A Shallow Model of the UTP in Isabelle/HOL

Abderrahmane Feliachi Simon Foster Marie-Claude Gaudel
Burkhart Wolff Frank Zeyda

March 31, 2016

Contents

1 UTP variables

theory *utp-var*
imports
../contrib/Kleene-Algebras/Quantales
../utils/cardinals
../utils/Continuum
../utils/finite-bijection
../utils/Lenses
../utils/Library-extra/Pfun
../utils/Library-extra/Derivative-extra
~~/src/HOL/Library/Prefix-Order
~~/src/HOL/Library/Adhoc-Overloading
~~/src/HOL/Library/Monad-Syntax
~~/src/HOL/Library/Countable
~~/src/HOL/Eisbach/Eisbach
utp-parser-utils
begin

no-notation *inner* (**infix** · *70*)

This theory describes the foundational structure of UTP variables, upon which the rest of our model rests. We start by defining alphabets, which is this shallow model are simple represented as types, though by convention usually a record type where each field corresponds to a variable.

type-synonym $'\alpha$ *alphabet* $= '\alpha$

UTP variables carry two type parameters, $'a$ that corresponds to the variable's type and $'\alpha$ that corresponds to alphabet of which the variable is a type. There is a thus a strong link between alphabets and variables in this model. Variable are characterized by two functions, *var-lookup* and *var-update*, that respectively lookup and update the variable's value in some alphabetised state space. These functions can readily be extracted from an Isabelle record type.

type-synonym $('a, '\alpha)$ *uvar* $= ('a, '\alpha)$ *lens*

The VAR function is a syntactic translations that allows to retrieve a variable given its name, assuming the variable is a field in a record.

syntax *-VAR* :: *id* ⇒ ('*a*, '*r*) *uvar* (*VAR -*)
translations *VAR x* => *FLDLENS x*

abbreviation *var-lookup* :: ('*a*, '*α*) *uvar* ⇒ '*α* ⇒ '*a* **where**
var-lookup ≡ *lens-get*

abbreviation *var-assign* :: ('*a*, '*α*) *uvar* ⇒ '*a* ⇒ ('*α* ⇒ '*α*) **where**
var-assign x v σ ≡ *lens-put x σ v*

abbreviation *var-update* :: ('*a*, '*α*) *uvar* ⇒ ('*a* ⇒ '*a*) ⇒ ('*α* ⇒ '*α*) **where**
var-update ≡ *weak-lens.update*

abbreviation *semi-uvar* ≡ *mwb-lens*

abbreviation *uvar* ≡ *vwb-lens*

We also define some lifting functions for variables to create input and output variables. These simply lift the alphabet to a tuple type since relations will ultimately be defined to a tuple alphabet.

definition *in-var* :: ('*a*, '*α*) *uvar* ⇒ ('*a*, '*α* × '*β*) *uvar* **where**
[*lens-defs*]: *in-var x* = *x* $;_L$ fst_L

definition *out-var* :: ('*a*, '*β*) *uvar* ⇒ ('*a*, '*α* × '*β*) *uvar* **where**
[*lens-defs*]: *out-var x* = *x* $;_L$ snd_L

definition *pr-var* :: ('*a*, '*β*) *uvar* ⇒ ('*a*, '*β*) *uvar* **where**
[*simp*]: *pr-var x* = *x*

lemma *in-var-semi-uvar* [*simp*]:
  semi-uvar x ⟹ *semi-uvar* (*in-var x*)
  by (*simp add*: *comp-mwb-lens fst-vwb-lens in-var-def*)

lemma *in-var-uvar* [*simp*]:
  uvar x ⟹ *uvar* (*in-var x*)
  by (*simp add*: *comp-vwb-lens fst-vwb-lens in-var-def*)

lemma *out-var-semi-uvar* [*simp*]:
  semi-uvar x ⟹ *semi-uvar* (*out-var x*)
  by (*simp add*: *comp-mwb-lens out-var-def snd-vwb-lens*)

lemma *out-var-uvar* [*simp*]:
  uvar x ⟹ *uvar* (*out-var x*)
  by (*simp add*: *comp-vwb-lens out-var-def snd-vwb-lens*)

lemma *in-out-indep* [*simp*]:
  in-var x ⋈ *out-var y*
  by (*simp add*: *lens-indep-def in-var-def out-var-def fst-lens-def snd-lens-def lens-comp-def*)

lemma *out-in-indep* [*simp*]:
  out-var x ⋈ *in-var y*
  by (*simp add*: *lens-indep-def in-var-def out-var-def fst-lens-def snd-lens-def lens-comp-def*)

lemma *in-var-indep* [*simp*]:

$x \bowtie y \Longrightarrow$ *in-var* $x \bowtie$ *in-var* y
by (*simp add*: *in-var-def out-var-def fst-vwb-lens lens-indep-left-comp*)

lemma *out-var-indep* [*simp*]:
$x \bowtie y \Longrightarrow$ *out-var* $x \bowtie$ *out-var* y
by (*simp add*: *lens-indep-left-comp out-var-def snd-vwb-lens*)

We also define some lookup abstraction simplifications.

lemma *var-lookup-in* [*simp*]: *lens-get* (*in-var x*) (A, A') = *lens-get x A*
by (*simp add*: *in-var-def fst-lens-def lens-comp-def*)

lemma *var-lookup-out* [*simp*]: *lens-get* (*out-var x*) (A, A') = *lens-get x* A'
by (*simp add*: *out-var-def snd-lens-def lens-comp-def*)

lemma *var-update-in* [*simp*]: *lens-put* (*in-var x*) (A, A') v = (*lens-put x A v*, A')
by (*simp add*: *in-var-def fst-lens-def lens-comp-def*)

lemma *var-update-out* [*simp*]: *lens-put* (*out-var x*) (A, A') v = (A, *lens-put x* A' *v*)
by (*simp add*: *out-var-def snd-lens-def lens-comp-def*)

Variables can also be used to effectively define sets of variables. Here we define the the universal alphabet (Σ) to be a variable with identity for both the lookup and update functions. Effectively this is just a function directly on the alphabet type.

abbreviation (*input*) *univ-alpha* :: $('\alpha, '\alpha)$ *uvar* (Σ) **where**
univ-alpha $\equiv 1_L$

nonterminal *svid* **and** *svar* **and** *salpha*

syntax
-salphaid :: *id* $\Rightarrow$ *salpha* (- [*999*] *999*)
-salphavar :: *svar* $\Rightarrow$ *salpha* (- [*999*] *999*)
-salphacomp :: *salpha* $\Rightarrow$ *salpha* $\Rightarrow$ *salpha* (**infixr** $\cdot$ *75*)
-svid :: *id* $\Rightarrow$ *svid* (- [*999*] *999*)
-svid-alpha :: *svid* (Σ)
-spvar :: *svid* $\Rightarrow$ *svar* (&- [*999*] *999*)
-sinvar :: *svid* $\Rightarrow$ *svar* ($- [*999*] *999*)
-soutvar :: *svid* $\Rightarrow$ *svar* ($-´ [*999*] *999*)

consts
svar :: $'v \Rightarrow 'e$
ivar :: $'v \Rightarrow 'e$
ovar :: $'v \Rightarrow 'e$

adhoc-overloading
svar pr-var **and** *ivar in-var* **and** *ovar out-var*

translations
-salphaid x => *x*
-salphacomp x y => $x +_L y$
-salphavar x => *x*
-svid-alpha => Σ
-svid x => *x*
-spvar x == *CONST svar x*
-sinvar x == *CONST ivar x*
-soutvar x == *CONST ovar x*

end

1.1 Deep UTP variables

theory *utp-dvar*
  imports *utp-var*
begin

UTP variables represented by record fields are shallow, nameless entities. They are fundamentally static in nature, since a new record field can only be introduced definitionally and cannot be otherwise arbitrarily created. They are nevertheless very useful as proof automation is excellent, and they can fully make use of the Isabelle type system. However, for constructs like alphabet extension that can introduce new variables they are inadequate. As a result we also introduce a notion of deep variables to complement them. A deep variable is not a record field, but rather a key within a store map that records the values of all deep variables. As such the Isabelle type system is agnostic of them, and the creation of a new deep variable does not change the portion of the alphabet specified by the type system.

In order to create a type of stores (or bindings) for variables, we must fix a universe for the variable valuations. This is the major downside of deep variables – they cannot have any type, but only a type whose cardinality is up to $\mathfrak{c}$, the cardinality of the continuum. This is why we need both deep and shallow variables, as the latter are unrestricted in this respect. Each deep variable will therefore specify the cardinality of the type it possesses.

1.2 Cardinalities

We first fix a datatype representing all possible cardinalities for a deep variable. These include finite cardinalities, $\aleph_0$ (countable), and $\mathfrak{c}$ (uncountable up to the continuum).

datatype $ucard = \mathit{fin}\ \mathit{nat} \mid \mathit{aleph0}\ (\aleph_0) \mid \mathit{cont}\ (\mathrm{c})$

Our universe is simply the set of natural numbers; this is sufficient for all types up to cardinality $\mathfrak{c}$.

type-synonym $uuniv = \mathit{nat}\ \mathit{set}$

We introduce a function that gives the set of values within our universe of the given cardinality. Since a cardinality of 0 is no proper type, we use finite cardinality 0 to mean cardinality 1, 1 to mean 2 etc.

fun $uuniv :: ucard \Rightarrow uuniv\ set\ (\mathcal{U}'(\text{-}'))$ **where**
$\mathcal{U}(\mathit{fin}\ n) = \{\{x\} \mid x.\ x \leq n\} \mid$
$\mathcal{U}(\aleph_0) = \{\{x\} \mid x.\ \mathit{True}\} \mid$
$\mathcal{U}(\mathrm{c}) = \mathit{UNIV}$

We also define the following function that gives the cardinality of a type within the *continuum* type class.

definition $\mathit{ucard\text{-}of} :: {}'a{::}\mathit{continuum}\ \mathit{itself} \Rightarrow \mathit{ucard}$ **where**
$\mathit{ucard\text{-}of}\ x = (\mathit{if}\ (\mathit{finite}\ (\mathit{UNIV} :: {}'a\ set))$
$\quad \mathit{then}\ \mathit{fin}(\mathit{card}(\mathit{UNIV} :: {}'a\ set) - 1)$
$\quad \mathit{else}\ \mathit{if}\ (\mathit{countable}\ (\mathit{UNIV} :: {}'a\ set))$
$\quad \mathit{then}\ \aleph_0$
$\quad \mathit{else}\ \mathrm{c})$

syntax
  -ucard :: *type* ⇒ *ucard* (*UCARD*′(-′))

translations
  $UCARD('a) == CONST\ ucard\text{-}of\ (TYPE('a))$

lemma *ucard-non-empty*:
  $\mathcal{U}(x) \neq \{\}$
  by (*induct x*, *auto*)

lemma *ucard-of-finite* [*simp*]:
  $finite\ (UNIV :: 'a::continuum\ set) \Longrightarrow UCARD('a) = fin(card(UNIV :: 'a\ set) - 1)$
  by (*simp add*: *ucard-of-def*)

lemma *ucard-of-countably-infinite* [*simp*]:
  $[\![\ countable(UNIV :: 'a::continuum\ set);\ infinite(UNIV :: 'a\ set)\ ]\!] \Longrightarrow UCARD('a) = \aleph_0$
  by (*simp add*: *ucard-of-def*)

lemma *ucard-of-uncountably-infinite* [*simp*]:
  $uncountable\ (UNIV :: 'a\ set) \Longrightarrow UCARD('a :: continuum) = \mathrm{c}$
  apply (*simp add*: *ucard-of-def*)
  using *countable-finite* **apply** *blast*
done

1.3 Injection functions

definition *uinject-finite* :: ′*a*::*finite* ⇒ *uuniv* **where**
$uinject\text{-}finite\ x = \{to\text{-}nat\text{-}fin\ x\}$

definition *uinject-aleph0* :: ′*a*::{*countable*, *infinite*} ⇒ *uuniv* **where**
$uinject\text{-}aleph0\ x = \{to\text{-}nat\text{-}bij\ x\}$

definition *uinject-continuum* :: ′*a*::{*continuum*, *infinite*} ⇒ *uuniv* **where**
$uinject\text{-}continuum\ x = to\text{-}nat\text{-}set\text{-}bij\ x$

definition *uinject* :: ′*a*::*continuum* ⇒ *uuniv* **where**
uinject x = (*if* (*finite* (*UNIV* :: ′*a set*))
        then {*to-nat-fin x*}
      else if (*countable* (*UNIV* :: ′*a set*))
        then {*to-nat-on* (*UNIV* :: ′*a set*) *x*}
      else to-nat-set x)

definition *uproject* :: *uuniv* ⇒ ′*a*::*continuum* **where**
$uproject = inv\ uinject$

lemma *uinject-finite*:
  $finite\ (UNIV :: 'a::continuum\ set) \Longrightarrow uinject = (\lambda\ x :: 'a.\ \{to\text{-}nat\text{-}fin\ x\})$
  by (*rule ext*, *auto simp add*: *uinject-def*)

lemma *uinject-uncountable*:
  $uncountable\ (UNIV :: 'a::continuum\ set) \Longrightarrow (uinject :: 'a \Rightarrow uuniv) = to\text{-}nat\text{-}set$
  by (*rule ext*, *auto simp add*: *uinject-def countable-finite*)

lemma *card-finite-lemma*:
  assumes *finite* (*UNIV* :: ′*a set*)
  shows $x < card\ (UNIV :: 'a\ set) \longleftrightarrow x \leq card\ (UNIV :: 'a\ set) - Suc\ 0$

proof −
  have *card* (*UNIV* :: *'a set*) > *0*
    by (*simp add*: *assms finite-UNIV-card-ge-0*)
  thus *?thesis*
    by *linarith*
qed

This is a key theorem that shows that the injection function provides a bijection between any continuum type and the subuniverse of types with a matching cardinality.

lemma *uinject-bij*:
  bij-betw (*uinject* :: *'a::continuum* ⇒ *uuniv*) *UNIV* $\mathcal{U}$(*UCARD*(*'a*))
proof (*cases finite* (*UNIV* :: *'a set*))
  case *True* **thus** *?thesis*
    apply (*auto simp add*: *uinject-def bij-betw-def inj-on-def image-def card-finite-lemma*[*THEN sym*])
    apply (*auto simp add*: *inj-eq to-nat-fin-inj to-nat-fin-bounded*)
    using *to-nat-fin-ex* **apply** *blast*
  done
  next
  case *False* **note** *infinite* = *this* **thus** *?thesis*
  proof (*cases countable* (*UNIV* :: *'a set*))
    case *True* **thus** *?thesis*
     apply (*auto simp add*: *uinject-def bij-betw-def inj-on-def infinite image-def card-finite-lemma*[*THEN sym*])
      apply (*meson image-to-nat-on infinite surj-def*)
    done
    next
    case *False* **note** *uncount* = *this* **thus** *?thesis*
      apply (*simp add*: *uinject-uncountable*)
      using *to-nat-set-bij* **apply** *blast*
    done
  qed
qed

lemma *uinject-card* [*simp*]: *uinject* (*x* :: *'a::continuum*) ∈ $\mathcal{U}$(*UCARD*(*'a*))
  by (*metis bij-betw-def rangeI uinject-bij*)

lemma *uinject-inv* [*simp*]:
  uproject (*uinject x*) = *x*
  by (*metis UNIV-I bij-betw-def inv-into-f-f uinject-bij uproject-def*)

lemma *uproject-inv* [*simp*]:
  x ∈ $\mathcal{U}$(*UCARD*(*'a::continuum*)) ⟹ *uinject* ((*uproject* :: *nat set* ⇒ *'a*) *x*) = *x*
  by (*metis bij-betw-inv-into-right uinject-bij uproject-def*)

1.4 Deep variables

A deep variable name stores both a name and the cardinality of the type it points to

record *dname* =
  dname-name :: *string*
  dname-card :: *ucard*

A vstore is a function mapping deep variable names to corresponding values in the universe, such that the deep variables specified cardinality is matched by the value it points to.

typedef *vstore* = {*f* :: *dname* ⇒ *uuniv*. ∀ *x*. *f*(*x*) ∈ $\mathcal{U}$(*dname-card x*)}

apply (*rule-tac* $x=\lambda$ *x*. {*0*} **in** *exI*)
apply (*auto*)
apply (*rename-tac x*)
apply (*case-tac dname-card x*)
apply (*simp-all*)
done

setup-lifting *type-definition-vstore*

typedef ($'a$::*continuum*) *dvar* = {*x* :: *dname*. *dname-card x* = *UCARD*($'a$)}
by (*auto*, *meson dname.select-convs*(*2*))

setup-lifting *type-definition-dvar*

lift-definition *mk-dvar* :: *string* ⇒ ($'a$::*continuum*) *dvar* ($\lceil$-$\rceil_d$)
is λ *n*. ⦇ *dname-name* = *n*, *dname-card* = *UCARD*($'a$) ⦈
by *auto*

lift-definition *dvar-name* :: $'a$::*continuum dvar* ⇒ *string* **is** *dname-name* **.**
lift-definition *dvar-card* :: $'a$::*continuum dvar* ⇒ *ucard* **is** *dname-card* **.**

lemma *dvar-name* [*simp*]: *dvar-name* $\lceil x\rceil_d$ = *x*
by (*transfer*, *simp*)

lift-definition *vstore-lookup* :: ($'a$::*continuum*) *dvar* ⇒ *vstore* ⇒ $'a$
is λ *x s*. (*uproject* :: *uuniv* ⇒ $'a$) (*s*(*x*)) **.**

lift-definition *vstore-put* :: ($'a$::*continuum*) *dvar* ⇒ $'a$ ⇒ *vstore* ⇒ *vstore*
is λ (*x* :: *dname*) (*v* :: $'a$) *f* . *f*(*x* := *uinject v*)
by (*auto*)

definition *vstore-upd* :: ($'a$::*continuum*) *dvar* ⇒ ($'a$ ⇒ $'a$) ⇒ *vstore* ⇒ *vstore*
where *vstore-upd x f s* = *vstore-put x* (*f* (*vstore-lookup x s*)) *s*

lemma *vstore-upd-comp* [*simp*]:
vstore-upd x f (*vstore-upd x g s*) = *vstore-upd x* (*f* ∘ *g*) *s*
by (*simp add*: *vstore-upd-def*, *transfer*, *simp*)

lemma *vstore-lookup-put* [*simp*]: *vstore-lookup x* (*vstore-put x v s*) = *v*
by (*transfer*, *simp*)

lemma *vstore-lookup-upd* [*simp*]: *vstore-lookup x* (*vstore-upd x f s*) = *f* (*vstore-lookup x s*)
by (*simp add*: *vstore-upd-def*)

lemma *vstore-upd-eta* [*simp*]: *vstore-upd x* (λ -. *vstore-lookup x s*) *s* = *s*
apply (*simp add*: *vstore-upd-def*, *transfer*, *auto*)
apply (*metis Domainp-iff dvar.domain fun-upd-idem-iff uproject-inv*)
done

lemma *vstore-lookup-put-diff-var* [*simp*]:
assumes *dvar-name x* ≠ *dvar-name y*
shows *vstore-lookup x* (*vstore-put y v s*) = *vstore-lookup x s*
using *assms* **by** (*transfer*, *auto*)

lemma *vstore-put-commute*:

assumes *dvar-name* $x \neq$ *dvar-name* y
shows *vstore-put* x u (*vstore-put* y v s) = *vstore-put* y v (*vstore-put* x u s)
using *assms*
by (*transfer*, *fastforce*)

lemma *vstore-put-put* [*simp*]:
vstore-put x u (*vstore-put* x v s) = *vstore-put* x u s
by (*transfer*, *simp*)

The vst class provides an interface for extracting a variable store from a state space. For now, the state-space is limited to countably infinite types, though we will in the future build a more expressive universe.

class *vst* =
fixes *get-vstore* :: $'a \Rightarrow$ *vstore*
and *put-vstore* :: $'a \Rightarrow$ *vstore* $\Rightarrow 'a$
assumes *put-get-vstore* [*simp*]: *get-vstore* (*put-vstore* s x) = x
and *get-put-vstore* [*simp*]: *put-vstore* s (*get-vstore* s) = s
and *put-put-vstore* [*simp*]: *put-vstore* (*put-vstore* s x) y = *put-vstore* s y

definition *dvar-lift* :: $'a$::*continuum dvar* $\Rightarrow$ ($'a$, $'\alpha$::*vst*) *uvar* (-$\uparrow$ [*999*] *999*)
where *dvar-lift* x = $(\!|$ *lens-get* = (λ v. *vstore-lookup* x (*get-vstore* v))
, *lens-put* = (λ s v. *put-vstore* s (*vstore-put* x v (*get-vstore* s)))
$|\!)$

definition [*simp*]: *in-dvar* x = *in-var* ($x\uparrow$)
definition [*simp*]: *out-dvar* x = *out-var* ($x\uparrow$)

adhoc-overloading
ivar in-dvar **and** *ovar out-dvar* **and** *svar dvar-lift*

lemma *uvar-dvar*: *uvar* ($x\uparrow$)
apply (*unfold-locales*)
apply (*simp-all add*: *dvar-lift-def*)
apply (*metis get-put-vstore vstore-upd-def vstore-upd-eta*)
done

Deep variables with different names are independent

lemma *dvar-indep-diff-name*:
assumes *dvar-name* $x \neq$ *dvar-name* y
shows $x\uparrow \bowtie y\uparrow$
using *assms*
apply (*auto simp add*: *assms dvar-lift-def lens-indep-def vstore-put-commute*)
using *assms* **apply** *auto*
done

lemma *dvar-indep-diff-name'* [*simp*]:
$x \neq y \Longrightarrow \lceil x \rceil_d\uparrow \bowtie \lceil y \rceil_d\uparrow$
by (*auto intro*: *dvar-indep-diff-name*)

A basic record structure for vstores

record *vstore-d* =
vstore :: *vstore*

instantiation *vstore-d-ext* :: (*type*) *vst*

begin
  definition [*simp*]: *get-vstore-vstore-d-ext* = *vstore*
  definition [*simp*]: *put-vstore-vstore-d-ext* = (λ *x s*. *vstore-update* (λ-. *s*) *x*)
instance
  by (*intro-classes*, *simp-all*)
end

end

2 UTP expressions

theory *utp-expr*
imports
  utp-var
  utp-dvar
begin

Before building the predicate model, we will build a model of expressions that generalise alphabetised predicates. Expressions are represented semantically as mapping from the alphabet to the expression's type. This general model will allow us to unify all constructions under one type. All definitions in the file are given using the *lifting* package.

Since we have two kinds of variable (deep and shallow) in the model, we will also need two versions of each construct that takes a variable. We make use of adhoc-overloading to ensure the correct instance is automatically chosen, within the user noticing a difference.

typedef ('*t*, 'α) *uexpr* = *UNIV* :: ('α *alphabet* $\Rightarrow$ '*t*) *set* **..**

notation *Rep-uexpr* ($[\![-]\!]_e$)

lemma *uexpr-eq-iff*:
  $e = f \longleftrightarrow (\forall\ b.\ [\![e]\!]_e\ b = [\![f]\!]_e\ b)$
  using *Rep-uexpr-inject*[*of e f*, *THEN sym*] **by** (*auto*)

named-theorems *ueval*

setup-lifting *type-definition-uexpr*

Get the alphabet of an expression

definition *alpha-of* :: ('*a*, 'α) *uexpr* $\Rightarrow$ ('α, 'α) *lens* (α'(-')) **where**
alpha-of e = 1_L

A variable expression corresponds to the lookup function of the variable.

lift-definition *var* :: ('*t*, 'α) *uvar* $\Rightarrow$ ('*t*, 'α) *uexpr* **is** *var-lookup* **.**

declare [[*coercion-enabled*]]
declare [[*coercion var*]]

definition *dvar-exp* :: '*t*::*continuum dvar* $\Rightarrow$ ('*t*, 'α::*vst*) *uexpr*
where *dvar-exp x* = *var* (*dvar-lift x*)

A literal is simply a constant function expression, always returning the same value.

lift-definition *lit* :: '*t* $\Rightarrow$ ('*t*, 'α) *uexpr*
  is λ *v b*. *v* **.**

We define lifting for unary, binary, and ternary functions, that simply apply the function to all possible results of the expressions.

lift-definition *uop* :: $('a \Rightarrow 'b) \Rightarrow ('a, '\alpha)$ *uexpr* $\Rightarrow ('b, '\alpha)$ *uexpr*
  is $\lambda\ f\ e\ b.\ f\ (e\ b)$ **.**
lift-definition *bop* ::
  $('a \Rightarrow 'b \Rightarrow 'c) \Rightarrow ('a, '\alpha)$ *uexpr* $\Rightarrow ('b, '\alpha)$ *uexpr* $\Rightarrow ('c, '\alpha)$ *uexpr*
  is $\lambda\ f\ u\ v\ b.\ f\ (u\ b)\ (v\ b)$ **.**
lift-definition *trop* ::
  $('a \Rightarrow 'b \Rightarrow 'c \Rightarrow 'd) \Rightarrow ('a, '\alpha)$ *uexpr* $\Rightarrow ('b, '\alpha)$ *uexpr* $\Rightarrow ('c, '\alpha)$ *uexpr* $\Rightarrow ('d, '\alpha)$ *uexpr*
  is $\lambda\ f\ u\ v\ w\ b.\ f\ (u\ b)\ (v\ b)\ (w\ b)$ **.**

We also define a UTP expression version of function abstract

lift-definition *ulambda* :: $('a \Rightarrow ('b, '\alpha)$ *uexpr*$) \Rightarrow ('a \Rightarrow 'b, '\alpha)$ *uexpr*
is $\lambda\ f\ A\ x.\ f\ x\ A$ **.**

We define syntax for expressions using adhoc overloading – this allows us to later define operators on different types if necessary (e.g. when adding types for new UTP theories).

consts
  ulit :: $'t \Rightarrow 'e$ (≪-≫)
  ueq :: $'a \Rightarrow 'a \Rightarrow 'b$ (**infixl** $=_u$ *50*)
  ueuvar :: $'v \Rightarrow 'p$

adhoc-overloading
  ulit lit **and**
  ueuvar var **and**
  ueuvar dvar-exp

syntax
  -uuvar :: *svar* $\Rightarrow$ *logic*

translations
  -uuvar x => *CONST var x*
  x <= *CONST ueuvar x*

syntax
  -uuvar :: *svar* $\Rightarrow$ *logic* (-)

We also set up some useful standard arithmetic operators for Isabelle by lifting the functions to binary operators.

instantiation *uexpr* :: (*plus*, *type*) *plus*
begin
  definition *plus-uexpr-def*: $u + v = bop\ (op\ +)\ u\ v$
instance ..
end

Instantiating uminus also provides negation for predicates later

instantiation *uexpr* :: (*uminus*, *type*) *uminus*
begin
  definition *uminus-uexpr-def*: $-\ u = uop\ uminus\ u$
instance ..
end

instantiation *uexpr* :: (*minus*, *type*) *minus*
begin
  definition *minus-uexpr-def*: $u - v = bop\ (op\ -)\ u\ v$
instance ..
end

instantiation *uexpr* :: (*times*, *type*) *times*
begin
  definition *times-uexpr-def*: $u * v = bop\ (op\ *)\ u\ v$
instance ..
end

instantiation *uexpr* :: (*inverse*, *type*) *inverse*
begin
  definition *inverse-uexpr-def*: $inverse\ u = uop\ inverse\ u$
  definition *divide-uexpr-def*: $u\ /\ v = bop\ (op\ /)\ u\ v$
instance ..
end

instantiation *uexpr* :: (*Divides.div*, *type*) *Divides.div*
begin
  definition *div-uexpr-def*: $u\ div\ v = bop\ (op\ div)\ u\ v$
  definition *mod-uexpr-def*: $u\ mod\ v = bop\ (op\ mod)\ u\ v$
instance ..
end

instantiation *uexpr* :: (*zero*, *type*) *zero*
begin
  definition *zero-uexpr-def*: $0 = lit\ 0$
instance ..
end

instantiation *uexpr* :: (*one*, *type*) *one*
begin
  definition *one-uexpr-def*: $1 = lit\ 1$
instance ..

end

instance *uexpr* :: (*semigroup-mult*, *type*) *semigroup-mult*
  by (*intro-classes*) (*simp add*: *times-uexpr-def one-uexpr-def*, *transfer*, *simp add*: *mult.assoc*)+

instance *uexpr* :: (*monoid-mult*, *type*) *monoid-mult*
  by (*intro-classes*) (*simp add*: *times-uexpr-def one-uexpr-def*, *transfer*, *simp*)+

instance *uexpr* :: (*semigroup-add*, *type*) *semigroup-add*
  by (*intro-classes*) (*simp add*: *plus-uexpr-def zero-uexpr-def*, *transfer*, *simp add*: *add.assoc*)+

instance *uexpr* :: (*monoid-add*, *type*) *monoid-add*
  by (*intro-classes*) (*simp add*: *plus-uexpr-def zero-uexpr-def*, *transfer*, *simp*)+

instance *uexpr* :: (*semiring*, *type*) *semiring*
  by (*intro-classes*) (*simp add*: *plus-uexpr-def times-uexpr-def*, *transfer*, *simp add*: *fun-eq-iff add.commute semiring-class.distrib-right semiring-class.distrib-left*)+

instance *uexpr* :: (*ring-1*, *type*) *ring-1*
by (*intro-classes*) (*simp add*: *plus-uexpr-def uminus-uexpr-def minus-uexpr-def times-uexpr-def zero-uexpr-def one-uexpr-def*, *transfer*, *simp add*: *fun-eq-iff*)+

instance *uexpr* :: (*numeral*, *type*) *numeral*
by (*intro-classes*, *simp add*: *plus-uexpr-def*, *transfer*, *simp add*: *add.assoc*)

Set up automation for numerals

lemma *numeral-uexpr-rep-eq*: $[\![numeral\ x]\!]_e\ b = numeral\ x$
by (*induct x*, *simp-all add*: *plus-uexpr-def one-uexpr-def numeral.simps lit.rep-eq bop.rep-eq*)

lemma *numeral-uexpr-simp*: *numeral x* = «*numeral x*»
by (*simp add*: *uexpr-eq-iff numeral-uexpr-rep-eq lit.rep-eq*)

definition *eq-upred* :: ('*a*, 'α) *uexpr* ⇒ ('*a*, 'α) *uexpr* ⇒ (*bool*, 'α) *uexpr*
where *eq-upred x y* = *bop HOL.eq x y*

adhoc-overloading
ueq eq-upred

definition *fun-apply f x* = *f x*
declare *fun-apply-def* [*simp*]

consts
uapply :: '*f* ⇒ '*k* ⇒ '*v*
udom :: '*f* ⇒ '*a set*
uran :: '*f* ⇒ '*b set*
ucard :: '*f* ⇒ *nat*

adhoc-overloading
uapply fun-apply **and** *uapply nth* **and** *uapply pfun-app* **and**
udom Domain **and** *udom pdom* **and** *udom seq-dom* **and**
udom Range **and** *uran pran* **and** *uran set* **and**
ucard card **and** *ucard pcard* **and** *ucard length*

nonterminal *utuple-args* **and** *umaplet* **and** *umaplets*

syntax
-ucoerce :: ('*a*, 'α) *uexpr* ⇒ *type* ⇒ ('*a*, 'α) *uexpr* (**infix** $:_u$ *50*)
-unil :: ('*a list*, 'α) *uexpr* (⟨⟩)
-ulist :: *args* => ('*a list*, 'α) *uexpr* (⟨(-)⟩)
-uappend :: ('*a list*, 'α) *uexpr* ⇒ ('*a list*, 'α) *uexpr* ⇒ ('*a list*, 'α) *uexpr* (**infixr** $\hat{}_u$ *80*)
-ulast :: ('*a list*, 'α) *uexpr* ⇒ ('*a*, 'α) *uexpr* ($last_u$'(-'))
-ufront :: ('*a list*, 'α) *uexpr* ⇒ ('*a list*, 'α) *uexpr* ($front_u$'(-'))
-uhead :: ('*a list*, 'α) *uexpr* ⇒ ('*a*, 'α) *uexpr* ($head_u$'(-'))
-utail :: ('*a list*, 'α) *uexpr* ⇒ ('*a list*, 'α) *uexpr* ($tail_u$'(-'))
-ucard :: ('*a list*, 'α) *uexpr* ⇒ (*nat*, 'α) *uexpr* ($\#_u$'(-'))
-ufilter :: ('*a list*, 'α) *uexpr* ⇒ ('*a set*, 'α) *uexpr* ⇒ ('*a list*, 'α) *uexpr* (**infixl** $\upharpoonleft_u$ *75*)
-uextract :: ('*a set*, 'α) *uexpr* ⇒ ('*a list*, 'α) *uexpr* ⇒ ('*a list*, 'α) *uexpr* (**infixl** $\upharpoonright_u$ *75*)
-uelems :: ('*a list*, 'α) *uexpr* ⇒ ('*a set*, 'α) *uexpr* ($elems_u$'(-'))
-usorted :: ('*a list*, 'α) *uexpr* ⇒ (*bool*, 'α) *uexpr* ($sorted_u$'(-'))
-udistinct :: ('*a list*, 'α) *uexpr* ⇒ (*bool*, 'α) *uexpr* ($distinct_u$'(-'))
-uless :: ('*a*, 'α) *uexpr* ⇒ ('*a*, 'α) *uexpr* ⇒ (*bool*, 'α) *uexpr* (**infix** $<_u$ *50*)
-uleq :: ('*a*, 'α) *uexpr* ⇒ ('*a*, 'α) *uexpr* ⇒ (*bool*, 'α) *uexpr* (**infix** $\leq_u$ *50*)
-ugreat :: ('*a*, 'α) *uexpr* ⇒ ('*a*, 'α) *uexpr* ⇒ (*bool*, 'α) *uexpr* (**infix** $>_u$ *50*)

-ugeq :: ('a, 'α) uexpr ⇒ ('a, 'α) uexpr ⇒ (bool, 'α) uexpr (**infix** $\geq_u$ 50)
-uempset :: ('a set, 'α) uexpr ($\{\}_u$)
-uset :: args => ('a set, 'α) uexpr ($\{(\text{-})\}_u$)
-uunion :: ('a set, 'α) uexpr ⇒ ('a set, 'α) uexpr ⇒ ('a set, 'α) uexpr (**infixl** $\cup_u$ 65)
-uinter :: ('a set, 'α) uexpr ⇒ ('a set, 'α) uexpr ⇒ ('a set, 'α) uexpr (**infixl** $\cap_u$ 70)
-umem :: ('a, 'α) uexpr ⇒ ('a set, 'α) uexpr ⇒ (bool, 'α) uexpr (**infix** $\in_u$ 50)
-unmem :: ('a, 'α) uexpr ⇒ ('a set, 'α) uexpr ⇒ (bool, 'α) uexpr (**infix** $\notin_u$ 50)
-usubset :: ('a set, 'α) uexpr ⇒ ('a set, 'α) uexpr ⇒ (bool, 'α) uexpr (**infix** $\subset_u$ 50)
-usubseteq :: ('a set, 'α) uexpr ⇒ ('a set, 'α) uexpr ⇒ (bool, 'α) uexpr (**infix** $\subseteq_u$ 50)
-utuple :: ('a, 'α) uexpr ⇒ utuple-args ⇒ ('a * 'b, 'α) uexpr ((1'(-,/ -')$_u$))
-utuple-arg :: ('a, 'α) uexpr ⇒ utuple-args (-)
-utuple-args :: ('a, 'α) uexpr => utuple-args ⇒ utuple-args (-,/ -)
-uunit :: ('a, 'α) uexpr ('(')$_u$)
-ufst :: ('a × 'b, 'α) uexpr ⇒ ('a, 'α) uexpr (π_1'(-'))
-usnd :: ('a × 'b, 'α) uexpr ⇒ ('b, 'α) uexpr (π_2'(-'))
-uapply :: ('a ⇒ 'b, 'α) uexpr ⇒ utuple-args ⇒ ('b, 'α) uexpr (-(|-|)$_u$ [999,0] 999)
-ulamba :: pttrn ⇒ logic ⇒ logic (λ - • - [0, 10] 10)
-udom :: logic ⇒ logic (dom_u'(-'))
-uran :: logic ⇒ logic (ran_u'(-'))
-uinl :: logic ⇒ logic (inl_u'(-'))
-uinr :: logic ⇒ logic (inr_u'(-'))
-umap-empty :: logic ($[]_u$)
-umap-plus :: logic ⇒ logic ⇒ logic (**infixl** $\oplus_u$ 85)
-umap-minus :: logic ⇒ logic ⇒ logic (**infixl** $\ominus_u$ 85)
-udom-res :: logic ⇒ logic ⇒ logic (**infixl** $\lhd_u$ 85)
-uran-res :: logic ⇒ logic ⇒ logic (**infixl** $\rhd_u$ 85)
-umaplet :: [logic, logic] => umaplet (- /↦/ -)
:: umaplet => umaplets (-)
-UMaplets :: [umaplet, umaplets] => umaplets (-,/ -)
-UMapUpd :: [logic, umaplets] => logic (-/'(-') [900,0] 900)
-UMap :: umaplets => logic ((1[-]$_u$))

translations
$f(|v|)_u$ <= CONST uapply f v
$dom_u(f)$ <= CONST udom f
$ran_u(f)$ <= CONST uran f
$\#_u(f)$ <= CONST ucard f

translations
x :$_u$ 'a == x :: ('a, -) uexpr
⟨⟩ == ≪[]≫
⟨x, xs⟩ == CONST bop (op #) x ⟨xs⟩
⟨x⟩ == CONST bop (op #) x ≪[]≫
x $\hat{}_u$ y == CONST bop (op @) x y
$last_u(xs)$ == CONST uop CONST last xs
$front_u(xs)$ == CONST uop CONST butlast xs
$head_u(xs)$ == CONST uop CONST hd xs
$tail_u(xs)$ == CONST uop CONST tl xs
$\#_u(xs)$ == CONST uop CONST ucard xs
$elems_u(xs)$ == CONST uop CONST set xs
$sorted_u(xs)$ == CONST uop CONST sorted xs
$distinct_u(xs)$ == CONST uop CONST distinct xs
xs $\upharpoonleft_u$ A == CONST bop CONST seq-filter xs A
A $\upharpoonright_u$ xs == CONST bop (op $\upharpoonright_l$) A xs

$x <_u y$ == *CONST bop* (*op* $<$) x y
$x \leq_u y$ == *CONST bop* (*op* $\leq$) x y
$x >_u y$ == $y <_u x$
$x \geq_u y$ == $y \leq_u x$
$\{\}_u$ == $\ll\{\}\gg$
$\{x, xs\}_u$ == *CONST bop* (*CONST insert*) x $\{xs\}_u$
$\{x\}_u$ == *CONST bop* (*CONST insert*) x $\ll\{\}\gg$
$A \cup_u B$ == *CONST bop* (*op* $\cup$) A B
$A \cap_u B$ == *CONST bop* (*op* $\cap$) A B
$f \oplus_u g$ => (f :: ((-, -) *pfun*, -) *uexpr*) + g
$f \ominus_u g$ => (f :: ((-, -) *pfun*, -) *uexpr*) $-$ g
$x \in_u A$ == *CONST bop* (*op* $\in$) x A
$x \notin_u A$ == *CONST bop* (*op* $\notin$) x A
$A \subset_u B$ == *CONST bop* (*op* $<$) A B
$A \subset_u B$ <= *CONST bop* (*op* $\subset$) A B
$f \subset_u g$ <= *CONST bop* (*op* $\subset_p$) f g
$A \subseteq_u B$ == *CONST bop* (*op* $\leq$) A B
$A \subseteq_u B$ <= *CONST bop* (*op* $\subseteq$) A B
$f \subseteq_u g$ <= *CONST bop* (*op* $\subseteq_p$) f g
$()_u$ == $\ll()\gg$
$(x, y)_u$ == *CONST bop* (*CONST Pair*) x y
-utuple x (*-utuple-args* y z) == *-utuple* x (*-utuple-arg* (*-utuple* y z))
$\pi_1(x)$ == *CONST uop CONST fst* x
$\pi_2(x)$ == *CONST uop CONST snd* x
$f(|x|)_u$ == *CONST bop CONST uapply* f x
$\lambda\ x \cdot p$ == *CONST ulambda* ($\lambda\ x.\ p$)
$dom_u(f)$ == *CONST uop CONST udom* f
$ran_u(f)$ == *CONST uop CONST uran* f
$inl_u(x)$ == *CONST uop CONST Inl* x
$inr_u(x)$ == *CONST uop CONST Inr* x
$[]_u$ == $\ll$*CONST pempty*$\gg$
$A \lhd_u f$ == *CONST bop* (*op* $\lhd_p$) A f
$f \rhd_u A$ == *CONST bop* (*op* $\rhd_p$) A f
-UMapUpd m (*-UMaplets xy ms*) == *-UMapUpd* (*-UMapUpd m xy*) *ms*
-UMapUpd m (*-umaplet x y*) == *CONST trop CONST pfun-upd m x y*
-UMap ms == *-UMapUpd* $[]_u$ *ms*
-UMap (*-UMaplets ms1 ms2*) <= *-UMapUpd* (*-UMap ms1*) *ms2*
-UMaplets ms1 (*-UMaplets ms2 ms3*) <= *-UMaplets* (*-UMaplets ms1 ms2*) *ms3*
$f(|x,y|)_u$ == *CONST bop CONST uapply* f $(x,y)_u$

Lifting set intervals

syntax
-uset-atLeastAtMost :: ($'a$, $'\alpha$) *uexpr* $\Rightarrow$ ($'a$, $'\alpha$) *uexpr* $\Rightarrow$ ($'a$ *set*, $'\alpha$) *uexpr* ((*1*{-..-}$_u$))
-uset-atLeastLessThan :: ($'a$, $'\alpha$) *uexpr* $\Rightarrow$ ($'a$, $'\alpha$) *uexpr* $\Rightarrow$ ($'a$ *set*, $'\alpha$) *uexpr* ((*1*{-..<-}$_u$))
-uset-compr :: *id* $\Rightarrow$ ($'a$ *set*, $'\alpha$) *uexpr* $\Rightarrow$ (*bool*, $'\alpha$) *uexpr* $\Rightarrow$ ($'b$, $'\alpha$) *uexpr* $\Rightarrow$ ($'b$ *set*, $'\alpha$) *uexpr* ((*1*{- :/ - |/ - $\cdot$/ -}$_u$))

lift-definition *ZedSetCompr* ::
($'a$ *set*, $'\alpha$) *uexpr* $\Rightarrow$ ($'a$ $\Rightarrow$ (*bool*, $'\alpha$) *uexpr* $\times$ ($'b$, $'\alpha$) *uexpr*) $\Rightarrow$ ($'b$ *set*, $'\alpha$) *uexpr*
is λ *A PF b*. { *snd* (*PF x*) *b* | *x*. $x \in A\ b \wedge$ *fst* (*PF x*) *b*} **.**

translations
$\{x..y\}_u$ == *CONST bop CONST atLeastAtMost* x y
$\{x..<y\}_u$ == *CONST bop CONST atLeastLessThan* x y
$\{x : A \mid P \cdot F\}_u$ == *CONST ZedSetCompr* A ($\lambda\ x.\ (P, F)$)

Lifting limits

definition *ulim-left* = $(\lambda\ p\ f.\ Lim\ (at\text{-}left\ p)\ f)$
definition *ulim-right* = $(\lambda\ p\ f.\ Lim\ (at\text{-}right\ p)\ f)$
definition *ucont-on* = $(\lambda\ f\ A.\ continuous\text{-}on\ A\ f)$

syntax
  -ulim-left :: $id \Rightarrow logic \Rightarrow logic \Rightarrow logic\ (lim_u{}'(\text{-} \to \text{-}^{-}{}')'(\text{-}'))$
  -ulim-right :: $id \Rightarrow logic \Rightarrow logic \Rightarrow logic\ (lim_u{}'(\text{-} \to \text{-}^{+}{}')'(\text{-}'))$
  -ucont-on :: $logic \Rightarrow logic \Rightarrow logic$ (**infix** $cont{-}on_u$ *90*)

translations
  $lim_u(x \to p^-)(e)$ == *CONST bop CONST ulim-left* $p\ (\lambda\ x \cdot e)$
  $lim_u(x \to p^+)(e)$ == *CONST bop CONST ulim-right* $p\ (\lambda\ x \cdot e)$
  $f\ cont{-}on_u\ A$ == *CONST bop CONST continuous-on A f*

lemmas *uexpr-defs* =
  alpha-of-def

  zero-uexpr-def
  one-uexpr-def
  plus-uexpr-def
  uminus-uexpr-def
  minus-uexpr-def
  times-uexpr-def
  inverse-uexpr-def
  divide-uexpr-def
  div-uexpr-def
  mod-uexpr-def
  eq-upred-def
  numeral-uexpr-simp
  ulim-left-def
  ulim-right-def
  ucont-on-def

2.1 Evaluation laws for expressions

lemma *lit-ueval* [*ueval*]: $[\![\ll x \gg]\!]_e b = x$
  by (*transfer*, *simp*)

lemma *var-ueval* [*ueval*]: $[\![var\ x]\!]_e b = var\text{-}lookup\ x\ b$
  by (*transfer*, *simp*)

lemma *uop-ueval* [*ueval*]: $[\![uop\ f\ x]\!]_e b = f\ ([\![x]\!]_e b)$
  by (*transfer*, *simp*)

lemma *bop-ueval* [*ueval*]: $[\![bop\ f\ x\ y]\!]_e b = f\ ([\![x]\!]_e b)\ ([\![y]\!]_e b)$
  by (*transfer*, *simp*)

lemma *trop-ueval* [*ueval*]: $[\![trop\ f\ x\ y\ z]\!]_e b = f\ ([\![x]\!]_e b)\ ([\![y]\!]_e b)\ ([\![z]\!]_e b)$
  by (*transfer*, *simp*)

declare *uexpr-defs* [*ueval*]

end

3 Unrestriction

theory *utp-unrest*
imports *utp-expr*
begin

Unrestriction is an encoding of semantic freshness, that allows us to reason about the presence of variables in predicates without being concerned with abstract syntax trees. An expression p is unrestricted by variable x, written $x \sharp p$, if altering the value of x has no effect on the valuation of p. This is a sufficient notion to prove many laws that would ordinarily rely on an *fv* function.

consts
$unrest :: 'a \Rightarrow 'b \Rightarrow bool$

syntax
$\text{-}unrest :: salpha \Rightarrow logic \Rightarrow logic \Rightarrow logic$ (**infix** $\sharp$ *20*)

translations
$\text{-}unrest\ x\ p == CONST\ unrest\ x\ p$

named-theorems *unrest*

lift-definition $unrest\text{-}upred :: ('a, '\alpha)\ uvar \Rightarrow ('b, '\alpha)\ uexpr \Rightarrow bool$
is $\lambda\ x\ e.\ \forall\ b\ v.\ e\ (var\text{-}assign\ x\ v\ b) = e\ b$ **.**

definition $unrest\text{-}dvar\text{-}upred :: 'a::continuum\ dvar \Rightarrow ('b, '\alpha::vst)\ uexpr \Rightarrow bool$ **where**
$unrest\text{-}dvar\text{-}upred\ x\ P = unrest\text{-}upred\ (x\uparrow)\ P$

adhoc-overloading
unrest unrest-upred

lemma *unrest-var-comp* [*unrest*]:
$[\![\ x \sharp P;\ y \sharp P\ ]\!] \Longrightarrow x{\cdot}y \sharp P$
by (*transfer*, *simp add*: *lens-defs*)

lemma *unrest-lit* [*unrest*]: $x \sharp \ll v \gg$
by (*transfer*, *simp*)

The following law demonstrates why we need variable independence: a variable expression is unrestricted by another variable only when the two variables are independent.

lemma *unrest-var* [*unrest*]: $[\![\ uvar\ x;\ x \bowtie y\ ]\!] \Longrightarrow y \sharp var\ x$
by (*transfer*, *auto*)

lemma *unrest-iuvar* [*unrest*]: $[\![\ uvar\ x;\ x \bowtie y\ ]\!] \Longrightarrow \$y \sharp \$x$
by (*metis in-var-indep in-var-uvar unrest-var*)

lemma *unrest-ouvar* [*unrest*]: $[\![\ uvar\ x;\ x \bowtie y\ ]\!] \Longrightarrow \$y' \sharp \$x'$
by (*metis out-var-indep out-var-uvar unrest-var*)

lemma *unrest-iuvar-ouvar* [*unrest*]:
fixes $x :: ('a, '\alpha)\ uvar$
assumes *uvar y*
shows $\$x \sharp \$y'$
by (*metis prod.collapse unrest-upred.rep-eq var.rep-eq var-lookup-out var-update-in*)

lemma *unrest-ouvar-iuvar* [*unrest*]:

fixes x :: ($'a$, $'\alpha$) *uvar*
assumes *uvar y*
shows $\$x\acute{}\ \sharp\ \$y$
by (*metis prod.collapse unrest-upred.rep-eq var.rep-eq var-lookup-in var-update-out*)

lemma *unrest-uop* [*unrest*]: $x \sharp e \Longrightarrow x \sharp$ *uop f e*
by (*transfer*, *simp*)

lemma *unrest-bop* [*unrest*]: $\llbracket x \sharp u; x \sharp v \rrbracket \Longrightarrow x \sharp$ *bop f u v*
by (*transfer*, *simp*)

lemma *unrest-trop* [*unrest*]: $\llbracket x \sharp u; x \sharp v; x \sharp w \rrbracket \Longrightarrow x \sharp$ *trop f u v w*
by (*transfer*, *simp*)

lemma *unrest-eq* [*unrest*]: $\llbracket x \sharp u; x \sharp v \rrbracket \Longrightarrow x \sharp u =_u v$
by (*simp add*: *eq-upred-def*, *transfer*, *simp*)

lemma *unrest-zero* [*unrest*]: $x \sharp 0$
by (*simp add*: *unrest-lit zero-uexpr-def*)

lemma *unrest-one* [*unrest*]: $x \sharp 1$
by (*simp add*: *one-uexpr-def unrest-lit*)

lemma *unrest-numeral* [*unrest*]: $x \sharp$ (*numeral n*)
by (*simp add*: *numeral-uexpr-simp unrest-lit*)

lemma *unrest-plus* [*unrest*]: $\llbracket x \sharp u; x \sharp v \rrbracket \Longrightarrow x \sharp u + v$
by (*simp add*: *plus-uexpr-def unrest*)

lemma *unrest-uminus* [*unrest*]: $x \sharp u \Longrightarrow x \sharp - u$
by (*simp add*: *uminus-uexpr-def unrest*)

lemma *unrest-minus* [*unrest*]: $\llbracket x \sharp u; x \sharp v \rrbracket \Longrightarrow x \sharp u - v$
by (*simp add*: *minus-uexpr-def unrest*)

lemma *unrest-times* [*unrest*]: $\llbracket x \sharp u; x \sharp v \rrbracket \Longrightarrow x \sharp u * v$
by (*simp add*: *times-uexpr-def unrest*)

lemma *unrest-divide* [*unrest*]: $\llbracket x \sharp u; x \sharp v \rrbracket \Longrightarrow x \sharp u / v$
by (*simp add*: *divide-uexpr-def unrest*)

end

4 Substitution

theory *utp-subst*
imports
utp-expr
utp-unrest
begin

4.1 Substitution definitions

We introduce a polymorphic constant that will be used to represent application of a substitution, and also a set of theorems to represent laws.

consts
  usubst :: $'s \Rightarrow 'a \Rightarrow 'a$ (**infixr** † *80*)

named-theorems *usubst*

A substitution is simply a transformation on the alphabet; it shows how variables should be mapped to different values.

type-synonym $'\alpha$ *usubst* = $'\alpha$ *alphabet* $\Rightarrow$ $'\alpha$ *alphabet*

lift-definition *subst* :: $'\alpha$ *usubst* $\Rightarrow$ $('a, '\alpha)$ *uexpr* $\Rightarrow$ $('a, '\alpha)$ *uexpr* **is**
$\lambda\ \sigma\ e\ b.\ e\ (\sigma\ b)$ **.**

adhoc-overloading
  usubst subst

Update the value of a variable to an expression in a substitution

consts *subst-upd* :: $'\alpha$ *usubst* $\Rightarrow$ $'v$ $\Rightarrow$ $('a, '\alpha)$ *uexpr* $\Rightarrow$ $'\alpha$ *usubst*

definition *subst-upd-uvar* :: $'\alpha$ *usubst* $\Rightarrow$ $('a, '\alpha)$ *uvar* $\Rightarrow$ $('a, '\alpha)$ *uexpr* $\Rightarrow$ $'\alpha$ *usubst* **where**
subst-upd-uvar $\sigma\ x\ v = (\lambda\ b.$ *var-assign* $x\ (\llbracket v \rrbracket_e b)\ (\sigma\ b))$

definition *subst-upd-dvar* :: $'\alpha$ *usubst* $\Rightarrow$ $'a$::*continuum dvar* $\Rightarrow$ $('a, '\alpha$::*vst*$)$ *uexpr* $\Rightarrow$ $'\alpha$ *usubst* **where**
subst-upd-dvar $\sigma\ x\ v$ = *subst-upd-uvar* $\sigma\ (x\uparrow)\ v$

adhoc-overloading
  subst-upd subst-upd-uvar **and** *subst-upd subst-upd-dvar*

Lookup the expression associated with a variable in a substitution

lift-definition *usubst-lookup* :: $'\alpha$ *usubst* $\Rightarrow$ $('a, '\alpha)$ *uvar* $\Rightarrow$ $('a, '\alpha)$ *uexpr* $(\langle\text{-}\rangle_s)$
is $\lambda\ \sigma\ x\ b.$ *var-lookup* $x\ (\sigma\ b)$ **.**

Relational lifting of a substitution to the first element of the state space

definition *usubst-rel-lift* :: $'\alpha$ *usubst* $\Rightarrow$ $('\alpha \times '\beta)$ *usubst* $(\lceil\text{-}\rceil_s)$ **where**
$\lceil\sigma\rceil_s = (\lambda\ (A,\ A').\ (\sigma\ A,\ A'))$

definition *usubst-rel-drop* :: $('\alpha \times '\alpha)$ *usubst* $\Rightarrow$ $'\alpha$ *usubst* $(\lfloor\text{-}\rfloor_s)$ **where**
$\lfloor\sigma\rfloor_s = (\lambda\ A.$ *fst* $(\sigma\ (A,$ *undefined*$)))$

nonterminal *smaplet* **and** *smaplets*

syntax
```
  -smaplet  :: [salpha, 'a] => smaplet              (- /↦s/ -)
            :: smaplet => smaplets                  (-)
  -SMaplets :: [smaplet, smaplets] => smaplets      (-,/ -)
  -SubstUpd :: ['m usubst, smaplets] => 'm usubst   (-/'(-') [900,0] 900)
  -Subst    :: smaplets => 'a ~=> 'b                ((1[-]))
```

translations
```
  -SubstUpd m (-SMaplets xy ms)      == -SubstUpd (-SubstUpd m xy) ms
  -SubstUpd m (-smaplet x y)         == CONST subst-upd m x y
  -Subst ms                          == -SubstUpd (CONST id) ms
  -Subst (-SMaplets ms1 ms2)         <= -SubstUpd (-Subst ms1) ms2
  -SMaplets ms1 (-SMaplets ms2 ms3) <= -SMaplets (-SMaplets ms1 ms2) ms3
```

4.2 Substitution laws

We set up a simple substitution tactic that applies substitution and unrestriction laws

method *subst-tac* = (*simp add*: *usubst unrest*)?

lemma *usubst-lookup-id* [*usubst*]: $\langle id \rangle_s\ x = var\ x$
  by (*transfer*, *simp*)

lemma *usubst-lookup-upd* [*usubst*]:
  assumes *semi-uvar x*
  shows $\langle \sigma(x \mapsto_s v) \rangle_s\ x = v$
  using *assms*
  by (*simp add*: *subst-upd-uvar-def*, *transfer*) (*simp*)

lemma *usubst-upd-idem* [*usubst*]:
  assumes *semi-uvar x*
  shows $\sigma(x \mapsto_s u, x \mapsto_s v) = \sigma(x \mapsto_s v)$
  by (*simp add*: *subst-upd-uvar-def assms comp-def*)

lemma *usubst-upd-comm*:
  assumes $x \bowtie y$
  shows $\sigma(x \mapsto_s u, y \mapsto_s v) = \sigma(y \mapsto_s v, x \mapsto_s u)$
  using *assms*
  by (*rule-tac ext*, *auto simp add*: *subst-upd-uvar-def assms comp-def lens-indep-comm*)

lemma *usubst-upd-comm2*:
  assumes $z \bowtie y$ **and** *semi-uvar x*
  shows $\sigma(x \mapsto_s u, y \mapsto_s v, z \mapsto_s s) = \sigma(x \mapsto_s u, z \mapsto_s s, y \mapsto_s v)$
  using *assms*
  by (*rule-tac ext*, *auto simp add*: *subst-upd-uvar-def assms comp-def lens-indep-comm*)

lemma *usubst-upd-var-id* [*usubst*]:
  $uvar\ x \Longrightarrow [x \mapsto_s var\ x] = id$
  apply (*simp add*: *subst-upd-uvar-def*)
  apply (*transfer*)
  apply (*rule ext*)
  apply (*auto*)
done

lemma *usubst-upd-comm-dash* [*usubst*]:
  fixes $x :: ('a, '\alpha)\ uvar$
  shows $\sigma(\$x' \mapsto_s v, \$x \mapsto_s u) = \sigma(\$x \mapsto_s u, \$x' \mapsto_s v)$
  using *in-out-indep usubst-upd-comm* **by** *force*

lemma *usubst-lookup-upd-indep* [*usubst*]:
  assumes *semi-uvar x* $x \bowtie y$
  shows $\langle \sigma(y \mapsto_s v) \rangle_s\ x = \langle \sigma \rangle_s\ x$
  using *assms*
  by (*simp add*: *subst-upd-uvar-def*, *transfer*, *simp*)

lemma *subst-unrest* [*usubst*] : $x \sharp P \Longrightarrow \sigma(x \mapsto_s v) \dagger P = \sigma \dagger P$
  by (*simp add*: *subst-upd-uvar-def*, *transfer*, *auto*)

lemma *id-subst* [*usubst*]: $id \dagger v = v$
  by (*transfer*, *simp*)

lemma *subst-lit* [*usubst*]: $\sigma \dagger \ll v \gg = \ll v \gg$
by (*transfer*, *simp*)

lemma *subst-var* [*usubst*]: $\sigma \dagger var\ x = \langle\sigma\rangle_s\ x$
by (*transfer*, *simp*)

We add the symmetric definition of input and output variables to substitution laws so that the variables are correctly normalised after substitution.

lemma *subst-uop* [*usubst*]: $\sigma \dagger uop\ f\ v = uop\ f\ (\sigma \dagger v)$
by (*transfer*, *simp*)

lemma *subst-bop* [*usubst*]: $\sigma \dagger bop\ f\ u\ v = bop\ f\ (\sigma \dagger u)\ (\sigma \dagger v)$
by (*transfer*, *simp*)

lemma *subst-trop* [*usubst*]: $\sigma \dagger trop\ f\ u\ v\ w = trop\ f\ (\sigma \dagger u)\ (\sigma \dagger v)\ (\sigma \dagger w)$
by (*transfer*, *simp*)

lemma *subst-plus* [*usubst*]: $\sigma \dagger (x + y) = \sigma \dagger x + \sigma \dagger y$
by (*simp add*: *plus-uexpr-def subst-bop*)

lemma *subst-times* [*usubst*]: $\sigma \dagger (x * y) = \sigma \dagger x * \sigma \dagger y$
by (*simp add*: *times-uexpr-def subst-bop*)

lemma *subst-minus* [*usubst*]: $\sigma \dagger (x - y) = \sigma \dagger x - \sigma \dagger y$
by (*simp add*: *minus-uexpr-def subst-bop*)

lemma *subst-zero* [*usubst*]: $\sigma \dagger 0 = 0$
by (*simp add*: *zero-uexpr-def subst-lit*)

lemma *subst-one* [*usubst*]: $\sigma \dagger 1 = 1$
by (*simp add*: *one-uexpr-def subst-lit*)

lemma *subst-eq-upred* [*usubst*]: $\sigma \dagger (x =_u y) = (\sigma \dagger x =_u \sigma \dagger y)$
by (*simp add*: *eq-upred-def usubst*)

lemma *subst-subst* [*usubst*]: $\sigma \dagger \varrho \dagger e = (\varrho \circ \sigma) \dagger e$
by (*transfer*, *simp*)

lemma *subst-upd-comp* [*usubst*]:
fixes $x :: ('a, '\alpha)\ uvar$
shows $\varrho(x \mapsto_s v) \circ \sigma = (\varrho \circ \sigma)(x \mapsto_s \sigma \dagger v)$
by (*rule ext*, *simp add*:*uexpr-defs subst-upd-uvar-def*, *transfer*, *simp*)

lemma *subst-lift-id* [*usubst*]: $\lceil id \rceil_s = id$
by (*simp add*: *usubst-rel-lift-def*)

lemma *subst-drop-id* [*usubst*]: $\lfloor id \rfloor_s = id$
by (*auto simp add*: *usubst-rel-drop-def*)

lemma *subst-lift-drop* [*usubst*]: $\lfloor \lceil \sigma \rceil_s \rfloor_s = \sigma$
by (*simp add*: *usubst-rel-lift-def usubst-rel-drop-def*)

nonterminal *uexprs* **and** *svars* **and** *salphas*

syntax
-psubst :: [$'\alpha$ *usubst*, *svars*, *uexprs*] $\Rightarrow$ *logic*
-subst :: ($'a$, $'\alpha$) *uexpr* $\Rightarrow$ *uexprs* $\Rightarrow$ *salphas* $\Rightarrow$ ($'a$, $'\alpha$) *uexpr* ((-⟦-'/-⟧) [999,999] 1000)
-uexprs :: [($'a$, $'\alpha$) *uexpr*, *uexprs*] => *uexprs* (-,/ -)
:: ($'a$, $'\alpha$) *uexpr* => *uexprs* (-)
-svars :: [*svar*, *svars*] => *svars* (-,/ -)
:: *svar* => *svars* (-)
-salphas :: [*salpha*, *salpha*] => *salphas* (-,/ -)
:: *salpha* => *salphas* (-)

translations
-subst P es vs => *CONST subst* (*-psubst* (*CONST id*) *vs es*) *P*

-psubst m (*-salphas x xs*) (*-uexprs v vs*) => *-psubst* (*-psubst m x v*) *xs vs*
-psubst m x v => *CONST subst-upd m x v*
-subst P e x <= *CONST subst* (*CONST subst-upd* (*CONST id*) *x e*) *P*

end

5 Lifting expressions

theory *utp-lift*
imports
utp-alphabet
begin

5.1 Lifting definitions

We define operators for converting an expression to and from a relational state space

abbreviation *lift-pre* :: ($'a$, $'\alpha$) *uexpr* $\Rightarrow$ ($'a$, $'\alpha \times '\beta$) *uexpr* ($\lceil - \rceil_<$)
where $\lceil P \rceil_< \equiv P \oplus_p fst_L$

abbreviation *drop-pre* :: ($'\alpha \times '\alpha$) *upred* $\Rightarrow$ $'\alpha$ *upred* ($\lfloor - \rfloor_<$)
where $\lfloor P \rfloor_< \equiv P \restriction_p fst_L$

abbreviation *lift-post* :: ($'a$, $'\beta$) *uexpr* $\Rightarrow$ ($'a$, $'\alpha \times '\beta$) *uexpr* ($\lceil - \rceil_>$)
where $\lceil P \rceil_> \equiv P \oplus_p snd_L$

abbreviation *drop-post* :: ($'\alpha \times '\alpha$) *upred* $\Rightarrow$ $'\alpha$ *upred* ($\lfloor - \rfloor_>$)
where $\lfloor P \rfloor_> \equiv P \restriction_p snd_L$

5.2 Lifting laws

lemma *lift-pre-var* [*simp*]:
$\lceil var\ x \rceil_< = \$x$
by (*alpha-tac*)

lemma *lift-post-var* [*simp*]:
$\lceil var\ x \rceil_> = \$x´$
by (*alpha-tac*)

5.3 Substitution laws

lemma *subst-lift-upd* [*usubst*]:
fixes *x* :: ($'a$, $'\alpha$) *uvar*

shows $\lceil \sigma(x \mapsto_s v) \rceil_s = \lceil \sigma \rceil_s(\$x \mapsto_s \lceil v \rceil_<)$
by (*simp add*: *usubst-rel-lift-def subst-upd-uvar-def*, *transfer*, *auto simp add*: *fst-lens-def*)

end

6 Alphabetised Predicates

theory *utp-pred*
imports
utp-expr
utp-subst
begin

An alphabetised predicate is a simply a boolean valued expression

type-synonym $'\alpha$ *upred* = (*bool*, $'\alpha$) *uexpr*

translations
(*type*) $'\alpha$ *upred* <= (*type*) (*bool*, $'\alpha$) *uexpr*

named-theorems *upred-defs*

6.1 Predicate syntax

We want to remain as close as possible to the mathematical UTP syntax, but also want to be conservative with HOL. For this reason we chose not to steal syntax from HOL, but where possible use polymorphism to allow selection of the appropriate operator (UTP vs. HOL). Thus we will first remove the standard syntax for conjunction, disjunction, and negation, and replace these with adhoc overloaded definitions.

no-notation
conj (**infixr** $\wedge$ *35*) **and**
disj (**infixr** $\vee$ *30*) **and**
Not ($\neg$ - [*40*] *40*)

consts
utrue :: $'a$ (*true*)
ufalse :: $'a$ (*false*)
uconj :: $'a \Rightarrow 'a \Rightarrow 'a$ (**infixr** $\wedge$ *35*)
udisj :: $'a \Rightarrow 'a \Rightarrow 'a$ (**infixr** $\vee$ *30*)
uimpl :: $'a \Rightarrow 'a \Rightarrow 'a$ (**infixr** $\Rightarrow$ *25*)
uiff :: $'a \Rightarrow 'a \Rightarrow 'a$ (**infixr** $\Leftrightarrow$ *25*)
unot :: $'a \Rightarrow 'a$ ($\neg$ - [*40*] *40*)
uex :: ($'a$, $'\alpha$) *uvar* $\Rightarrow 'p \Rightarrow 'p$
uall :: ($'a$, $'\alpha$) *uvar* $\Rightarrow 'p \Rightarrow 'p$
ushEx :: [$'a \Rightarrow 'p$] $\Rightarrow 'p$
ushAll :: [$'a \Rightarrow 'p$] $\Rightarrow 'p$

adhoc-overloading
uconj conj **and**
udisj disj **and**
unot Not

We set up two versions of each of the quantifiers: *uex* / *uall* and *ushEx* / *ushAll*. The former pair allows quantification of UTP variables, whilst the latter allows quantification of HOL variables. Both varieties will be needed at various points. Syntactically they are distinguish by a boldface quantifier for the HOL versions (achieved by the "bold" escape in Isabelle).

syntax
  $\text{-}uex$ :: $salpha \Rightarrow logic \Rightarrow logic$ ($\exists$ - $\cdot$ - [0, 10] 10)
  $\text{-}uall$ :: $salpha \Rightarrow logic \Rightarrow logic$ ($\forall$ - $\cdot$ - [0, 10] 10)
  $\text{-}ushEx$ :: $idt \Rightarrow logic \Rightarrow logic$ ($\exists$ - $\cdot$ - [0, 10] 10)
  $\text{-}ushAll$ :: $idt \Rightarrow logic \Rightarrow logic$ ($\forall$ - $\cdot$ - [0, 10] 10)
  $\text{-}ushBEx$ :: $idt \Rightarrow logic \Rightarrow logic \Rightarrow logic$ ($\exists$ - $\in$ - $\cdot$ - [0, 0, 10] 10)
  $\text{-}ushBAll$ :: $idt \Rightarrow logic \Rightarrow logic \Rightarrow logic$ ($\forall$ - $\in$ - $\cdot$ - [0, 0, 10] 10)

translations
  $\exists$ &$x \cdot P$ => $CONST\ uex\ x\ P$
  $\exists$ \$$x \cdot P$ == $CONST\ uex$ ($CONST\ in\text{-}var\ x$) P
  $\exists$ \$$x' \cdot P$ == $CONST\ uex$ ($CONST\ out\text{-}var\ x$) P
  $\exists\ x \cdot P$ == $CONST\ uex\ x\ P$
  $\forall$ &$x \cdot P$ => $CONST\ uall\ x\ P$
  $\forall$ \$$x \cdot P$ == $CONST\ uall$ ($CONST\ in\text{-}var\ x$) P
  $\forall$ \$$x' \cdot P$ == $CONST\ uall$ ($CONST\ out\text{-}var\ x$) P
  $\forall\ x \cdot P$ == $CONST\ uall\ x\ P$
  $\exists\ x \cdot P$ == $CONST\ ushEx$ ($\lambda\ x.\ P$)
  $\exists\ x \in A \cdot P$ => $\exists\ x \cdot \ll x \gg \in_u A \wedge P$
  $\forall\ x \cdot P$ == $CONST\ ushAll$ ($\lambda\ x.\ P$)
  $\forall\ x \in A \cdot P$ => $\forall\ x \cdot \ll x \gg \in_u A \Rightarrow P$

6.2 Predicate operators

We chose to maximally reuse definitions and laws built into HOL. For this reason, when introducing the core operators we proceed by lifting operators from the polymorphic algebraic hiearchy of HOL. Thus the initial definitions take place in the context of type class instantiations. We first introduce our own class called *refine* that will add the refinement operator syntax to the HOL partial order class.

class *refine* = *order*

abbreviation *refineBy* :: $'a{::}refine \Rightarrow 'a \Rightarrow bool$ (**infix** $\sqsubseteq$ 50) **where**
$P \sqsubseteq Q \equiv less\text{-}eq\ Q\ P$

Since, on the whole, lattices in UTP are the opposite way up to the standard definitions in HOL, we syntactically invert the lattice operators. This is the one exception where we do steal HOL syntax, but I think it makes sense for UTP.

notation *inf* (**infixl** $\sqcup$ 70)
notation *sup* (**infixl** $\sqcap$ 65)

notation *Inf* ($\bigsqcup$ - [900] 900)
notation *Sup* ($\bigsqcap$ - [900] 900)

notation *bot* ($\top$)
notation *top* ($\bot$)

We now introduce a partial order on expressions. Note this is more general than refinement since it lifts an order on any expression type (not just Boolean). However, the Boolean version does equate to refinement.

instantiation *uexpr* :: (*order*, *type*) *order*

begin
  lift-definition *less-eq-uexpr* :: $('a, 'b)$ *uexpr* $\Rightarrow$ $('a, 'b)$ *uexpr* $\Rightarrow$ *bool*
  is $\lambda\ P\ Q.\ (\forall\ A.\ P\ A \leq Q\ A)$ **.**
  definition *less-uexpr* :: $('a, 'b)$ *uexpr* $\Rightarrow$ $('a, 'b)$ *uexpr* $\Rightarrow$ *bool*
  where *less-uexpr* $P\ Q = (P \leq Q \wedge \neg\ Q \leq P)$
instance proof
  fix $x\ y\ z$ :: $('a, 'b)$ *uexpr*
  show $(x < y) = (x \leq y \wedge \neg\ y \leq x)$ **by** (*simp add*: *less-uexpr-def*)
  show $x \leq x$ **by** (*transfer*, *auto*)
  show $x \leq y \Longrightarrow y \leq z \Longrightarrow x \leq z$
    by (*transfer*, *blast intro*:*order.trans*)
  show $x \leq y \Longrightarrow y \leq x \Longrightarrow x = y$
    by (*transfer*, *rule ext*, *simp add*: *eq-iff*)
qed
end

We also trivially instantiate our refinement class

instance *uexpr* :: (*order*, *type*) *refine* **..**

Next we introduce the lattice operators, which is again done by lifting.

instantiation *uexpr* :: (*lattice*, *type*) *lattice*
begin
  lift-definition *sup-uexpr* :: $('a, 'b)$ *uexpr* $\Rightarrow$ $('a, 'b)$ *uexpr* $\Rightarrow$ $('a, 'b)$ *uexpr*
  is $\lambda P\ Q\ A.\ sup\ (P\ A)\ (Q\ A)$ **.**
  lift-definition *inf-uexpr* :: $('a, 'b)$ *uexpr* $\Rightarrow$ $('a, 'b)$ *uexpr* $\Rightarrow$ $('a, 'b)$ *uexpr*
  is $\lambda P\ Q\ A.\ inf\ (P\ A)\ (Q\ A)$ **.**
instance
  by (*intro-classes*) (*transfer*, *auto*)+
end

instantiation *uexpr* :: (*bounded-lattice*, *type*) *bounded-lattice*
begin
  lift-definition *bot-uexpr* :: $('a, 'b)$ *uexpr* **is** $\lambda\ A.\ bot$ **.**
  lift-definition *top-uexpr* :: $('a, 'b)$ *uexpr* **is** $\lambda\ A.\ top$ **.**
instance
  by (*intro-classes*) (*transfer*, *auto*)+
end

Finally we show that predicates form a Boolean algebra (under the lattice operators).

instance *uexpr* :: (*boolean-algebra*, *type*) *boolean-algebra*
  by (*intro-classes*, *simp-all add*: *uexpr-defs*)
    (*transfer*, *simp add*: *sup-inf-distrib1 inf-compl-bot sup-compl-top diff-eq*)+

instantiation *uexpr* :: (*complete-lattice*, *type*) *complete-lattice*
begin
  lift-definition *Inf-uexpr* :: $('a, 'b)$ *uexpr set* $\Rightarrow$ $('a, 'b)$ *uexpr*
  is $\lambda\ PS\ A.\ INF\ P{:}PS.\ P(A)$ **.**
  lift-definition *Sup-uexpr* :: $('a, 'b)$ *uexpr set* $\Rightarrow$ $('a, 'b)$ *uexpr*
  is $\lambda\ PS\ A.\ SUP\ P{:}PS.\ P(A)$ **.**
instance
  by (*intro-classes*)
    (*transfer*, *auto intro*: *INF-lower SUP-upper simp add*: *INF-greatest SUP-least*)+
end

With the lattice operators defined, we can proceed to give definitions for the standard predicate operators in terms of them.

definition *true-upred* = (*top* :: $'\alpha$ *upred*)
definition *false-upred* = (*bot* :: $'\alpha$ *upred*)
definition *conj-upred* = (*inf* :: $'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *upred*)
definition *disj-upred* = (*sup* :: $'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *upred*)
definition *not-upred* = (*uminus* :: $'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *upred*)
definition *diff-upred* = (*minus* :: $'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *upred*)

We also define the other predicate operators

lift-definition *impl*::$'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *upred* **is**
$\lambda\ P\ Q\ A.\ P\ A \longrightarrow Q\ A$ **.**

lift-definition *iff-upred* ::$'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *upred* **is**
$\lambda\ P\ Q\ A.\ P\ A \longleftrightarrow Q\ A$ **.**

lift-definition *ex* :: $('a,\ '\alpha)$ *uvar* $\Rightarrow$ $'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *upred* **is**
$\lambda\ x\ P\ b.\ (\exists\ v.\ P(\textit{var-assign}\ x\ v\ b))$ **.**

lift-definition *shEx* ::$['\beta \Rightarrow '\alpha\ \textit{upred}] \Rightarrow\ '\alpha$ *upred* **is**
$\lambda\ P\ A.\ \exists\ x.\ (P\ x)\ A$ **.**

lift-definition *all* :: $('a,\ '\alpha)$ *uvar* $\Rightarrow$ $'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *upred* **is**
$\lambda\ x\ P\ b.\ (\forall\ v.\ P(\textit{var-assign}\ x\ v\ b))$ **.**

lift-definition *shAll* ::$['\beta \Rightarrow '\alpha\ \textit{upred}] \Rightarrow\ '\alpha$ *upred* **is**
$\lambda\ P\ A.\ \forall\ x.\ (P\ x)\ A$ **.**

We have to add a u subscript to the closure operator as I don't want to override the syntax for HOL lists (we'll be using them later).

lift-definition *closure*::$'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *upred* ($[\text{-}]_u$) **is**
$\lambda\ P\ A.\ \forall A'.\ P\ A'$ **.**

lift-definition *taut* :: $'\alpha$ *upred* $\Rightarrow$ *bool* (‘-‘)
is $\lambda\ P.\ \forall\ A.\ P\ A$ **.**

adhoc-overloading
utrue true-upred **and**
ufalse false-upred **and**
unot not-upred **and**
uconj conj-upred **and**
udisj disj-upred **and**
uimpl impl **and**
uiff iff-upred **and**
uex ex **and**
uall all **and**
ushEx shEx **and**
ushAll shAll

6.3 Proof support

We set up a simple tactic with the help of *Eisbach* that applies predicate definitions, applies the transfer method to drop down to the core definitions, applies extensionality (to remove the resulting lambda term) and the applies auto. This simple tactic will suffice to prove most of the standard laws.

method *pred-tac* = ((*simp only*: *upred-defs*)? ; (*transfer*, (*rule-tac ext*)?, *auto simp add*: *lens-defs fun-eq-iff prod.case-eq-if*)?)

declare *true-upred-def* [*upred-defs*]
declare *false-upred-def* [*upred-defs*]
declare *conj-upred-def* [*upred-defs*]
declare *disj-upred-def* [*upred-defs*]
declare *not-upred-def* [*upred-defs*]
declare *diff-upred-def* [*upred-defs*]
declare *subst-upd-uvar-def* [*upred-defs*]
declare *subst-upd-dvar-def* [*upred-defs*]
declare *uexpr-defs* [*upred-defs*]
declare *usubst-rel-lift-def* [*upred-defs*]
declare *usubst-rel-drop-def* [*upred-defs*]

lemma *true-alt-def*: $true = \ll True \gg$
by (*pred-tac*)

lemma *false-alt-def*: $false = \ll False \gg$
by (*pred-tac*)

6.4 Unrestriction Laws

lemma *unrest-true* [*unrest*]: $x \sharp true$
by (*pred-tac*)

lemma *unrest-false* [*unrest*]: $x \sharp false$
by (*pred-tac*)

lemma *unrest-conj* [*unrest*]: $[\![x \sharp P; x \sharp Q]\!] \Longrightarrow x \sharp P \wedge Q$
by (*pred-tac*)

lemma *unrest-disj* [*unrest*]: $[\![x \sharp P; x \sharp Q]\!] \Longrightarrow x \sharp P \vee Q$
by (*pred-tac*)

lemma *unrest-impl* [*unrest*]: $[\![x \sharp P; x \sharp Q]\!] \Longrightarrow x \sharp P \Rightarrow Q$
by (*pred-tac*)

lemma *unrest-iff* [*unrest*]: $[\![x \sharp P; x \sharp Q]\!] \Longrightarrow x \sharp P \Leftrightarrow Q$
by (*pred-tac*)

lemma *unrest-not* [*unrest*]: $x \sharp P \Longrightarrow x \sharp (\neg P)$
by (*pred-tac*)

lemma *unrest-ex-same* [*unrest*]:
semi-uvar $x \Longrightarrow x \sharp (\exists\ x \cdot P)$
by *pred-tac*

lemma *unrest-ex-diff* [*unrest*]:
assumes $x \bowtie y$ $y \sharp P$
shows $y \sharp (\exists\ x \cdot P)$
using *assms*
apply (*pred-tac*)
using *lens-indep-comm* **apply** *fastforce+*
done

lemma *unrest-all-same* [*unrest*]:
  $semi\text{-}uvar\ x \Longrightarrow x \sharp (\forall\ x \cdot P)$
  by *pred-tac*

lemma *unrest-all-diff* [*unrest*]:
  assumes $x \bowtie y$ $y \sharp P$
  shows $y \sharp (\forall\ x \cdot P)$
  using *assms*
  by (*pred-tac*, *simp-all add*: *lens-indep-comm*)

lemma *unrest-shEx* [*unrest*]:
  assumes $\bigwedge\ y.\ x \sharp P(y)$
  shows $x \sharp (\exists\ y \cdot P(y))$
  using *assms* **by** *pred-tac*

lemma *unrest-shAll* [*unrest*]:
  assumes $\bigwedge\ y.\ x \sharp P(y)$
  shows $x \sharp (\forall\ y \cdot P(y))$
  using *assms* **by** *pred-tac*

lemma *unrest-closure* [*unrest*]:
  $x \sharp [P]_u$
  by *pred-tac*

6.5 Substitution Laws

lemma *subst-true* [*usubst*]: $\sigma \dagger true = true$
  by (*pred-tac*)

lemma *subst-false* [*usubst*]: $\sigma \dagger false = false$
  by (*pred-tac*)

lemma *subst-not* [*usubst*]: $\sigma \dagger (\neg\ P) = (\neg\ \sigma \dagger P)$
  by (*pred-tac*)

lemma *subst-impl* [*usubst*]: $\sigma \dagger (P \Rightarrow Q) = (\sigma \dagger P \Rightarrow \sigma \dagger Q)$
  by (*pred-tac*)

lemma *subst-iff* [*usubst*]: $\sigma \dagger (P \Leftrightarrow Q) = (\sigma \dagger P \Leftrightarrow \sigma \dagger Q)$
  by (*pred-tac*)

lemma *subst-disj* [*usubst*]: $\sigma \dagger (P \vee Q) = (\sigma \dagger P \vee \sigma \dagger Q)$
  by (*pred-tac*)

lemma *subst-conj* [*usubst*]: $\sigma \dagger (P \wedge Q) = (\sigma \dagger P \wedge \sigma \dagger Q)$
  by (*pred-tac*)

lemma *subst-closure* [*usubst*]: $\sigma \dagger [P]_u = [P]_u$
  by (*pred-tac*)

lemma *subst-shEx* [*usubst*]: $\sigma \dagger (\exists\ x \cdot P(x)) = (\exists\ x \cdot \sigma \dagger P(x))$
  by *pred-tac*

lemma *subst-shAll* [*usubst*]: $\sigma \dagger (\forall\ x \cdot P(x)) = (\forall\ x \cdot \sigma \dagger P(x))$
  by *pred-tac*

TODO: Generalise the quantifier substitution laws to n-ary substitutions

lemma *subst-ex-same* [*usubst*]:
  assumes *semi-uvar* x
  shows $(\exists\ x \cdot P)[\![v/x]\!] = (\exists\ x \cdot P)$
  by (*simp add*: *assms id-subst subst-unrest unrest-ex-same*)

lemma *subst-ex-indep* [*usubst*]:
  assumes $x \bowtie y$ $y \sharp v$
  shows $(\exists\ y \cdot P)[\![v/x]\!] = (\exists\ y \cdot P[\![v/x]\!])$
  using *assms*
  apply (*pred-tac*)
  using *lens-indep-comm* **apply** *fastforce+*
done

lemma *subst-all-same* [*usubst*]:
  assumes *semi-uvar* x
  shows $(\forall\ x \cdot P)[\![v/x]\!] = (\forall\ x \cdot P)$
  by (*simp add*: *assms id-subst subst-unrest unrest-all-same*)

lemma *subst-all-indep* [*usubst*]:
  assumes $x \bowtie y$ $y \sharp v$
  shows $(\forall\ y \cdot P)[\![v/x]\!] = (\forall\ y \cdot P[\![v/x]\!])$
  using *assms*
  by (*pred-tac*, *simp-all add*: *lens-indep-comm*)

6.6 Predicate Laws

Showing that predicates form a Boolean Algebra (under the predicate operators) gives us many useful laws.

interpretation *boolean-algebra diff-upred not-upred conj-upred op* $\leq$ *op* $<$ *disj-upred false-upred true-upred*
  by (*unfold-locales*, *pred-tac+*)

lemma *refBy-order*: $P \sqsubseteq Q$ = ‘$Q \Rightarrow P$‘
  by (*transfer*, *auto*)

lemma *conj-idem* [*simp*]: $((P::'\alpha\ upred) \wedge P) = P$
  by *pred-tac*

lemma *disj-idem* [*simp*]: $((P::'\alpha\ upred) \vee P) = P$
  by *pred-tac*

lemma *conj-comm*: $((P::'\alpha\ upred) \wedge Q) = (Q \wedge P)$
  by *pred-tac*

lemma *disj-comm*: $((P::'\alpha\ upred) \vee Q) = (Q \vee P)$
  by *pred-tac*

lemma *conj-subst*: $P = R \Longrightarrow ((P::'\alpha\ upred) \wedge Q) = (R \wedge Q)$
  by *pred-tac*

lemma *disj-subst*: $P = R \Longrightarrow ((P::'\alpha\ upred) \vee Q) = (R \vee Q)$
  by *pred-tac*

lemma *conj-assoc*:$(((P::'\alpha\ upred) \wedge Q) \wedge S) = (P \wedge (Q \wedge S))$

by *pred-tac*

lemma *disj-assoc*:$(((P::'\alpha\ upred) \vee Q) \vee S) = (P \vee (Q \vee S))$
by *pred-tac*

lemma *conj-disj-abs*:$((P::'\alpha\ upred) \wedge (P \vee Q)) = P$
by *pred-tac*

lemma *disj-conj-abs*:$((P::'\alpha\ upred) \vee (P \wedge Q)) = P$
by *pred-tac*

lemma *conj-disj-distr*:$((P::'\alpha\ upred) \wedge (Q \vee R)) = ((P \wedge Q) \vee (P \wedge R))$
by *pred-tac*

lemma *disj-conj-distr*:$((P::'\alpha\ upred) \vee (Q \wedge R)) = ((P \vee Q) \wedge (P \vee R))$
by *pred-tac*

lemma *true-disj-zero* [*simp*]:
$(P \vee \mathit{true}) = \mathit{true}$ $(\mathit{true} \vee P) = \mathit{true}$
by (*pred-tac*) (*pred-tac*)

lemma *true-conj-zero* [*simp*]:
$(P \wedge \mathit{false}) = \mathit{false}$ $(\mathit{false} \wedge P) = \mathit{false}$
by (*pred-tac*) (*pred-tac*)

lemma *imp-vacuous* [*simp*]: $(\mathit{false} \Rightarrow u) = \mathit{true}$
by *pred-tac*

lemma *imp-true* [*simp*]: $(p \Rightarrow \mathit{true}) = \mathit{true}$
by *pred-tac*

lemma *true-imp* [*simp*]: $(\mathit{true} \Rightarrow p) = p$
by *pred-tac*

lemma *p-and-not-p* [*simp*]: $(P \wedge \neg P) = \mathit{false}$
by *pred-tac*

lemma *p-or-not-p* [*simp*]: $(P \vee \neg P) = \mathit{true}$
by *pred-tac*

lemma *p-imp-p* [*simp*]: $(P \Rightarrow P) = \mathit{true}$
by *pred-tac*

lemma *p-iff-p* [*simp*]: $(P \Leftrightarrow P) = \mathit{true}$
by *pred-tac*

lemma *p-imp-false* [*simp*]: $(P \Rightarrow \mathit{false}) = (\neg P)$
by *pred-tac*

lemma *not-conj-deMorgans* [*simp*]: $(\neg ((P::'\alpha\ upred) \wedge Q)) = ((\neg P) \vee (\neg Q))$
by *pred-tac*

lemma *not-disj-deMorgans* [*simp*]: $(\neg ((P::'\alpha\ upred) \vee Q)) = ((\neg P) \wedge (\neg Q))$
by *pred-tac*

lemma *conj-disj-not-abs* [*simp*]: $((P::'\alpha\ upred) \wedge ((\neg P) \vee Q)) = (P \wedge Q)$
  by (*pred-tac*)

lemma *double-negation* [*simp*]: $(\neg \neg (P::'\alpha\ upred)) = P$
  by (*pred-tac*)

lemma *true-not-false* [*simp*]: $true \neq false\ false \neq true$
  by *pred-tac+*

lemma *closure-conj-distr*: $([P]_u \wedge [Q]_u) = [P \wedge Q]_u$
  by *pred-tac*

lemma *closure-imp-distr*: ‘$[P \Rightarrow Q]_u \Rightarrow [P]_u \Rightarrow [Q]_u$‘
  by *pred-tac*

lemma *true-iff* [*simp*]: $(P \Leftrightarrow true) = P$
  by *pred-tac*

lemma *impl-alt-def*: $(P \Rightarrow Q) = (\neg P \vee Q)$
  by *pred-tac*

lemma *eq-upred-refl* [*simp*]: $(x =_u x) = true$
  by *pred-tac*

lemma *eq-upred-sym*: $(x =_u y) = (y =_u x)$
  by *pred-tac*

lemma *conj-eq-in-var-subst*:
  fixes $x :: ('a, '\alpha)\ uvar$
  assumes *uvar x*
  shows $(P \wedge \$x =_u v) = (P[\![v/\$x]\!] \wedge \$x =_u v)$
  using *assms*
  by (*pred-tac*, (*metis vwb-lens-wb wb-lens.get-put*)+)

lemma *conj-eq-out-var-subst*:
  fixes $x :: ('a, '\alpha)\ uvar$
  assumes *uvar x*
  shows $(P \wedge \$x' =_u v) = (P[\![v/\$x']\!] \wedge \$x' =_u v)$
  using *assms*
  by (*pred-tac*, (*metis vwb-lens-wb wb-lens.get-put*)+)

lemma *shEx-bool* [*simp*]: *shEx P* = (*P True* ∨ *P False*)
  by (*pred-tac*, *metis* (*full-types*))

lemma *shAll-bool* [*simp*]: *shAll P* = (*P True* ∧ *P False*)
  by (*pred-tac*, *metis* (*full-types*))

lemma *upred-eq-true* [*simp*]: $(p =_u true) = p$
  by *pred-tac*

lemma *upred-eq-false* [*simp*]: $(p =_u false) = (\neg p)$
  by *pred-tac*

lemma *one-point*:
  assumes *semi-uvar x* $x \sharp v$

shows $(\exists\ x \cdot (P \wedge (var\ x =_u v))) = P\llbracket v/x\rrbracket$
using *assms*
by (*simp add*: *upred-defs*, *transfer*, *auto*)

lemma *uvar-assign-exists*:
$uvar\ x \Longrightarrow \exists\ v.\ b = var\text{-}assign\ x\ v\ b$
by (*rule-tac x=var-lookup x b* **in** *exI*, *simp*)

lemma *uvar-obtain-assign*:
assumes *uvar x*
obtains *v* **where** $b = var\text{-}assign\ x\ v\ b$
using *assms*
by (*drule-tac uvar-assign-exists*[*of - b*], *auto*)

lemma *taut-split-subst*:
assumes *uvar x*
shows $`P` \longleftrightarrow (\forall\ v.\ `P\llbracket\ll v\gg/x\rrbracket`)$
using *assms*
by (*pred-tac*, *metis uvar-assign-exists*)

lemma *eq-split*:
assumes $`P \Rightarrow Q`$ $`Q \Rightarrow P`$
shows $P = Q$
using *assms*
by (*pred-tac*)

lemma *subst-bool-split*:
assumes *uvar x*
shows $`P` = `(P\llbracket false/x\rrbracket \wedge P\llbracket true/x\rrbracket)`$
proof –
from *assms* **have** $`P` = (\forall\ v.\ `P\llbracket\ll v\gg/x\rrbracket`)$
by (*subst taut-split-subst*[*of x*], *auto*)
also have ... $= (`P\llbracket\ll True\gg/x\rrbracket` \wedge `P\llbracket\ll False\gg/x\rrbracket`)$
by (*metis* (*mono-tags*, *lifting*))
also have ... $= `(P\llbracket false/x\rrbracket \wedge P\llbracket true/x\rrbracket)`$
by (*pred-tac*)
finally show *?thesis* **.**
qed

lemma *taut-iff-eq*:
$`P \Leftrightarrow Q` \longleftrightarrow (P = Q)$
by *pred-tac*

lemma *subst-eq-replace*:
fixes $x :: ('a, '\alpha)\ uvar$
shows $(p\llbracket u/x\rrbracket \wedge u =_u v) = (p\llbracket v/x\rrbracket \wedge u =_u v)$
by *pred-tac*

lemma *exists-twice*: $semi\text{-}uvar\ x \Longrightarrow (\exists\ x \cdot \exists\ x \cdot P) = (\exists\ x \cdot P)$
by (*pred-tac*)

lemma *all-twice*: $semi\text{-}uvar\ x \Longrightarrow (\forall\ x \cdot \forall\ x \cdot P) = (\forall\ x \cdot P)$
by (*pred-tac*)

lemma *ex-commute*:

assumes $x \bowtie y$
shows $(\exists\ x \cdot \exists\ y \cdot P) = (\exists\ y \cdot \exists\ x \cdot P)$
using *assms*
apply (*pred-tac*)
using *lens-indep-comm* **apply** *fastforce+*
done

lemma *all-commute*:
assumes $x \bowtie y$
shows $(\forall\ x \cdot \forall\ y \cdot P) = (\forall\ y \cdot \forall\ x \cdot P)$
using *assms*
apply (*pred-tac*)
using *lens-indep-comm* **apply** *fastforce+*
done

6.7 Quantifier lifting

named-theorems *uquant-lift*

lemma *shEx-lift-conj-1* [*uquant-lift*]:
$((\exists\ x \cdot P(x)) \wedge Q) = (\exists\ x \cdot P(x) \wedge Q)$
by *pred-tac*

lemma *shEx-lift-conj-2* [*uquant-lift*]:
$(P \wedge (\exists\ x \cdot Q(x))) = (\exists\ x \cdot P \wedge Q(x))$
by *pred-tac*

end

7 Alphabetised relations

theory *utp-rel*
imports
utp-pred
utp-lift
begin

default-sort *type*

named-theorems *urel-defs*

consts
useq :: $'a \Rightarrow 'b \Rightarrow 'c$ (**infixr** ;; *15*)
uskip :: $'a$ (*II*)

definition $in\alpha$ :: $('\alpha, '\alpha \times '\beta)$ *uvar* **where**
$in\alpha = (\!|\ lens\text{-}get = fst,\ lens\text{-}put = \lambda\ (A, A')\ v.\ (v, A')\ |\!)$

definition $out\alpha$ :: $('\beta, '\alpha \times '\beta)$ *uvar* **where**
$out\alpha = (\!|\ lens\text{-}get = snd,\ lens\text{-}put = \lambda\ (A, A')\ v.\ (A, v)\ |\!)$

declare *inα-def* [*urel-defs*]
declare *outα-def* [*urel-defs*]

The alphabet of a relation consists of the input and output portions

lemma *alpha-in-out*:
  $\Sigma \approx_L in\alpha +_L out\alpha$
  by (*metis fst-lens-def fst-snd-id-lens inα-def lens-equiv-refl outα-def snd-lens-def*)

type-synonym $'\alpha$ *condition* $= '\alpha$ *upred*
type-synonym $('\alpha, '\beta)$ *relation* $= ('\alpha \times '\beta)$ *upred*
type-synonym $'\alpha$ *hrelation* $= ('\alpha \times '\alpha)$ *upred*

definition *cond*::$('\alpha, '\beta)$ *relation* $\Rightarrow ('\alpha, '\beta)$ *relation* $\Rightarrow ('\alpha, '\beta)$ *relation* $\Rightarrow ('\alpha, '\beta)$ *relation*
((3- ◁ - ▷/ -) [14,0,15] 14)
where $(P \triangleleft b \triangleright Q) \equiv (b \wedge P) \vee ((\neg b) \wedge Q)$

abbreviation *rcond*::$('\alpha, '\beta)$ *relation* $\Rightarrow '\alpha$ *condition* $\Rightarrow ('\alpha, '\beta)$ *relation* $\Rightarrow ('\alpha, '\beta)$ *relation*
((3- ◁ - $\triangleright_r$ / -) [14,0,15] 14)
where $(P \triangleleft b \triangleright_r Q) \equiv (P \triangleleft \lceil b \rceil_< \triangleright Q)$

lift-definition *seqr*::$(('\alpha \times '\beta)$ *upred*$) \Rightarrow (('\beta \times '\gamma)$ *upred*$) \Rightarrow ('\alpha \times '\gamma)$ *upred*
is $\lambda\ P\ Q\ r.\ r : (\{p.\ P\ p\}\ O\ \{q.\ Q\ q\})$ **.**

lift-definition *conv-r* :: $('a, '\alpha \times '\beta)$ *uexpr* $\Rightarrow ('a, '\beta \times '\alpha)$ *uexpr* (-$^-$ [999] 999)
is $\lambda\ e\ (b1, b2).\ e\ (b2, b1)$ **.**

lift-definition *assigns-r* :: $'\alpha$ *usubst* $\Rightarrow '\alpha$ *hrelation* $(\langle \text{-} \rangle_a)$
  is $\lambda\ \sigma\ (A, A').\ A' = \sigma(A)$ **.**

definition *skip-r* :: $'\alpha$ *hrelation* **where**
skip-r = *assigns-r id*

abbreviation *assign-r* :: $('t, '\alpha)$ *uvar* $\Rightarrow ('t, '\alpha)$ *uexpr* $\Rightarrow '\alpha$ *hrelation*
where *assign-r x v* $\equiv$ *assigns-r* $[x \mapsto_s v]$

abbreviation *assign-2-r* ::
  $('t1, '\alpha)$ *uvar* $\Rightarrow ('t2, '\alpha)$ *uvar* $\Rightarrow ('t1, '\alpha)$ *uexpr* $\Rightarrow ('t2, '\alpha)$ *uexpr* $\Rightarrow '\alpha$ *hrelation*
where *assign-2-r x y u v* $\equiv$ *assigns-r* $[x \mapsto_s u, y \mapsto_s v]$

nonterminal
  id-list **and** *uexpr-list*

syntax
  -id-unit :: *id* $\Rightarrow$ *id-list* (-)
  -id-list :: *id* $\Rightarrow$ *id-list* $\Rightarrow$ *id-list* (-,/ -)
  -uexpr-unit :: $('a, '\alpha)$ *uexpr* $\Rightarrow$ *uexpr-list* (- [40] 40)
  -uexpr-list :: $('a, '\alpha)$ *uexpr* $\Rightarrow$ *uexpr-list* $\Rightarrow$ *uexpr-list* (-,/ - [40,40] 40)
  -assignment :: *salphas* $\Rightarrow$ *uexprs* $\Rightarrow '\alpha$ *hrelation* (**infixr** := 55)
  -mk-usubst :: *salphas* $\Rightarrow$ *uexpr-list* $\Rightarrow '\alpha$ *usubst*

translations
  -mk-usubst (*-salphaid x*) (*-uexpr-unit v*) == $[x \mapsto_s v]$
  -mk-usubst (*-id-list x xs*) (*-uexpr-list v vs*) == (*-mk-usubst xs vs*)$(x \mapsto_s v)$
  -assignment xs vs => *CONST assigns-r* (*-psubst* (*CONST id*) *xs vs*)
  x := *v* <= *CONST assign-r x v*
  x,y := *u,v* <= *CONST assign-2-r x y u v*

adhoc-overloading
  useq seqr **and**

uskip skip-r

method *rel-tac* = ((*simp add*: *upred-defs urel-defs*)?, (*transfer*, (*rule-tac ext*)?, *auto simp add*: *lens-defs urel-defs relcomp-unfold fun-eq-iff prod.case-eq-if*)?)

A test is like a precondition, except that it identifies to the postcondition. It forms the basis for Kleene Algebra with Tests (KAT).

definition *lift-test* :: $'\alpha$ *condition* $\Rightarrow$ $'\alpha$ *hrelation* ($\lceil$-$\rceil_t$)
where $\lceil b \rceil_t = (\lceil b \rceil_< \wedge II)$

declare *cond-def* [*urel-defs*]
declare *skip-r-def* [*urel-defs*]

We implement a poor man's version of alphabet restriction that hides a variable within a relation

definition *rel-var-res* :: $'\alpha$ *hrelation* $\Rightarrow$ ($'a$, $'\alpha$) *uvar* $\Rightarrow$ $'\alpha$ *hrelation* (**infix** $\restriction_\alpha$ *80*) **where**
$P \restriction_\alpha x = (\exists\ \$x \cdot \exists\ \$x' \cdot P)$

declare *rel-var-res-def* [*urel-defs*]

7.1 Unrestriction Laws

lemma *unrest-iuvar* [*unrest*]: *semi-uvar x* $\Longrightarrow$ *out*α $\sharp$ $\$x$
by (*simp add*: *out*α*-def*, *transfer*, *auto*)

lemma *unrest-ouvar* [*unrest*]: *semi-uvar x* $\Longrightarrow$ *in*α $\sharp$ $\$x'$
by (*simp add*: *in*α*-def*, *transfer*, *auto*)

lemma *unrest-in*α*-var* [*unrest*]:
$\llbracket$ *semi-uvar x*; *in*α $\sharp$ P $\rrbracket$ $\Longrightarrow$ $\$x \sharp P$
by (*pred-tac*, *simp add*: *in*α*-def*)

lemma *unrest-out*α*-var* [*unrest*]:
$\llbracket$ *semi-uvar x*; *out*α $\sharp$ P $\rrbracket$ $\Longrightarrow$ $\$x' \sharp P$
by (*pred-tac*, *simp add*: *out*α*-def*)

lemma *in*α*-uvar* [*simp*]: *uvar in*α
by (*unfold-locales*, *auto simp add*: *in*α*-def*)

lemma *out*α*-uvar* [*simp*]: *uvar out*α
by (*unfold-locales*, *auto simp add*: *out*α*-def*)

lemma *unrest-pre-out*α [*unrest*]: *out*α $\sharp$ $\lceil b \rceil_<$
by (*transfer*, *auto simp add*: *out*α*-def*)

lemma *unrest-post-in*α [*unrest*]: *in*α $\sharp$ $\lceil b \rceil_>$
by (*transfer*, *auto simp add*: *in*α*-def*)

lemma *unrest-pre-in-var* [*unrest*]:
$x \sharp p1 \Longrightarrow \$x \sharp \lceil p1 \rceil_<$
by (*transfer*, *simp*)

lemma *unrest-post-out-var* [*unrest*]:
$x \sharp p1 \Longrightarrow \$x' \sharp \lceil p1 \rceil_>$
by (*transfer*, *simp*)

lemma *unrest-convr-outα* [*unrest*]:
  $in\alpha \sharp p \Longrightarrow out\alpha \sharp p^-$
  by (*transfer*, *auto simp add*: *inα-def outα-def*)

lemma *unrest-convr-inα* [*unrest*]:
  $out\alpha \sharp p \Longrightarrow in\alpha \sharp p^-$
  by (*transfer*, *auto simp add*: *inα-def outα-def*)

lemma *unrest-in-rel-var-res* [*unrest*]:
  $uvar\ x \Longrightarrow \$x \sharp (P \restriction_\alpha x)$
  by (*simp add*: *rel-var-res-def unrest*)

lemma *unrest-out-rel-var-res* [*unrest*]:
  $uvar\ x \Longrightarrow \$x' \sharp (P \restriction_\alpha x)$
  by (*simp add*: *rel-var-res-def unrest*)

7.2 Substitution laws

It should be possible to substantially generalise the following two laws

lemma *usubst-seq-left* [*usubst*]:
  $[\![semi\text{-}uvar\ x;\ out\alpha \sharp v]\!] \Longrightarrow (P ;; Q)[\![v/\$x]\!] = ((P[\![v/\$x]\!]) ;; Q)$
  apply (*rel-tac*)
  apply (*rename-tac x v P Q a y ya*)
  apply (*rule-tac x=ya* **in** *exI*)
  apply (*simp*)
  apply (*drule-tac x=a* **in** *spec*)
  apply (*drule-tac x=y* **in** *spec*)
  apply (*drule-tac x=ya* **in** *spec*)
  apply (*simp*)
  apply (*rename-tac x v P Q a ba y*)
  apply (*rule-tac x=y* **in** *exI*)
  apply (*drule-tac x=a* **in** *spec*)
  apply (*drule-tac x=y* **in** *spec*)
  apply (*drule-tac x=ba* **in** *spec*)
  apply (*simp*)
done

lemma *usubst-seq-right* [*usubst*]:
  $[\![semi\text{-}uvar\ x;\ in\alpha \sharp v]\!] \Longrightarrow (P ;; Q)[\![v/\$x']\!] = (P ;; Q[\![v/\$x']\!])$
  by (*rel-tac*, *metis+*)

lemma *usubst-condr* [*usubst*]:
  $\sigma \dagger (P \triangleleft b \triangleright Q) = (\sigma \dagger P \triangleleft \sigma \dagger b \triangleright \sigma \dagger Q)$
  by *rel-tac*

lemma *subst-skip-r* [*usubst*]:
  fixes $x :: ('a, '\alpha)\ uvar$
  shows $II[\![\lceil v \rceil_</\$x]\!] = (x := v)$
  by (*rel-tac*)

7.3 Relation laws

Homogeneous relations form a quantale

abbreviation *truer* :: $'\alpha\ hrelation\ (true_h)$ **where**

truer $\equiv$ *true*

abbreviation *falser* :: $'\alpha$ *hrelation* ($false_h$) **where**
falser $\equiv$ *false*

interpretation *upred-quantale*: *unital-quantale-plus*
 where *times* = *seqr* **and** *one* = *skip-r* **and** *Sup* = *Sup* **and** *Inf* = *Inf* **and** *inf* = *inf* **and** *less-eq* = *less-eq* **and** *less* = *less*
 and *sup* = *sup* **and** *bot* = *bot* **and** *top* = *top*
apply (*unfold-locales*)
apply (*rel-tac*)
apply (*unfold SUP-def*, *transfer*, *auto*)
apply (*unfold SUP-def*, *transfer*, *auto*)
apply (*unfold INF-def*, *transfer*, *auto*)
apply (*unfold INF-def*, *transfer*, *auto*)
apply (*rel-tac*)
apply (*rel-tac*)
done

lemma *drop-pre-inv* [*simp*]: $[\![$ *out*α $\sharp$ *p* $]\!] \Longrightarrow \lceil \lfloor p \rfloor_{<} \rceil_{<} = p$
 by (*pred-tac*, *auto simp add*: *out*α*-def lens-create-def fst-lens-def prod.case-eq-if*)

abbreviation *ustar* :: $'\alpha$ *hrelation* $\Rightarrow$ $'\alpha$ *hrelation* ($\text{-}^{\star}{}_{u}$ [*999*] *999*) **where**
$P^{\star}{}_{u}$ $\equiv$ *unital-quantale.qstar II op* ;; *Sup P*

definition *while* :: $'\alpha$ *condition* $\Rightarrow$ $'\alpha$ *hrelation* $\Rightarrow$ $'\alpha$ *hrelation* (*while* - *do* - *od*) **where**
while b do P od = $((\lceil b \rceil_{<} \wedge P)^{\star}{}_{u} \wedge (\neg\, \lceil b \rceil_{>}))$

declare *while-def* [*urel-defs*]

lemma *cond-idem*:$(P \triangleleft b \triangleright P) = P$ **by** *rel-tac*

lemma *cond-symm*:$(P \triangleleft b \triangleright Q) = (Q \triangleleft \neg\, b \triangleright P)$ **by** *rel-tac*

lemma *cond-assoc*: $((P \triangleleft b \triangleright Q) \triangleleft c \triangleright R) = (P \triangleleft b \wedge c \triangleright (Q \triangleleft c \triangleright R))$ **by** *rel-tac*

lemma *cond-distr*: $(P \triangleleft b \triangleright (Q \triangleleft c \triangleright R)) = ((P \triangleleft b \triangleright Q) \triangleleft c \triangleright (P \triangleleft b \triangleright R))$ **by** *rel-tac*

lemma *cond-unit-T*:$(P \triangleleft true \triangleright Q) = P$ **by** *rel-tac*

lemma *cond-unit-F*:$(P \triangleleft false \triangleright Q) = Q$ **by** *rel-tac*

lemma *cond-L6*: $(P \triangleleft b \triangleright (Q \triangleleft b \triangleright R)) = (P \triangleleft b \triangleright R)$ **by** *rel-tac*

lemma *cond-L7*: $(P \triangleleft b \triangleright (P \triangleleft c \triangleright Q)) = (P \triangleleft b \vee c \triangleright Q)$ **by** *rel-tac*

lemma *cond-and-distr*: $((P \wedge Q) \triangleleft b \triangleright (R \wedge S)) = ((P \triangleleft b \triangleright R) \wedge (Q \triangleleft b \triangleright S))$ **by** *rel-tac*

lemma *cond-or-distr*: $((P \vee Q) \triangleleft b \triangleright (R \vee S)) = ((P \triangleleft b \triangleright R) \vee (Q \triangleleft b \triangleright S))$ **by** *rel-tac*

lemma *cond-imp-distr*:
$((P \Rightarrow Q) \triangleleft b \triangleright (R \Rightarrow S)) = ((P \triangleleft b \triangleright R) \Rightarrow (Q \triangleleft b \triangleright S))$ **by** *rel-tac*

lemma *cond-eq-distr*:
$((P \Leftrightarrow Q) \triangleleft b \triangleright (R \Leftrightarrow S)) = ((P \triangleleft b \triangleright R) \Leftrightarrow (Q \triangleleft b \triangleright S))$ **by** *rel-tac*

lemma *cond-conj-distr*:$(P \wedge (Q \triangleleft b \triangleright S)) = ((P \wedge Q) \triangleleft b \triangleright (P \wedge S))$ **by** *rel-tac*

lemma *cond-disj-distr*:$(P \vee (Q \triangleleft b \triangleright S)) = ((P \vee Q) \triangleleft b \triangleright (P \vee S))$ **by** *rel-tac*

lemma *cond-neg*: $\neg (P \triangleleft b \triangleright Q) = (\neg P \triangleleft b \triangleright \neg Q)$ **by** *rel-tac*

lemma *comp-cond-left-distr*:
$((P \triangleleft b \triangleright_r Q) ;; R) = ((P ;; R) \triangleleft b \triangleright_r (Q ;; R))$
by *rel-tac*

These laws may seem to duplicate quantale laws, but they don't – they are applicable to non-homogeneous relations as well, which will become important later.

lemma *seqr-assoc*: $(P ;; (Q ;; R)) = ((P ;; Q) ;; R)$
by *rel-tac*

lemma *seqr-left-unit* [*simp*]:
$(II ;; P) = P$
by *rel-tac*

lemma *seqr-right-unit* [*simp*]:
$(P ;; II) = P$
by *rel-tac*

lemma *seqr-left-zero* [*simp*]:
$(\mathit{false} ;; P) = \mathit{false}$
by *pred-tac*

lemma *seqr-right-zero* [*simp*]:
$(P ;; \mathit{false}) = \mathit{false}$
by *pred-tac*

lemma *seqr-mono*:
$[\![P_1 \sqsubseteq P_2; Q_1 \sqsubseteq Q_2]\!] \Longrightarrow (P_1 ;; Q_1) \sqsubseteq (P_2 ;; Q_2)$
by (*rel-tac*, *blast*)

lemma *pre-skip-post*: $(\lceil b \rceil_< \wedge II) = (II \wedge \lceil b \rceil_>)$
by (*rel-tac*)

lemma *seqr-exists-left*:
semi-uvar $x \Longrightarrow ((\exists \$x \cdot P) ;; Q) = (\exists \$x \cdot (P ;; Q))$
by (*rel-tac*)

lemma *seqr-exists-right*:
semi-uvar $x \Longrightarrow (P ;; (\exists \$x' \cdot Q)) = (\exists \$x' \cdot (P ;; Q))$
by (*rel-tac*)

We should be able to generalise this law to arbitrary assignments at some point, but that requires additional conversion operators for substitutions that act only on *in*α.

lemma *assign-subst* [*usubst*]:
$[\![$ *semi-uvar* x; *semi-uvar* y $]\!] \Longrightarrow [\$x \mapsto_s \lceil u \rceil_<] \dagger (y := v) = (x,\ y := u,\ [x \mapsto_s u] \dagger v)$
by *rel-tac*

lemma *assigns-idem*: *semi-uvar* $x \Longrightarrow (x,x := u,v) = (x := v)$
by (*simp add*: *usubst*)

lemma *assigns-comp*: $(assigns\text{-}r\ f\ ;;\ assigns\text{-}r\ g) = assigns\text{-}r\ (g \circ f)$
by (*transfer*, *auto simp add*:*relcomp-unfold*)

lemma *assigns-r-comp*: $(\langle\sigma\rangle_a\ ;;\ P) = (\lceil\sigma\rceil_s \dagger P)$
by *rel-tac*

lemma *assign-r-comp*: $semi\text{-}uvar\ x \Longrightarrow (x := u\ ;;\ P) = ([\$x \mapsto_s \lceil u\rceil_<] \dagger P)$
by (*simp add*: *assigns-r-comp usubst*)

lemma *assign-test*: $semi\text{-}uvar\ x \Longrightarrow (x := \ll u\gg\ ;;\ x := \ll v\gg) = (x := \ll v\gg)$
by (*simp add*: *assigns-comp subst-upd-comp subst-lit usubst-upd-idem*)

lemma *skip-r-unfold*:
$uvar\ x \Longrightarrow II = (\$x\acute{} =_u \$x \wedge II\restriction_\alpha x)$
by (*rel-tac*, *blast*, *metis mwb-lens.put-put vwb-lens-mwb vwb-lens-wb wb-lens.get-put*)

lemma *assign-unfold*:
$uvar\ x \Longrightarrow (x := v) = (\$x\acute{} =_u \lceil v\rceil_< \wedge II\restriction_\alpha x)$
apply (*rel-tac*, *auto simp add*: *comp-def*)
using *vwb-lens.put-eq* **by** *fastforce*

lemma *seqr-or-distl*:
$((P \vee Q)\ ;;\ R) = ((P\ ;;\ R) \vee (Q\ ;;\ R))$
by *rel-tac*

lemma *seqr-or-distr*:
$(P\ ;;\ (Q \vee R)) = ((P\ ;;\ Q) \vee (P\ ;;\ R))$
by *rel-tac*

lemma *seqr-middle*:
assumes *uvar x*
shows $(P\ ;;\ Q) = (\exists\ v \cdot P[\![\ll v\gg/\$x\acute{}]\!]\ ;;\ Q[\![\ll v\gg/\$x]\!])$
using *assms*
apply (*rel-tac*)
apply (*rename-tac xa P Q a b y*)
apply (*rule-tac x=var-lookup xa y* **in** *exI*)
apply (*rule-tac x=y* **in** *exI*)
apply (*simp*)
done

theorem *precond-equiv*:
$P = (P\ ;;\ true) \longleftrightarrow (out\alpha \sharp P)$
by (*rel-tac*)

theorem *postcond-equiv*:
$P = (true\ ;;\ P) \longleftrightarrow (in\alpha \sharp P)$
by (*rel-tac*)

lemma *precond-right-unit*: $out\alpha \sharp p \Longrightarrow (p\ ;;\ true) = p$
by (*metis precond-equiv*)

lemma *postcond-left-unit*: $in\alpha \sharp p \Longrightarrow (true\ ;;\ p) = p$
by (*metis postcond-equiv*)

theorem *precond-left-zero*:
  assumes $out\alpha \sharp p$ $p \neq false$
  shows $(true ;; p) = true$
  using *assms*
  apply (*simp add*: *outα-def upred-defs*)
  apply (*transfer*, *auto simp add*: *relcomp-unfold*, *rule ext*, *auto*)
  apply (*rename-tac p b*)
  apply (*subgoal-tac* $\exists$ *b1 b2*. *p* (*b1*, *b2*))
  apply (*auto*)
done

7.4 Converse laws

lemma *convr-invol* [*simp*]: $p^{--} = p$
  by *pred-tac*

lemma *lit-convr* [*simp*]: $\ll v \gg^{-} = \ll v \gg$
  by *pred-tac*

lemma *uivar-convr* [*simp*]:
  fixes $x :: ('a, '\alpha)$ *uvar*
  shows $(\$x)^{-} = \$x'$
  by *pred-tac*

lemma *uovar-convr* [*simp*]:
  fixes $x :: ('a, '\alpha)$ *uvar*
  shows $(\$x')^{-} = \$x$
  by *pred-tac*

lemma *uop-convr* [*simp*]: $(uop\ f\ u)^{-} = uop\ f\ (u^{-})$
  by (*pred-tac*)

lemma *bop-convr* [*simp*]: $(bop\ f\ u\ v)^{-} = bop\ f\ (u^{-})\ (v^{-})$
  by (*pred-tac*)

lemma *eq-convr* [*simp*]: $(p =_u q)^{-} = (p^{-} =_u q^{-})$
  by (*pred-tac*)

lemma *disj-convr* [*simp*]: $(p \vee q)^{-} = (q^{-} \vee p^{-})$
  by (*pred-tac*)

lemma *conj-convr* [*simp*]: $(p \wedge q)^{-} = (q^{-} \wedge p^{-})$
  by (*pred-tac*)

lemma *seqr-convr* [*simp*]: $(p ;; q)^{-} = (q^{-} ;; p^{-})$
  by *rel-tac*

theorem *seqr-pre-transfer*: $in\alpha \sharp q \Longrightarrow ((P \wedge q) ;; R) = (P ;; (q^{-} \wedge R))$
  by (*rel-tac*)

theorem *seqr-post-out*: $in\alpha \sharp r \Longrightarrow (P ;; (Q \wedge r)) = ((P ;; Q) \wedge r)$
  by (*rel-tac*, *blast+*)

theorem *seqr-post-transfer*: $out\alpha \sharp q \Longrightarrow (P ;; (q \wedge R)) = (P \wedge q^{-} ;; R)$
  by (*simp add*: *seqr-pre-transfer unrest-convr-inα*)

lemma *seqr-pre-out*: $out\alpha \sharp p \Longrightarrow ((p \wedge Q) ;; R) = (p \wedge (Q ;; R))$
  by (*rel-tac*, *blast+*)

lemma *seqr-true-lemma*:
  $(P = (\neg (\neg P ;; true))) = (P = (P ;; true))$
  by *rel-tac*

lemma *shEx-lift-seq* [*uquant-lift*]:
  $((\exists\ x \cdot P(x)) ;; (\exists\ y \cdot Q(y))) = (\exists\ x \cdot \exists\ y \cdot P(x) ;; Q(y))$
  by *pred-tac*

While loop laws

lemma *while-cond-true*:
  $((while\ b\ do\ P\ od) \wedge \lceil b \rceil_<) = ((P \wedge \lceil b \rceil_<) ;; while\ b\ do\ P\ od)$
proof –
  have $(while\ b\ do\ P\ od \wedge \lceil b \rceil_<) = ((((\lceil b \rceil_< \wedge P)^\star{}_u \wedge (\neg \lceil b \rceil_>)) \wedge \lceil b \rceil_<)$
    by (*simp add*: *while-def*)
  also have ... $= (((II \vee ((\lceil b \rceil_< \wedge P) ;; (\lceil b \rceil_< \wedge P)^\star{}_u)) \wedge \neg \lceil b \rceil_>) \wedge \lceil b \rceil_<)$
    by (*simp add*: *disj-upred-def*)
  also have ... $= ((\lceil b \rceil_< \wedge (II \vee ((\lceil b \rceil_< \wedge P) ;; (\lceil b \rceil_< \wedge P)^\star{}_u))) \wedge (\neg \lceil b \rceil_>))$
    by (*simp add*: *conj-comm utp-pred.inf.left-commute*)
  also have ... $= (((\lceil b \rceil_< \wedge II) \vee (\lceil b \rceil_< \wedge ((\lceil b \rceil_< \wedge P) ;; (\lceil b \rceil_< \wedge P)^\star{}_u))) \wedge (\neg \lceil b \rceil_>))$
    by (*simp add*: *conj-disj-distr*)
  also have ... $= ((((\lceil b \rceil_< \wedge II) \vee ((\lceil b \rceil_< \wedge P) ;; (\lceil b \rceil_< \wedge P)^\star{}_u))) \wedge (\neg \lceil b \rceil_>))$
    by (*subst seqr-pre-out*[*THEN sym*], *simp add*: *unrest*, *rel-tac*)
  also have ... $= ((((II \wedge \lceil b \rceil_>) \vee ((\lceil b \rceil_< \wedge P) ;; (\lceil b \rceil_< \wedge P)^\star{}_u))) \wedge (\neg \lceil b \rceil_>))$
    by (*simp add*: *pre-skip-post*)
  also have ... $= ((II \wedge \lceil b \rceil_> \wedge \neg \lceil b \rceil_>) \vee (((\lceil b \rceil_< \wedge P) ;; ((\lceil b \rceil_< \wedge P)^\star{}_u)) \wedge (\neg \lceil b \rceil_>)))$
    by (*simp add*: *utp-pred.inf.assoc utp-pred.inf-sup-distrib2*)
  also have ... $= (((\lceil b \rceil_< \wedge P) ;; ((\lceil b \rceil_< \wedge P)^\star{}_u)) \wedge (\neg \lceil b \rceil_>))$
    by *simp*
  also have ... $= ((\lceil b \rceil_< \wedge P) ;; (((\lceil b \rceil_< \wedge P)^\star{}_u) \wedge (\neg \lceil b \rceil_>)))$
    by (*simp add*: *seqr-post-out unrest*)
  also have ... $= ((P \wedge \lceil b \rceil_<) ;; while\ b\ do\ P\ od)$
    by (*simp add*: *utp-pred.inf-commute while-def*)
  finally show *?thesis* **.**
qed

lemma *while-cond-false*:
  $((while\ b\ do\ P\ od) \wedge (\neg \lceil b \rceil_<)) = (II \wedge \neg \lceil b \rceil_<)$
proof –
  have $(while\ b\ do\ P\ od \wedge (\neg \lceil b \rceil_<)) = ((((\lceil b \rceil_< \wedge P)^\star{}_u \wedge (\neg \lceil b \rceil_>)) \wedge (\neg \lceil b \rceil_<))$
    by (*simp add*: *while-def*)
  also have ... $= (((II \vee ((\lceil b \rceil_< \wedge P) ;; (\lceil b \rceil_< \wedge P)^\star{}_u)) \wedge \neg \lceil b \rceil_>) \wedge (\neg \lceil b \rceil_<))$
    by (*simp add*: *disj-upred-def*)
  also have ... $= (((II \wedge \neg \lceil b \rceil_>) \wedge \neg \lceil b \rceil_<) \vee ((\neg \lceil b \rceil_<) \wedge (((\lceil b \rceil_< \wedge P) ;; ((\lceil b \rceil_< \wedge P)^\star{}_u)) \wedge \neg \lceil b \rceil_>)))$
    by (*simp add*: *conj-disj-distr utp-pred.inf.commute*)
  also have ... $= (((II \wedge \neg \lceil b \rceil_>) \wedge \neg \lceil b \rceil_<) \vee ((((\neg \lceil b \rceil_<) \wedge (\lceil b \rceil_< \wedge P) ;; ((\lceil b \rceil_< \wedge P)^\star{}_u)) \wedge \neg \lceil b \rceil_>)))$
    by (*simp add*: *seqr-pre-out unrest-not unrest-pre-outα utp-pred.inf.assoc*)
  also have ... $= (((II \wedge \neg \lceil b \rceil_>) \wedge \neg \lceil b \rceil_<) \vee (((false ;; ((\lceil b \rceil_< \wedge P)^\star{}_u)) \wedge \neg \lceil b \rceil_>)))$
    by (*simp add*: *conj-comm utp-pred.inf.left-commute*)
  also have ... $= ((II \wedge \neg \lceil b \rceil_>) \wedge \neg \lceil b \rceil_<)$
    by *simp*
  also have ... $= (II \wedge \neg \lceil b \rceil_<)$
    by *rel-tac*

finally show *?thesis* **.**
qed

theorem *while-unfold*:
while b do P od = ((*P* ;; *while b do P od*) $\triangleleft$ *b* $\triangleright_r$ *II*)
by (*metis* (*no-types*, *hide-lams*) *bounded-semilattice-sup-bot-class.sup-bot.left-neutral comp-cond-left-distr cond-def cond-idem disj-comm disj-upred-def seqr-right-zero upred-quantale.bot-zerol utp-pred.inf-bot-right utp-pred.inf-commute while-cond-false while-cond-true*)

end

7.5 Weakest precondition calculus

theory *utp-wp*
imports *utp-rel*
begin

A very quick implementation of wp – more laws still needed!

named-theorems *wp*

method *wp-tac* = (*simp add*: *wp*)

consts
uwp :: $'a \Rightarrow 'b \Rightarrow 'c$ (**infix** *wp 60*)

definition *wp-upred* :: $('\alpha, '\beta)$ *relation* $\Rightarrow$ $'\beta$ *condition* $\Rightarrow$ $'\alpha$ *condition* **where**
wp-upred Q r = $\lfloor \neg (Q \;;;\; \neg \lceil r \rceil_<) \rfloor_<$

adhoc-overloading
uwp wp-upred

declare *wp-upred-def* [*urel-defs*]

theorem *wp-assigns-r* [*wp*]:
(*assigns-r* σ) *wp r* = $\sigma \dagger r$
by *rel-tac*

theorem *wp-skip-r* [*wp*]:
II wp r = *r*
by *rel-tac*

theorem *wp-true* [*wp*]:
r $\neq$ *true* $\Longrightarrow$ *true wp r* = *false*
by *rel-tac*

theorem *wp-conj* [*wp*]:
P wp (*q* $\wedge$ *r*) = (*P wp q* $\wedge$ *P wp r*)
by *rel-tac*

theorem *wp-seq-r* [*wp*]: (*P* ;; *Q*) *wp r* = *P wp* (*Q wp r*)
by *rel-tac*

theorem *wp-cond* [*wp*]: (*P* $\triangleleft$ *b* $\triangleright_r$ *Q*) *wp r* = ((*b* $\Rightarrow$ *P wp r*) $\wedge$ (($\neg$ *b*) $\Rightarrow$ *Q wp r*))
by *rel-tac*

end

8 UTP Theories

theory *utp-theory*
imports *utp-rel*
begin

type-synonym $'\alpha$ *Healthiness-condition* $=$ $'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *upred*

definition
Healthy::$'\alpha$ *upred* $\Rightarrow$ $'\alpha$ *Healthiness-condition* $\Rightarrow$ *bool* (**infix** *is 30*)
where P *is* $H \equiv (P = H\ P)$

lemma *Healthy-def'*: P *is* $H \longleftrightarrow (H\ P = P)$
  unfolding *Healthy-def* **by** *auto*

declare *Healthy-def'* [*upred-defs*]

definition *Idempotent*$(H) \longleftrightarrow (\forall\ P.\ H(H(P)) = H(P))$

definition *Monotonic*$(H) \longleftrightarrow (\forall\ P\ Q.\ Q \sqsubseteq P \longrightarrow (H(Q) \sqsubseteq H(P)))$

definition *IMH*$(H) \longleftrightarrow$ *Idempotent*$(H) \wedge$ *Monotonic*(H)

definition *Antitone*$(H) \longleftrightarrow (\forall\ P\ Q.\ Q \sqsubseteq P \longrightarrow (H(P) \sqsubseteq H(Q)))$

definition *NM* : *NM*$(P) = (\neg\ P \wedge$ *true*$)$

lemma *Monotonic*(NM)
  apply (*simp add*:*Monotonic-def*)
  nitpick
  oops

lemma *Antitone*(NM)
  by (*simp add*:*Antitone-def NM*)

definition *Conjunctive* :: $'\alpha$ *Healthiness-condition* $\Rightarrow$ *bool* **where**
  Conjunctive$(H) \longleftrightarrow (\exists\ Q.\ \forall\ P.\ H(P) = (P \wedge Q))$

lemma *Conjuctive-Idempotent*:
  Conjunctive$(H) \Longrightarrow$ *Idempotent*(H)
  by (*auto simp add*: *Conjunctive-def Idempotent-def*)

lemma *Conjunctive-Monotonic*:
  Conjunctive$(H) \Longrightarrow$ *Monotonic*(H)
  unfolding *Conjunctive-def Monotonic-def*
  using *dual-order.trans* **by** *fastforce*

lemma *Conjunctive-conj*:
  assumes *Conjunctive*(HC)
  shows $HC(P \wedge Q) = (HC(P) \wedge Q)$
  using *assms* **unfolding** *Conjunctive-def*
  by (*metis utp-pred.inf.assoc utp-pred.inf.commute*)

lemma *Conjunctive-distr-conj*:

assumes *Conjunctive*(HC)
shows $HC(P \wedge Q) = (HC(P) \wedge HC(Q))$
using *assms* **unfolding** *Conjunctive-def*
by (*metis Conjunctive-conj assms utp-pred.inf.assoc utp-pred.inf-right-idem*)

lemma *Conjunctive-distr-disj*:
assumes *Conjunctive*(HC)
shows $HC(P \vee Q) = (HC(P) \vee HC(Q))$
using *assms* **unfolding** *Conjunctive-def*
using *utp-pred.inf-sup-distrib2* **by** *fastforce*

lemma *Conjunctive-distr-cond*:
assumes *Conjunctive*(HC)
shows $HC(P \triangleleft b \triangleright Q) = (HC(P) \triangleleft b \triangleright HC(Q))$
using *assms* **unfolding** *Conjunctive-def*
by (*metis cond-conj-distr utp-pred.inf-commute*)

definition *FunctionalConjunctive* :: $'\alpha$ *Healthiness-condition* $\Rightarrow$ *bool* **where**
FunctionalConjunctive(H) $\longleftrightarrow$ ($\exists\ F.\ \forall\ P.\ H(P) = (P \wedge F(P)) \wedge$ *Monotonic*(F))

definition *WeakConjunctive* :: $'\alpha$ *Healthiness-condition* $\Rightarrow$ *bool* **where**
WeakConjunctive(H) $\longleftrightarrow$ ($\forall\ P.\ \exists\ Q.\ H(P) = (P \wedge Q)$)

lemma *FunctionalConjunctive-Monotonic*:
FunctionalConjunctive(H) $\Longrightarrow$ *Monotonic*(H)
unfolding *FunctionalConjunctive-def* **by** (*metis Monotonic-def utp-pred.inf-mono*)

lemma *WeakConjunctive-Refinement*:
assumes *WeakConjunctive*(HC)
shows $P \sqsubseteq HC(P)$
using *assms* **unfolding** *WeakConjunctive-def* **by** (*metis utp-pred.inf.cobounded1*)

lemma *WeakCojunctive-Healthy-Refinement*:
assumes *WeakConjunctive*(HC) **and** *P is HC*
shows $HC(P) \sqsubseteq P$
using *assms* **unfolding** *WeakConjunctive-def Healthy-def* **by** *simp*

lemma *WeakConjunctive-implies-WeakConjunctive*:
Conjunctive(H) $\Longrightarrow$ *WeakConjunctive*(H)
unfolding *WeakConjunctive-def Conjunctive-def* **by** *pred-tac*

declare *Conjunctive-def* [*upred-defs*]
declare *Monotonic-def* [*upred-defs*]

end

9 Example UTP theory: Boyle's laws

theory *utp-boyle*
imports *utp-theory*
begin

Boyle's law states that k = p * V is invariant. We here encode this as a simple UTP theory. We first create a record to represent the alphabet of the theory consisting of the three variables k, p and V.

record *alpha-boyle* =
  boyle-k :: *real*
  boyle-p :: *real*
  boyle-V :: *real*

For now we have to explicitly cast the fields to UTP variables using the VAR syntactic transformation function – in future we'd like to automate this. We also have to add the definition equations for these variables to the simplification set for predicates to enable automated proof through our tactics.

definition $k = VAR\ boyle\text{-}k$
definition $p = VAR\ boyle\text{-}p$
definition $V = VAR\ boyle\text{-}V$

declare *k-def* [*upred-defs*] **and** *p-def* [*upred-defs*] **and** *V-def* [*upred-defs*]

Next we state Boyle's law using the healthiness condition B and likewise add it to the UTP predicate definitional equation set. The syntax differs a little from UTP; we try not to override HOL constants and so UTP predicate equality is subscripted. Moreover to distinguish variables standing for a predicate (like ϕ) from variables standing for UTP variables we have to prepend the latter with an ampersand.

definition $B(\varphi) = ((\exists\ k \cdot \varphi) \wedge (\&k =_u \&p * \&V))$

declare *B-def* [*upred-defs*]

We can then prove that B is both idempotent and monotone simply by application of the predicate tactic.

lemma *B-idempotent*:
  $B(B(P)) = B(P)$
  by *pred-tac*

lemma *B-monotone*:
  $X \sqsubseteq Y \Longrightarrow B(X) \sqsubseteq B(Y)$
  by *pred-tac*

We also create some example observations; the first satisfies Boyle's law and the second doesn't.

definition $\varphi_1 = ((\&p =_u 10) \wedge (\&V =_u 5) \wedge (\&k =_u 50))$

definition $\varphi_2 = ((\&p =_u 10) \wedge (\&V =_u 5) \wedge (\&k =_u 100))$

We prove that φ_1 satisfied by Boyle's law by simplication of its definitional equation and then application of the predicate tactic.

lemma *B-*φ_1: φ_1 *is* B
  by (*simp add*: φ_1*-def*, *pred-tac*)

We prove that φ_2 does not satisfy Boyle's law by showing it's in fact equal to φ_1. We do this via an automated Isar proof.

lemma *B-*φ_2: $B(\varphi_2) = \varphi_1$
proof −
  have $B(\varphi_2) = B((\&p =_u 10) \wedge (\&V =_u 5) \wedge (\&k =_u 100))$
    by (*simp add*: φ_2*-def*)
  also have ... $= ((\exists\ k \cdot (\&p =_u 10) \wedge (\&V =_u 5) \wedge (\&k =_u 100)) \wedge (\&k =_u \&p * \&V))$
    by *pred-tac*
  also have ... $= ((\&p =_u 10) \wedge (\&V =_u 5) \wedge (\&k =_u \&p * \&V))$

  by *pred-tac*
 also have ... = $((\&p =_u \mathit{10}) \wedge (\&V =_u \mathit{5}) \wedge (\&k =_u \mathit{50}))$
  by *pred-tac*
 also have ... = φ_1
  by (*simp add*: φ_1*-def*)
 finally show *?thesis* **.**
qed

end

10 Designs

theory *utp-designs*
imports
 utp-rel
 utp-wp
 utp-theory
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 ok. It is used to record the start and termination of a program.

10.1 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 $H1$, $H2$, $H3$ and $H4$.

record *alpha-d* = *des-ok*::*bool*

The ok variable is defined using the syntactic translation *VAR*

definition *ok* = *VAR des-ok*

declare *ok-def* [*upred-defs*]

lemma *uvar-ok* [*simp*]: *uvar ok*
 by (*unfold-locales*, *simp-all add*: *ok-def*)

type-synonym *'α alphabet-d* = *'α alpha-d-scheme alphabet*
type-synonym (*'a*, *'α*) *uvar-d* = (*'a*, *'α alphabet-d*) *uvar*
type-synonym (*'α*, *'β*) *relation-d* = (*'α alphabet-d*, *'β alphabet-d*) *relation*
type-synonym *'α hrelation-d* = *'α alphabet-d hrelation*

definition *des-lens* :: (*'α*, *'α alphabet-d*) *lens* **where**
des-lens = (| *lens-get* = *more*, *lens-put* = *fld-put more-update* |)

declare *des-lens-def* [*upred-defs*]

lemma *uvar-des-lens* [*simp*]: *uvar des-lens*
 by (*unfold-locales*, *simp-all add*: *des-lens-def*)

lemma *ok-indep-des-lens* [*simp*]: *ok* ⋈ *des-lens des-lens* ⋈ *ok*
 by (*rule lens-indepI*, *simp-all add*: *ok-def des-lens-def*)+

lemma *ok-des-bij-lens*: *bij-lens* $(ok +_L des\text{-}lens)$
by (*unfold-locales*, *simp-all add*: *ok-def des-lens-def lens-plus-def prod.case-eq-if*)

It would be nice to be able to prove some general distributivity properties about these lifting operators. I don't know if that's possible somehow...

abbreviation (*input*) *lift-desr* :: $('\alpha, '\beta)$ *relation* $\Rightarrow$ $('\alpha, '\beta)$ *relation-d* $(\lceil\text{-}\rceil_D)$
where $\lceil P\rceil_D \equiv P \oplus_p (des\text{-}lens \times_L des\text{-}lens)$

abbreviation *drop-desr* :: $('\alpha, '\beta)$ *relation-d* $\Rightarrow$ $('\alpha, '\beta)$ *relation* $(\lfloor\text{-}\rfloor_D)$
where $\lfloor P\rfloor_D \equiv P \restriction_p (des\text{-}lens \times_L des\text{-}lens)$

definition *design*::$('\alpha, '\beta)$ *relation-d* $\Rightarrow$ $('\alpha, '\beta)$ *relation-d* $\Rightarrow$ $('\alpha, '\beta)$ *relation-d* (**infixl** $\vdash$ *60*)
where $P \vdash Q = (\$ok \wedge P \Rightarrow \$ok' \wedge Q)$

An rdesign is a design that uses the Isabelle type system to prevent reference to ok in the assumption and commitment.

definition *rdesign*::$('\alpha, '\beta)$ *relation* $\Rightarrow$ $('\alpha, '\beta)$ *relation* $\Rightarrow$ $('\alpha, '\beta)$ *relation-d* (**infixl** $\vdash_r$ *60*)
where $(P \vdash_r Q) = \lceil P\rceil_D \vdash \lceil Q\rceil_D$

An ndesign is a normal design, i.e. where the assumption is a condition

definition *ndesign*::$'\alpha$ *condition* $\Rightarrow$ $('\alpha, '\beta)$ *relation* $\Rightarrow$ $('\alpha, '\beta)$ *relation-d* (**infixl** $\vdash_n$ *60*)
where $(p \vdash_n Q) = (\lceil p\rceil_< \vdash_r Q)$

definition *skip-d* :: $'\alpha$ *hrelation-d* (II_D)
where $II_D \equiv (true \vdash_r II)$

definition *assigns-d* :: $'\alpha$ *usubst* $\Rightarrow$ $'\alpha$ *hrelation-d*
where *assigns-d* $\sigma = (true \vdash_r assigns\text{-}r\ \sigma)$

syntax
-assignmentd :: *salphas* $\Rightarrow$ *uexprs* $\Rightarrow$ *logic* (**infixr** $:=_D$ *55*)

translations
-assignmentd xs vs => *CONST assigns-d* (*-psubst* (*CONST id*) *xs vs*)

definition J :: $'\alpha$ *hrelation-d*
where $J = ((\$ok \Rightarrow \$ok') \wedge \lceil II\rceil_D)$

definition *H1* $(P) \equiv \$ok \Rightarrow P$

definition *H2* $(P) \equiv P \;;; J$

definition *H3* $(P) \equiv P \;;; II_D$

definition *H4* $(P) \equiv ((P;;true) \Rightarrow P)$

abbreviation σf::$('\alpha, '\beta)$ *relation-d* $\Rightarrow$ $('\alpha, '\beta)$ *relation-d* $(\text{-}^f\ [1000]\ 1000)$
where $\sigma f\ D \equiv D[\![false/\$ok']\!]$

abbreviation σt::$('\alpha, '\beta)$ *relation-d* $\Rightarrow$ $('\alpha, '\beta)$ *relation-d* $(\text{-}^t\ [1000]\ 1000)$
where $\sigma t\ D \equiv D[\![true/\$ok']\!]$

definition *pre-design* :: $('\alpha, '\beta)$ *relation-d* $\Rightarrow$ $('\alpha, '\beta)$ *relation* $(pre_D'(\text{-}'))$ **where**
$pre_D(P) = \lfloor\neg\ P[\![true,false/\$ok,\$ok']\!]\rfloor_D$

definition *post-design* :: ($'\alpha$, $'\beta$) *relation-d* $\Rightarrow$ ($'\alpha$, $'\beta$) *relation* (*post*$_D$'(-')) **where**
$post_D(P) = \lfloor P[\![true,true/\$ok,\$ok']\!] \rfloor_D$

definition *wp-design* :: ($'\alpha$, $'\beta$) *relation-d* $\Rightarrow$ $'\beta$ *condition* $\Rightarrow$ $'\alpha$ *condition* (**infix** *wp*$_D$ *60*) **where**
$Q\ wp_D\ r = (\lfloor pre_D(Q)\ ;;\ true \rfloor_< \wedge (post_D(Q)\ wp\ r))$

declare *design-def* [*upred-defs*]
declare *rdesign-def* [*upred-defs*]
declare *skip-d-def* [*upred-defs*]
declare *J-def* [*upred-defs*]
declare *pre-design-def* [*upred-defs*]
declare *post-design-def* [*upred-defs*]
declare *wp-design-def* [*upred-defs*]

declare *H1-def* [*upred-defs*]
declare *H2-def* [*upred-defs*]
declare *H3-def* [*upred-defs*]
declare *H4-def* [*upred-defs*]

lemma *drop-desr-inv* [*simp*]: $\lfloor \lceil P \rceil_D \rfloor_D = P$
  by (*simp add*: *arestr-aext prod-mwb-lens*)

lemma *lift-desr-inv*:
  fixes P :: ($'\alpha$, $'\beta$) *relation-d*
  assumes $\$ok \sharp P$ $\$ok' \sharp P$
  shows $\lceil \lfloor P \rfloor_D \rceil_D = P$
proof −
  have *bij-lens* (*des-lens* $\times_L$ *des-lens* $+_L$ (*in-var ok* $+_L$ *out-var ok*) :: (-, $'\alpha$ *alpha-d-scheme* $\times$ $'\beta$ *alpha-d-scheme*) *lens*)
    (**is** *bij-lens* (*?P*))
  proof −
    have *?P* $\approx_L$ (*ok* $+_L$ *des-lens*) $\times_L$ (*ok* $+_L$ *des-lens*) (**is** *?P* $\approx_L$ *?Q*)
      apply (*simp add*: *in-var-def out-var-def prod-as-plus*)
      apply (*simp add*: *prod-as-plus*[*THEN sym*])
    apply (*meson lens-equiv-sym lens-equiv-trans lens-indep-prod lens-plus-comm lens-plus-prod-exchange ok-indep-des-lens*)
    done
    moreover have *bij-lens ?Q*
      by (*simp add*: *ok-des-bij-lens prod-bij-lens*)
    ultimately show *?thesis*
      by (*metis bij-lens-equiv lens-equiv-sym*)
  qed

  with *assms* **show** *?thesis*
    apply (*rule-tac aext-arestr*[*of - in-var ok* $+_L$ *out-var ok*])
    apply (*simp add*: *prod-mwb-lens*)
    apply (*simp*)
    apply (*metis alpha-in-var lens-indep-prod lens-indep-sym ok-indep-des-lens out-var-def prod-as-plus*)
    using *unrest-var-comp* **apply** *blast*
  done
qed

10.2 Design laws

lemma *prod-lens-indep-in-var* [*simp*]:

$a \bowtie x \Longrightarrow a \times_L b \bowtie$ *in-var* x
by (*metis in-var-def in-var-indep out-in-indep out-var-def plus-pres-lens-indep prod-as-plus*)

lemma *prod-lens-indep-out-var* [*simp*]:
$b \bowtie x \Longrightarrow a \times_L b \bowtie$ *out-var* x
by (*metis in-out-indep in-var-def out-var-def out-var-indep plus-pres-lens-indep prod-as-plus*)

lemma *unrest-out-des-lift* [*unrest*]: $out\alpha \sharp p \Longrightarrow out\alpha \sharp \lceil p \rceil_D$
by (*pred-tac*, *auto simp add*: *out*α*-def des-lens-def prod-lens-def*)

lemma *lift-dist-seq* [*simp*]:
$\lceil P ;; Q \rceil_D = (\lceil P \rceil_D ;; \lceil Q \rceil_D)$
by (*rel-tac*, *metis alpha-d.select-convs*(*2*))

theorem *design-refinement*:
assumes
$\$ok \sharp P1$ $\$ok' \sharp P1$ $\$ok \sharp P2$ $\$ok' \sharp P2$
$\$ok \sharp Q1$ $\$ok' \sharp Q1$ $\$ok \sharp Q2$ $\$ok' \sharp Q2$
shows $(P1 \vdash Q1 \sqsubseteq P2 \vdash Q2) \longleftrightarrow (`P1 \Rightarrow P2` \wedge `P1 \wedge Q2 \Rightarrow Q1`)$
proof –
have $(P1 \vdash Q1) \sqsubseteq (P2 \vdash Q2) \longleftrightarrow `(\$ok \wedge P2 \Rightarrow \$ok' \wedge Q2) \Rightarrow (\$ok \wedge P1 \Rightarrow \$ok' \wedge Q1)`$
by *pred-tac*
also with *assms* **have** ... $= `(P2 \Rightarrow \$ok' \wedge Q2) \Rightarrow (P1 \Rightarrow \$ok' \wedge Q1)`$
by (*subst subst-bool-split*[*of in-var ok*], *simp-all*, *subst-tac*)
also with *assms* **have** ... $= `(\neg P2 \Rightarrow \neg P1) \wedge ((P2 \Rightarrow Q2) \Rightarrow P1 \Rightarrow Q1)`$
by (*subst subst-bool-split*[*of out-var ok*], *simp-all*, *subst-tac*)
also have ... $\longleftrightarrow `(P1 \Rightarrow P2)` \wedge `P1 \wedge Q2 \Rightarrow Q1`$
by (*pred-tac*)
finally show *?thesis* **.**
qed

theorem *rdesign-refinement*:
$(P1 \vdash_r Q1 \sqsubseteq P2 \vdash_r Q2) \longleftrightarrow (`P1 \Rightarrow P2` \wedge `P1 \wedge Q2 \Rightarrow Q1`)$
apply (*simp add*: *rdesign-def*)
apply (*subst design-refinement*)
apply (*simp-all add*: *unrest*)
apply (*pred-tac*)
apply (*metis alpha-d.select-convs*(*2*))+
done

lemma *design-refine-intro*:
assumes $`P1 \Rightarrow P2`$ $`P1 \wedge Q2 \Rightarrow Q1`$
shows $P1 \vdash Q1 \sqsubseteq P2 \vdash Q2$
using *assms* **unfolding** *upred-defs*
by *pred-tac*

theorem *design-ok-false* [*usubst*]: $(P \vdash Q)[\![false/\$ok]\!] = true$
by (*simp add*: *design-def usubst*)

theorem *design-pre*:
$\$ok' \sharp P \Longrightarrow \neg (P \vdash Q)^f = (\$ok \wedge P^f)$
by (*simp add*: *design-def*, *subst-tac*)
(*metis* (*no-types*, *hide-lams*) *not-conj-deMorgans true-not-false*(*2*) *utp-pred.compl-top-eq*
utp-pred.sup.idem utp-pred.sup-compl-top)

declare *des-lens-def* [*upred-defs*]
declare *lens-create-def* [*upred-defs*]
declare *prod-lens-def* [*upred-defs*]
declare *in-var-def* [*upred-defs*]

theorem *rdesign-pre* [*simp*]: $pre_D(P \vdash_r Q) = P$
  by *pred-tac*

theorem *rdesign-post* [*simp*]: $post_D(P \vdash_r Q) = (P \Rightarrow Q)$
  by *pred-tac*

theorem *design-true-left-zero*: $(true ;; (P \vdash Q)) = true$
proof −
  have $(true ;; (P \vdash Q)) = (\exists\ ok_0 \cdot true⟦«ok_0»/\$ok'⟧ ;; (P \vdash Q)⟦«ok_0»/\$ok⟧)$
    by (*subst seqr-middle*[*of ok*], *simp-all*)
  also have ... $= ((true⟦false/\$ok'⟧ ;; (P \vdash Q)⟦false/\$ok⟧) \vee (true⟦true/\$ok'⟧ ;; (P \vdash Q)⟦true/\$ok⟧))$
    by (*simp add*: *disj-comm false-alt-def true-alt-def*)
  also have ... $= ((true⟦false/\$ok'⟧ ;; true_h) \vee (true ;; ((P \vdash Q)⟦true/\$ok⟧)))$
    by (*subst-tac*, *rel-tac*)
  also have ... $= true$
    by (*subst-tac*, *simp add*: *precond-right-unit unrest*)
  finally show *?thesis* **.**
qed

theorem *design-composition*:
  assumes
    $\$ok \sharp P1$ $\$ok' \sharp P1$ $\$ok \sharp P2$ $\$ok' \sharp P2$
    $\$ok \sharp Q1$ $\$ok' \sharp Q1$ $\$ok \sharp Q2$ $\$ok' \sharp Q2$
  shows $((P1 \vdash Q1) ;; (P2 \vdash Q2)) = (((\neg ((\neg P1) ;; true)) \wedge \neg (Q1 ;; (\neg P2))) \vdash (Q1 ;; Q2))$
proof −
  have $((P1 \vdash Q1) ;; (P2 \vdash Q2)) = (\exists\ ok_0 \cdot ((P1 \vdash Q1)⟦«ok_0»/\$ok'⟧ ;; (P2 \vdash Q2)⟦«ok_0»/\$ok⟧))$
    by (*rule seqr-middle*, *simp*)
  also have ...
    $= (((P1 \vdash Q1)⟦false/\$ok'⟧ ;; (P2 \vdash Q2)⟦false/\$ok⟧)$
      $\vee ((P1 \vdash Q1)⟦true/\$ok'⟧ ;; (P2 \vdash Q2)⟦true/\$ok⟧))$
    by (*simp add*: *true-alt-def false-alt-def*, *pred-tac*)
  also from *assms*
  have ... $= (((\$ok \wedge P1 \Rightarrow Q1) ;; (P2 \Rightarrow \$ok' \wedge Q2)) \vee ((\neg (\$ok \wedge P1)) ;; true))$
    by (*simp add*: *design-def usubst unrest*, *pred-tac*)
  also have ... $= ((\neg\$ok ;; true_h) \vee (\neg P1 ;; true) \vee (Q1 ;; \neg P2) \vee (\$ok' \wedge (Q1 ;; Q2)))$
    by (*rel-tac*)
  also have ... $= (\neg (\neg P1 ;; true) \wedge \neg (Q1 ;; \neg P2)) \vdash (Q1 ;; Q2)$
    by (*simp add*: *precond-right-unit design-def unrest*, *rel-tac*)
  finally show *?thesis* **.**
qed

theorem *rdesign-composition*:
  $((P1 \vdash_r Q1) ;; (P2 \vdash_r Q2)) = (((\neg ((\neg P1) ;; true_h)) \wedge \neg (Q1 ;; (\neg P2))) \vdash_r (Q1 ;; Q2))$
  by (*simp add*: *rdesign-def design-composition unrest alpha*)

lemma *skip-d-alt-def*: $II_D = true \vdash II$
  by (*rel-tac*)

theorem *design-skip-idem* [*simp*]:
  $(II_D ;; II_D) = II_D$

by (*simp add*: *skip-d-def urel-defs*, *pred-tac*)

theorem *design-composition-cond*:
assumes
$\$ok \sharp p1$ $out\alpha \sharp p1$ $\$ok \sharp P2$ $\$ok' \sharp P2$
$\$ok \sharp Q1$ $\$ok' \sharp Q1$ $\$ok \sharp Q2$ $\$ok' \sharp Q2$
shows $((p1 \vdash Q1) ;; (P2 \vdash Q2)) = ((p1 \wedge \neg (Q1 ;; (\neg P2))) \vdash (Q1 ;; Q2))$
using *assms*
by (*simp add*: *design-composition unrest precond-right-unit*)

theorem *rdesign-composition-cond*:
assumes $out\alpha \sharp p1$
shows $((p1 \vdash_r Q1) ;; (P2 \vdash_r Q2)) = ((p1 \wedge \neg (Q1 ;; (\neg P2))) \vdash_r (Q1 ;; Q2))$
using *assms*
by (*simp add*: *rdesign-def design-composition-cond unrest alpha*)

theorem *design-composition-wp*:
fixes $Q1\ Q2$ :: *'a hrelation-d*
assumes
$ok \sharp p1$ $ok \sharp p2$
$\$ok \sharp Q1$ $\$ok' \sharp Q1$ $\$ok \sharp Q2$ $\$ok' \sharp Q2$
shows $((\lceil p1 \rceil_< \vdash Q1) ;; (\lceil p2 \rceil_< \vdash Q2)) = ((\lceil p1 \wedge Q1\ wp\ p2 \rceil_<) \vdash (Q1 ;; Q2))$
using *assms*
by (*simp add*: *design-composition-cond unrest*, *rel-tac*)

theorem *rdesign-composition-wp*:
fixes $Q1\ Q2$ :: *'a hrelation*
shows $((\lceil p1 \rceil_< \vdash_r Q1) ;; (\lceil p2 \rceil_< \vdash_r Q2)) = ((\lceil p1 \wedge Q1\ wp\ p2 \rceil_<) \vdash_r (Q1 ;; Q2))$
by (*simp add*: *rdesign-composition-cond unrest*, *rel-tac*)

theorem *rdesign-wp* [*wp*]:
$(\lceil p \rceil_< \vdash_r Q)\ wp_D\ r = (p \wedge Q\ wp\ r)$
by *rel-tac*

theorem *wpd-seq-r*:
fixes $Q1\ Q2$ :: *'α hrelation*
shows $(\lceil p1 \rceil_< \vdash_r Q1 ;; \lceil p2 \rceil_< \vdash_r Q2)\ wp_D\ r = (\lceil p1 \rceil_< \vdash_r Q1)\ wp_D\ ((\lceil p2 \rceil_< \vdash_r Q2)\ wp_D\ r)$
apply (*simp add*: *wp*)
apply (*subst rdesign-composition-wp*)
apply (*simp only*: *wp*)
apply (*rel-tac*)
done

theorem *design-left-unit* [*simp*]:
$(II_D ;; P \vdash_r Q) = (P \vdash_r Q)$
by (*simp add*: *skip-d-def urel-defs*, *pred-tac*)

theorem *design-right-cond-unit* [*simp*]:
assumes $out\alpha \sharp p$
shows $(p \vdash_r Q ;; II_D) = (p \vdash_r Q)$
using *assms*
by (*simp add*: *skip-d-def rdesign-composition-cond*)

lemma *lift-des-skip-dr-unit* [*simp*]:
$(\lceil P \rceil_D ;; \lceil II \rceil_D) = \lceil P \rceil_D$

$(\lceil II \rceil_D ;; \lceil P \rceil_D) = \lceil P \rceil_D$
by *rel-tac rel-tac*

10.3 H1: No observation is allowed before initiation

lemma *H1-idem*:
$H1\ (H1\ P) = H1(P)$
by *pred-tac*

lemma *H1-monotone*:
$P \sqsubseteq Q \Longrightarrow H1(P) \sqsubseteq H1(Q)$
by *pred-tac*

lemma *H1-design-skip*:
$H1(II) = II_D$
by *rel-tac*

The H1 algebraic laws are valid only when $\alpha(R)$ is homogeneous. This should maybe be generalised.

theorem *H1-algebraic-intro*:
assumes
$(true_h ;; R) = true_h$
$(II_D ;; R) = R$
shows *R is H1*
proof –
have $R = (II_D ;; R)$ **by** (*simp add*: *assms*(*2*))
also have ... $= (H1(II) ;; R)$
by (*simp add*: *H1-design-skip*)
also have ... $= ((\$ok \Rightarrow II) ;; R)$
by (*simp add*: *H1-def*)
also have ... $= ((\neg \$ok ;; R) \vee R)$
by (*simp add*: *impl-alt-def seqr-or-distl*)
also have ... $= (((\neg \$ok ;; true_h) ;; R) \vee R)$
by (*simp add*: *precond-right-unit unrest*)
also have ... $= ((\neg \$ok ;; true_h) \vee R)$
by (*metis assms*(*1*) *seqr-assoc*)
also have ... $= (\$ok \Rightarrow R)$
by (*simp add*: *impl-alt-def precond-right-unit unrest*)
finally show *?thesis* **by** (*metis H1-def Healthy-def'*)
qed

lemma *nok-not-false*:
$(\neg \$ok) \neq false$
by (*pred-tac*, *metis alpha-d.select-convs*(*1*))

theorem *H1-left-zero*:
assumes *P is H1*
shows $(true_h ;; P) = true_h$
proof –
from *assms* **have** $(true_h ;; P) = (true_h ;; (\$ok \Rightarrow P))$
by (*simp add*: *H1-def Healthy-def'*)
also from *assms* **have** ... $= (true_h ;; (\neg \$ok \vee P))$
by (*simp add*: *impl-alt-def*)
also from *assms* **have** ... $= ((true_h ;; \neg \$ok) \vee (true_h ;; P))$
using *seqr-or-distr* **by** *blast*

also from *assms* **have** ... = $(true \vee (true \;;\; P))$
by (*simp add*: *nok-not-false precond-left-zero unrest*)
finally show *?thesis* **by** *rel-tac*
qed

theorem *H1-left-unit*:
fixes P :: $'\alpha$ *hrelation-d*
assumes P *is H1*
shows $(II_D \;;\; P) = P$
proof −
have $(II_D \;;\; P) = ((\$ok \Rightarrow II) \;;\; P)$
by (*metis H1-def H1-design-skip*)
also have ... = $((\neg \$ok \;;\; P) \vee P)$
by (*simp add*: *impl-alt-def seqr-or-distl*)
also from *assms* **have** ... = $(((\neg \$ok \;;\; true_h) \;;\; P) \vee P)$
by (*simp add*: *precond-right-unit unrest*)
also have ... = $((\neg \$ok \;;\; (true_h \;;\; P)) \vee P)$
by (*simp add*: *seqr-assoc*)
also from *assms* **have** ... = $(\$ok \Rightarrow P)$
by (*simp add*: *H1-left-zero impl-alt-def precond-right-unit unrest*)
finally show *?thesis* **using** *assms*
by (*simp add*: *H1-def Healthy-def'*)
qed

theorem *H1-algebraic*:
P *is H1* $\longleftrightarrow (true_h \;;\; P) = true_h \wedge (II_D \;;\; P) = P$
using *H1-algebraic-intro H1-left-unit H1-left-zero* **by** *blast*

theorem *H1-nok-left-zero*:
fixes P :: $'\alpha$ *hrelation-d*
assumes P *is H1*
shows $(\neg \$ok \;;\; P) = (\neg \$ok)$
proof −
have $(\neg \$ok \;;\; P) = ((\neg \$ok \;;\; true_h) \;;\; P)$
by (*simp add*: *precond-right-unit unrest*)
also have ... = $((\neg \$ok) \;;\; true_h)$
by (*metis H1-left-zero assms seqr-assoc*)
also have ... = $(\neg \$ok)$
by (*simp add*: *precond-right-unit unrest*)
finally show *?thesis* **.**
qed

10.4 H2: A specification cannot require non-termination

lemma *J-split*:
shows $(P \;;\; J) = (P^f \vee (P^t \wedge \$ok'))$
proof −
have $(P \;;\; J) = (P \;;\; ((\$ok \Rightarrow \$ok') \wedge \lceil II \rceil_D))$
by (*simp add*: *H2-def J-def design-def*)
also have ... = $(P \;;\; ((\$ok \Rightarrow \$ok \wedge \$ok') \wedge \lceil II \rceil_D))$
by *rel-tac*
also have ... = $((P \;;\; (\neg \$ok \wedge \lceil II \rceil_D)) \vee (P \;;\; (\$ok \wedge (\lceil II \rceil_D \wedge \$ok'))))$
by *rel-tac*
also have ... = $(P^f \vee (P^t \wedge \$ok'))$
proof −
have $(P \;;\; (\neg \$ok \wedge \lceil II \rceil_D)) = P^f$

proof −
have $(P ;; (\neg \$ok \wedge \lceil II \rceil_D)) = ((P \wedge \neg \$ok') ;; \lceil II \rceil_D)$
by *rel-tac*
also have ... $= (\exists \$ok' \cdot P \wedge \$ok' =_u \mathit{false})$
by (*rel-tac*, *metis* (*mono-tags*, *lifting*) *alpha-d.surjective alpha-d.update-convs*(*1*))
also have ... $= P^f$
by (*metis one-point out-var-uvar unrest-false uvar-ok vwb-lens-mwb*)
finally show *?thesis* **.**
qed
moreover have $(P ;; (\$ok \wedge (\lceil II \rceil_D \wedge \$ok'))) = (P^t \wedge \$ok')$
proof −
have $(P ;; (\$ok \wedge (\lceil II \rceil_D \wedge \$ok'))) = (P ;; (\$ok \wedge II))$
by (*rel-tac*, *metis alpha-d.equality*)
also have ... $= (P^t \wedge \$ok')$
by (*rel-tac*, *metis* (*full-types*) *alpha-d.surjective alpha-d.update-convs*(*1*))+
finally show *?thesis* **.**
qed
ultimately show *?thesis*
by *simp*
qed
finally show *?thesis* **.**
qed

lemma *H2-split*:
shows $H2(P) = (P^f \vee (P^t \wedge \$ok'))$
by (*simp add*: *H2-def J-split*)

theorem *H2-equivalence*:
P *is H2* $\longleftrightarrow$ ‘$P^f \Rightarrow P^t$‘
proof −
have ‘$P \Leftrightarrow (P ;; J)$‘ $\longleftrightarrow$ ‘$P \Leftrightarrow (P^f \vee (P^t \wedge \$ok'))$‘
by (*simp add*: *J-split*)
also from *assms* **have** ... $\longleftrightarrow$ ‘$(P \Leftrightarrow P^f \vee P^t \wedge \$ok')^f \wedge (P \Leftrightarrow P^f \vee P^t \wedge \$ok')^t$‘
by (*simp add*: *subst-bool-split*)
also from *assms* **have** ... = ‘$(P^f \Leftrightarrow P^f) \wedge (P^t \Leftrightarrow P^f \vee P^t)$‘
by *subst-tac*
also have ... = ‘$P^t \Leftrightarrow (P^f \vee P^t)$‘
by *pred-tac*
also have ... = ‘$(P^f \Rightarrow P^t)$‘
by *pred-tac*
finally show *?thesis* **using** *assms*
by (*metis H2-def Healthy-def' taut-iff-eq*)
qed

lemma *H2-equiv*:
P *is H2* $\longleftrightarrow P^t \sqsubseteq P^f$
using *H2-equivalence refBy-order* **by** *blast*

lemma *H2-design*:
assumes $\$ok \sharp P$ $\$ok' \sharp P$ $\$ok \sharp Q$ $\$ok' \sharp Q$
shows $H2(P \vdash Q) = P \vdash Q$
using *assms*
by (*simp add*: *H2-split design-def usubst unrest*, *pred-tac*)

lemma *H2-rdesign*:

$H2(P \vdash_r Q) = P \vdash_r Q$
by (*simp add*: *H2-design unrest rdesign-def*)

theorem *J-idem*:
$(J ;; J) = J$
by (*simp add*: *J-def urel-defs*, *pred-tac*)

theorem *H2-idem*:
$H2(H2(P)) = H2(P)$
by (*metis H2-def J-idem seqr-assoc*)

theorem *H2-not-okay*: $H2\ (\neg\ \$ok) = (\neg\ \$ok)$
proof −
have $H2\ (\neg\ \$ok) = ((\neg\ \$ok)^f \vee ((\neg\ \$ok)^t \wedge \$ok'))$
by (*simp add*: *H2-split*)
also have ... $= (\neg\ \$ok \vee (\neg\ \$ok) \wedge \$ok')$
by (*subst-tac*)
also have ... $= (\neg\ \$ok)$
by *pred-tac*
finally show *?thesis* **.**
qed

theorem *H1-H2-commute*:
$H1\ (H2\ P) = H2\ (H1\ P)$
proof −
have $H2\ (H1\ P) = ((\$ok \Rightarrow P) ;; J)$
by (*simp add*: *H1-def H2-def*)
also from *assms* **have** ... $= ((\neg\ \$ok \vee P) ;; J)$
by *rel-tac*
also have ... $= ((\neg\ \$ok ;; J) \vee (P ;; J))$
using *seqr-or-distl* **by** *blast*
also have ... $= ((H2\ (\neg\ \$ok)) \vee H2(P))$
by (*simp add*: *H2-def*)
also have ... $= ((\neg\ \$ok) \vee H2(P))$
by (*simp add*: *H2-not-okay*)
also have ... $= H1(H2(P))$
by *rel-tac*
finally show *?thesis* **by** *simp*
qed

lemma *ok-pre*: $(\$ok \wedge \lceil pre_D(P)\rceil_D) = (\$ok \wedge (\neg\ P^f))$
by (*pred-tac*)
(*metis* (*mono-tags*, *lifting*) *alpha-d.surjective alpha-d.update-convs*(*1*) *alpha-d.update-convs*(*2*))+

lemma *ok-post*: $(\$ok \wedge \lceil post_D(P)\rceil_D) = (\$ok \wedge (P^t))$
by (*pred-tac*)
(*metis alpha-d.cases-scheme alpha-d.ext-inject alpha-d.select-convs*(*1*) *alpha-d.select-convs*(*2*) *alpha-d.update-convs*(*1*)
alpha-d.update-convs(*2*))+

theorem *H1-H2-is-rdesign*:
assumes *P is H1 P is H2*
shows $P = pre_D(P) \vdash_r post_D(P)$
proof −
from *assms* **have** $P = (\$ok \Rightarrow H2(P))$
by (*simp add*: *H1-def Healthy-def'*)

also have ... = ($\$ok \Rightarrow (P^f \vee (P^t \wedge \$ok'))$)
by (*metis H2-split*)
also have ... = ($\$ok \wedge (\neg P^f) \Rightarrow \$ok' \wedge P^t$)
by *pred-tac*
also have ... = ($\$ok \wedge (\neg P^f) \Rightarrow \$ok' \wedge \$ok \wedge P^t$)
by *pred-tac*
also have ... = ($\$ok \wedge \lceil pre_D(P) \rceil_D \Rightarrow \$ok' \wedge \$ok \wedge \lceil post_D(P) \rceil_D$)
by (*simp add*: *ok-post ok-pre*)
also have ... = ($\$ok \wedge \lceil pre_D(P) \rceil_D \Rightarrow \$ok' \wedge \lceil post_D(P) \rceil_D$)
by *pred-tac*
also from *assms* **have** ... = $pre_D(P) \vdash_r post_D(P)$
by (*simp add*: *rdesign-def design-def*)
finally show *?thesis* **.**
qed

abbreviation *H1-H2 P* $\equiv$ *H1* (*H2 P*)

10.5 H3: The design assumption is a precondition

theorem *H3-idem*:
H3(*H3*(*P*)) = *H3*(*P*)
by (*metis H3-def design-skip-idem seqr-assoc*)

theorem *rdesign-H3-iff-pre*:
$P \vdash_r Q$ *is H3* $\longleftrightarrow P = (P ;; true)$
proof −
have $(P \vdash_r Q ;; II_D) = (P \vdash_r Q ;; true \vdash_r II)$
by (*simp add*: *skip-d-def*)
also from *assms* **have** ... = $(\neg (\neg P ;; true) \wedge \neg (Q ;; \neg true)) \vdash_r (Q ;; II)$
by (*simp add*: *rdesign-composition*)
also from *assms* **have** ... = $(\neg (\neg P ;; true) \wedge \neg (Q ;; \neg true)) \vdash_r Q$
by *simp*
also have ... = $(\neg (\neg P ;; true)) \vdash_r Q$
by *pred-tac*
finally have $P \vdash_r Q$ *is H3* $\longleftrightarrow P \vdash_r Q = (\neg (\neg P ;; true)) \vdash_r Q$
by (*metis H3-def Healthy-def'*)
also have ... $\longleftrightarrow P = (\neg (\neg P ;; true))$
by (*metis rdesign-pre*)
also have ... $\longleftrightarrow P = (P ;; true)$
by (*simp add*: *seqr-true-lemma*)
finally show *?thesis* **.**
qed

theorem *design-H3-iff-pre*:
assumes $\$ok \sharp P$ $\$ok' \sharp P$ $\$ok \sharp Q$ $\$ok' \sharp Q$
shows $P \vdash Q$ *is H3* $\longleftrightarrow P = (P ;; true)$
proof −
have $P \vdash Q = \lfloor P \rfloor_D \vdash_r \lfloor Q \rfloor_D$
by (*simp add*: *assms lift-desr-inv rdesign-def*)
moreover hence $\lfloor P \rfloor_D \vdash_r \lfloor Q \rfloor_D$ *is H3* $\longleftrightarrow \lfloor P \rfloor_D = (\lfloor P \rfloor_D ;; true)$
using *rdesign-H3-iff-pre* **by** *blast*
ultimately show *?thesis*
by (*metis assms drop-desr-inv lift-desr-inv lift-dist-seq aext-true*)
qed

theorem *H1-H3-commute*:

H1 (*H3 P*) = *H3* (*H1 P*)
by *rel-tac*

lemma *skip-d-absorb-J-1*:
$(II_D \;;\; J) = II_D$
by (*metis H2-def H2-rdesign skip-d-def*)

lemma *skip-d-absorb-J-2*:
$(J \;;\; II_D) = II_D$
proof −
have $(J \;;\; II_D) = ((\$ok \Rightarrow \$ok') \wedge \lceil II \rceil_D \;;\; true \vdash II)$
by (*simp add*: *J-def skip-d-alt-def*)
also have ... $= (\exists\ ok_0 \cdot ((\$ok \Rightarrow \$ok') \wedge \lceil II \rceil_D)[\![\ll ok_0 \gg/\$ok']\!] \;;\; (true \vdash II)[\![\ll ok_0 \gg/\$ok]\!])$
by (*subst seqr-middle*[*of ok*], *simp-all*)
also have ... $= ((((\$ok \Rightarrow \$ok') \wedge \lceil II \rceil_D)[\![false/\$ok']\!] \;;\; (true \vdash II)[\![false/\$ok]\!])$
$\vee (((\$ok \Rightarrow \$ok') \wedge \lceil II \rceil_D)[\![true/\$ok']\!] \;;\; (true \vdash II)[\![true/\$ok]\!]))$
by (*simp add*: *disj-comm false-alt-def true-alt-def*)
also have ... $= ((\neg \$ok \wedge \lceil II \rceil_D \;;\; true) \vee (\lceil II \rceil_D \;;\; \$ok' \wedge \lceil II \rceil_D))$
by *rel-tac*
also have ... $= II_D$
by *rel-tac*
finally show *?thesis* **.**
qed

lemma *H2-H3-absorb*:
H2 (*H3 P*) = *H3 P*
by (*metis H2-def H3-def seqr-assoc skip-d-absorb-J-1*)

lemma *H3-H2-absorb*:
H3 (*H2 P*) = *H3 P*
by (*metis H2-def H3-def seqr-assoc skip-d-absorb-J-2*)

theorem *H2-H3-commute*:
H2 (*H3 P*) = *H3* (*H2 P*)
by (*simp add*: *H2-H3-absorb H3-H2-absorb*)

theorem *H3-design-pre*:
assumes $\$ok \sharp p$ $out\alpha \sharp p$ $\$ok \sharp Q$ $\$ok' \sharp Q$
shows $H3(p \vdash Q) = p \vdash Q$
using *assms*
by (*metis Healthy-def′ design-H3-iff-pre precond-right-unit unrest-outα-var uvar-ok vwb-lens-mwb*)

theorem *H3-rdesign-pre*:
assumes $out\alpha \sharp p$
shows $H3(p \vdash_r Q) = p \vdash_r Q$
using *assms*
by (*simp add*: *H3-def*)

theorem *H1-H3-is-rdesign*:
assumes *P is H1 P is H3*
shows $P = pre_D(P) \vdash_r post_D(P)$
by (*metis H1-H2-is-rdesign H2-H3-absorb Healthy-def′ assms*)

theorem *H1-H3-is-normal-design*:
assumes *P is H1 P is H3*

shows $P = \lfloor pre_D(P) \rfloor_< \vdash_n post_D(P)$
by (*metis H1-H3-is-rdesign assms drop-pre-inv ndesign-def precond-equiv rdesign-H3-iff-pre*)

abbreviation *H1-H3 p* $\equiv$ *H1* (*H3 p*)

theorem *wpd-seq-r-H1-H2* [*wp*]:
fixes *P Q* :: *'α hrelation-d*
assumes *P is H1-H3 Q is H1-H3*
shows $(P \;;;\; Q)\ wp_D\ r = P\ wp_D\ (Q\ wp_D\ r)$
by (*smt H1-H3-commute H1-H3-is-rdesign H1-idem Healthy-def' assms*(*1*) *assms*(*2*) *drop-pre-inv precond-equiv rdesign-H3-iff-pre wpd-seq-r*)

10.6 H4: Feasibility

theorem *H4-idem*:
$H4(H4(P)) = H4(P)$
by *pred-tac*

end

11 Concurrent programming

theory *utp-concurrency*
imports *utp-designs*
begin

no-notation
Sublist.parallel (**infixl** ‖ *50*)

11.1 Design parallel composition

definition *design-par* :: (*'α*, *'β*) *relation-d* ⇒ (*'α*, *'β*) *relation-d* ⇒ (*'α*, *'β*) *relation-d* (**infixr** ‖ *85*)
where
$P \parallel Q = ((pre_D(P) \land pre_D(Q)) \vdash_r (post_D(P) \land post_D(Q)))$

declare *design-par-def* [*upred-defs*]

lemma *parallel-zero*: $P \parallel true = true$
proof −
have $P \parallel true = (pre_D(P) \land pre_D(true)) \vdash_r (post_D(P) \land post_D(true))$
by (*simp add*: *design-par-def*)
also have ... $= (pre_D(P) \land false) \vdash_r (post_D(P) \land true)$
by *rel-tac*
also have ... $= true$
by *rel-tac*
finally show *?thesis* **.**
qed

lemma *parallel-assoc*: $P \parallel Q \parallel R = (P \parallel Q) \parallel R$
by *rel-tac*

lemma *parallel-comm*: $P \parallel Q = Q \parallel P$
by *pred-tac*

lemma *parallel-idem*:

assumes *P is H1 P is H2*
shows $P \parallel P = P$
by (*metis H1-H2-is-rdesign assms conj-idem design-par-def*)

lemma *parallel-mono-1*:
assumes $P_1 \sqsubseteq P_2$ P_1 *is H1-H2* P_2 *is H1-H2*
shows $P_1 \parallel Q \sqsubseteq P_2 \parallel Q$
proof −
have $pre_D(P_1) \vdash_r post_D(P_1) \sqsubseteq pre_D(P_2) \vdash_r post_D(P_2)$
by (*metis H1-H2-commute H1-H2-is-rdesign H1-idem Healthy-def' assms*)
hence $(pre_D(P_1) \vdash_r post_D(P_1)) \parallel Q \sqsubseteq (pre_D(P_2) \vdash_r post_D(P_2)) \parallel Q$
by (*auto simp add*: *rdesign-refinement design-par-def*) (*pred-tac*+)
thus *?thesis*
by (*metis H1-H2-commute H1-H2-is-rdesign H1-idem Healthy-def' assms*)
qed

lemma *parallel-mono-2*:
assumes $Q_1 \sqsubseteq Q_2$ Q_1 *is H1-H2* Q_2 *is H1-H2*
shows $P \parallel Q_1 \sqsubseteq P \parallel Q_2$
by (*metis assms parallel-comm parallel-mono-1*)

11.2 Parallel by merge

We describe the partition of a state space into two pieces.

type-synonym $'\alpha$ *partition* $= {'\alpha} \times {'\alpha}$

definition *left-uvar* $x = x ;_L fst_L ;_L snd_L ;_L$ *des-lens*

definition *right-uvar* $x = x ;_L snd_L ;_L snd_L ;_L$ *des-lens*

declare *left-uvar-def* [*upred-defs*]

declare *right-uvar-def* [*upred-defs*]

Extract the ith element of the second part

definition *ind-uvar i x* $= x ;_L$ *list-lens i* $;_L snd_L ;_L$ *des-lens*

definition *pre-uvar* $x = x ;_L fst_L ;_L$ *des-lens*

definition *in-ind-uvar i x* = *in-var* (*ind-uvar i x*)

definition *out-ind-uvar i x* = *out-var* (*ind-uvar i x*)

definition *in-pre-uvar x* = *in-var* (*pre-uvar x*)

definition *out-pre-uvar x* = *out-var* (*pre-uvar x*)

definition *in-ind-uexpr i x* = *var* (*in-ind-uvar i x*)

definition *out-ind-uexpr i x* = *var* (*out-ind-uvar i x*)

definition *in-pre-uexpr x* = *var* (*in-pre-uvar x*)

definition *out-pre-uexpr x* = *var* (*out-pre-uvar x*)

declare *ind-uvar-def* [*urel-defs*]
declare *ind-uvar-def* [*upred-defs*]

declare *in-ind-uvar-def* [*upred-defs*]
declare *out-ind-uvar-def* [*upred-defs*]

declare *in-ind-uexpr-def* [*upred-defs*]
declare *out-ind-uexpr-def* [*upred-defs*]

declare *in-pre-uexpr-def* [*upred-defs*]
declare *out-pre-uexpr-def* [*upred-defs*]

lemma *left-uvar-indep-right-uvar* [*simp*]:
left-uvar x ⋈ *right-uvar y*
apply (*simp add*: *left-uvar-def right-uvar-def lens-comp-assoc*[*THEN sym*])
apply (*metis in-out-indep in-var-def lens-indep-left-comp out-var-def out-var-indep uvar-des-lens vwb-lens-mwb*)
done

lemma *right-uvar-indep-left-uvar* [*simp*]:
right-uvar x ⋈ *left-uvar y*
by (*simp add*: *lens-indep-sym*)

lemma *left-uvar* [*simp*]: *uvar x* ⟹ *uvar* (*left-uvar x*)
by (*simp add*: *left-uvar-def comp-vwb-lens fst-vwb-lens snd-vwb-lens*)

lemma *right-uvar* [*simp*]: *uvar x* ⟹ *uvar* (*right-uvar x*)
by (*simp add*: *right-uvar-def comp-vwb-lens fst-vwb-lens snd-vwb-lens*)

lemma *ind-uvar-indep* [*simp*]:
⟦*mwb-lens x*; *i* ≠ *j*⟧ ⟹ *ind-uvar i x* ⋈ *ind-uvar j x*
apply (*simp add*: *ind-uvar-def lens-comp-assoc*[*THEN sym*])
apply (*metis lens-indep-left-comp lens-indep-right-comp list-lens-indep out-var-def out-var-indep uvar-des-lens vwb-lens-mwb*)
done

lemma *ind-uvar-semi-uvar* [*simp*]:
semi-uvar x ⟹ *semi-uvar* (*ind-uvar i x*)
by (*auto intro*!: *comp-mwb-lens list-mwb-lens simp add*: *ind-uvar-def snd-vwb-lens*)

lemma *in-ind-uvar-semi-uvar* [*simp*]:
semi-uvar x ⟹ *semi-uvar* (*in-ind-uvar i x*)
by (*simp add*: *in-ind-uvar-def*)

lemma *out-ind-uvar-semi-uvar* [*simp*]:
semi-uvar x ⟹ *semi-uvar* (*out-ind-uvar i x*)
by (*simp add*: *out-ind-uvar-def*)

declare *id-vwb-lens* [*simp*]

syntax
-svarpre :: *svid* ⇒ *svid* (*-*$_<$ [*999*] *999*)
-svarleft :: *svid* ⇒ *svid* (*0*−*-* [*999*] *999*)
-svarright :: *svid* ⇒ *svid* (*1*−*-* [*999*] *999*)

translations
  -svarpre x == CONST pre-uvar x
  -svarleft x == CONST left-uvar x
  -svarright x == CONST right-uvar x

type-synonym $'\alpha$ *merge* = $('\alpha$ *alphabet-d* $\times$ $'\alpha$ *alphabet-d partition*, $'\alpha)$ *relation-d*

Separating simulations. I assume that the value of ok' should track the value of n.ok'.

definition $U0 = ((\$0{-}\Sigma' =_u \$\Sigma) \wedge (\$ok' =_u \$ok))$

definition $U1 = ((\$1{-}\Sigma' =_u \$\Sigma) \wedge (\$ok' =_u \$ok))$

declare *U0-def* [*upred-defs*]
declare *U1-def* [*upred-defs*]

The following implementation of parallel by merge is less general than the book version, in that it does not properly partition the alphabet into two disjoint segments. We could actually achieve this specifying lenses into the larger alphabet, but this would complicate the definition of programs. May reconsider later.

definition *par-by-merge* ::
  $'\alpha$ *hrelation-d* $\Rightarrow$ $'\alpha$ *merge* $\Rightarrow$ $'\alpha$ *hrelation-d* $\Rightarrow$ $'\alpha$ *hrelation-d* (**infixr** $\|_{\_}$ *85*)
where $P \|_M Q = ((((P ;; U0) \| (Q ;; U1)) \wedge \$\Sigma_<' =_u \$\Sigma) ;; M)$

definition $swap_m = \$0{-}\Sigma, \$1{-}\Sigma :=_D \$1{-}\Sigma, \$0{-}\Sigma$

declare *One-nat-def* [*simp del*]

declare $swap_m$*-def* [*upred-defs*]

end

12 Reactive processes

theory *utp-reactive*
imports
  utp-concurrency
  utp-event
begin

12.1 Preliminaries

type-synonym $'\alpha$ *trace* = $'\alpha$ *list*

fun *list-diff* ::$'\alpha$ *list* $\Rightarrow$ $'\alpha$ *list* $\Rightarrow$ $'\alpha$ *list option* **where**
   list-diff l [] = *Some l*
  | *list-diff* [] *l* = *None*
  | *list-diff* (*x#xs*) (*y#ys*) = (*if* (*x* = *y*) *then* (*list-diff xs ys*) *else None*)

lemma *list-diff-empty* [*simp*]: *the* (*list-diff l* []) = *l*
by (*cases l*) *auto*

lemma *prefix-subst* [*simp*]: $l \mathbin{@} t = m \Longrightarrow m - l = t$

by (*auto*)

lemma *prefix-subst1* [*simp*]: $m = l\ @\ t \Longrightarrow m - l = t$
by (*auto*)

The definitions of reactive process alphabets and healthiness conditions are given in the following. The healthiness conditions of reactive processes are defined by $R1$, $R2$, $R3$ and their composition R.

type-synonym $'\vartheta$ *refusal* = $'\vartheta$ *set*

record $'\vartheta$ *alpha-rp* = *alpha-d* +
rp-wait :: *bool*
rp-tr :: $'\vartheta$ *trace*
rp-ref :: $'\vartheta$ *refusal*

definition *wait* = *VAR rp-wait*
definition *tr* = *VAR rp-tr*
definition *ref* = *VAR rp-ref*

declare *wait-def* [*upred-defs*]
declare *tr-def* [*upred-defs*]
declare *ref-def* [*upred-defs*]

lemma *tr-ok-indep* [*simp*]: *tr* $\bowtie$ *ok ok* $\bowtie$ *tr*
by (*auto intro*!: *lens-indepI*, *pred-tac*+)

lemma *wait-ok-indep* [*simp*]: *wait* $\bowtie$ *ok ok* $\bowtie$ *wait*
by (*auto intro*!: *lens-indepI*, *pred-tac*+)

lemma *ref-ok-indep* [*simp*]: *ref* $\bowtie$ *ok ok* $\bowtie$ *ref*
by (*auto intro*!: *lens-indepI*, *pred-tac*+)

lemma *tr-wait-indep* [*simp*]: *tr* $\bowtie$ *wait wait* $\bowtie$ *tr*
by (*auto intro*!: *lens-indepI*, *pred-tac*+)

lemma *ref-wait-indep* [*simp*]: *ref* $\bowtie$ *wait wait* $\bowtie$ *ref*
by (*auto intro*!: *lens-indepI*, *pred-tac*+)

lemma *tr-ref-indep* [*simp*]: *ref* $\bowtie$ *tr tr* $\bowtie$ *ref*
by (*auto intro*!: *lens-indepI*, *pred-tac*+)

instantiation *alpha-rp-ext* :: (*type*, *vst*) *vst*
begin
definition *get-vstore-alpha-rp-ext* :: ($'a$, $'b$) *alpha-rp-ext* $\Rightarrow$ *vstore*
where [*simp*]: *get-vstore-alpha-rp-ext x* = *get-vstore* (*alpha-rp.more* (*alpha-d.extend undefined x*))
definition *put-vstore-alpha-rp-ext* :: ($'a$, $'b$) *alpha-rp-ext* $\Rightarrow$ *vstore* $\Rightarrow$ ($'a$, $'b$) *alpha-rp-ext*
where [*simp*]: *put-vstore-alpha-rp-ext s x* = *alpha-d.more* (*alpha-rp.more-update* (λv. *put-vstore v x*) (*alpha-d.extend undefined s*))
instance
apply (*intro-classes*, *auto simp add*: *alpha-rp.defs alpha-d.defs*)
apply (*metis alpha-d.select-convs*(*2*) *alpha-rp.select-convs*(*4*) *alpha-rp.surjective alpha-rp.update-convs*(*4*) *put-get-vstore*)
apply (*metis* (*no-types*, *lifting*) *alpha-d.select-convs*(*2*) *alpha-rp.surjective alpha-rp.update-convs*(*4*) *get-put-vstore*)
apply (*metis* (*no-types*, *lifting*) *alpha-d.select-convs*(*2*) *alpha-rp.surjective alpha-rp.update-convs*(*4*)

put-put-vstore)
done
end

lemma *uvar-wait* [*simp*]: *uvar wait*
 by (*unfold-locales*, *simp-all add*: *wait-def*)

lemma *uvar-tr* [*simp*]: *uvar tr*
 by (*unfold-locales*, *simp-all add*: *tr-def*)

lemma *uvar-ref* [*simp*]: *uvar ref*
 by (*unfold-locales*, *simp-all add*: *ref-def*)

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

type-synonym $('\vartheta,'\alpha)$ *alphabet-rp* = $('\vartheta,'\alpha)$ *alpha-rp-scheme alphabet*
type-synonym $('\vartheta,'\alpha,'\beta)$ *relation-rp* = $(('\vartheta,'\alpha)$ *alphabet-rp*, $('\vartheta,'\beta)$ *alphabet-rp*) *relation*
type-synonym $('\vartheta,'\alpha)$ *hrelation-rp* = $(('\vartheta,'\alpha)$ *alphabet-rp*, $('\vartheta,'\alpha)$ *alphabet-rp*) *relation*
type-synonym $('\vartheta,'\sigma)$ *predicate-rp* = $('\vartheta,'\sigma)$ *alphabet-rp upred*

abbreviation *wait-f*::$('\vartheta,\ '\alpha,\ '\beta)$ *relation-rp* $\Rightarrow$ $('\vartheta,\ '\alpha,\ '\beta)$ *relation-rp* $(\text{-}_f\ [1000]\ 1000)$
where *wait-f* $R \equiv R[\![false/\$wait]\!]$

abbreviation *wait-t*::$('\vartheta,\ '\alpha,\ '\beta)$ *relation-rp* $\Rightarrow$ $('\vartheta,\ '\alpha,\ '\beta)$ *relation-rp* $(\text{-}_t\ [1000]\ 1000)$
where *wait-t* $R \equiv R[\![true/\$wait]\!]$

lift-definition *lift-rea* :: $('\alpha,\ '\beta)$ *relation* $\Rightarrow$ $('\vartheta,\ '\alpha,\ '\beta)$ *relation-rp* $(\lceil\text{-}\rceil_R)$ **is**
$\lambda\ P\ (A,\ A').\ P\ (more\ A,\ more\ A')$ **.**

lift-definition *drop-rea* :: $('\vartheta,\ '\alpha,\ '\beta)$ *relation-rp* $\Rightarrow$ $('\alpha,\ '\beta)$ *relation* $(\lfloor\text{-}\rfloor_R)$ **is**
$\lambda\ P\ (A,\ A').\ P\ ((\!|\ des\text{-}ok = True,\ rp\text{-}wait = True,\ rp\text{-}tr = [],\ rp\text{-}ref = \{\},\ \ldots = A\ |\!),$
$(\!|\ des\text{-}ok = True,\ rp\text{-}wait = True,\ rp\text{-}tr = [],\ rp\text{-}ref = \{\},\ \ldots = A'\ |\!))$ **.**

12.2 R1: Events cannot be undone

definition *R1-def* [*upred-defs*]: $R1\ (P) = (P \wedge (\$tr \leq_u \$tr'))$

lemma *R1-idem*: $R1(R1(P)) = R1(P)$
 by *pred-tac*

lemma *R1-mono*: $P \sqsubseteq Q \Longrightarrow R1(P) \sqsubseteq R1(Q)$
 by *pred-tac*

lemma *R1-conj*: $R1(P \wedge Q) = (R1(P) \wedge R1(Q))$
 by *pred-tac*

lemma *R1-disj*: $R1(P \vee Q) = (R1(P) \vee R1(Q))$
 by *pred-tac*

lemma *R1-extend-conj*: $R1(P \wedge Q) = (R1(P) \wedge Q)$
 by *pred-tac*

lemma *R1-cond*: $R1(P \triangleleft b \triangleright Q) = (R1(P) \triangleleft b \triangleright R1(Q))$
 by *rel-tac*

lemma *R1-negate-R1*: $R1(\neg R1(P)) = R1(\neg P)$
  by *pred-tac*

lemma *R1-wait-true*: $(R1\ P)_t = R1(P)_t$
  by *pred-tac*

lemma *R1-wait-false*: $(R1\ P)_f = R1(P)_f$
  by *pred-tac*

lemma *R1-skip*: $R1(II) = II$
  by *rel-tac*

lemma *R1-by-refinement*:
  P *is* $R1 \longleftrightarrow ((\$tr \le_u \$tr') \sqsubseteq P)$
  by *rel-tac*

lemma *tr-le-trans*:
  $(\$tr \le_u \$tr' \ ;;\ \$tr \le_u \$tr') = (\$tr \le_u \$tr')$
  by (*rel-tac*, *metis alpha-rp.select-convs*(*2*) *order-refl*)

lemma *R1-seqr-closure*:
  assumes P *is* $R1$ Q *is* $R1$
  shows $(P\ ;;\ Q)$ *is* $R1$
  using *assms* **unfolding** *R1-by-refinement*
  by (*metis seqr-mono tr-le-trans*)

lemma *R1-ok'-true*: $(R1(P))^t = R1(P^t)$
  by *pred-tac*

lemma *R1-ok'-false*: $(R1(P))^f = R1(P^f)$
  by *pred-tac*

lemma *R1-ok-true*: $(R1(P))[\![true/\$ok]\!] = R1(P[\![true/\$ok]\!])$
  by *pred-tac*

lemma *R1-ok-false*: $(R1(P))[\![false/\$ok]\!] = R1(P[\![false/\$ok]\!])$
  by *pred-tac*

lemma *seqr-R1-true-right*: $((P\ ;;\ R1(true)) \vee P) = (P\ ;;\ (\$tr \le_u \$tr'))$
  by *rel-tac*

12.3 R2

definition *R2s-def* [*upred-defs*]: $R2s\ (P) = (P[\![\langle\rangle/\$tr]\!][\![(\$tr'-\$tr)/\$tr']\!])$
definition *R2-def* [*upred-defs*]: $R2(P) = R1(R2s(P))$

lemma *R2s-idem*: $R2s(R2s(P)) = R2s(P)$
  by (*pred-tac*)

lemma *R2-idem*: $R2(R2(P)) = R2(P)$
  by (*pred-tac*)

lemma *R2-mono*: $P \sqsubseteq Q \Longrightarrow R2(P) \sqsubseteq R2(Q)$
  by (*pred-tac*)

lemma *R2s-conj*: $R2s(P \wedge Q) = (R2s(P) \wedge R2s(Q))$

by (*pred-tac*)

lemma *R2-conj*: $R2(P \wedge Q) = (R2(P) \wedge R2(Q))$
by (*pred-tac*)

lemma *R2s-condr*: $R2s(P \triangleleft b \triangleright Q) = (R2s(P) \triangleleft R2s(b) \triangleright R2s(Q))$
by *rel-tac*

lemma *R2-condr*: $R2(P \triangleleft b \triangleright Q) = (R2(P) \triangleleft R2(b) \triangleright R2(Q))$
by *rel-tac*

lemma *tr-prefix-as-concat*: $(xs \leq_u ys) = (\exists\ zs \cdot ys =_u xs\ \hat{}_u \ll zs \gg)$
by (*rel-tac*, *simp add*: *less-eq-list-def prefixeq-def*)

lemma *R2-form*:
$R2(P) = (\exists\ tt \cdot P[\![\langle\rangle/\$tr]\!][\![\ll tt \gg/\$tr']\!] \wedge \$tr' =_u \$tr\ \hat{}_u \ll tt \gg)$
by (*rel-tac*, *metis prefix-subst strict-prefixE*)

lemma *uconc-left-unit* [*simp*]: $\langle\rangle\ \hat{}_u\ e = e$
by *pred-tac*

lemma *uconc-right-unit* [*simp*]: $e\ \hat{}_u\ \langle\rangle = e$
by *pred-tac*

This laws is proven only for homogeneous relations, can it be generalised?

lemma *R2-seqr-form*:
fixes $P\ Q$ :: $('\vartheta,'\alpha,'\alpha)$ *relation-rp*
shows $(R2(P)\ ;;\ R2(Q)) =$
$(\exists\ tt_1 \cdot \exists\ tt_2 \cdot ((P[\![\langle\rangle/\$tr]\!][\![\ll tt_1 \gg/\$tr']\!])\ ;;\ (Q[\![\langle\rangle/\$tr]\!][\![\ll tt_2 \gg/\$tr']\!]))$
$\wedge (\$tr' =_u \$tr\ \hat{}_u \ll tt_1 \gg\ \hat{}_u \ll tt_2 \gg))$
proof −
have $(R2(P)\ ;;\ R2(Q)) = (\exists\ tr_0 \cdot (R2(P))[\![\ll tr_0 \gg/\$tr']\!]\ ;;\ (R2(Q))[\![\ll tr_0 \gg/\$tr]\!])$
by (*subst seqr-middle*[*of tr*], *simp-all*)
also have ... =
$(\exists\ tr_0 \cdot \exists\ tt_1 \cdot \exists\ tt_2 \cdot ((P[\![\langle\rangle/\$tr]\!][\![\ll tt_1 \gg/\$tr']\!] \wedge \ll tr_0 \gg =_u \$tr\ \hat{}_u \ll tt_1 \gg)\ ;;$
$(Q[\![\langle\rangle/\$tr]\!][\![\ll tt_2 \gg/\$tr']\!] \wedge \$tr' =_u \ll tr_0 \gg\ \hat{}_u \ll tt_2 \gg)))$
by (*simp add*: *R2-form usubst unrest uquant-lift*, *rel-tac*)
also have ... =
$(\exists\ tr_0 \cdot \exists\ tt_1 \cdot \exists\ tt_2 \cdot ((\ll tr_0 \gg =_u \$tr\ \hat{}_u \ll tt_1 \gg \wedge P[\![\langle\rangle/\$tr]\!][\![\ll tt_1 \gg/\$tr']\!])\ ;;$
$(Q[\![\langle\rangle/\$tr]\!][\![\ll tt_2 \gg/\$tr']\!] \wedge \$tr' =_u \ll tr_0 \gg\ \hat{}_u \ll tt_2 \gg)))$
by (*simp add*: *conj-comm*)
also have ... =
$(\exists\ tt_1 \cdot \exists\ tt_2 \cdot \exists\ tr_0 \cdot ((P[\![\langle\rangle/\$tr]\!][\![\ll tt_1 \gg/\$tr']\!])\ ;;\ (Q[\![\langle\rangle/\$tr]\!][\![\ll tt_2 \gg/\$tr']\!]))$
$\wedge \ll tr_0 \gg =_u \$tr\ \hat{}_u \ll tt_1 \gg \wedge \$tr' =_u \ll tr_0 \gg\ \hat{}_u \ll tt_2 \gg)$
by (*simp add*: *seqr-pre-out seqr-post-out unrest*, *rel-tac*)
also have ... =
$(\exists\ tt_1 \cdot \exists\ tt_2 \cdot ((P[\![\langle\rangle/\$tr]\!][\![\ll tt_1 \gg/\$tr']\!])\ ;;\ (Q[\![\langle\rangle/\$tr]\!][\![\ll tt_2 \gg/\$tr']\!]))$
$\wedge (\exists\ tr_0 \cdot \ll tr_0 \gg =_u \$tr\ \hat{}_u \ll tt_1 \gg \wedge \$tr' =_u \ll tr_0 \gg\ \hat{}_u \ll tt_2 \gg))$
by *rel-tac*
also have ... =
$(\exists\ tt_1 \cdot \exists\ tt_2 \cdot ((P[\![\langle\rangle/\$tr]\!][\![\ll tt_1 \gg/\$tr']\!])\ ;;\ (Q[\![\langle\rangle/\$tr]\!][\![\ll tt_2 \gg/\$tr']\!]))$
$\wedge (\$tr' =_u \$tr\ \hat{}_u \ll tt_1 \gg\ \hat{}_u \ll tt_2 \gg))$
by *rel-tac*
finally show *?thesis* **.**
qed

lemma *R2-seqr-distribute*:
  fixes $P\ Q$ :: $('\vartheta,'\alpha,'\alpha)$ *relation-rp*
  shows $R2(R2(P)\ ;;\ R2(Q)) = (R2(P)\ ;;\ R2(Q))$
proof –
  have $R2(R2(P)\ ;;\ R2(Q)) =$
    $((\exists\ tt_1 \cdot \exists\ tt_2 \cdot (P[\![\langle\rangle/\$tr]\!][\![\ll tt_1\gg/\$tr']\!]\ ;;\ Q[\![\langle\rangle/\$tr]\!][\![\ll tt_2\gg/\$tr']\!])[\![(\$tr' - \$tr)/\$tr']\!]$
      $\wedge\ \$tr' - \$tr =_u \ll tt_1\gg\ \hat{}_u \ll tt_2\gg) \wedge \$tr' \geq_u \$tr)$
    by (*simp add*: *R2-seqr-form*, *simp add*: *R2s-def usubst unrest*, *rel-tac*)
  also have ... =
    $((\exists\ tt_1 \cdot \exists\ tt_2 \cdot (P[\![\langle\rangle/\$tr]\!][\![\ll tt_1\gg/\$tr']\!]\ ;;\ Q[\![\langle\rangle/\$tr]\!][\![\ll tt_2\gg/\$tr']\!])[\![(\ll tt_1\gg\ \hat{}_u \ll tt_2\gg)/\$tr']\!]$
      $\wedge\ \$tr' - \$tr =_u \ll tt_1\gg\ \hat{}_u \ll tt_2\gg) \wedge \$tr' \geq_u \$tr)$
      by (*subst subst-eq-replace*, *simp*)
  also have ... =
    $((\exists\ tt_1 \cdot \exists\ tt_2 \cdot (P[\![\langle\rangle/\$tr]\!][\![\ll tt_1\gg/\$tr']\!]\ ;;\ Q[\![\langle\rangle/\$tr]\!][\![\ll tt_2\gg/\$tr']\!])$
      $\wedge\ \$tr' - \$tr =_u \ll tt_1\gg\ \hat{}_u \ll tt_2\gg) \wedge \$tr' \geq_u \$tr)$
      by (*simp add*: *usubst unrest*)
  also have ... =
    $(\exists\ tt_1 \cdot \exists\ tt_2 \cdot (P[\![\langle\rangle/\$tr]\!][\![\ll tt_1\gg/\$tr']\!]\ ;;\ Q[\![\langle\rangle/\$tr]\!][\![\ll tt_2\gg/\$tr']\!])$
      $\wedge\ (\$tr' - \$tr =_u \ll tt_1\gg\ \hat{}_u \ll tt_2\gg \wedge \$tr' \geq_u \$tr))$
    by *pred-tac*
  also have ... =
    $((\exists\ tt_1 \cdot \exists\ tt_2 \cdot (P[\![\langle\rangle/\$tr]\!][\![\ll tt_1\gg/\$tr']\!]\ ;;\ Q[\![\langle\rangle/\$tr]\!][\![\ll tt_2\gg/\$tr']\!])$
      $\wedge\ \$tr' =_u \$tr\ \hat{}_u \ll tt_1\gg\ \hat{}_u \ll tt_2\gg))$
  proof –
    have $\bigwedge\ tt_1\ tt_2.\ (((\$tr' - \$tr =_u \ll tt_1\gg\ \hat{}_u \ll tt_2\gg) \wedge \$tr' \geq_u \$tr) :: ('\vartheta,'\alpha,'\alpha)$ *relation-rp*)
          $= (\$tr' =_u \$tr\ \hat{}_u \ll tt_1\gg\ \hat{}_u \ll tt_2\gg)$
      by (*rel-tac*, *metis prefix-subst strict-prefixE*)
    thus *?thesis* **by** *simp*
  qed
  also have ... = $(R2(P)\ ;;\ R2(Q))$
    by (*simp add*: *R2-seqr-form*)
  finally show *?thesis* **.**
qed

lemma *R1-R2-commute*:
  $R1(R2(P)) = R2(R1(P))$
  by *pred-tac*

12.4 R3

definition *skip-rea-def* [*urel-defs*]: $II_r = (II \vee (\neg\ \$ok \wedge \$tr \leq_u \$tr'))$

definition *R3-def* [*upred-defs*]: $R3\ (P) = (II \triangleleft \$wait \triangleright P)$

definition *R3c-def* [*upred-defs*]: $R3c\ (P) = (II_r \triangleleft \$wait \triangleright P)$

definition *RH-def* [*upred-defs*]: $RH(P) = R1(R2(R3c(P)))$

lemma *R3-idem*: $R3(R3(P)) = R3(P)$
  by *rel-tac*

lemma *R3-mono*: $P \sqsubseteq Q \Longrightarrow R3(P) \sqsubseteq R3(Q)$
  by *rel-tac*

lemma *R3-conj*: $R3(P \wedge Q) = (R3(P) \wedge R3(Q))$

by *rel-tac*

lemma *R3-disj*: $R3(P \lor Q) = (R3(P) \lor R3(Q))$
by *rel-tac*

lemma *R3-condr*: $R3(P \triangleleft b \triangleright Q) = (R3(P) \triangleleft b \triangleright R3(Q))$
by *rel-tac*

lemma *R3-skipr*: $R3(II) = II$
by *rel-tac*

lemma *R3-form*: $R3(P) = ((\$wait \land II) \lor (\neg \$wait \land P))$
by *rel-tac*

lemma *R3-semir-form*:
$(R3(P) ;; R3(Q)) = R3(P ;; R3(Q))$
by *rel-tac*

lemma *R3-semir-closure*:
assumes *P is R3 Q is R3*
shows $(P ;; Q)$ *is R3*
using *assms*
by (*metis Healthy-def′ R3-semir-form*)

lemma *R1-R3-commute*: $R1(R3(P)) = R3(R1(P))$
by *rel-tac*

lemma *R2-R3-commute*: $R2(R3(P)) = R3(R2(P))$
by (*rel-tac*, (*metis* (*no-types*, *lifting*) *alpha-rp.surjective alpha-rp.update-convs*(*2*) *append-Nil2 prefix-subst strict-prefixE*)+)

lemma *R2-R3c-commute*: $R2(R3c(P)) = R3c(R2(P))$
by (*rel-tac*, (*metis* (*no-types*, *lifting*) *alpha-rp.surjective alpha-rp.update-convs*(*2*) *append-Nil2 append-minus strict-prefixE*)+)

lemma *R3c-idem*: $R3c(R3c(P)) = R3c(P)$
by *rel-tac*

lemma *R1-skip-rea*: $R1(II_r) = II_r$
by *rel-tac*

lemma *R2-skip-rea*: $R2(II_r) = II_r$
apply (*rel-tac*)
apply (*metis* (*no-types*, *lifting*) *alpha-rp.surjective alpha-rp.update-convs*(*2*) *append-Nil2 prefix-subst strict-prefixE*)
done

end