CS 142: Lecture 6.2
Mutual Exclusion

Richard M. Murray
1 November 2017

Goals:
• Review Lamport’s algorithm (from Mon) and prove correctness
• Describe token-based algorithms for mutual exclusion (ring + tree)
• If time: performance comparison + DGC example

Reading:
• P. Sivilotti, *Introduction to Distributed Algorithms*, Chapter 7
Lamport’s Mutual Exclusion Algorithm

Idea: treat request queue as a distributed atomic variable
- reqQ: queue of timestamps requests for CS (sorted in increasing order)
- knownT: list of last “known times” for other processes
- Actions for agent i (Ui)
  - Request entry: add to reqQ; broadcast <reqi, ti> to all other processes
  - Receive req: add to reqQ; send <acki, ti>
  - Receive ack: update knownT[j]
  - Receive release: remove Uj’s request from reqQ
- Conditions to enter CS
  - L1: req at head of reqQ
  - L2: knownT[j] > ti for all other j
- To release CS
  - Remove req from reqQ
  - Broadcast <releasei> message

UNITY program: list of actions that can be executed by each agent (in any order)
- SendReq: mode = NC → mode := TRY || (∀j :: send(i, j, <reqi, ti>))
- EnterCS: mode = TRY ^ recQ[head] = <reqi, ti> ^ (∀j :: knownT[j] > ti) → mode := CS;
- ReleaseCS: mode = CS → mode := NC || reqQ.pop(<reqi, ti> || (∀j :: send(i, j, <reli, ti>)))
- RecvReq: (∀j :: recv(i, j) = <reqj, tj> → recQ.push/sort(<reqj, tj>) || send(i, j, <acki, ti>))
- RecvAck: (∀j :: recv(i, j) = <ackj, tj> → knownT[j] := tj)
- RecvRel: (∀j :: recv(i, j) = <relj, tj> → reqQ.pop(<relj, tj>)}
Sample Execution

- **SendReq:** \(\text{mode} = \text{NC} \rightarrow \text{TRY} || (\forall j :: \text{send}(i, j, \langle \text{req}_i, t_i \rangle))\)
- **RecvReq:** \(\forall i, j :: \text{recv}(i, j) = \langle \text{req}_j, t_j \rangle \rightarrow \text{recQ.push/sort}(\langle \text{req}_j, t_j \rangle) || \text{send}(i, j, \langle \text{ack}_i, t_i \rangle))\)
- **RecvAck:** \(\forall i, j :: \text{recv}(i, j) = \langle \text{ack}_j, t_j \rangle \rightarrow \text{knownT}[j] := t_j\)
- **EnterCS:** \(\text{mode} = \text{TRY} ^ \text{recQ}[\text{head}] = \langle \text{req}_i, t_i \rangle ^ (\forall j :: \text{knownT}[j] > t_i) \rightarrow \text{mode} = \text{CS} ;\)
- **ReleaseCS:** \(\text{mode} = \text{CS} \rightarrow \text{mode} = \text{NC} || \text{reqQ.pop}(\langle \text{rel}_i, t_i \rangle || (\forall j :: \text{send}(i, j, \langle \text{rel}_i, t_i \rangle))\)
- **RecvRel:** \(\forall i, j :: \text{recv}(i, j) = \langle \text{rel}_j, t_j \rangle \rightarrow \text{reqQ.pop}(\langle \text{ack}_j, t_j \rangle)\)

```
recQ: {\langle reqj, tj \rangle, ...}  
knwT1: [log, kT2, kT3]
```

**Diagram:**

- **reqQ1**
  - \{\langle req1, 2 \rangle\}
  - \{\langle req2, 1 \rangle, \langle req1, 2 \rangle\}
  - \{\langle req1, 2 \rangle\}

- **knwT1**
  - \[1, ? , ?\]
  - \[2, 1, ?\]
  - \[4, 3, ?\]
  - \[5, 3, 3\]
  - \[7, 6, 3\]

- **reqQ2**
  - \{\langle req2, 1 \rangle\}
  - \{\langle req2, 1 \rangle, \langle req1, 2 \rangle\}

- **knwT2**
  - \[?, ?, ?\]
  - \[2, 3, ?\]
  - \[2, 4, ?\]
  - \[2, 5, 2\]
  - \[2, 6, 2\]

- **reqQ3**
  - \{\langle req2, 1 \rangle\}
  - \{\langle req2, 1 \rangle, \langle req1, 2 \rangle\}

- **knwT3**
  - \[?, ?, 1\]
  - \[?, 1, 2\]
  - \[2, 1, 3\]
  - \[2, 6, 7\]
Proof of Correctness

Safety: need to show that no two processes are in CS at the same time

• Assume the converse: \(U_i\) and \(U_j\) are both in CS
• Both \(U_i\) and \(U_j\) must have their own requests at head of queue
• Head of \(U_i\): \(<\text{req}_i, t_i>\)
• Head of \(U_j\): \(<\text{req}_j, t_j>\)
• Assume WLOG \(t_i < t_j\) (if not, switch the argument)
• Since \(U_j\) is in its CS, then we must have \(t_j < U_j.\text{knownT}[i]\)
  \[\Rightarrow <\text{req}_i, t_i> \text{ must be in } U_j.\text{reqQ} \text{ (since messages are FIFO)}\]
• \(t_i < t_j \Rightarrow \text{req}_j\) can’t be at the head of \(U_j.\text{reqQ}\)
• \(\Rightarrow\) (contradiction)

Progress: need to show that eventually every request is eventually processed

• Approach: find a metric that is guaranteed to decrease (or increase)
• One metric: number of entries in \(U_i.\text{knownT}\) that are less than its request time (\(t_i\))
  - Represents number of agents who might not have received our request
• Is this a good metric? Check conditions that are needed for induction:
  - Bounded below by zero and if at zero then we eventually enter our critical section
  - Must always decrease as other processes enter their critical section (and someone will execute their CS at some point in time)
**Proof of Correctness (Progress)**

\[
\{\text{SendReq:}\} \text{ mode} = \text{TRY} \parallel (\forall j : \text{send}(i, j, \langle \text{req}_i, t_i \rangle))
\]

\[
\{\text{RecvReq:}\} (\forall j : \text{recv}(i, j) = \langle \text{req}_j, t_j \rangle \rightarrow \text{recQ.push/sort}(<\text{req}_j, t_j>) \parallel \text{send}(i, j, \langle \text{ack}_i, t_i \rangle))
\]

\[
\{\text{RecvAck:}\} (\forall j : \text{recv}(i, j) = \langle \text{ack}_j, t_j \rangle \rightarrow \text{knownT}[j] := t_j)
\]

\[
\{\text{EnterCS:}\} \text{ mode} = \text{TRY} \land \text{recQ[head]} = \langle \text{req}_i, t_i \rangle \land (\forall j : \text{knownT}[j] > t_i) \rightarrow \text{mode} = \text{CS};
\]

\[
\{\text{ReleaseCS:}\} \text{ mode} = \text{CS} \rightarrow \text{mode} = \text{NC} \parallel \text{reqQ.pop}(\langle \text{rel}_i, t_i \rangle) \parallel (\forall j : \text{send}(i, j, \langle \text{rel}_i, t_i \rangle))
\]

\[
\{\text{RecvRel:}\} (\forall j : \text{recv}(i, j) = \langle \text{rel}_j, t_j \rangle \rightarrow \text{reqQ.pop}(\langle \text{ack}_j, t_j \rangle)
\]

**Proof steps**

- Metric: number of entries in \(U_i.\text{knownT} \) that are less than its request time \((t_i)\)
- Need to show that this is guaranteed to decrease => eventually \(U_i\) can enter CS
- Consider an agent \(U_j\) with with an entry less than \(U_i\)'s request time:

\[
U_i.\text{knownT}[j] < t_i \quad \text{(where} \langle \text{req}_i, t_i \rangle \text{is the request from} \ U_i \text{)}
\]

- Agent \(U_j\)'s logical time is guaranteed to increase when \(\langle \text{req}_i, t_i \rangle\) is received by \(U_j\)
- Agent \(U_j\) will send \(U_i\) an acknowledgement with \(t_j > t_i\) (logical clock property) => metric will decrease by 1

**Additional steps for complete proof:**

- \____________________________________________________________________
Optimizations on Lamport’s Algorithm

Optimization #1 - if request sent with later timestamp than received, no ack needed

Optimization #2 (Ricart-Agrawala): merge release messages with replies

- Receive req: add to reqQ || send <acki, ti> to Uj only in certain conditions:
  - if not requesting access to CS nor in CS
  - if requesting CS and Uj timestamp is smaller than Ui request
- When Ui exits CS, send release (clears all deferred acknowledgements)
- Idea: eventually, the pending request will be granted and we will send a <release> message, which will serve as the acknowledgement

Optimization #3 (Maekawa): request permission from a subset of agents [SS94]

- Ui only sends requests to a subset of sites Ri, chosen such that (∀i,j : Ri ∩ Rj ≠ {})
- Rough idea: every pair of agent has an agent that “mediates” between the pair
- Each agent sends only one ack at time; wait until a release is received => mediating agent can only grant permission if they haven’t granted permission to another agent
- Proof is more complicated, but many fewer messages required

Timing analysis [SS94]

- Response time = amount of time to execute critical section (if no queue)
- Sync delay: Ui exits CS to Uj enters CS
- T = transport time: E = execution time

<table>
<thead>
<tr>
<th>Non-Token</th>
<th>Resp. time (ll)</th>
<th>Sync Delay</th>
<th>Messages (ll)</th>
<th>Messages (hl)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lamport</td>
<td>2T+E</td>
<td>T</td>
<td>3(N−1)</td>
<td>3(N−1)</td>
</tr>
<tr>
<td>Ricart-Agrawala</td>
<td>2T+E</td>
<td>T</td>
<td>2(N−1)</td>
<td>2(N−1)</td>
</tr>
<tr>
<td>Maekawa</td>
<td>2T+E</td>
<td>2T</td>
<td>3√N</td>
<td>5√N</td>
</tr>
</tbody>
</table>

ll = low load condition (one req at a time)
hl = high load cond. (Ui seldom in NC)
Token-Based Approaches to Mutual Exclusion

**Simple token ring:** send token clockwise (CW) around ring
- Problem: potentially long sync delays (especially in low load)

**Token ring with requests:** add request message type
- Minimize sync delay by waiting for requests to arrive (CCW)

SendReq (Try → CS)

- if $\text{holder} \neq \text{self}$
  - $\text{hungry} := \text{true}$
  - if $\neg \text{asked}$
    - send request (CCW)
    - $\text{asked} := \text{true}$
  - else
    - $\text{using} := \text{true}$
- [use the resource]
- $\text{using} := \text{false}$
- if $\text{pending\_requests}$
  - send token on (CW)
  - $\text{pending\_requests} := \text{false}$

RecvReq

- if $\text{holder} = \text{self} \land \neg \text{using}$
  - send token on (CW)
- else
  - $\text{pending\_requests} := \text{true}$
  - if $\text{holder} \neq \text{self} \land \neg \text{asked}$
    - send request (CCW)
    - $\text{asked} := \text{true}$
  - else
  - $\text{hungry} := \text{false}$

RecvToken

- $\text{asked} := \text{false}$
- if $\text{hungry}$
  - $\text{using} := \text{true}$
  - $\text{hungry} := \text{false}$
  - else
  - send token on (CW)
  - $\text{pending\_requests} := \text{false}$

- Both approaches require existence of ring topology
Token Tree Algorithm (Raymond)

Basic idea: pass request toward token & token toward request

- Maintain a tree with root being agent with token
- Each agent gets requests and passes them toward token
- Agent with token either
  - enters CS (if earliest request)
  - passes token to node w/ earlier request
- Passing the token also updates the direction of links (so that root stays with the token)
- Invariant: graph is (rooted) tree, root at token

Question: how do we prove this works?

- Safety: no two nodes are in CS at same time (easy)
- Progress: need to show that all requesting nodes eventually get access
  - Trick (as usual): figure out a metric that captures this
Remarks on Token Tree Algorithm

Algorithm
1. If node wants CS, doesn’t hold token and requestQ is empty, send request toward the root (= token location) and adds request to its requestQ
2. If agent receives request, place on requestQ and pass message toward the token
3. When root receives request, send token toward request and update parent link
4. When agent receives the token, remove top entry in requestQ, send token to that entry, and update parent link. If requestQ is non-empty, send request to (new) parent
   - Necessary step since we need token back to send to next entry in queue
5. Agent enters critical section when it has the token and its entry is at top of requestQ
6. After site has finished execution in critical session, got to step 4

Basic idea behind the proof [SS94]
- Agents execute requests in first come first serve (FCFS) order
- Let Ui = agent requesting access, Uh = agent holding the token
  - Always exists path Ui, Ui1, Ui2, … Ui_k-1, Ui_k, Uh
  - When Uh gets request from Ui_k, there are two possibilities
    - Ui_k-1 is at the top of Ui_k’s requisite => send token there => chain gets shorter
    - Some other agent Uj is at top queue => send token there first
    - Can show eventually get token back => will eventually get to Ui_k-1
Comparisons between different algorithms

Timing analysis [SS94]

- Response time = amount of time to execute critical section (if no queue)
- Sync delay: Ui exits CS to Uj enters CS
- T = transport time; E = execution time
- ll = low load condition (one req at a time)
- hl = high load condition (Ui seldom in NC)

![Diagram of critical section execution]

<p>| TABLE 6.1 |
| A comparison of performance (ll = light load, hl = heavy load) |</p>
<table>
<thead>
<tr>
<th>NON-TOKEN</th>
<th>Resp. time (ll)</th>
<th>Sync Delay</th>
<th>Messages (ll)</th>
<th>Messages (hl)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lamport</td>
<td>2T+E</td>
<td>T</td>
<td>3(N − 1)</td>
<td>3(N − 1)</td>
</tr>
<tr>
<td>Ricart-Agrawala</td>
<td>2T+E</td>
<td>T</td>
<td>2(N − 1)</td>
<td>2(N − 1)</td>
</tr>
<tr>
<td>Maekawa</td>
<td>2T+E</td>
<td>2T</td>
<td>3√N</td>
<td>5√N</td>
</tr>
<tr>
<td>TOKEN</td>
<td>Resp. time (ll)</td>
<td>Sync Delay</td>
<td>Messages (ll)</td>
<td>Messages (hl)</td>
</tr>
<tr>
<td>Suzuki and Kasami</td>
<td>2T+E</td>
<td>T</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Singhal’s Heuristic</td>
<td>2T+E</td>
<td>T</td>
<td>N/2</td>
<td>N</td>
</tr>
<tr>
<td>Raymond</td>
<td>T(log N)+E</td>
<td>T log(N)/2</td>
<td>log(N)</td>
<td>4</td>
</tr>
</tbody>
</table>
Summary: Mutual Exclusion

Key ideas:
- Distributed protocol for allowing access to a shared resource ("critical section")
- Two approaches: distributed atomic variables (Lamport + variants) or token-based
- User process specifications:
  - System specifications:
    - Safety: no two users (Ui) are in critical section (CS) at the same time
    - Progress: all agents will get a chance (as long as they keep requesting)

Friday: problem solving session (board talk)

Next week: synchronization and dining philosophers