Info

• Quiz 4 Friday Oct. 30
  • Topics:
    Leader Election (Bully Algorithm, Ring Algorithm)
    Consensus (Two Generals, FLP Impossibility Result)
  • No Byzantine Generals or Paxos on Quiz

• Today
  • Equivalence of Consensus and Other Problems
  • Byzantine Generals
  • Intro to Paxos?
Quiz Grades

• Grades for quizzes 1, 2, and 3 are posted in LMS
• Please check to make sure they are correct.
Project 2 Schedule

- Project 2 will be assigned on Friday
- Due Sunday Dec 6.
- Demos the week of Dec. 6
- Last day of class – Friday Dec. 11
Consensus Requirements

• **Strong Consensus:**
  • **Agreement:** No two processes decide on different values.
  • **Validity:** The value that is decided was proposed by some process.
  • **Termination:** All non-faulty processes eventually decide.

• **FLP Consensus Result:** it is impossible to achieve consensus in an asynchronous system where at most one process may fail.

• FLP Result addresses a weaker form of consensus.
  • **Termination:** Some non-faulty process eventually decides.
The Key Theorem

- **Theorem**: No consensus protocol is totally correct in spite of one fault.

- **Proof by contradiction**:
  - Assume such a protocol P exists.
  - Show that there are circumstances under which this protocol remains forever indecisive.
Consequences of FLP Result

- FLP result implies impossibility of solving other problems in asynchronous system with 1 fault.
  - Atomic broadcast
  - Leader election
  - Terminating Reliable Broadcast

- To show it is impossible to solve problem P in asynchronous system with at most 1 fault, show that an algorithm that solves P can be used to solve the consensus problem.
Impossibility of Atomic Broadcast

• **Theorem:** Given a algorithm for atomic broadcast, there is a algorithm for consensus that does not involve any additional messages.

• **Proof sketch:**
  - To propose a value $v$, a server uses the atomic broadcast protocol and broadcasts $v$; then every server waits for the delivery of the first message $v$ and decides $v$. The agreement and total order properties of atomic broadcast imply agreement of consensus.
THE BYZANTINE GENERALS PROBLEM

L. Lamport, R. Shostak, and M. Pease

*ACM Transactions on Programming Languages and Systems*, 1982
The Byzantine Generals

- N generals
- Each votes “attack” or “retreat” (v(i))
- Need all generals to reach same decision, based on votes.
- Communicate by sending synchronous messengers (who never get eaten).

- Some of the generals may be disloyal.
  - Try to prevent loyal generals from reaching agreement on correct plan.

- Need loyal generals to agree
  - Any two loyal generals use the same value for v(i), for each i
  - If the i\textsuperscript{th} general is loyal, then the value he sends is used by every loyal general as v(i)
The Byzantine Generals Problem

• To solve the agreement problem, need to solve the problem of how a single general sends its value to others.

• The Byzantine Generals Problem:
  A commanding general must send an order to N-1 lieutenants such that:
  IC 1. All loyal lieutenants obey the same order.
  IC 2. If the commanding general is loyal, then every loyal lieutenant obeys the order he sends.
IMPOSSIBILITY RESULTS

- **Theorem**: Let there be $t$ traitors among $n$ generals, there is no solution to the Byzantine generals problem for $n < 3t + 1$.

- We need $n > 3t$ to be able to solve the Byzantine Generals problem.