A Formal Development of a Polychronous Polytimed Coordination Language

Hai Nguyen Van
hai.nguyenvan.phie@gmail.com

Frédéric Boulanger
frederic.boulanger@centralesupelec.fr

Burkhart Wolff
burkhart.wolff@lri.fr

July 31, 2019
Contents

1 A Gentle Introduction to TESL 5
  1.1 Context ................................................. 5
  1.2 The TESL Language ....................................... 6
    1.2.1 Instantaneous Causal Operators ....................... 7
    1.2.2 Temporal Operators .................................. 7
    1.2.3 Asynchronous Operators .............................. 7

2 Core TESL: Syntax and Basics 9
  2.1 Syntactic Representation ................................. 9
    2.1.1 Basic elements of a specification ..................... 9
    2.1.2 Operators for the TESL language ...................... 9
    2.1.3 Field Structure of the Metric Time Space ............. 10
  2.2 Defining Runs ........................................... 11

3 Denotational Semantics 13
  3.1 Denotational interpretation for atomic TESL formulae .......... 13
  3.2 Denotational interpretation for TESL formulae ................ 14
    3.2.1 Image interpretation lemma .......................... 14
    3.2.2 Expansion law ....................................... 14
  3.3 Equational laws for the denotation of TESL formulae ........... 14
  3.4 Decreasing interpretation of TESL formulae .................. 15
  3.5 Some special cases ...................................... 16

4 Symbolic Primitives for Building Runs 17
  4.0.1 Symbolic Primitives for Runs .......................... 17
  4.1 Semantics of Primitive Constraints ........................ 18
    4.1.1 Defining a method for witness construction ............ 19
  4.2 Rules and properties of consistence ........................ 19
  4.3 Major Theorems ......................................... 20
    4.3.1 Interpretation of a context .......................... 20
    4.3.2 Expansion law ....................................... 20
  4.4 Equations for the interpretation of symbolic primitives ........ 20
    4.4.1 General laws ........................................ 20
    4.4.2 Decreasing interpretation of symbolic primitives ........ 21

5 Operational Semantics 23
  5.1 Operational steps ...................................... 23
  5.2 Basic Lemmas ........................................... 25
## Contents

### 6 Semantics Equivalence

6.1 Stepwise denotational interpretation of TESL atoms .......................... 29  
6.2 Coinduction Unfolding Properties .................................................. 31  
6.3 Interpretation of configurations ....................................................... 33  

### 7 Main Theorems

7.1 Initial configuration ................................................................. 35  
7.2 Soundness .................................................................................... 35  
7.3 Completeness ............................................................................... 36  
7.4 Progress ...................................................................................... 36  
7.5 Local termination ......................................................................... 37  

### 8 Properties of TESL

8.1 Stuttering Invariance .................................................................... 39  
8.1.1 Definition of stuttering ............................................................. 39  
8.1.2 Alternate definitions for counting ticks ........................................ 41  
8.1.3 Stuttering Lemmas ................................................................. 41  
8.1.4 Lemmas used to prove the invariance by stuttering ..................... 42  
8.1.5 Main Theorems ......................................................................... 50
Chapter 1

A Gentle Introduction to TESL

1.1 Context

The design of complex systems involves different formalisms for modeling their different parts or aspects. The global model of a system may therefore consist of a coordination of concurrent sub-models that use different paradigms such as differential equations, state machines, synchronous data-flow networks, discrete event models and so on, as illustrated in Figure 1.1. This raises the interest in architectural composition languages that allow for “bolting the respective sub-models together”, along their various interfaces, and specifying the various ways of collaboration and coordination [2].

We are interested in languages that allow for specifying the timed coordination of subsystems by addressing the following conceptual issues:

- events may occur in different sub-systems at unrelated times, leading to polychronous systems, which do not necessarily have a common base clock,
- the behavior of the sub-systems is observed only at a series of discrete instants, and time coordination has to take this discretization into account,
- the instants at which a system is observed may be arbitrary and should not change its behavior (stuttering invariance),
- coordination between subsystems involves causality, so the occurrence of an event may enforce the occurrence of other events, possibly after a certain duration has elapsed or an event has occurred a given number of times,
- the domain of time (discrete, rational, continuous . . . ) may be different in the subsystems, leading to polytimed systems,
- the time frames of different sub-systems may be related (for instance, time in a GPS satellite and in a GPS receiver on Earth are related although they are not the same).

In order to tackle the heterogeneous nature of the subsystems, we abstract their behavior as clocks. Each clock models an event, i.e., something that can occur or not at a given time. This time is measured in a time frame associated with each clock, and the nature of time (integer, rational, real, or any type with a linear order) is specific to each clock. When the event associated
with a clock occurs, the clock ticks. In order to support any kind of behavior for the subsystems, we are only interested in specifying what we can observe at a series of discrete instants. There are two constraints on observations: a clock may tick only at an observation instant, and the time on any clock cannot decrease from an instant to the next one. However, it is always possible to add arbitrary observation instants, which allows for stuttering and modular composition of systems. As a consequence, the key concept of our setting is the notion of a clock-indexed Kripke model: \( \Sigma^\infty = N \rightarrow \mathcal{K} \rightarrow (\mathcal{B} \times \mathcal{T}) \), where \( \mathcal{K} \) is an enumerable set of clocks, \( \mathcal{B} \) is the set of booleans – used to indicate that a clock ticks at a given instant – and \( \mathcal{T} \) is a universal metric time space for which we only assume that it is large enough to contain all individual time spaces of clocks and that it is ordered by some linear ordering \( (\leq_T) \).

The elements of \( \Sigma^\infty \) are called runs. A specification language is a set of operators that constrains the set of possible monotonic runs. Specifications are composed by intersecting the denoted run sets of constraint operators. Consequently, such specification languages do not limit the number of clocks used to model a system (as long as it is finite) and it is always possible to add clocks to a specification. Moreover, they are compositional by construction since the composition of specifications consists of the conjunction of their constraints.

This work provides the following contributions:

- defining the non-trivial language TESL\(^*\) in terms of clock-indexed Kripke models,
- proving that this denotational semantics is stuttering invariant,
- defining an adapted form of symbolic primitives and presenting the set of operational semantic rules,
- presenting formal proofs for soundness, completeness, and progress of the latter.

### 1.2 The TESL Language

The TESL language [1] was initially designed to coordinate the execution of heterogeneous components during the simulation of a system. We define here a minimal kernel of operators that
1.2. THE TESL LANGUAGE

will form the basis of a family of specification languages, including the original TESL language, which is described at http://wdi.supelec.fr/software/TESL/.

1.2.1 Instantaneous Causal Operators

TESL has operators to deal with instantaneous causality, i.e., to react to an event occurrence in the very same observation instant.

- **c1 implies c2** means that at any instant where c1 ticks, c2 has to tick too.
- **c1 implies not c2** means that at any instant where c1 ticks, c2 cannot tick.
- **c1 kills c2** means that at any instant where c1 ticks, and at any future instant, c2 cannot tick.

1.2.2 Temporal Operators

TESL also has chronometric temporal operators that deal with dates and chronometric delays.

- **c sporadic t** means that clock c must have a tick at time t on its own time scale.
- **c1 sporadic t on c2** means that clock c1 must have a tick at an instant where the time on c2 is t.
- **c1 time delayed by d on m implies c2** means that every time clock c1 ticks, c2 must have a tick at the first instant where the time on m is d later than it was when c1 had ticked. This means that every tick on c1 is followed by a tick on c2 after a delay d measured on the time scale of clock m.
- **time relation (c1, c2) in R** means that at every instant, the current time on clocks c1 and c2 must be in relation R. By default, the time lines of different clocks are independent. This operator allows us to link two time lines, for instance to model the fact that time in a GPS satellite and time in a GPS receiver on Earth are not the same but are related. Time being polymorphic in TESL, this can also be used to model the fact that the angular position on the camshaft of an engine moves twice as fast as the angular position on the crankshaft. We may consider only linear arithmetic relations to restrict the problem to a domain where the resolution is decidable.

1.2.3 Asynchronous Operators

The last category of TESL operators allows the specification of asynchronous relations between event occurrences. They do not specify the precise instants at which ticks have to occur, they only put bounds on the set of instants at which they should occur.

- **c1 weakly precedes c2** means that for each tick on c2, there must be at least one tick on c1 at a previous or at the same instant. This can also be expressed by stating that at each instant, the number of ticks since the beginning of the run must be lower or equal on c2 than on c1.

\[1\] See http://wdi.supelec.fr/software/TESL/GalleryEngine for more details
• c₁ strictly precedes c₂ means that for each tick on c₂, there must be at least one tick on c₁ at a previous instant. This can also be expressed by saying that at each instant, the number of ticks on c₂ from the beginning of the run to this instant, must be lower or equal to the number of ticks on c₁ from the beginning of the run to the previous instant.
Chapter 2

The Core of the TESL Language: Syntax and Basics

theory TESL
imports Main
begin

2.1 Syntactic Representation

We define here the syntax of TESL specifications.

2.1.1 Basic elements of a specification

The following items appear in specifications:

- Clocks, which are identified by a name.
- Tag constants are just constants of a type which denotes the metric time space.

datatype clock = Clk (string)
type synonym instant_index = (nat)
datatype 'τ tag_const = TConst (the_tag_const : 'τ) (⟨τ_cst⟩)

2.1.2 Operators for the TESL language

The type of atomic TESL constraints, which can be combined to form specifications.

datatype 'τ TESL_atomic =
| SporadicOn (clock) (τ tag_const) (clock) (⟨_ sporadic on _⟩ 55)
| TagRelation (clock) (clock) (⟨τ tag_const × τ tag_const⟩ ⇒ bool)
| (time-relation [_, _] ∈ _) 55)
| Implies (clock) (clock) (infixr (implies) 55)
| ImpliesNot (clock) (clock) (infixr (implies not) 55)
| TimeDelayedBy (clock) (τ tag_const) (clock) (clock)
| (⟨_ time-delayed by _ on _ implies _⟩ 55)
A TESL formula is just a list of atomic constraints, with implicit conjunction for the semantics.

type synonym 'τ TESL_formula = ('τ TESL_atomic list)

We call *positive atoms* the atomic constraints that create ticks from nothing. Only sporadic constraints are positive in the current version of TESL.

fun positive_atom :: ('τ TESL_atomic ⇒ bool) where
(positive_atom (_ sporadic _ on _) = True)
| (positive_atom _ _ _ ) = False)

The NoSporadic function removes sporadic constraints from a TESL formula.

abbreviation NoSporadic :: ('τ TESL_formula ⇒ 'τ TESL_formula)
where
NoSporadic f ≡ (List.filter (λf_atom. case f_atom of
_ sporadic _ on _ ⇒ False
| _ ⇒ True) f))

2.1.3 Field Structure of the Metric Time Space

In order to handle tag relations and delays, tags must belong to a field. We show here that this is the case when the type parameter of 'τ tag_const is itself a field.

instance tag_const :: (field)field
begin
  fun inverse_tag_const
  where (inverse (τ_cst t) = τ_cst (inverse t))

  fun divide_tag_const
  where (divide (τ_cst t1) (τ_cst t2) = τ_cst (divide t1 t2))

  fun uminus_tag_const
  where (uminus (τ_cst t) = τ_cst (uminus t))

  fun minus_tag_const
  where (minus (τ_cst t1) (τ_cst t2) = τ_cst (minus t1 t2))

  definition (one_tag_const ≡ τ_cst 1)

  fun times_tag_const
  where (times (τ_cst t1) (τ_cst t2) = τ_cst (times t1 t2))

  definition (zero_tag_const ≡ τ_cst 0)

  fun plus_tag_const
  where (plus (τ_cst t1) (τ_cst t2) = τ_cst (plus t1 t2))

instance (proof)
end

For comparing dates (which are represented by tags) on clocks, we need an order on tags.

instanceation tag_const :: (order)order
begin
2.2. DEFINING RUNS

For ensuring that time does never flow backwards, we need a total order on tags.

```isar
instantiation tag_const :: (linorder)linorder
begin
instance ⟨proof⟩
end
end
```

2.2 Defining Runs

theory Run
imports TESL
begin

Runs are sequences of instants, and each instant maps a clock to a pair \((h, t)\) where \(h\) indicates whether the clock ticks or not, and \(t\) is the current time on this clock. The first element of the pair is called the \textit{hamlet} of the clock (to tick or not to tick), the second element is called the \textit{time}.

abbreviation hamlet where \(\langle \text{hamlet} \equiv \text{fst} \rangle\)
abbreviation time where \(\langle \text{time} \equiv \text{snd} \rangle\)

type synonym \('\tau\ instanta = ('\tau \Rightarrow (\text{bool} \times '\tau \tag_const))\)

Runs have the additional constraint that time cannot go backwards on any clock in the sequence of instants. Therefore, for any clock, the time projection of a run is monotonous.

```isar
typedef (overloaded) '\tau::linordered_field run = 
\{ \(\varrho::\text{nat} \Rightarrow '\tau\ instanta. \forall c. \text{mono} (\lambda n. \text{time} (\varrho n c)) \} \langle proof⟩
lemma Abs_run_inverse_rewrite:
\(\forall c. \text{mono} (\lambda n. \text{time} (\varrho n c)) \implies \text{Rep_run} (\text{Abs_run} \varrho) = \varrho\) ⟨proof⟩
```

A \textit{dense} run is a run in which something happens (at least one clock ticks) at every instant.

```isar
definition dense_run \varrho \equiv (\forall n. \exists c. \text{hamlet} ((\text{Rep_run} \varrho) n c))
run_tick_count \varrho K n counts the number of ticks on clock \(K\) in the interval \([0, n]\) of run \(\varrho\).
```

```isar
fun run_tick_count :: ('\tau::linordered_field) run \Rightarrow clock \Rightarrow nat \Rightarrow nat
\langle (#\leq - - _)\rangle
where
\langle (#\leq \varrho K 0) \rangle \equiv (\text{if hamlet} ((\text{Rep_run} \varrho) 0 K)
then 1
```

run_tick_count_strictly ϱ K n counts the number of ticks on clock K in the interval \([0, n[\) of run ϱ.

fun run_tick_count_strictly :: (\('\tau::linordered_field\) run ⇒ clock ⇒ nat ⇒ nat) where
\[(\#< ϱ K 0) = 0\]
\[\text{and} \quad ((\#< ϱ K \text{Suc } n) = \#≤ ϱ K n)\]

first_time ϱ K n τ tells whether instant n in run ϱ is the first one where the time on clock K reaches τ.

definition first_time :: (\('a::linordered_field\) run ⇒ clock ⇒ nat ⇒ 'a tag_const ⇒ bool) where
\[(\text{first_time } ϱ K n τ \equiv \text{time } ((\text{Rep_run } ϱ n K) = τ) \land \n' < n \land \text{time } ((\text{Rep_run } ϱ n' K) = τ)\]

The time on a clock is necessarily less than τ before the first instant at which it reaches τ.

lemma before_first_time:
\(\text{assumes } \text{(first_time } ϱ K n τ) \land \text{m < n}\)
\(\text{shows } \text{time } ((\text{Rep_run } ϱ m K) < τ)\)

(proof)

This leads to an alternate definition of first_time:

lemma alt_first_time_def:
\(\text{assumes } \forall n. \text{time } ((\text{Rep_run } ϱ n K) < τ) \land \text{time } ((\text{Rep_run } ϱ n K) = τ) \land \text{time } ((\text{Rep_run } ϱ n K) = τ)
\(\text{shows } \text{(first_time } ϱ K n τ)\)

(proof)
Chapter 3
Denotational Semantics

theory Denotational
imports
  TESL
  Run
begin

The denotational semantics maps TESL formulae to sets of satisfying runs. Firstly, we define the semantics of atomic formulae (basic constructs of the TESL language), then we define the semantics of compound formulae as the intersection of the semantics of their components: a run must satisfy all the individual formulae of a compound formula.

3.1 Denotational interpretation for atomic TESL formulae

fun TESL_interpretation_atomic :: "('tau::linordered_field) TESL_atomic => 'tau run set" ("_esl")
where
— K1 sporadic tau on K2 means that K1 should tick at an instant where the time on K2 is tau.
  \{[ K1 sporadic tau on K2 ]_tesl =
  (\rho. \exists n::nat. hamlet ((Rep_run \rho) n K1) \land time ((Rep_run \rho) n K2) = tau)\}
— time-relation \{K1, K2\} \in R means that at each instant, the time on K1 and the time on K2 are in relation R.
  \{[ time-relation \{K1, K2\} \in R ]_tesl =
  (\rho. \forall n::nat. R (time ((Rep_run \rho) n K1), time ((Rep_run \rho) n K2)))\}
— master implies slave means that at each instant at which master ticks, slave also ticks.
  \{[ master implies slave ]_tesl =
  (\rho. \forall n::nat. hamlet ((Rep_run \rho) n master) \rightarrow hamlet ((Rep_run \rho) n slave))\}
— master implies not slave means that at each instant at which master ticks, slave does not tick.
  \{[ master implies not slave ]_tesl =
  (\rho. \forall n::nat. hamlet ((Rep_run \rho) n master) \rightarrow \neg hamlet ((Rep_run \rho) n slave))\}
— master time-delayed by delta tau on measuring implies slave means that at each instant at which master ticks,
  slave will tick after a delay delta tau measured on the time scale of measuring.
  \{[ master time-delayed by delta tau on measuring implies slave ]_tesl =
  (\rho. \forall n. hamlet ((Rep_run \rho) n master) \rightarrow
  (let measured_time = time ((Rep_run \rho) n measuring) in
   \forall m \geq n. first_time measuring m (measured_time + delta tau))\}

13
CHAPTER 3. DENOTATIONAL SEMANTICS

\[ \rightarrow \text{hamlet } ((\text{Rep\_run } \varrho) \text{ m slave}) \]

— \(K_1\) weakly precedes \(K_2\) means that each tick on \(K_2\) must be preceded by or coincide with at least one tick on \(K_1\). Therefore, at each instant \(n\), the number of ticks on \(K_2\) must be less or equal to the number of ticks on \(K_1\).

\[ \{ (\varrho, \forall n::\text{nat}. (\text{run\_tick\_count } \varrho K_2 n) \leq (\text{run\_tick\_count } \varrho K_1 n)) \} \]

— \(K_1\) strictly precedes \(K_2\) means that each tick on \(K_2\) must be preceded by at least one tick on \(K_1\) at a previous instant. Therefore, at each instant \(n\), the number of ticks on \(K_2\) must be less or equal to the number of ticks on \(K_1\) at instant \(n - 1\).

\[ \{ (\varrho, \forall n::\text{nat}. (\text{run\_tick\_count } \varrho K_2 n) \leq (\text{run\_tick\_count\_strictly } \varrho K_1 n)) \} \]

— \(K_1\) kills \(K_2\) means that when \(K_1\) ticks, \(K_2\) cannot tick and is not allowed to tick at any further instant.

\[ \{ (\varrho, \forall n::\text{nat}. \text{hamlet } ((\text{Rep\_run } \varrho) n K_1) \rightarrow (\forall m \geq n. \sim \text{hamlet } ((\text{Rep\_run } \varrho) m K_2))) \} \]

3.2 Denotational interpretation for TESL formulae

To satisfy a formula, a run has to satisfy the conjunction of its atomic formulae. Therefore, the interpretation of a formula is the intersection of the interpretations of its components.

\[
\text{run } \text{TESL\_interpretation} :: \ (('\tau::\text{linordered\_field}) \ \text{TESL\_formula} \Rightarrow '\tau \ \text{run set})
\]

\[
\text{where}
\]

\[ \{ [[ [] ]]_{\text{TESL}} = \{ . \text{True} \} \}
\]

\[ \{ [[ \varphi \# \Phi ]]_{\text{TESL}} = [[ \varphi ]]_{\text{TESL}} \cap [[ \Phi ]]_{\text{TESL}} \}
\]

lemma TESL\_interpretation\_homo:

\[ [[ \varphi ]]_{\text{TESL}} \cap [[ \Phi ]]_{\text{TESL}} = [ [ \varphi \# \Phi ]]_{\text{TESL}} \]

(proof)

3.2.1 Image interpretation lemma

theorem TESL\_interpretation\_image:

\[ [[ \Phi ]]_{\text{TESL}} = \bigcap (\lambda \varphi. [ [ \varphi ]]_{\text{TESL}} \ ' \text{set } \Phi) \]

(proof)

3.2.2 Expansion law

Similar to the expansion laws of lattices.

theorem TESL\_interp\_homo\_append:

\[ [[ \Phi_1 \circ \Phi_2 ]]_{\text{TESL}} = [[ \Phi_1 ]]_{\text{TESL}} \cap [[ \Phi_2 ]]_{\text{TESL}} \]

(proof)

3.3 Equational laws for the denotation of TESL formulae

lemma TESL\_interp\_assoc:

\[ [ [ (\Phi_1 \circ \Phi_2) \circ \Phi_3 ]]_{\text{TESL}} = [[ \Phi_1 \circ (\Phi_2 \circ \Phi_3) ]]_{\text{TESL}} \]

(proof)

lemma TESL\_interp\_commute:

\[ [ [ \Phi_1 \circ \Phi_2 ]]_{\text{TESL}} = [ [ \Phi_2 \circ \Phi_1 ]]_{\text{TESL}} \]

(proof)
3.4. DECREASING INTERPRETATION OF TESL FORMULAE

lemma TESL_interp_left_commute:
\[
[[ \Phi_1 \circ (\Phi_2 \circ \Phi_3)]]_{TESL} = [[ \Phi_2 \circ (\Phi_1 \circ \Phi_3)]]_{TESL}
\]
(proof)

lemma TESL_interp_idem:
\[
[[ \Phi \circ \Phi]]_{TESL} = [[ \Phi]]_{TESL}
\]
(proof)

lemma TESL_interp_left_idem:
\[
[[ (\Phi_1 \circ \Phi_2) \circ \Phi_2]]_{TESL} = [[ \Phi_1 \circ \Phi_2]]_{TESL}
\]
(proof)

lemma TESL_interp_right_idem:
\[
[[ (\Phi_1 \circ \Phi_2) \circ \Phi_2]]_{TESL} = [[ \Phi_1 \circ \Phi_2]]_{TESL}
\]
(proof)

lemmas TESL_interp_aci = TESL_interp_commute
TESL_interp_assoc
TESL_interp_left_commute
TESL_interp_left_idem

The empty formula is the identity element.

lemma TESL_interp_neutral1:
\[
[[ \[] \circ \Phi]]_{TESL} = [[ \Phi]]_{TESL}
\]
(proof)

lemma TESL_interp_neutral2:
\[
[[ \Phi \circ \[]]]_{TESL} = [[ \Phi]]_{TESL}
\]
(proof)

3.4 Decreasing interpretation of TESL formulae

Adding constraints to a TESL formula reduces the number of satisfying runs.

lemma TESL_sem_decreases_head:
\[
[[ \Phi]]_{TESL} \supseteq [[ \varphi \# \Phi]]_{TESL}
\]
(proof)

lemma TESL_sem_decreases_tail:
\[
[[ \Phi]]_{TESL} \supseteq [[ \Phi \circ [\varphi]]]_{TESL}
\]
(proof)

Repeating a formula in a specification does not change the specification.

lemma TESL_interp_formula_stuttering:
assumes \( \varphi \in \text{set } \Phi \)
shows \( [[ \varphi \# \Phi]]_{TESL} = [[ \Phi]]_{TESL} \)
(proof)

Removing duplicate formulae in a specification does not change the specification.

lemma TESL_interp_remdups_absorb:
\( [[ \Phi]]_{TESL} = [[ \text{remdups } \Phi]]_{TESL} \)
(proof)

Specifications that contain the same formulae have the same semantics.

lemma TESL_interp_set_lifting:
assumes \( \text{set } \Phi = \text{set } \Phi' \)
The semantics of specifications is contravariant with respect to their inclusion.

**Theorem TESL_interp_decreases_setinc:**

assumes \( \text{set } \Phi \subseteq \text{set } \Phi' \)

shows \( \langle \[ \[ \Phi \] \] \rangle_{TESL} \supseteq \langle \[ \[ \Phi' \] \] \rangle_{TESL} \)

(proof)

**Lemma TESL_interp_decreases_add_head:**

assumes \( \text{set } \Phi \subseteq \text{set } \Phi' \)

shows \( \langle \[ \varphi \# \Phi \] \rangle_{TESL} \supseteq \langle \[ \varphi \# \Phi' \] \rangle_{TESL} \)

(proof)

**Lemma TESL_interp_decreases_add_tail:**

assumes \( \text{set } \Phi \subseteq \text{set } \Phi' \)

shows \( \langle \[ \Phi \@ \varphi \] \rangle_{TESL} \supseteq \langle \[ \Phi' \@ \varphi \] \rangle_{TESL} \)

(proof)

**Lemma TESL_interp_absorb1:**

assumes \( \text{set } \Phi_1 \subseteq \text{set } \Phi_2 \)

shows \( \langle \[ \Phi_1 \@ \Phi_2 \] \rangle_{TESL} = \langle \[ \Phi_2 \] \rangle_{TESL} \)

(proof)

**Lemma TESL_interp_absorb2:**

assumes \( \text{set } \Phi_2 \subseteq \text{set } \Phi_1 \)

shows \( \langle \[ \Phi_1 \@ \Phi_2 \] \rangle_{TESL} = \langle \[ \Phi_1 \] \rangle_{TESL} \)

(proof)

### 3.5 Some special cases

**Lemma NoSporadic_stable [simp]:**

\( \langle \[ \Phi \] \rangle_{TESL} \subseteq \langle \[ \text{NoSporadic } \Phi \] \rangle_{TESL} \)

(proof)

**Lemma NoSporadic_idem [simp]:**

\( \langle \[ \Phi \] \rangle_{TESL} \cap \langle \[ \text{NoSporadic } \Phi \] \rangle_{TESL} = \langle \[ \Phi \] \rangle_{TESL} \)

(proof)

**Lemma NoSporadic_setinc:**

\( \text{set } (\text{NoSporadic } \Phi) \subseteq \text{set } \Phi \)

(proof)

end
Chapter 4

Symbolic Primitives for Building Runs

theory SymbolicPrimitive
  imports Run
begin

We define here the primitive constraints on runs, towards which we translate TESL specifications in the operational semantics. These constraints refer to a specific symbolic run and can therefore access properties of the run at particular instants (for instance, the fact that a clock ticks at instant \( n \) of the run, or the time on a given clock at that instant).

In the previous chapters, we had no reference to particular instants of a run because the TESL language should be invariant by stuttering in order to allow the composition of specifications: adding an instant where no clock ticks to a run that satisfies a formula should yield another run that satisfies the same formula. However, when constructing runs that satisfy a formula, we need to be able to refer to the time or hamlet of a clock at a given instant.

Counter expressions are used to get the number of ticks of a clock up to (strictly or not) a given instant index.

datatype cnt_expr =
  TickCountLess \( \langle \text{clock} \rangle \langle \text{instant\_index} \rangle \langle \#< \rangle \)
| TickCountLeq \( \langle \text{clock} \rangle \langle \text{instant\_index} \rangle \langle \#\leq \rangle \)

4.0.1 Symbolic Primitives for Runs

Tag values are used to refer to the time on a clock at a given instant index.

datatype tag_val =
  TSchematic \( \langle \text{clock} \bullet \text{instant\_index} \rangle \langle \text{\( \tau \)\_var} \rangle \)

datatype \( \text{\'r} \) constr =
  — \( \text{c} \downarrow \text{n} \oplus \text{\( \tau \)\_constr} \) constrains clock \( \text{c} \) to have time \( \text{\( \tau \)\_constr} \) at instant \( \text{n} \) of the run.
  — \( \text{Timestamp} \ (\langle \text{clock} \rangle \langle \text{instant\_index} \rangle \text{\( \text{\'r} \)\_tag\_const} \rangle \langle \_ \rangle \rangle \)
  — \( \text{n} \oplus \text{\( \delta t \)} \Rightarrow \text{\( \text{\( \tau \)\_tag\_const} \) const} \) constrains clock \( \text{\( \tau \)\_tag\_const} \) to tick at the first instant at which the time on \( \text{n} \) has increased by \( \delta t \) from the value it had at instant \( \text{n} \) of the run.
  — \( \text{TimeDelay} \ (\langle \text{clock} \rangle \langle \text{instant\_index} \rangle \text{\( \text{\'r} \)\_tag\_const} \rangle \langle \text{clock} \rangle \rangle \)
  — \( \text{c} \uparrow \text{n} \) constrains clock \( \text{c} \) to tick at instant \( \text{n} \) of the run.
The abstract machine has configurations composed of:

- the past \( \Gamma \), which captures choices that have already been made as a list of symbolic primitive constraints on the run;
- the current index \( n \), which is the index of the present instant;
- the present \( \Psi \), which captures the formulae that must be satisfied in the current instant;
- the future \( \Phi \), which captures the constraints on the future of the run.

**4.1 Semantics of Primitive Constraints**

The semantics of the primitive constraints is defined in a way similar to the semantics of TESL formulae.

```haskell
fun counter_expr_eval :: (\('\tau\cdot\text{linordered_field}\) \Rightarrow \text{cnt_expr} \Rightarrow \text{nat})
  (\(\langle \_, \_ \rangle_{\text{cntexpr}}\))
where
  \(\langle g \vdash \#< \text{clk indx} \rangle_{\text{cntexpr}} = \text{run_tick_count_strictly_g_clk_indx} \)

fun symbolic_run_interpretation_primitive :: (\('\tau\cdot\text{linordered_field}\) \Rightarrow \text{const} \Rightarrow \text{'\tau run set}) (\(\langle \_, \_ \rangle_{\text{prim}}\))
where
  \(\langle K \uparrow n \rangle_{\text{prim}} = (g \cdot \text{hamlet} ((\text{Rep_run} \ g) \ n \ K))\)
  \(\langle K \oslash n_0 \odot \delta \Rightarrow K' \rangle_{\text{prim}} = \)
    \( (g \cdot \forall n \geq n_0. \text{first_time} \ g \ n \ (\text{time} ((\text{Rep_run} \ g) \ n_0 \ K) + \delta)) \)
    \(\rightarrow \text{hamlet} ((\text{Rep_run} \ g) \ n \ K'))\)
  \(\langle K \neg \neg < n \rangle_{\text{prim}} = (g \cdot \neg \text{hamlet} ((\text{Rep_run} \ g) \ n \ K))\)
  \(\langle K \neg \neg \neg \geq n \rangle_{\text{prim}} = \)
    \( (g \cdot \forall i \geq n. \neg \text{hamlet} ((\text{Rep_run} \ g) \ i \ K))\)
  \(\langle K \uparrow n \odot \tau \rangle_{\text{prim}} = (g \cdot \text{time} ((\text{Rep_run} \ g) \ n \ K) = \tau)\)
  \(\langle \tau_{\text{var}}(K_1, n_1), \tau_{\text{var}}(K_2, n_2) \rangle \in \text{R} \rangle_{\text{prim}} = \)
    \( \{ g \cdot \text{R} (\text{time} ((\text{Rep_run} \ g) \ n_1 K_1), \text{time} ((\text{Rep_run} \ g) \ n_2 K_2)) \} \)
```
4.2. Rules and Properties of Consistence

The composition of primitive constraints is their conjunction, and we get the set of satisfying runs by intersection.

fun symbolic_run_interpretation :: \((\tau::\text{linordered_field}) \text{ constr list} \Rightarrow (\tau::\text{linordered_field}) \text{ run set}\)
where
\(\langle [\emptyset] \text{ prim} = \{ \rho. \text{ True} \} \rangle\)

lemma symbolic_run_interp_cons_morph:
\(\langle [\emptyset] \text{ prim} = \{ \rho. \text{ True} \} \rangle\)
(proof)
definition consistent_context :: \((\tau::\text{linordered_field}) \text{ constr list} \Rightarrow \text{bool}\)
where
\(\langle \text{consistent_context} \Gamma \equiv (\langle [\emptyset] \text{ prim} = \{ \} \rangle) \rangle\)

4.1.1 Defining a method for witness construction

In order to build a run, we can start from an initial run in which no clock ticks and the time is always 0 on any clock.

abbreviation initial_run :: \((\tau::\text{linordered_field}) \text{ run}) \langle \emptyset \rangle where
\(\langle \emptyset \equiv \text{Abs_run} ((\lambda n. (\text{False}, \text{nat} \Rightarrow \text{clock} \Rightarrow (\text{bool} \times \tau \text{ tag_const})))\rangle)

To help avoiding that time flows backward, setting the time on a clock at a given instant sets it for the future instants too.

fun time_update :: \(\text{nat} \Rightarrow \text{clock} \Rightarrow (\tau::\text{linordered_field}) \text{ tag_const} \Rightarrow (\text{nat} \Rightarrow \tau \text{ instant}) \Rightarrow (\text{nat} \Rightarrow \tau \text{ instant})\)
where
\(\langle \text{time_update} n K \rho \tau = (\lambda n' K'. \text{if } K = K' \land n \leq n' \text{ then } (\text{hamlet} (\rho n K), \tau) \text{ else } \rho n' K') \rangle\)

4.2 Rules and properties of consistence

lemma context_consistency_preservation1:
\(\langle \text{consistent_context} \ ((\gamma::(\tau::\text{linordered_field}) \text{ constr})@\Gamma) \Rightarrow \text{consistent_context} \Gamma \rangle\)
(proof)
inductive context_independency :: \((\tau::\text{linordered_field}) \text{ constr list} \Rightarrow \tau \text{ constr list} \Rightarrow \text{bool}) \langle |\_\_ |\_\_ \rangle\)
where
\(\langle \text{NotTicks_independency} \rangle:
\(\langle \langle K \uparrow n \rangle \notin \text{set} \Gamma \Rightarrow (K \uparrow n) \bowtie \Gamma \rangle\)
\(\langle \text{Ticks_independency} \rangle:
\(\langle K \uparrow n \notin \text{set} \Gamma \Rightarrow (K \uparrow n) \bowtie \Gamma \rangle\)
\(\langle \text{Timestamp_independency} \rangle:
\(\langle (\uparrow \tau'. \tau' = \tau \land (K \downarrow n @ \tau') \in \text{set} \Gamma) \Rightarrow (K \downarrow n @ \tau) \bowtie \Gamma \rangle\)
CHAPTER 4. SYMBOLIC PRIMITIVES FOR BUILDING RUNS

4.3 Major Theorems

4.3.1 Interpretation of a context

The interpretation of a context is the intersection of the interpretation of its components.

\[ \bigcap \left( \lambda \gamma. \left[ \left[ \gamma \right] \right]_{\text{prim}} \right) \cdot \text{set} \Gamma = \left[ \left[ \Gamma \right] \right]_{\text{prim}} \]

4.3.2 Expansion law

Similar to the expansion laws of lattices

\[ \left[ \left[ \left[ \Gamma_1 \oplus \Gamma_2 \right] \right] \right]_{\text{prim}} = \left[ \left[ \Gamma_1 \right] \right]_{\text{prim}} \cap \left[ \left[ \Gamma_2 \right] \right]_{\text{prim}} \]

4.4 Equations for the interpretation of symbolic primitives

4.4.1 General laws

\[ \text{lemma} \; \text{symrun_interp_assoc}: \]
\[ \left[ \left[ \left( \Gamma_1 \oplus \Gamma_2 \right) \oplus \Gamma_3 \right] \right]_{\text{prim}} = \left[ \left[ \Gamma_1 \oplus \left( \Gamma_2 \oplus \Gamma_3 \right) \right] \right]_{\text{prim}} \]

\[ \text{lemma} \; \text{symrun_interp_commute}: \]
\[ \left[ \left[ \Gamma_1 \oplus \Gamma_2 \right] \right]_{\text{prim}} = \left[ \left[ \Gamma_2 \oplus \Gamma_1 \right] \right]_{\text{prim}} \]

\[ \text{lemma} \; \text{symrun_interp_left_commute}: \]
\[ \left[ \left[ \Gamma_1 \oplus \left( \Gamma_2 \oplus \Gamma_3 \right) \right] \right]_{\text{prim}} = \left[ \left[ \Gamma_2 \oplus \left( \Gamma_1 \oplus \Gamma_3 \right) \right] \right]_{\text{prim}} \]

\[ \text{lemma} \; \text{symrun_interp_idem}: \]
\[ \left[ \left[ \Gamma \oplus \left[ \Gamma \right] \right] \right]_{\text{prim}} = \left[ \left[ \Gamma \right] \right]_{\text{prim}} \]

\[ \text{lemma} \; \text{symrun_interp_left_idem}: \]
\[ \left[ \left[ \Gamma \oplus \left( \Gamma_1 \oplus \Gamma_2 \right) \right] \right]_{\text{prim}} = \left[ \left[ \Gamma \oplus \Gamma_2 \right] \right]_{\text{prim}} \]

\[ \text{lemma} \; \text{symrun_interp_right_idem}: \]
\[ \left[ \left[ \left( \Gamma_1 \oplus \Gamma_2 \right) \oplus \Gamma_2 \right] \right]_{\text{prim}} = \left[ \left[ \Gamma_1 \oplus \Gamma_2 \right] \right]_{\text{prim}} \]

\[ \text{lemmas} \; \text{symrun_interp_aci} = \text{symrun_interp_commute} \]
\[ \text{symrun_interp_assoc} \]
\[ \text{symrun_interp_left_commute} \]
\[ \text{symrun_interp_left_idem} \]

— Identity element

\[ \text{lemma} \; \text{symrun_interp_neutral1}: \]
\[ \left[ \left[ \left[ \left[ \left[ \Gamma \right] \right] \right] \right] \right]_{\text{prim}} = \left[ \left[ \Gamma \right] \right]_{\text{prim}} \]

\[ \text{lemma} \; \text{symrun_interp_neutral2}: \]
\[ \left[ \left[ \left[ \left[ \left[ \Gamma \right] \right] \right] \right] \right]_{\text{prim}} = \left[ \left[ \Gamma \right] \right]_{\text{prim}} \]
4.4. EQUATIONS FOR THE INTERPRETATION OF SYMBOLIC PRIMITIVES

4.4.2 Decreasing interpretation of symbolic primitives

Adding constraints to a context reduces the number of satisfying runs.

lemma TESL_sem_decreases_head:
\[ \langle [\{ \Gamma \} \rangle_{prim} \supseteq \langle [\{ \gamma \# \Gamma \} \rangle_{prim} \rangle 
\]

(\text{proof})

lemma TESL_sem_decreases_tail:
\[ \langle [\{ \Gamma \} \rangle_{prim} \supseteq \langle [\{ \Gamma \# \{ \gamma \} \} \rangle_{prim} \rangle 
\]

(\text{proof})

Adding a constraint that is already in the context does not change the interpretation of the context.

lemma symrun_interp_formula_stuttering:
\[ \text{assumes } (\gamma \in \text{set } \Gamma) \]
\[ \text{shows } \langle [\{ \gamma \# \Gamma \} \rangle_{prim} = \langle [\{ \Gamma \} \rangle_{prim} \rangle 
\]

(\text{proof})

Removing duplicate constraints from a context does not change the interpretation of the context.

lemma symrun_interp_remdups_absorb:
\[ \langle [\{ \Gamma \} \rangle_{prim} = \langle [\{ \text{remdups } \Gamma \} \rangle_{prim} \rangle 
\]

(\text{proof})

Two identical sets of constraints have the same interpretation, the order in the context does not matter.

lemma symrun_interp_set_lifting:
\[ \text{assumes } (\text{set } \Gamma_1 = \text{set } \Gamma_2) \]
\[ \text{shows } \langle [\{ \Gamma_1 \} \rangle_{prim} = \langle [\{ \Gamma_2 \} \rangle_{prim} \rangle 
\]

(\text{proof})

The interpretation of contexts is contravariant with regard to set inclusion.

theorem symrun_interp_decreases_setinc:
\[ \text{assumes } (\text{set } \Gamma \subseteq \text{set } \Gamma') \]
\[ \text{shows } \langle [\{ \Gamma \} \rangle_{prim} \supseteq \langle [\{ \Gamma' \} \rangle_{prim} \rangle 
\]

(\text{proof})

lemma symrun_interp_decreases_add_head:
\[ \text{assumes } (\text{set } \Gamma \subseteq \text{set } \Gamma') \]
\[ \text{shows } \langle [\{ \gamma \# \Gamma \} \rangle_{prim} \supseteq \langle [\{ \gamma \# \Gamma' \} \rangle_{prim} \rangle 
\]

(\text{proof})

lemma symrun_interp_decreases_add_tail:
\[ \text{assumes } (\text{set } \Gamma \subseteq \text{set } \Gamma') \]
\[ \text{shows } \langle [\{ \Gamma \# \{ \gamma \} \} \rangle_{prim} \supseteq \langle [\{ \Gamma' \# \{ \gamma \} \} \rangle_{prim} \rangle 
\]

(\text{proof})

lemma symrun_interp_absorb1:
\[ \text{assumes } (\text{set } \Gamma_1 \subseteq \text{set } \Gamma_2) \]
\[ \text{shows } \langle [\{ \Gamma_1 \# \Gamma_2 \} \rangle_{prim} = \langle [\{ \Gamma_2 \} \rangle_{prim} \rangle 
\]

(\text{proof})

lemma symrun_interp_absorb2:
\[ \text{assumes } (\text{set } \Gamma_2 \subseteq \text{set } \Gamma_1) \]
shows $[[ Γ_1 ∘ Γ_2 ]]_{\text{prim}} = [[ Γ_1 ]]_{\text{prim}}$

(proof)

end
Chapter 5
Operational Semantics

The operational semantics defines rules to build symbolic runs from a TESL specification (a set of TESL formulae). Symbolic runs are described using the symbolic primitives presented in the previous chapter. Therefore, the operational semantics compiles a set of constraints on runs, as defined by the denotational semantics, into a set of symbolic constraints on the instants of the runs. Concrete runs can then be obtained by solving the constraints at each instant.

5.1 Operational steps

We introduce a notation to describe configurations:

- $\Gamma$ is the context, the set of symbolic constraints on past instants of the run;
- $n$ is the index of the current instant, the present;
- $\Psi$ is the TESL formula that must be satisfied at the current instant (present);
- $\Phi$ is the TESL formula that must be satisfied for the following instants (the future).

abbreviation uncurry_conf
:: ('τ::linordered_field) system ⇒ instant_index ⇒ 'τ TESL_formula ⇒ 'τ TESL_formula
⇒ 'τ config) (Γ, n, ⊢, ⊢) 80

where
⟨Γ, n ⊢ Ψ ⊢ Φ ≡ (Γ, n, Ψ, Φ)⟩

The only introduction rule allows us to progress to the next instant when there are no more constraints to satisfy for the present instant.

inductive operational_semantics_intro
:: ('τ::linordered_field) config ⇒ 'τ config ⇒ bool) (Γ, n, ⊢, ⊢) 70

where
instant_i:
The elimination rules describe how TESL formulae for the present are transformed into constraints on the past and on the future.

**inductive operational_semanticsElim**

\[ (((\tau: \text{linordered_field}) \text{ config} \Rightarrow ^* \text{ config} \Rightarrow \text{ bool}) (\_ \hookrightarrow_e \_)) \]

where

- \text{sporadic_on_e1}:
  - A sporadic constraint can be ignored in the present and rejected into the future.
  \[ (\Gamma, n \vdash (K_1 \text{ sporadic } \tau \text{ on } K_2) \# \Psi) \Rightarrow \Phi) \]
  \[ \hookrightarrow_e (\Gamma, n \vdash \Psi \Rightarrow ((K_1 \text{ sporadic } \tau \text{ on } K_2) \# \Phi)) \]

- \text{sporadic_on_e2}:
  - It can also be handled in the present by making the clock tick and have the expected time. Once it has been handled, it is no longer a constraint to satisfy, so it disappears into the future.
  \[ (\Gamma, n \vdash (K_1 \text{ sporadic } \tau \text{ on } K_2) \# \Psi) \Rightarrow \Phi) \]
  \[ \hookrightarrow_e (((K_1 \uparrow n) \# (K_2 \downarrow n \bowtie \tau) \# \Gamma), n \vdash \Psi \Rightarrow \Phi) \]

- \text{tagrel_e}:
  - A relation between time scales has to be obeyed at every instant.
  \[ (\Gamma, n \vdash (\text{time-relation } [K_1, K_2] \in R) \# \Psi) \Rightarrow \Phi) \]
  \[ \hookrightarrow_e (((\tau_{\text{ear}}(K_1, n), \tau_{\text{ear}}(K_2, n)) \in R) \# \Gamma), n \vdash \Psi \Rightarrow ((\text{time-relation } [K_1, K_2] \in R) \# \Phi)) \]

- \text{implies_e1}:
  - An implication can be handled in the present by forbidding a tick of the master clock. The implication is copied back into the future because it holds for the whole run.
  \[ (\Gamma, n \vdash (K_1 \text{ implies } K_2) \# \Psi) \Rightarrow \Phi) \]
  \[ \hookrightarrow_e (((K_1 \not\Rightarrow n) \# \Gamma), n \vdash \Psi \Rightarrow ((K_1 \text{ implies } K_2) \# \Phi)) \]

- \text{implies_e2}:
  - It can also be handled in the present by making both the master and the slave clocks tick.
  \[ (\Gamma, n \vdash (K_1 \text{ implies } K_2) \# \Psi) \Rightarrow \Phi) \]
  \[ \hookrightarrow_e (((K_1 \uparrow n) \# (K_2 \downarrow n) \bowtie \Gamma), n \vdash \Psi \Rightarrow ((K_1 \text{ implies } K_2) \# \Phi)) \]

- \text{implies_not_e1}:
  - A negative implication can be handled in the present by forbidding a tick of the master clock. The implication is copied back into the future because it holds for the whole run.
  \[ (\Gamma, n \vdash (K_1 \text{ implies not } K_2) \# \Psi) \Rightarrow \Phi) \]
  \[ \hookrightarrow_e (((K_1 \not\Rightarrow n) \# \Gamma), n \vdash \Psi \Rightarrow ((K_1 \text{ implies not } K_2) \# \Phi)) \]

- \text{implies_not_e2}:
  - It can also be handled in the present by making the master clock ticks and forbidding a tick on the slave clock.
  \[ (\Gamma, n \vdash (K_1 \text{ implies not } K_2) \# \Psi) \Rightarrow \Phi) \]
  \[ \hookrightarrow_e (((K_1 \uparrow n) \# (K_2 \not\Rightarrow n) \bowtie \Gamma), n \vdash \Psi \Rightarrow ((K_1 \text{ implies not } K_2) \# \Phi)) \]

- \text{timedelayed_e1}:
  - A timed delayed implication can be handled by forbidding a tick on the master clock.
  \[ (\Gamma, n \vdash (K_1 \text{ time-delayed by } \delta \tau \text{ on } K_2 \text{ implies } K_3) \# \Psi) \Rightarrow \Phi) \]
  \[ \hookrightarrow_e (((K_1 \not\Rightarrow n) \# (K_2 \not\Rightarrow n \bowtie \delta \tau \Rightarrow K_3) \# \Gamma), n \vdash \Psi \Rightarrow ((K_1 \text{ time-delayed by } \delta \tau \text{ on } K_2 \text{ implies } K_3) \# \Phi)) \]

- \text{timedelayed_e2}:
  - It can also be handled by making the master clock tick and adding a constraint that makes the slave clock tick when the delay has elapsed on the measuring clock.
  \[ (\Gamma, n \vdash (K_1 \text{ time-delayed by } \delta \tau \text{ on } K_2 \text{ implies } K_3) \# \Psi) \Rightarrow \Phi) \]
  \[ \hookrightarrow_e (((K_1 \uparrow n) \# (K_2 \not\Rightarrow n \bowtie \delta \tau \Rightarrow K_3) \# \Gamma), n \vdash \Psi \Rightarrow ((K_1 \text{ time-delayed by } \delta \tau \text{ on } K_2 \text{ implies } K_3) \# \Phi)) \]

- \text{weakly_precedes_e}:
  - A weak precedence relation has to hold at every instant.
  \[ (\Gamma, n \vdash (K_1 \text{ weakly precedes } K_2) \# \Psi) \Rightarrow \Phi) \]
  \[ \hookrightarrow_e (((# K_2 n, K_1 n) \in \lambda(x,y). x \bowtie y) \# \Gamma), n \vdash \Psi \Rightarrow ((K_1 \text{ weakly precedes } K_2) \# \Phi)) \]

- \text{strictly_precedes_e}:
  - A strict precedence relation has to hold at every instant.
5.2. BASIC LEMMAS

\[ (\langle \Gamma, n \vdash ((K_1 \text{ strictly precedes } K_2) \# \Psi) \triangleright \Phi \rangle \] \[ \mapsto \langle \Gamma, n \vdash (K_1 \not\parallel n) \# \Gamma \rangle, n \vdash \Psi \triangleright ((K_1 \text{ kills } K_2) \# \Phi) \) \]

<table>
<thead>
<tr>
<th>kills_el:</th>
</tr>
</thead>
<tbody>
<tr>
<td>A kill can be handled by forbidding a tick of the triggering clock.</td>
</tr>
<tr>
<td>(\langle \Gamma, n \vdash ((K_1 \text{ kills } K_2) # \Psi) \triangleright \Phi \rangle ] [ \mapsto \langle \Gamma, n \vdash (K_1 \not\parallel n) # \Gamma \rangle, n \vdash \Psi \triangleright ((K_1 \text{ kills } K_2) # \Phi) )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>kills_e2:</th>
</tr>
</thead>
<tbody>
<tr>
<td>It can also be handled by making the triggering clock tick and by forbidding any further tick of the killed clock.</td>
</tr>
<tr>
<td>(\langle \Gamma, n \vdash ((K_1 \text{ kills } K_2) # \Psi) \triangleright \Phi \rangle ] [ \mapsto \langle \Gamma, n \vdash (K_1 \not\parallel n) # \Gamma \rangle, n \vdash \Psi \triangleright ((K_1 \text{ kills } K_2) # \Phi) )</td>
</tr>
</tbody>
</table>

A step of the operational semantics is either the application of the introduction rule or the application of an elimination rule.

\textbf{inductive operational semantics step}:

\[ :: (\langle \tau :: \text{linordered field} \rangle \text{ config} \Rightarrow \tau \text{ config} \Rightarrow \text{bool} \] \[ (\_ \leftrightarrow \_ \_ 70) \]

\textbf{where intro part:}

\[ \langle \Gamma_1, n_1 \vdash \Psi_1 \triangleright \Phi_1 \rangle \mapsto \langle \Gamma_2, n_2 \vdash \Psi_2 \triangleright \Phi_2 \rangle \]

\[ \rightarrow \langle \Gamma_1, n_1 \vdash \Psi_1 \triangleright \Phi_1 \rangle \rightarrow \langle \Gamma_2, n_2 \vdash \Psi_2 \triangleright \Phi_2 \rangle \]

\textbf{elims part:}

\[ \langle \Gamma_1, n_1 \vdash \Psi_1 \triangleright \Phi_1 \rangle \mapsto \langle \Gamma_2, n_2 \vdash \Psi_2 \triangleright \Phi_2 \rangle \]

\[ \rightarrow \langle \Gamma_1, n_1 \vdash \Psi_1 \triangleright \Phi_1 \rangle \rightarrow \langle \Gamma_2, n_2 \vdash \Psi_2 \triangleright \Phi_2 \rangle \]

We introduce notations for the reflexive transitive closure of the operational semantic step, its transitive closure and its reflexive closure.

\textbf{abbreviation operational semantics step rtranclp}:

\[ :: (\langle \tau :: \text{linordered field} \rangle \text{ config} \Rightarrow \tau \text{ config} \Rightarrow \text{bool} \] \[ (\_ \leftrightarrow \_ \_ 70) \]

\textbf{where} \[ C_1 \leftrightarrow^* C_2 \equiv \text{ operational semantics step }^* C_1 C_2 \]

\textbf{abbreviation operational semantics step tranclp}:

\[ :: (\langle \tau :: \text{linordered field} \rangle \text{ config} \Rightarrow \tau \text{ config} \Rightarrow \text{bool} \] \[ (\_ \leftrightarrow^+ \_ \_ 70) \]

\textbf{where} \[ C_1 \leftrightarrow^+ C_2 \equiv \text{ operational semantics step }^+ C_1 C_2 \]

\textbf{abbreviation operational semantics step reflclp}:

\[ :: (\langle \tau :: \text{linordered field} \rangle \text{ config} \Rightarrow \tau \text{ config} \Rightarrow \text{bool} \] \[ (\_ \leftrightarrow= \_ \_ 70) \]

\textbf{where} \[ C_1 \leftrightarrow= C_2 \equiv \text{ operational semantics step }= C_1 C_2 \]

\textbf{abbreviation operational semantics step relpow}:

\[ :: (\langle \tau :: \text{linordered field} \rangle \text{ config} \Rightarrow \text{nat} \Rightarrow \tau \text{ config} \Rightarrow \text{bool} \] \[ (\_ \leftrightarrow\_ \_ 70) \]

\textbf{where} \[ C_1 \leftrightarrow^* C_2 \equiv (\text{ operational semantics step }^* \_ n) C_1 C_2 \]

\textbf{definition operational semantics elim inv}:

\[ :: (\langle \tau :: \text{linordered field} \rangle \text{ config} \Rightarrow \tau \text{ config} \Rightarrow \text{bool} \] \[ (\_ \leftrightarrow^e \_ \_ 70) \]

\textbf{where} \[ C_1 \leftrightarrow^e C_2 \equiv C_2 \rightarrow_e C_1 \]

5.2 Basic Lemmas

If a configuration can be reached in \( m \) steps from a configuration that can be reached in \( n \) steps from an original configuration, then it can be reached in \( n + m \) steps from the original.
configuration.

**Lemma operational_semantics_trans_generalized:**

assumes \( C_1 \rightarrow^n C_2 \)

assumes \( C_2 \rightarrow^* C_3 \)

shows \( C_1 \rightarrow^n *^* C_3 \)

**(proof)**

We consider the set of configurations that can be reached in one operational step from a given configuration.

**Abbreviation Cnext_solve**

\[ \langle \tau :: \text{linordered_field} \rangle \text{ config } \Rightarrow \langle \tau \rangle \text{ config set} \ (C_{\text{n}ext}) \]

where

\[ C_{\text{n}ext} \ S \equiv \{ S', S \rightarrow S' \} \]

Advancing to the next instant is possible when there are no more constraints on the current instant.

**Lemma Cnext_solve_instant:**

\[ \langle C_{\text{n}ext} (\Gamma, n \vdash \emptyset \triangleright \Phi) \rangle \supseteq \{ \Gamma, \text{Suc} \ n \vdash \Phi \triangleright \emptyset \} \]

**(proof)**

The following lemmas state that the configurations produced by the elimination rules of the operational semantics belong to the configurations that can be reached in one step.

**Lemma Cnext_solve_sporadicon:**

\[ \langle C_{\text{n}ext} (\Gamma, n \vdash ((K_1 \text{ sporadic } \tau \text{ on } K_2) \ # \ \Psi) \triangleright \Phi) \rangle \supseteq \{ \Gamma, n \vdash \Psi \triangleright ((K_1 \text{ sporadic } \tau \text{ on } K_2) \ # \ \Phi), \]

\[ ((K_1 \uparrow n) \ # (K_2 \downarrow n \ # \tau) \ # \Gamma), n \vdash \Psi \triangleright \Phi \} \]

**(proof)**

**Lemma Cnext_solve_tagrel:**

\[ \langle C_{\text{n}ext} (\Gamma, n \vdash ((\text{time-relation} \ [K_1, K_2] \in \mathcal{R}) \ # \ \Psi) \triangleright \Phi) \rangle \supseteq \{ \Gamma, n \vdash \Psi \triangleright ((\text{time-relation} \ [K_1, K_2] \in \mathcal{R}) \ # \ \Phi) \} \]

**(proof)**

**Lemma Cnext_solve_implies:**

\[ \langle C_{\text{n}ext} (\Gamma, n \vdash ((K_1 \text{ implies } K_2) \ # \ \Psi) \triangleright \Phi) \rangle \supseteq \{ \Gamma, n \vdash \Psi \triangleright ((K_1 \text{ implies } K_2) \ # \ \Phi), \]

\[ ((K_1 \uparrow n) \ # (K_2 \downarrow [n] \ # \Gamma), n \vdash \Psi \triangleright ((K_1 \text{ implies } K_2) \ # \ \Phi) \} \]

**(proof)**

**Lemma Cnext_solve_implies_not:**

\[ \langle C_{\text{n}ext} (\Gamma, n \vdash ((K_1 \text{ implies not } K_2) \ # \ \Psi) \triangleright \Phi) \rangle \supseteq \{ ((K_1 \uparrow [n] \ # \Gamma), n \vdash \Psi \triangleright ((K_1 \text{ implies not } K_2) \ # \ \Phi), \]

\[ ((K_1 \uparrow [n]) \ # (K_2 \downarrow [n]) \ # \Gamma), n \vdash \Psi \triangleright ((K_1 \text{ implies not } K_2) \ # \ \Phi) \} \]

**(proof)**

**Lemma Cnext_solve_time_delayed:**

\[ \langle C_{\text{n}ext} (\Gamma, n \vdash ((K_1 \text{ time-delayed by } \delta \tau \text{ on } K_2 \text{ implies } K_3) \ # \ \Psi) \triangleright \Phi) \rangle \supseteq \{ ((K_1 \uparrow [n] \ # \Gamma), n \vdash \Psi \triangleright ((K_1 \text{ time-delayed by } \delta \tau \text{ on } K_2 \text{ implies } K_3) \ # \ \Phi), \]

\[ ((K_1 \uparrow [n]) \ # (K_2 \oplus [n] \ # \delta \tau \Rightarrow K_3) \ # \Gamma), n \vdash \Psi \triangleright ((K_1 \text{ time-delayed by } \delta \tau \text{ on } K_2 \text{ implies } K_3) \ # \ \Phi) \} \]

**(proof)**

**Lemma Cnext_solve_weakly_precedes:**

\[ \langle C_{\text{n}ext} (\Gamma, n \vdash ((K_1 \text{ weakly precedes } K_2) \ # \ \Psi) \triangleright \Phi) \rangle \supseteq \{ ((\# K_2 \ n, \ # K_1 \ n) \in (\lambda(x,y). x \leq y) \ # \Gamma), n \]
5.2. BASIC LEMMAS

\[ \vdash \Psi \triangleright ((K_1 \text{ weakly precedes } K_2) \# \Phi) \]

(proof)

lemma Cnext_solve_strictly_precedes:
\[ \langle C_{next} (\Gamma, n \vdash ((K_1 \text{ strictly precedes } K_2) \# \Psi) \triangleright \Phi) \rangle \supseteq \{ ((\#^\leq K_2 n, \#^< K_1 n) \in (\lambda(x,y). x \leq y) \# \Gamma), n \vdash \Psi \triangleright ((K_1 \text{ strictly precedes } K_2) \# \Phi) \} \]

(proof)

lemma Cnext_solve_kills:
\[ \langle C_{next} (\Gamma, n \vdash ((K_1 \text{ kills } K_2) \# \Psi) \triangleright \Phi) \rangle \supseteq \{ ((K_1 \neg \uparrow n) \# \Gamma), n \vdash \Psi \triangleright ((K_1 \text{ kills } K_2) \# \Phi), ((K_1 \uparrow n) \# (K_2 \neg \uparrow \geq n) \# \Gamma), n \vdash \Psi \triangleright ((K_1 \text{ kills } K_2) \# \Phi) \} \]

(proof)

An empty specification can be reduced to an empty specification for an arbitrary number of steps.

lemma empty_spec_reductions:
\[ \langle [], 0 \vdash [] \triangleright [] \rangle \rightarrow^* \{ [], k \vdash [] \triangleright [] \} \]

(proof)

end
Chapter 6

Equivalence of the Operational and Denotational Semantics

theory Corecursive_PROP
imports
SymbolicPrimitive
Operational
Denotational
begin

6.1 Stepwise denotational interpretation of TESL atoms

In order to prove the equivalence of the denotational and operational semantics, we need to be able to ignore the past (for which the constraints are encoded in the context) and consider only the satisfaction of the constraints from a given instant index. For this purpose, we define an interpretation of TESL formulae for a suffix of a run. That interpretation is closely related to the denotational semantics as defined in the preceding chapters.

fun TESL_interpretation_atomic_stepwise :: ('τ::linordered_field) TESL_atomic ⇒ nat ⇒ 'τ run set) ( '${}_T E S L \geq${}_i =${}_\varrho$. \exists n \geq i. hamlet ((Rep_run \varrho) n K_1) \land time ((Rep_run \varrho) n K_2) = \tau )
where
  \langle \langle K_1 \text{ sporadic } \tau \text{ on } K_2 \rangle_T E S L ^ \geq i = \{ \varrho. \exists n \geq i. \text{ hamlet } ((\text{Rep}_\varrho)(n \ n K_1) \land \text{time } ((\text{Rep}_\varrho)(n \ n K_2)) = \tau ) \rangle \}
| \langle \langle \text{time-relation } \{ K_1, K_2 \} \in R \rangle_T E S L ^ \geq i = \{ \varrho. \forall n \geq i. \text{R } \text{time } ((\text{Rep}_\varrho)(n \ n K_1), \text{time } ((\text{Rep}_\varrho)(n \ n K_2))) \rangle \}
| \langle \langle \text{master implies slave } \rangle_T E S L ^ \geq i = \{ \varrho. \forall n \geq i. \text{hamlet } ((\text{Rep}_\varrho)(n \ n \text{master}) \rightarrow \text{hamlet } ((\text{Rep}_\varrho)(n \ n \text{slave})) \rangle \}
| \langle \langle \text{master implies not slave } \rangle_T E S L ^ \geq i = \{ \varrho. \forall n \geq i. \text{hamlet } ((\text{Rep}_\varrho)(n \ n \text{master}) \rightarrow \neg \text{hamlet } ((\text{Rep}_\varrho)(n \ n \text{slave})) \rangle \}
| \langle \langle \text{master time-delayed by } \delta \tau \text{ on measuring implies slave } \rangle_T E S L ^ \geq i = \{ \varrho. \forall n \geq i. \text{hamlet } ((\text{Rep}_\varrho)(n \ n \text{master}) \rightarrow \text{let measured_time = time } ((\text{Rep}_\varrho)(n \ n \text{measuring}) \text{ in } \forall m \geq n. \text{first_time } \varrho \text{ measuring } m \ (\text{measured_time } + \delta \tau) \rightarrow \text{hamlet } ((\text{Rep}_\varrho)(m \ n \text{slave})) \rangle \}
| \langle \langle K_1 \text{ weakly precedes } K_2 \rangle_T E S L ^ \geq i = \{ \varrho. \forall n \geq i. \text{run_tick_count } \varrho K_2 n \leq \text{(run_tick_count } \varrho K_1 n) \rangle \}

29
30  CHAPTER 6. SEMANTICS EQUIVALENCE

\[ \begin{align*}
\{ \text{K}_1 \text{ strictly precedes } \text{K}_2 \}^\leq_{T_{ESL}} & = \\
& \{ \varphi. \forall n \geq 1. (\text{run_tick_count } \varphi \text{ K}_2 n) \leq (\text{run_tick_count } \text{strictly } \varphi \text{ K}_1 n) \} \\
\{ \text{K}_1 \text{ kills } \text{K}_2 \}^\leq_{T_{ESL}} & = \\
& \{ \varphi. \forall n \geq 1. \text{hamlet } ((\text{Rep_run } \varphi) \text{ n } \text{K}_1) \rightarrow (\forall m \geq n. \neg \text{hamlet } ((\text{Rep_run } \varphi) \text{ m } \text{K}_2)) \}
\end{align*} \]

The denotational interpretation of TESL formulae can be unfolded into the stepwise interpretation.

**Lemma** TESL_interpret_unfold_stepwise_sporadicon:

\[ \begin{align*}
\{ \text{K}_1 \text{ sporadic } \tau \text{ on } \text{K}_2 \}^\cap_{T_{ESL}} & = \\
& \bigcup \{ Y. \exists n::\text{nat. } Y = \{ \text{K}_1 \text{ sporadic } \tau \text{ on } \text{K}_2 \}^\cap_{T_{ESL}} \geq n \}
\end{align*} \]

*Proof*

**Lemma** TESL_interpret_unfold_stepwise_tagrelgen:

\[ \begin{align*}
\{ \text{time-relation } \lfloor \text{K}_1, \text{K}_2 \rfloor \in R \}^\cap_{T_{ESL}} & = \\
& \bigcap \{ Y. \exists n::\text{nat. } Y = \{ \text{time-relation } \lfloor \text{K}_1, \text{K}_2 \rfloor \in R \}^\cap_{T_{ESL}} \geq n \}
\end{align*} \]

*Proof*

**Lemma** TESL_interpret_unfold_stepwise_implies:

\[ \begin{align*}
\{ \text{master implies slave } \}^\cap_{T_{ESL}} & = \\
& \bigcap \{ Y. \exists n::\text{nat. } Y = \{ \text{master implies slave } \}^\cap_{T_{ESL}} \geq n \}
\end{align*} \]

*Proof*

**Lemma** TESL_interpret_unfold_stepwise_implies_not:

\[ \begin{align*}
\{ \text{master implies not slave } \}^\cap_{T_{ESL}} & = \\
& \bigcap \{ Y. \exists n::\text{nat. } Y = \{ \text{master implies not slave } \}^\cap_{T_{ESL}} \geq n \}
\end{align*} \]

*Proof*

**Lemma** TESL_interpret_unfold_stepwise_timedelayed:

\[ \begin{align*}
\{ \text{master time-delayed by } \delta \tau \text{ on measuring implies slave } \}^\cap_{T_{ESL}} & = \\
& \bigcap \{ Y. \exists n::\text{nat. } Y = \{ \text{master time-delayed by } \delta \tau \text{ on measuring implies slave } \}^\cap_{T_{ESL}} \geq n \}
\end{align*} \]

*Proof*

**Lemma** TESL_interpret_unfold_stepwise_weakly_precedes:

\[ \begin{align*}
\{ \text{K}_1 \text{ weakly precedes } \text{K}_2 \}^\cap_{T_{ESL}} & = \\
& \bigcap \{ Y. \exists n::\text{nat. } Y = \{ \text{K}_1 \text{ weakly precedes } \text{K}_2 \}^\cap_{T_{ESL}} \geq n \}
\end{align*} \]

*Proof*

**Lemma** TESL_interpret_unfold_stepwise_strictly_precedes:

\[ \begin{align*}
\{ \text{K}_1 \text{ strictly precedes } \text{K}_2 \}^\cap_{T_{ESL}} & = \\
& \bigcap \{ Y. \exists n::\text{nat. } Y = \{ \text{K}_1 \text{ strictly precedes } \text{K}_2 \}^\cap_{T_{ESL}} \geq n \}
\end{align*} \]

*Proof*

**Lemma** TESL_interpret_unfold_stepwise_kills:

\[ \begin{align*}
\{ \text{master kills slave } \}^\cap_{T_{ESL}} & = \\
& \bigcap \{ Y. \exists n::\text{nat. } Y = \{ \text{master kills slave } \}^\cap_{T_{ESL}} \geq n \}
\end{align*} \]

*Proof*

Positive atomic formulae (the ones that create ticks from nothing) are unfolded as the union of the stepwise interpretations.

**Theorem** TESL_interpret_unfold_stepwise_positive_atoms:

*Assumes* positive_atom \( \varphi \)

*Shows* \( \{ \varphi ::'\tau::\text{linordered_field TESL_atomic } \}^\cup_{T_{ESL}} = \bigcup \{ Y. \exists n::\text{nat. } Y = \{ \varphi \}^\cup_{T_{ESL}} \geq n \} \)

*Proof*

Negative atomic formulae are unfolded as the intersection of the stepwise interpretations.

**Theorem** TESL_interpret_unfold_stepwise_negative_atoms:

*Assumes* \( \neg \text{positive_atom } \varphi \)
6.2. COINDUCTION UNFOLDING PROPERTIES

Some useful lemmas for reasoning on properties of sequences.

**Lemma**: `forall_nat_expansion`

\[(\forall n \geq (n_0::nat). P n) = (P n_0 \land (\forall n \geq Suc n_0. P n))\]

**Proof**

**Lemma**: `exists_nat_expansion`

\[(\exists n \geq (n_0::nat). P n) = (P n_0 \lor (\exists n \geq Suc n_0. P n))\]

**Proof**

**Lemma**: `forall_nat_set_suc`

\[\{x. \forall m \geq n. P x m\} = \{x. P x n\} \cap \{x. \forall m \geq Suc n. P x m\}\]

**Proof**

**Lemma**: `exists_nat_set_suc`

\[\{x. \exists m \geq n. P x m\} = \{x. P x n\} \cup \{x. \exists m \geq Suc n. P x m\}\]

**Proof**

6.2 Coinduction Unfolding Properties

The following lemmas show how to shorten a suffix, i.e. to unfold one instant in the construction of a run. They correspond to the rules of the operational semantics.

**Lemma**: `TESL_interp_stepwise_sporadicon_coind_unfold`

\[\[ K_1 \text{ sporadic } \tau \text{ on } K_2 \] T_{ESL} \geq n = \[ K_1 \uparrow n \] \text{prim} \cap \[ K_2 \downarrow \n \uparrow \text{prim} \] \quad \text{— rule sporadic_on_e2}\]
\[\cup \[ K_1 \text{ sporadic } \tau \text{ on } K_2 \] T_{ESL} \geq Suc n \] \quad \text{— rule sporadic_on_e1}\]

**Proof**

**Lemma**: `TESL_interp_stepwise_tagrel_coind_unfold`

\[\[ \text{time-relation } [K_1, K_2] \in R \] T_{ESL} \geq n = \quad \text{— rule tagrel_e}\]
\[\[ \tau_{var}(K_1, n), \tau_{var}(K_2, n) \] \in R \] \text{prim}\]
\[\cap \[ \text{time-relation } [K_1, K_2] \in R \] T_{ESL} \geq Suc n \]

**Proof**

**Lemma**: `TESL_interp_stepwise_implies_coind_unfold`

\[\[ \text{master implies slave} \] T_{ESL} \geq n = \quad \text{— rule implies_e1}\]
\[\langle \{ \text{master } \n \uparrow n \} \text{prim} \rangle \quad \text{— rule implies_e2}\]
\[\cap \{ \text{master implies slave} \] T_{ESL} \geq Suc n\]

**Proof**

**Lemma**: `TESL_interp_stepwise_implies_not_coind_unfold`

\[\{ \text{master implies not slave} \] T_{ESL} \geq n = \quad \text{— rule implies_not_e1}\]
\[\langle \{ \text{master } \n \uparrow n \} \text{prim} \rangle \quad \text{— rule implies_not_e2}\]
\[\cap \{ \text{master implies not slave} \] T_{ESL} \geq Suc n\]

**Proof**

**Lemma**: `TESL_interp_stepwise_timedelayed_coind_unfold`

\[\{ \text{master time-delayed by } \delta \tau \text{ on measuring implies slave} \] T_{ESL} \geq n = \quad \text{— rule timedelayed_e1}\]
\[\langle \{ \text{master } \n \uparrow n \} \text{prim} \rangle \quad \text{— rule timedelayed_e2}\]
\[\cup \{ \text{master } \n \uparrow n \} \text{prim} \cap \{ \text{measuring } \n \oplus \delta \tau \Rightarrow \text{slave} \} \text{prim}\]
\( \cap [ \text{master time-delayed by } \delta \tau \text{ on measuring implies slave } ]_{\text{TESL} \geq \text{Suc } n} \)

(prop)

lemma TESL_interp_stepwise_weakly_precedes_coind_unfold:
\[
\begin{align*}
& \{ [ K_1 \text{ weakly precedes } K_2 ]_{\text{TESL} \geq n} = - \text{ rule weakly_precedes_e} \\
& \cap [ (\# K_2 n, \# K_1 n) \in (\lambda(x, y). x \leq y)]_{\text{prim}} \\
& \cap [ K_1 \text{ weakly precedes } K_2 ]_{\text{TESL} \geq \text{Suc } n} \\
\end{align*}
\]

(prop)

lemma TESL_interp_stepwise_strictly_precedes_coind_unfold:
\[
\begin{align*}
& \{ [ K_1 \text{ strictly precedes } K_2 ]_{\text{TESL} \geq n} = - \text{ rule strictly_precedes_e} \\
& \cap [ (\# K_2 n, \# K_1 n) \in (\lambda(x, y). x \leq y)]_{\text{prim}} \\
& \cap [ K_1 \text{ strictly precedes } K_2 ]_{\text{TESL} \geq \text{Suc } n} \\
\end{align*}
\]

(prop)

lemma TESL_interp_stepwise_kills_coind_unfold:
\[
\begin{align*}
& \{ [ K_1 \text{ kills } K_2 ]_{\text{TESL} \geq n} = - \text{ rule kills_e1} \\
& \cap [ K_1 \text{ } \# \cap \{ K_2 \text{ } \# \geq n \}]_{\text{prim}} \\
& \cap [ K_1 \text{ kills } K_2 ]_{\text{TESL} \geq \text{Suc } n} \\
\end{align*}
\]

(prop)

The stepwise interpretation of a TESL formula is the intersection of the interpretation of its atomic components.

fun TESL_interpretation_stepwise \::: ('\tau :: linordered_field TESL_formula \Rightarrow nat \Rightarrow '\tau \text{ run set})
\( )
\)

where
\[
\begin{align*}
& \{ []_{\text{TESL} \geq n} = \{ \text{by True} \} \\
& \{ \varphi \# \Phi \}_T_{\text{TESL} \geq n} = \{ \varphi \}_T_{\text{TESL} \geq n} \cap \{ \Phi \}_T_{\text{TESL} \geq n} \\
\end{align*}
\]

lemma TESL_interpretation_stepwise_fixpoint:
\[
\begin{align*}
& \{ \Phi \}_T_{\text{TESL} \geq n} = \bigcap ((\lambda \varphi. \{ \varphi \}_T_{\text{TESL} \geq n} ) ' \text{ set } \Phi) \\
\end{align*}
\]

(prop)

The global interpretation of a TESL formula is its interpretation starting at the first instant.

lemma TESL_interpretation_stepwise_zero:
\[
\{ \varphi \}_T_{\text{TESL} \geq n} = \{ \varphi \}_T_{\text{TESL} \geq 0} \\
\]

(prop)

lemma TESL_interpretation_stepwise_zero':
\[
\{ \Phi \}_T_{\text{TESL} \geq n} = \{ \Phi \}_T_{\text{TESL} \geq 0} \\
\]

(prop)

lemma TESL_interpretation_stepwise_consmorph:
\[
\{ \varphi \}_T_{\text{TESL} \geq n} \cap \{ \Phi \}_T_{\text{TESL} \geq n} = \{ \varphi \# \Phi \}_T_{\text{TESL} \geq n} \\
\]

(prop)

theorem TESL_interp_stepwise_composition:
\[
\text{shows } (\{ \Phi_1 \circ \Phi_2 \}_T_{\text{TESL} \geq n} = \{ \Phi_1 \}_T_{\text{TESL} \geq n} \cap \{ \Phi_2 \}_T_{\text{TESL} \geq n} \\
\]

(prop)
6.3 Interpretation of configurations

The interpretation of a configuration of the operational semantics abstract machine is the intersection of:

- the interpretation of its context (the past),
- the interpretation of its present from the current instant,
- the interpretation of its future from the next instant.

```
fun HeronConf_interpretation
    :: ('a::linordered_field config ⇒ 'a run set) ⇒
        (HeronConf_interpretation config) type
where
    [Γ, n ⊢ Ψ ⊬ Φ]config = ([Γ] |pr| ∩ [[Ψ]] |TESL| ≥ n ∩ [[Φ]] |TESL| ≥ Suc n)
```

```
lemma HeronConf_interp_composition:
    ⟨[Γ, n ⊢ Ψ ⊬ Φ]config⟩ ∩
    ⟨[Γ', n ⊢ Ψ' ⊬ Φ']config⟩ =
    ⟨([Γ ⊆ Γ'], n ⊢ Ψ' ⊬ Ψ) ∪ ([Ψ ⊬ Φ']config)⟩
(proof)
```

When there are no remaining constraints on the present, the interpretation of a configuration is the same as the configuration at the next instant of its future. This corresponds to the introduction rule of the operational semantics.

```
lemma HeronConf_interp_stepwise_instant_cases:
    ⟨[Γ, n ⊢ Ψ ⊬ Φ]config⟩ =
    ⟨[Γ, Suc n ⊢ Ψ ⊬ Φ]config⟩
(proof)
```

The following lemmas use the unfolding properties of the stepwise denotational semantics to give rewriting rules for the interpretation of configurations that match the elimination rules of the operational semantics.

```
lemma HeronConf_interp_stepwise_sporadicon_cases:
    ⟨[Γ, n ⊢ (K1 sporadic τ on K2) # Ψ]config⟩ =
    ⟨([τ var (K1, n)], n ⊢ Ψ ⊬ Φ) config⟩ ∪
    ⟨((K1 ↑ n) # (K2 ↓ n @ τ) # Γ), n ⊢ Ψ ⊬ Φ]config⟩
(proof)
```

```
lemma HeronConf_interp_stepwise_tagrel_cases:
    ⟨[Γ, n ⊢ (time-relation ⌊K1, K2⌋ ∈ R) # Ψ]config⟩ =
    ⟨((τ var (K1, n), τ var (K2, n)) ∈ R) # Γ), n ⊢ Ψ ⊬ ((time-relation ⌊K1, K2⌋ ∈ R) # Φ) config⟩
(proof)
```

```
lemma HeronConf_interp_stepwise_implies_cases:
    ⟨[Γ, n ⊢ (K1 implies K2) # Ψ]config⟩ =
    ⟨(K1 →↑ n) # Γ), n ⊢ Ψ ⊬ (K1 implies K2) # Φ) config⟩ ∪
    ⟨((K1 ↑ n) # K2 ⊥ n) # Γ), n ⊢ Ψ ⊬ (K1 implies K2) # Φ]config⟩
(proof)
```

```
lemma HeronConf_interp_stepwise_implies_not_cases:
    ⟨[Γ, n ⊢ (K1 implies not K2) # Ψ]config⟩ =
    ⟨((K1 → n) # Γ), n ⊢ Ψ ⊬ (K1 implies not K2) # Φ) config⟩ ∪
    ⟨((K1 ↑ n) # (K2 ⊥ n) # Γ), n ⊢ Ψ ⊬ (K1 implies not K2) # Φ]config⟩
(proof)
```

```
lemma HeronConf_interp_stepwise_timedelayed_cases:
    ⟨[Γ, n ⊢ (K1 implies timedelayed K2) # Ψ]config⟩ =
    ⟨(K1 →↑ n) # Γ), n ⊢ Ψ ⊬ (K1 implies timedelayed K2) # Φ) config⟩ ∪
    ⟨((K1 ↑ n) # (K2 ⊥ n) # Γ), n ⊢ Ψ ⊬ (K1 implies timedelayed K2) # Φ]config⟩
(proof)
```

\[ \Gamma, n \vdash ([K_1 \text{ time-delayed by } \delta \tau \text{ on } K_2 \implies K_3] \# \Psi) \triangleright \Phi \] config

\[ = \Gamma \vdash ([K_1 \dashv n] \# \Gamma), n \vdash \Psi \triangleright ([K_1 \text{ time-delayed by } \delta \tau \text{ on } K_2 \implies K_3] \# \Phi) \] config

\[ \cup \Gamma \vdash ([K_1 \dashv n] \# (K_2 \oplus n \oplus \delta \tau \Rightarrow K_3) \# \Gamma), n \]

\[ \vdash \Psi \triangleright ([K_1 \text{ time-delayed by } \delta \tau \text{ on } K_2 \implies K_3] \# \Phi) \] config

\langle \text{proof} \rangle

\begin{align*}
\text{lemma } & \text{HeronConf_interp_stepwise_weakly_precedes_cases:} \\
& ([\Gamma, n \vdash ([K_1 \text{ weakly precedes } K_2] \# \Psi) \triangleright \Phi] \text{ config} \\
& = \Gamma \vdash ([([\# K_2 n, \# K_1 n] \in (\lambda(x,y). x \leq y)) \# \Gamma), n \\
& \vdash \Psi \triangleright ([K_1 \text{ weakly precedes } K_2] \# \Phi) \] config
\end{align*}

\langle \text{proof} \rangle

\begin{align*}
\text{lemma } & \text{HeronConf_interp_stepwise_strictly_precedes_cases:} \\
& ([\Gamma, n \vdash ([K_1 \text{ strictly precedes } K_2] \# \Psi) \triangleright \Phi] \text{ config} \\
& = \Gamma \vdash ([([\# K_2 n, \# K_1 n] \in (\lambda(x,y). x < y)) \# \Gamma), n \\
& \vdash \Psi \triangleright ([K_1 \text{ strictly precedes } K_2] \# \Phi) \] config
\end{align*}

\langle \text{proof} \rangle

\begin{align*}
\text{lemma } & \text{HeronConf_interp_stepwise_kills_cases:} \\
& ([\Gamma, n \vdash ([K_1 \text{ kills } K_2] \# \Psi) \triangleright \Phi] \text{ config} \\
& = \Gamma \vdash ([K_1 \dashv n] \# \Gamma), n \vdash \Psi \triangleright ([K_1 \text{ kills } K_2] \# \Phi) \] config
\end{align*}

\langle \text{proof} \rangle

end
Chapter 7

Main Theorems

theory Hygge_Theory
imports
  Corecursive_Prop
begin

Using the properties we have shown about the interpretation of configurations and the stepwise unfolding of the denotational semantics, we can now prove several important results about the construction of runs from a specification.

7.1 Initial configuration

The denotational semantics of a specification $\Psi$ is the interpretation at the first instant of a configuration which has $\Psi$ as its present. This means that we can start to build a run that satisfies a specification by starting from this configuration.

theorem solve_start:
  shows $\langle \llbracket \llbracket \Psi \rrbracket \rrbracket \triangleright ESL = \llbracket \llbracket \cdot, 0 \triangleright \cdot \rrbracket_{config} \rangle$
(proof)

7.2 Soundness

The interpretation of a configuration $S_2$ that is a refinement of a configuration $S_1$ is contained in the interpretation of $S_1$. This means that by making successive choices in building the instants of a run, we preserve the soundness of the constructed run with regard to the original specification.

lemma sound_reduction:
  assumes $(\Gamma_1, n_1 \triangleright \Psi_1 \triangleright \Phi_1) \iff (\Gamma_2, n_2 \triangleright \Psi_2 \triangleright \Phi_2)$
  shows $\llbracket \llbracket \Gamma_1 \rrbracket_{prim} \cap \llbracket \llbracket \Psi_1 \rrbracket_{ESL} \geq n_1 \cap \llbracket \llbracket \Phi_1 \rrbracket_{ESL} \geq \text{Suc } n_1$
    $\geq \llbracket \llbracket \Gamma_2 \rrbracket_{prim} \cap \llbracket \llbracket \Psi_2 \rrbracket_{ESL} \geq n_2 \cap \llbracket \llbracket \Phi_2 \rrbracket_{ESL} \geq \text{Suc } n_2 \rangle$ (is ?P)
(proof)

inductive_cases step_elim:$(S_1 \iff S_2)$

lemma sound_reduction':
  assumes $(S_1 \iff S_2)$
  shows $\llbracket S_1 \rrbracket_{config} \geq \llbracket S_2 \rrbracket_{config}$
(proof)
lemma sound_reduction_generalized:
          assumes (S₁ ↦^k S₂)
          shows (⟦ S₁ ⟧_{config} ⊇ ⟦ S₂ ⟧_{config})
(proof)

From the initial configuration, a configuration S obtained after any number k of reduction steps
denotes runs from the initial specification Ψ.

theorem soundness:
          assumes ⟨([], 0 ⊢ Ψ ⊢ []) ↦^k S⟩
          shows (⟦ Ψ ⟧_{TESL} ⊇ ⟦ S ⟧_{config})
(proof)

7.3 Completeness

We will now show that any run that satisfies a specification can be derived from the initial
configuration, at any number of steps.

We start by proving that any run that is denoted by a configuration S is necessarily denoted by
at least one of the configurations that can be reached from S.

lemma complete_direct_successors:
          shows (⟦ Γ, n ⊢ Ψ ⊢ Φ ⟧_{config} ⊆ (⋃ X ∈ C next (Γ, n ⊢ Ψ ⊢ Φ). ⟦ X ⟧_{config}))
(proof)

lemma complete_direct_successors':
          shows (⟦ S ⟧_{config} ⊆ (⋃ X ∈ next S. ⟦ X ⟧_{config}))
(proof)

Therefore, if a run belongs to a configuration, it necessarily belongs to a configuration derived
from it.

lemma branch_existence:
          assumes ⟨ϱ ∈ ⟦ S₁ ⟧_{config}⟩
          shows (∃ S₂. (S₁ ↦ S₂) ∧ (ϱ ∈ ⟦ S₂ ⟧_{config}))
(proof)

lemma branch_existence':
          assumes ⟨ϱ ∈ ⟦ S₁ ⟧_{config}⟩
          shows (∃ S₂. (S₁ ↦^k S₂) ∧ (ϱ ∈ ⟦ S₂ ⟧_{config}))
(proof)

Any run that belongs to the original specification Ψ has a corresponding configuration S at any
number k of reduction steps from the initial configuration. Therefore, any run that satisfies a
specification can be derived from the initial configuration at any level of reduction.

theorem completeness:
          assumes ⟨ϱ ∈ ⟦ Ψ ⟧_{TESL}⟩
          shows (∃ S. (([], 0 ⊢ Ψ ⊢ []) ↦^k S)
          ∧ ϱ ∈ ⟦ S ⟧_{config})
(proof)

7.4 Progress

Reduction steps do not guarantee that the construction of a run progresses in the sequence of
instants. We need to show that it is always possible to reach the next instant, and therefore any
future instant, through a number of steps.
lemma instant_index_increase:
assumes \( \langle \varrho \in [\{ \Gamma, n \vdash \Psi \triangleright \Phi \}]_{\text{config}} \rangle \)
shows \( \langle \exists \Gamma_k \Psi_k \Phi_k \cdot ((\Gamma, n \vdash \Psi \triangleright \Phi) \hookrightarrow^k (\Gamma_k, \text{Suc } n \vdash \Psi_k \triangleright \Phi_k)) \wedge \varrho \in [\{ \Gamma_k, \text{Suc } n \vdash \Psi_k \triangleright \Phi_k \}]_{\text{config}} \rangle \)
\(\langle \text{proof} \rangle\)

lemma instant_index_increase_generalized:
assumes \( n < n_k \)
assumes \( \langle \varrho \in [\{ \Gamma, n \vdash \Psi \triangleright \Phi \}]_{\text{config}} \rangle \)
shows \( \langle \exists \Gamma_k \Psi_k \Phi_k \cdot ((\Gamma, n \vdash \Psi \triangleright \Phi) \hookrightarrow^k (\Gamma_k, n_k \vdash \Psi_k \triangleright \Phi_k)) \wedge \varrho \in [\{ \Gamma_k, n_k \vdash \Psi_k \triangleright \Phi_k \}]_{\text{config}} \rangle \)
\(\langle \text{proof} \rangle\)

Any run that belongs to a specification \( \Psi \) has a corresponding configuration that develops it up to the \( n \)th instant.

theorem progress:
assumes \( \langle \varrho \in [\{ \Psi \}]_{\text{TESL}} \rangle \)
shows \( \langle \exists \mu \cdot ((\varnothing, 0 \vdash \varnothing) \hookrightarrow e (\Gamma, n \vdash \Psi \triangleright \Phi)) \wedge \varrho \in [\{ \Gamma, n \vdash \Psi \triangleright \Phi \}]_{\text{config}} \rangle \)
\(\langle \text{proof} \rangle\)

7.5 Local termination

Here, we prove that the computation of an instant in a run always terminates. Since this computation terminates when the list of constraints for the present instant becomes empty, we introduce a measure for this formula.

primrec measure_interpretation :: \( \langle \cdot : \text{linordered_field } \text{TESL_formula} \Rightarrow \text{nat} \rangle (\langle \cdot \rangle) \)
where
\[ \langle \cdot \rangle \emptyset = (0) \]
\[ \langle \cdot \rangle \varphi \# \Phi = \begin{cases} 1 + \langle \cdot \rangle \Phi & \text{sporadic} \rightarrow \varphi \rightarrow \Phi \rightarrow \text{on} \rightarrow \varnothing \rightarrow 1 + \langle \cdot \rangle \Phi \\ 2 + \langle \cdot \rangle \Phi & \end{cases} \]

fun measure_interpretation_config :: \( \langle \cdot : \text{linordered_field } \text{config} \Rightarrow \text{nat} \rangle (\langle \cdot \rangle) \)
where
\[ \langle \cdot \rangle \text{config} \cdot (\Gamma, n \vdash \Psi \triangleright \Phi) = \mu \cdot \Psi \]

We then show that the elimination rules make this measure decrease.

lemma elimination_rules_strictly_decreasing:
assumes \( (\Gamma_1, n_1 \vdash \Psi_1 \triangleright \Phi_1) \hookrightarrow e (\Gamma_2, n_2 \vdash \Psi_2 \triangleright \Phi_2) \)
shows \( \mu \cdot \Psi_1 \triangleright e \cdot \mu \cdot \Psi_2 \)
\(\langle \text{proof} \rangle\)

lemma elimination_rules_strictly_decreasing_meas:
assumes \( (\Psi_1, \Psi_1 \triangleright e) \in \text{measure } \mu \)
shows \( (\Psi_1, \Psi_1 \triangleright e) \in \text{measure } \mu \)
\(\langle \text{proof} \rangle\)

lemma elimination_rules_strictly_decreasing_meas':
assumes \( (S_1 \triangleright e) \)
shows \( (S_2, S_1 \triangleright e) \in \text{measure } \mu \)
\(\langle \text{proof} \rangle\)

Therefore, the relation made up of elimination rules is well-founded and the computation of an instant terminates.
theorem instant_computation_termination:
\[ \text{wfP } (\lambda(S_1:\text{linordered_field config}) S_2. (S_1 \rightarrow_{e} S_2)) \]
\[ \langle \text{proof} \rangle \]
end
Chapter 8

Properties of TESL

8.1 Stuttering Invariance

theory StutteringDefs

imports Denotational

begin

When composing systems into more complex systems, it may happen that one system has to perform some action while the rest of the complex system does nothing. In order to support the composition of TESL specifications, we want to be able to insert stuttering instants in a run without breaking the conformance of a run to its specification. This is what we call the stuttering invariance of TESL.

8.1.1 Definition of stuttering

We consider stuttering as the insertion of empty instants (instants at which no clock ticks) in a run. We characterize this insertion with a dilating function, which maps the instant indices of the original run to the corresponding instant indices of the dilated run. The properties of a dilating function are:

- it is strictly increasing because instants are inserted into the run,
- the image of an instant index is greater than it because stuttering instants can only delay the original instants of the run,
- no instant is inserted before the first one in order to have a well defined initial date on each clock,
- if \( n \) is not in the image of the function, no clock ticks at instant \( n \) and the date on the clocks do not change.

definition dilating_fun

where
\[
\begin{align*}
\text{dilating_fun} \ (	ext{f::nat} \Rightarrow \text{nat}) \ (\text{r::'a::linordered_field run}) & \equiv \\
\text{strict_mono f} \land (f \ 0 = 0) \land (\forall n. \ f \ n \geq n) \\
& \land ((\exists n_0. \ f \ n_0 = n) \rightarrow (\forall c. \ 
eg (\text{hamlet ((Rep_run r) n c)))))
\end{align*}
\]
A run \( r \) is a dilation of a run \( \text{sub} \) by function \( f \) if:

- \( f \) is a dilating function for \( r \)
- the time in \( r \) is the time in \( \text{sub} \) dilated by \( f \)
- the hamlet in \( r \) is the hamlet in \( \text{sub} \) dilated by \( f \)

\[
\langle \text{dilating } f \text{ sub } r \equiv \text{dilating_fun } f \; r \rangle
\]

where

\[

dilating \; f \; \text{sub} \; r \equiv \text{dilating_fun } f \; r
\]

\[
\land \; \forall \; n \; c. \; \text{time } \left( \text{Rep_run } \text{sub} \; n \; c \right) = \text{time } \left( \text{Rep_run } r \; (f \; n) \; c \right)
\]

\[
\land \; \forall \; n \; c. \; \text{hamlet } \left( \text{Rep_run } \text{sub} \; n \; c \right) = \text{hamlet } \left( \text{Rep_run } r \; (f \; n) \; c \right)
\]

A run is a subrun of another run if there exists a dilation between them.

\[
\langle \text{is_subrun } \Rightarrow \; \forall \; a : \; \text{linordered_field } \text{run} \Rightarrow \; \forall \; r \Rightarrow \; \text{bool} \rangle
\]

where

\[
\langle \text{sub} \; \ll \; r \; \equiv \; \exists \; f. \; \text{dilating } f \; \text{sub} \; r \rangle
\]

A contracting function is the reverse of a dilating fun, it maps an instant index of a diluted run to the index of the last instant of a non stuttering run that precedes it. Since several successive stuttering instants are mapped to the same instant of the non stuttering run, such a function is monotonous, but not strictly. The image of the first instant of the diluted run is necessarily the first instant of the non stuttering run, and the image of an instant index is less that this index because we remove stuttering instants.

\[
\langle \text{contracting_fun } g \equiv \text{mono } g \land g \; 0 = 0 \land \forall \; n. \; g \; n \leq n \rangle
\]

Figure 8.1 illustrates the relations between the instants of a run and the instants of a diluted run, with the mappings by the dilating function \( f \) and the contracting function \( g \):

A function \( g \) is contracting with respect to the dilation of run \( \text{sub} \) into run \( r \) by the dilating function \( f \) if:
8.1. STUTTERING INVARIANCE

- it is a contracting function;
- \((f \circ g)\) \(n\) is the index of the last original instant before instant \(n\) in run \(r\), therefore:
  - \((f \circ g)\) \(n\) \(\leq\) \(n\)
  - the time does not change on any clock between instants \((f \circ g)\) \(n\) and \(n\) of run \(r\);
  - no clock ticks before \(n\) strictly after \((f \circ g)\) \(n\) in run \(r\). See Figure 8.1 for a better understanding. Notice that in this example, \(2\) is equal to \((f \circ g)\) \(2\), \((f \circ g)\) \(3\), and \((f \circ g)\) \(4\).

definition contracting where
\(\langle\ contracting\ g\ r\ sub\ f\ \equiv\ contracting\_fun\ g\ \wedge\ (\forall\ n.\ f\ (g\ n)\ \leq\ n)\ \wedge\ (\forall\ c\ k.\ f\ (g\ n)\ \leq\ k\ \wedge\ k\ \leq\ n\ \rightarrow\ time\ (Rep\_run\ r)\ k\ c\ =\ time\ ((Rep\_run\ sub)\ (g\ n)\ c))\ \wedge\ (\forall\ n\ c\ k.\ f\ (g\ n)\ <\ k\ \wedge\ k\ \leq\ n\ \rightarrow\ \neg\ hamlet\ ((Rep\_run\ r)\ k\ c))\rangle\)

For any dilating function, we can build its inverse, as illustrated on Figure 8.1, which is a contracting function:

definition dil_inverse f::(nat \Rightarrow nat) \equiv (\lambda n. Max \{i. f i \leq n\})

8.1.2 Alternate definitions for counting ticks.

For proving the stuttering invariance of TESL specifications, we will need these alternate definitions for counting ticks, which are based on sets.

tick_count \(r\ c\ n\) is the number of ticks of clock \(c\) in run \(r\) upto instant \(n\).

definition tick_count :: ('a::linordered_field run \Rightarrow clock \Rightarrow nat \Rightarrow nat)
where
\(\langle\ tick\_count\ r\ c\ n\ =\ card\ \{i.\ i\ \leq\ n\ \wedge\ hamlet\ ((Rep\_run\ r)\ i\ c)\}\rangle\)

tick_count_strict \(r\ c\ n\) is the number of ticks of clock \(c\) in run \(r\) upto but excluding instant \(n\).

definition tick_count_strict :: ('a::linordered_field run \Rightarrow clock \Rightarrow nat \Rightarrow nat)
where
\(\langle\ tick\_count\_strict\ r\ c\ n\ =\ card\ \{i.\ i\ <\ n\ \wedge\ hamlet\ ((Rep\_run\ r)\ i\ c)\}\rangle\)

end

8.1.3 Stuttering Lemmas

theory StutteringLemmas

imports StutteringDefs

begin

In this section, we prove several lemmas that will be used to show that TESL specifications are invariant by stuttering.
The following one will be useful in proving properties over a sequence of stuttering instants.

**Lemma bounded_suc_ind:**

- **Assumes:** \( \forall k. k < n \implies P (\text{Suc} (z + k)) = P (z + k) \)
- **Shows:** \( k < n \implies P (\text{Suc} (z + k)) = P z \)

**Proof**

**8.1.4 Lemmas used to prove the invariance by stuttering**

Since a dilating function is strictly monotonous, it is injective.

**Lemma dilating_fun_injects:**

- **Assumes:** \( \text{dilating_fun} f r \)
- **Shows:** \( \text{inj_on} f A \)

**Proof**

**Lemma dilating_injects:**

- **Assumes:** \( \text{dilating} f \text{ sub} r \)
- **Shows:** \( \text{inj_on} f A \)

**Proof**

If a clock ticks at an instant in a dilated run, that instant is the image by the dilating function of an instant of the original run.

**Lemma ticks_image:**

- **Assumes:** \( \text{dilating_fun} f r \) and \( \text{hamlet} ((\text{Rep\_run} r) n c) \)
- **Shows:** \( \exists n_0. f n_0 = n \)

**Proof**

**Lemma ticks_image_sub:**

- **Assumes:** \( \text{dilating} f \text{ sub} r \) and \( \text{hamlet} ((\text{Rep\_run} r) n c) \)
- **Shows:** \( \exists n_0. f n_0 = n \)

**Proof**

**Lemma ticks_image_sub':**

- **Assumes:** \( \text{dilating} f \text{ sub} r \) and \( \exists c. \text{hamlet} ((\text{Rep\_run} r) n c) \)
- **Shows:** \( \exists n_0. f n_0 = n \)

**Proof**

The image of the ticks in an interval by a dilating function is the interval bounded by the image of the bounds of the original interval. This is proven for all 4 kinds of intervals: \([m, n[\), \([m, n[\), \([m, n[\) and \([m, n[\).

**Lemma dilating_fun_image_strict:**

- **Assumes:** \( \text{dilating\_fun} f r \)
- **Shows:** \( \{k. f m < k \land k < f n \land \text{hamlet} ((\text{Rep\_run} r) k c)\} = \text{image} f \{k. m < k \land k < n \land \text{hamlet} ((\text{Rep\_run} r) (f k) c)\} \)

**Proof**

**Lemma dilating_fun_image_left:**

- **Assumes:** \( \text{dilating\_fun} f r \)
- **Shows:** \( \{k. f m \leq k \land k < f n \land \text{hamlet} ((\text{Rep\_run} r) k c)\} = \text{image} f \{k. m \leq k \land k < n \land \text{hamlet} ((\text{Rep\_run} r) (f k) c)\} \)

**Proof**
8.1. **STUTTERING INVARIANCE**

```
lemma dilating_fun_image_right:
assumes (dilating_fun f r)
shows (\langle k. f m < k \land k \leq f n \land \text{hamlet ((Rep_run r) k c)} \rangle
   = \text{image f} \{k. m < k \land k \leq n \land \text{hamlet ((Rep_run r) (f k) c)}\})
(is (?IMG = image f ?SET))
(proof)
```

```
lemma dilating_fun_image:
assumes (dilating_fun f r)
shows (\langle k. f m \leq k \land k \leq f n \land \text{hamlet ((Rep_run r) k c)} \rangle
   = \text{image f} \{k. m \leq k \land k \leq n \land \text{hamlet ((Rep_run r) (f k) c)}\})
(is (?IMG = image f ?SET))
(proof)
```

On any clock, the number of ticks in an interval is preserved by a dilating function.

```
lemma ticks_as_often_strict:
assumes (dilating_fun f r)
shows (card \{p. n < p \land p < m \land \text{hamlet ((Rep_run r) (f p) c)}\}
   = card \{p. f n < p \land p < f m \land \text{hamlet ((Rep_run r) p c)}\})
(is (card ?SET = card ?IMG))
(proof)
```

```
lemma ticks_as_often_left:
assumes (dilating_fun f r)
shows (card \{p. n \leq p \land p < m \land \text{hamlet ((Rep_run r) (f p) c)}\}
   = card \{p. f n \leq p \land p < f m \land \text{hamlet ((Rep_run r) p c)}\})
(is (card ?SET = card ?IMG))
(proof)
```

```
lemma ticks_as_often_right:
assumes (dilating_fun f r)
shows (card \{p. n < p \land p \leq m \land \text{hamlet ((Rep_run r) (f p) c)}\}
   = card \{p. f n < p \land p \leq f m \land \text{hamlet ((Rep_run r) p c)}\})
(is (card ?SET = card ?IMG))
(proof)
```

```
lemma ticks_as_often:
assumes (dilating_fun f r)
shows (card \{p. n \leq p \land p \leq m \land \text{hamlet ((Rep_run r) (f p) c)}\}
   = card \{p. f n \leq p \land p \leq f m \land \text{hamlet ((Rep_run r) p c)}\})
(is (card ?SET = card ?IMG))
(proof)
```

The date of an event is preserved by dilation.

```
lemma ticks_tag_image:
assumes (dilating f sub r)
and \(\exists c. \text{hamlet ((Rep_run r) k c)}\)
and \(||\text{time ((Rep_run r) k c)} = \tau\)\)
shows \(\exists k_0. f k_0 = k \land \text{time ((Rep_run sub) k_0 c)} = \tau\)
(proof)
```

TESL operators are invariant by dilation.

```
lemma ticks_sub:
assumes (dilating f sub r)
shows \(\text{hamlet ((Rep_run sub) n a)} = \text{hamlet ((Rep_run r) (f n) a)}\)
(proof)
```
Lifting a total function to a partial function on an option domain.

**Definition opt_lift:**
\[
\text{opt_lift} :: ('a ⇒ 'a) ⇒ ('a option ⇒ 'a option)
\]
where
\[
\text{opt_lift} \ f \equiv \lambda x. \text{case } x \Rightarrow \text{None} | \text{Some } y \Rightarrow \text{Some } (f \ y)
\]

The set of instants when a clock ticks in a dilated run is the image by the dilation function of the set of instants when it ticks in the subrun.

**Lemma tick_set_sub:**
\[
\text{assumes } \langle \text{dilating } f \text{ sub } r \rangle
\]
\[
\text{shows } \langle \{k. \text{hamlet ((Rep_run r) } k \text{ c)}\} = \text{image } f \{k. \text{hamlet ((Rep_run sub) } k \text{ c)}\} \rangle
\]
\[
\text{(is } ?R = \text{image } f ?S)\rangle
\]

**Proof**

Strictly monotonous functions preserve the least element.

**Lemma Least_strict_mono:**
\[
\text{assumes } \langle \text{strict_mono } f \rangle
\]
and
\[
\langle \exists x : S. \forall y : S. x \leq y \rangle
\]
\[
\text{shows } \langle (\text{LEAST } y. y \in f \ ' S) = f (\text{LEAST } x. x \in S) \rangle
\]

**Proof**

A non empty set of nats has a least element.

**Lemma Least_nat_ex:**
\[
\langle (\text{n}::\text{nat}) \in S \Longrightarrow \exists x \in S. (\forall y \in S. x \leq y) \rangle
\]

**Proof**

The first instant when a clock ticks in a dilated run is the image by the dilation function of the first instant when it ticks in the subrun.

**Lemma Least_sub:**
\[
\text{assumes } \langle \text{dilating } f \text{ sub } r \rangle
\]
and
\[
\langle \exists k : \text{nat. hamlet ((Rep_run sub) } k \text{ c)}\rangle
\]
\[
\text{shows } \langle \text{LEAST } k. k \in \{t. \text{hamlet ((Rep_run r) } t \text{ c)}\}
\]
\[
= f (\text{LEAST } k. k \in \{t. \text{hamlet ((Rep_run sub) } t \text{ c)}\})
\]
\[
\text{(is } (\text{LEAST } k. k \in ?R) = f (\text{LEAST } k. k \in ?S))\rangle
\]

**Proof**

If a clock ticks in a run, it ticks in the subrun.

**Lemma ticks_imp_ticks_sub:**
\[
\text{assumes } \langle \text{dilating } f \text{ sub } r \rangle
\]
and
\[
\langle \exists k. \text{hamlet ((Rep_run r) } k \text{ c)}\rangle
\]
\[
\text{shows } \langle \exists k_0. \text{hamlet ((Rep_run sub) } k_0 \text{ c)}\rangle
\]

**Proof**

Stronger version: it ticks in the subrun and we know when.

**Lemma ticks_imp_ticks_subk:**
\[
\text{assumes } \langle \text{dilating } f \text{ sub } r \rangle
\]
and
\[
\langle \text{hamlet ((Rep_run r) } k \text{ c)}\rangle
\]
\[
\text{shows } \langle \exists k_0. f k_0 = k \land \text{hamlet ((Rep_run sub) } k_0 \text{ c)}\rangle
\]

**Proof**

A dilating function preserves the tick count on an interval for any clock.
8.1. STUTTERING INVARIANCE

**lemma** dilated_ticks_strict:
assumes \((\text{dilating } f \text{ sub } r)\)
shows \(\{i. f m < i \land i < f n \land \text{hamlet } ((\text{Rep\_run } r) i c)\}\)
  \[=\] \(\text{image } f \{i. m < i \land i < n \land \text{hamlet } ((\text{Rep\_run sub} ) i c)\}\)
(is \(\text{?RUN} = \text{image } f \ ?\text{SUB}\))
\(\langle\text{proof}\rangle\)

**lemma** dilated_ticks_left:
assumes \((\text{dilating } f \text{ sub } r)\)
shows \(\{i. f m \leq i \land i < f n \land \text{hamlet } ((\text{Rep\_run r} ) i c)\}\)
  \[=\] \(\text{image } f \{i. m \leq i \land i < n \land \text{hamlet } ((\text{Rep\_run sub} ) i c)\}\)
(is \(\text{?RUN} = \text{image } f \ ?\text{SUB}\))
\(\langle\text{proof}\rangle\)

**lemma** dilated_ticks_right:
assumes \((\text{dilating } f \text{ sub } r)\)
shows \(\{i. f m < i \land i \leq f n \land \text{hamlet } ((\text{Rep\_run r} ) i c)\}\)
  \[=\] \(\text{image } f \{i. m < i \land i \leq n \land \text{hamlet } ((\text{Rep\_run sub} ) i c)\}\)
(is \(\text{?RUN} = \text{image } f \ ?\text{SUB}\))
\(\langle\text{proof}\rangle\)

**lemma** dilated_ticks:
assumes \((\text{dilating } f \text{ sub } r)\)
shows \(\{i. f m \leq i \land i \leq f n \land \text{hamlet } ((\text{Rep\_run r} ) i c)\}\)
  \[=\] \(\text{image } f \{i. m \leq i \land i \leq n \land \text{hamlet } ((\text{Rep\_run sub} ) i c)\}\)
(is \(\text{?RUN} = \text{image } f \ ?\text{SUB}\))
\(\langle\text{proof}\rangle\)

No tick can occur in a dilated run before the image of 0 by the dilation function.

**lemma** empty_dilated_prefix:
assumes \((\text{dilating } f \text{ sub } r)\)
and \(\langle n < f 0 \rangle\)
shows \(\langle \neg \text{hamlet } ((\text{Rep\_run r} ) n c)\rangle\)
\(\langle\text{proof}\rangle\)

**corollary** empty_dilated_prefix':
assumes \((\text{dilating } f \text{ sub } r)\)
shows \(\langle f 0 \leq i \land i \leq f n \land \text{hamlet } ((\text{Rep\_run r} ) i c)\rangle\)
  \[=\] \(\{i. i \leq f n \land \text{hamlet } ((\text{Rep\_run r}) i c)\}\)
\(\langle\text{proof}\rangle\)

**corollary** dilated_prefix:
assumes \((\text{dilating } f \text{ sub } r)\)
shows \(\langle i. i \leq f n \land \text{hamlet } ((\text{Rep\_run r} ) i c)\rangle\)
  \[=\] \(\text{image } f \{i. i \leq n \land \text{hamlet } ((\text{Rep\_run sub} ) i c)\}\)
\(\langle\text{proof}\rangle\)

**corollary** dilated_strict_prefix:
assumes \((\text{dilating } f \text{ sub } r)\)
shows \(\langle i. i < f n \land \text{hamlet } ((\text{Rep\_run r} ) i c)\rangle\)
  \[=\] \(\text{image } f \{i. i < n \land \text{hamlet } ((\text{Rep\_run sub} ) i c)\}\)
\(\langle\text{proof}\rangle\)

A singleton of \text{nat} can be defined with a weaker property.

**lemma** nat_sing_prop:
\(\langle\text{i::nat. } i = k \land P(i)\rangle\)
  \[=\] \(\{i::\text{nat. } i = k \land P(k)\}\)
\(\langle\text{proof}\rangle\)
The set definition and the function definition of \texttt{tick\_count} are equivalent.

\texttt{lemma} \texttt{tick\_count\_is\_fun[code]}: \(\texttt{tick\_count} \ r \ c \ n = \texttt{run\_tick\_count} \ r \ c \ n\)

(\texttt{proof})

To show that the set definition and the function definition of \texttt{tick\_count\_strict} are equivalent, we first show that the \texttt{strictness} of \texttt{tick\_count\_strict} can be softened using \texttt{Suc}.

\texttt{lemma} \texttt{tick\_count\_strict\_suc}: \(\texttt{tick\_count\_strict} \ r \ c \ (\texttt{Suc} \ n) = \texttt{tick\_count} \ r \ c \ n\)

(\texttt{proof})

This leads to an alternate definition of the strict precedence relation.

\texttt{lemma} \texttt{strictly\_precedes\_alt\_def1}: \(\{ \rho. \forall n::\texttt{nat}. (\texttt{run\_tick\_count} \ \rho \ K_2 \ n) \leq (\texttt{run\_tick\_count\_strictly} \ \rho \ K_1 \ n) \}\)

= \(\{ \rho. \forall n::\texttt{nat}. (\texttt{run\_tick\_count\_strictly} \ \rho \ K_2 \ (\texttt{Suc} \ n)) \leq (\texttt{run\_tick\_count\_strictly} \ \rho \ K_1 \ n) \}\)

(\texttt{proof})

The strict precedence relation can even be defined using only \texttt{run\_tick\_count}:

\texttt{lemma} \texttt{zero\_gt\_all}: assumes \(\{ P (0::\texttt{nat}) \}\)

and \(\{ \forall n. n > 0 \implies P \ n \}\)

shows \(\{ P \ n \}\)

(\texttt{proof})

\texttt{lemma} \texttt{strictly\_precedes\_alt\_def2}: \(\{ \rho. \forall n::\texttt{nat}. (\texttt{run\_tick\_count} \ \rho \ K_2 \ n) \leq (\texttt{run\_tick\_count\_strictly} \ \rho \ K_1 \ n) \}\)

= \(\{ \rho. \neg \texttt{hamlet} ((\texttt{Rep\_run} \ \rho) \ 0 \ K_2)) \)

\wedge \(\forall n::\texttt{nat}. (\texttt{run\_tick\_count} \ \rho \ K_2 \ (\texttt{Suc} \ n)) \leq (\texttt{run\_tick\_count\_strictly} \ \rho \ K_1 \ n) \}\)

(\texttt{is} \(\{ ?P = ?P' \}\))

(\texttt{proof})

Some properties of \texttt{run\_tick\_count}, \texttt{tick\_count} and \texttt{Suc}:

\texttt{lemma} \texttt{run\_tick\_count\_suc}: \(\texttt{run\_tick\_count} \ r \ c \ (\texttt{Suc} \ n) = (\text{if} \ \texttt{hamlet} ((\texttt{Rep\_run} \ r) \ (\texttt{Suc} \ n) \ c)

\text{then} \ \texttt{Suc} \ (\texttt{run\_tick\_count} \ r \ c \ n)

\text{else} \ \texttt{run\_tick\_count} \ r \ c \ n)\)

(\texttt{proof})

\texttt{corollary} \texttt{tick\_count\_suc}: \(\texttt{tick\_count} \ r \ c \ (\texttt{Suc} \ n) = (\text{if} \ \texttt{hamlet} ((\texttt{Rep\_run} \ r) \ (\texttt{Suc} \ n) \ c)

\text{then} \ \texttt{Suc} \ (\texttt{tick\_count} \ r \ c \ n)

\text{else} \ \texttt{tick\_count} \ r \ c \ n)\)

(\texttt{proof})

Some generic properties on the cardinal of sets of nat that we will need later.

\texttt{lemma} \texttt{card\_suc}: \(\{ i. i \leq (\texttt{Suc} \ n) \land P \ i \} = \texttt{card} \ \{ i. i \leq n \land P \ i \} + \texttt{card} \ \{ i. i = (\texttt{Suc} \ n) \land P \ i \}\)

(\texttt{proof})

\texttt{lemma} \texttt{card\_le\_leq}: assumes \(\{ m < n \}\)

shows \(\{ i::\texttt{nat}. m < i \land i \leq n \land P \ i \}\)
= \text{card} \{i. n < i \land i < n \land P i\} + \text{card} \{i. i = n \land P i\}\rangle
\langle proof \rangle

\text{lemma card}_{\leq}\_0:\langle card \{i::nat. i \leq n \land P i\} = card \{i. i < n \land P i\} + card \{i. i = n \land P i\} \rangle
\langle proof \rangle

\text{lemma card}_{mn}:\langle \text{assumes } m < n \implies shows (card \{i::nat. i < n \land P i\} = card \{i. i \leq m \land P i\} + card \{i. m < i \land i < n \land P i\}) \rangle
\langle proof \rangle

\text{lemma card}_{mn'}:\langle \text{assumes } m < n \implies shows (card \{i::nat. i < n \land P i\} = card \{i. i < m \land P i\} + card \{i. m \leq i \land i < n \land P i\}) \rangle
\langle proof \rangle

\text{lemma nat_interval_union}:\langle \text{assumes } m \leq n \implies shows \{i::nat. i \leq n \land P i\} = \{i::nat. i \leq m \land P i\} \cup \{i::nat. m < i \land i < n \land P i\} \rangle
\langle proof \rangle

\text{lemma card}_{\text{sing_prop}}:\langle \text{card} \{i. i = n \land P i\} = (if P n then 1 else 0) \rangle
\langle proof \rangle

\text{lemma card}_{\text{prop_mono}}:\langle \text{assumes } m \leq n \implies shows \text{card} \{i::nat. i \leq m \land P i\} \leq \text{card} \{i. i \leq n \land P i\} \rangle
\langle proof \rangle

In a dilated run, no tick occurs strictly between two successive instants that are the images by \(f\) of instants of the original run.

\text{lemma no_tick_before_suc}:\langle \text{assumes } and (f n) < k \land k < (f (Suc n)) \implies shows \neg \text{hamlet ((Rep_run r) k c)} \rangle
\langle proof \rangle

From this, we show that the number of ticks on any clock at \(f (Suc n)\) depends only on the number of ticks on this clock at \(f n\) and whether this clock ticks at \(f (Suc n)\). All the instants in between are stuttering instants.

\text{lemma tick_count}_{f\_suc}:\langle \text{assumes } and (f n) < k \land k < (f (Suc n)) \implies shows \text{tick_count r c (f (Suc n))} = \text{tick_count r c (f n)} + \text{card} \{k. k = f (Suc n) \land \text{hamlet ((Rep_run r) k c)}\} \rangle
\langle proof \rangle

\text{corollary tick_count}_{f\_suc}':\langle \text{assumes } and ((f n) < k \land k < (f (Suc n))) \implies shows \text{tick_count r c (f (Suc n))} = \text{tick_count r c (f n)} + (if \text{hamlet ((Rep_run r) (f (Suc n)) c) then 1 else 0}) \rangle
\langle proof \rangle

\text{corollary tick_count}_{f\_suc}\_suc:
assumes \( \text{dilating } f \text{ sub } r \)
shows \( \langle \text{tick_count } r \text{ c } (f (\text{Suc } n)) = (\text{if } \text{hamlet } ((\text{Rep_run } r) (f (\text{Suc } n)) \text{ c}) \text{ then Suc } (\text{tick_count } r \text{ c } (f n)) \text{ else tick_count } r \text{ c } (f n)) \rangle \)

\[ \text{(proof)} \]

**Lemma tick_count_f_suc_sub:**
assumes \( \text{dilating } f \text{ sub } r \)
shows \( \langle \text{tick_count } r \text{ c } (f (\text{Suc } n)) = (\text{if } \text{hamlet } ((\text{Rep_run } sub) (\text{Suc } n) \text{ c}) \text{ then Suc } (\text{tick_count } r \text{ c } (f n)) \text{ else tick_count } r \text{ c } (f n)) \rangle \)

\[ \text{(proof)} \]

The number of ticks does not progress during stuttering instants.

**Lemma tick_count_latest:**
assumes \( \text{dilating } f \text{ sub } r \)
and \( (f \text{ n}_{p} < n \land (\forall k. f \text{ n}_{p} < k \land k \leq n \rightarrow (\exists k_{0}. f k_{0} = k))) \)
shows \( \langle \text{tick_count } r \text{ c } n = \text{tick_count } r \text{ c } (f \text{ n}_{p}) \rangle \)

\[ \text{(proof)} \]

We finally show that the number of ticks on any clock is preserved by dilation.

**Lemma tick_count_sub:**
assumes \( \text{dilating } f \text{ sub } r \)
shows \( \langle \text{tick_count } sub \text{ c } n = \text{tick_count } r \text{ c } (f n) \rangle \)

\[ \text{(proof)} \]

**Corollary run_tick_count_sub:**
assumes \( \text{dilating } f \text{ sub } r \)
shows \( \langle \text{run_tick_count } sub \text{ c } n = \text{run_tick_count } r \text{ c } (f n) \rangle \)

\[ \text{(proof)} \]

The number of ticks occurring strictly before the first instant is null.

**Lemma tick_count_strict_0:**
assumes \( \text{dilating } f \text{ sub } r \)
shows \( \langle \text{tick_count_strict } r \text{ c } (f 0) = 0 \rangle \)

\[ \text{(proof)} \]

The number of ticks strictly before an instant does not progress during stuttering instants.

**Lemma tick_count_strict_stable:**
assumes \( \text{dilating } f \text{ sub } r \)
assumes \( (f n) < k \land k < (f (\text{Suc } n)) \)
shows \( \langle \text{tick_count_strict } r \text{ c } k = \text{tick_count_strict } r \text{ c } (f (\text{Suc } n)) \rangle \)

\[ \text{(proof)} \]

Finally, the number of ticks strictly before an instant is preserved by dilation.

**Lemma tick_count_strict_sub:**
assumes \( \text{dilating } f \text{ sub } r \)
shows \( \langle \text{tick_count_strict } sub \text{ c } n = \text{tick_count_strict } r \text{ c } (f n) \rangle \)

\[ \text{(proof)} \]

The tick count on any clock can only increase.

**Lemma mono_tick_count:**
\( \langle \text{mono } (\lambda k. \text{tick_count } r \text{ c } k) \rangle \)
\[ \text{(proof)} \]
8.1. STUTTERING INVARIANCE

In a dilated run, for any stuttering instant, there is an instant which is the image of an instant in the original run, and which is the latest one before the stuttering instant.

**Lemma greatest_prev_image:**

assumes (dilating f sub r)
shows (\(\exists n_0. f n_0 = n\) \(\implies (\exists n_p. f n_p < n \land (\forall k. f n_p < k \land k \leq n \implies (\exists k_0. f k_0 = k)))\))

(proof)

If a strictly monotonous function on \(\mathbb{nat}\) increases only by one, its argument was increased only by one.

**Lemma strict_mono_suc:**

assumes (strict_mono f)
and (\(f sn = Suc (f n)\))
shows (\(sn = Suc n\))

(proof)

Two successive non stuttering instants of a dilated run are the images of two successive instants of the original run.

**Lemma next_non_stuttering:**

assumes (dilating f sub r)
and (\(f n_p < n \land (\forall k. f n_p < k \land k \leq n \implies (\exists k_0. f k_0 = k))\))
and (\(f sn_0 = Suc n\))
shows (\(sn_0 = Suc n_p\))

(proof)

The order relation between tick counts on clocks is preserved by dilation.

**Lemma dil_tick_count:**

assumes (sub \(\ll\) r)
and (\(\forall n. run_tick_count sub a n \leq run_tick_count sub b n\))
shows (\(run_tick_count r a n \leq run_tick_count r b n\))

(proof)

Time does not progress during stuttering instants.

**Lemma stutter_no_time:**

assumes (dilating f sub r)
and (\(\forall k. f n < k \land k \leq m \implies (\exists k_0. f k_0 = k)\))
and (\(m > f n\))
shows (\(time ((Rep_run r) m c) = time ((Rep_run r) (f n) c)\))

(proof)

**Lemma time_stuttering:**

assumes (dilating f sub r)
and (\(time ((Rep_run r) m c) = \tau\))
and (\(\forall k. f n < k \land k \leq m \implies (\exists k_0. f k_0 = k)\))
and (\(m > f n\))
shows (\(time ((Rep_run r) m c) = \tau\))

(proof)

The first instant at which a given date is reached on a clock is preserved by dilation.

**Lemma first_time_image:**

assumes (dilating f sub r)
shows (\(first_time sub c n t = first_time r c (f n) t\))

(proof)

The first instant of a dilated run is necessarily the image of the first instant of the original run.

**Lemma first_dilated_instant:**
For any instant $n$ of a dilated run, let $n_0$ be the last instant before $n$ that is the image of an original instant. All instants strictly after $n_0$ and before $n$ are stuttering instants.

lemma not_image_stut:
  assumes ⟨dilating f sub r⟩
  and ⟨$n_0 = \text{Max } \{i. f i \leq n\}\rangle
  and ⟨f n_0 < k \land k \leq n⟩
  shows ⟨\(\exists k_0. f k_0 = k\)⟩
⟨proof⟩
For any dilating function $f$, $\text{dil_inverse } f$ is a contracting function.

lemma contracting_inverse:
  assumes ⟨dilating f sub r⟩
  shows ⟨contracting (dil_inverse f) r sub f⟩
⟨proof⟩
The only possible contracting function toward a dense run (a run with no empty instants) is the inverse of the dilating function as defined by $\text{dil_inverse}$.

lemma dense_run_dil_inverse_only:
  assumes ⟨dilating f sub r⟩
  and ⟨contracting g r sub f⟩
  and ⟨dense_run sub⟩
  shows ⟨g = (dil_inverse f)⟩
⟨proof⟩

8.1.5 Main Theorems

theory Stuttering
imports StutteringLemmas
begin
Using the lemmas of the previous section about the invariance by stuttering of various properties of TESL specifications, we can now prove that the atomic formulae that compose TESL specifications are invariant by stuttering.

Sporadic specifications are preserved in a dilated run.

lemma sporadic_sub:
  assumes ⟨sub $\ll r⟩
  and ⟨$r \in [c \sporadic \tau on c']_{TESL}\rangle
  shows ⟨$r \in [c \sporadic \tau on c']_{TESL}\rangle
⟨proof⟩

Implications are preserved in a dilated run.

theorem implies_sub:
  assumes ⟨sub $\ll r⟩
  and ⟨$r \in [c_1 \implies c_2]_{TESL}\rangle
  shows ⟨$r \in [c_1 \implies c_2]_{TESL}\rangle
⟨proof⟩
8.1. STUTTERING INVARIANCE

theorem implies_not_sub:
  assumes (sub ≪ r)
  and (sub ∈ [c₁ implies not c₂]_{TESL})
  shows (r ∈ [c₁ implies not c₂]_{TESL})
⟨proof⟩

Precedence relations are preserved in a dilated run.

theorem weakly_precedes_sub:
  assumes (sub ≪ r)
  and (sub ∈ [c₁ weakly precedes c₂]_{TESL})
  shows (r ∈ [c₁ weakly precedes c₂]_{TESL})
⟨proof⟩

theorem strictly_precedes_sub:
  assumes (sub ≪ r)
  and (sub ∈ [c₁ strictly precedes c₂]_{TESL})
  shows (r ∈ [c₁ strictly precedes c₂]_{TESL})
⟨proof⟩

Time delayed relations are preserved in a dilated run.

theorem time_delayed_sub:
  assumes (sub ≪ r)
  and (sub ∈ [a time-delayed by δτ on ms implies b]_{TESL})
  shows (r ∈ [a time-delayed by δτ on ms implies b]_{TESL})
⟨proof⟩

Time relations are preserved through dilation of a run.

lemma tagrel_sub':
  assumes (sub ≪ r)
  and (sub ∈ [time-relation ⌊c₁, c₂⌋ ∈ R]_{TESL})
  shows R (time ((Rep_run r) n c₁), time ((Rep_run r) n c₂))
⟨proof⟩

corollary tagrel_sub:
  assumes (sub ≪ r)
  and (sub ∈ [time-relation ⌊c₁, c₂⌋ ∈ R]_{TESL})
  shows (r ∈ [time-relation ⌊c₁, c₂⌋ ∈ R]_{TESL})
⟨proof⟩

Time relations are also preserved by contraction

lemma tagrel_sub_inv:
  assumes (sub ≪ r)
  and (r ∈ [time-relation ⌊c₁, c₂⌋ ∈ R]_{TESL})
  shows (sub ∈ [time-relation ⌊c₁, c₂⌋ ∈ R]_{TESL})
⟨proof⟩

Kill relations are preserved in a dilated run.

theorem kill_sub:
  assumes (sub ≪ r)
  and (sub ∈ [c₁ kills c₂]_{TESL})
  shows (r ∈ [c₁ kills c₂]_{TESL})
⟨proof⟩

lemmas atomic_sub_lemmas = sporadic_sub tagrel_sub implies_sub implies_not_sub
  time_delayed_sub weakly_precedes_sub
strictly_precedes_sub kill_sub

We can now prove that all atomic specification formulae are preserved by the dilation of runs.

\[
\text{lemma atomic_sub:}
\begin{align*}
\text{assumes } & (\text{sub} \preceq \text{r}) \\
\text{and } & (\text{sub} \in \llbracket \varphi \rrbracket_{TESL}) \\
\text{shows } & (\text{r} \in \llbracket \varphi \rrbracket_{TESL})
\end{align*}
\]

\[
\text{(proof)}
\]

Finally, any TESL specification is invariant by stuttering.

\[
\text{theorem TESL_stuttering_invariant:}
\begin{align*}
\text{assumes } & (\text{sub} \preceq \text{r}) \\
\text{shows } & (\text{sub} \in \llbracket \llbracket \text{S} \rrbracket \rrbracket_{TESL} \Rightarrow \text{r} \in \llbracket \llbracket \text{S} \rrbracket \rrbracket_{TESL})
\end{align*}
\]

\[
\text{(proof)}
\]

Applying a TESL morphism to a tag simply changes its value.

\[
\text{overloading morphism_tagconst \equiv (morphism :: 'a tag\_const \Rightarrow ('a::linorder \Rightarrow 'a)) \Rightarrow 'a tag\_const}
\]

\[
\text{(begin)}
\begin{align*}
\text{definition morphism_tagconst :}
\quad & (\text{x::'a tag\_const}) \odot (\text{f::('a::linorder \Rightarrow 'a)}) = (\text{r\_st o f})(\text{the\_tag\_const x})
\end{align*}
\]

\[
\text{(end)}
\]

Applying a TESL morphism to an atomic formula only changes the dates.

\[
\text{overloading morphism\_TESL\_atomic \equiv (morphism :: 'a TESL\_atomic \Rightarrow ('a::linorder \Rightarrow 'a) \Rightarrow 'a TESL\_atomic)}
\]

\[
\text{(begin)}
\begin{align*}
\text{definition morphism\_TESL\_atomic :}
\quad & (\text{Ψ::'a TESL\_atomic}) \odot (\text{f::('a::linorder \Rightarrow 'a)}) = \\
\quad & \text{(case Ψ of}
\quad & \text{(C sporadic t on C') \Rightarrow (C sporadic (t \odot f) on C')}
\quad & \text{| (time-relation \llbracket [C, C'] \rrbracket \in R) \Rightarrow (time-relation \llbracket C, C' \rrbracket \in (\lambda(t, t'). R(t \odot f, t' \odot f)))}
\quad & \text{| (C implies C') \Rightarrow (C implies C')}
\quad & \text{| (C time-delayed by t on C' implies C'') \Rightarrow (C time-delayed by t \odot f on C' implies C'')}
\quad & \text{| (C weakly precedes C') \Rightarrow (C weakly precedes C')}
\quad & \text{| (C strictly precedes C') \Rightarrow (C strictly precedes C')}
\quad & \text{| (C kills C') \Rightarrow (C kills C'))}
\quad & \text{end)}
\end{align*}
\]

\[
\text{(end)}
\]

Applying a TESL morphism to a formula amounts to apply it to each atomic formula.

\[
\text{overloading morphism\_TESL\_formula \equiv (morphism :: 'a TESL\_formula \Rightarrow ('a::linorder \Rightarrow 'a) \Rightarrow 'a TESL\_formula)}
\]

\[
\text{(begin)}
\begin{align*}
\text{definition morphism\_TESL\_formula :}
\quad & (\text{Ψ::'a TESL\_formula}) \odot (\text{f::('a::linorder \Rightarrow 'a)}) = \text{map (λx. x \odot f)} \ Ψ
\end{align*}
\]

\[
\text{(end)}
\]
Applying a TESL morphism to a configuration amounts to apply it to the present and future formulae. The past (in the context $\Gamma$) is not changed.

\[
\text{overloading} \quad \text{morphism}_{\text{TESL\_config}} \equiv \langle \text{morphism} :: (\tau :: \text{linordered\_field}) \text{ config} \Rightarrow (\sigma \Rightarrow \tau) \Rightarrow \sigma \text{ config} \rangle
\]

\[
\text{begin} \quad \text{fun} \quad \text{morphism}_{\text{TESL\_config}} \quad \text{where} \quad \langle ((\Gamma, n \vdash \Psi \triangleright \Phi) :: (\tau :: \text{linordered\_field}) \text{ config}) \otimes (f :: (\sigma \Rightarrow \tau)) = (\Gamma, n \vdash (\Psi \otimes f) \triangleright (\Phi \otimes f)) \rangle
\]

A TESL formula is called consistent if it possesses Kripke-models in its denotational interpretation.

\[
\text{definition} \quad \text{consistent} :: (\tau :: \text{linordered\_field}) \text{ TESL\_formula} \Rightarrow \text{bool}
\quad \text{where} \quad \langle \text{consistent} \Psi \equiv [[] \Psi][]_{\text{T\_ESL}} \neq \{\} \rangle
\]

If we can derive a consistent finite context from a TESL formula, the formula is consistent.

\[
\text{theorem} \quad \text{consistency\_finite} :
\quad \text{assumes} \quad \langle \langle [], 0 \vdash \Psi \triangleright [] \rangle \mapsto^* (\Gamma_1, n_1 \vdash [] \triangleright []) \rangle
\quad \text{and} \quad \text{init\_invariant} : \langle \text{consistent\_context} \Gamma_1 \rangle
\quad \text{shows} \quad \langle \text{consistent} \Psi \rangle
\]

\[
\langle \text{proof} \rangle
\]

**Snippets on runs**

A run with no ticks and constant time for all clocks.

\[
\text{definition} \quad \text{const\_nontick\_run} :: (\tau :: \text{linordered\_field}) \text{ run} \Rightarrow \text{nat} \Rightarrow \text{clock} \Rightarrow (\tau) \text{ run}
\quad \text{where} \quad \langle \text{const\_nontick\_run} r k c = \text{Abs\_run}(\lambda n c. (\text{False}, f c)) \rangle
\]

Ensure a clock ticks in a run at a given instant.

\[
\text{definition} \quad \text{set\_tick} :: (\tau :: \text{linordered\_field}) \text{ run} \Rightarrow \text{nat} \Rightarrow \text{clock} \Rightarrow (\tau) \text{ run}
\quad \text{where} \quad \langle \text{set\_tick} r k c = \text{Abs\_run}(\lambda n c. \text{if } k = n \text{ then (True, time(Rep\_run r k c)) else Rep\_run r k c)} \rangle
\]

Ensure a clock does not tick in a run at a given instant.

\[
\text{definition} \quad \text{unset\_tick} :: (\tau :: \text{linordered\_field}) \text{ run} \Rightarrow \text{nat} \Rightarrow \text{clock} \Rightarrow (\tau) \text{ run}
\quad \text{where} \quad \langle \text{unset\_tick} r k c = \text{Abs\_run}(\lambda n c. \text{if } k = n \text{ then (False, time(Rep\_run r k c)) else Rep\_run r k c)} \rangle
\]

Replace all instants after $k$ in a run with the instants from another run. Warning: the result may not be a proper run since time may not be monotonous from instant $k$ to instant $k+1$.

\[
\text{definition} \quad \text{patch} :: (\tau :: \text{linordered\_field}) \text{ run} \Rightarrow \text{nat} \Rightarrow \text{run} \Rightarrow (\tau) \text{ run}
\quad \text{where} \quad \langle \text{patch} r k r' = \text{Abs\_run}(\lambda n c. \text{if } n \leq k \text{ then Rep\_run (r) n c else Rep\_run (r') n c}) \rangle
\]

For some infinite cases, the idea for a proof scheme looks as follows: if we can derive from the initial configuration $[], 0 \vdash \Psi \triangleright []$ a start-point of a lasso $\Gamma_1, n_1 \vdash \Psi_1 \triangleright \Phi_1,$ and if we can traverse the lasso one time $\Gamma_1, n_1 \vdash \Psi_1 \triangleright \Phi_1 \mapsto^+ \Gamma_2, n_2 \vdash \Psi_2 \triangleright \Phi_2$ to isomorphic one, we can always always make a derivation along the lasso. If the entry point of the lasso had traces with prefixes consistent to $\Gamma_1,$ then there exist traces consisting of this prefix and repetitions of the delta-prefix of the lasso which are consistent with $\Psi$ which implies the logical consistency of $\Psi.$
So far the idea. Remains to prove it. Why does one symbolic run along a lasso generalises to arbitrary runs?

```lean
theorem consistency_coinduct :
  assumes start : (([], 0 ⊢ Ψ ⊳ []) ↦∗ (Γ₁, n₁ ⊢ Ψ₁ ⊳ Φ₁))
  and loop : ((Γ₁, n₁ ⊢ Ψ₁ ⊳ Φ₁) ↦++ (Γ₂, n₂ ⊢ Ψ₂ ⊳ Φ₂))
  and init_invariant : (consistent_context Γ₁)
  and post_invariant : (consistent_context Γ₂)
  and retract_condition : ((Γ₂, n₂ ⊢ Ψ₂ ⊳ Φ₂) ⊗ (f ::'τ → 'τ) = (Γ₁, n₁ ⊢ Ψ₁ ⊳ Φ₁))
  shows (consistent (Ψ :: ('τ :: linordered_field)TESL_formula))

(proof)
```

dead
Bibliography
