A New, Fully Quantum Notion of Information Complexity, and an Application to Direct Sum for Bounded Round Quantum Communication Complexity

Dave Touchette [1]

We present the first general direct sum theorem for quantum communication complexity that holds for more than a single round of communication. A direct sum theorem states that to compute n tasks simultaneously requires as much resources as the amount of the given resource required for computing them separately. By a general direct sum theorem, we mean a direct sum theorem that holds for arbitrary relations on arbitrary inputs. The direct sum question, and the related direct product question, are of central importance in the different models of communication complexity. They have been the subject of a lot of attention in recent years. Many results were obtained for different models of classical communication complexity [8, 26, 40, 43, 27, 22]. Progress for quantum communication complexity has been slower, with most results focusing on a single round of communication [46, 10, 39]. Some notable exceptions for the multi-round case are the work of Klauck, Špalek and de Wolf [52] in which they derive a direct product theorem for disjointness, and the works of Shaltiel [59], Lee, Shraibman and Špalek [53] and Sherstov [60] deriving direct product theorems for functions for which the discrepancy or generalized discrepancy method is tight. Even for a single round of communication, a general direct sum theorem was only proved earlier this year, using techniques much different from ours [6]. Previous to that work, techniques were restricted to proving results for the restricted case of product inputs. As a corollary of our results, we also obtain slightly improved parameters for the direct sum theorem of Ref. [6], for the single round case.

The tools that we develop to achieve such a result should be of independent interest for the quantum communication complexity and quantum information theory communities. In particular, we introduce new notions of fully quantum information cost and complexity based on conditional mutual information, derive many properties for these, and provide a one-shot compression protocol that reduce the communication cost of a protocol proportionally to its information cost. To arrive at the new definitions, we provide a new interpretation of the classical information cost, relating it to classical channel simulation with side information, the quantum analog of which being state redistribution. Another particularly interesting potential application of quantum information complexity is for tightly characterizing the bounded round quantum communication complexity of the disjointness function, an open question for more than 10 years [4, 45]. We discuss below what we believe is the most significant progress in recent years towards answering this important question. The main bottleneck to arrive at such a tight characterization is related to the development of lower bounds on the von Neumann conditional mutual information, a problem of great interest in quantum information theory [55, 19, 54, 18].

Quantum Information Complexity The classical notion of information cost was introduced by Chakrabarti, Shi, Wirth and Yao [30], who used it to derive a direct sum result for the simultaneous message passing model. The notion they introduced is similar to what is known today as the external information cost. A notion similar to what is now known as the internal information cost was later introduced by Bar-Yossef, Jayram, Kumar and Sivakumar [7] to use a direct sum property for composite problems that decompose into simpler ones, like the disjointness function in term of the AND function. The modern notions of external and internal information cost were formally introduced by Barak, Braverman, Chen and Rao [8], in which they prove (non-tight) general direct sum theorems for randomized communication complexity. In particular, for input X and Y of Alice and Bob, respectively, shared randomness R, private randomness R_A, R_B available to Alice and Bob, respectively and protocol transcript $\Pi(X, Y, R, R_A, R_B)$, the internal information cost is defined as $IC_{int}(\Pi, \mu) = I(X; \Pi | YR) + I(Y; \Pi | XR)$, and the external one as $IC_{ext}(\Pi, \mu) = I(XY; \Pi | R)$. Note that we have used Π to represent both the protocol and the protocol transcript, while μ is the prior distribution on the inputs X, Y. It is important that only the shared randomness R enters in the information costs. The interpretation of internal information cost is usually as the amount of information about Alice's input leaked to Bob plus the amount of information about Bob's input leaked to Alice, while for the external information it is as the amount of information about the joint input of Alice and Bob leaked to an external observer. Subsequent work by Braverman and Rao [26] provided an operational interpretation of internal information complexity as the

[1] touchette.dave@gmail.com, Laboratoire d'informatique théorique et quantique, Département d'informatique et de recherche opérationnelle, Université de Montréal.

amortized distributional communication complexity, i.e. the communication complexity per copy for computing n copies of a task, in the asymptotic limit of large n. They also provide a general direct sum theorem for bounded round communication complexity. Braverman [20] provides a similar operational interpretation of a prior-free version of information complexity as the amortized randomized communication complexity. He also list several interesting open questions related to information complexity, one of which is to develop a quantum analog of information complexity. He also asks whether the inherent reversibility of quantum computing, among other properties of quantum information, will impose a limit on the potential applications of such a quantity. Note that our results finally settle this: an operationally motivated and useful notion of quantum information cost can indeed be defined.

In the quantum setting, many difficulties are immediately apparent in trying to generalize the classical definition. Firstly, by the no-cloning theorem [35, 64], there is no direct analogue for quantum communication of the notion of a transcript, available to all parties and containing all previous messages. In the entanglement assisted model, we can replace quantum communication by twice as much classical communication, by using teleportation [11]. However, if we consider the transcript obtained by replacing quantum communication by classical communication in this way, this transcript will be completely uncorrelated to the corresponding quantum messages and to the inputs. Indeed, the classical messages sent in the teleportation protocol are uniformly random, unless we take the remaining part of the EPR pair into account. A possible way around this might be to try to adapt the classical definition by measuring the correlations between the inputs and the whole state, after reception of each message, of the receiving party. We can then even sum over the information contained in all messages. This yield a sensible notion of quantum information cost which is partly classical, and a similar quantity was used by Jain, Radhakrishnan and Sen [45] to obtain a beautiful proof of a lower bound on the bounded round quantum communication complexity of the disjointness function. A further variation on this was used by Jain and Nayak [42] to obtain a lower bound for a variant of the Index function. Work on direct sum results for a single round of communication also consider related notions [46, 39, 6]. However, these partly classical notions of quantum information cost all suffer from the drawback that they are only a lower bound on the communication cost once they have been divided by the number of messages. Then, the corresponding notion of quantum information complexity does not have the clear operational interpretation of classical information complexity as the amortized communication complexity, and is probably restricted to applications in bounded round scenarios.

We propose a new notion of quantum information cost, and a corresponding notion of quantum information complexity. These are the first fully quantum definitions for such quantities. In particular, the notion of cost applies to arbitrary bipartite quantum protocols that are run on arbitrary bipartite quantum inputs, and the notion of complexity applies to arbitrary quantum tasks on arbitrary quantum input. Of particular interest in the setting of quantum communication complexity that we focus on in this work is the case of quantum protocols implementing classical tasks, e.g. evaluating arbitrary bipartite classical functions or relations on arbitrary bipartite input distributions below a specified error bound. However, the notion might also find applications for fully quantum tasks, for example quantum correlation complexity [48, 49], remote state preparation [38], or interactive variants of state redistribution [56, 34, 66] and its special cases of state merging [36, 37, 16, 5, 17], state splitting [5, 17], and source coding [58]. To arrive at such a definition, we propose a new interpretation of the classical internal information cost. Indeed, if we view each message generation in a protocol as a channel, then the information cost can be seen to be equal to the sum of the asymptotic costs of simulating many copies of each such channel with side information at the receiver and feedback to the sender [56], a task related to the reverse Shannon theorem [13, 63, 5, 12, 17]. Using known bounds for this task [56], this yield a strengthening of the classical amortized communication result for bounded round complexity [26, 20]. In the fully quantum setting, channel simulation, with side information at the receiver and with environment given as feedback to the sender, is equivalent to the state redistribution task. This insight leads to the new, fully quantum definitions of information cost and complexity. These new definitions are the firsts to satisfy all of the properties that we stated as desirable for these quantum notions. In particular, we prove the following properties in Ref. [1].

Theorem 1 The quantum information cost directly provides a lower bound on quantum communication cost for any protocol and input state, independent of the number of messages of the protocol (Lemma 1 in Ref. [1]).

The corresponding quantum information complexity is exactly equal to the amortized quantum communication complexity for any quantum task with fixed input state, and in particular for any distributional classical task (Theorem 2 in Ref. [1]).

Quantum information complexity obeys an exact direct sum property (Corollary 3 in Ref. [1]).

For these last two results, they hold both for a fixed or unlimited number of messages.

Protocol Compression and Direct Sum To obtain the direct sum result in Ref. [2], we also prove a protocol compression result stating that we can compress a single copy of a bounded round protocol proportionally to its information cost. A technical ingredient in this proof is a single-message one-shot state redistribution protocol. A state redistribution protocol on input state ρ^{ABC}, with the A and C registers initially held by Alice, and the B register held by Bob, is a protocol that effectively transmits the C register to Bob while keeping the overall correlation with a purifying register R, up to some small error ε. We obtain in a joint work with Berta and Christandl [3] a communication rate upper bounded by $H_{max}^{\varepsilon/4}(C|B) - H_{min}^{\varepsilon/4}(C|BR) + O(\log(1/\varepsilon))$. Independently of our work, similar upper bounds on one-shot state redistribution have been obtained by Datta, Hsieh and Oppenheim [33].

We then use the substate theorem of Jain, Radhakrishnan and Sen [44, 47, 41] to transform this into a bound in terms of von Neumann conditional entropies, and what remains is a term proportional to the von Neumann conditional mutual information, as in asymptotic state redistribution. Our compression protocol applies this single message compression iteratively. We formulate precisely the dependence on the additional error and the number of messages in Theorem 2.

By combining this protocol compression result with many properties of quantum information complexity in Theorem 1 above, we can obtain our main theorem, a direct sum theorem for bounded round quantum communication complexity that holds for all quantum tasks. Note that the theorem holds in the model in which we allow for arbitrary pre-shared entanglement. For concreteness, we state the result for classical relations.

Theorem 2 For each M-message protocol Π and input state ρ, there exists an M-message compression protocol Π' implementing Π on input ρ up to error $M\varepsilon$, and satisfying $QCC(\Pi') \in O((QIC(\Pi, \rho) + 1)/\varepsilon^2 + M/\varepsilon^2)$. (Lemma 6 in Ref. [2])

For any $\varepsilon_1, \cdots, \varepsilon_n, \varepsilon'' \in (0, 1/2)$, any relations $R_1, \cdots, R_n$ and any number of message M, $QCC^M(\otimes_i (R_i, \varepsilon_i)) \in \Omega(\sum_i ((\frac{\varepsilon''}{M})^2 QCC^M(R_i, \varepsilon_i + \varepsilon'') - M)))$. In particular, $QCC^M((R, \varepsilon)^{\otimes n}) \in \Omega(n((\frac{\varepsilon''}{M})^2 QCC^M(R, \varepsilon + \varepsilon'') - M))$ (Corollary 4 in Ref. [2]).

Other Applications for Quantum Information Complexity Two of the main areas of success of classical information complexity is in obtaining direct sum and direct product theorems, and in obtaining communication complexity lower bounds, in particular on composite functions built from simpler component functions. Quantum information complexity also satisfy an exact direct sum property for such composite functions. Indeed, we show that on a suitably chosen input distribution, the quantum information complexity of disjointness on n bits is exactly equal to n times the quantum information complexity of the AND function on 2 bits. A similar property was used by Jain, Radhakrishnan and Sen [45] to obtain a lower bound of $\Omega(n/M^2 + M)$ for the communication complexity of M-message quantum protocols, close to the best known upper bound of $O(n/M + M)$ [4, 45]. Since our notion of information cost is directly a lower bound on communication, while their notion, in general, must first be divided by M before yielding a lower bound on communication, we seem to get an improvement by a factor of M, which would match the best known upper bound. This result seems to lead to the most significant progress since the work of Ref. [45] towards obtaining the tight bounded round quantum communication complexity of disjointness; see Section 7 and 8 in Ref. [1] for details. However, the main bottleneck to complete the argument appears to be the fact that our notion of quantum information cost is defined in term of fully quantum conditional mutual information, a quantity that is much less understood than its classical counterpart. Obtaining meaningful lower bound on quantum conditional mutual information is a notoriously hard problem in quantum information theory [55], with some progress in recent years [19, 54, 18].

Other potential applications is in obtaining time-space trade-off for quantum streaming algorithms [52, 42], obtaining the exact, up to second order, communication complexity of some problems [24], investigating the direct sum question in an unlimited round setting [8], and obtaining direct product theorems (even single round).

References

[1] Dave Touchette. *Quantum Information Complexity and Amortized Communication.* arXiv preprint, quant-ph/1404.3733.

[2] Dave Touchette. *Direct sum for bounded round entanglement-assisted communication complexity.* arXiv preprint, quant-ph/1409.4391.

[3] Mario Berta, Matthias Christandl, Dave Touchette. *Smooth Entropy Bounds on One-Shot State Redistribution.* arXiv preprint, quant-ph/1409.4338.

[4] Scott Aaronson, and Andris Ambainis. *Quantum Search of Spatial Regions.* Proceedings of the 44rd Annual IEEE Symposium on Foundations of Computer Science (2003): 200-209.

[5] Anura Abeyesinghe, Igor Devetak, Patrick Hayden, and Andreas Winter. *The mother of all protocols: Restructuring quantum information's family tree.* Proceedings of the Royal Society of London. Series A (2009): 2537-2563.

[6] Anurag Anshu, Rahul Jain, Priyanka Mukhopadhyay, Ala Shayeghi, and Penghui Yao. *A new operational interpretation of relative entropy and trace distance between quantum states.* arXiv:quant-ph/1404.1366.

[7] Ziv Bar-Yossef, T. S. Jayram, Ravi Kumar, and D. Sivakumar. *An information statistics approach to data stream and communication complexity.* Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science (2002): 209-218.

[8] Boaz Barak, Mark Braverman, Xi Chen, and Anup Rao. *How to compress interactive communication.* Proceedings of the 42nd Annual ACM Symposium on Theory of Computing (2010): 67-76.

[9] Howard Barnum, Claude Crepeau, Daniel Gottesman, Adam Smith, and Alain Tapp. *Authentication of Quantum Messages.* Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science (2002): 449-458.

[10] Avraham Ben-Aroya, Oded Regev, and Ronald de Wolf. *A hypercontractive inequality for matrix-valued functions with applications to quantum computing and LDCs* Proceedings of the Forty-Ninth Annual IEEE Symposium on Foundations of Computer Science (2008): 477-486.

[11] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wooters. *Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels.* Physical Review Letters 70.13 (1993): 1895-1899.

[12] Charles H. Bennett, Igor Devetak, Aram W. Harrow, Peter W. Shor, and Andreas Winter. *Quantum Reverse Shannon Theorem.* arXiv:quant-ph/0912.5537.

[13] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. *Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem.* IEEE Transactions on Information Theory 48.10 (2002): 2637-2655.

[14] Charles H. Bennett and Stephen J. Wiesner. *Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states.* Physical Review Letters 69.20 (1992): 2881-2884.

[15] Mario Berta, and Matthias Christandl. *One-Shot Quantum State Redistribution.* Unpublished notes (2010).

[16] Mario Berta. *Single-shot quantum state merging.* Master's thesis, ETH Zurich, 2008.

[17] Mario Berta, Matthias Christandl, Renato Renner. *The Quantum Reverse Shannon Theorem based on One-Shot Information Theory.* Commununications in Mathematical Physics 306 (2011): 579-615.

[18] Mario Berta, Kaushik Seshadreesan, and Mark M. Wilde. *Renyi generalizations of the conditional quantum mutual information.* arXiv:quant-ph/1403.6102.

[19] Fernando G. S. L. Brandao, Matthias Christandl, Jon Yard. *Faithful Squashed Entanglement.* Commununications in Mathematical Physics 306 (2011): 805-830.

[20] Mark Braverman. *Interactive information complexity.* Proceedings of the 44th Annual ACM Symposium on Theory of Computing (2012): 505-524.

[21] Mark Braverman. *Coding for Interactive Computation: Progress and Challenges.* Proceedings of the 50th Annual Allerton Conference on Communication, Control, and Computing (2012): 1914:1921.

[22] Mark Braverman. *Interactive information and coding theory.* A survey accompanying an invited lecture at ICM'14 in Seoul.

[23] Mark Braverman, Faith Ellen, Rotem Oshman, Toniann Pitassi, and Vinod Vaikuntanathan. *Tight bounds for set disjointness in the message passing model.* Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (2013): 668-677.

[24] Mark Braverman, Ankit Garg, Denis Pankratov, and Omri Weinstein. *From information to exact communication.* Proceedings of the 45th Annual ACM Symposium on Theory of Computing (2013): 151-160.

[25] Mark Braverman, and Ankur Moitra. *An information complexity approach to extended formulations.* Proceedings of the 45th Annual ACM Symposium on Theory of Computing (2013): 161-170.

[26] Mark Braverman, and Anup Rao. *Information equals amortized communication.* Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science (2011): 748-757.

[27] Mark Braverman, Anup Rao, Omri Weinstein, Amir Yehudayoff. *Direct products in communication complexity.* Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (2013).

[28] André Chailloux, and Giannicola Scarpa. *Parallel Repetition of Entangled Games with Exponential Decay via the Superposed Information Cost.* arXiv:quant-ph/1310.7787, presented at QIP2014.

[29] Richard Cleve, and Harry Buhrman. *Substituting quantum entanglement for communication.* Physical Review A 56.2 (1997): 1201-1204.

[30] A. Chakrabarti, Yaoyun Shi ; A. Wirth, Andrew C.-C. Yao. *Informational complexity and the direct sum problem for simultaneous message complexity.* Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science (2001): 270-278.

[31] Wim van Dam, and Patrick Hayden. *Universal entanglement transformations without communication.* Physical Review A 67.6 (2003): 060302(R).

[32] Nilanjana Datta, and Min-Hsiu Hsieh. *The apex of the family tree of protocols: optimal rates and resource inequalities.* New Journal of Physics 13(9) (2011): 093042.

[33] Nilanjana Datta, Min-Hsiu Hsieh, and Jonathan Oppenheim. *An upper bound on the second order asymptotic expansion for the quantum communication cost of state redistribution.* arXiv preprint, quant-ph/1409.4352.

[34] Igor Devetak, and Jon Yard. *Exact cost of redistributing multipartite quantum states.* Physical Review Letters 100.23 (2008): 230501.

[35] Dennis Dieks. *Communication by EPR devices.* Physics Letters A 92.6 (1982):271-272.

[36] Michal Horodecki, Jonathan Oppenheim, Andreas Winter. *Partial quantum information.* Nature 436 (2005):673-676.

[37] Michal Horodecki, Jonathan Oppenheim, Andreas Winter. *Quantum state merging and negative information.* Comm. Math. Phys. 269, 107 (2007).

[38] Rahul Jain. *Communication complexity of remote state preparation with entanglement.* Quantum Information and Computation 6 (4,5), 461-464 (2006).

[39] Rahul Jain, Hartmut Klauck. *New results in the simultaneous message passing model via information theoretic techniques.* The 24th IEEE Conference on Computational Complexity (2009): 369-378.

[40] Rahul Jain, Hartmut Klauck, Ashwin Nayak. *Direct product theorems for classical communication complexity via subdistribution bounds.* The 40th ACM Symposium on Theory of Computing (2008): 599-608.

[41] Rahul Jain, and Ashwin Nayak. *Short proofs of the quantum Substate Theorem.* IEEE Trans. Inf. Theory 58(6), 3664 - 3669 (2012).

[42] Rahul Jain, and Ashwin Nayak. *The space complexity of recognizing well-parenthesized expressions in the streaming model: the Index function revisited.* To appear in: IEEE Transactions on Information Theory.

[43] Rahul Jain, Attila Pereszlnyi, and Penghui Yao. *A direct product theorem for bounded-round public-coin randomized communication complexity.* Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science (2012): 167-176.

[44] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. *Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states.* Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science (2002): 429-438.

[45] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. *A lower bound for bounded round quantum communication complexity of set disjointness.* Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (2003): 220-229.

[46] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. *Prior entanglement, message compression and privacy in quantum communication.* The 20th IEEE Conference on Computational Complexity (2005): 285-296.

[47] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. *A new information-theoretic property about quantum states with an application to privacy in quantum communication.* Journal of ACM 56(6), 33 (2009).

[48] Rahul Jain, Yaoyun Shi, Zhaohui Wei, and Shengyu Zhang. *Efficient protocols for generating bipartite classical distributions and quantum states.* IEEE Transctions on Information Theory, 59 (2013):51715178.

[49] Rahul Jain, Zhaohui Wei, Penghui Yao, and Shengyu Zhang. *Multipartite Quantum Correlation and Communication Complexities.* arXiv:quant-ph/1405.6015 (2014).

[50] Iordanis Kerenidis, Sophie Laplante, Virginie Lerays, Jérémie Roland, and David Xiao. *Lower Bounds on Information Complexity via Zero-Communication Protocols and Applications.* Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science (2012): 500-509.

[51] Hartmut Klauck, Ashwin Nayak, Amnon Ta-Shma, David Zuckerman. *Interaction in quantum communication and the complexity of set disjointness.* Proceedings of the 33rd Annual ACM Symposium on Theory of Computing (2001): 124-133.

[52] Hartmut Klauck, Robert Špalek, and Ronald de Wolf. *Quantum and classical strong direct product theorems and optimal time-space tradeoff.* SIAM J. Comput., 36 (2007): 1472-1493

[53] Troy Lee, Adi Shraibman, and Robert Špalek. *A direct product theorem for discrepancy.* Proceedings of the Twenty-Third Annual IEEE Conference on Computational Complexity (2008): 71-80.

[54] Ke Li, Andreas Winter. *Relative entropy and squashed entanglement.* Commun. Math. Phys. 326(1):63-80, 2014.

[55] Elliott H. Lieb, and Mary Beth Ruskai. *Proof of the strong subadditivity of quantum-mechanical entropy.* Journal of Mathematical Physics, 14 (1973): 1938-1941.

[56] Zhicheng Luo, and Igor Devetak. *Channel Simulation With Quantum Side Information.* IEEE Transactions on Information Theory 55.3 (2009): 1331-1342.

[57] Laura Mančinska, Thomas Vidick. *Unbounded entanglement can be needed to achieve the optimal success probability.* arXiv:quant-ph/1402.4145.

[58] Benjamin Schumacher. *Quantum coding* Physical Review A, 51(4):2738-2747, 1995.

[59] Ronen Shaltiel. *Towards proving strong direct product theorems.* Computational Complexity 12 (2003): 1-22.

[60] Alexander A. Sherstov. *Strong direct product theorems for quantum communication and query complexity.* Proceedings of the 43rd Annual ACM Symposium on Theory of Computing (2011): 41-50.

[61] John Watrous. *Theory of Quantum Information.* Lecture notes from Fall 2013, https://cs.uwaterloo.ca/ watrous/CS766/ (2013).

[62] Mark M. Wilde. *Quantum Information Theory.* Cambridge University Press (2013), Preliminary version available as: arXiv e-print quant-ph/1106.1445.

[63] Andreas Winter. *Compression of sources of probability distributions and density operators* arXiv: quant-ph/0208131 (2002).

[64] William K. Wootters, and Wojciech H. Zurek. *A single quantum cannot be cloned.* Nature 299.5886 (1982): 802-803.

[65] Andrew C.-C. Yao. *Quantum circuit complexity.* Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science (1993): 352-361.

[66] Jon T. Yard, and Igor Devetak. *Optimal Quantum Source Coding With Quantum Side Information at the Encoder and Decoder.* IEEE Transactions on Information Theory 55.11 (2009): 5339-5351.