On the limits of communication with non-local resources

Xiaodi Wu
MIT

Henry Yuen
MIT

February 28, 2015

Abstract

We obtain optimal bounds for the problem of conveying classical messages by communication between a sender and a receiver who can utilize non-local correlations obeying the Non-Signaling Principle. These include correlations arising from quantum entanglement, but also include "super-quantum" correlations (e.g. those that maximally violate the CHSH inequality). Our result simultaneously simplifies and generalizes the result of Nayak and Salzman (JACM vol.53, issue 1, pp. 184–206).

1 Introduction

Consider the following communication task T: Alice has a uniformly random n-bit message X in mind, and wants to engage in a communication protocol with Bob so that at the end of the protocol, Bob can guess Alice's message X with high probability. What is the communication required in order to perform task T? Holevo's theorem from quantum information theory [2] implies that, even if Alice is allowed to send quantum states to Bob, she must send at least $pn - h(p)$ qubits in order for Bob to recover X with probability p, where $h(\cdot)$ is the binary entropy function. Nayak and Salzman [4] significantly strengthen this bound and show that if Alice and Bob engage in a two-way quantum communication protocol, Alice is required to send at least $\frac{1}{2}(n - \log 1/p)$ qubits for Bob to recover X with probability p. This bound holds even if Alice and Bob share arbitrarily large entangled state before the protocol starts.

Here we study the communication cost of task T when Alice and Bob are only required to obey the *Non-signaling Principle*, which states that spatially separated parties cannot use non-local correlations to signal to each other, unless they communicate. Non-local correlations that arise from quantum states are non-signaling, but the converse is not true: there are non-local correlations (such as those maximally violating the CHSH bound) that are not explainable via quantum theory. Recently, physicists and computer scientists have been studying the consequences of the Non-signaling Principle without appealing to a specific physical theory such as quantum mechanics (e.g., [5, 6]). In this note we show that, even if Alice and Bob use arbitrary non-local correlations satisfying the Non-signaling Principle, they still must exchange at least $n - \log 1/p$ bits in order to succeed at task T with probability p. In particular, our proof simultaneously simplifies and generalizes the result of Nayak and Salzman.

Other related work. Recently, Navascues, et al. studied a class of super-quantum correlations called "Almost Quantum" correlations, and showed that using such correlations and one-way communication, Alice still must transmit n bits to Bob in order for Bob to guess Alice's n-bit input

with good probability [3]. Their result is a special case of our Theorem 3.1 and their proof of this shares the same spirit as ours. Independently, [1] proves a special case of the result of [4] when the Alice and Bob are restricted to using classical communication (but can use any amount of shared entanglement).

2 Preliminaries and Model

When referring to random variables, we will use capital letters (such as M). When using specific values of the random variables, we will use lower case letters (such as m). A bipartite conditional probability distribution $\Pr_{AB|UV}(a, b|u, v)$ is *non-signaling* if and only if for all a, b in the support of u, v, $\Pr_{A|U,V}(a|u, v) = \Pr_{A|U}(a|u)$ and $\Pr_{B|U,V}(b|u, v) = \Pr_{B|V}(b|v)$.

2.1 Communication with non-local boxes

We formally define our model of *non-local communication*. A *non-signaling device* $\mathcal{D} = (\mathcal{A}, \mathcal{B})$ is a bipartite device, where $\mathcal{A}$ takes input u and outputs a, $\mathcal{B}$ takes input y and outputs b, and there is a non-signaling probability distribution $\Pr_{AB|UV}(a, b|u, v)$ that describes the input/output behavior of the devices.

A *non-local communication protocol* is a number of rounds r, and a sequence of non-signaling devices $\mathcal{D}_1, \ldots, \mathcal{D}_r$. Each device $\mathcal{D}_i$ consists of two parts, $\mathcal{A}_i$ and $\mathcal{B}_i$, where $\mathcal{A}_i$ takes input (a_i, m_i^B) and outputs (a_{i+1}, m_{i+1}^A), and $\mathcal{B}_i$ takes input (b_i, m_{i+1}^A) and outputs (b_{i+1}, m_{i+1}^B). In such a protocol, Alice and Bob receive (possibly empty) external inputs x and y, and Alice first runs $\mathcal{A}_1(x, \mathsf{null})$ to produce (a_1, m_2^A), and sends m_2^A to Bob. Bob then runs $\mathcal{B}_1(y, m_2^A)$ to produce (b_2, m_2^B). This concludes the first round. In subsequent rounds $i > 1$, Alice runs $\mathcal{A}_i(a_i, m_i^B)$ and Bob runs $\mathcal{B}_i(b_i, m_{i+1}^A)$. The output of the protocol is the pair (m_{r+1}^A, m_{r+1}^B). Furthermore, each non-signaling device $\mathcal{D}_i$ depends only on its inputs: given its inputs, the distribution of outputs is independent of the input/output history of all previous devices $\mathcal{D}_j$ for $j < i$.

The next theorem shows that our model of non-local communication is general enough to simulate any two-way quantum communication protocol. We consider the most general model of (noiseless) two-way quantum communication: Alice and Bob are allowed to share an arbitrary entangled state at the beginning of the communication protocol, and during the protocol they exchange qubits over a (noiseless) quantum channel. At the end of the protocol, Alice and Bob make a local measurement on their quatum state (which includes their portion of the shared entanglement, as well as the qubits they received over the communication channel), and they output their measurement outcomes a and b, respectively. If Alice and Bob take external inputs x and y, respectively, then there is some conditional probability distribution $\Pr_{AB|XY}(a, b|x, y)$ – which we call the input/output distribution of the protocol – describing the behavior of the protocol.

We say a communication protocol P simulates another protocol Q (which may use a different model of communication than P's) if their input/output distributions are identical.

Theorem 2.1. *Two-way quantum communication protocols can be simulated by communication with non-local boxes, with a factor* 2 *increase in communication complexity.*

Proof. Let Q be a two-way quantum communication protocol with prior shared entanglement. We first convert this to a quantum protocol Q' where all the communication is classical. This can be done using quantum teleportation, which uses twice as many bits of communication as qubits

transmitted in Q. We perform a round-by-round simulation of Q' with a non-local communication protocol P, where we will assume for simplicity that in each round, only one of Alice or Bob speaks. Consider some round i in Q', and suppose that it is Alice's turn to speak. Given Alice's input x and Bob's input y, along with Π_i , the distribution of Alice's message m_{i+1}^A to Bob is determined. Furthermore m_{i+1}^A is independent of y, because quantum distributions are non-signaling. Therefore we can construct a non-local device $\mathcal{D}_i = (\mathcal{A}_i, \mathcal{B}_i)$ where $\mathcal{A}_i$ takes inputs (x, Π_i), and $\mathcal{B}_i$ takes inputs (y, Π_i). $\mathcal{A}_i$ will output (x, Π_i, m_{i+1}^A), where m_{i+1}^A is distributed according Alice's output in round i in Q', conditioned on x, y, and Π_i. $\mathcal{B}_i$ will output (y, Π_i) (i.e. repeat its input). $\mathcal{D}_i$ is a non-signaling device, and simulates the behavior of Alice and Bob in the ith round of Q'. Let protocol P be the sequence of devices $\mathcal{D}_1, \ldots, \mathcal{D}_r$ where r is the number of rounds in Q'. Its input/output distribution is identical to that of Q', which is identical to that of Q. The communication complexity of P is equal to that of Q', completing the proof. □

3 One-way communication

Theorem 3.1. *Suppose that Alice receives a random n-bit string X, and engages in a one-way non-local communication protocol with Bob. Let n_A denote the number of bits sent from Alice to Bob. The maximum probability that Bob can guess X is at most $Q(2^{n_A}, X)$, where $Q(\ell, X)$ is the probability mass of the ℓ most likely strings of X.*

Proof. We can model the protocol as follows: Alice and Bob have non-signaling boxes $\mathcal{A}$ and $\mathcal{B}$, whose joint input/output behavior is described by a non-signaling distribution $AB|XV$ (i.e., A is the random variable denoting the output of $\mathcal{A}$ on input X, and B is the random variable denoting the output of $\mathcal{B}$ on input V). In the protocol, Alice gets input $X = x$, runs $\mathcal{A}(x)$, and obtains a sample a. Alice sends a to Bob, who then runs $\mathcal{B}(a)$, and obtains sample b, which we can assume without loss of generality is an n-bit string. In this protocol, the final distribution of x, a, and b is $\Pr_X(x) \Pr_{A|X}(a|x) \Pr_{B|X,V,A}(b|x, a, a)$.

Consider the following thought experiment: instead of Alice sending a to Bob, Bob generates a uniformly random input v, and runs $\mathcal{B}(v)$ instead. The joint distribution of x, a, v, b is $\Pr_X(x) \Pr_V(v) \Pr_{A,B|X,V}(a, b|x, v)$. If we *postselect* on $v = a$, then the distribution of x, a, b will be exactly as in the original protocol. Then,

$$\Pr(B = X | V = A) = \frac{1}{\Pr(V = A)} \sum_{x,a} \Pr_X(x) \Pr_V(a) \Pr_{A,B|X,V}(a, x|x, a).$$

Now note that

$$\begin{aligned}
\sum_x \sum_a \Pr_V(a) \Pr_{A,B|X,V}(a, x|x, a) &= \sum_x \sum_a \Pr_{V|X}(a|x) \Pr_{A,B|X,V}(a, x|x, a) = \sum_x \sum_a \Pr_{A,B,V|X}(a, x, a|x) \\
&\leq \sum_x \sum_a \Pr_{A,B|X}(a, x|x) = \sum_x \Pr_{B|X}(x|x) \\
&= \sum_x \Pr_B(x) = 1,
\end{aligned}$$

where we used non-signaling to conclude $\Pr_{B|X}(\cdot|\cdot) = \Pr_B(\cdot)$. Let $\lambda_x = \frac{\sum_a \Pr_V(a) \Pr_{A,B|X,V}(a,x|x,a)}{\Pr(V=A)}$. Note that $0 \leq \lambda_x \leq 1$ (because $\lambda_x = \Pr(B = x | X = x, A = V)$), so $\sum_x \lambda_x \leq \frac{1}{\Pr(V=A)}$. Since $1/\Pr(V = A) = 2^{n_A}$, we have $\Pr(B = X|V = A) \leq Q(2^{n_A}, X)$. □

4 Two-way communication

We extend this postselection technique to the two-way case.

Theorem 4.1. *Suppose that Alice receives a random n-bit string X, and engages in a two-way non-local communication protocol P with Bob. Let n_A denote the total number of bits sent from Alice to Bob, over all rounds of communication. The maximum probability that Bob can guess X is at most $Q(2^{n_A}, X)$, where $Q(\ell, X)$ is the probability mass of the ℓ most likely strings of X.*

Proof. Consider the following modification to the protocol: whenever Alice sends a message m_{i+1}^A to Bob in round i, Bob will ignore the message and instead replace it with a uniformly random string v_i of the same length. Thus, this becomes a one-sided communication protocol, where only Bob is sending messages to Alice. Call this modified protocol P'. Observe that the original protocol P is recovered when we postselect on Bob correctly guessing Alice's messages in every round. We now analyze the ability of Bob to guess Alice's input X at the end of protocol P'. Let A_i (which, for notational brevity, includes Bob's message from the previous round) denote the input to $\mathcal{A}_i$, and let A_{i+1} denote its output. Let (B_i, V_i) denote the input to $\mathcal{B}_i$, and let B_{i+1} be its output. We first argue that in P' the output B_{i+1} of box $\mathcal{B}_i$ is independent of X. The case of $i = 1$ (the first round) is handled by the one-way argument above. Assume as our inductive hypothesis that B_i is independent of X. Then, for any fixed x, b_{i+1},

$$\begin{aligned}
\Pr_{B_{i+1}|X}(b_{i+1}|x) &= \sum_{a_i,b_i,v_i} \Pr_{A_i,B_i,V_i|X}(a_i, b_i, v_i|x) \Pr_{B_{i+1}|A_i,B_i,V_i}(b_{i+1}|a_i, b_i, v_i) \\
&= \sum_{a_i,b_i,v_i} \Pr_{B_i,V_i|X}(b_i, v_i|x) \Pr_{B_{i+1}|B_i,V_i}(b_{i+1}|b_i, v_i) \\
&= \sum_{b_i} \Pr_{B_i|X}(b_i|x) \sum_{v_i} \Pr_{V_i}(v_i) \Pr_{B_{i+1}|B_i,V_i}(b_{i+1}|b_i, v_i) \\
&= \sum_{b_i} \Pr_{B_i}(b_i) \Pr_{B_{i+1}|B_i}(b_{i+1}|b_i) \\
&= \Pr_{B_{i+1}}(b_{i+1})
\end{aligned}$$

where in the second equality we use the fact that $(\mathcal{A}_i, \mathcal{B}_i)$ is non-signaling, and in the fourth equality we used our inductive hypothesis that B_i is independent of X. This completes the induction.

Let B_{r+1} denote the output of Bob in the last round of P'. Let $V = (V_1, \ldots, V_r)$ and let $M^A = (M_1^A, \ldots, M_r^A)$ (i.e. Alice's messages to Bob). Then the probability that Bob successfully guesses X in the original protocol P is his guessing probability in P' conditioned on the event that $V = M^A$. Observe that the essential ingredient in the proof of Theorem 3.1 is that Bob's output is independent of X, which we have established here as well. Therefore, we similarly get that $\Pr(B_{r+1} = X|V = M^A) \leq Q(2^{n_A}, X)$, which completes the proof.

□

Acknowledgements

We thank Ashwin Nayak for helpful comments on our manuscript and for sending us the draft of [1]. HY is supported by an NSF Graduate Fellowship Grant No. 1122374 and National Science Foundation Grant No. 1218547. XW is funded by ARO contract W911NF-12-1-0486 and by the NSF Waterman Award of Scott Aaronson.

References

[1] Shima Bab Hadiashar, Matthias Christandl, Ashwin Nayak, and Renato Renner. Communication complexity of one-shot remote state preparation. *Manuscript*, 2015.

[2] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[3] Miguel Navascués, Yelena Guryanova, Matty J Hoban, and Antonio Acín. Almost quantum correlations. *arXiv preprint arXiv:1403.4621*, 2014.

[4] Ashwin Nayak and Julia Salzman. Limits on the ability of quantum states to convey classical messages. *Journal of the ACM (JACM)*, 53(1):184–206, 2006.

[5] Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, 1994.

[6] Wim Van Dam. Implausible consequences of superstrong nonlocality. *arXiv preprint quant-ph/0501159*, 2005.