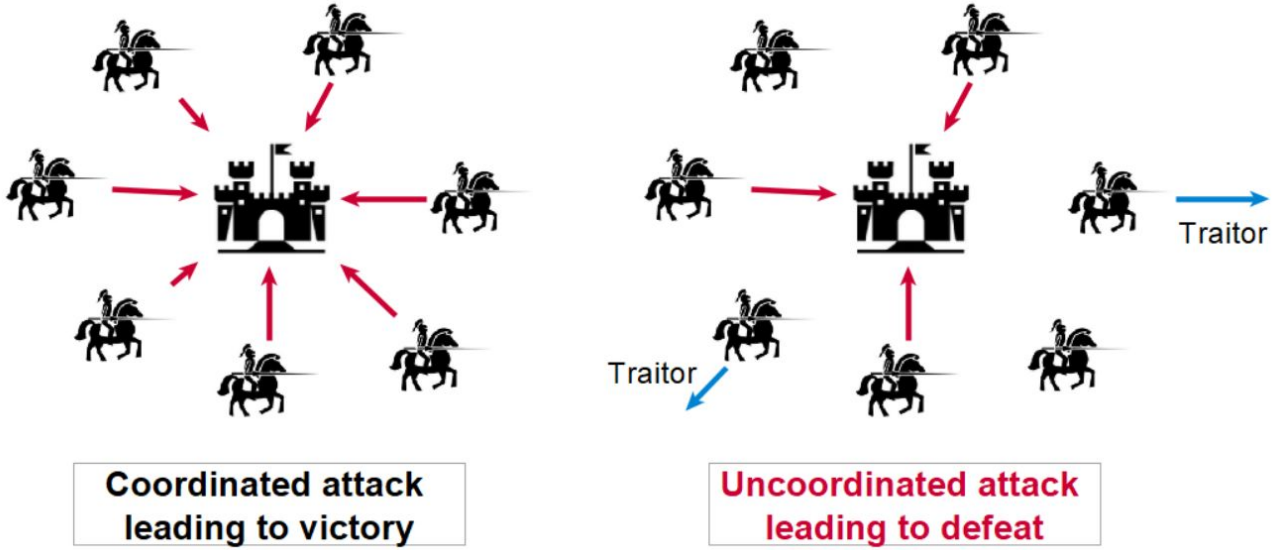
5 Qubit Qiskit Byzantine Generals Solution

COLUMBIA | COLUMBIA UNIVERSITY IRVING MEDICAL CENTER

Outline

- Problem
  - Background Analogy
  - Specific Variant
  - Success Criteria
- Five Qubit Solution Structure
  - Overview
  - Step by Step Breakdown
- Possible Scenarios
  - Case by Case
- Discussion
- Citations

Problem



You are one of several generals invading a city. As a group you are trying to decide whether to attack or retreat. You want to avoid the situation where some generals decide to attack while others retreat, in short you are trying to build consensus. You are only able to communicate via messengers in single channels. Things are complicated by the presence of possible traitor generals, who can selectively send disinformation.

Specific variant:

- Four generals, one of which is a designated commander
- Up to two possible traitors
- Additional pairwise quantum channels available
- Abort protocol default retreat strategy

Success Criteria

Broadcast:

1. All loyal generals agree on a common action.
2. If the commander is loyal, all loyal generals agree on the commanders action.

Detectable Broadcast:

1. If all players are loyal then broadcast is achieved.
2. If there are traitors than either broadcast is achieved or all loyal players abort the protocol.

5 Qubit Solution Structure

Overview:

1. Distribute copies of the 5 qubit state (Entanglement Resource)
2. Verify correlations in entangled state
3. Commander issues orders
4. Confirm orders/actions

5 Qubit Solution Structure

Distribute Entanglement Resource:

1. Exchange over pairwise quantum channels
2. Multiple copies indexed and exchanged
3. The state below, however the last term should be |11000> (it is mislabelled on GitHub)

$$(\sqrt{6}|00111\rangle + |01001\rangle + |01010\rangle + |01100\rangle + |10011\rangle + |10101\rangle + |10110\rangle + \sqrt{6}|11100\rangle) / \sqrt{18}$$

4. Commander receives first 2 qubits for every index all other lieutenants receive 1 qubit for every index

Notes:

State is symmetric under exchange of lieutenants.

Greater number of states shared needed to account for bitflip type errors.

State structure verified in next step, traitor cannot gain advantage by distributing an alternative state.

5 Qubit Solution Structure

Verify Correlations in Entangled State:

1. A random subset of indices are chosen and exchanged with all players
2. Pairwise exchange of outcomes for each chosen index
3. Correlations between outcomes are observed and compared with expected distribution
4. If Difference is significant, error/corruption occurs protocol is aborted

Notes:

Protects against state corruption and any initial traitor influence.

5 Qubit Solution Structure

Commander Issues Orders:

1. The commander sends an order either Attack or Retreat and a list of corresponding indices
2. Order and indices are communicated along classical pairwise channels

Notes:

The order and indices issued are subject to the loyalty of the commander as will be shown later.

5 Qubit Solution Structure

Confirm Orders/Actions:

1. Players engage in pairwise exchange of orders with one another
2. If conflicting orders arise, a pairwise turn-based game occurs for each disagreement (always 2 games with 3 lieutenants)

Turn-Based Game Structure:

- Randomly assign starting player
- Alternate sending single indices for which the opponent's measurement outcome is the opposite of the sender's claimed order
- Continue until indices are exhausted, any errors indicate the sender is a traitor
- Example, L1 traitor, order is attack, L1-L2 game begins

Player:	Index:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Commander	Measurement Outcome:	00	01	11	11	00	01	10	11	10	00	10	11	00	00	01	11	00	11	00	00	01	11	01	11	00	11	10	10	11	00	10
Lieutenant 1	Measurement Outcome:	1	1	0	0	1	0	1	0	1	1	0	0	1	1	0	0	1	0	1	1	0	0	1	0	1	0	1	1	0	1	0
Lieutenant 2	Measurement Outcome:	1	0	0	0	1	1	0	0	1	1	1	0	1	1	0	0	1	0	1	1	0	0	0	0	1	0	0	1	0	1	1
Lieutenant 3	Measurement Outcome:	1	0	0	0	1	0	1	0	0	1	1	0	1	1	1	0	1	0	1	1	1	0	0	0	1	0	1	0	0	1	1

- Red = indices sent by Commander corresponding to attack
- Gold & Pink = indices chosen by L1 to send to L2 for maximum success
- Gold = L1 successfully evades error, Pink = Error/L1 detected
- Average to 2/9 error rate (L1 detection rate)

Possible Scenarios

The structure of the problem permits the following possible scenarios:

1. No traitors at all
2. Commander as only traitor
3. Lieutenant as only traitor
4. Commander traitor and 1 Lieutenant traitor
5. 2 Lieutenant traitors

Player:	Index:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Commander	Measurement Outcome:	00	01	11	11	00	01	10	11	10	00	10	11	00	00	01	11	00	11	00	00	01	11	01	11	00	11	10	10	11	00	10
Lieutenant 1	Measurement Outcome:	1	1	0	0	1	0	1	0	1	1	0	0	1	1	0	0	1	0	1	1	0	0	1	0	1	0	1	1	0	1	0
Lieutenant 2	Measurement Outcome:	1	0	0	0	1	1	0	0	1	1	1	0	1	1	0	0	1	0	1	1	0	0	0	0	1	0	0	1	0	1	1
Lieutenant 3	Measurement Outcome:	1	0	0	0	1	0	1	0	0	1	1	0	1	1	1	0	1	0	1	1	1	0	0	0	1	0	1	0	0	1	1

Notes:
Example remaining game indices after verification with corresponding measurements for each player. Blue = retreat, red = attack.
Using the following mapping for commander orders: ‘00’ = Retreat, ‘11’ = Attack, ‘10’ = ‘01’ = Unused.
Scenarios are only distinguishable under the assumption that traitors take available dishonest actions.

Scenario I

No Traitors (The Trivial Case):

- Entanglement distributed
- Correlations verified
- Orders issued
- All lieutenants agree on which order they receive
    - No decider game is initiated
- Detectable broadcast achieved

Notes:

Highlights the subtlety of the success criteria, due to the indistinguishability of this scenario with certain others.

Scenario II

Commander as Only Traitor:

- Entanglement distributed
- Correlations verified
- Orders issued
  - Commander sends conflicting orders (commands + lists of indices)
  - WLOG, assume L1 receives order to attack, while L2 & L3 receive order to retreat.
- Confirm orders
  - L2 & L3 confirm successfully. L1 & L2 discover disagreement, L1 & L3 discover disagreement.
  - L1-L2 game begins, L1-L3 game begins
  - No errors between Lieutenants are detected
  - L1, L2, L3 all successfully confirm mutual loyalty, therefore commander is traitor
- Protocol is aborted, L1, L2, L3 retreat
- Detectable broadcast achieved

Scenario III

Lieutenant Only Traitor:

- Entanglement distributed
- Correlations verified
- Orders issued
  - Commander sends order + correct indices
  - WLOG, assume order is attack, L1 is traitor
- Confirm orders
  - L2 & L3 confirm successfully. L1 & L2 discover disagreement, L1 & L3 discover disagreement.
  - L1-L2 game begins, L1-L3 game begins
  - Both games L1 fails with minimum error rate of 2/9
  - L2 & L3 conclude L1 is traitor and fulfill commander's order (attack)
- Detectable broadcast achieved

Scenario IV

Commander Traitor and 1 Lieutenant Traitor:

- Entanglement distributed
- Correlations verified
- Orders issued (two variations)
  - WLOG, assume L1 is traitor
  - L1 receives attack, L2 & L3 receive retreat
    - L1 claims to receive retreat
    - No disagreements between L1, L2, L3
    - Detectable broadcast achieved
  - L2 receives attack, L1 & L3 receive retreat
    - L2-L3 game begins, L1-L2 game begins
    - L2-L3 game succeeds
    - L1-L2 game, L1 fails with minimum error rate of 2/9
    - Commander, L2 & L3 abort protocol and retreat
    - Detectable broadcast achieved

Notes:

Assumed collective information/behaviour of traitors is does not defeat protocol.

Variation 1 highlights the narrowness of detectable broadcast.

Scenario V

2 Lieutenant Traitors:

- Entanglement distributed
- Correlations verified
- Orders issued
  - WLOG, assume L1 & L2 traitor, order is attack
  - Orders exchanged, L1-L2 discover disagreement, L1-L3 discover disagreement
  - L1-L2 game begins, L1-L3 game begins
  - L2 & L3 fail with minimum error rate of 2/9
  - Commander and L1 abort protocol and retreat
  - Detectable broadcast achieved

Discussion

Why does this scheme work when classical schemes fail?

- Shared entanglement resource guarantees correlation, with only local information of each player
- Remainder of this scheme simply makes repeated reference to the shared entanglement resource

How many copies to distribute to get confident result?

- With fault-free logical qubits, traitor detection rate of 2/9.
- N >= 12 for 95% confidence

How does the introduction of error prone channels or limited correlation time qubits affect this scheme?

- Increase N to achieve equivalent confidence

Citations

Nielsen, Michael A.; Chuang, Isaac L. (2010). *Quantum Computation and Quantum Information* (2nd ed.). Cambridge: Cambridge University Press. ISBN 978-1-107-00217-3. OCLC 844974180

Vol 87, Num 21 Physical Review Letters 19 November 2001 Quantum Solution to the Byzantine Agreement Problem Matthias Fitzi,1 Nicolas Gisin,2 and Ueli Maurer

Fast Quantum Byzantine Agreement Michael Ben-Or, Avinatan Hassidim

https://medium.com/geekculture/byzantine-generals-turn-to-quantum-ab81bd938cc2

https://github.com/pdc-quantum/byzantine-generals-in-qiskit/

Sakurai, J. J.; Napolitano, Jim (2020). *Modern Quantum Mechanics* (3rd ed.). Cambridge. ISBN 978-1-108-64592-8. OCLC 1202949320.

http://theory.caltech.edu/~preskill/ph229/notes/chap7.pdf

Solving the liar detection problem using the four-qubit singlet state, Adan Cabello