Abstract

The Circus specification language combines elements for complex data and behavior specifications, using an integration of Z and CSP with a refinement calculus. Its semantics is based on Hoare and He’s unifying theories of programming (UTP).

Isabelle/Circus is a formalization of the UTP and the Circus language in Isabelle/HOL. It contains proof rules and tactic support that allows for proofs of refinement for Circus processes (involving both data and behavioral aspects).

This environment supports a syntax for the semantic definitions which is close to textbook presentations of Circus.

These theories are presented with details in [9]. This document is a technical appendix of this report.

Contents

1 Introduction

2 Background

2.1 Isabelle, HOL and Isabelle/HOL

2.1.1 isar

2.1.2 Higher-order logic (HOL)

2.1.3 Isabelle/HOL

2.2 Advanced Specification Constructs in Isabelle/HOL

2.2.1 Constant definitions.

2.2.2 Type definitions.

2.2.3 Extensible records.

2.3 Circus and its UTP Foundation

2.3.1 Predicates and Relations.

2.3.2 Designs and processes.
3 Isabelle/Circus

3.1 Alphabets and Variables .................................... 11
  3.1.1 Updating and accessing global variables. ............ 11
  3.1.2 Updating and accessing local variables. .......... 12
3.2 Synchronization infrastructure: Name sets and channels. . . . 13
  3.2.1 Name sets. ........................................ 13
  3.2.2 Channels. ........................................ 13
3.3 Actions and Processes ....................................... 14
  3.3.1 Basic actions. ..................................... 15
  3.3.2 The universal assignment action. .................... 15
  3.3.3 Communications. ................................... 16
  3.3.4 Hiding. ........................................ 17
  3.3.5 Recursion. ........................................ 18
  3.3.6 Circus Processes. .................................. 18

4 Using Isabelle/Circus ........................................... 18
  4.1 Writing specifications .................................... 19
  4.2 Relational and Functional Refinement in Circus .......... 20
  4.3 Refinement Proofs ..................................... 20

5 Conclusions .................................................... 22

6 Acknowledgement .................................................. 23

7 UTP variables .................................................... 24

8 Predicates and relations .......................................... 24
  8.1 Definitions ............................................. 24
  8.2 Proofs .................................................. 26
    8.2.1 Setup of automated tools ............................ 26
    8.2.2 Misc lemmas ..................................... 28

9 Designs .......................................................... 34
  9.1 Definitions ............................................. 34
  9.2 Proofs .................................................. 35

10 Reactive processes .............................................. 37
  10.1 Preliminaries .......................................... 38
  10.2 Definitions ........................................... 40
  10.3 Proofs .................................................. 41

11 CSP processes ................................................... 44
  11.1 Definitions ............................................. 44
  11.2 Proofs .................................................. 45
  11.3 CSP processes and reactive designs .................... 49
## 12 Circus actions

12.1 Definitions .................................................. 49
12.2 Proofs .......................................................... 50

## 13 Circus variables

## 14 Denotational semantics of Circus actions

14.1 Skip ............................................................. 54
14.2 Stop ............................................................. 54
14.3 Chaos ............................................................ 55
14.4 State update actions .......................................... 55
14.5 Sequential composition ...................................... 56
14.6 Internal choice ................................................ 57
14.7 External choice ............................................... 57
14.8 Reactive design assignment .................................. 58
14.9 Local state external choice .................................. 58
14.10 Schema expression .......................................... 59
14.11 Parallel composition ....................................... 59
14.12 Local parallel block ........................................ 61
14.13 Assignment .................................................... 61
14.14 Variable scope ............................................... 62
14.15 Guarded action ............................................... 63
14.16 Prefixed action ............................................... 64
14.17 Hiding .......................................................... 66
14.18 Recursion ....................................................... 67

## 15 Circus syntax

## 16 Refinement and Simulation

16.1 Definitions .................................................. 68
16.2 Proofs .......................................................... 69

## 17 Concrete example

17.1 Process definitions .......................................... 72
17.2 Simulation proofs ............................................ 72
1 Introduction

Many systems involve both complex (sometimes infinite) data structures and interactions between concurrent processes. Refinement of abstract specifications of such systems into more concrete ones, requires an appropriate formalisation of refinement and appropriate proof support.

There are several combinations of process-oriented modeling languages with data-oriented specification formalisms such as Z or B or CASL; examples are discussed in [3, 10, 17, 14]. In this paper, we consider Circus [18], a language for refinement, that supports modeling of high-level specifications, designs, and concrete programs. It is representative of a class of languages that provide facilities to model data types, using a predicate-based notation, and patterns of interactions, without imposing architectural restrictions. It is this feature that makes it suitable for reasoning about both abstract and low-level designs.

We present a “shallow embedding” of the Circus semantics enabling state variables and channels in Circus to have arbitrary HOL types. Therefore, the entire handling of typing can be completely shifted to the (efficiently implemented) Isabelle type-checker and is therefore implicit in proofs. This drastically simplifies definitions and proofs, and makes the reuse of standardized proof procedures possible. Compared to implementations based on a “deep embedding” such as [19] this significantly improves the usability of the resulting proof environment.

Our representation brings particular technical challenges and contributions concerning some important notions about variables. The main challenge was to represent alphabets and bindings in a typed way that preserves the semantics and improves deduction. We provide a representation of bindings without an explicit management of alphabets. However, the representation of some core concepts in the unifying theories of programming (UTP) and Circus constructs (variable scopes and renaming) became challenging. Thus, we propose a (stack-based) solution that allows the coding of state variables scoping with no need for renaming. This solution is even a contribution to the UTP theory that does not allow nested variable scoping. Some challenging and tricky definitions (e.g. channels and name sets) are explained in this paper.

This paper is organized as follows. The next section gives an introduction to the basics of our work: Isabelle/HOL, UTP and Circus with a short example of a Circus process. In Section 3, we present our embedding of the basic concepts of Circus (alphabet, variables ...). We introduce the representation of some Circus actions and process, with an overview of the Isabelle/Circus syntax. In Section 4, we show on an example, how Isabelle/Circus can be used to write specifications. We give some details on what is happening “behind the scenes” when the system parses each part of the specification. In the last part of this section, we show how to write proofs based on spec-
ifications, and give a refinement proof example. A more developed version of this paper can be found in [9].

2 Background

2.1 Isabelle, HOL and Isabelle/HOL

2.1.1 isar

[12] is a generic theorem prover implemented in SML. It is based on the so-called “LCF-style architecture”, which makes it possible to extend a small trusted logical kernel by user-programmed procedures in a logically safe way. New object logics can be introduced to Isabelle by specifying their syntax and semantics, by deriving its inference rules from there and program specific tactic support for the object logic. Isabelle is based on a typed \( \lambda \)-calculus including a Haskell-style type-system with type-classes (e.g. in \( \alpha :: \text{order} \), the type-variable ranges over all types that posses a partial ordering.)

2.1.2 Higher-order logic (HOL)

[7, 1] is a classical logic based on a simple type system. It provides the usual logical connectives like \( \land \), \( \to \), \( \neg \) as well as the object-logical quantifiers \( \forall x \cdot P x \) and \( \exists x \cdot P x \); in contrast to first-order logic, quantifiers may range over arbitrary types, including total functions \( f :: \alpha \Rightarrow \beta \). HOL is centered around extensional equality \( = :: \alpha \Rightarrow \alpha \Rightarrow \text{bool} \). HOL is more expressive than first-order logic, since, e.g., induction schemes can be expressed inside the logic. Being based on some polymorphically typed \( \lambda \)-calculus, HOL can be viewed as a combination of a programming language like SML or Haskell and a specification language providing powerful logical quantifiers ranging over elementary and function types.

2.1.3 Isabelle/HOL

is an instance of Isabelle with higher-order logic. It provides a rich collection of library theories like sets, pairs, relations, partial functions lists, multi-sets, orderings, and various arithmetic theories which only contain rules derived from conservative, i.e. logically safe definitions. Setups for the automated proof procedures like simp, auto, and arithmetic types such as \( \text{int} \) are provided.

2.2 Advanced Specification Constructs in Isabelle/HOL

2.2.1 Constant definitions.

In its easiest form, constant definitions are definitional logical axioms of the form \( c \equiv E \) where \( c \) is a fresh constant symbol not occurring in \( E \) which is
closed (both wrt. variables and type variables). For example:

\[
\text{definition upd::}(\alpha \Rightarrow \beta) \Rightarrow \alpha \Rightarrow (\alpha \Rightarrow \beta) \quad \text{("\_\_ := \_\_" )}
\]

where "upd f x v \equiv \lambda z. \text{if } x = z \text{ then } v \text{ else } f z"

The pragma ("\_\_ := \_\_") for the Isabelle syntax engine introduces the notation \( f(x:=y) \) for \( \text{upd f x y} \). Moreover, some elaborate preprocessing allows for recursive definitions, provided that a termination ordering can be established. Such recursive definitions are thus internally reduced to definitional axioms.

### 2.2.2 Type definitions.

Types can be introduced in Isabelle/HOL in different ways. The most general way to safely introduce new types is using the \texttt{typedef} construct. This allows introducing a type as a non-empty subset of an existing type. More precisely, the new type is specified to be isomorphic to this non-empty subset. For instance:

\[
\text{typedef mytype = } \{ x :: \text{nat. } x < 10 \}
\]

This definition requires that the set is non-empty: \( \exists x. x \in \{ x :: \text{nat. } x < 10 \} \), which is easy to prove in this case:

\[
\text{by (rule_tac x = 1 in exI, simp)}
\]

where \texttt{rule_tac} is a tactic that applies an introduction rule, and \texttt{exI} corresponds to the introduction of the existential quantification.

Similarly, the \texttt{datatype} command allows the definition of inductive datatypes. It introduces a datatype using a list of \textit{constructors}. For instance, a logical compiler is invoked for the following introduction of the type \texttt{option}:

\[
\text{datatype } \alpha \text{ option } = \text{None | Some } \alpha
\]

which generates the underlying type definition and derives distinctness rules and induction principles. Besides the \textit{constructors} \texttt{None} and \texttt{Some}, the following match-operator and his rules are also generated:

\[
\text{case } x \text{ of } \text{None } \Rightarrow \ldots \text{ | Some } a \Rightarrow \ldots
\]

### 2.2.3 Extensible records.

Isabelle/HOL's support for \textit{extensible records} is of particular importance for our work. Record types are denoted, for example, by:

\[
\text{record } T = a :: T_1 \\
\quad b :: T_2
\]

which implicitly introduces the record constructor \((a:=e_1, b:=e_2)\) and the update of record \( r \) in field \( a \), written as \( r(a:=x) \). Extensible records are represented internally by cartesian products with an implicit free component.
δ, i.e. in this case by a triple of the type \( T_1 \times T_2 \times \delta \). The third component can be referenced by a special selector more available on extensible records. Thus, the record \( T \) can be extended later on using the syntax:

```plaintext
record ET = T + c::T3
```

The key point is that theorems can be established, once and for all, on \( T \) types, even if future parts of the record are not yet known, and reused in the later definition and proofs over \( ET \)-values. Using this feature, we can model the effect of defining the alphabet of UTP processes incrementally while maintaining the full expressivity of HOL wrt. the types of \( T_1, T_2 \) and \( T_3 \).

### 2.3 Circus and its UTP Foundation

Circus is a formal specification language [18] which integrates the notions of states and complex data types (in a Z-like style) and communicating parallel processes inspired from CSP. From Z, the language inherits the notion of a schema used to model sets of (ground) states as well as syntactic machinery to describe pre-states and post-states; from CSP, the language inherits the concept of communication events and typed communication channels, the concepts of deterministic and non-deterministic choice (reflected by the process combinators \( P \Box P' \) and \( P \cap P' \)), the concept of concealment (hiding) \( P \backslash A \) of events in \( A \) occurring in in the evolution of process \( P \). Due to the presence of state variables, the Circus synchronous communication operator syntax is slightly different frome CSP: \( P \parallel n \mid c \mid n' \parallel P' \) means that \( P \) and \( P' \) communicate via the channels mentioned in \( c \); moreover, \( P \) may modify the variables mentioned in \( n \) only, and \( P' \) in \( n' \) only, \( n \) and \( n' \) are disjoint name sets.

Moreover, the language comes with a formal notion of refinement based on a denotational semantics. It follows the failure/divergence semantics [15], (but coined in terms of the UTP [13]) providing a notion of execution trace \( tr \), refusals \( ref \), and divergences. It is expressed in terms of the UTP [11] which makes it amenable to other refinement-notions in UTP. Figure 1 presents a simple Circus specification, FIG, the fresh identifiers generator.

#### 2.3.1 Predicates and Relations.

The UTP is a semantic framework based on an alphabetized relational calculus. An alphabetized predicate is a pair (alphabet, predicate) where the free variables appearing in the predicate are all in the alphabet, e.g. \( \{x, y\}, x > y \). As such, it is very similar to the concept of a schema in Z. In the base theory Isabelle/UTP of this work, we represent alphabetized predicates by sets of (extensible) records, e.g. \( \{A. x A > y A\} \).

An alphabetized relation is an alphabetized predicate where the alphabet is composed of input (undecorated) and output (dashed) variables. In this
channel \textit{req}
channel \textit{ret, out : ID}

process \textit{FIG} \equiv \text{begin}
\text{state} \ S \ =\ [\ idS : \mathbb{P} \ ID ]
\text{Init} \ \equiv \ idS := \emptyset
\underbrace{\Delta S}_{\text{Out}}\ 
\underbrace{v! : \text{ID}}_{\text{!}}\ 
\underbrace{v! \notin idS}_{\text{v!} \notin \text{idS}}\ 
\underbrace{idS' = idS \cup \{v!\}}_{\text{idS' = idS} \cup \{v\}}
\begin{array}{cc}
\hline
\text{Remove} & \Delta S \ \\
& x? : \text{ID} \\
& idS' = idS \setminus \{x\} \\
\end{array}

• Init ; \textbf{var} \ v : \text{ID} •
\begin{array}{c}
\mu X \bullet (\text{req} \rightarrow \text{Out}; \text{out!}v \rightarrow \text{Skip} \ \\
\Box \text{ref?}x \rightarrow \text{Remove}); \ X)
\end{array}
\text{end}

Figure 1: The Fresh Identifiers Generator in (Textbook) \textit{Circus}

case the predicate describes a relation between input and output variables, for example \(\{x, x', y, y'\}, x' = x + y\) which is a notation for: \(\{(A, A') . x A' = x A + y A\}\), which is a set of pairs, thus a relation.

Standard predicate calculus operators are used to combine alphabetized predicates. The definition of these operators is very similar to the standard one, with some additional constraints on the alphabets.

2.3.2 Designs and processes.

In UTP, in order to explicitly record the termination of a program, a subset of alphabetized relations is introduced. These relations are called \textit{designs} and their alphabet should contain the special boolean observational variable \textit{ok}. It is used to record the start and termination of a program. A UTP design is defined as follows in Isabelle:

\[(P \vdash Q) \equiv \lambda (A, A'). (ok A \land P (A, A')) \rightarrow (ok A' \land Q (A, A'))\]

Following the way of UTP to describe reactive processes, more observational variables are needed to record the interaction with the environment. Three observational variables are defined for this subset of relations: \textit{wait}, \textit{tr} and \textit{ref}. The boolean variable \textit{wait} records if the process is waiting for an interaction or has terminated. \textit{tr} records the list (trace) of interactions the process has performed so far. The variable \textit{ref} contains the set
of interactions (events) the process may refuse to perform. These observational variables define the basic alphabet of all reactive processes called “alpha_rp”.

Some healthiness conditions are defined over \texttt{wait}, \texttt{tr} and \texttt{ref} to ensure that a reactive process satisfies some properties [6] (see Table 2 in [9]).

A CSP process is a UTP reactive process that satisfies two additional healthiness conditions (all well-formedness conditions can be found in [9]). A process that satisfies these conditions is said to be CSP healthy.

3 Isabelle/Circus

The Isabelle/Circus environment allows a syntax of processes which is close to the textbook presentations of Circus (see Fig. 2). Similar to other specification constructs in Isabelle/HOL, this syntax is “parsed away”, \textit{i.e.} compiled into an internal representation of the denotational semantics of Circus, which is a formalization in form of a shallow embedding of the (essentially untyped) paper-and-pencil definitions by Oliveira et al. [13], based on UTP. Circus actions are defined as CSP healthy reactive processes.

In the UTP representation of reactive processes we have given in a previous paper [8], the process type is generic. It contains two type parameters that represent the channel type and the alphabet of the process. These parameters are very general, and they are instantiated for each specific process. This could be problematic when representing the Circus semantics, since some definitions rely directly on variables and channels (e.g. assignment and communication). In this section we present our solution to deal
with this kind of problems, and our representation of the Circus actions and processes.

We now describe the foundation as well as the semantic definition of some process operators of Circus. A distinguishing feature of Circus processes are explicit state variables which do not exist in other process algebras like, e.g., CSP. These can be:

- **global** state variables, *i.e.* they are declared via alphabetized predicates in the state section, or Z-like \( \Delta \) operations on global states that generate alphabetized relations, or

- **local** state variables, *i.e.* they are result of the variable declaration statement \( \text{var var @ Action} \). The scope of local variables is restricted to \( \text{Action} \).

On both kind of state variables, logical constraints may be expressed.

### 3.1 Alphabets and Variables

In order to define the set of variables of a specification, the Circus semantics considers the alphabet of its components, be it on the level of alphabetized predicates, alphabetized relations or actions. We recall that these items are represented by sets of records or sets of pairs of records. The alphabet of a process is defined by extending the basic reactive process alphabet (cf. Section 2.3.2) by its variable names and types. For the example FIG, where the global state variable \( \text{idS} \) is defined, this is reflected in Isabelle/Circus by the extension of the process alphabet by this variable, i.e. by the extension of the Isabelle/HOL record:

\[
\begin{align*}
\text{record } \alpha \alpha & = \alpha \alpha_{\text{rp}} + \text{idS :: ID set}
\end{align*}
\]

This introduces the record type \( \alpha \alpha \) that contains the observational variables of a reactive process, plus the variable \( \text{idS} \). Note that our Circus semantic representation allows “built-in” bindings of alphabets in a typed way. Moreover, there is no restriction on the associated HOL type. However, the inconvenience of this representation is that variables cannot be introduced “on the fly”; they must be known statically i.e. at type inference time. Another consequence is that a "syntactic" operation such as variable renaming has to be expressed as a "semantic" operation that maps one record type into another.

#### 3.1.1 Updating and accessing global variables.

Since the alphabets are represented by HOL records, i.e. a kind binding "name \( \mapsto \) value", we need a certain infrastructure to access data in them and to update them. The Isabelle representation as records gives us already
two functions (for each record) “select” and “update”. The “select” function returns the value of a given variable name, and the “update” functions updates the value of this variable. Since we may have different HOL types for different variables, a unique definition for select and update cannot be provided. There is an instance of these functions for each variable in the record. The name of the variable is used to distinguish the different instances: for the select function the name is used directly and for the update function the name is used as a prefix e.g. for a variable named “x” the names of the select and update functions are respectively \( x \) of type \( \alpha \) and \( x_{\text{update}} \). Since a variable is characterized essentially by these functions, we define a general type (synonym) called \( \text{var} \) which represents a variable as a pair of its select and update function (in the underlying state \( \sigma \)).

\[
\text{types} \ (\beta, \sigma) \ \text{var} = "(\sigma \Rightarrow \beta) \ast ((\beta \Rightarrow \beta) \Rightarrow \sigma \Rightarrow \sigma)"
\]

For a given alphabet (record) of type \( \sigma, (\beta, \text{the type } \sigma)\text{var} \) represents the type of the variables whose value type is \( \beta \). One can then extract the select and update functions from a given variable with the following functions:

\[
\text{definition select :: } (\beta, \sigma) \ \text{var} \Rightarrow \sigma \Rightarrow \beta
\]

\[
\text{where select } f \equiv (\text{fst } f)
\]

\[
\text{definition update :: } (\beta, \sigma) \ \text{var} \Rightarrow \beta \Rightarrow \sigma \Rightarrow \sigma
\]

\[
\text{where update } f \ v \equiv (\text{snd } f) \ (\lambda _ . \ v)
\]

Finally, we introduce a function called \( \text{VAR} \) to implement a syntactic translation of a variable name to an entity of type \( \text{var} \).

\[
\text{syntax } "_\text{VAR}" :: "\text{id }\Rightarrow(\beta, \sigma) \ \text{var}" ("\text{VAR }_")
\]

\[
\text{translations } \text{VAR } x => (x, _\text{update_ name } x)
\]

Note that in this syntactic translation rule, \( _\text{update_ name } x \) stands for the concatenation of the string \( _\text{update_} \) with the content of the variable \( x \); the resulting \( _\text{update_ } x \) in this example is mapped to the field-update function of the extensible record \( x_{\text{update}} \) by a default mechanism. On this basis, the assignment notation can be written as usual:

\[
\text{syntax } "_\text{assign}" :: "\text{id }\Rightarrow(\sigma \Rightarrow \beta) \Rightarrow(\alpha, \sigma) \ \text{action}" ("_\text{'}:=\text{'} _")
\]

\[
\text{translations } "x \text{'}:=\text{'} E" \Rightarrow "\text{CONST ASSIGN (VAR } x \text{) } E"
\]

and mapped to the semantics of the program variable \( (x, x_{\text{update}}) \) together with the universal ASSIGN operator defined later on, in Section 3.3.2.

### 3.1.2 Updating and accessing local variables.

In Circus, local program variables can be introduced on the fly, and their scopes are explicitly defined, as can be seen in the FIG example. In textbook
Circus, nested scopes are handled by variable renaming which is not possible in our representation due to the implicit representation of variable names. We represent local program variables by global variables, using the \texttt{var} type defined above, where selection and update involve an explicit stack discipline. Each variable is mapped to a list of values, and not to one value only (as for state variables). Entering the scope of a variable is just adding a new value as the head of the corresponding values list. Leaving a variable scope is just removing the head of the values list. The select and update functions correspond to selecting and updating the head of the list. This ensures dynamic scoping, as it is stated by the Circus semantics.

Note that this encoding scheme requires to make local variables lexically distinct from global variables; local variable instances are just distinguished from the global ones by the stack discipline.

3.2 Synchronization infrastructure: Name sets and channels.

3.2.1 Name sets.

An important notion, used in the definition of parallel Circus actions, is name sets as seen in Section 2.3. A name set is a set of variable names, which is a subset of the alphabet. This notion cannot be directly expressed in our representation since variable names are not explicitly represented. Thus its definition relies on the characterization of the variables in our representation. As for variables, name sets are defined by their functional characterization. They are used in the definition of the binding merge function $M\mathit{St}$ below:

$$\forall v \in (v \in ns_1 \Rightarrow v' = (1, v)) \land (v \in ns_2 \Rightarrow v' = (2, v)) \land (v \notin ns_1 \cup ns_2 \Rightarrow v' = v).$$

The disjoint name sets $ns_1$ and $ns_2$ are used to determine which variable values (extracted from local bindings of the parallel components) are used to update the global binding of the process. A name set can be functionally defined as a binding update function, that copies values from a local binding to the global one. For example, a name set $NS$ that only contains the variable $x$ can be defined as follows in Isabelle/Circus:

\begin{verbatim}
definition NS lb gb = x_update (x lb) gb
\end{verbatim}

where $lb$ and $gb$ stands for local and global bindings, $x$ and $x\_update$ are the select and update functions of variable $x$. Then the merge function can be defined by composing the application of the name sets to the global binding.

3.2.2 Channels.

Reactive processes interact with the environment via synchronizations and communications. A synchronization is an interaction via a channel without any exchange of data. A communication is a synchronization with data exchange. In order to reason about communications in the same way, a
datatype *channels* is defined using the channels names as constructors. For instance, in:

```
datatype channels = chan1 | chan2 nat | chan3 bool
```
we declare three channels: *chan1* that synchronizes without data, *chan2* that communicates natural values and *chan3* that exchanges boolean values.

This definition makes it possible to reason globally about communications since they have the same type. However, the channels may not have the same type: in the example above, the types of *chan1*, *chan2* and *chan3* are respectively *channels*, *nat ⇒ channels* and *bool ⇒ channels*. In the definition of some *Circus* operators, we need to compare two channels, and one can’t compare for example *chan1* with *chan2* since they don’t have the same type. A solution would be to compare *chan1* with (*chan2 v*). The types are equivalent in this case, but the problem remains because comparing (*chan2 0*) to (*chan2 1*) will state inequality just because the communicated values are not equal. We could define an inductive function over the datatype *channels* to compare channels, but this is only possible when all the channels are known *a priori*.

Thus, we add some constraint to the generic channels type: we require the *channels* type to implement a function *chan_eq* that tests the equality of two channels. Fortunately, Isabelle/HOL provides a construct for this kind of restriction: the type classes (sorts) mentioned in Section 2.1. We define a type class (interface) *chan_eq* that contains a signature of the *chan_eq* function.

```
class chan_eq = 
  fixes chan_eq :: "α ⇒ α ⇒ bool"
begin end
```
Concrete channels type must implement the interface (class) “*chan_eq*” that can be easily defined for this concrete type. Moreover, one can use this class to add some definition that depends on the channel equivalence function. For example, a trace equivalence function can be defined as follows:

```
fun tr_eq where
  tr_eq [] [] = True | tr_eq xs [] = False | tr_eq [] ys = False
  | tr_eq (x#xs) (y#ys) = if chan_eq x y then tr_eq xs ys else False
```
It is applicable to traces of elements whose type belongs to the sort *chan_eq*.

### 3.3 Actions and Processes

The *Circus* actions type is defined as the set of all the CSP healthy reactive processes. The type *(α, σ)relation_rp* is the reactive process type where α is of *channels* type and σ is a record extensions of *action_rp*, *i.e.* the global state variables. On this basis, we can encode the concept of a process
for a family of possible state instances. We introduce below the vital type 
action:

typedef(Action)
(α::chan_eq, σ) action = {p::(α, σ)relation_rp. is_CSP_process p}
proof - {...}
qed

As mentioned before, a type-definition introduces a new type by stating a set. In our case it is the set of reactive processes that satisfy the healthiness-conditions for CSP-processes, isomorphic to the new type.

Technically, this construct introduces two constants definitions Abs_Action and Rep_Action respectively of type (α, σ) relation_rp ⇒ (α, σ) action and (α, σ) action ⇒ (α, σ) relation_rp as well as the usual two axioms expressing the bijection Abs_Action(Rep_Action(X))=X and is_CSP_process p ⟹ Rep_Action(Abs_Action(p))=p where is_CSP_process captures the healthiness conditions.

Every Circus action is an abstraction of an alphabetized predicate. In [9], we introduce the definitions of all the actions and operators using their denotational semantics. The environment contains, for each action, the proof that this predicate is CSP healthy.

In this section, we present some of the important definitions, namely: basic actions, assignments, communications, hiding, and recursion.

3.3.1 Basic actions.

Stop is defined as a reactive design, with a precondition true and a post-condition stating that the system deadlocks and the traces are not evolving.

definition Stop ≡ Abs_Action (R (true ⊢ λ(A, A'). tr A' = tr A ∧ wait A'))

Skip is defined as a reactive design, with a precondition true and a post-condition stating that the system terminates and all the state variables are not changed. We represent this fact by stating that the more field (seen in Section 2.2) is not changed, since this field is mapped to all the state variables. Note that using the more-field is a tribute to our encoding of alphabets by extensible records and stands for all future extensions of the alphabet (e.g. state variables).

definition Skip ≡ Abs_Action (R (true ⊢ λ (A, A'). tr A’ = tr A ∧ ¬wait A’ ∧ more A = more A'))

3.3.2 The universal assignment action.

In Section 3.1.1, we described how global and local variables are represented by access- and updates functions introduced by fields in extensible records.
In these terms, the "lifting" to the assignment action in *Circus* processes is straightforward:

**definition**

\[
\text{ASSIGN}::\langle(\beta, \sigma) \triangleright (\sigma \Rightarrow \beta) \Rightarrow (\alpha::\text{ev_eq}, \sigma) \text{ action}\rangle
\]

where

\[
\text{ASSIGN } x e \equiv \text{Abs_Action} (R (\text{true } \vdash Y))
\]

where

\[
Y = \lambda (A, A'). \text{tr } A' = \text{tr } A \land \neg \text{wait } A' \land
\text{more } A' = (\text{assign } x (e (\text{more } A))) (\text{more } A)
\]

where **assign** is the projection into the update operation of a semantic variable described in section 3.1.1.

### 3.3.3 Communications.

The definition of prefixed actions is based on the definition of a special relation \(do_I\). In the *Circus* denotational semantics [13], various forms of prefixing were defined. In our theory, we define one general form, and the other forms are defined as special cases.

**definition** \(do_I\) \(c \times P \equiv X \triangleleft \text{wait } o \text{ fst } \triangleright Y\)

where

\[
X = (\lambda (A, A'). \text{tr } A = \text{tr } A' \land ((c ' P) \cap \text{ref } A') = \{}\})
\]

and

\[
Y = (\lambda (A, A'). \text{hd } ((\text{tr } A') - (\text{tr } A)) \in (c ' P) \land
(c (\text{select } x (\text{more } A))) = (\text{last } (\text{tr } A'))\)
\]

where \(c\) is a channel constructor, \(x\) is a variable (of \text{var} type) and \(P\) is a predicate. The \(do_I\) relation gives the semantics of an interaction: if the system is ready to interact, the trace is unchanged and the waiting channel is not refused. After performing the interaction, the new event in the trace corresponds to this interaction.

The semantics of the whole action is given by the following definition:

**definition** \(Prefix\) \(c \times P S \equiv \text{Abs_Action}(R (\text{true } \vdash Y)) ; S\)

where

\[
Y = \text{do}_I \ c \times P \land (\lambda (A, A'). \text{more } A' = \text{more } A)
\]

where \(c\) is a channel constructor, \(x\) is a variable (of \text{var} type), \(P\) is a predicate and \(S\) is an action. This definition states that the prefixed action semantics is given by the interaction semantics (\(do_I\)) sequentially composed with the semantics of the continuation (action \(S\)).

Different types of communication are considered:

- **Inputs**: the communication is done over a variable.
- **Constrained Inputs**: the input variable value is constrained with a predicate.
• Outputs: the communications exchanges only one value.

• Synchronizations: only the channel name is considered (no data).

The semantics of these different forms of communications is based on the general definition above.

**definition** read c x P ≡ Prefix c x true P  
**definition** write1 c a P ≡ Prefix c (λs. a s, (λ x. λy. y)) true P  
**definition** write0 c P ≡ Prefix (λ_.c) (λ_. _, (λ x. λy. y)) true P

where **read**, **write1** and **write0** respectively correspond to inputs, outputs and synchronization. Constrained inputs correspond to the general definition.

We configure the Isabelle syntax-engine such that it parses the usual communication primitives and gives the corresponding semantics:

**translations**

\[ c ? p \rightarrow P \rightarrow \text{CONST read c (VAR p) P} \]
\[ c ? p : b \rightarrow P \rightarrow \text{CONST Prefix c (VAR p) b P} \]
\[ c ! p \rightarrow P \rightarrow \text{CONST write1 c p P} \]
\[ a \rightarrow P \rightarrow \text{CONST write0 (TYPE(_)) a P} \]

### 3.3.4 Hiding.

The hiding operator is interesting because it depends on a channel set. This operator \( P \setminus cs \) is used to encapsulate the events that are in the channel set \( cs \). These events become no longer visible from the environment. The semantics of the hiding operator is given by the following reactive process:

**definition**  
Hide ::"[(α, σ) action , α set] ⇒ (α, σ) action" (infixl "\")  
where
\[ P \setminus cs \equiv \text{Abs_Action}( R(λ\ (A, A'). \exists s. (\text{Rep_Action P})(A, A'(\text{tr :=s, ref := (ref A') ∪ cs)}) \land (\text{tr A'} - \text{tr A}) = (\text{tr_filter (s - tr A) cs})); \text{Skip} \]

The definition uses a filtering function \( \text{tr_filter} \) that removes from a trace the events whose channels belong to a given set. The definition of this function is based on the function \( \text{chan_eq} \) we defined in the class \( \text{chan_eq} \). This explains the presence of the constraint on the type of the action channels in the hiding definition, and in the definition of the filtering function below:

**fun**  
\[ \text{tr_filter}:"a::chan_eq list ⇒a set ⇒a list" \]
\[ \text{tr_filter} [] cs = [] \]
\[ | \text{tr_filter} (x#xs) cs = (if (¬ \text{chan-in_set x cs}) \]
\[ \text{then} \ (x#(\text{tr_filter xs cs})) \]
\[ \text{else} \ (\text{tr_filter xs cs}) \]
where the `chan-in_set` function checks if a given channel belongs to a channel set using `chan_eq` as equality function.

### 3.3.5 Recursion.

To represent the recursion operator “μ” over actions, we use the universal least fix-point operator “lfp” defined in the HOL library for lattices and we follow again [13]. The use of least fix-points in [13] is the most substantial deviation from the standard CSP denotational semantics, which requires Scott-domains and complete partial orderings. The operator `lfp` is inherited from the “Complete Lattice class” under some conditions, and all theorems defined over this operator can be reused. In order to reuse this operator, we have to show that the least-fixpoint over functionals that enrich pairs of failure - and divergence trace sets monotonely, produces an action that satisfies the CSP healthiness conditions. This consistency proof for the recursion operator is the largest contained in the Isabelle/Circus library.

Therefore, we must prove that the Circus actions type defines a complete lattice. This leads to prove that the actions type belongs to the HOL “Complete Lattice class”. Since type classes in HOL are hierarchic, the proof is in three steps: first, a proof that the Circus actions type forms a lattice by instantiating the HOL “Lattice class”; second, a proof that actions type instantiates a subclass of lattices called “Bounded Lattice class”; third, proof of the instantiation from the “Complete Lattice class”. More on these proofs can be found in [9].

### 3.3.6 Circus Processes.

A Circus process is defined in our environment as a local theory by introducing qualified names for all its components. This is very similar to the notion of namespaces popular in programming languages. Defining a Circus process locally makes it possible to encapsulate definitions of alphabet, channels, schema expressions and actions in the same namespace. It is important for the foundation of Isabelle/Circus to avoid the ambiguity between local process entities definitions (e.g. `FIG.Out` and `DFIG.Out` in the example of Section 4).

### 4 Using Isabelle/Circus

We describe the front-end interface of Isabelle/Circus. In order to support a maximum of common Circus syntactic look-and-feel, we have programmed at the SML level of Isabelle a compiler that parses and (partially) pretty prints Circus process given in the syntax presented in Figure 2.
4.1 Writing specifications

A specification is a sequence of paragraphs. Each paragraph may be a declaration of alphabet, state, channels, name sets, channel sets, schema expressions or actions. The main action is introduced by the keyword where. Below, we illustrate how to use the environment to write a Circus specification using the FIG process example presented in Figure 1.

\[
\text{circusprocess } \text{FIG} = \\
\text{alphabet } = [v::\text{nat}, x::\text{nat}] \\
\text{state } = [\text{idS::nat set}] \\
\text{channel } = [\text{req, ret nat, out nat}] \\
\text{schema Init } = \text{idS }:= \{\} \\
\text{schema Out } = \exists a. v' = a \land v' \not\in \text{idS }\land \text{idS'} = \text{idS }\cup \{v'\} \\
\text{schema Remove } = x \not\in \text{idS }\land \text{idS'} = \text{idS }- \{x\} \\
\text{where var } v \cdot \text{Schema Init;} (\mu X \rightarrow \text{Schema Out;} \text{ out!v } \rightarrow \text{Skip}) \\
\text{ } \Box (\text{ret?x }\rightarrow \text{Schema Remove}); X
\]

Each line of the specification is translated into the corresponding semantic operator given in Section 3.3. We describe below the result of executing each command of FIG:

- the compiler introduces a scope of local components whose names are qualified by the process name (FIG in the example).

- **alphabet** generates a list of record fields to represent the binding. These fields map names to value lists.

- **state** generates a list of record fields that corresponds to the state variables. The names are mapped to single values. This command, together with **alphabet** command, generates a record that represents all the variables (for the FIG example the command generates the record FIG_alphabet, that contains the fields v and x of type nat list and the field idS of type nat set).

- **channel** introduces a datatype of typed communication channels (for the FIG example the command generates the datatype FIG_channels that contains the constructors req without communicated value and ret and out that communicate natural values).

- **schema** allows the definition of schema expressions represented as an alphabetized relation over the process variables (in the example the schema expressions FIG.Init, FIG.Out and FIG.Remove are generated).

- **action** introduces definitions for Circus actions in the process. These definitions are based on the denotational semantics of Circus actions.
The type parameters of the action type are instantiated with the locally defined channels and alphabet types.

- where introduces the main action as in action command (in the example the main action is FIG.FIG of type (FIG_channels, FIG_alphabet)action).

4.2 Relational and Functional Refinement in Circus

The main goal of Isabelle/Circus is to provide a proof environment for Circus processes. The “shallow-embedding” of Circus and UTP in Isabelle/HOL offers the possibility to reuse proof procedures, infrastructure and theorem libraries already existing in Isabelle/HOL. Moreover, once a process specification is encoded and parsed in Isabelle/Circus, proofs of, e. g., refinement properties can be developed using the ISAR language for structured proofs.

To show in more details how to use Isabelle/Circus, we provide a small example of action refinement proof. The refinement relation is defined as the universal reverse implication in the UTP. In Circus, it is defined as follows:

\[
\text{definition } \text{A1} \sqsubseteq c \text{ A2} \equiv (\text{Rep\_Action A1}) \sqsubseteq \text{utp} (\text{Rep\_Action A2})
\]

where A1 and A2 are Circus actions, \sqsubseteq c and \sqsubseteq \text{utp} stands respectively for refinement relation on Circus actions and on UTP predicate.

This definition assumes that the actions A1 and A2 share the same alphabet (binding) and the same channels. In general, refinement involves an important data evolution and growth. The data refinement is defined in [16, 5] by backwards and forwards simulations. In this paper, we restrict ourselves to a special case, the so-called functional backwards simulation. This refers to the fact that the abstraction relation R that relates concrete and abstract actions is just a function:

\[
\text{definition } \text{Simulation ("_ \leq_ _") where}
A1 \leq R A2 = \forall a b. (\text{Rep\_Action A2})(a,b) \rightarrow (\text{Rep\_Action A1})(R a,R b)
\]

where A1 and A2 are Circus actions and R is a function mapping the corresponding A1 alphabet to the A2 alphabet.

4.3 Refinement Proofs

We can use the definition of simulation to transform the proof of refinement to a simple proof of implication by unfolding the operators in terms of their underlying relational semantics. The problem with this approach is that the size of proofs will grow exponentially with the size of the processes. To avoid this problem, some general refinement laws were defined in [5] to deal with the refinement of Circus actions at operators level and not at UTP level. We introduced and proved a subset of these laws in our environment (see Table 1).
\[
\begin{align*}
P \preceq_S Q & \quad P' \preceq_S Q' & \text{SeqI} \\
P \preceq_S Q & \quad P' \preceq_S Q' \\
\mu X \bullet P \preceq_S \mu Y \bullet Q & \quad \text{MuI} \\
[X \preceq_S Y] & \\
P X \preceq_S Q Y & \quad \text{MonoP} \quad \text{MonoQ} \\
\mu X \bullet P X \preceq_S \mu Y \bullet Q Y & \quad \text{MuI} \\
[X \preceq_S Y] & \\
\text{ParI} & \quad \text{SkipI} \\
P \preceq_S Q & \quad P' \preceq_S Q' \\
P \Box P' \preceq_S Q' & \\
\text{DetI} & \\
\text{SchI} & \\
\text{SyncI} & \\
\text{InpI} & \quad \text{OutI} & \\
\text{GrdI} & \\
\end{align*}
\]

Table 1: Proved refinement laws

In Table 1, the relations \( x \sim_S y \) and \( g_1 \simeq_S g_2 \) record the fact that the variable \( x \) (respectively the guard \( g_1 \)) is refined by the variable \( y \) (respectively by the guard \( g_2 \)) w.r.t the simulation function \( S \).

These laws can be used in complex refinement proofs to simplify them at the Circus level. More rules can be defined and proved to deal with more complicated statements like combination of operators for example. Using these laws, and exploiting the advantages of a shallow embedding, the automated proof of refinement becomes surprisingly simple.

Coming back to our example, let us consider the DFIG specification below, where the management of the identifiers via the set \( \text{idS} \) is refined into a set of removed identifiers \( \text{retidS} \) and a number \( \text{max} \), which is the rank of the last issued identifier.

\[
\begin{align*}
\text{circusprocess DFIG} = \\
\text{alphabet} & = [w::\text{nat}, y::\text{nat}] \\
\text{state} & = [\text{retidS}::\text{nat set}, \text{max}::\text{nat}] \\
\text{schema Init} & = \text{retidS}' = \{\} \land \text{max}' = 0 \\
\text{schema Out} & = w' = \text{max} \land \text{max}' = \text{max} + 1 \land \text{retidS}' = \text{retidS} - \{\text{max}\} \\
\text{schema Remove} & = y < \text{max} \land y \notin \text{retidS} \land \text{retidS}' = \text{retidS} \cup \{y\} \\
& \land \text{max}' = \text{max} \\
\text{where var w \cdot Schema Init; (\mu X \cdot (\text{req} \rightarrow \text{Schema Out}; \text{out!w} \rightarrow \text{Skip}))} & \\
& \square (\text{ret?y} \rightarrow \text{Schema Remove}); X)
\end{align*}
\]

21
We provide the proof of refinement of FIG by DFIG just instantiating the simulation function $R$ by the following abstraction function, that maps the underlying concrete states to abstract states:

\[ \text{definition Sim } A = \text{FIG_alphabet.make } (w \ A) \ (y \ A) \]
\[ \{\{. \ a < (\max \ A) \land a \notin \{\text{retidS } A\}\}\} \]

where $A$ is the alphabet of DFIG, and FIG_alphabet.make yields an alphabet of type FIG_Alphabet initializing the values of $v$, $x$ and $idS$ by their corresponding values from DFIG_alphabet: $w$, $y$ and $\{a. a < \max \land a \notin \text{retidS}\}$.

To prove that DFIG is a refinement of FIG one must prove that the main action DFIG.DFIG refines the main action FIG.FIG. The definition is then simplified, and the refinement laws are applied to simplify the proof goal. Thus, the full proof consists of a few lines in ISAR:

\[ \text{theorem "FIG.FIG} \preceq \text{Sim DFIG.DFIG"} \]
\[ \text{apply (auto simp: DFIG.DFIG_def FIG.FIG_def mono_Seq} \]
\[ \text{intro!: VarI SeqI MuI DetI SyncI InpI OutI SkipI)} \]
\[ \text{apply (simp_all add: SimInit SimOut SimInit Sim_def)} \]
\[ \text{done} \]

First, the definitions of FIG.FIG and DFIG.DFIG are simplified and the defined refinement laws are used by the auto tactic as introduction rules. The second step replaces the definition of the simulation function and uses some proved lemmas to finish the proof. The three lemmas used in this proof: SimInit, SimOut and SimRemove give proofs of simulation for the schema Init, Out and Remove.

5 Conclusions

We have shown for the language Circus, which combines data-oriented modeling in the style of Z and behavioral modeling in the style of CSP, a semantics in form of a shallow embedding in Isabelle/HOL. In particular, by representing the somewhat non-standard concept of the alphabet in UTP in form of extensible records in HOL, we achieved a fairly compact, typed presentation of the language. In contrast to previous work based on some deep embedding [19], this shallow embedding allows arbitrary (higher-order) HOL-types for channels, events, and state-variables, such as, e.g., sets of relations etc. Besides, systematic renaming of local variables is avoided by compiling them essentially to global variables using a stack of variable instances. The necessary proofs for showing that the definitions are consistent — i.e. satisfy altogether is_CSP_healthy — have been done, together with a number of algebraic simplification laws on Circus processes.

Since the encoding effort can be hidden behind the scene by flexible extension mechanisms of the Isabelle, it is possible to have a compact notation
for both specifications and proofs. Moreover, existing standard tactics of Isabelle such as auto, simp and metis can be reused since our Circus semantics is representationally close to HOL. Thus, we provide an environment that can cope with combined refinements concerning data and behavior. Finally, we demonstrate its power — w.r.t. both expressivity and proof automation — with a small, but prototypic example of a process-refinement.

In the future, we intend to use Isabelle/Circus for the generation of test-cases, on the basis of [4], using the HOL-TestGen-environment [2].

6 Acknowledgement

We warmly thank Markarius Wenzel for his valuable help with the Isabelle framework. Furthermore, we are greatly indebted to Ana Cavalcanti for her comments on the semantic foundation of this work.
7 UTP variables

theory Var
imports Main
begin
declare implies-True-equals[simp] False-implies-equals[simp]

UTP variables are characterized by two functions, select and update. The variable type is then defined as a tuple (select * update).

type-synonym ('a, 'r) var = ('r ⇒ 'a) * (('a ⇒ 'a) ⇒ 'r ⇒ 'r)

The lookup function returns the corresponding select function of a variable.
definition lookup :: ('a, 'r) var ⇒ 'r ⇒ 'a
where lookup f ≡ (fst f)

The assign function uses the update function of a variable to update its value.
definition assign :: ('a, 'r) var ⇒ 'a ⇒ 'r ⇒ 'r
where assign f v ≡ (snd f) (λ - . v)

The VAR function allows to retrieve a variable given its name.
syntax -VAR :: id ⇒ ('a, 'r) var (VAR -)
translations VAR x => (x, -update-name x)
end

8 Predicates and relations

theory Relations
imports Var
begin
default-sort type

Unifying Theories of Programming (UTP) is a semantic framework based
on an alphabetized relational calculus. An alphabetized predicate is a pair
(alphabet, predicate) where the free variables appearing in the predicate are
all in the alphabet.

An alphabetized relation is an alphabetized predicate where the alphabet
is composed of input (undecorated) and output (dashed) variables. In this
case the predicate describes a relation between input and output variables.

8.1 Definitions

In this section, the definitions of predicates, relations and standard operators
are given.
type-synonym 'α alphabet = 'α

definition true::'α predicate
where true ≡ λA. True

definition false::'α predicate
where false ≡ λA. False

definition not::'α predicate ⇒ 'α predicate
where ¬ P ≡ λA. ¬ (P A)

definition conj::'α predicate ⇒ 'α predicate ⇒ 'α predicate
where P ∧ Q ≡ λA. P A ∧ Q A

definition disj::'α predicate ⇒ 'α predicate ⇒ 'α predicate
where P ∨ Q ≡ λA. P A ∨ Q A

definition impl::'α predicate ⇒ 'α predicate ⇒ 'α predicate
where P −→ Q ≡ λA. P A −→ Q A

definition iff::'α predicate ⇒ 'α predicate ⇒ 'α predicate
where P ←→ Q ≡ λA. P A ←→ Q A

definition cond::'α relation ⇒ 'α condition ⇒ 'α relation ⇒ 'α relation
where (P a b ⊑ Q) ≡ (b ∧ P) ∨ ((¬ b) ∧ Q)

definition comp::(('α × 'β) ⇒ bool) ⇒ (('β × 'γ) ⇒ bool) ⇒ ('α × 'γ) ⇒ bool
where P ; ; Q ≡ λr. r : {{p. P p} O {q. Q q}}

definition Assign::('a, 'b) var ⇒ 'a ⇒ 'b relation
where Assign x a ≡ λ(A, A'). A' = (assign x a) A

syntax
-assignment :: id ⇒ 'a ⇒ 'b relation (· ::= -)
translations
y ::= vv => CONST Assign (VAR y) vv


**Abbreviation** *(input)* closure::\(\alpha\) predicate \(\Rightarrow\) bool ([\(-\)])

where \([ \, P \, ] \equiv \forall \, A. \, P \, A\)

**Abbreviation** *(input)* ndet::\(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation

where \(P \cap Q \equiv P \lor Q\)

**Abbreviation** *(input)* join::\(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation \(\Rightarrow\) \(\alpha\) relation

where \(P \sqcup Q \equiv P \land Q\)

**Abbreviation** *(input)* ndetS::\(\alpha\) relation set \(\Rightarrow\) \(\alpha\) relation

where \(d \, S \equiv \lambda \, A. \, A \in \bigcup \{\{p. \, P \, p\} \mid P. \, P \in S\}\)

**Abbreviation** *(input)* conjS::\(\alpha\) relation set \(\Rightarrow\) \(\alpha\) relation

where \(\sqcap \, S \equiv \lambda \, A. \, A \in \bigcap \{\{p. \, P \, p\} \mid P. \, P \in S\}\)

**Abbreviation** *(input)* skip-r::\(\alpha\) relation

where \(\Pi \, r \equiv \lambda \, (A, \, A') \cdot A = A'\)

**Abbreviation** *(input)* Bot::\(\alpha\) relation

where \(Bot \equiv true\)

**Abbreviation** *(input)* Top::\(\alpha\) relation

where \(Top \equiv false\)

**Lemmas**

<table>
<thead>
<tr>
<th>utp-defs</th>
<th>true-def</th>
<th>false-def</th>
<th>conj-def</th>
<th>disj-def</th>
<th>not-def</th>
<th>impl-def</th>
<th>iff-def</th>
<th>ex-def</th>
<th>all-def</th>
<th>cond-def</th>
<th>comp-def</th>
<th>Assign-def</th>
</tr>
</thead>
</table>

8.2 Proofs

All useful proved lemmas over predicates and relations are presented here. First, we introduce the most important lemmas that will be used by automatic tools to simplify proofs. In the second part, other lemmas are proved using these basic ones.

8.2.1 Setup of automated tools

**Lemma** true-intro: true \(x\) \(\langle\)proof\(\rangle\)

**Lemma** false-elim: false \(x\) \(\Rightarrow\) \(C\) \(\langle\)proof\(\rangle\)

**Lemma** true-elim: true \(x\) \(\Rightarrow\) \(C\) \(\Rightarrow\) \(C\) \(\langle\)proof\(\rangle\)

**Lemma** not-intro: \((P. \, x \Rightarrow false \, x) \Rightarrow (\neg \, P) \, x\) \(\langle\)proof\(\rangle\)

**Lemma** not-elim: \((\neg \, P) \, x \Rightarrow P \, x \Rightarrow C\) \(\langle\)proof\(\rangle\)

**Lemma** not-dest: \((\neg \, P) \, x \Rightarrow \neg \, P \, x\) \(\langle\)proof\(\rangle\)

**Lemma** conj-intro: \(P \, x \Rightarrow Q \, x \Rightarrow (P \land Q) \, x\) \(\langle\)proof\(\rangle\)

**Lemma** conj-elim: \((P \land Q) \, x \Rightarrow (P \, x \Rightarrow Q \, x \Rightarrow C) \Rightarrow C\) \(\langle\)proof\(\rangle\)

**Lemma** disj-intro\(C\): \((\neg \, Q \, x \Rightarrow P \, x) \Rightarrow (P \lor Q) \, x\) \(\langle\)proof\(\rangle\)
lemma disj-elim: \((P \lor Q) x \implies (P x \implies C) \implies (Q x \implies C) \implies C\) (proof)

lemma impl-intro: \((P x \implies Q x) \implies (P \implies Q) x\) (proof)

lemma impl-elimC: \((P \implies Q) x \implies (\neg P x \implies R) \implies (Q x \implies R) \implies R\) (proof)

lemma iff-intro: \((P x \implies Q x) \implies (Q x \implies P x) \implies (P \iff Q) x\) (proof)

lemma iff-elimC:
\((P \iff Q) x \implies (P x \implies Q x \implies R) \implies (\neg P x \implies \neg Q x \implies R) \implies R\) (proof)

lemma all-intro: \((\forall a. \ P a x) \implies (\forall a. \ P a) x\) (proof)

lemma all-elim: \((\forall a. \ P a) x \implies (P a x \implies R) \implies R\) (proof)

lemma ex-intro: \(P a x \implies (\exists a. \ P a) x\) (proof)

lemma ex-elim: \((\exists a. \ P a) x \implies (\forall a. \ P a x \implies Q) \implies Q\) (proof)

lemma comp-intro: \(P (a, b) \implies Q (b, c) \implies (P ; ; Q) (a, c)\) (proof)

lemma comp-elim:
\((P ; ; Q) ac \implies (\forall a b c. \ ac = (a, c) \implies P (a, b) \implies Q (b, c) \implies C) \implies C\) (proof)

declare not-def [simp]

declare iff-intro [intro!]
and not-intro [intro!]
and impl-intro [intro!]
and disj-introC [intro!]
and conj-intro [intro!]
and true-intro [intro!]
and comp-intro [intro]

declare not-dest [dest!]
and iff-elimC [elim!]
and false-elim [elim!]
and impl-elimC [elim!]
and disj-elim [elim!]
and conj-elim [elim!]
and comp-elim [elim!]
and true-elim [elim!]

declare all-intro [intro!] and ex-intro [intro]
declare ex-elim [elim!] and all-elim [elim]

lemmas relation-rules = iff-intro not-intro impl-intro disj-introC conj-intro true-intro
comp-intro not-dest iff-elimC false-elim impl-elimC all-elim
disj-elim conj-elim comp-elim all-intro ex-intro ex-elim

27
lemma split-cond:
A (((P ▷ b ⊸ Q) x) = ((b x → A (P x)) ∧ (¬ b x → A (Q x))))
(proof)

lemma split-cond-asn:
A (((P ▷ b ⊸ Q) x) = (¬ ((b x ∧ ¬ A (P x)) ∨ (¬ b x ∧ ¬ A (Q x)))))
(proof)

lemmas cond-splits = split-cond split-cond-asn

8.2.2 Misc lemmas

lemma cond-idem:(P ▷ b ⊸ P) = P
(proof)

lemma cond-symn:(P ▷ b ⊸ Q) = (Q ▷ ¬ b ⊸ P)
(proof)

lemma cond-assoc: ((P ▷ b ⊸ Q) ▷ c ⊸ R) = (P ▷ b ∧ c ⊸ (Q ▷ c ⊸ R))
(proof)

lemma cond-distr: (P ▷ b ⊸ (Q ▷ c ⊸ R)) = ((P ▷ b ⊸ Q) ▷ c ⊸ (P ▷ b ⊸ R))
(proof)

lemma cond-unit-T:(P ▷ true ⊸ Q) = P
(proof)

lemma cond-unit-F:(P ▷ false ⊸ Q) = Q
(proof)

lemma cond-L6: (P ▷ b ⊸ (Q ▷ b ⊸ R)) = (P ▷ b ⊸ R)
(proof)

lemma cond-L7: (P ▷ b ⊸ (P ▷ c ⊸ Q)) = (P ▷ b ⊸ c ⊸ Q)
(proof)

lemma cond-and-distr: ((P ∧ Q) ▷ b ⊸ (R ∧ S)) = ((P ▷ b ⊸ R) ∧ (Q ▷ b ⊸ S))
(proof)

lemma cond-or-distr: ((P ∨ Q) ▷ b ⊸ (R ∨ S)) = ((P ▷ b ⊸ R) ∨ (Q ▷ b ⊸ S))
(proof)

lemma cond-imp-distr:
(((P → Q) ▷ b ⊸ (R → S)) = ((P ▷ b ⊸ R) → (Q ▷ b ⊸ S))
(proof)
\textbf{lemma} cond-eq-distr: 
\[ ((P \leftarrow\rightarrow Q) \triangleleft b \triangleright (R \leftarrow\rightarrow S)) = ((P \triangleleft b \triangleright R) \leftarrow\rightarrow (Q \triangleleft b \triangleright S)) \]  
(proof)

\textbf{lemma} comp-assoc: \((P ; ; (Q ; ; R)) = ((P ; ; Q) ; ; R)\)  
(proof)

\textbf{lemma} conj-comp: 
\[(\wedge a b c. P (a, b) = P (a, c)) \implies (P \wedge (Q ; ; R)) = ((P \wedge Q) ; ; R)\]  
(proof)

\textbf{lemma} comp-cond-left-distr: 
\[\text{assumes} \ \bigwedge x y z. b (x, y) = b (x, z) \] 
\[\text{shows} \ ((P \triangleleft b \triangleright Q) ; ; R) = ((P ; ; R) \triangleleft b \triangleright (Q ; ; R))\]  
(proof)

\textbf{lemma} ndet-symm: \((P ; ; Q) \cap Q = Q \cap P\)  
(proof)

\textbf{lemma} ndet-assoc: \(P \cap (Q \cap R) = (P \cap Q) \cap R\)  
(proof)

\textbf{lemma} ndet-idemp: \(P \cap P = P\)  
(proof)

\textbf{lemma} ndet-distr: \(P \cap (Q \cap R) = (P \cap Q) \cap (P \cap R)\)  
(proof)

\textbf{lemma} cond-ndet-distr: \((P \triangleleft b \triangleright (Q \cap R)) = ((P \cap (Q \triangleleft b \triangleright R))\)  
(proof)

\textbf{lemma} ndet-cond-distr: \((P \cap (Q \triangleright b \triangleleft R)) = (P \cap Q) \triangleright b \triangleleft (P \cap R)\)  
(proof)

\textbf{lemma} comp-ndet-l-distr: \((P \cap Q) ; ; R) = ((P ; ; R) \cap (Q ; ; R))\)  
(proof)

\textbf{lemma} comp-ndet-r-distr: \((P ; ; Q \cap R)) = (P ; ; Q \cap (P ; ; R))\)  
(proof)

\textbf{lemma} l2-5-1-A: \(\forall X \in S. [X \rightarrow (\bigcap S)]\)  
(proof)

\textbf{lemma} l2-5-1-B: \((\forall X \in S. [X \rightarrow P]) \rightarrow (\bigcap S) \rightarrow P\)  
(proof)

\textbf{lemma} l2-5-1: \([\bigcap S] \rightarrow P \leftrightarrow (\forall X \in S. [X \rightarrow P])\)  
(proof)
lemma empty-disj: \[ \bigcap \{ \} = \text{Top} \]
(proof)

lemma l2-5-1-2: [P \rightarrow (\bigcup S)]=[\forall X \in S. [P \rightarrow X]]
(proof)

lemma empty-conj: \[ \bigcup \{ \} = \text{Bot} \]
(proof)

lemma l2-5-2: \[ (\bigcup S \cap Q) = (\bigcup \{ P \cap Q \mid P \in S \}) \]
(proof)

lemma l2-5-3: \[ (\bigcup S) \cap \bigcup Q = (\bigcup \{ P \cap Q \mid P \in S \}) \]
(proof)

lemma l2-5-4: \[ (\bigcup S) \cap \bigcup Q = (\bigcup \{ P \cap Q \mid P \in S \}) \]
(proof)

lemma l2-5-5: \[ (\bigcup S) \cap \bigcup Q = (\bigcup \{ P \cap Q \mid P \in S \}) \]
(proof)

lemma all-idem : \( \forall b. \forall a. P a \) = \( \forall a. P a \)
(proof)

lemma comp-unit-R [simp]: \( P \; ; \Pi r \) = \( P \)
(proof)

lemma comp-unit-L [simp]: \( \Pi r \; ; \) \( P \) = \( P \)
(proof)

lemmas comp-unit-simps = comp-unit-R comp-unit-L

lemma not-cond: \( \neg(P \lessdot b \lozenge Q) \) = \( \neg P \lessdot b \lozenge (\neg Q) \)
(proof)

lemma cond-conj-not-distr: \[ ((P \lessdot b \lozenge Q) \land \neg(R \lessdot b \lozenge S)) = ((P \land \neg R) \lessdot b \lozenge (Q \land \neg S)) \]
(proof)

lemma imp-cond-distr: \( R \rightarrow (P \lessdot b \lozenge Q) \) = \( (R \rightarrow P) \lessdot b \lozenge (R \rightarrow Q) \)
(proof)

lemma cond-imp-distr: \( (P \lessdot b \lozenge Q) \rightarrow R \) = \( (P \rightarrow R) \lessdot b \lozenge (Q \rightarrow R) \)
(proof)

lemma cond-conj-distr: \( (P \lessdot b \lozenge Q) \land R \) = \( (P \land R) \lessdot b \lozenge (Q \land R) \)
(proof)

lemma cond-disj-distr: \( (P \lessdot b \lozenge Q) \lor R \) = \( (P \lor R) \lessdot b \lozenge (Q \lor R) \)
(proof)

**lemma** cond-know-b: \((b \land (P \triangleleft b \triangleright Q)) = (b \land P)\)

(proof)

**lemma** cond-know-nb: \(((\neg (b)) \land (P \triangleleft b \triangleright Q)) = ((\neg (b)) \land Q)\)

(proof)

**lemma** cond-ass-if: \((P \triangleleft b \triangleright Q) = (((b) \land (P \triangleleft b \triangleright Q)))\)

(proof)

**lemma** cond-ass-else: \((P \triangleleft b \triangleright Q) = (P \triangleleft (\neg (b)) \triangleright Q)\)

(proof)

**lemma** not-true-eq-false: \((\neg \text{true}) = \text{false}\)

(proof)

**lemma** not-false-eq-true: \((\neg \text{false}) = \text{true}\)

(proof)

**lemma** conj-idem: \(((P::\alpha \text{ predicate}) \land P) = P\)

(proof)

**lemma** disj-idem: \(((P::\alpha \text{ predicate}) \lor P) = P\)

(proof)

**lemma** conj-comm: \(((P::\alpha \text{ predicate}) \land Q) = (Q \land P)\)

(proof)

**lemma** disj-comm: \(((P::\alpha \text{ predicate}) \lor Q) = (Q \lor P)\)

(proof)

**lemma** conj-subst: \(P = R \implies ((P::\alpha \text{ predicate}) \land Q) = (R \land Q)\)

(proof)

**lemma** disj-subst: \(P = R \implies ((P::\alpha \text{ predicate}) \lor Q) = (R \lor Q)\)

(proof)

**lemma** conj-assoc: \(((P::\alpha \text{ predicate}) \land Q) \land S) = (P \land (Q \land S))\)

(proof)

**lemma** disj-assoc: \(((P::\alpha \text{ predicate}) \lor Q) \lor S) = (P \lor (Q \lor S))\)

(proof)

**lemma** conj-disj-abs: \(((P::\alpha \text{ predicate}) \land (P \lor Q)) = P\)

(proof)

**lemma** disj-conj-abs: \(((P::\alpha \text{ predicate}) \lor (P \land Q)) = P\)

(proof)
\textbf{lemma} \textit{conj-disj-distr}::\((\alpha \rightarrow (P \land Q) \land Q) = ((P \land Q) \lor (P \land R))\)
\begin{proof}
\end{proof}

\textbf{lemma} \textit{disj-conj-distr}::\((\alpha \rightarrow ((P \lor Q) \land R)) = ((P \land Q) \lor (P \land R))\)
\begin{proof}
\end{proof}

\textbf{lemma} \textit{true-conj-id}::\((P \land \text{true}) = P\)
\begin{proof}
\end{proof}

\textbf{lemma} \textit{true-disj-zero}::\((P \lor \text{true}) = \text{true}\)
\begin{proof}
\end{proof}

\textbf{lemma} \textit{true-conj-zero}::\((P \land \text{false}) = \text{false}\)
\begin{proof}
\end{proof}

\textbf{lemma} \textit{true-disj-id}::\((P \lor \text{false}) = P\)
\begin{proof}
\end{proof}

\textbf{lemma} \textit{imp-vacuous}::\((\text{false} \rightarrow \text{u}) = \text{true}\)
\begin{proof}
\end{proof}

\textbf{lemma} \textit{p-and-not-p}::\((P \land \neg P) = \text{false}\)
\begin{proof}
\end{proof}

\textbf{lemma} \textit{conj-disj-not-abs}::\((P \land ((\neg P) \lor Q)) = (P \land Q)\)
\begin{proof}
\end{proof}

\textbf{lemma} \textit{p-or-not-p}::\((P \lor \neg P) = \text{true}\)
\begin{proof}
\end{proof}

\textbf{lemma} \textit{double-negation}::\((\neg \neg (P::\alpha \rightarrow (P::\alpha \rightarrow Q))) = P\)
\begin{proof}
\end{proof}

\textbf{lemma} \textit{not-conj-deMorgans}::\((\neg ((P::\alpha \rightarrow Q) \land Q)) = ((\neg Q) \land (\neg Q))\)
\begin{proof}
\end{proof}

\textbf{lemma} \textit{not-disj-deMorgans}::\((\neg ((P::\alpha \rightarrow Q) \lor Q)) = ((\neg P) \land (\neg Q))\)
\begin{proof}
\end{proof}

\textbf{lemma} \textit{p-imp-p}::\((P \rightarrow (P \rightarrow P)) = \text{true}\)
\begin{proof}
\end{proof}

\textbf{lemma} \textit{imp-imp}::\(((P::\alpha \rightarrow Q) \rightarrow (Q \rightarrow R)) = ((P \land Q) \rightarrow (P \land Q) \rightarrow R)\)
\begin{proof}
\end{proof}

\textbf{lemma} \textit{imp-trans}::\((P \rightarrow (Q \land R) \rightarrow Q \rightarrow R) \rightarrow P \rightarrow R) = \text{true}\)
\begin{proof}
\end{proof}
\textbf{lemma} \textit{p-equiv-p}: $(P \iff P) = \text{true}$
\hspace{1cm} (proof)

\textbf{lemma} \textit{equiv-eq}: \(((P::\alpha\ \text{predicate}) \land Q) \lor (\neg P \land \neg Q) = \text{true}) \iff (P = Q)$
\hspace{1cm} (proof)

\textbf{lemma} \textit{equiv-eq1}: \(((P::\alpha\ \text{predicate}) \iff Q) = \text{true}) \iff (P = Q)$
\hspace{1cm} (proof)

\textbf{lemma} \textit{cond-subst}: $b = c \Longrightarrow (P \triangleleft b \triangleright Q) = (P \triangleleft c \triangleright Q)$
\hspace{1cm} (proof)

\textbf{lemma} \textit{ex-disj-distr}: $(\exists x.\ P\ x) \lor (\exists x.\ Q\ x)) = (\exists x.\ (P\ x \lor Q\ x))$
\hspace{1cm} (proof)

\textbf{lemma} \textit{all-disj-distr}: $(\forall x.\ P\ x) \lor (\forall x.\ Q\ x)) = (\forall x.\ (P\ x \lor Q\ x))$
\hspace{1cm} (proof)

\textbf{lemma} \textit{all-conj-distr}: $(\forall x.\ P\ x) \land (\forall x.\ Q\ x)) = (\forall x.\ (P\ x \land Q\ x))$
\hspace{1cm} (proof)

\textbf{lemma} \textit{all-triv}: $(\forall x.\ P) = P$
\hspace{1cm} (proof)

\textbf{lemma} \textit{closure-true}: [true]
\hspace{1cm} (proof)

\textbf{lemma} \textit{closure-p-eq-true}: $[P] \iff (P = \text{true})$
\hspace{1cm} (proof)

\textbf{lemma} \textit{closure-equiv-eq}: $[P \iff Q] \iff (P = Q)$
\hspace{1cm} (proof)

\textbf{lemma} \textit{closure-conj-distr}: $([P] \land [Q]) = [P \land Q]$
\hspace{1cm} (proof)

\textbf{lemma} \textit{closure-imp-distr}: $[P \rightarrow Q] \rightarrow [P] \rightarrow [Q]$
\hspace{1cm} (proof)

\textbf{lemma} \textit{true-iff[simp]}: $(P \iff \text{true}) = P$
\hspace{1cm} (proof)

\textbf{lemma} \textit{true-imp[simp]}: $(\text{true} \rightarrow P) = P$
\hspace{1cm} (proof)

\textbf{end}
9 Designs

theory Designs
imports Relations
begin

In UTP, in order to explicitly record the termination of a program, a subset of alphabetized relations is introduced. These relations are called designs and their alphabet should contain the special boolean observational variable \( \text{ok} \). It is used to record the start and termination of a program.

9.1 Definitions

In the following, the definitions of designs alphabets, designs and healthiness (well-formedness) conditions are given. The healthiness conditions of designs are defined by \( H_1, H_2, H_3 \) and \( H_4 \).

record alpha-d = ok::bool

type-synonym \( \alpha \) alphabet-d = \( \alpha \) alphabet-d-scheme alphabet

type-synonym \( \alpha \) relation-d = \( \alpha \) alphabet-d relation

definition design\( :: \alpha \) relation-d \( \Rightarrow \alpha \) relation-d \( \Rightarrow \alpha \) relation-d (\( \langle - \dashv - \rangle \))
where \( (P \vdash Q) \equiv \lambda (A,A') . (\text{ok } A \wedge P (A,A') \rightarrow (\text{ok } A' \wedge Q (A,A'))) \)

definition skip-d :: \( \alpha \) relation-d (\( \Pi d \))
where \( \Pi d \equiv (\text{true} \vdash \Pi r) \)

definition \( J \)
where \( J \equiv \lambda (A,A') . (\text{ok } A \rightarrow \text{ok } A') \wedge \text{more } A = \text{more } A' \)

type-synonym \( \alpha \) Healthiness-condition = \( \alpha \) relation \( \Rightarrow \alpha \) relation

definition Healthy\( :: \alpha \) relation \( \Rightarrow \alpha \) Healthiness-condition \( \Rightarrow \) bool (\( - \) is \( - \) healthy)
where \( P \) is \( H \) healthy \( \equiv (P = H \ P) \)

lemma Healthy-def\( ': P \) is \( H \) healthy = (\( H \ P = P \))
(proof)

definition \( H_1 \):(\( \alpha \) alphabet-d) Healthiness-condition
where \( H_1 (P) \equiv (\text{ok } \text{ fst} \rightarrow P) \)

definition \( H_2 \):(\( \alpha \) alphabet-d) Healthiness-condition
where \( H_2 (P) \equiv P ; ; J \)

definition \( H_3 \):(\( \alpha \) alphabet-d) Healthiness-condition
where \( H_3 (P) \equiv P ; ; \Pi d \)
definition \( H_4 \):\( \alpha \) Healthiness-condition
where \( H_4 (P) \equiv ((P; true) \leftrightarrow true) \)

definition \( \sigma_f \)::\( \alpha \) relation-d \( \Rightarrow \) \( \alpha \) relation-d
where \( \sigma_f D \equiv \lambda (A, A'). D (A, A' ok:=False) \)

definition \( \sigma_t \)::\( \alpha \) relation-d \( \Rightarrow \) \( \alpha \) relation-d
where \( \sigma_t D \equiv \lambda (A, A'). D (A, A' ok:=True) \)

definition \( \text{OKAY} \)::\( \alpha \) relation-d
where \( \text{OKAY} \equiv \lambda (A, A'). ok A \)

definition \( \text{OKAY}' \)::\( \alpha \) relation-d
where \( \text{OKAY}' \equiv \lambda (A, A'). ok A' \)

lemmas design-defs = design-def skip-d-def J-def Healthy-def H1-def H2-def H3-def H4-def \( \sigma_f \)-def \( \sigma_t \)-def OKAY-def OKAY'-def

9.2 Proofs

Proof of theorems and properties of designs and their healthiness conditions are given in the following.

lemma \( \text{t-comp-lz-d} \): \((true; (P \vdash Q)) = true\)
(proof)

lemma \( \text{pi-comp-left-unit} \): \((\Pi d; (P \vdash Q)) = (P \vdash Q)\)
(proof)

theorem \( \text{t3-1-4-2} \):
\(((P_1 \vdash Q_1) \triangleleft b \triangleright (P_2 \vdash Q_2)) = ((P_1 \triangleleft b \triangleright P_2) \vdash (Q_1 \triangleleft b \triangleright Q_2))\)
(proof)

lemma \( \text{conv-conj-distr} \): \( \sigma_t (P \land Q) = (\sigma_t P \land \sigma_t Q)\)
(proof)

lemma \( \text{conv-disj-distr} \): \( \sigma_t (P \lor Q) = (\sigma_t P \lor \sigma_t Q)\)
(proof)

lemma \( \text{conv-imp-distr} \): \( \sigma_t (P \rightarrow Q) = ((\sigma_t P) \rightarrow \sigma_t Q)\)
(proof)

lemma \( \text{conv-not-distr} \): \( \sigma_t (\neg P) = (\neg(\sigma_t P))\)
(proof)

lemma \( \text{div-conj-distr} \): \( \sigma_f (P \land Q) = (\sigma_f P \land \sigma_f Q)\)
(proof)

lemma \( \text{div-disj-distr} \): \( \sigma_f (P \lor Q) = (\sigma_f P \lor \sigma_f Q)\)
(proof)
lemma \textit{div-imp-distr}: \sigma f (P \rightarrow Q) = ((\sigma f P) \rightarrow \sigma f Q)
(\textit{proof})

lemma \textit{div-not-distr}: \sigma f (\neg P) = (\neg (\sigma f P))
(\textit{proof})

lemma \textit{ok-conv}: \sigma t \text{OKAY} = \text{OKAY}
(\textit{proof})

lemma \textit{ok-div}: \sigma f \text{OKAY} = \text{OKAY}
(\textit{proof})

lemma \textit{ok'-conv}: \sigma t \text{OKAY}' = \text{true}
(\textit{proof})

lemma \textit{ok'-div}: \sigma f \text{OKAY}' = \text{false}
(\textit{proof})

lemma \textit{H2-J-1}:  
\text{assumes} A: P \text{ is H2 healthy}  
\text{shows} [(\lambda (A, A'). (P(A, A'\{ok := False\})) \rightarrow P(A, A'\{ok := True\}))]
(\textit{proof})

lemma \textit{H2-J-2-a}: P (a,b) \rightarrow (P ;; J) (a,b)
(\textit{proof})

lemma \textit{ok-or-not-ok} : [P(a, b\{ok := True\}); P(a, b\{ok := False\})] \implies P(a, b)
(\textit{proof})

lemma \textit{H2-J-2-b} :  
\text{assumes} A: [(\lambda (A, A'). (P(A, A'\{ok := False\})) \rightarrow P(A, A'\{ok := True\}))]
\text{and} B : (P ;; J) (a,b)  
\text{shows} P (a,b)
(\textit{proof})

lemma \textit{H2-J-2} :  
\text{assumes} A: [(\lambda (A, A'). (P(A, A'\{ok := False\})) \rightarrow P(A, A'\{ok := True\}))]
\text{shows} P \text{ is H2 healthy}
(\textit{proof})

lemma \textit{H2-J}:  
[\lambda (A, A'). P(A, A'\{ok := False\}) \rightarrow P(A, A'\{ok := True\})] = P \text{ is H2 healthy}
(\textit{proof})

lemma \textit{design-eq1}: (P \vdash Q) = (P \vdash P \land Q)
(\textit{proof})

lemma \textit{H1-idem}: H1 o H1 = H1

36
10 Reactive processes

Following the way of UTP to describe reactive processes, more observational variables are needed to record the interaction with the environment. Three observational variables are defined for this subset of relations: $wait$, $tr$ and $ref$. The boolean variable $wait$ records if the process is waiting for an interaction or has terminated. $tr$ records the list (trace) of interactions the process has performed so far. The variable $ref$ contains the set of interactions (events) the process may refuse to perform.

In this section, we introduce first some preliminary notions, useful for trace manipulations. The definitions of reactive process alphabets and healthiness conditions are also given. Finally, proved lemmas and theorems are listed.
10.1 Preliminaries

type-synonym 'α trace = 'α list

fun list-diff::'α list ⇒ 'α list ⇒ 'α list option where
  list-diff [] = Some []
  | list-diff [] l = None
  | list-diff (x#xs) (y#ys) = (if (x = y) then (list-diff xs ys) else None)

instantiation list :: (type) minus
begin
  definition list-minus : l1 − l2 ≡ the (list-diff l1 l2)
  instance ⟨proof⟩
end

lemma list-diff-empty [simp]: the (list-diff l []) = l
⟨proof⟩

lemma prefix-diff-empty [simp]: l − [] = l
⟨proof⟩

lemma prefix-diff-eq [simp]: l − l = []
⟨proof⟩

lemma prefix-diff [simp]: (l @ t) − l = t
⟨proof⟩

lemma prefix-subst [simp]: l @ t = m → m − l = t
⟨proof⟩

lemma prefix-subst1 [simp]: m = l @ t → m − l = t
⟨proof⟩

lemma prefix-diff1 [simp]: ((l @ m) @ t) − (l @ m) = t
⟨proof⟩

lemma prefix-diff2 [simp]: (l @ (m @ t)) − (l @ m) = t
⟨proof⟩

lemma prefix-diff3 [simp]: (l @ m) − (l @ t) = (m − t)
⟨proof⟩

lemma prefix-diff4 [simp]: (a # m) − (a # t) = (m − t)
⟨proof⟩

class ev-eq
  fixes ev-eq :: 'a ⇒ 'a ⇒ bool
  assumes refl: ev-eq a a
  assumes comm: ev-eq a b = ev-eq b a

definition filter-chan-set a cs = (¬ (∃ e ∈ cs. ev-eq a e))

lemma in-imp-not-fcs:
  \( x \in S \implies \neg \text{filter-chan-set } x S \)

(proof)

fun tr-filter : 'a::ev-eq list => 'a set => 'a list where
  tr-filter [] cs = []
  | tr-filter (x#xs) cs = (if (filter-chan-set x cs) then (x#(tr-filter xs cs)) else (tr-filter xs cs))

lemma tr-filter-conc: (tr-filter (a@b) cs) = ((tr-filter a cs) @ (tr-filter b cs))
(proof)

lemma filter-chan-set-hd-tr-filter:
  tr-filter l cs ≠ [] ---\(\implies\) filter-chan-set (hd (tr-filter l cs)) cs
(proof)

lemma tr-filter-conc-eq1:
  (a@b = (tr-filter (a@c) cs)) \(\implies\) (b = (tr-filter c cs))
(proof)

lemma tr-filter-conc-eq2:
  (a@b = (tr-filter (a@c) cs)) \(\implies\) (a = (tr-filter a cs))
(proof)

lemma tr-filter-conc-eq:
  (a@b = (tr-filter (a@c) cs)) = (b = (tr-filter c cs) & a = (tr-filter a cs))
(proof)

lemma tr-filter-conc-eq3:
  (b = (tr-filter (a@c) cs)) = (∃ b1 b2. b=b1@b2 & b2 = (tr-filter c cs) & b1 = (tr-filter a cs))
(proof)

lemma tr-filter-un:
  tr-filter l (s1 ∪ s2) = tr-filter (tr-filter l s1) s2
(proof)

instantiation list :: (ev-eq) ev-eq
begin
  fun ev-eq-list where
  | ev-eq-list [] [] = True
  | ev-eq-list l [] = False
  | ev-eq-list [] l = False
  | ev-eq-list (x#xs) (y#ys) = (if (ev-eq x y) then (ev-eq-list xs ys) else False)

39
10.2 Definitions

abbreviation subl :: 'a list ⇒ 'a list ⇒ bool (- ≤ -) 
where l1 ≤ l2 == Sublist.prefixeq l1 l2

lemma list-diff-empty-eq: l1 - l2 = [] ⇒ l2 ≤ l1 ⇒ l1 = l2
(proof)

The definitions of reactive process alphabets and healthiness conditions are 
given in the following. The healthiness conditions of reactive processes are 
defined by $R_1, R_2, R_3$ and their composition $R$.

Note that we define here the class of UTP alphabets that contain $\text{wait}$, $\text{tr}$ and $\text{ref}$, or, in other words, we define here the class of reactive process 
alphabets.

type-synonym ('a, 's) alphabet-rp = ('a, 's) alpha-rp-scheme alphabet
type-synonym ('a, 's) relation-rp = ('a, 's) alphabet-rp relation

definition diff-tr s1 s2 = ((tr s1) - (tr s2))
definition spec :: [bool, bool, ('a, 's) relation-rp] ⇒ ('a, 's) relation-rp 
where spec b b' P ≡ λ (A, A'). P (A[wait := b], A'[ok := b'])

abbreviation Speciftt (-t t) where (P)^t_t ≡ spec True True P
abbreviation Specifff (-f f) where (P)^f_f ≡ spec False False P
abbreviation Speciftf (-t f) where (P)^t_f ≡ spec True False P
abbreviation Specifft (-f t) where (P)^f_t ≡ spec False True P
definition R1 ::(('a, 's) alphabet-rp) Healthiness-condition 
where R1 (P) ≡ λ(A, A'). (P (A, A')) ∧ (tr A ≤ tr A')
definition R2 ::(('a, 's) alphabet-rp) Healthiness-condition 
where R2 (P) ≡ λ(A, A'). (P (A[tr:=[]],A'[tr:= tr A' - tr A]) ∧ tr A ≤ tr A')
definition Πrea 
where Πrea ≡ λ(A, A'). (¬ok A ∧ tr A ≤ tr A') ∨ (ok A' ∧ tr A = tr A')
∧ (wait A = wait A′) ∧ ref A = ref A′ ∧ more A = more A′

**definition** \( R3::((\varnothing, \sigma) \text{ alphabet-rp}) \text{ Healthiness-condition} \)

**where** \( R3 (P) \equiv (\Pi \text{rea} \circ \text{wait} \circ \text{fst} \triangleright P) \)

**definition** \( R::((\varnothing, \sigma) \text{ alphabet-rp}) \text{ Healthiness-condition} \)

**where** \( R \equiv R3 \circ R2 \circ R1 \)

**lemmas** \( \text{rp-defs} = R1\text{-def} \ R2\text{-def} \ \Pi \text{rea}\text{-def} \ R3\text{-def} \ R\text{-def} \ spec\text{-def} \)

### 10.3 Proofs

**lemma** \( \text{tr-filter-empty} \ [\text{simp}]: \text{tr-filter} \ l \ \{\} = l \)

\( \langle \text{proof} \rangle \)

**lemma** \( \text{trf-imp-filters}: [xs = \text{tr-filter} \ ys \ cs; \ xs \neq []] \implies \text{filter-chan-set} \ (\text{hd} \ xs) \ cs \)

\( \langle \text{proof} \rangle \)

**lemma** \( \text{filters-imp-trf}:

\[ [\text{filter-chan-set} \ x \ cs; \ xs = \text{tr-filter} \ ys \ cs] \implies x\#xs = \text{tr-filter} \ (x\#ys) \ cs \]

\( \langle \text{proof} \rangle \)

**lemma** \( \text{alpha-d-more-eqI}: \)

**assumes** \( \text{tr} \ r = \text{tr} \ r' \ wait \ r = \text{wait} \ r' \ ref \ r = \text{ref} \ r' \ more \ r = \text{more} \ r' \)

**shows** \( \text{alpha-d.more} \ r = \text{alpha-d.more} \ r' \)

\( \langle \text{proof} \rangle \)

**lemma** \( \text{alpha-d-more-eqE}: \)

**assumes** \( \text{alpha-d.more} \ r = \text{alpha-d.more} \ r' \)

**obtains** \( \text{tr} \ r = \text{tr} \ r' \ wait \ r = \text{wait} \ r' \ ref \ r = \text{ref} \ r' \ more \ r = \text{more} \ r' \)

\( \langle \text{proof} \rangle \)

**lemma** \( \text{alpha-rp-eqE}: \)

**assumes** \( \ r = r' \)

**obtains** \( \text{ok} \ r = \text{ok} \ r' \ \text{tr} \ r = \text{tr} \ r' \ \text{wait} \ r = \text{wait} \ r' \ \text{ref} \ r = \text{ref} \ r' \ \text{more} \ r = \text{more} \ r' \)

\( \langle \text{proof} \rangle \)

**lemma** \( \text{R-idem}: R \circ R = R \)

\( \langle \text{proof} \rangle \)

**lemma** \( \text{R-idem2}: R (R \ P) = R \ P \)

\( \langle \text{proof} \rangle \)

**lemma** \( \text{R1-idem}: R1 \circ R1 = R1 \)

\( \langle \text{proof} \rangle \)

**lemma** \( \text{R1-idem2}: R1 (R1 \ x) = R1 \ x \)

41
proof

lemma R2-idem: R2 o R2 = R2
(proof)

lemma R2-idem2: R2 (R2 x) = R2 x
(proof)

lemma R3-idem: R3 o R3 = R3
(proof)

lemma R3-idem2: R3 (R3 x) = R3 x
(proof)

lemma R1-R2-commute: (R1 o R2) = (R2 o R1)
(proof)

lemma R1-R3-commute: (R1 o R3) = (R3 o R1)
(proof)

lemma R2-R3-commute: R2 o R3 = R3 o R2
(proof)

lemma R-abs-R1: R o R1 = R
(proof)

lemma R-abs-R2: R o R2 = R
(proof)

lemma R-abs-R3: R o R3 = R
(proof)

lemma R-is-R1:
  assumes A: P is R healthy
  shows P is R1 healthy
(proof)

lemma R-is-R2:
  assumes A: P is R healthy
  shows P is R2 healthy
(proof)

lemma R-is-R3:
  assumes A: P is R healthy
  shows P is R3 healthy
(proof)

lemma R-disj:
  assumes A: P is R healthy
assumes $B$: $Q$ is $R$ healthy
shows $(P \lor Q)$ is $R$ healthy
(proof)

lemma $R$-disj2: $R (P \lor Q) = (R P \lor R Q)$
(proof)

lemma $R$1-comp:
  assumes $P$ is $R1$ healthy
  and $Q$ is $R1$ healthy
  shows $(P; ; Q)$ is $R1$ healthy
(proof)

lemma $R$1-comp2:
  assumes $A$: $P$ is $R1$ healthy
  assumes $B$: $Q$ is $R1$ healthy
  shows $R1 (P; ; Q) = (R1 P; ; Q)$
(proof)

lemma J-is-$R1$: $J$ is $R1$ healthy
(proof)

lemma J-is-$R2$: $J$ is $R2$ healthy
(proof)

lemma $R$1-$H2$-commute2: $R1 (H2 P) = H2 (R1 P)$
(proof)

lemma $R$1-$H2$-commute: $R1 \circ H2 = H2 \circ R1$
(proof)

lemma $R$2-$H2$-commute2: $R2 (H2 P) = H2 (R2 P)$
(proof)

lemma $R$2-$H2$-commute: $R2 \circ H2 = H2 \circ R2$
(proof)

lemma $R$3-$H2$-commute2: $R3 (H2 P) = H2 (R3 P)$
(proof)

lemma $R$3-$H2$-commute: $R3 \circ H2 = H2 \circ R3$
(proof)

lemma $R$-join:
  assumes $x$ is $R$ healthy
  and $y$ is $R$ healthy
  shows $(x \cap y)$ is $R$ healthy
(proof)
lemma R-meet:
  assumes A: $x$ is $R$ healthy
  and B: $y$ is $R$ healthy
  shows $(x \sqcup y)$ is $R$ healthy
⟨proof⟩

lemma R-H2-commute: $R \circ H2 = H2 \circ R$
⟨proof⟩

lemma R-H2-commute2: $R (H2 \ P) = H2 (R \ P)$
⟨proof⟩

deﬁnition CSP1::(($\vartheta$, $\sigma$) alphabet-rp) Healthiness-condition
  where CSP1 $(P)$ ≡ $P \lor (\lambda (A, A'). \neg ok A \land tr A \leq tr A')$

definition J-csp
  where J-csp ≡ $\lambda (A, A'). \ (ok A \rightarrow ok A') \land tr A = tr A' \land wait A = wait A'$
                       $\land ref A = ref A' \land more A = more A'$

definition CSP2::(($\vartheta$, $\sigma$) alphabet-rp) Healthiness-condition
  where CSP2 $(P)$ ≡ $P ; ; J-csp$

definition is-CSP-process::($\vartheta$, $\sigma$) relation-rp ⇒ bool where
  is-CSP-process $P$ ≡ $P$ is CSP1 healthy $\land P$ is CSP2 healthy $\land P$ is $R$ healthy

lemmas csp-defs = CSP1-def J-csp-def CSP2-def is-CSP-process-def

lemma is-CSP-processE1 [elim?]:
  assumes is-CSP-process $P$
  obtains $P$ is CSP1 healthy $P$ is CSP2 healthy $P$ is $R$ healthy
⟨proof⟩
lemma is-CSP-processE2 [elim?]:
  assumes is-CSP-process P
  obtains CSP1 P = P CSP2 P = P R P = P
⟨proof⟩

11.2 Proofs

Theorems and lemmas relative to CSP processes are introduced here.

lemma CSP1-CSP2-commute: CSP1 o CSP2 = CSP2 o CSP1
⟨proof⟩

lemma CSP2-is-H2: H2 = CSP2
⟨proof⟩

lemma H2-CSP1-commute: H2 o CSP1 = CSP1 o H2
⟨proof⟩

lemma H2-CSP1-commute2: H2 (CSP1 P) = CSP1 (H2 P)
⟨proof⟩

lemma CSP1-R-commute:
  CSP1 (R P) = R (CSP1 P)
⟨proof⟩

lemma CSP2-R-commute:
  CSP2 (R P) = R (CSP2 P)
⟨proof⟩

lemma CSP1-idem: CSP1 = CSP1 o CSP1
⟨proof⟩

lemma CSP2-idem: CSP2 = CSP2 o CSP2
⟨proof⟩

lemma CSP-is-CSP1:
  assumes A: is-CSP-process P
  shows P is CSP1 healthy
⟨proof⟩

lemma CSP-is-CSP2:
  assumes A: is-CSP-process P
  shows P is CSP2 healthy
⟨proof⟩

lemma CSP-is-R:
  assumes A: is-CSP-process P
  shows P is R healthy
⟨proof⟩
lemma t-or-f-a: \( P(a, b) \implies ((P(a, b[ok := True])) \lor (P(a, b[ok := False]))) \)
(proof)

lemma CSP2-ok-a:
\((CSP2 \ P)(a, b[ok := True]) \implies (P(a, b[ok := True]) \lor P(a, b[ok := False]))\)
(proof)

lemma CSP2-ok-b:
\((P(a, b[ok := True]) \lor P(a, b[ok := False])) \implies (CSP2 \ P)(a, b[ok := True])\)
(proof)

lemma CSP2-ok:
\((CSP2 \ P)(a, b[ok := True]) = (P(a, b[ok := True]) \lor P(a, b[ok := False]))\)
(proof)

lemma CSP2-notok-a: \((CSP2 \ P)(a, b[ok := False]) \implies P(a, b[ok := False])\)
(proof)

lemma CSP2-notok-b: \(P(a, b[ok := False]) \implies (CSP2 \ P)(a, b[ok := False])\)
(proof)

lemma CSP2-notok:
\((CSP2 \ P)(a, b[ok := False]) = P(a, b[ok := False])\)
(proof)

lemma CSP2-t-f:
\(\text{assumes } A::(CSP2 \ (R \ r \ p))(a, b)\)
\(\text{and } B::((CSP2 \ (R \ r \ p))(a, b[ok := False]) \lor ((CSP2 \ (R \ r \ p))(a, b[ok := True])) \implies Q\)
\(\text{shows } Q\)
(proof)

lemma disj-CSP1:
\(\text{assumes } P \text{ is CSP1 healthy}\)
\(\text{and } Q \text{ is CSP1 healthy}\)
\(\text{shows } (P \lor Q) \text{ is CSP1 healthy}\)
(proof)

lemma disj-CSP2:
\(\text{P is CSP2 healthy } \Longrightarrow \text{ Q is CSP2 healthy } \Longrightarrow (P \lor Q) \text{ is CSP2 healthy}\)
(proof)

lemma disj-CSP:
\(\text{assumes } A::\text{is-CSP-process } P\)
\(\text{assumes } B::\text{is-CSP-process } Q\)
\(\text{shows } \text{is-CSP-process } (P \lor Q)\)
(proof)

lemma seq-CSP1:
\(\text{assumes } A::P \text{ is CSP1 healthy}\)
assumes $B$: $Q$ is CSP1 healthy
shows $(P ; ; Q)$ is CSP1 healthy
(proof)

lemma seq-CSP2:
assumes $A$: $Q$ is CSP2 healthy
shows $(P ; ; Q)$ is CSP2 healthy
(proof)

lemma seq-R:
assumes $P$ is R healthy
and $Q$ is R healthy
shows $(P ; ; Q)$ is R healthy
(proof)

lemma seq-CSP:
assumes $A$: $P$ is CSP1 healthy
and $B$: $P$ is R healthy
and $C$: is-CSP-process $Q$
shows is-CSP-process $(P ; ; Q)$
(proof)

lemma rd-ind-wait: $(R(...) \vdash (P \uparrow))$
  $= (R(...) \vdash (\lambda (A, A'). P (A, A'[ok := False])))$
  $= H1 (\lambda (A, A'). P (A, A'[ok := True])))$
(proof)

lemma rd-H1: $(R(...) \vdash (\lambda (A, A'). P (A, A'[ok := False])))$
  $= H1 (\lambda (A, A'). P (A, A'[ok := True])))$
(proof)

lemma rd-H1-H2: $(R(...) \vdash (\lambda (A, A'). P (A, A'[ok := False])))$
  $= (H1 o H2) (\lambda (A, A'). P (A, A'[ok := True])))$
(proof)

lemma rd-H1-H2-R-H1-H2:
  $(R (...) \vdash (H1 o H2) (\lambda (A, A'). P (A, A'[ok := False])))$
  $= (H1 o H2) (\lambda (A, A'). P (A, A'[ok := True])))$
  $= R o H1 o H2 P$
(proof)

lemma CSP1-is-R1-H1:
assumes $P$ is R1 healthy
shows CSP1 $P = R1 (H1 P)$
proof

lemma CSP1-is-R1-H1-2: CSP1 (R1 P) = R1 (H1 P)
(proof)

lemma CSP1-R1-commute: CSP1 o R1 = R1 o CSP1
(proof)

lemma CSP1-R1-commute2: CSP1 (R1 P) = R1 (CSP1 P)
(proof)

lemma CSP1-is-R1-H1-b:
(P = (R o R1 o H1 o H2) P) = (P = (R o CSP1 o H2) P)
(proof)

lemma CSP1-join:
assumes A: x is CSP1 healthy
and B: y is CSP1 healthy
shows (x \sqcap y) is CSP1 healthy
(proof)

lemma CSP2-join:
assumes A: x is CSP2 healthy
and B: y is CSP2 healthy
shows (x \sqcap y) is CSP2 healthy
(proof)

lemma CSP1-meet:
assumes A: x is CSP1 healthy
and B: y is CSP1 healthy
shows (x \sqcup y) is CSP1 healthy
(proof)

lemma CSP2-meet:
assumes A: x is CSP2 healthy
and B: y is CSP2 healthy
shows (x \sqcup y) is CSP2 healthy
(proof)

lemma CSP-join:
assumes A: is-CSP-process x
and B: is-CSP-process y
shows is-CSP-process (x \sqcap y)
(proof)

lemma CSP-meet:
assumes A: is-CSP-process x
and B: is-CSP-process y
shows is-CSP-process (x \sqcup y)
11.3 CSP processes and reactive designs

In this section, we prove the relation between CSP processes and reactive designs.

**Lemma rd-is-CSP1**: \( (R (r \vdash p)) \) is CSP1 healthy

**Lemma rd-is-CSP2**:
- **Assumes**: \( A : \forall a b. r (a, b (\| \text{ok} \leftarrow \text{True}) \rightarrow_r (a, b (\| \text{ok} \leftarrow \text{False})) \)
- **shows**: \( (R (r \vdash p)) \) is CSP2 healthy

**Lemma rd-is-CSP**:
- **Assumes**: \( A : \forall a b. r (a, b (\| \text{ok} \leftarrow \text{True}) \rightarrow_r (a, b (\| \text{ok} \leftarrow \text{False})) \)
- **shows**: \( \text{is-CSP-process} \ (R (r \vdash p)) \)

**Lemma CSP-is-rd**:
- **Assumes**: \( A : \text{is-CSP-process} P \)
- **shows**: \( P = (R (\neg(P f f) \vdash (P t f))) \)

12 Circus actions

**Theory** Circus-Actions

**Imports** ~~/src/HOL/HOLCF/HOLCF CSP-Processes

**Begin**

In this section, we introduce definitions for Circus actions with some useful theorems and lemmas.

**Default-sort** type

12.1 Definitions

The Circus actions type is defined as the set of all the CSP healthy reactive processes.

**Typedef** \((\theta::\text{ev-eq}, \sigma) \text{ action} = \{ p::(\theta, \sigma) \text{ relation-rp. is-CSP-process} p \}\)

**Morphisms** relation-of action-of

**Print-theorems**
The type-definition introduces a new type by stating a set. In our case, it is
the set of reactive processes that satisfy the healthiness-conditions for CSP-
processes, isomorphic to the new type. Technically, this construct introduces
two constants (morphisms) definitions \textit{relation of} and \textit{action of} as well as
the usual axioms expressing the bijection \textit{action of} \( (\text{relation of } ?x) = ?x \)
and \( ?y \in \{ p. \text{is-CSP-process } p \} \implies \text{relation of} (\text{action of } ?y) = ?y \).

\textbf{lemma relation-of-CSP}: is-CSP-process \( (\text{relation of } x) \)
\begin{proof}
\end{proof}

\textbf{lemma relation-of-CSP1}: \( (\text{relation of } x) \) is CSP1 healthy
\begin{proof}
\end{proof}

\textbf{lemma relation-of-CSP2}: \( (\text{relation of } x) \) is CSP2 healthy
\begin{proof}
\end{proof}

\textbf{lemma relation-of-R}: \( (\text{relation of } x) \) is R healthy
\begin{proof}
\end{proof}

\subsection{Proofs}

In the following, Circus actions are proved to be an instance of the \textit{Complete_Lattice}
class.

\textbf{lemma relation-of-spec-f-f}:
\( \forall a \, b. \, \text{(relation of } y \rightarrow \text{relation of } x) \, \text{(a, b)} \implies \)
\( (\text{relation of } y)^f (a|tr := [], b) \implies \)
\( (\text{relation of } x)^f (a|tr := [], b) \)
\begin{proof}
\end{proof}

\textbf{lemma relation-of-spec-t-f}:
\( \forall a \, b. \, \text{(relation of } y \rightarrow \text{relation of } x) \, \text{(a, b)} \implies \)
\( (\text{relation of } y)^f (a|tr := [], b) \implies \)
\( (\text{relation of } x)^f (a|tr := [], b) \)
\begin{proof}
\end{proof}

\textbf{instantiation action::(ev-eq, type) below}
\textbf{begin}
\textbf{definition ref-def} : \( P \sqsubseteq Q \equiv [(\text{relation of } Q) \rightarrow (\text{relation of } P)] \)
\textbf{instance} \begin{proof}
\end{proof}
\textbf{end}

\textbf{instance action :: (ev-eq, type) po}
\begin{proof}
\end{proof}

\textbf{instantiation action :: (ev-eq, type) lattice}
\textbf{begin}
\textbf{definition inf-action} : \( \inf P \, Q \equiv \text{action of} ((\text{relation of } P) \sqcap (\text{relation of } Q)) \)
\textbf{definition sup-action} : \( \sup P \, Q \equiv \text{action of} ((\text{relation of } P) \sqcup (\text{relation of } Q)) \)
\end{proof}

definition less-eq-action : (less-eq (P::('a, 'b) action) Q \equiv P \sqsubseteq Q)
definition less-action : (less (P::('a, 'b) action) Q \equiv P \sqsubseteq Q \land \lnot Q \sqsubseteq P)

instance (proof)

end

lemma bot-is-action: R (false \vdash true) \in \{ p. is-CSP-process p\}
(proof)

lemma bot-eq-true: R (false \vdash true) = R true
(proof)

instantiation action :: (ev-eq, type) bounded-lattice
begin

definition bot-action : (bot::('a, 'b) action) \equiv action-of (R(false \vdash true))
definition top-action : (top::('a, 'b) action) \equiv action-of (R(true \vdash false))

instance (proof)

end

lemma relation-of-top: relation-of top = R(true \vdash false)
(proof)

lemma relation-of-bot: relation-of bot = R true
(proof)

lemma non-emptyE: assumes A \neq {} obtains x where x : A
(proof)

lemma CSP1-Inf:
assumes *:A \neq {}
shows (\bigcap \ relation-of ' A) is CSP1 healthy
(proof)

lemma CSP2-Inf:
assumes *:A \neq {}
shows (\bigcap \ relation-of ' A) is CSP2 healthy
(proof)

lemma R-Inf:
assumes *:A \neq {}
shows (\bigcap \ relation-of ' A) is R healthy
(proof)
lemma \textit{CSP-Inf}:
\begin{align*}
\text{assumes } & A \neq \{
\text{shows } is-CSP-process \ (\bigcap relation-of \ ' A) \\
\text{(proof)}
\end{align*}

lemma \textit{Inf-is-action}: A \neq \{} \implies (\bigcup relation-of \ ' A) \in \{p. is-CSP-process p\}
\text{(proof)}

lemma \textit{CSP1-Sup}: A \neq \{ \implies (\bigcup relation-of \ ' A) \text{ is CSP1 healthy}
\text{(proof)}

lemma \textit{CSP2-Sup}: A \neq \{ \implies (\bigcup relation-of \ ' A) \text{ is CSP2 healthy}
\text{(proof)}

lemma \textit{R-Sup}: A \neq \{ \implies (\bigcup relation-of \ ' A) \text{ is R healthy}
\text{(proof)}

lemma \textit{CSP-Sup}: A \neq \{ \implies is-CSP-process (\bigcup relation-of \ ' A)
\text{(proof)}

lemma \textit{Sup-is-action}: A \neq \{ \implies (\bigcup relation-of \ ' A) \in \{p. is-CSP-process p\}
\text{(proof)}

lemma relation-of-Sup:
\begin{align*}
A \neq \{} \implies relation-of \ (action-of \ (\bigcup relation-of \ ' A) = \bigcup relation-of \ ' A
\text{(proof)}
\end{align*}

instantiation \textit{action :: (ev-eq, type) complete-lattice}
begin
\begin{align*}
definition \textit{Sup-action} : \\
(S:: ('a, 'b) action set) \equiv if S=\{\} then bot else action-of (\bigcup (relation-of \ ' S))
definition \textit{Inf-action} : \\
(S:: ('a, 'b) action set) \equiv if S=\{\} then top else action-of (\bigcap (relation-of \ ' S))
\end{align*}
\text{(proof)}
\end{align*}
end

end

13 Circus variables

theory \textit{Var-list}
\text{imports} Main
begin

Circus variables are represented by a stack (list) of values. they are char-
acterized by two functions, select and update. The Circus variable type is defined as a tuple (select * update) with a list of values instead of a single value.

**type-synonym** \((\text{\texttt{‘a}}, \text{\texttt{‘r}}) \text{var-list} = (’\sigma \Rightarrow ’\texttt{a list}) \ast ((’\texttt{a list} \Rightarrow ’\texttt{a list}) \Rightarrow ’\sigma \Rightarrow ’\texttt{r})\)

The select function returns the top value of the stack.

**definition** select :: \((’\texttt{a}, ’\texttt{r}) \text{var-list} \Rightarrow ’\texttt{a}\)

**where** select f \equiv \lambda A. hd ((fst f) A)

The increase function pushes a new value to the top of the stack.

**definition** increase :: \((’\texttt{a}, ’\texttt{r}) \text{var-list} \Rightarrow ’\texttt{a} \Rightarrow ’\texttt{r} \Rightarrow ’\texttt{r}\)

**where** increase f val \equiv (snd f) (\lambda l. val # l)

The increase0 function pushes an arbitrary value to the top of the stack.

**definition** increase0 :: \((’\texttt{a}, ’\texttt{r}) \text{var-list} \Rightarrow ’\texttt{r}\)

**where** increase0 f \equiv (snd f) (\lambda l. ((\text{\texttt{SOME val. True}}) # l))

The decrease function pops the top value of the stack.

**definition** decrease :: \((’\texttt{a}, ’\texttt{r}) \text{var-list} \Rightarrow ’\texttt{r} \Rightarrow ’\texttt{r}\)

**where** decrease f \equiv (snd f) (\lambda l. (tl l))

The update function updates the top value of the stack.

**definition** update :: \((’\texttt{a}, ’\texttt{r}) \text{var-list} \Rightarrow (’\texttt{a} \Rightarrow ’\texttt{a}) \Rightarrow ’\texttt{r} \Rightarrow ’\texttt{r}\)

**where** update f upd \equiv (snd f) (\lambda l. (upd (hd l)) # (tl l))

The update0 function initializes the top of the stack with an arbitrary value.

**definition** update0 :: \((’\texttt{a}, ’\texttt{r}) \text{var-list} \Rightarrow ’\texttt{r} \Rightarrow ’\texttt{r}\)

**where** update0 f \equiv (snd f) (\lambda l. ((\text{\texttt{SOME upd. True}}) (hd l)) # (tl l))

**axiomatization** where select-increase: \((\text{select v (increase v a s)}) = a\)

The VAR-LIST function allows to retrieve a Circus variable from its name.

**syntax** -VAR-LIST :: \id \Rightarrow (’\texttt{a}, ’\texttt{r}) \text{var-list} (\text{VAR'-LIST -})

**translations** VAR-LIST x \Rightarrow (x, -update-name x)

end

14 Denotational semantics of Circus actions

**theory** Denotational-Semantics

**imports** Circus-Actions Var-list

begin

In this section, we introduce the definitions of Circus actions denotational semantics. We provide the proof of well-formedness of every action. We also provide proofs concerning the monotonicity of operators over actions.

53
14.1 Skip

**definition Skip :: (′ϑ::ev-eq,′σ) action where**
\[ \text{Skip} \equiv \text{action-of} \]
\[ (R \text{ true } \vdash \lambda(A, A'). \text{tr } A' = \text{tr } A \land \neg \text{wait } A' \land \text{more } A = \text{more } A') \]

**lemma Skip-is-action:**
\[ (R \text{ true } \vdash \lambda(A, A'). \text{tr } A' = \text{tr } A \land \neg \text{wait } A' \land \text{more } A = \text{more } A') \in \{ p. \text{is-CSP-process } p \} \]
(\text{proof})

**lemmas Skip-is-CSP = Skip-is-action[simplified]**

**lemma relation-of-Skip:**
\[ \text{relation-of Skip} = \]
\[ (R \text{ true } \vdash \lambda(A, A'). \text{tr } A' = \text{tr } A \land \neg \text{wait } A' \land \text{more } A = \text{more } A') \]
(\text{proof})

**definition CSP3::((′ϑ::ev-eq,′σ) alphabet-rp) Healthiness-condition where**
\[ \text{CSP3}(P) \equiv \text{relation-of Skip ; ; } P \]

**definition CSP4::((′ϑ::ev-eq,′σ) alphabet-rp) Healthiness-condition where**
\[ \text{CSP4}(P) \equiv P ; ; \text{relation-of Skip} \]

**lemma Skip-is-CSP3: (relation-of Skip) is CSP3 healthy**
(\text{proof})

**lemma Skip-is-CSP4: (relation-of Skip) is CSP4 healthy**
(\text{proof})

**lemma Skip-comp-absorb: (relation-of Skip ; ; relation-of Skip) = relation-of Skip**
(\text{proof})

14.2 Stop

**definition Stop :: (′ϑ::ev-eq,′σ) action where**
\[ \text{Stop} \equiv \text{action-of} \ (R \text{ true } \vdash \lambda(A, A'). \text{tr } A' = \text{tr } A \land \text{wait } A') \]

**lemma Stop-is-action:**
\[ (R \text{ true } \vdash \lambda(A, A'). \text{tr } A' = \text{tr } A \land \text{wait } A') \in \{ p. \text{is-CSP-process } p \} \]
(\text{proof})

**lemmas Stop-is-CSP = Stop-is-action[simplified]**

**lemma relation-of-Stop:**
\[ \text{relation-of Stop} = (R \text{ true } \vdash \lambda(A, A'). \text{tr } A' = \text{tr } A \land \text{wait } A') \]
(\text{proof})
lemma Stop-is-CSP3: (relation-of Stop) is CSP3 healthy
(proof)

lemma Stop-is-CSP4: (relation-of Stop) is CSP4 healthy
(proof)

14.3 Chaos
definition Chaos :: (′ϑ::ev-eq,′σ) action
where Chaos ≡ action-of (R(false ⊢ true))

lemma Chaos-is-action: (R(false ⊢ true)) ∈ {p. is-CSP-process p}
(proof)

lemmas Chaos-is-CSP = Chaos-is-action[simplified]

lemma relation-of-Chaos: relation-of Chaos = (R(false ⊢ true))
(proof)

14.4 State update actions
definition Pre ::′σ relation ⇒ ′σ predicate
where Pre sc ≡ λA. ∃A′. sc (A, A′)

definition state-update-before ::′σ relation ⇒ (′ϑ::ev-eq,′σ) action ⇒ (′ϑ,′σ) action
where state-update-before sc Ac = action-of(R ((λ(A, A′). (Pre sc) (more A)) ⊢
(λ(A, A′). sc (more A, more A′) & ¬wait A′ & tr A = tr A′))
; ; relation-of Ac)

lemma state-update-before-is-action:
(R ((λ(A, A′). (Pre sc) (more A)) ⊢
(λ(A, A′).sc (more A, more A′) & ¬wait A′ & tr A = tr A′)) ; ; relation-of Ac) ∈ {p. is-CSP-process p}
(proof)

lemmas state-update-before-is-CSP = state-update-before-is-action[simplified]

lemma relation-of-state-update-before:
relation-of (state-update-before sc Ac) = (R ((λ(A, A′). (Pre sc) (more A)) ⊢
(λ(A, A′). sc (more A, more A′) & ¬wait A′ & tr A = tr A′)) ; ; relation-of Ac)
(proof)

lemma mono-state-update-before: mono (state-update-before sc)
(proof)

lemma state-update-before-is-CSP3: relation-of (state-update-before sc Ac) is CSP3 healthy

55
\textbf{lemma} state-update-before-is-CSP_4:
\begin{itemize}
\item \textbf{assumes} \( A : \text{relation-of } Ac \text{ is CSP}_4 \text{ healthy} \)
\item \textbf{shows} \( \text{relation-of } (\text{state-update-before sc Ac}) \text{ is CSP}_4 \text{ healthy} \)
\end{itemize}

\begin{proof}
\textbf{definition} state-update-after :: \( 'σ \text{ action } ⇒ (\text{relation-of Ac} ; ; \ R (\text{true } ⊢ (\lambda (A, A') \text{ sc } (\text{more A, more A'}) & \neg \text{wait A'} & \text{tr A } = \text{tr A}'))) \)
\begin{itemize}
\item \textbf{where} state-update-after sc Ac = action-of(relation-of Ac ; ; \ R (\text{true } ⊢ (\lambda (A, A'). \text{ sc } (\text{more A, more A'}) & \neg \text{wait A'} & \text{tr A } = \text{tr A}')))
\end{itemize}
\textbf{lemma} state-update-after-is-action:
\begin{itemize}
\item \( (\text{relation-of Ac} ; ; \ R (\text{true } ⊢ (\lambda (A, A'). \text{ sc } (\text{more A, more A'}) & \neg \text{wait A'} & \text{tr A } = \text{tr A}')))) \in \{ \text{p. is-CSP-process p} \}
\end{itemize}
\begin{proof}
\textbf{lemmas} state-update-after-is-CSP = state-update-after-is-action[simplified]
\end{proof}

\textbf{lemma} relation-of-state-update-after:
\begin{itemize}
\item \( \text{relation-of } (\text{state-update-after sc Ac}) = (\text{relation-of Ac} ; ; \ R (\text{true } ⊢ (\lambda (A, A'). \text{ sc } (\text{more A, more A'}) & \neg \text{wait A'} & \text{tr A } = \text{tr A}'))) \)
\end{itemize}
\begin{proof}
\textbf{lemma} mono-state-update-after: \textbf{mono} (state-update-after sc)
\begin{proof}
\end{proof}

\textbf{lemma} state-update-after-is-CSP_3:
\begin{itemize}
\item \textbf{assumes} \( A : \text{relation-of } Ac \text{ is CSP}_3 \text{ healthy} \)
\item \textbf{shows} \( \text{relation-of } (\text{state-update-after sc Ac}) \text{ is CSP}_3 \text{ healthy} \)
\end{itemize}
\begin{proof}
\textbf{lemma} state-update-after-is-CSP_4: \( \text{relation-of } (\text{state-update-after sc Ac}) \text{ is CSP}_4 \text{ healthy} \)
\begin{proof}
\end{proof}

\begin{section}{14.5 Sequential composition}
\textbf{definition} \( \text{Seq} : 'σ \text{ action } ⇒ (\text{relation-of } P \; ; \; \text{relation-of } Q) \)
\begin{itemize}
\item \textbf{where} \( P ; ; Q \equiv \text{action-of } (\text{relation-of } P \; ; \; \text{relation-of } Q) \)
\end{itemize}
\textbf{lemma} \( \text{Seq-is-action}: (\text{relation-of } P \; ; \; \text{relation-of } Q) \in \{ \text{p. is-CSP-process p} \} \)
\begin{proof}
\textbf{lemmas} \( \text{Seq-is-CSP} = \text{Seq-is-action[simplified]} \)
\end{proof}
\end{section}
lemma relation-of-Seq: relation-of \((P ;' Q)\) = (relation-of P ; relation-of Q)
⟨proof⟩

lemma mono-Seq: mono \((op ;' P)\)
⟨proof⟩

lemma CSP3-imp-left-Skip:
\[\text{assumes } A: \text{relation-of } P \text{ is } \text{CSP3 healthy}\]
\[\text{shows } (\text{Skip} ;' P) = P\]
⟨proof⟩

lemma CSP4-imp-right-Skip:
\[\text{assumes } A: \text{relation-of } P \text{ is } \text{CSP4 healthy}\]
\[\text{shows } (P ;' \text{Skip}) = P\]
⟨proof⟩

lemma Seq-assoc: \((A ;' (B ;' C))\) = ((A ;' B) ;' C)
⟨proof⟩

lemma Skip-absorb: \((\text{Skip} ;' \text{Skip})\) = \(\text{Skip}\)
⟨proof⟩

14.6 Internal choice

definition
\[Ndet::('\theta::ev-eq,'\sigma) \text{ action } \Rightarrow ('\theta,'\sigma) \text{ action } \Rightarrow ('\theta,'\sigma) \text{ action} \ (\text{infixl } \cap 18)\]
\[\text{where } P \cap Q \equiv \text{action-of } ((\text{relation-of } P) \lor (\text{relation-of } Q))\]

lemma Ndet-is-action: \(((\text{relation-of } P) \lor (\text{relation-of } Q)) \in \{p. \text{is-CSP-process } p\}\)
⟨proof⟩

lemmas Ndet-is-CSP = Ndet-is-action[simplified]

lemma relation-of-Ndet: relation-of \((P \cap Q)\) = ((relation-of P) \lor (relation-of Q))
⟨proof⟩

lemma mono-Ndet: mono \((op \cap P)\)
⟨proof⟩

14.7 External choice

definition
\[Det::('\theta::ev-eq,'\sigma) \text{ action } \Rightarrow ('\theta,'\sigma) \text{ action } \Rightarrow ('\theta,'\sigma) \text{ action} \ (\text{infixl } [+] 18)\]
\[\text{where } P [+ Q \equiv \text{action-of}(R((\neg((\text{relation-of } P)'_f) \land \neg((\text{relation-of } Q)'_f)) \vdash ((\text{relation-of } P)'_f \land ((\text{relation-of } Q)'_f))\]
\[\land \lambda (A, A'). tr A = tr A' \land \text{wait } A'\lor ((\text{relation-of } P)'_f \lor ((\text{relation-of } Q)'_f))))\]

notation(xsymbol)
lemma Det-is-action: 
\[(R((\neg((\text{relation-of } P)^f_1) \land \neg((\text{relation-of } Q)^f_1)) \vdash ((\text{relation-of } P)^f_1 \land \text{(relation-of } Q)^f_1)) \land \lambda(A, A'). \text{tr } A = \text{tr } A' \land \text{wait } A' \triangleright ((\text{relation-of } P)^f_1 \lor ((\text{relation-of } Q)^f_1)))]) \in \{p. \text{is-CSP-process } p\}\]

(proof)

lemmas Det-is-CSP = Det-is-action[simplified]

lemma relation-of-Det: 
\[\text{relation-of } (P \sqcap Q) = (R((\neg((\text{relation-of } P)^f_1) \land \neg((\text{relation-of } Q)^f_1)) \vdash ((\text{relation-of } P)^f_1 \land \text{(relation-of } Q)^f_1)) \land \lambda(A, A'). \text{tr } A = \text{tr } A' \land \text{wait } A' \triangleright ((\text{relation-of } P)^f_1 \lor ((\text{relation-of } Q)^f_1)))])\]

(proof)

lemma mono-Det: mono (op \([+]\) P)

(proof)

14.8 Reactive design assignment

definition rd-assign s = action-of (R (true \vdash \lambda(A, A'). \text{ref } A' = \text{ref } A \land \text{tr } A' = \text{tr } A \land \neg \text{wait } A' \land \text{more } A' = s))

lemma rd-assign-is-action: 
\[(R (\text{true } \vdash \lambda(A, A'). \text{ref } A' = \text{ref } A \land \text{tr } A' = \text{tr } A \land \neg \text{wait } A' \land \text{more } A' = s)) \in \{p. \text{is-CSP-process } p\}\]

(proof)

lemmas rd-assign-is-CSP = rd-assign-is-action[simplified]

lemma relation-of-rd-assign: 
\[\text{relation-of } (\text{rd-assign } s) = (R (\text{true } \vdash \lambda(A, A'). \text{ref } A' = \text{ref } A \land \text{tr } A' = \text{tr } A \land \neg \text{wait } A' \land \text{more } A' = s))\]

(proof)

14.9 Local state external choice

definition Loc::'σ ⇒ ('ψ::ev-eq,'σ) action ⇒ ('σ ⇒ (\'δ,'σ) action ⇒ ('δ,'σ) action

\[(\text{loc } \cdots \cdots) ≡ \text{('}\text{loc } \cdots \cdots\text{'})\]

where (loc s1 \(\triangleleft\) P) \(\triangleleft\) (loc s2 \(\triangleleft\) Q) ≡ 
\[(\text{((rd-assign s1)'}, P) □ ((\text{rd-assign s2}')}, Q)\]

58
14.10 Schema expression

**definition** Schema :: 'σ relation ⇒ ('∅::ev-eq,'σ) action where

\[ \text{Schema sc} \equiv \text{action-of}(R ((\lambda(A, A'). (\text{Pre sc}) (\text{more } A)) \mapsto (\lambda(A, A'). \text{sc} (\text{more } A, \text{more } A') \land \lnot\text{wait } A' \land tr A = tr A'))) \]

**lemma** Schema-is-action:

\[ (R ((\lambda(A, A'). (\text{Pre sc}) (\text{more } A)) \mapsto (\lambda(A, A'). \text{sc} (\text{more } A, \text{more } A') \land \lnot\text{wait } A' \land tr A = tr A'))) \in \{p. \text{is-CSP-process } p\} \]

(proof)

**lemmas** Schema-is-CSP = Schema-is-action[simplified]

**lemma** relation-of-Schema:

\[ \text{relation-of } \text{(Schema sc)} = (R ((\lambda(A, A'). (\text{Pre sc}) (\text{more } A)) \mapsto (\lambda(A, A'). \text{sc} (\text{more } A, \text{more } A') \land \lnot\text{wait } A' \land tr A = tr A'))) \]

(proof)

**lemma** Schema-is-state-update-before: Schema u = state-update-before u Skip

(proof)

14.11 Parallel composition

**type-synonym** σ local-state = (σ × ('σ ⇒ 'σ ⇒ 'σ))

**fun** MergeSt :: 'σ local-state ⇒ 'σ local-state ⇒ ('∅,'σ) relation-rp where

\[ \text{MergeSt } (s1,s1') (s2,s2') = ((\lambda(S, S'). (s1' s1') (\text{more } S) = \text{more } S'); \]

\[ (\lambda(S:(\emptyset,'σ) \text{alphabet-rp}, S'). (s2' s2') (\text{more } S) = \text{more } S')) \]

**definition** listCons ::'∅ ⇒ '∅ list list ⇒ '∅ list list (- ## -) where

\[ a ## l = ((\text{map } (\text{Cons } a)) l) \]

**fun** ParMergel :: '∅::ev-eq list ⇒ '∅ list ⇒ '∅ set ⇒ '∅ list list where

| ParMergel [] [] cs = [] |
| ParMergel (b#tr2) cs = (if (filter-chan-set b cs) then [] else (b ## (ParMergel [] tr2 cs))) |
| ParMergel (a#tr1) [] cs = (if (filter-chan-set a cs) then [] else (a ## (ParMergel tr1 [] cs))) |
| ParMergel (a#tr1) (b#tr2) cs = |
| \[ \text{if } (\text{filter-chan-set } a \text{ cs}) \text{ then } (\text{if } (\text{ev-eq } a b) \text{ then } (a ## (ParMergel tr1 tr2 cs)) \text{ else } (\text{if } (\text{filter-chan-set } b \text{ cs}) \text{ then } []) \text{ else } (b ## (ParMergel (a#tr1) tr2 cs))) \text{ else } (a ## (ParMergel tr1 (b#tr2) cs)) \text{ else } (a ## (ParMergel tr1 (b#tr2) cs)) \text{ & } (b ## (ParMergel (a#tr1) tr2 cs))) \] |
definition ParMerge::"\theta::ev-eq list \Rightarrow \theta list \Rightarrow \theta set \Rightarrow \theta list set" where
ParMerge tr1 tr2 cs = set (ParMerge tr1 tr2 cs)

lemma set-Cons1: tr1 \in set l \implies a \neq tr1 \in op \# a \# set l
(proof)

lemma tr-in-set-eq: (tr1 \in op \# b \# set l) = (tr1 \neq [] \land \land tr1 = b \land tl tr1 \in set l)
(proof)

definition M-par::"(\theta::ev-eq, \sigma) alpha-rp-scheme \Rightarrow (\sigma \Rightarrow \sigma \Rightarrow \sigma)
\Rightarrow (\theta, \sigma) alpha-rp-scheme \Rightarrow (\sigma \Rightarrow \sigma \Rightarrow \sigma)
\Rightarrow (\theta, \sigma) relation-rp where
M-par s1 x1 s2 x2 cs =
((\lambda(S, S'). ((diff-tr s' S) \in ParMerge (diff-tr s1 S) (diff-tr s2 S) cs & ev-eq (tr-filter (tr s1) cs) (tr-filter (tr s2) cs))) \land
((\lambda(S, S'). (wait s1 \lor wait s2) \land
ref S' \subseteq (((ref s1)\cup(ref s2))\cup(((ref s1)\cap(ref s2))\cup-(cs))))
\land wait o snd \lor
((\lambda(S, S'). (\neg wait s1 \lor \neg wait s2)) \land MergeSt ((more s1), x1) ((more s2), x2))))

definition Par::"(\theta::ev-eq, \sigma) action \Rightarrow
(\sigma \Rightarrow \sigma \Rightarrow \sigma) \Rightarrow \theta set \Rightarrow \sigma \Rightarrow \sigma \Rightarrow \sigma)
(\theta, \sigma) action \Rightarrow (\theta, \sigma) action (- [- - -] -) where
A1 \parallel ns1 | cs \parallel ns2 \parallel A2 \equiv (action-of (R ((\lambda(S, S').
\neg (\exists tr1 tr2. ((relation-of A1)_f ; (\lambda(S, S'). tr1 = (tr S))) (S, S'))
\land (spec False (wait S) (relation-of A2) ; ; (\lambda(S, -). tr2 = (tr S))) (S, S'))
\land ((tr-filter tr1 cs) = (tr-filter tr2 cs))) \land
\neg (\exists tr1 tr2. (spec False (wait S) (relation-of A1); ; (\lambda(S, S'). tr1 = (tr S))) (S, S'))
\land ((relation-of A2)_f ; ; (\lambda(S, S'). tr2 = (tr S))) (S, S')
\land ((tr-filter tr1 cs) = (tr-filter tr2 cs))) \parallel
(\lambda(S, S'). \exists s2. (((\lambda(A, A'). (relation-of A1)_f (A, s1)
\land ((relation-of A2)_f (A, s2)) ; ; M-par s1 ns1 s2 ns2 cs (S, S'))))))

lemma Par-is-action: (R ((\lambda(S, S').
\neg (\exists tr1 tr2. ((relation-of A1)_f ; ; (\lambda(S, S'). tr1 = (tr S))) (S, S'))
\land (spec False (wait S) (relation-of A2) ; ; (\lambda(S, S'). tr2 = (tr S))) (S, S'))
\land ((tr-filter tr1 cs) = (tr-filter tr2 cs))) \land
\neg (\exists tr1 tr2. (spec False (wait S) (relation-of A1); ; (\lambda(S, S'). tr1 = (tr S))) (S, S'))
\land ((relation-of A2)_f ; ; (\lambda(S, S'). tr2 = (tr S))) (S, S')
\land ((tr-filter tr1 cs) = (tr-filter tr2 cs))) \parallel
(\lambda(S, S'). \exists s2. (((\lambda(A, A'). (relation-of A1)_f (A, s1)
\land ((relation-of A2)_f (A, s2)); ; M-par s1 ns1 s2 ns2 cs (S, S')))))) \in \{p.
is-CSP-process p\}
(proof)
lemmas\ Par-is-CSP = Par-is-action[simplified]

lemma\ relation-of-Par:
relation-of\ \{A1 \parallel ns1 | cs | ns2 \parallel A2\} = (R ((\lambda (S, S')).
\neg (\exists tr1 tr2. ((relation-of A1)\subseteq | (\lambda (S, S'). tr1 = (tr S)) (S, S'))
\land (\spec False (\wait S) (relation-of A2)) ; ; (\lambda (S, S'). tr2 = (tr S)) (S, S'))
\land ((tr-filter tr1 cs) = (tr-filter tr2 cs))\} \land
\neg (\exists tr1 tr2. (\spec False (\wait S) (relation-of A1)); ; (\lambda (S, \cdot). tr1 = tr S)) (S, S'))
\land \neg \ land \neg \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \land \lang...
lemma Assign-is-state-update-before: \text{ASSIGN } x e = \text{state-update-before } (\lambda \ (s, s') \ . \ s' = (\text{update } x \ (\lambda \cdot \ (e \ s))) \ s) \ \text{Skip}

\langle proof \rangle

14.14 Variable scope

definition Var::('v, 'σ) var-list \Rightarrow ('θ, 'σ) action \Rightarrow ('θ::ev-eq,'σ) action where
Var v A \equiv \text{action-of(}
\begin{align*}
(R(true \vdash (\lambda \ (A, A')). \exists \ a. \ tr A' = tr A \land \neg\text{wait} A' \land more A' = (increase v a \ (more A))))); \\
(\text{relation-of } A); \\
(R(true \vdash (\lambda \ (A, A')). \ tr A' = tr A \land \neg\text{wait} A' \land more A' = (decrease v \ (more A)))))
\end{align*}
\)
syntax -var::idt \Rightarrow ('θ, 'σ) action \Rightarrow ('θ, 'σ) action (\text{var - \bullet - [1000] 999})
translations \text{var y \bullet Act} = \text{CONST Var (VAR-LIST y) Act}

lemma Var-is-action:
\begin{align*}
(\langle (R(true \vdash (\lambda \ (A, A')). \exists \ a. \ tr A' = tr A \land \neg\text{wait} A' \land more A' = (increase v a \ (more A))))); \\
(\text{relation-of } A); \\
(R(true \vdash (\lambda \ (A, A')). \ tr A' = tr A \land \neg\text{wait} A' \land more A' = (decrease v \ (more A))))) \rangle \in \{p. \text{is-CSP-process } p\}
\end{align*}
\langle proof \rangle

lemmas Var-is-CSP = Var-is-action[simplified]

lemma relation-of-Var:
\begin{align*}
\text{relation-of } (Var \ v A) = \\
(\langle (R(true \vdash (\lambda \ (A, A')). \exists \ a. \ tr A' = tr A \land \neg\text{wait} A' \land more A' = (increase v a \ (more A))))); \\
(\text{relation-of } A); \\
(R(true \vdash (\lambda \ (A, A')). \ tr A' = tr A \land \neg\text{wait} A' \land more A' = (decrease v \ (more A)))))
\end{align*}
\langle proof \rangle

lemma mono-Var : mono (Var x)
\langle proof \rangle

definition Let::('v, 'σ) var-list \Rightarrow ('θ, 'σ) action \Rightarrow ('θ::ev-eq,'σ) action where
Let v A \equiv \text{action-of(}
\begin{align*}
(R(true \vdash (\lambda \ (A, A')). \ tr A' = tr A \land \neg\text{wait} A' \land more A' = (decrease v \ (more A))))); \\
(\text{relation-of } A); \\
(R(true \vdash (\lambda \ (A, A')). \ tr A' = tr A \land \neg\text{wait} A' \land more A' = (decrease v \ (more A)))))
\end{align*}
\)
syntax -let::idt \Rightarrow ('θ, 'σ) action \Rightarrow ('θ, 'σ) action (\text{let - \bullet - [1000] 999})
translations \text{let y \bullet Act} = \text{CONST Let (VAR-LIST y) Act}

62
lemma Let-is-action:
\[ \text{relation-of } A; ; \]
\[ (R(\text{true} \vdash (\lambda (A, A'). \text{tr } A' = \text{tr } A \land \neg \text{wait } A' \land \text{more } A' = (\text{decrease } v \text{ (more } A))))) \in \{ \text{p. is-CSP-process } p \} \]
\( \langle \text{proof} \rangle \)

lemmas Let-is-CSP = Let-is-action[simplified]

lemma relation-of-Let:
\[ \text{relation-of (Let } v A) = \]
\[ (R(\text{true} \vdash (\lambda (A, A'). \text{tr } A' = \text{tr } A \land \neg \text{wait } A' \land \text{more } A' = (\text{decrease } v \text{ (more } A))))) \]
\( \langle \text{proof} \rangle \)

lemma mono-Let : mono (Let x)
\( \langle \text{proof} \rangle \)

lemma Var-is-state-update-before: Var v A = state-update-before (λ (s, s'). ∃ a. s' = increase v a s) (Let v A)
\( \langle \text{proof} \rangle \)

lemma Let-is-state-update-after: Let v A = state-update-after (λ (s, s'). s' = decrease v s) A
\( \langle \text{proof} \rangle \)

14.15 Guarded action

definition Guard::σ predicate ⇒ ('σ::ev-eq, 'σ) action ⇒ ('σ, 'σ) action (- 'κ -)
where g 'κ·P ≡ action-of (R (((g o more o fst) → ¬ ((relation-of P)'f)) \vdash
\[ (((g o more o fst) \land ((relation-of P)'f)) \lor
\[ ((\neg (g o more o fst)) \land (\lambda (A, A'). \text{tr } A' = \text{tr } A \land \text{wait } A')))))) \]

lemma Guard-is-action:
\[ (R ( (((g o more o fst) → ¬ ((relation-of P)'f)) \vdash
\[ (((g o more o fst) \land ((relation-of P)'f)) \lor
\[ ((\neg (g o more o fst)) \land (\lambda (A, A'). \text{tr } A' = \text{tr } A \land \text{wait } A')))))) \in \{ \text{p. is-CSP-process } p \} \]
\( \langle \text{proof} \rangle \)

lemmas Guard-is-CSP = Guard-is-action[simplified]

lemma relation-of-Guard:
\[ \text{relation-of (g 'κ·P) = (R (((g o more o fst) → ¬ ((relation-of P)'f)) \vdash
\[ (((g o more o fst) \land ((relation-of P)'f)) \lor
\[ ((\neg (g o more o fst)) \land (\lambda (A, A'). \text{tr } A' = \text{tr } A \land \text{wait } A')))))) \]

63
lemma mono-Guard : mono (Guard g)
(proof)

lemma false-Guard: false '∧· P = Stop
(proof)

lemma false-Guard1: \( \bigwedge \ a \ b \ g \ (\text{alpha-rp}.more \ a) = \text{False} \implies \text{(relation-of (g '∧· P))} (a, b) = \text{(relation-of Stop)} (a, b) \)
(proof)

lemma true-Guard: true '∧· P = P
(proof)

lemma true-Guard1: \( \bigwedge \ a \ b \ g \ (\text{alpha-rp}.more \ a) = \text{True} \implies \text{(relation-of (g '∧· P))} (a, b) = \text{(relation-of P)} (a, b) \)
(proof)

lemma Guard-is-state-update-before: g '∧· P = state-update-before (λ (s, s') . g s) P
(proof)

14.16 Prefixed action

definition do where
doce \equiv (λ(A, A'). \text{tr} A = \text{tr} A' \land (e \ (\text{more} \ A)) \notin (\text{ref} A') \triangleleft \text{wait} o \text{snd} \triangleright \text{(λ(A, A'). tr} A' = (\text{tr} A @[[e \ (\text{more} \ A)]]) )

definition do-I: ('σ \Rightarrow \varnothing) \Rightarrow \varnothing \text{ set} \Rightarrow (\varnothing, 'σ) \text{ relation-rp}
where
doe c S \equiv ((λ(A, A'). \text{tr} A = \text{tr} A' \land S \cap (\text{ref} A') = \{\})
\triangleleft \text{wait} o \text{snd} \triangleright
(λ(A, A'). \text{hd} (\text{tr} A' - \text{tr} A) \in S \land (c \ (\text{more} \ A) = (\text{last} (\text{tr} A')))))

definition iPrefix:('σ \Rightarrow \varnothing; ev-eq) \Rightarrow (\text{relation}) \Rightarrow ((\varnothing, 'σ) \text{ action} \Rightarrow (\varnothing, 'σ) \text{ action}) \Rightarrow (\varnothing \Rightarrow \varnothing \text{ set}) \Rightarrow (\varnothing, 'σ) \text{ action} \Rightarrow (\varnothing, 'σ) \text{ action where}
iPrefix c i j S P \equiv \text{action-of(R(true \vdash (λ (A, A'), (do-I c (S (\text{more} A)) (A, A') \& \text{more} A' = more A)))'; 'P}

definition oPrefix:('σ \Rightarrow \varnothing) \Rightarrow (\varnothing; ev-eq, 'σ) \text{ action} \Rightarrow (\varnothing, 'σ) \text{ action where}
oPrefix c P \equiv \text{action-of(R(true \vdash (do c) \land (λ (A, A'), more A' = more A)))'; 'P}

definition Prefix0: 'σ \Rightarrow (\varnothing; ev-eq, 'σ) \text{ action} \Rightarrow (\varnothing, 'σ) \text{ action where}
Prefix0 c P \equiv \text{action-of(R(true \vdash (do (λ - c)) \land (λ (A, A'), more A' = more A))'; 'P}

64
definition
read::('v ⇒ 'θ) ⇒ ('v, 'σ) var-list ⇒ ('θ::ev-eq, 'σ) action ⇒ ('θ, 'σ) action
where read c x P ≡ iPrefix (λ A. c (select x A)) (λ (s, s'). ∃ a. s' = increase x a s) (Let x) (λ-. range c) P

definition
read1::('v ⇒ 'θ) ⇒ ('v, 'σ) var-list ⇒ ('σ ⇒ 'e set) ⇒ ('θ::ev-eq, 'σ) action ⇒ ('θ, 'σ) action
where read1 c x S P ≡ iPrefix (λ A. c (select x A)) (λ (s, s'). ∃ a. a∈(S s) & s' = increase x a s) (Let x) (λs. c'(S s)) P

definition
write1::'v ⇒ ('θ::ev-eq, 'σ) action ⇒ ('θ, 'σ) action
where write1 c a P ≡ oPrefix (λ A. c (a A)) P

definition
write0::'v ⇒ ('θ::ev-eq, 'σ) action ⇒ ('θ, 'σ) action
where write0 c P ≡ Prefix0 c P

syntax
-readable ::[id, pttrn, ('θ, 'σ) action] => ('θ, 'σ) action ((-?/: / −)/-)
-readableSS ::[id, pttrn, 'θ set,('θ, 'σ) action] => ('θ, 'σ) action ((-?/-/: / −)/-)
-readableSS ::[id, pttrn, 'θ set,('θ, 'σ) action] => ('θ, 'σ) action ((-?/-/: / −)/-)
-write ::[id, 'σ, ('θ, 'σ) action] => ('θ, 'σ) action ((-!/: / −)/-)
-writeSS ::[id, 'σ, ('θ, 'σ) action] => ('θ, 'σ) action ((-!/: / −)/-)

translations
-readable c p P == CONST read c (VAR-LIST p) P
-readable c p b P == CONST read1 c (VAR-LIST p) (λ-. b) P
-readable c p b P == CONST read1 c (VAR-LIST p) b P
-write c p P == CONST write1 c p P
-writeSS a P == CONST write0 a P

lemma Prefix-is-action:
(R(true ⊨ (do c) ∧ (λ ⟨A, A'⟩. more A' = more A))) ∈ {p. is-CSP-process p}
(proof)

lemma Prefix1-is-action:
(R(true ⊨ (λ(A, A'). do-I c (S (alpha-rp.more A)) (A, A') ∧ alpha-rp.more A' = alpha-rp.more A)) ∈ {p. is-CSP-process p}
(proof)

lemma Prefix0-is-action:
(R(true ⊨ (do c) ∧ (λ ⟨A, A'⟩. more A' = more A))) ∈ {p. is-CSP-process p}
(proof)
lemmas Prefix-is-CSP = Prefix-is-action[simplified]

lemmas Prefix1-is-CSP = Prefix1-is-action[simplified]

lemmas Prefix0-is-CSP = Prefix0-is-action[simplified]

lemma relation-of-iPrefix:
relation-of (iPrefix c i j S P) =
((R(true ⊢ (λ (A, A'). (do-I c (S (more A))) (A, A') & more A' = more A))); relation-of P)
⟨proof⟩

lemma relation-of-oPrefix:
relation-of (oPrefix c P) =
((R(true ⊢ (do c) ∧ (λ (A, A'). more A' = more A))); relation-of P)
⟨proof⟩

lemma relation-of-Prefix0:
relation-of (Prefix0 c P) =
((R(true ⊢ (do (λ - . c)) ∧ (λ (A, A'). more A' = more A))); relation-of P)
⟨proof⟩

lemma mono-iPrefix : mono (iPrefix c i j s)
⟨proof⟩

lemma mono-oPrefix : mono (oPrefix c)
⟨proof⟩

lemma mono-Prefix0 : mono(Prefix0 c)
⟨proof⟩

14.17 Hiding

definition Hide::('θ::ev-eq, 'σ) action ⇒ 'θ set ⇒ ('θ, 'σ) action (infixl \ 18) where
P \ cs ≡ action-of(R(λ(S, S'). ∃ s. (diff-tr S' S) = (tr-filter (s - (tr S)) cs) &
(relation-of P)(S, S'(tr := s, ref := (ref S') ∪ cs [];)); (relation-of Skip))

definition
hid P cs := (R(λ(S, S'). ∃ s. (diff-tr S' S) = (tr-filter (s - (tr S)) cs) &
(relation-of P)(S, S'(tr := s, ref := (ref S') ∪ cs [];)); (relation-of Skip))

lemma hid-is-R: hid P cs is R healthy
⟨proof⟩

lemma hid-Skip: hid P cs = (hid P cs ; ; relation-of Skip)
(proof)

lemma hid-is-CSP1: hid P cs is CSP1 healthy
(proof)

lemma hid-is-CSP2: hid P cs is CSP2 healthy
(proof)

lemma hid-is-CSP: is-CSP-process (hid P cs)
(proof)

lemma Hide-is-action:
\[
(R(\lambda(S, S'). \exists s. (diff-tr S' S) = (tr-filter (s - (tr S)) cs) &
(relation-of P)(S, S'(\text{tr} := s, \text{ref} := (\text{ref} S') \cup cs)))\); \ (relation-of Skip)) \in \{p. is-CSP-process p\}
\]
(proof)

lemmas Hide-is-CSP = Hide-is-action[simplified]

lemma relation-of-Hide:
relation-of (P \ cs) = (R(\lambda(S, S'). \exists s. (diff-tr S' S) = (tr-filter (s - (tr S)) cs)
& (relation-of P)(S, S'(\text{tr} := s, \text{ref} := (\text{ref} S') \cup cs)))\); \ (relation-of Skip))
(proof)

lemma mono-Hide : mono(\lambda P. P \ cs)
(proof)

14.18 Recursion

To represent the recursion operator "\(\mu\)" over actions, we use the universal
least fix-point operator "\(\text{lfp}\)" defined in the HOL library for lattices. The
operator "\(\text{lfp}\)" is inherited from the "Complete Lattice class" under some
conditions. All theorems defined over this operator can be reused.

In the Circus-Actions theory, we presented the proof that Circus actions
form a complete lattice. The Knaster-Tarski Theorem (in its simplest for-
mulation) states that any monotone function on a complete lattice has a least
fixed-point. This is a consequence of the basic boundary properties of the
complete lattice operations. Instantiating the complete lattice class allows
one to inherit these properties with the definition of the least fixed-point for
monotonic functions over Circus actions.

syntax -MU::[idt, idt] \Rightarrow ('\theta, '\sigma) action \Rightarrow ('\theta, '\sigma) action (\mu - \bullet -)
translations -MU X P == CONST \text{lfp} (\lambda X. P)
(proof)(proof)end
15  Circus syntax

theory Circus-Syntax
imports Denotational-Semantics
keywords alphabet state channel nameset chanset schema action and
   circus-process :: thy-decl
begin

abbreviation list-select::[′r ⇒ ′a list] ⇒ (′r ⇒ ′a) where
   list-select Sel ≡ hd o Sel

abbreviation list-update::[(′a list ⇒ ′a list) ⇒ ′r ⇒ ′r] ⇒ (′a ⇒ ′a) ⇒ ′r ⇒ ′r where
   list-update Upd ≡ λ e. Upd (λ l. (e (hd l))#(tl l))

abbreviation list-update-const::[(′a list ⇒ ′a list) ⇒ ′r ⇒ ′r] ⇒ (′a ⇒ ′a list ⇒ ′r ⇒ ′r) where
   list-update-const Upd ≡ λ e. λ (A, A'). A' = Upd (λ l. e#(tl l)) A

abbreviation update-const::[(′a ⇒ ′a) ⇒ ′r ⇒ ′r] ⇒ (′a ⇒ ′r relation where
   update-const Upd ≡ λ e. λ (A, A'). A' = Upd (λ - e) A

syntax
   -syt-assign :: id ⇒ ′a ⇒ ′b relation (- := -)

⟨ML⟩

nonterminal circus-action and circus-schema

syntax
   -circus-action :: ′a => circus-action (-)
   -circus-schema :: ′a => circus-schema (-)

⟨ML⟩

end

16  Refinement and Simulation

theory Refinement
imports Denotational-Semantics Circus-Syntax
begin

16.1  Definitions

In the following, data (state) simulation and functional backwards simulation are defined. The simulation is defined as a function S, that corresponds
to a state abstraction function.

**definition** Simul $S$ $b = \text{extend (make (ok $b$) (wait $b$) (tr $b$) (ref $b$)) (S (more $b$))}

**definition** Simulation :: ($\theta$::ev-eq,$\sigma$) action $\Rightarrow$ ($\sigma 1 \Rightarrow \sigma$) $\Rightarrow$ ($\theta$, $\sigma 1$) action $\Rightarrow$ bool ( - $\preceq$ - )

where

$A \preceq S B \equiv \forall a\, b.\text{ (relation-of B) (a, b) }\rightarrow\text{ (relation-of A) (Simul S a, Simul S b)}$

### 16.2 Proofs

In order to simplify refinement proofs, some general refinement laws are defined to deal with the refinement of Circus actions at operators level and not at UTP level. Using these laws, and exploiting the advantages of a shallow embedding, the automated proof of refinement becomes surprisingly simple.

**lemma** Stop-Sim: $\text{Stop} \preceq S \text{Stop}$

**lemma** Skip-Sim: $\text{Skip} \preceq S \text{Skip}$

**lemma** Chaos-Sim: $\text{Chaos} \preceq S \text{Chaos}$

**lemma** Ndet-Sim:

assumes $A$: $P \preceq S Q$ and $B$: $P' \preceq S Q'$

shows $(P \cap P') \preceq S (Q \cap Q')$

**lemma** Det-Sim:

assumes $A$: $P \preceq S Q$ and $B$: $P' \preceq S Q'$

shows $(P \cap P') \preceq S (Q \cap Q')$

**lemma** Schema-Sim:

assumes $A$: $\bigwedge a.\text{ (Pre sc1) (S a) }\Rightarrow\text{ (Pre sc2) a}$

and $B$: $\bigwedge a b.\text{ [Pre sc1 (S a) ; sc2 (a, b)] }\Rightarrow\text{ sc1 (S a, S b) }$

shows $(\text{Schema sc1}) \preceq S (\text{Schema sc2})$

**lemma** Sub-Sim:

assumes $A$: $\bigwedge a.\text{ (Pre sc1) (S a) }\Rightarrow\text{ (Pre sc2) a}$

and $B$: $\bigwedge a b.\text{ [Pre sc1 (S a) ; sc2 (a, b)] }\Rightarrow\text{ sc1 (S a, S b) }$

and $C$: $P \preceq S Q$

shows $(\text{state-update-before sc1 P}) \preceq S (\text{state-update-before sc2 Q})$
lemma **Seq-Sim**:  
assumes $A: P \preceq_S Q$ and $B: P' \preceq_S Q'$  
shows $(P \cdot; P') \preceq_S (Q \cdot; Q')$

⟨proof⟩

lemma **Par-Sim**:  
assumes $A: P \preceq_S Q$ and $B: P' \preceq_S Q'$  
and $C: \forall a b. S (ns' a) (ns 2 a b) = ns2 (S a) (S b)$  
and $D: \forall a b. S (ns'1 a b) = ns1 (S a) (S b)$  
shows $(P \parallel ns1 \mid cs \parallel ns2 \parallel P') \preceq_S (Q \parallel ns'1 \mid cs \parallel ns'2 \parallel Q')$

⟨proof⟩

lemma **Assign-Sim**:  
assumes $A: \forall A. vy A = vx (S A)$  
and $B: \forall ff A. (S (y-update ff A)) = x-update ff (S A)$  
shows $(x := ' vx) \preceq_S (y := ' vy)$

⟨proof⟩

lemma **Var-Sim**:  
assumes $A: P \preceq_S Q$ and $B: \forall ff A. (S ((snd b) ff A)) = (snd a) ff (S A)$  
shows $(\text{Var } a P) \preceq_S (\text{Var } b Q)$

⟨proof⟩

lemma **Guard-Sim**:  
assumes $A: P \preceq_S Q$ and $B: \forall A. h A = g (S A)$  
shows $(g \& ' P) \preceq_S (h \& ' Q)$

⟨proof⟩

lemma **Write0-Sim**:  
assumes $A: P \preceq_S Q$  
shows $a \rightarrow P \preceq_S a \rightarrow Q$

⟨proof⟩

lemma **Read-Sim**:  
assumes $A: P \preceq_S Q$ and $B: \forall A. (d A) = c (S A)$  
shows $a'?'c' \rightarrow P \preceq_S a'?'d \rightarrow Q$

⟨proof⟩

lemma **Read1-Sim**:  
assumes $A: P \preceq_S Q$ and $B: \forall A. (d A) = c (S A)$  
shows $a'?'c'':s \rightarrow P \preceq_S a'?'d'':s \rightarrow Q$

⟨proof⟩

lemma **Read1S-Sim**:  
assumes $A: P \preceq_S Q$ and $B: \forall A. (d A) = c (S A)$ and $C: \forall A. (s' A) = s (S A)$  
shows $a'?'c'\in's \rightarrow P \preceq_S a'?'d'\in's' \rightarrow Q$

⟨proof⟩

70
lemma Write-Sim:  
assumes A: P ⪯ S Q and B: A. (d A) = c (S A)  
shows a¹c → P ⪯ S a¹d → Q  
⟨proof⟩

lemma Hide-Sim:  
assumes A: P ⪯ S Q  
shows (P \ cs) ⪯ S (Q \ cs)  
⟨proof⟩

lemma lfp-Siml:  
assumes A: ⋀ X. (X ⪯ S Q) ⇒ ((P X) ⪯ S Q) and B: mono P  
shows (lfp P) ⪯ S Q  
⟨proof⟩

lemma Mu-Sim:  
assumes A: ⋀ X Y. X ⪯ S Y =⇒ (P X) ⪯ S (Q Y) and B: mono P and C: mono Q  
shows (lfp P) ⪯ S (lfp Q)  
⟨proof⟩

lemma bot-Sim: bot ⪯ S bot  
⟨proof⟩

lemma sim-is-ref: P ⊑ Q = P ⪯ (id) Q  
⟨proof⟩

lemma ref-eq: ((P::(a::ev-eq,'b) action) = Q) = (P ⊑ Q & Q ⊑ P)  
⟨proof⟩

lemma rd-ref:  
assumes A:R (P ⊢ Q) ∈ {p. is-CSP-process p}  
and B:R (P' ⊢ Q') ∈ {p. is-CSP-process p}  
and C: ⋀ a b. P (a, b) =⇒ P' (a, b)  
and D: ⋀ a b. Q (a, b) =⇒ Q' (a, b)  
shows (action-of (R (P ⊢ Q))) ⊆ (action-of (R (P' ⊢ Q')))  
⟨proof⟩

lemma rd-impl:  
assumes A:R (P ⊢ Q) ∈ {p. is-CSP-process p}  
and B:R (P' ⊢ Q') ∈ {p. is-CSP-process p}  
and C: ⋀ a b. P (a, b) =⇒ P' (a, b)  
and D: ⋀ a b. Q (a, b) =⇒ Q' (a, b)  
shows R (P' ⊢ Q') (a, b) =⇒ R (P ⊢ Q) (a::(a::ev-eq,'b) alpha-rp-scheme, b)  
⟨proof⟩

end
17 Concrete example

theory Refinement-Example
imports Refinement
begin

In this section, we present a concrete example of the use of our environment. We define two Circus processes FIG and DFIG, using our syntax. We give the proof of refinement (simulation) of the first process by the second one using the simulation function $\text{Sim}$.

17.1 Process definitions

circus-process FIG =
  alphabet = [v::nat, x::nat]
  state = [idS::nat set]
  channel = [out nat, req, ret nat]
  schema Init = idS' = {}
  schema Out = $\exists$ a. $v'$ = a $\land$ a $\notin$ idS $\land$ idS' = idS $\cup$ {$v'$}
  schema Remove = $x$ $\in$ idS $\land$ idS' = idS $-$ {$x$}

where var $v$ • (Schema FIG.Init'; $\mu X$ • (((req $\rightarrow$ (Schema FIG.Out))'; $\text{out}!\cdot(\text{hd o v})$ $\rightarrow$ Skip))
  $\square$ (ret'?$x$ $\rightarrow$ (Schema FIG.Remove))'; $\cdot$ $X$)

circus-process DFIG =
  alphabet = [v::nat, x::nat]
  state = [retidS::nat set, max::nat]
  channel = FIG-channels
  schema Init = retidS' = {} $\land$ max' = 0
  schema Out = $v'$ = max $\land$ max' = (max + 1) $\land$ retidS' = retidS $-$ {$v'$}
  schema Remove = $x$ < max $\land$ retidS' = retidS $\cup$ {$x$} $\land$ max' = max

where var $v$ • (Schema DFIG.Init'; $\mu X$ • (((req $\rightarrow$ (Schema DFIG.Out))'; $\text{out}!\cdot(\text{hd o v})$ $\rightarrow$ Skip))
  $\square$ (ret'?$x$ $\rightarrow$ (Schema DFIG.Remove))'; $\cdot$ $X$)

definition Sim where
  Sim A = FIG-alphabet.make (DFIG-alphabet.$v$ A) (DFIG-alphabet.$x$ A)
  ({$a$. a < (DFIG-alphabet.max A) $\land$ a $\notin$ (DFIG-alphabet.retidS A)})

17.2 Simulation proofs

For the simulation proof, we give first proofs for simulation over the schema expressions. The proof is then given over the main actions of the processes.

lemma SimInit: (Schema FIG.Init) $\preceq$ Sim (Schema DFIG.Init)
(proof)
lemma SimOut: (Schema FIG.Out) \preceq Sim (Schema DFIG.Out) (proof)

lemma SimRemove: (Schema FIG.Remove) \preceq Sim (Schema DFIG.Remove) (proof)

lemma FIG.FIG \preceq Sim DFIG.DFIG (proof)
end

References


