Evaluating the Impact of Gate Errors on a Quantum-Aided Byzantine Agreement Protocol

Author: Jerzy Ksawery Wierzbicki (J.K.Wierzbicki@student.tudelft.nl)

Supervisors: Tim Coopmans

TU Delft Delft University of Technology

1. Introduction

Byzantine agreement is one of main challenges in Computer Science. It faces the problem of reaching agreement by honest parties in the presence of faulty or malicious nodes. Guba et al. [1] proposed an idea of parameter-dependent version of quantum-aided weak broadcast byzantine agreement protocol. The protocol however succeeds only with a certain probability.

2. The Problem

- The authors quantified the failure probability of the protocol under ideal conditions.
- They conducted a noise analysis based on hardware, with a primary focus on quantum computing rather than quantum networks.
- Understanding the impact of quantum noise on failure probability is a crucial step toward real-world deployment of such protocols.

3. Research Question

What is the maximum probability of gate error for the protocol to ensure the failure probability does not exceed 5%?

4. Quantum Information Background

Qubits:
- Basic unit of quantum information.
- Capable of existing in a superposition of classical states 0 and 1.

Entanglement:
- Two or more qubits become related in such a way that the state of one qubit can not be described without the state of the other qubits.
- Enables quantum communication.

Quantum Gates:
- Manipulate qubits.
- Build circuits to prepare quantum states.

5. Protocol's Background

- Protocol solves Byzantine agreement in a 3-node network (1 sender, 2 receivers).
- Tolerates up to 1 faulty node (t < n/2), where:
  - n = total number of components in the system.
  - t = maximum number of components with Byzantine faults.
- Improves on classical bound t < n/3 from Pease et al. [2].
- Relies on repeated distribution of a specific 4-qubit entangled state.
- Number of repetitions is denoted by m.

$$|\psi\rangle = \frac{1}{2\sqrt{3}}\left(2|0011\rangle - |0101\rangle - |0110\rangle - |1010\rangle - |1001\rangle + 2|1100\rangle\right).$$

The protocol consists of 4 phases:
- **Invocation phase –** The sender sends data bit and check set to the rest of the nodes.
- **Check phase –** The nodes validate the received bit with check set and decide on their output.
- **Cross-calling phase –** One receiving node (R_0) sends his output and check set to the other receiving node (R_1).
- **Cross-check phase –** Node R_1 based on all received information solves potential conflicts and decides on his final output. However, he has no influance on other nodes.

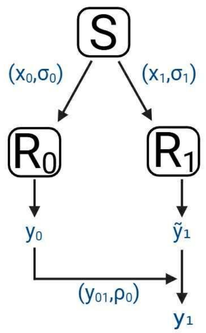


Figure 1: *Flow of information in the protocol*

6. Methodology

- Recreate experimental setup and failure probabilities from Guba et al. [1] as baseline.
- Introduce hardware noise using SquidASM [3].
- Vary noise parameters to assess impact on failure probabilities.
- Analyze what level of noise criticaly affects protocol performance.

7. Noise Model

A Pauli channel assumes that:
- With probability p_I , no error occurs.
- With probability p_X , a bit-flip occurs.
- With probability p_Y , a bit and phase flip occurs.
- With probability p_Z , a phase-flip occurs.

The sum of these probabilities must equal 1:

$$p_I + p_X + p_Y + p_Z = 1$$

More specifically the following case will be studied:

$$p_X = p_Y = p_Z$$

8. Experiment

- Circuit proposed in Guba et al. [1] was used to prepare the quantum state.
- For both experiments a Monte Carlo simulation with N=1000 random events was used.

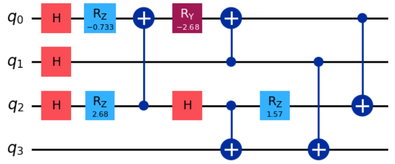
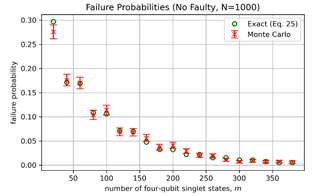
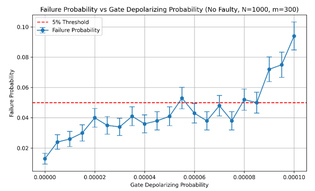


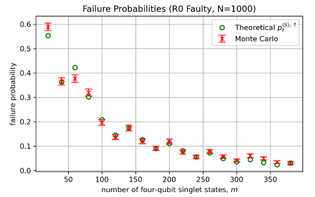
Figure 2: *Circuit from Figure 6 of [1].*

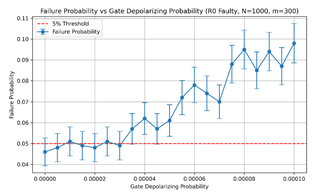
9. Results

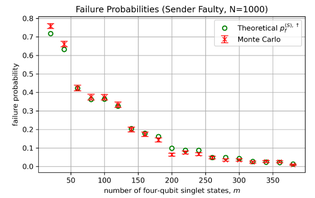
- Our results closely match the expected failure probabilities for noise-free simulations
- In all 3 scenarios, the threshold of 5% was first exceeded for gate error probability of 0.001%
- The standard mean error range suggests it might be exceeded sooner.











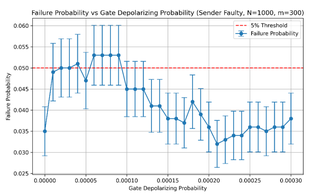


Figure 3: *Results of the noise free simulation*

Figure 4: *Results of the simulation with gate errors*

10. Conclusion and Future Work

Conclusion:
- Threshold of 0.001% of gate depolarizing probability was found.
- Comparison with existing literature [4] suggests two-qubit gates as a main bottleneck.

Future Work
- Incorporating other types of noise into the simulation.
- Varying gate error probabilities.
- Larger simulations.

References

[1] *Zoltán Guba et al., "Resource analysis for quantum-aided Byzantine agreement with the four-qubit singlet state," Quantum, vol. 8, p. 1324, Apr. 2024. ISSN: 2521-327X. DOI: 10.22331/q-2024-04-30-1324.*

[2] *M. Pease, R. Shostak, and L. Lamport, "Reaching Agreement in the Presence of Faults," Journal of the ACM (J. ACM) vol. 27, no. 2, pp. 228–234, Apr. 1980. ISSN: 0004-5411. DOI: 10.1145/322186.322188.*

[3] *SquidASM Developers, SquidASM Documentation. [Online]. Available: https://squidasm.readthedocs.io. [Accessed: June 2025].*

[4] *H. P. Bartling et al., "Universal high-fidelity quantum gates for spin qubits in diamond," Physical Review Applied, vol. 23, p. 034052, Mar. 2025. DOI: 10.1103/PhysRevApplied.23.034052.*