

Correct by Design with TLA+
FIRST DRAFT

Richard Tang

January 30, 2025

Contents

I	Introduction	4
1	Motivation	5
1.1	Catching Problems Early	5
1.2	The Generalized Problem	6
1.3	What is TLA+?	7
1.4	About This Book	7
1.5	How to Use This Book	8
2	TLA+ Primer	9
2.1	Purpose	9
2.2	Design	10
2.3	Spec	10
2.4	Safety	11
2.5	Liveness	12
2.6	Model Checker	12
II	Examples with TLA+	15
3	Simple Gossip Protocol	16
3.1	Design	16
3.2	Spec	17
3.3	Safety	18
3.4	Liveness	18
4	Simple Scheduler	20
4.1	Design	20
4.2	Spec	21
4.3	Safety	22
4.4	Liveness	22
5	Selective Retransmit	24
5.1	Design	26
5.2	Spec	27

5.3	Model Reduction	31
5.3.1	Removing Stale Acknowledgement	31
5.4	Safety	31
5.5	Liveness	31
6	Raft Consensus Protocol	32
6.1	Design	32
6.2	Spec	33
6.3	Model Reduction	37
6.3.1	Modeling Messages as a Set	37
6.3.2	Limit Term Divergence	37
6.3.3	Normalize Cluster Term	38
6.3.4	Sending Request as a Batch	39
6.3.5	Prune Messages with Stale Terms	39
6.3.6	Enable Symmetry	40
6.4	Safety	40
6.5	Liveness	40
III	Examples with PlusCal	42
7	SPSC Lockless Queue	44
7.1	Requirement	44
7.2	Spec	45
7.3	Safety	46
7.4	Liveness	46
7.5	Configuration	47
8	SPMC Lockless Queue	48
8.1	Design	48
8.2	Spec	49
8.3	Safety	51
8.4	Liveness	52
IV	Reference	53
9	Data Structure	54
9.1	Set	54
9.2	Tuple	54
10	Fairness and Liveness	56
10.1	Liveness	56
10.2	Weak Fairness	57
10.3	Strong Fairness	58

11 General Tips	60
11.1 Model Checker Debug	60
11.1.1 Dead Lock	60
11.1.2 Live Lock	60
11.2 Model Refinement	61
12 Abstraction Guideline	62
13 Reference	63

Part I

Introduction

Chapter 1

Motivation

1.1 Catching Problems Early

Years ago, I worked on a proprietary low power processor in an embedded system. The processor ran microcode featuring a custom instruction set. To enter a low power state, a set of (possibly hundreds) instructions were executed. These instructions progressively puts the system in lower power state. For example: turn off IP A, then turn off IP B, then turn off the power island to the IPs. To save cost and power, the low power processor had very limited debuggability support.

An experienced reader may start to notice some redflags.

If the microcode attempts to access the memory interface when the power island has been shut off, processor would hang. Since the power island has been shut off, the physical hardware debug port is also unavailable, leaving the developer with *no way* of live debugging related problem. At this point the developer needs to siphon through (possibly hundreds) of instructions to catch invariant violation *manually*.

As one can imagine, maintaining the microcode was very expensive. Fortunately, the proprietary low power processor only had a handful of instructions, I created an emulator for this proprietary processor to verify the microcode prior to deploying it on target. The emulator models the processor states as a state graph, with executed instruction transitions the state machine to the next state. At every state all the invariants are evaluated to ensure none have been violated. Some of the invariants included:

- Accessing memory interface after power off leads to a hang
- Accessing certain register in certain chip revision leads to a hang
- Verify IPs are shut off in the allowed order

The verification algorithm was implemented using a *depth-first search* algorithm, providing 100% microcode coverage before deploy on target.

To generalize, we can model arbitrary system as a set of states with a collection of invariant that must be upheld at all times. The complexity of the such arbitrarily system generally grows quadratically as the number of states grow linearly (eg. in a N state system, adding state $N+1$ may introduce N transitions into the new state). There are many engineering problems that exhibit a large number of states, such as lockless or waitfree data structure, distributed algorithms, OS scheduler, and more. As the number of states grow, the problem becomes more mentally taxing for designer to reason about.

How does a designer reason about the correctness of a proposed solution?

1.2 The Generalized Problem

Fast forward to now: I stumbled across TLA+, a formalized solution of what I was looking for.

The Turing Award winner Leslie Lamport invented the TLA+ 1999, but TLA+ didn't appear to have caught on until the 2010's. My opinion is TLA+ was invented ahead of its time, and the problem complexity finally caught up in the past decade or so, to allow TLA+ to demonstrate its strength.

We are at a point in the technology curve where vertical scaling is no longer practical, with CPU speed plateau'd in the past decade or so. The industry is exploring horizontal scaling solution, such as hardware vendor focusing adding more CPU cores, or software vendors buying many low end hardware instead of a few high end hardware. This shifts the technology complexity from vertical to horizontal, demanding solution to maximize concurrent resource utilization. There is one slight problem though:

Humans are not good at reasoning about things happening concurrently.

Our cognitive system is optimized for sequential reasoning. Enumerating all scenarios in one's mind to ensure an arbitrary design accommodates all the corner cases is challenging.

Consider a low power processor execution hundreds of instruction, how does the designer ensure the invariants are upheld after every instruction?

Consider a distributed system. The system is a cluster of independently operating entities and need to somehow collectively offer the correct system behaviour, while any one of the machines may receive instructions out of order,

crash, recover, etc.

Consider a single producer multiple consumer lockless queue. The consumers may reserve an index in the queue in certain order, but may release them in different order. What if one reader is really slow, and another reader is super fast and possibly lapse the slow reader?

Consider an OS scheduler with locks. Assume all the processes have the same priority. Can a process starve the other processes by repeatedly acquire and release the lock? How do we ensure scheduling is fair?

The *anti-pattern* is to keep bandaiding the design until user stops filing bug reports. This is never ideal. Per Murphy's law, anything that can go wrong *will go wrong*, and a hard to reproduce bug will come in at the most inconvenient time. How do we make sure the solution is *correct by design*? To solve this problem, we must rely on tools to do the reasoning *for us*.

1.3 What is TLA+?

TLA+ is a *system specification language*, with the intent to describe the system with implementation details removed. TLA+ allows designer to describe the system as a sequence of states. The designer can express transition condition from one state to another, describe invariants that must hold true in every state and liveness properties that the overall system should converge to. The key innovation of TLA+ is once the system is modeled as a finite state machine, the states can be *exhaustively* explored (via breath-first-search) to ensure certain properties are held through out the entire state space (either per state or a sequence of states).

1.4 About This Book

To my surprise, there's not as much material on TLA+ as I assumed for such a critical tool in the designer toolbox. This book was initially a set of notes I took as I was learning TLA+. I decided to formalize the notes into this short book, which I hope the readers find this helpful in their journey TLA+ journey.

The intent for the book is to teach reader how to write TLA+ spec for their design to provide confidence in *design correctness*. This book is targeted to software designer, hardware designer, system architect, and in general anyone who is interested in designing correct system.

To get the most out of the book, reader should have general computing science knowledge. Reader doesn't need to be expert at a particular language

to understand this book; TLA+ is effectively its own language. This book is example driven and will go through designs such as lockless queue, simple task scheduler, consensus algorithm, etc. Reader will likely enjoy a deeper insight if she has some familiarity with these topics.

1.5 How to Use This Book

This book was designed to be used as a reference, providing examples and references using TLA+.

Examples are split into two categories: A set of examples written using TLA+, and another set of examples written using PlusCal (the C-like syntax that transpiles down to TLA+). I believe they are useful for different use cases. The differences will be highlighted in their respective sections. All examples will follow a similar layout, covering the requirements, design, spec, and safety properties.

All examples in this book will be presented using TLA+ *mathematical notation*. Converting between Mathematical and ASCII notation is assumed straightforward due to the one-to-one mapping. Readers are encouraged to consult Table 8 in [1] as needed.

The last part of the book provides that language reference and some focused topic. Reader can use the last part of the book as a general reference.

Chapter 2

TLA+ Primer

2.1 Purpose

The key insight to TLA+ is modeling a system as a state machine. A simple digital clock can be represented by two variables, hour and minute and the number of possible states in a digital clock is $24 * 60 = 1440$. For example, a clock in state 10:00 will transition to state 10:01. Assume an arbitrarily system described by N variables, each variable having K possible values such arbitrary system can have up to N^K state.

For every specification, designer can specify *safety* property (or invariants) that must be true in *every* states. For example, in any state of the digital clock hour *must* be between 0 to 23, or formally described as $hour \in 0..23$. Similarly, minute must have value between 0 to 59, or $minute \in 0..59$. Examples invariants of a system include: Only one thread has exclusive access to a critical region, all variables in the system are within allowable value, resource allocation manager never allocates more than available resources.

Designer can also specify *liveness* property. These are properties to be satisfied by a *sequence of state*. One liveness property for the digital clock could be when the clock is 10:00, it will eventually become 11:00 (10:00 *leads* to 11:00). Example liveness property include: a distributed system eventually converges, the scheduler eventually schedules every tasks in the task queue, the resource allocation manager fairly allocates resources.

A TLA+ Spec can be checked by TLC, the model checker. TLC uses *breadth-first search* algorithm to explore *all* states in the state machine and ensure safety and liveness properties are upheld.

A TLA+ Spec describes the system using *temporal logic*. The syntax may appear unfamiliar if one hasn't seen it before, but like any other programming

language an initiated reader should become familiarized quickly. In this book I will use

2.2 Design

In this example, we will specify a *digital clock*. The digital clock has a few simple requirements:

- Two variables to represent state: hour and minute
- The clock increment one minute at a time
- Hour is between 0 to 23, inclusive
- Minute is between 0 to 59, inclusive
- Clock wraps around at midnight (ie. 23:59 transitions to 00:00)

2.3 Spec

The *Init* state of such system can be described as:

$$\begin{aligned} Init &\triangleq \\ &\wedge hour = 0 \\ &\wedge minute = 0 \end{aligned}$$

\triangleq is the *defines equal* symbol and \wedge is the *logical and* symbol. The above TLA+ syntax can be read as *Init* state is defined as both hour and minute are both 0.

The spec also always include a *Next* definition, an *action formula* describing how the system transition from one state to another. Action formula contains *primed* variables what happens to the variable in its next state. The *Next* action for the digital clock can be defined as:

$$\begin{aligned} NextHour &\triangleq \\ &\wedge minute = 59 \\ &\wedge hour' = (hour + 1) \% 24 \\ &\wedge minute' = 0 \\ NextMinute &\triangleq \\ &\wedge minute \neq 59 \\ &\wedge hour' = hour \\ &\wedge minute' = minute + 1 \\ Next &\triangleq \\ &\vee NextMinute \end{aligned}$$

$\vee \text{NextHour}$

Here's a breakdown of what the spec does:

- *Next* can take either *NextHour* or *NextMinute*
- *Next* takes *NextMinute* when *minute* is not 59. *NextMinute* doesn't update *Hour* and increments *Minute*.
- *Next* takes *NextHour* when *minute* is 59. *NextHour* increments *hour* modulus 24 and sets *minute* to 0.

Note that the formulas are *state descriptions*, not *assignment*. *minute = 59* describes the state transition takes when *minute equals 59*. Since this is an equality description, *minute = 59* and *59 = minute* are equivalent in TLA+.

Finally, the Spec itself is formally defined as:

$$\begin{aligned} \text{vars} &\triangleq \langle \text{hour}, \text{minute} \rangle \\ \text{Spec} &\triangleq \\ &\quad \wedge \text{Init} \\ &\quad \wedge \Box[\text{Next}]_{\text{vars}} \end{aligned}$$

Note this forms the basis for **all** TLA+ Spec. Every example in this book will include a Spec definition similar to this.

$\Box[\text{Next}]_{\text{vars}}$ deserves some special attention:

- *vars* is defined earlier to be *all* variables in the spec, in this case *hour* and *minute*. Combination of these variables at different values constitute the states of the system (eg. 23:59 and 00:00 are different states in the system).
- $\Box[\text{Next}]_{\text{vars}}$ is a box-action formula, where *Next* is an action and *vars* is a state function.
- \Box operator asserts the formula is always true for every step in the behaviour.
- And steps in the behaviour is defined as $[\text{Next}]_{\text{vars}}$, where *Next* describe the action and *vars* capturing all variables representing the state.

This can be roughly translate to: the system is valid for for every step *Next* can take, forming the basis of the Spec.

2.4 Safety

Safety property describes invariant that must hold true in *every* state of system. A common invariant is *type safety* checks. In a digital clock, hour can only be

in value between 0 to 23, and minute can only be value of 0 to 59:

$$\begin{aligned} Type_OK &\triangleq \\ &\wedge hour \in 0 \dots 23 \\ &\wedge minute \in 0 \dots 59 \end{aligned}$$

When hour or minute falls outside of the specified range, the model checker reports failure.

2.5 Liveness

Liveness property verifies certain behavioural across a sequence of state. One liveness property is to confirm the clock wraps around at midnight, a property that can only be verified after checking at least two states:

$$\begin{aligned} Liveness &\triangleq \\ &\wedge hour = 23 \wedge minute = 59 \leadsto hour = 0 \wedge minute = 0 \end{aligned}$$

\leadsto is the *leads to* operator, suggesting something is eventually true. TLA+ provides a set of operators to describe liveness property.

To verify liveness, we need to modify the spec slightly to enable *fairness* to prevent *stuttering*. In plain terms, fairness ensure a state always transition to *some other state*. Without fairness the spec is allowed to *stutter*, or *not transition* to any state. This by definition fails liveness property check as the model checker is unable to verify the behaviour across a sequence of states. To get a more comprehensive description of fairness, refer to the last part of the book.

$$\begin{aligned} Spec &\triangleq \\ &\wedge Init \\ &\wedge \Box [Next]_{vars} \\ &\wedge WF_{vars}(Next) \end{aligned}$$

$WF_{vars}(Next)$ is the fairness qualifier.

2.6 Model Checker

The TLA+ spec can be verified using TLC model checker. The model checker runs the spec and verifies all configured safety and liveness properties are satisfied. In short, the model checker a library written in Java, and can be invoked using command line java. For instruction on installing the model checker and related tools, please see [7].

After installing the model checker, we need two things to verify the spec:

- clock.tla: spec
- clock.cfg: config file

For reference, clock.tla is listed below:

MODULE <i>clock</i>
<pre> EXTENDS <i>Naturals</i> VARIABLES <i>hour</i>, <i>minute</i> vars \triangleq \langle<i>hour</i>, <i>minute</i>\rangle Type_OK \triangleq \wedge <i>hour</i> \in 0 .. 23 \wedge <i>minute</i> \in 0 .. 59 Liveness \triangleq \wedge <i>hour</i> = 23 \wedge <i>minute</i> = 59 \leadsto <i>hour</i> = 0 \wedge <i>minute</i> = 0 Init \triangleq \wedge <i>hour</i> = 0 \wedge <i>minute</i> = 0 NextMinute \triangleq \wedge <i>minute</i> = 59 \wedge <i>hour'</i> = (<i>hour</i> + 1)%24 \wedge <i>minute'</i> = 0 NextHour \triangleq \wedge <i>minute</i> \neq 59 \wedge <i>hour'</i> = <i>hour</i> \wedge <i>minute'</i> = <i>minute</i> + 1 Next \triangleq \vee NextMinute \vee NextHour Spec \triangleq \wedge Init \wedge \Box[Next]_{vars} \wedge WF_{vars}(Next) </pre>

The corresponding clock.cfg is listed below:

<pre> SPECIFICATION Spec INVARIANTS Type_OK PROPERTIES Liveness </pre>
--

After putting both clock.cfg and clock.tla in the same directory, one can now run the model checker. In this book I'll assume a commandline interface for the model checker:

```
java -cp /usr/local/lib/tla2tools.jar tlc2.TLC clock
...
Model checking completed. No error has been found.
...
The depth of the complete state graph search is 1440.
```

The 1440 states in the graph represents total number of minutes in a day.

Part II

Examples with TLA+

Chapter 3

Simple Gossip Protocol

In a distributed system, a cluster of nodes collectively provide a service. A distributed system may have 10s to 100s of nodes working together to offer the service in a geo diverse environment to maximize uptime. The nodes often have requirements to know about each other. In the context of distributed database, a node may need to know the key range another of its peers. The cluster needs a way to communicate this information. One such mechanism is the gossip protocol.

Gossip protocol allows nodes to fetch the latest cluster information in a distributed fashion. Prior to gossip protocol, nodes in a cluster learn about its neighbours by contacting a centralized server. This introduces a single failure point in the system. Gossip protocol relies on nodes to initiate the data exchange, and the nodes in the cluster periodically selects a set of neighbors to gossip with.

Assume a N node cluster, at some periodic interval a node selects k neighbours to gossip with. The total amount of gossip propagation time is described logarithmically below:

$$propagation_time = \log_k N * gossip_interval \quad (3.1)$$

With the total number of messages exchanged:

$$messages_exchanged = \log_k N * k \quad (3.2)$$

3.1 Design

In this chapter we will implement a simplified gossip model where:

- Each node has a version.
- Each node caches the version of all other nodes.

- A pair of nodes are randomly selected to gossip
- A node can restart. Restarting a node clears the node's version cache of the other nodes.
- A node can bump its own version.

If the gossip protocol works correctly, every node should eventually have the latest version of all the nodes.

3.2 Spec

In gossip protocol, every node needs to remember all its peers current version:

$$\begin{aligned}
 Init &\triangleq \\
 &\quad \wedge \text{version} = [i \in \text{Servers} \mapsto [j \in \text{Servers} \mapsto 0]] \\
 Next &\triangleq \\
 &\quad \vee \exists i \in \text{Servers} : \\
 &\quad \quad \wedge \text{Bump}(i) \\
 &\quad \vee \exists i, j \in \text{Servers} : \\
 &\quad \quad \wedge \text{Gossip}(i, j) \\
 &\quad \vee \exists i \in \text{Servers} : \\
 &\quad \quad \wedge \text{Restart}(i)
 \end{aligned}$$

The *Init* formula simply declares version to be a two dimension array with all elements initialized to 0. *Next* allows either bumping version of a server, pick a pair of nodes to gossip, or restart a server.

The following provides definition to these steps:

$$\begin{aligned}
 \text{Gossip}(i, j) &\triangleq \\
 \text{LET} & \\
 \quad \text{Max}(a, b) &\triangleq \text{IF } a > b \text{ THEN } a \text{ ELSE } b \\
 \quad \text{updated} &\triangleq [k \in \text{Servers} \mapsto \text{Max}(\text{version}[i][k], \text{version}[j][k])] \\
 \quad \text{version_a} &\triangleq [\text{version} \text{ EXCEPT } ![i] = \text{updated}] \\
 \quad \text{version_ab} &\triangleq [\text{version_a} \text{ EXCEPT } ![j] = \text{updated}] \\
 \text{IN} & \\
 &\quad \wedge \text{version}' = \text{version_ab}
 \end{aligned}$$

When two server gossip, they gossip about all the nodes (including themselves) and update both of their version cache with the more up-to-date entry between the two. The *LET..IN* syntax enables local macro definition. In this example, we use temporary variables defined inside *LET*, and update the primed variable inside the *IN* clause.

$$\text{Bump}(i) \triangleq$$

$$\begin{aligned}
& \wedge \text{version}[i][i] \neq \text{MaxVersion} \\
& \wedge \text{version}' = [\text{version} \text{ EXCEPT } ![i] = [k \in \text{Servers} \mapsto \\
& \quad \text{IF } i \neq k \text{ THEN } \text{version}[i][k] \text{ ELSE } \text{version}[i][k] + 1]]
\end{aligned}$$

The action only permits version bump if the Server hasn't made it to *MaxVersion*. When the Server bumps the version, it only bumps its own version and keeps all other version in its version cache as is.

$$\begin{aligned}
\text{Restart}(i) & \triangleq \\
& \wedge \text{version}' = [\text{version} \text{ EXCEPT } ![i] = [k \in \text{Servers} \mapsto \\
& \quad \text{IF } i \neq k \text{ THEN } 0 \text{ ELSE } \text{version}[i][i]]
\end{aligned}$$

Upon *Restart*, a server reloads from its local storage (so its own version persist), but the server needs to re-learn the cluster status (all other entries in its version cache is wiped).

The *Spec* defines three actions: *Bump*, *Restart*, *Gossip*. Without any fairness description, *Any* permutation of these actions are allowed by the Spec, and *will* be checked by the model checker:

- Restart, Restart, Restart,...
- Bump, Bump, Bump, Bump ...
- Restart, Gossip, Restart, Gossip, ...

We will discuss how to specify fairness in the Liveness section of this chapter.

3.3 Safety

3.4 Liveness

The expected behaviour of a system using gossip protocol is to ensure the cluster converges towards higher version number for all servers even in the presence of failure (represented by *Restart*). This means we need to guarantee *Bump* is always being called. Without this guarantee, the Spec can trap in a *Restart* and *Gossip* loop. To ensure *Bump* is always called, we need to add fairness description:

$$\begin{aligned}
\text{Spec} & \triangleq \\
& \wedge \text{Init} \\
& \wedge \Box[\text{Next}]_{\text{vars}} \\
& \wedge \text{WF}_{\text{vars}}(\text{Next}) \\
& \wedge \forall i \in \text{Servers} : \\
& \quad \text{WF}_{\text{vars}}(\text{Bump}(i))
\end{aligned}$$

The the model checker explores all possible transitions permitted by the Spec. This includes calling Restart repeatedly, calling Gossip repeatedly, calling any subset of the actions repeatedly. The fairness description gaurantees that if the enabling condition of an action is true, the action will take. If the system is trapped in a Restart and Gossip loop when Bump can be called, specifying fairness for Bump ensures Bump is called, breaking the loop.

With the Spec ensuring the system always migrate towards higher version number, we can now define the Liveness property:

$$\begin{aligned}
 \text{Liveness} &\triangleq \\
 &\exists i, j \in \text{Servers} : \\
 &\quad \wedge i \neq j \\
 &\quad \wedge \Box \Diamond (\text{version}[i][i] = \text{MaxVersion} \\
 &\quad \wedge \text{version}[i][i] = \text{MaxVersion} \\
 &\quad \wedge \text{version}[i][j] = \text{MaxVersion})
 \end{aligned}$$

The $\Box \Diamond$ represents *always eventually*. The liveness condition specifies that there exists a pair of Servers such that both of them *always eventually* makes it to MaxVersion and have Gossip with each other.

Since the Spec permits *Restart* to be called anytime, a liveness property where *all* Servers are up-to-date cannot be true. The model checker can always *Restart* one of the Servers before this property is met.

Likewise, replacing *always eventually* with *eventually always* ($\Diamond \Box$) also fails. $\Diamond \Box$ checks that once the system *eventually* enters a specified state, it *always* remains in that state. This cannot be true as the liveness condition is transient, since the model checker can always disturb any condition with a *Restart*.

For a more comprehensive discussion of fairness, refer to the last section of the book.

Chapter 4

Simple Scheduler

Task schedulers are fairly ubiquitous. Every device implements *something* to manage tasks. Modern desktop or mobile device processes non-trivial OS abstractions and with every process maintains its own virtual memory space for security reasons. Context switching process requires the OS to "clean" the hardware before running the new process.

For emedded devices such as hard drives or network cards, the security consideration may be relaxed as users are typically not allowed to run arbitrary code on the device. Sometimes these products don't have full blown operating system to save on memory and storage footprint, but still need some sort of scheduler to manage the tasks.

To solve the c10k [9] problem, some languages (eg. Rust) supports asynchronous programming, allowing the user to enable task switching *within* the same process to scale up system throughput. However, language like Rust only provides the *language support* for asynchronous programming, and user must supply their own async runtime. The async runtime must also must include a scheduler to manage the tasks.

Hopefully this provides

4.1 Design

In this section we will define a spec for a simple task scheduler. The task sechdeuler has the following requirements:

- Supporting N execution context (ie. CPUs)
- Supporting T number of tasks
- Tasks have identical priority and are scheduled coopertively

- System has a single global lock
- Any task can attempt to acquire the lock, Any task attempting to acquire the lock are gauranteed to be scheduled.
- If multiple tasks attempt to grab the lock, the tasks will be scheduled in lock request order.

4.2 Spec

We will model scheduler using the following variables:

$$\begin{aligned}
 Init &\triangleq \\
 &\wedge cpus = [i \in 0 \dots N - 1 \mapsto ""] \\
 &\wedge ready_q = S2T(Tasks) \\
 &\wedge blocked_q = \langle \rangle \\
 &\wedge lock_owner = ""
 \end{aligned}$$

A few things to note:

- The system has N executing context, represented as number of CPUs. When a task is running, $cpus[k]$ is set to *taskName*. When CPU is idle, $cpus[k]$ is set to an empty string.
- *ready_q* and *blocked_q* are initialized as *ordered tuple*, due to the cooperative scheduling requirement.
- *S2T* is a macro that converts a set into a ordered tuple. This is to accommodate the fact it appears I cannot define tuple in .cfg file.
- Finally, the single system lock is represented as *lock_owner*.

A task can be in three possible state: Ready, Blocked and Running. The *Next* box-action fomula will define a Ready and Running action, and the implementation will include related lock contention handling.

MODULE *scheduler*

$$\begin{aligned}
 MoveToReady(k) &\triangleq \\
 &\wedge cpus[k] \neq "" \\
 &\wedge lock_owner \neq cpus[k] \\
 &\wedge ready_q' = Append(ready_q, cpus[k]) \\
 &\wedge cpus' = [cpus \text{ EXCEPT } ![k] = ""] \\
 &\wedge UNCHANGED \langle lock_owner, blocked_q \rangle \\
 Lock(k) &\triangleq \\
 &lock \text{ is empty} \\
 \vee &\wedge cpus[k] \neq "" \\
 &\wedge lock_owner = "" \\
 &\wedge lock_owner' = cpus[k]
 \end{aligned}$$

$$\begin{aligned}
& \wedge \text{UNCHANGED } \langle \text{ready_q}, \text{cpus}, \text{blocked_q} \rangle \\
& \text{someone else has the lock} \\
& \vee \wedge \text{cpus}[k] \neq "" \\
& \wedge \text{lock_owner} \neq "" \\
& \wedge \text{lock_owner} \neq \text{cpus}[k] \text{ cannot double lock} \\
& \wedge \text{blocked_q}' = \text{Append}(\text{blocked_q}, \text{cpus}[k]) \\
& \wedge \text{cpus}' = [\text{cpus} \text{ EXCEPT } ![k] = ""] \\
& \wedge \text{UNCHANGED } \langle \text{ready_q}, \text{lock_owner} \rangle \\
\text{Unlock}(k) & \triangleq \\
& \wedge \text{cpus}[k] \neq "" \\
& \wedge \text{lock_owner} = \text{cpus}[k] \\
& \wedge \text{lock_owner}' = "" \\
& \wedge \text{cpus}' = [\text{cpus} \text{ EXCEPT } ![k] = ""] \\
& \wedge \text{ready_q}' = \text{ready_q} \circ \text{blocked_q} \circ \langle \text{cpus}[k] \rangle \\
& \wedge \text{blocked_q}' = \langle \rangle \\
\text{Running} & \triangleq \\
& \exists k \in \text{DOMAIN } \text{cpus} : \\
& \wedge \text{cpus}[k] \neq "" \\
& \wedge \vee \text{MoveToReady}(k) \\
& \vee \text{Lock}(k) \\
& \vee \text{Unlock}(k)
\end{aligned}$$

4.3 Safety

4.4 Liveness

I believe this is the most important part of cooperative scheduler design. While the scheduler can't *force* a task to relinquish a lock (the scheduler doesn't dictate when the task is *done*), the scheduler can ensure scheduling fairness by scheduling the next lock requester instead of the task that just relinquished the lock.

MODULE *scheduler*

$$\begin{aligned}
\text{Liveness} & \triangleq \\
& \forall t \in \text{Tasks} : \\
& \text{LET} \\
& \quad b \triangleq \{x \in \text{DOMAIN } \text{blocked_q} : \text{blocked_q}[x] = t\} \\
& \text{IN} \\
& \quad \wedge b \neq \{\} \leadsto b = \{\}
\end{aligned}$$

The formula defines set b to be either an empty set or a set of one task. Assume a set of {"p0", "p1", "p2"}. Possible value of b include: {}, {"p0"},

$\{p1\}$ and $\{p2\}$. The formula then states an non empty set of b leads to an *empty set* of b . In other words:

If a task ever becomes blocked, it will eventually become unblocked.

However, when we actually run the model checker, we will find the liveness property is *violated*. The failure scenario is basically one task holding onto the lock in one CPU, while the scheduler repeatedly schedule/deschedule a separate task in another CPU. While this is perfectly allowed, the model checker detects a possible path for the the system to trap in a local state and fail the liveness property.

Perhaps not surprisingly, if you construct similar liveness property to verify a task is *eventually* always scheduled, it will also fail. The model checker will provide a counter case where a task is never scheduled because another task is repeatedly acquire/release the global lock.

We need *Strong Fairness* to solve this problem:

$$\begin{array}{l}
 \text{MODULE scheduler} \\
 L \triangleq \\
 \quad \forall t \in \text{Tasks} : \\
 \quad \quad \forall n \in 0 \dots (N - 1) : \\
 \quad \quad \quad \text{WF}_{vars}(\text{HoldingLock}(t) \wedge \text{Unlock}(n)) \\
 \text{Spec} \triangleq \\
 \quad \wedge \text{Init} \\
 \quad \wedge \Box[\text{Next}]_{vars} \\
 \quad \wedge \text{WF}_{vars}(\text{Next}) \\
 \quad \wedge L
 \end{array}$$

Fairness ensures that we are never stuck in a repeated state.

Chapter 5

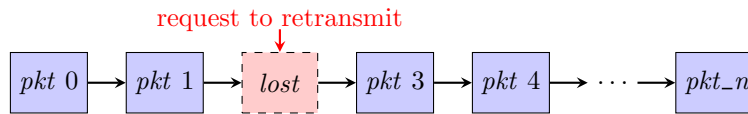
Selective Retransmit

Assume client device that playback a video stream. Structurally, a video is composed of frames, frames are then segmented into packets to stream across a network. The client device recombines the packets into a frame, then sequence the frame to playback the video.

However, network is not-deterministic. Depending on the route the packets take to get to the client, they may arrive out-of-order. The client may need to maintain a receive buffer for the packets, re-order the packets back into sequence before pushing the packets down to decoding engine.

The network may also drop packets if any of the switches along the way get busy. In the case of a packet drop, the client has a few options. The client can either discard the frame and let the decoding engine downstream to deal with it (which may result in visible artifacts during playback). The client can request the whole frame to be re-sent, which results in additional bandwidth consumption. The client can selectively request the missing packet to be retransmitted, which will minimize additional bandwidth consumption, but increases implementation complexity.

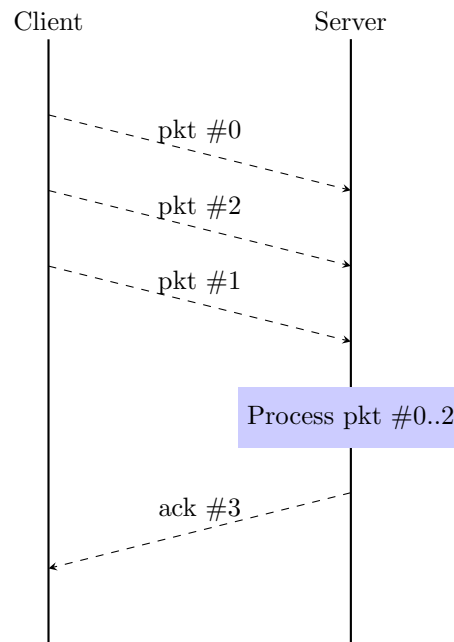
In this chapter, we will implement a simple selective retransmit algorithm.



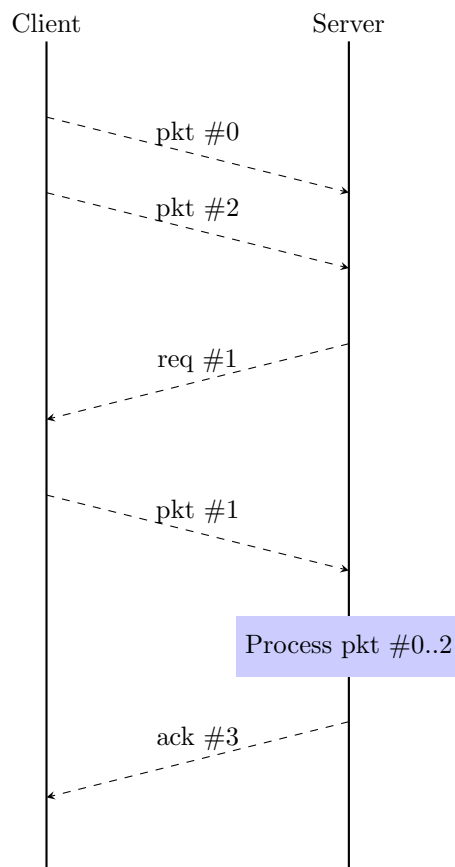
Since packets may arrive out-of-order, the server stamps the packets with sequence number to allow the client to order the packets as they arrive. Once the client has a set of ordered packets, it moves the packets from the receive buffer into the decoding engine to be displayed.

The video packets are often sent via unreliable channel to minimize network overhead and latency. The client sends acknowledgement back to the server to acknowledge the received packet. This indicates to the server it can send more video data to the client. Acknowledgements are not latency sensitive in nature, and take up a very small proportion of bandwidth, so they are transported through reliable channel.

The following illustrates packet reorder handling:



The following illustrates packet loss handling:



There are other design considerations. The server is allowed to send up to W packets before getting an acknowledgement, this reduces latency perceived by the user. The client also doesn't need to acknowledge all the packets, since the server assumes once an acknowledgement of packet N is received, then all packets prior to N have also been received.

5.1 Design

With the above description, we are now ready to provide a more formal description for our design:

- Client is the receiver that displays the video stream.
- Server is the sender that sends the video stream.
- Server always sends the packets in-order.
- Client may receive the packets out-of-order.

- Client may never receive some packet due to loss.
- Server can send up to W packets before an acknowledgement is received
- Packet sequence number is represented by a fixed number of bytes in the network header, the sequence number will eventually wrap around once it hits the maximum representable value. The maximum sequence number is represented as $N-1$.
- Client puts a received packet in its receive buffer. Packets in the receive buffer may be out-of-order due to network conditions.
- Client will remove the packets from the receive buffer once the sequence number of the received packets are contiguous. The client will also send an acknowledgement back to the Server with the most recently acknowledged sequence number.
- Data packets are transported using unreliable channel due to bandwidth and latency requirement.
- Control packets are transported using reliable channel due to relaxed and latency requirement.

We are now ready to implement the *Spec*.

5.2 Spec

The following is the skeleton of the *Spec*:

$$\begin{aligned}
 Init &\triangleq \\
 &\wedge network = \{\} \\
 &\wedge server_tx = 0 \\
 &\wedge server_tx_limit = W \\
 &\wedge server_tx_ack = 0 \\
 &\wedge client_rx = 0 \\
 &\wedge client_buffer = \{\} \\
 &\wedge lost = 0 \\
 \\
 Next &\triangleq \\
 &\vee Send \\
 &\vee \exists p \in network : \\
 &\quad Receive(p) \\
 &\vee ClientRetransmitRequest \\
 &\vee ClientAcknowledgement \\
 &\vee \exists p \in network : \\
 &\quad \wedge p.dst = \text{"client"} \\
 &\quad \wedge Drop(p)
 \end{aligned}$$

The server is represented by three variables:

- tx+1 represents the sequence number to be used in the next packet
- tx_liimit represents the highest sequence number server can send without waiting for an acknowledgement
- tx_ack represents the most recent acknowledged sequence number

The client is represented by two variables:

- client_rx is the most recently acknowledged sequence number
- client_buffer is the receive buffer holding all the packets waiting to be re-ordered prior to being acknowledged

The allowed actions include packet *Receive*, which the existential quantifier also has the side effect of re-ordering. *ClientRetransmitRequest* detects and sends retransmit request. *ClientAcknowledgement* sends acknowledgement. Finally, data packets may be dropped.

Before we start defining the actions, let us define some helper functions:

$$\begin{aligned}
 \text{MinS}(s) &\triangleq \\
 &\text{CHOOSE } x \in s : \forall y \in s : x \leq y \\
 \\
 \text{MaxS}(s) &\triangleq \\
 &\text{CHOOSE } x \in s : \forall y \in s : x \geq y \\
 \\
 \text{MaxIndex} &\triangleq \\
 &\text{LET} \\
 &\quad \text{upper} \triangleq \{x \in \text{client_buffer} : x > N - W\} \\
 &\quad \text{lower} \triangleq \{x \in \text{client_buffer} : x < W\} \\
 &\quad \text{maxv} \triangleq \text{IF } \text{upper} \neq \{\} \wedge \text{lower} \neq \{\} \\
 &\quad \text{THEN} \\
 &\quad \quad \text{MaxS}(\text{lower}) \\
 &\quad \text{ELSE} \\
 &\quad \quad \text{MaxS}(\text{client_buffer}) \\
 &\text{IN} \\
 &\quad \text{maxv} \\
 \\
 \text{MinIndex} &\triangleq \\
 &\text{LET} \\
 &\quad \text{upper} \triangleq \{x \in \text{client_buffer} : x > N - W\} \\
 &\quad \text{lower} \triangleq \{x \in \text{client_buffer} : x < W\} \\
 &\quad \text{minv} \triangleq \text{IF } \text{upper} \neq \{\} \wedge \text{lower} \neq \{\} \\
 &\quad \text{THEN} \\
 &\quad \quad \text{MinS}(\text{upper}) \\
 &\quad \text{ELSE} \\
 &\quad \quad \text{MinS}(\text{client_buffer}) \\
 &\text{IN}
 \end{aligned}$$

$$\begin{aligned}
& \text{minv} \\
\text{Range} & \triangleq \\
& \text{IF } \text{MaxIndex} \geq \text{MinIndex} \\
& \text{THEN} \\
& \quad \text{MaxIndex} - \text{MinIndex} + 1 \\
& \text{ELSE} \\
& \quad \text{MaxIndex} + 1 + N - \text{MinIndex}
\end{aligned}$$

At any moment the system allows a window of packets to be unacknowledged. Both the client and server are aware of the window size, represented by W . By looking at packets in its receive buffer and its most acknowledged sequence number, the client can determine which packets were lost. There's actually some nuisance to implement this.

Since the system does not allow more than W unacknowledged packets, the client can assume the window of packet in its receiver buffer must have sequence number $s \in \text{client_rx}.. \text{client_rx} + W$. Since the sequence number has a ceiling, the window of packets may wrap around the boundary. This introduces some complication around determining the minimum and maximum in the window of packet. The functions defined above calculates the range, maximum and minimum value in the window accounting for wraparound.

Now we can look at how the client acknowledgement logic:

$$\begin{aligned}
\text{MergeReady} & \triangleq \\
& \wedge \text{client_buffer} \neq \{\} \\
& \wedge (\text{client_rx} + 1) \% N = \text{MinIndex} \quad \text{contiguous with previous ack} \\
& \wedge \text{Range} = \text{Cardinality}(\text{client_buffer}) \quad \text{combined is contiguous} \\
\text{ClientAcknowledgement} & \triangleq \\
& \wedge \text{client_buffer} \neq \{\} \\
& \wedge \text{MergeReady} \\
& \wedge \text{client_buffer}' = \{\} \\
& \wedge \text{client_rx}' = \text{MaxIndex} \\
& \wedge \text{network}' = \text{AddMessage}([\text{dst} \mapsto \text{"server"}, \text{type} \mapsto \text{"ack"}, \text{ack} \mapsto \text{MaxIndex}], \text{network}) \\
& \wedge \text{UNCHANGED} \langle \text{server_tx}, \text{server_tx_ack}, \text{server_tx_limit}, \text{lost} \rangle
\end{aligned}$$

The client only acknowledges when it has a contiguous sequence of packets that follows its most recently acknowledged packet. When MergeReady is true, the client sends the acknowledgement back to the server.

$$\begin{aligned}
\text{ClientReceive}(pp) & \triangleq \\
& \wedge \text{network}' = \text{RemoveMessage}(pp, \text{network}) \\
& \wedge \text{client_buffer}' = \text{client_buffer} \cup \{pp.seq\} \\
& \wedge \text{UNCHANGED} \langle \text{server_tx}, \text{client_rx}, \text{server_tx_ack}, \text{server_tx_limit}, \text{lost} \rangle
\end{aligned}$$

```

Missing  $\triangleq$ 
  LET
    full_seq  $\triangleq$ 
      IF MaxIndex  $\geq$  client_rx + 1
      THEN
        {x  $\in$  client_rx + 1 .. MaxIndex : TRUE}
      ELSE
        {x  $\in$  0 .. MaxIndex : TRUE}  $\cup$  {x  $\in$  client_rx + 1 .. N - 1 : TRUE}
    all_client_msgs  $\triangleq$  {m  $\in$  network : m.dst = "client"}
    all_client_seqs  $\triangleq$  {m.seq : m  $\in$  all_client_msgs}
    network_missing  $\triangleq$  full_seq  $\setminus$  all_client_seqs
    client_missing  $\triangleq$  full_seq  $\setminus$  client_buffer
    to_request  $\triangleq$  network_missing  $\cap$  client_missing
  IN
    to_request

ClientRetransmitRequest  $\triangleq$ 
   $\wedge$   $\neg$  MergeReady
   $\wedge$  client_buffer  $\neq$  {}
   $\wedge$  Missing  $\neq$  {}
   $\wedge$  network' = AddMessage([dst  $\mapsto$  "server",
    type  $\mapsto$  "retransmit",
    seq  $\mapsto$  CHOOSE x  $\in$  Missing : TRUE],
    network)
   $\wedge$  UNCHANGED (server_tx, server_tx_limit, client_rx, client_buffer, server_tx_ack, lost)

```

ClientReceive moves the a packet from network into client receive buffer. The only reason why this is done as a separate step is to make debugging easier.

Missing returns a set of missing missing sequence number. This is done by cross checking the client receive buffer and the outstanding network packet targeting the client. In theory, the client doesn't know if a gap in its receive buffer means the packet is lost or will arrive soon. Practically, the client will assume a packet is lost after some configurable timeout and request a retransmit.

Let us take a look at server related definitions:

```

RemoveStaleAck(ack, msgs)  $\triangleq$ 
  LET
    acks  $\triangleq$  {(ack - k + N) % N : k  $\in$  1 .. W}
  IN
    {m  $\in$  msgs :  $\neg$ (m.dst = "server"  $\wedge$  m.type = "ack"  $\wedge$  m.ack  $\in$  acks)}

ServerReceive(pp)  $\triangleq$ 
   $\vee$   $\wedge$  pp.type = "ack"
   $\wedge$  server_tx_ack' = pp.ack

```

$$\begin{aligned}
& \wedge server_tx_limit' = (pp.ack + W) \% N \\
& \wedge network' = RemoveStaleAck(pp.ack, RemoveMessage(pp, network)) \\
& \wedge UNCHANGED \langle server_tx, client_rx, client_buffer, lost \rangle \\
& \vee \wedge pp.type = \text{"retransmit"} \\
& \wedge network' = AddMessage([dst \mapsto \text{"client"}, seq \mapsto pp.seq], \\
& \quad RemoveMessage(pp, network)) \\
& \wedge lost' = lost - 1 \\
& \wedge UNCHANGED \langle server_tx, server_tx_limit, client_rx, client_buffer, server_tx_ack \rangle
\end{aligned}$$

When the server receives an acknowledgement for sequence number K , it assumes $K-1$ and prior were all received by the client. *RemoveStaleAck* is a model optimization to drop all acknowledgements with sequence number less than K . Note that sequence number k , $k-N$, $k-2*N$, are all represented as k , and in theory the client may not be able to differentiate between them. Practically, N is sized large enough to represent a few seconds worth of data, so the system can safely assume a sequence number k is for the most recent N packets.

Upon receiving an acknowledgement from the client, the server bumps the *server_tx_limit* allowing it to send more data. The server can also receive a retransmit request and send the requested data. *lost* is configurable to determine how many packets can be dropped at the same time.

5.3 Model Reduction

5.3.1 Removing Stale Acknowledgement

TODO: $W * 2 \leq N$ TODO: stale ack removal TODO: describe network empty
 TODO: retransmit is assumed to be reliable, because making it unreliable doesn't make sense.

5.4 Safety

5.5 Liveness

Given the system may randomly drop packets, one possible liveness condition is to verify packets of all sequence number are received by the client at some point. This can be described as for all possible sequence number value k , k is eventually exists in client receive buffer.

$$\begin{aligned}
Liveness & \triangleq \\
& \forall i \in 0 \dots N-1 : \\
& \quad client_buffer = \{ \} \rightsquigarrow \exists j \in client_buffer : i = j
\end{aligned}$$

Chapter 6

Raft Consensus Protocol

6.1 Design

Raft is a consensus algorithm that enables a cluster of nodes to agree on a collective state even in the presence of failures. An application of Raft is database replication protocol. With a replication factor of 3 (eg. data is replicated across 3 nodes) and hard drive failure rate of 0.81% per year, the possibility of the total failure where the entire replication group goes down is $1 - 0.0081^3 = 99.9999\%$ uptime [4].

This chapter implements only the leader election portion of the protocol to limit the scope of the discussion. For a full description of the the Raft protocol, please refer to the original paper [5].

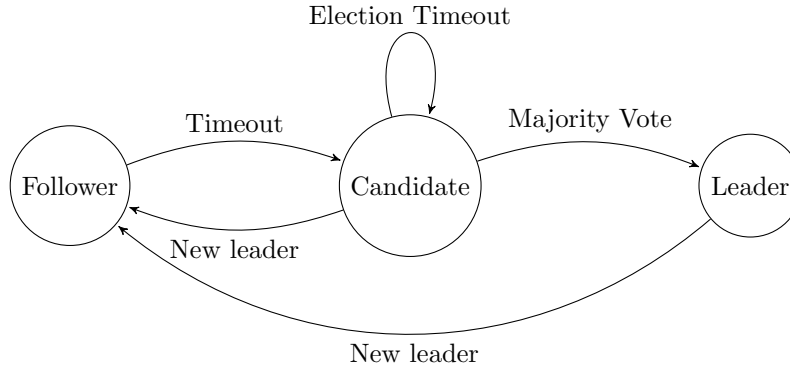
We will briefly describe Raft and its leader election process below:

- A Raft cluster have N nodes, the cluster work collective as a *system* to offer some service
- Each node can be in one of three possible states: Follower, Candidate, Leader
- During normal operations, a cluster of N nodes have a single leader and N-1 followers
- The leader handles all the client interactions. Requests sent to followers will be redirected to the leader
- The leader regularly sends heartbeat to the follower, indicate its alive
- If a follower fails to receive heartbeat from the leader after timeout, it will become a candidate, vote for itself, and campaign to be leader
- A candidate collect the majority of the vote becomes the leader

- If multiple candidates are campaigning and a split vote happen, candidates will eventually declare election timeout and start new round of election
- The cluster can have multiple leaders due to unfavourable network conditions, but the leaders must be on different terms
- A newly elected leader will send a heartbeat to other nodes to establish leadership
- All request and responses include the sender's term, allowing the receiver to react accordingly

The protocol also included description about log synchronization, state recovery, and more. Many details are omitted in this chapter to reduce modeling cost. The N nodes in the cluster operate *independently* following the above heuristics. Hopefully this highlights the complexity around verifying the correctness of the protocol.

The following illustrate the state diagram of one node in the cluster:



6.2 Spec

The following implements the skeleton portion of the leader election protocol:

$$\begin{aligned}
 Init &\triangleq \\
 &\wedge state = [s \in Servers \mapsto \text{"Follower"}] \\
 &\wedge messages = \{\} \\
 &\wedge voted_for = [s \in Servers \mapsto \text{""}] \\
 &\wedge vote_granted = [s \in Servers \mapsto \{\}] \\
 &\wedge vote_requested = [s \in Servers \mapsto 0] \\
 &\wedge term = [s \in Servers \mapsto 0] \\
 RequestVoteSet(i) &\triangleq \{
 \end{aligned}$$

$$\begin{aligned}
& [fSrc \mapsto i, fDst \mapsto s, fType \mapsto \text{"RequestVoteReq"}, fTerm \mapsto term[i]] \\
& \quad : s \in Servers \setminus \{i\} \\
& \} \\
Campaign(i) & \triangleq \\
& \wedge vote_requested[i] = 0 \\
& \wedge vote_requested' = [vote_requested \text{ EXCEPT } ![i] = 1] \\
& \wedge messages' = messages \cup RequestVoteSet(i) \\
& \wedge UNCHANGED \langle state, term, vote_granted, voted_for \rangle \\
KeepAliveSet(i) & \triangleq \{ \\
& [fSrc \mapsto i, fDst \mapsto s, fType \mapsto \text{"AppendEntryReq"}, fTerm \mapsto term[i]] \\
& \quad : s \in Servers \setminus \{i\} \\
& \} \\
Leader(i) & \triangleq \\
& \wedge state[i] = \text{"Leader"} \\
& \wedge messages' = messages \cup KeepAliveSet(i) \\
& \wedge UNCHANGED \langle state, voted_for, term, vote_granted, vote_requested \rangle \\
BecomeLeader(i) & \triangleq \\
& \wedge Cardinality(vote_granted[i]) > Cardinality(Servers) \div 2 \\
& \wedge state' = [state \text{ EXCEPT } ![i] = \text{"Leader"}] \\
& \wedge UNCHANGED \langle messages, voted_for, term, vote_granted, vote_requested \rangle \\
Candidate(i) & \triangleq \\
& \wedge state[i] = \text{"Candidate"} \\
& \wedge \vee Campaign(i) \\
& \quad \vee BecomeLeader(i) \\
& \quad \vee Timeout(i) \\
Follower(i) & \triangleq \\
& \wedge state[i] = \text{"Follower"} \\
& \wedge Timeout(i) \\
Receive(msg) & \triangleq \\
& \vee \wedge msg.fType = \text{"AppendEntryReq"} \\
& \quad \wedge AppendEntryReq(msg) \\
& \vee \wedge msg.fType = \text{"AppendEntryResp"} \\
& \quad \wedge AppendEntryResp(msg) \\
& \vee \wedge msg.fType = \text{"RequestVoteReq"} \\
& \quad \wedge RequestVoteReq(msg) \\
& \vee \wedge msg.fType = \text{"RequestVoteResp"} \\
& \quad \wedge RequestVoteResp(msg) \\
Next & \triangleq \\
& \vee \exists i \in Servers : \\
& \quad \vee Leader(i)
\end{aligned}$$

$$\begin{aligned} & \vee \text{Candidate}(i) \\ & \vee \text{Follower}(i) \\ & \vee \exists \text{msg} \in \text{messages} : \text{Receive}(\text{msg}) \end{aligned}$$

- *Next* either picks a server to make progress, or picks a message in the message pool to process. Message processing is done by *Receive*, handling is state agnostic
- *message* is defined to be a set that holds a collection of functions, where each function is a message with source, destination, type, and more specified
- *voted_for* tracks who a given node previously voted for. This prevents a node from voting more than once
- *vote_granted* tracks how many votes a candidate has received
- *vote_requested* tracks if a node has already issued request vote to its peers
- *Follower* either Receive or Timeout and campaign to be a leader
- *Candidate* campaigns to be a leader, and becomes one if it has enough vote. Failing to collect enough votes, *Candidate* start a new election on a new term. It can also receive a request with a higher term and transition to be a *Follower*.
- *Leader* will establish its leadership by sending *AppendEntryReq* to all its peers

The Spec implements four messages AppendEntry request/response, RequestVote request/response. Handling for all messages are fairly similar in structure. In this chapter we will look at *RequestVoteReq* only. Readers are encouraged to check the remaining definition as an exercise:

$$\begin{aligned} \text{RequestVoteReq}(\text{msg}) &\triangleq \\ \text{LET} & \\ & i \triangleq \text{msg.fDst} \\ & j \triangleq \text{msg.fSrc} \\ & \text{type} \triangleq \text{msg.fType} \\ & t \triangleq \text{msg.fTerm} \\ \text{IN} & \\ & \text{haven't voted, or whom we voted re-requested} \\ & \vee \wedge t = \text{term}[i] \\ & \wedge \vee \text{voted_for}[i] = j \\ & \quad \vee \text{voted_for}[i] = "" \\ & \wedge \text{voted_for}' = [\text{voted_for} \text{ EXCEPT } ![i] = j] \\ & \wedge \text{messages}' = \text{AddMessage}([\text{fSrc} \mapsto i, \\ & \quad \text{fDst} \mapsto j, \\ & \quad \text{fType} \mapsto \text{"RequestVoteResp"}], \end{aligned}$$

$$\begin{aligned}
& fTerm \mapsto t, \\
& fSuccess \mapsto 1], \\
& \text{RemoveMessage}(msg, messages)) \\
& \wedge \text{UNCHANGED } \langle state, term, vote_granted, vote_requested, establish_leadership \rangle \blacksquare \\
& \text{already voted someone else} \\
\vee \wedge t = term[i] \\
& \wedge voted_for[i] \neq j \\
& \wedge voted_for[i] \neq "" \\
& \wedge messages' = \text{AddMessage}([fSrc \mapsto i, \\
& \quad fDst \mapsto j, \\
& \quad fType \mapsto \text{"RequestVoteResp"}, \\
& \quad fTerm \mapsto t, \\
& \quad fSuccess \mapsto 0], \\
& \quad \text{RemoveMessage}(msg, messages)) \\
& \wedge \text{UNCHANGED } \langle state, voted_for, term, vote_granted, vote_requested, establish_leadership \rangle \blacksquare \\
\vee \wedge t < term[i] \\
& \wedge messages' = \text{AddMessage}([fSrc \mapsto i, \\
& \quad fDst \mapsto j, \\
& \quad fType \mapsto \text{"RequestVoteResp"}, \\
& \quad fTerm \mapsto term[i], \\
& \quad fSuccess \mapsto 0], \\
& \quad \text{RemoveMessage}(msg, messages)) \\
& \wedge \text{UNCHANGED } \langle state, voted_for, term, vote_granted, vote_requested, establish_leadership \rangle \blacksquare \\
& \text{revert back to follower} \\
\vee \wedge t > term[i] \\
& \wedge state' = [state \text{ EXCEPT } ![i] = \text{"Follower"}] \\
& \wedge term' = [term \text{ EXCEPT } ![i] = t] \\
& \wedge voted_for' = [voted_for \text{ EXCEPT } ![i] = j] \\
& \wedge vote_granted' = [vote_granted \text{ EXCEPT } ![i] = \{\}] \\
& \wedge vote_requested' = [vote_requested \text{ EXCEPT } ![i] = 0] \\
& \wedge establish_leadership' = [establish_leadership \text{ EXCEPT } ![i] = 0] \\
& \wedge messages' = \text{AddMessage}([fSrc \mapsto i, \\
& \quad fDst \mapsto j, \\
& \quad fType \mapsto \text{"RequestVoteResp"}, \\
& \quad fTerm \mapsto t, \\
& \quad fSuccess \mapsto 1], \\
& \quad \text{RemoveMessage}(msg, messages))
\end{aligned}$$

The handling is split into three cases:

- If received request is on a higher term, processing node grants vote and becomes a Follower
- If received request is on a lower term, processing node ignores request
- If received request is on the same term, processing node only grants vote if it hasn't voted, or has had voted for the same requester prior

6.3 Model Reduction

The model checker will run the spec as defined, but due to the exponential growth of states it is unlikely to complete in a reasonable amount of time. We need to simplify the model and possibly trades off some correctness. Careful consideration must go into finding the right balance between maximizing model correctness and minimizing model checker runtime.

The main strategy is to *bound* the state graph. The following describe a set of optimization implemented for this example.

6.3.1 Modeling Messages as a Set

In the original Raft TLA+ Spec [6], messages are modeled as an *unordered map* to track the count of each message. It is possible for a sender to repeatedly send the same message (eg. keepalive), and grow the message count in an unbounded fashion.

messages in this example has been implemented as a set, which effectively limits message instance count to one. It is still possible for messages to grow unboundedly because of the monotonically increasing term value. Further changes are described below.

6.3.2 Limit Term Divergence

It is possible for a node to *never* make progress. Such case can occur when a node is partitioned off while the rest of the cluster elects new leader and move onto newer terms. Many of the interesting behaviours of Raft are how it addresses these cases. In a cluster of nodes with mixed terms, the nodes with older term will eventually converge onto newer terms when they are contacted by new leader. This converging behaviour will happen whether the stale node is either 1 or N terms away from the current leader, and the former is much less costly to simulate than the latter because the reduced number of states.

We can include *LimitDivergence* as a conjunction in *Timeout*:

$$\begin{aligned}
 \text{LimitDivergence}(i) &\triangleq \\
 &\text{LET} \\
 &\quad \text{values} \triangleq \{ \text{term}[s] : s \in \text{Servers} \} \\
 &\quad \text{max_v} \triangleq \text{CHOOSE } x \in \text{values} : \forall y \in \text{values} : x \geq y \\
 &\quad \text{min_v} \triangleq \text{CHOOSE } x \in \text{values} : \forall y \in \text{values} : x \leq y \\
 &\text{IN} \\
 &\quad \vee \wedge \text{term}[i] \neq \text{max_v} \\
 &\quad \vee \wedge \text{term}[i] = \text{max_v} \\
 &\quad \quad \wedge \text{term}[i] - \text{min_v} < \text{MaxDiff}
 \end{aligned}$$

$$\begin{aligned}
\text{Timeout}(i) &\triangleq \\
&\wedge \text{LimitDivergence}(i) \\
&\wedge \text{state}' = [\text{state} \text{ EXCEPT } ![i] = \text{"Candidate"}] \\
&\wedge \text{voted_for}' = [\text{voted_for} \text{ EXCEPT } ![i] = i] \quad \text{voted for myself} \\
&\wedge \text{vote_granted}' = [\text{vote_granted} \text{ EXCEPT } ![i] = \{i\}] \\
&\wedge \text{vote_requested}' = [\text{vote_requested} \text{ EXCEPT } ![i] = 0] \\
&\wedge \text{term}' = [\text{term} \text{ EXCEPT } ![i] = @ + 1] \quad \text{bump term} \\
&\wedge \text{establish_leadership}' = [\text{establish_leadership} \text{ EXCEPT } ![i] = 0] \\
&\wedge \text{UNCHANGED } \langle \text{messages} \rangle \\
&/ \text{PrintT}(\text{state}')
\end{aligned}$$

6.3.3 Normalize Cluster Term

However, term *itself* can grow unbounded. This is a key tenet converging protocols rely on, an monotonically increasing counter. We want to *normalize* the range of terms in the cluster so the minimum value resets back to 0. This provides an upper bound to the state graph.

$$\begin{aligned}
\text{Normalize} &\triangleq \\
&\text{LET} \\
&\quad \text{values} \triangleq \{ \text{term}[s] : s \in \text{Servers} \} \\
&\quad \text{max_v} \triangleq \text{CHOOSE } x \in \text{values} : \forall y \in \text{values} : x \geq y \\
&\quad \text{min_v} \triangleq \text{CHOOSE } x \in \text{values} : \forall y \in \text{values} : x \leq y \\
&\text{IN} \\
&\quad \wedge \text{max_v} = \text{MaxTerm} \\
&\quad \wedge \text{term}' = [s \in \text{Servers} \mapsto \text{term}[s] - \text{min_v}] \\
&\quad \wedge \text{messages}' = \{ \} \\
&\quad \wedge \text{UNCHANGED } \langle \text{state}, \text{voted_for}, \text{vote_granted}, \text{vote_requested}, \text{establish_leadership} \rangle \blacksquare \\
\text{Next} &\triangleq \\
&\vee \wedge \forall i \in \text{Servers} : \text{term}[i] \neq \text{MaxTerm} \\
&\quad \wedge \vee \exists i \in \text{Servers} : \\
&\quad \quad \vee \text{Leader}(i) \\
&\quad \quad \vee \text{Candidate}(i) \\
&\quad \quad \vee \text{Follower}(i) \\
&\quad \vee \exists \text{msg} \in \text{messages} : \text{Receive}(\text{msg}) \\
&\vee \wedge \exists i \in \text{Servers} : \text{term}[i] = \text{MaxTerm} \\
&\quad \wedge \text{Normalize}
\end{aligned}$$

The implementation ensures only the state machine only moves forward when none of the nodes is on *MaxTerm*. If any of the node is on *MaxTerm*, the cluster terms are normalized.

Another caveat here is in the initial implementation I didn't update messages. This led to liveness property violation as the messages had terms disagree-

ing with the system state. To simplify the spec I simply cleared all messages. This indirectly verifies a portion of the packet loss handling in the spec as well.

6.3.4 Sending Request as a Batch

The send requests were initially implemented using the existential quantifier. This introduces many interleaving states. This was replaced with a universal quantifier so the set of messages are only sent once. The implementation no longer tracks if the responses were received, since the spec should handle packet loss scenarios as well.

$$\begin{aligned}
\text{RequestVoteSet}(i) &\triangleq \{ \\
&\quad [fSrc \mapsto i, fDst \mapsto s, fType \mapsto \text{"RequestVoteReq"}, fTerm \mapsto term[i]] \\
&\quad : s \in Servers \setminus \{i\} \\
&\} \\
\text{Campaign}(i) &\triangleq \\
&\quad \wedge vote_requested[i] = 0 \\
&\quad \wedge vote_requested' = [vote_requested \text{ EXCEPT } ![i] = 1] \\
&\quad \wedge messages' = messages \cup \text{RequestVoteSet}(i) \\
&\quad \wedge \text{UNCHANGED } \langle state, term, vote_granted, voted_for, establish_leadership \rangle \\
\text{KeepAliveSet}(i) &\triangleq \{ \\
&\quad [fSrc \mapsto i, fDst \mapsto s, fType \mapsto \text{"AppendEntryReq"}, fTerm \mapsto term[i]] \\
&\quad : s \in Servers \setminus \{i\} \\
&\} \\
\text{Leader}(i) &\triangleq \\
&\quad \wedge state[i] = \text{"Leader"} \\
&\quad \wedge establish_leadership[i] = 0 \\
&\quad \wedge establish_leadership' = [establish_leadership \text{ EXCEPT } ![i] = 1] \\
&\quad \wedge messages' = messages \cup \text{KeepAliveSet}(i) \\
&\quad \wedge \text{UNCHANGED } \langle state, voted_for, term, vote_granted, vote_requested \rangle
\end{aligned}$$

6.3.5 Prune Messages with Stale Terms

When a node's term advances, all messages targeted to this node with older terms are discarded. Keeping messages with stale terms allows the model checker to verify the node correctly discards them, but can exponentially grow the state machine. To simplify the model, we can prune stale messages as we add a new message:

$$\begin{aligned}
\text{AddMessage}(to_add, msgs) &\triangleq \\
&\quad \text{LET} \\
&\quad \quad pruned \triangleq \{msg \in msgs : \\
&\quad \quad \quad \neg(msg.fDst = to_add.fDst \wedge msg.fTerm < to_add.fTerm)\} \\
&\quad \text{IN}
\end{aligned}$$

$$pruned \cup \{to_add\}$$

$$RemoveMessage(to_remove, msgs) \triangleq$$

6.3.6 Enable Symmetry

Since the behaviour is symmetric between nodes, we can enable symmetry to speed up model checker runtime:

$$Perms \triangleq Permutations(Servers)$$

6.4 Safety

One of the goals for the protocol is to ensure the cluster only have one leader. It is possible for the clusters to have multiple leaders due to unfavourable network connections. For example, a leader node is partitioned off and a new leader is elected. However, even when the cluster have multiple leaders, they *must* be on different terms. The leader with the highest term is effectively the *true leader*. This invariant can be implemented like so:

$$\begin{aligned} LeaderUniqueTerm &\triangleq \\ &\forall s1, s2 \in Servers : \\ &(state[s1] = \text{"Leader"} \wedge state[s2] = \text{"Leader"} \wedge s1 \neq s2) \Rightarrow (term[s1] \neq term[s2]) \blacksquare \end{aligned}$$

For every pair of nodes, they cannot both be Leaders and have the same term.

6.5 Liveness

In any failure recovery scenario, the nodes in the cluster converges to a higher term value either voluntary or involuntarily. For example:

- A node timed out and starts a new election on a new term
- A partitioned follower receives heartbeat from a new leader on a new term
- A candidate receiving a request vote from another candidate on a higher term

In any case, a node's term number always increase. This can be described as below:

$$\begin{aligned} Converge &\triangleq \\ &\forall s \in Servers : \\ &term[s] = 0 \rightsquigarrow term[s] = MaxTerm - MaxDiff \end{aligned}$$

Instead of *MaxTerm*, we use *MaxTerm-MaxDiff* to ensure the liveness property is always upheld even after *Normalization*. However, running the spec against TLC now will encounter a set of stuttering issues. We also need to update the fairness description to ensure all possible actions are called when the enabling conditions are *eventually always* true:

$$\begin{aligned}
\textit{Liveness} &\triangleq \\
&\wedge \forall i \in \textit{Servers} : \\
&\quad \wedge \textit{WF}_{\textit{vars}}(\textit{Leader}(i)) \\
&\quad \wedge \textit{WF}_{\textit{vars}}(\textit{Candidate}(i)) \\
&\quad \wedge \textit{WF}_{\textit{vars}}(\textit{Follower}(i)) \\
&\wedge \textit{WF}_{\textit{vars}}(\exists \textit{msg} \in \textit{messages} : \textit{Receive}(\textit{msg}))
\end{aligned}$$

Part III

Examples with PlusCal

PlusCal is a C-like syntax that allows designer to describe their *Spec* in a more programming language like fashion. I'm of the opinion that these are suitable to describe concurrent algorithm, where the code execution between multiple contexts may interleave in any way imaginable. While it certainly is possible to express these in TLA+ directly, I find it to be error prone, somewhat comparable to writing in Assembly instead of C. In this section we will describe a few PlusCal example.

Chapter 7

SPSC Lockless Queue

A single producer single consumer (SPSC) lockless queue is a data exchange queue between a producer and a consumer. The SPSC lockfree queue enables data exchange between producer and consumer without the use of a lock, allowing both producer and consumer to make progress in all scenarios.

An example application of SPSC queue is a data exchange interface between ASIC and the CPU in a driver implementation.

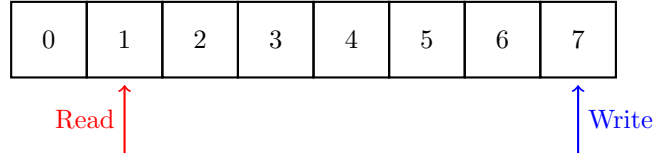
A real implementation need to account for memory ordering effects specific to the architecture. For example, ARM has weak memory ordering model where read/write may appear out-of-order between CPUs. In this chapter we will assume *logical* execution order where each command is perceived issued sequentially (even across CPUs) to focus the discussion on describing the system using TLA+.

7.1 Requirement

The following describes the SPSC queue requirements:

- Two executing context, reader and writer
- Writer advances $wptr$ after writes
- Reader advances $rptr$ after reads
- If $rptr$ equals $wptr$, queue is empty
- If $(wptr + 1) \% N$ equals $rptr$, queue is full

The following is an example of a SPSC queue:



Since reader and writer execute in different context, the instructions in read and write can interleave in *any* way imaginable:

- Reader empty check can happen just as writer is writing data
- Writer full check can happen just as reader is reading data
- Reading and writing can occur concurrently

The key observations is the index held by write pointer is reserved by the writer. Similarly, index held by the read pointer is reserved by the reader. The only exception is when read pointer equals to write pointer, then the queue is empty. Given the possible ways the reader and writer execution can interleave, we can use TLA+ to verify the design.

7.2 Spec

TLA+ specification can be written using its native formal specification language, or a C-like syntax called PlusCal (which transpiles down to its native form). In this example, I chose to implement the specification using PlusCal, since the content to be verified is psuedo implementation. While it is possible specify SPSC in native TLA+, I find the approach more error prone as each line is effectively an individual state to be modeled.

The following is a snippet of the *Spec* written in PlusCal:

```

procedure reader()
begin
  r_chk_empty:      if rptr = wptr then
    r_early_ret:    return ;
  end if ;
  r_read_buf:      assert buffer[rptr] ≠ 0 ;
  r_cs:            buffer[rptr] := 0 ;
  r_upd_rptr:      rptr := (rptr + 1)%N ;
  return ;
end procedure ;

procedure writer()
begin
  w_chk_full:      if (wptr + 1)%N = rptr then
    w_early_ret:    return ;

```

```

    end if ;
w_write_buf:    assert buffer[wptr] = 0 ;
w_cs:          buffer[wptr] := wptr + 1000 ;
w_upd_wptr:    wptr := (wptr + 1) % N ;
    return ;
end procedure ;

```

Note some lines start with *label* (eg. `r_chk_empty`). All the actions associated with the label is assumed executed atomically. This is reflected in the generated TLA+ code:

```

r_chk_empty(self)  $\triangleq$   $\wedge pc[self] = \text{"r\_chk\_empty"}$ 
 $\wedge$  IF  $rptr = wptr$ 
THEN  $\wedge pc' = [pc \text{ EXCEPT } ![self] = \text{"r\_early\_ret"}]$ 
ELSE  $\wedge pc' = [pc \text{ EXCEPT } ![self] = \text{"r\_read\_buf"}]$ 
 $\wedge$  UNCHANGED  $\langle rptr, wptr, buffer, stack \rangle$ 

```

7.3 Safety

Some safety requirement we can enforce include:

```

MUTEX  $\triangleq$ 
 $\neg((pc[WRITER] = \text{"w\_cs"}) \wedge (pc[READER] = \text{"r\_cs"}) \wedge rptr = wptr)$ 

Inv_Basics  $\triangleq$ 
 $\wedge ((written \cup writing) \cup unused) = all$ 
 $\wedge reading \subseteq written$  reading is a subset of written
 $\wedge \forall i \in unused : buffer[i] = 0$ 
 $\wedge \vee Cardinality(to\_be\_read) + 1 = Cardinality(reading)$ 
 $\vee Cardinality(to\_be\_read) = Cardinality(reading) + 1$ 
 $\vee Cardinality(to\_be\_read) = Cardinality(reading)$ 
 $\wedge MUTEX$ 

```

7.4 Liveness

All indices are eventually used:

```

Liveness  $\triangleq$ 
 $\forall k \in 0 \dots N - 1 :$ 
 $\diamond(buffer[k] \neq 0)$ 
Unused index 0 becomes used, used index 0 becomes unused.
Liveness2  $\triangleq$ 
 $\wedge (buffer[0] = 0) \rightsquigarrow buffer[0] = 1000$ 
 $\wedge (buffer[0] = 1000) \rightsquigarrow buffer[0] = 0$ 

```

7.5 Configuration

Chapter 8

SPMC Lockless Queue

As the name suggest, a SPMC lockless queue supports a single producer multiple consumer usage topology.

In previously described SPSC, the reader assumes write index is reserved, and the writer assumes read index is reserved. While the relationship between read and write context remains true in SPMC, the complication is now readers compete to reserve an index during read. Some design considerations include:

- Readers must have a way to reserve an index to read
- Readers may complete the read in order different from when they reserve the indices
- Readers can perform the reads independently

A primitive in modern CPU architecture is the compare-and-swap (CAS) instruction. To use CAS, issuer needs to specify a memory location, a current value and a new value. Only when value in the memory location matches the current value, the new value will be written. The instruction ensure this is done atomically. If multiple CPUs issue CAS at the same time to the same memory location, only one CPU will *win* as the other CPU's current value check will fail. Many of the concurrent algorithms are built ontop of this primitive.

8.1 Design

Some of the design limitation include:

- A resource is exclusively updated by one owner, and read by one or more readers
- For shared resource that can be updated by multiple owners, the CPU can gaurantees exclusive update from a single resource

For the design:

- SPMC is implemented as a circular queue with size of N
- The status of individual index is represented as an status array of size N
- The status of each index is either UNUSED, WRITTEN, or READING
- Each reader maintain its own read pointer
- A *outstanding* counter is incremented by the writer when write is complete, and decremented by the reader when it reserves a read

Whenever the write finishes a write, it increments *outstanding* to indicate some buffer is ready to read.

To read, a reader performs a two-step reservation:

- The reader decrements *outstanding*. A successful decrement means the reader is *gauranteed* a read index.
- After successful decrement of *outstanding*, the reader walk its read pointer until it successfully reserve the next available index to read. A This is done by attempting to CAS update an index from WRITTEN to READING. If the update fails, then the index was already reserved by another reader.

There may be more than one approach in implementing SPMC, the above description is what we will implement in this chapter.

8.2 Spec

The following is the core reader implementation:

```

procedure reader( )
variable
    i = self ;
begin
    r_chk_empty:
        if outstanding  $\neq$  0 then
            outstanding := outstanding - 1 ;
        else
            r_early_ret:
                return ;
        end if ;
    r_try_lock:
        if status[rptr[i]] = WRITTEN then
            status[rptr[i]] := READING ;
        else

```

```

    r_retry:
        rp_ptr[i] := (rp_ptr[i] + 1)%N ;
        goto r_try_lock ;
    end if ;
r_data_chk:
    assert buffer[rp_ptr[i]] = rp_ptr[i] + 1000 ;
r_read_buf:
    buffer[rp_ptr[i]] := 0 ;
r_unlock:
    status[rp_ptr[i]] := UNUSED ;
r_done:
    return ;
end procedure ;

```

The reader performs a non-zero check on outstanding. If outstanding is zero, queue is empty and reader early returns.

If outstanding is K, then at most K readers can reserve a index to read. If system has M readers, then M-K readers will fail to reserve a read index. The readers now compete to reserve a read. More specifically:

- Reader loads outstanding, stores that onto local variable A
- Reader early returns if A is zero
- Reader calls $rv = \text{CAS}(A, A-1)$
- If rv is non-success, go back to the top

If rv is non-success, another reader has *won* the reservation. The current reader can attempt to reserve again if *outstanding* is non-zero.

If rv is success, the reader is *gauranteed* a read. However, readers may need to compete to reserve an available index. This is done by attempting to CAS update the index status from WRITTEN to READING. Failing the CAS indicate another reader has reserved this index, and the reader will bump the read pointer and try to reserve the next index.

Now let us take a look at the writer implementation:

```

procedure writer( ) begin
    w_chk_full:
        if outstanding = N - 1 then
            w_early_ret:
                return ;
            end if ;
    w_chk_st:

```

```

if status[wptr]  $\neq$  UNUSED then
  w_early_ret2:
    return ;
end if ;
w_write_buf:
  buffer[wptr] := wptr + 1000 ;
w_mark_written:
  status[wptr] := WRITTEN ;
w_inc_wptr:
  wptr := (wptr + 1) % N ;
w_inc:
  outstanding := outstanding + 1 ;
w_done:
  return ;
end procedure ;

```

The writer first checks *outstanding*, and early return if queue is full. After fullness check, the writer then checks if the current index is *UNUSED*. This is to account for the edge case where a reader has performed the reservation first step to decrement *outstanding* but haven't done the actual read. If both checks pass, then writer now has an *UNUSED* index it can write to.

The SPMC algorithm can be tricky to get right. There are many things to consider when designing a SPMC queue. Considerations include:

- Readers can lapse each other
- Readers can lapse writer
- One reader can starve other readers
- A slow reader can block the system

And under all circumstances, system *correctness* must be maintained.

8.3 Safety

When a reader reserves an index to read, the reader must have exclusive access. This can be described as: For any pair of readers inside critical section, they must operate on different indices:

$$\begin{aligned}
 \textit{ExclusiveReservation} &\triangleq \\
 &\forall x, y \in \textit{READERS} : \\
 &(x \neq y \wedge pc[x] = \textit{"r_read_buf"} \wedge pc[y] = \textit{"r_read_buf"}) \\
 &\Rightarrow (rptr[x] \neq rptr[y])
 \end{aligned}$$

Similarly, for any reader and writer inside critical section, they must operate on different indices as well:

$$\begin{aligned} \text{ExclusiveReadWrite} &\triangleq \\ &\forall x \in \text{READERS} : \\ &(\text{pc}[x] = \text{"r_read_buf"} \wedge \text{pc}[\text{WRITER}] = \text{"w_write_buf"}) \Rightarrow (\text{rptr}[x] \neq \text{wptr}) \blacksquare \end{aligned}$$

8.4 Liveness

All indices must be used as the system runs. The following verifies all unused indices are eventually used, and all used indices are eventually unused:

$$\begin{aligned} \text{Liveness} &\triangleq \\ &\wedge \forall k \in 0 \dots N-1 : \\ &\quad \text{buffer}[k] = 0 \leadsto \text{buffer}[k] \neq 0 \\ &\wedge \forall k \in 0 \dots N-1 : \\ &\quad \text{buffer}[k] \neq 0 \leadsto \text{buffer}[k] = 0 \end{aligned}$$

The following describes a more subtle scenario. We need to ensure the system remains functional even if readers complete out-of-order. The following describe such scenario, where two non-contiguous indices have been reserved for reading. In this case we expect the indices to eventually be re-used. This means the system remains functional after such scenario.

$$\begin{aligned} \text{Liveness2} &\triangleq \\ &\forall k \in 0 \dots N-3 : \\ &\quad \wedge (\text{status}[k] = \text{READING} \wedge \text{status}[k+1] = \text{UNUSED} \wedge \text{status}[k+2] = \text{READING}) \blacksquare \\ &\quad \leadsto (\text{status}[k] = \text{WRITTEN}) \\ &\quad \wedge (\text{status}[k] = \text{READING} \wedge \text{status}[k+1] = \text{UNUSED} \wedge \text{status}[k+2] = \text{READING}) \blacksquare \\ &\quad \leadsto (\text{status}[k+2] = \text{WRITTEN}) \end{aligned}$$

Part IV

Reference

Chapter 9

Data Structure

Like other languages, TLA+ provides its data structure. I assume the readers are already familiar with common data structure, and this chapter will only focus on the TLA+ language semantics.

9.1 Set

This is the most common data structure used in TLA+ spec. The following is a few examples on how a set can be used:

$a \triangleq$	$\{0, 1, 2\}$	
$b \triangleq$	$\{2, 3, 4\}$	
$c \triangleq$	$a \cup b$	$\{0, 1, 2, 3, 4\}$
$d \triangleq$	$a \cap b$	$\{2\}$
$e \triangleq$	$\exists x \in c : x > 3$	TRUE - because 4 in c is bigger than 3
$f \triangleq$	$\exists x \in c : x > 5$	FALSE - nothing in c is bigger than 5
$g \triangleq$	$\forall x \in c : x < 3$	FALSE - not all elements in c are smaller than 3
$h \triangleq$	$\forall x \in c : x < 5$	TRUE - all elements in c are smaller than 5
$i \triangleq$	$\{x \in c : x < 3\}$	$\{0, 1, 2\}$ - all elements less than 3
$j \triangleq$	$Cardinality(c)$	5 - the number of elements in c
$k \triangleq$	$c \setminus d$	$\{0, 1, 3, 4\}$ - c subtracts d

9.2 Tuple

$A \triangleq$	$\langle 0, 1, 2 \rangle$	
$B \triangleq$	$\langle 2, 3, 4 \rangle$	
$C \triangleq$	$A \circ B$	tuple: 0, 1, 2, 2, 3, 4
$D \triangleq$	$Len(C)$	6
$E \triangleq$	$\forall x \in 1 \dots Len(C) : C[x] \neq 10$	TRUE - every C[x] is not 10
		First tuple element is at index 1 (not 0)
$F \triangleq$	$\exists x \in 1 \dots Len(C) : C[x] = 2$	TRUE - there exists a C[x] that is 2

$$G \triangleq \{x \in 1 \dots \text{Len}(C) : C[x] = 2\} \quad \{3, 4\} \text{ - when index is 3 or 4, } C[x] = 2$$

Chapter 10

Fairness and Liveness

For rigorous definition and proof, please refer to (TODO: citations). This chapter focus on the application aspect of liveness and fairness and define an elevator spec that goes up and down.



10.1 Liveness

Consider the following elevator *Spec*:

MODULE <i>elevator</i>	
EXTENDS	<i>Integers</i>
VARIABLES	<i>a</i>
<i>vars</i>	$\triangleq \langle a \rangle$
<i>TOP</i>	$\triangleq 4$
<i>BOTTOM</i>	$\triangleq 1$
<i>Init</i>	\triangleq
	$\wedge a = BOTTOM$
<i>Up</i>	\triangleq
	$\wedge a \neq TOP$
	$\wedge a' = a + 1$
<i>Down</i>	\triangleq
	$\wedge a \neq BOTTOM$
	$\wedge a' = a - 1$
<i>Spec</i>	\triangleq
	$\wedge Init$
	$\wedge \Box[Up \vee Down]_a$

The building has a set of floors and the elevator can go either up or down. The elevator keeps going up until it's the top floor, or keep going down until

it's the bottom floor. TLC will pass the *Spec* as is.

Let's introduce a liveness property. The elevator should always at least go to the second floor:

$$\begin{aligned} \text{Liveness} &\triangleq \\ &\wedge a = 1 \leadsto a = 2 \end{aligned}$$

Running the *Spec* against TLC will report a violation:

```
Error: Temporal properties were violated.
Error: The following behavior constitutes a counter-example:
State 1: <Initial predicate>
a = 1
State 2: Stuttering
```

Since the *Spec* permits *stuttering*, the state machine is allowed to perpetually stay on 1F and *never* go to 2F. This can be fixed by introducing fairness description.

10.2 Weak Fairness

Weak fairness is defined as:

$$\Diamond \Box (ENABLED \langle A \rangle_v) \Rightarrow \Box \Diamond \langle A \rangle_v \quad (10.1)$$

$ENABLED \langle A \rangle$ represents *conditions required* for action A. The above translates to: if conditions required for action A to occur is *eventually always* true, then action A will *always eventually* happen.

Without weak fairness defined, the elevator may *stutter* at 1F and never go to 2F. Weak fairness states that if the conditions of an action is *eventually always* true (ie. elevator decides to stay on 1F but *can* go up), the elevator *always eventually* go up.

$$\begin{aligned} \text{Spec} &\triangleq \\ &\wedge \text{Init} \\ &\wedge \Box [\text{Down} \vee \text{Up}]_a \\ &\wedge \text{WF}_a(\text{Down}) \\ &\wedge \text{WF}_a(\text{Up}) \end{aligned}$$

Running the spec against TLC passes again. What if we want to verify the elevator eventually always goes to the top, not just to 2F? Let's modify the Liveness property again:

$$\text{Liveness} \triangleq$$

$$\wedge a = BOTTOM \rightsquigarrow a = TOP$$

TLC now reports the following violation:

Error: Temporal properties were violated.

Error: The following behavior constitutes a counter-example:

State 1: <Initial predicate>

a = 1

State 2: <Up line 10, col 5 to line 11, col 17 of module elevator>■

a = 2

Back to state 1: <Down line 13, col 5 to line 14, col 17 of module elevator>■

TLC identified a case where the elevator is perpetually stuck going between 1F and 2F, but never go to 3F. Weak fairness is no longer enough, because the the elevator is not stuck on 2F repeatedly, but stuck going between 1F and 2F. This is where we need strong fairness.

10.3 Strong Fairness

Strong fairness is defined as:

$$\Box\Diamond(ENABLED\langle A \rangle_v) \Rightarrow \Box\Diamond\langle A \rangle_v \quad (10.2)$$

The difference between weak and strong fairness is the *eventually always* vs. *always eventually*.

In weak fairness, once the state machine is stuck in a state forever, the state machine always transition to a possible next state permitted by the *Spec* (eg. if the elevator is stuck on 1F but can go to 2F, it will). With strong fairness, the elevator doesn't need to be stuck on 2F to go to 3F. If the elevator *always eventually* makes it to 2F, it *always eventually* go to 3F.

Intuitively we are tempted to enable strong fairness like so:

$$\begin{aligned} Spec &\triangleq \\ &\wedge Init \\ &\wedge \Box[Up \vee Down]_a \\ &\wedge WF_a(Down) \\ &\wedge SF_a(UP) \end{aligned}$$

However, TLC *still* reports the same violation. What's going on?

If we take a closer look at the enabling condition for *Up*, it only requires current floor to be not the *top floor*. When the elevator is stuck in a loop going Up and Down between 1F and 2F indefinitely, strong fairness for Up is *already satisfied*. What we really want is strong fairness on *Up* for *every floor*, instead

of *any floor except top floor*. So if elevator makes to 2F once, it will *always eventually* go to 3F. If elevator makes to 3F once, it will *always eventually* go to 4F, so on and so forth. The following is the change required:

$$\begin{aligned}
 Spec &\triangleq \\
 &\wedge Init \\
 &\wedge \Box [Up \vee Down]_a \\
 &\wedge WF_a(Down) \\
 &\wedge \forall f \in BOTTOM \dots TOP - 1 : \\
 &\quad \wedge WF_a(Up \wedge f = a)
 \end{aligned}$$

Once again with this change TLC will pass.

Chapter 11

General Tips

11.1 Model Checker Debug

Debugging in TLC is a bit different than debugging with normal programs. A step in the model checker is really a state transition. Even if the model checker completes, it's still worthwhile to dump and audit the states just to make sure the Spec is defined correctly.

```
tlc elevator -dump out > /dev/null && cat out.dump | head -n5
State 1:
a = 1
State 2:
a = 2
```

You may want to grep the output to look for state being set to certain values to confirm the Spec is working as intended.

11.1.1 Dead Lock

Deadlock typically happens when the model checker ran out of things to do. This is typically a result of an incomplete Spec definition, where certain edge cases were not accounted for. The model checker typically provides a fairly comprehensive backtrace leading up to the dead lock to simplify debug.

11.1.2 Live Lock

Livelock happens when the model checker identifies a case where the liveness property is violated. An example is the elevator stuck going between two floors instead of keep going to the top floor, or the system is stuck dropping and re-transmitting the same packet.

These are typically fixed by providing additional fairness description to the Spec, telling the model checker how continue in the case of a live lock.

For a detail fairness description please refer to Chapter 10.

11.2 Model Refinement

This is, in some sense, the *art* associated with writing model checker verifiable TLA+ spec. Model checking is only valuable if it can be verified within a reasonable amount of time. Since the model complexity grows exponentially, there's little value in attempting to hyper-optimize the details. Designer should focus on optimizing the broad stroke, such as removing features that are harder to get wrong, and focus the model on the bits that have the highest return on investment.

One useful way of trimming out low value portion of the Spec is to audit the state dump. Even in the case of a non-terminating run, a partial state dump can help identify low value details we can remove from the Spec.

One key value of TLA+ is it highlights all the corner cases in the system. Even if you end up removing certain details from the Spec, it still likely highlights to you certain condition you were unaware of.

As a broad stroke principle: when the Spec has millions or higher more states, it is unlikely to terminate within a few seconds. From first principles if you can find one failure case in a million states, you can also likely reduce the scope of the model to reproduce the failure in much fewer states.

Chapter 12

Abstraction Guideline

Chapter 13

Reference

Bibliography

- [1] <https://lamport.azurewebsites.net/tla/book.html>
- [2] Srikumar Subramanian <https://sriku.org/posts/fairness-in-tlaplus/>, 2015
- [3] Richard M. Murray, Nok Wongpiromsarn *Linear Temporal Logic, Lecture 3*, 2012
- [4] <https://www.backblaze.com/blog/cloud-storage-durability/>
- [5] <https://raft.github.io/raft.pdf>
- [6] <https://github.com/ongardie/raft.tla>
- [7] <https://github.com/tlaplus/tlaplus>
- [8] <https://ahelwer.ca/post/2023-11-01-tla-finite-monotonic/>
- [9] https://en.wikipedia.org/wiki/C10k_problem