\mathrm{EXC}_{n,m}}(\Pi_Q) = \Theta(s)$, then there must also exist a classical strategy $\Pi_C$ with $C_{CC}^{\mathrm{EXC}_{n,m}}(\Pi_C) = \Theta(2^s)$ whose probability of error can be made arbitrarily small.*

*Proof.* We revise Bob's local part of the protocol presented in Theorem 3 to prove this argument. As before, Alice prepares an approximate classical encoding of the real and imaginary parts of all the amplitudes of the state $|\psi_s\rangle$ to accuracy $\epsilon$ using $\Theta\left(2^s \log(\frac{1}{\epsilon})\right)$ bits, and sends these bits to Bob. Again, we emphasize that in studying communication tasks, we don't limit the computational cost of each player: they can do whatever they want without worrying about time or space as computational resources on the local side. Hence Bob can translate the classical information of the amplitudes into a new quantum state $|\tilde{\psi_s}\rangle$, and make as many copies as he needs. A subtlety here is that the state with exactly the same value of amplitudes may not be perfectly normalized, but since Bob can manipulate the state preparation protocol to infinite accuracy, it follows that the normalized state $|\tilde{\psi_s}\rangle$ is very close to $|\psi_s\rangle$ (say, $\epsilon$-close in trace distance, the rigorous proof of which is lengthy but straightforward, so we will omit it). And therefore, the perturbation on the probability for any measurement outcome is bounded (the idea of the proof is similar to the inverse of Almost-As-Good-As-New-Lemma (AAGANL) [6]). So Bob can just feed $|\tilde{\psi_s}\rangle$ into his local circuit of $\Pi_Q$, and run the protocol a multiple number of times (say, $t$) with his copies. Denote the perturbation on the probabilities as $\epsilon'$ (detailed proof will follow up), then Bob just refuses to output anything corresponding to a certain outcome that appears for less than $c$ (constant) times, and the probability that he makes a mistake decays exponentially with $t$ by Chernoff bound, hence can be made arbitrarily small by increasing $t$, i.e., preparing more copies. □

In this revised protocol we do not need to consider the details of the protocol $\Pi_Q$. Since the encoding of the original state is approximate, a nonzero probability of error will be inevitable, but it can be made arbitrarily small by amplification. Therefore we have the following corollary:

**Corollary.** *The infinite gap between quantum information and communication costs still holds when the error allowed is sufficiently small.*

The general idea is that as the tolerable probability of error goes from $\frac{1}{2^m}$ (random guess, no communication needed) to 0, the lower bound of $C_{CC}$ will grow from 0 to $\Omega(n)$ (the complete characterization of its behavior remains unknown), and by Theorem 4, $Q_{CC}$ is at least logarithmic in $C_{CC}$. (For instance, the lower bound $C_{CC}$ should approach $\Omega(n)$ for an allowed probability of error that is sufficiently close to 0, then the corresponding $Q_{CC}$ is lower bounded by $\Omega(\log n)$, though for an infinite separation of $Q_{CC}$ and $Q_{IC}$ the restriction can be loosened.) Note that for the special case $m = \sqrt{n}$, if we allow an error of $\frac{1}{2^{m+1}}$ (half of random guess), then it is possible to give a strategy with only 1 bit of classical communication [1], so we expect the allowed error to be smaller than $\frac{1}{2^{m+1}}$ if we want to establish an infinite separation.

# 5 Concluding remarks

In this paper, we considered the exclusion game and showed that an infinite gap exists between its quantum communication complexity and quantum information complexity, whether we allow for zero error or a vanishingly small error. It remains an open question whether the $\Omega(\log n)$ bound is tight, i.e., it is not known if a gap between $Q_{CC}$ and $C_{CC}$ exists for this game (Fig. 1).

The general formulation of communication tasks presented in this paper may open up some new doors. Analogously, the task of quantum state discrimination, where we essentially reduce $k$ possibilities to 1, can be generalized to $k \to (k-m)$ state exclusion task via semidefinite programming (SDP), which may provide insight for the generalization of communication models. For example, a duality between quantum random access coding (QRAC) [7, 8] and the exclusion game under certain restrictions may be formalized in this spirit. We expect interesting new results to emerge in this direction.

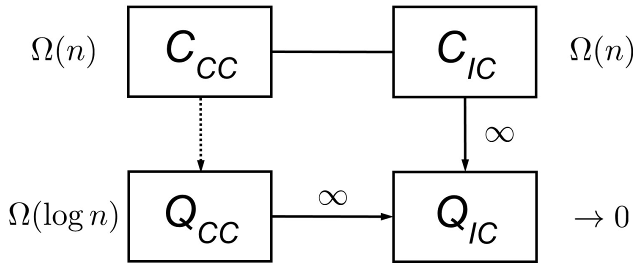

Figure 1: Exclusion game $\mathrm{EXC}_{n,m}$ with $\omega(n^{\frac{1}{2}+\epsilon}) \leq m \leq \alpha n$ in the large $n$ limit, where $0 < \alpha < \frac{1}{2}$ is a constant. Solid arrows indicate established separations (pointing towards the smaller one), while the dashed one indicates an unknown separation.

## 6 Acknowledgements

We thank Scott Aaronson for teaching the wonderful 6.845 Quantum Complexity Theory course, and for his insightful guidance and suggestions. We also thank Adam Bouland for being a helpful and friendly TA for this course.

## References

[1] C. Perry, R. Jain, and J. Oppenheim. Communication tasks with infinite quantum-classical separation. *ArXiv e-prints*, July 2014.

[2] A. Ganor, G. Kol, and R. Raz. Exponential separation of Information and Communication. *Electronic Colloquium on Computational Complexity (ECCC)*, 2014. URL `http://eccc.hpi-web.de/report/2014/049/`.

[3] Carlton Caves, Christopher Fuchs, and Rüdiger Schack. Conditions for compatibility of quantum-state assignments. *Phys. Rev. A*, 66:062111, Dec 2002. doi: 10.1103/PhysRevA.66.062111. URL `http://link.aps.org/doi/10.1103/PhysRevA.66.062111`.

[4] Matthew F. Pusey, Jonathan Barrett, and Terry Rudolph. On the reality of the quantum state. *Nat. Phys.*, 8(6):475–478, 2012. URL `http://dx.doi.org/10.1038/nphys2309`.

[5] Somshubhro Bandyopadhyay, Rahul Jain, Jonathan Oppenheim, and Christopher Perry. Conclusive exclusion of quantum states. *Phys. Rev. A*, 89:022336, Feb 2014. doi: 10.1103/PhysRevA.89.022336. URL `http://link.aps.org/doi/10.1103/PhysRevA.89.022336`.

[6] S. Aaronson. Limitations of Quantum Advice and One-Way Communication. *eprint arXiv:quant-ph/0402095*, February 2004.

[7] A. Nayak. Optimal lower bounds for quantum automata and random access codes. *eprint arXiv:quant-ph/9904093*, April 1999.

[8] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense Quantum Coding and a Lower Bound for 1-way Quantum Automata. *eprint arXiv:quant-ph/9804043*, April 1998.