Dynamic Architectures

Diego Marmsoler

October 11, 2017

Abstract

The architecture of a system describes the system's overall organization into components and connections between those components. With the emergence of mobile computing, dynamic architectures have become increasingly important. In such architectures, components may appear or disappear, and connections may change over time. In the following we mechanize a theory of dynamic architectures and verify the soundness of a corresponding calculus. Therefore, we first formalize the notion of configuration traces [5] as a model for dynamic architectures. Then, the behavior of single components is formalized in terms of behavior traces and an operator is introduced and studied to extract the behavior of a single component out of a given configuration trace. Then, behavior trace assertions are introduced as a temporal specification technique to specify behavior of components. Reasoning about component behavior in a dynamic context is formalized in terms of a calculus for dynamic architectures [3]. Finally, the soundness of the calculus is verified by introducing an alternative interpretation for behavior trace assertions over configuration traces and proving the rules of the calculus. Since projection may lead to finite as well as infinite behavior traces, they are formalized in terms of coinductive lists. Thus, our theory is based on Lochbihler's [1] formalization of coinductive lists. The theory may be applied to verify properties for dynamic architectures.

Contents

1 A Theory of Dynamic Architectures

The following theory formalizes configuration traces [4, 5] as a model for dynamic architectures. Since configuration traces may be finite as well as infinite, the theory depends on Lochbihler's theory of co-inductive lists [1].

theory *Configuration-Traces*
  imports *Coinductive.Coinductive-List*
begin

In the following we first provide some preliminary results for natural numbers, extended natural numbers, and lazy lists. Then, we introduce a locale @textdynamic_architectures which introduces basic definitions and corresponding properties for dynamic architectures.

1.1 Natural Numbers

We provide one additional property for natural numbers.

lemma *boundedGreatest*:
  assumes $P\ (i{::}nat)$
    and $\forall\, n' > n.\ \neg\ P\ n'$
  shows $\exists\, i' {\leq} n.\ P\ i' \wedge (\forall\, n'.\ P\ n' \longrightarrow n' {\leq} i')$
⟨*proof*⟩

1.2 Extended Natural Numbers

We provide one simple property for the *strict* order over extended natural numbers.

lemma *enat-min*:
  assumes $m \geq enat\ n'$
    and $enat\ n < m - enat\ n'$
  shows $enat\ n + enat\ n' < m$
  ⟨*proof*⟩

1.3 Lazy Lists

In the following we provide some additional notation and properties for lazy lists.

notation *LNil* $([]_l)$
notation *LCons* (**infixl** $\#_l$ *60*)
notation *lappend* (**infixl** $@_l$ *60*)

lemma *lnth-lappend*[*simp*]:
  assumes *lfinite xs*
    and $\neg$ *lnull ys*
  shows *lnth* (*xs* $@_l$ *ys*) (*the-enat* (*llength xs*)) = *lhd ys*
⟨*proof*⟩

lemma *lfilter-ltake*:
  assumes $\forall\, (n{::}nat) {\leq} llength\ xs.\ n {\geq} i \longrightarrow (\neg\ P\ (lnth\ xs\ n))$
  shows *lfilter P xs* = *lfilter P* (*ltake i xs*)
⟨*proof*⟩

lemma *lfilter-lfinite*[*simp*]:
  assumes *lfinite* (*lfilter P t*)
    and $\neg$ *lfinite t*

shows $\exists\, n.\ \forall\, n'{>}n.\ \neg\ P\ (lnth\ t\ n')$
⟨*proof*⟩

1.4 A Model of Dynamic Architectures

typedecl *cnf*
type-synonym *trace* = *nat* ⇒ *cnf*
consts *arch*:: *trace set*

In the following we formalize dynamic architectures in terms of configuration traces, i.e., sequences of architecture configurations.

Our model is provided in terms of a locale over three type parameters:

- id: a type for component identifiers
- cmp: a type for components
- cnf: a type for architecture configurations

locale *dynamic-component* =
fixes *tCMP* :: *'id* ⇒ *cnf* ⇒ *'cmp* (σ_(-) [*0*,*110*]*60*)
and *active* :: *'id* ⇒ *cnf* ⇒ *bool* (‖-‖_ [*0*,*110*]*60*)
begin

The locale requires two parameters:

- *tCMP* is an operator to obtain a component with a certain identifier from an architecture configuration.
- *active* is a predicate to assert whether a certain component is activated within an architecture configuration.

The locale provides some general properties about its parameters and introduces six important operators over configuration traces:

- An operator to extract the behavior of a certain component out of a given configuration trace.
- An operator to obtain the number of activations of a certain component within a given configuration trace.
- An operator to obtain the least point in time (before a certain point in time) from which on a certain component is not activated anymore.
- An operator to obtain the latest point in time where a certain component was activated.
- Two operators to map time-points between configuration traces and behavior traces.

Moreover, the locale provides several properties about the operators and their relationships.

lemma *nact-active*:
fixes *t*::*nat* ⇒ *cnf*
and *n*::*nat*
and *n''*
and *id*

assumes $\|id\|_{t\ n}$
and $n'' \geq n$
and $\neg\ (\exists\, n'{\geq}n.\ n' < n'' \wedge \|id\|_{t\ n'})$
shows $n{=}n''$
⟨*proof*⟩

lemma *nact-exists*:
fixes $t{::}nat \Rightarrow cnf$
assumes $\exists\, i{\geq}n.\ \|c\|_{t\ i}$
shows $\exists\, i{\geq}n.\ \|c\|_{t\ i} \wedge (\nexists k.\ n{\leq}k \wedge k{<}i \wedge \|c\|_{t\ k})$
⟨*proof*⟩

lemma *lActive-least*:
assumes $\exists\, i{\geq}n.\ i < llength\ t \wedge \|c\|_{lnth\ t\ i}$
shows $\exists\, i{\geq}n.\ (i < llength\ t \wedge \|c\|_{lnth\ t\ i} \wedge (\nexists k.\ n{\leq}k \wedge k{<}i \wedge k{<}llength\ t \wedge \|c\|_{lnth\ t\ k}))$
⟨*proof*⟩

1.5 Projection

In the following we introduce an operator which extracts the behavior of a certain component out of a given configuration trace.

definition *proj*:: *'id* ⇒ (*cnf llist*) ⇒ (*'cmp llist*) ($\pi_{\_}(\text{-})$ [*0,110*]*60*)
where $proj\ c = lmap\ (\lambda cnf.\ (\sigma_c(cnf))) \circ (lfilter\ (active\ c))$

lemma *proj-lnil* [*simp,intro*]:
$\pi_c([]_l) = []_l$ ⟨*proof*⟩

lemma *proj-lnull* [*simp*]:
$\pi_c(t) = []_l \longleftrightarrow (\forall\, k \in lset\ t.\ \neg\ \|c\|_k)$
⟨*proof*⟩

lemma *proj-LCons* [*simp*]:
$\pi_i(x\ \#_l\ xs) = (if\ \|i\|_x\ then\ (\sigma_i(x))\ \#_l\ (\pi_i(xs))\ else\ \pi_i(xs))$
⟨*proof*⟩

lemma *proj-llength*[*simp*]:
$llength\ (\pi_c(t)) \leq llength\ t$
⟨*proof*⟩

lemma *proj-ltake*:
assumes $\forall\, (n'{::}nat){\leq}llength\ t.\ n'{\geq}n \longrightarrow (\neg\ \|c\|_{lnth\ t\ n'})$
shows $\pi_c(t) = \pi_c(ltake\ n\ t)$ ⟨*proof*⟩

lemma *proj-finite-bound*:
assumes $lfinite\ (\pi_c(inf\text{-}llist\ t))$
shows $\exists\, n.\ \forall\, n'{>}n.\ \neg\ \|c\|_{t\ n'}$
⟨*proof*⟩

1.5.1 Monotonicity and Continuity

lemma *proj-mcont*:
shows *mcont lSup lprefix lSup lprefix* (*proj c*)
⟨*proof*⟩

lemma *proj-mcont2mcont*:

assumes *mcont lub ord lSup lprefix f*
shows *mcont lub ord lSup lprefix* $(\lambda x.\ \pi_c(f\ x))$
⟨*proof*⟩

lemma *proj-mono-prefix*[*simp*]:
assumes *lprefix t t'*
shows *lprefix* $(\pi_c(t))$ $(\pi_c(t'))$
⟨*proof*⟩

1.5.2 Finiteness

lemma *proj-finite*[*simp*]:
assumes *lfinite t*
shows *lfinite* $(\pi_c(t))$
⟨*proof*⟩

lemma *proj-finite2*:
assumes $\forall (n'::nat) \leq llength\ t.\ n' \geq n \longrightarrow (\neg\ \|c\|_{lnth\ t\ n'})$
shows *lfinite* $(\pi_c(t))$ ⟨*proof*⟩

lemma *proj-append-lfinite*[*simp*]:
fixes *t t'*
assumes *lfinite t*
shows $\pi_c(t\ @_l\ t') = (\pi_c(t))\ @_l\ (\pi_c(t'))$ (**is** *?lhs=?rhs*)
⟨*proof*⟩

lemma *proj-one*:
assumes $\exists\, i.\ i < llength\ t \wedge \|c\|_{lnth\ t\ i}$
shows $llength\ (\pi_c(t)) \geq 1$
⟨*proof*⟩

1.5.3 Projection not Active

lemma *proj-not-active*[*simp*]:
assumes $enat\ n < llength\ t$
and $\neg\ \|c\|_{lnth\ t\ n}$
shows $\pi_c(ltake\ (Suc\ n)\ t) = \pi_c(ltake\ n\ t)$ (**is** *?lhs = ?rhs*)
⟨*proof*⟩

lemma *proj-not-active-same*:
assumes $enat\ n \leq (n'::enat)$
and $\neg$ *lfinite t* $\vee\ n'-1 < llength\ t$
and $\nexists\, k.\ k \geq n \wedge k < n' \wedge k < llength\ t \wedge \|c\|_{lnth\ t\ k}$
shows $\pi_c(ltake\ n'\ t) = \pi_c(ltake\ n\ t)$
⟨*proof*⟩

1.5.4 Projection Active

lemma *proj-active*[*simp*]:
assumes $enat\ i < llength\ t\ \|c\|_{lnth\ t\ i}$
shows $\pi_c(ltake\ (Suc\ i)\ t) = (\pi_c(ltake\ i\ t))\ @_l\ ((\sigma_c(lnth\ t\ i))\ \#_l\ []_l)$ (**is** *?lhs = ?rhs*)
⟨*proof*⟩

lemma *proj-active-append*:
assumes *a1*: $(n::nat) \leq i$
and *a2*: $enat\ i < (n'::enat)$

and *a3*: $\neg$ *lfinite t* $\vee$ *n'−1* < *llength t*
and *a4*: $\|c\|_{lnth\ t\ i}$
and $\forall i'.\ (n \leq i' \wedge enat\ i' < n' \wedge i' < llength\ t \wedge \|c\|_{lnth\ t\ i'}) \longrightarrow (i' = i)$
shows $\pi_c(ltake\ n'\ t) = (\pi_c(ltake\ n\ t))\ @_l\ ((\sigma_c(lnth\ t\ i))\ \#_l\ []_l)$ (**is** *?lhs = ?rhs*)
⟨*proof*⟩

1.5.5 Same and not Same

lemma *proj-same-not-active*:
assumes $n \leq n'$
and *enat* $(n'-1)$ < *llength t*
and $\pi_c(ltake\ n'\ t) = \pi_c(ltake\ n\ t)$
shows $\nexists k.\ k \geq n \wedge k < n' \wedge \|c\|_{lnth\ t\ k}$
⟨*proof*⟩

lemma *proj-not-same-active*:
assumes *enat n* $\leq$ $(n'::enat)$
and $(\neg$ *lfinite t*$)$ $\vee$ *n'−1* < *llength t*
and $\neg(\pi_c(ltake\ n'\ t) = \pi_c(ltake\ n\ t))$
shows $\exists k.\ k \geq n \wedge k < n' \wedge enat\ k < llength\ t \wedge \|c\|_{lnth\ t\ k}$
⟨*proof*⟩

1.6 Activations

We also introduce an operator to obtain the number of activations of a certain component within a given configuration trace.

definition *nAct* :: *'id* $\Rightarrow$ *enat* $\Rightarrow$ (*cnf llist*) $\Rightarrow$ *enat* $(\langle\text{- \#}_{\text{--}}\rangle)$ **where**
$\langle c\ \#_n\ t\rangle \equiv llength\ (\pi_c(ltake\ n\ t))$

lemma *nAct-0*[*simp*]:
$\langle c\ \#_0\ t\rangle = 0$ ⟨*proof*⟩

lemma *nAct-NIL*[*simp*]:
$\langle c\ \#_n\ []_l\rangle = 0$ ⟨*proof*⟩

lemma *nAct-Null*:
assumes *llength t* $\geq$ *n*
and $\langle c\ \#_n\ t\rangle = 0$
shows $\forall i < n.\ \neg\ \|c\|_{lnth\ t\ i}$
⟨*proof*⟩

lemma *nAct-ge-one*[*simp*]:
assumes *llength t* $\geq$ *n*
and *i* < *n*
and $\|c\|_{lnth\ t\ i}$
shows $\langle c\ \#_n\ t\rangle \geq enat\ 1$
⟨*proof*⟩

lemma *nAct-finite*[*simp*]:
assumes $n \neq \infty$
shows $\exists n'.\ \langle c\ \#_n\ t\rangle = enat\ n'$
⟨*proof*⟩

lemma *nAct-enat-the-nat*[*simp*]:
assumes $n \neq \infty$

shows *enat* (*the-enat* ($\langle c\ \#_n\ t\rangle$)) = $\langle c\ \#_n\ t\rangle$
⟨*proof*⟩

1.6.1 Monotonicity and Continuity

lemma *nAct-mcont*:
shows *mcont lSup lprefix Sup op* ≤ (*nAct c n*)
⟨*proof*⟩

lemma *nAct-mono*:
assumes $n \leq n'$
shows $\langle c\ \#_n\ t\rangle \leq \langle c\ \#_{n'}\ t\rangle$
⟨*proof*⟩

lemma *nAct-strict-mono-back*:
assumes $\langle c\ \#_n\ t\rangle < \langle c\ \#_{n'}\ t\rangle$
shows $n < n'$
⟨*proof*⟩

1.6.2 Not Active

lemma *nAct-not-active*[*simp*]:
fixes *n*::*nat*
and *n'*::*nat*
and *t*::(*cnf llist*)
and *c*::'*id*
assumes *enat i* < *llength t*
and ¬ $\|c\|_{lnth\ t\ i}$
shows $\langle c\ \#_{Suc\ i}\ t\rangle = \langle c\ \#_i\ t\rangle$
⟨*proof*⟩

lemma *nAct-not-active-same*:
assumes *enat n* ≤ (*n'*::*enat*)
and *n'*−*1* < *llength t*
and ∄*k*. *enat k*≥*n* ∧ *k*<*n'* ∧ $\|c\|_{lnth\ t\ k}$
shows $\langle c\ \#_{n'}\ t\rangle = \langle c\ \#_n\ t\rangle$
⟨*proof*⟩

1.6.3 Active

lemma *nAct-active*[*simp*]:
fixes *n*::*nat*
and *n'*::*nat*
and *t*::(*cnf llist*)
and *c*::'*id*
assumes *enat i* < *llength t*
and $\|c\|_{lnth\ t\ i}$
shows $\langle c\ \#_{Suc\ i}\ t\rangle$ = *eSuc* ($\langle c\ \#_i\ t\rangle$)
⟨*proof*⟩

lemma *nAct-active-suc*:
fixes *n*::*nat*
and *n'*::*enat*
and *t*::(*cnf llist*)
and *c*::'*id*
assumes ¬ *lfinite t* ∨ *n'*−*1* < *llength t*

and $n \leq i$
and *enat* $i < n'$
and $\|c\|_{lnth\ t\ i}$
and $\forall i'.\ (n \leq i' \wedge enat\ i' < n' \wedge i' < llength\ t \wedge \|c\|_{lnth\ t\ i'}) \longrightarrow (i' = i)$
shows $\langle c\ \#_{n'}\ t\rangle = eSuc\ (\langle c\ \#_n\ t\rangle)$
⟨*proof*⟩

lemma *nAct-less*:
assumes *enat* $k < llength\ t$
and $n \leq k$
and $k < (n'::enat)$
and $\|c\|_{lnth\ t\ k}$
shows $\langle c\ \#_n\ t\rangle < \langle c\ \#_{n'}\ t\rangle$
⟨*proof*⟩

lemma *nAct-less-active*:
assumes $n' - 1 < llength\ t$
and $\langle c\ \#_{enat\ n}\ t\rangle < \langle c\ \#_{n'}\ t\rangle$
shows $\exists i{\geq}n.\ i{<}n' \wedge \|c\|_{lnth\ t\ i}$
⟨*proof*⟩

1.6.4 Same and Not Same

lemma *nAct-same-not-active*:
assumes $\langle c\ \#_{n'}\ inf\text{-}llist\ t\rangle = \langle c\ \#_n\ inf\text{-}llist\ t\rangle$
shows $\forall k{\geq}n.\ k{<}n' \longrightarrow \neg\ \|c\|_{t\ k}$
⟨*proof*⟩

lemma *nAct-not-same-active*:
assumes $\langle c\ \#_{enat\ n}\ t\rangle < \langle c\ \#_{n'}\ t\rangle$
and $\neg\ lfinite\ t \vee n' - 1 < llength\ t$
shows $\exists (i::nat){\geq}n.\ enat\ i{<}\ n' \wedge i{<}llength\ t \wedge \|c\|_{lnth\ t\ i}$
⟨*proof*⟩

lemma *nAct-less-llength-active*:
assumes $x < llength\ (\pi_c(t))$
and $enat\ x = \langle c\ \#_{enat\ n'}\ t\rangle$
shows $\exists (i::nat){\geq}n'.\ i{<}llength\ t \wedge \|c\|_{lnth\ t\ i}$
⟨*proof*⟩

lemma *nAct-exists*:
assumes $x < llength\ (\pi_c(t))$
shows $\exists (n'::nat).\ enat\ x = \langle c\ \#_{n'}\ t\rangle$
⟨*proof*⟩

1.7 Projection and Activation

In the following we provide some properties about the relationship between the projection and activations operator.

lemma *nAct-le-proj*:
$\langle c\ \#_n\ t\rangle \leq llength\ (\pi_c(t))$
⟨*proof*⟩

lemma *proj-nAct*:
assumes $(enat\ n < llength\ t)$

shows $\pi_c(ltake\ n\ t) = ltake\ (\langle c\ \#_n\ t\rangle)\ (\pi_c(t))$ (**is** *?lhs = ?rhs*)
⟨*proof*⟩

lemma *proj-active-nth*:
assumes $enat\ (Suc\ i) < llength\ t\ \|c\|_{lnth\ t\ i}$
shows $lnth\ (\pi_c(t))\ (the\text{-}enat\ (\langle c\ \#_i\ t\rangle)) = \sigma_c(lnth\ t\ i)$
⟨*proof*⟩

lemma *nAct-eq-proj*:
assumes $\neg(\exists\, i{\geq}n.\ \|c\|_{lnth\ t\ i})$
shows $\langle c\ \#_n\ t\rangle = llength\ (\pi_c(t))$ (**is** *?lhs = ?rhs*)
⟨*proof*⟩

lemma *nAct-llength-proj*:
assumes $\exists\, i{\geq}n.\ \|c\|_{t\ i}$
shows $llength\ (\pi_c(inf\text{-}llist\ t)) \geq eSuc\ (\langle c\ \#_n\ inf\text{-}llist\ t\rangle)$
⟨*proof*⟩

1.8 Least not Active

In the following, we introduce an operator to obtain the least point in time before a certain point in time where a component was deactivated.

definition $lNAct :: 'id \Rightarrow (nat \Rightarrow cnf) \Rightarrow nat \Rightarrow nat\ (\langle\text{-} \leftarrow \text{-}\rangle_{\text{-}})$
where $\langle c \leftarrow t\rangle_n \equiv (LEAST\ n'.\ n{=}n' \vee (n'{<}n \wedge (\nexists k.\ k{\geq}n' \wedge k{<}n \wedge \|c\|_{t\ k})))$

lemma *lNact0*[*simp*]:
$\langle c \leftarrow t\rangle_0 = 0$
⟨*proof*⟩

lemma *lNact-least*:
assumes $n{=}n' \vee n'{<}n \wedge (\nexists k.\ k{\geq}n' \wedge k{<}n \wedge \|c\|_{t\ k})$
shows $\langle c \leftarrow t\rangle_n \leq n'$
⟨*proof*⟩

lemma *lNAct-ex*: $\langle c \leftarrow t\rangle_n{=}n \vee \langle c \leftarrow t\rangle_n{<}n \wedge (\nexists k.\ k{\geq}\langle c \leftarrow t\rangle_n \wedge k{<}n \wedge \|c\|_{t\ k})$
⟨*proof*⟩

lemma *lNact-notActive*:
fixes $c\ t\ n\ k$
assumes $k{\geq}\langle c \leftarrow t\rangle_n$
and $k{<}n$
shows $\neg\|c\|_{t\ k}$
⟨*proof*⟩

lemma *lNactGe*:
fixes $c\ t\ n\ n'$
assumes $n' \geq \langle c \leftarrow t\rangle_n$
and $\|c\|_{t\ n'}$
shows $n' \geq n$
⟨*proof*⟩

lemma *lNactLe*[*simp*]:
fixes $n\ n'$
shows $\langle c \leftarrow t\rangle_n \leq n$
⟨*proof*⟩

lemma *lNactLe-nact*:
fixes $n\ n'$
assumes $n'{=}n \vee (n'{<}n \wedge (\nexists k.\ k{\geq}n' \wedge k{<}n \wedge \|c\|_{t\ k}))$
shows $\langle c \leftarrow t\rangle_n \leq n'$
⟨*proof*⟩

lemma *lNact-active*:
fixes *cid t n*
assumes $\forall k{<}n.\ \|cid\|_{t\ k}$
shows $\langle cid \leftarrow t\rangle_n = n$
⟨*proof*⟩

lemma *nAct-mono-back*:
fixes *c t* **and** *n* **and** n'
assumes $\langle c\ \#_{n'}\ inf\text{-}llist\ t\rangle \geq \langle c\ \#_n\ inf\text{-}llist\ t\rangle$
shows $n'{\geq}\langle c \leftarrow t\rangle_n$
⟨*proof*⟩

lemma *nAct-mono-lNact*:
assumes $\langle c \leftarrow t\rangle_n \leq n'$
shows $\langle c\ \#_n\ inf\text{-}llist\ t\rangle \leq \langle c\ \#_{n'}\ inf\text{-}llist\ t\rangle$
⟨*proof*⟩

1.9 Next Active

In the following, we introduce an operator to obtain the next point in time when a component is activated.

definition *nxtAct* :: *'id* ⇒ (*nat* ⇒ *cnf*) ⇒ *nat* ⇒ *nat* (⟨- → -⟩-)
where $\langle c \rightarrow t\rangle_n \equiv (THE\ n'.\ n'{\geq}n \wedge \|c\|_{t\ n'} \wedge (\nexists k.\ k{\geq}n \wedge k{<}n' \wedge \|c\|_{t\ k}))$

lemma *nxtActI*:
fixes *n*::*nat*
and *t*::*nat* ⇒ *cnf*
and *c*::*'id*
assumes $\exists i{\geq}n.\ \|c\|_{t\ i}$
shows $\langle c \rightarrow t\rangle_n \geq n \wedge \|c\|_{t\ \langle c \rightarrow t\rangle_n} \wedge (\nexists k.\ k{\geq}n \wedge k{<}\langle c \rightarrow t\rangle_n \wedge \|c\|_{t\ k})$
⟨*proof*⟩

lemma *nxtActLe*:
fixes $n\ n'$
assumes $\exists i{\geq}n.\ \|c\|_{t\ i}$
shows $n \leq \langle c \rightarrow t\rangle_n$
⟨*proof*⟩

lemma *nxtAct-active*:
fixes *i*::*nat*
and *t*::*nat* ⇒ *cnf*
and *c*::*'id*
assumes $\|c\|_{t\ i}$
shows $\langle c \rightarrow t\rangle_i = i$ ⟨*proof*⟩

lemma *nxtActive-no-active*:
assumes $\exists!i.\ i{\geq}n \wedge \|c\|_{t\ i}$
shows $\neg\ (\exists\, i'{\geq}Suc\ \langle c \rightarrow t\rangle_n.\ \|c\|_{t\ i'})$

⟨*proof*⟩

lemma *nxt-geq-lNact*[*simp*]:
assumes $\exists\, i{\geq}n.\ \|c\|_{t\ i}$
shows $\langle c \rightarrow t\rangle_n {\geq} \langle c \leftarrow t\rangle_n$
⟨*proof*⟩

lemma *active-geq-nxtAct*:
assumes $\|c\|_{t\ i}$
and *the-enat* $(\langle c\ \#_i$ *inf-llist* $t\rangle) {\geq}$ *the-enat* $(\langle c\ \#_n$ *inf-llist* $t\rangle)$
shows $i {\geq} \langle c \rightarrow t\rangle_n$
⟨*proof*⟩

lemma *nAct-same*:
assumes $\langle c \leftarrow t\rangle_n \leq n'$ **and** $n' \leq \langle c \rightarrow t\rangle_n$
shows *the-enat* $(\langle c\ \#_{enat\ n'}$ *inf-llist* $t\rangle)$ = *the-enat* $(\langle c\ \#_{enat\ n}$ *inf-llist* $t\rangle)$
⟨*proof*⟩

lemma *nAct-mono-nxtAct*:
assumes $\exists\, i{\geq}n.\ \|c\|_{t\ i}$
and $\langle c \rightarrow t\rangle_n \leq n'$
shows $\langle c\ \#_n$ *inf-llist* $t\rangle \leq \langle c\ \#_{n'}$ *inf-llist* $t\rangle$
⟨*proof*⟩

1.10 Last Activation

In the following we introduce an operator to obtain the latest point in time where a certain component was activated within a certain configuration trace.

definition *lActive* :: *'id* ⇒ (*nat* ⇒ *cnf*) ⇒ *nat* (⟨- ∧ -⟩)
where $\langle c \wedge t\rangle \equiv (GREATEST\ i.\ \|c\|_{t\ i})$

lemma *lActive-active*:
assumes $\|c\|_{t\ i}$
and $\forall\, n' > n.\ \neg\ (\|c\|_{t\ n'})$
shows $\|c\|_{t\ (\langle c \wedge t\rangle)}$
⟨*proof*⟩

lemma *lActive-less*:
assumes $\|c\|_{t\ i}$
and $\forall\, n' > n.\ \neg\ (\|c\|_{t\ n'})$
shows $\langle c \wedge t\rangle \leq n$
⟨*proof*⟩

lemma *lActive-greatest*:
assumes $\|c\|_{t\ i}$
and $\forall\, n' > n.\ \neg\ (\|c\|_{t\ n'})$
shows $i \leq \langle c \wedge t\rangle$
⟨*proof*⟩

lemma *lActive-greater-active*:
assumes $n > \langle c \wedge t\rangle$
and $\forall\, n'' > n'.\ \neg\ \|c\|_{t\ n''}$
shows $\neg\ \|c\|_{t\ n}$
⟨*proof*⟩

lemma *lActive-greater-active-all*:
assumes $\forall\, n'' > n'.\ \neg\ \|c\|_{t\ n''}$
shows $\neg(\exists\, n > \langle c \wedge t\rangle.\ \|c\|_{t\ n})$
⟨*proof*⟩

lemma *lActive-equality*:
assumes $\|c\|_{t\ i}$
and $(\bigwedge x.\ \|c\|_{t\ x} \Longrightarrow x \leq i)$
shows $\langle c \wedge t\rangle = i$ ⟨*proof*⟩

lemma *nxtActive-lactive*:
assumes $\exists\, i{\geq}n.\ \|c\|_{t\ i}$
and $\neg\ (\exists\, i{>}\langle c \rightarrow t\rangle_n.\ \|c\|_{t\ i})$
shows $\langle c \rightarrow t\rangle_n{=}\langle c \wedge t\rangle$
⟨*proof*⟩

1.11 Mapping Time Points

In the following we introduce two operators to map time-points between configuration traces and behavior traces.

1.11.1 Configuration Trace to Behavior Trace

First we provide an operator which maps a point in time of a configuration trace to the corresponding point in time of a behavior trace.

definition *cnf2bhv* :: *'id* ⇒ (*nat* ⇒ *cnf*) ⇒ *nat* ⇒ *nat* (*-↓-(-)* [*150*,*150*,*150*] *110*)
where $_c{\downarrow_t}(n) \equiv$ *the-enat*(*llength* (π_c(*inf-llist t*))) − *1* + (*n* − ⟨*c* ∧ *t*⟩)

lemma *cnf2bhv-mono*:
assumes $n'{\geq}n$
shows $_c{\downarrow_t}(n') \geq {}_c{\downarrow_t}(n)$
⟨*proof*⟩

lemma *cnf2bhv-mono-strict*:
assumes $n{\geq}\langle c \wedge t\rangle$ **and** $n'{>}n$
shows $_c{\downarrow_t}(n') > {}_c{\downarrow_t}(n)$
⟨*proof*⟩

Note that the functions are nat, that means that also in the case the difference is negative they will return a 0!

lemma *cnf2bhv-ge-llength*[*simp*]:
assumes $n{\geq}\langle c \wedge t\rangle$
shows $_c{\downarrow_t}(n) \geq$ *the-enat*(*llength* (π_c(*inf-llist t*))) − *1*
⟨*proof*⟩

lemma *cnf2bhv-greater-llength*[*simp*]:
assumes $n{>}\langle c \wedge t\rangle$
shows $_c{\downarrow_t}(n) >$ *the-enat*(*llength* (π_c(*inf-llist t*))) − *1*
⟨*proof*⟩

lemma *cnf2bhv-suc*[*simp*]:
assumes $n{\geq}\langle c \wedge t\rangle$
shows $_c{\downarrow_t}(Suc\ n) = Suc\ ({}_c{\downarrow_t}(n))$
⟨*proof*⟩

lemma *cnf2bhv-lActive*[*simp*]:
shows $_c\downarrow_t(\langle c \wedge t\rangle) = \textit{the-enat}(\textit{llength}\ (\pi_c(\textit{inf-llist}\ t))) - 1$
⟨*proof*⟩

lemma *cnf2bhv-lnth-lappend*:
assumes *act*: $\exists\, i.\ \|c\|_{t\ i}$
and *nAct*: $\nexists\, i.\ i{\geq}n \wedge \|c\|_{t\ i}$
shows $\textit{lnth}\ ((\pi_c(\textit{inf-llist}\ t))\ @_l\ (\textit{inf-llist}\ t'))\ (_c\downarrow_t(n)) = \textit{lnth}\ (\textit{inf-llist}\ t')\ (n - \langle c \wedge t\rangle - 1)$
(**is** *?lhs* = *?rhs*)
⟨*proof*⟩

lemma *nAct-cnf2proj-Suc-dist*:
assumes $\exists\, i{\geq}n.\ \|c\|_{t\ i}$
and $\neg(\exists\, i{>}\langle c \rightarrow t\rangle_n.\ \|c\|_{t\ i})$
shows $\textit{Suc}\ (\textit{the-enat}\ \langle c\ \#_{\textit{enat}\ n}\textit{inf-llist}\ t\rangle){=}_c\downarrow_t(\textit{Suc}\ \langle c \rightarrow t\rangle_n)$
⟨*proof*⟩

1.11.2 Behavior Trace to Configuration Trace

Next we define an operator to map a point in time of a behavior trace back to a corresponding point in time for a configuration trace.

definition *bhv2cnf* :: *'id* ⇒ (*nat* ⇒ *cnf*) ⇒ *nat* ⇒ *nat* (-↑-(-) [*150*,*150*,*150*] *110*)
where $_c\uparrow_t(n) \equiv \langle c \wedge t\rangle + (n - (\textit{the-enat}(\textit{llength}\ (\pi_c(\textit{inf-llist}\ t))) - 1))$

lemma *bhv2cnf-mono*:
assumes $n'{\geq}n$
shows $_c\uparrow_t(n') \geq {}_c\uparrow_t(n)$
⟨*proof*⟩

lemma *bhv2cnf-mono-strict*:
assumes $n'{>}n$
and $n \geq \textit{the-enat}\ (\textit{llength}\ (\pi_c(\textit{inf-llist}\ t))) - 1$
shows $_c\uparrow_t(n') > {}_c\uparrow_t(n)$
⟨*proof*⟩

Note that the functions are nat, that means that also in the case the difference is negative they will return a 0!

lemma *bhv2cnf-ge-lActive*[*simp*]:
shows $_c\uparrow_t(n) \geq \langle c \wedge t\rangle$
⟨*proof*⟩

lemma *bhv2cnf-greater-lActive*[*simp*]:
assumes $n{>}\textit{the-enat}(\textit{llength}\ (\pi_c(\textit{inf-llist}\ t))) - 1$
shows $_c\uparrow_t(n) > \langle c \wedge t\rangle$
⟨*proof*⟩

lemma *bhv2cnf-lActive*[*simp*]:
assumes $\exists\, i.\ \|c\|_{t\ i}$
and *lfinite* $(\pi_c(\textit{inf-llist}\ t))$
shows $_c\uparrow_t(\textit{the-enat}(\textit{llength}\ (\pi_c(\textit{inf-llist}\ t)))) = \textit{Suc}\ (\langle c \wedge t\rangle)$
⟨*proof*⟩

1.11.3 Relating the Mappings

In the following we provide some properties about the relationship between the two mapping operators.

lemma *bhv2cnf-cnf2bhv*:
assumes $n \geq \langle c \wedge t \rangle$
shows ${}_c\uparrow_t({}_c\downarrow_t(n)) = n$ (**is** *?lhs* = *?rhs*)
⟨*proof*⟩

lemma *cnf2bhv-bhv2cnf*:
assumes $n \geq$ *the-enat* (*llength* (π_c(*inf-llist t*))) − *1*
shows ${}_c\downarrow_t({}_c\uparrow_t(n)) = n$ (**is** *?lhs* = *?rhs*)
⟨*proof*⟩

lemma *p2c-mono-c2p*:
assumes $n \geq \langle c \wedge t \rangle$
and $n' \geq {}_c\downarrow_t(n)$
shows ${}_c\uparrow_t(n') \geq n$
⟨*proof*⟩

lemma *p2c-mono-c2p-strict*:
assumes $n \geq \langle c \wedge t \rangle$
and $n <_c\uparrow_t(n')$
shows ${}_c\downarrow_t(n) < n'$
⟨*proof*⟩

lemma *c2p-mono-p2c*:
assumes $n \geq$ *the-enat* (*llength* (π_c(*inf-llist t*))) − *1*
and $n' \geq {}_c\uparrow_t(n)$
shows ${}_c\downarrow_t(n') \geq n$
⟨*proof*⟩

lemma *c2p-mono-p2c-strict*:
assumes $n \geq$ *the-enat* (*llength* (π_c(*inf-llist t*))) − *1*
and $n <_c\downarrow_t(n')$
shows ${}_c\uparrow_t(n) < n'$
⟨*proof*⟩

end

end

2 A Calculus for Dynamic Architectures

The following theory formalizes our calculus for dynamic architectures [2, 3] and verifies its soundness. The calculus allows to reason about temporal-logic specifications of component behavior in a dynamic setting. The theory is based on our theory of configuration traces and introduces the notion of behavior trace assertion to specify component behavior in a dynamic setting.

theory *Dynamic-Architecture-Calculus*
imports *Configuration-Traces*
begin

2.1 Extended Natural Numbers

We first provide one additional property for extended natural numbers.

lemma *the-enat-mono*[*simp*]:
assumes $m \neq \infty$
and $n \leq m$
shows *the-enat* $n \leq$ *the-enat* m
⟨*proof*⟩

2.2 Lazy Lists

Finally, we provide an additional property for lazy lists.

lemma *llength-geq-enat-lfiniteD*: *llength xs* $\leq$ *enat n* $\Longrightarrow$ *lfinite xs*
⟨*proof*⟩

context *dynamic-component*
begin

2.3 Dynamic Evaluation of Temporal Operators

In the following we introduce a function to evaluate a behavior trace assertion over a given configuration trace.

definition *eval*:: $'id \Rightarrow (nat \Rightarrow cnf) \Rightarrow (nat \Rightarrow 'cmp) \Rightarrow nat$
$\Rightarrow ((nat \Rightarrow 'cmp) \Rightarrow nat \Rightarrow bool) \Rightarrow bool$
where *eval cid t t′ n* $\gamma \equiv$
$(\exists\, i{\geq}n.\ \|cid\|_{t\ i}) \wedge \gamma\ (lnth\ ((\pi_{cid}(inf\text{-}llist\ t))\ @_l\ (inf\text{-}llist\ t'))\ (the\text{-}enat(\langle cid\ \#_n\ inf\text{-}llist\ t\rangle)) \vee$
$(\exists\, i.\ \|cid\|_{t\ i}) \wedge (\nexists\, i'.\ i'{\geq}n \wedge \|cid\|_{t\ i'}) \wedge \gamma\ (lnth\ ((\pi_{cid}(inf\text{-}llist\ t))\ @_l\ (inf\text{-}llist\ t'))\ ({}_{cid}{\downarrow_t}(n)) \vee$
$(\nexists\, i.\ \|cid\|_{t\ i}) \wedge \gamma\ (lnth\ ((\pi_{cid}(inf\text{-}llist\ t))\ @_l\ (inf\text{-}llist\ t'))\ n$

eval takes a component identifier *cid*, a configuration trace t, a behavior trace t', and point in time n and evaluates behavior trace assertion γ as follows:

- If component *cid* is again activated in the future, γ is evaluated at the next point in time where *cid* is active in t.
- If component *cid* is not again activated in the future but it is activated at least once in t, then γ is evaluated at the point in time given by ${}_{cid}{\downarrow_t}n$.
- If component *cid* is never active in t, then γ is evaluated at time point n.

The following proposition evaluates definition *eval* by showing that a behavior trace assertion γ holds over configuration trace t and continuation t' whenever it holds for the concatenation of the corresponding projection with t'.

proposition *eval-corr*:
eval cid t t′ 0 $\gamma \longleftrightarrow \gamma$ (*lnth* ((*π* *cid*(*inf-llist t*)) @*l* (*inf-llist t′*))) *0*
⟨*proof*⟩

2.3.1 Simplification Rules

lemma *validCI-act*[*simp*]:
assumes $\exists\, i{\geq}n.\ \|cid\|_{t\ i}$
and γ (*lnth* ((*π* *cid*(*inf-llist t*)) @*l* (*inf-llist t′*))) (*the-enat*(⟨*cid* #*n* *inf-llist t*⟩))
shows *eval cid t t′ n* γ

⟨*proof*⟩

lemma *validCI-cont*[*simp*]:
assumes $\exists\, i.\ \|cid\|_{t\ i}$
and $\nexists\, i'.\ i' \geq n \wedge \|cid\|_{t\ i'}$
and $\gamma\ (lnth\ ((\pi_{cid}(inf\text{-}llist\ t))\ @_l\ (inf\text{-}llist\ t'))\ (_{cid}\downarrow_t(n))$
shows *eval cid t t′ n γ*
⟨*proof*⟩

lemma *validCI-not-act*[*simp*]:
assumes $\nexists\, i.\ \|cid\|_{t\ i}$
and $\gamma\ (lnth\ ((\pi_{cid}(inf\text{-}llist\ t))\ @_l\ (inf\text{-}llist\ t'))\ n$
shows *eval cid t t′ n γ*
⟨*proof*⟩

lemma *validCE-act*[*simp*]:
assumes $\exists\, i \geq n.\ \|cid\|_{t\ i}$
and *eval cid t t′ n γ*
shows $\gamma\ (lnth\ ((\pi_{cid}(inf\text{-}llist\ t))\ @_l\ (inf\text{-}llist\ t'))\ (the\text{-}enat(\langle cid\ \#_n\ inf\text{-}llist\ t\rangle))$
⟨*proof*⟩

lemma *validCE-cont*[*simp*]:
assumes $\exists\, i.\ \|cid\|_{t\ i}$
and $\nexists\, i'.\ i' \geq n \wedge \|cid\|_{t\ i'}$
and *eval cid t t′ n γ*
shows $\gamma\ (lnth\ ((\pi_{cid}(inf\text{-}llist\ t))\ @_l\ (inf\text{-}llist\ t'))\ (_{cid}\downarrow_t(n))$
⟨*proof*⟩

lemma *validCE-not-act*[*simp*]:
assumes $\nexists\, i.\ \|cid\|_{t\ i}$
and *eval cid t t′ n γ*
shows $\gamma\ (lnth\ ((\pi_{cid}(inf\text{-}llist\ t))\ @_l\ (inf\text{-}llist\ t'))\ n$
⟨*proof*⟩

2.3.2 No Activations

proposition *validity1*:
assumes $n \leq n'$
and $\exists\, i \geq n'.\ \|c\|_{t\ i}$
and $\forall\, k \geq n.\ k < n' \longrightarrow \neg\ \|c\|_{t\ k}$
shows *eval c t t′ n γ* $\Longrightarrow$ *eval c t t′ n′ γ*
⟨*proof*⟩

proposition *validity2*:
assumes $n \leq n'$
and $\exists\, i \geq n'.\ \|c\|_{t\ i}$
and $\forall\, k \geq n.\ k < n' \longrightarrow \neg\ \|c\|_{t\ k}$
shows *eval c t t′ n′ γ* $\Longrightarrow$ *eval c t t′ n γ*
⟨*proof*⟩

2.4 Basic Operators

In the following we introduce some basic operators for behavior trace assertions.

2.4.1 Predicates

Every predicate can be transformed to a behavior trace assertion.

definition *pred* :: *bool* ⇒ ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*)
  where *pred P* ≡ λ *t n*. *P*

lemma *predI*[*intro*]:
  fixes *cid t t' n P*
  assumes *P*
  shows *eval cid t t' n* (*pred P*)
⟨*proof*⟩

lemma *predE*[*elim*]:
  fixes *cid t t' n P*
  assumes *eval cid t t' n* (*pred P*)
  shows *P*
⟨*proof*⟩

2.4.2 True and False

definition *true* :: (*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*
  where *true* ≡ λ*t n*. *HOL.True*

definition *false* :: (*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*
  where *false* ≡ λ*t n*. *HOL.False*

2.4.3 Implication

definition *imp* :: ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*) ⇒ ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*)
  ⇒ ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*) (**infixl** $\longrightarrow^b$ *10*)
  where $\gamma \longrightarrow^b \gamma' \equiv \lambda\ t\ n.\ \gamma\ t\ n \longrightarrow \gamma'\ t\ n$

lemma *impI*[*intro*!]:
  assumes *eval cid t t' n* $\gamma \longrightarrow$ *eval cid t t' n* γ'
  shows *eval cid t t' n* ($\gamma \longrightarrow^b \gamma'$)
⟨*proof*⟩

lemma *impE*[*elim*!]:
  assumes *eval cid t t' n* ($\gamma \longrightarrow^b \gamma'$)
  shows *eval cid t t' n* $\gamma \longrightarrow$ *eval cid t t' n* γ'
⟨*proof*⟩

2.4.4 Disjunction

definition *or* :: ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*) ⇒ ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*)
  ⇒ ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*) (**infixl** $\vee^b$ *15*)
  where $\gamma \vee^b \gamma' \equiv \lambda\ t\ n.\ \gamma\ t\ n \vee \gamma'\ t\ n$

lemma *orI*[*intro*!]:
  assumes *eval cid t t' n* $\gamma \vee$ *eval cid t t' n* γ'
  shows *eval cid t t' n* ($\gamma \vee^b \gamma'$)
⟨*proof*⟩

lemma *orE*[*elim*!]:
  assumes *eval cid t t' n* ($\gamma \vee^b \gamma'$)
  shows *eval cid t t' n* $\gamma \vee$ *eval cid t t' n* γ'

⟨*proof*⟩

2.4.5 Conjunction

definition *and* :: ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*) ⇒ ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*)
⇒ ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*) (**infixl** $\wedge^b$ *20*)
where $\gamma \wedge^b \gamma' \equiv \lambda\ t\ n.\ \gamma\ t\ n \wedge \gamma'\ t\ n$

lemma *andI*[*intro*!]:
assumes *eval cid t t' n* $\gamma \wedge$ *eval cid t t' n* γ'
shows *eval cid t t' n* ($\gamma \wedge^b \gamma'$)
⟨*proof*⟩

lemma *andE*[*elim*!]:
assumes *eval cid t t' n* ($\gamma \wedge^b \gamma'$)
shows *eval cid t t' n* $\gamma \wedge$ *eval cid t t' n* γ'
⟨*proof*⟩

2.4.6 Negation

definition *not* :: ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*) ⇒ ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*) ($\neg^b$ - [*19*] *19*)
where $\neg^b\ \gamma \equiv \lambda\ t\ n.\ \neg\ \gamma\ t\ n$

lemma *notI*[*intro*!]:
assumes ¬ *eval cid t t' n* γ
shows *eval cid t t' n* ($\neg^b\ \gamma$)
⟨*proof*⟩

lemma *notE*[*elim*!]:
assumes *eval cid t t' n* ($\neg^b\ \gamma$)
shows ¬ *eval cid t t' n* γ
⟨*proof*⟩

2.4.7 Quantifiers

definition *all* :: (*'a* ⇒ ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*))
⇒ ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*) (**binder** $\forall_b$ *10*)
where *all P* ≡ λ*t n*. (∀ *y*. (*P y t n*))

lemma *allI*[*intro*!]:
assumes ∀ *p*. *eval cid t t' n* (γ *p*)
shows *eval cid t t' n* (*all* (λ*p*. γ *p*))
⟨*proof*⟩

lemma *allE*[*elim*!]:
assumes *eval cid t t' n* (*all* (λ*p*. γ *p*))
shows ∀ *p*. *eval cid t t' n* (γ *p*)
⟨*proof*⟩

definition *exists* :: (*'a* ⇒ ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*))
⇒ ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*) (**binder** $\exists_b$ *10*)
where *exists P* ≡ λ*t n*. (∃ *y*. (*P y t n*))

lemma *existsI*[*intro*!]:
assumes ∃ *p*. *eval cid t t' n* (γ *p*)
shows *eval cid t t' n* (*exists* (λ*p*. γ *p*))

⟨*proof*⟩

lemma *existsE*[*elim*!]:
  assumes *eval cid t t′ n* (*exists* (λ*p*. *γ p*))
  shows ∃ *p*. *eval cid t t′ n* (*γ p*)
⟨*proof*⟩

2.5 Temporal Operators

We are now able to formalize all the rules of the calculus presented in [3].

2.5.1 Atomic Assertions

First we provide rules for basic behavior assertions.

definition *ass* :: (′*cmp* ⇒ *bool*) ⇒ ((*nat* ⇒ ′*cmp*) ⇒ *nat* ⇒ *bool*)
  where *ass φ* ≡ λ *t n*. *φ* (*t n*)

lemma *assIA*[*intro*]:
  fixes *c*::′*id*
    and *t*::*nat* ⇒ *cnf*
    and *t′*::*nat* ⇒ ′*cmp*
    and *n*::*nat*
  assumes ∃ *i*≥*n*. ‖*c*‖$_{t\ i}$
    and *φ* (*σ*$_c$(*t* ⟨*c* → *t*⟩$_n$))
  shows *eval c t t′ n* (*ass φ*)
⟨*proof*⟩

lemma *assIN1*[*intro*]:
  fixes *c*::′*id*
    and *t*::*nat* ⇒ *cnf*
    and *t′*::*nat* ⇒ ′*cmp*
    and *n*::*nat*
  assumes *act*: ∃ *i*. ‖*c*‖$_{t\ i}$
    and *nAct*: ∄ *i*. *i*≥*n* ∧ ‖*c*‖$_{t\ i}$
    and *al*: *φ* (*t′* (*n* − ⟨*c* ∧ *t*⟩ − *1*))
  shows *eval c t t′ n* (*ass φ*)
⟨*proof*⟩

lemma *assIN2*[*intro*]:
  fixes *c*::′*id*
    and *t*::*nat* ⇒ *cnf*
    and *t′*::*nat* ⇒ ′*cmp*
    and *n*::*nat*
  assumes *nAct*: ∄ *i*. ‖*c*‖$_{t\ i}$
    and *al*: *φ* (*t′ n*)
  shows *eval c t t′ n* (*ass φ*)
⟨*proof*⟩

lemma *assIANow*[*intro*]:
  fixes *t n c φ*
  assumes *φ* (*σ*$_c$(*t n*))
    and ‖*c*‖$_{t\ n}$
  shows *eval c t t′ n* (*ass φ*)
⟨*proof*⟩

lemma *assEA*[*elim*]:
  fixes *c*::*'id*
    and *t*::*nat* ⇒ *cnf*
    and *t'*::*nat* ⇒ *'cmp*
    and *n*::*nat*
    and *i*::*nat*
  assumes ∃ *i*≥*n*. ‖*c*‖$_{t\ i}$
    and *eval c t t' n* (*ass φ*)
  shows *φ* (*σ*$_c$(*t* ⟨*c* → *t*⟩$_n$))
⟨*proof*⟩

lemma *assEN1*[*elim*]:
  fixes *c*::*'id*
    and *t*::*nat* ⇒ *cnf*
    and *t'*::*nat* ⇒ *'cmp*
    and *n*::*nat*
  assumes *act*: ∃ *i*. ‖*c*‖$_{t\ i}$
    and *nAct*: ∄ *i*. *i*≥*n* ∧ ‖*c*‖$_{t\ i}$
    and *al*: *eval c t t' n* (*ass φ*)
  shows *φ* (*t'* (*n* − ⟨*c* ∧ *t*⟩ − *1*))
⟨*proof*⟩

lemma *assEN2*[*elim*]:
  fixes *c*::*'id*
    and *t*::*nat* ⇒ *cnf*
    and *t'*::*nat* ⇒ *'cmp*
    and *n*::*nat*
  assumes *nAct*: ∄ *i*. ‖*c*‖$_{t\ i}$
    and *al*: *eval c t t' n* (*ass φ*)
  shows *φ* (*t'* *n*)
⟨*proof*⟩

lemma *assEANow*[*elim*]:
  fixes *t n c φ*
  assumes *eval c t t' n* (*ass φ*)
    and ‖*c*‖$_{t\ n}$
  shows *φ* (*σ*$_c$(*t n*))
⟨*proof*⟩

2.5.2 Next Operator

definition *nxt* :: ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*) ⇒ ((*nat* ⇒ *'cmp*) ⇒ *nat* ⇒ *bool*) (○(-) *24*)
  where ○(*γ*) ≡ λ *t n*. *γ t* (*Suc n*)

lemma *nxtIA*[*intro*]:
  fixes *c*::*'id*
    and *t*::*nat* ⇒ *cnf*
    and *t'*::*nat* ⇒ *'cmp*
    and *n*::*nat*
  assumes ∃ *i*≥*n*. ‖*c*‖$_{t\ i}$
    and ⟦∃ *i*>⟨*c* → *t*⟩$_n$. ‖*c*‖$_{t\ i}$⟧ ⟹ ∃ *n'* ≥ *n*. (∃!*i*. *n*≤*i* ∧ *i*<*n'* ∧ ‖*c*‖$_{t\ i}$) ∧ *eval c t t' n' γ*
    and ⟦¬(∃ *i*>⟨*c* → *t*⟩$_n$. ‖*c*‖$_{t\ i}$)⟧ ⟹ *eval c t t'* (*Suc* ⟨*c* → *t*⟩$_n$) *γ*
  shows *eval c t t' n* (○(*γ*))
⟨*proof*⟩

lemma *nxtIN*[*intro*]:
fixes c::$'id$
and t::$nat \Rightarrow cnf$
and t'::$nat \Rightarrow 'cmp$
and n::nat
assumes $\neg(\exists\, i{\geq}n.\ \|c\|_{t\ i})$
and *eval* $c\ t\ t'\ (Suc\ n)\ \gamma$
shows *eval* $c\ t\ t'\ n\ (\bigcirc(\gamma))$
⟨*proof*⟩

lemma *nxtEA1*[*elim*]:
fixes c::$'id$
and t::$nat \Rightarrow cnf$
and t'::$nat \Rightarrow 'cmp$
and n::nat
assumes $\exists\, i{>}\langle c \rightarrow t\rangle_n.\ \|c\|_{t\ i}$
and *eval* $c\ t\ t'\ n\ (\bigcirc(\gamma))$
and $n'{\geq}n$
and $\exists!i.\ i{\geq}n \wedge i{<}n' \wedge \|c\|_{t\ i}$
shows *eval* $c\ t\ t'\ n'\ \gamma$
⟨*proof*⟩

lemma *nxtEA2*[*elim*]:
fixes c::$'id$
and t::$nat \Rightarrow cnf$
and t'::$nat \Rightarrow 'cmp$
and n::nat
and i
assumes $\exists\, i{\geq}n.\ \|c\|_{t\ i}$ **and** $\neg(\exists\, i{>}\langle c \rightarrow t\rangle_n.\ \|c\|_{t\ i})$
and *eval* $c\ t\ t'\ n\ (\bigcirc(\gamma))$
shows *eval* $c\ t\ t'\ (Suc\ \langle c \rightarrow t\rangle_n)\ \gamma$
⟨*proof*⟩

lemma *NxtEN*[*elim*]:
fixes c::$'id$
and t::$nat \Rightarrow cnf$
and t'::$nat \Rightarrow 'cmp$
and n::nat
assumes $\neg(\exists\, i{\geq}n.\ \|c\|_{t\ i})$
and *eval* $c\ t\ t'\ n\ (\bigcirc(\gamma))$
shows *eval* $c\ t\ t'\ (Suc\ n)\ \gamma$
⟨*proof*⟩

2.5.3 Eventually Operator

definition *evt* :: $((nat \Rightarrow 'cmp) \Rightarrow nat \Rightarrow bool) \Rightarrow ((nat \Rightarrow 'cmp) \Rightarrow nat \Rightarrow bool)$ $(\Diamond(\text{-})\ 23)$
where $\Diamond(\gamma) \equiv \lambda\ t\ n.\ \exists\, n'{\geq}n.\ \gamma\ t\ n'$

lemma *evtIA*[*intro*]:
fixes c::$'id$
and t::$nat \Rightarrow cnf$
and t'::$nat \Rightarrow 'cmp$
and n::nat
and n'::nat
assumes $\exists\, i{\geq}n.\ \|c\|_{t\ i}$
and $n'{\geq}\langle c \leftarrow t\rangle_n$

and $[\![\exists\, i{\geq}n'.\ \|c\|_{t\ i}]\!] \Longrightarrow \exists\, n''{\geq}\langle c \leftarrow t\rangle_{n'}.\ n''{\leq}\ \langle c \rightarrow t\rangle_{n'} \wedge \mathit{eval}\ c\ t\ t'\ n''\ \gamma$
and $[\![\neg(\exists\, i{\geq}n'.\ \|c\|_{t\ i})]\!] \Longrightarrow \mathit{eval}\ c\ t\ t'\ n'\ \gamma$
shows $\mathit{eval}\ c\ t\ t'\ n\ (\Diamond(\gamma))$
⟨*proof*⟩

lemma *evtIN*[*intro*]:
fixes $c{::}'id$
and $t{::}nat \Rightarrow cnf$
and $t'{::}nat \Rightarrow 'cmp$
and $n{::}nat$
and $n'{::}nat$
assumes $\neg(\exists\, i{\geq}n.\ \|c\|_{t\ i})$
and $n'{\geq}n$
and $\mathit{eval}\ c\ t\ t'\ n'\ \gamma$
shows $\mathit{eval}\ c\ t\ t'\ n\ (\Diamond(\gamma))$
⟨*proof*⟩

lemma *evtEA*[*elim*]:
fixes $c{::}'id$
and $t{::}nat \Rightarrow cnf$
and $t'{::}nat \Rightarrow 'cmp$
and $n{::}nat$
assumes $\exists\, i{\geq}n.\ \|c\|_{t\ i}$
and $\mathit{eval}\ c\ t\ t'\ n\ (\Diamond(\gamma))$
shows $\exists\, n'{\geq}\langle c \rightarrow t\rangle_n.$
$(\exists\, i{\geq}n'.\ \|c\|_{t\ i} \wedge (\forall\, n''{\geq}\ \langle c \leftarrow t\rangle_{n'}.\ n''{\leq}\langle c \rightarrow t\rangle_{n'} \longrightarrow \mathit{eval}\ c\ t\ t'\ n''\ \gamma)) \vee$
$(\neg(\exists\, i{\geq}n'.\ \|c\|_{t\ i}) \wedge \mathit{eval}\ c\ t\ t'\ n'\ \gamma)$
⟨*proof*⟩

lemma *evtEN*[*elim*]:
fixes $c{::}'id$
and $t{::}nat \Rightarrow cnf$
and $t'{::}nat \Rightarrow 'cmp$
and $n{::}nat$
and $n'{::}nat$
assumes $\neg(\exists\, i{\geq}n.\ \|c\|_{t\ i})$
and $\mathit{eval}\ c\ t\ t'\ n\ (\Diamond(\gamma))$
shows $\exists\, n'{\geq}n.\ \mathit{eval}\ c\ t\ t'\ n'\ \gamma$
⟨*proof*⟩

2.5.4 Globally Operator

definition *glob* :: $((nat \Rightarrow 'cmp) \Rightarrow nat \Rightarrow bool) \Rightarrow ((nat \Rightarrow 'cmp) \Rightarrow nat \Rightarrow bool)$ $(\Box(\text{-})\ 22)$
where $\Box(\gamma) \equiv \lambda\ t\ n.\ \forall\, n'{\geq}n.\ \gamma\ t\ n'$

lemma *globIA*[*intro*]:
fixes $c{::}'id$
and $t{::}nat \Rightarrow cnf$
and $t'{::}nat \Rightarrow 'cmp$
and $n{::}nat$
assumes $\exists\, i{\geq}n.\ \|c\|_{t\ i}$
and $\bigwedge n'.\ [\![\exists\, i{\geq}n'.\ \|c\|_{t\ i};\ n'{\geq}\langle c \rightarrow t\rangle_n]\!] \Longrightarrow \exists\, n''{\geq}\langle c \leftarrow t\rangle_{n'}.\ n''{\leq}\langle c \rightarrow t\rangle_{n'} \wedge \mathit{eval}\ c\ t\ t'\ n''\ \gamma$
and $\bigwedge n'.\ [\![\neg(\exists\, i{\geq}n'.\ \|c\|_{t\ i});\ n'{\geq}\langle c \rightarrow t\rangle_n]\!] \Longrightarrow \mathit{eval}\ c\ t\ t'\ n'\ \gamma$
shows $\mathit{eval}\ c\ t\ t'\ n\ (\Box(\gamma))$
⟨*proof*⟩

lemma *globIN*[*intro*]:
fixes c::$'id$
and t::$nat \Rightarrow cnf$
and t'::$nat \Rightarrow 'cmp$
and n::nat
assumes $\neg(\exists\, i{\geq}n.\ \|c\|_{t\ i})$
and $\bigwedge n'.\ n'{\geq}n \Longrightarrow eval\ c\ t\ t'\ n'\ \gamma$
shows $eval\ c\ t\ t'\ n\ (\Box(\gamma))$
⟨*proof*⟩

lemma *globEA*[*elim*]:
fixes c::$'id$
and t::$nat \Rightarrow cnf$
and t'::$nat \Rightarrow 'cmp$
and n::nat
and n'::nat
assumes $\exists\, i{\geq}n.\ \|c\|_{t\ i}$
and $eval\ c\ t\ t'\ n\ (\Box(\gamma))$
and $n'{\geq}\langle c \leftarrow t\rangle_n$
shows $eval\ c\ t\ t'\ n'\ \gamma$
⟨*proof*⟩

lemma *globEN*[*elim*]:
fixes c::$'id$
and t::$nat \Rightarrow cnf$
and t'::$nat \Rightarrow 'cmp$
and n::nat
and n'::nat
assumes $\neg(\exists\, i{\geq}n.\ \|c\|_{t\ i})$
and $eval\ c\ t\ t'\ n\ (\Box(\gamma))$
and $n'{\geq}n$
shows $eval\ c\ t\ t'\ n'\ \gamma$
⟨*proof*⟩

2.5.5 Until Operator

definition *until* :: $((nat \Rightarrow 'cmp) \Rightarrow nat \Rightarrow bool) \Rightarrow ((nat \Rightarrow 'cmp) \Rightarrow nat \Rightarrow bool)$
$\Rightarrow ((nat \Rightarrow 'cmp) \Rightarrow nat \Rightarrow bool)$ (**infixl** $\mathfrak{U}$ *21*)
where $\gamma'\ \mathfrak{U}\ \gamma \equiv \lambda\ t\ n.\ \exists\, n''{\geq}n.\ \gamma\ t\ n'' \wedge (\forall\, n'{\geq}n.\ n' < n'' \longrightarrow \gamma'\ t\ n')$

lemma *untilIA*[*intro*]:
fixes c::$'id$
and t::$nat \Rightarrow cnf$
and t'::$nat \Rightarrow 'cmp$
and n::nat
and n'::nat
assumes $\exists\, i{\geq}n.\ \|c\|_{t\ i}$
and $n'{\geq}\langle c \leftarrow t\rangle_n$
and $[\![\exists\, i{\geq}n'.\ \|c\|_{t\ i}]\!] \Longrightarrow \exists\, n''{\geq}\langle c \leftarrow t\rangle_{n'}.\ n''{\leq}\ \langle c \rightarrow t\rangle_{n'} \wedge eval\ c\ t\ t'\ n''\ \gamma \wedge$
$(\forall\, n'''{\geq}\langle c \rightarrow t\rangle_n.\ n'''{<}\ \langle c \leftarrow t\rangle_{n''}$
$\longrightarrow (\exists\, n''''{\geq}\langle c \leftarrow t\rangle_{n'''}.\ n''''{\leq}\ \langle c \rightarrow t\rangle_{n'''} \wedge eval\ c\ t\ t'\ n''''\ \gamma'))$
and $[\![\neg(\exists\, i{\geq}n'.\ \|c\|_{t\ i})]\!] \Longrightarrow eval\ c\ t\ t'\ n'\ \gamma \wedge$
$(\forall\, n''{\geq}\langle c \rightarrow t\rangle_n.\ n''{<}\ n'$
$\longrightarrow ((\exists\, i{\geq}n''.\ \|c\|_{t\ i}) \wedge (\exists\, n'''{\geq}\langle c \leftarrow t\rangle_{n''}.\ n'''{\leq}\ \langle c \rightarrow t\rangle_{n''} \wedge eval\ c\ t\ t'\ n'''\ \gamma')) \vee$
$(\neg(\exists\, i{\geq}n''.\ \|c\|_{t\ i}) \wedge eval\ c\ t\ t'\ n''\ \gamma'))$
shows $eval\ c\ t\ t'\ n\ (\gamma'\ \mathfrak{U}\ \gamma)$

⟨*proof*⟩

lemma *untilIN*[*intro*]:
  fixes c::$'id$
    and t::$nat \Rightarrow cnf$
    and t'::$nat \Rightarrow 'cmp$
    and n::nat
    and n'::nat
  assumes $\neg(\exists\, i{\geq}n.\ \|c\|_{t\ i})$
    and $n'{\geq}n$
    and $eval\ c\ t\ t'\ n'\ \gamma$
    and *a1*: $\bigwedge n''.\ [\![n{\leq}n'';\ n''{<}n']\!] \Longrightarrow eval\ c\ t\ t'\ n''\ \gamma'$
  shows $eval\ c\ t\ t'\ n\ (\gamma'\ \mathfrak{U}\ \gamma)$
⟨*proof*⟩

lemma *untilEA*[*elim*]:
  fixes n::nat
    and n'::nat
    and t::$nat \Rightarrow cnf$
    and t'::$nat \Rightarrow 'cmp$
    and c::$'id$
  assumes $\exists\, i{\geq}n.\ \|c\|_{t\ i}$
    and $eval\ c\ t\ t'\ n\ (\gamma'\ \mathfrak{U}\ \gamma)$
  shows $\exists\, n'{\geq}\langle c \rightarrow t\rangle_n.$
    $((\exists\, i{\geq}n'.\ \|c\|_{t\ i}) \wedge (\forall\, n''{\geq}\ \langle c \leftarrow t\rangle_{n'}.\ n''{\leq}\langle c \rightarrow t\rangle_{n'} \longrightarrow eval\ c\ t\ t'\ n''\ \gamma)$
      $\wedge\ (\forall\, n''{\geq}\langle c \leftarrow t\rangle_n.\ n'' < \langle c \leftarrow t\rangle_{n'} \longrightarrow eval\ c\ t\ t'\ n''\ \gamma') \vee$
    $(\neg(\exists\, i{\geq}n'.\ \|c\|_{t\ i})) \wedge eval\ c\ t\ t'\ n'\ \gamma \wedge (\forall\, n''{\geq}\langle c \leftarrow t\rangle_n.\ n'' < n' \longrightarrow eval\ c\ t\ t'\ n''\ \gamma'))$
⟨*proof*⟩

lemma *untilEN*[*elim*]:
  fixes n::nat
    and n'::nat
    and t::$nat \Rightarrow cnf$
    and t'::$nat \Rightarrow 'cmp$
    and c::$'id$
  assumes $\nexists\, i.\ i{\geq}n \wedge \|c\|_{t\ i}$
    and $eval\ c\ t\ t'\ n\ (\gamma'\ \mathfrak{U}\ \gamma)$
  shows $\exists\, n'{\geq}n.\ eval\ c\ t\ t'\ n'\ \gamma \wedge$
    $(\forall\, n''{\geq}n.\ n'' < n' \longrightarrow eval\ c\ t\ t'\ n''\ \gamma')$
⟨*proof*⟩

2.5.6 Weak Until

definition *wuntil* :: $((nat \Rightarrow 'cmp) \Rightarrow nat \Rightarrow bool) \Rightarrow ((nat \Rightarrow 'cmp) \Rightarrow nat \Rightarrow bool)$
  $\Rightarrow ((nat \Rightarrow 'cmp) \Rightarrow nat \Rightarrow bool)$ (**infixl** $\mathfrak{W}$ *20*)
  where $\gamma'\ \mathfrak{W}\ \gamma \equiv \gamma'\ \mathfrak{U}\ \gamma \vee^b \Box(\gamma')$

end

end

References

[1] A. Lochbihler. Coinduction. *The Archive of Formal Proof s. http://afp.sourceforge.net/entries/Coinductive.shtml*, 2010.

[2] D. Marmsoler. On the semantics of temporal specifications of component-behavior for dynamic architectures. In *Eleventh International Symposium on Theoretical Aspects of Software Engineering*. Springer, 2017.

[3] D. Marmsoler. Towards a calculus for dynamic architectures. In *International Colloquium on Theoretical Aspects of Computing*. Springer, 2017.

[4] D. Marmsoler and M. Gleirscher. On activation, connection, and behavior in dynamic architectures. *Scientific Annals of Computer Science*, 26(2):187248, 2016.

[5] D. Marmsoler and M. Gleirscher. Specifying properties of dynamic architectures using configuration traces. In *International Colloquium on Theoretical Aspects of Computing*, pages 235–254. Springer, 2016.