Towards a quantum-inspired proof for IP = PSPACE

Ayal Green, Guy Kindler, Yupan Liu. Hebrew University of Jerusalem, Israel

Abstract

We explore quantum-inspired interactive proof systems where the prover is limited.

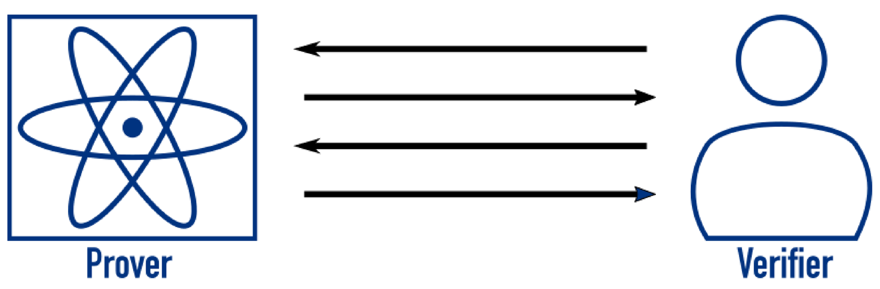
- We improve on a result by [AG17] showing a quantum-inspired interactive protocol (IP) for PreciseBQP where the prover is only assumed to be a PreciseBQP machine, and show that the result can be strengthened to show an IP for $\mathsf{NP}^{\mathsf{PP}}$ with a prover which is only assumed to be an $\mathsf{NP}^{\mathsf{PP}}$ machine - which was not known before.
- We also show how the protocol can be used to directly verify QMA computations, thus connecting the sum-check protocol by [AAV13] with the result of [AG17, LFKN90].

Our results shed lights on a quantum-inspired proof for PSPACE = IP, since PreciseQMA captures the full PSPACE power.

Definition: In-class interactive proofs (informal)

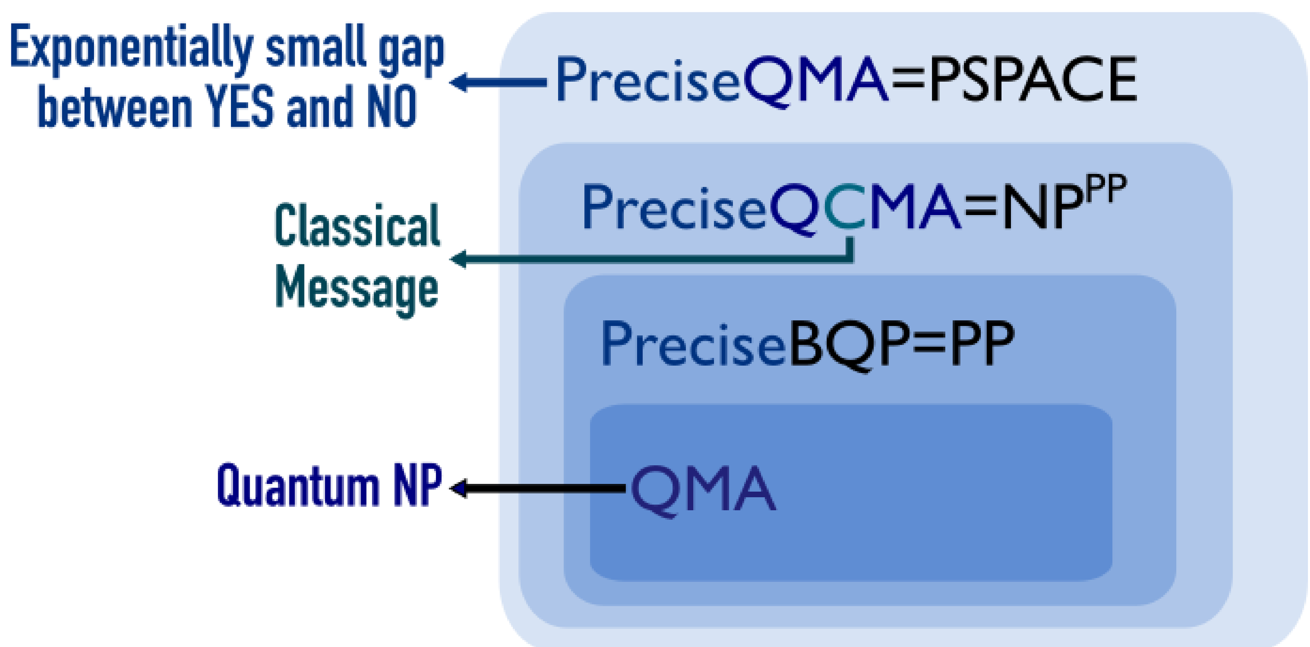
Let $\mathsf{IP}[\mathcal{P},\mathcal{V}]$ denote the following *efficient* interactive proofs:

- $\mathcal{P}$-power prover can delegate *any* problem in a language $\mathcal{L} \in \mathcal{P}$ to $\mathcal{V}$-power verifier, $\mathcal{V}$ usually is BPP.
- Soundness against *any* prover when the input $x \notin \mathcal{L}$.



Main Results

<u>Theorem</u> PreciseQCMA $\subseteq$ IP[PreciseQCMA, BPP].



Our Protocol for PreciseQCMA

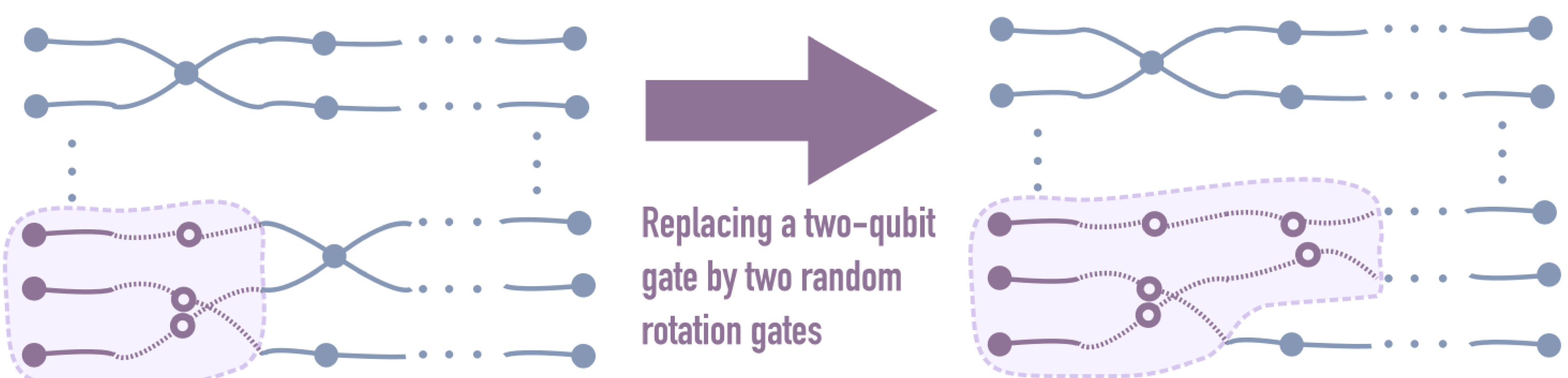
For any language $\mathcal{L} \in$ PreciseQCMA, given an instance $x \in \mathcal{L}$, one can verify $\mathcal{L}$ by the following:

Step 1 The verifier V ask the prover P for a witness w for x, where w is a *classical* message.

Step 2 The prover P and the verifier V follow an in-class interactive proof protocol W for PreciseBQP, and the verifier accepts if and only if W accepts.

Proof Technique: How to verify *precise* quantum computation?

[AG17] shows that PreciseBQP $\subseteq$ IP[PreciseBQP, BPP]. Namely, a protocol can verify the acceptance probability of a quantum circuit consisting of *polynomially many* local gates on n qubits, to within *inverse-exponential accuracy*.



Proof Technique: How to find a witness?

The prover can distinguish whether x is a *yes* or a *no* instance. However, in order to find a witness w of the given instance $x \in \mathcal{L}$, it is not enough – the prover need to do *adaptive search*.

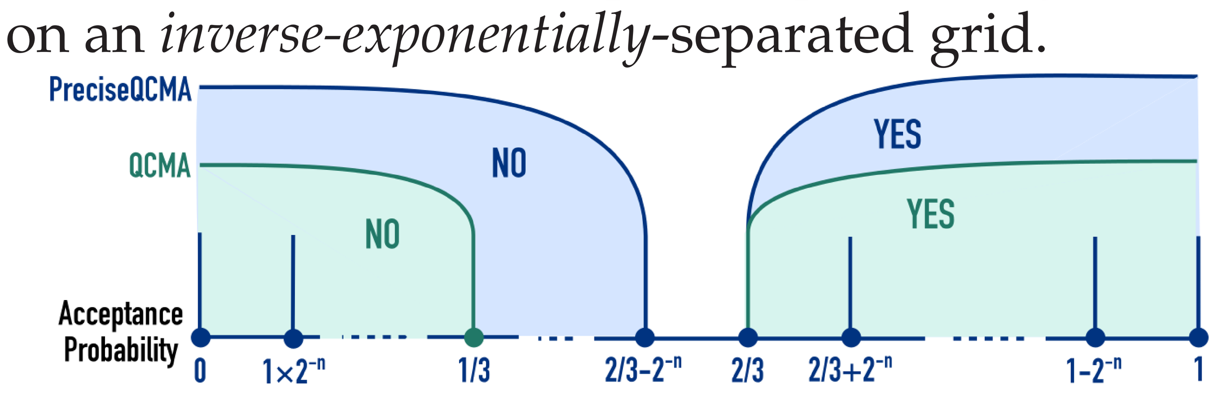
Witness-finding algorithm for NP: Adaptive Search

1. The verifier asks the prover if the claim S_0, "*there exists a witness for the instance x where the first bit is* 0", is true.
2. If the answer is "no", the verifier can ask about S_0, where the value of the bit is flipped. Otherwise, the first bit is 0.

The prover can find the first bit b of the witness, and the verifier can continue by asking about the statements S_b0 and S_b1, etc. .

Why this algorithm can be extended to PreciseQCMA?

- Such a PreciseQCMA oracle can verify the acceptance probability of a witness within an *inverse-exponential* accuracy.
- A certain structure of the PreciseQCMA verification circuit, which ensures that its acceptance probability for any witness lies on an *inverse-exponentially*-separated grid.



Open Problem: Towards an interactive proof for PostQMA

[MN17] shows that PostQMA = PSPACE. Since the gap between the *yes* and *no* case accept probabilities is constant, a witness-preserving amplification for PostQMA similar to QMA might lead an interactive proof for PSPACE.

Observation QMA $\subseteq$ IP[PreciseBQP, BPP].

Main idea Using the witness-preserving gap amplification for QMA [MW05, NWZ09], the acceptance probability of a correct QMA witness can be computed using a precise efficient quantum computation. Such a quantum circuit with a '*random*' witness can be verified by the protocol in [AG17].

Open problem 1 Is there a witness-preserving gap amplification technique for PostQMA? Such a technique is unknown due to the use of conditioned probability.

Open Problem: Towards an interactive proof for PreciseQMA

Could we extend our protocols for PreciseQCMA and QMA to PreciseQMA? Such quantum-inspired IP protocols might provide a direct proof for BQPSPACE $\subseteq$ IP. But there are obstacles:

The protocol for PreciseQCMA Even allowing quantum messages, it is not clear how a BQP verifier obtain exponential accuracy without needing *exponentially many copies* of the witness.

The protocol for QMA Amplifying an *exponentially-small gap* using the witness-preserving gap amplification technique used in [NWZ09] requires *exponentially many rounds*.

Open problem 2 Is there a direct proof for BQPSPACE $\subseteq$ IP?

References

[AAV13] Dorit Aharonov, Itai Arad, and Thomas Vidick. Guest column: the quantum pcp conjecture. *ACM SIGACT News*, 44(2):47–79, 2013.

[AG17] Dorit Aharonov and Ayal Green. A quantum inspired proof of $\mathsf{P}^{\#\mathsf{P}} \subseteq \mathsf{IP}$. *arXiv preprint arXiv:1710.09078*, 2017.

[LFKN90] Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. In *Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science*, pages 2–10. IEEE, 1990.

[MN17] Tomoyuki Morimae and Harumichi Nishimura. Merlinization of complexity classes above bqp. *Quantum Information & Computation*, 17(11-12):959–972, 2017.

[MW05] Chris Marriott and John Watrous. Quantum arthur–merlin games. *Computational Complexity*, 14(2):122–152, 2005.

[NWZ09] Daniel Nagaj, Pawel Wocjan, and Yong Zhang. Fast amplification of qma. *Quantum Information & Computation*, 9(11):1053–1068, 2009.