

Quantum delegation with an off-the-shelf device

Anne Broadbent


University of Ottawa

Abstract

Given that reliable cloud quantum computers are becoming closer to reality, the concept of delegation of quantum computations and its verifiability is of central interest. Many models have been proposed, each with specific strengths and weaknesses. Here, we put forth a new model where the client trusts only its classical processing, makes no computational assumptions, and interacts with a quantum server in a single round. In addition, during a set-up phase, the client specifies the size n of the computation and receives an untrusted, off-the-shelf (OTS) quantum device that is used to report the outcome of a single constant-sized measurement from a predetermined logarithmic-sized input. In the OTS model, we thus picture that a single quantum server does the bulk of the computations, while the OTS device is used as an untrusted and generic verification device, all in a single round.

We show how to delegate polynomial-time quantum computations in the OTS model. Scaling up the technique also yields an interactive proof system for all of QMA, which, furthermore, we show can be accomplished in statistical zero-knowledge. This yields the first relativistic (one-round), two-prover zero-knowledge proof system for QMA.

As a proof approach, we provide a new self-test for n -EPR pairs using only constant-sized Pauli measurements, and show how it provides a new avenue for the use of simulatable codes for local Hamiltonian verification. Along the way, we also provide an enhanced version of a well-known



stability result due to Gowers and Hatami and show how it completes a common argument used in self-testing.

Based on joint work with Arthur Mehta and Yuming Zhao
arxiv:2304.03448.