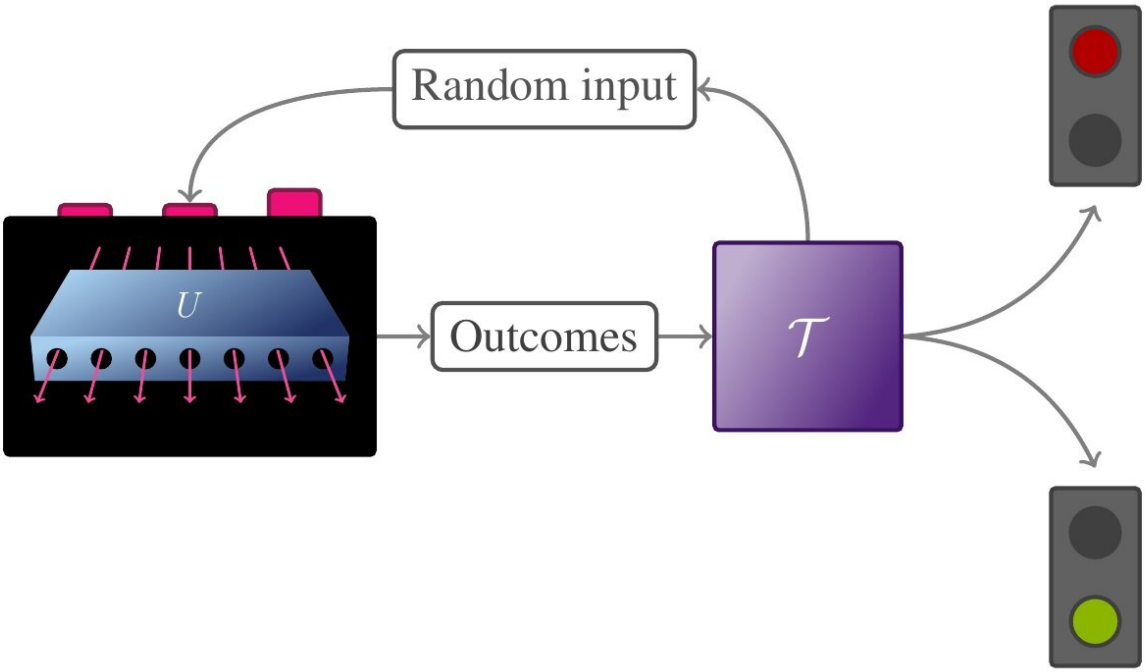
Quantum supremacy and its efficient certification difficult to achieve simultaneously

June 5 2019, by Lisa Zyga



A test to certify quantum supremacy will accept a probability distribution if it is classically hard, and otherwise will reject it. Credit: Hangleiter et al.

In an ironic twist, physicists have shown that the very property that can be used to show that quantum computing devices can solve some problems that classical computers cannot also makes it impossible to

efficiently certify that this "quantum supremacy" has indeed been achieved, for a wide variety of schemes. In quantum computing, the issue of certification is crucial for formally verifying the superior computing power of quantum devices.

The team from Germany, Dominik Hangleiter, Martin Kliesch, Jens Eisert, and Christian Gogolin, has published a paper on their work on quantum supremacy certification in a recent issue of *Physical Review Letters.*

"We rigorously prove an intuition that many in the field shared, namely, that certifying random sampling schemes proposed for a quantum supremacy demonstration requires exponentially many samples," Hangleiter, at the Free University of Berlin, told *Phys.org*. "One of the most intriguing findings of our work is that this is due to the very property that allows to prove approximate sampling hardness in the first place, namely, the flatness of the sampled distributions. Our work also points towards a potential way out of this dilemma: interactive or quantum certification protocols."

The term "quantum supremacy" refers to the possibility that quantum computing devices can solve some problems that are practically infeasible for classical computers to solve. One problem that is considered intractable for classical computers is random sampling from certain very flat distributions (in which all outcomes are nearly equally likely) over exponentially large datasets.

Currently, no universal, fault-tolerant quantum computer is available to experiment with, but even the limited quantum devices that are available today are thought to be capable of performing the random sampling task. Intuitively, this is because quantum devices can prepare a state in the correct superposition of all elements of a set, while classical devices need to access the exponentially many probabilities one by one.

One of the limitations of all physical devices (quantum or classical) is that they are only capable of approximate sampling. So in order to demonstrate quantum supremacy, researchers must show that a quantum device's approximate sampling is close enough to ideal sampling so that it is still intractable for classical computers.

All current proofs of this concept, which is called approximate sampling hardness, use small second moments. In the random sampling task, a distribution is randomly chosen. Essentially, small second moments mean that the randomly chosen distribution concentrates around the uniform distribution and is therefore very flat.

In the new paper, the researchers show that small second moments also forbid efficient certification from the samples alone. That is, sampling distributions with small second moments cannot be certified with polynomially many samples, but instead require exponentially many samples. This makes certification inefficient and unrealistic to perform in a reasonable amount of time.

The results hold for a variety of widely used sampling schemes, including boson sampling and universal random circuit sampling, among others. However, the results do not mean that efficient certification is necessarily impossible by any method. The researchers hope that, instead, the findings will motivate the development of alternative certification schemes, as well as proofs of approximate sampling hardness that apply to distributions with larger second moments.

"Our work guides the way for where to look for feasible certification schemes," Hangleiter said. "In particular, it often makes sense to use device-specific knowledge to leverage certification. One direction of research is to develop device-specific certification schemes both for quantum sampling schemes, but thinking further, also for more elaborate tasks that can be performed on quantum computers.

"Quantum sampling schemes are very 'clean' quantum supremacy proposals in the sense that they allow for a complexity-theoretic hardness argument. At the same time, they do not have real applications (yet). A second direction of research is to develop schemes that are feasible on near-term devices and yet hard, which also solve a useful task, as well as to find applications for the known sampling schemes."

More information: Dominik Hangleiter, Martin Kliesch, Jens Eisert, and Christian Gogolin. "Sample Complexity of Device-Independently Certified 'Quantum Supremacy.'" *Physical Review Letters*. DOI: 10.1103/PhysRevLett.122.210502

Also at arXiv:1812.01023 [quant-ph]