Resource Estimation for Proof of Quantumness

Jiayu Zhang

1 Background

In this project, we will investigate problems related to the resource estimation of proof-of-quantumness protocols.

Let's first review what is a proof-of-quantumness (PoQ) protocol. Let's imagine someone, like Microsoft, claim that they have built a super-powerful quantum computer. How could we verify that they are really doing some quantum stuff, instead of simply using a classical computer to cheat the world? One way to do it is to ask it to factor a big number—which is relatively easy for quantum computers by Shor's algorithm but is very hard for classical computers. One related notion is "quantum supremacy' ', where we would like to demonstrate that quantum computers could solve some problems better than classical computers. The difference between quantum supremacy and PoQ is that, in the demonstration of quantum supremacy the verifier could be inefficient—we rely on big classical supercomputers to verify the outputs of quantum chips; but in PoQ the verifier needs to be efficient: for example, in the Shor-based protocol above, the verifier only needs to check whether the outputs of the quantum computer is really a factoring of the original number.

Recently there are a series of new PoQ protocols based on post-quantum cryptography. One remarkable example is [BCMVV], which construct a PoQ protocol based on lattice cryptography. Later works [BKVV,LG21] give some optimization.

People would like to demonstrate these PoQ protocols in practice. To prepare for it, it's necessary to first give an estimation on how much quantum resource we need to implement these PoQ protocols. There are some existing works in this direction, like [Zhu22].

2 Problems

In this project we will work on the problem of estimating the resources for realizing quantum protocols.

In the protocols in [BCMVV,BKVV,LG21,Zhu22], an important step is roughly as follows. Below we first define a function and then describe the quantum operation.

For $A \in \mathbb{Z}_q^{m\times n}, y \in \mathbb{Z}_q^m, b \in \{0,1\}, x \in \mathbb{Z}_q^n$, define

$$f_{A,y}(b,x) = \lfloor Ax + by \rfloor \in \{0,1\}^m.$$

Let's explain the notations. Here $\mathbb{Z}_q$ means that all the additions are performed modulo q, A is a $m \times n$ matrix, Ax is the matrix-vector multiplication which produces an m-dimension vector, and by is the scalar multiplication between b and y, which is simply zero-vector when $b = 0$ and y when $b = 1$. The notation $\lfloor \cdot \rfloor$ is the rounding operation, which extracts the most significant bit in base 2. The operation is applied on each component of the vector.

For example, when $m = 3, n = 3, q = 3$, $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$, $x = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$, $b = 1$, $y = \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$, the calculation is as follows:

$$Ax + by = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 4 \\ 5 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} \pmod 3.$$

So,

$$f_{A,y}(b,x) = \lfloor Ax + by \rfloor = \begin{bmatrix} \lfloor 0 \rfloor \\ \lfloor 1 \rfloor \\ \lfloor 2 \rfloor \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}.$$

Then for given A, y (which are given as classical data), the quantum operation is as follows:

1. Prepare states $|+\rangle \otimes |+_q\rangle^{\otimes n}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|+_q\rangle = \frac{1}{\sqrt{q}}(\sum_{i\in\{0,1\cdots q-1\}} |i\rangle)$. This state will play the role of b and x in the expression above.
2. Evaluate $f_{A,y}$ on this state and measure the result. If the outcome is o, the remaining quantum state will be in the superposition of (b,x) that satisfies $f_{A,y}(b,x) = o$.

Question 1: How many quantum gates do we need to implement this quantum operation? Give your estimation.

Question 2: (Research Level) How much quantum resource do we need to implement a PoQ protocol?

Note: [Zhu22] contains some results on algorithms and estimates for implementing this PoQ protocol. But the focus of [Zhu22] is mainly the number of qubits needed. Here we would like to do the resource estimation in a different aspect. It will be better if you could do the estimate in more aspects. It will be great if you could discover more efficient algorithms for implementing these quantum operations!

3 Contacts

Jiayu Zhang (zhangjy@zgclab.edu.cn)

4 References

[BCMVV] Z. Brakerski, P. Christiano, U. Mahadev, U. Vazirani and T. Vidick, "A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device," 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), Paris, France, 2018, pp. 320-331, doi: 10.1109/FOCS.2018.00038.

[BKVV] Zvika Brakerski, Venkata Koppula, Umesh Vazirani, Thomas Vidick, "Simpler Proofs of Quantumness", TQC 2020.

[LG21] Zhenning Liu, Alexandru Gheorghiu, "Depth-efficient proofs of quantumness", Quantum, arXiv:2107.02163v3

[Zhu22] Dawei Zhu et al, "Interactive Protocols for Classically-Verifiable Quantum Advantage", arXiv:2112.05156v2