Optimizing conditional entropies for quantum correlations

Omar Fawzi

Inria

omar.fawzi@ens-lyon.fr

Peter Brown

Inria

peter.brown@inria.fr

Hamza Fawzi

Cambridge University

hamzafawzi@gmail.com

The rates of quantum cryptographic protocols are usually expressed in terms of a conditional entropy minimized over a certain set of quantum states. In the so-called device-independent setting, the minimization is over all the quantum states of arbitrary dimension jointly held by the adversary and the parties that are consistent with the statistics that are seen by the parties. We introduce new quantum divergences and use techniques from noncommutative polynomial optimization to approximate such entropic quantities.

Based on https://arxiv.org/abs/2007.12575