UNIVERSITÉ DE LORRAINE

École doctorale IAEM Lorraine

Formal Verification of Distributed Algorithms using Distributed-PlusCal

Report

soutenu le 23 septembre 2016

A thesis submitted to obtain a

Master de l'Université de Lorraine

(mention informatique)

by

Heba Al-kayed

Composition du jury

Président :	Le président
Rapporteurs :	Le rapporteur 1 Le rapporteur 2 Le rapporteur 3
Examinateurs :	L'examinateur 1 L'examinateur 2

Laboratoire Lorrain de Recherche en Informatique et ses Applications — UMR 7503

Mis en page avec la classe thesul.

Remerciements

Les remerciements.

Je dédie cette thèse
à ma machine.
Oui, à Pandore,
qui fut la première de toutes.

Summary

1

Introduction

- Model checking is a verification method that is automatic and model-based(system is represented by a model, a specification is represented as a formula and we check whether the model satisfies the formula ==> if not we have counter models), it is intended to be used for concurrent systems.

- distributed system bugs are difficult to find by testing, they tend to be non-reproducible or not covered by test-cases.

- TLA+ -

2

Background info

This chapter is an overview of TLA+ and PlusCal.

2.1 TLA$^+$

TLA$^+$ is a formal specification language in which algorithms and systems can be described at a high level of abstraction and can be formally verified using the model checker TLC or the interactive proof assistant TLAPS. TLA$^+$ is based on mathematical set theory for describing data structures in terms of sets and functions, and on the Temporal Logic of Actions TLA for specifying their executions as state machines. TLA$^+$ specifications usually have the form

$$Init \wedge \Box[Next]_{vars} \wedge L$$

where *Init* is a predicate describing the possible initial states, *Next* is a predicate that constrains the possible state transitions, *vars* is the tuple of all state variables that appear in the specification, and L is a liveness or fairness property expressed as a formula of temporal logic. Transition formulas such as *Next*, also called *actions*, are at the core of TLA$^+$, and represent instantaneous state changes. They contain unprimed state variables denoting the value of the variable before the transition as well as primed state variables that denote the value after the transition.

For example, figure 2.1 shows a TLA$^+$ specification of a simple memory. It declares four constant parameters *Address*, *Value*, *InitValue*, and *NoValue*, and states a hypothesis on the values that these parameters can be instantiated with. The state space of the specification is represented by the two variables *chan* and *mem*. Intuitively, *mem* holds the current memory, whereas *chan* is an output channel that reflects the result of the preceding operation.

The remainder of the TLA$^+$ module contains operator definitions that represent parts of the specification and of correctness properties. The state predicate *Init* fixes the initial values of the two variables. The actions $Read(a)$ and $Write(a, v)$ represent reading the value at memory address a and writing value v to memory address a, respectively. In this specification, the memory is modeled as a function mapping addresses to values. The TLA$^+$ expression $[x \in S \mapsto e]$ denotes the function with domain S such that every element x of S is mapped to e. This is reminiscent of a λ-expression but also makes explicit the domain of the function. Function application $f[x]$ is written using square brackets. Finally, the expression $[f \text{ EXCEPT } ![x] = e]$ denotes the function that is similar to f, except that argument x is mapped to e, one can think of it as a function overwrite.

The action *Next* defines the possible state transitions as the disjunction of *Read* and *Write* actions, and *Spec* represents the overall specification of the memory.

TLA$^+$ is an untyped language. Type correctness can be verified as a property of the specification. For our example, the predicate *TypeOK* indicates the possible values that the variables *chan* and *mem* are expected to hold at any state of the specification. Formally, the implication $Spec \Rightarrow \Box TypeOK$ can be established as a theorem.

```
---------------------------- MODULE SimpleMemory ----------------------------
CONSTANTS Address, Value, InitValue, NoValue

ASSUME
  /\ InitValue \in Value
  /\ NoValue \notin Value

VARIABLES chan, mem

\* initial condition
Init ==
  /\ chan = NoValue
  /\ mem = [a \in Address |-> InitValue]

\* transitions: reading and writing
Read(a) ==
  /\ chan' = mem[a]
  /\ mem' = mem

Write(a,v) ==
  /\ mem' = [mem EXCEPT ![a] = v]
  /\ chan' = NoValue

Next ==
  \/ \E a \in Address : Read(a)
  \/ \E a \in Address, v \in Value : Write(a,v)

\* overall specification
Spec == Init /\ [][Next]_<<chan,mem>>

\* predicate specifying type correctness
TypeOK ==
  /\ chan \in Value \cup {NoValue}
  /\ mem \in [Address -> Value]
=============================================================================
```

FIGURE 2.1 – A memory specification in TLA$^+$.

TLA+ is a formal specification language, that is designed to model digital systems, and verify them using tools like the TLC model checker.

The models are above the code level, they can be considered a part of the design phase, they are less concerned with the implementation details and are used to describe the possible executions of a system abstractly.

The importance of modeling systems specially concurrent and distributed systems is to make sure everything is working properly, working properly differs based on the system mentioned but it always means satisfying certain properties on individual executions, let's assume that by working properly we mean that the system should perform a certain task and generate a certain output, we can check that on some executions however, by using TLA+ we can check these properties on every possible execution.

TLA+ revolves around thinking abstractly about the algorithm that we want to model, it uses state machines to describe the systems, TLA+ achieves this by considering the system to be a sequence of steps, where is a step is a change from one state to the next. TLA+ describes a state as an assignment of values to variables.

TLA+ uses state machines to achieve abstraction, where a state machine is described by defining the variables, the possible initialization values for the variables, the relation between their values and the

current state as well as their possible values in the following state, where a state is the assignment of values to variables.

The listing 2.1 is the Semaphores example in TLA+, Semaphores are integer variables that are used to solve the critical section problem.

Some of the keywords used in the example are *EXTENDS* at line 5 which is used to import a TLA+ standard library, *VARIABLES* at line 12 defines our variables as they must be defined before they are used, *CONSTANT* is used to define constants that are substituted for during modeling, constants maintain the same value through every execution.

ProcSet at line 16 is a set with the number of processes. *Init* at line 19 initializes the defined variables.

start, enter, cs, exit are our actions or steps, they are the states where we assign values to our variables, they are represented as a TLA+ conjunction because a state is a formula rather than a sequence of commands.

The variable *pc* is defined and used as a program control variable to represent the control state, its main job is to handle the navigation from one action to the other, for example at line 35 it is used to check if the the *pc* variable value is "cs" and that the next value for the *pc* variable is "exit". Specifying the next value to be given to a variable is done by using the primed version of a variable, for example the next value for the variable *pc* is *pc'*.

The *EXCEPT* construct used in the next state value of a variable is provided by TLA+, since *pc* for example is a function whose domain consists of the elements of *ProcSet* and range is initially "start" for all, then *pc'= [pc EXCEPT ![self] = "exit"]* is a way of saying that we want to modify the function pc where the domain value is *[self]* to take the range value "exit" and leave the values for the other domain entries unchanged, which can also be written as

[x ∈ DOMAIN pc ⟼ if x = self then "exit" else pc[x]].

Spec is a conjunction of the initial predicate *Init* and the next-state relation *Next*. The *[][Next]_vars* at line 50 means that the transition is described by either *Next* or the values of *sem* and *pc* are unchanged which is known as a stuttering step.

Listing 2.1 – SemaphoreMutex in TLA+

```
1
2  ---------------------------- MODULE SemaphoreMutex ----------------------------
3
4  EXTENDS Naturals \* Import operators
5
6  CONSTANT N \* Value of N is the same through every behaviour
7
8  ASSUME N \in Nat
9
10 \* BEGIN TRANSLATION
11 VARIABLES sem, pc \* Define the varibales
12
13 vars == << sem, pc >> \* Sequence of variables
14
15 ProcSet == (1..N) \* Number of Processes
16
17 \* Possible Initialization for variables
18 Init == (* Global variables *)
19         /\ sem = 1
20         /\ pc = [self \in ProcSet |-> "start"]
21
```

```
\* algorithm starting point, set next step to "enter"
start(self) == /\ pc[self] = "start"
               /\ pc' = [pc EXCEPT ![self] = "enter"]
               /\ /\ UNCHANGED sem \* sem' = sem

\* in this step prepare to enter cs, next value of sem will be sem - 1
enter(self) == /\ pc[self] = "enter"
               /\ (sem > 0)
               /\ sem' = sem - 1
               /\ pc' = [pc EXCEPT ![self] = "cs"]

\* cs step, next step is to go to "exit" step
cs(self) == /\ pc[self] = "cs"
            /\ pc' = [pc EXCEPT ![self] = "exit"]
            /\ /\ UNCHANGED sem \*sem' = sem

\* set next value of sem to sem + 1 and next step to "start" again
exit(self) == /\ pc[self] = "exit"
              /\ sem' = sem + 1
              /\ pc' = [pc EXCEPT ![self] = "st"]

\* a disconjunction of the possible steps
p(self) == st(self) \/ enter(self) \/ cs(self) \/ exit(self)

\* a next state is possible for at least one process
Next == (\E self \in 1..N: p(self))

Spec == Init /\ [][Next]_vars

\* END TRANSLATION
=============================================================================
```

For More details on the syntax and grammer of TLA+, see **??**.

2.2 PlusCal algorithm language

PlusCal is a language used for writing algorithms, algorithm languages are responsible for describing algorithms rather than programs, the distinction here is that an algorithm is the program without an actual implementation.

An algorithm language is used to focus on the aspects of the algorithm like data manipulation rather than irrelevant and distracting details such as programming-language objects and data structures.

PlusCal can be used to describe both concurrent and sequential algorithms, it is based on TLA+ specification language, it was initially introduced to accompany TLA+ since TLA+ syntax may seem unfamiliar to most users, this enabled users to express their algorithms using a more familiar syntax. A PlusCal expression can be any TLA+ expression which make PlusCal more powerful and expressive than most algorithm languages like pseudo-code.

The TLA+ Toolbox can be used to translate PlusCal to the corresponding TLA+ code that is needed to check for the algorithm's correctness through the TLC model checker.

PlusCal offers two syntax styles one called c-syntax resembling c programming style and a clearer but longer p-syntax(p for pascal), we can find many familiar constructs like *if* statements and *while* statements. A language manual is available on the PlusCal Web site for both syntaxes.

PlusCal statements are placed within labels, labels are used to indicate atomicity between statements, where an atomic step starts at a label and ends at the next label, these atomic steps are translated into actions in TLA+.

The specification 2.2 below is for the Semaphores example we discussed earlier, the PlusCal algorithm is placed inside a comment within the tla file, denoted by *–algorithm* before the name of the algorithm at line 2. The TLA+ translation of this example is in listing 2.1.

Listing 2.2 – PlusCal

```
1  (**********************
2  --algorithm SemaphoreMutex{
3  variables sem = 1;
4
5  process(p \in 1..N)
6  {
7   start : while (TRUE){
8           enter : when (sem > 0);
9                   sem := sem - 1;
10              cs    : skip ;
11              exit  : sem := sem + 1 ;
12          }
13   }
14  }
15  ************************)
```

The overall translation strategy is explained here [Lam09].

// maybe mention procedures and macros

3

Related work

There have been other PlusCal extensions, we will be mentioning **??**, a tool represented as a part of a master thesis, it aims to produce an implementation in Go(C based language developed by Google) based on a PlusCal/TLA+ specification.

3.1 PGO

PGo is a source to source compiler written in Java. It compiles specifications written in an extension of PlusCal, called Modular PlusCal to Go programs, PGo can compile Modular PlusCal to PlusCal, PlusCal to Go, and Modular PlusCal to Go.

3.1.1 Modular PlusCal

Modular PlusCal is an extension of PlusCal, using Modular PlusCal the user can separate the specification into two components, a system functionality specification concerned with what the algorithm is supposed to achieve and an environment specification concerned about how we may want it achieved.

For example, if we consider a server/client based communication system, the system functionality can be a client requesting services, this is called system functionality, which is not related to how the client is requesting that service via a TCP connection for example, this is called an environment specification. Another added value for this separation is that the programmer can reuse concept defined in one specification in another specification since the environment specification isn't dependent on the functionality of the system.

Modular PlusCal introduced Architypes, Mapping Macros, and Instances to achieve the modularization of the spec.

Architypes
They are considered to be the blue print of a PlusCal process, they are used to specify the system behaviours. They have the same semantics except for the inability to access global variables unless passed to the architypes as arguments.

Using the *ref* keyword before a global variable that is sent as an argument lets us know that this architype can modify it.

these restrictions provide the needed isolation between system and environment behaviours.

Mapping Macros They specify the environment, they define interfaces for reading and writing on a global variable that represents a network. like pluscal macros they cannot contain any labels inside them, all statements are apart of the same step.

Modeling mapping macros independently from system functionality allows the user to reuse the mapping macros.

Instances Instances are the glue that holds the archtypes and mapping macros together. instantiates a process or a group of processes using the specified architype, each argument passed is bound with a mapping macro to control read and write functions on it.

- show a smaller example or grammer

4

Distributed PlusCal

Distributed PlusCal is an extension of PlusCal, they are algorithm languages meant for writing algorithms not programs. they are both translated to TLA+.

Since distributed algorithms are based on continuous interactions among components, they benefit greatly from testing failure conditions like deadlocks or race conditions at early stages of development at design level, and TLA+ provides a flexibility and an expressiveness that makes it able to specify and verify those algorithms. One of the popular examples of incorporating TLA+ to verify distributed algorithms is its usage at Amazon Web Services [NRZ+15].

Our motivations for creating Disrtibuted PlusCal are quite similar to the motivations that created PlusCal, we wanted a syntax that would spare the user from having to model primitives that usually accompany distributed algorithms such as sub-processes and communication channels.

Since we extended the existing PluCal translator responsible for parsing PlusCal into TLA+ we inherited the same semantics and grammar and added our own which can be found in the figure below.

⟨ Process ⟩ ⊨ *process* (⟨ variable decleration ⟩)⟨ local-variables ⟩ ⟨ body ⟩{⟨ body ⟩}
⟨ local-variables ⟩ ⊨ Ø|*variables* ⟨declaration-list⟩ |*channels* ⟨declaration-list⟩ |*FIFOs* ⟨declaration-list⟩
⟨ declaration-list ⟩ ⊨ ⟨ variable-declaration ⟩ | ⟨ variable-declaration ⟩, ⟨ decleration-list⟩
⟨ body ⟩ ⊨ ⟨ labeled-statement-list ⟩

FIGURE 4.1 – Grammar for Distributed PlusCal

In the sections that follow we will be explaining what we implemented, why it is needed and how it is translated into TLA+, for this we will be doing a walk-through on the two phase commit example, the two phase commit is a protocol used for distributed transactions that consist of multiple operations, performed at multiple sites, the goal of it is to reach consensus between the different elements that carry out the transaction together such that if an element decides to abort all other elements abort as well and the transaction is rolled back, and in order to actually commit all elements must agree and be able to commit.

4.1 Communication Channels

PlusCal enables the user to define variables with TLA+ syntax, the variable types can be sets, sequence, sequence of sets etc,

- differentiate sets and sequences and mentions the operators of each with small examples

4.1.1 channels

-set based example with it's translation

4.1.2 FIFO channels

-sequence based example with it's translation

4.1.3 Supported channel functions

expected syntax and limitations - send, receive, broadcast, multicast, clear

4.2 Sub-Processes

A PlusCal process has a block that holds the body of the process, Distributed PlusCal gives each process the opportunity to define more than one block where each block has a body of labeled statements, This enables the process to be executing multiple tasks in parallel, for example a sub-process can be used to send date to other processes while another sub-process can be responsible for receiving data asynchronously, the programmer can divide tasks between sub-processes and give a sub-process a theme if needed, that is by dividing the algorithm into multiple sub-processes where each sub-process works independently, this is to some extent a form of modularization.

//i've tried saying this modularization thing in different ways by now not sure if the idea is clear or if this is even a 'big deal' for modeling a spec!

// more on the benefits of this for distributed algorithms especially

The body of a sub-process maintains the same syntax as the body of a PlusCal process, all the sub-processes share the same variables declared for the process, this makes communication between them possible if needed.

The example below shows the sub-processes are defined for the two phase commit algorithm, the example is written in c-syntax and the sub-processes are surrounded by curly braces.

Listing 4.1 – Distributed PlusCal Sub-Processes

```
1
2  (* PlusCal options (-distpcal) *)
3
4  (***
5  --algorithm TPC {
6
7    \* message channels
8    channels coord, agt[Agent];
9
10   fair process (a \in Agent)
11   variable aState = "unknown"; {
12
13 a1: if (aState = "unknown") {
14           with(st \in {"accept", "refuse"}) {
15             aState := st;
16             send(coord, [type |-> st, agent |-> self]);
17           };
18      };
19      a2: await(aState \in {"commit", "abort"})
20
21   } {
22
23      a3:await (aState # "unknown");
24         receive(agt[self], aState);
```

```
25
26      a4:clear(agt);
27    }
28
29    fair process (c = Coord)
30    variables cState = "unknown",
31              commits = {}, msg = {};
32               \* agents that agree to commit
33    {
34      c1: await(cState \in {"commit", "abort"});
35          broadcast(agt, [ag \in Agent|-> cState]);
36    } {
37
38       c2:while (cState \notin {"abort", "commit"}) {
39          receive(coord, msg);
40               if (msg.type = "refuse") {
41                    cState := "abort";
42               }
43               else if (msg.type = "accept") {
44                    commits := commits \cup {msg.agent};
45                     if (commits = Agent) {
46                        cState := "commit";
47                     }
48                 }
49          }
50    }
51   }
52 ***)
```

The first process consists of two sub-processes, the first one contains the labels (a1, a2) and the second one contains (a3, a4).

//The send, receive and clear and broadcast would've been explained already //in the previous section.

The variable *aState* is shared between the sub-processes, in fact it is used for communication between them, label a2 holds an *await* statement at line 19 that is waiting for aState to have the value of either *"commit"* or *"abort"*, the variable is being set to one of these values by a3 in the second sub-process by the receive function at line 24.

it's important to note that the sub-processes do not allow variable declarations they only use variables declared for the entire process.

4.2.1 TLA+ Translation

Defining sub-processes had some effects on the translation to TLA+, because when you declare sub-processes you are actually partitioning the process, so now whenever we are referring to a process we need to know not only which process it is but also which sub-process are we referring to.

The entire TLA+ translation of the two phase commit example can be found in appendix A.1, now we will be focusing on elements that we introduced to the general structure of the TLA+ file.

— **SubProcSet**

SubProcSet is the set of all the sub-process identifiers per process.

Listing 4.2 – TLA+ translation for Sub-Processes

```
1
```

```
ProcSet == (Agent) \cup {Coord}

SubProcSet == [n \in ProcSet |-> IF n \in Agent THEN 1..2
                                 ELSE (**Coord**) 1..2]
```

— **pc variable**

The *pc* variable in TLA+ that is used to indicate the current point of execution and the next statement to be executed with respect to a process, now it has to indicate also which sub-process is involved.
The pc variable is initialized to a sequence of actions depending on the type of the process, for example if *self* is in Agent, this means it's a process of type Agent that has the following actions associated with it (a1, a2, a3, a4), However, a1 is considered the entry point for the first sub-process and a3 for the second one. so we need to initialize pc variable to look something like this

Process Type	Sub-Process	Entry Point
Agent	1	a1
	2	a3
Coord	1	c1
	2	c2

In TLA+ a function with domain 1..n for some n in Nat is a sequence, so the pc values consist of sequences to represent the above table, so we initialize pc in the listing 4.3 to have pc[Agent] = <"a1", "a3"> and pc[Coord] = <"c1", "c2">.
//sequences and sets would've been explained in the previous section for the channels

Listing 4.3 – TLA+ translation for Sub-Processes

```

Init == (* Global variables *)
        /\ coord = {}
        /\ agt = [a0 \in Agent |-> {}]
        (* Node a *)
        /\ aState = [self \in Agent |-> "unknown"]
        (* Node c *)
        /\ cState = "unknown"
        /\ commits = {}
        /\ msg = {}
        /\ pc = [self \in ProcSet |-> CASE self \in Agent -> <<"a1","a3">>
                                       [] self = Coord -> <<"c1","c2">>]
```

The example in listing 4.4 shows how the *pc* variable is used, the second pair of brackets that is added when accessing the *pc* variable is used to indicate the sub-process, at line 3 we check that the sub-process is currently at this action, then at line 10 we specify that the next action to be executed for the sub-process is action a2.

Listing 4.4 – TLA+ translation for Sub-Processes

```

\* Process 1 Sub-Process 1 : an action with the statements in a1 label
a1(self) == /\ pc[self] [1] = "a1"
            /\ IF aState[self] = "unknown"
                  THEN /\ \E st \in {"accept", "refuse"}:
                            /\ aState' = [aState EXCEPT ![self] = st]
                            /\ coord' = (coord \cup {[type |-> st, agent
```

```
                                |-> self]})
8                     ELSE /\ TRUE
9                          /\ UNCHANGED << coord, aState >>
10                /\ pc' = [pc EXCEPT ![self] = [@  EXCEPT ![1] = "a2"]]
11                /\ UNCHANGED << agt, cState, commits, msg >>
```

5

Code Documentation

5.1 general structure of the toolbox and it's components

try to describe the general flow

5.2 parsing and expansion process

5.3 some software-based diagram

or maybe an AST description graph

6

Conclusion and future work

Appendices

A

Distributed PlusCal to TLA+ Examples

A.1 Two Phase Commit

Listing A.1 – TLA+ translation for Sub-Processes

```
1
2  ------------------------------ MODULE 2pc ------------------------------
3  EXTENDS Sequences, Naturals
4
5  CONSTANTS Coord, Agent
6
7  State == {"unknown", "accept", "refuse", "commit", "abort"}
8
9
10 (* PlusCal options (-distpcal) *)
11
12 (***
13 --algorithm TPC {
14
15   \* message channels
16   channels coord, agt[Agent];
17
18   fair process (a \in Agent)
19   variable aState = "unknown"; {
20
21 a1: if (aState = "unknown") {
22         with(st \in {"accept", "refuse"}) {
23           aState := st;
24           send(coord, [type |-> st, agent |-> self]);
25         };
26     };
27     a2: await(aState \in {"commit", "abort"})
28
29   } {
30
31     a3:await (aState # "unknown");
32        receive(agt[self], aState);
33
34     a4:clear(agt);
35   }
```

```
36
37    fair process (c = Coord)
38    variables cState = "unknown",
39              commits = {}, msg = {};
40               \* agents that agree to commit
41    {
42      c1: await(cState \in {"commit", "abort"});
43          broadcast(agt, [ag \in Agent|-> cState]);
44    } {
45
46       c2:while (cState \notin {"abort", "commit"}) {
47          receive(coord, msg);
48              if (msg.type = "refuse") {
49                  cState := "abort";
50              }
51              else if (msg.type = "accept") {
52                  commits := commits \cup {msg.agent};
53                   if (commits = Agent) {
54                      cState := "commit";
55                   }
56                }
57          }
58    }
59   }
60  ***)
61  \* BEGIN TRANSLATION
62  VARIABLES coord, agt, pc, aState, cState, commits, msg
63
64  vars == << coord, agt, pc, aState, cState, commits, msg >>
65
66  ProcSet == (Agent) \cup {Coord}
67
68  SubProcSet == [n \in ProcSet |-> IF n \in Agent THEN 1..2
69                                   ELSE (**Coord**) 1..2]
70
71  Init == (* Global variables *)
72          /\ coord = {}
73          /\ agt = [a0 \in Agent |-> {}]
74          (* Node a *)
75          /\ aState = [self \in Agent |-> "unknown"]
76          (* Node c *)
77          /\ cState = "unknown"
78          /\ commits = {}
79          /\ msg = {}
80          /\ pc = [self \in ProcSet |-> CASE self \in Agent -> <<"a1","a3">>
81                                          [] self = Coord -> <<"c1","c2">>]
82
83  a1(self) == /\ pc[self] [1] = "a1"
84              /\ IF aState[self] = "unknown"
85                    THEN /\ \E st \in {"accept", "refuse"}:
86                              /\ aState' = [aState EXCEPT ![self] = st]
87                              /\ coord' = (coord \cup {[type |-> st, agent |->
                                    self]})
88                    ELSE /\ TRUE
89                         /\ UNCHANGED << coord, aState >>
90              /\ pc' = [pc EXCEPT ![self] = [@  EXCEPT ![1] = "a2"]]
91              /\ UNCHANGED << agt, cState, commits, msg >>
92
```

```
93  a2(self) == /\ pc[self] [1] = "a2"
94              /\ (aState[self] \in {"commit", "abort"})
95              /\ pc' = [pc EXCEPT ![self] = [@  EXCEPT ![1] = "Done"]]
96              /\ UNCHANGED << coord, agt, aState, cState, commits, msg >>
97
98  a3(self) == /\ pc[self] [2] = "a3"
99              /\ (aState[self] # "unknown")
100             /\ \E a1519 \in agt[self]:
101                  /\ aState' = [aState EXCEPT ![self] = a1519]
102                  /\ agt' = [agt EXCEPT ![self] = agt[self] \ {a1519}]
103             /\ pc' = [pc EXCEPT ![self] = [@  EXCEPT ![2] = "a4"]]
104             /\ UNCHANGED << coord, cState, commits, msg >>
105
106 a4(self) == /\ pc[self] [2] = "a4"
107             /\ agt' = [a0 \in Agent |-> {}]
108             /\ pc' = [pc EXCEPT ![self] = [@  EXCEPT ![2] = "Done"]]
109             /\ UNCHANGED << coord, aState, cState, commits, msg >>
110
111 a(self) == a1(self) \/ a2(self) \/ a3(self) \/ a4(self)
112
113 c1 == /\ pc[Coord] [1] = "c1"
114       /\ (cState \in {"commit", "abort"})
115       /\ agt' = [ag \in Agent |-> agt[ag] \cup  {cState} ]
116       /\ pc' = [pc EXCEPT ![Coord] = [@  EXCEPT ![1] = "Done"]]
117       /\ UNCHANGED << coord, aState, cState, commits, msg >>
118
119 c2 == /\ pc[Coord] [2] = "c2"
120       /\ IF cState \notin {"abort", "commit"}
121             THEN /\ \E c1512 \in coord:
122                       /\ coord' = coord \ {c1512}
123                       /\ msg' = c1512
124                  /\ IF msg'.type = "refuse"
125                        THEN /\ cState' = "abort"
126                             /\ UNCHANGED commits
127                        ELSE /\ IF msg'.type = "accept"
128                                   THEN /\ commits' = (commits \cup {msg'.agent})
129                                        /\ IF commits' = Agent
130                                              THEN /\ cState' = "commit"
131                                              ELSE /\ TRUE
132                                                   /\ UNCHANGED cState
133                                   ELSE /\ TRUE
134                                        /\ UNCHANGED << cState, commits >>
135                  /\ pc' = [pc EXCEPT ![Coord] = [@  EXCEPT ![2] = "c2"]]
136             ELSE /\ pc' = [pc EXCEPT ![Coord] = [@  EXCEPT ![2] = "Done"]]
137                  /\ UNCHANGED << coord, cState, commits, msg >>
138       /\ UNCHANGED << agt, aState >>
139
140 c == c1 \/ c2
141
142 (* Allow infinite stuttering to prevent deadlock on termination. *)
143 Terminating == /\ \A self \in ProcSet : \A sub \in SubProcSet[self]:
        pc[self][sub] = "Done"
144                /\ UNCHANGED vars
145
146 Next == c
147           \/ (\E self \in Agent: a(self))
148           \/ Terminating
149
```

```
Spec == /\ Init /\ [][Next]_vars
        /\ \A self \in Agent : WF_vars(a(self))
        /\ WF_vars(c)

Termination == <>(\A self \in ProcSet: \A sub \in SubProcSet[self] :
    pc[self][sub] = "Done")

\* END TRANSLATION
=============================================================================
```

In the translation above, every label is transformed into an action, some actions are also created when needed, for example the receive function and the clear function in process 1 sub-process 2 both modify the same channel and it would be wrong to place the two assignments in the same atomic step thus an auxiliary action is created to hold the body of the clear function.

- insert labels in example, before await and also for receive and clear then modify the example

A.2 Lamport Mutex

Bibliographie

[Lam09] Leslie Lamport. The pluscal algorithm language. volume 5684, pages 36–60, 08 2009.

[NRZ+15] Chris Newcombe, Tim Rath, Fan Zhang, Bogdan Munteanu, Marc Brooker, and Michael Deardeuff. How amazon web services uses formal methods. *Communications of the ACM*, 58 :66–73, 03 2015.