The Flow of Information in Interactive Quantum Protocols: the Cost of Forgetting*†

Mathieu Laurière‡[1] **and Dave Touchette**§[2]

1 **NYU-ECNU Institute of Mathematical Sciences at NYU Shanghai, China**
mathieu.lauriere@gmail.com
2 **Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, and Perimeter Institute for Theoretical Physics, Waterloo, Canada**
touchette.dave@gmail.com

Abstract

In two-party interactive quantum communication protocols, we study a recently defined notion of quantum information cost (QIC), which has most of the important properties of its classical analogue (IC). Notably, its link with amortized quantum communication complexity has been used to prove an (almost) tight lower bound on the bounded round quantum complexity of Disjointness. However, QIC was defined through a purification of the input state. This is valid for fully quantum inputs and tasks but difficult to interpret even for classical tasks. Also, its link with other notions of information cost that had appeared in the literature was not clear.

We settle both these issues: for quantum communication with classical inputs, we characterize QIC in terms of information about the input registers, avoiding any reference to the notion of a purification of the classical input state. We provide an operational interpretation of this new characterization as the sum of the costs of revealing and of forgetting information about the inputs. To obtain this result, we prove a general Information Flow Lemma assessing the transfer of information in general interactive quantum processes. Specializing this lemma to interactive quantum protocols accomplishing classical tasks, we are able to demistify the link between QIC and other previous notions of information cost in quantum protocols. Furthermore, we clarify the link between QIC and IC by simulating quantumly classical protocols.

Finally, we apply these concepts to argue that any quantum protocol that does not forget information solves Disjointness on n-bits in $\Omega(n)$ communication, completely losing the quadratic quantum speedup. Hence forgetting information is here a necessary feature in order to obtain any significant improvement over classical protocols. We also prove that QIC at 0-error is exactly n for Inner Product, and $n(1-o(1))$ for a random Boolean function on $n+n$ bits.

1998 ACM Subject Classification F.1.3 Complexity Measures and Classes, E.4 Coding and Information Theory

Keywords and phrases Communication Complexity, Information Complexity, Quantum Computation and Information

Digital Object Identifier 10.4230/LIPIcs.ITCS.2017.47

* A long version of this work can be found on arXiv.org, see https://arxiv.org/abs/1701.02062.

† The authors are very grateful to Anurag Anshu, André Chailloux, Ankit Garg, Iordanis Kerenidis, Ashwin Nayak, and Penghui Yao for many useful discussions.

‡ M.L. has been supported by ERC grant QCC. D.T. is supported in part by NSERC, CIFAR, Industry Canada and ARL CDQI program. IQC and PI are supported in part by the Government of Canada and the Province of Ontario. Part of this research was conducted while M.L. was a PhD student with the Institut de Recherche en Informatique Fondamentale, Université Paris Diderot

§ Part of this research was conducted while D.T. was a PhD student with the Département d'informatique et de recherche opérationnelle, Université de Montréal and was supported in part by a FRQNT B2 Doctoral research scholarship, and by CryptoWorks21.

8th Innovations in Theoretical Computer Science Conference (ITCS 2017).
Editor: Christos H. Papadimitrou; Article No. 47; pp. 47:1–47:1

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany