

Black-Box Interactive Proofs for Quantum Many-vs-one Problems

Extended Abstract

[Abdelkhalig Elfatih]

[African Institute for Mathematical Sciences]

Abstract. In some quantum testing problems, an algorithm that may jointly measure many copies of the unknown object is dramatically more powerful than one restricted to processing copies one at a time. A resource-bounded experimentalist may delegate the difficult part of the task to an unrestricted but untrusted helper, and verify the answer with limited resources of their own. This thesis develops a framework for such delegation in a black-box setting, where the verifier knows only the problem and trusts no algorithmic detail of the helper. The resulting protocols are organized into four classes, and the search for delegable problems is reduced to identifying a geometric structure on the space of possible inputs.

Motivation

Quantum testing problems often exhibit an exponential complexity gap between joint-measurement and single-copy strategies. This asymmetry leaves memory-constrained algorithms unable to efficiently solve tasks that unconstrained ones find easy, motivating the need to safely delegate costly computations to an untrusted prover. We work in the *black-box* paradigm of Caro et al. [2025]. Here, the verifier knows only the problem description and a bound on an honest prover’s per-round query complexity, never the actual algorithm used, which may be proprietary or opaque. Crucially, since the prover may report any answer that suits its interests, the protocol must catch dishonesty with high probability without the verifier performing the computation themselves.

Research Question

For which many-vs-one quantum testing problems can a memory-constrained verifier benefit from delegation to an untrusted prover via a black-box interactive proof? Benefit requires genuine query savings over unassisted verification; soundness must hold against arbitrarily powerful dishonest provers. We focus on many-vs-one distinguishing problems: deciding whether an unknown instance equals a designated accept state or lies in a structured reject set.

Contributions

(i) **A four-class landscape.** We identify TCB and RSM (classes defined by black-box test-and-compute protocols), and OSP and ORP (structural classes defined intrinsically by orbital geometry on the instance space). Via $\text{OSP} \subseteq \text{RSM} \subseteq \text{TCB}$, a structural certificate yields a protocol certificate, while structural obstructions rule out delegability entirely, shifting the search from protocol design to identifying orbital structure. Furthermore, $\text{ORP} \not\subseteq \text{TCB}$: ORP requires a learning step producing a classical label to branch among OSP schemes, which cannot occur within a single TCB compute round.

(ii) **A universal RSM protocol.** Every RSM instance admits the same interactive proof (Algorithm 1), obtained by instantiating its components $(\mathcal{C}, \mathcal{R})$. Generalizing the purity-testing protocol of Caro et al. [2025], this transforms any structural OSP certificate into a concrete black-box interactive proof.

Related Work

Classical interactive proofs of proximity [Chiesa et al., 2018, Biswas et al., 2025] rely largely on problem-specific constructions rather than structural characterizations, an obstacle transferring to the quantum setting. Caro et al. [2025] initiated the systematic study of interactive proofs for quantum testing, introducing the black-box variant for purity testing; this thesis develops a general framework around it.

References

Caro et al. (2025). [Insert full details]

Chiesa et al. (2018). [Insert full details]

Biswas et al. (2025). [Insert full details]