Constant-round Blind Classical Verification of Quantum Sampling

Han-Hsuan Lin
Dept. of Computer Science, NTHU

In a recent breakthrough, Mahadev constructed a classical verification of quantum computation (CVQC) protocol for a classical client to delegate decision problems in BQP to an untrusted quantum prover under computational assumptions. In this work, we explore further the feasibility of CVQC with the more general sampling problems in BQP and with the desirable blindness property. We contribute affirmative solutions to both as follows.

We initiate the study of CVQC for quantum sampling problems (denoted by $\SampBQP$). In a CVQC protocol for a $\SampBQP$ problem, the prover and the verifier are given an input $x\in \{0,1\}^n$ and a quantum circuit C, and the goal of the classical client is to learn a sample from the output $z \leftarrow C(x)$ up to a small error, from its interaction with an untrusted prover. We demonstrate its feasibility by constructing a four-message CVQC protocol for $\SampBQP$ based on the quantum Learning With Error assumption.

The blindness of CVQC protocols refers to a property of the protocol where the prover learns nothing, and hence is blind, about the client's input. It is a highly desirable property that has been intensively studied for the delegation of quantum computation. We provide a simple yet powerful generic compiler that transforms any CVQC protocol to a blind one while preserving its completeness and soundness errors as well as the number of rounds.