IQP Circuits, Different Constructions and Noise Effects

Longxiang Yuan

1 Background

Instantaneous Quantum Polynomial (IQP) verification holds a pivotal role in demonstrating quantum computational advantage due to its efficient classical verification and inherent resistance to classical simulation.

There are various different important families of IQP circuits. First, a central construction is the X-program circuits with $\theta = \pi/8$ [SB09, BCJ23]. Circuits in this family has the form

$$U_H = \prod_{p \in \mathrm{row}(H)} \exp\Big(\frac{i\pi}{8} X^p\Big) \tag{1}$$

where $H \in \mathbb{F}_2^{m \times n}$ and $X^p := X^{p_1} \otimes X^{p_2} \otimes \cdots \otimes X^{p_n}$.

Second, we examine circuits constructed with an initial layer of Hadamard gates applied to all qubits, followed by a diagonal component comprising T, CS, and CCZ gates, and concluding with a final layer of Hadamard gates on all qubits. In this work, we refer to this class of circuits as IQP-3 circuits.

In IQP verification protocols, the output state of an IQP circuit initialized in the all-zero state is measured, yielding an n-bit string x. Verification proceeds by computing a linear statistic called the signal, defined as $s \cdot x = \sum_{i=1}^{n} s_i x_i \pmod 2$, where s is a predetermined n-bit string. Since the signal is a random variable that varies with each measurement of x, the procedure is repeated multiple times to estimate its expected value.

2 Problems

2.1 Relationship between X-Program and IQP-3 Circuits

Are X-program circuits with $\theta = \pi/8$ and IQP-3 circuits equivalent? Specifically:

1. Can every X-program circuit be recompiled into an equivalent IQP-3 circuit (up to a global phase)?
2. Conversely, does every IQP-3 circuit admit an X-program representation?

2.2 Analyze the noise effect for measuring $s \cdot x$

When an IQP circuit is executed on noisy quantum hardware, gate-level errors accumulate during computation. These errors affect the measurement statistics when estimating the expectation value of the output signal $s \cdot x$. What are the noise rate constraints based on circuit parameters like gate count and depth to ensure reliable signal measurement?

3 Contacts

Longxiang Yuan (ylx23@mails.tsinghua.edu.cn)

Zhengfeng Ji (jizhengfeng@mail.tsinghua.edu.cn)

4 References

[SB09] D. Shepherd and M. J. Bremner. Temporally unstructured quantum computation, Proc. R. Soc. A 465, 1413 (2009).

[BCJ23] Michael J. Bremner, Bin Cheng, and Zhengfeng Ji. IQP Sampling and Verifiable Quantum Advantage: Stabilizer Scheme and Classical Security, August 2023. arXiv:2308.07152 [quant-ph].

[GH23] David Gross and Dominik Hangleiter. Secret extraction attacks against obfuscated IQP circuits, December 2023. arXiv:2312.10156 [quant-ph].