Abortable Linearizable Modules

Rachid Guerraoui  Viktor Kuncak  Giuliano Losa

May 27, 2015

Abstract

We define the Abortable Linearizable Module automaton (ALM for short) and prove its key composition property using the IOA theory of HOLCF. The ALM is at the heart of the Speculative Linearizability framework. This framework simplifies devising correct speculative algorithms by enabling their decomposition into independent modules that can be analyzed and proved correct in isolation. It is particularly useful when working in a distributed environment, where the need to tolerate faults and asynchrony has made current monolithic protocols so intricate that it is no longer tractable to check their correctness. Our theory contains a typical example of a refinement proof in the I/O-automata framework of Lynch and Tuttle.

Contents

1 Introduction 2

2 Definition and properties of the longest common postfix of a set of lists 3

3 The ALM Automata specification 3

4 Proof that the composition of two instances of the ALM automaton behaves like a single instance of the ALM automaton 7
  4.1 A case split useful in the proofs 7
  4.2 Invariants of a single ALM instance 8
  4.3 Invariants of the composition of two ALM instances 9
  4.4 Proofs of invariance 10
  4.5 The refinement proof 12

5 Conclusion 12
1 Introduction

Linearizability [2] is a key design methodology for reasoning about implementations of concurrent abstract data types in both shared memory and message passing systems. It presents the illusion that operations execute sequentially and fault-free, despite the asynchrony and faults that are often present in a concurrent system, especially a distributed one.

However, devising complete linearizable objects is very difficult, especially in the presence of process crashes and asynchrony, requiring complex algorithms (such as Paxos [3]) to work correctly under general circumstances, and often resulting in bad average-case behavior. Concurrent algorithm designers therefore resort to speculation, i.e. to optimizing existing algorithms to handle common scenarios more efficiently. More precisely, a speculative systems has a fall-back mode that works in all situations and several optimization modes, each of which is very efficient in a particular situation but might not work at all in some other situation. By observing its execution, a speculative system speculates about which particular situation it will be subject to and chooses the most efficient mode for that situation. If speculation reveals wrong, a new speculation is made in light of newly available observations. Unfortunately, building speculative system ad-hoc results in protocols so complex that it is no longer tractable to prove their correctness.

We present an I/O-automaton [4] specification, called ALM (a shorthand for Abortable Linearizable Module), which can be used to build a speculative linearizable algorithm out of independent modules that implement the different modes of the speculative algorithm. The ALM is at the heart of the Speculative Linearizability framework [1].

The ALM automaton produces traces that are linearizable with respect to a generic type of object. Moreover, the composition of two instances of the ALM automaton behaves like a single instance. Hence it is guaranteed that the composition of any number of instances of the ALM automaton is linearizable.

The properties stated above greatly simplify the development and analysis of speculative systems: Instead of having to reason about an entanglement of complex protocols, one can devise several modules with the property that, when taken in isolation, each module refines the ALM automaton. Hence complex protocols can be divided into smaller modules that can be analyzed independently of each other. In particular, it allows to optimize an existing protocol by creating separate optimization modules, prove each optimization correct in isolation, and obtain the correctness of the overall protocol from the correctness of the existing one.

In this document we define the ALM automaton and prove the Composition Theorem, which states that the composition of two instances of the ALM automaton behaves as a single instance of the ALM automaton. We use a refinement mapping to establish this fact.
2 Definition and properties of the longest common postfix of a set of lists

definition common-postfix-p :: ('a list) set => 'a list => bool
  — Predicate that recognizes the common postfix of a set of lists
  — The common postfix of the empty set is the empty list
  where
  common-postfix-p ≡ λ xss xs . if xss = {} then xs = [] else ALL xs' . xs' ∈ xss
                        — suffixeq xs xs'

definition l-c-p-pred :: 'a list set => 'a list => bool
  — Predicate that recognizes the longest common postfix of a set of lists
  where
  l-c-p-pred ≡ λ xss xs . common-postfix-p xss xs ∧ (ALL xs' . common-postfix-p xss xs' — suffixeq xs' xs)

definition l-c-p :: 'a list set => 'a list
  — The longest common postfix of a set of lists
  where
  l-c-p ≡ λ xss . THE xs . l-c-p-pred xss xs

lemma l-c-p-ok: l-c-p-pred xss (l-c-p xss)
  — Proof that the definition of the longest common postfix of a set of lists is consistent

lemma l-c-p-lemma:
  — A useful lemma
  (ls ≠ {} ∧ (∀ l ∈ ls . (∃ l'. l = l' @ xs))) —> suffixeq xs (l-c-p ls)

lemma l-c-p-common-postfix: common-postfix-p xss (l-c-p xss)
  ⟨proof⟩

lemma l-c-p-longest: common-postfix-p xss xs —> suffixeq xs (l-c-p xss)
  ⟨proof⟩

end

3 The ALM Automata specification

definition common-postfix-p :: ('a list) set => 'a list => bool
  — Predicate that recognizes the common postfix of a set of lists
  — The common postfix of the empty set is the empty list
  where
  common-postfix-p ≡ λ xss xs . if xss = {} then xs = [] else ALL xs' . xs' ∈ xss
                        — suffixeq xs xs'

definition l-c-p-pred :: 'a list set => 'a list => bool
  — Predicate that recognizes the longest common postfix of a set of lists
  where
  l-c-p-pred ≡ λ xss xs . common-postfix-p xss xs ∧ (ALL xs' . common-postfix-p xss xs' — suffixeq xs' xs)

definition l-c-p :: 'a list set => 'a list
  — The longest common postfix of a set of lists
  where
  l-c-p ≡ λ xss . THE xs . l-c-p-pred xss xs

lemma l-c-p-ok: l-c-p-pred xss (l-c-p xss)
  — Proof that the definition of the longest common postfix of a set of lists is consistent

lemma l-c-p-lemma:
  — A useful lemma
  (ls ≠ {} ∧ (∀ l ∈ ls . (∃ l'. l = l' @ xs))) —> suffixeq xs (l-c-p ls)

lemma l-c-p-common-postfix: common-postfix-p xss (l-c-p xss)
  ⟨proof⟩

lemma l-c-p-longest: common-postfix-p xss xs —> suffixeq xs (l-c-p xss)
  ⟨proof⟩

end
— A non-empty set of clients
typedec\ue200d\ue200d data
— Data contained in requests
datatype \text{request} =
— A request is composed of a sender and data
\text{Req} \text{client} \text{data}
definition \text{request-snd} :: \text{request} \Rightarrow \text{client}
where \text{request-snd} \equiv \lambda r. \text{case} r \text{of} \text{Req} c - \Rightarrow c
type-synonym \text{hist} = \text{request list}
— Type of histories of requests.
datatype \text{ALM-action} =
— The actions of the ALM automaton
\text{Invoke} \text{client} \text{request}
\mid \text{Commit} \text{client} \text{nat} \text{hist}
\mid \text{Switch} \text{client} \text{nat} \text{hist} \text{request}
\mid \text{Initialize} \text{nat} \text{hist}
\mid \text{Linearize} \text{nat} \text{hist}
\mid \text{Abort} \text{nat}
datatype \text{phase} = \text{Sleep} \mid \text{Pending} \mid \text{Ready} \mid \text{Aborted}
— Executions phases of a client
definition \text{linearizations} :: \text{request} \text{set} \Rightarrow \text{hist} \text{set}
— The possible linearizations of a set of requests
where \text{linearizations} \equiv \lambda \text{reqs}. \{ h . \text{set} h \subseteq \text{reqs} \wedge \text{distinct} h \}
definition \text{postfix-all} :: \text{hist} \Rightarrow \text{hist} \text{set} \Rightarrow \text{hist} \text{set}
— appends to the right the first argument to every member of the history set
where \text{postfix-all} \equiv \lambda h \text{hs}. \{ h' . \exists h''. h' = h'' \circ h \wedge h'' \in hs \}
definition \text{ALM-asig} :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{ALM-action signature}
— The action signature of ALM automata
— Input actions, output actions, and internal actions
where \text{ALM-asig} \equiv \lambda \text{id1} \text{id2}. (\{ \text{act} . \exists c r h .
\mid \text{act} = \text{Invoke} c r \mid \text{act} = \text{Switch} c \text{id1} h r\}, \{ \text{act} . \exists c h r \text{id}' .
\mid \text{id1} \leq \text{id}' \land \text{id}' < \text{id2} \land \text{act} = \text{Commit} c \text{id}' h
\mid \text{act} = \text{Switch} c \text{id2} h r\}, \{ \text{act} . \exists h .
\mid \text{act} = \text{Abort} \text{id1}
\mid \text{act} = \text{Linearize} \text{id1} h\})
record ALM-state =
    — The state of the ALM automata
    pending :: client ⇒ request
    — Associates a pending request to a client process
    initHists :: hist set
    — The set of init histories submitted by clients
    phase :: client ⇒ phase
    — Associates a phase to a client process
    hist :: hist
    — Represents the chosen linearization of the concurrent history of the current instance only
    aborted :: bool
    initialized :: bool

definition pendingReqs :: ALM-state ⇒ request set
    — the set of requests that have been invoked but that are not yet in the hist parameter
where
    pendingReqs ≡ λ s . { r . ∃ c .
        r = pending s c
        ∧ r ∉ set (hist s)
        ∧ phase s c ∈ {Pending, Aborted} }

definition initValidReqs :: ALM-state ⇒ request set
    — any request that appears in an init hist after the longest common prefix or that is pending
where
    initValidReqs ≡ λ s . { r .
        ( r ∈ pendingReqs s ∨ (∃ h ∈ initHists s . r ∈ set h))
        ∧ r ∉ set (l-c-p (initHists s)) }

definition ALM-trans :: nat ⇒ nat ⇒ (ALM-action, ALM-state)transition set
    — the transitions of the ALM automaton
where
    ALM-trans ≡ λ id1 id2 . { trans .
        let s = fst trans; s' = snd (snd trans); a = fst (snd trans) in
        case a of Invoke c r ⇒
            if phase s c = Ready ∧ request-snd r = c ∧ r ∉ set (hist s)
            then s' = s[(pending := (pending s)(c := r)),
                  phase := (phase s)(c := Pending)]
            else s' = s
        | Linearize i h ⇒
            initialized s ∧ ¬ aborted s
            ∧ h ∈ postfix-all (hist s) (linearizations (pendingReqs s ))
    )
\[ s' = s[\text{hist} := h] \]

| Initialize i h ⇒
| (\exists c . \text{phase} \ s \ c \neq \text{Sleep}) \land \neg \text{aborted} \ s \land \neg \text{initialized} \ s
| \land h \in \text{postfix-all} \ (l-c-p \ (\text{initHists} \ s)) \ (\text{linearizations} \ (\text{initValidReqs} \ s))
| \land s' = s[\text{hist} := h, \text{initialized} := \text{True}] |

| Abort i ⇒
| \neg \text{aborted} \ s \land (\exists c . \text{phase} \ s \ c \neq \text{Sleep})
| \land s' = s[\text{aborted} := \text{True}] |

| Commit c i h ⇒
| \text{phase} \ s \ c = \text{Pending} \land \text{pending} \ s \ c \in \text{set} \ (\text{hist} \ s)
| \land h = \text{dropWhile} \ (\lambda r . r \neq \text{pending} \ s \ c) \ (\text{hist} \ s)
| \land s' = s[\text{phase} := (\text{phase} \ s)(c := \text{Ready})] |

| Switch c i h r ⇒
| if i = id1
| then if \text{phase} \ s \ c = \text{Sleep}
| then s' = s[\text{initHists} := \{h\} \cup (\text{initHists} \ s), \text{phase} := (\text{phase} \ s)(c := \text{Pending}), \text{pending} := (\text{pending} \ s)(c := r)]
| else s' = s
| else if i = id2
| then \text{aborted} \ s
| \land \text{phase} \ s \ c = \text{Pending} \land r = \text{pending} \ s \ c
| \land (\text{if initialized} \ s)
| then (h \in \text{postfix-all} \ (\text{hist} \ s) \ (\text{linearizations} \ (\text{pendingReqs} \ s)))
| else (h \in \text{postfix-all} \ (l-c-p \ (\text{initHists} \ s)) \ (\text{linearizations} \ (\text{initValidReqs} \ s)))
| \land s' = s[\text{phase} := (\text{phase} \ s)(c := \text{Aborted})] |
| else False |

**definition** \text{ALM-start} :: nat ⇒ ALM-state set

— the set of start states

**where**
\text{ALM-start} ≡ \lambda \ id . \{ s .
\forall c . \text{phase} \ s \ c = (\text{if id} \neq 0 \ then \text{Sleep} \ else \text{Ready})
\land \text{hist} \ s = []
\land \neg \text{aborted} \ s
\land (\text{if id} \neq 0 \ then \neg \text{initialized} \ s \ else \text{initialized} \ s)
\land \text{initHists} \ s = [] \}

**definition** \text{ALM-ioa} :: nat ⇒ nat ⇒ (ALM-action, ALM-state)ioa

— The ALM automaton

**where**
\text{ALM-ioa} ≡ \lambda (id1::nat) \ id2 .
(ALM-asig id1 \ id2, ALM-start \ id1,
type-synonym compo-state = ALM-state × ALM-state

definition composeALMs :: nat ⇒ nat ⇒ (ALM-action, compro-state) ioa
— the composition of two ALMs

where
composeALMs ≡ λ id1 id2.
  hide (ALM-ioa 0 id1 || ALM-ioa id1 id2)
  {act . EX c tr r . act = Switch c id1 tr r}

end

4 Proof that the composition of two instances of
the ALM automaton behaves like a single instance of the ALM automaton

theory CompositionCorrectness
imports ALM
begin

declare split-if-asm [split]
declare Let-def [simp]

4.1 A case split useful in the proofs

definition in-trans-cases-fun :: nat => nat => (ALM-state * ALM-state) =>
(AML-state * ALM-state) => bool
— Helper function used to decompose proofs

where
in-trans-cases-fun == % id1 id2 s t .
  (EX ca ra. (fst s, Invoke ca ra, fst t) : ALM-trans 0 id1 & (snd s, Invoke ca ra, snd t) : ALM-trans id1 id2)
  | (EX ca h ra. (fst s, Switch ca id1 h ra, fst t) : ALM-trans 0 id1 & (snd s, Switch ca id1 h ra, snd t) : ALM-trans id1 id2)
  | (EX c id' h. fst t = fst s & (snd s, Commit c id' h, snd t) : ALM-trans id1 id2 & id1 <= id' & id' < id2)
  | (EX c h r. fst t = fst s & (snd s, Switch c id2 h r, snd t) : ALM-trans id1 id2)
  | (EX h. fst t = fst s & (snd s, Linearize id1 h, snd t) : ALM-trans id1 id2)
  | (fst t = fst s & (snd s, Abort id1, snd t) : ALM-trans id1 id2)
  | (EX h. fst t = fst s & (snd s, Initialize id1 h, snd t) : ALM-trans id1 id2)
  | (EX ca ta ra. (fst s, Switch ca 0 ta ra, fst t) : ALM-trans 0 id1 & snd t = snd s)
  | (EX ca id' h. (fst s, Commit ca id' h, fst t) : ALM-trans 0 id1 & snd t = snd s & id' < id1)
  | (EX h. (fst s, Linearize 0 h, fst t) : ALM-trans 0 id1 & snd t = snd s)
  | (EX h. (fst s, Initialize 0 h, fst t) : ALM-trans 0 id1 & snd t = snd s)
lemma composeALMsE:
— A rule for decomposing proofs
assumes id1 ∼= 0 and id1 < id2 and in-trans-comp:s −(a::ALM-action)−− composeALMs id1 id2−> t
shows decom: in-trans-cases-fun id1 id2 s t
(proof)

lemma my-rule1:id1 ∼= 0; id1 < id2; s −a−− composeALMs id1 id2−> t;
[in-trans-cases-fun id1 id2 s t] == P ==⇒ P ⟨proof⟩
lemma my-rule2:0 < id1; id1 < id2; s −a−− composeALMs id1 id2−> t;
[in-trans-cases-fun id1 id2 s t] ==⇒ P ==⇒ P ⟨proof⟩

4.2 Invariants of a single ALM instance

definition P1a :: (ALM-state ∗ ALM-state) ⇒ bool
where
— In ALM 1, a pending request of client c has client c as sender
P1a == % s . let s1 = fst s; s2 = snd s in
   ALL c . phase s1 c ∈ {Pending, Aborted} −→ request-snd (pending s1 c) = c

definition P1b :: (ALM-state ∗ ALM-state) ⇒ bool
where
— In ALM 2, a pending request of client c has client c as sender
P1b == % s . let s1 = fst s; s2 = snd s in
   ALL c . phase s2 c = Sleep −→ request-snd (pending s2 c) = c

definition P2 :: (ALM-state ∗ ALM-state) ⇒ bool
where
P2 == % s . let s1 = fst s; s2 = snd s in
   (∀ c . phase s2 c = Sleep) −→ (¬ initialized s2 ∧ hist s2 = [])

definition P3 :: (ALM-state ∗ ALM-state) ⇒ bool
where
P3 == % s . let s1 = fst s; s2 = snd s in
   ∀ c . (phase s2 c = Ready −→ initialized s2)

definition P4 :: (ALM-state ∗ ALM-state) ⇒ bool
where
— The set of init histories of ALM 2 is empty when no client ever invoked anything
P4 == % s . let s1 = fst s; s2 = snd s in
   (∀ c . phase s2 c = Sleep) = (initHists s2 = { })

definition P5 :: (ALM-state ∗ ALM-state) ⇒ bool
— In ALM 1 a client never sleeps
where
P5 == % s . let s1 = fst s; s2 = snd s in
   ∀ c . phase s1 c ≠ Sleep
4.3 Invariants of the composition of two ALM instances

definition \( P6 : (\text{ALM-state} \times \text{ALM-state}) \Rightarrow \text{bool} \)  
— Non-interference across instances  
where  
\[ P6 \equiv \% s . \text{let } s1 = \text{fst } s; s2 = \text{snd } s \text{ in} \]  
\[ \sim \text{aborted } s1 \longrightarrow (\text{ALL } c . \text{phase } s2 c = \text{Sleep}) \wedge (\text{ALL } c . \text{phase } s1 c \sim \text{Aborted} = (\text{phase } s2 c = \text{Sleep})) \]

definition \( P7 : (\text{ALM-state} \times \text{ALM-state}) \Rightarrow \text{bool} \)  
— Before initialization of the ALM 2, pending requests are the same as in ALM 1 and no new requests may be accepted (phase is not Ready)  
where  
\[ P7 \equiv \% s . \text{let } s1 = \text{fst } s; s2 = \text{snd } s \text{ in} \]  
\[ \text{ALL } c . \text{phase } s1 c = \text{Aborted} \wedge \sim \text{initialized } s2 \longrightarrow (\text{pending } s2 c = \text{pending } s1 c \wedge \text{phase } s2 c \in \{\text{Pending}, \text{Aborted}\}) \]

definition \( P8 : (\text{ALM-state} \times \text{ALM-state}) \Rightarrow \text{bool} \)  
— Init histories of ALM 2 are built from the history of ALM 1 plus pending requests of ALM 1  
where  
\[ P8 \equiv \% s . \text{let } s1 = \text{fst } s; s2 = \text{snd } s \text{ in} \]  
\[ \forall h \in \text{initHists } s2 . h \in \text{postfix-all } (\text{hist } s1) \text{ (linearizations (pendingReqs } s1)) \]

definition \( P9 : (\text{ALM-state} \times \text{ALM-state}) \Rightarrow \text{bool} \)  
— ALM 2 does not abort before ALM 1 aborts  
where  
\[ P9 \equiv \% s . \text{let } s1 = \text{fst } s; s2 = \text{snd } s \text{ in} \]  
\[ \sim \text{aborted } s2 \longrightarrow \sim \text{aborted } s1 \]

definition \( P10 : (\text{ALM-state} \times \text{ALM-state}) \Rightarrow \text{bool} \)  
— ALM 1 is always initialized and when ALM 2 is not initialized its history is empty  
where  
\[ P10 \equiv \% s . \text{let } s1 = \text{fst } s; s2 = \text{snd } s \text{ in} \]  
\[ \sim \text{initialized } s1 \wedge \sim \text{initialized } s2 \longrightarrow (\text{hist } s2 = []) \]

definition \( P11 : (\text{ALM-state} \times \text{ALM-state}) \Rightarrow \text{bool} \)  
— After ALM 2 has been invoked and before it is initialized, any request found in init histories after their longest common prefix is pending in ALM 1  
where  
\[ P11 \equiv \% s . \text{let } s1 = \text{fst } s; s2 = \text{snd } s \text{ in} \]  
\[ \sim (\exists c . \text{phase } s2 c \neq \text{Sleep}) \wedge \sim \text{initialized } s2 \longrightarrow \text{initValidReqs } s2 \subseteq \text{pendingReqs } s1 \]

definition \( P12 : (\text{ALM-state} \times \text{ALM-state}) \Rightarrow \text{bool} \)  
— After ALM 2 has been invoked and before it is initialized, the longest common prefix of the init histories of ALM 2 is built from appending a set of request pending
in ALM 1 to the history of ALM 1

\[ P12 \iff \% s . \text{let } s1 = \text{fst } s; s2 = \text{snd } s \text{ in} \]
\[ \begin{align*}
\exists c . \text{phase } s2 c &\neq \text{Sleep} \implies \exists rs . \text{postfix-all} ((l-c-p \text{ initHists } s2) = rs @ (\text{hist } s1) \\
&\land \text{set } rs \subseteq \text{pendingReqs } s1 \land \text{distinct } rs)
\end{align*} \]

**definition** \( P13 :: (\text{ALM-state} \times \text{ALM-state}) \rightarrow \text{bool} \)

where

— After ALM 2 has been invoked and before it is initialized, any history that may be chosen at initialization is a valid linearization of the concurrent history of ALM 1

\[ P13 \iff \% s . \text{let } s1 = \text{fst } s; s2 = \text{snd } s \text{ in} \]
\[ \begin{align*}
\exists c . \text{phase } s2 c &\neq \text{Sleep} \land \neg \text{initialized } s2 \implies \text{postfix-all} ((l-c-p \text{ initHists } s2)) \subseteq \text{postfix-all} (\text{hist } s1) \land \text{linearizations (pendingReqs } s1)\)
\end{align*} \]

**definition** \( P14 :: (\text{ALM-state} \times \text{ALM-state}) \rightarrow \text{bool} \)

where

— The history of ALM 1 is a postfix of the history of ALM 2 and requests appearing in ALM 2 after the history of ALM 1 are not in the history of ALM 1

\[ P14 \iff \% s . \text{let } s1 = \text{fst } s; s2 = \text{snd } s \text{ in} \]
\[ \begin{align*}
\text{hist } s2 &\neq [] \lor \text{initialized } s2 \implies \exists rs . \text{hist } s2 = rs @ (\text{hist } s1) \\
&\land \text{set } rs \cap \text{set } (\text{hist } s1) = \{\}\)
\end{align*} \]

**definition** \( P15 :: (\text{ALM-state} \times \text{ALM-state}) \rightarrow \text{bool} \)

where

— A client that hasn’t yet invoked ALM 2 has no request committed in ALM 2 except for its pending request

\[ P15 \iff \% s . \text{let } s1 = \text{fst } s; s2 = \text{snd } s \text{ in} \]
\[ \forall r . \text{let } c = \text{request-snd } r \text{ in } \text{phase } s2 c = \text{Sleep} \land r \in \text{set } (\text{hist } s2) \implies (r \in \text{set } (\text{hist } s1) \lor r \in \text{pendingReqs } s1)\]

### 4.4 Proofs of invariance

**lemma** \( \text{invariant-imp} \): \[ \text{invariant } \text{ioa } P; \forall s . P s \implies Q s \] \implies \text{invariant } \text{ioa } Q

(\text{proof})

**declare** \( \text{phase.split } \text{[split]} \)

**declare** \( \text{phase.split-asm } \text{[split]} \)

**declare** \( \text{ALM-action.split } \text{[split]} \)

**declare** \( \text{ALM-action.split-asm } \text{[split]} \)

**lemma** \( \text{dropWhile-lemma} \): \[ \forall ys . xs = ys \@ zs \land \text{hd } zs = x \land zs \neq [] \land x \notin \text{set } ys \implies \text{dropWhile } (\lambda x'. x' \neq x) \text{ zs} = zs \]

— A useful lemma about truncating histories

(\text{proof})

**lemma** \( \text{P2-invariant} \): \[ ||\text{id1} < \text{id2}; \text{id1} \neq 0|| \implies \text{invariant } (\text{composeALMs } \text{id1} \text{id2}) \text{ P2} \]

10
\textbf{lemma} \( P5\)-invariant: \([i1 < i2; \, i1 \neq 0] \implies \text{invariant} \, \text{(composeALMs} \, i1 \, i2) \, P5 \)

\textbf{lemma} \( P6\)-invariant: \([i1 \neq 0 \land i1 < i2] \implies \text{invariant} \, \text{(composeALMs} \, i1 \, i2) \, P6 \)

\textbf{lemma} \( P9\)-invariant: \([i1 < i2; \, i1 \neq 0] \implies \text{invariant} \, \text{(composeALMs} \, i1 \, i2) \, P9 \)

\textbf{lemma} \( P10\)-invariant: \([i1 < i2; \, i1 \sim 0] \implies \text{invariant} \, \text{(composeALMs} \, i1 \, i2) \, P10 \)

\textbf{lemma} \( P3\)-invariant: \([i1 < i2; \, i1 \neq 0] \implies \text{invariant} \, \text{(composeALMs} \, i1 \, i2) \, P3 \)

\textbf{lemma} \( P7\)-invariant: \([i1 < i2; \, i1 \neq 0] \implies \text{invariant} \, \text{(composeALMs} \, i1 \, i2) \, P7 \)

\textbf{lemma} \( P4\)-invariant: \([i1 < i2; \, i1 \neq 0] \implies \text{invariant} \, \text{(composeALMs} \, i1 \, i2) \, P4 \)

\textbf{lemma} \( P8\)-invariant: \([i1 < i2; \, i1 \neq 0] \implies \text{invariant} \, \text{(composeALMs} \, i1 \, i2) \, P8 \)

\textbf{lemma} \( P12\)-invariant: \([i1 < i2; \, i1 \neq 0] \implies \text{invariant} \, \text{(composeALMs} \, i1 \, i2) \, P12 \)

\textbf{lemma} \( P11\)-invariant: \([i1 < i2; \, i1 \neq 0] \implies \text{invariant} \, \text{(composeALMs} \, i1 \, i2) \, P11 \)

\textbf{lemma} \( P1a\)-invariant: \([i1 < i2; \, i1 \neq 0] \implies \text{invariant} \, \text{(composeALMs} \, i1 \, i2) \, P1a \)

\textbf{lemma} \( P1b\)-invariant: \([i1 < i2; \, i1 \neq 0] \implies \text{invariant} \, \text{(composeALMs} \, i1 \, i2) \, P1b \)
lemma P13-invariant: $[\text{id1} < \text{id2}; \text{id1} \neq 0] \implies \text{invariant (composeALMs id1 id2)}$ P13
(\text{proof})

lemma P14-invariant: $[\text{id1} < \text{id2}; \text{id1} \neq 0] \implies \text{invariant (composeALMs id1 id2)}$ P14
(\text{proof})

lemma P15-invariant: $[\text{id1} < \text{id2}; \text{id1} \neq 0] \implies \text{invariant (composeALMs id1 id2)}$ P15
(\text{proof})

4.5 The refinement proof

definition ref-mapping :: (ALM-state * ALM-state) => ALM-state
— The refinement mapping between the composition of two ALMs and a single ALM
where
ref-mapping \equiv \lambda (s1, s2).
\{pending = \lambda c. (if phase s1 c \neq \text{Aborted} then pending s1 c else pending s2 c),
initHists = \{\},
phase = \lambda c. (if phase s1 c \neq \text{Aborted} then phase s1 c else phase s2 c),
hist = (if hist s2 = [] then hist s1 else hist s2),
aborted = aborted s2,
initialized = True\}

theorem composition: $[\text{id1} \neq 0; \text{id1} < \text{id2}] \implies ((\text{composeALMs id1 id2}) =< (\text{ALM-toa 0 id2}))$
— The composition theorem
(\text{proof})

end

5 Conclusion

In this document we have defined the ALM automaton (a shorthand for Aborable Linearizable Modules) and we have proved that the composition of two instances of the ALM automaton behaves like a single instance of the ALM automaton. This theorem justifies the compositional proof technique presented in [1].

References

able at http://lara.epfl.ch/w/slin.

