Semantics and Data Refinement of Invariant Based Programs

Viorel Preoteasa and Ralph-Johan Back

August 28, 2014

Abstract

The invariant based programming is a technique of constructing correct programs by first identifying the basic situations (pre- and post-conditions and invariants) that can occur during the execution of the program, and then defining the transitions and proving that they preserve the invariants. Data refinement is a technique of building correct programs working on concrete datatypes as refinements of more abstract programs. In the theories presented here we formalize the predicate transformer semantics for invariant based programs and their data refinement.

Contents

1 Introduction 2

2 Preliminaries 2
   2.1 Simplification Lemmas 2

3 Program Statements as Predicate Transformers 3
   3.1 Assert statement 3
   3.2 Assume statement 4
   3.3 Demonic update statement 4
   3.4 Angelic update statement 4
   3.5 The guard of a statement 5

4 Hoare Triples 5
   4.1 Hoare rule for recursive statements 7

5 Predicate Transformers Semantics of Invariant Diagrams 8

6 Data Refinement of Diagrams 12
1 Introduction

Invariant based programming \([1, 2, 3, 4]\) is an approach to construct correct programs where we start by identifying all basic situations (pre- and post-conditions, and loop invariants) that could arise during the execution of the algorithm. These situations are determined and described before any code is written. After that, we identify the transitions between the situations, which together determine the flow of control in the program. The transitions are verified at the same time as they are constructed. The correctness of the program is thus established as part of the construction process.

These theories present the predicate transformer semantics for invariant based programs and their data refinement. The complete treatment of the semantics of invariant based programs was presented in \([4]\). There we introduced big and small step semantics, predicate transformer semantics, and we proved complete and correct Hoare rules for invariant based programs. These results were also formalized in the PVS theorem prover. In \([6]\) we have studied data refinement of invariant based programs, and we outlined the steps for proving the Deutsch-Schorr-Waite marking algorithm using data refinement of invariant based programs. These theories represent a mechanical formalization of the data refinement results from \([6]\) and some of the results from \([4]\). In another formalization we will show how the theory presented here can be used in the complete verification of the marking algorithm.

2 Preliminaries

theory Preliminaries
imports Main ../LatticeProperties/Complete-Lattice-Prop
../LatticeProperties/Conj-Disj
begin

notation
  less-eq (infix \(\sqsubseteq\)) and
  less (infix \(\subseteq\)) and
  inf (infixl \(\sqcap\)) and
  sup (infixl \(\sqcup\)) and
  top (\(\top\)) and
  bot (\(\bot\)) and
  Inf (\([\sqcap]\) [900] 900) and
  Sup (\([\sqcup]\) [900] 900)

2.1 Simplification Lemmas

declare fun-upd-idem[simp]

lemma simp-eq-emptyset:
(X = {}) = (∀ x. x /∈ X)
⟨proof⟩

lemma mono-comp: mono f ⇒ mono g ⇒ mono (f o g)
⟨proof⟩

Some lattice simplification rules

lemma inf-bot-bot:
(x::′a::{semilattice-inf,order-bot}) ∩ ⊥ = ⊥
⟨proof⟩

eend

3 Program Statements as Predicate Transformers

theory Statements
imports Preliminaries
begin

Program statements are modeled as predicate transformers, functions from predicates to predicates. If State is the type of program states, then a program S is a a function from State set to State set. If q ∈ State set, then the elements of S q are the initial states from which S is guarantied to terminate in a state from q.

However, most of the time we will work with an arbitrary compleate lattice, or an arbitrary boolean algebra instead of the complete boolean algebra of predicate transformers.

We will introduce in this section assert, assume, demonic choice, angelic choice, demonic update, and angelic update statements. We will prove also that these statements are monotonic.

lemma mono-top[simp]: mono top
⟨proof⟩

lemma mono-choice[simp]: mono S ⇒ mono T ⇒ mono (S ∩ T)
⟨proof⟩

3.1 Assert statement

The assert statement of a predicate p when executed from a state s fails if s /∈ p and behaves as skip otherwise.

definition
assert::′a::semilattice-inf ⇒ 'a ⇒ 'a ({. .} [0] 1000) where
{.p.} q ≡ p ∩ q

lemma mono-assert [simp]: mono {.p.}
⟨proof⟩
3.2 Assume statement

The assume statement of a predicate \( p \) when executed from a state \( s \) is not enabled if \( s \not\in p \) and behaves as skip otherwise.

**definition**

\[
\text{assume} :: \text{'}a::\text{boolean-algebra} \Rightarrow \text{'}a \Rightarrow \text{'}a ([. -. . [0] 1000) where
\]

\[
[. p .] q \equiv -p \sqcup q
\]

**lemma** mono-assume [simp]: mono (assume \( P \))

(\text{proof})

3.3 Demonic update statement

The demonic update statement of a relation \( Q : \text{State} \rightarrow \text{State} \rightarrow \text{bool} \), when executed in a state \( s \) computes nondeterministically a new state \( s' \) such \( Q s s' \) is true. In order for this statement to be correct all possible choices of \( s' \) should be correct. If there is no state \( s' \) such that \( Q s s' \), then the demonic update of \( Q \) is not enabled in \( s \).

**definition**

\[
\text{demonic} :: (\text{'}a::\text{ord}) \Rightarrow \text{'}b::\text{ord} \Rightarrow \text{'}a \rightarrow \text{set} ([. -. . [0] 1000) where
\]

\[
[Q] p = \{ s : Q s \leq p \}
\]

**lemma** mono-demonic [simp]: mono [:\( Q :\) ]

(\text{proof})

**theorem** demonic-bottom:

\[
[\bot] ([\bot::\text{order-bot}]) = \{ s : (R s) = \bot \}
\]

(\text{proof})

**theorem** demonic-bottom-top [simp]:

\[
[\bot::\text{order-bot}] = \top
\]

(\text{proof})

**theorem** demonic-sup-inf:

\[
[Q \sqcup Q'] = [Q] \cap [Q']
\]

(\text{proof})

3.4 Angelic update statement

The angelic update statement of a relation \( Q : \text{State} \rightarrow \text{State} \rightarrow \text{bool} \) is similar to the demonic version, except that it is enough that at least for one choice \( s' \), \( Q s s' \) is correct. If there is no state \( s' \) such that \( Q s s' \), then the angelic update of \( Q \) fails in \( s \).

**definition**

\[
\text{angelic} :: (\text{'}a \Rightarrow \text{'}b::\text{ord}) \Rightarrow \text{'}b::\text{ord} \Rightarrow \text{'}a \rightarrow \text{set} ([. -. . [0] 1000) where
\]

\[
([. -. . [0] 1000)
\]

(\text{proof})
\{ Q : p = \{ s . (Q s) \cap p \neq \bot \} \}

**Syntax**

- **update** :: **patterns** => **patterns** => **logic** => **logic** (¬ ∼ - . - 0)

**Translations**

- update (patterns x xs) (patterns y ys) t \(\cong\) CONST id (abs (pattern x xs) (Coll (pattern y ys) t))
- update x y t \(\cong\) CONST id (abs x (Coll y t))

**Theorem angelic-bottom** [simp]:

angelic R ⊥ \(\cong\) \{ \}

**proof**

**Theorem angelic-disjunctive** [simp]:

\{:(R:(a ⇒ b::complete-distrib-lattice)):\} \(\in\) Apply.Disjunctive

**proof**

3.5 The guard of a statement

The guard of a statement S is the set of initial states from which S is enabled or fails.

**Definition**

\((\text{grd } S) :\cdot :\cdot :\cdot :\text{boolean-algebra}) = (S \bot)

**Lemma grd-choice** [simp]:

\(\text{grd } (S \cap T) = (\text{grd } S) \cup (\text{grd } T)\)

**proof**

**Lemma grd-demonic**:

\(\text{grd }[:\text{Q}:] = \{ s \cdot \exists s'. s' \in (Q s) \}\)

**proof**

**Lemma grd-demonic-2** [simp]:

\(\{ s \notin (\text{grd }[:\text{Q}:]) \} = (\forall s'. s' \notin (Q s))\)

**proof**

**Theorem grd-angelic**:

\(\text{grd }[:R:] = \text{UNIV}\)

**proof**

end

4 Hoare Triples

**Theory Hoare**

**Imports** Statements

**Begin**

A hoare triple for p, q ∈ State set, and S : State set → State set is valid, denoted \(\models p\{S\}q\), if every execution of S starting from state s ∈ p always
terminates, and if it terminates in state $s'$, then $s' \in q$. When $S$ is modeled as a predicate transformer, this definition is equivalent to requiring that $p$ is a subset of the initial states from which the execution of $S$ is guaranteed to terminate in $q$, that is $p \subseteq S q$.

The formal definition of a valid hoare triple only assumes that $p$ (and also $S q$) ranges over a complete lattice.

definition

Hoare ::= 'a::complete-distrib-lattice ⇒ ('b ⇒ 'a) ⇒ 'b ⇒ bool ($[|=\{ |-\}|(-)$ $[0,0,900] 900$) where

$[|= p \{ |S| \} q = (p \leq (S q))$

theorem hoare-sequential:

$\text{mono } S \implies ([|= p \{ |S \circ T| \} r) = (\exists q. [|= p \{ |S| \} q \land [|= q \{ |T| \} r))$

(\text{proof})

theorem hoare-choice:

$[|= p \{ |S \cap T| \} q = ([|= p \{ |S| \} q \land [|= p \{ |T| \} q)$

(\text{proof})

theorem hoare-assume:

$([|= P \{ |[R.|]| \} Q) = (P \cap R \leq Q)$

(\text{proof})

theorem hoare-mono:

$\text{mono } S \implies Q \leq R \implies [|= P \{ |S| \} Q \implies [|= P \{ |S| \} R$

(\text{proof})

theorem hoare-pre:

$R \leq P \implies [|= P \{ |S| \} Q \implies [|= R \{ |S| \} Q$

(\text{proof})

theorem hoare-Sup:

$(\forall p \in P . [|= p \{ |S| \} q) = [|= \text{Sup } P \{ |S| \} q$

(\text{proof})

lemma hoare-magic [simp]: $[|= P \{ |\top| \} Q$

(\text{proof})

lemma hoare-demonic: $[|= P \{ |:R:| \} Q = (\forall s . s \in P \rightarrow R s \subseteq Q)$

(\text{proof})

lemma hoare-not-guard:

$\text{mono } (S :: (-::order-bot) \Rightarrow -) \Rightarrow [|= p \{ |S| \} q = [|= (p \cup (- \text{grd } S)) \{ |S| \} q$

(\text{proof})
4.1 Hoare rule for recursive statements

A statement $S$ is refined by another statement $S'$ if $\models p\{S\} q$ is true for all $p$ and $q$ such that $\models p\{S\} q$ is true. This is equivalent to $S \leq S'$.

Next theorem can be used to prove refinement of a recursive program. A recursive program is modeled as the least fixpoint of a monotonic mapping from predicate transformers to predicate transformers.

**Theorem lfp-ufl-induction:**

$\text{mono } f \Rightarrow (\forall w . (p w) \leq f (\text{Sup-less } p w)) \Rightarrow \text{Sup (range } p) \leq \text{lfp } f$

**Definition post-fun** ($p::'a::\text{order}$) $q = (\text{if } p \leq q \text{ then } \top \text{ else } \bot)$

**Lemma post-mono** [simp]: $\text{mono } (\text{post-fun } p :: (\_\_\_\_::\{\text{order-bot,order-top}\}))$

**Lemma post-top** [simp]: $\text{post-fun } p \, p = \top$

**Lemma post-refin** [simp]: $\text{mono } S \Rightarrow ((S \, p)::'a::\text{bounded-lattice}) \cap (\text{post-fun } p) \, x \leq S \, x$

Next theorem shows the equivalence between the validity of Hoare triples and refinement statements. This theorem together with the theorem for refinement of recursive programs will be used to prove a Hoare rule for recursive programs.

**Theorem hoare-refinement-post:**

$\text{mono } f \Rightarrow (\models x \{f\} y = (\{x\} o (\text{post-fun } y) \leq f)$

Next theorem gives a Hoare rule for recursive programs. If we can prove correct the unfolding of the recursive definition applied to a program $f$, $\models p \, w \{F \, f\} y$, assuming that $f$ is correct when starting from $p \, v$, $v \leq w$, $\models \text{SUP - L } p \, w \{f\} \, y$, then the recursive program is correct $\models \text{SUP } p \{\text{lfp } F\} \, y$

**Lemma assert-Sup**: $\bigcup (X::'a::\text{complete-distrib-lattice set}). = \bigcup (\text{assert } ' X)$

**Lemma assert-Sup-range**: $\bigcup (\text{range } (p::'W \Rightarrow 'a::\text{complete-distrib-lattice})). = \bigcup (\text{range } (\text{assert } o p))$

**Lemma Sup-range-comp**: $\bigcup \text{range } p \, o \, S = \bigcup \text{range } (\lambda w . ((p \, w) \, o \, S))$

7
lemma Sup-less-comp: (Sup-less P) w o S = Sup-less (λ w . ((P w) o S)) w
⟨proof⟩

lemma Sup-less-assert: Sup-less (λw. (. (p w)::complete-distrib-lattice .)) w = {Sup-less p w.}
⟨proof⟩

declare mono-comp[simp]

theorem hoare-fixpoint:
mono-mono F ⇒
(!! w f . mono f ∧ |= Sup-less p w {} f y ⇒|= p w {} F f y) ⇒|= (Sup (range p)) {} lfp F {} y
⟨proof⟩

theorem (∀ t . |= ((s . t ∈ R s}) {[S]} q) ⇒|= ((:R:) p) {[S]} q
⟨proof⟩
end

5 Predicate Transformers Semantics of Invariant Diagrams

theory Diagram
imports Hoare
begin

This theory introduces the concept of a transition diagram and proves a number of Hoare total correctness rules for these diagrams. As before the diagrams are introduced using their predicate transformer semantics.

A transition diagram $D$ is a function from pairs of indexes to predicate transformers: $D : I \times I \rightarrow (\text{State set} \rightarrow \text{State set})$, or more general $D : I \times I \rightarrow \text{Ptran}$, where $\text{Ptran}$ is a complete lattice. The elements of $I$ are called situations and intuitively a diagram is executed starting in a situation $i \in I$ by choosing a transition $D(i,j)$ which is enabled and continuing similarly from $j$ if there are enabled transitions. The execution of a diagram stops when there are no more transitions enabled or when it fails.

The semantics of a transition diagram is an indexed predicate transformer $(I \rightarrow \text{State set})$. If $Q : I \rightarrow \text{State set}$ is an indexed predicate, then $p = pt D Q i$ is a weakest predicate such that if the execution of $D$ starts in a state $s \in p$ from situation $i$, then it terminates, and if it terminates in situation $j$ and state $s'$, then $s' \in Q j$.

We introduce first the indexed predicate transformer $\text{step} D$ of executing one step of diagram $D$. The predicate $\text{step} D Q i$ is true for those states $s$ from which the execution of one step of $D$ starting in situation $i$ ends in
one of the situations \( j \) such that \( Q_j \) is true.

**Definition**

\[
\text{step } D \ i j = (\text{INF } j . \ D (i, j) \ (Q j)) :: - :: \text{complete-lattice}
\]

**Definition**

\[
dmono D = (\forall \ ij . \ mono \ (D ij))
\]

**Lemma**

\[
dmono-mono [simp]: \ dmono D \implies \ mono \ (D ij)
\]

**Theorem**

\[
\text{mono-step [simp]:} \quad \ dmono D \implies \ mono \ (\text{step } D)
\]

The indexed predicate transformer of a transition diagram is defined as the least fixpoint of the unfolding of the execution of the diagram. The indexed predicate transformer \( dgr D U \) is the choice between executing one step of \( D \) followed by \( U \) \((\text{step } D) \circ U\) or skip if no transition of \( D \) is enabled (assume \( \neg \text{grd} \ (\text{step } D) \)).

**Definition**

\[
dgr D U = ((\text{step } D) \circ U) \sqcap [- \text{(grd} \ (\text{step } D))].
\]

**Theorem**

\[
\text{mono-mono-dgr [simp]:} \quad \ dmono D \implies \ mono \text{-mono} \ (dgr D)
\]

**Definition**

\[
pt D = \text{lfp} \ (dgr D)
\]

If \( U \) is an indexed predicate transformer and if \( P, Q : I \rightarrow \text{State set} \) are indexed predicates, then the meaning of the Hoare triple defined earlier, \( \models P \{U\} Q \), is that if we start \( U \) in a state \( s \) from a situation \( i \) such that \( s \in P i \), then \( U \) terminates, and if it terminates in \( s' \) and situation \( j \), then \( s' \in Q j \) is true.

Next theorem shows that in a diagram all transitions are correct if and only if \( \text{step } D \) is correct.

**Theorem**

\[
\text{hoare-step:} \quad (\forall \ i j . \models (P i) \{\ D(i,j) \} \ (Q j) ) = (\models P \{\ step D \} \ Q)
\]

Next theorem provides the first proof rule for total correctness of transition diagrams. If all transitions are correct and if a global variant decreases on every transition then the diagram is correct and it terminates. The variant must decrease according to a well founded and transitive relation.

**Theorem**

\[
\text{hoare-diagram:} \quad dmono D \implies (\forall \ w i j . \models X w i \{\ D(i,j) \} \text{Sup-less} \ X w j) \implies
\models (\text{Sup} \ (\text{range } X)) \{\ pt D \} \ (\text{Sup} \ (\text{range } X) \sqcap \neg \text{(grd} \ (\text{step } D))]
\]
This theorem is a more general form of the more familiar form with a variant \( t \) which must decrease. If we take \( X \) \( w_i = (Y_i \land t_i = w) \), then the second hypothesis of the theorem above becomes \( \Rightarrow Y_i \land t_i = w \{ D(i,j) \} \) \( Y_i \land t_i < w \). However, the more general form of the theorem is needed, because in data refinements, the form \( Y_i \land t_i = w \) cannot be preserved.

The drawback of this theorem is that the variant must be decreased on every transition which may be too cumbersome for practical applications. A similar situation occur when introducing proof rules for mutually recursive procedures. There the straightforward generalization of the proof rule of a recursive procedure to mutually recursive procedures suffers of a similar problem. We would need to prove that the variant decreases before every recursive call. Nipkow [5] has introduced a rule for mutually recursive procedures in which the variant is required to decrease only in a sequence of recursive calls before calling again a procedure in this sequence. We introduce a similar proof rule in which the variant depends also on the situation indexes.

locale DiagramTermination =
  fixes pair:: 'a ⇒ 'b ⇒ ('c::well-founded-transitive)
begin

definition
  SUP-L-P \( X \) \( u_i \) = \( (SUP \ v. \ \text{pair } v \ i < u) \). \( X \ v \ i :: - :: \text{complete-lattice} \)

definition
  SUP-LE-P \( X \) \( u_i \) = \( (SUP \ v. \ \text{pair } v \ i \leq u) \). \( X \ v \ i :: - :: \text{complete-lattice} \)

lemma SUP-L-P-upper:
  \( \text{pair } v \ i < u \Rightarrow P \ v \ i \leq \text{SUP-L-P } P \ u \ i \)
  ⟨proof⟩

lemma SUP-L-P-least:
  \( \text{pair } v \ i < u \Rightarrow P \ v \ i \leq Q \) \( \Rightarrow \text{SUP-L-P } P \ u \ i \leq Q \)
  ⟨proof⟩

lemma SUP-LE-P-upper:
  \( \text{pair } v \ i \leq u \Rightarrow P \ v \ i \leq \text{SUP-LE-P } P \ u \ i \)
  ⟨proof⟩

lemma SUP-LE-P-least:
  \( \text{pair } v \ i \leq u \Rightarrow P \ v \ i \leq Q \) \( \Rightarrow \text{SUP-LE-P } P \ u \ i \leq Q \)
  ⟨proof⟩

lemma SUP-SUP-L [simp]: \( \text{Sup } (\text{range } (\text{SUP-LE-P } X)) = \text{Sup } (\text{range } X) \)
  ⟨proof⟩
**lemma** SUP-L-SUP-LE-P [simp]: Sup-less (SUP-LE-P X) = SUP-L-P X

⟨proof⟩

end

**theorem** (in DiagramTermination) hoare-diagram2:

\[ \text{dmono } D \implies (\forall u i j . \models X u i \{ \mid D(i, j) \}) \implies \]
\[ \models (\text{Sup (range } X)) \{ \mid pt \ D \} ((\text{Sup (range } X)) \cap (-(\text{grd (step } D)))) \]

⟨proof⟩

**lemma** mono-pt [simp]: dmono D \implies mono (pt D)

⟨proof⟩

**theorem** (in DiagramTermination) hoare-diagram3:

\[ \text{dmono } D \implies \]
\[ (\forall u i j . \models X u i \{ \mid D(i, j) \}) \implies\]
\[ P \leq \text{Sup (range } X) \implies ((\text{Sup (range } X)) \cap (-(\text{grd (step } D)))) \leq Q \implies\]
\[ \models P \{ \mid pt \ D \} Q \]

⟨proof⟩

The following definition introduces the concept of correct Hoare triples for diagrams.

**definition** (in DiagramTermination)

\[ \text{Hoare-dgr :: ('b \Rightarrow ('u::{complete-distrib-lattice, boolean-algebra}))) \Rightarrow ('b \times 'b \Rightarrow 'u \Rightarrow 'u) \Rightarrow ('b \Rightarrow 'u) \Rightarrow bool \{ (\neg)\{ \neg \}\{ \neg \}\}
\]
\[ [0,0,900,900] \]

where

\[ \models P \{ \mid D \} Q \equiv (\exists X . (\forall u i j . \models X u i \{ \mid D(i, j) \}) \implies\]
\[ P \leq \text{Sup (range } X) \land Q = ((\text{Sup (range } X)) \cap (-(\text{grd (step } D)))) \]

**definition** (in DiagramTermination)

\[ \text{Hoare-dgr1 :: ('b \Rightarrow ('u::{complete-distrib-lattice, boolean-algebra}))) \Rightarrow ('b \times 'b \Rightarrow 'u \Rightarrow 'u) \Rightarrow ('b \Rightarrow 'u) \Rightarrow bool \{ (\neg)\{ \neg \}\{ \neg \}\}
\]
\[ [0,0,900,900] \]

where

\[ \models P \{ \mid D \} Q \equiv (\exists X . (\forall u i j . \models X u i \{ \mid D(i, j) \}) \implies\]
\[ P \leq \text{Sup (range } X) \land ((\text{Sup (range } X)) \cap (-(\text{grd (step } D)))) \leq Q \]

**theorem** (in DiagramTermination) hoare-dgr-correctness:

\[ \text{dmono } D \implies (\models P \{ \mid D \} Q) \implies (\models P \{ \mid pt \ D \} Q) \]

⟨proof⟩

**theorem** (in DiagramTermination) hoare-dgr-correctness1:

\[ \text{dmono } D \implies (\models P \{ \mid D \} Q) \implies (\models P \{ \mid pt \ D \} Q) \]

⟨proof⟩

**definition**

dgr-demonic Q \( ij = [\: Q \ ij :] \)
**6 Data Refinement of Diagrams**

theory DataRefinement
imports Diagram
begin

Next definition introduces the concept of data refinement of $S_1$ to $S_2$ using the data abstractions $R$ and $R'$.

**definition**

$DataRefinement :: \langle 'a\cdot\text{type} \Rightarrow 'b\cdot\text{type} \rangle$
\[ \Rightarrow \langle 'b\cdot\text{type} \Rightarrow 'c\cdot\text{ord} \rangle \Rightarrow \langle 'a\cdot\text{type} \Rightarrow 'd\cdot\text{type} \rangle \Rightarrow \langle 'd\cdot\text{type} \Rightarrow 'c\cdot\text{ord} \rangle \Rightarrow \text{bool} \]
\[ DataRefinement S1 R R' S2 = ((R \circ S1) \leq (S2 \circ R')) \]

If demonic $Q$ is correct with respect to $p$ and $q$, and $(\text{assert } p) \circ (\text{demonic } Q)$ is data refined by $S$, then $S$ is correct with respect to angelic $R \ p$ and angelic $R' \ q$.

**theorem** data-refinement:
\[ \text{mono } R \implies \models \ p \ \{ | S | \} \ q \implies DataRefinement \ S \ R \ R' \ S' \implies \]
\[ \models \ (R \ p) \ \{ | S' | \} \ (R' \ q) \]
\[ \langle \text{proof} \rangle \]

**theorem** data-refinement2:
\[ \text{mono } R \implies \models \ p \ \{ | S | \} \ q \implies DataRefinement \ (\{ p \} \ o S) \ R \ R' \ S' \implies \]
\[ \vdash (R \circ p) \{ | S' | \} (R' \circ q) \]

**Theorem** data-refinement-hoare:

\[ \text{mono } S \implies \text{ mono } D \implies \text{ DataRefinement } ((\circ p \circ (\cdot S;)) \{ :R; \} ) D S = \]
\[ (\forall s . : | s' . s \in R s' \land s \in p \} \{ | S | \} (D ((Q s); 'a::order))) \]

**Proof**

**Theorem** data-refinement-choice1:

\[ \text{DataRefinement } S_1 D D' S_2 \implies \text{ DataRefinement } S_1 D D' S_2' \implies \text{ DataRefinement } (S_1 \cap S_1') D D' (S_2 \cap S_2') \]

**Proof**

**Theorem** data-refinement-choice2:

\[ \text{mono } D \implies \text{ DataRefinement } S_1 D D' S_2 \implies \text{ DataRefinement } S_1' D D' S_2' \implies \text{ DataRefinement } (S_1 \cap S_1') D D' (S_2 \cap S_2') \]

**Proof**

**Theorem** data-refinement-top [simp]:

\[ \text{DataRefinement } S_1 D D' (\top \cdot : :: \cdot \text{order-top}) \]

**Proof**

**Definition** apply-fun::('a::'b) => 'a::'c (infixl 5) where

\[ (A \cdot B) = (\lambda x . (A x) (B x)) \]

**Definition**

\[ \text{Disjunctive-fun } R = (\forall i . (R i) \in \text{Apply. Disjunctive}) \]

**Lemma** Disjunctive-Sup:

\[ \text{Disjunctive-fun } R \implies (R \cdot (\text{Sup } X)) = \text{ Sup } \{ y . \exists x \in X . y = (R \cdot x) \} \]

**Proof**

**Lemma** (in DiagramTermination) disjunctive-SUP-L-P:

\[ \text{Disjunctive-fun } R \implies (R \cdot (\text{SUP-L-P } (\langle P w \rangle))) (\langle P w \rangle)) (\langle P u i \rangle) \]

**Proof**

**Lemma** apply-fun-range: \[ \{ y . \exists x . y = (R \cdot P x) \} = \text{ range } (\lambda x . R \cdot P x) \]

**Proof**

**Lemma** simp: \[ \text{Disjunctive-fun } R \implies \text{ mono } ((R i) :: 'a::complete-lattice \Rightarrow 'b::complete-lattice) \]

**Proof**

**Theorem** (in DiagramTermination) dgr-data-refinement-1:

\[ \text{dmono } D' \Rightarrow \text{ Disjunctive-fun } R \Rightarrow \]
\[ (\forall w i j . : P w i \{ | D (i, j) | \} \text{ SUP-L-P } (\langle P w \rangle) j) \]

13
∀ w i j . DataRefinement ((assert (P w i)) o (D (i,j))) (R i) (R j) (D' (i, j)))

⇒ (R .. (Sup (range P))) \{ | pt D' | \} ((R .. (Sup (range P))) \cap (-(grd (step D')))))

\langle proof \rangle

**definition**
\[ DgrDataRefinement1 D R D' = (\forall i j . DataRefinement (D (i , j)) (R i) (R j) (D' (i, j))) \]

**definition**
\[ DgrDataRefinement2 P D R D' = (\forall i j . DataRefinement \{(P i \} o D (i , j)) (R i) (R j) (D' (i, j))) \]

**theorem** DataRefinement-mono:
\[ T \leq S \implies mono R \implies DataRefinement S R R' S' \implies DataRefinement T R R' S' \]

\langle proof \rangle

**definition**
\[ mono-fun R = (\forall i . mono (R i)) \]

**theorem** DgrDataRefinement-mono:
\[ Q \leq P \implies mono-fun R \implies DgrDataRefinement2 P D R D' \implies DgrDataRefinement2 Q D R D' \]

\langle proof \rangle

Next theorem is the diagram version of the data refinement theorem. If the diagram demonic choice T is correct, and it is refined by D, then D is also correct. One important point in this theorem is that if the diagram demonic choice T terminates, then D also terminates.

**theorem** (in DiagramTermination) Diagram-DataRefinement1:
\[ dmono D \implies Disjunctive-fun R \implies DgrDataRefinement1 D R D' \implies DgrDataRefinement1 D R D' \implies \]

\[ \vdash (R .. P) \{ | D' | \} ((R .. P) \cap (-(grd (step D'))))) \]

\langle proof \rangle

**lemma** comp-left-mono [simp]: \[ S \leq S' \implies S o T \leq S' o T \]

\langle proof \rangle

**lemma** assert-pred-mono [simp]: \[ p \leq q \implies \{ .p. \} \leq \{ .q. \} \]

\langle proof \rangle

**theorem** (in DiagramTermination) Diagram-DataRefinement2:
\[ dmono D \implies Disjunctive-fun R \implies DgrDataRefinement2 P D R D' \implies DgrDataRefinement2 P D R D' \implies \]

\[ \vdash (R .. P) \{ | D' | \} ((R .. P) \cap (-(grd (step D'))))) \]

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

\textbf{lemma} \ (R\ ':\ 'a::complete-lattice \Rightarrow \ 'b::complete-lattice) \in \text{Apply.Disjunctive} \Rightarrow 
\text{DataRefinement} \ S \ R \ R' \ S' \Rightarrow \ R \ (\neg \text{grd} \ S) \leq \neg \text{grd} \ S'

\[\text{proof}\]

\textbf{end}

\textbf{References}


