Unifying Theories of Programming in ProofPower-Z

January 28, 2008

Contents

1 UTP Relations Theory

1.1 Creating the Theory

SML

```
open_theory "utp−z−library";
force_delete_theory "utp−rel" handle Fail _ => ();
new_theory "utp−rel";
open_theory "utp−rel";
set_flags[("z_type_check_only",false),("z_use_axioms",true),
        ("standard_z_paras",false),("standard_z_terms",false)];

(* Setting PP to accept the refinement symbol *)
val _ =
        ReaderWriterSupport.PrettyNames.add_new_symbols
                [(["refinedby"],
                Value "⊑",
                ReaderWriterSupport.PrettyNames.Simple)]
        handle Fail _ => ()
;

(* Setting PP to accept the equivalence symbol *)
val _ =
        ReaderWriterSupport.PrettyNames.add_new_symbols
                [(["equivalentto"],
                Value "≡",
                ReaderWriterSupport.PrettyNames.Simple)]
        handle Fail _ => ()
;
```

1.2 Definitions

1.2.1 Names and Alphabets

z

$$[\boldsymbol{NAME}]$$

z

$$any\_name : NAME$$

z

$$\boldsymbol{ALPHABET} \mathrel{\widehat=} \mathbb{P}\ NAME$$

z

$$\boldsymbol{dash} : NAME \rightarrowtail NAME$$

z

$$\boldsymbol{one}, \boldsymbol{two} : NAME \rightarrowtail NAME$$

$$\mathrm{ran}\ one \cap \mathrm{ran}\ two = \varnothing$$

z

$$\boldsymbol{dashed} : ALPHABET$$

$$dashed = \mathrm{ran}\ dash$$

z

$$\boldsymbol{undashed} : ALPHABET$$

$$undashed = \{n : NAME \mid n \notin \mathrm{ran}\ dash\}$$

z

$$\boldsymbol{in\_a} : ALPHABET \rightarrow ALPHABET$$

$$\forall\ a{:}ALPHABET \bullet in\_a\ a = a \cap undashed$$

z

$$\boldsymbol{out\_a} : ALPHABET \rightarrow ALPHABET$$

$$\forall\ a{:}ALPHABET \bullet out\_a\ a = a \cap dashed$$

z

$$\boldsymbol{homogeneous} : \mathbb{P}\ ALPHABET$$

$$\begin{aligned} homogeneous = \{&a : ALPHABET \\ &\mid (\forall\ n : undashed \bullet n \in a \Leftrightarrow dash\ n \in a)\} \end{aligned}$$

z

$$\boldsymbol{composable} : \mathbb{P}\ (ALPHABET \times ALPHABET)$$

$$\begin{aligned} composable = \{&a1,\ a2 : ALPHABET \\ &\mid (\forall\ n : undashed \bullet n \in a2 \Leftrightarrow dash\ n \in a1)\} \end{aligned}$$

1.2.2 Bindings

z

$$\begin{aligned} \boldsymbol{VALUE} ::= {} & Int(\mathbb{Z}) \mid Bool(\mathbb{B}) \\ & \mid Channel(NAME) \\ & \mid Seq(seq\ VALUE) \mid Set(\mathbb{P}\ VALUE) \\ & \mid Pair(VALUE \times VALUE) \\ & \mid Sync \end{aligned}$$

z

$$\boldsymbol{INT\_VAL} \mathrel{\widehat=} \{n{:}\mathbb{Z} \bullet Int(n)\}$$

z

$$\boldsymbol{BOOL\_VAL} \mathrel{\widehat=} \{Bool(true), Bool(false)\}$$

z

$$\boldsymbol{CHANNEL\_VAL} \mathrel{\widehat{=}} \{n{:}NAME \bullet Channel(n)\}$$

z

$$\boldsymbol{SEQ\_VAL} \mathrel{\widehat{=}} \{s{:}\mathrm{seq}\ VALUE \bullet Seq(s)\}$$

z

$$\boldsymbol{SET\_VAL} \mathrel{\widehat{=}} \{s{:}\mathbb{P}\ VALUE \bullet Set(s)\}$$

z

$$\boldsymbol{PAIR\_VAL} \mathrel{\widehat{=}} \{v1,v2{:}VALUE \bullet Pair(v1,v2)\}$$

z

$$\boldsymbol{EVENT\_VAL} \mathrel{\widehat{=}} \{c{:}CHANNEL\_VAL;\ v{:}VALUE \bullet Pair(c,v)\}$$

z

$$\boldsymbol{SEQ\_EVENT\_VAL} \mathrel{\widehat{=}} \{s{:}\mathrm{seq}\ EVENT\_VAL \bullet Seq(s)\}$$

z

$$\boldsymbol{SET\_EVENT\_VAL} \mathrel{\widehat{=}} \{s{:}\mathbb{F}\ EVENT\_VAL \bullet Set(s)\}$$

z

$$\boldsymbol{SET\_SEQ\_EVENT\_VAL} \mathrel{\widehat{=}} \{s{:}\mathbb{F}\ SEQ\_EVENT\_VAL \bullet Set(s)\}$$

z

$$\boldsymbol{PAIR\_SEQ\_EVENT\_VAL} \mathrel{\widehat{=}} \{s1,s2{:}SEQ\_EVENT\_VAL \bullet Pair(s1,s2)\}$$

z

$$\boldsymbol{UNARY\_F} \mathrel{\widehat{=}} VALUE \nrightarrow VALUE$$

z

$$(\forall f{:}UNARY\_F;\ v{:}VALUE \bullet f\ v \in VALUE)$$

z

$\boldsymbol{any\_un\_fun} : UNARY\_F$

z

$\boldsymbol{BINARY\_F} \mathrel{\widehat{=}} (VALUE \times VALUE) \rightarrowtail\!\!\!\!\!\!\rightarrow VALUE$

z

$(\forall f{:}BINARY\_F;\ vv{:}VALUE \times VALUE \bullet f\ vv \in VALUE)$

z

$\boldsymbol{any\_bin\_fun} : BINARY\_F$

z

$\boldsymbol{RELATION} \mathrel{\widehat{=}} VALUE \leftrightarrow VALUE$

z

$\boldsymbol{any\_rel} : RELATION$

z

$$
\begin{aligned}
\boldsymbol{EXPRESSION} ::= {} & Val(VALUE) \\
& \mid Var\ (NAME) \\
& \mid Fun_1\ (UNARY\_F \times EXPRESSION) \\
& \mid Fun_2\ (BINARY\_F \times EXPRESSION \times EXPRESSION) \\
& \mid Rel\ (RELATION \times EXPRESSION \times EXPRESSION)
\end{aligned}
$$

z

$\boldsymbol{BINDING} \mathrel{\widehat{=}} NAME \rightarrowtail\!\!\!\!\!\!\rightarrow VALUE$

z

$\boldsymbol{BINDINGS} \mathrel{\widehat{=}} \mathbb{P}\ BINDING$

z

$\boldsymbol{FV} : EXPRESSION \rightarrow \mathbb{P}\ NAME$

$$\forall\ v{:}VALUE;\ n{:}NAME;\ exp1,exp2{:}EXPRESSION;$$
$$f1{:}UNARY\_F;\ f2{:}BINARY\_F;\ r{:}RELATION$$
$$\bullet\ FV\ (Val(v)) = \varnothing$$
$$\land\ FV\ (Var(n)) = \{n\}$$
$$\land\ FV(Fun_1(f1,exp1)) = FV(exp1)$$
$$\land\ FV(Fun_2(f2,exp1,exp2)) = FV(exp1) \cup FV(exp2)$$
$$\land\ FV(Rel(r,exp1,exp2)) = FV(exp1) \cup FV(exp2)$$

z

$$\boldsymbol{WF\_BINDING\_EXPRESSION_R} \mathrel{\widehat=}$$
$$\{b{:}BINDING;\ e{:}EXPRESSION \mid FV(e) \subseteq dom\ b\}$$

z

$$\boldsymbol{Eval} : WF\_BINDING\_EXPRESSION_R \to VALUE$$

$$\forall\ b{:}BINDING;\ v{:}VALUE;\ n{:}NAME;\ exp1,exp2{:}EXPRESSION;$$
$$f1{:}UNARY\_F;\ f2{:}BINARY\_F;\ r{:}RELATION$$
$$\bullet\ Eval\ (b,Val(v)) = v$$
$$\land\ (\ ((b,Var(n)) \in WF\_BINDING\_EXPRESSION_R) \Rightarrow$$
$$Eval\ (b,Var(n)) = b\ n\ )$$
$$\land\ (\ ((b,exp1) \in WF\_BINDING\_EXPRESSION_R) \Rightarrow$$
$$Eval\ (b,Fun_1(f1,exp1)) = f1\ (Eval(b,exp1))\ )$$
$$\land\ (\ ((b,exp1) \in WF\_BINDING\_EXPRESSION_R$$
$$\land\ (b,exp2) \in WF\_BINDING\_EXPRESSION_R) \Rightarrow$$
$$Eval\ (b,Fun_2(f2,exp1,exp2)) =$$
$$f2\ (Eval(b,exp1),Eval(b,exp2))\ )$$
$$\land\ (\ ((b,exp1) \in WF\_BINDING\_EXPRESSION_R$$
$$\land\ (b,exp2) \in WF\_BINDING\_EXPRESSION_R) \Rightarrow$$
$$Eval\ (b,Rel(r,exp1,exp2)) =$$
$$Bool((Eval(b,exp1),Eval(b,exp2)) \in r)\ )$$

1.2.3 UTP Relations Predicates

z

$$\boldsymbol{REL\_PREDICATE} \mathrel{\widehat=}$$

$$\{a{:}ALPHABET;\ bs{:}BINDINGS \mid (\forall b{:}bs \bullet dom\ b = a)\}$$

z

$$\boldsymbol{UnrestVar} : REL\_PREDICATE \rightarrow \mathbb{P}\ NAME$$

$$\begin{array}{l}
\forall\ u{:}REL_PREDICATE \\
\quad \bullet\ UnrestVar\ u = \{n{:}u.1 \mid (\forall\ b{:}u.2;\ v{:}VALUE \\
\qquad\qquad\qquad \bullet\ b \oplus \{n \mapsto v\} \in u.2)\}
\end{array}$$

z

$$\boldsymbol{unrestTypedVar} : (REL\_PREDICATE \times NAME \times \mathbb{P}\ VALUE) \rightarrow \mathbb{B}$$

$$\begin{array}{l}
\forall\ r{:}REL_PREDICATE;\ n{:}NAME;\ T{:}\mathbb{P}\ VALUE \bullet \\
unrestTypedVar(r,n,T) \Leftrightarrow (\forall b{:}r.2;\ v{:}T \bullet b \oplus \{n \mapsto v\} \in r.2)
\end{array}$$

z

$$\boldsymbol{REL\_CONDITION} : \mathbb{P}\ REL\_PREDICATE$$

$$\begin{array}{l}
REL_CONDITION = \{r : REL_PREDICATE \\
\qquad\qquad \mid (r.1 \setminus undashed) \subseteq UnrestVar(r)\ \}
\end{array}$$

z

$$\boldsymbol{dashCond} : REL\_CONDITION \rightarrow REL\_PREDICATE$$

$$\begin{array}{l}
\forall\ u{:}REL_CONDITION \bullet \\
\quad dashCond(u) = (\{n{:}u.1 \mid n \in undashed \bullet dash\ n\} \cup u.1, \\
\qquad\qquad \{b{:}u.2 \\
\qquad\qquad \bullet \\
\qquad\qquad \{n{:}dom\ b \cap undashed \bullet dash\ n \mapsto b\ n\} \\
\qquad\qquad \cup \\
\qquad\qquad \{n{:}dash\ (\!| dom\ b \cap dashed |\!)
\end{array}$$

$$
\begin{array}{l}
\boldsymbol{U} : ((NAME \rightarrowtail NAME) \times ALPHABET) \nrightarrow REL\_PREDICATE \\
\hline
\forall\ f{:}NAME \rightarrowtail NAME\ ;\ a'{:}ALPHABET \\
\quad \mid a' \subseteq dashed \\
\quad \bullet (\exists a{:}ALPHABET \\
\qquad \mid a \subseteq undashed \\
\qquad \wedge\ a' = dash\ (\!| a |\!) \\
\qquad \bullet\ U\ (f,a') = \\
\qquad (\{n{:}NAME \mid n \in a \bullet dash(f\ \ n)\} \cup\ a, \\
\qquad\quad \{\ b{:}BINDING \\
\qquad\quad \mid dom\ b = \{n{:}NAME \mid n \in a \bullet dash(f\ \ n)\} \\
\qquad\qquad \cup\ a \\
\qquad\quad \wedge\ (\forall\ n{:}NAME \mid n \in a \bullet \\
\qquad\qquad b(dash(f\ \ n)) = b(n))\ \} \\
\qquad\quad) \\
\quad)
\end{array}
$$

1.2.4 Syntactic Restrictions

$$
\begin{array}{l}
\boldsymbol{WF\_Equals_R} \mathrel{\widehat=} \\
\quad \{a{:}ALPHABET;\ n{:}NAME;\ e{:}EXPRESSION \mid n \in a \wedge FV(e) \subseteq a\}
\end{array}
$$

$$
\begin{array}{l}
\boldsymbol{WF\_ALPHABET\_EXPRESSION} \mathrel{\widehat=} \\
\quad \{a{:}ALPHABET;e1,e2{:}EXPRESSION \mid (FV(e1) \cup FV(e2)) \subseteq a\}
\end{array}
$$

$$
\begin{array}{l}
\boldsymbol{WF\_Cond_R} \mathrel{\widehat=} \\
\quad \{u1,b,u2{:}REL\_PREDICATE \mid (b.1 \subseteq u1.1 \wedge u1.1 = u2.1)\}
\end{array}
$$

$$
\boldsymbol{WF\_Semi_R} \mathrel{\widehat=}
$$

$\quad \{u1,u2{:}REL\_PREDICATE \mid (u1.1,\ u2.1) \in composable\ \}$

z

$\boldsymbol{WF\_Skip_R} \mathrel{\widehat=} \{a{:}ALPHABET \mid a \in homogeneous\ \}$

z

$\boldsymbol{WF\_Assign_R} \mathrel{\widehat=}$

$\quad \{a{:}ALPHABET;\ ns{:}seq\ NAME;\ exps{:}seq\ EXPRESSION$

$\quad \mid (\forall n{:}ran\ ns \bullet n \in a \land n \in undashed)$

$\quad \land (\forall e{:}ran\ exps \bullet FV(e) \subseteq a \land FV(e) \subseteq undashed)$

$\quad \land \#ns = \#exps \neq 0$

$\quad \land a \in homogeneous\}$

z

$\boldsymbol{WF\_Subst_R} \mathrel{\widehat=}$

$\quad \{u{:}REL\_PREDICATE;\ e{:}EXPRESSION;\ n{:}NAME$

$\quad \mid FV(e) \subseteq u.1 \land n \in u.1\}$

z

$\boldsymbol{WF\_Var_{R\_EndR}} \mathrel{\widehat=}$

$\quad \{a{:}ALPHABET;\ n{:}NAME \mid a \in homogeneous \land n \in undashed$

$\qquad\qquad \land \{n,dash(n)\} \subseteq a\}$

z

$\boldsymbol{WF\_VarT_{R\_EndTR}} \mathrel{\widehat=}$

$\quad \{a{:}ALPHABET;\ n{:}NAME;\ T{:}SET\_VAL \mid (a,n) \in WF\_Var_{R\_EndR}\}$

z

$\boldsymbol{WF\_Extend\_rest_R} \mathrel{\widehat=}$

$\quad \{u : REL\_PREDICATE;\ a : ALPHABET$

$\quad \mid a \subseteq undashed \land (a \cup \{n{:}a \bullet dash\ n\}) \cap u.1 = \varnothing\}$

z

$\boldsymbol{WF\_REL\_PREDICATE\_PAIR} \mathrel{\widehat=}$

$\{u1,u2{:}REL\_PREDICATE \mid u1.1 = u2.1\}$

z

$WF\_Glb_{R\_LubR} \mathrel{\widehat=} \{a{:}ALPHABET;\ us{:}\mathbb{P}\ REL\_PREDICATE$
$\mid (\forall u\_us{:}us \bullet u\_us.1 = a)\}$

1.2.5 Operations on Values

z

$rel\ \_ \leq_{\boldsymbol{R}} \_$

z

$\_ \leq_{\boldsymbol{R}} \_ : VALUE \leftrightarrow VALUE$

$(\_ \leq_R \_) = \{s1,s2{:}SEQ\_VAL$
$\mid ((Seq^\sim)s1)\ prefix_Z\ ((Seq^\sim)s2)\}$

z

$rel\ \_ <_{\boldsymbol{R}} \_$

z

$\_ <_{\boldsymbol{R}} \_ : VALUE \leftrightarrow VALUE$

$(\_ <_R \_) = \{s1,s2{:}SEQ\_VAL$
$\mid ((Seq^\sim)s1)\ prefix_Z\ ((Seq^\sim)s2)$
$\land ((Seq^\sim)s1) \neq ((Seq^\sim)s2)\}$

z

$rel\ \_ \in_{\boldsymbol{R}} \_$

z

$\_ \in_{\boldsymbol{R}} \_ : VALUE \leftrightarrow VALUE$

$(\_ \in_R \_) = \{e{:}VALUE;\ s{:}SET\_VAL \mid e \in ((Set^\sim)s)\}$

z

$$rel\ \_ \notin_{\boldsymbol{R}} \_$$

z

$$\_ \notin_{\boldsymbol{R}} \_ : VALUE \leftrightarrow VALUE$$

$$(\_ \notin_R \_) = \{e{:}VALUE;\ s{:}SET\_VAL \mid e \notin ((Set^{\sim})s)\}$$

z

$$rel\ \_ \subseteq_{\boldsymbol{R}} \_$$

z

$$\_ \subseteq_{\boldsymbol{R}} \_ : VALUE \leftrightarrow VALUE$$

$$(\_ \subseteq_R \_) = \{s1,s2{:}SET\_VAL \mid ((Set^{\sim})s1) \subseteq ((Set^{\sim})s2)\}$$

z

$$\boldsymbol{MkSingleton}: VALUE \rightarrow VALUE$$

$$\forall\ v{:}VALUE \bullet MkSingleton(v) = Seq(\langle v \rangle)$$

z

$$\boldsymbol{MkPair}: (VALUE \times VALUE) \rightarrow VALUE$$

$$\forall\ v1,v2{:}VALUE \bullet MkPair(v1,v2) = Pair(v1,v2)$$

z

$$fun\ \_\ \boldsymbol{SeqDif}_{\boldsymbol{R}}\ \_$$

z

$$\_\ \boldsymbol{SeqDif}_{\boldsymbol{R}}\ \_ : (VALUE \times VALUE) \nrightarrow VALUE$$

$$\forall\ s1,s2{:}VALUE \mid \{s1,s2\} \subseteq SEQ\_VAL$$
$$\quad \wedge\ ((Seq^{\sim})\ s2)\ prefix_{Z}\ ((Seq^{\sim})\ s1)$$
$$\quad \bullet\ s1\ SeqDif_{R}\ s2 =$$
$$\qquad Seq(\ ((Seq^{\sim})s1) -_{Z} ((Seq^{\sim})s2)\ )$$

z

$$fun\ \_\ {}^\frown_{\boldsymbol{R}}\ \_$$

z

$$\_\ {}^\frown_{\boldsymbol{R}}\ \_ : (VALUE \times VALUE) \rightarrow\!\!\!\!\!\!+\ VALUE$$

$$\forall\ s1,s2{:}VALUE$$
$$\quad \mid \{s1,s2\} \subseteq SEQ\_VAL$$
$$\quad \bullet\ s1\ {}^\frown_{R}\ s2 = Seq(\ ((Seq^{\sim})s1)\ {}^\frown\ ((Seq^{\sim})s2)\ )$$

z

$$fun\ \_\ \upharpoonright_{\boldsymbol{R}}\ \_$$

z

$$\_\ \upharpoonright_{\boldsymbol{R}}\ \_ : (VALUE \times VALUE) \rightarrow\!\!\!\!\!\!+\ VALUE$$

$$\forall\ s,st\ {:}VALUE$$
$$\quad \mid s \in SEQ\_VAL \wedge st \in SET\_VAL$$
$$\quad \bullet\ s \upharpoonright_{R} st = Seq(((Seq^{\sim})s) \upharpoonright ((Set^{\sim})st))$$

z

$$fun\ \_\ \cup_{\boldsymbol{R}}\ \_$$

z

$$\_\ \cup_{\boldsymbol{R}}\ \_ : (VALUE \times VALUE) \rightarrow\!\!\!\!\!\!+\ VALUE$$

$$\forall\ s1,s2{:}VALUE$$
$$\quad \mid \{s1,s2\} \subseteq SET\_VAL$$

$\bullet\ s1 \cup_R s2 = Set(\ ((Set^{\sim})s1) \cup ((Set^{\sim})s2)\ )$

z

$fun\ \_ \cap_{\boldsymbol{R}} \_$

z

$\_ \cap_{\boldsymbol{R}} \_ : (VALUE \times VALUE) \nrightarrow VALUE$

$\forall\ s1,s2 : VALUE$
$\quad | \{s1,s2\} \subseteq SET\_VAL$
$\quad \bullet\ s1 \cap_R s2 = Set(\ ((Set^{\sim})s1) \cap ((Set^{\sim})s2)\ )$

z

$fun\ \_ \setminus_{\boldsymbol{R}} \_$

z

$\_ \setminus_{\boldsymbol{R}} \_ : (VALUE \times VALUE) \nrightarrow VALUE$

$\forall\ s1,s2 : VALUE$
$\quad | \{s1,s2\} \subseteq SET\_VAL$
$\quad \bullet\ s1 \setminus_R s2 = Set(\ ((Set^{\sim})s1) \setminus ((Set^{\sim})s2)\ )$

1.2.6 Relations Constructs

z

$\boldsymbol{True_R} : ALPHABET \rightarrow REL\_PREDICATE$

$\forall\ a : ALPHABET \bullet True_R\ a = (a, \{b : BINDING \mid dom\ b = a\})$

z

$\boldsymbol{False_R} : ALPHABET \rightarrow REL\_PREDICATE$

$\forall\ a : ALPHABET \bullet False_R\ a = (a, \varnothing)$

z

$$fun\ \_\ \equiv_{\boldsymbol{R}}\ \_$$

z

$$\_\ \equiv_{\boldsymbol{R}}\ \_ : (REL\_PREDICATE \times REL\_PREDICATE) \rightarrow REL\_PREDICATE$$

$$\forall\ u1,u2{:}REL\_PREDICATE$$
$$\bullet\ (u1.1 = u2.1 \wedge u1.2 = u2.2 \Rightarrow u1 \equiv_R u2 = True_R\ u1.1)$$
$$\wedge\ (u1.1 \neq u2.1 \vee u1.2 \neq u2.2 \Rightarrow u1 \equiv_R u2 = False_R\ u1.1)$$

z

$$=_{\boldsymbol{R}} : WF\_Equals_R \rightarrow REL\_PREDICATE$$

$$\forall\ a\_n\_e{:}WF\_Equals_R$$
$$\bullet =_R (a\_n\_e) =$$
$$(a\_n\_e.1,\ \{b{:}BINDING$$
$$\mid dom\ b = a\_n\_e.1$$
$$\wedge\ b(a\_n\_e.2) =$$
$$Eval(b,a\_n\_e.3)\})$$

z

$$=_{+\boldsymbol{R}} : WF\_ALPHABET\_EXPRESSION \rightarrow REL\_PREDICATE$$

$$\forall\ a\_e\_e{:}WF\_ALPHABET\_EXPRESSION$$
$$\bullet =_{+R} (a\_e\_e) =$$
$$(a\_e\_e.1,\ \{b{:}BINDING$$
$$\mid dom\ b = a\_e\_e.1$$
$$\wedge\ Eval(b,a\_e\_e.2) =$$
$$Eval(b,a\_e\_e.3)\})$$

z

$$\neg_{\boldsymbol{R}} : REL\_PREDICATE \rightarrow REL\_PREDICATE$$

$\forall\ u{:}REL\_PREDICATE \bullet \neg_R\ u = (u.1,\ (True_R\ u.1).2 \setminus u.2)$

z

$fun\ \_ \oplus_{\boldsymbol{R}} \_$

z

$\_ \oplus_{\boldsymbol{R}} \_ : REL\_PREDICATE \times ALPHABET \rightarrow REL\_PREDICATE$

$$\forall\ u{:}REL\_PREDICATE;\ a : ALPHABET \bullet u \oplus_R a = (u.1 \cup a, \{b{:}BINDING \mid (u.1 \lhd b) \in u.2 \land dom\ b = u.1 \cup a\})$$

z

$fun\ \_ \wedge_{\boldsymbol{R}} \_$

z

$\_ \wedge_{\boldsymbol{R}} \_ : REL\_PREDICATE \times REL\_PREDICATE \rightarrow REL\_PREDICATE$

$$\forall\ u1,u2{:}REL\_PREDICATE \bullet u1 \wedge_R u2 = (u1.1 \cup u2.1, (u1 \oplus_R u2.1).2 \cap (u2 \oplus_R u1.1).2)$$

z

$fun\ \_ \vee_{\boldsymbol{R}} \_$

z

$\_ \vee_{\boldsymbol{R}} \_ : REL\_PREDICATE \times REL\_PREDICATE \rightarrow REL\_PREDICATE$

$$\forall\ u1,u2{:}REL\_PREDICATE \bullet u1 \vee_R u2 = (u1.1 \cup u2.1, (u1 \oplus_R u2.1).2 \cup (u2 \oplus_R u1.1).2)$$

z

$\mathit{fun}\ \_\ \boldsymbol{\Rightarrow_R}\ \_$

z

$\_\ \boldsymbol{\Rightarrow_R}\ \_ : \mathit{REL\_PREDICATE} \times \mathit{REL\_PREDICATE} \rightarrow \mathit{REL\_PREDICATE}$

$\forall\ u1,u2{:}\mathit{REL\_PREDICATE} \bullet u1 \Rightarrow_R u2 = (\neg_R\ u1) \vee_R u2$

z

$\mathit{fun}\ \_\ \boldsymbol{\Leftrightarrow_R}\ \_$

z

$\_\ \boldsymbol{\Leftrightarrow_R}\ \_ : \mathit{REL\_PREDICATE} \times \mathit{REL\_PREDICATE} \rightarrow \mathit{REL\_PREDICATE}$

$\forall\ u1,u2{:}\mathit{REL\_PREDICATE} \bullet$

$\quad u1 \Leftrightarrow_R u2 = (u1 \Rightarrow_R u2) \wedge_R (u2 \Rightarrow_R u1)$

z

$\mathit{fun}\ \_\ \boldsymbol{\lhd_R}\ \_\ \boldsymbol{\rhd_R}\ \_$

z

$\_\ \boldsymbol{\lhd_R}\ \_\ \boldsymbol{\rhd_R}\ \_ : \mathit{WF\_Cond}_R \rightarrow \mathit{REL\_PREDICATE}$

$\forall\ u1\_b\_u2{:}\ \mathit{WF\_Cond}_R$

$\quad \bullet\ u1\_b\_u2.1 \lhd_R u1\_b\_u2.2 \rhd_R u1\_b\_u2.3 =$

$\qquad (u1\_b\_u2.2 \wedge_R u1\_b\_u2.1)$

$\qquad \vee_R ((\neg_R\ u1\_b\_u2.2) \wedge_R u1\_b\_u2.3)$

z

$\mathit{fun}\ \_\ \boldsymbol{;_R}\ \_$

z

$\_\ \boldsymbol{;_R}\ \_ : \mathit{WF\_Semi}_R \rightarrow \mathit{REL\_PREDICATE}$

$\forall\ u1\_u2\colon WF\_Semi_R$

$\bullet\ u1\_u2.1\ ;_R\ u1\_u2.2\ =$

$(in\_a\ u1\_u2.1.1 \cup out\_a\ u1\_u2.2.1,$

$\{b1{:}u1\_u2.1.2;\ b2{:}u1\_u2.2.2$

$\mid (\forall n{:}dom\ b2$

$\mid n \in undashed$

$\bullet\ b2(n){=}b1\ (dash\ n))$

$\bullet\ (undashed \lhd b1) \cup (dashed \lhd b2)\})$

z

$\mathbf{\Pi_R}\colon WF\_Skip_R \rightarrow REL\_PREDICATE$

$\forall\ a{:}WF\_Skip_R$

$\bullet\ \Pi_R\ a = (a,\ \{b : BINDING$

$\mid dom\ b = a$

$\wedge\ (\forall\ n{:}a \mid n \in undashed$

$\bullet\ b(n) = b(dash(n)))\})$

z

$\boldsymbol{Assign_R} : WF\_Assign_R \rightarrow REL\_PREDICATE$

$\forall\ aa{:}WF\_Assign_R$

$\bullet$

$(\ \#aa.2 = 1$

$\wedge\ (\exists n{:}NAME \mid n = head(aa.2) \bullet$

$Assign_R(aa) =$

$=_R(aa.1,dash(n),head\ aa.3)$

$\wedge_R\ \Pi_R\ (aa.1 \setminus \{n,\ dash(n)\}))\ )$

$\vee\ (\ \#aa.2 > 1$

$\wedge\ (\exists n{:}NAME \mid n = head(aa.2) \bullet$

$Assign_R(aa) =$

$=_R(aa.1,dash(n),head\ aa.3)$

$$\wedge_R \ (Assign_R(aa.1 \setminus \{n, dash(n)\},$$
$$tail\ \ aa.2,$$
$$tail\ \ aa.3))) \ )$$

z

$fun\ \_ \boldsymbol{-_R} \_$

z

$\_ \boldsymbol{-_R} \_ : REL\_PREDICATE \times ALPHABET \rightarrow REL\_PREDICATE$

$\forall\ u{:}REL\_PREDICATE;\ a{:}ALPHABET$
$\quad \bullet\ u -_R a = (u.1 \setminus a,\ \{b{:}u.2 \bullet a \lhd b\})$

z

$\exists_{\boldsymbol{-R}}: ALPHABET \times REL\_PREDICATE \rightarrow REL\_PREDICATE$

$\forall\ a{:}ALPHABET;\ u{:}REL\_PREDICATE \bullet \exists_{-R}\ (a,\ u) = u -_R a$

z

$\forall_{\boldsymbol{-R}}: ALPHABET \times REL\_PREDICATE \rightarrow REL\_PREDICATE$

$\forall\ a{:}ALPHABET;\ u{:}REL\_PREDICATE$
$\quad \bullet\ \forall_{-R}\ (a,\ u) = \neg_R\ (\exists_{-R}(a, \neg_R\ u))$

z

$\exists_{\boldsymbol{R}}: ALPHABET \times REL\_PREDICATE \rightarrow REL\_PREDICATE$

$\forall\ a{:}ALPHABET;\ u{:}REL\_PREDICATE$
$\quad \bullet\ \exists_R\ (a,\ u) = (\exists_{-R}\ (a,\ u)) \oplus_R a$

z

$\forall_{\boldsymbol{R}}: ALPHABET \times REL\_PREDICATE \rightarrow REL\_PREDICATE$

$\forall\ a{:}ALPHABET;\ u{:}REL\_PREDICATE$
$\quad \bullet\ \forall_R\ (a,\ u) = \neg_R\ (\exists_R(a, \neg_R\ u))$

z

$\boldsymbol{/_R} : WF\_Subst_R \rightarrow REL\_PREDICATE$

$\forall\ u\_e\_n{:}WF\_Subst_R$
$\quad \bullet\ /_R\ u\_e\_n =$
$\qquad (u\_e\_n.1.1, \{b{:}BINDING \mid dom\ b = u\_e\_n.1.1$
$\qquad\quad \wedge\ b \oplus \{u\_e\_n.3 \mapsto Eval(b, u\_e\_n.2)\}$
$\qquad\quad \in u\_e\_n.1.2\ \})$

z

$fun\ \_\ \boldsymbol{intchoice_R}\ \_$

z

$\_\ \boldsymbol{intchoice_R}\ \_ : WF\_REL\_PREDICATE\_PAIR \rightarrow REL\_PREDICATE$

$\forall\ pair\_u{:}WF\_REL\_PREDICATE\_PAIR$
$\quad \bullet\ pair\_u.1\ intchoice_R\ pair\_u.2 = pair\_u.1 \vee_R pair\_u.2$

z

$fun\ \_\ \boldsymbol{conj_R}\ \_$

z

$\_\ \boldsymbol{conj_R}\ \_ : WF\_REL\_PREDICATE\_PAIR \rightarrow REL\_PREDICATE$

$\forall\ pair\_u{:}WF\_REL\_PREDICATE\_PAIR$
$\quad \bullet\ pair\_u.1\ conj_R\ pair\_u.2 = pair\_u.1 \wedge_R pair\_u.2$

z

$\boldsymbol{var_R}: WF\_Var_{R\_End\,R} \rightarrow REL\_PREDICATE$

$$\forall\ a\_n{:}WF\_Var_{R\_EndR} \bullet var_R\ a\_n = \exists\_{}_R\ (\{a\_n.2\}, \Pi_R\ a\_n.1)$$

z

$$\boldsymbol{end_R}{:}\ WF\_Var_{R\_EndR} \rightarrow REL\_PREDICATE$$

$$\forall\ a\_n{:}WF\_Var_{R\_EndR} \bullet end_R\ a\_n = \exists\_{}_R\ (\{dash\ a\_n.2\}, \Pi_R\ a\_n.1)$$

z

$$fun\ \_ +_{\boldsymbol{R}} \_$$

z

$$\_ +_{\boldsymbol{R}} \_{:}\ WF\_Extend\_rest_R \rightarrow REL\_PREDICATE$$

$$\forall\ u\_a{:}WF\_Extend\_rest_R \bullet u\_a.1 +_R u\_a.2 = u\_a.1 \wedge_R \Pi_R(u\_a.2 \cup \{n{:}u\_a.2 \bullet dash\ n\})$$

1.2.7 Refinement

z

$$fun\ \langle_{\boldsymbol{R}}\ \_\ \rangle_{\boldsymbol{R}}$$

z

$$\langle_{\boldsymbol{R}}\ \_\ \rangle_{\boldsymbol{R}} : REL\_PREDICATE \rightarrow REL\_PREDICATE$$

$$\forall\ u{:}REL\_PREDICATE \bullet \langle_R\ u\ \rangle_R = \forall\_{}_R\ (u.1, u)$$

z

$$fun\ \_ \sqsubseteq_{\boldsymbol{R}} \_$$

z

$$\_ \sqsubseteq_{\boldsymbol{R}} \_ : WF\_REL\_PREDICATE\_PAIR \rightarrow REL\_PREDICATE$$

$$\forall\ pair\_u{:}WF\_REL\_PREDICATE\_PAIR$$
$$\bullet\ pair\_u.1 \sqsubseteq_R pair\_u.2 =$$
$$\langle_R\ (pair\_u.2 \Rightarrow_R pair\_u.1)\ \rangle_R$$

1.2.8 The Complete Lattice

z

$$\boldsymbol{monotonic} : \mathbb{P}\ (REL\_PREDICATE \rightarrow REL\_PREDICATE)$$

$$monotonic = \{f{:}REL\_PREDICATE \rightarrow REL\_PREDICATE$$
$$\mid (\ \forall\ u1,u2 : REL\_PREDICATE$$
$$\bullet\ (u1 \sqsubseteq_R u2) \Rightarrow_R (f(u1) \sqsubseteq_R f(u2)) =$$
$$True_R\ \varnothing)\}$$

z

$$\boldsymbol{Bot_R}{:}\ ALPHABET \rightarrow REL\_PREDICATE$$

$$\forall\ a{:}ALPHABET \bullet Bot_R\ a = True_R\ a$$

z

$$\boldsymbol{Top_R}{:}\ ALPHABET \rightarrow REL\_PREDICATE$$

$$\forall\ a{:}ALPHABET \bullet Top_R\ a = False_R\ a$$

Greatest lower bound .

z

$$\bigcap_{\boldsymbol{R}} : WF\_Glb_{R\_LubR} \rightarrow REL\_PREDICATE$$

$$\forall\ a\_us{:}\ WF\_Glb_{R\_LubR};\ u{:}REL\_PREDICATE$$
$$\bullet\ (u \sqsubseteq_R (\bigcap_R a\_us) = True_R\ \varnothing) \Leftrightarrow$$
$$(u.1 = a\_us.1$$
$$\wedge\ (\forall u1{:}a\_us.2 \bullet (u \sqsubseteq_R u1) = True_R\ \varnothing))$$

Least upper bound .

$$
\begin{array}{l}
\bigcup_{\boldsymbol{R}} : WF\_Glb_{R\_Lub R} \rightarrow REL\_PREDICATE \\
\hline
\forall\ a\_us : WF\_Glb_{R\_Lub R};\ u : REL\_PREDICATE \\
\quad \bullet\ ((\bigcup_R\ a\_us \sqsubseteq_R u) = True_R\ \varnothing) \Leftrightarrow \\
\qquad (u.1 = a\_us.1 \\
\qquad \wedge\ (\forall u1 : a\_us.2 \bullet (u1 \sqsubseteq_R u) = True_R\ \varnothing))
\end{array}
$$

Recursion .

$$
\begin{array}{l}
\boldsymbol{REL\_FUNCTION} \mathrel{\widehat=} \\
\quad \{f : REL\_PREDICATE \nrightarrow REL\_PREDICATE \\
\qquad \mid (\exists a : ALPHABET \bullet \\
\qquad\quad (\forall u\_dom : dom\ f;\ u\_ran : ran\ f \\
\qquad\quad \bullet\ a = u\_dom.1 = u\_ran.1))\}
\end{array}
$$

$$
\begin{array}{l}
\boldsymbol{\mu_R} : REL\_FUNCTION \rightarrow REL\_PREDICATE \\
\hline
\forall\ f : REL\_FUNCTION \\
\quad \bullet\ (\exists\ a : ALPHABET \\
\qquad \mid (\forall u\_dom : dom\ f \bullet a = u\_dom.1) \\
\qquad \bullet\ \mu_R\ f = \bigcap_R(a, \{u : REL\_PREDICATE \\
\qquad\qquad \mid a = u.1 \\
\qquad\qquad \wedge\ f(u) \sqsubseteq_R u = True_R\ \varnothing\}))
\end{array}
$$

In order to get a simpler definition of the greatest fixed point, we make the following calculation.

$$
\begin{array}{l}
\boldsymbol{\nu_R} : REL\_FUNCTION \rightarrow REL\_PREDICATE \\
\hline
\end{array}
$$

$$
\begin{array}{l}
\forall\ f\colon REL\_FUNCTION \\
\qquad \bullet\ (\exists\ a{:}ALPHABET \\
\qquad\qquad \mid (\forall u\_dom{:}dom\ f\ \bullet\ a = u\_dom.1) \\
\qquad\qquad \bullet\ \nu_R\ f = \bigcup_R(a,\{u{:}REL\_PREDICATE \\
\qquad\qquad\qquad\qquad \mid a = u.1 \\
\qquad\qquad\qquad\qquad \wedge\ u \sqsubseteq_R f(u) = True_R\ \varnothing\}))
\end{array}
$$

z

$$
\boldsymbol{varT_R}\colon WF\_VarT_{R\_EndTR} \to REL\_PREDICATE
$$

$$
\begin{array}{l}
\forall\ a\_n\_t{:}WF\_VarT_{R\_EndTR} \\
\qquad \bullet\ varT_R\ a\_n\_t = \bigcap_R(a\_n\_t.1 \setminus \{a\_n\_t.2\}, \\
\qquad\qquad\qquad\qquad \{v{:}VALUE \\
\qquad\qquad\qquad\qquad \mid v \in ((Set^{\sim})a\_n\_t.3) \\
\qquad\qquad\qquad\qquad \bullet\ var_R\ (a\_n\_t.1, a\_n\_t.2)\ ;_R \\
\qquad\qquad\qquad\qquad Assign_R(a\_n\_t.1, \\
\qquad\qquad\qquad\qquad\qquad \langle a\_n\_t.2\rangle, \\
\qquad\qquad\qquad\qquad\qquad \langle Val(v)\rangle)\ \})
\end{array}
$$

z

$$
\boldsymbol{endT_R}\colon WF\_VarT_{R\_EndTR} \to REL\_PREDICATE
$$

$$
\begin{array}{l}
\forall\ a\_n\_t{:}WF\_VarT_{R\_EndTR} \\
\qquad \bullet\ endT_R\ a\_n\_t = \bigcap_R(a\_n\_t.1 \setminus \{dash\ (a\_n\_t.2)\}, \\
\qquad\qquad\qquad\qquad \{v{:}VALUE \\
\qquad\qquad\qquad\qquad \mid v \in ((Set^{\sim})a\_n\_t.3) \\
\qquad\qquad\qquad\qquad \bullet\ Assign_R(a\_n\_t.1, \langle a\_n\_t.2\rangle, \\
\qquad\qquad\qquad\qquad\qquad \langle Val(v)\rangle)\ ;_R \\
\qquad\qquad\qquad\qquad\quad end_R\ (a\_n\_t.1, a\_n\_t.2)\})
\end{array}
$$

2 UTP Theory for the Observational Variable *okay*

2.1 Creating the Theory

SML

```
open_theory "utp−rel";
force_delete_theory "utp−okay" handle Fail _ => ();
new_theory "utp−okay";
open_theory "utp−okay";
set_flags[("z_type_check_only",false),("z_use_axioms",true),
        ("standard_z_paras",false),("standard_z_terms",false)];
```

2.2 Definitions

Z

$$\textbf{okay} : NAME$$

$$okay \in undashed$$

Z

$$(\forall b{:}BINDING \mid okay \in dom\ b \bullet b\ okay \in BOOL\_VAL)$$
$$\land\ (\forall b{:}BINDING \mid dash\ okay \in dom\ b \bullet b\ (dash\ okay) \in BOOL\_VAL)$$

Z

$$\textbf{ALPHABET\_OKAY} \mathrel{\widehat{=}} \{okay,\ dash\ okay\}$$

Z

$$\textbf{unrestOKAY},\ \textbf{unrestOKAY}' : REL\_PREDICATE \to \mathbb{B}$$

$$\forall\ r{:}REL\_PREDICATE \bullet$$
$$\quad unrestOKAY(r) = unrestTypedVar(r,okay,BOOL\_VAL)$$
$$\quad \land\ unrestOKAY'(r) = unrestTypedVar(r,dash\ okay,BOOL\_VAL)$$

z

$$\textbf{\textit{OKAY}} : REL\_PREDICATE$$

$$OKAY = =_R(ALPHABET\_OKAY, okay, Val(Bool(true)))$$

z

$$\textbf{\textit{OKAY}}' : REL\_PREDICATE$$

$$OKAY' = =_R(ALPHABET\_OKAY, dash\ okay, Val(Bool(true)))$$

2.2.1 Substitutions

z

$$fun\ \_\ \sigma_f$$

z

$$\_\ \boldsymbol{\sigma_f} : REL\_PREDICATE \nrightarrow REL\_PREDICATE$$

$$\forall\ d{:}REL\_PREDICATE \\ \quad \mid dash\ okay \in d.1 \\ \quad \bullet\ d\ \sigma_f = /_R(d, Val(Bool(false)),\ dash\ okay)$$

z

$$fun\ \_\ \sigma_t$$

z

$$\_\ \boldsymbol{\sigma_t} : REL\_PREDICATE \rightarrow REL\_PREDICATE$$

$$\forall\ d{:}REL\_PREDICATE \\ \quad \mid dash\ okay \in d.1 \\ \quad \bullet\ d\ \sigma_t = /_R(d, Val(Bool(true)),\ dash\ okay)$$

3 UTP Designs Theory

3.1 Creating the Theory

SML

```
open_theory "utp−okay";
force_delete_theory "utp−des" handle Fail _ => ();
new_theory "utp−des";
open_theory "utp−des";
set_flags[("z_type_check_only",false),("z_use_axioms",true),
        ("standard_z_paras",false),("standard_z_terms",false)];
(* Setting PP to accept the refinement symbol *)
val _ =
        ReaderWriterSupport.PrettyNames.add_new_symbols
                [(["refinedby"],
                Value "⊑",
                ReaderWriterSupport.PrettyNames.Simple)]
        handle Fail _ => ()
;
```

3.2 Definitions

Z

$$\boldsymbol{ALPHABET\_DES} \mathrel{\widehat=} \{a{:}ALPHABET \mid ALPHABET\_OKAY \subseteq a\}$$

Z

$$\boldsymbol{DES\_PREDICATE} \mathrel{\widehat=} \{u{:}REL\_PREDICATE \mid u.1 \in ALPHABET\_DES\}$$

3.2.1 Syntactic Restrictions

Z

$$\boldsymbol{WF\_DES\_PREDICATE\_PAIR} \mathrel{\widehat=} \{d1,d2{:}DES\_PREDICATE \mid d1.1 = d2.1\}$$

Z

$$\boldsymbol{WF\_DESIGN\_PAIR} \mathrel{\widehat=} \{d1,d2{:}WF\_DES\_PREDICATE\_PAIR$$

$$| \ d1.1.1 = d2.1.1\}$$

z

$$\boldsymbol{WF\_Assign_D} \mathrel{\widehat=} \{aa{:}WF\_Assign_R \mid aa.1 \in ALPHABET\_DES\}$$

z

$$\boldsymbol{WF\_Skip_D} \mathrel{\widehat=} \{a{:}ALPHABET\_DES \mid a \in WF\_Skip_R\}$$

z

$$\begin{array}{l}
\boldsymbol{DES_FUNCTION} \mathrel{\widehat=} \\
\quad \{f{:}WF_DES_PREDICATE_PAIR \rightarrow\!\!\!\!\!\!+ \ DES_PREDICATE \\
\qquad \mid (\exists a{:}ALPHABET \bullet \\
\qquad\quad (\forall pair{:}dom\ f;\ u_ran{:}ran\ f \\
\qquad\quad \bullet\ a = pair.1.1 = u_ran.1))\}
\end{array}$$

3.2.2 Designs Constructs

z

$$fun\ \_\ \vdash_{\boldsymbol{D}}\ \_$$

z

$$\begin{array}{l}
_\ \vdash_{\boldsymbol{D}}\ _{:}\ WF_DES_PREDICATE_PAIR \rightarrow REL_PREDICATE \\
\hline
\forall\ d{:}WF_DES_PREDICATE_PAIR \\
\quad \bullet\ d.1 \vdash_D d.2 = \\
\qquad (=_R(d.1.1, okay, Val(Bool(true))) \\
\qquad\quad \wedge_R\ d.1) \Rightarrow_R \\
\qquad (=_R(d.1.1, dash(okay), Val(Bool(true))) \\
\qquad\quad \wedge_R\ d.2)
\end{array}$$

z

$$\boldsymbol{DESIGN} \mathrel{\widehat=} ran\ (\ \_\ \vdash_D\ \_)$$

z

$$\boldsymbol{\Pi_D}{:}\ WF\_Skip_D \rightarrow REL\_PREDICATE$$

$$\forall\ a{:}WF\_Skip_D \bullet \Pi_D\ a = True_R\ a \vdash_D (\Pi_R\ a)$$

z

$$\boldsymbol{Assign_D} : WF\_Assign_D \to REL\_PREDICATE$$

$$\forall\ aa{:}WF\_Assign_D \bullet Assign_D(aa) = True_R\ aa.1 \vdash_D (Assign_R(aa))$$

z

$$\boldsymbol{Top_D} : ALPHABET\_DES \to DES\_PREDICATE$$

$$\forall\ a{:}ALPHABET\_DES \bullet Top_D(a) = {=_R}(a, okay, Val(Bool(false)))$$

z

$$\boldsymbol{Bot_D} : ALPHABET\_DES \to DES\_PREDICATE$$

$$\forall\ a{:}ALPHABET\_DES \bullet Bot_D(a) = True_R\ a$$

3.3 Healthiness Conditions

z

$$\boldsymbol{H1} : REL\_PREDICATE \to REL\_PREDICATE$$

$$\forall\ d{:}REL\_PREDICATE \bullet H1\ d = ({=_R}(\{okay\}, okay, Val(Bool(true)))) \Rightarrow_R d$$

z

$$\boldsymbol{H1\_healthy} : \mathbb{P}\ REL\_PREDICATE$$

$$H1\_healthy = \{d{:}REL\_PREDICATE \mid H1\ d = d\}$$

z

$$\boldsymbol{H2\_healthy} : \mathbb{P}\ REL\_PREDICATE$$

$$\begin{array}{l}
H2_healthy = \\
\quad \{d{:}REL_PREDICATE \\
\quad \mid dash\ okay \in d.1\ \wedge \\
\quad \langle_R\ (/_R\ (d, Val(Bool(false)), dash\ okay)) \\
\qquad \Rightarrow_R\ (/_R\ (d, Val(Bool(true)), dash\ okay))\ \rangle_R \\
\qquad = True_R\ \varnothing\}
\end{array}$$

z

$$\boldsymbol{J} : ALPHABET \rightarrowtail\!\!\!\!\!\leftarrow DES\_PREDICATE$$

$$\begin{array}{l}
\forall\ a'{:}ALPHABET \\
\quad \mid a' \subseteq dashed \wedge dash\ okay \in a' \\
\quad \bullet (\exists a{:}ALPHABET \\
\qquad \mid a \subseteq undashed \\
\qquad \wedge\ a' = dash\ (\!|a|\!) \\
\qquad \bullet\ J\ a' = (\ (=_R(a \cup a', okay, Val(Bool(true)))) \Rightarrow_R \\
\qquad\qquad (=_R(a \cup a', dash\ okay, \\
\qquad\qquad\qquad Val(Bool(true))))\ ) \\
\qquad\qquad \wedge_R\ (\Pi_R\ ((a \cup a') \setminus\ ALPHABET_OKAY))\ )
\end{array}$$

z

$$\boldsymbol{H2} : REL\_PREDICATE \rightarrowtail\!\!\!\!\!\leftarrow REL\_PREDICATE$$

$$\begin{array}{l}
\forall\ d{:}REL_PREDICATE \\
\quad \mid dash\ okay \in d.1 \\
\quad \bullet\ H2\ d = (d\ ;_R\ (J\ (out_a\ d.1)))
\end{array}$$

z

$$\boldsymbol{H2\_J\_healthy} : \mathbb{P}\ REL\_PREDICATE$$

$$H2\_J\_healthy = \{d{:}REL\_PREDICATE \mid dash\ okay \in d.1 \land H2\ d = d\}$$

z

$$\boldsymbol{H3} : REL\_PREDICATE \rightarrow REL\_PREDICATE$$

$$\begin{array}{l}
\forall\ d{:}REL_PREDICATE;\ a{:}ALPHABET \\
\qquad \mid a \in WF_Skip_R \\
\qquad \land\ (d,(\Pi_R\ a)) \in WF_Semi_R \\
\qquad \bullet\ H3\ d = (d\ ;_R\ (\Pi_R\ a))
\end{array}$$

z

$$\boldsymbol{H3\_healthy} : \mathbb{P}\ REL\_PREDICATE$$

$$H3\_healthy = \{d{:}REL\_PREDICATE \mid H3\ d = d\}$$

z

$$\boldsymbol{H4\_healthy} : \mathbb{P}\ REL\_PREDICATE$$

$$\begin{array}{l}
H4_healthy = \\
\qquad \{d{:}REL_PREDICATE \mid \\
\qquad\qquad (\forall a{:}ALPHABET \mid (d,True_R\ a) \in WF_Semi_R \\
\qquad\qquad\qquad\qquad \bullet\ True_R\ a\ ;_R\ d = True_R\ a)\}
\end{array}$$

4 UTP Theory for the Observational Variables $wait$, $trace$, and ref

4.1 Creating the Theory

SML

```
open_theory "utp−rel";
force_delete_theory "utp−wtr" handle Fail _ => ();
new_theory "utp−wtr";
open_theory "utp−wtr";
set_flags[("z_type_check_only",false),("z_use_axioms",true),
        ("standard_z_paras",false),("standard_z_terms",false)];
```

4.2 Definitions

Z

$$\begin{array}{|l} \textbf{wait} : NAME \\ \hline wait \in undashed \end{array}$$

Z

$$(\forall b{:}BINDING \mid wait \in \mathrm{dom}\ b \bullet b\ wait \in BOOL\_VAL)$$
$$\land\ (\forall b{:}BINDING \mid dash\ wait \in \mathrm{dom}\ b \bullet b\ (dash\ wait) \in BOOL\_VAL)$$

Z

$$\textbf{ALPHABET\_WAIT} \mathrel{\widehat=} \{wait,\ dash\ wait\}$$

Z

$$\begin{array}{|l} \textbf{WAIT} : REL\_PREDICATE \\ \hline WAIT = \ =_R(\{wait\}, wait, Val(Bool(true))) \end{array}$$

Z

$$\textbf{WAIT'} : REL\_PREDICATE$$

$WAIT' = =_R(\{dash\ wait\}, dash\ wait, Val(Bool(true)))$

z

$\boldsymbol{tr} : NAME$

$tr \in undashed$

z

$(\forall b{:}BINDING \mid tr \in dom\ b \bullet b\ tr \in SEQ\_EVENT\_VAL)$
$\land\ (\forall b{:}BINDING \mid dash\ tr \in dom\ b \bullet b\ (dash\ tr) \in SEQ\_EVENT\_VAL)$

z

$\boldsymbol{ALPHABET\_TR} \mathrel{\widehat{=}} \{tr, dash\ tr\}$

z

$\boldsymbol{ref} : NAME$

$ref \in undashed$

z

$(\forall b{:}BINDING \mid ref \in dom\ b \bullet b\ ref \in SET\_EVENT\_VAL)$
$\land\ (\forall b{:}BINDING \mid dash\ ref \in dom\ b \bullet b\ (dash\ ref) \in SET\_EVENT\_VAL)$

z

$\boldsymbol{ALPHABET\_REF} \mathrel{\widehat{=}} \{ref, dash\ ref\}$

z

$\boldsymbol{unrestWAIT, unrestWAIT'} : REL\_PREDICATE \to \mathbb{B}$

$\forall\ r{:}REL\_PREDICATE \bullet$
$\quad unrestWAIT(r) = unrestTypedVar(r, wait, BOOL\_VAL)$
$\quad \land\ unrestWAIT'(r) = unrestTypedVar(r, dash\ wait, BOOL\_VAL)$

z

$$\boldsymbol{unrestTR}, \boldsymbol{unrestTR'} : REL\_PREDICATE \to \mathbb{B}$$

$$\forall\ r{:}REL\_PREDICATE \bullet$$
$$\quad unrestTR(r) = unrestTypedVar(r, tr, SEQ\_EVENT\_VAL)$$
$$\quad \land\ unrestTR'(r) = unrestTypedVar(r, dash\ tr, SEQ\_EVENT\_VAL)$$

z

$$\boldsymbol{unrestREF}, \boldsymbol{unrestREF'} : REL\_PREDICATE \to \mathbb{B}$$

$$\forall\ r{:}REL\_PREDICATE \bullet$$
$$\quad unrestREF(r) = unrestTypedVar(r, ref, SET\_EVENT\_VAL)$$
$$\quad \land\ unrestREF'(r) =$$
$$\qquad unrestTypedVar(r, dash\ ref, SET\_EVENT\_VAL)$$

z

$$wait \neq tr \land wait \neq ref$$

z

$$tr \neq wait \land tr \neq ref$$

z

$$ref \neq tr \land ref \neq wait$$

4.3 Substitution

z

$$fun\ \_\ \omega_f$$

z

$$\_\ \boldsymbol{\omega_f} : REL\_PREDICATE \nrightarrow REL\_PREDICATE$$

$$\forall\ r{:}REL\_PREDICATE$$
$$\quad \mid wait \in r.1$$

$\bullet\ r\ \omega_f\ = /_R(r, Val(Bool(false)),\ wait)$

z

$fun\ \_\ \omega_t$

z

$\_\ \boldsymbol{\omega_t} : REL\_PREDICATE \nrightarrow REL\_PREDICATE$

$\forall\ r{:}REL\_PREDICATE$

$\quad |\ wait \in r.1$

$\quad \bullet\ r\ \omega_t\ = /_R(r, Val(Bool(true)),\ wait)$

SML

```
open_theory "utp−okay";
force_delete_theory "utp−rea" handle Fail _ => ();
new_theory "utp−rea";
open_theory "utp−rea";
new_parent "utp−wtr";
set_flags[("z_type_check_only",false),("z_use_axioms",true),
        ("standard_z_paras",false),("standard_z_terms",false)];
```

4.4 Definitions

Z

$$\boldsymbol{ALPHABET\_OWTR} \mathrel{\widehat=} ALPHABET\_OKAY \cup ALPHABET\_WAIT \cup ALPHABET\_TR \cup ALPHABET\_REF$$

Z

$$\boldsymbol{ALPHABET\_REA} \mathrel{\widehat=} \{a{:}ALPHABET \mid ALPHABET\_OWTR \subseteq a\}$$

Z

$$\boldsymbol{REA\_PREDICATE} \mathrel{\widehat=} \{d{:}REL\_PREDICATE \mid d.1 \in ALPHABET\_REA\}$$

Z

$$okay \neq wait \land okay \neq tr \land wait \neq ref$$

4.4.1 Syntactic Restrictions

Z

$$\boldsymbol{WF\_Skip_{REA}} \mathrel{\widehat=} \{a{:}ALPHABET\_REA \mid a \in homogeneous\}$$

4.4.2 Reactive Constructs

Z

$$\boldsymbol{\Pi_{REA}}\colon WF\_Skip_{REA} \rightarrow REA\_PREDICATE$$

$$
\begin{array}{l}
\forall\ a{:}\mathit{WF\_Skip}_{REA} \\
\quad \bullet\ \mathit{\Pi}_{REA}\ a = \\
\qquad (\ (=_R(a, okay, Val(Bool(false)))) \\
\qquad\quad \wedge_R\ (=_{+R}(ALPHABET\_OWTR, \\
\qquad\qquad Rel((\_ \leq_R \_), Var(tr), \\
\qquad\qquad\quad Var(dash\ tr)), \\
\qquad\qquad Val(Bool(true))))\ ) \\
\qquad \vee_R\ (\ (=_R(a, dash\ okay, Val(Bool(true)))) \\
\qquad\quad \wedge_R\ (=_R(a, dash\ tr, Var(tr))) \\
\qquad\quad \wedge_R\ (=_R(a, dash\ wait, Var(wait))) \\
\qquad\quad \wedge_R\ (=_R(a, dash\ ref, Var(ref)))\ )
\end{array}
$$

4.5 Healthiness Conditions

z

$$
\begin{array}{l}
\boldsymbol{R1} : REL\_PREDICATE \rightarrow REL\_PREDICATE \\
\hline
\forall r{:}REL\_PREDICATE \\
\quad \bullet\ R1\ r = r \wedge_R (=_{+R}(ALPHABET\_OWTR, \\
\qquad\qquad Rel((\_ \leq_R \_), Var(tr), \\
\qquad\qquad\quad Var(dash\ tr)), \\
\qquad\qquad Val(Bool(true))))
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{R1\_healthy} : \mathbb{P}\ REL\_PREDICATE \\
\hline
R1\_healthy = \{r{:}REL\_PREDICATE \mid r = R1\ r\}
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{R2} : REL\_PREDICATE \rightarrow\!\!\!\!\!+\ REL\_PREDICATE \\
\hline
\forall r{:}REL\_PREDICATE \\
\quad \mid ALPHABET\_OWTR \subseteq r.1
\end{array}
$$

$$
\begin{array}{l}
\quad \bullet\ R2\ r = \quad /_R\ ((/_R(r, Val(Seq(\langle\rangle)), tr)), \\
\qquad\qquad\qquad Fun_2((\_\ SeqDif_R\ \_), \\
\qquad\qquad\qquad\qquad Var(dash\ tr), Var(tr)), dash\ tr)
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{R2\_healthy} : \mathbb{P}\ REL\_PREDICATE \\
\hline
R2\_healthy = \{r{:}REL\_PREDICATE \mid r = R2\ r\}
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{R3} : REA\_PREDICATE \rightarrow REA\_PREDICATE \\
\hline
\forall r{:}REA\_PREDICATE \\
\qquad \mid r.1 \in WF\_Skip_{REA} \\
\qquad \bullet\ R3\ r = \quad (\Pi_{REA}\ r.1) \\
\qquad\qquad\qquad \lhd_R\ (=_R(\{wait\}, wait, Val(Bool(true)))) \\
\qquad\qquad\qquad \rhd_R\ r
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{R3\_healthy} : \mathbb{P}\ REA\_PREDICATE \\
\hline
R3\_healthy = \{r{:}REA\_PREDICATE \mid r.1 \in WF\_Skip_{REA} \wedge r = R3\ r\}
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{R} : REA\_PREDICATE \rightarrow REA\_PREDICATE \\
\hline
\forall r{:}REA\_PREDICATE \mid r.1 \in WF\_Skip_{REA} \bullet R\ r = R1(R2(R3(r)))
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{R\_healthy} : \mathbb{P}\ REA\_PREDICATE \\
\hline
R\_healthy = \{r{:}REA\_PREDICATE \mid r.1 \in WF\_Skip_{REA} \wedge r = R\ r\}
\end{array}
$$

z

$$
\boldsymbol{REA\_PROCESS} \mathrel{\widehat{=}} \{r{:}REA\_PREDICATE \mid r \in R\_healthy\}
$$

5 UTP CSP Theory

5.1 Creating the Theory

SML

```
open_theory "utp−des";
force_delete_theory "utp−csp" handle Fail _ => ();
new_theory "utp−csp";
open_theory "utp−csp";
new_parent "utp−rea";
set_flags[("z_type_check_only",false),("z_use_axioms",true),
        ("standard_z_paras",false),("standard_z_terms",false)];

(* Setting PP to accept the refinement symbol *)
val _ =
        ReaderWriterSupport.PrettyNames.add_new_symbols
                [(["refinedby"],
                Value "⊑",
                ReaderWriterSupport.PrettyNames.Simple)]
        handle Fail _ => ()
;
(* Setting PP to accept the equivalence symbol *)
val _ =
        ReaderWriterSupport.PrettyNames.add_new_symbols
                [(["equivalentto"],
                Value "≡",
                ReaderWriterSupport.PrettyNames.Simple)]
        handle Fail _ => ()
;
```

5.2 Healthiness Conditions

Z

$$\boldsymbol{unrestALPHABET\_CSP} : REL\_PREDICATE \rightarrow \mathbb{B}$$

$$\forall\ r{:}REL\_PREDICATE \bullet$$
$$\quad unrestALPHABET\_CSP(r) \Leftrightarrow$$
$$\qquad (unrestOKAY(r) \land unrestWAIT(r)$$
$$\qquad \land\ unrestTR(r) \land unrestREF(r))$$

z

$$\boldsymbol{unrestALPHABET\_CSP'} : REL\_PREDICATE \rightarrow \mathbb{B}$$

$$\forall\ r{:}REL\_PREDICATE \bullet$$
$$\quad unrestALPHABET\_CSP'(r) \Leftrightarrow$$
$$\qquad (unrestOKAY'(r) \land unrestWAIT'(r)$$
$$\qquad \land\ unrestTR'(r) \land unrestREF'(r))$$

z

$$\boldsymbol{VAR\_NAME} \mathrel{\widehat{=}} \{n{:}NAME \mid n \notin ALPHABET\_OWTR \land n \in undashed\}$$

z

$$\boldsymbol{CSP1} : REL\_PREDICATE \rightarrow REL\_PREDICATE$$

$$\forall\ r{:}REL\_PREDICATE \bullet$$
$$\quad CSP1\ r = r \lor_R ($$
$$\qquad (=_R(ALPHABET\_OWTR, okay, Val(Bool(false))))$$
$$\qquad\quad \land_R (=_{+R}(ALPHABET\_OWTR,$$
$$\qquad\qquad Rel((\_ \leq_R \_), Var(tr),$$
$$\qquad\qquad\quad Var(dash\ tr)),$$
$$\qquad\qquad Val(Bool(true))))\ )$$

z

$$\boldsymbol{CSP1\_healthy} : \mathbb{P}\ REL\_PREDICATE$$

$$CSP1\_healthy = \{r{:}REL\_PREDICATE \mid r = CSP1\ r\}$$

z

$$\boldsymbol{CSP2} : REL\_PREDICATE \pfun REL\_PREDICATE$$

$$\forall r{:}REL\_PREDICATE \mid \{dash(okay),dash(wait),dash(tr),dash(ref)\} \subseteq r.1 \bullet CSP2\ r = r\ ;_R\ J(out\_a\ r.1)$$

z

$$\boldsymbol{CSP2\_healthy} : \mathbb{P}\ REL\_PREDICATE$$

$$CSP2\_healthy = \{r{:}REL\_PREDICATE \mid \{dash(okay),dash(wait),dash(tr),dash(ref)\} \subseteq r.1 \land r = CSP2\ r\}$$

z

$$\boldsymbol{CSP\_PROCESS} \mathrel{\widehat=} \{p{:}REA\_PROCESS \mid ALPHABET\_OWTR \subseteq p.1 \land p \in CSP1\_healthy \land p \in CSP2\_healthy\}$$

5.3 Definitions

5.3.1 Syntactic Restrictions

z

$$\boldsymbol{WF\_CSP\_PROCESS\_PAIR} \mathrel{\widehat=} \{p1,p2{:}CSP\_PROCESS \mid p1.1 = p2.1\}$$

z

$$\boldsymbol{WF\_PREFIXING} \mathrel{\widehat=} \{a{:}ALPHABET\_REA;\ n{:}VAR\_NAME;\ e{:}EXPRESSION \mid a \in WF\_Skip_{REA} \land FV\ e \subseteq a\}$$

5.3.2 CSP Constructs

z

$$\boldsymbol{STOP} : WF\_Skip_{REA} \to CSP\_PROCESS$$

```
├──────────────────────────────
│ ∀ a:WF_Skip_REA •
│       STOP a = R(Assign_R(a,⟨wait⟩,⟨Val(Bool(true))⟩))
```

SML

```
│val CSP_STOP_design_thm =
│       new_axiom (["CSP_STOP_design_thm"],
│              ⓩ∀ a:ALPHABET_REA
│               | a ∈ WF_Skip_REA
│               • STOP a
│               = R (True_R a
│                     ⊢_D ((=_R(a,dash tr,
│                                        Var(tr)))
│                           ∧_R (=_R(a,
│                                 dash wait,
│                                 Val(Bool(true))))))⌝);
│
```

Z

```
│ SKIP : WF_Skip_REA → CSP_PROCESS
├──────────────────────────────
│ ∀ a:WF_Skip_REA •
│       SKIP a = R (∃_R({ref},Π_REA a))
```

SML

```
│val CSP_SKIP_design_thm =
│       new_axiom (["CSP_SKIP_design_thm"],
│              ⓩ∀ a:ALPHABET_REA
│               | a ∈ WF_Skip_REA
│               • SKIP a
│              = R(True_R a
│                     ⊢_D ((=_R(a, dash tr,
│                                        Var(tr)))
```

```
                                ∧_R (=_R(a,
                                     dash wait,
                                     Val(Bool(false))))))              ⌝);
```

Z

$$\textbf{CHAOS} : WF\_Skip_{REA} \rightarrow CSP\_PROCESS$$

$$\forall\ a{:}WF\_Skip_{REA} \bullet CHAOS\ a = R(True_R\ a)$$

SML

```
val CSP_CHAOS_design_thm =
        new_axiom (["CSP_CHAOS_design_thm"],
                ⌜∀ a:ALPHABET_REA
                 | a ∈ WF_Skip_REA
                 • CHAOS a = R(False_R a ⊢_D
                                True_R a)⌝);
```

Z

$$fun\ \_\ \boxtimes_{\boldsymbol{CSP}}\ \_$$

Z

$$\_\ \boxtimes_{\boldsymbol{CSP}}\ \_ : WF\_CSP\_PROCESS\_PAIR \rightarrow CSP\_PROCESS$$

$$\forall pp{:}WF\_CSP\_PROCESS\_PAIR \bullet pp.1 \boxtimes_{CSP} pp.2 = CSP2((pp.1 \wedge_R pp.2) \lhd_R STOP\ (pp.1).1 \rhd_R (pp.1 \vee_R pp.2))$$

SML

```
val CSP_⊠_CSP_design_thm_2 =
        new_axiom (["CSP_⊠_CSP_design_thm_2"],
                ⌜ ∀ p1,p2:CSP_PROCESS
```

$| \ (p1,p2) \in WF\_CSP\_PROCESS\_PAIR$
$\bullet \ p1 \boxtimes_{CSP} p2$
$= R($
$(\neg_R \ (p1 \ \sigma_f \ \omega_f) \wedge_R \neg_R \ (p2 \ \sigma_f \ \omega_f))$
$\vdash_D$
$(\ ((p1 \ \sigma_t \ \omega_f) \wedge_R (p2 \ \sigma_t \ \omega_f))$
$\lhd_R \ ((=_{+R}(p1.1, Var(dash \ tr), Var(tr)))$
$\quad \wedge_R \ (=_R \ (p1.1, dash \ wait, Val(Bool(true)))))$
$\rhd_R$
$((p1 \ \sigma_t \ \omega_f) \vee_R (p2 \ \sigma_t \ \omega_f)) \ )$
$)^\urcorner);$

z

$\mathbf{\Phi}$: $CSP\_PROCESS \rightarrow CSP\_PROCESS$

$\forall \ p{:}CSP\_PROCESS$
$\bullet \ \Phi \ p = R(\ p \wedge_R (((=_R(ALPHABET\_OWTR, dash \ tr, \ Var(tr)))$
$\qquad \wedge_R \ (=_R(ALPHABET\_OWTR, dash \ wait,$
$\qquad\qquad Val(Bool(true)))))$
$\qquad \vee_R \ (=_{+R}(ALPHABET\_OWTR,$
$\qquad\qquad Rel((\_ <_R \_), Var(tr),$
$\qquad\qquad\quad Var(dash \ tr)),$
$\qquad\qquad Val(Bool(true))))) \ )$

z

fun ***do_A*** _

z

do_A _ : $WF\_PREFIXING \rightarrow CSP\_PROCESS$

$\forall a\_n\_e{:}WF\_PREFIXING$
$\bullet \ do\_A \ a\_n\_e = \Phi(\ ((=_R(a\_n\_e.1, dash \ tr, \ Var(tr)))$
$\qquad \wedge_R \ (=_{+R}(a\_n\_e.1,$

$$
\begin{array}{l}
\qquad\qquad Rel((\_ \notin_R \_),\\
\qquad\qquad\quad Fun_2(MkPair,\\
\qquad\qquad\qquad Val(Channel(a\_n\_e.2)),\ a\_n\_e.3),\\
\qquad\qquad\qquad Var(dash\ ref)),\\
\qquad\qquad\qquad Val(Bool(true)))))\\
\quad \lhd_R\\
\quad (=_R(a\_n\_e.1, dash\ wait, Val(Bool(true))))\\
\quad \rhd_R\\
\quad (=_R(a\_n\_e.1, dash\ tr,\ Fun_2((\_ \frown_R \_),\\
\qquad\qquad Var(tr),\\
\qquad\qquad Fun_1(MkSingleton,\\
\qquad\qquad Fun_2(MkPair,\\
\qquad\qquad Val(Channel(a\_n\_e.2)),\ a\_n\_e.3)\\
\qquad\qquad\qquad)))))
\end{array}
$$

z

$fun\ \_ \rightarrow_{\boldsymbol{CSP}} \_$

z

$$
\begin{array}{l}
\_ \rightarrow_{\boldsymbol{CSP}} \_ : (WF\_PREFIXING \times CSP\_PROCESS) \rightarrow\\
\qquad\qquad CSP\_PROCESS\\
\hline
\forall a\_n\_e : WF\_PREFIXING\\
\bullet\ a\_n\_e \rightarrow_{CSP} SKIP\ a\_n\_e.1 =\\
\qquad CSP2((=_R(a\_n\_e.1, dash\ okay,\ Val(Bool(true))))\\
\qquad\qquad \land_R\ do\_A(a\_n\_e))\\
\land\ (\forall\ p : CSP\_PROCESS \bullet a\_n\_e \rightarrow_{CSP} p = (a\_n\_e \rightarrow_{CSP} SKIP
\end{array}
$$

z

$fun\ \boldsymbol{do\_C}\ \_$

z

$\boldsymbol{do\_C}\ \_ : WF\_PREFIXING \rightarrow CSP\_PROCESS$

$$
\begin{array}{l}
\forall a\_n\_e{:}\,WF\_PREFIXING \\
\quad \bullet\ do\_C\ a\_n\_e = ((=_R(a\_n\_e.1, dash\ tr,\ Var(tr))) \\
\qquad \land_R\ (=_{+R}(a\_n\_e.1, \\
\qquad\quad Rel((\_ \notin_R \_), \\
\qquad\qquad Fun_2(MkPair, \\
\qquad\qquad\quad Val(Channel(a\_n\_e.2)), \\
\qquad\qquad\quad a\_n\_e.3), \\
\qquad\qquad\quad Var(dash\ ref)), \\
\qquad\qquad Val(Bool(true))))) \\
\qquad \lhd_R \\
\qquad (=_R(a\_n\_e.1, dash\ wait, Val(Bool(true)))) \\
\qquad \rhd_R \\
\qquad (=_R(a\_n\_e.1, \\
\qquad\quad dash\ tr, \\
\qquad\quad Fun_2((\_ \frown_R \_), \\
\qquad\qquad Var(tr), \\
\qquad\qquad Fun_1(MkSingleton, \\
\qquad\qquad Fun_2(MkPair, \\
\qquad\qquad Val(Channel(a\_n\_e.2)), \\
\qquad\qquad\qquad a\_n\_e.3) \\
\qquad\qquad\qquad\quad))))
\end{array}
$$

SML

```
val CSP_→CSP_design_thm =
    new_axiom (["CSP_→CSP_design_thm"],
    ⌜ ∀a_n_e:WF_PREFIXING
    • a_n_e →CSP SKIP a_n_e.1 = R( TrueR a_n_e.1
                        ⊢D do_C(a_n_e))⌝);
```

5.4 Further Healthiness Conditions

Z

$\boldsymbol{CSP3\_healthy} : \mathbb{P}\ CSP\_PROCESS$

$$CSP3\_healthy = \{r{:}CSP\_PROCESS \mid (=_R(r.1,wait,Val(Bool(false)))) \Rightarrow_R (r \equiv_R \exists_R(\{ref\},r)) = True_R\ r.1\}$$

Z

$\boldsymbol{CSP4\_healthy} : \mathbb{P}\ CSP\_PROCESS$

$$CSP4\_healthy = \{r{:}CSP\_PROCESS \mid (r,SKIP\ r.1) \in WF\_Semi_R \land r \;;_R\; SKIP\ r.1 = r\}$$

SML

6 UTP Circus Theory

6.1 Creating the Theory

SML

```
open_theory "utp-csp";
force_delete_theory "utp-circus" handle Fail _ => ();
new_theory "utp-circus";
open_theory "utp-circus";
set_flags[("z_type_check_only",false),("z_use_axioms",true),
        ("standard_z_paras",false),("standard_z_terms",false)];
(* Setting PP to accept the refinement symbol *)
val _ =
        ReaderWriterSupport.PrettyNames.add_new_symbols
                [(["refinedby"],
                Value "⊑",
                ReaderWriterSupport.PrettyNames.Simple)]
        handle Fail _ => ()
;
```

6.2 Definitions

Z

$\boldsymbol{Z\_VAR\_NAME} \mathrel{\widehat=} \{n{:}NAME \mid n \notin ALPHABET\_OWTR\}$

Z

$$\begin{aligned}\boldsymbol{VAR\_DECLS} \mathrel{\widehat=} \{&vars{:}seq\ Z\_VAR\_NAME;\ types{:}seq\ EXPRESSION\\ &\mid dom\ vars \in (\mathbb{F}\ \_) \land dom\ types \in (\mathbb{F}\ \_)\\ &\land \#(ran\ vars) = \#(ran\ types) > 0\}\end{aligned}$$

Z

$\boldsymbol{CIRCUS\_PREDICATE} : \mathbb{P}\ REA\_PREDICATE$

$$\begin{aligned}CIRCUS\_PREDICATE = \{&c : REA\_PREDICATE\\ &\mid unrestALPHABET\_CSP(c)\end{aligned}$$

$\land\ unrestALPHABET\_CSP'(c)\ \}$

z

$$\boldsymbol{CIRCUS\_CONDITION} : \mathbb{P}\ REA\_PREDICATE$$

$$\begin{aligned} CIRCUS\_CONDITION = \{ & c : REA\_PREDICATE \\ & \mid unrestALPHABET\_CSP(c) \\ & \land\ unrestALPHABET\_CSP'(c) \\ & \land\ c -_R ALPHABET\_OWTR \in REL\_CONDITION\} \end{aligned}$$

6.2.1 Syntactic Restrictions

z

$$\boldsymbol{WF\_Skip_C} \mathrel{\widehat=} \{a{:}WF\_Skip_R \mid ALPHABET\_OWTR \subseteq a\ \}$$

z

$$\boldsymbol{WF\_Guard_C} \mathrel{\widehat=} \{g{:}CIRCUS\_CONDITION;\ a{:}CSP\_PROCESS \mid g.1 = a.1\}$$

z

$$\begin{aligned} & \boldsymbol{WF\_if_{C\_fiC}} \mathrel{\widehat=} \\ & \quad \{g{:}CIRCUS\_CONDITION;\ a{:}CSP\_PROCESS \mid g.1 = a.1\} \end{aligned}$$

z

$$\boldsymbol{WF\_Semi_C} \mathrel{\widehat=} \{a1,a2{:}CSP\_PROCESS \mid (a1,a2) \in WF\_Semi_R\ \}$$

z

$$\begin{aligned} & \boldsymbol{WF\_Var_C} \mathrel{\widehat=} \\ & \quad \{n{:}VAR\_NAME;\ t{:}SET\_VAL;\ a{:}CSP\_PROCESS \\ & \quad \mid n \notin ALPHABET\_OWTR \land n \in undashed \land \{n,dash(n)\} \subseteq a.1\} \end{aligned}$$

z

$$\begin{aligned} & \boldsymbol{WF\_Assign_C} \mathrel{\widehat=} \\ & \quad \{a{:}ALPHABET;\ ns{:}seq\ VAR\_NAME;\ exps{:}seq\ EXPRESSION \\ & \quad \mid (\forall n{:}ran\ ns \bullet n \in a \land n \in undashed) \end{aligned}$$

$$\begin{array}{l}
\quad \land (\forall e{:}ran\ exps \bullet FV(e) \subseteq a \land FV(e) \subseteq undashed) \\
\quad \land \#ns = \#exps \neq 0 \\
\quad \land a \in homogeneous \\
\quad \land ALPHABET_OWTR \subseteq a\}
\end{array}$$

z

$$\begin{array}{l}
\boldsymbol{WF_SpecStatement_C} \mathrel{\widehat=} \\
\quad \{a{:}ALPHABET;\ f{:}\mathbb{F}\ VAR_NAME;\ preC{:}\ CIRCUS_CONDITION; \\
\qquad postC{:}\ CIRCUS_PREDICATE \\
\quad \mid f \subseteq a \land f \subseteq undashed \land a \in homogeneous \\
\quad \land preC.1 = postC.1 = a \\
\quad \land ALPHABET_OWTR \subseteq a\}
\end{array}$$

z

$$\begin{array}{l}
\boldsymbol{WF_Condition_C} \mathrel{\widehat=} \{a{:}ALPHABET;\ g{:}\ CIRCUS_CONDITION \\
\qquad\qquad \mid a \in homogeneous \land a = g.1\}
\end{array}$$

z

$$\begin{array}{l}
\boldsymbol{WF_SchemaExp_C} \mathrel{\widehat=} \\
\quad \{decls{:}VAR_DECLS;\ p{:}REL_PREDICATE \\
\quad \mid (p.1 \setminus ALPHABET_OWTR) = ran\ (decls.1)\}
\end{array}$$

z

$$\begin{array}{l}
\boldsymbol{WF_param_C} \mathrel{\widehat=} \\
\quad \{\ x{:}VAR_NAME;\ T{:}EXPRESSION;\ a{:}CSP_PROCESS;\ e{:}EXPRESSION \\
\quad \mid x \in a.1 \land FV(e) \subseteq a.1\}
\end{array}$$

z

$$\begin{array}{l}
\boldsymbol{WF_val_C} \mathrel{\widehat=} \\
\quad \{\ x{:}VAR_NAME;\ t{:}SET_VAL;\ a{:}CSP_PROCESS;\ e{:}EXPRESSION \\
\quad \mid x \notin FV(e) \land x \in a.1 \land FV(e) \subseteq a.1\}
\end{array}$$

z

$$\boldsymbol{WF\_res_C} \mathrel{\widehat=}$$

$\{ x{:}VAR\_NAME;\ t{:}SET\_VAL;\ a{:}CSP\_PROCESS;\ y{:}VAR\_NAME$
$\mid \{x,y\} \subseteq a.1 \}$

z

$\boldsymbol{WF\_vres_C} \mathrel{\widehat{=}}$
$\{ x{:}VAR\_NAME;\ t{:}SET\_VAL;\ a{:}CSP\_PROCESS;\ y{:}VAR\_NAME$
$\mid x \neq y \land \{x,y\} \subseteq a.1 \}$

z

$\boldsymbol{WF\_PREFIXING_C} \mathrel{\widehat{=}}$
$\{ a\_n\_e{:}WF\_PREFIXING;\ A{:}CSP\_PROCESS \mid a\_n\_e.1 = A.1 \}$

z

$\boldsymbol{WF\_PREFIXING_{CinR}} \mathrel{\widehat{=}}$
$\{a{:}ALPHABET\_REA;\ c{:}VAR\_NAME;\ x{:}VAR\_NAME;$
$p{:}CIRCUS\_CONDITION;$
$A{:}\ CSP\_PROCESS \mid (a = A.1) \land (\{x, dash(x)\} \subseteq a)\}$

6.2.2 Circus Constructs

z

$\boldsymbol{Stop} : WF\_Skip_C \rightarrow CSP\_PROCESS$

$\forall a{:}WF\_Skip_C \bullet$
$Stop\ a = R(True_R\ a \vdash_D (\ =_R(a,\ dash\ tr, Var(tr))$
$\land_R =_R(a,$
$dash\ wait,$
$Val(Bool(true)))\ ))$

z

$\boldsymbol{Skip} : WF\_Skip_C \rightarrow CSP\_PROCESS$

$\forall a{:}WF\_Skip_C \bullet$
$Skip\ a = R(True_R\ a \vdash_D (\ =_R(a,\ dash\ tr, Var(tr))$

$$\wedge_R =_R(a,\ dash\ wait,\ Val(Bool(false)))\ \wedge_R\ (\Pi_R\ (a \backslash ALPHABET\_OWTR))))$$

z

$\boldsymbol{Chaos} : WF\_Skip_C \rightarrow CSP\_PROCESS$

$\forall a{:}WF\_Skip_C \bullet Chaos\ a = R(False_R\ a \vdash_D True_R\ a)$

z

$fun\ \_\ \boldsymbol{;_C}\ \_$

z

$\_\ \boldsymbol{;_C}\ \_ : WF\_Semi_C \rightarrow CSP\_PROCESS$

$\forall\ u1\_u2{:}\ WF\_Semi_C$
$\quad \bullet\ u1\_u2.1\ ;_C\ u1\_u2.2 = u1\_u2.1\ ;_R\ u1\_u2.2$

z

$fun\ \_\ \boldsymbol{\&_C}\ \_$

z

$\_\ \boldsymbol{\&_C}\ \_ : WF\_Guard_C \rightarrow CSP\_PROCESS$

$\forall\ g{:}CIRCUS\_CONDITION;\ a{:}\ CSP\_PROCESS$
$\quad \mid (g,a) \in WF\_Guard_C$
$\quad \bullet\ g\ \&_C\ a =$
$\quad R($
$\quad (g \Rightarrow_R \neg_R\ (a\ \omega_f\ \sigma_f))$
$\quad \vdash_D$
$\quad (((g \wedge_R (a\ \omega_f\ \sigma_t)))$
$\quad\quad \vee_R\ (\ \neg_R\ g \wedge_R =_R(a.1,\ dash\ tr,\ Var(tr))$

$\wedge_R =_R(a.1, dash\ wait,$
$Val(Bool(true)))\ ))$
$)$

z

$fun\ \_ \boxtimes_{\boldsymbol{C}} \_$

z

$\_ \boxtimes_{\boldsymbol{C}} \_ : WF\_CSP\_PROCESS\_PAIR \rightarrow CSP\_PROCESS$

$\forall aa : WF\_CSP\_PROCESS\_PAIR$
$\bullet\ aa.1 \boxtimes_C aa.2 =$
$R($
$(\neg_R\ (aa.1\ \omega_f\ \sigma_f) \wedge_R \neg_R\ (aa.2\ \omega_f\ \sigma_f))$
$\vdash_D$
$(\ ((aa.1\ \omega_f\ \sigma_t) \wedge_R (aa.2\ \omega_f\ \sigma_t))$
$\lhd_R\ ((=_{+R}(aa.1.1, Var(dash\ tr), Var(tr)))$
$\wedge_R$
$(=_R\ (aa.1.1, dash\ wait, Val(Bool(true)))))$
$\rhd_R$
$((aa.1\ \omega_f\ \sigma_t) \vee_R (aa.2\ \omega_f\ \sigma_t))\ )$
$)$

z

$fun\ \_ \sqcap_{\boldsymbol{C}} \_$

z

$\_ \sqcap_{\boldsymbol{C}} \_ : WF\_CSP\_PROCESS\_PAIR \rightarrow CSP\_PROCESS$

$\forall aa : WF\_CSP\_PROCESS\_PAIR$
$\bullet\ aa.1 \sqcap_C aa.2 = aa.1 \vee_R aa.2$

z

$fun \ \_ \longrightarrow_{\boldsymbol{C}} \_$

z

$\_ \longrightarrow_{\boldsymbol{C}} \_ : WF\_PREFIXING_C \to CSP\_PROCESS$

$\forall \ a\_a : WF\_PREFIXING_C$

$\bullet \ a\_a.1 \to_C a\_a.2 = R(True_R \ (a\_a.1).1 \vdash_D (do\_C \ a\_a.1)$

$\qquad \wedge_R (\Pi_R \ ((a\_a.1).1 \setminus ALPHABET\_OWTR))) \ ;_C \ a\_a.2$

z

$fun \ \_ \longrightarrow_{\boldsymbol{CSync}} \_$

z

$\_ \longrightarrow_{\boldsymbol{CSync}} \_ : ((ALPHABET \times VAR\_NAME) \times CSP\_PROCESS)$

$\qquad \to CSP\_PROCESS$

$\forall a : ALPHABET; \ c : VAR\_NAME; \ A : CSP\_PROCESS$

$\bullet \ (a,c) \to_{CSync} A = (a,c,Val(Sync)) \to_C A$

z

$fun \ \_ \longrightarrow_{\boldsymbol{Cout}} \_$

z

$\_ \longrightarrow_{\boldsymbol{Cout}} \_ : WF\_PREFIXING_C \to CSP\_PROCESS$

$\forall \ a\_a : WF\_PREFIXING_C$

$\bullet \ a\_a.1 \to_{Cout} a\_a.2 = a\_a.1 \to_C a\_a.2$

z

$\boldsymbol{var_C} : WF\_Var_C \to CSP\_PROCESS$

$$
\begin{array}{l}
\forall\ n{:}\mathit{VAR\_NAME};\ t{:}\mathit{SET\_VAL};\ a{:}\mathit{CSP\_PROCESS} \\
\qquad \mid (n,t,a) \in \mathit{WF\_Var}_C \\
\qquad \bullet\ \mathit{var}_C\ (n,t,a) = \mathit{varT}_R(a.1,n,t)\ ;_R\ a\ ;_R \\
\qquad\qquad\qquad\qquad \mathit{endT}_R(a.1,n,t)
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{NonRef}\colon (\mathit{VAR\_NAME} \times \mathit{VAR\_NAME} \times \mathit{CIRCUS\_CONDITION}) \rightarrow \\
\qquad\qquad \mathit{SET\_EVENT\_VAL} \\
\hline
\forall c{:}\mathit{VAR\_NAME};\ x{:}\mathit{VAR\_NAME};\ p{:}\mathit{CIRCUS\_CONDITION} \\
\bullet\ \mathit{NonRef}(c,x,p) = \mathit{Set}(\{v{:}\mathit{VALUE} \\
\qquad\qquad\qquad \mid /_R(p,\mathit{Val}(v),x) = \mathit{True}_R\ p.1 \\
\qquad\qquad\qquad \bullet\ \mathit{Pair}(\mathit{Channel}(c),v)\})
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{Traces}\colon (\mathit{VAR\_NAME} \times \mathit{VAR\_NAME} \times \mathit{CIRCUS\_CONDITION}) \rightarrow \\
\qquad\qquad \mathit{SET\_SEQ\_EVENT\_VAL} \\
\hline
\forall c{:}\mathit{VAR\_NAME};\ x{:}\mathit{VAR\_NAME};\ p{:}\mathit{CIRCUS\_CONDITION} \\
\bullet\ \mathit{Traces}(c,x,p) = \mathit{Set}(\{v{:}\mathit{VALUE} \\
\qquad\qquad\qquad \mid /_R(p,\mathit{Val}(v),x) = \mathit{True}_R\ p.1 \\
\qquad\qquad\qquad \bullet\ \mathit{Seq}(\langle \mathit{Pair}(\mathit{Channel}(c),v)\rangle)\})
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{do\_I}\colon (\mathit{ALPHABET\_REA} \times \mathit{VAR\_NAME} \times \mathit{VAR\_NAME} \times \mathit{CIRCUS\_CONDITION}) \\
\qquad\qquad \rightarrow \mathit{CSP\_PROCESS} \\
\hline
\forall a{:}\mathit{ALPHABET\_REA};\ c{:}\mathit{VAR\_NAME};\ x{:}\mathit{VAR\_NAME};\ p{:}\mathit{CIRCUS\_CONDITION} \\
\qquad \bullet\ \mathit{do\_I}(a,c,x,p) = \\
\qquad\qquad ((=_R(a,\mathit{dash}\ tr,\ \mathit{Var}(tr))) \\
\qquad\qquad \wedge_R\ (=_{+R}(a, \\
\qquad\qquad\qquad\qquad \mathit{Fun}_2((\_ \cap_R \_), \\
\qquad\qquad\qquad\qquad\qquad \mathit{Val}(\mathit{NonRef}(c,x,p)),
\end{array}
$$

$$
\begin{array}{l}
\qquad\qquad\qquad\qquad\qquad\qquad \mathit{Var}(\mathit{dash\ ref})),\\
\qquad\qquad\qquad\qquad\qquad \mathit{Val}(\mathit{Set}(\varnothing)))))\\
\qquad\qquad \lhd_R\\
\qquad\qquad (=_R(a, \mathit{dash\ wait}, \mathit{Val}(\mathit{Bool}(\mathit{true}))))\\
\qquad\qquad \rhd_R\\
\qquad\qquad (=_{+R} (a,\\
\qquad\qquad\qquad \mathit{Rel}\ ((\_ \in_R \_),\\
\qquad\qquad\qquad\qquad \mathit{Fun}_2((\_ \ \mathit{SeqDif}_R \ \_),\\
\qquad\qquad\qquad\qquad\qquad \mathit{Var}(\mathit{dash\ tr}),\\
\qquad\qquad\qquad\qquad\qquad \mathit{Var}(\mathit{tr})),\\
\qquad\qquad\qquad\qquad \mathit{Val}(\mathit{Traces}(c,x,p))\\
\qquad\qquad\qquad\qquad),\\
\qquad\qquad\qquad \mathit{Val}\ (\mathit{Bool\ true})))
\end{array}
$$

z

$$\mathit{fun}\ \_ \longrightarrow_{\boldsymbol{CinR}} \_$$

z

$$
\begin{array}{l}
\_ \longrightarrow_{\boldsymbol{CinR}} \_ : ((\mathit{ALPHABET\_REA} \times \mathit{VAR\_NAME} \times \mathit{VAR\_NAME} \times\\
\qquad\qquad\qquad \mathit{CIRCUS\_CONDITION}) \times\\
\qquad\qquad\qquad \mathit{CSP\_PROCESS}) \rightarrow \mathit{CSP\_PROCESS}\\
\hline
\forall a{:}\mathit{ALPHABET\_REA};\ c{:}\mathit{VAR\_NAME};\ x{:}\mathit{VAR\_NAME};\\
\qquad p{:}\mathit{CIRCUS\_CONDITION};\ A{:}\mathit{CSP\_PROCESS}\\
\bullet\ (a,c,x,p) \rightarrow_{CinR} A =\\
\qquad \mathit{var}_C(x, \mathit{Set}(\{v{:}\mathit{VALUE}\}),\\
\qquad\qquad R(\\
\qquad\qquad \mathit{True}_R\ A.1\\
\qquad\qquad \vdash_D\\
\qquad\qquad \mathit{do\_I}(a,c,x,p) \wedge_R \mathit{\Pi}_R(A.1 \setminus \{x,\ \mathit{dash}\ x\})\\
\qquad\qquad) ;_C\\
\qquad\qquad A)
\end{array}
$$

z

$fun\ \_ \boldsymbol{\rightarrow_{Cin}}\ \_$

z

$$\_ \boldsymbol{\rightarrow_{Cin}} \_ : ((ALPHABET\_REA \times VAR\_NAME \times VAR\_NAME) \times CSP\_PROCESS) \rightarrow CSP\_PROCESS$$

$$\forall a{:}ALPHABET\_REA;\ c{:}VAR\_NAME;\ x{:}VAR\_NAME;\ A{:}CSP\_PROCESS \bullet (a,c,x) \rightarrow_{Cin} A = (a,c,x,True_R\ A.1) \rightarrow_{CinR} A$$

z

$$\boldsymbol{MTrInter} : (SEQ\_EVENT\_VAL \times SEQ\_EVENT\_VAL) \rightarrow SET\_SEQ\_EVENT\_VAL$$

$$\forall s1,s2 : SEQ\_EVENT\_VAL \bullet MTrInter(s1,s2) = Set(\{s{:}((Seq^{\sim})s1)\ [\![]\!]_Z\ ((Seq^{\sim})s2) \bullet Seq(s)\})$$

z

$$\boldsymbol{MTrPar} : (PAIR\_SEQ\_EVENT\_VAL \times SET\_EVENT\_VAL) \rightarrow SET\_SEQ\_EVENT\_VAL$$

$$\forall ps{:}PAIR\_SEQ\_EVENT\_VAL\ ;\ cs{:}SET\_EVENT\_VAL \bullet MTrPar(ps,cs) = Set(\{s{:}((Seq^{\sim})((Pair^{\sim})ps).1)\ [\![_Z\ ((Set^{\sim})cs)\ ]\!]_Z\ ((Seq^{\sim})((Pair^{\sim})ps).2) \bullet Seq(s)\})$$

z

$$\boldsymbol{MTrParPred}: SET\_EVENT\_VAL \rightarrow REL\_PREDICATE$$

$$\forall\ cs{:}SET\_EVENT\_VAL \bullet$$

$MTrParPred\ cs =$
$=_{+R}$ $(\{tr,\ dash\ tr\},$
$Rel\ ((\_ \in_R \_),$
$Fun_2((\_\ SeqDif_R\ \_),\ Var(dash\ tr),$
$Var(tr)),$
$Fun_2(MTrPar,$
$Fun_2(MkPair,$
$Fun_2((\_\ SeqDif_R\ \_),$
$Var(one\ tr),$
$Var(tr)),$
$Fun_2((\_\ SeqDif_R\ \_),$
$Var(two\ tr),$
$Var(tr))),$
$Val(cs))),$
$Val\ (Bool\ true))$

z

$\boldsymbol{MSync}$: $SET\_EVENT\_VAL \rightarrow REL\_PREDICATE$

$\forall\ cs{:}SET\_EVENT\_VAL\ \bullet$
$MSync\ cs =$
$(=_{+R}(\{one\ tr, two\ tr\},$
$Fun_2((\_ \upharpoonright_R \_),$
$Var(one\ tr),$
$Val(cs)),$
$Fun_2((\_ \upharpoonright_R \_),$
$Var(two\ tr),$
$Val(cs))))$

z

$\boldsymbol{BranchesWaiting}$: $REL\_PREDICATE$

$BranchesWaiting =$

$=_R(\{one\ \ wait\},one\ \ wait,Val(Bool(true)))$
$\vee_R\ =_R(\{two\ \ wait\},two\ \ wait,Val(Bool(true)))$

z

$\boldsymbol{BranchesNotWaiting}$: $REL\_PREDICATE$

$BranchesWaiting\ =$
$=_R(\{one\ \ wait\},one\ \ wait,Val(Bool(false)))$
$\wedge_R\ =_R(\{two\ \ wait\},two\ \ wait,Val(Bool(false)))$

z

$\boldsymbol{MRefPar}$: $SET\_EVENT\_VAL \rightarrow REL\_PREDICATE$

$\forall cs{:}SET\_EVENT\_VAL\ \bullet$
$MRefPar(cs)\ =$
$=_{+R}\ (\{dash\ \ ref\},$
$Rel\ (\ (\_ \subseteq_R \_),$
$Var(dash\ \ ref),$
$Fun_2(\ (\_ \cup_R \_),$
$Fun_2((\_ \cap_R \_),$
$Fun_2((\_ \cup_R \_),$
$Var(one\ \ ref),$
$Var(two\ \ ref)\qquad),$
$Val(cs)),$
$Fun_2((\_ \setminus_R \_),$
$Fun_2((\_ \cap_R \_),$
$Var(one\ \ ref),$
$Var(two\ \ ref)$
$),$
$Val(cs))\ )\ ),$
$Val\ (Bool\ \ true))$

z

$\boldsymbol{MSt}$: $(ALPHABET \times ALPHABET \times ALPHABET) \rightarrow REL\_PREDICATE$

$$
\begin{array}{l}
\forall ns1, ns2, st : ALPHABET \bullet \\
\quad st = \varnothing \Rightarrow MSt(st, ns1, ns2) = True_R\ \varnothing \\
\quad \land\ st \neq \varnothing \Rightarrow \\
\quad\quad (\exists n : st \bullet \\
\quad\quad\quad n \in ns1 \Rightarrow MSt(st, ns1, ns2) = \\
\quad\quad\quad\quad (=_R(\{dash\ n, one\ n\}, \\
\quad\quad\quad\quad\quad dash\ n, \\
\quad\quad\quad\quad\quad Var(one\ n))) \\
\quad\quad\quad\quad \land_R\ MSt(st \setminus \{n\}, \\
\quad\quad\quad\quad\quad ns1, ns2) \\
\quad\quad\quad \land\ n \in ns2 \Rightarrow MSt(st, ns1, ns2) = \\
\quad\quad\quad\quad (=_R(\{dash\ n, two\ n\}, \\
\quad\quad\quad\quad\quad dash\ n, \\
\quad\quad\quad\quad\quad Var(two\ n))) \\
\quad\quad\quad\quad \land_R\ MSt(st \setminus \{n\}, \\
\quad\quad\quad\quad\quad ns1, ns2) \\
\quad\quad\quad \land\ n \notin ns1 \cup ns2 \Rightarrow MSt(st, ns1, ns2) = \\
\quad\quad\quad\quad (=_R(\{dash\ n, n\}, \\
\quad\quad\quad\quad\quad dash\ n, \\
\quad\quad\quad\quad\quad Var(n))) \\
\quad\quad\quad\quad \land_R\ MSt(st \setminus \{n\}, \\
\quad\quad\quad\quad\quad ns1, ns2) \\
\quad\quad)
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{MWtRefStPar} : (SET\_EVENT\_VAL \times ALPHABET \times ALPHABET \times ALPHABET) \\
\quad\quad \rightarrow\ REL\_PREDICATE \\
\hline
\forall ns1, ns2, st : ALPHABET;\ cs : SET\_EVENT\_VAL \bullet \\
\quad MWtRefStPar(cs, st, ns1, ns2) = \\
\quad\quad BranchesWaiting \land_R MRefPar(cs) \\
\quad\quad \lhd_R
\end{array}
$$

$$(=_R(\{dash\ wait\}, dash\ wait, Val(Bool(true))))$$
$$\rhd_R$$
$$BranchesNotWaiting \wedge_R MSt(st, ns1, ns2)$$

z

$\boldsymbol{MPar}$: $(SET\_EVENT\_VAL \times ALPHABET \times ALPHABET \times ALPHABET) \rightarrow REL\_PREDICATE$

$\forall ns1, ns2, st : ALPHABET;\ cs : SET\_EVENT\_VAL \bullet$
$$MPar(cs, st, ns1, ns2) =$$
$$MTrParPred(cs)$$
$$\wedge_R MSync(cs)$$
$$\wedge_R MWtRefStPar(cs, st, ns1, ns2)$$

z

$\boldsymbol{DivPar}$: $(CSP\_PROCESS \times CSP\_PROCESS \times SET\_EVENT\_VAL) \rightarrow REL\_PREDICATE$

$\forall a1, a2 : CSP\_PROCESS;\ cs : SET\_EVENT\_VAL$
$$\bullet\ DivPar\ (a1, a2, cs) =$$
$$\exists\_R(\{dash(one\ tr), dash(two\ tr)\},$$
$$((a1\ \omega_f\ \sigma_f)\ ;_C$$
$$(=_R(a1.1,\ dash(one\ tr),\ Var(tr))))$$
$$\wedge_R$$
$$((a2\ \omega_f)\ ;_C$$
$$(=_R(a2.1,\ dash(two\ tr),\ Var(tr))))$$
$$\wedge_R MSync(cs)$$
$$)$$

z

$fun\ \_\ \llbracket_{\boldsymbol{C}}\ \_\ \rrbracket_{\boldsymbol{C}}\ \_$

z

$\_\ \llbracket_{\boldsymbol{C}}\ \_\ \rrbracket_{\boldsymbol{C}}\ \_$: $(CSP\_PROCESS \times$

$$(ALPHABET \times SET\_EVENT\_VAL \times ALPHABET)$$
$$\times\ CSP\_PROCESS) \rightarrow CSP\_PROCESS$$

$\forall a1,a2{:}CSP\_PROCESS;\ cs{:}SET\_EVENT\_VAL;\ ns1,ns2{:}ALPHABET$
$\quad |\ (a1,a2) \in WF\_CSP\_PROCESS\_PAIR$
$\qquad \wedge\ ns1 \cap dashed = ns2 \cap dashed = \varnothing$
$\qquad \wedge\ ns1 \cap ns2 = \varnothing$
$\quad \bullet\ a1\ [\![_C\ (ns1,cs,ns2)\ ]\!]_C\ a2 =$
$\quad R($
$\quad (\neg_R\ (DivPar(a1,a2,cs))\ \wedge_R\ \neg_R\ (DivPar(a2,a1,cs)))$
$\quad \vdash_D$
$\quad (\ (\ (((a1\ \omega_f\ \sigma_t)\ ;_C\ U(one,out\_a\ a1.1))$
$\qquad \wedge_R\ ((a2\ \omega_f\ \sigma_t)\ ;_C\ U(two,out\_a\ a2.1)))$
$\qquad +_R\ (\{tr\} \cup (a1.1\ \setminus\ (ALPHABET\_OWTR \cup dashed)))\ )$
$\quad ;_C\ (MPar(cs,a1.1 \setminus (ALPHABET\_OWTR \cup dashed),ns1,ns2))\ )$
$\quad)$

z

$\boldsymbol{MTrInterPred}$: $REL\_PREDICATE$

$MTrInterPred =$
$\quad =_{+R}\ (\{tr,\ dash\ tr\},$
$\qquad Rel\ ((\_ \in_R \_),$
$\qquad\quad Fun_2((\_\ SeqDif_R\ \_),\ Var(dash\ tr),$
$\qquad\qquad\qquad Var(tr)),$
$\qquad\quad Fun_2(MTrInter,$
$\qquad\qquad Fun_2((\_\ SeqDif_R\ \_),$
$\qquad\qquad\quad Var(one\ tr),$
$\qquad\qquad\quad Var(tr)),$
$\qquad\qquad Fun_2((\_\ SeqDif_R\ \_),$
$\qquad\qquad\quad Var(two\ tr),$
$\qquad\qquad\quad Var(tr))\ )),$
$\qquad Val\ (Bool\ true))$

z

$$\boldsymbol{MRefInter}: REL\_PREDICATE$$

$$
\begin{array}{l}
MRefInter = \\
\quad =_{+R} (\{dash\ ref\}, \\
\quad\quad Rel\ (\ (\_ \subseteq_R \_), \\
\quad\quad\quad Var(dash\ ref), \\
\quad\quad\quad Fun_2((\_ \cap_R \_), \\
\quad\quad\quad\quad Var(one\ ref), \\
\quad\quad\quad\quad Var(two\ ref))), \\
\quad\quad Val\ (Bool\ true))
\end{array}
$$

z

$$\boldsymbol{MWtRefStInter}: (ALPHABET \times ALPHABET \times ALPHABET) \rightarrow REL\_PREDICATE$$

$$
\begin{array}{l}
\forall ns1, ns2, st{:}ALPHABET \bullet \\
\quad MWtRefStInter(st, ns1, ns2) = \\
\quad\quad BranchesNotWaiting \wedge_R MRefInter \\
\quad\quad \lhd_R \\
\quad\quad (=_R(\{dash\ wait\}, dash\ wait, Val(Bool(true)))) \\
\quad\quad \rhd_R \\
\quad\quad BranchesWaiting \wedge_R MSt(st, ns1, ns2)
\end{array}
$$

z

$$\boldsymbol{MInter}: (ALPHABET \times ALPHABET \times ALPHABET) \rightarrow REL\_PREDICATE$$

$$
\begin{array}{l}
\forall ns1, ns2, st{:}ALPHABET \bullet \\
\quad MInter(st, ns1, ns2) = \\
\quad\quad MTrInterPred \\
\quad\quad \wedge_R MWtRefStInter(st, ns1, ns2)
\end{array}
$$

z

$$\boldsymbol{DivInter}: (CSP\_PROCESS \times CSP\_PROCESS) \rightarrow REL\_PREDICATE$$

$$\begin{array}{l}
\forall a1,a2:CSP_PROCESS \\
\quad \bullet\ DivInter\ (a1,a2) = \\
\qquad \exists_{}_R(\{dash(one\ tr),dash(two\ tr)\}, \\
\qquad\quad ((a1\ \omega_f\ \sigma_f)\ ;_C \\
\qquad\quad\ (=_R(a1.1,\ dash(one\ tr),\ Var(tr)))) \\
\qquad\quad \wedge_R \\
\qquad\quad ((a2\ \omega_f)\ ;_C \\
\qquad\quad\ (=_R(a2.1,\ dash(two\ tr),\ Var(tr)))) \\
\qquad)
\end{array}$$

z

$$fun\ \_\ \ [\![_C\ \_\ ]\!]_C\ \_$$

z

$$\begin{array}{l}
_\ \ [\![_C\ _\ ]\!]_C\ _: (CSP_PROCESS \times (ALPHABET \times ALPHABET) \\
\qquad\qquad \times CSP_PROCESS) \rightarrow CSP_PROCESS
\end{array}$$

$$\begin{array}{l}
\forall a1,a2:CSP_PROCESS;\ ns1,ns2:ALPHABET \\
\quad \mid (a1,a2) \in WF_CSP_PROCESS_PAIR \\
\quad \wedge\ ns1 \cap ns2 = \varnothing \\
\quad \bullet\ a1\ [\![_C\ (ns1,ns2)\ ]\!]_C\ a2 = \\
\quad R(\\
\quad (\neg_R\ (DivInter(a1,a2))\ \wedge_R\ \neg_R\ (DivInter(a2,a1))) \\
\quad \vdash_D \\
\quad (((((a1\ \omega_f\ \sigma_t)\ ;_C\ U(one,out_a\ a1.1)) \\
\qquad \wedge_R\ ((a2\ \omega_f\ \sigma_t);_C\ U(two,out_a\ a1.1)))\ +_R \\
\qquad (\{tr\} \cup (a1.1 \setminus (ALPHABET_OWTR \cup dashed)))) \\
\qquad \wedge_R\ (\Pi_R\ (a1.1 \setminus ALPHABET_OWTR)))\ ;_C \\
\qquad (MInter((a1.1 \setminus ALPHABET_OWTR)\setminus dashed,ns1,ns2)) \\
\quad)
\end{array}$$

z

$fun\ \_\ \boldsymbol{\backslash_C}\ \_$

z

$\_\ \boldsymbol{\backslash_C}\ \_ : (CSP\_PROCESS \times SET\_EVENT\_VAL) \rightarrow CSP\_PROCESS$

$$
\begin{array}{l}
\forall a{:}CSP\_PROCESS;\ cs{:}SET\_EVENT\_VAL \bullet \\
\quad \exists s{:}VAR\_NAME \\
\quad \mid s \notin a.1 \\
\quad \bullet\ a \backslash_C cs = \\
\quad R(\ \exists_{-R}(\ \{s\}, \\
\qquad (/_R(/_R((a \oplus_R \{s\}),\ Var(s),\ dash\ tr), \\
\qquad\qquad Fun_2((\_ \cup_R \_),\ Val(cs),\ Var(ref)), \\
\qquad\qquad\qquad dash\ ref)) \\
\qquad \wedge_R \\
\qquad (=_{+R}(\{tr, dash\ tr, s\}, \\
\qquad\quad Fun_2((\_\ SeqDif_R\ \_), \\
\qquad\qquad Var(dash\ tr), \\
\qquad\qquad Var(tr)), \\
\qquad\quad Fun_2((\_ \backslash_R \_), \\
\qquad\qquad Val(Set(EVENT\_VAL)), \\
\qquad\qquad Val(cs))))\ )\ )\ ;_C\ Skip(a.1)
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{CIRCUS\_FUNCTION} \mathrel{\widehat=} \\
\quad \{f{:}CSP\_PROCESS \nrightarrow CSP\_PROCESS \\
\qquad \mid (\exists a{:}ALPHABET \bullet \\
\qquad\quad (\forall u\_dom{:}dom\ f;\ u\_ran{:}ran\ f \\
\qquad\quad \bullet\ a = u\_dom.1 = u\_ran.1))\}
\end{array}
$$

z

$\boldsymbol{\mu_C} : CIRCUS\_FUNCTION \rightarrow CSP\_PROCESS$

$\forall f\colon CIRCUS\_FUNCTION \bullet \mu_C\ f = \mu_R\ f$

z

$\boldsymbol{Assign_C} : WF\_Assign_C \rightarrow CSP\_PROCESS$

$\forall a{:}ALPHABET;\ ns\colon seq\ VAR\_NAME;\ exps\colon seq\ EXPRESSION$
$\quad \mid (a,ns,exps) \in WF\_Assign_C$
$\quad \bullet\ Assign_C(a,ns,exps) =$
$\quad R(\ True_R(a)$
$\qquad \vdash_D$
$\qquad (\ Assign_R(a,ns,exps)$
$\qquad\quad \wedge_R\ (=_R(a,\ dash\ tr,\ Var(tr)))$
$\qquad\quad \wedge_R\ (=_R(a,dash\ wait,\ Val(Bool(false))))\ )$
$\quad)$

z

$\boldsymbol{SpecStatement_C} : WF\_SpecStatement_C \rightarrow CSP\_PROCESS$

$\forall a{:}ALPHABET;\ f\colon \mathbb{F}\ VAR\_NAME;\ preC\colon CIRCUS\_CONDITION;$
$\quad postC\colon CIRCUS\_PREDICATE$
$\quad \mid (a,f,preC,postC) \in WF\_SpecStatement_C$
$\quad \bullet\ SpecStatement_C(a,f,preC,postC) =$
$\quad R(\ preC$
$\qquad \vdash_D$
$\qquad (\ postC$
$\qquad\quad \wedge_R\ (=_R(a,\ dash\ tr,\ Var(tr)))$
$\qquad\quad \wedge_R\ (=_R(a,\ dash\ wait,\ Val(Bool(false))))$
$\qquad\quad \wedge_R\ (\Pi_R(a \setminus (ALPHABET\_OWTR$
$\qquad\qquad\quad \cup (f \cup \{n{:}f \bullet dash\ n\}))))$
$\qquad\quad)$
$\quad)$

z

$fun\ \boldsymbol{\{_C}\ \_\ \boldsymbol{\}_C}$

z

$$\{_C \; \_ \; \}_C : WF\_Condition_C \rightarrow CSP\_PROCESS$$

$$\forall\ a{:}ALPHABET;\ g{:}\ CIRCUS\_CONDITION$$
$$\quad \mid (a,g) \in WF\_Condition_C$$
$$\quad \bullet \{_C\ (a,g)\ \}_C = SpecStatement_C(a,\{\},g,True_R\ a)$$

z

$$fun\ \langle_C \; \_ \; \rangle_C$$

z

$$\langle_C \; \_ \; \rangle_C : WF\_Condition_C \rightarrow CSP\_PROCESS$$

$$\forall\ a{:}ALPHABET;\ g{:}\ CIRCUS\_CONDITION$$
$$\quad \mid (a,g) \in WF\_Condition_C$$
$$\quad \bullet \langle_C\ (a,g)\ \rangle_C = R(True_R(a) \vdash_D g)$$

z

$$\boldsymbol{Typing} : (VAR\_DECLS \times ALPHABET) \leftrightarrow REL\_PREDICATE$$

$$\forall\ decls{:}VAR\_DECLS;\ a{:}ALPHABET$$
$$\quad \mid ran\ (decls.1) \subseteq a$$
$$\quad \bullet$$
$$\quad (\ \#decls.1 = 1$$
$$\qquad \wedge\ (\ \exists n{:}Z\_VAR\_NAME;\ e{:}EXPRESSION$$
$$\qquad\quad \mid n = head(decls.1) \wedge e = head(decls.2)$$
$$\qquad\quad \bullet\ Typing(decls,a) =$$
$$\qquad\qquad =_{+R} (a,\ Rel((\_ \in_R \_),$$
$$\qquad\qquad\qquad Var(n),e),$$
$$\qquad\qquad\quad Val\ (Bool\ true))\ )$$
$$\quad)$$
$$\quad \vee\ (\ \#decls.1 > 1$$
$$\qquad \wedge\ (\ \exists n{:}Z\_VAR\_NAME;\ e{:}EXPRESSION$$

$$
\begin{array}{l}
\qquad\qquad\qquad\qquad \mid n = head(decls.1) \land e = head(decls.2) \\
\qquad\qquad\qquad\qquad \bullet\ Typing(decls,a) = \\
\qquad\qquad\qquad\qquad\qquad =_{+R}\ (a,\ Rel((\_ \in_R \_), \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad Var(n),e), \\
\qquad\qquad\qquad\qquad\qquad\qquad Val\ (Bool\ true)) \\
\qquad\qquad\qquad\qquad\qquad \land_R\ \ Typing((tail\ decls.1, \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad tail\ decls.2), \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad a)\ ) \\
\qquad)
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{SchemaExp_C}\text{: } WF\_SchemaExp_C \to CSP\_PROCESS \\
\hline
\forall\ decls{:}VAR\_DECLS;\ p{:}REL\_PREDICATE \\
\qquad \mid (decls,p) \in WF\_SchemaExp_C \\
\qquad \bullet\ \ (\exists f{:}\mathbb{F}\ Z\_VAR\_NAME \mid f \subseteq undashed \\
\qquad\qquad\qquad\qquad \land\ ran\ (decls.1 \upharpoonright dashed) = dash\ (\!| f |\!)) \\
\qquad \bullet\ SchemaExp_C(decls,p) = \\
\qquad\qquad SpecStatement_C(\\
\qquad\qquad\qquad ran(decls.1) \cup ALPHABET\_OWTR, \\
\qquad\qquad\qquad f, \\
\qquad\qquad\qquad \exists_{-R}(ran(decls.1) \setminus undashed, \\
\qquad\qquad\qquad\qquad Typing(decls,p.1) \land_R\ p), \\
\qquad\qquad\qquad Typing(decls,p.1) \land_R\ p)\ )
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{GUARDED\_ACTIONS} \mathrel{\widehat{=}} \\
\qquad \{conditions{:}seq\ CIRCUS\_CONDITION; \\
\qquad\qquad actions{:}seq\ CSP\_PROCESS \\
\qquad\qquad \mid dom\ conditions \in (\mathbb{F}\ \_) \land dom\ actions \in (\mathbb{F}\ \_) \\
\qquad\qquad\ \land \#(ran\ conditions) = \#(ran\ actions) > 0 \\
\qquad\qquad\ \land (\exists a{:}ALPHABET\ \bullet \\
\qquad\qquad\qquad (\forall c{:}(ran\ conditions) \bullet c.1 = a)
\end{array}
$$

```
|                    ∧ (∀A:(ran actions) • A.1 = a))}
```

```
z
| TrueGuards : GUARDED_ACTIONS → REL_PREDICATE
|------------------------------------
| ∀ gactions:GUARDED_ACTIONS
|      •
|      ( #gactions.1 = 1
|            ∧ ( ∃ g:CIRCUS_CONDITION; a:CSP_PROCESS
|                  | g = head(gactions.1)
|                  ∧ a = head(gactions.2)
|                  • TrueGuards(gactions) = g )
|      )
|      ∨ ( #gactions.1 > 1
|            ∧ ( ∃ g:CIRCUS_CONDITION; a:CSP_PROCESS
|                  | g = head(gactions.1)
|                  ∧ a = head(gactions.2)
|                  • TrueGuards(gactions) =
|                        g ∨_R
|                        TrueGuards(tail gactions.1,
|                                 tail gactions.2) )
|      )
```

```
z
| NonDivActions : GUARDED_ACTIONS → REL_PREDICATE
|------------------------------------
| ∀ gactions:GUARDED_ACTIONS
|      •
|      ( #gactions.1 = 1
|            ∧ ( ∃ g:CIRCUS_CONDITION; a:CSP_PROCESS
|                  | g = head(gactions.1)
|                  ∧ a = head(gactions.2)
|                  • NonDivActions(gactions) =
```

$$g \Rightarrow_R (\neg_R (a\ \omega_f\ \sigma_f))\ )$$

$)$

$\vee$ ($\#gactions.1 > 1$

$\wedge$ ($\exists\ g{:}CIRCUS\_CONDITION;\ a{:}CSP\_PROCESS$

$\mid g = head(gactions.1)$

$\wedge\ a = head(gactions.2)$

$\bullet\ NonDivActions(gactions) =$

$(g \Rightarrow_R (\neg_R (a\ \omega_f\ \sigma_f)))$

$\wedge_R$

$NonDivActions(tail\ gactions.1,$

$tail\ gactions.2)\ )$

$)$

z

$\boldsymbol{ExecActions} : GUARDED\_ACTIONS \rightarrow REL\_PREDICATE$

$\forall\ gactions{:}GUARDED\_ACTIONS$

$\bullet$

($\#gactions.1 = 1$

$\wedge$ ($\exists\ g{:}CIRCUS\_CONDITION;\ a{:}CSP\_PROCESS$

$\mid g = head(gactions.1)$

$\wedge\ a = head(gactions.2)$

$\bullet\ ExecActions(gactions) =$

$g \wedge_R (a\ \omega_f\ \sigma_t)\ )$

$)$

$\vee$ ($\#gactions.1 > 1$

$\wedge$ ($\exists\ g{:}CIRCUS\_CONDITION;\ a{:}CSP\_PROCESS$

$\mid g = head(gactions.1)$

$\wedge\ a = head(gactions.2)$

$\bullet\ ExecActions(gactions) =$

$(g \wedge_R (a\ \omega_f\ \sigma_t))$

$\vee_R$

$ExecActions(tail\ gactions.1,$

$tail\ gactions.2)\ )$

$)$

z

$fun\ \boldsymbol{if_C}\ \_\ \boldsymbol{fi_C}$

z

$\boldsymbol{if_C}\ \_\ \boldsymbol{fi_C} : GUARDED\_ACTIONS \rightarrow CSP\_PROCESS$

$\forall\ gactions : GUARDED\_ACTIONS$

$\bullet\ \ if_C\ gactions\ fi_C =$

$R($

$(TrueGuards(gactions) \wedge_R NonDivActions(gactions))$

$\vdash_D$

$ExecActions(gactions)$

$)$

z

$fun\ \boldsymbol{ifb_C}\ \_\ \boldsymbol{\mapsto_C}\ \_\ \boldsymbol{else_C}\ \_\ \boldsymbol{\mapsto_C}\ \_\ \boldsymbol{fib_C}$

z

$\boldsymbol{ifb_C}\ \_\ \boldsymbol{\mapsto_C}\ \_\ \boldsymbol{else_C}\ \_\ \boldsymbol{\mapsto_C}\ \_\ \boldsymbol{fib_C}:$

$(CIRCUS\_CONDITION \times CSP\_PROCESS \times$

$CIRCUS\_CONDITION \times CSP\_PROCESS) \nrightarrow$

$CSP\_PROCESS$

$\forall\ g1, g2 : CIRCUS\_CONDITION;\ a1, a2 : CSP\_PROCESS$

$\mid (\langle g1, g2 \rangle, \langle a1, a2 \rangle) \in GUARDED\_ACTIONS$

$\bullet\ \ ifb_C\ g1 \mapsto_C a1\ \ else_C\ g2 \mapsto_C a2\ fib_C =$

$R(\ (\ (g1 \vee_R g2) \wedge_R$

$((g1 \Rightarrow_R (\neg_R\ (a1\ \omega_f\ \sigma_f)))$

$\wedge_R (g2 \Rightarrow_R (\neg_R\ (a2\ \omega_f\ \sigma_f))))\ )$

$$\vdash_D$$
$$(\ (g1\ \wedge_R\ (\neg_R\ (a1\ \omega_f\ \sigma_t)))$$
$$\quad \vee_R\ (g2\ \wedge_R\ (\neg_R\ (a2\ \omega_f\ \sigma_t)))\ )$$
$$)$$

z

$\boldsymbol{param_C}$: $WF\_param_C \rightarrow CSP\_PROCESS$

$$\forall\ x{:}VAR\_NAME;\ T{:}EXPRESSION;\ a{:}CSP\_PROCESS;\ e{:}EXPRESSION$$
$$\mid (x,T,a,e) \in WF\_param_C$$
$$\bullet\ param_C(x,T,a,e) = /_R(a,e,x)$$

z

$\boldsymbol{val_C}$: $WF\_val_C \rightarrow CSP\_PROCESS$

$$\forall\ x{:}VAR\_NAME;\ t{:}SET\_VAL;\ a{:}CSP\_PROCESS;\ e{:}EXPRESSION$$
$$\mid (x,t,a,e) \in WF\_val_C$$
$$\bullet\ val_C(x,t,a,e) =$$
$$\quad var_C\ (x,t,Assign_R(a.1,\langle x\rangle,\langle e\rangle)\ ;_C\ a)$$

z

$\boldsymbol{res_C}$: $WF\_res_C \rightarrow CSP\_PROCESS$

$$\forall\ x{:}VAR\_NAME;\ t{:}SET\_VAL;\ a{:}CSP\_PROCESS;\ y{:}VAR\_NAME$$
$$\mid (x,t,a,y) \in WF\_res_C$$
$$\bullet\ res_C(x,t,a,y) =$$
$$\quad var_C\ (x,t,a\ ;_R\ Assign_R(a.1,\langle y\rangle,\langle Var(x)\rangle))$$

z

$\boldsymbol{vres_C}$: $WF\_vres_C \rightarrow CSP\_PROCESS$

$$
\begin{array}{l}
\forall\ x{:}VAR\_NAME;\ t{:}SET\_VAL;\ a{:}CSP\_PROCESS;\ y{:}VAR\_NAME \\
\quad \mid (x,t,a,y) \in WF\_vres_C \\
\quad \bullet\ vres_C(x,t,a,y) = \\
\qquad var_C\ (x,t, \\
\qquad\quad Assign_R(a.1,\langle x\rangle,\langle Var(y)\rangle)\ ;_R \\
\qquad\quad a\ ;_R \\
\qquad\quad Assign_R(a.1,\langle y\rangle,\langle Var(x)\rangle))
\end{array}
$$

6.3 Healthiness Conditions

z

$$
\begin{array}{l}
\boldsymbol{C1} : CSP\_PROCESS \rightarrow CSP\_PROCESS \\
\hline
\forall a{:}CSP\_PROCESS \bullet C1\ \ a = a\ ;_R\ Skip(a.1)
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{C1\_healthy} : \mathbb{P}\ CSP\_PROCESS \\
\hline
C1\_healthy = \{a{:}CSP\_PROCESS \mid a = C1\ \ a\}
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{C2} : CSP\_PROCESS \rightarrow CSP\_PROCESS \\
\hline
\forall a{:}CSP\_PROCESS \bullet C2\ \ a = (a\ [\![_C\ (a.1,\varnothing)\ ]\!]_C\ Skip(a.1))
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{C2\_healthy} : \mathbb{P}\ CSP\_PROCESS \\
\hline
C2\_healthy = \{a{:}CSP\_PROCESS \mid a = C2\ \ a\}
\end{array}
$$

z

$$
\begin{array}{l}
\boldsymbol{C3} : CSP\_PROCESS \rightarrow CSP\_PROCESS \\
\hline
\end{array}
$$

$$
\begin{array}{l}
\forall a{:}CSP\_PROCESS \bullet \\
\quad C3\ a = R(((\neg_R\ (a\ \sigma_f\ \omega_f))\ ;_R\ True_R(a.1)) \\
\qquad \vdash_D \\
\qquad (a\ \sigma_t\ \omega_f))
\end{array}
$$

Z

$$\boldsymbol{C3\_healthy} : \mathbb{P}\ CSP\_PROCESS$$

$$C3\_healthy = \{a{:}CSP\_PROCESS \mid a = C3\ a\}$$

Z

$$
\begin{array}{ll}
\boldsymbol{CIRCUS\_ACTION} \mathrel{\widehat=} & \{c{:}CSP\_PROCESS \mid c \in C1\_healthy \\
& \land\ c \in C2\_healthy \\
& \land\ c \in C3\_healthy\}
\end{array}
$$

SML

```
z_output_theory{out_file="utp−circus.th.doc",
                theory="utp−circus"};
```

7 THE Z THEORY utp-z-library

7.1 Parents

$cache'/home/consiste/marcel/proofpower/pp{-}examples/circus/db/circus$
$z\_library$

7.2 Global Variables

$(\_ \ \boldsymbol{prefix_Z} \ \_)[\boldsymbol{X}]$
$(\mathbb{Z} \leftrightarrow X) \leftrightarrow \mathbb{Z} \leftrightarrow X$
$(\_ \ \boldsymbol{-_Z} \ \_)[\boldsymbol{X}]$ $\quad (\mathbb{Z} \leftrightarrow X) \times (\mathbb{Z} \leftrightarrow X) \leftrightarrow \mathbb{Z} \leftrightarrow X$
$(\_ \ \boldsymbol{[\![]\!]_Z} \ \_)[\boldsymbol{X}]$
$(\mathbb{Z} \leftrightarrow X) \times (\mathbb{Z} \leftrightarrow X) \leftrightarrow \mathbb{P} (\mathbb{Z} \leftrightarrow X)$
$(\_ \ \boldsymbol{[\![_Z} \ \_ \ \boldsymbol{]\!]_Z} \ \_)[\boldsymbol{X}]$
$(\mathbb{Z} \leftrightarrow X) \times \mathbb{P}\ X \times (\mathbb{Z} \leftrightarrow X) \leftrightarrow \mathbb{P} (\mathbb{Z} \leftrightarrow X)$

7.3 Fixity

fun* 0 *rightassoc
$(\_ \ -_Z \ \_) \qquad (\_ \ [\![_Z \ \_ \ ]\!]_Z \ \_) \ (\_ \ [\![]\!]_Z \ \_)$

rel $\quad (\_ \ prefix_Z \ \_)$

7.4 Axioms

$\_ \ \boldsymbol{prefix_Z} \ \_ \quad \vdash [X]((\_ \ prefix_Z \ \_)[X] \in seq\ X \leftrightarrow seq\ X$
$\quad \land (\forall\ s,\ t : seq\ X$
$\quad\quad \bullet (s,\ t) \in (\_ \ prefix_Z \ \_)[X] \Leftrightarrow s \subseteq t))$
$\_ \ \boldsymbol{-_Z} \ \_ \quad \vdash [X]((\_ \ -_Z \ \_)[X] \in (seq\ X) \times (seq\ X) \nrightarrow seq\ X$
$\quad \land dom\ (\_ \ -_Z \ \_)[X] = \{s,\ t : seq\ X \mid t\ prefix_Z\ s\}$
$\quad \land (\forall\ s,\ t : seq\ X$
$\quad\quad \mid t\ prefix_Z\ s$
$\quad\quad \bullet \exists\ r : seq\ X$
$\quad\quad\quad \bullet s = t \frown r \land (\_ \ -_Z \ \_)[X]\ (s,\ t) = r))$
$\_ \ \boldsymbol{[\![]\!]_Z} \ \_ \quad \vdash [X]((\_ \ [\![]\!]_Z \ \_)[X] \in (seq\ X) \times (seq\ X) \rightarrow \mathbb{P}\ (seq\ X)$
$\quad \land (\forall\ s1,\ s2 : seq\ X$

$$
\begin{array}{l}
\quad \bullet\ s1 = \langle\rangle \\
\qquad \Rightarrow (\_ \llbracket\rrbracket_Z \_)[X]\ (s1, s2) = \{s2\} \land s2 = \langle\rangle \\
\qquad \Rightarrow (\_ \llbracket\rrbracket_Z \_)[X]\ (s1, s2) = \{s1\} \\
\qquad\quad \land s1 \neq \langle\rangle \\
\qquad\quad \land s2 \neq \langle\rangle \\
\qquad \Rightarrow (\exists\ e1, e2 : X; tl1, tl2 : seq\ X \\
\qquad\quad \mid s1 = \langle e1\rangle \frown tl1 \land s2 = \langle e2\rangle \frown tl2 \\
\qquad\quad \bullet (\_ \llbracket\rrbracket_Z \_)[X]\ (s1, s2) \\
\qquad\qquad = \{s : seq\ X \\
\qquad\qquad\quad \mid s \in (\_ \llbracket\rrbracket_Z \_)[X]\ (tl1, \langle e2\rangle \frown tl2) \\
\qquad\qquad\quad \bullet \langle e1\rangle \frown s\} \\
\qquad\qquad\quad \cup \{s : seq\ X \\
\qquad\qquad\quad \mid s \in (\_ \llbracket\rrbracket_Z \_)[X]\ (\langle e1\rangle \frown tl1, tl2) \\
\qquad\qquad\quad \bullet \langle e2\rangle \frown s\})))
\end{array}
$$

$\_ \llbracket_Z \_ \rrbracket_Z \_$

$$
\begin{array}{l}
\vdash [X]((\_ \llbracket_Z \_ \rrbracket_Z \_)[X] \\
\qquad \in (seq\ X) \times \mathbb{P}\ X \times (seq\ X) \rightarrow \mathbb{P}\ (seq\ X) \\
\quad \land (\forall\ s1, s2 : seq\ X; cs : \mathbb{P}\ X \\
\quad \bullet\ s1 = \langle\rangle \land s2 = \langle\rangle \\
\qquad \Rightarrow (\_ \llbracket_Z \_ \rrbracket_Z \_)[X]\ (s1, cs, s2) = \{\langle\rangle\} \\
\qquad\quad \land s1 \neq \langle\rangle \\
\qquad\quad \land s2 = \langle\rangle \\
\qquad \Rightarrow (\exists\ e1 : X; tl1 : seq\ X \\
\qquad\qquad \mid s1 = \langle e1\rangle \frown tl1 \\
\qquad\qquad \bullet (e1 \in cs \\
\qquad\qquad\quad \Rightarrow (\_ \llbracket_Z \_ \rrbracket_Z \_)[X]\ (s1, cs, s2) \\
\qquad\qquad\qquad = \{\langle\rangle\}) \\
\qquad\qquad \land (e1 \notin cs \\
\qquad\qquad\quad \Rightarrow (\_ \llbracket_Z \_ \rrbracket_Z \_)[X]\ (s1, cs, s2) \\
\qquad\qquad\qquad = \{s : seq\ X \\
\qquad\qquad\qquad\quad \mid s \\
\qquad\qquad\qquad\qquad \in (\_ \llbracket_Z \_ \rrbracket_Z \_)[X] \\
\qquad\qquad\qquad\qquad\quad (tl1, cs, \langle\rangle) \\
\qquad\qquad\qquad\quad \bullet \langle e1\rangle \frown s\})) \\
\qquad\quad \land s1 = \langle\rangle \\
\qquad\quad \land s2 \neq \langle\rangle
\end{array}
$$

$$
\begin{array}{l}
\Rightarrow (\exists\, \mathit{e2} : X;\ \mathit{tl2} : \mathit{seq}\ X \\
\quad\quad \mid \mathit{s2} = \langle \mathit{e2} \rangle \frown \mathit{tl2} \\
\quad\quad \bullet (\mathit{e2} \in \mathit{cs} \\
\quad\quad\quad\quad \Rightarrow (\_ \llbracket_Z \_ \rrbracket_Z \_)[X]\ (\mathit{s1}, \mathit{cs}, \mathit{s2}) \\
\quad\quad\quad\quad\quad = \{\langle\rangle\}) \\
\quad\quad\quad \wedge (\mathit{e2} \notin \mathit{cs} \\
\quad\quad\quad\quad \Rightarrow (\_ \llbracket_Z \_ \rrbracket_Z \_)[X]\ (\mathit{s1}, \mathit{cs}, \mathit{s2}) \\
\quad\quad\quad\quad\quad = \{s : \mathit{seq}\ X \\
\quad\quad\quad\quad\quad\quad \mid s \\
\quad\quad\quad\quad\quad\quad\quad \in (\_ \llbracket_Z \_ \rrbracket_Z \_)[X] \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad (\langle\rangle, \mathit{cs}, \mathit{tl2}) \\
\quad\quad\quad\quad\quad\quad \bullet \langle \mathit{e2} \rangle \frown s\})) \\
\quad \wedge \mathit{s1} \neq \langle\rangle \\
\quad \wedge \mathit{s2} \neq \langle\rangle \\
\Rightarrow (\exists\, \mathit{e1}, \mathit{e2} : X;\ \mathit{tl1}, \mathit{tl2} : \mathit{seq}\ X \\
\quad \mid \mathit{s1} = \langle \mathit{e1} \rangle \frown \mathit{tl1} \wedge \mathit{s2} = \langle \mathit{e2} \rangle \frown \mathit{tl2} \\
\quad \bullet (\mathit{e1} = \mathit{e2} \wedge \mathit{e1} \in \mathit{cs} \\
\quad\quad\quad \Rightarrow (\_ \llbracket_Z \_ \rrbracket_Z \_)[X]\ (\mathit{s1}, \mathit{cs}, \mathit{s2}) \\
\quad\quad\quad\quad = \{s : \mathit{seq}\ X \\
\quad\quad\quad\quad\quad \mid s \\
\quad\quad\quad\quad\quad\quad \in (\_ \llbracket_Z \_ \rrbracket_Z \_)[X]\ (\mathit{tl1}, \mathit{cs}, \mathit{tl2}) \\
\quad\quad\quad\quad\quad \bullet \langle \mathit{e1} \rangle \frown s\}) \\
\quad\quad \wedge (\mathit{e1} = \mathit{e2} \wedge \mathit{e1} \notin \mathit{cs} \\
\quad\quad\quad \Rightarrow (\_ \llbracket_Z \_ \rrbracket_Z \_)[X]\ (\mathit{s1}, \mathit{cs}, \mathit{s2}) \\
\quad\quad\quad\quad = \{s : \mathit{seq}\ X \\
\quad\quad\quad\quad\quad \mid s \\
\quad\quad\quad\quad\quad\quad \in (\_ \llbracket_Z \_ \rrbracket_Z \_)[X] \\
\quad\quad\quad\quad\quad\quad\quad\quad (\mathit{tl1}, \mathit{cs}, \langle \mathit{e2} \rangle \frown \mathit{tl2}) \\
\quad\quad\quad\quad\quad\quad\quad \cup (\_ \llbracket_Z \_ \rrbracket_Z \_)[X] \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad (\langle \mathit{e1} \rangle \frown \mathit{tl1}, \mathit{cs}, \mathit{tl2}) \\
\quad\quad\quad\quad\quad \bullet \langle \mathit{e1} \rangle \frown s\}) \\
\quad\quad \wedge (\mathit{e1} \neq \mathit{e2} \wedge \mathit{e1} \in \mathit{cs} \wedge \mathit{e2} \in \mathit{cs} \\
\quad\quad\quad \Rightarrow (\_ \llbracket_Z \_ \rrbracket_Z \_)[X]\ (\mathit{s1}, \mathit{cs}, \mathit{s2}) = \{\langle\rangle\}) \\
\quad\quad \wedge (\mathit{e1} \neq \mathit{e2} \wedge \mathit{e1} \in \mathit{cs} \wedge \mathit{e2} \notin \mathit{cs} \\
\quad\quad\quad \Rightarrow (\_ \llbracket_Z \_ \rrbracket_Z \_)[X]\ (\mathit{s1}, \mathit{cs}, \mathit{s2}) \\
\quad\quad\quad\quad = \{s : \mathit{seq}\ X
\end{array}
$$

$$
\begin{array}{l}
\quad\quad\quad\quad \mid s \\
\quad\quad\quad\quad\quad \in (\_ \llbracket_Z \_ \rrbracket_Z \_)[X] \\
\quad\quad\quad\quad\quad\quad\quad (\langle e1 \rangle \frown tl1,\ cs,\ tl2) \\
\quad\quad\quad\quad \bullet \langle e2 \rangle \frown s\}) \\
\land\ (e1 \neq e2 \land e1 \notin cs \land e2 \in cs \\
\quad \Rightarrow (\_ \llbracket_Z \_ \rrbracket_Z \_)[X]\ (s1,\ cs,\ s2) \\
\quad\quad = \{s : seq\ X \\
\quad\quad\quad\quad \mid s \\
\quad\quad\quad\quad\quad \in (\_ \llbracket_Z \_ \rrbracket_Z \_)[X] \\
\quad\quad\quad\quad\quad\quad\quad (tl1,\ cs,\ \langle e2 \rangle \frown tl2) \\
\quad\quad\quad\quad \bullet \langle e1 \rangle \frown s\}) \\
\land\ (e1 \neq e2 \land e1 \notin cs \land e2 \notin cs \\
\quad \Rightarrow (\_ \llbracket_Z \_ \rrbracket_Z \_)[X]\ (s1,\ cs,\ s2) \\
\quad\quad = \{s : seq\ X \\
\quad\quad\quad\quad\quad \mid s \\
\quad\quad\quad\quad\quad\quad \in (\_ \llbracket_Z \_ \rrbracket_Z \_)[X] \\
\quad\quad\quad\quad\quad\quad\quad\quad (\langle e1 \rangle \frown tl1,\ cs,\ tl2) \\
\quad\quad\quad\quad\quad \bullet \langle e2 \rangle \frown s\} \\
\quad\quad\quad\quad\quad \cup \{s : seq\ X \\
\quad\quad\quad\quad\quad \mid s \\
\quad\quad\quad\quad\quad\quad \in (\_ \llbracket_Z \_ \rrbracket_Z \_)[X] \\
\quad\quad\quad\quad\quad\quad\quad\quad (tl1,\ cs,\ \langle e2 \rangle \frown tl2) \\
\quad\quad\quad\quad\quad \bullet \langle e1 \rangle \frown s\})))
\end{array}
$$

7.5 Theorems

z_head_singleton_thm

$\vdash \forall x : \mathbb{U} \bullet head\ \langle x \rangle = x$

z_head_singleton_⁀_thm

$\vdash \forall x : \mathbb{U};\ xs : (seq\ \_) \bullet head\ (\langle x \rangle \frown xs) = x$

z_tail_singleton_thm

$\vdash \forall x : \mathbb{U} \bullet tail\ \langle x \rangle = \langle\rangle$

z_singleton_⁀_app_thm

$$
\begin{array}{l}
\vdash \forall x : \mathbb{U};\ s : (seq\ \_);\ i : dom\ s \\
\quad\quad \bullet (\langle x \rangle \frown s)\ (1 + i) = s\ i
\end{array}
$$

z_tail_singleton_⁀_thm

$\vdash \forall\ x : \mathbb{U};\ xs : (seq\ \_) \bullet tail\ (\langle x \rangle \frown xs) = xs$

z_∈_seq_⇔_app_eq_thm

$\vdash \forall\ s : (seq\ \_);\ m : dom\ s;\ x : \mathbb{U}$
$\quad \bullet (m,\ x) \in s \Leftrightarrow s\ m = x$

z_⁀_app_eq_thm

$\vdash \forall\ s,\ t : (seq\ \_)$
$\quad \bullet (\forall\ m : dom\ s \bullet (s \frown t)\ m = s\ m)$
$\quad\ \ \wedge (\forall\ n : dom\ t \bullet (s \frown t)\ (n + \#\ s) = t\ n)$

z_singleton_⁀_∈_seq₁_thm

$\vdash \forall\ s : (seq\ \_);\ x : \mathbb{U} \bullet \langle x \rangle \frown s \in (seq_1\ \_)$

z_head_seqd_thm

$\vdash \ulcorner\forall\ x\ l\bullet\ {}_{\mathrm{Z}}\ulcorner head\ \ulcorner\$\text{"}Z'\langle\rangle\text{"}\ (Cons\ x\ l)\urcorner\urcorner = x\urcorner$

z_tail_seqd_thm

$\vdash \ulcorner\forall\ x\ l\bullet\ {}_{\mathrm{Z}}\ulcorner tail\ \ulcorner\$\text{"}Z'\langle\rangle\text{"}\ (Cons\ x\ l)\urcorner\urcorner = {}_{\mathrm{Z}}\ulcorner\ulcorner\$\text{"}Z'\langle\rangle\text{"}\ l\urcorner\urcorner\urcorner$

z_⇸_app_∈_rel_thm

$\vdash \forall\ X : \mathbb{U};\ Y : \mathbb{U};\ f : X \nrightarrow Y;\ x : X$
$\quad \mid x \in dom\ f$
$\quad \bullet (x,\ f\ x) \in f$

z_ifun_dom_eq_ran_eq_thm

$\vdash \forall\ x,\ x',\ y,\ y' : \mathbb{N};\ f : \mathbb{N} \rightarrowtail \mathbb{N}$
$\quad \bullet x = x' \wedge f\ x = y \wedge f\ x' = y' \Rightarrow y = y'$

z_↣_dom_¬_eq_⇒_ran_¬_eq_thm

$\vdash \forall\ x,\ x',\ y,\ y' : \mathbb{N};\ f : \mathbb{N} \rightarrowtail \mathbb{N}$
$\quad \bullet \neg\ x = x' \wedge f\ x = y \wedge f\ x' = y' \Rightarrow \neg\ y = y'$

z_↣_ran_¬_eq_⇒_dom_¬_eq_thm

$\vdash \forall\ x,\ x',\ y,\ y' : \mathbb{N};\ f : \mathbb{N} \rightarrowtail \mathbb{N}$
$\quad \bullet \neg\ y = y' \wedge f\ x = y \wedge f\ x' = y' \Rightarrow \neg\ x = x'$

∃_∧_*distribution_thm*

$\ulcorner\forall\ x$
$\quad \bullet P1\ x \wedge \neg\ P2\ x \wedge \neg\ P3\ x$
$\qquad \vee (P2\ x \wedge \neg\ P1\ x \wedge \neg\ P3\ x)$
$\qquad\ \ \wedge P3\ x$
$\qquad\ \ \wedge \neg\ P1\ x$
$\qquad\ \ \wedge \neg\ P2\ x\urcorner$
$\quad \vdash \ulcorner\exists\ x\bullet\ P1\ x \Rightarrow Q1\ x\urcorner$

$\land \ulcorner \exists\ x \bullet\ P2\ x \Rightarrow Q2\ x \urcorner$
$\land \ulcorner \exists\ x \bullet\ P3\ x \Rightarrow Q3\ x \urcorner$
$\Leftrightarrow \ulcorner \exists\ x$
$\bullet\ (P1\ x \Rightarrow Q1\ x)$
$\land\ (P2\ x \Rightarrow Q2\ x)$
$\land\ (P3\ x \Rightarrow Q3\ x) \urcorner$

z_inocuous_ref_dash_quantification_thm

$\vdash (\forall\ ref', cs : \mathbb{P}\ \mathbb{N}$
$\bullet\ \exists\ ref1, ref2 : \mathbb{P}\ \mathbb{N}$
$\bullet\ ref'$
$= (ref1 \cup ref2) \cap cs \cup (ref1 \cap ref2 \setminus cs))$
$\Leftrightarrow true$

z_⇸_◁_app_idem_thm

$\vdash [X,$
$Y](\forall\ f : X \nrightarrow Y;\ x : \mathbb{U};\ a : \mathbb{U}$
$\mid f \in X \nrightarrow Y \land x \in dom\ f \land x \in a$
$\bullet\ (a \lhd f)\ x = f\ x)$

z_seq_subtype_thm

$\vdash \forall\ S, T : \mathbb{U} \mid S \subseteq T \bullet s \in seq\ S \Rightarrow s \in seq\ T$

z_prefix$_Z$_clauses_thm

$\vdash \forall\ s : (seq\ \_) \bullet \langle\rangle\ prefix_Z\ s$

z_prefix$_Z$_id_thm

$\vdash \forall\ s : (seq\ \_) \bullet s\ prefix_Z\ s$

z_seqdiff$_Z$_thm

$\vdash \forall\ s1, s2 : (seq\ \_)$
$\mid s2\ prefix_Z\ s1$
$\bullet\ s1 -_Z s2 \in (seq\ \_)$

***z_seq_cases_thm*1**

$\vdash [X](\forall\ s : seq\ X$
$\bullet\ s = \langle\rangle \lor (\exists\ s1 : seq\ X;\ x : X \bullet s = s1 \frown \langle x \rangle))$

z_size_seq_cases_thm

$\vdash [X]((\forall\ s : seq\ X \mid \#\ s = 0 \bullet s = \langle\rangle)$
$\land\ (\forall\ s : seq\ X;\ i : \mathbb{N}$
$\mid \#\ s = i + 1$
$\bullet\ \exists\ s1 : seq\ X;\ x : X \bullet \#\ s1 = i \land s = s1 \frown \langle x \rangle))$

***z_⁀_one_one_thm*1**

$\vdash \forall\ s1, t1, s2, t2 : (seq\ \_)$

$| \; \# \; s2 = \# \; t2 \land s1 \frown s2 = t1 \frown t2$
$\bullet \; s1 = t1 \land s2 = t2$

$\boldsymbol{z\_\frown\_one\_one\_thm2}$

$\vdash \forall \; s, \; t, \; r : (seq \; \_) \bullet s \frown t = s \frown r \Leftrightarrow t = r$

$\boldsymbol{z\_\frown\_unit\_thm} \vdash \forall \; s, \; t : (seq \; \_) \bullet s = s \frown t \Leftrightarrow t = \langle\rangle$

$\boldsymbol{z\_seqdiff_Z\_zero\_thm}$

$\vdash \forall \; s : (seq \; \_) \bullet s -_Z s = \langle\rangle$

$\boldsymbol{z\_seqdiff_Z\_zero\_thm1}$

$\vdash \forall \; s1, \; s2 : (seq \; \_)$
$| \; s2 \; prefix_Z \; s1 \land s1 -_Z s2 = \langle\rangle$
$\bullet \; s1 = s2$

8 THE Z THEORY utp-rel

8.1 Parents

$utp{-}z{-}library$

8.2 Global Variables

$\boldsymbol{NAME}$	$\mathbb{P}\ NAME$
$\boldsymbol{any\_name}$	$NAME$
$\boldsymbol{ALPHABET}$	$\mathbb{P}\ (\mathbb{P}\ NAME)$
$\boldsymbol{dash}$	$NAME \leftrightarrow NAME$
$\boldsymbol{one}$	$NAME \leftrightarrow NAME$
$\boldsymbol{two}$	$NAME \leftrightarrow NAME$
$\boldsymbol{dashed}$	$\mathbb{P}\ NAME$
$\boldsymbol{undashed}$	$\mathbb{P}\ NAME$
$\boldsymbol{in\_a}$	$\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME$
$\boldsymbol{out\_a}$	$\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME$
$\boldsymbol{homogeneous}$	$\mathbb{P}\ (\mathbb{P}\ NAME)$
$\boldsymbol{composable}$	$\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME$
$\boldsymbol{VALUE}$	$\mathbb{P}\ VALUE$
$\boldsymbol{Int}$	$\mathbb{Z} \leftrightarrow VALUE$
$\boldsymbol{Bool}$	$\mathbb{B} \leftrightarrow VALUE$
$\boldsymbol{Channel}$	$NAME \leftrightarrow VALUE$
$\boldsymbol{Seq}$	$(\mathbb{Z} \leftrightarrow VALUE) \leftrightarrow VALUE$
$\boldsymbol{Set}$	$\mathbb{P}\ VALUE \leftrightarrow VALUE$
$\boldsymbol{Pair}$	$VALUE \times VALUE \leftrightarrow VALUE$
$\boldsymbol{Sync}$	$VALUE$
$\boldsymbol{INT\_VAL}$	$\mathbb{P}\ VALUE$
$\boldsymbol{BOOL\_VAL}$	$\mathbb{P}\ VALUE$
$\boldsymbol{CHANNEL\_VAL}$	$\mathbb{P}\ VALUE$
$\boldsymbol{SEQ\_VAL}$	$\mathbb{P}\ VALUE$
$\boldsymbol{SET\_VAL}$	$\mathbb{P}\ VALUE$
$\boldsymbol{PAIR\_VAL}$	$\mathbb{P}\ VALUE$
$\boldsymbol{EVENT\_VAL}$	$\mathbb{P}\ VALUE$
$\boldsymbol{SEQ\_EVENT\_VAL}$	$\mathbb{P}\ VALUE$
$\boldsymbol{SET\_EVENT\_VAL}$	

$\mathbb{P}\ VALUE$

$\boldsymbol{SET\_SEQ\_EVENT\_VAL}$ $\mathbb{P}\ VALUE$

$\boldsymbol{PAIR\_SEQ\_EVENT\_VAL}$ $\mathbb{P}\ VALUE$

$\boldsymbol{UNARY\_F}$ $\mathbb{P}\ (VALUE \leftrightarrow VALUE)$

$\boldsymbol{any\_un\_fun}$ $VALUE \leftrightarrow VALUE$

$\boldsymbol{BINARY\_F}$ $\mathbb{P}\ (VALUE \times VALUE \leftrightarrow VALUE)$

$\boldsymbol{any\_bin\_fun}$ $VALUE \times VALUE \leftrightarrow VALUE$

$\boldsymbol{RELATION}$ $\mathbb{P}\ (VALUE \leftrightarrow VALUE)$

$\boldsymbol{any\_rel}$ $VALUE \leftrightarrow VALUE$

$\boldsymbol{EXPRESSION}$ $\mathbb{P}\ EXPRESSION$

$\boldsymbol{Val}$ $VALUE \leftrightarrow EXPRESSION$

$\boldsymbol{Var}$ $NAME \leftrightarrow EXPRESSION$

$\boldsymbol{Fun_1}$ $(VALUE \leftrightarrow VALUE) \times EXPRESSION \leftrightarrow EXPRESSION$

$\boldsymbol{Fun_2}$ $(VALUE \times VALUE \leftrightarrow VALUE) \times EXPRESSION \times EXPRESSION \leftrightarrow EXPRESSION$

$\boldsymbol{Rel}$ $(VALUE \leftrightarrow VALUE) \times EXPRESSION \times EXPRESSION \leftrightarrow EXPRESSIO$

$\boldsymbol{BINDING}$ $\mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{BINDINGS}$ $\mathbb{P}\ (\mathbb{P}\ (NAME \leftrightarrow VALUE))$

$\boldsymbol{FV}$ $EXPRESSION \leftrightarrow \mathbb{P}\ NAME$

$\boldsymbol{WF\_BINDING\_EXPRESSION_R}$ $(NAME \leftrightarrow VALUE) \leftrightarrow EXPRESSION$

$\boldsymbol{Eval}$ $(NAME \leftrightarrow VALUE) \times EXPRESSION \leftrightarrow VALUE$

$\boldsymbol{REL\_PREDICATE}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{UnrestVar}$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME$

$\boldsymbol{unrestTypedVar}$ $(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times NAME \times \mathbb{P}\ VALUE \leftrightarrow \mathbb{B}$

$\boldsymbol{REL\_CONDITION}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{dashCond}$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{U}$ $(NAME \leftrightarrow NAME) \times \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{WF\_Equals_R}$ $\mathbb{P}\ (\mathbb{P}\ NAME \times NAME \times EXPRESSION)$

$\boldsymbol{WF\_ALPHABET\_EXPRESSION}$ $\mathbb{P}\ (\mathbb{P}\ NAME \times EXPRESSION \times EXPRESSION)$

$\boldsymbol{WF\_Cond_R}$ $\mathbb{P}$ $((\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$

$\qquad\qquad \times (\mathbb{P}\ \mathit{NAME} \times \mathbb{P}\ (\mathit{NAME} \leftrightarrow \mathit{VALUE}))$
$\qquad\qquad \times (\mathbb{P}\ \mathit{NAME} \times \mathbb{P}\ (\mathit{NAME} \leftrightarrow \mathit{VALUE})))$
$\boldsymbol{WF\_Semi_R} \quad \mathbb{P}\ \mathit{NAME} \times \mathbb{P}\ (\mathit{NAME} \leftrightarrow \mathit{VALUE}) \leftrightarrow \mathbb{P}\ \mathit{NAME} \times \mathbb{P}\ (\mathit{NAME} \leftrightarrow \mathit{VALUE})$
$\boldsymbol{WF\_Skip_R} \quad \mathbb{P}\ (\mathbb{P}\ \mathit{NAME})$
$\boldsymbol{WF\_Assign_R} \quad \mathbb{P}\ (\mathbb{P}\ \mathit{NAME} \times (\mathbb{Z} \leftrightarrow \mathit{NAME}) \times (\mathbb{Z} \leftrightarrow \mathit{EXPRESSION}))$
$\boldsymbol{WF\_Subst_R} \quad \mathbb{P}\ ((\mathbb{P}\ \mathit{NAME} \times \mathbb{P}\ (\mathit{NAME} \leftrightarrow \mathit{VALUE})) \times \mathit{EXPRESSION} \times \mathit{NAME})$
$\boldsymbol{WF\_Var_{R\_EndR}}$
$\qquad \mathbb{P}\ \mathit{NAME} \leftrightarrow \mathit{NAME}$
$\boldsymbol{WF\_VarT_{R\_EndTR}}$
$\qquad \mathbb{P}\ (\mathbb{P}\ \mathit{NAME} \times \mathit{NAME} \times \mathit{VALUE})$
$\boldsymbol{WF\_Extend\_rest_R}$
$\qquad \mathbb{P}\ \mathit{NAME} \times \mathbb{P}\ (\mathit{NAME} \leftrightarrow \mathit{VALUE}) \leftrightarrow \mathbb{P}\ \mathit{NAME}$
$\boldsymbol{WF\_REL\_PREDICATE\_PAIR}$
$\qquad \mathbb{P}\ \mathit{NAME} \times \mathbb{P}\ (\mathit{NAME} \leftrightarrow \mathit{VALUE}) \leftrightarrow \mathbb{P}\ \mathit{NAME} \times \mathbb{P}\ (\mathit{NAME} \leftrightarrow \mathit{VALUE})$
$\boldsymbol{WF\_Glb_{R\_LubR}}$
$\qquad \mathbb{P}\ \mathit{NAME} \leftrightarrow \mathbb{P}\ \mathit{NAME} \leftrightarrow \mathbb{P}\ (\mathit{NAME} \leftrightarrow \mathit{VALUE})$
$(\_ \leq_{\boldsymbol{R}} \_) \quad \mathit{VALUE} \leftrightarrow \mathit{VALUE}$
$(\_ <_{\boldsymbol{R}} \_) \quad \mathit{VALUE} \leftrightarrow \mathit{VALUE}$
$(\_ \in_{\boldsymbol{R}} \_) \quad \mathit{VALUE} \leftrightarrow \mathit{VALUE}$
$(\_ \notin_{\boldsymbol{R}} \_) \quad \mathit{VALUE} \leftrightarrow \mathit{VALUE}$
$(\_ \subseteq_{\boldsymbol{R}} \_) \quad \mathit{VALUE} \leftrightarrow \mathit{VALUE}$
$\boldsymbol{MkSingleton} \quad \mathit{VALUE} \leftrightarrow \mathit{VALUE}$
$\boldsymbol{MkPair} \quad \mathit{VALUE} \times \mathit{VALUE} \leftrightarrow \mathit{VALUE}$
$(\_\ \boldsymbol{SeqDif_R}\ \_)$
$\qquad \mathit{VALUE} \times \mathit{VALUE} \leftrightarrow \mathit{VALUE}$
$(\_ \frown_{\boldsymbol{R}} \_) \quad \mathit{VALUE} \times \mathit{VALUE} \leftrightarrow \mathit{VALUE}$
$(\_ \upharpoonright_{\boldsymbol{R}} \_) \quad \mathit{VALUE} \times \mathit{VALUE} \leftrightarrow \mathit{VALUE}$
$(\_ \cup_{\boldsymbol{R}} \_) \quad \mathit{VALUE} \times \mathit{VALUE} \leftrightarrow \mathit{VALUE}$
$(\_ \cap_{\boldsymbol{R}} \_) \quad \mathit{VALUE} \times \mathit{VALUE} \leftrightarrow \mathit{VALUE}$
$(\_ \setminus_{\boldsymbol{R}} \_) \quad \mathit{VALUE} \times \mathit{VALUE} \leftrightarrow \mathit{VALUE}$
$\boldsymbol{True_R} \quad \mathbb{P}\ \mathit{NAME} \leftrightarrow \mathbb{P}\ \mathit{NAME} \times \mathbb{P}\ (\mathit{NAME} \leftrightarrow \mathit{VALUE})$
$\boldsymbol{False_R} \quad \mathbb{P}\ \mathit{NAME} \leftrightarrow \mathbb{P}\ \mathit{NAME} \times \mathbb{P}\ (\mathit{NAME} \leftrightarrow \mathit{VALUE})$
$(\_ \equiv_{\boldsymbol{R}} \_) \quad (\mathbb{P}\ \mathit{NAME} \times \mathbb{P}\ (\mathit{NAME} \leftrightarrow \mathit{VALUE}))$
$\qquad\qquad \times (\mathbb{P}\ \mathit{NAME} \times \mathbb{P}\ (\mathit{NAME} \leftrightarrow \mathit{VALUE}))$
$\qquad\qquad \leftrightarrow \mathbb{P}\ \mathit{NAME} \times \mathbb{P}\ (\mathit{NAME} \leftrightarrow \mathit{VALUE})$
$=_{\boldsymbol{R}} \quad \mathbb{P}\ \mathit{NAME} \times \mathit{NAME} \times \mathit{EXPRESSION} \leftrightarrow \mathbb{P}\ \mathit{NAME} \times \mathbb{P}\ (\mathit{NAME} \leftrightarrow \mathit{VALU}$
$=_{+\boldsymbol{R}} \quad \mathbb{P}\ \mathit{NAME} \times \mathit{EXPRESSION} \times \mathit{EXPRESSION}$

$\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\neg_{\boldsymbol{R}}$	$\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$(\_ \oplus_{\boldsymbol{R}} \_)$	$(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times \mathbb{P}\ NAME$ $\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$(\_ \wedge_{\boldsymbol{R}} \_)$	$(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$(\_ \vee_{\boldsymbol{R}} \_)$	$(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$(\_ \Rightarrow_{\boldsymbol{R}} \_)$	$(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$(\_ \Leftrightarrow_{\boldsymbol{R}} \_)$	$(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$(\_ \lhd_{\boldsymbol{R}} \_ \rhd_{\boldsymbol{R}} \_)$	
	$(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$(\_ ;_{\boldsymbol{R}} \_)$	$(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{\Pi_R}$	$\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{Assign_R}$	$\mathbb{P}\ NAME \times (\mathbb{Z} \leftrightarrow NAME) \times (\mathbb{Z} \leftrightarrow EXPRESSION)$ $\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$(\_ -_{\boldsymbol{R}} \_)$	$(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times \mathbb{P}\ NAME$ $\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\exists_{-\boldsymbol{R}}$	$\mathbb{P}\ NAME \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\forall_{-\boldsymbol{R}}$	$\mathbb{P}\ NAME \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\exists_{\boldsymbol{R}}$	$\mathbb{P}\ NAME \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\forall_{\boldsymbol{R}}$	$\mathbb{P}\ NAME \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$ $\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$/_{\boldsymbol{R}}$	$(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times EXPRESSION \times NAME$

$\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_\ \boldsymbol{intchoice_R}\ \_)$

$(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_\ \boldsymbol{conj_R}\ \_)$ $(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{var_R}$ $\mathbb{P}\ NAME \times NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{end_R}$ $\mathbb{P}\ NAME \times NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_ +_{\boldsymbol{R}} \_)$ $(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times \mathbb{P}\ NAME$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\langle_{\boldsymbol{R}}\ \_\ \rangle_{\boldsymbol{R}})$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_ \sqsubseteq_{\boldsymbol{R}} \_)$ $(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{monotonic}$ $\mathbb{P}$
$(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE$

$\boldsymbol{Bot_R}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{Top_R}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\bigcap_{\boldsymbol{R}}$ $\mathbb{P}\ NAME \times (\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\bigcup_{\boldsymbol{R}}$ $\mathbb{P}\ NAME \times (\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{REL\_FUNCTION}$ $\mathbb{P}$
$(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE$

$\boldsymbol{\mu_R}$ $(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{\nu_R}$ $(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{varT_R}$ $\mathbb{P}\ NAME \times NAME \times VALUE \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{endT_R}$ $\mathbb{P}\ NAME \times NAME \times VALUE \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

8.3 Fixity

$\boldsymbol{fun}\ \mathbf{0}\ \boldsymbol{rightassoc}$

$(\_\ conj_R\ \_)$ $(\_ \cap_R \_)$ $(\_ \sqsubseteq_R \_)$
$(\_\ intchoice_R\ \_)$ $(\_ \Leftrightarrow_R \_)$ $(\_ \equiv_R \_)$

$$
\begin{array}{lllll}
(\_\ SeqDif_R\ \_) & (\_\ \oplus_R\ \_) & (\_\ {}^\frown{}_R\ \_) & & \\
(\_\ +_R\ \_) & (\_\ \wedge_R\ \_) & (\_\ \lhd_R\ \_\ \rhd_R\ \_) & & \\
(\_\ -_R\ \_) & (\_\ \vee_R\ \_) & (\_\ \upharpoonright_R\ \_) & & \\
(\_\ ;_R\ \_) & (\_\ \Rightarrow_R\ \_) & (\langle_R\ \_\ \rangle_R) & & \\
(\_\ \backslash_R\ \_) & (\_\ \cup_R\ \_) & & &
\end{array}
$$

$$
\textbf{\textit{rel}} \quad (\_\ <_R\ \_) \quad (\_\ \subseteq_R\ \_) \quad (\_\ \in_R\ \_) \quad (\_\ \notin_R\ \_) \quad (\_\ \leq_R\ \_)
$$

8.4 Axioms

$$
\begin{array}{ll}
\textbf{\textit{any\_name}} & \vdash any\_name \in NAME \wedge true \\
\textbf{\textit{dash}} & \vdash dash \in NAME \rightarrowtail NAME \wedge true \\
\textbf{\textit{one}} & \\
\textbf{\textit{two}} & \vdash \{one,\ two\} \subseteq NAME \rightarrowtail NAME \wedge \operatorname{ran} one \cap \operatorname{ran} two = \varnothing \\
\textbf{\textit{dashed}} & \vdash dashed \in ALPHABET \wedge dashed = \operatorname{ran} dash \\
\textbf{\textit{undashed}} & \vdash undashed \in ALPHABET \\
 & \quad \wedge\ undashed = \{n : NAME \mid n \notin \operatorname{ran} dash\} \\
\textbf{\textit{in\_a}} & \vdash in\_a \in ALPHABET \rightarrow ALPHABET \\
 & \quad \wedge\ (\forall\ a : ALPHABET \bullet in\_a\ a = a \cap undashed) \\
\textbf{\textit{out\_a}} & \vdash out\_a \in ALPHABET \rightarrow ALPHABET \\
 & \quad \wedge\ (\forall\ a : ALPHABET \bullet out\_a\ a = a \cap dashed) \\
\textbf{\textit{homogeneous}} & \vdash homogeneous \in \mathbb{P}\ ALPHABET \\
 & \quad \wedge\ homogeneous \\
 & \qquad = \{a : ALPHABET \\
 & \qquad\quad \mid \forall\ n : undashed \bullet n \in a \Leftrightarrow dash\ n \in a\} \\
\textbf{\textit{composable}} & \vdash composable \in \mathbb{P}\ (ALPHABET \times ALPHABET) \\
 & \quad \wedge\ composable \\
 & \qquad = \{a1,\ a2 : ALPHABET \\
 & \qquad\quad \mid \forall\ n : undashed \bullet n \in a2 \Leftrightarrow dash\ n \in a1\} \\
\textbf{\textit{Int}} & \\
\textbf{\textit{Bool}} & \\
\textbf{\textit{Channel}} & \\
\textbf{\textit{Seq}} & \\
\textbf{\textit{Set}} & \\
\textbf{\textit{Pair}} & \\
\textbf{\textit{Sync}} & \vdash (Sync \in VALUE \\
 & \quad \wedge\ Int \in \mathbb{Z} \rightarrowtail VALUE
\end{array}
$$

$$
\begin{array}{ll}
 & \land\ Bool \in \mathbb{B} \rightarrowtail VALUE \\
 & \land\ Channel \in NAME \rightarrowtail VALUE \\
 & \land\ Seq \in \mathrm{seq}\ VALUE \rightarrowtail VALUE \\
 & \land\ Set \in \mathbb{P}\ VALUE \rightarrowtail VALUE \\
 & \land\ Pair \in VALUE \times VALUE \rightarrowtail VALUE) \\
 & \land\ disjoint\ \langle \mathrm{ran}\ Int, \\
 & \quad \mathrm{ran}\ Bool, \\
 & \quad \mathrm{ran}\ Channel, \\
 & \quad \mathrm{ran}\ Seq, \\
 & \quad \mathrm{ran}\ Set, \\
 & \quad \mathrm{ran}\ Pair, \\
 & \quad \{Sync\}\rangle \\
 & \land\ (\forall\ W : \mathbb{P}\ VALUE \\
 & \quad \mid \{Sync\} \\
 & \qquad\quad \cup\ (Int\ (\!|\ \mathbb{Z}\ |\!) \\
 & \qquad\qquad \cup\ (Bool\ (\!|\ \mathbb{B}\ |\!) \\
 & \qquad\qquad\quad \cup\ (Channel\ (\!|\ NAME\ |\!) \\
 & \qquad\qquad\qquad \cup\ (Seq\ (\!|\ \mathrm{seq}\ W\ |\!) \\
 & \qquad\qquad\qquad\quad \cup\ (Set\ (\!|\ \mathbb{P}\ W\ |\!) \\
 & \qquad\qquad\qquad\qquad \cup\ Pair\ (\!|\ W \times W\ |\!)))))) \\
 & \qquad \subseteq W \\
 & \quad \bullet\ VALUE \subseteq W) \\
\boldsymbol{Constraint\ 1} & \vdash \forall\ f : UNARY\_F;\ v : VALUE \bullet f\ v \in VALUE \\
\boldsymbol{any\_un\_fun} & \vdash any\_un\_fun \in UNARY\_F \land true \\
\boldsymbol{Constraint\ 2} & \vdash \forall\ f : BINARY\_F;\ vv : VALUE \times VALUE \bullet f\ vv \in VALUE \\
\boldsymbol{any\_bin\_fun} & \vdash any\_bin\_fun \in BINARY\_F \land true \\
\boldsymbol{any\_rel} & \vdash any\_rel \in RELATION \land true \\
\boldsymbol{Val} & \\
\boldsymbol{Var} & \\
\boldsymbol{Fun_1} & \\
\boldsymbol{Fun_2} & \\
\boldsymbol{Rel} & \vdash (Val \in VALUE \rightarrowtail EXPRESSION \\
 & \quad \land\ Var \in NAME \rightarrowtail EXPRESSION \\
 & \quad \land\ Fun_1 \in UNARY\_F \times EXPRESSION \rightarrowtail EXPRESSION \\
 & \quad \land\ Fun_2 \\
 & \qquad \in BINARY\_F \times EXPRESSION \times EXPRESSION \rightarrowtail EXPRESSION \\
 & \quad \land\ Rel \\
 & \qquad \in RELATION \times EXPRESSION \times EXPRESSION
\end{array}
$$

$$
\begin{array}{ll}
 & \qquad\qquad \rightarrowtail \mathit{EXPRESSION}) \\
 & \quad \land\ \mathit{disjoint}\ \langle \mathit{ran}\ \mathit{Val}, \\
 & \qquad \mathit{ran}\ \mathit{Var}, \\
 & \qquad \mathit{ran}\ \mathit{Fun}_1, \\
 & \qquad \mathit{ran}\ \mathit{Fun}_2, \\
 & \qquad \mathit{ran}\ \mathit{Rel}\rangle \\
 & \quad \land\ (\forall\ W : \mathbb{P}\ \mathit{EXPRESSION} \\
 & \quad\ \mid \mathit{Val}\ (\!|\ \mathit{VALUE}\ |\!) \\
 & \qquad\qquad \cup\ (\mathit{Var}\ (\!|\ \mathit{NAME}\ |\!) \\
 & \qquad\qquad\quad \cup\ (\mathit{Fun}_1\ (\!|\ \mathit{UNARY\_F} \times W\ |\!) \\
 & \qquad\qquad\qquad \cup\ (\mathit{Fun}_2\ (\!|\ \mathit{BINARY\_F} \times W \times W\ |\!) \\
 & \qquad\qquad\qquad\quad \cup\ \mathit{Rel}\ (\!|\ \mathit{RELATION} \times W \times W\ |\!)))) \\
 & \qquad\quad \subseteq W \\
 & \quad\ \bullet\ \mathit{EXPRESSION} \subseteq W) \\
\textbf{\textit{FV}} & \vdash \mathit{FV} \in \mathit{EXPRESSION} \rightarrow \mathbb{P}\ \mathit{NAME} \\
 & \quad \land\ (\forall\ v : \mathit{VALUE}; \\
 & \qquad n : \mathit{NAME}; \\
 & \qquad \mathit{exp1}, \mathit{exp2} : \mathit{EXPRESSION}; \\
 & \qquad \mathit{f1} : \mathit{UNARY\_F}; \\
 & \qquad \mathit{f2} : \mathit{BINARY\_F}; \\
 & \qquad r : \mathit{RELATION} \\
 & \quad\ \bullet\ \mathit{FV}\ (\mathit{Val}\ v) = \varnothing \\
 & \qquad \land\ \mathit{FV}\ (\mathit{Var}\ n) = \{n\} \\
 & \qquad \land\ \mathit{FV}\ (\mathit{Fun}_1\ (\mathit{f1}, \mathit{exp1})) = \mathit{FV}\ \mathit{exp1} \\
 & \qquad \land\ \mathit{FV}\ (\mathit{Fun}_2\ (\mathit{f2}, \mathit{exp1}, \mathit{exp2})) \\
 & \qquad\quad = \mathit{FV}\ \mathit{exp1} \cup \mathit{FV}\ \mathit{exp2} \\
 & \qquad \land\ \mathit{FV}\ (\mathit{Rel}\ (r, \mathit{exp1}, \mathit{exp2})) = \mathit{FV}\ \mathit{exp1} \cup \mathit{FV}\ \mathit{exp2}) \\
\textbf{\textit{Eval}} & \vdash \mathit{Eval} \in \mathit{WF\_BINDING\_EXPRESSION}_R \rightarrow \mathit{VALUE} \\
 & \quad \land\ (\forall\ b : \mathit{BINDING}; \\
 & \qquad v : \mathit{VALUE}; \\
 & \qquad n : \mathit{NAME}; \\
 & \qquad \mathit{exp1}, \mathit{exp2} : \mathit{EXPRESSION}; \\
 & \qquad \mathit{f1} : \mathit{UNARY\_F}; \\
 & \qquad \mathit{f2} : \mathit{BINARY\_F}; \\
 & \qquad r : \mathit{RELATION} \\
 & \quad\ \bullet\ \mathit{Eval}\ (b, \mathit{Val}\ v) = v \\
 & \qquad \land\ ((b, \mathit{Var}\ n) \in \mathit{WF\_BINDING\_EXPRESSION}_R \\
 & \qquad\quad \Rightarrow \mathit{Eval}\ (b, \mathit{Var}\ n) = b\ n)
\end{array}
$$

$$
\begin{array}{l}
\land ((b, exp1) \in WF\_BINDING\_EXPRESSION_R \\
\quad \Rightarrow Eval\ (b, Fun_1\ (f1, exp1)) \\
\quad\quad = f1\ (Eval\ (b, exp1))) \\
\land ((b, exp1) \in WF\_BINDING\_EXPRESSION_R \\
\quad\quad \land (b, exp2) \in WF\_BINDING\_EXPRESSION_R \\
\quad \Rightarrow Eval\ (b, Fun_2\ (f2, exp1, exp2)) \\
\quad\quad = f2\ (Eval\ (b, exp1), Eval\ (b, exp2))) \\
\land ((b, exp1) \in WF\_BINDING\_EXPRESSION_R \\
\quad\quad \land (b, exp2) \in WF\_BINDING\_EXPRESSION_R \\
\quad \Rightarrow Eval\ (b, Rel\ (r, exp1, exp2)) \\
\quad\quad = Bool \\
\quad\quad\quad ((Eval\ (b, exp1), Eval\ (b, exp2)) \\
\quad\quad\quad\quad \in r)))
\end{array}
$$

UnrestVar $\vdash UnrestVar \in REL\_PREDICATE \rightarrow \mathbb{P}\ NAME$

$$
\begin{array}{l}
\land (\forall\ u : REL\_PREDICATE \\
\quad \bullet\ UnrestVar\ u \\
\quad\quad = \{n : u.1 \\
\quad\quad\quad \mid \forall\ b : u.2;\ v : VALUE \bullet b \oplus \{n \mapsto v\} \in u.2\})
\end{array}
$$

unrestTypedVar

$$
\begin{array}{l}
\vdash unrestTypedVar \in REL\_PREDICATE \times NAME \times \mathbb{P}\ VALUE \rightarrow \mathbb{B} \\
\quad \land (\forall\ r : REL\_PREDICATE;\ n : NAME;\ T : \mathbb{P}\ VALUE \\
\quad\quad \bullet\ unrestTypedVar\ (r, n, T) \\
\quad\quad\quad \Leftrightarrow (\forall\ b : r.2;\ v : T \bullet b \oplus \{n \mapsto v\} \in r.2))
\end{array}
$$

REL_CONDITION

$$
\begin{array}{l}
\vdash REL\_CONDITION \in \mathbb{P}\ REL\_PREDICATE \\
\quad \land REL\_CONDITION \\
\quad\quad = \{r : REL\_PREDICATE \\
\quad\quad\quad \mid r.1 \setminus undashed \subseteq UnrestVar\ r\}
\end{array}
$$

dashCond $\vdash dashCond \in REL\_CONDITION \rightarrow REL\_PREDICATE$

$$
\begin{array}{l}
\land (\forall\ u : REL\_CONDITION \\
\quad \bullet\ dashCond\ u \\
\quad\quad = (\{n : u.1 \mid n \in undashed \bullet dash\ n\} \cup u.1, \\
\quad\quad\quad \{b : u.2 \\
\quad\quad\quad\quad \bullet \{n : dom\ b \cap undashed \\
\quad\quad\quad\quad\quad \bullet\ dash\ n \mapsto b\ n\} \\
\quad\quad\quad\quad\quad \cup \{n : dash\ (\!|\ dom\ b \cap dashed\ |\!) \\
\quad\quad\quad\quad\quad \bullet\ n \mapsto b\ (dash\ n)\}\}))
\end{array}
$$

U $\vdash U \in (NAME \rightarrowtail NAME) \times ALPHABET \twoheadrightarrow REL\_PREDICATE$

$$
\begin{array}{l}
\land (\forall f : NAME \rightarrowtail NAME; a' : ALPHABET \\
\quad | a' \subseteq dashed \\
\quad \bullet \exists a : ALPHABET \\
\quad\quad | a \subseteq undashed \land a' = dash \limits⦇ a ⦈ \\
\quad\quad \bullet U (f, a') \\
\quad\quad\quad = (\{n : NAME \mid n \in a \bullet dash (f\ n)\} \cup a, \\
\quad\quad\quad\quad \{b : BINDING \\
\quad\quad\quad\quad\quad | dom\ b \\
\quad\quad\quad\quad\quad\quad\quad = \{n : NAME \mid n \in a \bullet dash (f\ n)\} \cup a \\
\quad\quad\quad\quad\quad\quad \land (\forall n : NAME \\
\quad\quad\quad\quad\quad\quad\quad | n \in a \\
\quad\quad\quad\quad\quad\quad\quad \bullet b (dash (f\ n)) = b\ n)\}))
\end{array}
$$

$\_ \leq_{\boldsymbol{R}} \_$

$$
\begin{array}{l}
\vdash (\_ \leq_R \_) \in VALUE \leftrightarrow VALUE \\
\quad \land (\_ \leq_R \_) \\
\quad\quad = \{s1, s2 : SEQ\_VAL \\
\quad\quad\quad | (Seq \sim) s1\ prefix_Z\ (Seq \sim)\ s2\}
\end{array}
$$

$\_ <_{\boldsymbol{R}} \_$

$$
\begin{array}{l}
\vdash (\_ <_R \_) \in VALUE \leftrightarrow VALUE \\
\quad \land (\_ <_R \_) \\
\quad\quad = \{s1, s2 : SEQ\_VAL \\
\quad\quad\quad | (Seq \sim) s1\ prefix_Z\ (Seq \sim)\ s2 \\
\quad\quad\quad\quad \land (Seq \sim)\ s1 \neq (Seq \sim)\ s2\}
\end{array}
$$

$\_ \in_{\boldsymbol{R}} \_$

$$
\begin{array}{l}
\vdash (\_ \in_R \_) \in VALUE \leftrightarrow VALUE \\
\quad \land (\_ \in_R \_) \\
\quad\quad = \{e : VALUE; s : SET\_VAL \\
\quad\quad\quad | e \in (Set \sim)\ s\}
\end{array}
$$

$\_ \notin_{\boldsymbol{R}} \_$

$$
\begin{array}{l}
\vdash (\_ \notin_R \_) \in VALUE \leftrightarrow VALUE \\
\quad \land (\_ \notin_R \_) \\
\quad\quad = \{e : VALUE; s : SET\_VAL \\
\quad\quad\quad | e \notin (Set \sim)\ s\}
\end{array}
$$

$\_ \subseteq_{\boldsymbol{R}} \_$

$$
\begin{array}{l}
\vdash (\_ \subseteq_R \_) \in VALUE \leftrightarrow VALUE \\
\quad \land (\_ \subseteq_R \_) \\
\quad\quad = \{s1, s2 : SET\_VAL \\
\quad\quad\quad | (Set \sim)\ s1 \subseteq (Set \sim)\ s2\}
\end{array}
$$

MkSingleton

$$
\begin{array}{l}
\vdash MkSingleton \in VALUE \rightarrow VALUE \\
\quad \land (\forall v : VALUE \bullet MkSingleton\ v = Seq \langle v \rangle)
\end{array}
$$

MkPair

$$
\begin{array}{l}
\vdash MkPair \in VALUE \times VALUE \rightarrow VALUE \\
\quad \land (\forall v1, v2 : VALUE \\
\quad\quad \bullet MkPair (v1, v2) = Pair (v1, v2))
\end{array}
$$

$$
\begin{array}{ll}
\_\ \boldsymbol{SeqDif_R}\ \_ & \vdash (\_\ \mathit{SeqDif}_R\ \_) \in \mathit{VALUE} \times \mathit{VALUE} \nrightarrow \mathit{VALUE} \\
& \quad \land (\forall\ s1, s2 : \mathit{VALUE} \\
& \qquad \mid \{s1, s2\} \subseteq \mathit{SEQ\_VAL} \\
& \qquad\quad \land (\mathit{Seq}\ \sim)\ s2\ \mathit{prefix}_Z\ (\mathit{Seq}\ \sim)\ s1 \\
& \qquad \bullet s1\ \mathit{SeqDif}_R\ s2 \\
& \qquad\quad = \mathit{Seq}\ ((\mathit{Seq}\ \sim)\ s1 -_Z (\mathit{Seq}\ \sim)\ s2)) \\
\_\ \frown_{\boldsymbol{R}}\ \_ & \vdash (\_\ \frown_R\ \_) \in \mathit{VALUE} \times \mathit{VALUE} \nrightarrow \mathit{VALUE} \\
& \quad \land (\forall\ s1, s2 : \mathit{VALUE} \\
& \qquad \mid \{s1, s2\} \subseteq \mathit{SEQ\_VAL} \\
& \qquad \bullet s1 \frown_R s2 = \mathit{Seq}\ ((\mathit{Seq}\ \sim)\ s1 \frown (\mathit{Seq}\ \sim)\ s2)) \\
\_\ \upharpoonright_{\boldsymbol{R}}\ \_ & \vdash (\_\ \upharpoonright_R\ \_) \in \mathit{VALUE} \times \mathit{VALUE} \nrightarrow \mathit{VALUE} \\
& \quad \land (\forall\ s, st : \mathit{VALUE} \\
& \qquad \mid s \in \mathit{SEQ\_VAL} \land st \in \mathit{SET\_VAL} \\
& \qquad \bullet s \upharpoonright_R st = \mathit{Seq}\ ((\mathit{Seq}\ \sim)\ s \upharpoonright (\mathit{Set}\ \sim)\ st)) \\
\_\ \cup_{\boldsymbol{R}}\ \_ & \vdash (\_\ \cup_R\ \_) \in \mathit{VALUE} \times \mathit{VALUE} \nrightarrow \mathit{VALUE} \\
& \quad \land (\forall\ s1, s2 : \mathit{VALUE} \\
& \qquad \mid \{s1, s2\} \subseteq \mathit{SET\_VAL} \\
& \qquad \bullet s1 \cup_R s2 = \mathit{Set}\ ((\mathit{Set}\ \sim)\ s1 \cup (\mathit{Set}\ \sim)\ s2)) \\
\_\ \cap_{\boldsymbol{R}}\ \_ & \vdash (\_\ \cap_R\ \_) \in \mathit{VALUE} \times \mathit{VALUE} \nrightarrow \mathit{VALUE} \\
& \quad \land (\forall\ s1, s2 : \mathit{VALUE} \\
& \qquad \mid \{s1, s2\} \subseteq \mathit{SET\_VAL} \\
& \qquad \bullet s1 \cap_R s2 = \mathit{Set}\ ((\mathit{Set}\ \sim)\ s1 \cap (\mathit{Set}\ \sim)\ s2)) \\
\_\ \setminus_{\boldsymbol{R}}\ \_ & \vdash (\_\ \setminus_R\ \_) \in \mathit{VALUE} \times \mathit{VALUE} \nrightarrow \mathit{VALUE} \\
& \quad \land (\forall\ s1, s2 : \mathit{VALUE} \\
& \qquad \mid \{s1, s2\} \subseteq \mathit{SET\_VAL} \\
& \qquad \bullet s1 \setminus_R s2 = \mathit{Set}\ ((\mathit{Set}\ \sim)\ s1 \setminus (\mathit{Set}\ \sim)\ s2)) \\
\boldsymbol{True_R} & \vdash \mathit{True}_R \in \mathit{ALPHABET} \rightarrow \mathit{REL\_PREDICATE} \\
& \quad \land (\forall\ a : \mathit{ALPHABET} \\
& \qquad \bullet \mathit{True}_R\ a = (a, \{b : \mathit{BINDING} \mid \mathrm{dom}\ b = a\})) \\
\boldsymbol{False_R} & \vdash \mathit{False}_R \in \mathit{ALPHABET} \rightarrow \mathit{REL\_PREDICATE} \\
& \quad \land (\forall\ a : \mathit{ALPHABET} \bullet \mathit{False}_R\ a = (a, \varnothing)) \\
\_\ \equiv_{\boldsymbol{R}}\ \_ & \vdash (\_\ \equiv_R\ \_) \\
& \qquad \in \mathit{REL\_PREDICATE} \times \mathit{REL\_PREDICATE} \rightarrow \mathit{REL\_PREDICATE} \\
& \quad \land (\forall\ u1, u2 : \mathit{REL\_PREDICATE} \\
& \qquad \bullet (u1.1 = u2.1 \land u1.2 = u2.2 \\
& \qquad\qquad \Rightarrow u1 \equiv_R u2 = \mathit{True}_R\ u1.1) \\
& \qquad\quad \land (u1.1 \neq u2.1 \lor u1.2 \neq u2.2
\end{array}
$$

$\Rightarrow u1 \equiv_R u2 = False_R\ u1.1))$

$\boldsymbol{=_R}$ $\vdash =_R \in WF\_Equals_R \rightarrow REL\_PREDICATE$
$\wedge (\forall\ a\_n\_e : WF\_Equals_R$
$\bullet =_R a\_n\_e$
$= (a\_n\_e.1,$
$\{b : BINDING$
$\mid dom\ b = a\_n\_e.1$
$\wedge\ b\ a\_n\_e.2 = Eval\ (b,\ a\_n\_e.3)\}))$

$\boldsymbol{=_{+R}}$ $\vdash =_{+R} \in WF\_ALPHABET\_EXPRESSION \rightarrow REL\_PREDICATE$
$\wedge (\forall\ a\_e\_e : WF\_ALPHABET\_EXPRESSION$
$\bullet =_{+R} a\_e\_e$
$= (a\_e\_e.1,$
$\{b : BINDING$
$\mid dom\ b = a\_e\_e.1$
$\wedge\ Eval\ (b,\ a\_e\_e.2)$
$= Eval\ (b,\ a\_e\_e.3)\}))$

$\boldsymbol{\neg_R}$ $\vdash \neg_R \in REL\_PREDICATE \rightarrow REL\_PREDICATE$
$\wedge (\forall\ u : REL\_PREDICATE$
$\bullet \neg_R\ u = (u.1,\ (True_R\ u.1).2 \setminus u.2))$

$\_ \boldsymbol{\oplus_R} \_$ $\vdash (\_ \oplus_R \_) \in REL\_PREDICATE \times ALPHABET \rightarrow REL\_PREDICATE$
$\wedge (\forall\ u : REL\_PREDICATE;\ a : ALPHABET$
$\bullet\ u \oplus_R a$
$= (u.1 \cup a,$
$\{b : BINDING$
$\mid u.1 \lhd b \in u.2 \wedge dom\ b = u.1 \cup a\}))$

$\_ \boldsymbol{\wedge_R} \_$ $\vdash (\_ \wedge_R \_)$
$\in REL\_PREDICATE \times REL\_PREDICATE \rightarrow REL\_PREDICATE$
$\wedge (\forall\ u1,\ u2 : REL\_PREDICATE$
$\bullet\ u1 \wedge_R u2$
$= (u1.1 \cup u2.1,$
$(u1 \oplus_R u2.1).2 \cap (u2 \oplus_R u1.1).2))$

$\_ \boldsymbol{\vee_R} \_$ $\vdash (\_ \vee_R \_)$
$\in REL\_PREDICATE \times REL\_PREDICATE \rightarrow REL\_PREDICATE$
$\wedge (\forall\ u1,\ u2 : REL\_PREDICATE$
$\bullet\ u1 \vee_R u2$
$= (u1.1 \cup u2.1,$
$(u1 \oplus_R u2.1).2 \cup (u2 \oplus_R u1.1).2))$

$\_ \boldsymbol{\Rightarrow_R} \_$ $\vdash (\_ \Rightarrow_R \_)$

$\in REL\_PREDICATE \times REL\_PREDICATE \rightarrow REL\_PREDICATE$
$\wedge (\forall\ u1, u2 : REL\_PREDICATE$
$\bullet\ u1 \Rightarrow_R u2 = \neg_R\ u1 \vee_R u2)$

$\_ \Leftrightarrow_R \_$ $\vdash (\_ \Leftrightarrow_R \_)$
$\in REL\_PREDICATE \times REL\_PREDICATE \rightarrow REL\_PREDICATE$
$\wedge (\forall\ u1, u2 : REL\_PREDICATE$
$\bullet\ u1 \Leftrightarrow_R u2 = (u1 \Rightarrow_R u2) \wedge_R u2 \Rightarrow_R u1)$

$\_ \lhd_R \_ \rhd_R \_$
$\vdash (\_ \lhd_R \_ \rhd_R \_) \in WF\_Cond_R \rightarrow REL\_PREDICATE$
$\wedge (\forall\ u1\_b\_u2 : WF\_Cond_R$
$\bullet\ u1\_b\_u2.1 \lhd_R u1\_b\_u2.2 \rhd_R u1\_b\_u2.3$
$= (u1\_b\_u2.2 \wedge_R u1\_b\_u2.1)$
$\vee_R \neg_R\ u1\_b\_u2.2 \wedge_R u1\_b\_u2.3)$

$\_ ;_R \_$ $\vdash (\_ ;_R \_) \in WF\_Semi_R \rightarrow REL\_PREDICATE$
$\wedge (\forall\ u1\_u2 : WF\_Semi_R$
$\bullet\ u1\_u2.1 ;_R u1\_u2.2$
$= (in\_a\ u1\_u2.1.1 \cup out\_a\ u1\_u2.2.1,$
$\{b1 : u1\_u2.1.2; b2 : u1\_u2.2.2$
$\mid \forall\ n : dom\ b2$
$\mid n \in undashed$
$\bullet\ b2\ n = b1\ (dash\ n)$
$\bullet\ undashed \lhd b1 \cup dashed \lhd b2\})$)

Π_R $\vdash \Pi_R \in WF\_Skip_R \rightarrow REL\_PREDICATE$
$\wedge (\forall\ a : WF\_Skip_R$
$\bullet\ \Pi_R\ a$
$= (a,$
$\{b : BINDING$
$\mid dom\ b = a$
$\wedge (\forall\ n : a$
$\mid n \in undashed$
$\bullet\ b\ n = b\ (dash\ n))\}))$

$Assign_R$ $\vdash Assign_R \in WF\_Assign_R \rightarrow REL\_PREDICATE$
$\wedge (\forall\ aa : WF\_Assign_R$
$\bullet\ \#\ aa.2 = 1$
$\wedge (\exists\ n : NAME$
$\mid n = head\ aa.2$
$\bullet\ Assign_R\ aa$
$= =_R (aa.1, dash\ n, head\ aa.3)$

$$
\begin{array}{ll}
 & \quad\quad\quad\quad \wedge_R\ \mathit{\Pi}_R\ (aa.1 \setminus \{n,\ dash\ n\})) \\
 & \quad\quad \vee\ \#\ aa.2 > 1 \\
 & \quad\quad\quad \wedge\ (\exists\ n : NAME \\
 & \quad\quad\quad\quad \mid n = head\ aa.2 \\
 & \quad\quad\quad\quad \bullet\ Assign_R\ aa \\
 & \quad\quad\quad\quad\quad = =_R (aa.1,\ dash\ n,\ head\ aa.3) \\
 & \quad\quad\quad\quad\quad\quad \wedge_R\ Assign_R \\
 & \quad\quad\quad\quad\quad\quad\quad (aa.1 \setminus \{n,\ dash\ n\}, \\
 & \quad\quad\quad\quad\quad\quad\quad\ \ tail\ aa.2, \\
 & \quad\quad\quad\quad\quad\quad\quad\ \ tail\ aa.3))) \\
\boldsymbol{\_ -_R \_} & \vdash (\_ -_R \_) \in REL\_PREDICATE \times ALPHABET \rightarrow REL\_PREDICATE \\
 & \quad \wedge\ (\forall\ u : REL\_PREDICATE;\ a : ALPHABET \\
 & \quad\quad \bullet\ u -_R a = (u.1 \setminus a,\ \{b : u.2 \bullet a \lhd b\})) \\
\boldsymbol{\exists_{-R}} & \vdash \exists_{-R} \in ALPHABET \times REL\_PREDICATE \rightarrow REL\_PREDICATE \\
 & \quad \wedge\ (\forall\ a : ALPHABET;\ u : REL\_PREDICATE \\
 & \quad\quad \bullet\ \exists_{-R}\ (a,\ u) = u -_R a) \\
\boldsymbol{\forall_{-R}} & \vdash \forall_{-R} \in ALPHABET \times REL\_PREDICATE \rightarrow REL\_PREDICATE \\
 & \quad \wedge\ (\forall\ a : ALPHABET;\ u : REL\_PREDICATE \\
 & \quad\quad \bullet\ \forall_{-R}\ (a,\ u) = \neg_R\ (\exists_{-R}\ (a,\ \neg_R\ u))) \\
\boldsymbol{\exists_R} & \vdash \exists_R \in ALPHABET \times REL\_PREDICATE \rightarrow REL\_PREDICATE \\
 & \quad \wedge\ (\forall\ a : ALPHABET;\ u : REL\_PREDICATE \\
 & \quad\quad \bullet\ \exists_R\ (a,\ u) = \exists_{-R}\ (a,\ u) \oplus_R a) \\
\boldsymbol{\forall_R} & \vdash \forall_R \in ALPHABET \times REL\_PREDICATE \rightarrow REL\_PREDICATE \\
 & \quad \wedge\ (\forall\ a : ALPHABET;\ u : REL\_PREDICATE \\
 & \quad\quad \bullet\ \forall_R\ (a,\ u) = \neg_R\ (\exists_R\ (a,\ \neg_R\ u))) \\
\boldsymbol{/_R} & \vdash /_R \in WF\_Subst_R \rightarrow REL\_PREDICATE \\
 & \quad \wedge\ (\forall\ u\_e\_n : WF\_Subst_R \\
 & \quad\quad \bullet\ /_R\ u\_e\_n \\
 & \quad\quad\quad = (u\_e\_n.1.1, \\
 & \quad\quad\quad\quad \{b : BINDING \\
 & \quad\quad\quad\quad\quad \mid dom\ b = u\_e\_n.1.1 \\
 & \quad\quad\quad\quad\quad\quad \wedge\ b \oplus \{u\_e\_n.3 \mapsto Eval\ (b,\ u\_e\_n.2)\} \\
 & \quad\quad\quad\quad\quad\quad\quad \in u\_e\_n.1.2\})) \\
\boldsymbol{\_\ intchoice_R\ \_} & \\
 & \vdash (\_\ intchoice_R\ \_) \\
 & \quad\quad \in WF\_REL\_PREDICATE\_PAIR \rightarrow REL\_PREDICATE \\
 & \quad \wedge\ (\forall\ pair\_u : WF\_REL\_PREDICATE\_PAIR \\
 & \quad\quad \bullet\ pair\_u.1\ intchoice_R\ pair\_u.2
\end{array}
$$

$$= pair\_u.1 \vee_R pair\_u.2)$$

$\_\ conj_R\ \_$ $\vdash (\_\ conj_R\ \_) \in WF\_REL\_PREDICATE\_PAIR \rightarrow REL\_PREDICATE$
$\wedge (\forall pair\_u : WF\_REL\_PREDICATE\_PAIR$
$\bullet pair\_u.1\ conj_R\ pair\_u.2$
$= pair\_u.1 \wedge_R pair\_u.2)$

var_R $\vdash var_R \in WF\_Var_{R\_End R} \rightarrow REL\_PREDICATE$
$\wedge (\forall a\_n : WF\_Var_{R\_End R}$
$\bullet var_R\ a\_n = \exists\_{}_R (\{a\_n.2\}, \Pi_R\ a\_n.1))$

end_R $\vdash end_R \in WF\_Var_{R\_End R} \rightarrow REL\_PREDICATE$
$\wedge (\forall a\_n : WF\_Var_{R\_End R}$
$\bullet end_R\ a\_n = \exists\_{}_R (\{dash\ a\_n.2\}, \Pi_R\ a\_n.1))$

$\_ +_R \_$ $\vdash (\_ +_R \_) \in WF\_Extend\_rest_R \rightarrow REL\_PREDICATE$
$\wedge (\forall u\_a : WF\_Extend\_rest_R$
$\bullet u\_a.1 +_R u\_a.2$
$= u\_a.1 \wedge_R \Pi_R (u\_a.2 \cup \{n : u\_a.2 \bullet dash\ n\}))$

$\langle_R \_ \rangle_R$ $\vdash (\langle_R \_ \rangle_R) \in REL\_PREDICATE \rightarrow REL\_PREDICATE$
$\wedge (\forall u : REL\_PREDICATE$
$\bullet \langle_R\ u\ \rangle_R = \forall\_{}_R (u.1, u))$

$\_ \sqsubseteq_R \_$ $\vdash (\_ \sqsubseteq_R \_) \in WF\_REL\_PREDICATE\_PAIR \rightarrow REL\_PREDICATE$
$\wedge (\forall pair\_u : WF\_REL\_PREDICATE\_PAIR$
$\bullet pair\_u.1 \sqsubseteq_R pair\_u.2$
$= \langle_R\ pair\_u.2 \Rightarrow_R pair\_u.1\ \rangle_R)$

$monotonic$ $\vdash monotonic \in \mathbb{P} (REL\_PREDICATE \rightarrow REL\_PREDICATE)$
$\wedge monotonic$
$= \{f : REL\_PREDICATE \rightarrow REL\_PREDICATE$
$\mid \forall u1, u2 : REL\_PREDICATE$
$\bullet (u1 \sqsubseteq_R u2) \Rightarrow_R f\ u1 \sqsubseteq_R f\ u2 = True_R\ \varnothing\}$

Bot_R $\vdash Bot_R \in ALPHABET \rightarrow REL\_PREDICATE$
$\wedge (\forall a : ALPHABET \bullet Bot_R\ a = True_R\ a)$

Top_R $\vdash Top_R \in ALPHABET \rightarrow REL\_PREDICATE$
$\wedge (\forall a : ALPHABET \bullet Top_R\ a = False_R\ a)$

$\bigcap_R$ $\vdash \bigcap_R \in WF\_Glb_{R\_Lub R} \rightarrow REL\_PREDICATE$
$\wedge (\forall a\_us : WF\_Glb_{R\_Lub R}; u : REL\_PREDICATE$
$\bullet u \sqsubseteq_R \bigcap_R a\_us = True_R\ \varnothing$
$\Leftrightarrow u.1 = a\_us.1$
$\wedge (\forall u1 : a\_us.2 \bullet u \sqsubseteq_R u1 = True_R\ \varnothing))$

$\bigcup_R$ $\vdash \bigcup_R \in WF\_Glb_{R\_Lub R} \rightarrow REL\_PREDICATE$
$\wedge (\forall a\_us : WF\_Glb_{R\_Lub R}; u : REL\_PREDICATE$

$$
\begin{array}{ll}
& \quad\quad \bullet \bigcup_R \ a\_us \sqsubseteq_R u = True_R \ \varnothing \\
& \quad\quad\quad \Leftrightarrow u.1 = a\_us.1 \\
& \quad\quad\quad\quad \wedge (\forall \ u1 : a\_us.2 \bullet u1 \sqsubseteq_R u = True_R \ \varnothing)) \\
\boldsymbol{\mu_R} & \vdash \mu_R \in REL\_FUNCTION \rightarrow REL\_PREDICATE \\
& \quad \wedge (\forall \ f : REL\_FUNCTION \\
& \quad\quad \bullet \exists \ a : ALPHABET \\
& \quad\quad\quad \mid \forall \ u\_dom : dom \ f \bullet a = u\_dom.1 \\
& \quad\quad\quad \bullet \mu_R \ f \\
& \quad\quad\quad\quad = \bigcap_R \\
& \quad\quad\quad\quad\quad (a, \\
& \quad\quad\quad\quad\quad\quad \{u : REL\_PREDICATE \\
& \quad\quad\quad\quad\quad\quad\quad \mid a = u.1 \wedge f \ u \sqsubseteq_R u = True_R \ \varnothing\})) \\
\boldsymbol{\nu_R} & \vdash \nu_R \in REL\_FUNCTION \rightarrow REL\_PREDICATE \\
& \quad \wedge (\forall \ f : REL\_FUNCTION \\
& \quad\quad \bullet \exists \ a : ALPHABET \\
& \quad\quad\quad \mid \forall \ u\_dom : dom \ f \bullet a = u\_dom.1 \\
& \quad\quad\quad \bullet \nu_R \ f \\
& \quad\quad\quad\quad = \bigcup_R \\
& \quad\quad\quad\quad\quad (a, \\
& \quad\quad\quad\quad\quad\quad \{u : REL\_PREDICATE \\
& \quad\quad\quad\quad\quad\quad\quad \mid a = u.1 \wedge u \sqsubseteq_R f \ u = True_R \ \varnothing\})) \\
\boldsymbol{varT_R} & \vdash varT_R \in WF\_VarT_{R\_EndTR} \rightarrow REL\_PREDICATE \\
& \quad \wedge (\forall \ a\_n\_t : WF\_VarT_{R\_EndTR} \\
& \quad\quad \bullet varT_R \ a\_n\_t \\
& \quad\quad\quad = \bigcap_R \\
& \quad\quad\quad\quad (a\_n\_t.1 \setminus \{a\_n\_t.2\}, \\
& \quad\quad\quad\quad\quad \{v : VALUE \\
& \quad\quad\quad\quad\quad\quad \mid v \in (Set \ {}^\sim) \ a\_n\_t.3 \\
& \quad\quad\quad\quad\quad\quad \bullet var_R \ (a\_n\_t.1, a\_n\_t.2) \\
& \quad\quad\quad\quad\quad\quad\quad ;_R \ Assign_R \\
& \quad\quad\quad\quad\quad\quad\quad\quad (a\_n\_t.1, \\
& \quad\quad\quad\quad\quad\quad\quad\quad\quad \langle a\_n\_t.2 \rangle, \\
& \quad\quad\quad\quad\quad\quad\quad\quad\quad \langle Val \ v \rangle)\})) \\
\boldsymbol{endT_R} & \vdash endT_R \in WF\_VarT_{R\_EndTR} \rightarrow REL\_PREDICATE \\
& \quad \wedge (\forall \ a\_n\_t : WF\_VarT_{R\_EndTR} \\
& \quad\quad \bullet endT_R \ a\_n\_t \\
& \quad\quad\quad = \bigcap_R \\
& \quad\quad\quad\quad (a\_n\_t.1 \setminus \{dash \ a\_n\_t.2\},
\end{array}
$$

$\{v : VALUE$
$\quad | \; v \in (Set \;\sim) \; a\_n\_t.3$
$\quad \bullet \; Assign_R$
$\qquad\qquad (a\_n\_t.1, \; \langle a\_n\_t.2 \rangle, \; \langle Val \; v \rangle)$
$\qquad\quad ;_R \; end_R \; (a\_n\_t.1, \; a\_n\_t.2)\}))$

REL_Semi$_R$_idem_thm

$\vdash \forall \; a1, \; a2 : ALPHABET; \; n1, \; n2 : NAME$
$\quad | \; (a1, \; n1, \; Val \; (Bool \; false)) \in WF\_Equals_R$
$\qquad \wedge \; n1 \in undashed$
$\qquad \wedge \; n2 \in undashed$
$\qquad \wedge \; (a2,$
$\qquad\qquad Rel \; ((\_ \leq_R \_), \; Var \; n2, \; Var \; (dash \; n2)),$
$\qquad\qquad Val \; (Bool \; true))$
$\qquad\quad \in WF\_ALPHABET\_EXPRESSION$
$\qquad \wedge \; a2 \subseteq a1$
$\qquad \wedge \; (=_R \; (a1, \; n1, \; Val \; (Bool \; false))$
$\qquad\qquad\quad \wedge_R \; =_{+R}$
$\qquad\qquad\qquad (a2,$
$\qquad\qquad\qquad\quad Rel$
$\qquad\qquad\qquad\qquad ((\_ \leq_R \_),$
$\qquad\qquad\qquad\qquad\quad Var \; n2,$
$\qquad\qquad\qquad\qquad\quad Var \; (dash \; n2)),$
$\qquad\qquad\qquad\quad Val \; (Bool \; true)),$
$\qquad\qquad =_R \; (a1, \; n1, \; Val \; (Bool \; false))$
$\qquad\qquad\quad \wedge_R \; =_{+R}$
$\qquad\qquad\qquad (a2,$
$\qquad\qquad\qquad\quad Rel$
$\qquad\qquad\qquad\qquad ((\_ \leq_R \_),$
$\qquad\qquad\qquad\qquad\quad Var \; n2,$
$\qquad\qquad\qquad\qquad\quad Var \; (dash \; n2)),$
$\qquad\qquad\qquad\quad Val \; (Bool \; true)))$
$\qquad\quad \in WF\_Semi_R$
$\quad \bullet \; (=_R \; (a1, \; n1, \; Val \; (Bool \; false))$
$\qquad\qquad \wedge_R \; =_{+R}$
$\qquad\qquad\quad (a2,$
$\qquad\qquad\qquad Rel$
$\qquad\qquad\qquad\quad ((\_ \leq_R \_),$
$\qquad\qquad\qquad\qquad Var \; n2,$

$Var\ (dash\ n2)),$
$Val\ (Bool\ true)))$
$;_R\ =_R\ (a1,\ n1,\ Val\ (Bool\ false))$
$\wedge_R\ =_{+R}$
$(a2,$
Rel
$((\_ \leq_R \_),$
$Var\ n2,$
$Var\ (dash\ n2)),$
$Val\ (Bool\ true))$
$=\ =_R\ (a1,\ n1,\ Val\ (Bool\ false))$
$\wedge_R\ =_{+R}$
$(a2,$
$Rel\ ((\_ \leq_R \_),\ Var\ n2,\ Var\ (dash\ n2)),$
$Val\ (Bool\ true))$

REL_◁R_▷R_∨R_reach_thm

$\vdash \forall\ u1,\ u2,\ b1,\ b2 : REL\_PREDICATE$
$|\ (u1,\ b2,\ u2) \in WF\_Cond_R$
$\wedge\ (u1,\ b1 \vee_R b2,\ u2) \in WF\_Cond_R$
$\bullet\ u1 \lhd_R b1 \rhd_R u1 \lhd_R b2 \rhd_R u2$
$=\ u1 \lhd_R b1 \vee_R b2 \rhd_R u2$

REL_◁R_▷R_∧R_interchange_thm

$\vdash \forall\ u1,\ u2,\ u3,\ b1,\ b2 : REL\_PREDICATE$
$|\ (u1 \wedge_R u2,\ b1,\ u3 \wedge_R u4) \in WF\_Cond_R$
$\wedge\ (u1,\ b1,\ u3) \in WF\_Cond_R$
$\wedge\ (u2,\ b2,\ u4) \in WF\_Cond_R$
$\bullet\ (u1 \wedge_R u2) \lhd_R b1 \rhd_R u3 \wedge_R u4$
$=\ (u1 \lhd_R b1 \rhd_R u3) \wedge_R u2 \lhd_R b2 \rhd_R u4$

REL_◁R_▷R_∨R_interchange_thm

$\vdash \forall\ u1,\ u2,\ u3,\ b1,\ b2 : REL\_PREDICATE$
$|\ (u1 \vee_R u2,\ b1,\ u3 \vee_R u4) \in WF\_Cond_R$
$\wedge\ (u1,\ b1,\ u3) \in WF\_Cond_R$
$\wedge\ (u2,\ b2,\ u4) \in WF\_Cond_R$
$\bullet\ (u1 \vee_R u2) \lhd_R b1 \rhd_R u3 \vee_R u4$
$=\ (u1 \lhd_R b1 \rhd_R u3) \vee_R u2 \lhd_R b2 \rhd_R u4$

REL_◁R_▷R_⇒R_interchange_thm

$\vdash \forall\ u1,\ u2,\ u3,\ b1,\ b2 : REL\_PREDICATE$
$|\ (u1 \Rightarrow_R u2,\ b1,\ u3 \Rightarrow_R u4) \in WF\_Cond_R$

$\land\ (u1,\ b1,\ u3) \in WF\_Cond_R$
$\land\ (u2,\ b2,\ u4) \in WF\_Cond_R$
$\bullet\ (u1 \Rightarrow_R u2) \lhd_R b1 \rhd_R u3 \Rightarrow_R u4$
$= (u1 \lhd_R b1 \rhd_R u3) \Rightarrow_R u2 \lhd_R b2 \rhd_R u4$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_\Leftrightarrow_R\_interchange\_thm}$
$\vdash \forall\ u1,\ u2,\ u3,\ b1,\ b2 : REL\_PREDICATE$
$\mid (u1 \Leftrightarrow_R u2,\ b1,\ u3 \Leftrightarrow_R u4) \in WF\_Cond_R$
$\land\ (u1,\ b1,\ u3) \in WF\_Cond_R$
$\land\ (u2,\ b2,\ u4) \in WF\_Cond_R$
$\bullet\ (u1 \Leftrightarrow_R u2) \lhd_R b1 \rhd_R u3 \Leftrightarrow_R u4$
$= (u1 \lhd_R b1 \rhd_R u3) \Leftrightarrow_R u2 \lhd_R b2 \rhd_R u4$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_Semi_R\_interchange\_thm}$
$\vdash \forall\ u1,\ u2,\ u3,\ b1,\ b2 : REL\_PREDICATE$
$\mid (u1,\ u2) \in WF\_Semi_R$
$\land\ (u3,\ u4) \in WF\_Semi_R$
$\land\ (u1 \ ;_R\ u2,\ b1,\ u3 \ ;_R\ u4) \in WF\_Cond_R$
$\land\ (u1,\ b1,\ u3) \in WF\_Cond_R$
$\land\ (u2,\ b2,\ u4) \in WF\_Cond_R$
$\bullet\ (u1 \ ;_R\ u2) \lhd_R b1 \rhd_R u3 \ ;_R\ u4$
$= (u1 \lhd_R b1 \rhd_R u3) \ ;_R\ u2 \lhd_R b2 \rhd_R u4$

$\boldsymbol{REL\_\Pi_R\_Semi_R\_unit\_thm}$
$\vdash \forall\ u1 : REL\_PREDICATE;\ a : ALPHABET$
$\mid a \in WF\_Skip_R \land u1.1 = a$
$\bullet\ u1 \ ;_R\ \Pi_R\ a = u1 \land u1 = \Pi_R\ a \ ;_R\ u1$

$\boldsymbol{REL\_\Pi_R\_Semi_R\_unit\_thm2}$
$\vdash \forall\ u1 : REL\_PREDICATE;\ a : ALPHABET$
$\mid a \in WF\_Skip_R \land (\Pi_R\ a,\ u1) \in WF\_Semi_R$
$\bullet\ \Pi_R\ a \ ;_R\ u1 = u1$

$\boldsymbol{REL\_Semi_R\_\lhd_R\_\rhd_R\_left\_dist\_thm}$
$\vdash \forall\ u1,\ u2,\ u3,\ b : REL\_PREDICATE$
$\mid (u1,\ u3) \in WF\_Semi_R \land (u1,\ b,\ u2) \in WF\_Cond_R$
$\bullet\ (u1 \lhd_R b \rhd_R u2) \ ;_R\ u3$
$= (u1 \ ;_R\ u3) \lhd_R b \rhd_R u2 \ ;_R\ u3$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_\cap_R\_dist\_thm}$
$\vdash \forall\ u1,\ u2,\ u3,\ b : REL\_PREDICATE$
$\mid (u1,\ b,\ u2) \in WF\_Cond_R \land (u1,\ b,\ u3) \in WF\_Cond_R$
$\bullet\ u1 \lhd_R b \rhd_R u2\ intchoice_R\ u3$
$= (u1 \lhd_R b \rhd_R u2)\ intchoice_R\ u1 \lhd_R b \rhd_R u3$

REL_Assign$_R$_order_idem_thm

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\\
\quad n1,\ n2,\ n3 : NAME;\\
\quad e1,\ e2,\ e3 : EXPRESSION\\
\mid (a,\ \langle n1,\ n2,\ n3\rangle,\ \langle e1,\ e2,\ e3\rangle) \in WF_Assign_R\\
\bullet\ Assign_R\ (a,\ \langle n1,\ n2,\ n3\rangle,\ \langle e1,\ e2,\ e3\rangle)\\
\quad = Assign_R\ (a,\ \langle n2,\ n3,\ n1\rangle,\ \langle e2,\ e3,\ e1\rangle)
\end{array}$$

REL_Assign_eval_subst_thm

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\\
\quad n : NAME;\\
\quad e : EXPRESSION;\\
\quad f : VALUE \nrightarrow VALUE\\
\mid (a,\ \langle n\rangle,\ \langle e\rangle) \in WF_Assign_R\\
\bullet\ Assign_R\ (a,\ \langle n\rangle,\ \langle e\rangle)\\
\qquad ;_R\ Assign_R\ (a,\ \langle n\rangle,\ \langle Fun_1\ (f,\ Var\ n)\rangle)\\
\quad = Assign_R\ (a,\ \langle n\rangle,\ \langle Fun_1\ (f,\ e)\rangle)
\end{array}$$

REL_Assign$_R$_$\lhd_R$_$\rhd_R$_subst_thm

$$\begin{array}{l}
\vdash \forall\ u1,\ u2,\ b : REL_PREDICATE;\\
\quad a : ALPHABET;\\
\quad n : NAME;\\
\quad e : EXPRESSION\\
\mid (u1,\ b,\ u2) \in WF_Cond_R\\
\quad \land (Assign_R\ (a,\ \langle n\rangle,\ \langle e\rangle),\ u1) \in WF_Semi_R\\
\quad \land (a,\ \langle n\rangle,\ \langle e\rangle) \in WF_Assign_R\\
\quad \land (b,\ e,\ n) \in WF_Subst_R\\
\bullet\ Assign_R\ (a,\ \langle n\rangle,\ \langle e\rangle)\ ;_R\ u1 \lhd_R b \rhd_R u2\\
\quad = (Assign_R\ (a,\ \langle n\rangle,\ \langle e\rangle)\ ;_R\ u1) \lhd_R\\
\qquad /_R\ (b,\ e,\ n) \rhd_R\\
\qquad Assign_R\ (a,\ \langle n\rangle,\ \langle e\rangle)\ ;_R\ u2
\end{array}$$

REL_$\sqcap_R$_Semi$_R$_left_dist_thm

$$\begin{array}{l}
\vdash \forall\ u1,\ u2,\ u3 : REL_PREDICATE\\
\quad \mid u1.1 = u2.1 \land (u1,\ u3) \in WF_Semi_R\\
\quad \bullet\ (u1\ intchoice_R\ u2)\ ;_R\ u3\\
\qquad = (u1\ ;_R\ u3)\ intchoice_R\ u2\ ;_R\ u3
\end{array}$$

REL_$\sqcap_R$_Semi$_R$_right_dist_thm

$$\begin{array}{l}
\vdash \forall\ u1,\ u2,\ u3 : REL_PREDICATE\\
\quad \mid u2.1 = u3.1 \land (u1,\ u3) \in WF_Semi_R\\
\quad \bullet\ u1\ ;_R\ u2\ intchoice_R\ u3
\end{array}$$

$= (u1 \ ;_R \ u2) \ intchoice_R \ u1 \ ;_R \ u3$

$\boldsymbol{REL\_\cap_R\_\lhd_R\_\rhd_R\_dist\_thm}$

$\vdash \forall \ u1, \ u2, \ u3, \ b : REL\_PREDICATE$
$\mid u1.1 = u2.1 \land (u2, \ b, \ u3) \in WF\_Cond_R$
$\bullet \ u1 \ intchoice_R \ u2 \lhd_R b \rhd_R u3$
$= (u1 \ intchoice_R \ u2) \lhd_R b \rhd_R u1 \ intchoice_R \ u3$

$\boldsymbol{REL\_fixed\_point\_thm}$

$\vdash \forall \ F : REL\_FUNCTION$
$\mid F \in monotonic$
$\bullet \ F \ (\mu_R \ F) = \mu_R \ F$

$\boldsymbol{REL\_Var_R\_com\_thm}$

$\vdash \forall \ a : ALPHABET; \ n1, \ n2 : NAME$
$\mid (a, \ n1) \in WF\_Var_{R\_EndR}$
$\land (a, \ n2) \in WF\_Var_{R\_EndR}$
$\bullet \ var_R \ (a, \ n1) \ ;_R \ var_R \ (a, \ n2)$
$= var_R \ (a, \ n2) \ ;_R \ var_R \ (a, \ n1)$

$\boldsymbol{REL\_End_R\_com\_thm}$

$\vdash \forall \ a : ALPHABET; \ n1, \ n2 : NAME$
$\mid (a, \ n1) \in WF\_Var_{R\_EndR}$
$\land (a, \ n2) \in WF\_Var_{R\_EndR}$
$\bullet \ end_R \ (a, \ n1) \ ;_R \ end_R \ (a, \ n2)$
$= end_R \ (a, \ n2) \ ;_R \ end_R \ (a, \ n1)$

$\boldsymbol{REL\_Var_R\_End_R\_com\_thm}$

$\vdash \forall \ a : ALPHABET; \ n1, \ n2 : NAME$
$\mid (a, \ n1) \in WF\_Var_{R\_EndR}$
$\land (a, \ n2) \in WF\_Var_{R\_EndR}$
$\land n1 \neq n2$
$\bullet \ var_R \ (a, \ n1) \ ;_R \ end_R \ (a, \ n2)$
$= end_R \ (a, \ n2) \ ;_R \ var_R \ (a, \ n1)$

$\boldsymbol{REL\_Var_R\_initial\_value\_thm}$

$\vdash \forall \ a : ALPHABET; \ n : NAME$
$\mid (a, \ \langle n \rangle, \ \langle Val \ v \rangle) \in WF\_Assign_R$
$\land (a, \ n1) \in WF\_Var_{R\_EndR}$
$\bullet \ var_R \ (a, \ n)$
$= \bigcap_R$
$(a,$
$\{v : VALUE$
$\bullet \ var_R \ (a, \ n)$

$;_R\ Assign_R\ (a, \langle n \rangle, \langle Val\ v \rangle)\})$

$\boldsymbol{REL\_Var_R\_\lhd_R\_\rhd_R\_dist\_thm}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\ n : NAME;\ u1,\ u2,\ b : REL_PREDICATE \\
\quad \mid (a,\ n) \in WF_Var_{R_EndR} \\
\quad\quad \land\ (u1,\ b,\ u2) \in WF_Cond_R \\
\quad\quad \land\ (var_R\ (a,\ n),\ u1) \in WF_Semi_R \\
\quad\quad \land\ (var_R\ (a,\ n),\ u2) \in WF_Semi_R \\
\quad\quad \land\ n \notin b.1 \\
\quad \bullet\ var_R\ (a,\ n)\ ;_R\ u1 \lhd_R b \rhd_R u2 \\
\quad\quad = (var_R\ (a,\ n)\ ;_R\ u1) \lhd_R \\
\quad\quad\quad b \rhd_R \\
\quad\quad\quad var_R\ (a,\ n)\ ;_R\ u2
\end{array}$$

$\boldsymbol{REL\_End_R\_\lhd_R\_\rhd_R\_dist\_thm}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\ n : NAME;\ u1,\ u2,\ b : REL_PREDICATE \\
\quad \mid (a,\ n) \in WF_Var_{R_EndR} \\
\quad\quad \land\ (u1,\ b,\ u2) \in WF_Cond_R \\
\quad\quad \land\ (end_R\ (a,\ n),\ u1) \in WF_Semi_R \\
\quad\quad \land\ (end_R\ (a,\ n),\ u2) \in WF_Semi_R \\
\quad\quad \land\ n \notin b.1 \\
\quad \bullet\ end_R\ (a,\ n)\ ;_R\ u1 \lhd_R b \rhd_R u2 \\
\quad\quad = (end_R\ (a,\ n)\ ;_R\ u1) \lhd_R \\
\quad\quad\quad b \rhd_R \\
\quad\quad\quad end_R\ (a,\ n)\ ;_R\ u2
\end{array}$$

$\boldsymbol{REL\_Var_R\_End_R\_idem\_thm}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\ n : NAME \\
\quad \mid (a,\ n) \in WF_Var_{R_EndR} \\
\quad \bullet\ var_R\ (a,\ n)\ ;_R\ end_R\ (a,\ n) = \Pi_R\ a
\end{array}$$

$\boldsymbol{REL\_End_R\_Var_R\_Assign_R\_idem\_thm}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\ n : NAME;\ e : EXPRESSION \\
\quad \mid (a,\ \langle n \rangle,\ \langle e \rangle) \in WF_Assign_R \land n \notin FV\ e \\
\quad \bullet\ end_R\ (a,\ n) \\
\quad\quad\quad ;_R\ var_R\ (a,\ n)\ ;_R\ Assign_R\ (a,\ \langle n \rangle,\ \langle e \rangle) \\
\quad\quad = Assign_R\ (a,\ \langle n \rangle,\ \langle e \rangle)
\end{array}$$

$\boldsymbol{REL\_Assign_R\_End_R\_idem\_thm}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\ n : NAME;\ e : EXPRESSION \\
\quad \mid (a,\ \langle n \rangle,\ \langle e \rangle) \in WF_Assign_R \\
\quad \bullet\ Assign_R\ (a,\ \langle n \rangle,\ \langle e \rangle)\ ;_R\ end_R\ (a,\ n) \\
\quad\quad = end_R\ (a,\ n)
\end{array}$$

$\boldsymbol{REL\_Extend_R\_Var_R\_dist\_thm}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\ n : NAME;\ u1,\ u2 : REL_PREDICATE \\
\quad \mid (a,\ n) \in WF_Var_{R_EndR} \\
\qquad \land (u1 +_R \{n\},\ u2) \in WF_Semi_R \\
\qquad \land \{n,\ dash\ n\} \cap u1.1 = \varnothing \\
\quad \bullet\ var_R\ (a,\ n) \\
\qquad\quad ;_R\ (u1 +_R \{n\})\ ;_R\ u2\ ;_R\ end_R\ (a,\ n) \\
\qquad = u1\ ;_R\ var_R\ (a,\ n)\ ;_R\ u2\ ;_R\ end_R\ (a,\ n)
\end{array}$$

$\boldsymbol{REL\_End_R\_Extend_R\_dist\_thm}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\ n : NAME;\ u1,\ u2 : REL_PREDICATE \\
\quad \mid (a,\ n) \in WF_Var_{R_EndR} \\
\qquad \land (u1,\ u2 +_R \{n\}) \in WF_Semi_R \\
\qquad \land \{n,\ dash\ n\} \cap u2.1 = \varnothing \\
\quad \bullet\ var_R\ (a,\ n) \\
\qquad\quad ;_R\ u1\ ;_R\ (u2 +_R \{n\})\ ;_R\ end_R\ (a,\ n) \\
\qquad = var_R\ (a,\ n)\ ;_R\ u1\ ;_R\ end_R\ (a,\ n)\ ;_R\ u2
\end{array}$$

$\boldsymbol{REL\_\bigcup_R\_\cap_R\_dist\_thm}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET; \\
\qquad us : \mathbb{P}\ REL_PREDICATE; \\
\qquad u : REL_PREDICATE \\
\quad \mid (a,\ us) \in UNIFORM_REL_PREDICATE_SET \land u.1 = a \\
\quad \bullet \bigcup_R\ (a,\ us)\ intchoice_R\ u \\
\qquad = \bigcup_R\ (a,\ \{u1 : us \bullet u1\ \ intchoice_R\ u\})
\end{array}$$

$\boldsymbol{REL\_\bigcap_R\_\cup_R\_dist\_thm}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET; \\
\qquad us : \mathbb{P}\ REL_PREDICATE; \\
\qquad u : REL_PREDICATE \\
\quad \mid (a,\ us) \in UNIFORM_REL_PREDICATE_SET \land u.1 = a \\
\quad \bullet \bigcap_R\ (a,\ us)\ conj_R\ u \\
\qquad = \bigcap_R\ (a,\ \{u1 : us \bullet u1\ \ conj_R\ u\})
\end{array}$$

$\boldsymbol{REL\_Semi_R\_left\_univ\_disj\_thm}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET; \\
\qquad us : \mathbb{P}\ REL_PREDICATE; \\
\qquad u : REL_PREDICATE \\
\quad \mid (a,\ us) \in UNIFORM_REL_PREDICATE_SET \\
\qquad \land (\bigcap_R\ (a,\ us),\ u) \in WF_Semi_R \\
\quad \bullet \bigcap_R\ (a,\ us)\ ;_R\ u = \bigcap_R\ (a,\ \{u1 : us \bullet u1\ ;_R\ u\})
\end{array}$$

$\boldsymbol{REL\_Semi_R\_right\_univ\_disj\_thm}$

$\vdash \forall\ a : ALPHABET;$
$us : \mathbb{P}\ REL\_PREDICATE;$
$u : REL\_PREDICATE$
$\mid (a,\ us) \in UNIFORM\_REL\_PREDICATE\_SET$
$\land\ (u,\ \bigcap_R\ (a,\ us)) \in WF\_Semi_R$
$\bullet\ u\ ;_R\ \bigcap_R\ (a,\ us) = \bigcap_R\ (a,\ \{u1 : us \bullet u\ ;_R\ u1\})$

REL_$\forall_R$_idem_thm

$\vdash \forall\ a : ALPHABET;\ d : REL\_PREDICATE$
$\bullet\ \forall_R\ (a,\ \forall_R\ (a,\ u)) = \forall_R\ (a,\ u)$

REL_$\exists_R$_idem_thm

$\vdash \forall\ n : ALPHABET;\ u : REL\_PREDICATE$
$\bullet\ \exists_R\ (a,\ \exists_R\ (a,\ u)) = \exists_R\ (a,\ u)$

REL_$\neg_R$_$\forall_R$_deMorgans_thm

$\vdash \forall\ n : ALPHABET;\ u : REL\_PREDICATE$
$\bullet\ \neg_R\ (\forall_R\ (a,\ u)) = \exists_R\ (a,\ \neg_R\ u)$

REL_$\neg_R$_$\exists_R$_deMorgans_thm

$\vdash \forall\ n : ALPHABET;\ u : REL\_PREDICATE$
$\bullet\ \neg_R\ (\exists_R\ (a,\ u)) = \forall_R\ (a,\ \neg_R\ u)$

REL_$\forall_R$_comm_thm

$\vdash \forall\ a1,\ a2 : ALPHABET;\ u : REL\_PREDICATE$
$\mid a1 \cap a2 = \varnothing$
$\bullet\ \forall_R\ (a1,\ \forall_R\ (a2,\ u)) = \forall_R\ (a2,\ \forall_R\ (a1,\ u))$

REL_$\exists_R$_comm_thm

$\vdash \forall\ a1,\ a2 : ALPHABET;\ u : REL\_PREDICATE$
$\mid a1 \cap a2 = \varnothing$
$\bullet\ \exists_R\ (a1,\ \exists_R\ (a2,\ u)) = \exists_R\ (a2,\ \exists_R\ (a1,\ u))$

REL_$\neg_R$_$\lhd_R$_$\rhd_R$_thm

$\vdash \forall\ u1,\ u2,\ b : REL\_PREDICATE$
$\mid (u1,\ b,\ u2) \in WF\_Cond_R$
$\bullet\ \neg_R\ (u1 \lhd_R b \rhd_R u2) = \neg_R\ u1 \lhd_R b \rhd_R \neg_R\ u2$

REL_$\lhd_R$_$\rhd_R$_$\land_R$_$\neg_R$_$\lhd_R$_$\rhd_R$_thm

$\vdash \forall\ u1,\ u2,\ u3,\ u4,\ b : REL\_PREDICATE$
$\mid (u1,\ b,\ u2) \in WF\_Cond_R$
$\land\ (u3,\ b,\ u4) \in WF\_Cond_R$
$\land\ (u1 \land_R \neg_R\ u3,\ b,\ u1 \land_R \neg_R\ u4) \in WF\_Cond_R$
$\bullet\ (u1 \lhd_R b \rhd_R u2) \land_R \neg_R\ (u3 \lhd_R b \rhd_R u4)$
$= (u1 \land_R \neg_R\ u3) \lhd_R b \rhd_R u1 \land_R \neg_R\ u4$

REL_$\Rightarrow_R$_$\lhd_R$_$\rhd_R$_dist_thm

$$\vdash \forall\ u1,\ u2,\ u3,\ b : REL\_PREDICATE$$
$$\mid (u2,\ b,\ u3) \in WF\_Cond_R$$
$$\bullet\ u1 \Rightarrow_R u2 \lhd_R b \rhd_R u3$$
$$= (u1 \Rightarrow_R u2) \lhd_R b \rhd_R u1 \Rightarrow_R u3$$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_\Rightarrow_R\_dist\_thm}$

$$\vdash \forall\ u1,\ u2,\ u3,\ b : REL\_PREDICATE$$
$$\mid (u1,\ b,\ u2) \in WF\_Cond_R$$
$$\bullet\ (u1 \lhd_R b \rhd_R u2) \Rightarrow_R u3$$
$$= (u1 \Rightarrow_R u3) \lhd_R b \rhd_R u2 \Rightarrow_R u3$$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_\land_R\_dist\_thm}$

$$\vdash \forall\ u1,\ u2,\ u3,\ b : REL\_PREDICATE$$
$$\mid (u1,\ b,\ u2) \in WF\_Cond_R$$
$$\bullet\ (u1 \lhd_R b \rhd_R u2) \land_R u3$$
$$= (u1 \land_R u3) \lhd_R b \rhd_R u2 \land_R u3$$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_\lor_R\_dist\_thm}$

$$\vdash \forall\ u1,\ u2,\ u3,\ b : REL\_PREDICATE$$
$$\mid (u1,\ b,\ u2) \in WF\_Cond_R$$
$$\bullet\ (u1 \lhd_R b \rhd_R u2) \lor_R u3$$
$$= (u1 \lor_R u3) \lhd_R b \rhd_R u2 \lor_R u3$$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_know\_cond\_thm}$

$$\vdash \forall\ u1,\ u2,\ b : REL\_PREDICATE$$
$$\mid (u1,\ b,\ u2) \in WF\_Cond_R$$
$$\bullet\ b \land_R u1 \lhd_R b \rhd_R u2 = b \land_R u1$$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_know\_cond\_thm1}$

$$\vdash \forall\ u1,\ u2,\ b : REL\_PREDICATE$$
$$\mid (u1,\ b,\ u2) \in WF\_Cond_R$$
$$\bullet\ \lnot_R\ b \land_R u1 \lhd_R b \rhd_R u2 = \lnot_R\ b \land_R u2$$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_ass\_if\_cond\_thm}$

$$\vdash \forall\ u1,\ u2,\ b : REL\_PREDICATE$$
$$\mid (u1,\ b,\ u2) \in WF\_Cond_R$$
$$\bullet\ u1 \lhd_R b \rhd_R u2 = (b \land_R u1) \lhd_R b \rhd_R u2$$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_ass\_else\_cond\_thm}$

$$\vdash \forall\ u1,\ u2,\ b : REL\_PREDICATE$$
$$\mid (u1,\ b,\ u2) \in WF\_Cond_R$$
$$\bullet\ u1 \lhd_R b \rhd_R u2 = u1 \lhd_R b \rhd_R \lnot_R\ b \land_R u2$$

$\boldsymbol{REL\_Equals_R\_Semi_R\_left\_one\_point\_thm}$

$$\vdash \forall\ a : ALPHABET;$$
$$old : NAME;$$

$e : EXPRESSION;$
$u : REL\_PREDICATE$
$| \; old \in undashed$
$\land (a, dash\ old, e) \in WF\_Equals_R$
$\land (u, e, old) \in WF\_Subst_R$
$\land (=_R (a, dash\ old, e), u) \in WF\_Semi_R$
$\bullet =_R (a, dash\ old, e) ;_R u = /_R (u, e, old)$

$\boldsymbol{REL\_Equals_R\_Semi_R\_right\_one\_point\_thm}$

$\vdash \forall a : ALPHABET;$
$old : NAME;$
$e : EXPRESSION;$
$u : REL\_PREDICATE$
$| \; old \in undashed$
$\land (a, old, e) \in WF\_Equals_R$
$\land (u, e, dash\ old) \in WF\_Subst_R$
$\land (u, =_R (a, old, e)) \in WF\_Semi_R$
$\bullet u ;_R =_R (a, old, e) = /_R (u, e, dash\ old)$

8.5 Definitions

$\boldsymbol{NAME}$ $\vdash NAME = \mathbb{U}$

$\boldsymbol{ALPHABET}$ $\vdash ALPHABET = \mathbb{P}\ NAME$

$\boldsymbol{VALUE}$ $\vdash VALUE = \mathbb{U}$

$\boldsymbol{INT\_VAL}$ $\vdash INT\_VAL = \{n : \mathbb{Z} \bullet Int\ n\}$

$\boldsymbol{BOOL\_VAL}$ $\vdash BOOL\_VAL = \{Bool\ true, Bool\ false\}$

$\boldsymbol{CHANNEL\_VAL}$ $\vdash CHANNEL\_VAL = \{n : NAME \bullet Channel\ n\}$

$\boldsymbol{SEQ\_VAL}$ $\vdash SEQ\_VAL = \{s : seq\ VALUE \bullet Seq\ s\}$

$\boldsymbol{SET\_VAL}$ $\vdash SET\_VAL = \{s : \mathbb{P}\ VALUE \bullet Set\ s\}$

$\boldsymbol{PAIR\_VAL}$ $\vdash PAIR\_VAL = \{v1, v2 : VALUE \bullet Pair\ (v1, v2)\}$

$\boldsymbol{EVENT\_VAL}$ $\vdash EVENT\_VAL$
$= \{c : CHANNEL\_VAL; v : VALUE$
$\bullet Pair\ (c, v)\}$

$\boldsymbol{SEQ\_EVENT\_VAL}$
$\vdash SEQ\_EVENT\_VAL = \{s : seq\ EVENT\_VAL \bullet Seq\ s\}$

$\boldsymbol{SET\_EVENT\_VAL}$
$\vdash SET\_EVENT\_VAL = \{s : \mathbb{F}\ EVENT\_VAL \bullet Set\ s\}$

$\boldsymbol{SET\_SEQ\_EVENT\_VAL}$
$\vdash SET\_SEQ\_EVENT\_VAL$

$= \{s : \mathbb{F}\ SEQ\_EVENT\_VAL$
$\bullet\ Set\ s\}$

$\boldsymbol{PAIR\_SEQ\_EVENT\_VAL}$
$\vdash PAIR\_SEQ\_EVENT\_VAL$
$= \{s1, s2 : SEQ\_EVENT\_VAL$
$\bullet\ Pair\ (s1, s2)\}$

$\boldsymbol{UNARY\_F} \vdash UNARY\_F = VALUE \mapsto VALUE$

$\boldsymbol{BINARY\_F} \vdash BINARY\_F = VALUE \times VALUE \mapsto VALUE$

$\boldsymbol{RELATION} \vdash RELATION = VALUE \leftrightarrow VALUE$

$\boldsymbol{EXPRESSION} \vdash EXPRESSION = \mathbb{U}$

$\boldsymbol{BINDING} \vdash BINDING = NAME \mapsto VALUE$

$\boldsymbol{BINDINGS} \vdash BINDINGS = \mathbb{P}\ BINDING$

$\boldsymbol{WF\_BINDING\_EXPRESSION_R}$
$\vdash WF\_BINDING\_EXPRESSION_R$
$= \{b : BINDING; e : EXPRESSION$
$\mid FV\ e \subseteq dom\ b\}$

$\boldsymbol{REL\_PREDICATE}$
$\vdash REL\_PREDICATE$
$= \{a : ALPHABET; bs : BINDINGS$
$\mid \forall\ b : bs \bullet dom\ b = a\}$

$\boldsymbol{WF\_Equals_R} \vdash WF\_Equals_R$
$= \{a : ALPHABET; n : NAME; e : EXPRESSION$
$\mid n \in a \wedge FV\ e \subseteq a\}$

$\boldsymbol{WF\_ALPHABET\_EXPRESSION}$
$\vdash WF\_ALPHABET\_EXPRESSION$
$= \{a : ALPHABET; e1, e2 : EXPRESSION$
$\mid FV\ e1 \cup FV\ e2 \subseteq a\}$

$\boldsymbol{WF\_Cond_R} \vdash WF\_Cond_R$
$= \{u1, b, u2 : REL\_PREDICATE$
$\mid b.1 \subseteq u1.1 \wedge u1.1 = u2.1\}$

$\boldsymbol{WF\_Semi_R} \vdash WF\_Semi_R$
$= \{u1, u2 : REL\_PREDICATE$
$\mid (u1.1, u2.1) \in composable\}$

$\boldsymbol{WF\_Skip_R} \vdash WF\_Skip_R = \{a : ALPHABET \mid a \in homogeneous\}$

$\boldsymbol{WF\_Assign_R} \vdash WF\_Assign_R$
$= \{a : ALPHABET;$
$ns : seq\ NAME;$
$exps : seq\ EXPRESSION$

$| (\forall\ n : ran\ ns \bullet n \in a \land n \in undashed)$
$\land (\forall\ e : ran\ exps \bullet FV\ e \subseteq a \land FV\ e \subseteq undashed)$
$\land (\#\ ns = \#\ exps$
$\land \#\ exps \neq 0)$
$\land a \in homogeneous\}$

$\boldsymbol{WF\_Subst_R}$ $\vdash WF\_Subst_R$
$= \{u : REL\_PREDICATE;\ e : EXPRESSION;\ n : NAME$
$| FV\ e \subseteq u.1 \land n \in u.1\}$

$\boldsymbol{WF\_Var_{R\_EndR}}$
$\vdash WF\_Var_{R\_EndR}$
$= \{a : ALPHABET;\ n : NAME$
$| a \in homogeneous$
$\land n \in undashed$
$\land \{n,\ dash\ n\} \subseteq a\}$

$\boldsymbol{WF\_VarT_{R\_EndTR}}$
$\vdash WF\_VarT_{R\_EndTR}$
$= \{a : ALPHABET;\ n : NAME;\ T : SET\_VAL$
$| (a,\ n) \in WF\_Var_{R\_EndR}\}$

$\boldsymbol{WF\_Extend\_rest_R}$
$\vdash WF\_Extend\_rest_R$
$= \{u : REL\_PREDICATE;\ a : ALPHABET$
$| a \subseteq undashed$
$\land (a \cup \{n : a \bullet dash\ n\}) \cap u.1 = \varnothing\}$

$\boldsymbol{WF\_REL\_PREDICATE\_PAIR}$
$\vdash WF\_REL\_PREDICATE\_PAIR$
$= \{u1,\ u2 : REL\_PREDICATE$
$| u1.1 = u2.1\}$

$\boldsymbol{WF\_Glb_{R\_LubR}}$
$\vdash WF\_Glb_{R\_LubR}$
$= \{a : ALPHABET;\ us : \mathbb{P}\ REL\_PREDICATE$
$| \forall\ u\_us : us \bullet u\_us.1 = a\}$

$\boldsymbol{REL\_FUNCTION}$ $\vdash REL\_FUNCTION$
$= \{f : REL\_PREDICATE \nrightarrow REL\_PREDICATE$
$| \exists\ a : ALPHABET$
$\bullet \forall\ u\_dom : dom\ f;\ u\_ran : ran\ f$
$\bullet a = u\_dom.1 \land u\_dom.1 = u\_ran.1\}$

8.6 Theorems

$\boldsymbol{ALPHABET\_\cup\_thm}$

$\vdash \forall a1, a2 : ALPHABET \bullet a1 \cup a2 \in ALPHABET$

$\boldsymbol{ALPHABET\_\cap\_thm}$

$\vdash \forall a1, a2 : ALPHABET \bullet a1 \cap a2 \in ALPHABET$

$\boldsymbol{ALPHABET\_Sub\_thm}$

$\vdash \forall a1, a2 : ALPHABET \bullet a1 \setminus a2 \in ALPHABET$

$\boldsymbol{ALPHABET\_\subseteq\_thm}$

$\vdash \forall a1, a2 : ALPHABET$
$\quad \bullet a1 \subseteq a2 \Rightarrow a1 \cup a2 = a2 \cup a1 \wedge a2 \cup a1 = a2$

$\boldsymbol{ALPHABET\_name\_thm}$

$\vdash \forall n : NAME \bullet \{n\} \in ALPHABET$

$\boldsymbol{ALPHABET\_dash\_thm}$

$\vdash \forall n : NAME \bullet \{dash\ n\} \in ALPHABET$

$\boldsymbol{ALPHABET\_dash\_thm1}$

$\vdash \forall n : NAME \bullet dash\ n \in NAME$

$\boldsymbol{ALPHABET\_dash\_\in\_dashed\_thm}$

$\vdash \forall n : NAME \bullet dash\ n \in dashed$

$\boldsymbol{ALPHABET\_dash\_\notin\_undashed\_thm}$

$\vdash \forall n : NAME \bullet dash\ n \notin undashed$

$\boldsymbol{ALPHABET\_dashed\_\vee\_undashed\_thm}$

$\vdash \forall n : NAME \bullet \neg\ n \in undashed \Rightarrow n \in dashed$

$\boldsymbol{ALPHABET\_dashed\_\vee\_undashed\_thm1}$

$\vdash \forall n : NAME \bullet n \in undashed \Rightarrow \neg\ n \in dashed$

$\boldsymbol{ALPHABET\_dashed\_\vee\_undashed\_thm2}$

$\vdash \forall n : NAME \bullet \neg\ n \in dashed \Rightarrow n \in undashed$

$\boldsymbol{ALPHABET\_dashed\_\vee\_undashed\_thm3}$

$\vdash \forall n : NAME \bullet n \in dashed \Rightarrow \neg\ n \in undashed$

$\boldsymbol{ALPHABET\_undashed\_\cap\_dashed\_\varnothing\_thm}$

$\vdash undashed \cap dashed = \varnothing$

$\boldsymbol{ALPHABET\_in\_a\_\cup\_out\_a\_thm}$

$\vdash \forall a : ALPHABET \bullet in\_a\ a \cup out\_a\ a = a$

$\boldsymbol{ALPHABET\_in\_a\_\cap\_out\_a\_thm}$

$\vdash \forall a : ALPHABET \bullet in\_a\ a \cap out\_a\ a = \varnothing$

$\boldsymbol{ALPHABET\_out\_a\_dist\_in\_a\_\cup\_out\_a\_eq\_out\_a\_thm}$

$\vdash \forall a1, a2 : ALPHABET$
$\quad \bullet out\_a\ (in\_a\ a1 \cup out\_a\ a2) = out\_a\ a2$

$\boldsymbol{ALPHABET\_in\_a\_dist\_in\_a\_\cup\_out\_a\_eq\_in\_a\_thm}$

$\vdash \forall\ a1,\ a2 : ALPHABET$
$\quad \bullet\ in\_a\ (in\_a\ a1 \cup out\_a\ a2) = in\_a\ a1$

$\boldsymbol{ALPHABET\_in\_\cup\_out\_left\_dist\_thm}$

$\vdash \forall\ a1,\ a2,\ a3 : ALPHABET$
$\quad \bullet\ in\_a\ (a1 \cup a2) \cup out\_a\ a3$
$\quad\quad = in\_a\ a1 \cup out\_a\ a3 \cup (in\_a\ a2 \cup out\_a\ a3)$

$\boldsymbol{ALPHABET\_hom\_\Rightarrow\_comp\_thm}$

$\vdash \forall\ a : ALPHABET$
$\quad \bullet\ a \in homogeneous \Rightarrow (a,\ a) \in composable$

$\boldsymbol{ALPHABET\_comp\_\Rightarrow\_hom\_thm}$

$\vdash \forall\ a : ALPHABET$
$\quad \bullet\ (a,\ a) \in composable \Rightarrow a \in homogeneous$

$\boldsymbol{ALPHABET\_comp\_\Leftrightarrow\_hom\_thm}$

$\vdash \forall\ a : ALPHABET$
$\quad \bullet\ (a,\ a) \in composable \Leftrightarrow a \in homogeneous$

$\boldsymbol{ALPHABET\_homogeneous\_\cup\_thm}$

$\vdash \forall\ a : ALPHABET;\ n : NAME$
$\quad |\ a \in homogeneous \land n \in undashed$
$\quad \bullet\ \{n,\ dash\ n\} \cup a \in homogeneous$

$\boldsymbol{ALPHABET\_homogeneous\_set\_dif\_thm}$

$\vdash \forall\ a : ALPHABET;\ n : NAME$
$\quad |\ a \in homogeneous \land n \in undashed$
$\quad \bullet\ a \setminus \{n,\ dash\ n\} \in homogeneous$

$\boldsymbol{ALPHABET\_homogeneous\_dash\_thm}$

$\vdash \forall\ a : ALPHABET;\ n : NAME$
$\quad |\ a \in homogeneous \land n \in undashed \land n \in a$
$\quad \bullet\ dash\ n \in a$

$\boldsymbol{ALPHABET\_comp\_\Rightarrow\_contr\_comp\_thm}$

$\vdash \forall\ a1,\ a2 : ALPHABET;\ n : NAME$
$\quad |\ n \in a1 \land n \in undashed \land (a1,\ a2) \in composable$
$\quad \bullet\ (a1 \setminus \{n\},\ a2) \in composable$

$\boldsymbol{ALPHABET\_comp\_\Rightarrow\_contr\_comp\_thm1}$

$\vdash \forall\ a1,\ a2 : ALPHABET;\ a : ALPHABET$
$\quad |\ a \cap dashed = \varnothing \land (a1,\ a2) \in composable$
$\quad \bullet\ (a1 \setminus a,\ a2) \in composable$

$\boldsymbol{ALPHABET\_comp\_\Rightarrow\_contr\_comp\_thm2}$

$\vdash \forall\ a1,\ a2 : ALPHABET;\ a : ALPHABET$

$| \ a \cap undashed = \varnothing \land (a1, a2) \in composable$
$\bullet \ (a1, a2 \setminus a) \in composable$

$\boldsymbol{ALPHABET\_a1\_a2\_a3\_composable\_thm}$
$\vdash \forall a1, a2, a3 : ALPHABET$
$| \ (a1, a2) \in composable \land (a2, a3) \in composable$
$\bullet \ (in\_a \ a1 \cup out\_a \ a2, a3) \in composable$

$\boldsymbol{ALPHABET\_a1\_a2\_a3\_composable\_thm1}$
$\vdash \forall a1, a2, a3 : ALPHABET$
$| \ (a1, a2) \in composable \land (a2, a3) \in composable$
$\bullet \ (a1, in\_a \ a2 \cup out\_a \ a3) \in composable$

$\boldsymbol{ALPHABET\_\cup\_composable\_thm}$
$\vdash \forall a1, a2, a3 : ALPHABET$
$| \ (a1, a3) \in composable \land (a2, a3) \in composable$
$\bullet \ (a1 \cup a2, a3) \in composable$

$\boldsymbol{ALPHABET\_\cup\_composable\_thm1}$
$\vdash \forall a1, a2, a3 : ALPHABET$
$| \ (a1, a2) \in composable \land (a1, a3) \in composable$
$\bullet \ (a1, a2 \cup a3) \in composable$

$\boldsymbol{ALPHABET\_\in\_set\_dif\_thm}$
$\vdash \forall a : ALPHABET; n1, n2 : NAME$
$| \ n1 \neq n2$
$\land \ a \in homogeneous$
$\land \ \{n1, n2\} \subseteq undashed$
$\land \ \{n2, dash \ n2\} \subseteq a$
$\bullet \ n2 \in a \setminus \{n1, dash \ n1\}$

$\boldsymbol{ALPHABET\_\in\_set\_dif\_thm1}$
$\vdash \forall a : ALPHABET; n1, n2 : NAME$
$| \ n1 \neq n2$
$\land \ a \in homogeneous$
$\land \ \{n1, n2\} \subseteq undashed$
$\land \ \{n2, dash \ n2\} \subseteq a$
$\bullet \ dash \ n2 \in a \setminus \{n1, dash \ n1\}$

$\boldsymbol{ALPHABET\_in\_thm}$
$\vdash \forall a : ALPHABET \bullet in\_a \ a \in ALPHABET$

$\boldsymbol{ALPHABET\_out\_thm}$
$\vdash \forall a : ALPHABET \bullet out\_a \ a \in ALPHABET$

$\boldsymbol{ALPHABET\_out\_undashed\_\cup\_dashed\_thm}$
$\vdash \forall a1, a2 : ALPHABET$

$| \ a1 \subseteq undashed \land a2 \subseteq dashed$
$\bullet \ out\_a \ (a1 \cup a2) = a2$

$\boldsymbol{ALPHABET\_in\_undashed\_\cup\_dashed\_thm}$
$\vdash \forall \ a1, \ a2 : ALPHABET$
$| \ a1 \subseteq undashed \land a2 \subseteq dashed$
$\bullet \ in\_a \ (a1 \cup a2) = a1$

$\boldsymbol{ALPHABET\_dash\_(\!|\_|\!)\_thm}$
$\vdash \forall \ a : ALPHABET \bullet dash \ (\!| \ a \ |\!) \in ALPHABET$

$\boldsymbol{ALPHABET\_\subseteq\_\cup\_(\!|\_|\!)\_thm}$
$\vdash \forall \ n : NAME; \ a : ALPHABET$
$| \ n \in a \land a \subseteq undashed$
$\bullet \ \{n, \ dash \ n\} \subseteq a \cup dash \ (\!| \ a \ |\!)$

$\boldsymbol{ALPHABET\_dash\_(\!|\_|\!)\_\subseteq\_dashed\_thm}$
$\vdash \forall \ a : ALPHABET \ | \ a \subseteq undashed \bullet dash \ (\!| \ a \ |\!) \subseteq dashed$

$\boldsymbol{ALPHABET\_(\!|\_|\!)\_homogeneous\_thm}$
$\vdash \forall \ a : ALPHABET$
$| \ a \subseteq undashed$
$\bullet \ a \cup dash \ (\!| \ a \ |\!) \in homogeneous$

$\boldsymbol{ALPHABET\_\in\_in\_a\_\lor\_out\_a\_\Leftrightarrow\_\in\_a\_thm}$
$\vdash \forall \ a : ALPHABET; \ n : NAME$
$\bullet \ n \in in\_a \ a \lor n \in out\_a \ a \Leftrightarrow n \in a$

$\boldsymbol{ALPHABET\_out\_Equals\_dash\_(\!|\_|\!)\_thm}$
$\vdash \forall \ a1, \ a2 : ALPHABET$
$| \ a2 \subseteq undashed \land out\_a \ a1 = dash \ (\!| \ a2 \ |\!)$
$\bullet \ (a1, \ a2) \in composable$

$\boldsymbol{BINDINGS\_thm}$ $\vdash \forall \ bs : BINDINGS; \ b : bs \bullet b \in NAME \nrightarrow VALUE$

$\boldsymbol{REL\_\neg\_true\_eq\_false\_thm}$
$\vdash \neg \ Bool \ true = Bool \ false$

$\boldsymbol{REL\_\neg\_false\_eq\_true\_thm}$
$\vdash \neg \ Bool \ false = Bool \ true$

$\boldsymbol{BINDINGS\_\neg\_Bool\_false\_eq\_Bool\_true\_thm}$
$\vdash \forall \ b : BINDING$
$\bullet \ \neg$
$Eval \ (b, \ Val \ (Bool \ false))$
$= Eval \ (b, \ Val \ (Bool \ true))$

$\boldsymbol{BINDINGS\_\neg\_Bool\_true\_eq\_Bool\_false\_thm}$
$\vdash \forall \ b : BINDING$
$\bullet \ \neg$

$$Eval\ (b,\ Val\ (Bool\ true)) \\ \quad = Eval\ (b,\ Val\ (Bool\ false))$$

BINDINGS_◁_∪_◁_app_thm

$$\vdash \forall\ fs,\ gs : BINDINGS;\ f : fs;\ g : gs;\ n : dom\ f \\ \quad \mid n \in undashed \\ \quad \bullet\ (undashed \lhd f \cup dashed \lhd g)\ n = f\ n$$

BINDINGS_◁_∪_◁_dash_app_thm

$$\vdash \forall\ fs,\ gs : BINDINGS;\ f : fs;\ g : gs;\ n : NAME \\ \quad \mid n \in undashed \land dash\ n \in dom\ g \\ \quad \bullet\ (undashed \lhd f \cup dashed \lhd g)\ (dash\ n) = g\ (dash\ n)$$

BINDINGS_◁_idem_thm

$$\vdash \forall\ a : ALPHABET;\ b : BINDING;\ n : dom\ b \\ \quad \mid n \in a \\ \quad \bullet\ (a \lhd b)\ n = b\ n$$

BINDINGS_⩤_idem_thm

$$\vdash \forall\ n : NAME;\ a1,\ a2 : ALPHABET;\ b : BINDING \\ \quad \mid n \in dom\ b \land n \in a1 \land a2 \cap a1 = \{\} \\ \quad \bullet\ (a2 ⩤ b)\ n = b\ n$$

REL_FV_Val_⊆_a_thm

$$\vdash \forall\ a : ALPHABET;\ v : VALUE \bullet FV\ (Val\ v) \subseteq a$$

REL_Eval_Val_thm

$$\vdash \forall\ b : BINDING;\ v : VALUE \bullet Eval\ (b,\ Val\ v) = v$$

REL_FV_Var_thm

$$\vdash \forall\ n : NAME \bullet FV\ (Var\ n) = \{n\}$$

REL_PREDICATE_∈_WF_BINDING_EXPRESSION$_R$_thm

$$\vdash \forall\ b : BINDING;\ n : NAME \\ \quad \mid n \in dom\ b \\ \quad \bullet\ (b,\ Var\ n) \in WF\_BINDING\_EXPRESSION_R$$

REL_Eval_Var_thm

$$\vdash \forall\ b : BINDING;\ n : NAME \\ \quad \mid n \in dom\ b \\ \quad \bullet\ Eval\ (b,\ Var\ n) = b\ n$$

REL_Var_∈_EXPRESSION_thm

$$\vdash \forall\ n : NAME \bullet Var\ n \in EXPRESSION$$

REL_≤$_R$_∈_EXPRESSION_thm

$$\vdash \forall\ n1,\ n2 : NAME \\ \quad \bullet\ Rel\ ((\_ \le_R \_),\ Var\ n1,\ Var\ n2) \in EXPRESSION$$

REL_PREDICATE_thm

$\vdash \forall\ u : REL\_PREDICATE \bullet u.1 \in ALPHABET \land u.2 \in BINDINGS$

$\boldsymbol{WF\_REL\_PREDICATE\_PAIR\_thm}$

$$\begin{aligned}&\vdash \forall\ pair\_u : WF\_REL\_PREDICATE\_PAIR\\ &\quad \bullet pair\_u.1 \in REL\_PREDICATE\\ &\qquad \land pair\_u.2 \in REL\_PREDICATE\\ &\qquad \land pair\_u.1.1 = pair\_u.2.1\\ &\qquad \land (pair\_u.2, pair\_u.1) \in WF\_REL\_PREDICATE\_PAIR\end{aligned}$$

$\boldsymbol{REL\_\cap_R\_com\_thm1}$

$$\begin{aligned}&\vdash \forall\ u1, u2 : REL\_PREDICATE\\ &\quad \mid u1.1 = u2.1\\ &\quad \bullet (u1, u2) \in WF\_REL\_PREDICATE\_PAIR\end{aligned}$$

$\boldsymbol{WF\_Glb_R\_Lub_R\_thm}$

$$\begin{aligned}&\vdash \forall\ a\_us : WF\_Glb_{R\_Lub R}\\ &\quad \bullet a\_us.1 \in ALPHABET \land a\_us.2 \in \mathbb{P}\ REL\_PREDICATE\end{aligned}$$

$\boldsymbol{REL\_PREDICATE\_\land_R\_thm}$

$$\begin{aligned}&\vdash \forall\ u1, u2 : REL\_PREDICATE\\ &\quad \bullet (u1.1 \cup u2.1, (u1 \oplus_R u2.1).2 \cap (u2 \oplus_R u1.1).2)\\ &\qquad \in REL\_PREDICATE\end{aligned}$$

$\boldsymbol{REL\_PREDICATE\_\land_R\_thm1}$

$\vdash \forall\ u1, u2 : REL\_PREDICATE \bullet u1 \land_R u2 \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_\lor_R\_thm}$

$$\begin{aligned}&\vdash \forall\ u1, u2 : REL\_PREDICATE\\ &\quad \bullet (u1.1 \cup u2.1, (u1 \oplus_R u2.1).2 \cup (u2 \oplus_R u1.1).2)\\ &\qquad \in REL\_PREDICATE\end{aligned}$$

$\boldsymbol{REL\_PREDICATE\_\lor_R\_thm1}$

$\vdash \forall\ u1, u2 : REL\_PREDICATE \bullet u1 \lor_R u2 \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_Extend\_unrest\_thm}$

$$\begin{aligned}&\vdash \forall\ u : REL\_PREDICATE; a : ALPHABET\\ &\quad \bullet u \oplus_R a \in REL\_PREDICATE\end{aligned}$$

$\boldsymbol{REL\_PREDICATE\_\cup\_thm}$

$$\begin{aligned}&\vdash \forall\ u1, u2 : REL\_PREDICATE\\ &\quad \mid u1.1 = u2.1\\ &\quad \bullet (u1.1, u1.2 \cup u2.2) \in REL\_PREDICATE\end{aligned}$$

$\boldsymbol{REL\_PREDICATE\_\cap\_thm}$

$$\begin{aligned}&\vdash \forall\ u1, u2 : REL\_PREDICATE\\ &\quad \mid u1.1 = u2.1\\ &\quad \bullet (u1.1, u1.2 \cap u2.2) \in REL\_PREDICATE\end{aligned}$$

$\boldsymbol{REL\_PREDICATE\_True_R\_thm}$

$\vdash \forall\ u : REL\_PREDICATE$
$\bullet\ (u.1,\ \{b : BINDING \mid dom\ b = u.1\})$
$\in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_True_R\_thm1}$

$\vdash \forall\ a : ALPHABET \bullet True_R\ a \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_False_R\_thm}$

$\vdash \forall\ u : REL\_PREDICATE \bullet (u.1,\ \{\}) \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_False_R\_thm1}$

$\vdash \forall\ a : ALPHABET \bullet False_R\ a \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_Equals_R\_thm}$

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ e : EXPRESSION$
$\mid (a,\ n,\ e) \in WF\_Equals_R$
$\bullet =_R (a,\ n,\ e) \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_Equals\_exps_R\_thm}$

$\vdash \forall\ a : ALPHABET;\ e1,\ e2 : EXPRESSION$
$\mid (a,\ e1,\ e2) \in WF\_ALPHABET\_EXPRESSION$
$\bullet =_{+R} (a,\ e1,\ e2) \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_WF\_Equals_R\_thm}$

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ e : EXPRESSION$
$\mid (a,\ n,\ e) \in WF\_Equals_R$
$\bullet\ n \in a \land FV\ e \subseteq a$

$\boldsymbol{REL\_PREDICATE\_\in\_WF\_Equals_R\_thm}$

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ e : EXPRESSION$
$\mid n \in a \land FV\ e \subseteq a$
$\bullet\ (a,\ n,\ e) \in WF\_Equals_R$

$\boldsymbol{REL\_PREDICATE\_WF\_Equals_R\_WF\_ALPHABET\_EXTENSION\_thm}$

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ e : EXPRESSION$
$\bullet\ (a,\ n,\ e) \in WF\_Equals_R$
$\Leftrightarrow (a,\ Var\ n,\ e) \in WF\_ALPHABET\_EXPRESSION$

$\boldsymbol{REL\_PREDICATE\_Extend\_rest\_thm}$

$\vdash \forall\ u : REL\_PREDICATE;\ a : ALPHABET$
$\mid (u,\ a) \in WF\_Extend\_rest_R$
$\bullet\ u +_R a \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_\in\_WF\_ALPHABET\_EXPRESSION\_thm}$

$\vdash \forall\ a : ALPHABET;\ e1,\ e2 : EXPRESSION$
$\mid FV\ e1 \cup FV\ e2 \subseteq a$
$\bullet\ (a,\ e1,\ e2) \in WF\_ALPHABET\_EXPRESSION$

$\boldsymbol{REL\_PREDICATE\_\in\_WF\_ALPHABET\_EXPRESSION\_thm1}$

$\vdash \forall\ a : ALPHABET;\ n : NAME$
$\quad \mid \{n,\ dash\ n\} \subseteq a$
$\quad \bullet (a,\ Var\ n,\ Var\ (dash\ n)) \in WF\_ALPHABET\_EXPRESSION$

REL_PREDICATE_$\neg_R$_thm

$\vdash \forall\ u : REL\_PREDICATE$
$\quad \bullet (u.1,\ \{b : BINDING \mid dom\ b = u.1\} \setminus u.2)$
$\quad\ \in REL\_PREDICATE$

***REL_PREDICATE_$\neg_R$_thm*1**

$\vdash \forall\ u : REL\_PREDICATE \bullet \neg_R\ u \in REL\_PREDICATE$

REL_PREDICATE_$\Rightarrow_R$_thm

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE \bullet u1 \Rightarrow_R u2 \in REL\_PREDICATE$

REL_PREDICATE_$\Leftrightarrow_R$_thm

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE \bullet u1 \Leftrightarrow_R u2 \in REL\_PREDICATE$

REL_PREDICATE_WF_Cond$_R$_thm

$\vdash \forall\ u1,\ u2,\ b : REL\_PREDICATE$
$\quad \mid (u1,\ b,\ u2) \in WF\_Cond_R$
$\quad \bullet b.1 \subseteq u1.1 \wedge u1.1 = u2.1$

REL_PREDICATE_$\in$_WF_Cond$_R$_thm

$\vdash \forall\ u1,\ u2,\ b : REL\_PREDICATE$
$\quad \mid b.1 \subseteq u1.1 \wedge u1.1 = u2.1$
$\quad \bullet (u1,\ b,\ u2) \in WF\_Cond_R$

REL_PREDICATE_$\lhd_R$_$\rhd_R$_thm

$\vdash \forall\ u1,\ u2,\ b : REL\_PREDICATE$
$\quad \mid (u1,\ b,\ u2) \in WF\_Cond_R$
$\quad \bullet u1 \lhd_R b \rhd_R u2 \in REL\_PREDICATE$

REL_PREDICATE_$\neg_R$_alphabet_thm

$\vdash \forall\ u : REL\_PREDICATE \bullet (\neg_R\ u).1 = u.1$

REL_PREDICATE_WF_Cond$_R$_clauses_thm

$\vdash \forall\ u1,\ u2,\ b : REL\_PREDICATE$
$\quad \mid (u1,\ b,\ u2) \in WF\_Cond_R$
$\quad \bullet (u1,\ b,\ \neg_R\ u2) \in WF\_Cond_R$
$\quad\ \wedge (u1,\ \neg_R\ b,\ u2) \in WF\_Cond_R$
$\quad\ \wedge (u1,\ \neg_R\ b,\ \neg_R\ u2) \in WF\_Cond_R$
$\quad\ \wedge (\neg_R\ u1,\ b,\ u2) \in WF\_Cond_R$
$\quad\ \wedge (\neg_R\ u1,\ b,\ \neg_R\ u2) \in WF\_Cond_R$
$\quad\ \wedge (\neg_R\ u1,\ \neg_R\ b,\ u2) \in WF\_Cond_R$
$\quad\ \wedge (\neg_R\ u1,\ \neg_R\ b,\ \neg_R\ u2) \in WF\_Cond_R$

REL_PREDICATE_WF_Cond$_R$_sym_thm

$\vdash \forall\ u1,\ u2,\ b : REL\_PREDICATE$
$\quad | \ (u1,\ b,\ u2) \in WF\_Cond_R$
$\quad \bullet \ (u2,\ b,\ u1) \in WF\_Cond_R$

REL_PREDICATE_Semi$_R$_thm

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad | \ (u1,\ u2) \in WF\_Semi_R$
$\quad \bullet \ u1 \ ;_R\ u2 \in REL\_PREDICATE$

REL_PREDICATE_WF_Semi$_R$_thm

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad | \ (u1,\ u2) \in WF\_Semi_R$
$\quad \bullet \ (u1.1,\ u2.1) \in composable$

REL_PREDICATE_$\in$_WF_Semi$_R$_thm

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad | \ (u1.1,\ u2.1) \in composable$
$\quad \bullet \ (u1,\ u2) \in WF\_Semi_R$

REL_PREDICATE_Π_R_thm

$\vdash \forall\ a : ALPHABET$
$\quad | \ a \in WF\_Skip_R$
$\quad \bullet \ \Pi_R\ a \in REL\_PREDICATE$

REL_PREDICATE_WF_Skip$_R$_thm

$\vdash \forall\ a : ALPHABET \ | \ a \in WF\_Skip_R \bullet a \in homogeneous$

REL_PREDICATE_$\in$_WF_Skip$_R$_thm

$\vdash \forall\ a : ALPHABET \ | \ a \in homogeneous \bullet a \in WF\_Skip_R$

REL_PREDICATE_WF_Assign$_R$_thm

$\vdash \forall\ a : ALPHABET;\ ns : seq\ NAME;\ exps : seq\ EXPRESSION$
$\quad | \ (a,\ ns,\ exps) \in WF\_Assign_R$
$\quad \bullet \ (\forall\ n : ran\ ns \bullet n \in a \land n \in undashed)$
$\qquad \land (\forall\ e : ran\ exps \bullet FV\ e \subseteq a \land FV\ e \subseteq undashed)$
$\qquad \land (\#\ ns = \#\ exps$
$\qquad \land \#\ exps \neq 0)$
$\qquad \land\ a \in homogeneous$

REL_PREDICATE_Contract$_R$_thm

$\vdash \forall\ u : REL\_PREDICATE;\ a : ALPHABET$
$\quad \bullet \ u -_R a \in REL\_PREDICATE$

REL_PREDICATE_$\exists$_Sub$_R$_thm

$\vdash \forall\ a : ALPHABET;\ u : REL\_PREDICATE$
$\quad \bullet \ \exists\_{}_R\ (a,\ u) \in REL\_PREDICATE$

REL_PREDICATE_$\exists_R$_thm

$\vdash \forall\ a : ALPHABET;\ u : REL\_PREDICATE$
$\quad \bullet \exists_R\ (a,\ u) \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_True_R\_alphabet\_thm}$

$\vdash \forall\ a : ALPHABET \bullet (True_R\ a).1 = a$

$\boldsymbol{REL\_PREDICATE\_False_R\_alphabet\_thm}$

$\vdash \forall\ a : ALPHABET \bullet (False_R\ a).1 = a$

$\boldsymbol{REL\_PREDICATE\_\forall\_Sub_R\_thm}$

$\vdash \forall\ a : ALPHABET;\ u : REL\_PREDICATE$
$\quad \bullet \forall\_{}_R\ (a,\ u) \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_\forall_R\_thm}$

$\vdash \forall\ a : ALPHABET;\ u : REL\_PREDICATE$
$\quad \bullet \forall_R\ (a,\ u) \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_Subst_R\_thm}$

$\vdash \forall\ u : REL\_PREDICATE;\ e : EXPRESSION;\ n : NAME$
$\quad |\ (u,\ e,\ n) \in WF\_Subst_R$
$\quad \bullet /_R\ (u,\ e,\ n) \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_WF\_Subst_R\_thm}$

$\vdash \forall\ u : REL\_PREDICATE;\ e : EXPRESSION;\ n : NAME$
$\quad |\ (u,\ e,\ n) \in WF\_Subst_R$
$\quad \bullet FV\ \ e \subseteq u.1 \land n \in u.1$

$\boldsymbol{REL\_PREDICATE\_\in\_WF\_Subst_R\_thm}$

$\vdash \forall\ u : REL\_PREDICATE;\ e : EXPRESSION;\ n : NAME$
$\quad |\ FV\ \ e \subseteq u.1 \land n \in u.1$
$\quad \bullet (u,\ e,\ n) \in WF\_Subst_R$

$\boldsymbol{REL\_PREDICATE\_\langle_R\_\rangle_R\_thm}$

$\vdash \forall\ u : REL\_PREDICATE \bullet \langle_R\ u\ \rangle_R \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_\sqsubseteq_R\_thm}$

$\vdash \forall\ pair\_u : WF\_REL\_PREDICATE\_PAIR$
$\quad \bullet pair\_u.1 \sqsubseteq_R pair\_u.2 \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_Var_R\_thm}$

$\vdash \forall\ a : ALPHABET;\ n : NAME$
$\quad |\ (a,\ n) \in WF\_Var_{R\_EndR}$
$\quad \bullet var_R\ (a,\ n) \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_WF\_Var_R\_End_R\_thm}$

$\vdash \forall\ a : ALPHABET;\ n : NAME$
$\quad |\ (a,\ n) \in WF\_Var_{R\_EndR}$
$\quad \bullet a \in homogeneous \land n \in undashed \land \{n,\ dash\ n\} \subseteq a$

$\boldsymbol{REL\_PREDICATE\_WF\_Var_R\_End_R\_WF\_Skip_R\_thm}$

$\vdash \forall\ a : ALPHABET;\ n : NAME$
$\quad \mid (a,\ n) \in WF\_Var_{R\_End R}$
$\quad \bullet\ a \in WF\_Skip_R$

$\boldsymbol{REL\_PREDICATE\_End_R\_thm}$

$\vdash \forall\ a : ALPHABET;\ n : NAME$
$\quad \mid (a,\ n) \in WF\_Var_{R\_End R}$
$\quad \bullet\ end_R\ (a,\ n) \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_\sqcap_R\_thm}$

$\vdash \forall\ pair\_u : WF\_REL\_PREDICATE\_PAIR$
$\quad \bullet\ pair\_u.1\ intchoice_R\ pair\_u.2 \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_Bot_R\_thm}$

$\vdash \forall\ a : ALPHABET \bullet Bot_R\ a \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_Top_R\_thm}$

$\vdash \forall\ a : ALPHABET \bullet Top_R\ a \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_\bigcap_R\_thm}$

$\vdash \forall\ a\_us : WF\_Glb_{R\_Lub R} \bullet \bigcap_R\ a\_us \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_\bigcup_R\_thm}$

$\vdash \forall\ a\_us : WF\_Glb_{R\_Lub R} \bullet \bigcup_R\ a\_us \in REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_Extend\_unrest\_alphabet\_thm}$

$\vdash \forall\ u : REL\_PREDICATE;\ a : ALPHABET$
$\quad \bullet\ (u \oplus_R a).1 = u.1 \cup a$

$\boldsymbol{REL\_PREDICATE\_\wedge_R\_alphabet\_thm}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad \mid u1.1 = u2.1$
$\quad \bullet\ (u1 \wedge_R u2).1 = u1.1$

$\boldsymbol{REL\_PREDICATE\_\wedge_R\_alphabet\_thm1}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad \bullet\ (u1 \wedge_R u2).1 = u1.1 \cup u2.1$

$\boldsymbol{REL\_PREDICATE\_\vee_R\_alphabet\_thm}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad \mid u1.1 = u2.1$
$\quad \bullet\ (u1 \vee_R u2).1 = u1.1$

$\boldsymbol{REL\_PREDICATE\_\vee_R\_alphabet\_thm1}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad \bullet\ (u1 \vee_R u2).1 = u1.1 \cup u2.1$

$\boldsymbol{REL\_PREDICATE\_Equals_R\_alphabet\_thm}$

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ e : EXPRESSION$
$\quad \mid (a,\ n,\ e) \in WF\_Equals_R$

$\bullet\ (=_R\ (a,\ n,\ e)).1 = a$

REL_PREDICATE_Equals_exps$_R$_alphabet_thm

$\vdash \forall\ a : ALPHABET;\ e1,\ e2 : EXPRESSION$
$\quad |\ (a,\ e1,\ e2) \in WF\_ALPHABET\_EXPRESSION$
$\quad \bullet\ (=_{+R}\ (a,\ e1,\ e2)).1 = a$

REL_PREDICATE_$\Rightarrow_R$_alphabet_thm

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad \bullet\ (u1 \Rightarrow_R u2).1 = u1.1 \cup u2.1$

REL_PREDICATE_$\Leftrightarrow_R$_alphabet_thm

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad \bullet\ (u1 \Leftrightarrow_R u2).1 = u1.1 \cup u2.1$

REL_PREDICATE_Π_R_alphabet_thm

$\vdash \forall\ a : ALPHABET \mid a \in WF\_Skip_R \bullet (\Pi_R\ a).1 = a$

REL_PREDICATE_$\lhd_R$_$\rhd_R$_alphabet_thm

$\vdash \forall\ u1,\ u2,\ b : REL\_PREDICATE$
$\quad |\ (u1,\ b,\ u2) \in WF\_Cond_R$
$\quad \bullet\ (u1 \lhd_R b \rhd_R u2).1 = u1.1$

REL_PREDICATE_Semi$_R$_alphabet_thm

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad |\ (u1,\ u2) \in WF\_Semi_R$
$\quad \bullet\ (u1\ ;_R\ u2).1 = in\_a\ u1.1 \cup out\_a\ u2.1$

REL_PREDICATE_Var$_R$_alphabet_thm

$\vdash \forall\ a : ALPHABET;\ n : NAME$
$\quad |\ (a,\ n) \in WF\_Var_{R\_EndR}$
$\quad \bullet\ (var_R\ (a,\ n)).1 = a \setminus \{n\}$

REL_PREDICATE_End$_R$_alphabet_thm

$\vdash \forall\ a : ALPHABET;\ n : NAME$
$\quad |\ (a,\ n) \in WF\_Var_{R\_EndR}$
$\quad \bullet\ (end_R\ (a,\ n)).1 = a \setminus \{dash\ n\}$

REL_PREDICATE_Contract$_R$_alphabet_thm

$\vdash \forall\ a : ALPHABET;\ u : REL\_PREDICATE$
$\quad \bullet\ (u -_R a).1 = u.1 \setminus a$

REL_PREDICATE_$\exists$_Sub$_R$_alphabet_thm

$\vdash \forall\ a : ALPHABET;\ u : REL\_PREDICATE$
$\quad \bullet\ (\exists_{-R}\ (a,\ u)).1 = u.1 \setminus a$

REL_PREDICATE_$\exists_R$_alphabet_thm

$\vdash \forall\ a : ALPHABET;\ u : REL\_PREDICATE$
$\quad \bullet\ (\exists_R\ (a,\ u)).1 = u.1 \cup a$

$\boldsymbol{REL\_PREDICATE\_\forall\_Sub_R\_alphabet\_thm}$

$\vdash \forall a : ALPHABET; u : REL\_PREDICATE$
$\bullet (\forall_{-R} (a, u)).1 = u.1 \setminus a$

$\boldsymbol{REL\_PREDICATE\_\forall_R\_alphabet\_thm}$

$\vdash \forall a : ALPHABET; u : REL\_PREDICATE$
$\bullet (\forall_R (a, u)).1 = u.1 \cup a$

$\boldsymbol{REL\_PREDICATE\_Subst_R\_alphabet\_thm}$

$\vdash \forall u : REL\_PREDICATE; e : EXPRESSION; n : NAME$
$\mid (u, e, n) \in WF\_Subst_R$
$\bullet (/_R (u, e, n)).1 = u.1$

$\boldsymbol{REL\_PREDICATE\_\langle_R\_\rangle_R\_alphabet\_thm}$

$\vdash \forall u : REL\_PREDICATE \bullet \langle_R u \rangle_R.1 = \varnothing$

$\boldsymbol{REL\_PREDICATE\_\sqcap_R\_alphabet\_thm}$

$\vdash \forall pair\_u : WF\_REL\_PREDICATE\_PAIR$
$\bullet (pair\_u.1\ intchoice_R\ pair\_u.2).1 = pair\_u.1.1$

$\boldsymbol{REL\_PREDICATE\_\sqsubseteq_R\_alphabet\_thm}$

$\vdash \forall pair\_u : WF\_REL\_PREDICATE\_PAIR$
$\bullet (pair\_u.1 \sqsubseteq_R pair\_u.2).1 = \varnothing$

$\boldsymbol{REL\_PREDICATE\_Bot_R\_alphabet\_thm}$

$\vdash \forall a : ALPHABET \bullet (Bot_R\ a).1 = a$

$\boldsymbol{REL\_PREDICATE\_Top_R\_alphabet\_thm}$

$\vdash \forall a : ALPHABET \bullet (Top_R\ a).1 = a$

$\boldsymbol{REL\_\neg_R\_True_R\_thm}$

$\vdash \forall a : ALPHABET \bullet \neg_R (True_R\ a) = False_R\ a$

$\boldsymbol{REL\_\neg_R\_False_R\_thm}$

$\vdash \forall a : ALPHABET \bullet \neg_R (False_R\ a) = True_R\ a$

$\boldsymbol{REL\_True_R\_False_R\_thm}$

$\vdash \forall a : ALPHABET \bullet True_R\ a \neq False_R\ a$

$\boldsymbol{REL\_Equals_R\_Equals_R\_exps\_thm}$

$\vdash \forall a : ALPHABET; n : NAME; e : EXPRESSION$
$\mid (a, n, e) \in WF\_Equals_R$
$\bullet =_R (a, n, e) = =_{+R} (a, Var\ n, e)$

$\boldsymbol{REL\_Extend\_unrest\_idem\_thm}$

$\vdash \forall u : REL\_PREDICATE \bullet u \oplus_R u.1 = u$

$\boldsymbol{REL\_Extend\_unrest\_idem\_thm1}$

$\vdash \forall u : REL\_PREDICATE; a : ALPHABET$
$\bullet u \oplus_R u.1 \cup a = u \oplus_R a$

$\boldsymbol{REL\_Extend\_unrest\_idem\_thm2}$

$\vdash \forall\ u : REL\_PREDICATE;\ a : ALPHABET$
$\quad | \ a \subseteq u.1$
$\quad \bullet\ u \oplus_R a = u$

REL_Extend_unrest_idem_thm3

$\vdash \forall\ u : REL\_PREDICATE \bullet u \oplus_R \{\} = u$

REL_$\wedge_R$_Extend_unrest_contraction_thm

$\vdash \forall\ u1, u2 : REL\_PREDICATE;\ a1, a2 : ALPHABET$
$\quad | \ a1 = u1.1 \vee a1 = u2.1$
$\quad \bullet\ (u1 \wedge_R u2) \oplus_R a1 \cup a2 = (u1 \wedge_R u2) \oplus_R a2$

REL_$\vee_R$_Extend_unrest_contraction_thm

$\vdash \forall\ u1, u2 : REL\_PREDICATE;\ a1, a2 : ALPHABET$
$\quad | \ a1 = u1.1 \vee a1 = u2.1$
$\quad \bullet\ (u1 \vee_R u2) \oplus_R a1 \cup a2 = (u1 \vee_R u2) \oplus_R a2$

REL_$\wedge_R$_idem_thm

$\vdash \forall\ u : REL\_PREDICATE \bullet u \wedge_R u = u$

REL_$\vee_R$_idem_thm

$\vdash \forall\ u : REL\_PREDICATE \bullet u \vee_R u = u$

REL_$\wedge_R$_com_thm

$\vdash \forall\ u1, u2 : REL\_PREDICATE \bullet u1 \wedge_R u2 = u2 \wedge_R u1$

REL_$\vee_R$_com_thm

$\vdash \forall\ u1, u2 : REL\_PREDICATE \bullet u1 \vee_R u2 = u2 \vee_R u1$

REL_$\wedge_R$_subst_thm

$\vdash \forall\ u1, u2, u3 : REL\_PREDICATE$
$\quad | \ u1 = u2$
$\quad \bullet\ u1 \wedge_R u3 = u2 \wedge_R u3$

REL_$\vee_R$_subst_thm

$\vdash \forall\ up1, u2, u3 : REL\_PREDICATE$
$\quad | \ u1 = u2$
$\quad \bullet\ u1 \vee_R u3 = u2 \vee_R u3$

BINDINGS_$\lhd$_idemp_thm

$\vdash \forall\ a1, a2 : ALPHABET;\ b : BINDING$
$\quad \bullet\ a1 \lhd (a1 \cup a2) \lhd b = a1 \lhd b$
$\quad \wedge\ a1 \lhd (a2 \cup a1) \lhd b = a1 \lhd b$

BINDINGS_$\lhd$_idemp_thm1

$\vdash \forall\ b : BINDING \bullet dom\ b \lhd b = b$

REL_Extend_unrest_$\cap$_distr_thm

$\vdash \forall\ u1, u2, u3 : REL\_PREDICATE$
$\quad \bullet\ ((u1.1 \cup u2.1, (u1 \oplus_R u2.1).2 \cap (u2 \oplus_R u1.1).2)$

$\oplus_R\ u3.1).2$

$= (u1 \oplus_R u2.1 \cup u3.1).2 \cap (u2 \oplus_R u1.1 \cup u3.1).2$

REL_Extend_unrest_∪_distr_thm

$\vdash \forall\ u1, u2, u3 : REL\_PREDICATE$

$\bullet\ ((u1.1 \cup u2.1, (u1 \oplus_R u2.1).2 \cup (u2 \oplus_R u1.1).2)$

$\oplus_R\ u3.1).2$

$= (u1 \oplus_R u2.1 \cup u3.1).2 \cup (u2 \oplus_R u1.1 \cup u3.1).2$

REL_Extend_unrest_comm_thm

$\vdash \forall\ u : REL\_PREDICATE; a1, a2 : ALPHABET$

$\bullet\ u \oplus_R a1 \cup a2 = u \oplus_R a2 \cup a1$

REL_Contract$_R$_comb_thm

$\vdash \forall\ a1, a2 : ALPHABET; u : REL\_PREDICATE$

$\bullet\ (u -_R a1) -_R a2 = u -_R a1 \cup a2$

REL_Contract$_R$_∪_idem_thm

$\vdash \forall\ a1, a2 : ALPHABET; u : REL\_PREDICATE$

$\bullet\ u -_R a1 \cup a2 = u -_R a2 \cup a1$

REL_$\wedge_R$_assoc_thm

$\vdash \forall\ u1, u2, u3 : REL\_PREDICATE$

$\bullet\ (u1 \wedge_R u2) \wedge_R u3 = u1 \wedge_R u2 \wedge_R u3$

REL_$\wedge_R$_True$_R$_thm

$\vdash \forall\ u1, u2 : REL\_PREDICATE; a : ALPHABET$

$|\ a = u1.1 \wedge u1.1 = u2.1$

$\bullet\ u1 = True_R\ a \wedge u2 = True_R\ a$

$\Leftrightarrow u1 \wedge_R u2 = True_R\ a$

REL_$\vee_R$_assoc_thm

$\vdash \forall\ u1, u2, u3 : REL\_PREDICATE$

$\bullet\ (u1 \vee_R u2) \vee_R u3 = u1 \vee_R u2 \vee_R u3$

REL_$\wedge_R$_$\vee_R$_abs_thm

$\vdash \forall\ u1, u2 : REL\_PREDICATE$

$|\ u1.1 = u2.1$

$\bullet\ u1 \wedge_R u1 \vee_R u2 = u1$

***REL_$\wedge_R$_$\vee_R$_abs_thm*1**

$\vdash \forall\ u1, u2 : REL\_PREDICATE$

$|\ u2.1 \subseteq u1.1$

$\bullet\ u1 \wedge_R u1 \vee_R u2 = u1$

REL_$\vee_R$_$\wedge_R$_abs_thm

$\vdash \forall\ u1, u2 : REL\_PREDICATE$

$|\ u1.1 = u2.1$

$\bullet\ u1 \lor_R u1 \land_R u2 = u1$

$\boldsymbol{REL\_\lor_R\_\land_R\_abs\_thm1}$

$\vdash \forall\ u1, u2 : REL\_PREDICATE$
$\mid u2.1 \subseteq u1.1$
$\bullet\ u1 \lor_R u1 \land_R u2 = u1$

$\boldsymbol{REL\_\land_R\_\lor_R\_dist\_thm}$

$\vdash \forall\ u1, u2, u3 : REL\_PREDICATE$
$\bullet\ u1 \land_R u2 \lor_R u3 = (u1 \land_R u2) \lor_R u1 \land_R u3$

$\boldsymbol{REL\_\lor_R\_\land_R\_dist\_thm}$

$\vdash \forall\ u1, u2, u3 : REL\_PREDICATE$
$\bullet\ u1 \lor_R u2 \land_R u3 = (u1 \lor_R u2) \land_R u1 \lor_R u3$

$\boldsymbol{REL\_True_R\_\land_R\_id\_thm}$

$\vdash \forall\ u : REL\_PREDICATE \bullet u \land_R True_R\ u.1 = u$

$\boldsymbol{REL\_True_R\_\land_R\_id\_thm1}$

$\vdash \forall\ a : ALPHABET;\ u : REL\_PREDICATE$
$\mid a \subseteq u.1$
$\bullet\ u \land_R True_R\ a = u$

$\boldsymbol{REL\_True_R\_\lor_R\_zero\_thm}$

$\vdash \forall\ u : REL\_PREDICATE \bullet u \lor_R True_R\ u.1 = True_R\ u.1$

$\boldsymbol{REL\_True_R\_\lor_R\_zero\_thm1}$

$\vdash \forall\ a : ALPHABET;\ u : REL\_PREDICATE$
$\mid u.1 \subseteq a$
$\bullet\ u \lor_R True_R\ a = True_R\ a$

$\boldsymbol{REL\_True_R\_\lor_R\_zero\_thm2}$

$\vdash \forall\ a : ALPHABET;\ u : REL\_PREDICATE$
$\bullet\ u \lor_R True_R\ a = True_R\ (a \cup u.1)$

$\boldsymbol{REL\_False_R\_\land_R\_zero\_thm}$

$\vdash \forall\ u : REL\_PREDICATE \bullet u \land_R False_R\ u.1 = False_R\ u.1$

$\boldsymbol{REL\_False_R\_\land_R\_zero\_thm1}$

$\vdash \forall\ a : ALPHABET;\ u : REL\_PREDICATE$
$\mid u.1 \subseteq a$
$\bullet\ u \land_R False_R\ a = False_R\ a$

$\boldsymbol{REL\_False_R\_\land_R\_zero\_thm2}$

$\vdash \forall\ a : ALPHABET;\ u : REL\_PREDICATE$
$\bullet\ u \land_R False_R\ a = False_R\ (a \cup u.1)$

$\boldsymbol{REL\_False_R\_\lor_R\_id\_thm}$

$\vdash \forall\ u : REL\_PREDICATE \bullet u \lor_R False_R\ u.1 = u$

$\boldsymbol{REL\_False_R\_\lor_R\_id\_thm1}$

$\vdash \forall\ a : ALPHABET;\ u : REL\_PREDICATE$
$\quad |\ a \subseteq u.1$
$\quad \bullet\ u \vee_R False_R\ a = u$

REL_$\Rightarrow_R$_vacuous_thm

$\vdash \forall\ u : REL\_PREDICATE;\ a : ALPHABET$
$\quad |\ u.1 \subseteq a$
$\quad \bullet\ False_R\ a \Rightarrow_R u = True_R\ a$

REL_u_$\wedge_R$_$\neg_R$_u_Eq_False$_R$_thm

$\vdash \forall\ u : REL\_PREDICATE \bullet u \wedge_R \neg_R\ u = False_R\ u.1$

REL_$\wedge_R$_$\vee_R$_$\neg_R$_abs_thm

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad \bullet\ u1 \wedge_R \neg_R\ u1 \vee_R u2 = u1 \wedge_R u2$

REL_u_$\vee_R$_$\neg_R$_u_Eq_True$_R$_thm

$\vdash \forall\ u : REL\_PREDICATE \bullet u \vee_R \neg_R\ u = True_R\ u.1$

REL_$\neg_R$_double_negation_thm

$\vdash \forall\ u : REL\_PREDICATE \bullet \neg_R\ (\neg_R\ u) = u$

REL_$\neg_R$_$\wedge_R$_deMorgan_thm

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad \bullet\ \neg_R\ (u1 \wedge_R u2) = \neg_R\ u1 \vee_R \neg_R\ u2$

REL_$\neg_R$_$\vee_R$_deMorgan_thm

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad \bullet\ \neg_R\ (u1 \vee_R u2) = \neg_R\ u1 \wedge_R \neg_R\ u2$

REL_u_$\Rightarrow_R$_u_$\Leftrightarrow$_True$_R$_thm

$\vdash \forall\ u : REL\_PREDICATE \bullet u \Rightarrow_R u = True_R\ u.1$

REL_$\Rightarrow_R$_$\Rightarrow_R$_thm

$\vdash \forall\ u1,\ u2,\ u3 : REL\_PREDICATE$
$\quad \bullet\ u1 \Rightarrow_R u2 \Rightarrow_R u3 = (u1 \wedge_R u2) \Rightarrow_R u3$

REL_$\Rightarrow_R$_trans_thm

$\vdash \forall\ u1,\ u2,\ u3 : REL\_PREDICATE;\ a : ALPHABET$
$\quad |\ a = u1.1 \wedge u1.1 = u2.1 \wedge u2.1 = u3.1$
$\quad \bullet\ ((u1 \Rightarrow_R u2) \wedge_R u2 \Rightarrow_R u3) \Rightarrow_R u1 \Rightarrow_R u3$
$\quad\ = True_R\ a$

REL_modus_ponens_thm

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE;\ a : ALPHABET$
$\quad |\ a = u1.1 \wedge u1.1 = u2.1$
$\quad \bullet\ u1 \Rightarrow_R u2 = True_R\ a \wedge u1 = True_R\ a$
$\quad\ \Rightarrow u2 = True_R\ a$

REL_u_$\Leftrightarrow_R$_u_$\Leftrightarrow$_True$_R$_thm

$\vdash \forall u : REL\_PREDICATE \bullet u \Leftrightarrow_R u = True_R\ u.1$

$\boldsymbol{REL\_\Leftrightarrow_R\_Eq\_thm}$

$\vdash \forall u1, u2 : REL\_PREDICATE; a : ALPHABET$
$\quad | \ a = u1.1 \land u1.1 = u2.1$
$\quad \bullet (u1 \land_R u2) \lor_R \neg_R u1 \land_R \neg_R u2 = True_R\ a$
$\quad\ \ \Leftrightarrow u1 = u2$

$\boldsymbol{REL\_\Leftrightarrow_R\_Eq\_thm1}$

$\vdash \forall u1, u2 : REL\_PREDICATE; a : ALPHABET$
$\quad | \ a = u1.1 \land u1.1 = u2.1$
$\quad \bullet u1 \Leftrightarrow_R u2 = True_R\ a \Leftrightarrow u1 = u2$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_subst\_thm}$

$\vdash \forall u1, u2, cond1, cond2 : REL\_PREDICATE$
$\quad | \ cond1 = cond2$
$\quad \bullet u1 \lhd_R cond1 \rhd_R u2 = u1 \lhd_R cond2 \rhd_R u2$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_idem\_thm}$

$\vdash \forall u, b : REL\_PREDICATE$
$\quad | \ (u, b, u) \in WF\_Cond_R$
$\quad \bullet u \lhd_R b \rhd_R u = u$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_symm\_thm}$

$\vdash \forall u1, u2, b : REL\_PREDICATE$
$\quad | \ (u1, b, u2) \in WF\_Cond_R$
$\quad \bullet u1 \lhd_R b \rhd_R u2 = u2 \lhd_R \neg_R b \rhd_R u1$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_assoc\_thm}$

$\vdash \forall u1, u2, u3, b1, b2 : REL\_PREDICATE$
$\quad | \ (u1 \lhd_R b1 \rhd_R u2, b2, u3) \in WF\_Cond_R$
$\quad\ \ \land (u1, b1 \land_R b2, u2 \lhd_R b2 \rhd_R u3) \in WF\_Cond_R$
$\quad\ \ \land (u1, b1, u2) \in WF\_Cond_R$
$\quad \bullet (u1 \lhd_R b1 \rhd_R u2) \lhd_R b2 \rhd_R u3$
$\quad\ \ = u1 \lhd_R b1 \land_R b2 \rhd_R u2 \lhd_R b2 \rhd_R u3$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_dist\_thm}$

$\vdash \forall u1, u2, u3, b1, b2 : REL\_PREDICATE$
$\quad | \ (u2, b2, u3) \in WF\_Cond_R$
$\quad\ \ \land (u1, b1, u2) \in WF\_Cond_R$
$\quad\ \ \land (u1, b1, u3) \in WF\_Cond_R$
$\quad \bullet u1 \lhd_R b1 \rhd_R u2 \lhd_R b2 \rhd_R u3$
$\quad\ \ = (u1 \lhd_R b1 \rhd_R u2) \lhd_R b2 \rhd_R u1 \lhd_R b1 \rhd_R u3$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_unit\_thm}$

$\vdash \forall u1, u2 : REL\_PREDICATE; a : ALPHABET$

$| \; (u1,\ True_R\ a,\ u2) \in WF\_Cond_R$
$\bullet\ u1 \lhd_R True_R\ a \rhd_R u2 = u2 \lhd_R False_R\ a \rhd_R u1$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_unreach\_thm}$

$\vdash \forall\ u1,\ u2,\ u3,\ b1 : REL\_PREDICATE$
$| \; (u2,\ b1,\ u3) \in WF\_Cond_R$
$\land (u1,\ b1,\ u3) \in WF\_Cond_R$
$\bullet\ u1 \lhd_R b1 \rhd_R u2 \lhd_R b1 \rhd_R u3 = u1 \lhd_R b1 \rhd_R u3$

$\boldsymbol{REL\_\Pi_R\_step\_thm}$

$\vdash \forall\ a : ALPHABET;\ n : NAME$
$| \; n \in undashed$
$\land a \in WF\_Skip_R$
$\land (a,\ n,\ Var\ n) \in WF\_Equals_R$
$\bullet =_R (a,\ dash\ n,\ Var\ n) \land_R \Pi_R\ (a \setminus \{n,\ dash\ n\})$
$= \Pi_R\ a$

$\boldsymbol{REL\_Assign_R\_unchanged\_not\_metioned\_thm}$

$\vdash \forall\ a : ALPHABET;\ n1,\ n2 : NAME;\ e : EXPRESSION$
$| \; (a,\ \langle n1,\ n2\rangle,\ \langle e,\ Var\ n2\rangle) \in WF\_Assign_R$
$\land n1 \neq n2$
$\bullet\ Assign_R\ (a,\ \langle n1\rangle,\ \langle e\rangle)$
$= Assign_R\ (a,\ \langle n1,\ n2\rangle,\ \langle e,\ Var\ n2\rangle)$

$\boldsymbol{REL\_Semi_R\_assoc\_thm}$

$\vdash \forall\ u1,\ u2,\ u3 : REL\_PREDICATE$
$| \; (u1,\ u2) \in WF\_Semi_R \land (u2,\ u3) \in WF\_Semi_R$
$\bullet\ u1 \;;_R u2 \;;_R u3 = (u1 \;;_R u2) \;;_R u3$

$\boldsymbol{UTP\_Semi_R\_\lor_R\_left\_dist\_thm}$

$\vdash \forall\ u1,\ u2,\ u3 : REL\_PREDICATE$
$| \; u1.1 = u2.1 \land u2.1 = u3.1 \land u3.1 \in homogeneous$
$\bullet\ (u1 \lor_R u2) \;;_R u3 = (u1 \;;_R u3) \lor_R u2 \;;_R u3$

$\boldsymbol{REL\_Semi_R\_\lor_R\_left\_dist\_thm1}$

$\vdash \forall\ u1,\ u2,\ u3 : REL\_PREDICATE$
$| \; u1.1 = u2.1 \land (u1,\ u3) \in WF\_Semi_R$
$\bullet\ (u1 \lor_R u2) \;;_R u3 = (u1 \;;_R u3) \lor_R u2 \;;_R u3$

$\boldsymbol{REL\_Semi_R\_\lor_R\_right\_dist\_thm}$

$\vdash \forall\ u1,\ u2,\ u3 : REL\_PREDICATE$
$| \; u1.1 = u2.1 \land u2.1 = u3.1 \land u3.1 \in homogeneous$
$\bullet\ u1 \;;_R u2 \lor_R u3 = (u1 \;;_R u2) \lor_R u1 \;;_R u3$

$\boldsymbol{REL\_Semi_R\_\lor_R\_right\_dist\_thm1}$

$\vdash \forall\ u1,\ u2,\ u3 : REL\_PREDICATE$

$| \ u2.1 = u3.1 \wedge (u1, u2) \in WF\_Semi_R$
$\bullet \ u1 \ ;_R \ u2 \vee_R u3 = (u1 \ ;_R \ u2) \vee_R u1 \ ;_R \ u3$

REL_Contract$_R$_Semi$_R$_expansion_thm

$\vdash \forall \ a : ALPHABET; \ u1, u2 : REL\_PREDICATE$
$| \ a \cap dashed = \varnothing \wedge (u1, u2) \in WF\_Semi_R$
$\bullet \ (u1 -_R a) \ ;_R \ u2 = (u1 \ ;_R \ u2) -_R a$

REL_Semi$_R$_Contract$_R$_expansion_thm

$\vdash \forall \ a : ALPHABET; \ u1, u2 : REL\_PREDICATE$
$| \ a \cap undashed = \varnothing \wedge (u1, u2) \in WF\_Semi_R$
$\bullet \ u1 \ ;_R \ u2 -_R a = (u1 \ ;_R \ u2) -_R a$

REL_∃_Sub$_R$_Semi$_R$_expansion_thm

$\vdash \forall \ a : ALPHABET; \ u1, u2 : REL\_PREDICATE$
$| \ a \cap dashed = \varnothing \wedge (u1, u2) \in WF\_Semi_R$
$\bullet \ \exists_{-R} (a, u1) \ ;_R \ u2 = \exists_{-R} (a, u1 \ ;_R \ u2)$

REL_Semi$_R$_∃_Sub$_R$_expansion_thm

$\vdash \forall \ a : ALPHABET; \ u1, u2 : REL\_PREDICATE$
$| \ a \cap undashed = \varnothing \wedge (u1, u2) \in WF\_Semi_R$
$\bullet \ u1 \ ;_R \ \exists_{-R} (a, u2) = \exists_{-R} (a, u1 \ ;_R \ u2)$

REL_∃_Sub$_R$_comb_thm

$\vdash \forall \ a1, a2 : ALPHABET; \ u : REL\_PREDICATE$
$\bullet \ \exists_{-R} (a1, \exists_{-R} (a2, u)) = \exists_{-R} (a1 \cup a2, u)$

REL_∃_Sub$_R$_∨$_R$_dist_thm

$\vdash \forall \ u1, u2 : REL\_PREDICATE; \ a : ALPHABET$
$| \ a = u1.1 \wedge u1.1 = u2.1$
$\bullet \ \exists_{-R} (a, u1) \vee_R \exists_{-R} (a, u2)$
$= \exists_{-R} (a, u1 \vee_R u2)$

REL_∀_Sub$_R$_∧$_R$_dist_thm

$\vdash \forall \ u1, u2 : REL\_PREDICATE; \ a : ALPHABET$
$| \ a = u1.1 \wedge u1.1 = u2.1$
$\bullet \ \forall_{-R} (a, u1) \wedge_R \forall_{-R} (a, u2)$
$= \forall_{-R} (a, u1 \wedge_R u2)$

REL_∀_Sub$_R$_True$_R$_thm

$\vdash \forall \ a : ALPHABET \bullet \forall_{-R} (a, True_R \ a) = True_R \ \varnothing$

REL_∀_Sub$_R$_u_Eq_True$_R$_thm

$\vdash \forall \ u : REL\_PREDICATE$
$\bullet \ \forall_{-R} (u.1, u) = True_R \ \varnothing \Leftrightarrow u = True_R \ u.1$

REL_⟨$_R$_⟩$_R$_True$_R$_thm

$\vdash \forall \ a : ALPHABET \bullet \langle_R \ True_R \ a \ \rangle_R = True_R \ \varnothing$

$\boldsymbol{REL\_\langle_R\_\rangle_R\_Eq\_True_R\_thm}$

$\vdash \forall\ u : REL\_PREDICATE$
$\quad \bullet \langle_R\ u\ \rangle_R = True_R\ \varnothing \Leftrightarrow u = True_R\ u.1$

$\boldsymbol{REL\_\langle_R\_\Leftrightarrow_R\_\rangle_R\_thm}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad |\ u1.1 = u2.1$
$\quad \bullet \langle_R\ u1\ \Leftrightarrow_R\ u2\ \rangle_R = True_R\ \varnothing \Leftrightarrow u1 = u2$

$\boldsymbol{REL\_\langle_R\_\rangle_R\_\wedge_R\_dist\_thm}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad |\ u1.1 = u2.1$
$\quad \bullet \langle_R\ u1\ \rangle_R \wedge_R \langle_R\ u2\ \rangle_R = \langle_R\ u1\ \wedge_R\ u2\ \rangle_R$

$\boldsymbol{REL\_\langle_R\_\rangle_R\_\Rightarrow_R\_dist\_thm}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad |\ u1.1 = u2.1$
$\quad \bullet \langle_R\ u1\ \Rightarrow_R\ u2\ \rangle_R \Rightarrow_R \langle_R\ u1\ \rangle_R \Rightarrow_R \langle_R\ u2\ \rangle_R$
$\quad\quad = True_R\ \varnothing$

$\boldsymbol{REL\_Subst_R\_idem\_thm}$

$\vdash \forall\ u : REL\_PREDICATE;\ n1,\ n2 : NAME$
$\quad |\ (u,\ Var\ n2,\ n1) \in WF\_Subst_R$
$\quad\quad \wedge (u,\ Var\ n1,\ n2) \in WF\_Subst_R$
$\quad\quad \wedge n2 \in UnrestVar\ u$
$\quad \bullet /_R\ (/_R\ (u,\ Var\ n2,\ n1),\ Var\ n1,\ n2) = u$

$\boldsymbol{REL\_True_R\_Subst\_idem\_thm}$

$\vdash \forall\ a : ALPHABET;\ e : EXPRESSION;\ n : NAME$
$\quad |\ (True_R\ a,\ e,\ n) \in WF\_Subst_R$
$\quad \bullet /_R\ (True_R\ a,\ e,\ n) = True_R\ a$

$\boldsymbol{REL\_\cap_R\_com\_thm}$

$\vdash \forall\ pair\_u : WF\_REL\_PREDICATE\_PAIR$
$\quad \bullet pair\_u.1\ intchoice_R\ pair\_u.2$
$\quad\quad = pair\_u.2\ intchoice_R\ pair\_u.1$

$\boldsymbol{REL\_\cap_R\_assoc\_thm}$

$\vdash \forall\ u1,\ u2,\ u3 : REL\_PREDICATE$
$\quad |\ (u1,\ u2) \in WF\_REL\_PREDICATE\_PAIR$
$\quad\quad \wedge (u2,\ u3) \in WF\_REL\_PREDICATE\_PAIR$
$\quad \bullet u1\ intchoice_R\ u2\ intchoice_R\ u3$
$\quad\quad = (u1\ intchoice_R\ u2)\ intchoice_R\ u3$

$\boldsymbol{REL\_\cap_R\_idem\_thm}$

$\vdash \forall\ u : REL\_PREDICATE \bullet u\ intchoice_R\ u = u$

REL_$\cap_R$_dist_thm

$\vdash \forall\ u1,\ u2,\ u3 : REL\_PREDICATE$
$\quad |\ (u1,\ u2) \in WF\_REL\_PREDICATE\_PAIR$
$\quad \wedge\ (u2,\ u3) \in WF\_REL\_PREDICATE\_PAIR$
$\quad \bullet\ u1\ intchoice_R\ u2\ intchoice_R\ u3$
$\quad = (u1\ intchoice_R\ u2)$
$\quad\quad intchoice_R\ u1\ intchoice_R\ u3$

REL_var$_R$_Semi$_R$_thm

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ u : REL\_PREDICATE$
$\quad |\ (a,\ n) \in WF\_Var_{R\_EndR} \wedge a = u.1$
$\quad \bullet\ var_R\ (a,\ n)\ ;_R\ u = \exists_{-R}\ (\{n\},\ u)$

REL_Semi$_R$_end$_R$_thm

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ u : REL\_PREDICATE$
$\quad |\ (a,\ n) \in WF\_Var_{R\_EndR} \wedge a = u.1$
$\quad \bullet\ u\ ;_R\ end_R\ (a,\ n) = \exists_{-R}\ (\{dash\ n\},\ u)$

REL_var$_R$_composable_idem_thm

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ u : REL\_PREDICATE$
$\quad |\ (a,\ n) \in WF\_Var_{R\_EndR} \wedge (\Pi_R\ a,\ u) \in WF\_Semi_R$
$\quad \bullet\ (var_R\ (a,\ n),\ u) \in WF\_Semi_R$

REL_end$_R$_composable_idem_thm

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ u : REL\_PREDICATE$
$\quad |\ (a,\ n) \in WF\_Var_{R\_EndR} \wedge (u,\ \Pi_R\ a) \in WF\_Semi_R$
$\quad \bullet\ (u,\ end_R\ (a,\ n)) \in WF\_Semi_R$

REL_var$_R$_end$_R$_thm

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ u : REL\_PREDICATE$
$\quad |\ (a,\ n) \in WF\_Var_{R\_EndR} \wedge a = u.1$
$\quad \bullet\ var_R\ (a,\ n)\ ;_R\ u\ ;_R\ end_R\ (a,\ n)$
$\quad = \exists_{-R}\ (\{n,\ dash\ n\},\ u)$

REL_Bot$_R$_element_thm

$\vdash \forall\ a : ALPHABET;\ u : REL\_PREDICATE$
$\quad |\ a = u.1$
$\quad \bullet\ Bot_R\ a \sqsubseteq_R u = True_R\ \varnothing$

REL_Top$_R$_element_thm

$\vdash \forall\ a : ALPHABET;\ u : REL\_PREDICATE$
$\quad |\ a = u.1$
$\quad \bullet\ u \sqsubseteq_R Top_R\ a = True_R\ \varnothing$

REL_$\sqsubseteq_R$_reflex_thm

$\vdash \forall\ u : REL\_PREDICATE \bullet u \sqsubseteq_R u = True_R\ \varnothing$

$\boldsymbol{REL\_\sqsubseteq_R\_anti\_symmetry\_thm}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad |\ u1.1 = u2.1$
$\quad \bullet\ u1 = u2 \Leftrightarrow (u1 \sqsubseteq_R u2) \wedge_R u2 \sqsubseteq_R u1 = True_R\ \varnothing$

$\boldsymbol{REL\_\sqsubseteq_R\_transitivity\_thm}$

$\vdash \forall\ u1,\ u2,\ u3 : REL\_PREDICATE$
$\quad |\ u1.1 = u2.1 \wedge u2.1 = u3.1$
$\quad \bullet\ ((u1 \sqsubseteq_R u2) \wedge_R u2 \sqsubseteq_R u3) \Rightarrow_R u1 \sqsubseteq_R u3$
$\quad\quad = True_R\ \varnothing$

$\boldsymbol{REL\_PREDICATE\_\bigcap_R\_alphabet\_thm}$

$\vdash \forall\ a\_us : WF\_Glb_{R\_Lub R} \bullet (\bigcap_R\ a\_us).1 = a\_us.1$

$\boldsymbol{REL\_PREDICATE\_\bigcap_R\_\varnothing\_alphabet\_thm}$

$\vdash \forall\ a : ALPHABET \bullet (\bigcap_R\ (a,\ \{\})).1 = a$

$\boldsymbol{REL\_PREDICATE\_\bigcup_R\_alphabet\_thm}$

$\vdash \forall\ a\_us : WF\_Glb_{R\_Lub R} \bullet (\bigcup_R\ a\_us).1 = a\_us.1$

$\boldsymbol{REL\_PREDICATE\_\bigcup_R\_\varnothing\_alphabet\_thm}$

$\vdash \forall\ a : ALPHABET \bullet (\bigcup_R\ (a,\ \{\})).1 = a$

$\boldsymbol{REL\_lower\_bound\_thm}$

$\vdash \forall\ a : ALPHABET;$
$\quad\quad us : \mathbb{P}\ REL\_PREDICATE;$
$\quad\quad u : REL\_PREDICATE$
$\quad |\ (a,\ us) \in WF\_Glb_{R\_Lub R} \wedge u \in us$
$\quad \bullet\ \bigcap_R\ (a,\ us) \sqsubseteq_R u = True_R\ \varnothing$

$\boldsymbol{REL\_greatest\_lower\_bound\_thm}$

$\vdash \forall\ a : ALPHABET;$
$\quad\quad us : \mathbb{P}\ REL\_PREDICATE;$
$\quad\quad u : REL\_PREDICATE$
$\quad |\ u.1 = a$
$\quad\quad \wedge (a,\ us) \in WF\_Glb_{R\_Lub R}$
$\quad\quad \wedge (\forall\ u1 : us \bullet u \sqsubseteq_R u1 = True_R\ \varnothing)$
$\quad \bullet\ u \sqsubseteq_R \bigcap_R\ (a,\ us) = True_R\ \varnothing$

$\boldsymbol{REL\_\bigcap_R\_\varnothing\_thm}$

$\vdash \forall\ a : ALPHABET \bullet \bigcap_R\ (a,\ \{\}) = Top_R\ a$

$\boldsymbol{REL\_\bigcup_R\_\varnothing\_thm}$

$\vdash \forall\ a : ALPHABET \bullet \bigcup_R\ (a,\ \{\}) = Bot_R\ a$

$\boldsymbol{REL\_weakest\_fixed\_point\_thm}$

$\vdash \forall\ F : REL\_FUNCTION;\ Y : REL\_PREDICATE$
$\quad |\ Y \in dom\ F \wedge F\ Y \sqsubseteq_R Y = True_R\ \varnothing$

$\bullet\ \mu_R\ F \sqsubseteq_R Y = True_R\ \varnothing$

VALUE_EVENT_VAL_thm

$\vdash EVENT\_VAL \subseteq VALUE$

VALUE_SEQ_EVENT_VAL_thm

$\vdash \forall\ v : SEQ\_EVENT\_VAL \bullet v \in SEQ\_VAL$

REL_⊕_∈_BINDING_thm

$\vdash \forall\ b : BINDING;\ n : NAME;\ v : VALUE$
$\quad \bullet\ b \oplus \{n \mapsto v\} \in BINDING$

REL_◁_∈_BINDING_thm

$\vdash \forall\ b : BINDING;\ a : ALPHABET \bullet a \lhd b \in BINDING$

REL_⊕_dom_thm

$\vdash \forall\ b : BINDING;\ n1,\ n2 : NAME;\ v : VALUE$
$\quad |\ n1 \in dom\ b$
$\quad \bullet\ n1 \in dom\ (b \oplus \{n2 \mapsto v\})$

REL_◁_dom_thm

$\vdash \forall\ b : BINDING;\ a : ALPHABET;\ n : NAME$
$\quad |\ n \in dom\ b \land n \in a$
$\quad \bullet\ n \in dom\ (a \lhd b)$

REL_FV_Val_thm

$\vdash \forall\ v : VALUE \bullet FV\ (Val\ v) = \{\}$

REL_FV_Rel_thm

$\vdash \forall\ r : RELATION;\ e1,\ e2 : EXPRESSION$
$\quad \bullet\ FV\ (Rel\ (r,\ e1,\ e2)) = FV\ e1 \cup FV\ e2$

REL_PREDICATE_WF_ALPHABET_EXPRESSION_thm

$\vdash \forall\ a : ALPHABET;\ e1,\ e2 : EXPRESSION$
$\quad |\ (a,\ e1,\ e2) \in WF\_ALPHABET\_EXPRESSION$
$\quad \bullet\ FV\ e1 \cup FV\ e2 \subseteq a$

REL_Eval_Rel_thm

$\vdash \forall\ b : BINDING;\ r : RELATION;\ e1,\ e2 : EXPRESSION$
$\quad |\ (b,\ e1) \in WF\_BINDING\_EXPRESSION_R$
$\quad\ \ \land (b,\ e2) \in WF\_BINDING\_EXPRESSION_R$
$\quad \bullet\ Eval\ (b,\ Rel\ (r,\ e1,\ e2))$
$\quad\ \ = Bool\ ((Eval\ (b,\ e1),\ Eval\ (b,\ e2)) \in r)$

REL_Eval_Fun_2_thm

$\vdash \forall\ b : BINDING;\ f : BINARY\_F;\ e1,\ e2 : EXPRESSION$
$\quad |\ (b,\ e1) \in WF\_BINDING\_EXPRESSION_R$
$\quad\ \ \land (b,\ e2) \in WF\_BINDING\_EXPRESSION_R$
$\quad \bullet\ Eval\ (b,\ Fun_2\ (f,\ e1,\ e2))$

$= f\ (Eval\ (b,\ e1),\ Eval\ (b,\ e2))$

$\boldsymbol{REL\_Fun_2\_\in\_VALUE\_thm}$

$$\vdash \forall\ f : BINARY\_F;\ b : BINDING;\ n1,\ n2 : NAME \mid n1 \in dom\ b \land n2 \in dom\ b \bullet f\ (b\ n1,\ b\ n2) \in VALUE$$

$\boldsymbol{REL\_\oplus\_Eval\_thm}$

$$\vdash \forall\ b : BINDING;\ n1,\ n2 : NAME;\ v : VALUE \mid n1 \in dom\ b \land n1 \neq n2 \bullet Eval\ (b,\ Var\ n1) = Eval\ (b \oplus \{n2 \mapsto v\},\ Var\ n1)$$

$\boldsymbol{REL\_\lhd\_Eval\_thm}$

$$\vdash \forall\ b : BINDING;\ n : NAME;\ a : ALPHABET \mid n \in dom\ b \land n \in a \bullet Eval\ (a \lhd b,\ Var\ n) = b\ n$$

$\boldsymbol{REL\_\oplus\_app\_thm}$

$$\vdash \forall\ b : BINDING;\ n1,\ n2 : NAME \mid n2 \in dom\ b \land n2 \neq n1 \bullet b\ n2 = (b \oplus \{n1 \mapsto v\})\ n2$$

$\boldsymbol{REL\_\oplus\_app\_thm1}$

$$\vdash \forall\ b : BINDING;\ n1,\ n2 : NAME;\ v : VALUE \mid n2 \in dom\ b \land n2 \neq n1 \bullet b\ n2 = (b \oplus \{n1 \mapsto v\})\ n2$$

$\boldsymbol{REL\_\oplus\_\oplus\_com\_thm}$

$$\vdash \forall\ b : BINDING;\ n1,\ n2 : NAME;\ v1,\ v2 : VALUE \mid n1 \neq n2 \bullet b \oplus \{n1 \mapsto v1\} \oplus \{n2 \mapsto v2\} = b \oplus \{n2 \mapsto v2\} \oplus \{n1 \mapsto v1\}$$

$\boldsymbol{REL\_\lhd\_\oplus\_assoc\_thm}$

$$\vdash \forall\ a : ALPHABET;\ b : BINDING;\ n : NAME;\ v : VALUE \mid n \in a \bullet a \lhd (b \oplus \{n \mapsto v\}) = a \lhd b \oplus \{n \mapsto v\}$$

$\boldsymbol{REL\_FV\_Fun_2\_thm}$

$$\vdash \forall\ f : BINARY\_F;\ e1,\ e2 : EXPRESSION \bullet FV\ (Fun_2\ (f,\ e1,\ e2)) = FV\ e1 \cup FV\ e2$$

$\boldsymbol{REL\_Fun_2\_\in\_EXPRESSION\_thm}$

$$\vdash \forall\ n1,\ n2 : NAME;\ f : BINARY\_F \bullet Fun_2\ (f,\ Var\ n1,\ Var\ n2) \in EXPRESSION$$

$\boldsymbol{REL\_Fun_2\_\in\_EXPRESSION\_thm1}$

$$\vdash \forall\ e1,\ e2 : EXPRESSION;\ f : BINARY\_F$$

$\bullet\ Fun_2\ (f,\ e1,\ e2) \in EXPRESSION$

$\boldsymbol{REL\_SeqDif_R\_\in\_EXPRESSION\_thm}$

$\vdash \forall\ n1,\ n2 : NAME$
$\bullet\ Fun_2\ ((\_\ SeqDif_R\ \_),\ Var\ n1,\ Var\ n2)$
$\in EXPRESSION$

$\boldsymbol{ALPHABET\_n\_\neq\_dash\_n\_thm}$

$\vdash \forall\ n : NAME \mid n \in undashed \bullet n \neq dash\ n$

$\boldsymbol{ALPHABET\_n1\_\neq\_dash\_n2\_thm}$

$\vdash \forall\ n1,\ n2 : NAME$
$\mid n1 \neq n2 \wedge n1 \in undashed \wedge n2 \in undashed$
$\bullet\ n1 \neq dash\ n2 \wedge dash\ n2 \neq n1$

$\boldsymbol{ALPHABET\_dash\_n1\_\neq\_dash\_n2\_thm}$

$\vdash \forall\ n1,\ n2 : NAME$
$\mid n1 \neq n2 \wedge n1 \in undashed \wedge n2 \in undashed$
$\bullet\ dash\ n1 \neq dash\ n2 \wedge dash\ n2 \neq dash\ n1$

$\boldsymbol{REL\_BOOL\_true\_\in\_VALUE\_thm}$

$\vdash Bool\ true \in VALUE$

$\boldsymbol{REL\_BOOL\_false\_\in\_VALUE\_thm}$

$\vdash Bool\ false \in VALUE$

$\boldsymbol{REL\_Val\_\in\_EXPRESSION\_thm}$

$\vdash \forall\ v : VALUE \bullet Val\ v \in EXPRESSION$

$\boldsymbol{BINDINGS\_\lhd_R\_thm}$

$\vdash \forall\ b : BINDING;\ a : ALPHABET \bullet a \lhd b \in BINDING$

$\boldsymbol{REL\_PREDICATE\_WF\_Subst_R\_\wedge_R\_dist\_thm}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE;\ e : EXPRESSION;\ n : NAME$
$\mid (u1,\ e,\ n) \in WF\_Subst_R \wedge (u2,\ e,\ n) \in WF\_Subst_R$
$\bullet\ (u1 \wedge_R u2,\ e,\ n) \in WF\_Subst_R$

$\boldsymbol{REL\_PREDICATE\_WF\_Subst_R\_\vee_R\_dist\_thm}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE;\ e : EXPRESSION;\ n : NAME$
$\mid (u1,\ e,\ n) \in WF\_Subst_R \wedge (u2,\ e,\ n) \in WF\_Subst_R$
$\bullet\ (u1 \vee_R u2,\ e,\ n) \in WF\_Subst_R$

$\boldsymbol{REL\_PREDICATE\_WF\_Subst_R\_\lhd_R\_\rhd_R\_dist\_thm}$

$\vdash \forall\ u1,\ u2,\ b : REL\_PREDICATE;\ e : EXPRESSION;\ n : NAME$
$\mid (u1,\ e,\ n) \in WF\_Subst_R$
$\wedge\ (u2,\ e,\ n) \in WF\_Subst_R$
$\wedge\ (u1,\ b,\ u2) \in WF\_Cond_R$
$\bullet\ (u1 \lhd_R b \rhd_R u2,\ e,\ n) \in WF\_Subst_R$

$\boldsymbol{REL\_PREDICATE\_WF\_Subst_R\_\neg_R\_dist\_thm}$

$\vdash \forall\ u : REL\_PREDICATE;\ e : EXPRESSION;\ n : NAME$
$\quad | \ (u,\ e,\ n) \in WF\_Subst_R$
$\quad \bullet \ (\neg_R\ u,\ e,\ n) \in WF\_Subst_R$

$\boldsymbol{REL\_\lhd_R\_True_R\_\rhd_R\_app\_thm}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE;\ a : ALPHABET$
$\quad | \ (u1,\ True_R\ a,\ u2) \in WF\_Cond_R$
$\quad \bullet \ u1 \lhd_R True_R\ a \rhd_R u2 = u1$

$\boldsymbol{REL\_\lhd_R\_False_R\_\rhd_R\_app\_thm}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE;\ a : ALPHABET$
$\quad | \ (u1,\ False_R\ a,\ u2) \in WF\_Cond_R$
$\quad \bullet \ u1 \lhd_R False_R\ a \rhd_R u2 = u2$

$\boldsymbol{REL\_Subst_R\_\wedge_R\_dist\_thm}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE;\ v : VALUE;\ n : NAME$
$\quad | \ (u1,\ Val\ v,\ n) \in WF\_Subst_R$
$\quad\quad \wedge (u2,\ Val\ v,\ n) \in WF\_Subst_R$
$\quad \bullet \ /_R\ (u1 \wedge_R u2,\ Val\ v,\ n)$
$\quad\quad = /_R\ (u1,\ Val\ v,\ n) \wedge_R /_R\ (u2,\ Val\ v,\ n)$

$\boldsymbol{REL\_Subst_R\_\wedge_R\_dist\_thm1}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE;$
$\quad\quad f : BINARY\_F;$
$\quad\quad n1,\ n2,\ n3 : NAME$
$\quad | \ (u1,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3) \in WF\_Subst_R$
$\quad\quad \wedge (u2,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3)$
$\quad\quad\quad \in WF\_Subst_R$
$\quad \bullet \ /_R\ (u1 \wedge_R u2,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3)$
$\quad\quad = /_R\ (u1,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3)$
$\quad\quad\quad\quad \wedge_R /_R\ (u2,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3)$

$\boldsymbol{REL\_Subst_R\_\neg_R\_dist\_thm}$

$\vdash \forall\ u : REL\_PREDICATE;\ v : VALUE;\ n : NAME$
$\quad | \ (u,\ Val\ v,\ n) \in WF\_Subst_R$
$\quad \bullet \ /_R\ (\neg_R\ u,\ Val\ v,\ n) = \neg_R\ (/_R\ (u,\ Val\ v,\ n))$

$\boldsymbol{REL\_\vee_R\_\wedge_R\_repl\_thm}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad \bullet \ u1 \vee_R u2 = \neg_R\ (\neg_R\ u1 \wedge_R \neg_R\ u2)$

$\boldsymbol{REL\_\wedge_R\_\vee_R\_repl\_thm}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE$
$\quad \bullet \ u1 \wedge_R u2 = \neg_R\ (\neg_R\ u1 \vee_R \neg_R\ u2)$

$\boldsymbol{REL\_Subst_R\_\vee_R\_dist\_thm}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE;\ v : VALUE;\ n : NAME$
$\quad \mid (u1,\ Val\ v,\ n) \in WF\_Subst_R$
$\quad\quad \wedge (u2,\ Val\ v,\ n) \in WF\_Subst_R$
$\quad \bullet\ /_R\ (u1 \vee_R u2,\ Val\ v,\ n)$
$\quad\quad = /_R\ (u1,\ Val\ v,\ n) \vee_R /_R\ (u2,\ Val\ v,\ n)$

$\boldsymbol{REL\_Subst_{R}\_\Rightarrow_{R}\_dist\_thm}$

$\vdash \forall\ u1,\ u2 : REL\_PREDICATE;\ v : VALUE;\ n : NAME$
$\quad \mid (u1,\ Val\ v,\ n) \in WF\_Subst_R$
$\quad\quad \wedge (u2,\ Val\ v,\ n) \in WF\_Subst_R$
$\quad \bullet\ /_R\ (u1 \Rightarrow_R u2,\ Val\ v,\ n)$
$\quad\quad = /_R\ (u1,\ Val\ v,\ n) \Rightarrow_R /_R\ (u2,\ Val\ v,\ n)$

$\boldsymbol{REL\_Subst_{R}\_\lhd_{R}\_\rhd_{R}\_dist\_thm}$

$\vdash \forall\ u1,\ u2,\ b : REL\_PREDICATE;\ v : VALUE;\ n : NAME$
$\quad \mid (b,\ Val\ v,\ n) \in WF\_Subst_R$
$\quad\quad \wedge (u1,\ b,\ u2) \in WF\_Cond_R$
$\quad \bullet\ /_R\ (u1 \lhd_R b \rhd_R u2,\ Val\ v,\ n)$
$\quad\quad = /_R\ (u1,\ Val\ v,\ n) \lhd_R$
$\quad\quad\quad /_R\ (b,\ Val\ v,\ n) \rhd_R$
$\quad\quad\quad /_R\ (u2,\ Val\ v,\ n)$

$\boldsymbol{REL\_Subst_{R}\_id\_thm}$

$\vdash \forall\ a : ALPHABET;\ n1,\ n2 : NAME;\ oldv,\ newv : VALUE$
$\quad \mid (a,\ n1,\ Val\ oldv) \in WF\_Equals_R$
$\quad\quad \wedge n2 \in a$
$\quad\quad \wedge n1 \neq n2$
$\quad \bullet\ /_R\ (=_R (a,\ n1,\ Val\ oldv),\ Val\ newv,\ n2)$
$\quad\quad = =_R (a,\ n1,\ Val\ oldv)$

$\boldsymbol{REL\_Subst_{R}\_id\_thm2}$

$\vdash \forall\ a : ALPHABET;$
$\quad\quad n1,\ n2,\ n3 : NAME;$
$\quad\quad r : RELATION;$
$\quad\quad v1,\ v2 : VALUE$
$\quad \mid (a,\ Rel\ (r,\ Var\ n1,\ Var\ n2),\ Val\ v1)$
$\quad\quad\quad \in WF\_ALPHABET\_EXPRESSION$
$\quad\quad \wedge n1 \neq n3$
$\quad\quad \wedge n2 \neq n3$
$\quad\quad \wedge n3 \in a$
$\quad \bullet\ /_R$
$\quad\quad\quad (=_{+R} (a,\ Rel\ (r,\ Var\ n1,\ Var\ n2),\ Val\ v1),$

$Val\ v2,$
$n3)$
$= =_{+R}\ (a,\ Rel\ (r,\ Var\ n1,\ Var\ n2),\ Val\ v1)$

REL_Subst$_R$_com_thm1

$\vdash \forall\ r : REL\_PREDICATE;\ n1,\ n2 : NAME;\ v1,\ v2 : VALUE$
$\mid (r,\ Val\ v1,\ n1) \in WF\_Subst_R \land n2 \in r.1 \land n2 \neq n1$
$\bullet\ /_R\ (/_R\ (r,\ Val\ v1,\ n1),\ Val\ v2,\ n2)$
$= /_R\ (/_R\ (r,\ Val\ v2,\ n2),\ Val\ v1,\ n1)$

REL_Subst$_R$_com_thm

$\vdash \forall\ r : REL\_PREDICATE;$
$n1,\ n2,\ n3,\ n4 : NAME;$
$f : BINARY\_F;$
$v : VALUE$
$\mid (r,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3) \in WF\_Subst_R$
$\land\ n4 \in r.1$
$\land\ n4 \neq n1$
$\land\ n4 \neq n2$
$\land\ n4 \neq n3$
$\bullet\ /_R$
$(/_R\ (r,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3),$
$Val\ v,$
$n4)$
$= /_R$
$(/_R\ (r,\ Val\ v,\ n4),$
$Fun_2\ (f,\ Var\ n1,\ Var\ n2),$
$n3)$

REL_Subst$_R$_app_thm

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ oldv,\ newv : VALUE$
$\mid (a,\ n,\ Val\ oldv) \in WF\_Equals_R$
$\bullet\ /_R\ (=_R\ (a,\ n,\ Val\ oldv),\ Val\ newv,\ n)$
$= =_{+R}\ (a,\ Val\ newv,\ Val\ oldv)$

REL_PREDICATE_decompose_thm

$\vdash \forall\ u : REL\_PREDICATE \bullet u = (u.1,\ u.2)$

REL_Subst$_R$_id_thm1

$\vdash \forall\ r : REL\_PREDICATE;\ n : NAME;\ v : VALUE;\ T : \mathbb{P}\ VALUE$
$\mid (r,\ Val\ v,\ n) \in WF\_Subst_R$
$\land\ unrestTypedVar\ (r,\ n,\ T)$
$\land\ (\forall\ b : BINDING \mid n \in dom\ b \bullet b\ n \in T)$

$\bullet\ /_R\ (r,\ Val\ v,\ n) = r$

REL_Equals$_R$_$\wedge_R$_alphabet_ext_thm

$$\begin{array}{l} \vdash \forall\ a : ALPHABET; \\ \quad n : NAME; \\ \quad v : VALUE; \\ \quad r : REL\_PREDICATE \\ \quad \mid (a,\ n,\ Val\ v) \in WF\_Equals_R \wedge a \subseteq r.1 \\ \quad \bullet =_R (a,\ n,\ Val\ v) \wedge_R r \\ \quad\quad = =_R (r.1,\ n,\ Val\ v) \wedge_R r \end{array}$$

REL_Equals$_R$_$\vee_R$_alphabet_ext_thm

$$\begin{array}{l} \vdash \forall\ a : ALPHABET; \\ \quad n : NAME; \\ \quad v : VALUE; \\ \quad r : REL\_PREDICATE \\ \quad \mid (a,\ n,\ Val\ v) \in WF\_Equals_R \wedge a \subseteq r.1 \\ \quad \bullet =_R (a,\ n,\ Val\ v) \vee_R r \\ \quad\quad = =_R (r.1,\ n,\ Val\ v) \vee_R r \end{array}$$

REL_Equals$_R$_exps_thm

$$\begin{array}{l} \vdash \forall\ a : ALPHABET;\ e : EXPRESSION \\ \quad \mid (a,\ e,\ e) \in WF\_ALPHABET\_EXPRESSION \\ \quad \bullet =_{+R} (a,\ e,\ e) = True_R\ a \end{array}$$

***REL_Equals$_R$_exps_thm*1**

$$\begin{array}{l} \vdash \forall\ a : ALPHABET;\ v1,\ v2 : VALUE \\ \quad \mid (a,\ Val\ v1,\ Val\ v2) \in WF\_ALPHABET\_EXPRESSION \\ \quad\quad \wedge\ v1 \neq v2 \\ \quad \bullet =_{+R} (a,\ Val\ v1,\ Val\ v2) = False_R\ a \end{array}$$

***REL_Subst$_R$_app_thm*1**

$$\begin{array}{l} \vdash \forall\ a : ALPHABET; \\ \quad r : RELATION; \\ \quad n1,\ n2 : NAME; \\ \quad v1,\ v2 : VALUE \\ \quad \mid (a,\ Rel\ (r,\ Var\ n1,\ Var\ n2),\ Val\ v1) \\ \quad\quad \in WF\_ALPHABET\_EXPRESSION \\ \quad\quad \wedge\ n1 \neq n2 \\ \quad \bullet\ /_R \\ \quad\quad\quad (=_{+R} (a,\ Rel\ (r,\ Var\ n1,\ Var\ n2),\ Val\ v1), \\ \quad\quad\quad\quad Val\ v2, \\ \quad\quad\quad\quad n1) \end{array}$$

$= =_{+R}\ (a,\ Rel\ (r,\ Val\ v2,\ Var\ n2),\ Val\ v1)$

REL_Subst$_R$_app_thm2

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\\
\quad r : RELATION;\\
\quad f : BINARY_F;\\
\quad n1,\ n2,\ n3 : NAME;\\
\quad v1,\ v2 : VALUE\\
\mid n1 \in a \land n2 \in a \land n3 \in a\\
\bullet\ /_R\\
\quad (=_{+R}\ (a,\ Rel\ (r,\ Val\ v1,\ Var\ n1),\ Val\ v2),\\
\quad\ Fun_2\ (f,\ Var\ n2,\ Var\ n3),\\
\quad\ n1)\\
= =_{+R}\\
\quad (a,\\
\quad\ Rel\ (r,\ Val\ v1,\ Fun_2\ (f,\ Var\ n2,\ Var\ n3)),\\
\quad\ Val\ v2)
\end{array}$$

REL_Bool_equivalence_thm

$$\vdash \forall\ b1,\ b2 : \mathbb{B} \bullet Bool\ b1 = Bool\ b2 \Leftrightarrow b1 \Leftrightarrow b2$$

REL_$\neg_R$_Equals$_R$_true_thm

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\ n : NAME\\
\mid (a,\ n,\ Val\ (Bool\ true)) \in WF_Equals_R\\
\quad \land (\forall\ b : BINDING \mid n \in dom\ b \bullet b\ n \in BOOL_VAL)\\
\bullet \neg_R\ (=_R\ (a,\ n,\ Val\ (Bool\ true)))\\
\quad = =_R\ (a,\ n,\ Val\ (Bool\ false))
\end{array}$$

REL_Subst$_R$_$\neg_R$_dist_thm1

$$\begin{array}{l}
\vdash \forall\ u : REL_PREDICATE;\ f : BINARY_F;\ n1,\ n2,\ n3 : NAME\\
\mid (u,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3) \in WF_Subst_R\\
\bullet\ /_R\ (\neg_R\ u,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3)\\
\quad = \neg_R\ (/_R\ (u,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3))
\end{array}$$

REL_Subst$_R$_$\vee_R$_dist_thm1

$$\begin{array}{l}
\vdash \forall\ u1,\ u2 : REL_PREDICATE;\\
\quad f : BINARY_F;\\
\quad n1,\ n2,\ n3 : NAME\\
\mid (u1,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3) \in WF_Subst_R\\
\quad \land (u2,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3)\\
\qquad \in WF_Subst_R\\
\bullet\ /_R\ (u1 \vee_R u2,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3)\\
\quad = /_R\ (u1,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3)
\end{array}$$

$\vee_R \ /_R \ (u2, \ Fun_2 \ (f, \ Var \ n1, \ Var \ n2), \ n3)$

REL_Subst$_R$_id_thm3

$$\vdash \forall \ a : ALPHABET; \ n1, n2, n3, n4 : NAME; \ oldv : VALUE; \ f : BINARY\_F \mid (a, n1, Val \ oldv) \in WF\_Equals_R \land n2 \in a \land n3 \in a \land n4 \in a \land n1 \neq n2 \bullet /_R \ (=_R (a, n1, Val \ oldv), Fun_2 \ (f, Var \ n3, Var \ n4), n2) = =_R (a, n1, Val \ oldv)$$

ALPHABET_seqd_double_size_thm

$$\vdash \forall \ n1, n2 : NAME \bullet \# \langle n1, n2 \rangle = 2$$

ALPHABET_seqd_singleton_size_thm

$$\vdash \forall \ n1 : NAME \bullet \# \langle n1 \rangle = 1$$

ALPHABET_seqd_double_head_thm

$$\vdash \forall \ n1, n2 : NAME \bullet head \ \langle n1, n2 \rangle = n1$$

ALPHABET_seqd_double_tail_thm

$$\vdash \forall \ n1, n2 : NAME \bullet tail \ \langle n1, n2 \rangle = \langle n2 \rangle$$

EXPRESSION_seqd_double_size_thm

$$\vdash \forall \ e1, e2 : EXPRESSION \bullet \# \langle e1, e2 \rangle = 2$$

EXPRESSION_seqd_singleton_size_thm

$$\vdash \forall \ e1 : EXPRESSION \bullet \# \langle e1 \rangle = 1$$

EXPRESSION_seqd_double_head_thm

$$\vdash \forall \ e1, e2 : EXPRESSION \bullet head \ \langle e1, e2 \rangle = e1$$

EXPRESSION_seqd_double_tail_thm

$$\vdash \forall \ e1, e2 : EXPRESSION \bullet tail \ \langle e1, e2 \rangle = \langle e2 \rangle$$

REL_$\lhd_R$_$\rhd_R$_idem_thm1

$$\vdash \forall \ P, Q, b : REL\_PREDICATE \mid (P, b, Q) \in WF\_Cond_R \bullet P \lhd_R b \rhd_R P \lhd_R b \rhd_R Q = P \lhd_R b \rhd_R Q$$

REL_$\Rightarrow_R$_$\land_R$_distribution_thm

$$\vdash \forall \ a, b, c, d, e, f : REL\_PREDICATE$$

$$\begin{array}{l}
\mid a.1 = c.1 \\
\quad \land c.1 \subseteq b.1 \\
\quad \land b.1 = d.1 \\
\quad \land d.1 = e.1 \\
\quad \land e.1 = f.1 \\
\bullet ((a \land_R b) \Rightarrow_R c \land_R d) \land_R (a \land_R e) \Rightarrow_R c \land_R f \\
\quad = (a \land_R b \lor_R e) \Rightarrow_R c \land_R (b \Rightarrow_R d) \land_R e \Rightarrow_R f
\end{array}$$

$\boldsymbol{REL\_PREDICATE\_WF\_Skip_R\_thm2}$

$$\vdash \forall a : WF\_Skip_R \bullet a \in ALPHABET \land a \in homogeneous$$

$\boldsymbol{REL\_UnrestTypedVar\_True_R\_thm}$

$$\begin{array}{l}
\vdash \forall a : ALPHABET; n : NAME; T : \mathbb{P}\ VALUE \\
\quad \mid n \in a \\
\quad \bullet unrestTypedVar\ (True_R\ a, n, T) \Leftrightarrow true
\end{array}$$

$\boldsymbol{REL\_UnrestTypedVar\_\land_R\_thm}$

$$\begin{array}{l}
\vdash \forall u1, u2 : REL_PREDICATE; n : NAME; T : \mathbb{P}\ VALUE \\
\quad \bullet unrestTypedVar\ (u1, n, T) \\
\quad\quad \land unrestTypedVar\ (u2, n, T) \\
\quad \Rightarrow unrestTypedVar\ (u1 \land_R u2, n, T)
\end{array}$$

$\boldsymbol{REL\_\neg_R\_\lor_R\_\land_R\_abs\_thm}$

$$\begin{array}{l}
\vdash \forall P, Q : REL_PREDICATE \\
\quad \bullet \neg_R P \lor_R P \land_R Q = \neg_R P \lor_R Q
\end{array}$$

$\boldsymbol{REL\_\Rightarrow_R\_abs\_thm}$

$$\begin{array}{l}
\vdash \forall P, Q, R : REL_PREDICATE \\
\quad \bullet (P \land_R Q) \Rightarrow_R P \land_R R = (P \land_R Q) \Rightarrow_R R
\end{array}$$

$\boldsymbol{REL\_\land_R\_\lhd_R\_\rhd_R\_dist\_thm}$

$$\begin{array}{l}
\vdash \forall u, u1, u2, b : REL_PREDICATE \\
\quad \mid (u1, b, u2) \in WF_Cond_R \\
\quad \bullet u \land_R u1 \lhd_R b \rhd_R u2 \\
\quad\quad = (u \land_R u1) \lhd_R b \rhd_R u \land_R u2
\end{array}$$

$\boldsymbol{REL\_UnrestTypedVar\_Equals_R\_Var\_thm}$

$$\begin{array}{l}
\vdash \forall n1, n2, n3 : NAME; T : \mathbb{P}\ VALUE; a : ALPHABET \\
\quad \mid (a, n2, Var\ n3) \in WF_Equals_R \\
\quad\quad \land (\forall b : BINDING \mid n1 \in dom\ b \bullet b\ n1 \in T) \\
\quad\quad \land n1 \neq n2 \\
\quad\quad \land n1 \neq n3 \\
\quad\quad \land n1 \in a \\
\quad \bullet unrestTypedVar\ (=_R (a, n2, Var\ n3), n1, T)
\end{array}$$

$\boldsymbol{REL\_\oplus\_Eval\_thm1}$

$\vdash \forall\ b : BINDING;\ n : NAME;\ v1,\ v2 : VALUE$
$\quad \bullet\ Eval\ (b,\ Val\ v1) = Eval\ (b \oplus \{n \mapsto v2\},\ Val\ v1)$

REL_UnrestTypedVar_Equals$_R$_Val_thm

$\vdash \forall\ n1,\ n2 : NAME;$
$\quad T : \mathbb{P}\ VALUE;$
$\quad a : ALPHABET;$
$\quad val : VALUE$
$\quad |\ (a,\ n2,\ Val\ val) \in WF\_Equals_R$
$\quad \land (\forall\ b : BINDING \mid n1 \in dom\ b \bullet b\ n1 \in T)$
$\quad \land\ n1 \neq n2$
$\quad \land\ n1 \in a$
$\quad \bullet\ unrestTypedVar\ (=_R\ (a,\ n2,\ Val\ val),\ n1,\ T)$

REL_Subst$_R$_id_thm4

$\vdash \forall\ r : REL\_PREDICATE;$
$\quad n1,\ n2,\ n3 : NAME;$
$\quad f : BINARY\_F;$
$\quad T : \mathbb{P}\ VALUE$
$\quad |\ (r,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3) \in WF\_Subst_R$
$\quad \land\ unrestTypedVar\ (r,\ n3,\ T)$
$\quad \land (\forall\ b : BINDING \mid n3 \in dom\ b \bullet b\ n3 \in T)$
$\quad \bullet\ /_R\ (r,\ Fun_2\ (f,\ Var\ n1,\ Var\ n2),\ n3) = r$

REL_Subst$_R$_app_thm3

$\vdash \forall\ a : ALPHABET;\ n1,\ n2 : NAME;\ v : VALUE$
$\quad |\ (a,\ n1,\ Var\ n2) \in WF\_Equals_R \land n1 \neq n2$
$\quad \bullet\ /_R\ (=_R\ (a,\ n1,\ Var\ n2),\ Val\ v,\ n2)$
$\quad = =_R\ (a,\ n1,\ Val\ v)$

ALPHABET_dash_n_$\neq$_n_thm

$\vdash \forall\ n : NAME \mid n \in undashed \bullet dash\ n \neq n$

REL_Subst$_R$_app_thm4

$\vdash \forall\ a : ALPHABET;$
$\quad f : BINARY\_F;$
$\quad n1,\ n2,\ n3 : NAME;$
$\quad v : VALUE$
$\quad |\ n1 \in a \land n2 \in a \land n3 \in a$
$\quad \bullet\ /_R$
$\qquad (=_R\ (a,\ n1,\ Val\ v),$
$\qquad Fun_2\ (f,\ Var\ n2,\ Var\ n3),$
$\qquad n1)$

$= =_{+R} (a, \ Fun_2 \ (f, \ Var \ n2, \ Var \ n3), \ Val \ v)$

REL_inv_Seq_thm

$\vdash \forall \ s : seq \ VALUE \bullet (Seq \ {}^\sim) \ (Seq \ s) = s$

REL_SeqDif$_R$_thm

$\vdash \forall \ s1, \ s2 : VALUE$
$\quad | \ \{s1, \ s2\} \subseteq SEQ\_VAL$
$\quad \quad \wedge \ (Seq \ {}^\sim) \ s2 \ prefix_Z \ (Seq \ {}^\sim) \ s1$
$\quad \bullet \ s1 \ SeqDif_R \ s2 \in SEQ\_VAL$

REL_Prefix$_Z$_clauses_thm

$\vdash \forall \ s : seq \ VALUE \bullet \langle\rangle \ prefix_Z \ s$

REL_Prefix$_Z$_SeqDif$_R$_thm

$\vdash \forall \ s1, \ s2 : VALUE$
$\quad | \ \{s1, \ s2\} \subseteq SEQ\_VAL$
$\quad \quad \wedge \ (Seq \ {}^\sim) \ s2 \ prefix_Z \ (Seq \ {}^\sim) \ s1$
$\quad \bullet \ (Seq \ {}^\sim) \ (Seq \ \langle\rangle)$
$\quad \quad \quad prefix_Z \ (Seq \ {}^\sim) \ (s1 \ SeqDif_R \ s2)$

REL_$\lhd$_Eval_thm1

$\vdash \forall \ b : BINDING; \ a : ALPHABET; \ v : VALUE$
$\quad \bullet \ Eval \ (a \lhd b, \ Val \ v) = v$

REL_$\lhd$_Eval_thm2

$\vdash \forall \ b : BINDING;$
$\quad \quad a : ALPHABET;$
$\quad \quad r : RELATION;$
$\quad \quad n1, \ n2 : NAME$
$\quad | \ n1 \in dom \ b \wedge n1 \in a \wedge n2 \in dom \ b \wedge n2 \in a$
$\quad \bullet \ Eval \ (a \lhd b, \ Rel \ (r, \ Var \ n1, \ Var \ n2))$
$\quad \quad = Bool \ ((Eval \ (b, \ Var \ n1), \ Eval \ (b, \ Var \ n2)) \in r)$

REL_Prefix$_Z$_id_thm

$\vdash \forall \ s : seq \ VALUE \bullet s \ prefix_Z \ s$

REL_Prefix$_Z$_id_thm1

$\vdash \forall \ s : VALUE$
$\quad | \ s \in SEQ\_VAL$
$\quad \bullet \ (Seq \ {}^\sim) \ s \ prefix_Z \ (Seq \ {}^\sim) \ s$

REL_Seq$_Z$_id_thm1

$\vdash \forall \ s1, \ s2 : seq \ VALUE \bullet Seq \ s1 = Seq \ s2 \Leftrightarrow s1 = s2$

REL_Seq$_Z$_inv_id_thm

$\vdash \forall \ v1, \ v2 : VALUE$
$\quad | \ v1 \in ran \ Seq \wedge v2 \in ran \ Seq$

$\bullet\ (Seq \sim)\ v1 = (Seq \sim)\ v2 \Leftrightarrow v1 = v2$

$\boldsymbol{REL\_Equals_{R}\_\wedge_{R}\_alphabet\_ext\_thm1}$

$$\vdash \forall\ a : ALPHABET;\ n1, n2 : NAME;\ r : REL\_PREDICATE \\ \mid (a, n1, Var\ n2) \in WF\_Equals_R \wedge a \subseteq r.1 \\ \bullet =_R (a, n1, Var\ n2) \wedge_R r \\ = =_R (r.1, n1, Var\ n2) \wedge_R r$$

$\boldsymbol{REL\_\lhd_{R}\_\rhd_{R}\_idem\_thm2}$

$$\vdash \forall\ u1, u2 : REL\_PREDICATE \\ \mid u1.1 = u2.1 \\ \bullet (u1 \wedge_R u2) \lhd_R u1 \rhd_R u1 \vee_R u2 = u2$$

$\boldsymbol{ALPHABET\_homogeneous\_set\_dif\_thm2}$

$$\vdash \forall\ a1, a2 : ALPHABET \\ \mid a1 \in homogeneous \wedge a2 \in homogeneous \\ \bullet a1 \setminus a2 \in homogeneous$$

$\boldsymbol{ALPHABET\_homogeneous\_\cup\_thm1}$

$$\vdash \forall\ a1, a2 : ALPHABET \\ \mid a1 \in homogeneous \wedge a2 \in homogeneous \\ \bullet a1 \cup a2 \in homogeneous$$

$\boldsymbol{REL\_Equals\_exps\_{R}\_\wedge_{R}\_alphabet\_ext\_thm}$

$$\vdash \forall\ a : ALPHABET; \\ n1, n2 : NAME; \\ rel : RELATION; \\ v : VALUE; \\ r : REL\_PREDICATE \\ \mid (a, Rel\ (rel, Var\ n1, Var\ n2), Val\ v) \\ \in WF\_ALPHABET\_EXPRESSION \\ \wedge a \subseteq r.1 \\ \bullet =_{+R} (a, Rel\ (rel, Var\ n1, Var\ n2), Val\ v) \wedge_R r \\ = =_{+R} (r.1, Rel\ (rel, Var\ n1, Var\ n2), Val\ v) \\ \wedge_R r$$

$\boldsymbol{REL\_Equals\_exps\_{R}\_\vee_{R}\_alphabet\_ext\_thm}$

$$\vdash \forall\ a : ALPHABET; \\ n1, n2 : NAME; \\ rel : RELATION; \\ v : VALUE; \\ r : REL\_PREDICATE \\ \mid (a, Rel\ (rel, Var\ n1, Var\ n2), Val\ v) \\ \in WF\_ALPHABET\_EXPRESSION$$

$\land\ a \subseteq r.1$

$\bullet =_{+R} (a, Rel\ (rel, Var\ n1, Var\ n2), Val\ v) \lor_R r$
$= =_{+R} (r.1, Rel\ (rel, Var\ n1, Var\ n2), Val\ v)$
$\lor_R r$

REL_⊕_idem_thm

$\vdash \forall\ b : BINDING; n : NAME; v : VALUE$
$\mid n \in dom\ b \land b\ n = v$
$\bullet\ b \oplus \{n \mapsto v\} = b$

REL_Subst_R_∧_R_idem_thm

$\vdash \forall\ r : REL\_PREDICATE; n : NAME; v : VALUE$
$\mid n \in r.1$
$\bullet\ /_R\ (r, Val\ v, n) \land_R =_R (r.1, n, Val\ v)$
$= r \land_R =_R (r.1, n, Val\ v)$

REL_∧_R_⇒_R_simpl_thm

$\vdash \forall\ u1, u2 : REL\_PREDICATE$
$\bullet\ u1 \land_R u1 \Rightarrow_R u2 = u1 \land_R u2$

REL_∧_R_⇒_R_simpl_thm1

$\vdash \forall\ u1, u2 : REL\_PREDICATE$
$\mid u1.1 \subseteq u2.1$
$\bullet\ u2 \land_R u1 \Rightarrow_R u2 = u2$

REL_∨_R_∧_R_⇒_R_simpl_thm

$\vdash \forall\ u1, u2 : REL\_PREDICATE$
$\mid u1.1 \subseteq u2.1$
$\bullet\ (u1 \lor_R u2) \land_R u1 \Rightarrow_R u2 = u2$

REL_⟨_R_⇒_R_⟩_R_thm

$\vdash \forall\ u1, u2 : REL\_PREDICATE$
$\mid u1.1 = u2.1$
$\bullet\ \langle_R\ u1 \Rightarrow_R u2\ \rangle_R = True_R\ \varnothing$
$\Leftrightarrow u1 \Rightarrow_R u2 = True_R\ u1.1$

BINDINGS_empty_dom_thm

$\vdash \{b : BINDING \mid dom\ b = \{\}\} = \{\{\}\}$

REL_◁_R_▷_R_cases_thm

$\vdash \forall\ u1, u2, b : REL\_PREDICATE$
$\mid (u1, b, u2) \in WF\_Cond_R$
$\bullet\ u1 \lhd_R b \rhd_R u2$
$= (b \land_R u1) \lhd_R b \rhd_R \lnot_R b \land_R u2$

REL_UnrestTypedVar_False_R_thm

$\vdash \forall\ a : ALPHABET; n : NAME; T : \mathbb{P}\ VALUE$

$| \ n \in a$

$\bullet \ unrestTypedVar \ (False_R \ a, \ n, \ T) \Leftrightarrow true$

***VALUE_SEQ_EVENT_VAL_thm*1**

$\vdash SEQ\_EVENT\_VAL \subseteq VALUE$

VALUE_SEQ_VAL_thm

$\vdash \forall \ s : SEQ\_VAL \bullet (Seq \ \sim) \ s \in seq \ VALUE$

***REL_inv_Seq_thm*1**

$\vdash \forall \ s : SEQ\_VAL \bullet Seq \ ((Seq \ \sim) \ s) = s$

***VALUE_SEQ_VAL_thm*1**

$\vdash \forall \ s : seq \ VALUE \bullet Seq \ s \in SEQ\_VAL$

VALUE_Prefix_thm

$\vdash (\_ \leq_R \_)$
$= \{s1, \ s2 : seq \ VALUE$
$| \ s1 \ prefix_Z \ s2$
$\bullet (Seq \ s1, \ Seq \ s2)\}$

***ALPHABET_$\subseteq$_thm*1**

$\vdash \forall \ a1, \ a2 : ALPHABET \mid a1 \subseteq a2 \land \neg \ x2 \in a2 \bullet \neg \ x2 \in a1$

ALPHABET_$\neq$_thm

$\vdash \forall \ a1, \ a2 : ALPHABET$
$\bullet \ a1 \neq a2 \Rightarrow a1 \cap a2 = \varnothing \land a1 \cap a2 = \varnothing \Rightarrow a1 \neq a2$

BINDINGS_$\cup$_thm

$\vdash \forall \ b1, \ b2 : BINDING$
$| \ dom \ b1 \lhd b2 = dom \ b2 \lhd b1$
$\bullet \ b1 \cup b2 \in BINDING$

***BINDINGS_$\cup$_thm*1**

$\vdash \forall \ b1, \ b2 : BINDING$
$| \ dom \ b1 \cap dom \ b2 = \{\}$
$\bullet \ b1 \cup b2 \in BINDING$

BINDINGS_dom_$\cup$_thm

$\vdash \forall \ b1, \ b2 : BINDING; \ n : NAME$
$\bullet \ n \in dom \ (b1 \cup b2) \Leftrightarrow n \in dom \ b1 \lor n \in dom \ b2$

***BINDINGS_dom_$\cup$_thm*1**

$\vdash \forall \ b1, \ b2 : BINDING; \ n : NAME$
$\bullet \ dom \ (b1 \cup b2) = dom \ b1 \cup dom \ b2$

***BINDINGS_dom_$\cup$_thm*2**

$\vdash \forall \ b1, \ b2 : BINDING \bullet dom \ (b1 \cup b2) = dom \ b1 \cup dom \ b2$

BINDINGS_$\lhd$_$\cup$_com_thm

$\vdash \forall \ f, \ g : BINDING$

$\bullet\ undashed \lhd f \cup dashed \lhd g$
$= dashed \lhd g \cup undashed \lhd f$

$\boldsymbol{BINDINGS\_\lhd\_\cup\_\lhd\_app\_thm2}$
$\vdash \forall f : BINDING;\ g : BINDING;\ n : dom\ f$
$\mid n \in undashed$
$\bullet\ (undashed \lhd f \cup dashed \lhd g)\ n = f\ n$

$\boldsymbol{BINDINGS\_\lhd\_\cup\_\lhd\_app\_thm3}$
$\vdash \forall f : BINDING;\ g : BINDING;\ n : dom\ f$
$\mid n \in dashed$
$\bullet\ (dashed \lhd f \cup undashed \lhd g)\ n = f\ n$

$\boldsymbol{REL\_\lhd\_dom\_thm1}$
$\vdash \forall b : BINDING;\ a : ALPHABET;\ n : NAME$
$\mid n \in dom\ (a \lhd b) \land n \in a$
$\bullet\ n \in dom\ b$

$\boldsymbol{REL\_\lhd\_dom\_thm2}$
$\vdash \forall b : BINDING;\ a : ALPHABET \bullet dom\ (a \lhd b) = a \cap dom\ b$

$\boldsymbol{REL\_\lhd\_dom\_thm3}$
$\vdash \forall b : BINDING;\ a : ALPHABET;\ n : NAME$
$\mid n \in dom\ b \land \neg\ n \in a$
$\bullet\ \neg$
$n \in dom\ (a \lhd b)$

$\boldsymbol{REL\_\lhd\_idem\_thm}$
$\vdash \forall b : BINDING;\ a : ALPHABET \bullet a \lhd a \lhd b = a \lhd b$

$\boldsymbol{REL\_\leq_R\_trans\_thm}$
$\vdash \forall a, b, c : SEQ\_VAL \bullet a \leq_R b \land b \leq_R c \Rightarrow a \leq_R c$

$\boldsymbol{BINDINGS\_\lhd\_idem\_thm3}$
$\vdash \forall a : ALPHABET;\ b : BINDING \bullet a \lhd a \lhd b = a \lhd b$

$\boldsymbol{BINDINGS\_dom\_\lhd\_thm}$
$\vdash \forall a : ALPHABET;\ b : BINDING;\ n : NAME$
$\mid n \in a \land n \in dom\ (a \lhd b)$
$\bullet\ n \in dom\ b$

$\boldsymbol{REL\_\Rightarrow_R\_\land_R\_distr\_thm}$
$\vdash \forall a, b, c : REL\_PREDICATE$
$\bullet\ (a \Rightarrow_R b) \land_R a \Rightarrow_R c = a \Rightarrow_R b \land_R c$

$\boldsymbol{ALPHABET\_homogeneous\_dash\_thm1}$
$\vdash \forall a : ALPHABET;\ n : NAME$
$\mid a \in homogeneous \land n \in undashed \land dash\ n \in a$
$\bullet\ n \in a$

$\textbf{\textit{REL\_Eval\_Fun}}_{\mathbf{1}}\textbf{\textit{\_thm}}$

$$\begin{array}{l}
\vdash \forall\ b : BINDING;\ f : UNARY_F;\ e1 : EXPRESSION \\
\quad \mid (b,\ e1) \in WF_BINDING_EXPRESSION_R \\
\quad \bullet\ Eval\ (b,\ Fun_1\ (f,\ e1)) = f\ (Eval\ (b,\ e1))
\end{array}$$

$\textbf{\textit{REL\_FV\_Fun}}_{\mathbf{1}}\textbf{\textit{\_thm}}$

$$\begin{array}{l}
\vdash \forall\ f : UNARY_F;\ e1 : EXPRESSION \\
\quad \bullet\ FV\ (Fun_1\ (f,\ e1)) = FV\ e1
\end{array}$$

$\textbf{\textit{REL\_PREDICATE\_VarT}}_{\boldsymbol{R}}\textbf{\textit{\_thm}}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\ n : NAME;\ T : SET_VAL \\
\quad \mid (a,\ n,\ T) \in WF_VarT_{R_EndT\,R} \\
\quad \bullet\ varT_R\ (a,\ n,\ T) \in REL_PREDICATE
\end{array}$$

$\textbf{\textit{REL\_PREDICATE\_EndT}}_{\boldsymbol{R}}\textbf{\textit{\_thm}}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\ n : NAME;\ T : SET_VAL \\
\quad \mid (a,\ n,\ T) \in WF_VarT_{R_EndT\,R} \\
\quad \bullet\ endT_R\ (a,\ n,\ T) \in REL_PREDICATE
\end{array}$$

$\textbf{\textit{ALPHABET\_comp\_}}\boldsymbol{\Rightarrow}\textbf{\textit{\_contr\_comp\_thm3}}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\ n : NAME \\
\quad \mid n \in a \land n \in undashed \land (a,\ a) \in composable \\
\quad \bullet\ (a,\ a \cup (a \setminus \{n,\ dash\ n\})) \in composable
\end{array}$$

$\textbf{\textit{REL\_PREDICATE\_Var}}_{\boldsymbol{R}}\textbf{\textit{\_Semi}}_{\boldsymbol{R}}\textbf{\textit{\_Assign}}_{\boldsymbol{R}}\textbf{\textit{\_thm}}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\ n : NAME;\ v : VALUE;\ T : SET_VAL \\
\quad \mid a \in homogeneous \land n \in undashed \land \{n,\ dash\ n\} \subseteq a \\
\quad \bullet\ var_R\ (a,\ n)\ ;_R\ Assign_R\ (a,\ \langle n\rangle,\ \langle Val\ v\rangle) \\
\quad\quad \in REL_PREDICATE
\end{array}$$

$\textbf{\textit{REL\_PREDICATE\_Var}}_{\boldsymbol{R}}\textbf{\textit{\_Semi}}_{\boldsymbol{R}}\textbf{\textit{\_Assign}}_{\boldsymbol{R}}\textbf{\textit{\_thm2}}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\ n : NAME;\ v : VALUE;\ T : SET_VAL \\
\quad \mid a \in homogeneous \\
\quad\quad \land\ n \in undashed \\
\quad\quad \land\ \{n,\ dash\ n\} \subseteq a \\
\quad\quad \land\ v \in (Set\ {}^\sim)\ T \\
\quad \bullet\ var_R\ (a,\ n)\ ;_R\ Assign_R\ (a,\ \langle n\rangle,\ \langle Val\ v\rangle) \\
\quad\quad \in REL_PREDICATE
\end{array}$$

$\textbf{\textit{REL\_PREDICATE\_Var}}_{\boldsymbol{R}}\textbf{\textit{\_Semi}}_{\boldsymbol{R}}\textbf{\textit{\_Assign}}_{\boldsymbol{R}}\textbf{\textit{\_thm3}}$

$$\begin{array}{l}
\vdash \forall\ a : ALPHABET;\ n : NAME;\ T : SET_VAL \\
\quad \mid a \in homogeneous \land n \in undashed \land \{n,\ dash\ n\} \subseteq a \\
\quad \bullet\ \{v : VALUE \\
\quad\quad \mid v \in (Set\ {}^\sim)\ T \\
\quad\quad \bullet\ var_R\ (a,\ n)\ ;_R\ Assign_R\ (a,\ \langle n\rangle,\ \langle Val\ v\rangle)\}
\end{array}$$

$\subseteq$ *REL_PREDICATE*

ALPHABET_dash_n_∩_undashed_thm

$\vdash \forall\ n : NAME \bullet \{dash\ n\} \cap undashed = \varnothing$

REL_PREDICATE_∈_WF_Assign$_R$_thm

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ v : VALUE$
$\quad |\ n \in a \land n \in undashed \land a \in homogeneous$
$\quad \bullet\ (a,\ \langle n \rangle,\ \langle Val\ v \rangle) \in WF\_Assign_R$

REL_PREDICATE_Assign$_R$_thm

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ v : VALUE$
$\quad |\ (a,\ \langle n \rangle,\ \langle Val\ v \rangle) \in WF\_Assign_R$
$\quad\ \ \land n \in undashed$
$\quad\ \ \land \{n,\ dash\ n\} \subseteq a$
$\quad\ \ \land a \in homogeneous$
$\quad \bullet\ Assign_R\ (a,\ \langle n \rangle,\ \langle Val\ v \rangle) \in REL\_PREDICATE$

REL_PREDICATE_Assign$_R$_alphabet_thm2

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ v : VALUE$
$\quad |\ (a,\ \langle n \rangle,\ \langle Val\ v \rangle) \in WF\_Assign_R$
$\quad\ \ \land n \in undashed$
$\quad\ \ \land \{n,\ dash\ n\} \subseteq a$
$\quad\ \ \land a \in homogeneous$
$\quad \bullet\ (Assign_R\ (a,\ \langle n \rangle,\ \langle Val\ v \rangle)).1 = a$

REL_PREDICATE_Assign$_R$_Semi$_R$_End$_R$_thm

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ v : VALUE;\ T : SET\_VAL$
$\quad |\ a \in homogeneous \land n \in undashed \land \{n,\ dash\ n\} \subseteq a$
$\quad \bullet\ Assign_R\ (a,\ \langle n \rangle,\ \langle Val\ v \rangle)\ ;_R\ end_R\ (a,\ n)$
$\quad\ \ \in REL\_PREDICATE$

REL_PREDICATE_Assign$_R$_Semi$_R$_End$_R$_thm2

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ v : VALUE;\ T : SET\_VAL$
$\quad |\ a \in homogeneous$
$\quad\ \ \land n \in undashed$
$\quad\ \ \land \{n,\ dash\ n\} \subseteq a$
$\quad\ \ \land v \in (Set\ ^\sim)\ T$
$\quad \bullet\ Assign_R\ (a,\ \langle n \rangle,\ \langle Val\ v \rangle)\ ;_R\ end_R\ (a,\ n)$
$\quad\ \ \in REL\_PREDICATE$

REL_PREDICATE_Assign$_R$_Semi$_R$_End$_R$_thm3

$\vdash \forall\ a : ALPHABET;\ n : NAME;\ T : SET\_VAL$
$\quad |\ a \in homogeneous \land n \in undashed \land \{n,\ dash\ n\} \subseteq a$
$\quad \bullet\ \{v : VALUE$

$| \ v \in (Set \sim) \ T$
$\bullet \ Assign_R \ (a, \langle n \rangle, \langle Val \ v \rangle) \ ;_R \ end_R \ (a, n)\}$
$\subseteq REL\_PREDICATE$

$\boldsymbol{REL\_PREDICATE\_VarT_R\_alphabet\_thm}$
$\vdash \forall \ a : ALPHABET; \ n : NAME; \ T : SET\_VAL$
$| \ (a, n, T) \in WF\_VarT_{R\_EndTR}$
$\bullet \ (varT_R \ (a, n, T)).1 = a \setminus \{n\}$

$\boldsymbol{REL\_PREDICATE\_EndT_R\_alphabet\_thm}$
$\vdash \forall \ a : ALPHABET; \ n : NAME; \ T : SET\_VAL$
$| \ (a, n, T) \in WF\_VarT_{R\_EndTR}$
$\bullet \ (endT_R \ (a, n, T)).1 = a \setminus \{dash \ n\}$

$\boldsymbol{REL\_\oplus\_\oplus\_thm}$ $\vdash \forall \ b : BINDING; \ n : NAME; \ v1, v2 : VALUE$
$\bullet \ b \oplus \{n \mapsto v1\} \oplus \{n \mapsto v2\} = b \oplus \{n \mapsto v2\}$

$\boldsymbol{REL\_UnrestTypedVar\_\vee_R\_thm}$
$\vdash \forall \ u1, u2 : REL\_PREDICATE; \ n : NAME; \ T : \mathbb{P} \ VALUE$
$\bullet \ unrestTypedVar \ (u1, n, T)$
$\wedge \ unrestTypedVar \ (u2, n, T)$
$\Rightarrow \ unrestTypedVar \ (u1 \vee_R u2, n, T)$

$\boldsymbol{REL\_UnrestVar\_Contract_R\_dist\_thm}$
$\vdash \forall \ a : ALPHABET; \ P : REL\_PREDICATE$
$\bullet \ UnrestVar \ P \setminus a \subseteq UnrestVar \ (P -_R a)$

$\boldsymbol{REL\_CONDITION\_Contract_R\_thm}$
$\vdash \forall \ a : ALPHABET; \ P : REL\_CONDITION$
$\bullet \ P -_R a \in REL\_CONDITION$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_cases\_thm1}$
$\vdash \forall \ u1, u2, b : REL\_PREDICATE$
$| \ (u1, b, u2) \in WF\_Cond_R$
$\bullet \ u1 \lhd_R b \rhd_R u2 = u1 \lhd_R b \rhd_R \neg_R b \wedge_R u2$

$\boldsymbol{REL\_\lhd_R\_\rhd_R\_cases\_thm2}$
$\vdash \forall \ u1, u2, b : REL\_PREDICATE$
$| \ (u1, b, u2) \in WF\_Cond_R$
$\bullet \ u1 \lhd_R b \rhd_R u2 = (b \wedge_R u1) \lhd_R b \rhd_R u2$

$\boldsymbol{ALPHABET\_n1\_\neq\_dash\_n2\_thm1}$
$\vdash \forall \ n1, n2 : NAME$
$| \ n1 \neq n2 \wedge n1 \in undashed \wedge n2 \in undashed$
$\bullet \ n2 \neq dash \ n1 \wedge dash \ n1 \neq n2$

9 THE Z THEORY utp-okay

9.1 Parents

$utp{-}rel$

9.2 Global Variables

$\boldsymbol{okay}$ $NAME$
$\boldsymbol{ALPHABET\_OKAY}$
$\mathbb{P}\ NAME$
$\boldsymbol{unrestOKAY}$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{B}$
$\boldsymbol{unrestOKAY'}$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{B}$
$\boldsymbol{OKAY}$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{OKAY'}$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$(\_\ \boldsymbol{\sigma_f})$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$(\_\ \boldsymbol{\sigma_t})$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

9.3 Fixity

$\boldsymbol{fun\ 0\ rightassoc}$
$(\_\ \sigma_f)\ (\_\ \sigma_t)$

9.4 Axioms

$\boldsymbol{okay}$ $\vdash okay \in NAME \land okay \in undashed$

$\boldsymbol{Constraint\ 1} \vdash (\forall\ b : BINDING \mid okay \in dom\ b \bullet b\ okay \in BOOL\_VAL)$
$\quad \land (\forall\ b : BINDING$
$\quad\quad \mid dash\ okay \in dom\ b$
$\quad\quad \bullet b\ (dash\ okay) \in BOOL\_VAL)$

$\boldsymbol{unrestOKAY}$
$\boldsymbol{unrestOKAY'}$ $\vdash \{unrestOKAY, unrestOKAY'\} \subseteq REL\_PREDICATE \rightarrow$
$\quad \land (\forall\ r : REL\_PREDICATE$
$\quad\quad \bullet (unrestOKAY\ r$
$\quad\quad\quad \Leftrightarrow unrestTypedVar\ (r, okay, BOOL\_VAL))$
$\quad\quad \land (unrestOKAY'\ r$
$\quad\quad\quad \Leftrightarrow unrestTypedVar\ (r, dash\ okay, BOOL\_VAL)))$

$\boldsymbol{OKAY}$ $\vdash OKAY \in REL\_PREDICATE$
$\quad \land\ OKAY = =_R (ALPHABET\_OKAY,\ okay,\ Val\ (Bool\ true))$

$\boldsymbol{OKAY'}$ $\vdash OKAY' \in REL\_PREDICATE$
$\quad \land\ OKAY'$
$\quad\quad = =_R (ALPHABET\_OKAY,\ dash\ okay,\ Val\ (Bool\ true))$

$\_\ \boldsymbol{\sigma_f}$ $\vdash (\_\ \sigma_f) \in REL\_PREDICATE \nrightarrow REL\_PREDICATE$
$\quad \land\ (\forall\ d : REL\_PREDICATE$
$\quad\quad |\ dash\ okay \in d.1$
$\quad\quad \bullet\ d\ \sigma_f = /_R\ (d,\ Val\ (Bool\ false),\ dash\ okay))$

$\_\ \boldsymbol{\sigma_t}$ $\vdash (\_\ \sigma_t) \in REL\_PREDICATE \rightarrow REL\_PREDICATE$
$\quad \land\ (\forall\ d : REL\_PREDICATE$
$\quad\quad |\ dash\ okay \in d.1$
$\quad\quad \bullet\ d\ \sigma_t = /_R\ (d,\ Val\ (Bool\ true),\ dash\ okay))$

9.5 Definitions

ALPHABET_OKAY
$\vdash ALPHABET\_OKAY = \{okay,\ dash\ okay\}$

9.6 Theorems

OKAY_⊆_NAME_thm
$\vdash \{okay,\ dash\ okay\} \subseteq NAME$

OKAY_values_thm
$\vdash \forall\ b : BINDING$
$\quad |\ okay \in dom\ b$
$\quad \bullet\ b\ okay = Bool\ true \lor b\ okay = Bool\ false$

OKAY_DASH_alues_thm
$\vdash \forall\ b : BINDING$
$\quad |\ dash\ okay \in dom\ b$
$\quad \bullet\ b\ (dash\ okay) = Bool\ true$
$\quad\quad \lor\ b\ (dash\ okay) = Bool\ false$

OKAY_clauses_thm
$\vdash \forall\ b : BINDING$
$\quad |\ \{okay,\ dash\ okay\} \subseteq dom\ b$
$\quad \bullet\ (\neg\ b\ okay = Bool\ true \Rightarrow b\ okay = Bool\ false)$
$\quad\quad \land\ (\neg\ b\ okay = Bool\ false \Rightarrow b\ okay = Bool\ true)$
$\quad\quad \land\ (\neg$

$b\ (dash\ okay) = Bool\ true$
$\Rightarrow b\ (dash\ okay) = Bool\ false)$
$\wedge\ (\neg$
$b\ (dash\ okay) = Bool\ false$
$\Rightarrow b\ (dash\ okay) = Bool\ true)$
$\wedge\ (b\ okay = Bool\ true \Rightarrow \neg\ b\ okay = Bool\ false)$
$\wedge\ (b\ okay = Bool\ false \Rightarrow \neg\ b\ okay = Bool\ true)$
$\wedge\ (b\ (dash\ okay) = Bool\ true$
$\Rightarrow \neg$
$b\ (dash\ okay) = Bool\ false)$
$\wedge\ (b\ (dash\ okay) = Bool\ false$
$\Rightarrow \neg$
$b\ (dash\ okay) = Bool\ true)$

OKAY_Equals_true_thm

$\vdash \forall\ a : ALPHABET;\ n : NAME$
$\mid ALPHABET\_OKAY \subseteq a \wedge n \in ALPHABET\_OKAY$
$\bullet =_R (a, n, Val\ (Bool\ true))$
$= \neg_R (=_R (a, n, Val\ (Bool\ false)))$

OKAY_Equals_false_thm

$\vdash \forall\ a : ALPHABET;\ n : NAME$
$\mid ALPHABET\_OKAY \subseteq a \wedge n \in ALPHABET\_OKAY$
$\bullet =_R (a, n, Val\ (Bool\ false))$
$= \neg_R (=_R (a, n, Val\ (Bool\ true)))$

OKAY_okay_WF_Equals$_R$_thm

$\vdash (\{okay\}, okay, Val\ (Bool\ false)) \in WF\_Equals_R$

OKAY_ALPHABET_OKAY_thm

$\vdash ALPHABET\_OKAY \in ALPHABET$

OKAY_okay_WF_Equals$_R$_thm1

$\vdash \forall\ a : ALPHABET$
$\mid \{okay, dash\ okay\} \subseteq a$
$\bullet (a, dash\ okay, Var\ okay) \in WF\_Equals_R$

OKAY_okay_WF_Equals$_R$_thm2

$\vdash \forall\ a : ALPHABET;\ v : VALUE$
$\mid \{okay, dash\ okay\} \subseteq a$
$\bullet (a, okay, Val\ v) \in WF\_Equals_R$
$\wedge (a, dash\ okay, Val\ v) \in WF\_Equals_R$

OKAY_OKAY_alphabet_thm

$\vdash OKAY.1 = \{okay, dash\ okay\}$

$\boldsymbol{OKAY\_OKAY\_DASH\_alphabet\_thm}$

$\vdash OKAY'.1 = \{okay, dash\ okay\}$

$\boldsymbol{OKAY\_okay\_dash\_converge\_\wedge_R\_distr\_thm}$

$\vdash \forall r1, r2 : REL\_PREDICATE$
$| \ dash\ okay \in r1.1 \wedge dash\ okay \in r2.1$
$\bullet (r1 \wedge_R r2)\ \sigma_t = (r1\ \sigma_t) \wedge_R r2\ \sigma_t$

$\boldsymbol{OKAY\_okay\_dash\_converge\_\vee_R\_distr\_thm}$

$\vdash \forall r1, r2 : REL\_PREDICATE$
$| \ dash\ okay \in r1.1 \wedge dash\ okay \in r2.1$
$\bullet (r1 \vee_R r2)\ \sigma_t = (r1\ \sigma_t) \vee_R r2\ \sigma_t$

$\boldsymbol{OKAY\_okay\_dash\_converge\_\Rightarrow_R\_distr\_thm}$

$\vdash \forall r1, r2 : REL\_PREDICATE$
$| \ dash\ okay \in r1.1 \wedge dash\ okay \in r2.1$
$\bullet (r1 \Rightarrow_R r2)\ \sigma_t = (r1\ \sigma_t) \Rightarrow_R r2\ \sigma_t$

$\boldsymbol{OKAY\_okay\_dash\_converge\_\neg_R\_distr\_thm}$

$\vdash \forall r : REL\_PREDICATE$
$| \ dash\ okay \in r.1$
$\bullet \neg_R\ r\ \sigma_t = \neg_R\ (r\ \sigma_t)$

$\boldsymbol{OKAY\_okay\_dash\_diverge\_\wedge_R\_distr\_thm}$

$\vdash \forall r1, r2 : REL\_PREDICATE$
$| \ dash\ okay \in r1.1 \wedge dash\ okay \in r2.1$
$\bullet (r1 \wedge_R r2)\ \sigma_f = (r1\ \sigma_f) \wedge_R r2\ \sigma_f$

$\boldsymbol{OKAY\_okay\_dash\_diverge\_\vee_R\_distr\_thm}$

$\vdash \forall r1, r2 : REL\_PREDICATE$
$| \ dash\ okay \in r1.1 \wedge dash\ okay \in r2.1$
$\bullet (r1 \vee_R r2)\ \sigma_f = (r1\ \sigma_f) \vee_R r2\ \sigma_f$

$\boldsymbol{OKAY\_okay\_dash\_diverge\_\Rightarrow_R\_distr\_thm}$

$\vdash \forall r1, r2 : REL\_PREDICATE$
$| \ dash\ okay \in r1.1 \wedge dash\ okay \in r2.1$
$\bullet (r1 \Rightarrow_R r2)\ \sigma_f = (r1\ \sigma_f) \Rightarrow_R r2\ \sigma_f$

$\boldsymbol{OKAY\_okay\_dash\_diverge\_\neg_R\_distr\_thm}$

$\vdash \forall r : REL\_PREDICATE$
$| \ dash\ okay \in r.1$
$\bullet \neg_R\ r\ \sigma_f = \neg_R\ (r\ \sigma_f)$

$\boldsymbol{OKAY\_OKAY\_def\_\in\_WF\_Equals_R\_thm}$

$\vdash (ALPHABET\_OKAY, okay, Val\ (Bool\ true)) \in WF\_Equals_R$

$\boldsymbol{OKAY\_not\_OKAY\_def\_\in\_WF\_Equals_R\_thm}$

$\vdash (ALPHABET\_OKAY, okay, Val\ (Bool\ false)) \in WF\_Equals_R$

OKAY_OKAY_∈_REL_PREDICATE_thm

$\vdash OKAY \in REL\_PREDICATE$

OKAY_okay_dash_converge_is_REL_PREDICATE_thm

$\vdash \forall\ r : REL\_PREDICATE$
$\quad | \ dash\ okay \in r.1$
$\quad \bullet\ r\ \sigma_t \in REL\_PREDICATE$

OKAY_okay_dash_diverge_is_REL_PREDICATE_thm

$\vdash \forall\ r : REL\_PREDICATE$
$\quad | \ dash\ okay \in r.1$
$\quad \bullet\ r\ \sigma_f \in REL\_PREDICATE$

OKAY_okay_dash_converge_alphabet_thm

$\vdash \forall\ r : REL\_PREDICATE$
$\quad | \ dash\ okay \in r.1$
$\quad \bullet\ (r\ \sigma_t).1 = r.1$

OKAY_okay_dash_diverge_alphabet_thm

$\vdash \forall\ r : REL\_PREDICATE$
$\quad | \ dash\ okay \in r.1$
$\quad \bullet\ (r\ \sigma_f).1 = r.1$

OKAY_okay_dash_converge_subst_thm

$\vdash \forall\ r : REL\_PREDICATE$
$\quad | \ dash\ okay \in r.1$
$\quad \bullet\ r \wedge_R =_R (r.1,\ dash\ okay,\ Val\ (Bool\ true))$
$\quad\ \ = (r\ \sigma_t)$
$\quad\quad \wedge_R =_R (r.1,\ dash\ okay,\ Val\ (Bool\ true))$

OKAY_okay_dash_diverge_subst_thm

$\vdash \forall\ r : REL\_PREDICATE$
$\quad | \ dash\ okay \in r.1$
$\quad \bullet\ r \wedge_R =_R (r.1,\ dash\ okay,\ Val\ (Bool\ false))$
$\quad\ \ = (r\ \sigma_f)$
$\quad\quad \wedge_R =_R (r.1,\ dash\ okay,\ Val\ (Bool\ false))$

***OKAY_okay_dash_diverge_subst_thm*1**

$\vdash \forall\ r : REL\_PREDICATE$
$\quad | \ dash\ okay \in r.1$
$\quad \bullet\ r \wedge_R \neg_R (=_R (r.1,\ dash\ okay,\ Val\ (Bool\ true)))$
$\quad\ \ = (r\ \sigma_f)$
$\quad\quad \wedge_R \neg_R$
$\quad\quad\quad (=_R (r.1,\ dash\ okay,\ Val\ (Bool\ true)))$

OKAY_okay_dist_over_$\lhd_R$_$\rhd_R$_dist_thm

$$
\begin{array}{l}
\vdash \forall\ u1,\ u2,\ b : REL\_PREDICATE \\
\quad \mid (u1,\ b,\ u2) \in WF\_Cond_R \\
\quad \bullet\ OKAY \wedge_R u1 \lhd_R b \rhd_R u2 \\
\qquad = (OKAY \wedge_R u1) \lhd_R b \rhd_R OKAY \wedge_R u2
\end{array}
$$

10 THE Z THEORY utp-des

10.1 Parents

$utp\!-\!okay$

10.2 Global Variables

$\boldsymbol{ALPHABET\_DES}$ $\mathbb{P}\ (\mathbb{P}\ NAME)$

$\boldsymbol{DES\_PREDICATE}$

$\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{WF\_DES\_PREDICATE\_PAIR}$

$\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{WF\_DESIGN\_PAIR}$

$(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$

$\boldsymbol{WF\_Assign_D}$ $\mathbb{P}\ (\mathbb{P}\ NAME \times (\mathbb{Z} \leftrightarrow NAME) \times (\mathbb{Z} \leftrightarrow EXPRESSION))$

$\boldsymbol{WF\_Skip_D}$ $\mathbb{P}\ (\mathbb{P}\ NAME)$

$\boldsymbol{DES\_FUNCTION}$ $\mathbb{P}$

$((\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$

$(\_ \vdash_{\boldsymbol{D}} \_)$ $(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{DESIGN}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{\Pi_D}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{Assign_D}$ $\mathbb{P}\ NAME \times (\mathbb{Z} \leftrightarrow NAME) \times (\mathbb{Z} \leftrightarrow EXPRESSION)$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{Top_D}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{Bot_D}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{H1}$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{H1\_healthy}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{H2\_healthy}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{J}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{H2}$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{H2\_J\_healthy}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{H3}$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{H3\_healthy}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{H4\_healthy}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

10.3 Fixity

fun* 0 *rightassoc

$(\_ \vdash_D \_)$

10.4 Axioms

$\_ \vdash_{\boldsymbol{D}} \_$

$$\begin{array}{l} \vdash (\_ \vdash_D \_) \in WF\_DES\_PREDICATE\_PAIR \rightarrow REL\_PREDICATE \\ \quad \wedge (\forall\ d : WF\_DES\_PREDICATE\_PAIR \\ \quad\quad \bullet\ d.1 \vdash_D d.2 \\ \quad\quad\quad = (=_R (d.1.1,\ okay,\ Val\ (Bool\ true)) \wedge_R d.1) \\ \quad\quad\quad\quad \Rightarrow_R =_R (d.1.1,\ dash\ okay,\ Val\ (Bool\ true)) \\ \quad\quad\quad\quad\quad \wedge_R d.2) \end{array}$$

$\boldsymbol{\Pi_D}$

$$\begin{array}{l} \vdash \Pi_D \in WF\_Skip_D \rightarrow REL\_PREDICATE \\ \quad \wedge (\forall\ a : WF\_Skip_D \bullet \Pi_D\ a = True_R\ a \vdash_D \Pi_R\ a) \end{array}$$

$\boldsymbol{Assign_D}$

$$\begin{array}{l} \vdash Assign_D \in WF\_Assign_D \rightarrow REL\_PREDICATE \\ \quad \wedge (\forall\ aa : WF\_Assign_D \\ \quad\quad \bullet\ Assign_D\ aa = True_R\ aa.1 \vdash_D Assign_R\ aa) \end{array}$$

$\boldsymbol{Top_D}$

$$\begin{array}{l} \vdash Top_D \in ALPHABET\_DES \rightarrow DES\_PREDICATE \\ \quad \wedge (\forall\ a : ALPHABET\_DES \\ \quad\quad \bullet\ Top_D\ a = =_R (a,\ okay,\ Val\ (Bool\ false))) \end{array}$$

$\boldsymbol{Bot_D}$

$$\begin{array}{l} \vdash Bot_D \in ALPHABET\_DES \rightarrow DES\_PREDICATE \\ \quad \wedge (\forall\ a : ALPHABET\_DES \bullet Bot_D\ a = True_R\ a) \end{array}$$

$\boldsymbol{H1}$

$$\begin{array}{l} \vdash H1 \in REL\_PREDICATE \rightarrow REL\_PREDICATE \\ \quad \wedge (\forall\ d : REL\_PREDICATE \\ \quad\quad \bullet\ H1\ d \\ \quad\quad\quad = =_R (\{okay\},\ okay,\ Val\ (Bool\ true)) \Rightarrow_R d) \end{array}$$

$\boldsymbol{H1\_healthy}$

$$\begin{array}{l} \vdash H1\_healthy \in \mathbb{P}\ REL\_PREDICATE \\ \quad \wedge H1\_healthy = \{d : REL\_PREDICATE \mid H1\ d = d\} \end{array}$$

$\boldsymbol{H2\_healthy}$

$$\begin{array}{l} \vdash H2\_healthy \in \mathbb{P}\ REL\_PREDICATE \\ \quad \wedge H2\_healthy \\ \quad\quad = \{d : REL\_PREDICATE \\ \quad\quad\quad \mid dash\ okay \in d.1 \end{array}$$

$\land \langle_R$
$\quad /_R\ (d,\ Val\ (Bool\ false),\ dash\ okay)$
$\quad\quad \Rightarrow_R /_R$
$\quad\quad\quad (d,$
$\quad\quad\quad\quad Val\ (Bool\ true),$
$\quad\quad\quad\quad dash\ okay)\ \rangle_R$
$\quad = True_R\ \varnothing\}$

J $\vdash J \in ALPHABET \nrightarrow DES\_PREDICATE$
$\land (\forall\ a' : ALPHABET$
$\quad \mid a' \subseteq dashed \land dash\ okay \in a'$
$\quad \bullet \exists\ a : ALPHABET$
$\quad\quad \mid a \subseteq undashed \land a' = dash\ (\!|\ a\ |\!)$
$\quad\quad \bullet J\ a'$
$\quad\quad\quad = (=_R\ (a \cup a',\ okay,\ Val\ (Bool\ true))$
$\quad\quad\quad\quad \Rightarrow_R =_R$
$\quad\quad\quad\quad\quad (a \cup a',$
$\quad\quad\quad\quad\quad\quad dash\ okay,$
$\quad\quad\quad\quad\quad\quad Val\ (Bool\ true)))$
$\quad\quad\quad\quad \land_R\ \mathit{\Pi}_R\ (a \cup a' \setminus ALPHABET\_OKAY))$

***H*2** $\vdash H2 \in REL\_PREDICATE \nrightarrow REL\_PREDICATE$
$\land (\forall\ d : REL\_PREDICATE$
$\quad \mid dash\ okay \in d.1$
$\quad \bullet H2\ d = d\ ;_R\ J\ (out\_a\ d.1))$

H*2*_J_healthy $\vdash H2\_J\_healthy \in \mathbb{P}\ REL\_PREDICATE$
$\land H2\_J\_healthy$
$\quad = \{d : REL\_PREDICATE$
$\quad\quad \mid dash\ okay \in d.1 \land H2\ d = d\}$

***H*3** $\vdash H3 \in REL\_PREDICATE \rightarrow REL\_PREDICATE$
$\land (\forall\ d : REL\_PREDICATE;\ a : ALPHABET$
$\quad \mid a \in WF\_Skip_R \land (d,\ \mathit{\Pi}_R\ a) \in WF\_Semi_R$
$\quad \bullet H3\ d = d\ ;_R\ \mathit{\Pi}_R\ a)$

H*3*_healthy $\vdash H3\_healthy \in \mathbb{P}\ REL\_PREDICATE$
$\land H3\_healthy = \{d : REL\_PREDICATE \mid H3\ d = d\}$

H*4*_healthy $\vdash H4\_healthy \in \mathbb{P}\ REL\_PREDICATE$
$\land H4\_healthy$
$\quad = \{d : REL\_PREDICATE$
$\quad\quad \mid \forall\ a : ALPHABET$
$\quad\quad\quad \mid (d,\ True_R\ a) \in WF\_Semi_R$

$\bullet\ True_R\ a\ ;_R\ d = True_R\ a\}$

DES_refinement_thm

$\vdash \forall\ d1,\ d2 : WF\_DES\_PREDICATE\_PAIR$
$\quad \mid (d1,\ d2) \in WF\_DESIGN\_PAIR$
$\quad \bullet\ d1.1 \vdash_D d1.2 \sqsubseteq_R d2.1 \vdash_D d2.2$
$\quad\quad = \langle_R\ (d1.1 \wedge_R d2.2) \Rightarrow_R d1.2\ \rangle_R$
$\quad\quad\quad \wedge_R \langle_R\ d1.1 \Rightarrow_R d2.1\ \rangle_R$

DES_Assign$_D$_eval_subst_thm

$\vdash \forall\ a : ALPHABET\_DES;$
$\quad n : NAME;$
$\quad e : EXPRESSION;$
$\quad f : VALUE \nrightarrow VALUE$
$\quad \mid (a,\ \langle n \rangle,\ \langle e \rangle) \in WF\_Assign_D$
$\quad \bullet\ Assign_D\ (a,\ \langle n \rangle,\ \langle e \rangle)$
$\quad\quad ;_R\ Assign_D\ (a,\ \langle n \rangle,\ \langle Fun_1\ (f,\ Var\ n) \rangle)$
$\quad = Assign_D\ (a,\ \langle n \rangle,\ \langle Fun_1\ (f,\ e) \rangle)$

DES_Assign$_D$_$\lhd_R$_$\rhd_R$_subst_thm

$\vdash \forall\ d1,\ d2,\ b : REL\_PREDICATE;$
$\quad a : ALPHABET\_DES;$
$\quad n : NAME;$
$\quad e : EXPRESSION$
$\quad \mid (d1,\ b,\ d2) \in WF\_Cond_D$
$\quad\quad \wedge (Assign_D\ (a,\ \langle n \rangle,\ \langle e \rangle),\ d1) \in WF\_Semi_D$
$\quad\quad \wedge (a,\ \langle n \rangle,\ \langle e \rangle) \in WF\_Assign_D$
$\quad\quad \wedge (b,\ e,\ n) \in WF\_Subst_D$
$\quad \bullet\ Assign_D\ (a,\ \langle n \rangle,\ \langle e \rangle)\ ;_R\ d1 \lhd_R b \rhd_R d2$
$\quad\quad = (Assign_D\ (a,\ \langle n \rangle,\ \langle e \rangle)\ ;_R\ d1) \lhd_R$
$\quad\quad\quad /_R\ (b,\ e,\ n) \rhd_R$
$\quad\quad\quad Assign_D\ (a,\ \langle n \rangle,\ \langle e \rangle)\ ;_R\ d2$

DES_Π_D_left_unit_thm

$\vdash \forall\ a : ALPHABET\_DES;\ d : WF\_DES\_PREDICATE\_PAIR$
$\quad \mid a \in WF\_Skip_D \wedge (\Pi_D\ a,\ d1) \in WF\_Semi_D$
$\quad \bullet\ \Pi_D\ a\ ;_R\ d.1 \vdash_D d.2 = d.1 \vdash_D d.2$

DES_$\lhd_R$_$\rhd_R$_designs_thm

$\vdash \forall\ d1,\ d2 : WF\_DES\_PREDICATE\_PAIR;\ b : REL\_PREDICATE$
$\quad \mid (d1,\ b,\ d2) \in WF\_Cond_D$
$\quad \bullet\ (d1.1 \vdash_D d1.2) \lhd_R b \rhd_R d2.1 \vdash_D d2.2$
$\quad\quad = (d1.1 \lhd_R b \rhd_R d2.1) \vdash_D d1.2 \lhd_R b \rhd_R d2.2$

$\boldsymbol{DES\_Semi_R\_designs\_thm}$

$$
\begin{array}{l}
\vdash \forall\ d1,\ d2 : WF\_DES\_PREDICATE\_PAIR \\
\quad \mid (d1.1,\ d2.1) \in WF\_Semi_D \\
\quad \bullet\ (d1.1 \vdash_D d1.2)\ ;_R\ d2.1 \vdash_D d2.2 \\
\quad\quad = (\neg_R\ (\neg_R\ d1.1\ ;_R\ True_R\ d2.1.1) \\
\quad\quad\quad\quad \wedge_R \neg_R\ (d1.2\ ;_R\ \neg_R\ d2.1)) \\
\quad\quad\quad \vdash_D d1.2\ ;_R\ d2.2
\end{array}
$$

$\boldsymbol{DES\_weakest\_fixed\_point\_designs\_thm}$

$$
\begin{array}{l}
\vdash \forall\ F,\ G : DES\_FUNCTION; \\
\quad\quad fd : DES\_PREDICATE \rightarrow DES\_PREDICATE; \\
\quad\quad pair\_d : WF\_DES\_PREDICATE\_PAIR; \\
\quad\quad d,\ Q : DES\_PREDICATE; \\
\quad\quad fp,\ fq,\ P : DES\_PREDICATE \rightarrow DES\_PREDICATE \\
\quad \bullet\ fd\ (pair\_d.1 \vdash_D pair\_d.2) \\
\quad\quad\quad = F\ pair\_d \vdash_D G\ pair\_d \\
\quad\quad \wedge\ fp\ d = F\ (d,\ pair\_d.2) \\
\quad\quad \wedge\ P\ d = \nu_R\ fp \\
\quad\quad \wedge\ fq\ d = P\ d \Rightarrow_R G\ (P\ d,\ d) \\
\quad\quad \wedge\ Q = \mu_D\ fq \\
\quad\quad \wedge\ \mu_R\ fd = P\ Q \vdash_D Q
\end{array}
$$

$\boldsymbol{DES\_algebraic\_H1\_thm}$

$$
\begin{array}{l}
\vdash \forall\ d : REL\_PREDICATE;\ a : ALPHABET \\
\quad \mid a \in WF\_Skip_R \wedge (\Pi_D\ a,\ d) \in WF\_Semi_R \\
\quad \bullet\ d \in H1\_healthy \\
\quad\quad \Leftrightarrow True_R\ a\ ;_R\ d = True_R\ a \wedge \Pi_D\ a\ ;_R\ d = d
\end{array}
$$

$\boldsymbol{DES\_Semi_R\_designs\_thm1}$

$$
\begin{array}{l}
\vdash \forall\ d1,\ d2 : WF\_DES\_PREDICATE\_PAIR \\
\quad \mid (d1.1,\ d2.1) \in WF\_Semi_D \wedge d1.1.1 \cap dashed = \varnothing \\
\quad \bullet\ (d1.1 \vdash_D d1.2)\ ;_R\ d2.1 \vdash_D d2.2 \\
\quad\quad = (d1.1 \wedge_R \neg_R\ (d1.2\ ;_R\ \neg_R\ d2.1)) \\
\quad\quad\quad \vdash_D d1.2\ ;_R\ d2.2
\end{array}
$$

$\boldsymbol{DES\_\neg_R\_design\_thm}$

$$
\begin{array}{l}
\vdash \forall\ d : WF\_DES\_PREDICATE\_PAIR \\
\quad \bullet\ \neg_R\ (d.1 \vdash_D d.2) \\
\quad\quad = =_R (d.1.1,\ okay,\ Val\ (Bool\ true)) \\
\quad\quad\quad \wedge_R\ d.1 \\
\quad\quad\quad\quad \wedge_R =_R (d.1.1,\ okay,\ Val\ (Bool\ true)) \\
\quad\quad\quad\quad\quad \Rightarrow_R \neg_R\ d.2
\end{array}
$$

$\boldsymbol{DES\_design\_contradiction\_thm}$

$\vdash \forall\ d : DES\_PREDICATE \bullet d \vdash_D \neg_R\ d = d \vdash_D False_R\ d.1$

$\boldsymbol{DES\_\Pi_D\_H1\_\Pi_R\_thm}$

$\vdash \forall\ a : WF\_Skip_D \bullet \Pi_D\ a = H1\ (\Pi_R\ a)$

$\boldsymbol{DES\_post\_H1\_thm}$

$\vdash \forall\ d : WF\_DES\_PREDICATE\_PAIR$
$\bullet\ d.1 \vdash_D d.2 = d.1 \vdash_D H1\ d.2$

$\boldsymbol{DES\_post\_\neg_R\_H1\_thm}$

$\vdash \forall\ d : WF\_DES\_PREDICATE\_PAIR$
$\bullet\ d.1 \vdash_D \neg_R\ d.2 = d.1 \vdash_D \neg_R\ (H1\ d.2)$

$\boldsymbol{DES\_H2\_J\_thm}$ $\vdash H2\_healthy = H2\_J\_healthy$

$\boldsymbol{DES\_H2\_H1\_com\_thm}$

$\vdash \forall\ d : REL\_PREDICATE$
$\mid dash\ okay \in d.1$
$\bullet\ H1\ (H2\ d) = H2\ (H1\ d)$

$\boldsymbol{DES\_J\_Semi_R\_idem\_thm}$

$\vdash \forall\ a' : ALPHABET$
$\mid a' \subseteq dashed \wedge dash\ okay \in a'$
$\bullet\ J\ a'\ ;_R\ J\ a' = J\ a'$

$\boldsymbol{DES\_Designs\_H1\_H2\_thm}$

$\vdash \forall\ d : REL\_PREDICATE$
$\bullet\ d \in DESIGN \Leftrightarrow d \in H1\_healthy \cap H2\_healthy$

10.5 Definitions

$\boldsymbol{ALPHABET\_DES}$ $\vdash ALPHABET\_DES = \{a : ALPHABET \mid ALPHABET\_C$

$\boldsymbol{DES\_PREDICATE}$

$\vdash DES\_PREDICATE$
$= \{u : REL\_PREDICATE$
$\mid u.1 \in ALPHABET\_DES\}$

$\boldsymbol{WF\_DES\_PREDICATE\_PAIR}$

$\vdash WF\_DES\_PREDICATE\_PAIR$
$= \{d1,\ d2 : DES\_PREDICATE$
$\mid d1.1 = d2.1\}$

$\boldsymbol{WF\_DESIGN\_PAIR}$

$\vdash WF\_DESIGN\_PAIR$
$= \{d1,\ d2 : WF\_DES\_PREDICATE\_PAIR$
$\mid d1.1.1 = d2.1.1\}$

$\boldsymbol{WF\_Assign_D} \vdash WF\_Assign_D$
$= \{aa : WF\_Assign_R$
$\mid aa.1 \in ALPHABET\_DES\}$

$\boldsymbol{WF\_Skip_D} \vdash WF\_Skip_D = \{a : ALPHABET\_DES \mid a \in WF\_Skip_R\}$

$\boldsymbol{DES\_FUNCTION} \vdash DES\_FUNCTION$
$= \{f : WF\_DES\_PREDICATE\_PAIR \nrightarrow DES\_PREDICATE$
$\mid \exists\ a : ALPHABET$
$\bullet \forall\ pair : dom\ f;\ u\_ran : ran\ f$
$\bullet\ a = pair.1.1 \land pair.1.1 = u\_ran.1\}$

$\boldsymbol{DESIGN} \vdash DESIGN = ran\ (\_ \vdash_D \_)$

10.6 Theorems

$\boldsymbol{ALPHABET\_DES\_thm}$
$\vdash \forall\ a : ALPHABET\_DES \bullet a \in ALPHABET$

$\boldsymbol{DES\_PREDICATE\_thm}$
$\vdash \forall\ d : DES\_PREDICATE$
$\bullet\ d \in REL\_PREDICATE$
$\land \{okay,\ dash\ okay\} \subseteq d.1$
$\land d.1 \in ALPHABET\_DES$

$\boldsymbol{WF\_DES\_PREDICATE\_PAIR\_thm}$
$\vdash \forall\ pair\_d : WF\_DES\_PREDICATE\_PAIR$
$\bullet\ pair\_d.1 \in DES\_PREDICATE$
$\land pair\_d.2 \in DES\_PREDICATE$
$\land pair\_d.1.1 = pair\_d.2.1$
$\land (pair\_d.2,\ pair\_d.1) \in WF\_DES\_PREDICATE\_PAIR$

$\boldsymbol{DES\_okay\_dash\_okay\_\subseteq\_ALPHABET\_DES\_thm}$
$\vdash \forall\ a : ALPHABET\_DES \bullet \{okay,\ dash\ okay\} \subseteq a$

$\boldsymbol{DES\_PREDICATE\_\vdash_D\_thm}$
$\vdash \forall\ d : WF\_DES\_PREDICATE\_PAIR$
$\bullet\ d.1 \vdash_D d.2 \in DES\_PREDICATE$

$\boldsymbol{DES\_H1\_thm} \vdash \forall\ d : REL\_PREDICATE \bullet H1\ d \in REL\_PREDICATE$

$\boldsymbol{DES\_J\_thm} \vdash \forall\ a' : ALPHABET$
$\mid a' \subseteq dashed \land dash\ okay \in a'$
$\bullet\ J\ a' \in DES\_PREDICATE$

$\boldsymbol{DES\_\vdash_D\_alphabet\_thm}$
$\vdash \forall\ d : WF\_DES\_PREDICATE\_PAIR \bullet (d.1 \vdash_D d.2).1 = d.1.1$

$\boldsymbol{DES\_H1\_alphabet\_thm}$

$\vdash \forall\ d : REL\_PREDICATE \bullet (H1\ \ d).1 = d.1 \cup \{okay\}$

$\boldsymbol{DES\_J\_alphabet\_thm}$

$$\begin{array}{l}\vdash \forall\ a' : ALPHABET\\ \quad \mid a' \subseteq dashed \land dash\ okay \in a'\\ \quad \bullet \exists\ a : ALPHABET\\ \quad\quad \bullet a \subseteq undashed\\ \quad\quad\quad \land a' = dash \llparenthesis\ a\ \rrparenthesis\\ \quad\quad\quad \land (J\ \ a').1 = a \cup a'\end{array}$$

$\boldsymbol{DES\_Semi_R\_J\_comp\_thm}$

$$\begin{array}{l}\vdash \forall\ d : DES\_PREDICATE\\ \quad \bullet (d.1,\ (J\ (out\_a\ \ d.1)).1) \in composable\end{array}$$

$\boldsymbol{DES\_Semi_R\_J\_comp\_thm1}$

$$\begin{array}{l}\vdash \forall\ d : REL\_PREDICATE\\ \quad \mid dash\ okay \in d.1\\ \quad \bullet (d.1,\ (J\ (out\_a\ \ d.1)).1) \in composable\end{array}$$

$\boldsymbol{DES\_Semi_R\_J\_alphabet\_thm}$

$\vdash \forall\ d : DES\_PREDICATE \bullet (d\ ;_R\ J\ (out\_a\ \ d.1)).1 = d.1$

$\boldsymbol{DES\_Semi_R\_J\_alphabet\_thm1}$

$$\begin{array}{l}\vdash \forall\ d : REL\_PREDICATE\\ \quad \mid dash\ okay \in d.1\\ \quad \bullet (d\ ;_R\ J\ (out\_a\ \ d.1)).1 = d.1\end{array}$$

$\boldsymbol{DES\_H2\_thm}$ $\vdash \forall\ d : REL\_PREDICATE$

$$\begin{array}{l}\quad \mid dash\ okay \in d.1\\ \quad \bullet H2\ \ d \in REL\_PREDICATE\end{array}$$

$\boldsymbol{DES\_H2\_alphabet\_thm}$

$$\begin{array}{l}\vdash \forall\ d : REL\_PREDICATE\\ \quad \mid dash\ okay \in d.1\\ \quad \bullet (H2\ \ d).1 = d.1\end{array}$$

$\boldsymbol{DES\_J\_Semi_R\_J\_\in\_comp\_thm}$

$$\begin{array}{l}\vdash \forall\ a' : ALPHABET\\ \quad \mid a' \subseteq dashed \land dash\ okay \in a'\\ \quad \bullet ((J\ \ a').1,\ (J\ \ a').1) \in composable\end{array}$$

$\boldsymbol{DESIGNS\_True_R\_Semi_R\_left\_zero\_thm}$

$$\begin{array}{l}\vdash \forall\ d : WF\_DES\_PREDICATE\_PAIR;\ a : ALPHABET\_DES\\ \quad \mid (True_R\ \ a,\ d.1 \vdash_D d.2) \in WF\_Semi_R\\ \quad \bullet True_R\ \ a\ ;_R\ d.1 \vdash_D d.2\\ \quad\quad = True_R\ (a \cup out\_a\ \ d.1.1)\end{array}$$

$\boldsymbol{DES\_H1\_idem\_thm}$

$\vdash \forall\ d : REL\_PREDICATE \bullet H1\ (H1\ d) = H1\ d$

DES_H2_idem_thm

$\vdash \forall\ d : REL\_PREDICATE$
$\quad \mid dash\ okay \in d.1$
$\quad \bullet H2\ (H2\ d) = H2\ d$

ALPHABET_DES_thm1

$\vdash \forall\ a : ALPHABET\_DES \bullet ALPHABET\_OKAY \subseteq a$

DES_PREDICATE_$\wedge_R$_thm

$\vdash \forall\ d1,\ d2 : DES\_PREDICATE \bullet d1 \wedge_R d2 \in DES\_PREDICATE$

DES_PREDICATE_$\vee_R$_thm

$\vdash \forall\ d1,\ d2 : DES\_PREDICATE \bullet d1 \vee_R d2 \in DES\_PREDICATE$

DES_PREDICATE_$\Rightarrow_R$_thm

$\vdash \forall\ d1,\ d2 : DES\_PREDICATE \bullet d1 \Rightarrow_R d2 \in DES\_PREDICATE$

DES_PREDICATE_$\neg_R$_thm

$\vdash \forall\ d : DES\_PREDICATE \bullet \neg_R\ d \in DES\_PREDICATE$

DES_OKAY_$\in$_DES_PREDICATE_thm

$\vdash OKAY \in DES\_PREDICATE$

DES_OKAY_DASH_$\in$_DES_PREDICATE_thm

$\vdash OKAY' \in DES\_PREDICATE$

DES_PREDICATE_okay_dash_converge_thm

$\vdash \forall\ d : DES\_PREDICATE \bullet d\ \sigma_t \in DES\_PREDICATE$

DES_PREDICATE_okay_dash_diverge_thm

$\vdash \forall\ d : DES\_PREDICATE \bullet d\ \sigma_f \in DES\_PREDICATE$

DES_design_thm

$\vdash \forall\ P,\ Q : DES\_PREDICATE$
$\quad \mid (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\quad \bullet P \vdash_D Q = (OKAY \wedge_R P) \Rightarrow_R OKAY' \wedge_R Q$

DES_OKAY_converge_thm

$\vdash OKAY\ \sigma_t = OKAY$

DES_OKAY_diverge_thm

$\vdash OKAY\ \sigma_f = OKAY$

DES_OKAY_DASH_converge_thm

$\vdash OKAY'\ \sigma_t = True_R\ ALPHABET\_OKAY$

DES_OKAY_DASH_diverge_thm

$\vdash OKAY'\ \sigma_f = False_R\ ALPHABET\_OKAY$

DES_okay_dash_converge_$\wedge_R$_distr_thm

$\vdash \forall\ d1,\ d2 : DES\_PREDICATE$
$\quad \bullet (d1 \wedge_R d2)\ \sigma_t = (d1\ \sigma_t) \wedge_R d2\ \sigma_t$

$\boldsymbol{DES\_okay\_dash\_diverge\_\wedge_R\_distr\_thm}$

$\vdash \forall\ d1,\ d2 : DES\_PREDICATE$
$\quad \bullet\ (d1\ \wedge_R\ d2)\ \sigma_f = (d1\ \sigma_f)\ \wedge_R\ d2\ \sigma_f$

$\boldsymbol{DES\_okay\_dash\_converge\_\vee_R\_distr\_thm}$

$\vdash \forall\ d1,\ d2 : DES\_PREDICATE$
$\quad \bullet\ (d1\ \vee_R\ d2)\ \sigma_t = (d1\ \sigma_t)\ \vee_R\ d2\ \sigma_t$

$\boldsymbol{DES\_okay\_dash\_diverge\_\vee_R\_distr\_thm}$

$\vdash \forall\ d1,\ d2 : DES\_PREDICATE$
$\quad \bullet\ (d1\ \vee_R\ d2)\ \sigma_f = (d1\ \sigma_f)\ \vee_R\ d2\ \sigma_f$

$\boldsymbol{DES\_okay\_dash\_converge\_\neg_R\_distr\_thm}$

$\vdash \forall\ d : DES\_PREDICATE \bullet \neg_R\ d\ \sigma_t = \neg_R\ (d\ \sigma_t)$

$\boldsymbol{DES\_okay\_dash\_diverge\_\neg_R\_distr\_thm}$

$\vdash \forall\ d : DES\_PREDICATE \bullet \neg_R\ d\ \sigma_f = \neg_R\ (d\ \sigma_f)$

$\boldsymbol{DES\_okay\_dash\_converge\_\Rightarrow_R\_distr\_thm}$

$\vdash \forall\ d1,\ d2 : DES\_PREDICATE$
$\quad \bullet\ (d1\ \Rightarrow_R\ d2)\ \sigma_t = (d1\ \sigma_t)\ \Rightarrow_R\ d2\ \sigma_t$

$\boldsymbol{DES\_okay\_dash\_diverge\_\Rightarrow_R\_distr\_thm}$

$\vdash \forall\ d1,\ d2 : DES\_PREDICATE$
$\quad \bullet\ (d1\ \Rightarrow_R\ d2)\ \sigma_f = (d1\ \sigma_f)\ \Rightarrow_R\ d2\ \sigma_f$

$\boldsymbol{DES\_okay\_dash\_converge\_id\_thm}$

$\vdash \forall\ d : DES\_PREDICATE$
$\quad \mid unrestTypedVar\ (d,\ dash\ okay,\ BOOL\_VAL)$
$\quad \bullet\ d\ \sigma_t = d$

$\boldsymbol{DES\_okay\_dash\_diverge\_id\_thm}$

$\vdash \forall\ d : DES\_PREDICATE$
$\quad \mid unrestTypedVar\ (d,\ dash\ okay,\ BOOL\_VAL)$
$\quad \bullet\ d\ \sigma_f = d$

$\boldsymbol{DES\_design\_converge\_thm}$

$\vdash \forall\ P,\ Q : DES\_PREDICATE$
$\quad \mid (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\quad\quad \wedge\ unrestTypedVar\ (P,\ dash\ okay,\ BOOL\_VAL)$
$\quad\quad \wedge\ unrestTypedVar\ (Q,\ dash\ okay,\ BOOL\_VAL)$
$\quad \bullet\ (P\ \vdash_D\ Q)\ \sigma_t = (OKAY\ \wedge_R\ P)\ \Rightarrow_R\ Q$

$\boldsymbol{DES\_design\_diverge\_thm}$

$\vdash \forall\ P,\ Q : DES\_PREDICATE$
$\quad \mid (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\quad\quad \wedge\ unrestTypedVar\ (P,\ dash\ okay,\ BOOL\_VAL)$
$\quad\quad \wedge\ unrestTypedVar\ (Q,\ dash\ okay,\ BOOL\_VAL)$

$\bullet\ (P \vdash_D Q)\ \sigma_f = \neg_R\ (OKAY \wedge_R P)$

DES_conj$_R$_designs_thm

$\vdash \forall\ d1,\ d2 : WF\_DES\_PREDICATE\_PAIR$
$\mid (d1,\ d2) \in WF\_DESIGN\_PAIR$
$\bullet\ (d1.1 \vdash_D d1.2)\ conj_R\ d2.1 \vdash_D d2.2$
$= (d1.1 \vee_R d2.1)$
$\vdash_D (d1.1 \Rightarrow_R d1.2) \wedge_R d2.1 \Rightarrow_R d2.2$

DES_design_alphabet_thm

$\vdash \forall\ P,\ Q : DES\_PREDICATE$
$\mid (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\bullet\ (P \vdash_D Q).1 = P.1$

DES_post_condition_OKAY_intro_thm

$\vdash \forall\ P,\ Q : REL\_PREDICATE$
$\mid (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\bullet\ P \vdash_D Q = P \vdash_D OKAY \wedge_R Q$

DES_intchoice$_R$_designs_thm

$\vdash \forall\ d1,\ d2 : WF\_DES\_PREDICATE\_PAIR$
$\mid (d1,\ d2) \in WF\_DESIGN\_PAIR$
$\bullet\ (d1.1 \vdash_D d1.2)\ intchoice_R\ d2.1 \vdash_D d2.2$
$= (d1.1 \wedge_R d2.1) \vdash_D d1.2 \vee_R d2.2$

DES_false_pre_thm

$\vdash \forall\ a : ALPHABET;\ u : DES\_PREDICATE$
$\mid (False_R\ a,\ u) \in WF\_DES\_PREDICATE\_PAIR$
$\bullet\ False_R\ a \vdash_D u = True_R\ a$

DES_H1_healthy_thm

$\vdash \forall\ d : DES\_PREDICATE \mid d \in H1\_healthy \bullet d = H1\ d$

DES_H2_healthy_thm

$\vdash \forall\ d : DES\_PREDICATE$
$\mid d \in H2\_healthy$
$\bullet\ \langle_R\ (d\ \sigma_f) \Rightarrow_R d\ \sigma_t\ \rangle_R = True_R\ \varnothing$
$\wedge\ dash\ okay \in d.1$

DES_H2_healthy_okay_dash_options_$\vee_R$_thm

$\vdash \forall\ d : DES\_PREDICATE$
$\mid d \in H2\_healthy$
$\bullet\ (d\ \sigma_t) \vee_R d\ \sigma_f = d\ \sigma_t$

DES_H2_healthy_okay_dash_options_$\wedge_R$_thm

$\vdash \forall\ d : DES\_PREDICATE$
$\mid d \in H2\_healthy$

$\bullet\ (d\ \sigma_t) \wedge_R d\ \sigma_f = d\ \sigma_f$

$\boldsymbol{DES\_pre\_post\_rewrite\_thm}$

$\vdash \forall\ d : DES\_PREDICATE$
$\mid d \in H1\_healthy \wedge d \in H2\_healthy$
$\bullet\ d = \neg_R\ (d\ \sigma_f) \vdash_D d\ \sigma_t$

$\boldsymbol{DES\_H1\_H2\_is\_healthy\_thm}$

$\vdash \forall\ d : DES\_PREDICATE$
$\bullet\ H1\ (H2\ d) \in H1\_healthy \wedge H1\ (H2\ d) \in H2\_healthy$

$\boldsymbol{DES\_PREDICATE\_Design\_thm}$

$\vdash \forall\ P,\ Q : DES\_PREDICATE$
$\mid (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\bullet\ P \vdash_D Q \in DES\_PREDICATE$

$\boldsymbol{DES\_H1\_healthy\_thm1}$

$\vdash \forall\ P,\ Q : DES\_PREDICATE$
$\mid (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\bullet\ P \vdash_D Q \in H1\_healthy$

$\boldsymbol{DES\_okay\_\in\_WF\_Equals_R\_thm}$

$\vdash \forall\ a : ALPHABET\_DES$
$\bullet\ (a,\ okay,\ Val\ (Bool\ true)) \in WF\_Equals_R$

$\boldsymbol{DES\_dash\_okay\_\in\_WF\_Equals_R\_thm}$

$\vdash \forall\ a : ALPHABET\_DES$
$\bullet\ (a,\ dash\ okay,\ Val\ (Bool\ true)) \in WF\_Equals_R$

$\boldsymbol{DES\_pre\_condition\_OKAY\_intro\_thm}$

$\vdash \forall\ P,\ Q : DES\_PREDICATE$
$\mid P.1 = Q.1$
$\bullet\ P \vdash_D Q = (OKAY \wedge_R P) \vdash_D Q$

$\boldsymbol{DES\_okay\_dash\_converge\_\wedge_R\_distr\_thm1}$

$\vdash \forall\ d1,\ d2 : REL\_PREDICATE$
$\mid dash\ okay \in d1.1 \wedge dash\ okay \in d2.1$
$\bullet\ (d1 \wedge_R d2)\ \sigma_t = (d1\ \sigma_t) \wedge_R d2\ \sigma_t$

$\boldsymbol{DES\_okay\_dash\_converge\_\Rightarrow_R\_distr\_thm1}$

$\vdash \forall\ d1,\ d2 : REL\_PREDICATE$
$\mid dash\ okay \in d1.1 \wedge dash\ okay \in d2.1$
$\bullet\ (d1 \Rightarrow_R d2)\ \sigma_t = (d1\ \sigma_t) \Rightarrow_R d2\ \sigma_t$

$\boldsymbol{DES\_design\_diverge\_thm1}$

$\vdash \forall\ P,\ Q : DES\_PREDICATE$
$\mid (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\bullet\ (P \vdash_D Q)\ \sigma_f = \neg_R\ (OKAY \wedge_R P\ \sigma_f)$

11 THE Z THEORY utp-wtr

11.1 Parents

$utp-rel$

11.2 Global Variables

$\boldsymbol{wait}$	$NAME$
$\boldsymbol{ALPHABET\_WAIT}$	$\mathbb{P}\ NAME$
$\boldsymbol{WAIT}$	$\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{WAIT'}$	$\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{tr}$	$NAME$
$\boldsymbol{ALPHABET\_TR}$	$\mathbb{P}\ NAME$
$\boldsymbol{ref}$	$NAME$
$\boldsymbol{ALPHABET\_REF}$	$\mathbb{P}\ NAME$
$\boldsymbol{unrestWAIT}$	$\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{B}$
$\boldsymbol{unrestWAIT'}$	$\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{B}$
$\boldsymbol{unrestTR}$	$\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{B}$
$\boldsymbol{unrestTR'}$	$\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{B}$
$\boldsymbol{unrestREF}$	$\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{B}$
$\boldsymbol{unrestREF'}$	$\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{B}$
$(\_\ \boldsymbol{\omega_f})$	$\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$(\_\ \boldsymbol{\omega_t})$	$\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

11.3 Fixity

$\boldsymbol{fun}\ \mathbf{0}\ \boldsymbol{rightassoc}$

$(\_\ \omega_f)\ (\_\ \omega_t)$

11.4 Axioms

$$\begin{array}{ll}
\textbf{\textit{wait}} & \vdash wait \in NAME \land wait \in undashed \\
\textbf{\textit{Constraint 1}} & \vdash (\forall b : BINDING \mid wait \in dom\ b \bullet b\ wait \in BOOL_VAL) \\
& \quad \land (\forall b : BINDING \\
& \qquad \mid dash\ wait \in dom\ b \\
& \qquad \bullet b\ (dash\ wait) \in BOOL_VAL) \\
\textbf{\textit{WAIT}} & \vdash WAIT \in REL_PREDICATE \\
& \quad \land WAIT = =_R (\{wait\}, wait, Val\ (Bool\ true)) \\
\textbf{\textit{WAIT}}' & \vdash WAIT' \in REL_PREDICATE \\
& \quad \land WAIT' \\
& \qquad = =_R (\{dash\ wait\}, dash\ wait, Val\ (Bool\ true)) \\
\textbf{\textit{tr}} & \vdash tr \in NAME \land tr \in undashed \\
\textbf{\textit{Constraint 2}} & \vdash (\forall b : BINDING \\
& \qquad \mid tr \in dom\ b \\
& \qquad \bullet b\ tr \in SEQ_EVENT_VAL) \\
& \quad \land (\forall b : BINDING \\
& \qquad \mid dash\ tr \in dom\ b \\
& \qquad \bullet b\ (dash\ tr) \in SEQ_EVENT_VAL) \\
\textbf{\textit{ref}} & \vdash ref \in NAME \land ref \in undashed \\
\textbf{\textit{Constraint 3}} & \vdash (\forall b : BINDING \mid ref \in dom\ b \bullet b\ ref \in SET_EVENT_VAL) \\
& \quad \land (\forall b : BINDING \\
& \qquad \mid dash\ ref \in dom\ b \\
& \qquad \bullet b\ (dash\ ref) \in SET_EVENT_VAL) \\
\textbf{\textit{unrestWAIT}} & \\
\textbf{\textit{unrestWAIT}}' & \qquad \qquad \vdash \{unrestWAIT, unrestWAIT'\} \subseteq REL_PREDICATE \rightarrow \mathbb{B} \\
& \quad \land (\forall r : REL_PREDICATE \\
& \qquad \bullet (unrestWAIT\ r \\
& \qquad\qquad \Leftrightarrow unrestTypedVar\ (r, wait, BOOL_VAL)) \\
& \qquad\quad \land (unrestWAIT'\ r \\
& \qquad\qquad \Leftrightarrow unrestTypedVar\ (r, dash\ wait, BOOL_VAL))) \\
\textbf{\textit{unrestTR}} & \\
\textbf{\textit{unrestTR}}' & \vdash \{unrestTR, unrestTR'\} \subseteq REL_PREDICATE \rightarrow \mathbb{B} \\
& \quad \land (\forall r : REL_PREDICATE \\
& \qquad \bullet (unrestTR\ r \\
& \qquad\qquad \Leftrightarrow unrestTypedVar\ (r, tr, SEQ_EVENT_VAL)) \\
& \qquad\quad \land (unrestTR'\ r \\
& \qquad\qquad \Leftrightarrow unrestTypedVar
\end{array}$$

$(r,\ dash\ tr,\ SEQ\_EVENT\_VAL)))$

$\boldsymbol{unrestREF}$

$\boldsymbol{unrestREF'}$ $\vdash \{unrestREF,\ unrestREF'\} \subseteq REL\_PREDICATE \to \mathbb{B}$
$\land (\forall\ r : REL\_PREDICATE$
$\bullet (unrestREF\ r$
$\Leftrightarrow unrestTypedVar\ (r,\ ref,\ SET\_EVENT\_VAL))$
$\land (unrestREF'\ r$
$\Leftrightarrow unrestTypedVar$
$(r,\ dash\ ref,\ SET\_EVENT\_VAL)))$

$\boldsymbol{Constraint\ 4} \vdash wait \neq tr \land wait \neq ref$

$\boldsymbol{Constraint\ 5} \vdash tr \neq wait \land tr \neq ref$

$\boldsymbol{Constraint\ 6} \vdash ref \neq tr \land ref \neq wait$

$\_\ \boldsymbol{\omega_f}$ $\vdash (\_\ \omega_f) \in REL\_PREDICATE \nrightarrow REL\_PREDICATE$
$\land (\forall\ r : REL\_PREDICATE$
$\mid wait \in r.1$
$\bullet\ r\ \omega_f = /_R\ (r,\ Val\ (Bool\ false),\ wait))$

$\_\ \boldsymbol{\omega_t}$ $\vdash (\_\ \omega_t) \in REL\_PREDICATE \nrightarrow REL\_PREDICATE$
$\land (\forall\ r : REL\_PREDICATE$
$\mid wait \in r.1$
$\bullet\ r\ \omega_t = /_R\ (r,\ Val\ (Bool\ true),\ wait))$

11.5 Definitions

$\boldsymbol{ALPHABET\_WAIT}$
$\vdash ALPHABET\_WAIT = \{wait,\ dash\ wait\}$

$\boldsymbol{ALPHABET\_TR}$ $\vdash ALPHABET\_TR = \{tr,\ dash\ tr\}$

$\boldsymbol{ALPHABET\_REF}$ $\vdash ALPHABET\_REF = \{ref,\ dash\ ref\}$

11.6 Theorems

$\boldsymbol{WTR\_\subseteq\_NAME\_thm}$
$\vdash \{tr,\ dash\ tr,\ wait,\ dash\ wait,\ ref,\ dash\ ref\} \subseteq NAME$

$\boldsymbol{WTR\_wait\_values\_thm}$
$\vdash \forall\ b : BINDING$
$\mid wait \in dom\ b$
$\bullet\ b\ wait = Bool\ true \lor b\ wait = Bool\ false$

$\boldsymbol{WTR\_wait\_dash\_values\_thm}$
$\vdash \forall\ b : BINDING$

$| \ dash \ wait \in dom \ b$
$\bullet \ b \ (dash \ wait) = Bool \ true$
$\lor \ b \ (dash \ wait) = Bool \ false$

WTR_wait_clauses_thm

$\vdash \forall \ b : BINDING$
$| \ \{wait, \ dash \ wait\} \subseteq dom \ b$
$\bullet \ (\neg \ b \ wait = Bool \ true \Rightarrow b \ wait = Bool \ false)$
$\land \ (\neg \ b \ wait = Bool \ false \Rightarrow b \ wait = Bool \ true)$
$\land \ (\neg$
$b \ (dash \ wait) = Bool \ true$
$\Rightarrow b \ (dash \ wait) = Bool \ false)$
$\land \ (\neg$
$b \ (dash \ wait) = Bool \ false$
$\Rightarrow b \ (dash \ wait) = Bool \ true)$
$\land \ (b \ wait = Bool \ true \Rightarrow \neg \ b \ wait = Bool \ false)$
$\land \ (b \ wait = Bool \ false \Rightarrow \neg \ b \ wait = Bool \ true)$
$\land \ (b \ (dash \ wait) = Bool \ true$
$\Rightarrow \neg$
$b \ (dash \ wait) = Bool \ false)$
$\land \ (b \ (dash \ wait) = Bool \ false$
$\Rightarrow \neg$
$b \ (dash \ wait) = Bool \ true)$

WTR_wait_Equals_true_thm

$\vdash \forall \ a : ALPHABET; \ n : NAME$
$| \ ALPHABET\_WAIT \subseteq a \land n \in ALPHABET\_WAIT$
$\bullet =_R (a, \ n, \ Val \ (Bool \ true))$
$= \neg_R \ (=_R (a, \ n, \ Val \ (Bool \ false)))$

WTR_wait_Equals_false_thm

$\vdash \forall \ a : ALPHABET; \ n : NAME$
$| \ ALPHABET\_WAIT \subseteq a \land n \in ALPHABET\_WAIT$
$\bullet =_R (a, \ n, \ Val \ (Bool \ false))$
$= \neg_R \ (=_R (a, \ n, \ Val \ (Bool \ true)))$

WTR_tr_dash_tr_WF_ALPHABET_EXPRESSION_thm

$\vdash (\{tr, \ dash \ tr\}, \ Var \ tr, \ Var \ (dash \ tr))$
$\in WF\_ALPHABET\_EXPRESSION$

WTR_tr_$\leq_R$_dash_tr_$\in$_WF_ALPHABET_EXPRESSION_thm

$\vdash \forall \ a : ALPHABET$
$| \ ALPHABET\_TR \subseteq a$

$\bullet\ (a,$
$\quad Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$\quad Val\ (Bool\ true))$
$\in WF\_ALPHABET\_EXPRESSION$

$\boldsymbol{WTR\_tr\_dash\_tr\_\leq_R\_thm}$

$\vdash =_{+R}$
$\quad (ALPHABET\_TR,$
$\quad Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$\quad Val\ (Bool\ true))$
$\in REL\_PREDICATE$

$\boldsymbol{WTR\_tr\_dash\_tr\_\leq_R\_thm1}$

$\vdash \forall\ a : ALPHABET$
$\mid ALPHABET\_TR \subseteq a$
$\bullet =_{+R}$
$\quad (a,$
$\quad Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$\quad Val\ (Bool\ true))$
$\in REL\_PREDICATE$

$\boldsymbol{WTR\_ALPHABET\_TR\_thm}$

$\vdash ALPHABET\_TR \in ALPHABET$

$\boldsymbol{WTR\_ALPHABET\_WAIT\_thm}$

$\vdash ALPHABET\_WAIT \in ALPHABET$

$\boldsymbol{WTR\_ALPHABET\_REF\_thm}$

$\vdash ALPHABET\_REF \in ALPHABET$

$\boldsymbol{WTR\_wait\_WF\_Equals_R\_thm}$

$\vdash (\{wait\},\ wait,\ Val\ (Bool\ true)) \in WF\_Equals_R$
$\wedge (\{wait\},\ wait,\ Val\ (Bool\ false)) \in WF\_Equals_R$

$\boldsymbol{WTR\_wait\_WF\_Equals_R\_thm1}$

$\vdash \forall\ a : ALPHABET$
$\mid \{wait,\ dash\ wait\} \subseteq a$
$\bullet\ (a,\ dash\ wait,\ Var\ wait) \in WF\_Equals_R$

$\boldsymbol{WTR\_tr\_WF\_Equals_R\_thm1}$

$\vdash \forall\ a : ALPHABET$
$\mid \{tr,\ dash\ tr\} \subseteq a$
$\bullet\ (a,\ dash\ tr,\ Var\ tr) \in WF\_Equals_R$

$\boldsymbol{WTR\_ref\_WF\_Equals_R\_thm1}$

$\vdash \forall\ a : ALPHABET$
$\mid \{ref,\ dash\ ref\} \subseteq a$

$\bullet\ (a,\ dash\ ref,\ Var\ ref) \in WF\_Equals_R$

WTR_tr_prefix_dash_tr_thm

$\vdash \forall\ b : BINDING$
$\mid tr \in dom\ b$
$\land\ dash\ tr \in dom\ b$
$\land\ b\ tr \leq_R b\ (dash\ tr)$
$\bullet\ b\ tr \leq_R b\ (dash\ tr)$
$\Leftrightarrow Seq\ \langle\rangle \leq_R b\ (dash\ tr)\ SeqDif_R\ b\ tr$

WTR_WAIT_wait_false_thm

$\vdash WAIT\ \omega_f = False_R\ \{wait\}$

WTR_WAIT_wait_true_thm

$\vdash WAIT\ \omega_t = True_R\ \{wait\}$

WTR_$\lhd_R$_$\rhd_R$_thm

$\vdash \forall\ r1,\ r2,\ b : REL\_PREDICATE$
$\mid (r1,\ b,\ r2) \in WF\_Cond_R \land wait \in b.1$
$\bullet\ wait \in (r1 \lhd_R b \rhd_R r2).1$

WTR_wait_true_$\land_R$_distr_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$
$\mid wait \in r1.1 \land wait \in r2.1$
$\bullet\ (r1 \land_R r2)\ \omega_t = (r1\ \omega_t) \land_R r2\ \omega_t$

WTR_wait_false_$\land_R$_distr_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$
$\mid wait \in r1.1 \land wait \in r2.1$
$\bullet\ (r1 \land_R r2)\ \omega_f = (r1\ \omega_f) \land_R r2\ \omega_f$

WTR_wait_true_$\lor_R$_distr_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$
$\mid wait \in r1.1 \land wait \in r2.1$
$\bullet\ (r1 \lor_R r2)\ \omega_t = (r1\ \omega_t) \lor_R r2\ \omega_t$

WTR_wait_false_$\lor_R$_distr_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$
$\mid wait \in r1.1 \land wait \in r2.1$
$\bullet\ (r1 \lor_R r2)\ \omega_f = (r1\ \omega_f) \lor_R r2\ \omega_f$

WTR_wait_true_$\Rightarrow_R$_distr_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$
$\mid wait \in r1.1 \land wait \in r2.1$
$\bullet\ (r1 \Rightarrow_R r2)\ \omega_t = (r1\ \omega_t) \Rightarrow_R r2\ \omega_t$

WTR_wait_false_$\Rightarrow_R$_distr_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$

$| \ wait \in r1.1 \wedge wait \in r2.1$
$\bullet (r1 \Rightarrow_R r2) \ \omega_f = (r1 \ \omega_f) \Rightarrow_R r2 \ \omega_f$

WTR_wait_true_$\neg_R$_distr_thm

$\vdash \forall r : REL\_PREDICATE$
$| \ wait \in r.1$
$\bullet \neg_R \ r \ \omega_t = \neg_R \ (r \ \omega_t)$

WTR_wait_false_$\neg_R$_distr_thm

$\vdash \forall r : REL\_PREDICATE$
$| \ wait \in r.1$
$\bullet \neg_R \ r \ \omega_f = \neg_R \ (r \ \omega_f)$

WTR_wait_true_$\lhd_R$_$\rhd_R$_distr_thm

$\vdash \forall r1, r2, b : REL\_PREDICATE$
$| \ (r1, b, r2) \in WF\_Cond_R \wedge wait \in b.1$
$\bullet (r1 \lhd_R b \rhd_R r2) \ \omega_t$
$= (r1 \ \omega_t) \lhd_R b \ \omega_t \rhd_R r2 \ \omega_t$

WTR_wait_false_$\lhd_R$_$\rhd_R$_distr_thm

$\vdash \forall r1, r2, b : REL\_PREDICATE$
$| \ (r1, b, r2) \in WF\_Cond_R \wedge wait \in b.1$
$\bullet (r1 \lhd_R b \rhd_R r2) \ \omega_f$
$= (r1 \ \omega_f) \lhd_R b \ \omega_f \rhd_R r2 \ \omega_f$

WTR_tr_$\in$_ran_Seq_thm

$\vdash \forall b : BINDING \ | \ tr \in dom \ b \bullet b \ tr \in ran \ Seq$

WTR_dash_tr_$\in$_ran_Seq_thm

$\vdash \forall b : BINDING$
$| \ dash \ tr \in dom \ b$
$\bullet b \ (dash \ tr) \in ran \ Seq$

WTR_dash_tr_equals_tr_thm

$\vdash \forall b : BINDING$
$| \ tr \in dom \ b$
$\wedge \ dash \ tr \in dom \ b$
$\wedge \ b \ tr \leq_R b \ (dash \ tr)$
$\bullet b \ (dash \ tr) = b \ tr$
$\Leftrightarrow b \ (dash \ tr) \ SeqDif_R \ b \ tr = Seq \ \langle\rangle$

WTR_wait_false_is_REL_PREDICATE_thm

$\vdash \forall r : REL\_PREDICATE$
$| \ wait \in r.1$
$\bullet r \ \omega_f \in REL\_PREDICATE$

WTR_wait_true_is_REL_PREDICATE_thm

$$\vdash \forall\ r : REL\_PREDICATE \\ \quad \mid wait \in r.1 \\ \quad \bullet\ r\ \omega_t \in REL\_PREDICATE$$

WTR_wait_true_alphabet_thm

$$\vdash \forall\ r : REL\_PREDICATE \mid wait \in r.1 \bullet (r\ \omega_t).1 = r.1$$

WTR_wait_false_alphabet_thm

$$\vdash \forall\ r : REL\_PREDICATE \mid wait \in r.1 \bullet (r\ \omega_f).1 = r.1$$

WTR_wait_true_subst_thm

$$\vdash \forall\ r : REL\_PREDICATE \\ \quad \mid wait \in r.1 \\ \quad \bullet\ r \wedge_R =_R (r.1,\ wait,\ Val\ (Bool\ true)) \\ \quad\quad = (r\ \omega_t) \wedge_R =_R (r.1,\ wait,\ Val\ (Bool\ true))$$

WTR_wait_false_subst_thm

$$\vdash \forall\ r : REL\_PREDICATE \\ \quad \mid wait \in r.1 \\ \quad \bullet\ r \wedge_R =_R (r.1,\ wait,\ Val\ (Bool\ false)) \\ \quad\quad = (r\ \omega_f) \wedge_R =_R (r.1,\ wait,\ Val\ (Bool\ false))$$

***WTR_wait_false_subst_thm*1**

$$\vdash \forall\ r : REL\_PREDICATE \\ \quad \mid wait \in r.1 \\ \quad \bullet\ r \wedge_R \neg_R (=_R (r.1,\ wait,\ Val\ (Bool\ true))) \\ \quad\quad = (r\ \omega_f) \\ \quad\quad\quad \wedge_R \neg_R (=_R (r.1,\ wait,\ Val\ (Bool\ true)))$$

12 THE Z THEORY utp-rea

12.1 Parents

$utp{-}wtr \qquad utp{-}okay$

12.2 Global Variables

$\boldsymbol{ALPHABET\_OWTR}$
$\quad \mathbb{P}\ NAME$

$\boldsymbol{ALPHABET\_REA} \quad \mathbb{P}\ (\mathbb{P}\ NAME)$

$\boldsymbol{REA\_PREDICATE}$
$\quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{WF\_Skip_{REA}} \quad \mathbb{P}\ (\mathbb{P}\ NAME)$

$\boldsymbol{\Pi_{REA}} \quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{R1} \quad \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{R1\_healthy} \quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{R2} \quad \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{R2\_healthy} \quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{R3} \quad \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{R3\_healthy} \quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{R} \quad \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{R\_healthy} \quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{REA\_PROCESS} \quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

12.3 Axioms

$\boldsymbol{Constraint\ 1} \vdash okay \neq wait \land okay \neq tr \land wait \neq ref$

$$
\begin{array}{ll}
\boldsymbol{\Pi_{REA}} & \vdash \Pi_{REA} \in WF\_Skip_{REA} \to REA\_PREDICATE \\
& \quad \land (\forall\ a : WF\_Skip_{REA} \\
& \quad\quad \bullet \Pi_{REA}\ a \\
& \quad\quad\quad = (=_R\ (a,\ okay,\ Val\ (Bool\ false)) \\
& \quad\quad\quad\quad\quad \land_R =_{+R} \\
& \quad\quad\quad\quad\quad\quad (ALPHABET\_OWTR, \\
& \quad\quad\quad\quad\quad\quad\quad Rel \\
& \quad\quad\quad\quad\quad\quad\quad\quad ((\_ \leq_R \_), \\
& \quad\quad\quad\quad\quad\quad\quad\quad\quad Var\ tr, \\
& \quad\quad\quad\quad\quad\quad\quad\quad\quad Var\ (dash\ tr)),
\end{array}
$$

$$
\begin{array}{ll}
 & \quad\quad\quad\quad \mathit{Val}\ (\mathit{Bool}\ \mathit{true})))\\
 & \quad\quad\quad \vee_R =_R (a,\ \mathit{dash}\ \mathit{okay},\ \mathit{Val}\ (\mathit{Bool}\ \mathit{true}))\\
 & \quad\quad\quad\quad \wedge_R =_R (a,\ \mathit{dash}\ \mathit{tr},\ \mathit{Var}\ \mathit{tr})\\
 & \quad\quad\quad\quad\quad \wedge_R =_R (a,\ \mathit{dash}\ \mathit{wait},\ \mathit{Var}\ \mathit{wait})\\
 & \quad\quad\quad\quad\quad\quad \wedge_R =_R (a,\ \mathit{dash}\ \mathit{ref},\ \mathit{Var}\ \mathit{ref}))\\
\boldsymbol{R1} & \vdash \mathit{R1} \in \mathit{REL\_PREDICATE} \rightarrow \mathit{REL\_PREDICATE}\\
 & \quad \wedge (\forall\ r : \mathit{REL\_PREDICATE}\\
 & \quad\quad \bullet \mathit{R1}\ r\\
 & \quad\quad\quad = r\\
 & \quad\quad\quad\quad \wedge_R =_{+R}\\
 & \quad\quad\quad\quad\quad (\mathit{ALPHABET\_OWTR},\\
 & \quad\quad\quad\quad\quad\quad \mathit{Rel}\\
 & \quad\quad\quad\quad\quad\quad\quad ((\_ \leq_R \_),\\
 & \quad\quad\quad\quad\quad\quad\quad\quad \mathit{Var}\ \mathit{tr},\\
 & \quad\quad\quad\quad\quad\quad\quad\quad \mathit{Var}\ (\mathit{dash}\ \mathit{tr})),\\
 & \quad\quad\quad\quad\quad\quad \mathit{Val}\ (\mathit{Bool}\ \mathit{true})))\\
\boldsymbol{R1\_healthy} & \vdash \mathit{R1\_healthy} \in \mathbb{P}\ \mathit{REL\_PREDICATE}\\
 & \quad \wedge\ \mathit{R1\_healthy} = \{r : \mathit{REL\_PREDICATE} \mid r = \mathit{R1}\ r\}\\
\boldsymbol{R2} & \vdash \mathit{R2} \in \mathit{REL\_PREDICATE} \mathrel{+\!\!\!\rightarrow} \mathit{REL\_PREDICATE}\\
 & \quad \wedge (\forall\ r : \mathit{REL\_PREDICATE}\\
 & \quad\quad \mid \mathit{ALPHABET\_OWTR} \subseteq r.1\\
 & \quad\quad \bullet \mathit{R2}\ r\\
 & \quad\quad\quad = /_R\\
 & \quad\quad\quad\quad (/_R\ (r,\ \mathit{Val}\ (\mathit{Seq}\ \langle\rangle),\ \mathit{tr}),\\
 & \quad\quad\quad\quad\quad \mathit{Fun}_2\\
 & \quad\quad\quad\quad\quad\quad ((\_\ \mathit{SeqDif}_R\ \_),\\
 & \quad\quad\quad\quad\quad\quad\quad \mathit{Var}\ (\mathit{dash}\ \mathit{tr}),\\
 & \quad\quad\quad\quad\quad\quad\quad \mathit{Var}\ \mathit{tr}),\\
 & \quad\quad\quad\quad\quad \mathit{dash}\ \mathit{tr}))\\
\boldsymbol{R2\_healthy} & \vdash \mathit{R2\_healthy} \in \mathbb{P}\ \mathit{REL\_PREDICATE}\\
 & \quad \wedge\ \mathit{R2\_healthy} = \{r : \mathit{REL\_PREDICATE} \mid r = \mathit{R2}\ r\}\\
\boldsymbol{R3} & \vdash \mathit{R3} \in \mathit{REA\_PREDICATE} \mathrel{+\!\!\!\rightarrow} \mathit{REA\_PREDICATE}\\
 & \quad \wedge (\forall\ r : \mathit{REA\_PREDICATE}\\
 & \quad\quad \mid r.1 \in \mathit{WF\_Skip}_{REA}\\
 & \quad\quad \bullet \mathit{R3}\ r\\
 & \quad\quad\quad = \mathit{\Pi}_{REA}\ r.1 \lhd_R\\
 & \quad\quad\quad\quad =_R (\{\mathit{wait}\},\ \mathit{wait},\ \mathit{Val}\ (\mathit{Bool}\ \mathit{true})) \rhd_R\\
 & \quad\quad\quad\quad r)
\end{array}
$$

R3_healthy $\vdash$ *R3_healthy* $\in \mathbb{P}$ *REA_PREDICATE*
$\land$ *R3_healthy*
$= \{r : REA\_PREDICATE$
$\mid r.1 \in WF\_Skip_{REA} \land r = R3\ r\}$

R $\vdash R \in REA\_PREDICATE \rightarrow REA\_PREDICATE$
$\land (\forall\ r : REA\_PREDICATE$
$\mid r.1 \in WF\_Skip_{REA}$
$\bullet\ R\ r = R1\ (R2\ (R3\ r)))$

R_healthy $\vdash$ *R_healthy* $\in \mathbb{P}$ *REA_PREDICATE*
$\land$ *R_healthy*
$= \{r : REA\_PREDICATE$
$\mid r.1 \in WF\_Skip_{REA} \land r = R\ r\}$

REA_H1_wait_dash_okay_thm
$\vdash \forall\ r : REA\_PREDICATE;\ b1,\ b2 : BOOL\_VAL$
$\bullet\ /_R$
$(/_R\ (H1\ r,\ Val\ b1,\ dash\ okay),$
$Val\ b2,$
$dash\ wait)$
$= H1$
$(/_R$
$(/_R\ (r,\ Val\ b1,\ dash\ okay),$
$Val\ b2,$
$dash\ wait))$

REA_Π_{REA}_Π_R_thm
$\vdash \forall\ a : ALPHABET\_REA$
$\mid a \in WF\_Skip_{REA}$
$\bullet\ \Pi_{REA}\ a$
$= (=_R\ (a,\ okay,\ Val\ (Bool\ false))$
$\land_R =_{+R}$
$(ALPHABET\_OWTR,$
Rel
$((\_ \leq_R \_),$
$Var\ tr,$
$Var\ (dash\ tr)),$
$Val\ (Bool\ true)))$
$\lor_R\ \Pi_R\ a$

REA_Π_{REA}_$\lhd_R$_$\rhd_R$_thm
$\vdash \forall\ a : ALPHABET\_REA$

$| \ a \in WF\_Skip_{REA}$
$\bullet \ \Pi_{REA} \ a$
$= \Pi_R \ a \lhd_R$
$=_R (a, okay, Val (Bool \ true)) \rhd_R$
$=_{+R}$
$(ALPHABET\_OWTR,$
$Rel ((\_ \leq_R \_), Var \ tr, Var (dash \ tr)),$
$Val (Bool \ true))$

REA_okay_Π_{REA}_thm

$\vdash \forall \ a : ALPHABET\_REA$
$| \ a \in WF\_Skip_{REA}$
$\bullet =_R (a, okay, Val (Bool \ true)) \wedge_R \Pi_{REA} \ a$
$= =_R (a, okay, Val (Bool \ true)) \wedge_R \Pi_R \ a$

REA_okay_Π_{REA}_unit_thm

$\vdash \forall \ a : ALPHABET\_REA; r : REA\_PREDICATE$
$| \ a \in WF\_Skip_{REA} \wedge (\Pi_{REA} \ a, r) \in WF\_Semi_R$
$\bullet (=_R (a, okay, Val (Bool \ true)) \wedge_R \Pi_{REA} \ a)$
$;_R \ r$
$= =_R (a, okay, Val (Bool \ true)) \wedge_R r$

REA_Π_{REA}_H2_healthy_thm

$\vdash \forall \ a : ALPHABET\_REA$
$| \ a \in WF\_Skip_{REA}$
$\bullet \ \Pi_{REA} \ a \in H2\_healty$

REA_Π_{REA}_R1_healthy_thm

$\vdash \forall \ a : ALPHABET\_REA$
$| \ a \in WF\_Skip_{REA}$
$\bullet \ \Pi_{REA} \ a \in R1\_healthy$

REA_Π_{REA}_R1_H1_thm

$\vdash \forall \ a : ALPHABET\_REA$
$| \ a \in WF\_Skip_{REA}$
$\bullet \ \Pi_{REA} \ a = H1 (R1 (\Pi_{REA} \ a))$

REA_R1_H2_com_thm

$\vdash \forall \ r : REL\_PREDICATE$
$| \ dash \ okay \in r.1$
$\bullet \ H2 (R1 \ r) = R1 (H2 \ r)$

REA_Π_{REA}_R1_H1_Π_R_thm

$\vdash \forall \ a : ALPHABET\_REA$
$| \ a \in WF\_Skip_{REA}$

$\bullet\ \Pi_{REA}\ a = R1\ (H1\ (\Pi_R\ a))$

REA_closure_$\lhd_R$_$\rhd_R$_R1_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE;\ b : REL\_PREDICATE$
$\quad |\ (r1,\ b,\ r2) \in WF\_Cond_R \land \{r1,\ r2\} \subseteq R1\_healthy$
$\quad \bullet\ R1\ (r1 \lhd_R b \rhd_R r2) = r1 \lhd_R b \rhd_R r2$

REA_closure_Semi$_R$_R1_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$
$\quad |\ (r1,\ r2) \in WF\_Semi_R \land \{r1,\ r2\} \subseteq R1\_healthy$
$\quad \bullet\ R1\ (r1\ ;_R\ r2) = r1\ ;_R\ r2$

REA_R1_$\land_R$_$\neg_R$_R1_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$
$\quad \bullet\ R1\ r1 \land_R \neg_R (R1\ r2) = R1\ (r1 \land_R \neg_R\ r2)$

REA_R1_wait_thm

$\vdash \forall\ r : REL\_PREDICATE;\ b : BOOL\_VAL$
$\quad |\ wait \in r.1$
$\quad \bullet\ /_R\ (R1\ r,\ Val\ b,\ wait)$
$\quad\quad = R1\ (/_R\ (r,\ Val\ b,\ wait))$

REA_R1_dash_okay_thm

$\vdash \forall\ r : REL\_PREDICATE;\ b : BOOL\_VAL$
$\quad |\ dash\ okay \in r.1$
$\quad \bullet\ /_R\ (R1\ r,\ Val\ b,\ dash\ okay)$
$\quad\quad = R1\ (/_R\ (r,\ Val\ b,\ dash\ okay))$

REA_R2_idem_thm

$\vdash \forall\ r : REL\_PREDICATE$
$\quad |\ ALPHABET\_OWTR \subseteq r.1$
$\quad \bullet\ R2\ (R2\ r) = R2\ r$

REA_R2_H1_com_thm

$\vdash \forall\ r : REA\_PREDICATE$
$\quad |\ ALPHABET\_OWTR \subseteq r.1$
$\quad \bullet\ H1\ (R2\ r) = R2\ (H1\ r)$

REA_R2_H2_com_thm

$\vdash \forall\ r : REL\_PREDICATE$
$\quad |\ \{dash\ okay\} \cup ALPHABET\_OWTR \subseteq r.1$
$\quad \bullet\ H2\ (R2\ r) = R2\ (H2\ r)$

REA_closure_$\land_R$_R2_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$
$\quad |\ ALPHABET\_OWTR \subseteq r1.1 \cup r2.1$
$\quad\quad \land \{r1,\ r2\} \subseteq R2\_healthy$

$\bullet\ R2\ (r1 \wedge_R r2) = r1 \wedge_R r2$

REA_closure_$\vee_R$_R2_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$
$\quad |\ ALPHABET\_OWTR \subseteq r1.1 \cup r2.1$
$\quad\ \wedge \{r1,\ r2\} \subseteq R2\_healthy$
$\quad \bullet\ R2\ (r1 \vee_R r2) = r1 \vee_R r2$

REA_closure_$\lhd_R$_$\rhd_R$_R2_thm

$\vdash \forall\ r1,\ r2,\ b : REL\_PREDICATE$
$\quad |\ ALPHABET\_OWTR \subseteq r1.1$
$\quad\ \wedge (r1,\ b,\ r2) \in WF\_Cond_R$
$\quad\ \wedge \{r1,\ r2,\ b\} \subseteq R2\_healthy$
$\quad \bullet\ R2\ (r1 \lhd_R b \rhd_R r2) = r1 \lhd_R b \rhd_R r2$

REA_closure_Semi$_R$_R2_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$
$\quad |\ tr \in r1.1$
$\quad\ \wedge dash\ tr \in r2.1$
$\quad\ \wedge (r1,\ r2) \in WF\_Semi_R$
$\quad\ \wedge \{r1,\ r2\} \subseteq R2\_healthy$
$\quad \bullet\ R2\ (r1\ ;_R\ r2) = r1\ ;_R\ r2$

REA_R3_H2_com_thm

$\vdash \forall\ r : REL\_PREDICATE$
$\quad |\ dash\ okay \in r.1 \wedge r.1 \in WF\_Skip_{REA}$
$\quad \bullet\ H2\ (R3\ r) = R3\ (H2\ r)$

REA_R3_R1_H1_quasi_com_thm

$\vdash \forall\ r : REA\_PREDICATE$
$\quad |\ r.1 \in WF\_Skip_{REA}$
$\quad \bullet\ R3\ (R1\ (H1\ r)) = R1\ (H1\ (R3\ r))$

REA_R3_$\neg$_okay_wait_thm

$\vdash \forall\ r : REA\_PREDICATE$
$\quad |\ r \in R3\_healthy$
$\quad \bullet =_R (r.1,\ okay,\ Val\ (Bool\ false))$
$\qquad\quad \wedge_R =_R (r.1,\ wait,\ Val\ (Bool\ true)) \wedge_R R3\ r$
$\qquad = =_R (r.1,\ okay,\ Val\ (Bool\ false))$
$\qquad\quad \wedge_R =_R (r.1,\ wait,\ Val\ (Bool\ true))$
$\qquad\qquad \wedge_R =_{+R}$
$\qquad\qquad\quad (r.1,$
$\qquad\qquad\qquad Rel$
$\qquad\qquad\qquad\quad ((\_ \leq_R \_),$

$$Var\ tr,$$
$$Var\ (dash\ tr)),$$
$$Val\ (Bool\ true))$$

REA_closure_$\wedge_R$_R3_thm

$$\vdash \forall\ r1,\ r2 : REA\_PREDICATE \mid \{r1,\ r2\} \subseteq R3\_healthy \bullet R3\ (r1 \wedge_R r2) = r1 \wedge_R r2$$

REA_closure_$\vee_R$_R3_thm

$$\vdash \forall\ r1,\ r2 : REA\_PREDICATE \mid \{r1,\ r2\} \subseteq R3\_healthy \bullet R3\ (r1 \vee_R r2) = r1 \vee_R r2$$

REA_closure_$\lhd_R$_$\rhd_R$_R3_thm

$$\vdash \forall\ r1,\ r2 : REA\_PREDICATE;\ b : REL\_PREDICATE \mid (r1,\ b,\ r2) \in WF\_Cond_R \wedge \{r1,\ r2\} \subseteq R3\_healthy \bullet R3\ (r1 \lhd_R b \rhd_R r2) = r1 \lhd_R b \rhd_R r2$$

REA_closure_Semi$_R$_R3_thm

$$\vdash \forall\ r1,\ r2 : REA\_PREDICATE \mid (r1,\ r2) \in WF\_Semi_R \wedge \{r1,\ r2\} \subseteq R3\_healthy \wedge r2 \in R1\_healthy \bullet R3\ (r1 \ ;_R r2) = r1 \ ;_R r2$$

REA_R3_wait_true_thm

$$\vdash \forall\ r : REA\_PREDICATE \mid r.1 \in WF\_Skip_{REA} \bullet /_R\ (R3\ r,\ Val\ (Bool\ true),\ wait) = /_R\ (\Pi_{REA}\ r.1,\ Val\ (Bool\ true),\ wait)$$

REA_R3_wait_false_thm

$$\vdash \forall\ r : REA\_PREDICATE \mid r.1 \in WF\_Skip_{REA} \bullet /_R\ (R3\ r,\ Val\ (Bool\ false),\ wait) = /_R\ (r,\ Val\ (Bool\ false),\ wait)$$

REA_R3_dash_okay_thm

$$\vdash \forall\ r : REA\_PREDICATE;\ b : BOOL\_VAL \mid r.1 \in WF\_Skip_{REA} \bullet /_R\ (R3\ r,\ Val\ b,\ dash\ okay) = /_R\ (\Pi_{REA}\ r.1,\ Val\ b,\ dash\ okay) \lhd_R =_R (r.1,\ wait,\ Val\ (Bool\ true)) \rhd_R /_R\ (r,\ Val\ b,\ dash\ okay)$$

$\boldsymbol{REA\_tr\_\leq_R\_dash\_tr\_Semi_R\_zero\_thm}$

$$
\begin{array}{l}
\vdash \forall\ p : REA\_PROCESS \\
\quad \mid p.1 \in homogeneous \\
\quad \bullet =_{+R} \\
\qquad\quad (p.1, \\
\qquad\quad\ Rel\ ((\_ \leq_R \_), Var\ tr, Var\ (dash\ tr)), \\
\qquad\quad\ Val\ (Bool\ true)) \\
\qquad ;_R\ p \\
\quad\ = =_{+R} \\
\qquad (p.1, \\
\qquad\ Rel\ ((\_ \leq_R \_), Var\ tr, Var\ (dash\ tr)), \\
\qquad\ Val\ (Bool\ true))
\end{array}
$$

$\boldsymbol{REA\_\neg\_okay\_tr\_\leq_R\_dash\_tr\_Semi_R\_zero\_thm}$

$$
\begin{array}{l}
\vdash \forall\ p : REA\_PROCESS \\
\quad \mid p.1 \in homogeneous \\
\quad \bullet (=_R (p.1, okay, Val\ (Bool\ false)) \\
\qquad\quad \wedge_R =_{+R} \\
\qquad\qquad (p.1, \\
\qquad\qquad\ Rel \\
\qquad\qquad\quad ((\_ \leq_R \_), \\
\qquad\qquad\quad\ Var\ tr, \\
\qquad\qquad\quad\ Var\ (dash\ tr)), \\
\qquad\qquad\ Val\ (Bool\ true))) \\
\qquad ;_R\ p \\
\quad\ = =_R (p.1, okay, Val\ (Bool\ false)) \\
\qquad \wedge_R =_{+R} \\
\qquad\quad (p.1, \\
\qquad\quad\ Rel\ ((\_ \leq_R \_), Var\ tr, Var\ (dash\ tr)), \\
\qquad\quad\ Val\ (Bool\ true))
\end{array}
$$

$\boldsymbol{REA\_\Pi_{REA}\_Semi_R\_rea\_thm}$

$$
\begin{array}{l}
\vdash \forall\ p : REA\_PROCESS \\
\quad \mid p.1 \in WF\_Skip_{REA} \\
\quad \bullet \Pi_{REA}\ p.1\ ;_R\ p \\
\quad\ = p \lhd_R \\
\qquad =_R (p.1, okay, Val\ (Bool\ true)) \rhd_R \\
\qquad =_{+R} \\
\qquad\quad (p.1, \\
\qquad\quad\ Rel\ ((\_ \leq_R \_), Var\ tr, Var\ (dash\ tr)),
\end{array}
$$

$Val\ (Bool\ true))$

REA_closure_$\wedge_R$_R_thm

$\vdash \forall\ r1,\ r2 : REA\_PREDICATE$
$\quad | \{r1,\ r2\} \subseteq R\_healthy$
$\quad \bullet\ R\ (r1\ \wedge_R\ r2) = r1\ \wedge_R\ r2$

REA_closure_$\vee_R$_R_thm

$\vdash \forall\ r1,\ r2 : REA\_PREDICATE$
$\quad | \{r1,\ r2\} \subseteq R\_healthy$
$\quad \bullet\ R\ (r1\ \vee_R\ r2) = r1\ \vee_R\ r2$

REA_closure_$\lhd_R$_$\rhd_R$_R_thm

$\vdash \forall\ r1,\ r2 : REA\_PREDICATE;\ b : REL\_PREDICATE$
$\quad | (r1,\ b,\ r2) \in WF\_Cond_R \wedge \{r1,\ r2,\ b\} \subseteq R\_healthy$
$\quad \bullet\ R\ (r1\ \lhd_R\ b\ \rhd_R\ r2) = r1\ \lhd_R\ b\ \rhd_R\ r2$

REA_closure_Semi$_R$_R_thm

$\vdash \forall\ r1,\ r2 : REA\_PREDICATE$
$\quad | (r1,\ r2) \in WF\_Semi_R \wedge \{r1,\ r2\} \subseteq R\_healthy$
$\quad \bullet\ R\ (r1\ ;_R\ r2) = r1\ ;_R\ r2$

REA_R_dash_okay_thm

$\vdash \forall\ r : REA\_PREDICATE;\ b : BOOL\_VAL$
$\quad | r.1 \in WF\_Skip_{REA}$
$\quad \bullet\ /_R\ (R\ r,\ Val\ b,\ dash\ okay)$
$\quad\quad = /_R\ (\Pi_{REA}\ r.1,\ Val\ b,\ dash\ okay)\ \lhd_R$
$\quad\quad\quad =_R (r.1,\ wait,\ Val\ (Bool\ true))\ \rhd_R$
$\quad\quad\quad R1\ (R2\ (/_R\ (r,\ Val\ b,\ dash\ okay)))$

12.4 Definitions

ALPHABET_OWTR

$\vdash ALPHABET\_OWTR$
$\quad = ALPHABET\_OKAY \cup ALPHABET\_WAIT \cup ALPHABET\_TR$
$\quad\quad \cup ALPHABET\_REF$

ALPHABET_REA $\vdash ALPHABET\_REA = \{a : ALPHABET \mid ALPHABET\_O$

REA_PREDICATE

$\vdash REA\_PREDICATE$
$\quad = \{d : REL\_PREDICATE$
$\quad\quad | d.1 \in ALPHABET\_REA\}$

WF_Skip$_{REA}$ $\vdash WF\_Skip_{REA} = \{a : ALPHABET\_REA \mid a \in homogeneous\}$

REA_PROCESS $\vdash REA\_PROCESS = \{r : REA\_PREDICATE \mid r \in R\_hea$

12.5 Theorems

$\boldsymbol{ALPHABET\_REA\_thm}$

$\vdash \forall\ a : ALPHABET\_REA \bullet a \in ALPHABET$

$\boldsymbol{ALPHABET\_REA\_thm1}$

$$\begin{array}{l} \vdash \forall\ a : ALPHABET\_REA \\ \quad \bullet\ ALPHABET\_TR \subseteq a \\ \quad\quad \wedge\ ALPHABET\_OKAY \subseteq a \\ \quad\quad \wedge\ ALPHABET\_WAIT \subseteq a \\ \quad\quad \wedge\ ALPHABET\_REF \subseteq a \end{array}$$

$\boldsymbol{ALPHABET\_REA\_thm2}$

$\vdash \forall\ a : ALPHABET\_REA \bullet ALPHABET\_OWTR \subseteq a$

$\boldsymbol{REA\_PREDICATE\_thm}$

$$\begin{array}{l} \vdash \forall\ r : REA\_PREDICATE \\ \quad \bullet\ r \in REL\_PREDICATE \\ \quad\quad \wedge\ \{okay, \\ \quad\quad\quad dash\ okay, \\ \quad\quad\quad tr, \\ \quad\quad\quad dash\ tr, \\ \quad\quad\quad wait, \\ \quad\quad\quad dash\ wait, \\ \quad\quad\quad ref, \\ \quad\quad\quad dash\ ref\} \\ \quad\quad\quad \subseteq r.1 \\ \quad\quad \wedge\ r.1 \in ALPHABET\_REA \end{array}$$

$\boldsymbol{REA\_PROCESS\_thm}$

$\vdash \forall\ r : REA\_PROCESS \bullet r \in REA\_PREDICATE$

$\boldsymbol{REA\_tr\_\leq_R\_dash\_tr\_\in\_WF\_ALPHABET\_EXPRESSION\_thm}$

$$\begin{array}{l} \vdash \forall\ a : ALPHABET\_REA \\ \quad \bullet\ (a, \\ \quad\quad\quad Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)), \\ \quad\quad\quad Val\ (Bool\ true)) \\ \quad\quad \in WF\_ALPHABET\_EXPRESSION \end{array}$$

$\boldsymbol{REA\_ALPHABET\_OWTR\_thm}$

$\vdash ALPHABET\_OWTR \in ALPHABET\_REA$

$\boldsymbol{REA\_PREDICATE\_ALPHABET\_OWTR\_thm}$

$\vdash \forall\ r : REA\_PREDICATE \bullet ALPHABET\_OWTR \subseteq r.1$

$\boldsymbol{REA\_tr\_dash\_tr\_\leq_R\_thm}$

$\vdash =_{+R}$
$(ALPHABET\_OWTR,$
$Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$Val\ (Bool\ true))$
$\in REL\_PREDICATE$

REA_tr_dash_tr_$\leq_R$_thm1

$\vdash \forall\ a : ALPHABET$
$\mid ALPHABET\_OWTR \subseteq a$
$\bullet =_{+R}$
$(a,$
$Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$Val\ (Bool\ true))$
$\in REL\_PREDICATE$

REA_tr_dash_tr_$\leq_R$_$\in$_WF_ALPHABET_EXPRESSION_thm

$\vdash \forall\ a : ALPHABET$
$\mid ALPHABET\_OWTR \subseteq a$
$\bullet (a,$
$Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$Val\ (Bool\ true))$
$\in WF\_ALPHABET\_EXPRESSION$

REA_R1_thm $\vdash \forall\ r : REL\_PREDICATE \bullet R1\ r \in REL\_PREDICATE$

REA_R1_alphabet_thm1

REA_R1_alphabet_thm

$\vdash \forall\ r : REL\_PREDICATE \bullet (R1\ r).1 = r.1 \cup ALPHABET\_OWTR$

REA_R1_thm1 $\vdash \forall\ r : REA\_PREDICATE \bullet R1\ r \in REA\_PREDICATE$

REA_R2_thm $\vdash \forall\ r : REL\_PREDICATE$
$\mid ALPHABET\_OWTR \subseteq r.1$
$\bullet R2\ r \in REL\_PREDICATE$

REA_R2_alphabet_thm

$\vdash \forall\ r : REL\_PREDICATE$
$\mid ALPHABET\_OWTR \subseteq r.1$
$\bullet (R2\ r).1 = r.1$

REA_R2_thm1 $\vdash \forall\ r : REA\_PREDICATE \bullet R2\ r \in REA\_PREDICATE$

REA_Π_{REA}_thm

$\vdash \forall\ a : ALPHABET\_REA$
$\mid a \in WF\_Skip_{REA}$
$\bullet \Pi_{REA}\ a \in REA\_PREDICATE$

REA_Π_{REA}_alphabet_thm

$\vdash \forall\ a : ALPHABET\_REA$
$\quad | \ a \in WF\_Skip_{REA}$
$\quad \bullet (\Pi_{REA}\ a).1 = a$

REA_R3_thm $\vdash \forall\ r : REA\_PREDICATE$
$\quad | \ r.1 \in WF\_Skip_{REA}$
$\quad \bullet R3\ r \in REA\_PREDICATE$

REA_R3_alphabet_thm
$\vdash \forall\ r : REA\_PREDICATE$
$\quad | \ r.1 \in WF\_Skip_{REA}$
$\quad \bullet (R3\ r).1 = r.1$

REA_R_thm $\vdash \forall\ r : REA\_PREDICATE$
$\quad | \ r.1 \in WF\_Skip_{REA}$
$\quad \bullet R\ r \in REA\_PREDICATE$

REA_R_alphabet_thm
$\vdash \forall\ r : REA\_PREDICATE$
$\quad | \ r.1 \in WF\_Skip_{REA}$
$\quad \bullet (R\ r).1 = r.1$

REA_reactive_vars_⊆_NAME_thm
$\vdash \{okay,$
$\quad dash\ okay,$
$\quad tr,$
$\quad dash\ tr,$
$\quad wait,$
$\quad dash\ wait,$
$\quad ref,$
$\quad dash\ ref\}$
$\quad \subseteq NAME$

REA_reactive_vars_⊆_ALPHABET_REA_thm
$\vdash \forall\ a : ALPHABET\_REA$
$\quad \bullet \{okay,$
$\qquad dash\ okay,$
$\qquad tr,$
$\qquad dash\ tr,$
$\qquad wait,$
$\qquad dash\ wait,$
$\qquad ref,$
$\qquad dash\ ref\}$
$\qquad \subseteq a$

$\boldsymbol{REA\_R1\_idem\_thm}$

$\vdash \forall\ r : REL\_PREDICATE \bullet R1\ (R1\ r) = R1\ r$

$\boldsymbol{REA\_R1\_def\_\in\_REA\_PREDICATE\_thm}$

$$\vdash =_{+R} (ALPHABET\_OWTR,\ Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),\ Val\ (Bool\ true)) \in REA\_PREDICATE$$

$\boldsymbol{REA\_R2\_def\_\in\_WF\_Subst_R\_thm1}$

$$\vdash \forall\ r : REA\_PREDICATE \bullet (r,\ Val\ (Seq\ \langle\rangle),\ tr) \in WF\_Subst_R$$

$\boldsymbol{REA\_R2\_def\_alphabet\_thm1}$

$$\vdash \forall\ r : REA\_PREDICATE \bullet (/_R\ (r,\ Val\ (Seq\ \langle\rangle),\ tr)).1 = r.1$$

$\boldsymbol{REA\_R2\_def\_\in\_WF\_Subst_R\_thm}$

$$\vdash \forall\ r : REA\_PREDICATE \bullet (/_R\ (r,\ Val\ (Seq\ \langle\rangle),\ tr),\ Fun_2\ ((\_\ SeqDif_R\ \_),\ Var\ (dash\ tr),\ Var\ tr),\ dash\ tr) \in WF\_Subst_R$$

$\boldsymbol{REA\_R2\_def\_alphabet\_thm}$

$$\vdash \forall\ r : REA\_PREDICATE \bullet (/_R\ (/_R\ (r,\ Val\ (Seq\ \langle\rangle),\ tr),\ Fun_2\ ((\_\ SeqDif_R\ \_),\ Var\ (dash\ tr),\ Var\ tr),\ dash\ tr)).1 = r.1$$

$\boldsymbol{REA\_R2\_def\_\in\_REL\_PREDICATE\_thm1}$

$$\vdash \forall\ r : REA\_PREDICATE \bullet /_R\ (r,\ Val\ (Seq\ \langle\rangle),\ tr) \in REL\_PREDICATE$$

$\boldsymbol{REA\_R2\_def\_\in\_REL\_PREDICATE\_thm}$

$$\vdash \forall\ r : REA\_PREDICATE \bullet /_R\ (/_R\ (r,\ Val\ (Seq\ \langle\rangle),\ tr),\ Fun_2$$

$((\_ \ SeqDif_R \ \_),$
$Var \ (dash \ tr),$
$Var \ tr),$
$dash \ tr)$
$\in REL\_PREDICATE$

$\boldsymbol{REA\_R2\_def\_\in\_REA\_PREDICATE\_thm1}$

$\vdash \forall r : REA\_PREDICATE$
$\bullet /_R \ (r, \ Val \ (Seq \ \langle\rangle), \ tr) \in REA\_PREDICATE$

$\boldsymbol{REA\_R2\_def\_\in\_REA\_PREDICATE\_thm}$

$\vdash \forall r : REA\_PREDICATE$
$\bullet /_R$
$(/_R \ (r, \ Val \ (Seq \ \langle\rangle), \ tr),$
Fun_2
$((\_ \ SeqDif_R \ \_),$
$Var \ (dash \ tr),$
$Var \ tr),$
$dash \ tr)$
$\in REA\_PREDICATE$

$\boldsymbol{REA\_R1\_def\_alphabet\_thm}$

$\vdash (=_{+R}$
$(ALPHABET\_OWTR,$
$Rel \ ((\_ \leq_R \_), \ Var \ tr, \ Var \ (dash \ tr)),$
$Val \ (Bool \ true))).1$
$= ALPHABET\_OWTR$

$\boldsymbol{REA\_PREDICATE\_\wedge_R\_thm}$

$\vdash \forall r1, r2 : REA\_PREDICATE \bullet r1 \wedge_R r2 \in REA\_PREDICATE$

$\boldsymbol{REA\_PREDICATE\_\wedge_R\_thm1}$

$\vdash \forall r1 : REL\_PREDICATE; \ r2 : REA\_PREDICATE$
$\bullet r1 \wedge_R r2 \in REA\_PREDICATE$

$\boldsymbol{REA\_PREDICATE\_\wedge_R\_thm2}$

$\vdash \forall r1 : REA\_PREDICATE; \ r2 : REL\_PREDICATE$
$\bullet r1 \wedge_R r2 \in REA\_PREDICATE$

$\boldsymbol{REA\_PREDICATE\_\vee_R\_thm}$

$\vdash \forall r1, r2 : REA\_PREDICATE \bullet r1 \vee_R r2 \in REA\_PREDICATE$

$\boldsymbol{REA\_PREDICATE\_\vee_R\_thm1}$

$\vdash \forall r1 : REL\_PREDICATE; \ r2 : REA\_PREDICATE$
$\bullet r1 \vee_R r2 \in REA\_PREDICATE$

$\boldsymbol{REA\_PREDICATE\_\vee_R\_thm2}$

$\vdash \forall\ r1 : REA\_PREDICATE;\ r2 : REL\_PREDICATE$
$\quad \bullet\ r1 \lor_R r2 \in REA\_PREDICATE$

$\boldsymbol{REA\_PREDICATE\_\Rightarrow_R\_thm}$

$\vdash \forall\ r1, r2 : REA\_PREDICATE \bullet r1 \Rightarrow_R r2 \in REA\_PREDICATE$

$\boldsymbol{REA\_PREDICATE\_\Rightarrow_R\_thm1}$

$\vdash \forall\ r1 : REL\_PREDICATE;\ r2 : REA\_PREDICATE$
$\quad \bullet\ r1 \Rightarrow_R r2 \in REA\_PREDICATE$

$\boldsymbol{REA\_PREDICATE\_\Rightarrow_R\_thm2}$

$\vdash \forall\ r1 : REA\_PREDICATE;\ r2 : REL\_PREDICATE$
$\quad \bullet\ r1 \Rightarrow_R r2 \in REA\_PREDICATE$

$\boldsymbol{REA\_PREDICATE\_\neg_R\_thm}$

$\vdash \forall\ r : REA\_PREDICATE \bullet \neg_R\ r \in REA\_PREDICATE$

$\boldsymbol{REA\_R2\_\land_R\_dist\_thm}$

$\vdash \forall\ r1, r2 : REA\_PREDICATE$
$\quad \bullet\ R2\ (r1 \land_R r2) = R2\ r1 \land_R R2\ r2$

$\boldsymbol{REA\_tr\_prefix\_dash\_tr\_thm}$

```
⊢ =_{+R}
        (ALPHABET_OWTR,
         Rel
             ((_ ≤_R _),
              Val (Seq ⟨⟩),
              Fun_2
                  ((_ SeqDif_R _),
                   Var (dash tr),
                   Var tr)),
         Val (Bool true))
      ∧_R =_{+R}
        (ALPHABET_OWTR,
         Rel ((_ ≤_R _), Var tr, Var (dash tr)),
         Val (Bool true))
  = =_{+R}
      (ALPHABET_OWTR,
       Rel ((_ ≤_R _), Var tr, Var (dash tr)),
       Val (Bool true))
```

$\boldsymbol{REA\_R2\_R1\_def\_unit\_thm}$

```
⊢ R1
      (R2
         (=_{+R}
```

$$
\begin{array}{l}
\qquad\qquad (ALPHABET\_OWTR,\\
\qquad\qquad\quad Rel\\
\qquad\qquad\qquad ((\_ \leq_R \_),\\
\qquad\qquad\qquad\quad Var\ tr,\\
\qquad\qquad\qquad\quad Var\ (dash\ tr)),\\
\qquad\qquad\quad Val\ (Bool\ true))))\\
\quad = R1\ (True_R\ ALPHABET\_OWTR)
\end{array}
$$

$\boldsymbol{REA\_R1\_extends\_over\_\wedge_R\_thm}$

$$
\begin{array}{l}
\vdash \forall\ r1,\ r2 : REL\_PREDICATE\\
\quad \bullet\ R1\ r1 \wedge_R r2 = R1\ (r1 \wedge_R r2)
\end{array}
$$

$\boldsymbol{REA\_R1\_\wedge_R\_dist\_thm}$

$$
\begin{array}{l}
\vdash \forall\ r1,\ r2 : REL\_PREDICATE\\
\quad \bullet\ R1\ r1 \wedge_R R1\ r2 = R1\ (r1 \wedge_R r2)
\end{array}
$$

$\boldsymbol{REA\_R1\_\vee_R\_dist\_thm}$

$$
\begin{array}{l}
\vdash \forall\ r1,\ r2 : REL\_PREDICATE\\
\quad \bullet\ R1\ r1 \vee_R R1\ r2 = R1\ (r1 \vee_R r2)
\end{array}
$$

$\boldsymbol{REA\_R1\_R2\_com\_thm}$

$$
\vdash \forall\ r : REA\_PREDICATE \bullet R1\ (R2\ r) = R1\ (R2\ (R1\ r))
$$

$\boldsymbol{REA\_R3\_idem\_thm}$

$$
\begin{array}{l}
\vdash \forall\ r : REA\_PREDICATE\\
\quad |\ r.1 \in WF\_Skip_{REA}\\
\quad \bullet\ R3\ (R3\ r) = R3\ r
\end{array}
$$

$\boldsymbol{REA\_R1\_alphabet\_WF\_Skip_{REA}\_thm}$

$$
\begin{array}{l}
\vdash \forall\ r : REA\_PREDICATE\\
\quad |\ r.1 \in WF\_Skip_{REA}\\
\quad \bullet\ (R1\ r).1 \in WF\_Skip_{REA}
\end{array}
$$

$\boldsymbol{REA\_R2\_alphabet\_WF\_Skip_{REA}\_thm}$

$$
\begin{array}{l}
\vdash \forall\ r : REA\_PREDICATE\\
\quad |\ r.1 \in WF\_Skip_{REA}\\
\quad \bullet\ (R2\ r).1 \in WF\_Skip_{REA}
\end{array}
$$

$\boldsymbol{REA\_R3\_def\_\in\_WF\_Cond_R\_thm}$

$$
\begin{array}{l}
\vdash \forall\ r : REA\_PREDICATE\\
\quad |\ r.1 \in WF\_Skip_{REA}\\
\quad \bullet\ (\mathit{\Pi}_{REA}\ r.1,\\
\qquad =_R (\{wait\},\ wait,\ Val\ (Bool\ true)),\\
\qquad r)\\
\quad\ \in WF\_Cond_R
\end{array}
$$

$\boldsymbol{REA\_R3\_def\_\in\_WF\_Cond_R\_thm1}$

$\vdash \forall\ r : \mathit{REA\_PREDICATE}$
$\quad | \ r.1 \in \mathit{WF\_Skip}_{\mathit{REA}}$
$\quad \bullet\ (\Pi_{\mathit{REA}}\ r.1,\ =_R (r.1,\ \mathit{wait},\ \mathit{Val}\ (\mathit{Bool}\ \mathit{true})),\ r)$
$\quad\ \ \in \mathit{WF\_Cond}_R$

REA_dash_tr_Equals_tr_∈_WF_Equals$_R$_thm

$\vdash \forall\ a : \mathit{ALPHABET\_REA}$
$\quad \bullet\ (a,\ \mathit{dash}\ \mathit{tr},\ \mathit{Var}\ \mathit{tr}) \in \mathit{WF\_Equals}_R$

***REA_dash_tr_equals_tr_thm*1**

$\vdash \forall\ a : \mathit{ALPHABET\_REA}$
$\quad \bullet\ =_R (a,\ \mathit{dash}\ \mathit{tr},\ \mathit{Var}\ \mathit{tr})$
$\qquad \wedge_R =_{+R}$
$\qquad\quad (\mathit{ALPHABET\_OWTR},$
$\qquad\quad\ \ \mathit{Rel}\ ((\_ \leq_R \_),\ \mathit{Var}\ \mathit{tr},\ \mathit{Var}\ (\mathit{dash}\ \mathit{tr})),$
$\qquad\quad\ \ \mathit{Val}\ (\mathit{Bool}\ \mathit{true}))$
$\quad\ \ = =_R (a,\ \mathit{dash}\ \mathit{tr},\ \mathit{Var}\ \mathit{tr})$

REA_Π$_{REA}$_R*1*_healthy_thm

$\vdash \forall\ a : \mathit{ALPHABET\_REA}$
$\quad | \ a \in \mathit{WF\_Skip}_{\mathit{REA}}$
$\quad \bullet\ \Pi_{\mathit{REA}}\ a \in \mathit{R1\_healthy}$

REA_R*3*_R*1*_com_thm

$\vdash \forall\ r : \mathit{REA\_PREDICATE}$
$\quad | \ r.1 \in \mathit{WF\_Skip}_{\mathit{REA}}$
$\quad \bullet\ \mathit{R1}\ (\mathit{R3}\ r) = \mathit{R3}\ (\mathit{R1}\ r)$

REA_R*3*_rewrite_thm

$\vdash \forall\ r : \mathit{REA\_PREDICATE}$
$\quad | \ r.1 \in \mathit{WF\_Skip}_{\mathit{REA}}$
$\quad \bullet\ \mathit{R3}\ r$
$\quad\ \ = \Pi_{\mathit{REA}}\ r.1 \lhd_R$
$\qquad =_R (r.1,\ \mathit{wait},\ \mathit{Val}\ (\mathit{Bool}\ \mathit{true})) \rhd_R$
$\qquad r$

***REA_R*3*_def_cond_∈_REA_PREDICATE_thm*1**

$\vdash \forall\ a : \mathit{ALPHABET\_REA};\ v : \mathit{VALUE}$
$\quad \bullet\ =_R (a,\ \mathit{wait},\ \mathit{Val}\ v) \in \mathit{REA\_PREDICATE}$

REA_R*2*_∨$_R$_dist_thm

$\vdash \forall\ r1,\ r2 : \mathit{REA\_PREDICATE}$
$\quad \bullet\ \mathit{R2}\ (r1 \vee_R r2) = \mathit{R2}\ r1 \vee_R \mathit{R2}\ r2$

REA_R*2*_¬$_R$_dist_thm

$\vdash \forall\ r : \mathit{REA\_PREDICATE} \bullet \mathit{R2}\ (\neg_R\ r) = \neg_R\ (\mathit{R2}\ r)$

$\boldsymbol{REA\_R2\_\lhd_R\_\rhd_R\_dist\_thm}$

$\vdash \forall\ r1,\ r2,\ b : REA\_PREDICATE$
$\quad |\ (r1,\ b,\ r2) \in WF\_Cond_R$
$\quad \bullet\ R2\ (r1 \lhd_R b \rhd_R r2) = R2\ r1 \lhd_R R2\ b \rhd_R R2\ r2$

$\boldsymbol{REA\_Equals_R\_\in\_REA\_PREDICATE\_thm}$

$\vdash \forall\ a : ALPHABET\_REA;\ v : VALUE;\ n : NAME$
$\quad |\ n \in a$
$\quad \bullet\ =_R (a,\ n,\ Val\ v) \in REA\_PREDICATE$

$\boldsymbol{REA\_Equals_R\_\in\_REA\_PREDICATE\_thm1}$

$\vdash \forall\ a : ALPHABET\_REA;\ n1,\ n2 : NAME$
$\quad |\ n1 \in a \wedge n2 \in a$
$\quad \bullet\ =_R (a,\ n1,\ Var\ n2) \in REA\_PREDICATE$

$\boldsymbol{REA\_R2\_Equals_R\_unit\_thm}$

$\vdash \forall\ v : VALUE;\ a : ALPHABET\_REA;\ n : NAME$
$\quad |\ n \neq tr \wedge n \neq dash\ tr \wedge n \in a$
$\quad \bullet\ R2\ (=_R (a,\ n,\ Val\ v)) = =_R (a,\ n,\ Val\ v)$

$\boldsymbol{REA\_R1\_\lhd_R\_\rhd_R\_dist\_thm}$

$\vdash \forall\ u1,\ u2,\ b : REL\_PREDICATE$
$\quad |\ (u1,\ b,\ u2) \in WF\_Cond_R$
$\quad \bullet\ R1\ (u1 \lhd_R b \rhd_R u2) = R1\ u1 \lhd_R b \rhd_R R1\ u2$

$\boldsymbol{REA\_R2\_Equals_R\_unit\_thm1}$

$\vdash \forall\ a : ALPHABET\_REA;\ n1,\ n2 : NAME$
$\quad |\ n1 \neq tr$
$\quad\quad \wedge\ n1 \neq dash\ tr$
$\quad\quad \wedge\ n2 \neq tr$
$\quad\quad \wedge\ n2 \neq dash\ tr$
$\quad\quad \wedge\ n1 \in a$
$\quad\quad \wedge\ n2 \in a$
$\quad \bullet\ R2\ (=_R (a,\ n1,\ Var\ n2)) = =_R (a,\ n1,\ Var\ n2)$

$\boldsymbol{REA\_PREDICATE\_dash\_tr\_Equals\_tr\_thm}$

$\vdash \forall\ a : ALPHABET\_REA$
$\quad \bullet\ =_R (a,\ dash\ tr,\ Var\ tr) \in REA\_PREDICATE$

$\boldsymbol{REA\_dash\_tr\_Equals\_tr\_alphabet\_thm}$

$\vdash \forall\ a : ALPHABET\_REA \bullet (=_R (a,\ dash\ tr,\ Var\ tr)).1 = a$

$\boldsymbol{REA\_dash\_tr\_equals\_tr\_thm}$

$\vdash \forall\ a : ALPHABET\_REA$
$\quad \bullet\ =_{+R}$
$\quad\quad (a,$

$$
\begin{array}{l}
\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Fun}_2 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad ((\_\ \mathit{SeqDif}_R\ \_), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Var}\ (\mathit{dash}\ \mathit{tr}), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Var}\ \mathit{tr}), \\
\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Val}\ (\mathit{Seq}\ \langle\rangle)) \\
\quad\quad\quad\quad\quad\quad\quad \wedge_R =_{+R} \\
\quad\quad\quad\quad\quad\quad\quad\quad (\mathit{ALPHABET\_OWTR}, \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Rel}\ ((\_ \leq_R \_),\ \mathit{Var}\ \mathit{tr},\ \mathit{Var}\ (\mathit{dash}\ \mathit{tr})), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Val}\ (\mathit{Bool}\ \mathit{true})) \\
\quad\quad\quad\quad\quad\quad = =_R (a,\ \mathit{dash}\ \mathit{tr},\ \mathit{Var}\ \mathit{tr})
\end{array}
$$

REA_R2_dash_tr_Equals_tr_unit_thm

$$
\begin{array}{l}
\vdash \forall\ a : \mathit{ALPHABET\_REA} \\
\quad \bullet\ \mathit{R1}\ (\mathit{R2}\ (=_R (a,\ \mathit{dash}\ \mathit{tr},\ \mathit{Var}\ \mathit{tr}))) \\
\quad\quad = =_R (a,\ \mathit{dash}\ \mathit{tr},\ \mathit{Var}\ \mathit{tr})
\end{array}
$$

REA_R1_dash_tr_Equals_tr_unit_thm

$$
\begin{array}{l}
\vdash \forall\ a : \mathit{ALPHABET\_REA} \\
\quad \bullet\ \mathit{R1}\ (=_R (a,\ \mathit{dash}\ \mathit{tr},\ \mathit{Var}\ \mathit{tr})) \\
\quad\quad = =_R (a,\ \mathit{dash}\ \mathit{tr},\ \mathit{Var}\ \mathit{tr})
\end{array}
$$

REA_R2_dash_wait_unit_thm

$$
\begin{array}{l}
\vdash \forall\ v : \mathit{VALUE};\ a : \mathit{ALPHABET\_REA} \\
\quad \bullet\ \mathit{R2}\ (=_R (a,\ \mathit{dash}\ \mathit{wait},\ \mathit{Val}\ v)) \\
\quad\quad = =_R (a,\ \mathit{dash}\ \mathit{wait},\ \mathit{Val}\ v)
\end{array}
$$

REA_wait_false_id_thm

$$
\begin{array}{l}
\vdash \forall\ r : \mathit{REA\_PREDICATE} \\
\quad \mid \mathit{unrestTypedVar}\ (r,\ \mathit{wait},\ \mathit{BOOL\_VAL}) \\
\quad \bullet\ r\ \omega_f = r
\end{array}
$$

REA_wait_true_id_thm

$$
\begin{array}{l}
\vdash \forall\ r : \mathit{REA\_PREDICATE} \\
\quad \mid \mathit{unrestTypedVar}\ (r,\ \mathit{wait},\ \mathit{BOOL\_VAL}) \\
\quad \bullet\ r\ \omega_t = r
\end{array}
$$

REA_Equals_wait_false_thm

$$
\begin{array}{l}
\vdash =_R (\mathit{ALPHABET\_OWTR},\ \mathit{okay},\ \mathit{Val}\ (\mathit{Bool}\ \mathit{false})) \\
\quad = =_R (\mathit{ALPHABET\_OWTR},\ \mathit{okay},\ \mathit{Val}\ (\mathit{Bool}\ \mathit{false}))\ \omega_f
\end{array}
$$

***REA_Equals_wait_false_thm*1**

$$
\begin{array}{l}
\vdash =_R (\mathit{ALPHABET\_OWTR},\ \mathit{okay},\ \mathit{Val}\ (\mathit{Bool}\ \mathit{true})) \\
\quad = =_R (\mathit{ALPHABET\_OWTR},\ \mathit{okay},\ \mathit{Val}\ (\mathit{Bool}\ \mathit{true}))\ \omega_f
\end{array}
$$

REA_Equals_wait_true_thm

$$
\vdash =_R (\mathit{ALPHABET\_OWTR},\ \mathit{okay},\ \mathit{Val}\ (\mathit{Bool}\ \mathit{false}))
$$

$= =_R\ (ALPHABET\_OWTR,\ okay,\ Val\ (Bool\ false))\ \omega_t$

***REA_Equals_wait_true_thm*1**

$\vdash =_R\ (ALPHABET\_OWTR,\ okay,\ Val\ (Bool\ true))$
$= =_R\ (ALPHABET\_OWTR,\ okay,\ Val\ (Bool\ true))\ \omega_t$

REA_R*2*_*Π_{REA}*_idem_thm

$\vdash \forall\ a : ALPHABET\_REA$
$\mid a \in WF\_Skip_{REA}$
$\bullet\ R1\ (R2\ (\Pi_{REA}\ a)) = R1\ (\Pi_{REA}\ a)$

REA_R*3*_R*2*_com_thm

$\vdash \forall\ r : REA\_PREDICATE$
$\mid r.1 \in WF\_Skip_{REA}$
$\bullet\ R1\ (R2\ (R3\ r)) = R1\ (R3\ (R2\ r))$

REA_R_idem_thm

$\vdash \forall\ r : REA\_PREDICATE$
$\mid r.1 \in WF\_Skip_{REA}$
$\bullet\ R\ (R\ r) = R\ r$

REA_PREDICATE_wait_*$\in$*_ALPHABET_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet wait \in r.1$

REA_PREDICATE_okay_dash_*$\in$*_ALPHABET_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet dash\ okay \in r.1$

REA_PREDICATE_wait_true_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet r\ \omega_t \in REA\_PREDICATE$

REA_PREDICATE_wait_false_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet r\ \omega_f \in REA\_PREDICATE$

REA_PREDICATE_okay_dash_converge_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet r\ \sigma_t \in REA\_PREDICATE$

REA_PREDICATE_okay_dash_diverge_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet r\ \sigma_f \in REA\_PREDICATE$

REA_PREDICATE_wait_true_alphabet_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet (r\ \omega_t).1 = r.1$

REA_PREDICATE_wait_false_alphabet_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet (r\ \omega_f).1 = r.1$

REA_PREDICATE_okay_dash_converge_alphabet_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet (r\ \sigma_t).1 = r.1$

REA_PREDICATE_okay_dash_diverge_alphabet_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet (r\ \sigma_f).1 = r.1$

REA_R*1*_def_*$\in$*_REL_PREDICATE_thm

$\vdash =_{+R}$

$(ALPHABET\_OWTR,$
$Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$Val\ (Bool\ true))$
$\in REL\_PREDICATE$

REA_R1_def_wait_false_id_thm

$\vdash =_{+R}$
$(ALPHABET\_OWTR,$
$Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$Val\ (Bool\ true))\ \omega_f$
$= =_{+R}$
$(ALPHABET\_OWTR,$
$Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$Val\ (Bool\ true))$

REA_R1_def_wait_true_id_thm

$\vdash =_{+R}$
$(ALPHABET\_OWTR,$
$Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$Val\ (Bool\ true))\ \omega_t$
$= =_{+R}$
$(ALPHABET\_OWTR,$
$Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$Val\ (Bool\ true))$

REA_R1_def_okay_dash_diverge_id_thm

$\vdash =_{+R}$
$(ALPHABET\_OWTR,$
$Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$Val\ (Bool\ true))\ \sigma_f$
$= =_{+R}$
$(ALPHABET\_OWTR,$
$Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$Val\ (Bool\ true))$

REA_R1_def_okay_dash_converge_id_thm

$\vdash =_{+R}$
$(ALPHABET\_OWTR,$
$Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$Val\ (Bool\ true))\ \sigma_t$
$= =_{+R}$
$(ALPHABET\_OWTR,$

$Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$Val\ (Bool\ true))$

REA_R2_def_wait_false_com_thm

$\vdash \forall\ r : REA\_PREDICATE$
$\bullet\ /_R$
$(/_R\ (r,\ Val\ (Seq\ \langle\rangle),\ tr),$
Fun_2
$((\_\ SeqDif_R\ \_),$
$Var\ (dash\ tr),$
$Var\ tr),$
$dash\ tr)\ \omega_f$
$=\ /_R$
$(/_R\ (r\ \omega_f,\ Val\ (Seq\ \langle\rangle),\ tr),$
Fun_2
$((\_\ SeqDif_R\ \_),$
$Var\ (dash\ tr),$
$Var\ tr),$
$dash\ tr)$

REA_R2_def_wait_true_com_thm

$\vdash \forall\ r : REA\_PREDICATE$
$\bullet\ /_R$
$(/_R\ (r,\ Val\ (Seq\ \langle\rangle),\ tr),$
Fun_2
$((\_\ SeqDif_R\ \_),$
$Var\ (dash\ tr),$
$Var\ tr),$
$dash\ tr)\ \omega_t$
$=\ /_R$
$(/_R\ (r\ \omega_t,\ Val\ (Seq\ \langle\rangle),\ tr),$
Fun_2
$((\_\ SeqDif_R\ \_),$
$Var\ (dash\ tr),$
$Var\ tr),$
$dash\ tr)$

REA_R2_def_okay_dash_diverge_com_thm

$\vdash \forall\ r : REA\_PREDICATE$
$\bullet\ /_R$
$(/_R\ (r,\ Val\ (Seq\ \langle\rangle),\ tr),$

$$
\begin{array}{l}
\quad\quad Fun_2 \\
\quad\quad\quad ((\_\ SeqDif_R\ \_), \\
\quad\quad\quad\quad Var\ (dash\ tr), \\
\quad\quad\quad\quad Var\ tr), \\
\quad\quad dash\ tr)\ \sigma_f \\
= /_R \\
\quad (/_R\ (r\ \sigma_f,\ Val\ (Seq\ \langle\rangle),\ tr), \\
\quad\quad Fun_2 \\
\quad\quad\quad ((\_\ SeqDif_R\ \_), \\
\quad\quad\quad\quad Var\ (dash\ tr), \\
\quad\quad\quad\quad Var\ tr), \\
\quad\quad dash\ tr)
\end{array}
$$

REA_R2_def_okay_dash_converge_com_thm

$$
\begin{array}{l}
\vdash \forall\ r : REA\_PREDICATE \\
\quad \bullet /_R \\
\quad\quad (/_R\ (r,\ Val\ (Seq\ \langle\rangle),\ tr), \\
\quad\quad\quad Fun_2 \\
\quad\quad\quad\quad ((\_\ SeqDif_R\ \_), \\
\quad\quad\quad\quad\quad Var\ (dash\ tr), \\
\quad\quad\quad\quad\quad Var\ tr), \\
\quad\quad\quad dash\ tr)\ \sigma_t \\
\quad = /_R \\
\quad\quad (/_R\ (r\ \sigma_t,\ Val\ (Seq\ \langle\rangle),\ tr), \\
\quad\quad\quad Fun_2 \\
\quad\quad\quad\quad ((\_\ SeqDif_R\ \_), \\
\quad\quad\quad\quad\quad Var\ (dash\ tr), \\
\quad\quad\quad\quad\quad Var\ tr), \\
\quad\quad\quad dash\ tr)
\end{array}
$$

REA_R1_wait_false_com_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet R1\ r\ \omega_f = R1\ (r\ \omega_f)$

REA_R1_wait_true_com_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet R1\ r\ \omega_t = R1\ (r\ \omega_t)$

REA_R1_okay_dash_diverge_com_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet R1\ r\ \sigma_f = R1\ (r\ \sigma_f)$

REA_R1_okay_dash_converge_com_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet R1\ r\ \sigma_t = R1\ (r\ \sigma_t)$

REA_R2_wait_false_com_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet R2\ r\ \omega_f = R2\ (r\ \omega_f)$

$\boldsymbol{REA\_R2\_wait\_true\_com\_thm}$

$\vdash \forall\ r : REA\_PREDICATE \bullet R2\ r\ \omega_t = R2\ (r\ \omega_t)$

$\boldsymbol{REA\_R2\_okay\_dash\_diverge\_com\_thm}$

$\vdash \forall\ r : REA\_PREDICATE \bullet R2\ r\ \sigma_f = R2\ (r\ \sigma_f)$

$\boldsymbol{REA\_R2\_okay\_dash\_converge\_com\_thm}$

$\vdash \forall\ r : REA\_PREDICATE \bullet R2\ r\ \sigma_t = R2\ (r\ \sigma_t)$

$\boldsymbol{REA\_R1\_def\_\in\_WF\_ALPHABET\_EXPRESSION\_thm}$

$$\begin{array}{l} \vdash (ALPHABET\_OWTR, \\ \quad Rel\ ((\_ \leq_R \_), Var\ tr, Var\ (dash\ tr)), \\ \quad Val\ (Bool\ true)) \\ \ \in WF\_ALPHABET\_EXPRESSION \end{array}$$

$\boldsymbol{REA\_R2\_OKAY\_def\_ext\_unit\_thm}$

$$\begin{array}{l} \vdash \forall\ v : VALUE \\ \quad \bullet R2\ (=_R (ALPHABET\_OWTR, okay, Val\ v)) \\ \quad\ = =_R (ALPHABET\_OWTR, okay, Val\ v) \end{array}$$

$\boldsymbol{REA\_R2\_OKAY\_def\_ext\_unit\_thm1}$

$$\begin{array}{l} \vdash \forall\ v : VALUE; a : ALPHABET\_REA \\ \quad \bullet R2\ (=_R (a, okay, Val\ v)) = =_R (a, okay, Val\ v) \end{array}$$

$\boldsymbol{REA\_closure\_\wedge_R\_R1\_thm}$

$$\begin{array}{l} \vdash \forall\ r1, r2 : REL\_PREDICATE \\ \quad \mid \{r1, r2\} \subseteq R1\_healthy \\ \quad \bullet R1\ (r1 \wedge_R r2) = r1 \wedge_R r2 \end{array}$$

$\boldsymbol{REA\_closure\_\vee_R\_R1\_thm}$

$$\begin{array}{l} \vdash \forall\ r1, r2 : REL\_PREDICATE \\ \quad \mid \{r1, r2\} \subseteq R1\_healthy \\ \quad \bullet R1\ (r1 \vee_R r2) = r1 \vee_R r2 \end{array}$$

$\boldsymbol{REA\_PREDICATE\_True_R\_thm}$

$\vdash \forall\ a : ALPHABET\_REA \bullet True_R\ a \in REA\_PREDICATE$

$\boldsymbol{REA\_PREDICATE\_Equals_R\_thm}$

$$\begin{array}{l} \vdash \forall\ a : ALPHABET\_REA; n : NAME; e : EXPRESSION \\ \quad \mid (a, n, e) \in WF\_Equals_R \\ \quad \bullet =_R (a, n, e) \in REA\_PREDICATE \end{array}$$

$\boldsymbol{REA\_wait\_\in\_WF\_Equals_R\_thm}$

$$\begin{array}{l} \vdash \forall\ a : ALPHABET\_REA \\ \quad \bullet (a, wait, Val\ (Bool\ true)) \in WF\_Equals_R \end{array}$$

$\boldsymbol{REA\_not\_wait\_\in\_WF\_Equals_R\_thm}$

$$\begin{array}{l} \vdash \forall\ a : ALPHABET\_REA \\ \quad \bullet (a, wait, Val\ (Bool\ false)) \in WF\_Equals_R \end{array}$$

$\boldsymbol{REA\_wait\_dash\_\in\_WF\_Equals_R\_thm}$

$\vdash \forall\ a : ALPHABET\_REA$
$\quad \bullet\ (a,\ dash\ wait,\ Val\ (Bool\ true)) \in WF\_Equals_R$

$\boldsymbol{REA\_not\_wait\_dash\_\in\_WF\_Equals_R\_thm}$

$\vdash \forall\ a : ALPHABET\_REA$
$\quad \bullet\ (a,\ dash\ wait,\ Val\ (Bool\ false)) \in WF\_Equals_R$

$\boldsymbol{REA\_R2\_True_R\_unit\_thm}$

$\vdash \forall\ a : ALPHABET\_REA \bullet R2\ (True_R\ a) = True_R\ a$

$\boldsymbol{REA\_R2\_\Rightarrow_R\_dist\_thm}$

$\vdash \forall\ r1,\ r2 : REA\_PREDICATE$
$\quad \bullet\ R2\ (r1 \Rightarrow_R r2) = R2\ r1 \Rightarrow_R R2\ r2$

$\boldsymbol{REA\_ALPHABET\_OWTR\_homogeneous\_thm}$

$\vdash ALPHABET\_OWTR \in homogeneous$

$\boldsymbol{REA\_PREDICATE\_False_R\_thm}$

$\vdash \forall\ a : ALPHABET\_REA \bullet False_R\ a \in REA\_PREDICATE$

$\boldsymbol{REA\_PROCESS\_thm1}$

$\vdash \forall\ r : REA\_PROCESS \bullet r \in REA\_PREDICATE \land r \in R\_healthy$

$\boldsymbol{REA\_R\_healthy\_thm}$

$\vdash \forall\ r : REA\_PREDICATE$
$\quad |\ r \in R\_healthy \land r.1 \in WF\_Skip_{REA}$
$\quad \bullet\ r = R\ r$

$\boldsymbol{REA\_PREDICATE\_\in\_WF\_Skip_{REA}\_thm}$

$\vdash \forall\ a : ALPHABET\_REA$
$\quad |\ a \in homogeneous$
$\quad \bullet\ a \in WF\_Skip_{REA}$

$\boldsymbol{REA\_R\_healthy\_is\_R1\_healthy\_thm}$

$\vdash \forall\ r : REA\_PROCESS\ |\ r \in R\_healthy \bullet r \in R1\_healthy$

$\boldsymbol{REA\_R1\_healthy\_thm}$

$\vdash \forall\ r : REA\_PROCESS \bullet r = R1\ r$

$\boldsymbol{REA\_R\_healthy\_R1\_zero\_thm}$

$\vdash \forall\ r : REA\_PROCESS$
$\quad \bullet\ r$
$\qquad \lor_R =_{+R}$
$\qquad\quad (ALPHABET\_OWTR,$
$\qquad\quad\ \ Rel\ ((\_ \le_R \_),\ Var\ tr,\ Var\ (dash\ tr)),$
$\qquad\quad\ \ Val\ (Bool\ true))$
$\quad = =_{+R}$
$\qquad (r.1,$

$Rel\ ((\_ \leq_R \_), Var\ tr, Var\ (dash\ tr)),$
$Val\ (Bool\ true))$

$\boldsymbol{REA\_R\_R1\_idem\_thm}$
$\vdash \forall\ r : REA\_PREDICATE$
$\mid r.1 \in WF\_Skip_{REA}$
$\bullet\ R\ (R1\ r) = R\ r$

$\boldsymbol{REA\_okay\_dash\_diverge\_wait\_false\_com\_thm}$
$\vdash \forall\ r : REA\_PREDICATE \bullet (r\ \sigma_f)\ \omega_f = (r\ \omega_f)\ \sigma_f$

$\boldsymbol{REA\_okay\_dash\_converge\_wait\_false\_com\_thm}$
$\vdash \forall\ r : REA\_PREDICATE \bullet (r\ \sigma_t)\ \omega_f = (r\ \omega_f)\ \sigma_t$

$\boldsymbol{REA\_WF\_Skip_{REA}\_\cup\_dist\_thm}$
$\vdash \forall\ a1, a2 : WF\_Skip_{REA} \bullet a1 \cup a2 \in WF\_Skip_{REA}$

$\boldsymbol{REA\_\Pi_{REA}\_alphabet\_\vee_R\_dist\_thm1}$
$\vdash \forall\ r1, r2 : REA\_PREDICATE$
$\mid r1.1 \in WF\_Skip_{REA}$
$\wedge\ r2.1 \in WF\_Skip_{REA}$
$\wedge\ r1.1 = r2.1$
$\bullet\ \Pi_{REA}\ (r1 \vee_R r2).1 = \Pi_{REA}\ r1.1 \vee_R \Pi_{REA}\ r2.1$

$\boldsymbol{REA\_R3\_\vee_R\_dist\_thm1}$
$\vdash \forall\ r1, r2 : REA\_PREDICATE$
$\mid r1.1 \in WF\_Skip_{REA}$
$\wedge\ r2.1 \in WF\_Skip_{REA}$
$\wedge\ r1.1 = r2.1$
$\bullet\ R3\ (r1 \vee_R r2) = R3\ r1 \vee_R R3\ r2$

$\boldsymbol{REA\_R\_healthy\_\vee_R\_dist\_thm1}$
$\vdash \forall\ r1, r2 : REA\_PREDICATE$
$\mid r1 \in R\_healthy \wedge r2 \in R\_healthy \wedge r1.1 = r2.1$
$\bullet\ r1 \vee_R r2 \in R\_healthy$

$\boldsymbol{REA\_PROCESS\_\vee_R\_thm1}$
$\vdash \forall\ r1, r2 : REA\_PROCESS$
$\mid r1.1 = r2.1$
$\bullet\ r1 \vee_R r2 \in REA\_PROCESS$

$\boldsymbol{REA\_PREDICATE\_Semi_R\_thm}$
$\vdash \forall\ A1, A2 : REA\_PREDICATE$
$\mid (A1, A2) \in WF\_Semi_R$
$\bullet\ A1 ;_R A2 \in REA\_PREDICATE$

$\boldsymbol{REA\_R\_healthy\_is\_R3\_healthy\_thm}$
$\vdash \forall\ r : REA\_PROCESS \mid r \in R\_healthy \bullet r \in R3\_healthy$

$\boldsymbol{REA\_R3\_healthy\_thm}$

$\vdash \forall\ r : REA\_PROCESS \bullet r = R3\ r$

$\boldsymbol{REA\_R1\_\vee_R\_dist\_thm1}$

$\vdash \forall\ r1, r2 : REA\_PREDICATE$
$\quad | \ r1.1 \in WF\_Skip_{REA}$
$\quad \wedge r2.1 \in WF\_Skip_{REA}$
$\quad \wedge r2.1 = r1.1$
$\quad \bullet R\ r1 \vee_R R\ r2 = R\ (r1 \vee_R r2)$

$\boldsymbol{REA\_Semi_R\_is\_R\_healthy\_thm1}$

$\vdash \forall\ r1, r2 : REA\_PROCESS$
$\quad | \ (r1, r2) \in WF\_Semi_R \wedge r1.1 = r2.1$
$\quad \bullet r1 \ ;_R\ r2 \in R\_healthy$

$\boldsymbol{REA\_PROCESS\_Semi_R\_thm1}$

$\vdash \forall\ r1, r2 : REA\_PROCESS$
$\quad | \ (r1, r2) \in WF\_Semi_R \wedge r1.1 = r2.1$
$\quad \bullet r1 \ ;_R\ r2 \in REA\_PROCESS$

$\boldsymbol{REA\_R1\_R2\_is\_healthy\_thm}$

$\vdash \forall\ r : REA\_PROCESS \mid r \in R\_healthy \bullet R1\ (R2\ r) = r$

$\boldsymbol{REA\_closure\_Semi_R\_R\_thm1}$

$\vdash \forall\ r1, r2 : REA\_PROCESS$
$\quad | \ (r1, r2) \in WF\_Semi_R$
$\quad \wedge r1.1 = r2.1$
$\quad \wedge r1 \in R\_healthy$
$\quad \wedge r2 \in R\_healthy$
$\quad \bullet R\ (r1 \ ;_R\ r2) = r1 \ ;_R\ r2$

$\boldsymbol{REA\_PREDICATE\_thm1}$

$\vdash \forall\ r : REA\_PREDICATE$
$\quad \bullet r \in REL\_PREDICATE$
$\quad \wedge ALPHABET\_OWTR \subseteq r.1$
$\quad \wedge r.1 \in ALPHABET\_REA$

$\boldsymbol{REA\_dash\_wait\_\in\_WF\_Equals_R\_thm}$

$\vdash \forall\ a : ALPHABET\_REA$
$\quad \bullet (a, dash\ wait, Val\ (Bool\ true)) \in WF\_Equals_R$

$\boldsymbol{REA\_PREDICATE\_Equals_R\_dash\_wait\_thm}$

$\vdash \forall\ a : ALPHABET\_REA$
$\quad \bullet =_R (a, dash\ wait, Val\ (Bool\ true))$
$\quad \in REA\_PREDICATE$

$\boldsymbol{REA\_okay\_\in\_WF\_Equals_R\_thm}$

$\vdash \forall\ a : ALPHABET\_REA$
$\bullet\ (a,\ okay,\ Val\ (Bool\ true)) \in WF\_Equals_R$

$\boldsymbol{REA\_not\_okay\_\in\_WF\_Equals_R\_thm}$
$\vdash \forall\ a : ALPHABET\_REA$
$\bullet\ (a,\ okay,\ Val\ (Bool\ false)) \in WF\_Equals_R$

$\boldsymbol{REA\_UnrestTypedVar\_wait\_false\_thm}$
$\vdash \forall\ r : REA\_PREDICATE$
$\bullet\ unrestTypedVar\ (r\ \omega_f,\ wait,\ BOOL\_VAL)$

$\boldsymbol{REA\_UnrestTypedVar\_wait\_true\_thm}$
$\vdash \forall\ r : REA\_PREDICATE$
$\bullet\ unrestTypedVar\ (r\ \omega_t,\ wait,\ BOOL\_VAL)$

$\boldsymbol{REA\_UnrestTypedVar\_okay\_dash\_converge\_thm}$
$\vdash \forall\ r : REA\_PREDICATE$
$\bullet\ unrestTypedVar\ (r\ \sigma_t,\ dash\ okay,\ BOOL\_VAL)$

$\boldsymbol{REA\_UnrestTypedVar\_okay\_dash\_diverge\_thm}$
$\vdash \forall\ r : REA\_PREDICATE$
$\bullet\ unrestTypedVar\ (r\ \sigma_f,\ dash\ okay,\ BOOL\_VAL)$

$\boldsymbol{REA\_R3\_\wedge_R\_dist\_thm1}$
$\vdash \forall\ r1,\ r2 : REA\_PREDICATE$
$\mid r1.1 \in WF\_Skip_{REA}$
$\wedge\ r2.1 \in WF\_Skip_{REA}$
$\wedge\ r1.1 = r2.1$
$\bullet\ R3\ (r1 \wedge_R r2) = R3\ r1 \wedge_R R3\ r2$

$\boldsymbol{REA\_R\_healthy\_\wedge_R\_dist\_thm1}$
$\vdash \forall\ r1,\ r2 : REA\_PREDICATE$
$\mid r1 \in R\_healthy \wedge r2 \in R\_healthy \wedge r1.1 = r2.1$
$\bullet\ r1 \wedge_R r2 \in R\_healthy$

$\boldsymbol{REA\_PROCESS\_\wedge_R\_thm1}$
$\vdash \forall\ r1,\ r2 : REA\_PROCESS$
$\mid r1.1 = r2.1$
$\bullet\ r1 \wedge_R r2 \in REA\_PROCESS$

$\boldsymbol{REA\_Equals\_wait\_false\_thm2}$
$\vdash =_R (ALPHABET\_OWTR,\ dash\ okay,\ Val\ (Bool\ true))$
$= =_R$
$(ALPHABET\_OWTR,$
$dash\ okay,$
$Val\ (Bool\ true))\ \omega_f$

$\boldsymbol{REA\_R1\_wait\_false\_thm}$

$\vdash \forall\ u : REA\_PROCESS \bullet R1\ \ u\ \omega_f\ =\ R1\ \ (u\ \omega_f)$

REA_R1_wait_false_thm1

$\vdash \forall\ u : REA\_PREDICATE \bullet R1\ \ u\ \omega_f\ =\ R1\ \ (u\ \omega_f)$

REA_dash_okay_diverge_id_thm

$\vdash \forall\ r : REA\_PREDICATE$
$\quad |\ unrestTypedVar\ (r,\ dash\ okay,\ BOOL\_VAL)$
$\quad \bullet\ r\ \sigma_f\ =\ r$

REA_dash_okay_converge_id_thm

$\vdash \forall\ r : REA\_PREDICATE$
$\quad |\ unrestTypedVar\ (r,\ dash\ okay,\ BOOL\_VAL)$
$\quad \bullet\ r\ \sigma_t\ =\ r$

REA_okay_dash_diverge_idem_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet (r\ \sigma_f)\ \sigma_f\ =\ r\ \sigma_f$

REA_okay_dash_converge_idem_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet (r\ \sigma_t)\ \sigma_t\ =\ r\ \sigma_t$

REA_wait_false_idem_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet (r\ \omega_f)\ \omega_f\ =\ r\ \omega_f$

REA_wait_true_idem_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet (r\ \omega_t)\ \omega_t\ =\ r\ \omega_t$

R_healthy_thm

$\vdash \forall\ r : REA\_PROCESS \bullet r \in R\_healthy$

REA_R_not_wait_thm

$\vdash \forall\ r : REA\_PREDICATE$
$\quad |\ r.1 \in WF\_Skip_{REA}$
$\quad \bullet\ R\ \ r\ \omega_f\ =\ R1\ \ (R2\ \ r)\ \omega_f$

REA_R1_def_∈_R1_healthy_thm

$$
\begin{aligned}
\vdash R1 & \\
&\quad (=_{+R} \\
&\qquad (ALPHABET\_OWTR, \\
&\qquad\ \ Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)), \\
&\qquad\ \ Val\ (Bool\ true))) \\
&= =_{+R} \\
&\quad (ALPHABET\_OWTR, \\
&\quad\ \ Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)), \\
&\quad\ \ Val\ (Bool\ true))
\end{aligned}
$$

REA_PREDICATE_$\lhd_R$_$\rhd_R$_thm

$\vdash \forall\ u1,\ u2,\ b : REA\_PREDICATE$
$\quad |\ (u1,\ b,\ u2) \in WF\_Cond_R$

$\bullet\ u1 \lhd_R b \rhd_R u2 \in REA\_PREDICATE$

REA_PREDICATE_thm2

$\vdash \forall r : REA\_PREDICATE \bullet r \in REL\_PREDICATE$

REA_wait_∈_REA_PREDICATE_thm

$\vdash \forall r : REA\_PREDICATE \bullet wait \in r.1$

REA_dash_okay_∈_REA_PREDICATE_thm

$\vdash \forall r : REA\_PREDICATE \bullet dash\ okay \in r.1$

REA_¬$_R$_wait_false_com_thm

$\vdash \forall r : REA\_PREDICATE \bullet \neg_R\ r\ \omega_f = \neg_R\ (r\ \omega_f)$

REA_¬$_R$_wait_true_com_thm

$\vdash \forall r : REA\_PREDICATE \bullet \neg_R\ r\ \omega_t = \neg_R\ (r\ \omega_t)$

REA_¬$_R$_dash_okay_false_com_thm

$\vdash \forall r : REA\_PREDICATE \bullet \neg_R\ r\ \sigma_f = \neg_R\ (r\ \sigma_f)$

REA_¬$_R$_dash_okay_true_com_thm

$\vdash \forall r : REA\_PREDICATE \bullet \neg_R\ r\ \sigma_t = \neg_R\ (r\ \sigma_t)$

13 THE Z THEORY utp-csp

13.1 Parents

$utp{-}rea \qquad utp{-}des$

13.2 Global Variables

$\boldsymbol{unrestALPHABET\_CSP}$
$\quad \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{B}$
$\boldsymbol{unrestALPHABET\_CSP'}$
$\quad \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{B}$
$\boldsymbol{VAR\_NAME}\ \mathbb{P}\ NAME$
$\boldsymbol{CSP1} \quad \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{CSP1\_healthy} \quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{CSP2} \quad \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{CSP2\_healthy} \quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{CSP\_PROCESS} \quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{WF\_CSP\_PROCESS\_PAIR}$
$\quad \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{WF\_PREFIXING} \quad \mathbb{P}\ (\mathbb{P}\ NAME \times NAME \times EXPRESSION)$
$\boldsymbol{STOP} \quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{SKIP} \quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{CHAOS} \quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$(\_ \boxtimes_{CSP} \_) \quad (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{\Phi} \quad \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$(\boldsymbol{do\_A}\ \_) \quad \mathbb{P}\ NAME \times NAME \times EXPRESSION \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALU$
$(\_ \rightarrow_{CSP} \_) \quad (\mathbb{P}\ NAME \times NAME \times EXPRESSION)$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$(\boldsymbol{do\_C}\ \_) \quad \mathbb{P}\ NAME \times NAME \times EXPRESSION \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALU$
$\boldsymbol{CSP3\_healthy} \quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{CSP4\_healthy} \quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

13.3 Fixity

fun* 0 *rightassoc

$$(do\_A\ \_) \qquad (do\_C\ \_) \qquad (\_\ \boxtimes_{CSP}\ \_) \qquad (\_\ \rightarrow_{CSP}\ \_)$$

13.4 Axioms

unrestALPHABET_CSP

$$\begin{array}{l}
\vdash unrestALPHABET_CSP \in REL_PREDICATE \rightarrow \mathbb{B} \\
\quad \wedge (\forall\ r : REL_PREDICATE \\
\quad\ \ \bullet unrestALPHABET_CSP\ r \\
\quad\quad \Leftrightarrow unrestOKAY\ r \\
\quad\quad\ \ \wedge unrestWAIT\ r \\
\quad\quad\ \ \wedge unrestTR\ r \\
\quad\quad\ \ \wedge unrestREF\ r)
\end{array}$$

unrestALPHABET_CSP′

$$\begin{array}{l}
\vdash unrestALPHABET_CSP' \in REL_PREDICATE \rightarrow \mathbb{B} \\
\quad \wedge (\forall\ r : REL_PREDICATE \\
\quad\ \ \bullet unrestALPHABET_CSP'\ r \\
\quad\quad \Leftrightarrow unrestOKAY'\ r \\
\quad\quad\ \ \wedge unrestWAIT'\ r \\
\quad\quad\ \ \wedge unrestTR'\ r \\
\quad\quad\ \ \wedge unrestREF'\ r)
\end{array}$$

***CSP*1**

$$\begin{array}{l}
\vdash CSP1 \in REL_PREDICATE \rightarrow REL_PREDICATE \\
\quad \wedge (\forall\ r : REL_PREDICATE \\
\quad\ \ \bullet CSP1\ r \\
\quad\quad = r \\
\quad\quad\quad \vee_R =_R \\
\quad\quad\quad\quad\quad (ALPHABET_OWTR, \\
\quad\quad\quad\quad\quad\ \ okay, \\
\quad\quad\quad\quad\quad\ \ Val\ (Bool\ false)) \\
\quad\quad\quad\quad \wedge_R =_{+R} \\
\quad\quad\quad\quad\quad (ALPHABET_OWTR, \\
\quad\quad\quad\quad\quad\ \ Rel \\
\quad\quad\quad\quad\quad\quad\quad ((_\ \leq_R\ _), \\
\quad\quad\quad\quad\quad\quad\quad\ \ Var\ tr, \\
\quad\quad\quad\quad\quad\quad\quad\ \ Var\ (dash\ tr)), \\
\quad\quad\quad\quad\quad\ \ Val\ (Bool\ true)))
\end{array}$$

$\boldsymbol{CSP1\_healthy}$ $\quad \vdash CSP1\_healthy \in \mathbb{P}\ REL\_PREDICATE$

$\quad \land CSP1\_healthy = \{r : REL\_PREDICATE \mid r = CSP1\ r\}$

$\boldsymbol{CSP2}$ $\quad \vdash CSP2 \in REL\_PREDICATE \nrightarrow REL\_PREDICATE$

$\quad \land (\forall\ r : REL\_PREDICATE$

$\quad\quad \mid \{dash\ okay, dash\ wait, dash\ tr, dash\ ref\} \subseteq r.1$

$\quad\quad \bullet CSP2\ r = r\ ;_R\ J\ (out\_a\ r.1))$

$\boldsymbol{CSP2\_healthy}$ $\quad \vdash CSP2\_healthy \in \mathbb{P}\ REL\_PREDICATE$

$\quad \land CSP2\_healthy$

$\quad\quad = \{r : REL\_PREDICATE$

$\quad\quad\quad \mid \{dash\ okay, dash\ wait, dash\ tr, dash\ ref\}$

$\quad\quad\quad\quad \subseteq r.1$

$\quad\quad\quad \land r = CSP2\ r\}$

$\boldsymbol{STOP}$ $\quad \vdash STOP \in WF\_Skip_{REA} \rightarrow CSP\_PROCESS$

$\quad \land (\forall\ a : WF\_Skip_{REA}$

$\quad\quad \bullet STOP\ a$

$\quad\quad\quad = R\ (Assign_R\ (a, \langle wait \rangle, \langle Val\ (Bool\ true) \rangle)))$

$\boldsymbol{CSP\_STOP\_design\_thm}$

$\quad \vdash \forall\ a : ALPHABET\_REA$

$\quad\quad \mid a \in WF\_Skip_{REA}$

$\quad\quad \bullet STOP\ a$

$\quad\quad\quad = R$

$\quad\quad\quad\quad (True_R\ a$

$\quad\quad\quad\quad\quad \vdash_D =_R (a, dash\ tr, Var\ tr)$

$\quad\quad\quad\quad\quad\quad \land_R =_R$

$\quad\quad\quad\quad\quad\quad\quad (a, dash\ wait, Val\ (Bool\ true)))$

$\boldsymbol{SKIP}$ $\quad \vdash SKIP \in WF\_Skip_{REA} \rightarrow CSP\_PROCESS$

$\quad \land (\forall\ a : WF\_Skip_{REA}$

$\quad\quad \bullet SKIP\ a = R\ (\exists_R\ (\{ref\}, \mathit{\Pi}_{REA}\ a)))$

$\boldsymbol{CSP\_SKIP\_design\_thm}$

$\quad \vdash \forall\ a : ALPHABET\_REA$

$\quad\quad \mid a \in WF\_Skip_{REA}$

$\quad\quad \bullet SKIP\ a$

$\quad\quad\quad = R$

$\quad\quad\quad\quad (True_R\ a$

$\quad\quad\quad\quad\quad \vdash_D =_R (a, dash\ tr, Var\ tr)$

$\quad\quad\quad\quad\quad\quad \land_R =_R$

$\quad\quad\quad\quad\quad\quad\quad (a, dash\ wait, Val\ (Bool\ false)))$

$\boldsymbol{CHAOS}$ $\quad \vdash CHAOS \in WF\_Skip_{REA} \rightarrow CSP\_PROCESS$

$\land\ (\forall\ a : WF\_Skip_{REA} \bullet CHAOS\ a = R\ (True_R\ a))$

CSP_CHAOS_design_thm

$\vdash \forall\ a : ALPHABET\_REA$
$\quad |\ a \in WF\_Skip_{REA}$
$\quad \bullet\ CHAOS\ a = R\ (False_R\ a \vdash_D True_R\ a)$

_ $\boxtimes_{CSP}$ _

$\vdash (\_ \boxtimes_{CSP} \_) \in WF\_CSP\_PROCESS\_PAIR \to CSP\_PROCESS$
$\quad \land\ (\forall\ pp : WF\_CSP\_PROCESS\_PAIR$
$\quad\quad \bullet\ pp.1 \boxtimes_{CSP} pp.2$
$\quad\quad\quad = CSP2$
$\quad\quad\quad\quad ((pp.1 \land_R pp.2) \lhd_R$
$\quad\quad\quad\quad\quad STOP\ pp.1.1 \rhd_R$
$\quad\quad\quad\quad\quad pp.1 \lor_R pp.2))$

CSP_ $\boxtimes_{CSP}$ _design_thm_2

$\vdash \forall\ p1, p2 : CSP\_PROCESS$
$\quad |\ (p1, p2) \in WF\_CSP\_PROCESS\_PAIR$
$\quad \bullet\ p1 \boxtimes_{CSP} p2$
$\quad\quad = R$
$\quad\quad\quad ((\neg_R\ ((p1\ \sigma_f)\ \omega_f) \land_R \neg_R\ ((p2\ \sigma_f)\ \omega_f))$
$\quad\quad\quad\quad \vdash_D (((p1\ \sigma_t)\ \omega_f) \land_R (p2\ \sigma_t)\ \omega_f) \lhd_R$
$\quad\quad\quad\quad\quad =_{+R} (p1.1, Var\ (dash\ tr), Var\ tr)$
$\quad\quad\quad\quad\quad\quad \land_R =_R$
$\quad\quad\quad\quad\quad\quad\quad (p1.1,$
$\quad\quad\quad\quad\quad\quad\quad\quad dash\ wait,$
$\quad\quad\quad\quad\quad\quad\quad\quad Val\ (Bool\ true)) \rhd_R$
$\quad\quad\quad\quad\quad ((p1\ \sigma_t)\ \omega_f) \lor_R (p2\ \sigma_t)\ \omega_f)$

Φ

$\vdash \Phi \in CSP\_PROCESS \to CSP\_PROCESS$
$\quad \land\ (\forall\ p : CSP\_PROCESS$
$\quad\quad \bullet\ \Phi\ p$
$\quad\quad\quad = R$
$\quad\quad\quad\quad (p$
$\quad\quad\quad\quad\quad \land_R (=_R$
$\quad\quad\quad\quad\quad\quad\quad (ALPHABET\_OWTR,$
$\quad\quad\quad\quad\quad\quad\quad\quad dash\ tr,$
$\quad\quad\quad\quad\quad\quad\quad\quad Var\ tr)$
$\quad\quad\quad\quad\quad\quad \land_R =_R$
$\quad\quad\quad\quad\quad\quad\quad (ALPHABET\_OWTR,$
$\quad\quad\quad\quad\quad\quad\quad\quad dash\ wait,$
$\quad\quad\quad\quad\quad\quad\quad\quad Val\ (Bool\ true)))$

$$
\begin{array}{l}
\quad\quad\quad\quad\quad\quad\quad \vee_R =_{+R} \\
\quad\quad\quad\quad\quad\quad\quad\quad (ALPHABET\_OWTR, \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad Rel \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad ((\_ <_R \_), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad Var\ tr, \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad Var\ (dash\ tr)), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad Val\ (Bool\ true))))
\end{array}
$$

do_A _ $\vdash (do\_A\ \_) \in WF\_PREFIXING \to CSP\_PROCESS$

$$
\begin{array}{l}
\wedge\ (\forall\ a\_n\_e : WF\_PREFIXING \\
\quad \bullet\ do\_A\ a\_n\_e \\
\quad\quad = \Phi \\
\quad\quad\quad ((=_R (a\_n\_e.1,\ dash\ tr,\ Var\ tr) \\
\quad\quad\quad\quad\quad \wedge_R =_{+R} \\
\quad\quad\quad\quad\quad\quad (a\_n\_e.1, \\
\quad\quad\quad\quad\quad\quad\quad Rel \\
\quad\quad\quad\quad\quad\quad\quad\quad ((\_ \notin_R \_), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad Fun_2 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad (MkPair, \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad Val \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad (Channel \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad a\_n\_e.2), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad a\_n\_e.3), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad Var\ (dash\ ref)), \\
\quad\quad\quad\quad\quad\quad\quad Val\ (Bool\ true))) \lhd_R \\
\quad\quad\quad\quad =_R \\
\quad\quad\quad\quad\quad (a\_n\_e.1, \\
\quad\quad\quad\quad\quad\quad dash\ wait, \\
\quad\quad\quad\quad\quad\quad Val\ (Bool\ true)) \rhd_R \\
\quad\quad\quad\quad =_R \\
\quad\quad\quad\quad\quad (a\_n\_e.1, \\
\quad\quad\quad\quad\quad\quad dash\ tr, \\
\quad\quad\quad\quad\quad\quad Fun_2 \\
\quad\quad\quad\quad\quad\quad\quad ((\_ \frown_R \_), \\
\quad\quad\quad\quad\quad\quad\quad\quad Var\ tr, \\
\quad\quad\quad\quad\quad\quad\quad\quad Fun_1 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad (MkSingleton, \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad Fun_2
\end{array}
$$

$(MkPair,$
Val
$(Channel$
$a\_n\_e.2),$
$a\_n\_e.3))))))$

$\_ \rightarrow_{CSP} \_$ $\vdash (\_ \rightarrow_{CSP} \_)$
$\in WF\_PREFIXING \times CSP\_PROCESS \rightarrow CSP\_PROCESS$
$\wedge (\forall\ a\_n\_e : WF\_PREFIXING$
$\bullet\ a\_n\_e \rightarrow_{CSP} SKIP\ a\_n\_e.1$
$= CSP2$
$(=_R$
$(a\_n\_e.1,$
$dash\ okay,$
$Val\ (Bool\ true))$
$\wedge_R\ do\_A\ a\_n\_e)$
$\wedge (\forall\ p : CSP\_PROCESS$
$\bullet\ a\_n\_e \rightarrow_{CSP} p$
$= (a\_n\_e \rightarrow_{CSP} SKIP\ a\_n\_e.1)\ ;_R\ p))$

$do\_C\ \_$ $\vdash (do\_C\ \_) \in WF\_PREFIXING \rightarrow CSP\_PROCESS$
$\wedge (\forall\ a\_n\_e : WF\_PREFIXING$
$\bullet\ do\_C\ a\_n\_e$
$= (=_R (a\_n\_e.1,\ dash\ tr,\ Var\ tr)$
$\wedge_R =_{+R}$
$(a\_n\_e.1,$
Rel
$((\_ \notin_R \_),$
Fun_2
$(MkPair,$
$Val\ (Channel\ a\_n\_e.2),$
$a\_n\_e.3),$
$Var\ (dash\ ref)),$
$Val\ (Bool\ true))) \lhd_R$
$=_R$
$(a\_n\_e.1,$
$dash\ wait,$
$Val\ (Bool\ true)) \rhd_R$
$=_R$
$(a\_n\_e.1,$

$$
\begin{array}{l}
\quad dash\ tr, \\
\quad Fun_2 \\
\quad\quad ((\_ \frown_R \_), \\
\quad\quad\ Var\ tr, \\
\quad\quad\ Fun_1 \\
\quad\quad\quad (MkSingleton, \\
\quad\quad\quad\ Fun_2 \\
\quad\quad\quad\quad (MkPair, \\
\quad\quad\quad\quad\ Val \\
\quad\quad\quad\quad\quad (Channel \\
\quad\quad\quad\quad\quad\quad a\_n\_e.2), \\
\quad\quad\quad\quad\ a\_n\_e.3)))))
\end{array}
$$

$\boldsymbol{CSP\_\rightarrow_{CSP}\_design\_thm}$

$$
\begin{array}{l}
\vdash \forall\ a\_n\_e : WF\_PREFIXING \\
\quad \bullet\ a\_n\_e \rightarrow_{CSP} SKIP\ a\_n\_e.1 \\
\quad\quad = R\ (True_R\ a\_n\_e.1 \vdash_D do\_C\ a\_n\_e)
\end{array}
$$

$\boldsymbol{CSP3\_healthy}$ $\quad \vdash CSP3\_healthy \in \mathbb{P}\ CSP\_PROCESS$

$$
\begin{array}{l}
\wedge\ CSP3\_healthy \\
\quad = \{r : CSP\_PROCESS \\
\quad\quad \mid =_R (r.1,\ wait,\ Val\ (Bool\ false)) \\
\quad\quad\quad\quad \Rightarrow_R r \equiv_R \exists_R (\{ref\},\ r) \\
\quad\quad\quad = True_R\ r.1\}
\end{array}
$$

$\boldsymbol{CSP4\_healthy}$ $\quad \vdash CSP4\_healthy \in \mathbb{P}\ CSP\_PROCESS$

$$
\begin{array}{l}
\wedge\ CSP4\_healthy \\
\quad = \{r : CSP\_PROCESS \\
\quad\quad \mid (r,\ SKIP\ r.1) \in WF\_Semi_R \\
\quad\quad\quad \wedge\ r\ ;_R SKIP\ r.1 = r\}
\end{array}
$$

$\boldsymbol{CSP\_CSP2\_healthy\_Design\_thm}$

$$
\begin{array}{l}
\vdash \forall\ P,\ Q : REA\_PREDICATE \\
\quad \mid (P \vdash_D Q).1 \in homogeneous \\
\quad\quad \wedge\ (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR \\
\quad \bullet\ R\ (P \vdash_D Q) \in CSP2\_healthy
\end{array}
$$

$\boldsymbol{CSP\_rea\_des\_CSP1\_thm}$

$$
\begin{array}{l}
\vdash \forall\ d : WF\_DES\_PREDICATE\_PAIR \\
\quad \bullet\ R\ (d.1 \vdash_D d.2) = CSP1\ (R\ (d.1 \vdash_D d.2))
\end{array}
$$

$\boldsymbol{CSP\_closure\_\wedge_R\_CSP1\_thm}$

$$
\vdash \forall\ r1,\ r2 : REL\_PREDICATE
$$

$| \{r1, r2\} \subseteq CSP1\_healthy$
$\bullet\ CSP1\ (r1 \wedge_R r2) = r1 \wedge_R r2$

$\boldsymbol{CSP\_closure\_\vee_R\_CSP1\_thm}$
$\vdash \forall\ r1, r2 : REL\_PREDICATE$
$| \{r1, r2\} \subseteq CSP1\_healthy$
$\bullet\ CSP1\ (r1 \vee_R r2) = r1 \vee_R r2$

$\boldsymbol{CSP\_closure\_\lhd_R\_\rhd_R\_CSP1\_thm}$
$\vdash \forall\ r1, r2, b : REL\_PREDICATE$
$| (r1, b, r2) \in WF\_Cond_R \wedge \{r1, r2\} \subseteq CSP1\_healthy$
$\bullet\ CSP1\ (r1 \lhd_R b \rhd_R r2) = r1 \lhd_R b \rhd_R r2$

$\boldsymbol{CSP\_closure\_Semi_R\_CSP1\_thm}$
$\vdash \forall\ r1, r2 : REL\_PREDICATE$
$| (r1, r2) \in WF\_Semi_R \wedge \{r1, r2\} \subseteq CSP1\_healthy$
$\bullet\ CSP1\ (r1 ;_R r2) = r1 ;_R r2$

$\boldsymbol{CSP\_CSP1\_wait\_dash\_okay\_thm}$
$\vdash \forall\ r : REL\_PREDICATE; b1, b2 : BOOL\_VAL$
$| \{wai, dash\ okay\} \subseteq r.1$
$\bullet\ /_R$
$(/_R\ (CSP1\ r, Val\ b1, wait),$
$Val\ b2,$
$dash\ okay)$
$= CSP1$
$(/_R$
$(/_R\ (r, Val\ b1, wait),$
$Val\ b2,$
$dash\ okay))$

$\boldsymbol{CSP\_des\_post\_\wedge_R\_CSP1\_thm}$
$\vdash \forall\ d, r1, r2 : REL\_PREDICATE$
$| (d, r1 \wedge_R r2) \in WF\_DES\_PREDICATE\_PAIR$
$\wedge \{r1, r2\} \subseteq R1\_healthy$
$\bullet\ d \vdash_D r1 \wedge_R CSP1\ r2 = d \vdash_D r1 \wedge_R r2$

$\boldsymbol{CSP\_des\_post\_\wedge_R\_\neg_R\_CSP1\_thm}$
$\vdash \forall\ d, r1, r2 : REL\_PREDICATE$
$| (d, r1 \wedge_R \neg_R r2) \in WF\_DES\_PREDICATE\_PAIR$
$\wedge \{r1, r2\} \subseteq R1\_healthy\_def$
$\bullet\ d \vdash_D r1 \wedge_R \neg_R (CSP1\ r2) = d \vdash_D r1 \wedge_R \neg_R r2$

$\boldsymbol{CSP\_des\_post\_\lhd_R\_\rhd_R\_CSP1\_thm}$
$\vdash \forall\ d, r1, r2, rb : REL\_PREDICATE$

$$
\begin{array}{l}
\quad | \ (r1, rb, r2) \in WF\_Cond_R \\
\quad\quad \land (d, r1 \lhd_R CSP1\ rb \rhd_R r2) \\
\quad\quad\quad \in WF\_DES\_PREDICATE\_PAIR \\
\quad\quad \land \{r1, rb, r2\} \subseteq R1\_healthy \\
\quad \bullet\ d \vdash_D r1 \lhd_R CSP1\ rb \rhd_R r2 \\
\quad\quad = d \vdash_D r1 \lhd_R rb \rhd_R r2
\end{array}
$$

CSP_CSP2_R1_com_thm

$$
\begin{array}{l}
\vdash \forall r : REL\_PREDICATE \\
\quad | \ \{dash\ okay, dash\ tr, dash\ wait, dash\ ref\} \subseteq r.1 \\
\quad \bullet\ CSP2\ (R1\ r) = R1\ (CSP2\ r)
\end{array}
$$

CSP_CSP2_R2_com_thm

$$
\begin{array}{l}
\vdash \forall r : REL\_PREDICATE \\
\quad | \ \{dash\ okay, dash\ tr, dash\ wait, dash\ ref\} \subseteq r.1 \\
\quad\quad \land ALPHABET\_OWTR \subseteq r.1 \\
\quad \bullet\ CSP2\ (R2\ r) = R2\ (CSP2\ r)
\end{array}
$$

CSP_CSP2_R3_com_thm

$$
\begin{array}{l}
\vdash \forall r : REA\_PREDICATE \\
\quad | \ r.1 \in WF\_Skip_{REA} \\
\quad \bullet\ CSP2\ (R3\ r) = R3\ (CSP2\ r)
\end{array}
$$

CSP_CSP2_H1_com_thm

$$
\begin{array}{l}
\vdash \forall r : REL\_PREDICATE \\
\quad | \ \{dash\ okay, dash\ tr, dash\ wait, dash\ ref\} \subseteq r.1 \\
\quad \bullet\ CSP2\ (H1\ r) = H1\ (CSP2\ r)
\end{array}
$$

CSP_CSP2_H2_com_thm

$$
\begin{array}{l}
\vdash \forall r : REL\_PREDICATE \\
\quad | \ \{dash\ okay, dash\ tr, dash\ wait, dash\ ref\} \subseteq r.1 \\
\quad \bullet\ CSP2\ (H2\ r) = H2\ (CSP2\ r)
\end{array}
$$

CSP_CSP2_CSP1_com_thm

$$
\begin{array}{l}
\vdash \forall r : REL\_PREDICATE \\
\quad | \ \{dash\ okay, dash\ tr, dash\ wait, dash\ ref\} \subseteq r.1 \\
\quad \bullet\ CSP2\ (CSP1\ r) = CSP1\ (CSP2\ r)
\end{array}
$$

CSP_CSP2_∧_closure_thm

$$
\begin{array}{l}
\vdash \forall r1, r2 : REL\_PREDICATE \\
\quad | \ \{dash\ okay, dash\ tr, dash\ wait, dash\ ref\} \\
\quad\quad\quad \subseteq r1.1 \cup r2.1 \\
\quad\quad \land \{r1, r2\} \subseteq CSP2\_healthy \\
\quad \bullet\ r1 \land_R r2 \sqsubseteq_R CSP2\ (r1 \land_R r2) = True_R\ \varnothing
\end{array}
$$

CSP_CSP2_∨_closure_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$
$\quad | \ \{dash\ okay,\ dash\ tr,\ dash\ wait,\ dash\ ref\}$
$\qquad \subseteq r1.1 \cup r2.1$
$\quad \wedge \{r1,\ r2\} \subseteq CSP2\_healthy$
$\quad \bullet\ CSP2\ (r1 \vee_R r2) = r1 \vee_R r2$

CSP_closure_$\lhd_R$_$\rhd_R$_CSP2_thm

$\vdash \forall\ r1,\ r2,\ b : REL\_PREDICATE$
$\quad | \ \{dash\ okay,\ dash\ tr,\ dash\ wait,\ dash\ ref\} \subseteq r1.1$
$\quad \wedge (r1,\ b,\ r2) \in WF\_Cond_R$
$\quad \wedge \{r1,\ r2\} \subseteq CSP2\_healthy$
$\quad \bullet\ CSP2\ (r1 \lhd_R b \rhd_R r2) = r1 \lhd_R b \rhd_R r2$

CSP_Π_{REA}_$Semi_R$_left_unit_thm

$\vdash \forall\ a : ALPHABET;\ r : REL\_PREDICATE$
$\quad | \ a \in WF\_Skip_{REA\_def} \wedge (\Pi_{REA}\ a,\ r) \in WF\_Semi_R$
$\quad \bullet\ \Pi_{REA}\ a\ ;_R\ r = r$

CSP_CSP2_dash_okay_thm

$\vdash \forall\ r : REL\_PREDICATE$
$\quad | \ \{dash\ okay,\ dash\ tr,\ dash\ wait,\ dash\ ref\} \subseteq r.1$
$\quad \bullet\ /_R\ (CSP2\ r,\ Val\ (Bool\ true),\ dash\ okay)$
$\quad = /_R\ (r,\ Val\ (Bool\ true),\ dash\ okay)$
$\qquad \vee_R /_R\ (r,\ Val\ (Bool\ false),\ dash\ okay)$

CSP_CSP2_not_dash_okay_thm

$\vdash \forall\ r : REL\_PREDICATE$
$\quad | \ \{dash\ okay,\ dash\ tr,\ dash\ wait,\ dash\ ref\} \subseteq r.1$
$\quad \bullet\ /_R\ (CSP2\ r,\ Val\ (Bool\ false),\ dash\ okay)$
$\quad = /_R\ (r,\ Val\ (Bool\ false),\ dash\ okay)$

CSP_CSP3_healthy_thm

$\vdash \forall\ r : CSP\_PROCESS$
$\quad \bullet\ r \in CSP3\_healthy \Leftrightarrow \Pi_{REA}\ r.1\ ;_R\ r = r$

CSP_SKIP_CSP3_thm

$\vdash \forall\ a : WF\_Skip_{REA} \bullet CSP3\ (SKIP\ a) = SKIP\ a$

CSP_CSP3_idem_thm

$\vdash \forall\ r : CSP\_PROCESS \bullet CSP3\ (CSP3\ r) = CSP3\ r$

CSP_closure_$\vee_R$_CSP3_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$
$\quad | \ \{r1,\ r2\} \subseteq CSP3\_healthy$
$\quad \bullet\ CSP3\ (r1 \vee_R r2) = r1 \vee_R r2$

CSP_closure_$\lhd_R$_$\rhd_R$_CSP3_thm

$\vdash \forall\ r1,\ r2,\ b : REL\_PREDICATE$
$\quad |\ (r1,\ b,\ r2) \in WF\_Cond_R$
$\quad\quad \wedge \{r1,\ r2\} \subseteq CSP3\_healthy$
$\quad\quad \wedge\ ref \notin b.1$
$\quad \bullet\ CSP3\ (r1 \lhd_R b \rhd_R r2) = r1 \lhd_R b \rhd_R r2$

CSP_closure_Semi$_R$_CSP3_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$
$\quad |\ (r1,\ r2) \in WF\_Semi_R \wedge \{r1,\ r2\} \subseteq CSP3\_healthy$
$\quad \bullet\ CSP3\ (r1\ ;_R\ r2) = r1\ ;_R\ r2$

CSP_SKIP_CSP4_thm

$\vdash \forall\ a : WF\_Skip_{REA} \bullet CSP4\ (SKIP\ a) = SKIP\ a$

CSP_STOP_CSP4_thm

$\vdash \forall\ a : WF\_Skip_{REA} \bullet CSP4\ (STOP\ a) = STOP\ a$

CSP_CHAOS_CSP4_thm

$\vdash \forall\ a : WF\_Skip_{REA} \bullet CSP4\ (CHAOS\ a) = CHAOS\ a$

CSP_closure_$\vee_R$_CSP4_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$
$\quad |\ \{r1,\ r2\} \subseteq CSP4\_healthy$
$\quad \bullet\ CSP4\ (r1 \vee_R r2) = r1 \vee_R r2$

CSP_closure_$\lhd_R$_$\rhd_R$_CSP4_thm

$\vdash \forall\ r1,\ r2,\ b : REL\_PREDICATE$
$\quad |\ (r1,\ b,\ r2) \in WF\_Cond_R \wedge \{r1,\ r2\} \subseteq CSP4\_healthy$
$\quad \bullet\ CSP4\ (r1 \lhd_R b \rhd_R r2) = r1 \lhd_R b \rhd_R r2$

CSP_closure_Semi$_R$_CSP4_thm

$\vdash \forall\ r1,\ r2 : REL\_PREDICATE$
$\quad |\ (r1,\ r2) \in WF\_Semi_R \wedge \{r1,\ r2\} \subseteq CSP4\_healthy$
$\quad \bullet\ CSP4\ (r1\ ;_R\ r2) = r1\ ;_R\ r2$

CSP_designs_thm

$\vdash \forall\ p : CSP\_PROCESS$
$\quad \bullet\ p$
$\quad\quad = R$
$\quad\quad\quad (/_R$
$\quad\quad\quad\quad (/_R\ (p,\ Val\ (Bool\ false),\ dash\ okay),$
$\quad\quad\quad\quad\quad Val\ (Bool\ false),$
$\quad\quad\quad\quad\quad wait)$
$\quad\quad\quad\quad \vdash_D /_R$
$\quad\quad\quad\quad\quad (/_R\ (p,\ Val\ (Bool\ true),\ dash\ okay),$
$\quad\quad\quad\quad\quad\quad Val\ (Bool\ false),$

$wait))$

CSP_STOP_dash_okay_true_thm

$$
\begin{array}{l}
\vdash \forall\ a : WF\_Skip_{REA} \\
\quad \bullet\ /_R \\
\qquad (/_R\ (STOP\ a,\ Val\ (Bool\ true),\ dash\ okay), \\
\qquad\ Val\ (Bool\ false), \\
\qquad\ wait) \\
\quad = CSP1 \\
\qquad (=_R\ (a,\ dash\ tr,\ Var\ tr) \\
\qquad\quad \wedge_R =_R (a,\ dash\ wait,\ Val\ (Bool\ true)))
\end{array}
$$

CSP_STOP_not_dash_okay_true_thm

$$
\begin{array}{l}
\vdash /_R \\
\qquad (/_R\ (STOP\ a,\ Val\ (Bool\ false),\ dash\ okay), \\
\qquad\ Val\ (Bool\ false), \\
\qquad\ wait) \\
\quad = CSP1\ (\neg_R\ (=_R\ (a,\ okay,\ Val\ (Bool\ false))))
\end{array}
$$

CSP_STOP_Semi$_{\boldsymbol{R}}$_left_zero_thm

$$
\begin{array}{l}
\vdash \forall\ p : CSP\_PROCESS \\
\quad \mid p.1 = ALPHABET\_OWTR \\
\quad \bullet\ STOP\ p.1\ ;_R\ p = STOP\ p.1
\end{array}
$$

CSP_CHAOS_Semi$_{\boldsymbol{R}}$_left_zero_thm

$$
\begin{array}{l}
\vdash \forall\ p : CSP\_PROCESS \\
\quad \mid p.1 = ALPHABET\_OWTR \\
\quad \bullet\ CHAOS\ p.1\ ;_R\ p = CHAOS\ p.1
\end{array}
$$

CSP_$\boxtimes_{\boldsymbol{CSP}}$_diverge_thm

$$
\begin{array}{l}
\vdash \forall\ p1,\ p2 : CSP\_PROCESS \\
\quad \mid p1.1 = p2.1 \wedge p2.1 = ALPHABET\_OWTR \\
\quad \bullet\ /_R \\
\qquad (/_R \\
\qquad\qquad (p1 \boxtimes_{CSP} p2, \\
\qquad\qquad\ Val\ (Bool\ false), \\
\qquad\qquad\ dash\ okay), \\
\qquad\ Val\ (Bool\ false), \\
\qquad\ wait) \\
\quad = (/_R \\
\qquad\quad (/_R\ (p1,\ Val\ (Bool\ false),\ dash\ okay), \\
\qquad\quad\ Val\ (Bool\ false), \\
\qquad\quad\ wait)
\end{array}
$$

$$
\begin{array}{l}
\quad \lor_R \ /_R \\
\qquad (/_R\ (p2,\ Val\ (Bool\ false),\ dash\ okay), \\
\qquad\quad Val\ (Bool\ false), \\
\qquad\quad wait))\ \lhd_R \\
=_R\ (p1.1,\ okay,\ Val\ (Bool\ true))\ \rhd_R \\
/_R \\
\qquad (/_R\ (p1,\ Val\ (Bool\ false),\ dash\ okay), \\
\qquad\quad Val\ (Bool\ false), \\
\qquad\quad wait) \\
\quad\ \land_R\ /_R \\
\qquad\quad (/_R \\
\qquad\qquad (p2, \\
\qquad\qquad\quad Val\ (Bool\ false), \\
\qquad\qquad\quad dash\ okay), \\
\qquad\quad\ Val\ (Bool\ false), \\
\qquad\quad\ wait)
\end{array}
$$

CSP*_$\boxtimes_{CSP}$_*precondition_thm

$$
\begin{array}{l}
\vdash \forall\ p1,\ p2,\ p3 : CSP\_PROCESS \\
\quad |\ p1.1 = p2.1 \land p2.1 = p3.1 \land p3.1 = ALPHABET\_OWTR \\
\quad \bullet\ \lnot_R \\
\qquad (/_R \\
\qquad\quad (/_R \\
\qquad\qquad (p1\ \boxtimes_{CSP}\ p2, \\
\qquad\qquad\quad Val\ (Bool\ false), \\
\qquad\qquad\quad dash\ okay), \\
\qquad\quad\ Val\ (Bool\ false), \\
\qquad\quad\ wait)) \\
\qquad \vdash_D\ p3 \\
\quad = \lnot_R \\
\qquad (/_R \\
\qquad\quad (/_R \\
\qquad\qquad (p1, \\
\qquad\qquad\quad Val\ (Bool\ false), \\
\qquad\qquad\quad dash\ okay), \\
\qquad\quad\ Val\ (Bool\ false), \\
\qquad\quad\ wait) \\
\qquad\ \lor_R\ /_R \\
\qquad\quad (/_R
\end{array}
$$

$$
\begin{array}{l}
\qquad\qquad\qquad\qquad (p2, \\
\qquad\qquad\qquad\qquad\quad Val\ (Bool\ false), \\
\qquad\qquad\qquad\qquad\quad dash\ okay), \\
\qquad\qquad\qquad\quad Val\ (Bool\ false), \\
\qquad\qquad\qquad\quad wait)) \\
\qquad\qquad \vdash_D\ p3
\end{array}
$$

CSP_$\boxtimes_{CSP}$_converge_thm

$$
\begin{array}{l}
\vdash \forall\ p1,\ p2 : CSP\_PROCESS \\
\quad \mid p1.1 = p2.1 \land p2.1 = ALPHABET\_OWTR \\
\quad \bullet\ /_R \\
\qquad (/_R \\
\qquad\qquad (p1\ \boxtimes_{CSP}\ p2, \\
\qquad\qquad\quad Val\ (Bool\ false), \\
\qquad\qquad\quad dash\ okay), \\
\qquad\quad Val\ (Bool\ true), \\
\qquad\quad wait) \\
\quad\ = ((p1\ \land_R\ p2) \lhd_R \\
\qquad\quad STOP\ p1.1 \rhd_R \\
\qquad\quad /_R \\
\qquad\qquad (/_R \\
\qquad\qquad\qquad (p1\ \lor_R\ p2, \\
\qquad\qquad\qquad\quad Val\ (Bool\ true), \\
\qquad\qquad\qquad\quad dash\ okay), \\
\qquad\qquad\quad Val\ (Bool\ false), \\
\qquad\qquad\quad wait)) \\
\qquad \lor_R\ (p1\ \land_R\ p2) \lhd_R \\
\qquad\qquad STOP\ p1.1 \rhd_R \\
\qquad\qquad /_R \\
\qquad\qquad\quad (/_R \\
\qquad\qquad\qquad\quad (p1\ \lor_R\ p2, \\
\qquad\qquad\qquad\qquad Val\ (Bool\ false), \\
\qquad\qquad\qquad\qquad dash\ okay), \\
\qquad\qquad\qquad Val\ (Bool\ false), \\
\qquad\qquad\qquad wait)
\end{array}
$$

CSP_$\boxtimes_{CSP}$_design_lemma_thm

$$
\begin{array}{l}
\vdash \forall\ p1,\ p2 : CSP\_PROCESS \\
\quad \mid p1.1 = p2.1 \land p2.1 = ALPHABET\_OWTR \\
\quad \bullet\ \neg_R
\end{array}
$$

$$
\begin{aligned}
&\quad (/_R \\
&\qquad (/_R \\
&\qquad\quad (\mathit{p1} \boxtimes_{CSP} \mathit{p2}, \\
&\qquad\qquad \mathit{Val}\ (\mathit{Bool}\ \mathit{false}), \\
&\qquad\qquad \mathit{dash}\ \mathit{okay}), \\
&\qquad\quad \mathit{Val}\ (\mathit{Bool}\ \mathit{false}), \\
&\qquad\quad \mathit{wait})) \\
&\ \vdash_D /_R \\
&\qquad (/_R \\
&\qquad\quad (\mathit{p1} \boxtimes_{CSP} \mathit{p2}, \\
&\qquad\qquad \mathit{Val}\ (\mathit{Bool}\ \mathit{true}), \\
&\qquad\qquad \mathit{dash}\ \mathit{okay}), \\
&\qquad\quad \mathit{Val}\ (\mathit{Bool}\ \mathit{false}), \\
&\qquad\quad \mathit{wait}) \\
&= (\neg_R \\
&\qquad (/_R \\
&\qquad\quad (/_R \\
&\qquad\qquad (\mathit{p1}, \\
&\qquad\qquad\quad \mathit{Val}\ (\mathit{Bool}\ \mathit{false}), \\
&\qquad\qquad\quad \mathit{dash}\ \mathit{okay}), \\
&\qquad\qquad \mathit{Val}\ (\mathit{Bool}\ \mathit{false}), \\
&\qquad\qquad \mathit{wait})) \\
&\quad \wedge_R \neg_R \\
&\qquad (/_R \\
&\qquad\quad (/_R \\
&\qquad\qquad (\mathit{p2}, \\
&\qquad\qquad\quad \mathit{Val}\ (\mathit{Bool}\ \mathit{false}), \\
&\qquad\qquad\quad \mathit{dash}\ \mathit{okay}), \\
&\qquad\qquad \mathit{Val}\ (\mathit{Bool}\ \mathit{false}), \\
&\qquad\qquad \mathit{wait}))) \\
&\ \vdash_D /_R \\
&\qquad (/_R\ (\mathit{p1},\ \mathit{Val}\ (\mathit{Bool}\ \mathit{true}),\ \mathit{dash}\ \mathit{okay}), \\
&\qquad\quad \mathit{Val}\ (\mathit{Bool}\ \mathit{false}), \\
&\qquad\quad \mathit{wait}) \\
&\qquad \wedge_R /_R \\
&\qquad\quad (/_R \\
&\qquad\qquad (\mathit{p2}, \\
&\qquad\qquad\quad \mathit{Val}\ (\mathit{Bool}\ \mathit{true}),
\end{aligned}
$$

$$
\begin{array}{l}
\qquad\qquad\qquad \mathit{dash\ okay}), \\
\qquad\quad \mathit{Val}\ (\mathit{Bool\ false}), \\
\qquad\quad \mathit{wait})\ \lhd_R \\
=_{+R}\ (\mathit{p1.1},\ \mathit{Var}\ (\mathit{dash\ tr}),\ \mathit{Var\ tr}) \\
\qquad \wedge_R =_R \\
\qquad\qquad (\mathit{p1.1}, \\
\qquad\qquad\quad \mathit{dash\ wait}, \\
\qquad\qquad\quad \mathit{Val}\ (\mathit{Bool\ true}))\ \rhd_R \\
/_R \\
\qquad (/_R \\
\qquad\qquad\quad (\mathit{p1}, \\
\qquad\qquad\qquad \mathit{Val}\ (\mathit{Bool\ true}), \\
\qquad\qquad\qquad \mathit{dash\ okay}), \\
\qquad\quad \mathit{Val}\ (\mathit{Bool\ false}), \\
\qquad\quad \mathit{wait}) \\
\qquad \vee_R\ /_R \\
\qquad\qquad (/_R \\
\qquad\qquad\qquad (\mathit{p2}, \\
\qquad\qquad\qquad\quad \mathit{Val}\ (\mathit{Bool\ true}), \\
\qquad\qquad\qquad\quad \mathit{dash\ okay}), \\
\qquad\qquad\quad \mathit{Val}\ (\mathit{Bool\ false}), \\
\qquad\qquad\quad \mathit{wait})
\end{array}
$$

13.5 Definitions

$$
\begin{array}{l}
\boldsymbol{VAR\_NAME} \vdash \mathit{VAR\_NAME} \\
\qquad = \{n : \mathit{NAME} \\
\qquad\quad \mid n \notin \mathit{ALPHABET\_OWTR} \wedge n \in \mathit{undashed}\} \\
\boldsymbol{CSP\_PROCESS} \qquad \vdash \mathit{CSP\_PROCESS} \\
\qquad = \{p : \mathit{REA\_PROCESS} \\
\qquad\quad \mid \mathit{ALPHABET\_OWTR} \subseteq p.1 \\
\qquad\quad\ \wedge p \in \mathit{CSP1\_healthy} \\
\qquad\quad\ \wedge p \in \mathit{CSP2\_healthy}\} \\
\boldsymbol{WF\_CSP\_PROCESS\_PAIR} \\
\quad \vdash \mathit{WF\_CSP\_PROCESS\_PAIR} \\
\qquad = \{\mathit{p1},\ \mathit{p2} : \mathit{CSP\_PROCESS} \\
\qquad\quad \mid \mathit{p1.1} = \mathit{p2.1}\} \\
\boldsymbol{WF\_PREFIXING} \qquad \vdash \mathit{WF\_PREFIXING}
\end{array}
$$

$= \{a : \mathit{ALPHABET\_REA};\ n : \mathit{VAR\_NAME};\ e : \mathit{EXPRESSION}$
$\mid a \in \mathit{WF\_Skip}_{\mathit{REA}} \land FV\ \ e \subseteq a\}$

13.6 Theorems

CSP_CSP1_thm $\vdash \forall\ r : \mathit{REL\_PREDICATE} \bullet \mathit{CSP1}\ \ r \in \mathit{REL\_PREDICATE}$

CSP_CSP1_alphabet_thm
$\vdash \forall\ r : \mathit{REL\_PREDICATE}$
$\bullet (\mathit{CSP1}\ \ r).1 = r.1 \cup \mathit{ALPHABET\_OWTR}$

CSP_CSP1_idem_thm
$\vdash \forall\ r : \mathit{REL\_PREDICATE} \bullet \mathit{CSP1}\ (\mathit{CSP1}\ \ r) = \mathit{CSP1}\ \ r$

CSP_REA_PREDICATE_∈_DES_PREDICATE_thm
$\vdash \forall\ r : \mathit{REA\_PREDICATE} \bullet r \in \mathit{DES\_PREDICATE}$

CSP_CSP2_H2_thm
$\vdash \forall\ r : \mathit{REL\_PREDICATE}$
$\mid \{\mathit{dash\ okay},\ \mathit{dash\ wait},\ \mathit{dash\ tr},\ \mathit{dash\ ref}\} \subseteq r.1$
$\bullet \mathit{CSP2}\ \ r = \mathit{H2}\ \ r$

CSP_CSP2_idem_thm
$\vdash \forall\ r : \mathit{REL\_PREDICATE}$
$\mid \{\mathit{dash\ okay},\ \mathit{dash\ wait},\ \mathit{dash\ tr},\ \mathit{dash\ ref}\} \subseteq r.1$
$\bullet \mathit{CSP2}\ (\mathit{CSP2}\ \ r) = \mathit{CSP2}\ \ r$

CSP_R_design_not_wait_thm
$\vdash \forall\ r : \mathit{REA\_PREDICATE}$
$\mid r.1 \in \mathit{WF\_Skip}_{\mathit{REA}}$
$\bullet R\ \ r\ \ \omega_f = \mathit{R1}\ (\mathit{R2}\ (r\ \ \omega_f))$

CSP_R_design_∈_REA_PREDICATE_thm
$\vdash \forall\ P,\ Q : \mathit{REA\_PREDICATE}$
$\mid (P,\ Q) \in \mathit{WF\_DES\_PREDICATE\_PAIR}$
$\bullet P \vdash_D Q \in \mathit{REA\_PREDICATE}$

CSP_design_wait_false_dist_thm
$\vdash \forall\ P,\ Q : \mathit{REA\_PREDICATE}$
$\mid (P,\ Q) \in \mathit{WF\_DES\_PREDICATE\_PAIR}$
$\land P.1 \in \mathit{WF\_Skip}_{\mathit{REA}}$
$\bullet (P \vdash_D Q)\ \omega_f = (P\ \ \omega_f) \vdash_D Q\ \ \omega_f$

CSP_design_wait_true_dist_thm
$\vdash \forall\ P,\ Q : \mathit{REA\_PREDICATE}$
$\mid (P,\ Q) \in \mathit{WF\_DES\_PREDICATE\_PAIR}$
$\land P.1 \in \mathit{WF\_Skip}_{\mathit{REA}}$

$\bullet\ (P \vdash_D Q)\ \omega_t = (P\ \omega_t) \vdash_D Q\ \omega_t$

CSP_design_wait_false_id_thm

$\vdash \forall\ P,\ Q : \mathit{REA\_PREDICATE}$
$\quad | \ (P,\ Q) \in \mathit{WF\_DES\_PREDICATE\_PAIR}$
$\quad\ \wedge\ P.1 \in \mathit{WF\_Skip}_{\mathit{REA}}$
$\quad\ \wedge\ \mathit{unrestTypedVar}\ (P,\ \mathit{wait},\ \mathit{BOOL\_VAL})$
$\quad\ \wedge\ \mathit{unrestTypedVar}\ (Q,\ \mathit{wait},\ \mathit{BOOL\_VAL})$
$\quad \bullet\ (P \vdash_D Q)\ \omega_f = P \vdash_D Q$

CSP_design_wait_true_id_thm

$\vdash \forall\ P,\ Q : \mathit{REA\_PREDICATE}$
$\quad | \ (P,\ Q) \in \mathit{WF\_DES\_PREDICATE\_PAIR}$
$\quad\ \wedge\ P.1 \in \mathit{WF\_Skip}_{\mathit{REA}}$
$\quad\ \wedge\ \mathit{unrestTypedVar}\ (P,\ \mathit{wait},\ \mathit{BOOL\_VAL})$
$\quad\ \wedge\ \mathit{unrestTypedVar}\ (Q,\ \mathit{wait},\ \mathit{BOOL\_VAL})$
$\quad \bullet\ (P \vdash_D Q)\ \omega_t = P \vdash_D Q$

CSP_CSP1_using_OKAY_thm

$\vdash \forall\ r : \mathit{REL\_PREDICATE}$
$\quad \bullet\ \mathit{CSP1}\ r$
$\quad\ = r$
$\qquad \vee_R \neg_R\ \mathit{OKAY}$
$\qquad\quad \wedge_R =_{+R}$
$\qquad\qquad (\mathit{ALPHABET\_OWTR},$
$\qquad\qquad\ \mathit{Rel}$
$\qquad\qquad\quad ((\_ \leq_R \_),$
$\qquad\qquad\quad\ \mathit{Var}\ \mathit{tr},$
$\qquad\qquad\quad\ \mathit{Var}\ (\mathit{dash}\ \mathit{tr})),$
$\qquad\qquad\ \mathit{Val}\ (\mathit{Bool}\ \mathit{true}))$

CSP_CSP1_using_OKAY_∈_REA_PREDICATE_thm

$\vdash \neg_R\ \mathit{OKAY}$
$\qquad \wedge_R =_{+R}$
$\qquad\quad (\mathit{ALPHABET\_OWTR},$
$\qquad\quad\ \mathit{Rel}\ ((\_ \leq_R \_),\ \mathit{Var}\ \mathit{tr},\ \mathit{Var}\ (\mathit{dash}\ \mathit{tr})),$
$\qquad\quad\ \mathit{Val}\ (\mathit{Bool}\ \mathit{true}))$
$\quad \in \mathit{REA\_PREDICATE}$

CSP_R2_OKAY_$\wedge_R$_r_dist_thm

$\vdash \forall\ r : \mathit{REA\_PREDICATE} \bullet \mathit{R2}\ (\mathit{OKAY} \wedge_R r) = \mathit{OKAY} \wedge_R \mathit{R2}\ r$

CSP_R_design_not_wait_converge_thm

$\vdash \forall\ P,\ Q : \mathit{REA\_PREDICATE}$

$$
\begin{array}{l}
\quad\quad | \ (P,\ Q) \in \mathit{WF\_DES\_PREDICATE\_PAIR} \\
\quad\quad\quad \land\ P.\mathit{1} \in \mathit{WF\_Skip}_{\mathit{REA}} \\
\quad\quad\quad \land\ \mathit{unrestTypedVar}\ (P,\ \mathit{dash\ okay},\ \mathit{BOOL\_VAL}) \\
\quad\quad\quad \land\ \mathit{unrestTypedVar}\ (Q,\ \mathit{dash\ okay},\ \mathit{BOOL\_VAL}) \\
\quad\quad\quad \land\ \mathit{unrestTypedVar}\ (P,\ \mathit{wait},\ \mathit{BOOL\_VAL}) \\
\quad\quad\quad \land\ \mathit{unrestTypedVar}\ (Q,\ \mathit{wait},\ \mathit{BOOL\_VAL}) \\
\quad\quad \bullet\ (R\ (P \vdash_D Q)\ \omega_f)\ \sigma_t \\
\quad\quad\quad = \mathit{CSP1}\ (\mathit{R1}\ (\mathit{R2}\ (P \Rightarrow_R Q)))
\end{array}
$$

$\boldsymbol{CSP\_R\_design\_not\_wait\_diverge\_thm}$

$$
\begin{array}{l}
\vdash \forall\ P,\ Q : \mathit{REA\_PREDICATE} \\
\quad\quad | \ (P,\ Q) \in \mathit{WF\_DES\_PREDICATE\_PAIR} \\
\quad\quad\quad \land\ P.\mathit{1} \in \mathit{WF\_Skip}_{\mathit{REA}} \\
\quad\quad\quad \land\ \mathit{unrestTypedVar}\ (P,\ \mathit{dash\ okay},\ \mathit{BOOL\_VAL}) \\
\quad\quad\quad \land\ \mathit{unrestTypedVar}\ (Q,\ \mathit{dash\ okay},\ \mathit{BOOL\_VAL}) \\
\quad\quad\quad \land\ \mathit{unrestTypedVar}\ (P,\ \mathit{wait},\ \mathit{BOOL\_VAL}) \\
\quad\quad\quad \land\ \mathit{unrestTypedVar}\ (Q,\ \mathit{wait},\ \mathit{BOOL\_VAL}) \\
\quad\quad \bullet\ (R\ (P \vdash_D Q)\ \omega_f)\ \sigma_f \\
\quad\quad\quad = \mathit{R1}\ (\neg_R\ (\mathit{OKAY} \land_R \mathit{R2}\ P))
\end{array}
$$

$\boldsymbol{CSP\_CSP1\_idem\_thm1}$

$$\vdash \forall\ r : \mathit{REL\_PREDICATE} \bullet \mathit{CSP1}\ (\mathit{CSP1}\ r) = \mathit{CSP1}\ r$$

$\boldsymbol{CSP\_CSP1\_R1\_com\_thm}$

$$\vdash \forall\ r : \mathit{REL\_PREDICATE} \bullet \mathit{CSP1}\ (\mathit{R1}\ r) = \mathit{R1}\ (\mathit{CSP1}\ r)$$

$\boldsymbol{CSP\_CSP1\_REA\_PREDICATE\_thm}$

$$\vdash \forall\ r : \mathit{REA\_PREDICATE} \bullet \mathit{CSP1}\ r \in \mathit{REA\_PREDICATE}$$

$\boldsymbol{CSP\_CSP1\_R3\_com\_thm}$

$$
\begin{array}{l}
\vdash \forall\ r : \mathit{REA\_PREDICATE} \\
\quad\quad | \ r.\mathit{1} \in \mathit{WF\_Skip}_{\mathit{REA}} \\
\quad\quad \bullet\ \mathit{CSP1}\ (\mathit{R3}\ r) = \mathit{R3}\ (\mathit{CSP1}\ r)
\end{array}
$$

$\boldsymbol{CSP\_PROCESS\_\in\_REA\_PREDICATE\_thm}$

$$\vdash \forall\ c : \mathit{CSP\_PROCESS} \bullet c \in \mathit{REA\_PREDICATE}$$

$\boldsymbol{CSP\_PROCESS\_thm}$

$$
\begin{array}{l}
\vdash \forall\ c : \mathit{CSP\_PROCESS} \\
\quad\quad \bullet\ c \in \mathit{REA\_PROCESS} \\
\quad\quad\quad \land\ \mathit{ALPHABET\_OWTR} \subseteq c.\mathit{1} \\
\quad\quad\quad \land\ c \in \mathit{CSP1\_healthy} \\
\quad\quad\quad \land\ c \in \mathit{CSP2\_healthy}
\end{array}
$$

$\boldsymbol{CSP\_R\_design\_alphabet\_thm}$

$$\vdash \forall\ P,\ Q : \mathit{REA\_PREDICATE}$$

$| \ (P,\ Q) \in \mathit{WF\_DES\_PREDICATE\_PAIR}$
$\quad \wedge\ P.1 \in \mathit{WF\_Skip}_{REA}$
$\bullet\ (R\ (P \vdash_D Q)).1 = P.1$

$\boldsymbol{CSP\_CSP1\_CSP\_PROCESS\_thm}$
$\vdash \forall\ c : \mathit{CSP\_PROCESS} \bullet \mathit{CSP1}\ c = c$

$\boldsymbol{CSP\_OKAY\_\wedge_R\_CSP1\_abs\_thm}$
$\vdash \forall\ r : \mathit{REL\_PREDICATE}$
$\quad | \ \mathit{ALPHABET\_OWTR} \subseteq r.1$
$\quad \bullet\ \mathit{OKAY} \wedge_R \mathit{CSP1}\ r = \mathit{OKAY} \wedge_R r$

$\boldsymbol{CSP\_CSP1\_okay\_dash\_diverge\_com\_thm}$
$\vdash \forall\ r : \mathit{REA\_PREDICATE} \bullet \mathit{CSP1}\ (r\ \sigma_f) = \mathit{CSP1}\ r\ \sigma_f$

$\boldsymbol{CSP\_CSP1\_okay\_dash\_converge\_com\_thm}$
$\vdash \forall\ r : \mathit{REA\_PREDICATE} \bullet \mathit{CSP1}\ (r\ \sigma_t) = \mathit{CSP1}\ r\ \sigma_t$

$\boldsymbol{CSP\_CSP1\_wait\_false\_com\_thm}$
$\vdash \forall\ r : \mathit{REA\_PREDICATE} \bullet \mathit{CSP1}\ (r\ \omega_f) = \mathit{CSP1}\ r\ \omega_f$

$\boldsymbol{CSP\_CSP1\_wait\_true\_com\_thm}$
$\vdash \forall\ r : \mathit{REA\_PREDICATE} \bullet \mathit{CSP1}\ (r\ \omega_t) = \mathit{CSP1}\ r\ \omega_t$

$\boldsymbol{CSP\_CSP1\_ext\_alphabet\_thm}$
$\vdash \forall\ r : \mathit{REA\_PREDICATE}$
$\quad \bullet\ \mathit{CSP1}\ r$
$\quad = r$
$\qquad \vee_R =_R (r.1,\ \mathit{okay},\ \mathit{Val}\ (\mathit{Bool\ false}))$
$\qquad\quad \wedge_R =_{+R}$
$\qquad\qquad (\mathit{ALPHABET\_OWTR},$
$\qquad\qquad \mathit{Rel}$
$\qquad\qquad\quad ((\_ \leq_R \_),$
$\qquad\qquad\quad \mathit{Var}\ tr,$
$\qquad\qquad\quad \mathit{Var}\ (\mathit{dash}\ tr)),$
$\qquad\qquad \mathit{Val}\ (\mathit{Bool\ true}))$

$\boldsymbol{CSP\_UnrestALPHABET\_CSP\_True_R\_thm}$
$\vdash \forall\ a : \mathit{ALPHABET\_REA}$
$\quad | \ \mathit{ALPHABET\_OWTR} \subseteq a$
$\quad \bullet\ \mathit{unrestALPHABET\_CSP}\ (\mathit{True}_R\ a)$

$\boldsymbol{CSP\_UnrestALPHABET\_CSP\_False_R\_thm}$
$\vdash \forall\ a : \mathit{ALPHABET\_REA}$
$\quad | \ \mathit{ALPHABET\_OWTR} \subseteq a$
$\quad \bullet\ \mathit{unrestALPHABET\_CSP}\ (\mathit{False}_R\ a)$

$\boldsymbol{CSP\_UnrestALPHABET\_CSP\_dash\_True_R\_thm}$

$\vdash \forall\ a : ALPHABET\_REA$
$\mid ALPHABET\_OWTR \subseteq a$
$\bullet\ unrestALPHABET\_CSP'\ (True_R\ a)$

CSP_UnrestALPHABET_CSP_dash_False$_R$_thm

$\vdash \forall\ a : ALPHABET\_REA$
$\mid ALPHABET\_OWTR \subseteq a$
$\bullet\ unrestALPHABET\_CSP'\ (False_R\ a)$

CSP_CSP1_healthy_thm

$\vdash \forall\ c : CSP\_PROCESS \bullet c = CSP1\ c$

CSP_CSP2_healthy_thm

$\vdash \forall\ c : CSP\_PROCESS \bullet c = CSP2\ c$

CSP_CSP1_R1_H1_thm

$\vdash \forall\ c : CSP\_PROCESS \bullet CSP1\ c = R1\ (H1\ c)$

CSP_CSP2_thm $\vdash \forall\ c : CSP\_PROCESS \bullet CSP2\ c \in CSP\_PROCESS$

CSP_REA_PREDICATE_H2_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet H2\ r \in REA\_PREDICATE$

CSP_REA_PREDICATE_H1_thm

$\vdash \forall\ r : REA\_PREDICATE \bullet H1\ r \in REA\_PREDICATE$

CSP_REA_PREDICATE_H2_$\in$_WF_Skip$_{REA}$_thm

$\vdash \forall\ r : REA\_PREDICATE$
$\mid r.1 \in WF\_Skip_{REA}$
$\bullet\ (H2\ r).1 \in WF\_Skip_{REA}$

CSP_REA_PREDICATE_H1_$\in$_WF_Skip$_{REA}$_thm

$\vdash \forall\ r : REA\_PREDICATE$
$\mid r.1 \in WF\_Skip_{REA}$
$\bullet\ (H1\ r).1 \in WF\_Skip_{REA}$

CSP_PROCESS_reactive_design_thm

$\vdash \forall\ c : CSP\_PROCESS$
$\mid c.1 \in homogeneous$
$\bullet\ c = R\ (\neg_R\ ((c\ \omega_f)\ \sigma_f) \vdash_D (c\ \omega_f)\ \sigma_t)$

CSP_CSP1_$\vee_R$_dist_thm

$\vdash \forall\ r1, r2 : REA\_PROCESS$
$\bullet\ CSP1\ (r1 \vee_R r2) = CSP1\ r1 \vee_R CSP1\ r2$

CSP_CSP1_healthy_$\vee_R$_dist_thm

$\vdash \forall\ r1, r2 : REA\_PROCESS$
$\mid r1 \in CSP1\_healthy \wedge r2 \in CSP1\_healthy$
$\bullet\ r1 \vee_R r2 \in CSP1\_healthy$

CSP_CSP2_$\vee_R$_dist_thm1

$\vdash \forall\ r1,\ r2 : REA\_PROCESS$
$\quad | \ r2.1 = r1.1$
$\quad \bullet\ CSP2\ (r1 \lor_R r2) = CSP2\ r1 \lor_R CSP2\ r2$

CSP_CSP2_healthy_$\lor_R$_dist_thm1

$\vdash \forall\ r1,\ r2 : REA\_PROCESS$
$\quad | \ r1 \in CSP2\_healthy$
$\quad\ \ \land r2 \in CSP2\_healthy$
$\quad\ \ \land r1.1 = r2.1$
$\quad \bullet\ r1 \lor_R r2 \in CSP2\_healthy$

CSP_PROCESS_$\lor_R$_thm

$\vdash \forall\ A1,\ A2 : CSP\_PROCESS$
$\quad | \ A1.1 = A2.1$
$\quad \bullet\ A1 \lor_R A2 \in CSP\_PROCESS$

CSP_empty_$\mathbb{F}$_VAR_NAME_thm

$\vdash \{\} \in \mathbb{F}\ VAR\_NAME$

CSP_REA_PREDICATE_Design_thm

$\vdash \forall\ P,\ Q : REA\_PREDICATE$
$\quad | \ (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\quad \bullet\ P \vdash_D Q \in REA\_PREDICATE$

CSP_REA_PREDICATE_R_Design_thm

$\vdash \forall\ P,\ Q : REA\_PREDICATE$
$\quad | \ (P \vdash_D Q).1 \in homogeneous$
$\quad\ \ \land (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\quad \bullet\ R\ (P \vdash_D Q) \in REA\_PREDICATE$

CSP_R_healthy_Design_thm

$\vdash \forall\ P,\ Q : REA\_PREDICATE$
$\quad | \ (P \vdash_D Q).1 \in homogeneous$
$\quad\ \ \land (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\quad \bullet\ R\ (P \vdash_D Q) \in R\_healthy$

CSP_REA_PROCESS_Design_thm

$\vdash \forall\ P,\ Q : REA\_PREDICATE$
$\quad | \ (P \vdash_D Q).1 \in homogeneous$
$\quad\ \ \land (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\quad \bullet\ R\ (P \vdash_D Q) \in REA\_PROCESS$

CSP_REL_PREDICATE_Design_thm

$\vdash \forall\ P,\ Q : REA\_PREDICATE$
$\quad | \ (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\quad \bullet\ P \vdash_D Q \in REL\_PREDICATE$

$\boldsymbol{CSP\_reactive\_design\_\vee_R\_thm}$

$\vdash \forall\ p1,\ q1,\ p2,\ q2 : REA\_PREDICATE$
$\quad \mid (p1,\ q1) \in WF\_DES\_PREDICATE\_PAIR$
$\quad\quad \wedge (p2,\ q2) \in WF\_DES\_PREDICATE\_PAIR$
$\quad\quad \wedge p2.1 = p1.1$
$\quad\quad \wedge q2.1 = q1.1$
$\quad\quad \wedge p1.1 \in WF\_Skip_{REA}$
$\quad \bullet R\ (p1 \vdash_D q1) \vee_R R\ (p2 \vdash_D q2)$
$\quad\quad = R\ ((p1 \wedge_R p2) \vdash_D q1 \vee_R q2)$

$\boldsymbol{CSP\_CSP1\_R1\_H1\_thm2}$

$\vdash \forall\ r : REA\_PREDICATE \bullet R1\ (H1\ r) = R1\ (CSP1\ r)$

$\boldsymbol{CSP\_R2\_CSP1\_def\_id\_thm}$

$\vdash R1$
$\quad (\neg_R\ OKAY$
$\quad\quad \wedge_R =_{+R}$
$\quad\quad\quad (ALPHABET\_OWTR,$
$\quad\quad\quad\quad Rel$
$\quad\quad\quad\quad\quad ((\_ \leq_R \_),$
$\quad\quad\quad\quad\quad\quad Var\ tr,$
$\quad\quad\quad\quad\quad\quad Var\ (dash\ tr)),$
$\quad\quad\quad\quad Val\ (Bool\ true)))$
$\quad = R1$
$\quad\quad (R2$
$\quad\quad\quad (\neg_R\ OKAY$
$\quad\quad\quad\quad \wedge_R =_{+R}$
$\quad\quad\quad\quad\quad (ALPHABET\_OWTR,$
$\quad\quad\quad\quad\quad\quad Rel$
$\quad\quad\quad\quad\quad\quad\quad ((\_ \leq_R \_),$
$\quad\quad\quad\quad\quad\quad\quad\quad Var\ tr,$
$\quad\quad\quad\quad\quad\quad\quad\quad Var\ (dash\ tr)),$
$\quad\quad\quad\quad\quad\quad Val\ (Bool\ true))))$

$\boldsymbol{CSP\_CSP1\_R2\_com\_thm}$

$\vdash \forall\ r : REA\_PREDICATE$
$\quad \bullet R1\ (R2\ (CSP1\ r)) = R1\ (CSP1\ (R2\ r))$

$\boldsymbol{CSP\_CSP1\_R1\_H1\_thm1}$

$\vdash \forall\ r : REA\_PREDICATE$
$\quad \mid r \in R1\_healthy$
$\quad \bullet R1\ (H1\ r) = CSP1\ r$

CSP_CSP*1*_healthy_Design_thm

$\vdash \forall\ P,\ Q : REA\_PREDICATE$
$\quad \mid (P \vdash_D Q).1 \in homogeneous$
$\quad\quad \land (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\quad \bullet\ R\ (P \vdash_D Q) \in CSP1\_healthy$

CSP_CSP_PROCESS_Design_thm

$\vdash \forall\ P,\ Q : REA\_PREDICATE$
$\quad \mid (P \vdash_D Q).1 \in homogeneous$
$\quad\quad \land (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\quad \bullet\ R\ (P \vdash_D Q) \in CSP\_PROCESS$

CSP_CSP_PROCESS_∈_homogeneous_thm

$\vdash \forall\ A : CSP\_PROCESS \bullet A.1 \in homogeneous$

CSP_closure_Semi$_R$_CSP*1*_thm

$\vdash \forall\ r1,\ r2 : REA\_PREDICATE$
$\quad \mid r2.1 = r1.1$
$\quad\quad \land (r1,\ r2) \in WF\_Semi_R$
$\quad\quad \land \{r1,\ r2\} \subseteq CSP1\_healthy$
$\quad \bullet\ CSP1\ (r1\ ;_R\ r2) = r1\ ;_R\ r2$

CSP_closure_Semi$_R$_CSP*2*_thm

$\vdash \forall\ r1,\ r2 : REA\_PREDICATE$
$\quad \mid \{dash\ okay,\ dash\ tr,\ dash\ wait,\ dash\ ref\}$
$\quad\quad\quad \subseteq out\_a\ r2.1$
$\quad\quad \land (r1,\ r2) \in WF\_Semi_R$
$\quad\quad \land \{r1,\ r2\} \subseteq CSP2\_healthy$
$\quad \bullet\ CSP2\ (r1\ ;_R\ r2) = r1\ ;_R\ r2$

CSP_REA_PREDICATE_do_C_thm

$\vdash \forall\ n : VAR\_NAME;\ e : EXPRESSION;\ a : WF\_Skip_{REA}$
$\quad \mid (a,\ n,\ e) \in WF\_PREFIXING$
$\quad \bullet\ do\_C\ (a,\ n,\ e) \in REA\_PREDICATE$

CSP_REA_PREDICATE_do_C_alphabet_thm

$\vdash \forall\ n : VAR\_NAME;\ e : EXPRESSION;\ a : WF\_Skip_{REA}$
$\quad \mid (a,\ n,\ e) \in WF\_PREFIXING$
$\quad \bullet\ (do\_C\ (a,\ n,\ e)).1 = a$

CSP_PROCESS_Semi$_R$_thm

$\vdash \forall\ A1,\ A2 : CSP\_PROCESS$
$\quad \mid (A1,\ A2) \in WF\_Semi_R \land A1.1 = A2.1$
$\quad \bullet\ A1\ ;_R\ A2 \in CSP\_PROCESS$

CSP_R_design_R*1*_thm

$\vdash \forall\ P,\ Q : REA\_PREDICATE$
$\quad | \ Q \in R1\_healthy$
$\quad \bullet\ R\ (P \vdash_D R1\ Q) = R\ (P \vdash_D Q)$

$\boldsymbol{CSP\_design\_wait\_false\_id\_thm1}$
$\vdash \forall\ P,\ Q : REA\_PREDICATE$
$\quad | \ (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\quad\quad \wedge\ P.1 \in WF\_Skip_{REA}$
$\quad \bullet\ (P \vdash_D Q)\ \omega_f = (P\ \omega_f) \vdash_D Q\ \omega_f$

$\boldsymbol{CSP\_design\_okay\_dash\_converge\_id\_thm}$
$\vdash \forall\ P,\ Q : REA\_PREDICATE$
$\quad | \ (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\quad\quad \wedge\ P.1 \in WF\_Skip_{REA}$
$\quad \bullet\ (P \vdash_D Q)\ \sigma_t = (OKAY \wedge_R P\ \sigma_t) \Rightarrow_R Q\ \sigma_t$

$\boldsymbol{CSP\_okay\_dash\_diverge\_thm}$
$\vdash \forall\ u : REA\_PROCESS \bullet R1\ u\ \sigma_f = R1\ (u\ \sigma_f)$

$\boldsymbol{CSP\_R\_okay\_dash\_diverge\_thm}$
$\vdash \forall\ u : REA\_PROCESS \bullet R\ u\ \sigma_f = R1\ (R2\ u)\ \sigma_f$

$\boldsymbol{CSP\_R\_wait\_false\_thm}$
$\vdash \forall\ u : REA\_PROCESS \bullet R\ u\ \omega_f = R1\ (R2\ u)\ \omega_f$

$\boldsymbol{CSP\_R\_design\_not\_wait\_converge\_thm1}$
$\vdash \forall\ P,\ Q : REA\_PREDICATE$
$\quad | \ (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\quad\quad \wedge\ P.1 \in WF\_Skip_{REA}$
$\quad \bullet\ (R\ (P \vdash_D Q)\ \omega_f)\ \sigma_t$
$\quad\quad = CSP1$
$\quad\quad\quad (R1\ (R2\ (((P\ \omega_f)\ \sigma_t) \Rightarrow_R (Q\ \omega_f)\ \sigma_t)))$

$\boldsymbol{CSP\_R\_design\_not\_wait\_diverge\_thm1}$
$\vdash \forall\ P,\ Q : REA\_PREDICATE$
$\quad | \ (P,\ Q) \in WF\_DES\_PREDICATE\_PAIR$
$\quad\quad \wedge\ P.1 \in WF\_Skip_{REA}$
$\quad \bullet\ (R\ (P \vdash_D Q)\ \omega_f)\ \sigma_f$
$\quad\quad = R1\ (\neg_R\ (OKAY \wedge_R R2\ ((P\ \omega_f)\ \sigma_f)))$

$\boldsymbol{CSP\_R2\_Condition\_thm}$
$\vdash \forall\ g : REA\_PREDICATE$
$\quad | \ unrestALPHABET\_CSP\ g \wedge unrestALPHABET\_CSP'\ g$
$\quad \bullet\ R2\ g = g$

$\boldsymbol{CSP\_R1\_\neg_R\_OKAY\_is\_CSP1\_thm}$
$\vdash R1\ (\neg_R\ OKAY)$

$$
\begin{aligned}
&= =_R\ (\mathit{ALPHABET\_OWTR},\ \mathit{okay},\ \mathit{Val}\ (\mathit{Bool}\ \mathit{false}))\\
&\quad \wedge_R =_{+R}\\
&\qquad (\mathit{ALPHABET\_OWTR},\\
&\qquad\ \ \mathit{Rel}\ ((\_ \leq_R \_),\ \mathit{Var}\ \mathit{tr},\ \mathit{Var}\ (\mathit{dash}\ \mathit{tr})),\\
&\qquad\ \ \mathit{Val}\ (\mathit{Bool}\ \mathit{true}))
\end{aligned}
$$

CSP_not_wait_false_not_okay_dash_$\Rightarrow_R$_okay_dash_thm

$$
\begin{aligned}
&\vdash \forall\ A : \mathit{CSP\_PROCESS}\\
&\quad \bullet\ ((A\ \omega_f)\ \sigma_f) \Rightarrow_R (A\ \omega_f)\ \sigma_t = \mathit{True}_R\ \mathit{A.1}
\end{aligned}
$$

14 THE Z THEORY utp-circus

14.1 Parents

$utp\!-\!csp$

14.2 Global Variables

$\boldsymbol{Z\_VAR\_NAME}$ $\mathbb{P}\ NAME$
$\boldsymbol{VAR\_DECLS}$ $(\mathbb{Z} \leftrightarrow NAME) \leftrightarrow \mathbb{Z} \leftrightarrow EXPRESSION$
$\boldsymbol{CIRCUS\_PREDICATE}$
$\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{CIRCUS\_CONDITION}$
$\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{WF\_Skip_C}$ $\mathbb{P}\ (\mathbb{P}\ NAME)$
$\boldsymbol{WF\_Guard_C}$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{WF\_if_{C\_fiC}}$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{WF\_Semi_C}$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{WF\_Var_C}$ $\mathbb{P}\ (NAME \times VALUE \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)))$
$\boldsymbol{WF\_Assign_C}$ $\mathbb{P}\ (\mathbb{P}\ NAME \times (\mathbb{Z} \leftrightarrow NAME) \times (\mathbb{Z} \leftrightarrow EXPRESSION))$
$\boldsymbol{WF\_SpecStatement_C}$
$\mathbb{P}$
$(\mathbb{P}$
$NAME$
$\times\ \mathbb{P}$
$NAME$
$\times\ (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\times\ (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)))$
$\boldsymbol{WF\_Condition_C}$
$\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{WF\_SchemaExp_C}$
$(\mathbb{Z} \leftrightarrow NAME) \times (\mathbb{Z} \leftrightarrow EXPRESSION)$
$\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$
$\boldsymbol{WF\_param_C}$ $\mathbb{P}$
$(NAME$
$\times\ EXPRESSION$
$\times\ (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\times\ EXPRESSION)$

$\boldsymbol{WF\_val_C}$ $\quad \mathbb{P}$
$(NAME$
$\quad \times\ VALUE$
$\quad \times\ (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times\ EXPRESSION)$

$\boldsymbol{WF\_res_C}$ $\quad \mathbb{P}\ (NAME \times VALUE \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times NAME)$

$\boldsymbol{WF\_vres_C}$ $\quad \mathbb{P}\ (NAME \times VALUE \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times NAME)$

$\boldsymbol{WF\_PREFIXING_C}$
$\quad \mathbb{P}\ NAME \times NAME \times EXPRESSION \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALU$

$\boldsymbol{WF\_PREFIXING_{CinR}}$
$\quad \mathbb{P}$
$(\mathbb{P}$
$\quad NAME$
$\quad \times\ NAME$
$\quad \times\ NAME$
$\quad \times\ (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times\ (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)))$

$\boldsymbol{Stop}$ $\quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{Skip}$ $\quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{Chaos}$ $\quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_ \ ;_{\boldsymbol{C}}\ \_)$ $\quad (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times\ (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_ \ \&_{\boldsymbol{C}}\ \_)$ $\quad (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times\ (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_ \ \boxtimes_{\boldsymbol{C}}\ \_)$ $\quad (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times\ (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_ \ \sqcap_{\boldsymbol{C}}\ \_)$ $\quad (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times\ (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_ \ \rightarrow_{\boldsymbol{C}}\ \_)$ $\quad (\mathbb{P}\ NAME \times NAME \times EXPRESSION)$
$\quad \times\ (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_ \ \rightarrow_{\boldsymbol{CSync}}\ \_)$
$\quad (\mathbb{P}\ NAME \times NAME) \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_ \rightarrow_{\boldsymbol{Cout}} \_)$ $\quad (\mathbb{P}\ NAME \times NAME \times EXPRESSION)$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{var_C}$ $\quad NAME \times VALUE \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{NonRef}$ $\quad NAME \times NAME \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \leftrightarrow VALUE$

$\boldsymbol{Traces}$ $\quad NAME \times NAME \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \leftrightarrow VALUE$

$\boldsymbol{do\_I}$ $\quad \mathbb{P}\ NAME \times NAME \times NAME \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_ \rightarrow_{\boldsymbol{CinR}} \_)$ $\quad (\mathbb{P}\ NAME \times NAME \times NAME \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)))$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_ \rightarrow_{\boldsymbol{Cin}} \_)$ $\quad (\mathbb{P}\ NAME \times NAME \times NAME) \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{MTrInter}$ $\quad VALUE \times VALUE \leftrightarrow VALUE$

$\boldsymbol{MTrPar}$ $\quad VALUE \times VALUE \leftrightarrow VALUE$

$\boldsymbol{MTrParPred}$ $\quad VALUE \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{MSync}$ $\quad VALUE \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{BranchesWaiting}$
$\quad \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{BranchesNotWaiting}$
$\quad \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{MRefPar}$ $\quad VALUE \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{MSt}$ $\quad \mathbb{P}\ NAME \times \mathbb{P}\ NAME \times \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{MWtRefStPar}$ $\quad VALUE \times \mathbb{P}\ NAME \times \mathbb{P}\ NAME \times \mathbb{P}\ NAME$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{MPar}$ $\quad VALUE \times \mathbb{P}\ NAME \times \mathbb{P}\ NAME \times \mathbb{P}\ NAME$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{DivPar}$ $\quad (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times VALUE$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_ \llbracket_C \_ \rrbracket_C \_)$
$\quad (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times (\mathbb{P}\ NAME \times VALUE \times \mathbb{P}\ NAME)$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{MTrInterPred}$ $\quad \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{MRefInter} \quad \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{MWtRefStInter}$

$\quad \mathbb{P}\ NAME \times \mathbb{P}\ NAME \times \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{MInter} \quad \mathbb{P}\ NAME \times \mathbb{P}\ NAME \times \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{DivInter} \quad (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_ \ [\![_C \ \_ \ ]\!]_C \ \_)$

$\quad (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ NAME)$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\_ \setminus_C \_) \quad (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times VALUE$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{CIRCUS\_FUNCTION}$

$\quad \mathbb{P}$
$\quad (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE$

$\boldsymbol{\mu_C} \quad (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{Assign_C} \quad \mathbb{P}\ NAME \times (\mathbb{Z} \leftrightarrow NAME) \times (\mathbb{Z} \leftrightarrow EXPRESSION)$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{SpecStatement_C}$

$\quad \mathbb{P}$
$\quad NAME$
$\quad \times\ \mathbb{P}$
$\quad NAME$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\{_C \ \_ \ \}_C) \quad \mathbb{P}\ NAME \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$(\langle_C \ \_ \ \rangle_C) \quad \mathbb{P}\ NAME \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{Typing} \quad ((\mathbb{Z} \leftrightarrow NAME) \times (\mathbb{Z} \leftrightarrow EXPRESSION)) \times \mathbb{P}\ NAME$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{SchemaExp_C} \quad ((\mathbb{Z} \leftrightarrow NAME) \times (\mathbb{Z} \leftrightarrow EXPRESSION))$
$\quad \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE))$
$\quad \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{GUARDED\_ACTIONS}$

$$(\mathbb{Z} \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \leftrightarrow \mathbb{Z} \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$$

$\boldsymbol{TrueGuards}$ $(\mathbb{Z} \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times (\mathbb{Z} \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{NonDivActions}$

$$(\mathbb{Z} \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times (\mathbb{Z} \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$$

$\boldsymbol{ExecActions}$ $(\mathbb{Z} \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times (\mathbb{Z} \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{(if_C\ \_\ fi_C)}$

$$(\mathbb{Z} \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times (\mathbb{Z} \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$$

$\boldsymbol{(ifb_C\ \_\ \mapsto_C\ \_\ else_C\ \_\ \mapsto_C\ \_\ fib_C)}$

$$(\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$$

$\boldsymbol{param_C}$ $NAME \times EXPRESSION \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times EXPRESSION \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{val_C}$ $NAME \times VALUE \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times EXPRESSIO$ $\leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{res_C}$ $NAME \times VALUE \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{vres_C}$ $NAME \times VALUE \times (\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)) \times NAME \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{C1}$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{C1\_healthy}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{C2}$ $\mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\boldsymbol{C2\_healthy}$ $\mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\textbf{C3}$ $\quad \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE) \leftrightarrow \mathbb{P}\ NAME \times \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\textbf{C3\_healthy}$ $\quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

$\textbf{CIRCUS\_ACTION}$

$\quad \mathbb{P}\ NAME \leftrightarrow \mathbb{P}\ (NAME \leftrightarrow VALUE)$

14.3 Fixity

fun* 0 *rightassoc

$(ifb_C\ \_\ \mapsto_C\ \_\ else_C\ \_\ \mapsto_C\ \_\ fib_C)$
$(if_C\ \_\ fi_C)$
$(\_\ \&_C\ \_)$
$(\_\ ;_C\ \_)$
$(\_\ \setminus_C\ \_)$
$(\_\ \sqcap_C\ \_)$
$(\_\ \boxtimes_C\ \_)$
$(\_\ \rightarrow_{CinR}\ \_)$
$(\_\ \rightarrow_{Cin}\ \_)$
$(\_\ \rightarrow_{Cout}\ \_)$
$(\_\ \rightarrow_{CSync}\ \_)$
$(\_\ \rightarrow_C\ \_)$
$(\_\ [\![_C\ \_\ ]\!]_C\ \_)$
$(\_\ [\![[_C\ \_\ ]\!]]_C\ \_)$
$(\{_C\ \_\ \}_C)$
$(\langle_C\ \_\ \rangle_C)$

14.4 Axioms

$\textbf{CIRCUS\_PREDICATE}$

$$\vdash CIRCUS\_PREDICATE \in \mathbb{P}\ REA\_PREDICATE \\ \land CIRCUS\_PREDICATE \\ = \{c : REA\_PREDICATE \\ \mid unrestALPHABET\_CSP\ c \land unrestALPHABET\_CSP'\ c\}$$

$\textbf{CIRCUS\_CONDITION}$

$$\vdash CIRCUS\_CONDITION \in \mathbb{P}\ REA\_PREDICATE \\ \land CIRCUS\_CONDITION \\ = \{c : REA\_PREDICATE \\ \mid unrestALPHABET\_CSP\ c \\ \land unrestALPHABET\_CSP'\ c$$

$$\land\ c -_R ALPHABET\_OWTR \in REL\_CONDITION\}$$

Stop

$$
\begin{array}{l}
\vdash Stop \in WF\_Skip_C \rightarrow CSP\_PROCESS \\
\quad \land (\forall\ a : WF\_Skip_C \\
\quad\quad \bullet\ Stop\ a \\
\quad\quad\quad = R \\
\quad\quad\quad\quad (True_R\ a \\
\quad\quad\quad\quad\quad \vdash_D =_R (a,\ dash\ tr,\ Var\ tr) \\
\quad\quad\quad\quad\quad\quad \land_R =_R \\
\quad\quad\quad\quad\quad\quad\quad (a, \\
\quad\quad\quad\quad\quad\quad\quad\quad dash\ wait, \\
\quad\quad\quad\quad\quad\quad\quad\quad Val\ (Bool\ true))))
\end{array}
$$

Skip

$$
\begin{array}{l}
\vdash Skip \in WF\_Skip_C \rightarrow CSP\_PROCESS \\
\quad \land (\forall\ a : WF\_Skip_C \\
\quad\quad \bullet\ Skip\ a \\
\quad\quad\quad = R \\
\quad\quad\quad\quad (True_R\ a \\
\quad\quad\quad\quad\quad \vdash_D =_R (a,\ dash\ tr,\ Var\ tr) \\
\quad\quad\quad\quad\quad\quad \land_R =_R \\
\quad\quad\quad\quad\quad\quad\quad (a, \\
\quad\quad\quad\quad\quad\quad\quad\quad dash\ wait, \\
\quad\quad\quad\quad\quad\quad\quad\quad Val\ (Bool\ false)) \\
\quad\quad\quad\quad\quad\quad\quad \land_R\ \Pi_R\ (a \setminus ALPHABET\_OWTR)))
\end{array}
$$

Chaos

$$
\begin{array}{l}
\vdash Chaos \in WF\_Skip_C \rightarrow CSP\_PROCESS \\
\quad \land (\forall\ a : WF\_Skip_C \\
\quad\quad \bullet\ Chaos\ a = R\ (False_R\ a \vdash_D True_R\ a))
\end{array}
$$

_ ;$_C$ _

$$
\begin{array}{l}
\vdash (\_\ ;_C\ \_) \in WF\_Semi_C \rightarrow CSP\_PROCESS \\
\quad \land (\forall\ u1\_u2 : WF\_Semi_C \\
\quad\quad \bullet\ u1\_u2.1\ ;_C\ u1\_u2.2 = u1\_u2.1\ ;_R\ u1\_u2.2)
\end{array}
$$

_ &$_C$ _

$$
\begin{array}{l}
\vdash (\_\ \&_C\ \_) \in WF\_Guard_C \rightarrow CSP\_PROCESS \\
\quad \land (\forall\ g : CIRCUS\_CONDITION;\ a : CSP\_PROCESS \\
\quad\quad \mid (g,\ a) \in WF\_Guard_C \\
\quad\quad \bullet\ g\ \&_C\ a \\
\quad\quad\quad = R \\
\quad\quad\quad\quad ((g \Rightarrow_R \neg_R\ ((a\ \omega_f)\ \sigma_f)) \\
\quad\quad\quad\quad\quad \vdash_D (g \land_R (a\ \omega_f)\ \sigma_t) \\
\quad\quad\quad\quad\quad\quad \lor_R \neg_R\ g \\
\quad\quad\quad\quad\quad\quad\quad \land_R =_R (a.1,\ dash\ tr,\ Var\ tr) \\
\quad\quad\quad\quad\quad\quad\quad\quad \land_R =_R
\end{array}
$$

$$
\begin{array}{l}
\qquad\qquad\qquad\qquad\qquad (a.1, \\
\qquad\qquad\qquad\qquad\qquad\quad dash\ wait, \\
\qquad\qquad\qquad\qquad\qquad\quad Val\ (Bool\ true))))
\end{array}
$$

$$
\begin{array}{ll}
\_\ \boxtimes_{\boldsymbol{C}}\ \_ & \vdash (\_\ \boxtimes_C\ \_) \in WF\_CSP\_PROCESS\_PAIR \rightarrow CSP\_PROCESS \\
& \quad \wedge (\forall\ aa : WF\_CSP\_PROCESS\_PAIR \\
& \qquad \bullet\ aa.1\ \boxtimes_C\ aa.2 \\
& \qquad\quad = R \\
& \qquad\qquad ((\neg_R\ ((aa.1\ \omega_f)\ \sigma_f) \\
& \qquad\qquad\qquad \wedge_R\ \neg_R\ ((aa.2\ \omega_f)\ \sigma_f)) \\
& \qquad\qquad\quad \vdash_D\ (((aa.1\ \omega_f)\ \sigma_t) \\
& \qquad\qquad\qquad\quad \wedge_R\ (aa.2\ \omega_f)\ \sigma_t)\ \lhd_R \\
& \qquad\qquad\qquad =_{+R} \\
& \qquad\qquad\qquad\qquad (aa.1.1, \\
& \qquad\qquad\qquad\qquad\quad Var\ (dash\ tr), \\
& \qquad\qquad\qquad\qquad\quad Var\ tr) \\
& \qquad\qquad\qquad\quad \wedge_R =_R \\
& \qquad\qquad\qquad\qquad\quad (aa.1.1, \\
& \qquad\qquad\qquad\qquad\qquad dash\ wait, \\
& \qquad\qquad\qquad\qquad\qquad Val\ (Bool\ true))\ \rhd_R \\
& \qquad\qquad\qquad ((aa.1\ \omega_f)\ \sigma_t) \\
& \qquad\qquad\qquad\quad \vee_R\ (aa.2\ \omega_f)\ \sigma_t)) \\
\_\ \cap_{\boldsymbol{C}}\ \_ & \vdash (\_\ \cap_C\ \_) \in WF\_CSP\_PROCESS\_PAIR \rightarrow CSP\_PROCESS \\
& \quad \wedge (\forall\ aa : WF\_CSP\_PROCESS\_PAIR \\
& \qquad \bullet\ aa.1\ \cap_C\ aa.2 = aa.1\ \vee_R\ aa.2) \\
\_\ \boldsymbol{\rightarrow_C}\ \_ & \vdash (\_\ \rightarrow_C\ \_) \in WF\_PREFIXING_C \rightarrow CSP\_PROCESS \\
& \quad \wedge (\forall\ a\_a : WF\_PREFIXING_C \\
& \qquad \bullet\ a\_a.1\ \rightarrow_C\ a\_a.2 \\
& \qquad\quad = R \\
& \qquad\qquad\quad (True_R\ a\_a.1.1 \\
& \qquad\qquad\qquad \vdash_D\ (do\_C\ a\_a.1) \\
& \qquad\qquad\qquad\quad \wedge_R\ \Pi_R \\
& \qquad\qquad\qquad\qquad (a\_a.1.1 \setminus ALPHABET\_OWTR)) \\
& \qquad\qquad ;_C\ a\_a.2) \\
\_\ \boldsymbol{\rightarrow_{CSync}}\ \_ & \vdash (\_\ \rightarrow_{CSync}\ \_) \\
& \qquad \in (ALPHABET \times VAR\_NAME) \times CSP\_PROCESS \\
& \qquad\quad \rightarrow CSP\_PROCESS \\
& \quad \wedge (\forall\ a : ALPHABET;\ c : VAR\_NAME;\ A : CSP\_PROCESS \\
& \qquad \bullet\ (a,\ c) \rightarrow_{CSync} A = (a,\ c,\ Val\ Sync) \rightarrow_C A)
\end{array}
$$

$\_ \to_{Cout} \_$ $\quad \vdash (\_ \to_{Cout} \_) \in WF\_PREFIXING_C \to CSP\_PROCESS$
$\quad \land (\forall\ a\_a : WF\_PREFIXING_C$
$\quad \bullet\ a\_a.1 \to_{Cout} a\_a.2 = a\_a.1 \to_C a\_a.2)$

$\boldsymbol{var_C}$ $\quad \vdash var_C \in WF\_Var_C \to CSP\_PROCESS$
$\quad \land (\forall\ n : VAR\_NAME;\ t : SET\_VAL;\ a : CSP\_PROCESS$
$\quad \mid (n, t, a) \in WF\_Var_C$
$\quad \bullet\ var_C\ (n, t, a)$
$\quad = varT_R\ (a.1, n, t)$
$\quad ;_R\ a\ ;_R\ endT_R\ (a.1, n, t))$

NonRef $\quad \vdash NonRef$
$\quad \in VAR\_NAME \times VAR\_NAME \times CIRCUS\_CONDITION$
$\quad \to SET\_EVENT\_VAL$
$\quad \land (\forall\ c : VAR\_NAME;$
$\quad x : VAR\_NAME;$
$\quad p : CIRCUS\_CONDITION$
$\quad \bullet\ NonRef\ (c, x, p)$
$\quad = Set$
$\quad \{v : VALUE$
$\quad \mid /_R\ (p, Val\ v, x) = True_R\ p.1$
$\quad \bullet\ Pair\ (Channel\ c, v)\})$

Traces $\quad \vdash Traces$
$\quad \in VAR\_NAME \times VAR\_NAME \times CIRCUS\_CONDITION$
$\quad \to SET\_SEQ\_EVENT\_VAL$
$\quad \land (\forall\ c : VAR\_NAME;$
$\quad x : VAR\_NAME;$
$\quad p : CIRCUS\_CONDITION$
$\quad \bullet\ Traces\ (c, x, p)$
$\quad = Set$
$\quad \{v : VALUE$
$\quad \mid /_R\ (p, Val\ v, x) = True_R\ p.1$
$\quad \bullet\ Seq\ \langle Pair\ (Channel\ c, v)\rangle\})$

do_I $\quad \vdash do\_I$
$\quad \in ALPHABET\_REA$
$\quad \times VAR\_NAME$
$\quad \times VAR\_NAME$
$\quad \times CIRCUS\_CONDITION$
$\quad \to CSP\_PROCESS$
$\quad \land (\forall\ a : ALPHABET\_REA;$

$$
\begin{array}{l}
\quad c : VAR\_NAME; \\
\quad x : VAR\_NAME; \\
\quad p : CIRCUS\_CONDITION \\
\bullet\ do\_I\ (a, c, x, p) \\
\quad = (=_R (a, dash\ tr, Var\ tr) \\
\qquad \wedge_R =_{+R} \\
\qquad\quad (a, \\
\qquad\quad Fun_2 \\
\qquad\qquad ((\_ \cap_R \_), \\
\qquad\qquad Val\ (NonRef\ (c, x, p)), \\
\qquad\qquad Var\ (dash\ ref)), \\
\qquad\quad Val\ (Set\ \varnothing))) \lhd_R \\
\qquad =_R (a, dash\ wait, Val\ (Bool\ true)) \rhd_R \\
\qquad =_{+R} \\
\qquad\quad (a, \\
\qquad\quad Rel \\
\qquad\qquad ((\_ \in_R \_), \\
\qquad\qquad Fun_2 \\
\qquad\qquad\quad ((\_\ SeqDif_R\ \_), \\
\qquad\qquad\quad Var\ (dash\ tr), \\
\qquad\qquad\quad Var\ tr), \\
\qquad\qquad Val\ (Traces\ (c, x, p))), \\
\qquad\quad Val\ (Bool\ true))) \\
\_ \boldsymbol{\rightarrow_{CinR}} \_ \quad \vdash (\_ \rightarrow_{CinR} \_) \\
\quad \in (ALPHABET\_REA \\
\qquad \times VAR\_NAME \\
\qquad \times VAR\_NAME \\
\qquad \times CIRCUS\_CONDITION) \\
\qquad \times CSP\_PROCESS \\
\qquad \rightarrow CSP\_PROCESS \\
\wedge (\forall\ a : ALPHABET\_REA; \\
\quad c : VAR\_NAME; \\
\quad x : VAR\_NAME; \\
\quad p : CIRCUS\_CONDITION; \\
\quad A : CSP\_PROCESS \\
\bullet\ (a, c, x, p) \rightarrow_{CinR} A \\
\quad = var_C \\
\qquad (x,
\end{array}
$$

$Set\ \{v : VALUE\},$
R
$(True_R\ A.1$
$\vdash_D\ do\_I\ (a,\ c,\ x,\ p)$
$\wedge_R\ \Pi_R$
$(A.1 \setminus \{x,\ dash\ x\}))$
$;_C\ A))$

$\_ \rightarrow_{Cin} \_$ $\vdash (\_ \rightarrow_{Cin} \_)$
$\in (ALPHABET\_REA \times VAR\_NAME \times VAR\_NAME)$
$\times CSP\_PROCESS$
$\rightarrow CSP\_PROCESS$
$\wedge (\forall\ a : ALPHABET\_REA;$
$c : VAR\_NAME;$
$x : VAR\_NAME;$
$A : CSP\_PROCESS$
$\bullet (a,\ c,\ x) \rightarrow_{Cin} A$
$= (a,\ c,\ x,\ True_R\ A.1) \rightarrow_{CinR} A)$

MTrInter $\vdash MTrInter$
$\in SEQ\_EVENT\_VAL \times SEQ\_EVENT\_VAL$
$\rightarrow SET\_SEQ\_EVENT\_VAL$
$\wedge (\forall\ s1,\ s2 : SEQ\_EVENT\_VAL$
$\bullet MTrInter\ (s1,\ s2)$
$= Set$
$\{s : (Seq\ \sim)\ s1\ [\![]\!]_Z\ (Seq\ \sim)\ s2$
$\bullet Seq\ s\})$

MTrPar $\vdash MTrPar$
$\in PAIR\_SEQ\_EVENT\_VAL \times SET\_EVENT\_VAL$
$\rightarrow SET\_SEQ\_EVENT\_VAL$
$\wedge (\forall\ ps : PAIR\_SEQ\_EVENT\_VAL;\ cs : SET\_EVENT\_VAL$
$\bullet MTrPar\ (ps,\ cs)$
$= Set$
$\{s$
$: (Seq\ \sim)\ ((Pair\ \sim)\ ps).1\ [\![_Z$
$(Set\ \sim)\ cs\ ]\!]_Z$
$(Seq\ \sim)\ ((Pair\ \sim)\ ps).2$
$\bullet Seq\ s\})$

MTrParPred $\vdash MTrParPred \in SET\_EVENT\_VAL \rightarrow REL\_PREDICAT$
$\wedge (\forall\ cs : SET\_EVENT\_VAL$

$$
\begin{array}{l}
\quad\quad \bullet\ \mathit{MTrParPred}\ cs \\
\quad\quad\quad = =_{+R} \\
\quad\quad\quad\quad (\{tr,\ dash\ tr\}, \\
\quad\quad\quad\quad\quad \mathit{Rel} \\
\quad\quad\quad\quad\quad\quad ((\_ \in_R \_), \\
\quad\quad\quad\quad\quad\quad\quad \mathit{Fun}_2 \\
\quad\quad\quad\quad\quad\quad\quad\quad ((\_\ \mathit{SeqDif}_R\ \_), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Var}\ (dash\ tr), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Var}\ tr), \\
\quad\quad\quad\quad\quad\quad\quad \mathit{Fun}_2 \\
\quad\quad\quad\quad\quad\quad\quad\quad (\mathit{MTrPar}, \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Fun}_2 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad (\mathit{MkPair}, \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Fun}_2 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad ((\_\ \mathit{SeqDif}_R\ \_), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Var}\ (one\ tr), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Var}\ tr), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Fun}_2 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad ((\_\ \mathit{SeqDif}_R\ \_), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Var}\ (two\ tr), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Var}\ tr)), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad \mathit{Val}\ cs)), \\
\quad\quad\quad\quad\quad \mathit{Val}\ (\mathit{Bool}\ true)))
\end{array}
$$

$$
\begin{array}{ll}
\boldsymbol{MSync} & \vdash \mathit{MSync} \in \mathit{SET\_EVENT\_VAL} \rightarrow \mathit{REL\_PREDICATE} \\
& \quad \wedge\ (\forall\ cs : \mathit{SET\_EVENT\_VAL} \\
& \quad\quad \bullet\ \mathit{MSync}\ cs \\
& \quad\quad\quad = =_{+R} \\
& \quad\quad\quad\quad (\{one\ tr,\ two\ tr\}, \\
& \quad\quad\quad\quad\quad \mathit{Fun}_2\ ((\_ \upharpoonright_R \_),\ \mathit{Var}\ (one\ tr),\ \mathit{Val}\ cs), \\
& \quad\quad\quad\quad\quad \mathit{Fun}_2\ ((\_ \upharpoonright_R \_),\ \mathit{Var}\ (two\ tr),\ \mathit{Val}\ cs)))
\end{array}
$$

$$
\begin{array}{ll}
\boldsymbol{BranchesWaiting} & \\
& \vdash \mathit{BranchesWaiting} \in \mathit{REL\_PREDICATE} \\
& \quad \wedge\ \mathit{BranchesWaiting} \\
& \quad\quad = =_R (\{one\ wait\},\ one\ wait,\ \mathit{Val}\ (\mathit{Bool}\ true)) \\
& \quad\quad\quad \vee_R =_R \\
& \quad\quad\quad\quad (\{two\ wait\},\ two\ wait,\ \mathit{Val}\ (\mathit{Bool}\ true))
\end{array}
$$

$$
\begin{array}{ll}
\boldsymbol{BranchesNotWaiting} & \\
& \vdash \mathit{BranchesNotWaiting} \in \mathit{REL\_PREDICATE}
\end{array}
$$

$$
\begin{array}{ll}
 & \land\ \mathit{BranchesWaiting} \\
 & \quad = =_R (\{one\ wait\},\ one\ wait,\ Val\ (Bool\ false)) \\
 & \qquad \land_R =_R \\
 & \qquad\quad (\{two\ wait\},\ two\ wait,\ Val\ (Bool\ false)) \\
\boldsymbol{MRefPar} & \vdash MRefPar \in SET\_EVENT\_VAL \to REL\_PREDICATE \\
 & \land\ (\forall\ cs : SET\_EVENT\_VAL \\
 & \quad \bullet\ MRefPar\ cs \\
 & \qquad = =_{+R} \\
 & \qquad\quad (\{dash\ ref\}, \\
 & \qquad\quad Rel \\
 & \qquad\qquad ((\_ \subseteq_R \_), \\
 & \qquad\qquad Var\ (dash\ ref), \\
 & \qquad\qquad Fun_2 \\
 & \qquad\qquad\quad ((\_ \cup_R \_), \\
 & \qquad\qquad\quad Fun_2 \\
 & \qquad\qquad\qquad ((\_ \cap_R \_), \\
 & \qquad\qquad\qquad Fun_2 \\
 & \qquad\qquad\qquad\quad ((\_ \cup_R \_), \\
 & \qquad\qquad\qquad\quad Var\ (one\ ref), \\
 & \qquad\qquad\qquad\quad Var\ (two\ ref)), \\
 & \qquad\qquad\qquad Val\ cs), \\
 & \qquad\qquad\quad Fun_2 \\
 & \qquad\qquad\qquad ((\_ \setminus_R \_), \\
 & \qquad\qquad\qquad Fun_2 \\
 & \qquad\qquad\qquad\quad ((\_ \cap_R \_), \\
 & \qquad\qquad\qquad\quad Var\ (one\ ref), \\
 & \qquad\qquad\qquad\quad Var\ (two\ ref)), \\
 & \qquad\qquad\qquad Val\ cs))), \\
 & \qquad\quad Val\ (Bool\ true))) \\
\boldsymbol{MSt} & \vdash MSt \in ALPHABET \times ALPHABET \times ALPHABET \to REL\_PREDICA \\
 & \land\ (\forall\ ns1,\ ns2,\ st : ALPHABET \\
 & \quad \bullet\ st = \varnothing \\
 & \qquad \Rightarrow MSt\ (st,\ ns1,\ ns2) = True_R\ \varnothing \land st \neq \varnothing \\
 & \qquad \Rightarrow (\exists\ n : st \\
 & \qquad\quad \bullet\ n \in ns1 \\
 & \qquad\qquad \Rightarrow MSt\ (st,\ ns1,\ ns2) \\
 & \qquad\qquad\quad = =_R \\
 & \qquad\qquad\qquad (\{dash\ n,\ one\ n\},
\end{array}
$$

$$
\begin{array}{l}
\qquad\qquad\qquad\qquad dash\ n, \\
\qquad\qquad\qquad\qquad Var\ (one\ n)) \\
\qquad\qquad\qquad \wedge_R\ MSt\ (st \setminus \{n\},\ ns1,\ ns2) \\
\qquad\quad \wedge\ n \in ns2 \\
\qquad \Rightarrow MSt\ (st,\ ns1,\ ns2) \\
\qquad\qquad = =_R \\
\qquad\qquad\qquad (\{dash\ n,\ two\ n\}, \\
\qquad\qquad\qquad\quad dash\ n, \\
\qquad\qquad\qquad\quad Var\ (two\ n)) \\
\qquad\qquad\quad \wedge_R\ MSt\ (st \setminus \{n\},\ ns1,\ ns2) \\
\qquad\quad \wedge\ n \notin ns1 \cup ns2 \\
\qquad \Rightarrow MSt\ (st,\ ns1,\ ns2) \\
\qquad\quad = =_R\ (\{dash\ n,\ n\},\ dash\ n,\ Var\ n) \\
\qquad\qquad \wedge_R\ MSt\ (st \setminus \{n\},\ ns1,\ ns2)))
\end{array}
$$

$$
\begin{array}{ll}
\boldsymbol{MWtRefStPar} & \vdash MWtRefStPar \\
& \quad \in SET\_EVENT\_VAL \times ALPHABET \times ALPHABET \times ALPHABET \\
& \qquad \rightarrow REL\_PREDICATE \\
& \quad \wedge\ (\forall\ ns1,\ ns2,\ st : ALPHABET;\ cs : SET\_EVENT\_VAL \\
& \qquad \bullet\ MWtRefStPar\ (cs,\ st,\ ns1,\ ns2) \\
& \qquad\quad = BranchesWaiting \\
& \qquad\qquad \wedge_R\ MRefPar\ cs \lhd_R \\
& \qquad\qquad\quad =_R \\
& \qquad\qquad\qquad (\{dash\ wait\}, \\
& \qquad\qquad\qquad\quad dash\ wait, \\
& \qquad\qquad\qquad\quad Val\ (Bool\ true)) \rhd_R \\
& \qquad\qquad\quad BranchesNotWaiting \\
& \qquad\qquad\qquad \wedge_R\ MSt\ (st,\ ns1,\ ns2)) \\
\boldsymbol{MPar} & \vdash MPar \\
& \quad \in SET\_EVENT\_VAL \times ALPHABET \times ALPHABET \times ALPHABET \\
& \qquad \rightarrow REL\_PREDICATE \\
& \quad \wedge\ (\forall\ ns1,\ ns2,\ st : ALPHABET;\ cs : SET\_EVENT\_VAL \\
& \qquad \bullet\ MPar\ (cs,\ st,\ ns1,\ ns2) \\
& \qquad\quad = MTrParPred\ cs \\
& \qquad\qquad \wedge_R\ MSync\ cs \\
& \qquad\qquad\quad \wedge_R\ MWtRefStPar\ (cs,\ st,\ ns1,\ ns2)) \\
\boldsymbol{DivPar} & \vdash DivPar \\
& \quad \in CSP\_PROCESS \times CSP\_PROCESS \times SET\_EVENT\_VAL \\
& \qquad \rightarrow REL\_PREDICATE
\end{array}
$$

$$
\begin{array}{l}
\land\ (\forall\ a1,\ a2 : CSP\_PROCESS;\ cs : SET\_EVENT\_VAL \\
\quad \bullet\ DivPar\ (a1,\ a2,\ cs) \\
\quad\quad = \exists_{-R} \\
\quad\quad\quad (\{dash\ (one\ tr),\ dash\ (two\ tr)\}, \\
\quad\quad\quad\quad (((a1\ \omega_f)\ \sigma_f) \\
\quad\quad\quad\quad\quad\quad ;_C =_R \\
\quad\quad\quad\quad\quad\quad\quad (a1.1,\ dash\ (one\ tr),\ Var\ tr)) \\
\quad\quad\quad\quad\quad \land_R\ ((a2\ \omega_f) \\
\quad\quad\quad\quad\quad\quad\quad ;_C =_R \\
\quad\quad\quad\quad\quad\quad\quad\quad (a2.1, \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad dash\ (two\ tr), \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad Var\ tr)) \\
\quad\quad\quad\quad\quad\quad \land_R\ MSync\ cs))
\end{array}
$$

$\_\ [\![_{\boldsymbol{C}}\ \_\ ]\!]_{\boldsymbol{C}}\ \_$

$$
\begin{array}{l}
\vdash (\_\ [\![_C\ \_\ ]\!]_C\ \_) \\
\quad\quad \in CSP\_PROCESS \\
\quad\quad\quad \times (ALPHABET \times SET\_EVENT\_VAL \times ALPHABET) \\
\quad\quad\quad \times\ CSP\_PROCESS \\
\quad\quad\quad \to CSP\_PROCESS \\
\quad \land\ (\forall\ a1,\ a2 : CSP\_PROCESS; \\
\quad\quad cs : SET\_EVENT\_VAL; \\
\quad\quad ns1,\ ns2 : ALPHABET \\
\quad\quad \mid (a1,\ a2) \in WF\_CSP\_PROCESS\_PAIR \\
\quad\quad\quad \land\ (ns1 \cap dashed = ns2 \cap dashed \\
\quad\quad\quad \land\ ns2 \cap dashed = \varnothing) \\
\quad\quad\quad \land\ ns1 \cap ns2 = \varnothing \\
\quad\quad \bullet\ a1\ [\![_C\ (ns1,\ cs,\ ns2)\ ]\!]_C\ a2 \\
\quad\quad\quad = R \\
\quad\quad\quad\quad ((\neg_R\ (DivPar\ (a1,\ a2,\ cs)) \\
\quad\quad\quad\quad\quad\quad \land_R\ \neg_R\ (DivPar\ (a2,\ a1,\ cs))) \\
\quad\quad\quad\quad\quad \vdash_D\ (((((a1\ \omega_f)\ \sigma_t) \\
\quad\quad\quad\quad\quad\quad\quad\quad ;_C\ U\ (one,\ out\_a\ a1.1)) \\
\quad\quad\quad\quad\quad\quad\quad \land_R\ ((a2\ \omega_f)\ \sigma_t) \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad ;_C\ U\ (two,\ out\_a\ a2.1)) \\
\quad\quad\quad\quad\quad\quad\quad +_R\ \{tr\} \\
\quad\quad\quad\quad\quad\quad\quad\quad \cup\ (a1.1 \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad \setminus (ALPHABET\_OWTR \\
\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad \cup\ dashed)))
\end{array}
$$

$$
\begin{array}{l}
\quad ;_C \; MPar \\
\qquad (cs, \\
\qquad\quad a1.1 \\
\qquad\qquad \setminus (ALPHABET\_OWTR \\
\qquad\qquad\quad \cup \; dashed), \\
\qquad\quad ns1, \\
\qquad\quad ns2)))
\end{array}
$$

MTrInterPred $\vdash MTrInterPred \in REL\_PREDICATE$

$$
\begin{array}{l}
\wedge \; MTrInterPred \\
\quad = =_{+R} \\
\qquad (\{tr, \; dash \; tr\}, \\
\qquad\quad Rel \\
\qquad\qquad ((\_ \in_R \_), \\
\qquad\qquad\quad Fun_2 \\
\qquad\qquad\qquad ((\_ \; SeqDif_R \; \_), \\
\qquad\qquad\qquad\quad Var \; (dash \; tr), \\
\qquad\qquad\qquad\quad Var \; tr), \\
\qquad\qquad\quad Fun_2 \\
\qquad\qquad\qquad (MTrInter, \\
\qquad\qquad\qquad\quad Fun_2 \\
\qquad\qquad\qquad\qquad ((\_ \; SeqDif_R \; \_), \\
\qquad\qquad\qquad\qquad\quad Var \; (one \; tr), \\
\qquad\qquad\qquad\qquad\quad Var \; tr), \\
\qquad\qquad\qquad\quad Fun_2 \\
\qquad\qquad\qquad\qquad ((\_ \; SeqDif_R \; \_), \\
\qquad\qquad\qquad\qquad\quad Var \; (two \; tr), \\
\qquad\qquad\qquad\qquad\quad Var \; tr))), \\
\qquad\quad Val \; (Bool \; true))
\end{array}
$$

MRefInter $\vdash MRefInter \in REL\_PREDICATE$

$$
\begin{array}{l}
\wedge \; MRefInter \\
\quad = =_{+R} \\
\qquad (\{dash \; ref\}, \\
\qquad\quad Rel \\
\qquad\qquad ((\_ \subseteq_R \_), \\
\qquad\qquad\quad Var \; (dash \; ref), \\
\qquad\qquad\quad Fun_2 \\
\qquad\qquad\qquad ((\_ \cap_R \_), \\
\qquad\qquad\qquad\quad Var \; (one \; ref),
\end{array}
$$

$$
\begin{array}{ll}
& \quad\quad\quad\quad\quad\quad Var\ (two\ ref))), \\
& \quad\quad\quad\quad Val\ (Bool\ true)) \\
\boldsymbol{MWtRefStInter} & \\
& \vdash MWtRefStInter \\
& \quad\quad \in ALPHABET \times ALPHABET \times ALPHABET \rightarrow REL\_PREDICATE \\
& \quad \land (\forall\ ns1, ns2, st : ALPHABET \\
& \quad\quad \bullet MWtRefStInter\ (st, ns1, ns2) \\
& \quad\quad\quad = BranchesNotWaiting \\
& \quad\quad\quad\quad \land_R\ MRefInter \lhd_R \\
& \quad\quad\quad\quad\quad =_R \\
& \quad\quad\quad\quad\quad\quad (\{dash\ wait\}, \\
& \quad\quad\quad\quad\quad\quad\quad dash\ wait, \\
& \quad\quad\quad\quad\quad\quad\quad Val\ (Bool\ true)) \rhd_R \\
& \quad\quad\quad\quad\quad BranchesWaiting \land_R MSt\ (st, ns1, ns2)) \\
\boldsymbol{MInter} & \vdash MInter \\
& \quad\quad \in ALPHABET \times ALPHABET \times ALPHABET \rightarrow REL\_PREDICATE \\
& \quad \land (\forall\ ns1, ns2, st : ALPHABET \\
& \quad\quad \bullet MInter\ (st, ns1, ns2) \\
& \quad\quad\quad = MTrInterPred \\
& \quad\quad\quad\quad \land_R\ MWtRefStInter\ (st, ns1, ns2)) \\
\boldsymbol{DivInter} & \vdash DivInter \in CSP\_PROCESS \times CSP\_PROCESS \rightarrow REL\_PREDICATE \\
& \quad \land (\forall\ a1, a2 : CSP\_PROCESS \\
& \quad\quad \bullet DivInter\ (a1, a2) \\
& \quad\quad\quad = \exists_{-R} \\
& \quad\quad\quad\quad (\{dash\ (one\ tr), dash\ (two\ tr)\}, \\
& \quad\quad\quad\quad\quad (((a1\ \omega_f)\ \sigma_f) \\
& \quad\quad\quad\quad\quad\quad\quad ;_C =_R \\
& \quad\quad\quad\quad\quad\quad\quad\quad (a1.1, dash\ (one\ tr), Var\ tr)) \\
& \quad\quad\quad\quad\quad\quad \land_R\ (a2\ \omega_f) \\
& \quad\quad\quad\quad\quad\quad\quad ;_C =_R \\
& \quad\quad\quad\quad\quad\quad\quad\quad (a2.1, \\
& \quad\quad\quad\quad\quad\quad\quad\quad\quad dash\ (two\ tr), \\
& \quad\quad\quad\quad\quad\quad\quad\quad\quad Var\ tr))) \\
\boldsymbol{\_\ [\![_C\ \_\ ]\!]_C\ \_} & \\
& \vdash (\_\ [\![_C\ \_\ ]\!]_C\ \_) \\
& \quad\quad \in CSP\_PROCESS \\
& \quad\quad\quad \times (ALPHABET \times ALPHABET) \\
& \quad\quad\quad \times CSP\_PROCESS
\end{array}
$$

$$
\begin{array}{ll}
& \quad \rightarrow CSP\_PROCESS \\
& \land (\forall\ a1,\ a2 : CSP\_PROCESS;\ ns1,\ ns2 : ALPHABET \\
& \quad \mid (a1,\ a2) \in WF\_CSP\_PROCESS\_PAIR \land ns1 \cap ns2 = \varnothing \\
& \quad \bullet\ a1\ [\![_C\ (ns1,\ ns2)\ ]\!]_C\ a2 \\
& \qquad = R \\
& \qquad\quad ((\neg_R\ (DivInter\ (a1,\ a2)) \\
& \qquad\qquad\quad \land_R\ \neg_R\ (DivInter\ (a2,\ a1))) \\
& \qquad\qquad \vdash_D\ ((((((a1\ \omega_f)\ \sigma_t) \\
& \qquad\qquad\qquad\qquad ;_C\ U\ (one,\ out\_a\ a1.1)) \\
& \qquad\qquad\qquad\quad \land_R\ ((a2\ \omega_f)\ \sigma_t) \\
& \qquad\qquad\qquad\qquad ;_C\ U\ (two,\ out\_a\ a1.1)) \\
& \qquad\qquad\qquad +_R\ \{tr\} \\
& \qquad\qquad\qquad\quad \cup\ (a1.1 \\
& \qquad\qquad\qquad\qquad \setminus\ (ALPHABET\_OWTR \\
& \qquad\qquad\qquad\qquad\quad \cup\ dashed))) \\
& \qquad\qquad\quad \land_R\ \Pi_R\ (a1.1 \setminus ALPHABET\_OWTR)) \\
& \qquad\qquad ;_C\ MInter \\
& \qquad\qquad\quad (a1.1 \setminus ALPHABET\_OWTR \setminus dashed, \\
& \qquad\qquad\quad ns1, \\
& \qquad\qquad\quad ns2))) \\
\_ \setminus_C \_ & \vdash (\_ \setminus_C \_) \in CSP\_PROCESS \times SET\_EVENT\_VAL \rightarrow CSP\_PROCESS \\
& \land (\forall\ a : CSP\_PROCESS;\ cs : SET\_EVENT\_VAL \\
& \quad \bullet\ \exists\ s : VAR\_NAME \\
& \qquad \mid s \notin a.1 \\
& \qquad \bullet\ a \setminus_C cs \\
& \qquad\quad = R \\
& \qquad\qquad (\exists_{-R} \\
& \qquad\qquad\quad (\{s\}, \\
& \qquad\qquad\quad /_R \\
& \qquad\qquad\qquad (/_R \\
& \qquad\qquad\qquad\quad (a \oplus_R \{s\}, \\
& \qquad\qquad\qquad\quad Var\ s, \\
& \qquad\qquad\qquad\quad dash\ tr), \\
& \qquad\qquad\qquad Fun_2 \\
& \qquad\qquad\qquad\quad ((\_ \cup_R \_), \\
& \qquad\qquad\qquad\quad Val\ cs, \\
& \qquad\qquad\qquad\quad Var\ ref), \\
& \qquad\qquad\qquad dash\ ref)
\end{array}
$$

$$
\begin{array}{l}
\qquad\qquad\qquad\qquad \wedge_R =_{+R} \\
\qquad\qquad\qquad\qquad\quad (\{tr,\ dash\ tr,\ s\}, \\
\qquad\qquad\qquad\qquad\quad\ \ Fun_2 \\
\qquad\qquad\qquad\qquad\qquad ((\_\ SeqDif_R\ \_), \\
\qquad\qquad\qquad\qquad\qquad\ \ Var\ (dash\ tr), \\
\qquad\qquad\qquad\qquad\qquad\ \ Var\ tr), \\
\qquad\qquad\qquad\qquad\quad\ \ Fun_2 \\
\qquad\qquad\qquad\qquad\qquad ((\_\ \backslash_R\ \_), \\
\qquad\qquad\qquad\qquad\qquad\ \ Val \\
\qquad\qquad\qquad\qquad\qquad\quad (Set \\
EVENT\_VAL), \\
\qquad\qquad\qquad\qquad\qquad\ \ Val\ cs)))) \\
\qquad\qquad ;_C\ Skip\ a.1)
\end{array}
$$

$\boldsymbol{\mu_C}$ $\vdash \mu_C \in CIRCUS\_FUNCTION \rightarrow CSP\_PROCESS$
$\quad \wedge (\forall f : CIRCUS\_FUNCTION \bullet \mu_C\ f = \mu_R\ f)$

$\boldsymbol{Assign_C}$

$$
\begin{array}{l}
\vdash Assign_C \in WF\_Assign_C \rightarrow CSP\_PROCESS \\
\quad \wedge (\forall a : ALPHABET; \\
\qquad ns : seq\ VAR\_NAME; \\
\qquad exps : seq\ EXPRESSION \\
\quad\ \ \mid (a,\ ns,\ exps) \in WF\_Assign_C \\
\quad\ \ \bullet Assign_C\ (a,\ ns,\ exps) \\
\qquad = R \\
\qquad\quad (True_R\ a \\
\qquad\qquad \vdash_D Assign_R\ (a,\ ns,\ exps) \\
\qquad\qquad\quad \wedge_R =_R (a,\ dash\ tr,\ Var\ tr) \\
\qquad\qquad\qquad \wedge_R =_R \\
\qquad\qquad\qquad\quad (a, \\
\qquad\qquad\qquad\quad\ \ dash\ wait, \\
\qquad\qquad\qquad\quad\ \ Val\ (Bool\ false))))
\end{array}
$$

$\boldsymbol{SpecStatement_C}$

$$
\begin{array}{l}
\vdash SpecStatement_C \in WF\_SpecStatement_C \rightarrow CSP\_PROCESS \\
\quad \wedge (\forall a : ALPHABET; \\
\qquad f : \mathbb{F}\ VAR\_NAME; \\
\qquad preC : CIRCUS\_CONDITION; \\
\qquad postC : CIRCUS\_PREDICATE \\
\quad\ \ \mid (a,\ f,\ preC,\ postC) \in WF\_SpecStatement_C \\
\quad\ \ \bullet SpecStatement_C\ (a,\ f,\ preC,\ postC) \\
\qquad = R
\end{array}
$$

$$
\begin{array}{l}
(preC \\
\quad \vdash_D postC \\
\quad\quad \wedge_R =_R (a, dash\ tr, Var\ tr) \\
\quad\quad\quad \wedge_R =_R \\
\quad\quad\quad\quad (a, \\
\quad\quad\quad\quad\ dash\ wait, \\
\quad\quad\quad\quad\ Val\ (Bool\ false)) \\
\quad\quad\quad\quad \wedge_R \mathit{\Pi}_R \\
\quad\quad\quad\quad\quad (a \\
\quad\quad\quad\quad\quad\quad \setminus (ALPHABET\_OWTR \\
\quad\quad\quad\quad\quad\quad\quad \cup (f \\
\quad\quad\quad\quad\quad\quad\quad\quad \cup \{n : f \\
\quad\quad\quad\quad\quad\quad\quad\quad \bullet dash \\
n\})))))
\end{array}
$$

$$
\begin{array}{ll}
\boldsymbol{\{_C\ \_\ \}_C} & \vdash (\{_C\ \_\ \}_C) \in WF\_Condition_C \rightarrow CSP\_PROCESS \\
& \quad \wedge (\forall a : ALPHABET; g : CIRCUS\_CONDITION \\
& \quad\quad \mid (a, g) \in WF\_Condition_C \\
& \quad\quad \bullet \{_C\ (a, g)\ \}_C \\
& \quad\quad\quad = SpecStatement_C\ (a, \{\}, g, True_R\ a)) \\
\boldsymbol{\langle_C\ \_\ \rangle_C} & \vdash (\langle_C\ \_\ \rangle_C) \in WF\_Condition_C \rightarrow CSP\_PROCESS \\
& \quad \wedge (\forall a : ALPHABET; g : CIRCUS\_CONDITION \\
& \quad\quad \mid (a, g) \in WF\_Condition_C \\
& \quad\quad \bullet \langle_C\ (a, g)\ \rangle_C = R\ (True_R\ a \vdash_D g)) \\
\boldsymbol{Typing} & \vdash Typing \in VAR\_DECLS \times ALPHABET \nrightarrow REL\_PREDICATE \\
& \quad \wedge (\forall decls : VAR\_DECLS; a : ALPHABET \\
& \quad\quad \mid ran\ decls.1 \subseteq a \\
& \quad\quad \bullet \#\ decls.1 = 1 \\
& \quad\quad\quad\quad \wedge (\exists n : Z\_VAR\_NAME; e : EXPRESSION \\
& \quad\quad\quad\quad\quad \mid n = head\ decls.1 \wedge e = head\ decls.2 \\
& \quad\quad\quad\quad\quad \bullet Typing\ (decls, a) \\
& \quad\quad\quad\quad\quad\quad = =_{+R} \\
& \quad\quad\quad\quad\quad\quad\quad (a, \\
& \quad\quad\quad\quad\quad\quad\quad\ Rel\ ((\_ \in_R \_), Var\ n, e), \\
& \quad\quad\quad\quad\quad\quad\quad\ Val\ (Bool\ true))) \\
& \quad\quad\quad \vee \#\ decls.1 > 1 \\
& \quad\quad\quad\quad \wedge (\exists n : Z\_VAR\_NAME; e : EXPRESSION \\
& \quad\quad\quad\quad\quad \mid n = head\ decls.1 \wedge e = head\ decls.2 \\
& \quad\quad\quad\quad\quad \bullet Typing\ (decls, a)
\end{array}
$$

$$
\begin{array}{l}
\quad = \, =_{+R} \\
\qquad (a, \\
\qquad\quad Rel\ ((\_ \in_R \_),\ Var\ n,\ e), \\
\qquad\quad Val\ (Bool\ true)) \\
\qquad \wedge_R\ Typing \\
\qquad\quad ((tail\ decls.1,\ tail\ decls.2), \\
\qquad\quad\ a)))
\end{array}
$$

$$
\begin{array}{ll}
\boldsymbol{SchemaExp_C} & \vdash SchemaExp_C \in WF\_SchemaExp_C \rightarrow CSP\_PROCESS \\
& \wedge\ (\forall\ decls : VAR\_DECLS;\ p : REL\_PREDICATE \\
& \quad \mid (decls,\ p) \in WF\_SchemaExp_C \\
& \quad \bullet\ \exists\ f : \mathbb{F}\ Z\_VAR\_NAME \\
& \qquad \mid f \subseteq undashed \\
& \qquad\quad \wedge\ ran\ (decls.1 \upharpoonright dashed) = dash\ \llparenthesis\ f\ \rrparenthesis \\
& \qquad \bullet\ SchemaExp_C\ (decls,\ p) \\
& \qquad\quad = SpecStatement_C \\
& \qquad\qquad (ran\ decls.1 \cup ALPHABET\_OWTR, \\
& \qquad\qquad\ f, \\
& \qquad\qquad\ \exists_{-R} \\
& \qquad\qquad\quad (ran\ decls.1 \setminus undashed, \\
& \qquad\qquad\qquad Typing\ (decls,\ p.1) \wedge_R p), \\
& \qquad\qquad Typing\ (decls,\ p.1) \wedge_R p)) \\
\boldsymbol{TrueGuards} & \vdash TrueGuards \in GUARDED\_ACTIONS \rightarrow REL\_PREDICATE \\
& \wedge\ (\forall\ gactions : GUARDED\_ACTIONS \\
& \quad \bullet\ \#\ gactions.1 = 1 \\
& \qquad \wedge\ (\exists\ g : CIRCUS\_CONDITION;\ a : CSP\_PROCESS \\
& \qquad\quad \mid g = head\ gactions.1 \wedge a = head\ gactions.2 \\
& \qquad\quad \bullet\ TrueGuards\ gactions = g) \\
& \quad \vee\ \#\ gactions.1 > 1 \\
& \qquad \wedge\ (\exists\ g : CIRCUS\_CONDITION;\ a : CSP\_PROCESS \\
& \qquad\quad \mid g = head\ gactions.1 \wedge a = head\ gactions.2 \\
& \qquad\quad \bullet\ TrueGuards\ gactions \\
& \qquad\qquad = g \\
& \qquad\qquad\quad \vee_R\ TrueGuards \\
& \qquad\qquad\qquad (tail\ gactions.1, \\
& \qquad\qquad\qquad\ tail\ gactions.2))) \\
\boldsymbol{NonDivActions} & \\
& \vdash NonDivActions \in GUARDED\_ACTIONS \rightarrow REL\_PREDICATE \\
& \quad \wedge\ (\forall\ gactions : GUARDED\_ACTIONS
\end{array}
$$

$$
\begin{array}{l}
\quad\quad \bullet\ \#\ gactions.1 = 1 \\
\quad\quad\quad \wedge\ (\exists\ g : CIRCUS\_CONDITION;\ a : CSP\_PROCESS \\
\quad\quad\quad\quad \mid g = head\ gactions.1 \wedge a = head\ gactions.2 \\
\quad\quad\quad\quad \bullet\ NonDivActions\ gactions \\
\quad\quad\quad\quad\quad = g \Rightarrow_R \neg_R\ ((a\ \omega_f)\ \sigma_f)) \\
\quad\quad\quad \vee\ \#\ gactions.1 > 1 \\
\quad\quad\quad \wedge\ (\exists\ g : CIRCUS\_CONDITION;\ a : CSP\_PROCESS \\
\quad\quad\quad\quad \mid g = head\ gactions.1 \wedge a = head\ gactions.2 \\
\quad\quad\quad\quad \bullet\ NonDivActions\ gactions \\
\quad\quad\quad\quad\quad = (g \Rightarrow_R \neg_R\ ((a\ \omega_f)\ \sigma_f)) \\
\quad\quad\quad\quad\quad\quad \wedge_R\ NonDivActions \\
\quad\quad\quad\quad\quad\quad\quad (tail\ gactions.1, \\
\quad\quad\quad\quad\quad\quad\quad\ \ tail\ gactions.2))) \\
\boldsymbol{ExecActions} \vdash ExecActions \in GUARDED\_ACTIONS \rightarrow REL\_PREDICATE \\
\quad \wedge\ (\forall\ gactions : GUARDED\_ACTIONS \\
\quad\quad \bullet\ \#\ gactions.1 = 1 \\
\quad\quad\quad \wedge\ (\exists\ g : CIRCUS\_CONDITION;\ a : CSP\_PROCESS \\
\quad\quad\quad\quad \mid g = head\ gactions.1 \wedge a = head\ gactions.2 \\
\quad\quad\quad\quad \bullet\ ExecActions\ gactions = g \wedge_R (a\ \omega_f)\ \sigma_t) \\
\quad\quad\quad \vee\ \#\ gactions.1 > 1 \\
\quad\quad\quad \wedge\ (\exists\ g : CIRCUS\_CONDITION;\ a : CSP\_PROCESS \\
\quad\quad\quad\quad \mid g = head\ gactions.1 \wedge a = head\ gactions.2 \\
\quad\quad\quad\quad \bullet\ ExecActions\ gactions \\
\quad\quad\quad\quad\quad = (g \wedge_R (a\ \omega_f)\ \sigma_t) \\
\quad\quad\quad\quad\quad\quad \vee_R\ ExecActions \\
\quad\quad\quad\quad\quad\quad\quad (tail\ gactions.1, \\
\quad\quad\quad\quad\quad\quad\quad\ \ tail\ gactions.2))) \\
\boldsymbol{if_C\ \_\ fi_C} \vdash (if_C\ \_\ fi_C) \in GUARDED\_ACTIONS \rightarrow CSP\_PROCESS \\
\quad \wedge\ (\forall\ gactions : GUARDED\_ACTIONS \\
\quad\quad \bullet\ if_C\ gactions\ fi_C \\
\quad\quad\quad = R \\
\quad\quad\quad\quad ((TrueGuards\ gactions \\
\quad\quad\quad\quad\quad\quad \wedge_R\ NonDivActions\ gactions) \\
\quad\quad\quad\quad\quad \vdash_D ExecActions\ gactions)) \\
\boldsymbol{ifb_C\ \_ \mapsto_C \_\ else_C\ \_ \mapsto_C \_\ fib_C} \\
\quad \vdash (ifb_C\ \_ \mapsto_C \_\ else_C\ \_ \mapsto_C \_\ fib_C) \\
\quad\quad \in CIRCUS\_CONDITION \\
\quad\quad\quad \times\ CSP\_PROCESS
\end{array}
$$

$$
\begin{array}{ll}
 & \quad\quad \times\ CIRCUS\_CONDITION \\
 & \quad\quad \times\ CSP\_PROCESS \\
 & \quad\quad \nrightarrow\ CSP\_PROCESS \\
 & \wedge\ (\forall\ g1,\ g2 : CIRCUS\_CONDITION; \\
 & \quad a1,\ a2 : CSP\_PROCESS \\
 & \quad \mid ((\langle g1,\ g2\rangle,\ \langle a1,\ a2\rangle) \in GUARDED\_ACTIONS \\
 & \quad \bullet\ ifb_C\ g1 \mapsto_C a1\ else_C\ g2 \mapsto_C a2\ fib_C \\
 & \quad = R \\
 & \quad\quad (((g1 \vee_R g2) \\
 & \quad\quad\quad \wedge_R (g1 \Rightarrow_R \neg_R ((a1\ \omega_f)\ \sigma_f)) \\
 & \quad\quad\quad\quad \wedge_R g2 \Rightarrow_R \neg_R ((a2\ \omega_f)\ \sigma_f)) \\
 & \quad\quad\quad \vdash_D (g1 \wedge_R \neg_R ((a1\ \omega_f)\ \sigma_t)) \\
 & \quad\quad\quad\quad \vee_R g2 \wedge_R \neg_R ((a2\ \omega_f)\ \sigma_t))) \\
\boldsymbol{param_C} & \vdash param_C \in WF\_param_C \rightarrow CSP\_PROCESS \\
 & \wedge\ (\forall\ x : VAR\_NAME; \\
 & \quad T : EXPRESSION; \\
 & \quad a : CSP\_PROCESS; \\
 & \quad e : EXPRESSION \\
 & \quad \mid (x,\ T,\ a,\ e) \in WF\_param_C \\
 & \quad \bullet\ param_C\ (x,\ T,\ a,\ e) = /_R\ (a,\ e,\ x)) \\
\boldsymbol{val_C} & \vdash val_C \in WF\_val_C \rightarrow CSP\_PROCESS \\
 & \wedge\ (\forall\ x : VAR\_NAME; \\
 & \quad t : SET\_VAL; \\
 & \quad a : CSP\_PROCESS; \\
 & \quad e : EXPRESSION \\
 & \quad \mid (x,\ t,\ a,\ e) \in WF\_val_C \\
 & \quad \bullet\ val_C\ (x,\ t,\ a,\ e) \\
 & \quad = var_C\ (x,\ t,\ Assign_R\ (a.1,\ \langle x\rangle,\ \langle e\rangle)\ ;_C\ a)) \\
\boldsymbol{res_C} & \vdash res_C \in WF\_res_C \rightarrow CSP\_PROCESS \\
 & \wedge\ (\forall\ x : VAR\_NAME; \\
 & \quad t : SET\_VAL; \\
 & \quad a : CSP\_PROCESS; \\
 & \quad y : VAR\_NAME \\
 & \quad \mid (x,\ t,\ a,\ y) \in WF\_res_C \\
 & \quad \bullet\ res_C\ (x,\ t,\ a,\ y) \\
 & \quad = var_C \\
 & \quad\quad (x,\ t,\ a\ ;_R\ Assign_R\ (a.1,\ \langle y\rangle,\ \langle Var\ x\rangle))) \\
\boldsymbol{vres_C} & \vdash vres_C \in WF\_vres_C \rightarrow CSP\_PROCESS
\end{array}
$$

$$
\begin{array}{ll}
 & \land\ (\forall\ x : VAR\_NAME;\\
 & \quad t : SET\_VAL;\\
 & \quad a : CSP\_PROCESS;\\
 & \quad y : VAR\_NAME\\
 & \quad \mid (x,\ t,\ a,\ y) \in WF\_vres_C\\
 & \quad \bullet\ vres_C\ (x,\ t,\ a,\ y)\\
 & \qquad = var_C\\
 & \qquad\quad (x,\\
 & \qquad\quad\ t,\\
 & \qquad\quad\ Assign_R\ (a.1,\ \langle x\rangle,\ \langle Var\ y\rangle)\\
 & \qquad\qquad ;_R\ a\\
 & \qquad\qquad\quad ;_R\ Assign_R\\
 & \qquad\qquad\qquad (a.1,\ \langle y\rangle,\ \langle Var\ x\rangle)))\\
\boldsymbol{C1} & \vdash C1 \in CSP\_PROCESS \to CSP\_PROCESS\\
 & \quad \land\ (\forall\ a : CSP\_PROCESS \bullet C1\ a = a\ ;_R\ Skip\ a.1)\\
\boldsymbol{C1\_healthy} & \vdash C1\_healthy \in \mathbb{P}\ CSP\_PROCESS\\
 & \quad \land\ C1\_healthy = \{a : CSP\_PROCESS \mid a = C1\ a\}\\
\boldsymbol{C2} & \vdash C2 \in CSP\_PROCESS \to CSP\_PROCESS\\
 & \quad \land\ (\forall\ a : CSP\_PROCESS\\
 & \qquad \bullet\ C2\ a = a\ [\![_C\ (a.1,\ \varnothing)\ ]\!]_C\ Skip\ a.1)\\
\boldsymbol{C2\_healthy} & \vdash C2\_healthy \in \mathbb{P}\ CSP\_PROCESS\\
 & \quad \land\ C2\_healthy = \{a : CSP\_PROCESS \mid a = C2\ a\}\\
\boldsymbol{C3} & \vdash C3 \in CSP\_PROCESS \to CSP\_PROCESS\\
 & \quad \land\ (\forall\ a : CSP\_PROCESS\\
 & \qquad \bullet\ C3\ a\\
 & \qquad\quad = R\\
 & \qquad\qquad ((\neg_R\ ((a\ \sigma_f)\ \omega_f)\ ;_R\ True_R\ a.1)\\
 & \qquad\qquad\quad \vdash_D\ (a\ \sigma_t)\ \omega_f))\\
\boldsymbol{C3\_healthy} & \vdash C3\_healthy \in \mathbb{P}\ CSP\_PROCESS\\
 & \quad \land\ C3\_healthy = \{a : CSP\_PROCESS \mid a = C3\ a\}
\end{array}
$$

14.5 Definitions

$$
\begin{array}{ll}
\boldsymbol{Z\_VAR\_NAME} & \vdash Z\_VAR\_NAME = \{n : NAME \mid n \notin ALPHABET\_OWT\\
\boldsymbol{VAR\_DECLS} & \vdash VAR\_DECLS\\
 & = \{vars : seq\ Z\_VAR\_NAME;\ types : seq\ EXPRESSION\\
 & \quad \mid dom\ vars \in (\mathbb{F}\ \_)\\
 & \qquad \land\ dom\ types \in (\mathbb{F}\ \_)
\end{array}
$$

$\wedge \; \# \; (ran \; vars) = \# \; (ran \; types)$
$\wedge \; \# \; (ran \; types) > 0\}$

$\boldsymbol{WF\_Skip_C} \vdash WF\_Skip_C = \{a : WF\_Skip_R \mid ALPHABET\_OWTR \subseteq a\}$

$\boldsymbol{WF\_Guard_C} \vdash WF\_Guard_C$
$= \{g : CIRCUS\_CONDITION; \; a : CSP\_PROCESS$
$\mid g.1 = a.1\}$

$\boldsymbol{WF\_if_{C\_fiC}} \vdash WF\_if_{C\_fiC}$
$= \{g : CIRCUS\_CONDITION; \; a : CSP\_PROCESS$
$\mid g.1 = a.1\}$

$\boldsymbol{WF\_Semi_C} \vdash WF\_Semi_C$
$= \{a1, \; a2 : CSP\_PROCESS$
$\mid (a1, \; a2) \in WF\_Semi_R\}$

$\boldsymbol{WF\_Var_C} \vdash WF\_Var_C$
$= \{n : VAR\_NAME; \; t : SET\_VAL; \; a : CSP\_PROCESS$
$\mid n \notin ALPHABET\_OWTR$
$\wedge \; n \in undashed$
$\wedge \; \{n, \; dash \; n\} \subseteq a.1\}$

$\boldsymbol{WF\_Assign_C} \vdash WF\_Assign_C$
$= \{a : ALPHABET;$
$ns : seq \; VAR\_NAME;$
$exps : seq \; EXPRESSION$
$\mid (\forall \; n : ran \; ns \bullet n \in a \wedge n \in undashed)$
$\wedge \; (\forall \; e : ran \; exps \bullet FV \; e \subseteq a \wedge FV \; e \subseteq undashed)$
$\wedge \; (\# \; ns = \# \; exps$
$\wedge \; \# \; exps \neq 0)$
$\wedge \; a \in homogeneous$
$\wedge \; ALPHABET\_OWTR \subseteq a\}$

$\boldsymbol{WF\_SpecStatement_C}$
$\vdash WF\_SpecStatement_C$
$= \{a : ALPHABET;$
$f : \mathbb{F} \; VAR\_NAME;$
$preC : CIRCUS\_CONDITION;$
$postC : CIRCUS\_PREDICATE$
$\mid f \subseteq a$
$\wedge \; f \subseteq undashed$
$\wedge \; a \in homogeneous$
$\wedge \; (preC.1 = postC.1$
$\wedge \; postC.1 = a)$

$\wedge\ ALPHABET\_OWTR \subseteq a\}$

$\boldsymbol{WF\_Condition_C}$

$\vdash WF\_Condition_C = \{a : ALPHABET;\ g : CIRCUS\_CONDITION \mid a \in homogeneous \wedge a = g.1\}$

$\boldsymbol{WF\_SchemaExp_C}$

$\vdash WF\_SchemaExp_C = \{decls : VAR\_DECLS;\ p : REL\_PREDICATE \mid p.1 \setminus ALPHABET\_OWTR = ran\ decls.1\}$

$\boldsymbol{WF\_param_C}$ $\vdash WF\_param_C = \{x : VAR\_NAME;\ T : EXPRESSION;\ a : CSP\_PROCESS;\ e : EXPRESSION \mid x \in a.1 \wedge FV\ e \subseteq a.1\}$

$\boldsymbol{WF\_val_C}$ $\vdash WF\_val_C = \{x : VAR\_NAME;\ t : SET\_VAL;\ a : CSP\_PROCESS;\ e : EXPRESSION \mid x \notin FV\ e \wedge x \in a.1 \wedge FV\ e \subseteq a.1\}$

$\boldsymbol{WF\_res_C}$ $\vdash WF\_res_C = \{x : VAR\_NAME;\ t : SET\_VAL;\ a : CSP\_PROCESS;\ y : VAR\_NAME \mid \{x, y\} \subseteq a.1\}$

$\boldsymbol{WF\_vres_C}$ $\vdash WF\_vres_C = \{x : VAR\_NAME;\ t : SET\_VAL;\ a : CSP\_PROCESS;\ y : VAR\_NAME \mid x \neq y \wedge \{x, y\} \subseteq a.1\}$

$\boldsymbol{WF\_PREFIXING_C}$

$\vdash WF\_PREFIXING_C = \{a\_n\_e : WF\_PREFIXING;\ A : CSP\_PROCESS \mid a\_n\_e.1 = A.1\}$

$\boldsymbol{WF\_PREFIXING_{CinR}}$

$\vdash$ $WF\_PREFIXING_{CinR}$
$= \{a : ALPHABET\_REA;$
$c : VAR\_NAME;$
$x : VAR\_NAME;$
$p : CIRCUS\_CONDITION;$
$A : CSP\_PROCESS$
$\mid a = A.1 \wedge \{x, dash\ x\} \subseteq a\}$

CIRCUS_FUNCTION

$\vdash CIRCUS\_FUNCTION$
$= \{f : CSP\_PROCESS \nrightarrow CSP\_PROCESS$
$\mid \exists a : ALPHABET$
$\bullet \forall u\_dom : dom\ f;\ u\_ran : ran\ f$
$\bullet a = u\_dom.1 \wedge u\_dom.1 = u\_ran.1\}$

GUARDED_ACTIONS

$\vdash GUARDED\_ACTIONS$
$= \{conditions : seq\ CIRCUS\_CONDITION;$
$actions : seq\ CSP\_PROCESS$
$\mid dom\ conditions \in (\mathbb{F}\ \_)$
$\wedge dom\ actions \in (\mathbb{F}\ \_)$
$\wedge (\#\ (ran\ conditions) = \#\ (ran\ actions)$
$\wedge \#\ (ran\ actions) > 0)$
$\wedge (\exists a : ALPHABET$
$\bullet (\forall c : ran\ conditions \bullet c.1 = a)$
$\wedge (\forall A : ran\ actions \bullet A.1 = a))\}$

CIRCUS_ACTION

$\vdash CIRCUS\_ACTION$
$= \{c : CSP\_PROCESS$
$\mid c \in C1\_healthy$
$\wedge c \in C2\_healthy$
$\wedge c \in C3\_healthy\}$

14.6 Theorems

$\boldsymbol{C\_ALPHABET\_WF\_Skip_C\_thm}$

$\vdash \forall a : WF\_Skip_C \bullet a \in WF\_Skip_R \wedge a \in ALPHABET\_REA$

$\boldsymbol{C\_PREDICATE\_Stop_C\_thm}$

$\vdash \forall a : WF\_Skip_C \bullet Stop\ a \in CSP\_PROCESS$

$\boldsymbol{CIRCUS\_ACTION\_\in\_CSP\_PROCESS\_thm}$

$\vdash \forall\ a : CIRCUS\_ACTION \bullet a \in CSP\_PROCESS$

$\boldsymbol{C\_PREDICATE\_Stop_C\_alphabet\_thm}$

$\vdash \forall\ a : WF\_Skip_C \bullet (Stop\ a).1 = a$

$\boldsymbol{C\_Stop_C\_diverge\_not\_wait\_thm}$

$$\begin{array}{l} \vdash \forall\ a : WF\_Skip_C \\ \quad \bullet (Stop\ a\ \omega_f)\ \sigma_f \\ \quad\quad = =_R (a,\ okay,\ Val\ (Bool\ false)) \\ \quad\quad\quad \wedge_R =_{+R} \\ \quad\quad\quad\quad (ALPHABET\_OWTR, \\ \quad\quad\quad\quad\ Rel\ ((\_ \leq_R \_),\ Var\ tr,\ Var\ (dash\ tr)), \\ \quad\quad\quad\quad\ Val\ (Bool\ true)) \end{array}$$

$\boldsymbol{C\_Stop_C\_converge\_not\_wait\_thm}$

$$\begin{array}{l} \vdash \forall\ a : WF\_Skip_C \\ \quad \bullet (Stop\ a\ \omega_f)\ \sigma_t \\ \quad\quad = CSP1 \\ \quad\quad\quad (=_R (ALPHABET\_OWTR,\ dash\ tr,\ Var\ tr) \\ \quad\quad\quad\quad \wedge_R =_R (a,\ dash\ wait,\ Val\ (Bool\ true))) \end{array}$$

$\boldsymbol{C\_true\_guard\_thm1}$

$$\begin{array}{l} \vdash \forall\ a : WF\_Skip_C;\ A : CSP\_PROCESS \\ \quad \mid (True_R\ a,\ A) \in WF\_Guard_C \\ \quad \bullet True_R\ a\ \&_C\ A = A \end{array}$$

$\boldsymbol{C\_true\_guard\_thm}$

$$\begin{array}{l} \vdash \forall\ a : WF\_Skip_C;\ A : CIRCUS\_ACTION \\ \quad \mid (True_R\ a,\ A) \in WF\_Guard_C \\ \quad \bullet True_R\ a\ \&_C\ A = A \end{array}$$

$\boldsymbol{C\_false\_guard\_thm1}$

$$\begin{array}{l} \vdash \forall\ a : WF\_Skip_C;\ A : CSP\_PROCESS \\ \quad \mid (False_R\ a,\ A) \in WF\_Guard_C \\ \quad \bullet False_R\ a\ \&_C\ A = Stop\ a \end{array}$$

$\boldsymbol{C\_false\_guard\_thm}$

$$\begin{array}{l} \vdash \forall\ a : WF\_Skip_C;\ A : CIRCUS\_ACTION \\ \quad \mid (False_R\ a,\ A) \in WF\_Guard_C \\ \quad \bullet False_R\ a\ \&_C\ A = Stop\ a \end{array}$$

$\boldsymbol{C\_assumption\_unit\_thm}$

$\vdash \forall\ a : WF\_Skip_C \bullet \{_C\ (a,\ True_R\ a)\ \}_C = Skip\ a$

$\boldsymbol{C\_assumption\_zero\_thm}$

$\vdash \forall\ a : WF\_Skip_C \bullet \{_C\ (a,\ False_R\ a)\ \}_C = Chaos\ a$

$\boldsymbol{C\_\sqcap_{C\_idem\_thm1}}$

$\vdash \forall A : CSP\_PROCESS \bullet A \sqcap_C A = A$

$\boldsymbol{C\_\sqcap_{C\_idem\_thm}}$

$\vdash \forall A : CIRCUS\_ACTION \bullet A \sqcap_C A = A$

$\boldsymbol{C\_\sqcap_C\_com\_thm1}$

$\vdash \forall A1, A2 : CSP\_PROCESS$
$\mid (A1, A2) \in WF\_CSP\_PROCESS\_PAIR$
$\bullet A1 \sqcap_C A2 = A2 \sqcap_C A1$

$\boldsymbol{C\_\sqcap_C\_com\_thm}$

$\vdash \forall A1, A2 : CIRCUS\_ACTION$
$\mid (A1, A2) \in WF\_CSP\_PROCESS\_PAIR$
$\bullet A1 \sqcap_C A2 = A2 \sqcap_C A1$

$\boldsymbol{C\_CIRCUS\_ACTION\_\in\_REL\_PREDICATE\_thm}$

$\vdash \forall A : CIRCUS\_ACTION \bullet A \in REL\_PREDICATE$

$\boldsymbol{C\_ALPHABET\_OWTR\_\subseteq\_CIRCUS\_ACTION\_thm}$

$\vdash \forall A : CIRCUS\_ACTION \bullet ALPHABET\_OWTR \subseteq A.1$

$\boldsymbol{C\_\boxtimes_C\_com\_thm1}$

$\vdash \forall A1, A2 : CSP\_PROCESS$
$\mid (A1, A2) \in WF\_CSP\_PROCESS\_PAIR$
$\bullet A1 \boxtimes_C A2 = A2 \boxtimes_C A1$

$\boldsymbol{C\_\boxtimes_C\_com\_thm}$

$\vdash \forall A1, A2 : CIRCUS\_ACTION$
$\mid (A1, A2) \in WF\_CSP\_PROCESS\_PAIR$
$\bullet A1 \boxtimes_C A2 = A2 \boxtimes_C A1$

$\boldsymbol{C\_\sqcap_{C\_refinement\_thm1}}$

$\vdash \forall A1, A2 : CSP\_PROCESS$
$\mid (A1, A2) \in WF\_CSP\_PROCESS\_PAIR$
$\bullet (A1 \sqcap_C A2) \sqsubseteq_R A1 = True_R \varnothing$

$\boldsymbol{C\_\sqcap_{C\_refinement\_thm}}$

$\vdash \forall A1, A2 : CIRCUS\_ACTION$
$\mid (A1, A2) \in WF\_CSP\_PROCESS\_PAIR$
$\bullet (A1 \sqcap_C A2) \sqsubseteq_R A1 = True_R \varnothing$

$\boldsymbol{C\_Stop_C\_\boxtimes_C\_unit\_thm1}$

$\vdash \forall a : ALPHABET; A : CSP\_PROCESS$
$\mid a \in WF\_Skip_C \land a = A.1$
$\bullet Stop\ a \boxtimes_C A = A$

$\boldsymbol{C\_Stop_C\_\boxtimes_C\_unit\_thm}$

$\vdash \forall a : ALPHABET; A : CIRCUS\_ACTION$
$\mid a \in WF\_Skip_C \land a = A.1$

$\bullet\ Stop\ a \boxtimes_C A = A$

$\boldsymbol{C\_\boxtimes_C\_idem\_thm}$

$\vdash \forall A : CSP\_PROCESS \bullet A \boxtimes_C A = A$

$\boldsymbol{C\_Chaos\_alphabet\_thm}$

$\vdash \forall a : ALPHABET \mid a \in WF\_Skip_C \bullet (Chaos\ a).1 = a$

$\boldsymbol{C\_Guard\_\in\_CSP\_PROCESS\_thm}$

$\vdash \forall g : CIRCUS\_CONDITION; A : CSP\_PROCESS$
$\quad \mid (g, A) \in WF\_Guard_C$
$\quad \bullet g \mathbin{\&_C} A \in CSP\_PROCESS$

$\boldsymbol{C\_Guard_C\_\sqcap_{C\_dist\_thm}}$

$\vdash \forall g : CIRCUS\_CONDITION; A1, A2 : CSP\_PROCESS$
$\quad \mid (g, A1) \in WF\_Guard_C \land (g, A2) \in WF\_Guard_C$
$\quad \bullet g \mathbin{\&_C} A1 \sqcap_C A2 = (g \mathbin{\&_C} A1) \sqcap_C g \mathbin{\&_C} A2$

$\boldsymbol{C\_Guard\_\sqcap_C\_elim\_thm}$

$\vdash \forall g : CIRCUS\_CONDITION; A1, A2 : CSP\_PROCESS$
$\quad \mid (A1, A2) \in WF\_CSP\_PROCESS\_PAIR$
$\quad\quad \land (g, A1) \in WF\_Guard_C$
$\quad \bullet (g \mathbin{\&_C} A1 \sqcap_C A2) \sqsubseteq_R g \mathbin{\&_C} A1 = True_R\ \varnothing$

$\boldsymbol{C\_Semi_C\_\sqcap_{C\_left\_dist\_thm}}$

$\vdash \forall A1, A2, A3 : CSP\_PROCESS$
$\quad \mid A1.1 = A2.1 \land A2.1 = A3.1 \land (A1, A2) \in WF\_Semi_C$
$\quad \bullet A1 \mathbin{;_C} A2 \sqcap_C A3 = (A1 \mathbin{;_C} A2) \sqcap_C A1 \mathbin{;_C} A3$

$\boldsymbol{C\_Semi_C\_\sqcap_{C\_left\_dist\_thm1}}$

$\vdash \forall A1, A2, A3 : CIRCUS\_ACTION$
$\quad \mid A1.1 = A2.1 \land A2.1 = A3.1 \land (A1, A2) \in WF\_Semi_C$
$\quad \bullet A1 \mathbin{;_C} A2 \sqcap_C A3 = (A1 \mathbin{;_C} A2) \sqcap_C A1 \mathbin{;_C} A3$

$\boldsymbol{C\_\rightarrow_C\_\sqcap_{C\_dist\_thm}}$

$\vdash \forall a : ALPHABET;$
$\quad\quad n : VAR\_NAME;$
$\quad\quad e : EXPRESSION;$
$\quad\quad A1, A2 : CSP\_PROCESS$
$\quad \mid A1.1 = A2.1 \land ((a, n, e), A1) \in WF\_PREFIXING_C$
$\quad \bullet (a, n, e) \rightarrow_C A1 \sqcap_C A2$
$\quad\quad = ((a, n, e) \rightarrow_C A1) \sqcap_C (a, n, e) \rightarrow_C A2$

$\boldsymbol{C\_\rightarrow_{CSync}\_\sqcap_{C\_dist\_thm}}$

$\vdash \forall a : ALPHABET; n : VAR\_NAME; A1, A2 : CSP\_PROCESS$
$\quad \mid A1.1 = A2.1$
$\quad\quad \land a = A1.1$

$\land\ a \in WF\_Skip_{REA}$
$\land\ FV\ (Val\ Sync) \subseteq a$
$\bullet\ (a, n) \rightarrow_{CSync} A1 \cap_C A2$
$= ((a, n) \rightarrow_{CSync} A1) \cap_C (a, n) \rightarrow_{CSync} A2$

$\boldsymbol{C\_{\rightarrow}_{COut}\_{\cap}_{C\_dist\_thm}}$

$\vdash \forall\ a : ALPHABET;$
$n : VAR\_NAME;$
$e : EXPRESSION;$
$A1, A2 : CSP\_PROCESS$
$\mid A1.1 = A2.1 \land ((a, n, e), A1) \in WF\_PREFIXING_C$
$\bullet\ (a, n, e) \rightarrow_{Cout} A1 \cap_C A2$
$= ((a, n, e) \rightarrow_{Cout} A1) \cap_C (a, n, e) \rightarrow_{Cout} A2$

$\boldsymbol{C\_REA\_PREDICATE\_do\_I\_thm}$

$\vdash \forall\ a : ALPHABET\_REA;$
$c, x : VAR\_NAME;$
$p : CIRCUS\_CONDITION$
$\bullet\ do\_I\ (a, c, x, p) \in REA\_PREDICATE$

$\boldsymbol{C\_REA\_PREDICATE\_do\_I\_alphabet\_thm}$

$\vdash \forall\ a : ALPHABET\_REA;$
$c, x : VAR\_NAME;$
$p : CIRCUS\_CONDITION$
$\bullet\ (do\_I\ (a, c, x, p)).1 = a$

$\boldsymbol{C\_CSP\_PROCESS\_Var_C\_thm}$

$\vdash \forall\ n : VAR\_NAME;\ t : SET\_VAL;\ a : CSP\_PROCESS$
$\mid (n, t, a) \in WF\_Var_C$
$\bullet\ var_C\ (n, t, a) \in CSP\_PROCESS$

$\boldsymbol{C\_CSP\_PROCESS\_Var_C\_alphabet\_thm}$

$\vdash \forall\ n : VAR\_NAME;\ t : SET\_VAL;\ a : CSP\_PROCESS$
$\mid (n, t, a) \in WF\_Var_C$
$\bullet\ (var_C\ (n, t, a)).1$
$= in\_a\ (a.1 \setminus \{n\}) \cup out\_a\ (a.1 \setminus \{dash\ n\})$

$\boldsymbol{C\_CSP\_PROCESS\_PrefixInR_C\_thm}$

$\vdash \forall\ a : ALPHABET\_REA;$
$c : VAR\_NAME;$
$x : VAR\_NAME;$
$p : CIRCUS\_CONDITION;$
$A : CSP\_PROCESS$
$\mid (a, c, x, p, A) \in WF\_PREFIXING_{CinR}$

$\bullet\ (a,\ c,\ x,\ p) \rightarrow_{CinR} A \in CSP\_PROCESS$

$\boldsymbol{C\_CSP\_PROCESS\_PrefixInR_C\_alphabet\_thm}$

$\vdash \forall\ a : ALPHABET\_REA;$
$\quad c : VAR\_NAME;$
$\quad x : VAR\_NAME;$
$\quad p : CIRCUS\_CONDITION;$
$\quad A : CSP\_PROCESS$
$\quad |\ (a,\ c,\ x,\ p,\ A) \in WF\_PREFIXING_{CinR}$
$\quad \bullet\ ((a,\ c,\ x,\ p) \rightarrow_{CinR} A).1$
$\quad = in\_a\ (A.1 \setminus \{x\}) \cup out\_a\ (A.1 \setminus \{dash\ x\})$

$\boldsymbol{C\_\rightarrow_{CinR}\_\cap_C\_dist\_thm}$

$\vdash \forall\ a : ALPHABET\_REA;$
$\quad c,\ x : VAR\_NAME;$
$\quad p : CIRCUS\_CONDITION;$
$\quad A1,\ A2 : CSP\_PROCESS$
$\quad |\ A1.1 = A2.1$
$\quad \wedge (a,\ c,\ x,\ p,\ A1) \in WF\_PREFIXING_{CinR}$
$\quad \bullet\ (a,\ c,\ x,\ p) \rightarrow_{CinR} A1 \cap_C A2$
$\quad = ((a,\ c,\ x,\ p) \rightarrow_{CinR} A1)$
$\qquad \cap_C (a,\ c,\ x,\ p) \rightarrow_{CinR} A2$

$\boldsymbol{C\_\rightarrow_{Cin}\_\cap_C\_dist\_thm}$

$\vdash \forall\ a : ALPHABET\_REA;$
$\quad c,\ x : VAR\_NAME;$
$\quad A1,\ A2 : CSP\_PROCESS$
$\quad |\ \{x,\ dash\ x\} \subseteq a \wedge A1.1 = A2.1 \wedge A1.1 = a$
$\quad \bullet\ (a,\ c,\ x) \rightarrow_{Cin} A1 \cap_C A2$
$\quad = ((a,\ c,\ x) \rightarrow_{Cin} A1) \cap_C (a,\ c,\ x) \rightarrow_{Cin} A2$

$\boldsymbol{C\_Guard\_not\_wait\_diverge\_thm}$

$\vdash \forall\ g : CIRCUS\_CONDITION;\ A : CSP\_PROCESS$
$\quad |\ (g,\ A) \in WF\_Guard_C$
$\quad \bullet\ ((g\ \&_C\ A)\ \omega_f)\ \sigma_f = CSP1\ (g \wedge_R (A\ \omega_f)\ \sigma_f)$

$\boldsymbol{C\_Guard_C\_not\_wait\_converge\_thm}$

$\vdash \forall\ g : CIRCUS\_CONDITION;\ A : CSP\_PROCESS$
$\quad |\ (g,\ A) \in WF\_Guard_C$
$\quad \bullet\ ((g\ \&_C\ A)\ \omega_f)\ \sigma_t$
$\quad = CSP1$
$\qquad (R1$
$\qquad\quad ((g \wedge_R (A\ \omega_f)\ \sigma_t)$

$$
\begin{array}{l}
\quad \vee_R \neg_R\ g \\
\qquad \wedge_R =_R (A.1,\ dash\ tr,\ Var\ tr) \\
\qquad\quad \wedge_R =_R \\
\qquad\qquad (A.1, \\
\qquad\qquad\ \ dash\ wait, \\
\qquad\qquad\ \ Val\ (Bool\ true))))
\end{array}
$$

C_Guard_alphabet_thm

$$
\begin{array}{l}
\vdash \forall\ g : CIRCUS\_CONDITION;\ A : CSP\_PROCESS \\
\quad \mid (g,\ A) \in WF\_Guard_C \\
\quad \bullet (g\ \&_C\ A).1 = A.1
\end{array}
$$

C_Guard$_C$_expansion_thm

$$
\begin{array}{l}
\vdash \forall\ g1,\ g2 : CIRCUS\_CONDITION;\ A : CSP\_PROCESS \\
\quad \mid (g1 \vee_R g2,\ A) \in WF\_Guard_C \wedge g1.1 = g2.1 \\
\quad \bullet (g1 \vee_R g2)\ \&_C\ A = (g1\ \&_C\ A) \boxtimes_C g2\ \&_C\ A
\end{array}
$$

15 INDEX