Semantics and Data Refinement of Invariant Based Programs

Viorel Preoteasa and Ralph-Johan Back

May 27, 2015

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 5
3.5 The guard of a statement 5
4 Hoare Triples 6
4.1 Hoare rule for recursive statements 7
5 Predicate Transformers Semantics of Invariant Diagrams 9
6 Data Refinement of Diagrams 15
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 50) and
  less (infix \sqsubseteq 50) and
  inf (infixl \cap 70) and
  sup (infixl \cup 65) and
  top (\top) and
  bot (\bot) and
  Inf (\cap - [900] 900) and
  Sup (\cup - [900] 900)

2.1 Simplification Lemmas

declare fun-upd-idem[simp]

lemma simp-eq-emptyset:

}\n
\((X = \{}\) = (\forall x. x \notin X)\)

by blast

**lemma** mono-comp: mono \(f \implies \text{mono } g \implies \text{mono } (f \circ g)\)

by (unfold mono-def) auto

Some lattice simplification rules

**lemma** inf-bot-bot:

\((x :: 'a :: \text{semilattice-inf}, \text{order-bot})) \sqcap \bot = \bot\)

apply (rule antisym)

by auto

end

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 function from \(State\) to \(State\). If \(q \in State\), then the elements of \(S q\) are the initial states from which \(S\) is guaranteed to terminate in a state from \(q\).

However, most of the time we will work with an arbitrary complete 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

by (simp add: mono-def top-fun-def)

**lemma** mono-choice[simp]: mono \(S \implies \text{mono } T \implies \text{mono } (S \sqcap T)\)

apply (simp add: mono-def inf-fun-def)

apply safe

apply (rule-tac y = \(S\) \(x\) in order-trans)

apply simp-all

apply (rule-tac y = \(T\) \(x\) in order-trans)

by simp-all

3.1 Assert statement

The assert statement of a predicate \(p\) when executed from a state \(s\) fails if \(s \notin p\) 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.}
apply (simp add: assert-def mono-def, safe)
apply (rule-tac y = x in order-trans)
by simp-all

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
assume :: 'a::boolean-algebra ⇒ 'a ⇒ 'a ([. . ] [0] 1000) where
[. p .] q ≡ ¬p ⊔ q

lemma mono-assume [simp]: mono (assume P)
apply (simp add: assume-def mono-def)
apply safe
apply (rule-tac y = y in order-trans)
by simp-all

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
demonic :: ('a ⇒ 'b::ord) ⇒ 'b::ord ⇒ 'a set ([. . ] [0] 1000) where
[:Q:] p = \{ s \mid Q s \leq p \}

lemma mono-demonic [simp]: mono [:Q:]
apply (simp add: mono-defemonic-def)
by auto

theorem demonic-bottom:
[:R:] (⊥::('a::order-bot)) = \{ s \mid (R s) = ⊥ \}
apply (unfold demonic-def, safe, simp-all)
apply (rule antisym)
by auto

theorem demonic-bottom-top [simp]:
[:⊥::order-bot:] = ⊤
by (simp add: fun-eq-iff inf-fun-def sup-fun-def demonic-def top-fun-def bot-fun-def)

**Theorem 3.4 Angelic update statement**

The angelic update statement of a relation \( Q : \text{State} \to \text{State} \to \text{bool} \) 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**

\[
\text{angelic} :: (\forall a : \text{a} \Rightarrow b : \text{b} : \text{semilattice-inf, order-bot}) \Rightarrow \text{a} \Rightarrow \text{b} :: \{\text{semilattice-inf, order-bot}\}
\]

**Syntax**

\[
\text{update} :: \text{patterns} \Rightarrow \text{patterns} \Rightarrow \text{logic} \Rightarrow \text{logic} (\rightarrow \rightarrow \rightarrow 0)
\]

**Translations**

\[
\text{update} (\text{patterns} x xs) (\text{patterns} y ys) t == \text{CONST \text{id}} (\text{-abs (pattern} x xs) (-\text{Coll (pattern} y ys) t))
\]

**Term**

\[
\{ : y, z \rightarrow x, z'. P x y z z' : \}
\]

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

\[
\text{angelic } R \bot = \{\}
\]

by (simp add: angelic-def inf-bot-bot)

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

\[
\{ :(R:\forall a : \text{a} : \text{complete-distrib-lattice}) : \} \in \text{Apply.Disjunctive}
\]

by (simp add: Apply.Disjunctive-def angelic-def inf-Sup, blast)

**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**

\[
((\text{grd } S) :\forall a : \text{boolean-algebra}) = -(S \text{ bot})
\]

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

\[
\text{grd}(S \sqcap T) = (\text{grd } S) \sqcup (\text{grd } T)
\]

by (simp add: grd-def inf-fun-def)

**Lemma grd-demonic:**

\[
\{[Q] \} = \{ s . \exists s'. s' \in (Q s) \}
\]

apply (simp add: grd-def demonic-def)

by blast

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

\[
(s \notin \text{grd} \{[Q] \}) = (\forall s'. s' \notin (Q s))
\]
by (simp add: grd-demonic)

theorem grd-angelic:
  \( \text{grd} \{; R;\} = \text{UNIV} \)
by (simp add: grd-def)
end

4 Hoare Triples

theory Hoare
imports Statements
begin

A hoare triple for \( p, q \in \text{State set} \), and \( S : \text{State set} \rightarrow \text{State set} \) is valid, denoted \( \models p \{S\} q \), if every execution of \( S \) starting from state \( s \in p \) 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 \Rightarrow '('b \Rightarrow 'a \Rightarrow 'b \Rightarrow bool \ (\models (-)[| - |])(-))\ [0,0,900] 900) where
                      \( \models p \{S\} q = (p \leq (S q)) \)

theorem hoare-sequential:
  \( \text{mono} \ S \Longrightarrow (\models p \{S o T\} r) = ((\exists \ q. \ (\models p \{S\} q) \land (\models q \{T\} r))) \)
by (metis (no-types) Hoare-def monoD o-def order-refl order-trans)

theorem hoare-choice:
  \( \models p \{S \cap T\} q = ((\models p \{S\} q \land (\models p \{T\} q)) \)
by (simp-all add: Hoare-def inf-fun-def)

theorem hoare-assume:
  \( (\models P \{\ldots R \ldots\} Q) = (P \cap R \leq Q) \)
apply (simp add: Hoare-def assume-def)
apply safe
apply (case-tac (inf P R) \leq (inf (sup (\ldots R \ldots) Q) R))
apply (simp add: inf-sup-distrib2)
apply (simp add: le-infI1)
apply (case-tac (sup (\ldots R \ldots) (inf P R)) \leq sup (\ldots R \ldots) Q)
apply (simp add: sup-inf-distrib1)
by (simp add: le-supI2)

theorem hoare-mono:
  \( \text{mono} \ S \Longrightarrow Q \leq R \Longrightarrow (\models P \{S\} Q) \Longrightarrow (\models P \{S\} R) \)
apply (simp add: mono-def Hoare-def)
apply (rule-tac y = S Q in order-trans)
by auto

theorem hoare-pre:
\[ R \leq P \implies \vdash P \{S\} Q \implies \vdash R \{S\} Q \]
by (simp add: Hoare-def)

theorem hoare-Sup:
\[ (\forall p \in P . \vdash p \{S\} q) = \vdash \Sup P \{S\} q \]
apply (simp add: Hoare-def, safe, simp add: Sup-least)
apply (rule-tac y = \big\{P\big\} in order-trans, simp-all)
by (simp add: Sup-upper)

lemma hoare-magic [simp]:
\[ \vdash P \{T\} Q \]
by (simp add: Hoare-def top-fun-def)

lemma hoare-demonic:
\[ \vdash P \{R\} Q = (\forall s . s \in P \implies R s \subseteq Q) \]
apply (unfold Hoare-def demonic-def)
by auto

lemma hoare-not-guard:
mono (S :: (\_::order-bot) \Rightarrow _) \implies \vdash p \{S\} q = \vdash (p \cup (- \text{ grd } S)) \{S\} q
apply (simp add: Hoare-def grd-def, safe)
apply (drule monoD)
by auto

4.1 Hoare rule for recursive statements

A statement \( S \) is refined by another statement \( S' \) if \( \vdash p\{S'\}q \) is true for all \( p \) and \( q \) such that \( \vdash p\{S\}q \) 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-wf-induction:
mono f \implies (\forall w . (p w) \leq f (\text{Sup-less } p w)) \implies \Sup (\text{range } p) \leq \text{lfp } f
apply (rule fp-wf-induction, simp-all)
by (drule lfp-unfold, simp)

definition post-fun (p::a::order) q = (if p \leq q then \top else \bot)

lemma post-mono [simp]: mono (post-fun p :: (\_::(order-bot,order-top)))
apply (simp add: post-fun-def mono-def, safe)
apply (subgoal-tac p \leq y, simp)
by (rule-tac y = x in order-trans, simp-all)

lemma post-top [simp]: post-fun p p = \top
by (simp add: post-fun-def)

**lemma** post-refin [simp]: mono $S \Rightarrow ((S p)::'a::bounded-lattice) \sqcap (post-fun p) x \leq S x$

apply (simp add: le-fun-def post-fun-def, safe)
by (rule-tac $f = S$ in monoD, simp-all)

Next theorem gives a Hoare rule for recursive programs. If we can prove

**Sup-less-comp** lemma

$v < w$ \iff \Sup p w = \bigvee (\lambda f. f x) \sqcap \post-fun y xa \in \text{order-trans, simp-all}

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:

mono $f \Rightarrow (\vdash x \{ f \} y) = (\{ x. \} o (post-fun y) \leq f) \equiv$

safe

apply (simp-all add: Hoare-def)
apply (simp-all add: le-fun-def)
apply (simp add: assert-def, safe)
apply (rule-tac $y = f y \sqcap \post-fun y xa \in \text{order-trans, simp-all})$
apply (rule-tac $y = x \in \text{order-trans, simp-all})$
apply (simp add: assert-def)
by (drule-tac $x = y$ in spec, simp)

Next theorem gives a Hoare rule for recursive programs. If we can prove

correct the unfolding of the recursive definition applid to a program $f$,

$\vdash p w \{ \lfp F \} y$, assuming that $f$ is correct when starting from $p v$, $v < w$, $\vdash \Sup p \sqcap L p w \{ f \} y$, then the recursive program is correct

$\vdash \Sup p \sqcap \lfp F \} y$

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

by (simp add: fun-eq-iff assert-def Sup-inf)

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

by (simp add: fun-eq-iff assert-def Sup-inf)

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

by (simp add: fun-eq-iff)

**lemma** Sup-less-comp: $(\text{Sup-less } P) w o S = \text{Sup-less } (\lambda w . ((P w) o S)) w$

apply (simp add: Sup-less-def fun-eq-iff, safe)
apply (subgoal-tac $(\lambda f. f (S x)) \cdot (y. \exists v<w. \forall x. y x = P v x)) = ((\lambda f. f x) \cdot (y. \exists v<w. \forall x. y x = P v (S x))))$

by (auto simp add: SUP-def simp del: Sup-image-eq)

**lemma** Sup-less-assert: $(\lambda w. \{ (p w)::'a::complete-distrib-lattice .\}) w = \{ \text{Sup-less } p w.\}$

apply (simp add: Sup-less-def assert-Sup image-def)
apply (subgoal-tac $(y. \exists v<w. y = \{ p v\} = (y. \exists x. (\exists v<w. x = p v) \land y \land x))$)
by \textit{auto}

\textbf{declare} \textit{mono-comp[simp]}

\textbf{theorem} \textit{hoare-fixpoint}:
\textit{mono-mono} \textit{F} \implies
\langle \exists w \ b. \ mono \ b \land \models \text{Sup-less} \ p \ w \ {\mid b \mid} \ y \implies \models p \ w \ {\mid F \ b \mid} \ y \implies \models \text{Sup} (\text{range} \ p) \ {\mid lfp \ F \mid} \ y \rangle

\textbf{apply} \ (\text{simp add: mono-mono-def hoare-refinement-post assert-Sup-range Sup-range-comp del: Sup-image-eq})
\textbf{apply} \ (\text{rule lfp-wf-induction})
\textbf{apply} \ \text{auto}
\textbf{apply} \ (\text{simp add: Sup-less-comp})
\textbf{apply} \ \text{drule-tac x} = \{ Sup-less \ p \ w \} \circ \text{post-fun} \ y \ \textbf{in spec, safe}
\textbf{apply} \ \text{simp}
\textbf{by} \ (\text{simp add: hoare-refinement-post})

\textbf{theorem} \ \textbf{\forall} t. \models (\{ s. t \in R \ s \} \ {\mid S \mid} \ q) \implies \models (\{ R \} \ p) \ {\mid S \mid} \ q
\textbf{apply} \ (\text{simp add: Hoare-def angelic-def subset-eq})
\textbf{by} \ \textit{auto}

\section{Predicate Transformers Semantics of Invariant Diagrams}

\textbf{theory} \textit{Diagram}
\textbf{imports} \textit{Hoare}
\textbf{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 \textit{D} is a function from pairs of indexes to predicate transformers: \textit{D} : \textit{I} \times \textit{I} \to (\text{State set} \to \text{State set}), or more general \textit{D} : \textit{I} \times \textit{I} \to \textit{Ptran}, where \textit{Ptran} is a complete lattice. The elements of \textit{I} are called situations and intuitively a diagram is executed starting in a situation \textit{i} \in \textit{I} by choosing a transition \textit{D}(\textit{i}, \textit{j}) which is enabled and continuing similarly from \textit{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 \((\textit{I} \to \text{State set})\). If \textit{Q} : \textit{I} \to \text{State set} is an indexed predicate, then \textit{p} = \textit{pt} \textit{D} \textit{Q} \textit{i} is a weakest predicate such that if the execution of \textit{D} starts in a state \textit{s} \in \textit{p} from situation \textit{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**

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

**definition**

\[
d\text{mono} \ D = (\forall \ ij . \ mono \ (D \ ij))
\]

**lemma** \( \text{dmono-mono} \ [\text{simp}]: \ d\text{mono} \ D \Longrightarrow \ mono \ (D \ ij) \)

by \( \text{(simp add: dmono-def)} \)

**theorem** \( \text{mono-step} \ [\text{simp}]: \)

\[
d\text{mono} \ D \Longrightarrow \ mono \ (\text{step} \ D)
\]

apply \( \text{(simp add: dmono-def mono-def le-fun-def step-def Inf-fun-def)} \)

apply \( \text{auto} \)

apply \( \text{(rule INF-greatest)} \)

apply \( \text{auto} \)

apply \( \text{(rule-tac y = D(xa, j) (x j) in order-trans)} \)

apply \( \text{auto} \)

apply \( \text{(rule INF-lower)} \)

by \( \text{auto} \)

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 \( d\text{gr} \ D \ U \) 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**

\[
d\text{gr} \ D \ U = ((\text{step} \ D) \circ U) \cap [..(\neg\text{grd}((\text{step} \ D))].
\]

**theorem** \( \text{mono-mono-dgr} \ [\text{simp}]: \ d\text{mono} \ D \Longrightarrow \ mono-mono \ (d\text{gr} \ D) \)

apply \( \text{(simp add: mono-mono-def mono-def)} \)

apply \( \text{safe} \)

apply \( \text{(simp-all add: dgr-def)} \)

apply \( \text{(simp-all add: le-fun-def inf-fun-def)} \)

apply \( \text{safe} \)

apply \( \text{(rule-tac y = (step D (xa) xb) in order-trans)} \)

apply \( \text{simp-all} \)

apply \( \text{(case-tac mono (step D))} \)

apply \( \text{(simp add: mono-def)} \)

apply \( \text{(simp add: le-fun-def)} \)

apply \( \text{simp} \)

apply \( \text{(rule-tac y = (step D (f x) xa) in order-trans)} \)

apply \( \text{simp-all} \)

apply \( \text{(case-tac mono (step D))} \)

10
apply (simp add: mono-def)
apply (simp-all add: le-fun-def)
apply (rule-tac y = (assume (~ grd (step D)) x xa) in order-trans)
apply simp-all
apply (case-tac mono (assume (~ grd (step D))))
apply (simp add: mono-def le-fun-def)
by simp

definition
pt D = 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 \( step \ D \) is correct.

theorem hoare-step:
\[
(\forall \ i \ j . \models (P \ i) \{ D(i,j) \} (Q \ j)) = (\models P \{ step \ D \} Q)
\]
apply safe
apply (simp add: le-fun-def Hoare-def step-def)
apply safe
apply (rule INF-greatest)
apply auto
apply (simp add: le-fun-def Hoare-def step-def)
apply (erule-tac x = i in allE)
apply (rule-tac y = INF j. D(i, j) (Q j) in order-trans)
apply auto
apply (rule INF-lower)
by auto

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 hoare-diagram:
\[
dmono D \Rightarrow (\forall \ w \ i \ j . \models X w i \{ D(i,j) \} \text{Sup-less} X w j) \Rightarrow \models (\text{Sup}(\text{range} X)) \{ pt D \} (\text{Sup}(\text{range} X) \cap -(\text{grd}(\text{step} D)))
\]
apply (simp add: hoare-step pt-def del: Sup-image-eq)
apply auto
apply (simp add: dgr-def)
apply (simp add: hoare-choice)
apply safe
apply (simp add: hoare-sequential)
apply auto
apply (simp add: hoare-assume)
apply (rule le-infI1)
by (rule SUP-upper, auto)

This theorem is a more general form of the more familiar form with a variant t which must decrease. If we take $X \cdot w \cdot i = (Y \cdot i \wedge t \cdot i = w)$, then the second hypothesis of the theorem above becomes $\vdash Y \cdot i \wedge t \cdot i = w \{ D(i, j) \} Y \cdot i \wedge t \cdot i < w$. However, the more general form of the theorem is needed, because in data refinements, the form $Y \cdot i \wedge t \cdot i = w$ cannot be preserved.

The drawback of this theorem is that the variant must be decreased on every transitions which may be too cumbersome for practical applications. A similar situation occurs 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::{v. pair v i < u}. X v i :: - :: complete-lattice)
definition SUP-LE-P X u i = (SUP v::{v. pair v i ≤ u}. X v i :: - :: complete-lattice)
lemma SUP-L-P-upper:
  pair v i < u → P v i ≤ SUP-L-P P u i
by (auto simp add: SUP-L-P-def intro: SUP-upper)
lemma SUP-L-P-least:
  (!! v. pair v i < u → P v i ≤ Q) → SUP-L-P P u i ≤ Q
by (simp add: SUP-L-P-def, rule SUP-least, auto)
lemma SUP-LE-P-upper:
  pair v i ≤ u → P v i ≤ SUP-LE-P P u i
by (auto simp add: SUP-LE-P-def intro: SUP-upper)
lemma SUP-LE-P-least:
  (!! v. pair v i ≤ u → P v i ≤ Q) → SUP-LE-P P u i ≤ Q
by (simp add: SUP-LE-P-def, rule SUP-least, auto)
lemma SUP-SUP-L [simp]: Sup (range (SUP-LE-P X)) = Sup (range X)
apply (simp add: fun-eq-iff Sup-fun-def, clarify)
apply (rule antisym)
apply (rule SUP-least)
unfolding comp-def
apply (rule SUP-LE-P-least)
apply (rule SUP-upper, simp)
apply (rule SUP-least)
apply (rule_tac y = SUP-LE-P X (pair xa x) x in order-trans)
apply (rule SUP-LE-P-upper, simp)
apply (rule SUP-upper, simp)

lemma SUP-L-SUP-LE-P [simp]: Sup-less (SUP-LE-P X) = SUP-L-P X
apply (rule antisym)
apply (subst le-fun-def, safe)
apply (rule Sup-less-least)
apply (subst le-fun-def, safe)
apply (rule SUP-LE-P-least)
apply (rule SUP-L-P-upper, simp)
apply (simp add: le-fun-def, safe)
apply (rule SUP-L-P-least)
apply (rule-tac y = SUP-LE-P X (pair v xa) xa in order-trans)
apply (rule SUP-LE-P-upper, simp)
apply (cut-tac P = SUP-LE-P X in Sup-less-upper)
by (simp, simp add: le-fun-def)

end

theorem (in DiagramTermination) hoare-diagram2:
dmono D ⇒ (∀ u i j. | X u i. D(i, j) |) SUP-L-P X (pair u i) j ⇒
| (Sup (range X)) (pt D) ((Sup (range X)) ⊓ (grd (step D)))
apply (frule-tac X = SUP-LE-P X in hoare-diagram)
apply (auto simp del: Sup-image-eq)
apply (simp add: SUP-LE-P-def)
apply (unfold SUP-def hoare-Sup [THEN sym])
apply auto
apply (rule-tac Q = SUP-L-P X (pair p i) j in hoare-mono)
apply auto
apply (rule SUP-L-P-least)
apply (rule SUP-L-P-upper)
apply (rule order-trans3)
by auto

lemma mono-pt [simp]: dmono D ⇒ mono (pt D)
apply (drule mono-mono-dgr)
by (simp add: pt-def)

theorem (in DiagramTermination) hoare-diagram3:
dmono D ⇒
(∀ u i j. | X u i. D(i, j) |) SUP-L-P X (pair u i) j ⇒
P ≤ Sup (range X) ⇒ ((Sup (range X)) ⊓ (grd (step D))) ≤ Q ⇒
The following definition introduces the concept of correct Hoare triples for diagrams.

definition (in DiagramTermination)
Hoare-dgr :: ('b ⇒ ('u::{complete-distrib-lattice, boolean-algebra})) ⇒ ('b × 'b ⇒ 'u ⇒ 'u ⇒ bool) ⇒ (P { pt D } Q) ≡ (∃ X. (∀ u i j. P u i j) ∧ SUP-L-P X (pair u i) j) ∧ P = Sup (range X) ∧ Q = ((Sup (range X)) ⊓ (−(grd (step D))))

definition (in DiagramTermination)
Hoare-dgr1 :: ('b ⇒ ('u::{complete-distrib-lattice, boolean-algebra})) ⇒ ('b ⇒ 'u) ⇒ ('b ⇒ 'u ⇒ bool) ⇒ (I P { D } Q) ≡ (∃ X. (∀ u i j. P u i j) ∧ P = Sup (range X) ∧ ((Sup (range X)) ⊓ (−(grd (step D)))) ≤ Q

theorem (in DiagramTermination) hoare-dgr-correctness:
dmono D ⇒ (P { D } Q) ⇒ (P { pt D } Q)
apply (simp add: Hoare-dgr-def)
apply safe
apply (rule hoare-diagram3)
by auto

theorem (in DiagramTermination) hoare-dgr-correctness1:
dmono D ⇒ (I P { D } Q) ⇒ (P { pt D } Q)
apply (simp add: Hoare-dgr1-def)
apply safe
apply (rule hoare-diagram3)
by auto

definition
dgr-demonic Q ij = [: Q ij :]

theorem dgr-demonic-mono[simp]:
dmono (dgr-demonic Q)
by (simp add: dmono-def dgr-demonic-def)

definition
dangelic \( R Q i \) = angelic \( (R i) (Q i) \)

**Lemma grd-dgr:**

\[ ((\text{grd} (\text{step} D) i) : (\text{a} : \text{complete-boolean-algebra})) = \bigcup \{ P . \exists j . P = \text{grd} (D(i,j)) \} \]

- apply (simp add: grd-def step-def)
- apply (unfold step-def INF-def uminus-Inf)
- apply (case-tac (uminus ' range (λj::'b. D (i, j) ⊥)) = \{ P::'a. ∃j::'b. P = - D (i, j) ⊥ \})
- apply auto

**Lemma grd-dgr-set:**

\[ ((\text{grd} (\text{step} D) i) : (\text{a} : \text{set})) = \text{Union} \{ P . \exists j . P = \text{grd} (D(i,j)) \} \]

by (simp add: grd-dgr)

**Lemma not-grd-dgr [simp]:**

\[ a \notin ((\text{grd} (\text{step} D) i)) = (\forall j . a \notin \text{grd} (D(i,j))) \]

- apply (simp add: grd-dgr)
- by auto

**Lemma not-grd-dgr2 [simp]:**

\[ a \notin ((\text{grd} (\text{step} D) i)) = (\forall j . a \notin \text{grd} (D(i,j))) \]

- apply (subst not-grd-dgr [THEN sym])
- by simp

end

### 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**

\[ \text{DataRefinement} :: \text{'a::type ⇒ 'b::type) ⇒ ('b::type ⇒ 'c::ord) ⇒ ('a::type ⇒ 'd::type) ⇒ ('d::type ⇒ 'c::ord) ⇒ bool} \]

where

\[ \text{DataRefinement} S_1 R R' S_2 = ((R o S_1) \leq (S_2 o R')) \]

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

**Theorem data-refinement:**

\[ \text{mono} R \Longrightarrow \vdash p \{ S \} q \Longrightarrow \text{DataRefinement} S R R' S' \Longrightarrow \vdash (R p) \{ S' \} (R' q) \]

- apply (simp add: DataRefinement-def Hoare-def le-fun-def)
- apply (drule-tac x = q in spec)
- apply (rule-tac y = R (S q) in order-trans)
apply (drule-tac x = p and y = S q in monoD)
by simp-all

theorem data-refinement2:
mono R \implies \vdash p \{\| S \|\} q \implies \text{DataRefinement} (\{p\} o S) R R' S' \implies 
\vdash \langle R p \rangle \{\| S' \|\} \langle R' q \rangle
apply (simp add: DataRefinement-def Hoare-def le-fun-def assert-def)
apply (drule-tac x = q in spec)
apply (subgoal-tac p \cap S q = p)
apply simp
apply (rule antisym)
by simp-all

theorem data-refinement-hoare:
mono S \implies mono D \implies \text{DataRefinement} (\{p\} o \{Q\}) \{R\} D S = 
(\forall s . s : Q s \land s \in p \{\| S \|\} (D ((Q s)::a::order)))
apply (simp add: le-fun-def assert-def angelic-def demonic-def Hoare-def DataRefinement-def)
apply safe
apply (simp-all)
apply (drule-tac x = Q s in spec)
apply auto [1]
apply (drule-tac x = xb in spec)
apply simp
apply (simp add: less-eq-set-def le-fun-def)
apply (drule-tac x = xa in spec)
apply (simp-all add: mono-def)
by auto

theorem data-refinement-choice1:
\text{DataRefinement} S1 D D' S2 \implies \text{DataRefinement} S1 D D' S2' \implies 
\text{DataRefinement} S1 D D' (S2 \cap S2')
by (simp add: DataRefinement-def hoare-choice le-fun-def inf-fun-def)

theorem data-refinement-choice2:
mono D \implies \text{DataRefinement} S1 D D' S2 \implies \text{DataRefinement} S1' D D' S2'
\implies 
\text{DataRefinement} (S1 \cap S1') D D' (S2 \cap S2')
apply (simp add: DataRefinement-def inf-fun-def le-fun-def)
apply safe
apply (rule-tac y = D (S1 x) in order-trans)
apply (drule-tac x = S1 x \cap S1' x and y = S1 x in monoD)
apply simp-all
apply (rule-tac y = D (S1' x) in order-trans)
apply (drule-tac x = S1 x \cap S1' x and y = S1' x in monoD)
by simp-all

theorem data-refinement-top [simp]:
DataRefinement $S1 \ D \ D'$ (\vdash::order-top)
by (simp add: DataRefinement-def le-fun-def top-fun-def)

definition apply-fun::('a\Rightarrow'b\Rightarrow'c)\Rightarrow('a\Rightarrow'b)\Rightarrow'a\Rightarrow'c (infixl .. 5) where
$(A .. B) = (\lambda x . (A x) (B x))$

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

lemma Disjunctive-Sup:
Disjunctive-fun $R \Rightarrow (R .. (\text{Sup} \ X)) = \text{Sup} \ \{y . \exists x \in X . y = (R .. x)\}$
apply (subst fun-eq-iff)
apply (simp add: apply-fun-def)
safe
apply (subst (asm) Disjunctive-fun-def)
apply (dlrule tac $x = x$ in spec)
apply (simp add: Apply.Disjunctive-def)
apply (subgoal-tac $(R \ x \ ' (\lambda f \ x) \ ' X) ::= ((\lambda f \ x) \ ' \{y . \exists x \in X . y = (\lambda x. R \ xa \ (x xa))\})$
by (auto simp add: SUP-def simp del: Sup-image-eq)

lemma (in DiagramTermination) disjunctive-SUP-L-P:
Disjunctive-fun $R \Rightarrow (R .. (\text{SUP-L-P} \ P \ (\text{pair} \ u \ i))) = (\text{SUP-L-P} \ (\lambda w . (R .. (P \ w))) \ (\text{pair} \ u \ i))$
apply (subst fun-eq-iff)
apply (simp add: SUP-L-P-def apply-fun-def Disjunctive-fun-def Apply.Disjunctive-def, safe)
apply (subgoal-tac $(R \ x \ ' (\lambda v \ P \ v \ x) \ ' \{\text{pair} v \ x \sqsubset \text{pair} u \ i\}) =
((\lambda v. R x (P \ v \ x)) \ ' \{\text{pair} v \ x \sqsubset \text{pair} u \ i\}))$
by (auto simp add: SUP-def simp del: Sup-image-eq)

lemma apply-fun-range: $\{y . \exists x . y = (R .. P \ x)\} = \text{range} \ (\lambda x . R .. P \ x)$
by auto

lemma [simp]: Disjunctive-fun $R \Rightarrow \text{mono} \ ((R \ i):'a::\text{complete-lattice} \Rightarrow 'b::\text{complete-lattice})$
by (simp add: Disjunctive-fun-def)

theorem (in DiagramTermination) dgr-data-refinement-1:
\text{dmono} \ D' \Rightarrow \text{Disjunctive-fun} \ R \Rightarrow
(\forall w i j . \vdash P w i \ D(i,j) \ \text{SUP-L-P} \ P \ (\text{pair} w \ i) \ j) \Rightarrow
(\forall w i j . \text{DataRefinement} \ ((\text{assert} \ (P \ w \ i)) \ o \ (D \ i \ j)) \ (R \ i) \ (R \ j) \ (D' \ i \ j))$
\Rightarrow
(\forall w i j . \vdash (R .. (\text{Sup} \ (\text{range} \ P))) \ D'(i,j) \ (\text{Sup} \ (\text{range} \ P))) \ \cap \ (-\text{\text{grd} \ (\text{step} \ D')})$
apply (simp add: Disjunctive-Sup apply-fun-range del: Sup-image-eq)
apply (rule hoare-diagram2)
safe
apply simp-all
apply safe
apply (simp add: disjunctive-SUP-L-P [THEN sym])
apply (simp add: apply-fun-def)
apply (rule-tac $S = D \ (i, j)$ in data-refinement2)
by auto

definition
\text{DgrDataRefinement1} \ D \ R \ D' = (\forall \ i \ j . \ \text{DataRefinement} \ (D \ (i, j)) \ (R \ i) \ (R \ j) \ (D' \ (i, j)))

definition
\text{DgrDataRefinement2} \ P \ D \ R \ D' = (\forall \ i \ j . \ \text{DataRefinement} \ (\{\ . P \ i. \} \circ D \ (i, j)) \ (R \ i) \ (R \ j) \ (D' \ (i, j)))

theorem \text{DataRefinement-mono}:
\text{T} \leq \text{S} \implies \text{mono} \ R \implies \text{DataRefinement} \ \text{S} \ R \ \text{S}' \implies \text{DataRefinement} \ \text{T} \ R \ \text{R}' \ \text{S}'
apply (simp add: DataRefinement-def mono-def)
apply (subst le-fun-def)
apply (simp add: le-fun-def)
apply safe
apply (rule-tac $y = R \ (S \ x)$ in order-trans)
by simp-all

definition
\text{mono-fun} \ R = (\forall \ i . \ \text{mono} \ (R \ i))

theorem \text{DgrDataRefinement-mono}:
\text{Q} \leq \text{P} \implies \text{mono-fun} \ R \implies \text{DgrDataRefinement2} \ P \ D \ R \ D' \implies \text{DgrDataRefinement2} \ Q \ D \ R \ D'
apply (simp add: DgrDataRefinement2-def)
apply auto
apply (rule-tac $S = \{\ . P \ i. \} \circ D(i, j)$ in DataRefinement-mono)
apply (simp-all add: le-fun-def assert-def)
apply safe
apply (rule-tac $y = Q \ i$ in order-trans)
by (simp-all add: mono-fun-def)

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) \text{Diagram-DataRefinement1}:
\text{dmono} \ D \implies \text{Disjunctive-fun} \ R \implies \vdash P (\{ D \}) \ Q \implies \text{DgrDataRefinement1} \ D \ R \ D' \implies \\
\vdash (R \cdot P) (\{ D' \}) ((R \cdot P) \cap (\neg (\text{grd} \ (\text{step} \ D'))))
apply (unfold Hoare-dgr-def DgrDataRefinement1-def dgr-demonic-def)
apply safe
apply (rule-tac $x = \lambda \ w . \ R \cdot (X \ w)$ in exI)
apply safe

18
apply (unfold disjunctive-SUP-L-P [THEN sym])
apply (simp add: apply-fun-def)
apply (rule-tac S = D (i,j) and R = R i and R' = R j in data-refinement)
by (simp-all add: Disjunctive-Sup apply-fun-range del: Sup-image-eq)

lemma comp-left-mono [simp]: $S \leq S' \Longrightarrow S \circ T \leq S' \circ T$
by (simp add: le-fun-def)

lemma assert-pred-mono [simp]: $p \leq q \Longrightarrow \{p\} \leq \{q\}$
apply (simp add: le-fun-def assert-def)
apply safe
apply (rule-tac $y = p$ in order-trans)
by simp-all

theorem (in DiagramTermination) Diagram-DataRefinement2:
dmono D \Longrightarrow Disjunctive-fun R \Longrightarrow \vdash P \parallel D Q \Longrightarrow DgrDataRefinement2 P
D R D' \Longrightarrow
\vdash (R \circ P) \parallel (D') (\bigcap (\neg (\grad (\step D'))))
apply (unfold Hoare-dgr-def DgrDataRefinement2-def dgr-demonic-def)
apply auto
apply (rule-tac $x = \lambda w . R \circ (X w)$ in exI)
apply safe
apply (unfold disjunctive-SUP-L-P [THEN sym])
apply (simp add: apply-fun-def)
apply (rule-tac S = D (i,j) and R = R i and R' = R j in data-refinement2)
apply (simp-all add: Disjunctive-Sup)
apply (rule-tac S = \{Sup (range X) i\} \circ D (i,j) in DataRefinement-mono)
apply (rule comp-left-mono)
apply (rule assert-pred-mono)
apply (simp add: Sup-fun-def comp-def)
apply (rule SUP-upper)
apply (auto simp add: apply-fun-def apply-fun-range SUP-def image-image fun-eq-iff simp del: Sup-image-eq)
apply (metis Apply.DisjunctiveD Disjunctive-fun-def range-composition)+
done

lemma (R': 'a::complete-lattice \Rightarrow 'b::complete-lattice) \in Apply.Disjunctive \Longrightarrow
DataRefinement S R R' S' \Longrightarrow R (\neg \grad S) \leq \neg \grad S'
apply (simp add: DataRefinement-def grd-def le-fun-def)
apply (drule-tac $x = \perp$ in spec)
by simp

end
References


