Abortable Linearizable Modules

Rachid Guerraoui    Viktor Kuncak    Giuliano Losa

August 28, 2014

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

theory LCP
imports Main ~~/src/HOL/Library/Sublist
begin

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

theory ALM
imports ~~/src/HOL/HOLCF/IOA/meta-theory/IOA LCP
begin

typedecl client
— A non-empty set of clients
typedec data
— Data contained in requests
datatype request =
— A request is composed of a sender and data
  Req client data
definition request-snd :: request ⇒ client
  where request-snd ≡ λ r. case r of Req c - ⇒ c
type-synonym hist = request list
— Type of histories of requests.
datatype ALM-action =
— The actions of the ALM automaton
  Invoke client request
  | Commit client nat hist
  | Switch client nat hist request
  | Initialize nat hist
  | Linearize nat hist
  | Abort nat
datatype phase = Sleep | Pending | Ready | Aborted
— Executions phases of a client
definition linearizations :: request set ⇒ hist set
— The possible linearizations of a set of requests
  where
    linearizations ≡ λ reqs . { h . set h ⊆ reqs ∧ distinct h}
definition postfix-all :: hist ⇒ hist set ⇒ hist set
— appends to the right the first argument to every member of the history set
  where
    postfix-all ≡ λ h hs . { h′ . ∃ h′′ . h′ = h′′ @ h ∧ h′′ ∈ hs}
definition ALM-asig :: nat ⇒ nat ⇒ ALM-action signature
— The action signature of ALM automata
— Input actions, output actions, and internal actions
  where
    ALM-asig ≡ λ id1 id2 . ( 
      { act . ∃ c r h .
        act = Invoke c r | act = Switch c id1 h r},
      { act . ∃ c h r id′.
        id1 <= id′ ∧ id′ < id2 ∧ act = Commit c id′ h
          | act = Switch c id2 h r},
      { act . ∃ h .
        act = Abort id1
          | act = Linearize id1 h
    )
\[ \text{act} = \text{Initialize id1 h}\] 

**record** ALM-state =
— The state of the ALM automata
pending :: client \(\Rightarrow\) request
— Associates a pending request to a client process
initHists :: hist set
— The set of init histories submitted by clients
phase :: client \(\Rightarrow\) 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 \(\Rightarrow\) request set
— the set of requests that have been invoked but that are not yet in the hist parameter

**where**

\[
\text{pendingReqs} \equiv \lambda \ s . \{ r . \exists \ c .
\begin{align*}
\text{r} &= \text{pending}\ s\ c \\
\land &\ r \notin \text{set}(\text{hist}\ s) \\
\land &\ \text{phase}\ s\ c \in \{\text{Pending},\ \text{Aborted}\}
\end{align*}
\]

**definition** initValidReqs :: ALM-state \(\Rightarrow\) request set
— any request that appears in an init hist after the longest common prefix or that is pending

**where**

\[
\text{initValidReqs} \equiv \lambda \ s . \{ r .
\begin{align*}
(r &\in \text{pendingReqs}\ s \lor (\exists \ h \in \text{initHists}\ s . \ r \in \text{set}\ h)) \\
\land &\ r \notin \text{set}(\text{l-c-p}(\text{initHists}\ s))
\end{align*}
\]

**definition** ALM-trans :: nat \(\Rightarrow\) nat \(\Rightarrow\) (ALM-action, ALM-state)transition set
— the transitions of the ALM automaton

**where**

\[
\text{ALM-trans} \equiv \lambda \ id1\ id2 . \{\text{trans} .
\begin{align*}
\text{let}\ s &= \text{fst}\ \text{trans};\ s' &= \text{snd}\ (\text{snd}\ \text{trans});\ a &= \text{fst}\ (\text{snd}\ \text{trans})\ \text{in}
\end{align*}
\]

\[
\begin{cases}
\text{case}\ a\ \text{of}\ \text{Invoke}\ c\ r \Rightarrow \\
\text{if}\ \text{phase}\ s\ c = \text{Ready}\ \land\ \text{request-snd}\ r = c\ \land\ r \notin \text{set}(\text{hist}\ s) \\
\text{then}\ s' &= s[\text{pending} := (\text{pending}\ s)(c := r), \text{phase} := (\text{phase}\ s)(c := \text{Pending})] \\
\text{else}\ s' &= s
\end{cases}
\]

\[
|\text{Linearize}\ i\ h \Rightarrow \\
\text{initialized}\ s \land \neg\ \text{aborted}\ s \\
\land h \in \text{postfix-all}(\text{hist}\ s)\ (\text{linearizations}(\text{pendingReqs}\ s))
\]
\[ s' = s[\text{hist} := h] \]

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

\[ \text{Abort } i \Rightarrow \]
\[ \neg \text{aborted } s \wedge (\exists c \cdot \text{phase } s \ c \neq \text{Sleep}) \]
\[ \wedge s' = s[\text{aborted} := \text{True}] \]

\[ \text{Commit } c \text{ i h } \Rightarrow \]
\[ \text{phase } s \ c = \text{Pending} \wedge \text{pending } s \ c \ \epsilon \ \text{set } (\text{hist } s) \]
\[ \wedge h = \text{dropWhile } (\lambda r . \ r \neq \text{pending } s \ c) \ (\text{hist } s) \]
\[ \wedge s' = s[\text{phase} := (\text{phase } s)(c := \text{Ready})] \]

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

definition \text{ALM-start} :: \text{nat} \Rightarrow \text{ALM-state}\set
— the set of start states

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

definition \text{ALM-ioa} :: \text{nat} \Rightarrow \text{nat} \Rightarrow (\text{ALM-action, ALM-state})\text{ioa}
— The ALM automaton

where
\[ \text{ALM-ioa} \equiv \lambda (\text{id1}::\text{nat}) \text{id2} . \]
\[ (\text{ALM-asig } id1 \text{id2}, \]
\[ \text{ALM-start } id1, \]
\begin{verbatim}
ALM-trans id1 id2,
\{}, {}\}

type-synonym compo-state = ALM-state × ALM-state

definition composeALMs :: nat ⇒ nat ⇒ (ALM-action, compo-state) ioa
— the composition of two ALMs
where
composeALMs ≡ λ 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) =>
(ALM-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
c 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 & id' < id1)
| (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)
\end{verbatim}
lemma composeALMsE:
— A rule for decomposing proofs
assumes id1 \sim \neq 0 \text{ and } id1 < id2 \text{ and } \text{in-trans-comp:s} - (a::ALM-action) - - \text{composeALMs}
shows \text{decomp: in-trans-cases-fun id1 id2 s t}
(proof)

lemma my-rule: |id1 \neq 0; id1 < id2; s -a-\text{-composeALMs id1 id2-> t;}

lemma my-rule2: |0 < id1; id1 < id2; s -a-\text{-composeALMs id1 id2-> t;}

4.2 Invariants of a single ALM instance

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

definition P1b :: (ALM-state * ALM-state) \Rightarrow bool
where
— In ALM 2, a pending request of client c has client c as sender
P1b == \% s . let s1 = \text{fst s}; s2 = \text{snd s} in
\text{ALL c . phase s2 c} \neq \text{Sleep} - -\text{request-snd (pending s2 c) = c
}

definition P2 :: (ALM-state * ALM-state) \Rightarrow bool
where
P2 == \% s . let s1 = \text{fst s}; s2 = \text{snd s} in
(\forall c . \text{phase s2 c} = \text{Sleep}) - -\text{initialized s2 }\land \text{hist s2} = []

definition P3 :: (ALM-state * ALM-state) \Rightarrow bool
where
P3 == \% s . let s1 = \text{fst s}; s2 = \text{snd s} in
\forall c . (\text{phase s2 c} = \text{Ready} - -\text{initialized s2}

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

definition P5 :: (ALM-state * ALM-state) \Rightarrow bool
where
— In ALM 1 a client never sleeps
P5 == \% s . let s1 = \text{fst s}; s2 = \text{snd s} in
\forall c . \text{phase s1 c} \neq \text{Sleep}
4.3 Invariants of the composition of two ALM instances

**Definition P6 :: (ALM-state ∗ ALM-state) ⇒ bool**
— Non-interference across instances

**Where**

P6 == % s . let s1 = fst s; s2 = snd s in

\(\neg \text{aborted} s1 \implies (\text{ALL } c \cdot \text{phase } s2 c = \text{Sleep}) \land \text{ALL } c \cdot \text{phase } s1 c \sim \text{Aborted} = (\text{phase } s2 c = \text{Sleep})\)

**Definition P7 :: (ALM-state ∗ ALM-state) ⇒ 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 == % s . let s1 = fst s; s2 = snd s in

\(\text{ALL } c \cdot \text{phase } s1 c = \text{Aborted} \land \neg \text{initialized} s2 \implies (\text{pending } s2 c = \text{pending } s1 c \land \text{phase } s2 c \in \{\text{Pending}, \text{Aborted}\})\)

**Definition P8 :: (ALM-state ∗ ALM-state) ⇒ bool**
— Init histories of ALM 2 are built from the history of ALM 1 plus pending requests of ALM 1

**Where**

P8 == % s . let s1 = fst s; s2 = snd s in

\(\forall h \in \text{initHists } s2 . h \in \text{postfix-all } (\text{hist } s1) \in \text{linearizations } (\text{pendingReqs } s1)\)

**Definition P9 :: (ALM-state ∗ ALM-state) ⇒ bool**
— ALM 2 does not abort before ALM 1 aborts

**Where**

P9 == % s . let s1 = fst s; s2 = snd s in

\(\text{aborted } s2 \implies \text{aborted } s1\)

**Definition P10 :: (ALM-state ∗ ALM-state) ⇒ bool**
— ALM 1 is always initialized and when ALM 2 is not initialized its history is empty

**Where**

P10 == % s . let s1 = fst s; s2 = snd s in

\(\text{initialized } s1 \land (\neg \text{initialized } s2 \implies (\text{hist } s2 = []))\)

**Definition P11 :: (ALM-state ∗ ALM-state) ⇒ 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 == % s . let s1 = fst s; s2 = snd s in

\((\exists c \cdot \text{phase } s2 c \neq \text{Sleep}) \land \neg \text{initialized } s2 \implies \text{initValidReqs } s2 \subseteq \text{pendingReqs } s1\)

**Definition P12 :: (ALM-state ∗ ALM-state) ⇒ 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

\[ P12 \equiv \% \quad s \quad . \quad \text{let} \quad s1 = \text{fst} \quad s; \quad s2 = \text{snd} \quad s \quad \text{in} \]

\[ (\exists \quad c \quad . \quad \text{phase} \quad s2 \quad c \neq \text{Sleep}) \rightarrow (\exists \quad rs \quad . \quad l-c-p \quad (\text{initHists} \quad s2) = rs \circ (\text{hist} \quad s1) \]

\( \land \quad \text{set} \quad rs \subseteq \text{pendingReqs} \quad s1 \quad \land \quad \text{distinct} \quad rs) \]

**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

\[ P13 \equiv \% \quad s \quad . \quad \text{let} \quad s1 = \text{fst} \quad s; \quad s2 = \text{snd} \quad s \quad \text{in} \]

\[ ((\exists \quad c \quad . \quad \text{phase} \quad s2 \quad c \neq \text{Sleep}) \land \neg \text{initialized} \quad s2) \rightarrow \text{postfix-all} \quad (l-c-p \quad (\text{initHists} \quad s2)) \subseteq \text{postfix-all} \quad (\text{hist} \quad s1) \]

\( \land \quad \text{set} \quad rs \cap \text{set} \quad (\text{hist} \quad s1) = \{\} \]

**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

\[ P14 \equiv \% \quad s \quad . \quad \text{let} \quad s1 = \text{fst} \quad s; \quad s2 = \text{snd} \quad s \quad \text{in} \]

\[ (\text{hist} \quad s2 \neq [] \lor \text{initialized} \quad s2) \rightarrow (\exists \quad rs \quad . \quad \text{hist} \quad s2 = rs \circ (\text{hist} \quad s1) \]

\( \land \quad \text{set} \quad rs \cap \text{set} \quad (\text{hist} \quad s1) = \{\} \]

**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

\[ P15 \equiv \% \quad s \quad . \quad \text{let} \quad s1 = \text{fst} \quad s; \quad s2 = \text{snd} \quad s \quad \text{in} \]

\[ \forall \quad r \quad . \quad \text{let} \quad c = \text{request-snd} \quad r \quad \text{in} \quad \text{phase} \quad s2 \quad c = \text{Sleep} \quad \land \quad r \in \text{set} \quad (\text{hist} \quad s2) \rightarrow (r \in \text{set} \quad (\text{hist} \quad s1) \lor r \in \text{pendingReqs} \quad s1) \]

### 4.4 Proofs of invariance

**lemma** invariant-imp: \[[\text{invariant} \quad \text{ioa} \quad P; \forall \quad s \quad . \quad P \quad s \rightarrow Q \quad s] \Rightarrow \text{invariant} \quad \text{ioa} \quad Q \]

⟨proof⟩

**declare** phase.split [split]

**declare** phase.split-asn [split]

**declare** ALM-action.split [split]

**declare** ALM-action.split-asn [split]

**lemma** dropWhile-lemma: \[\forall \quad ys , \quad zs \equiv ys \circ zs \land \text{hd} \quad zs = x \land zs \neq [] \land x \notin \text{set} \quad ys \rightarrow \text{dropWhile} \quad (\lambda \quad x'. \quad x' \neq x) \quad zs = zs \]

— A useful lemma about truncating histories

⟨proof⟩

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

10
lemma P5-invariant: \[ |id_1 < id_2; id_1 \neq 0| \implies \text{invariant (composeALMs id_1 id_2)} \]
lemma P6-invariant: \[ |id_1 \neq 0 ; id_1 < id_2| \implies \text{invariant (composeALMs id_1 id_2)} \]
lemma P9-invariant: \[ |id_1 < id_2; id_1 \neq 0| \implies \text{invariant (composeALMs id_1 id_2)} \]
lemma P10-invariant: \[ |id_1 < id_2; id_1 \sim 0| \implies \text{invariant (composeALMs id_1 id_2)} \]
lemma P3-invariant: \[ |id_1 < id_2; id_1 \neq 0| \implies \text{invariant (composeALMs id_1 id_2)} \]
lemma P7-invariant: \[ |id_1 < id_2; id_1 \neq 0| \implies \text{invariant (composeALMs id_1 id_2)} \]
lemma P4-invariant: \[ |id_1 < id_2; id_1 \neq 0| \implies \text{invariant (composeALMs id_1 id_2)} \]
lemma P8-invariant: \[ |id_1 < id_2; id_1 \neq 0| \implies \text{invariant (composeALMs id_1 id_2)} \]
lemma P12-invariant: \[ |id_1 < id_2; id_1 \neq 0| \implies \text{invariant (composeALMs id_1 id_2)} \]
lemma P11-invariant: \[ |id_1 < id_2; id_1 \neq 0| \implies \text{invariant (composeALMs id_1 id_2)} \]
lemma P1a-invariant: \[ |id_1 < id_2; id_1 \neq 0| \implies \text{invariant (composeALMs id_1 id_2)} \]
lemma P1b-invariant: \[ |id_1 < id_2; id_1 \neq 0| \implies \text{invariant (composeALMs id_1 id_2)} \]
**lemma** P13-invariant: \([\operatorname{id}1 < \operatorname{id}2; \operatorname{id}1 \neq 0] \implies \text{invariant (composeALMs \operatorname{id}1 \\operatorname{id}2)}\) P13

\langle proof \rangle

**lemma** P14-invariant: \([\operatorname{id}1 < \operatorname{id}2; \operatorname{id}1 \neq 0] \implies \text{invariant (composeALMs \operatorname{id}1 \\operatorname{id}2)}\) P14

\langle proof \rangle

**lemma** P15-invariant: \([\operatorname{id}1 < \operatorname{id}2; \operatorname{id}1 \neq 0] \implies \text{invariant (composeALMs \operatorname{id}1 \\operatorname{id}2)}\) P15

\langle proof \rangle

4.5 The refinement proof

**definition** ref-mapping :: \((\text{ALM-state} \times \text{ALM-state}) \rightarrow \text{ALM-state}\)

— The refinement mapping between the composition of two ALMs and a single ALM

**where**

\[
\begin{align*}
\text{ref-mapping} & \equiv \lambda (s1, s2). \\
& \begin{cases}
\text{pending} = \lambda c. (\text{if phase } s1 c \neq \text{Aborted} \text{ then pending } s1 c \text{ else pending } s2 c), \\
\text{initHists} = \{\}, \\
\text{phase} = \lambda c. (\text{if phase } s1 c \neq \text{Aborted} \text{ then phase } s1 c \text{ else phase } s2 c), \\
\text{hist} = (\text{if hist } s2 = [] \text{ then hist } s1 \text{ else hist } s2), \\
\text{aborted} = \text{aborted } s2, \\
\text{initialized} = \text{True}
\end{cases}
\end{align*}
\]

**theorem** composition: \([\operatorname{id}1 \neq 0; \operatorname{id}1 < \operatorname{id}2] \implies ((\text{composeALMs } \operatorname{id}1 \ \operatorname{id}2) = <)\ (\text{ALM-ioa 0 } \operatorname{id}2))

— The composition theorem

\langle proof \rangle

5 Conclusion

In this document we have defined the ALM automaton (a shorthand for Aboratable 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.

