

Predicate-transformer semantics of general recursion

Pierre Senellart, based on an article by Wim H. Hesselink

Friday, March 23rd 2001

Purposes of the exposé

- Introduce the formalism of predicate-transformer semantics;
- Give a formal fixpoint definition of the predicate-transformers wp and wlp ;
- Show that local conditions, such as total functions and determinacy, are preserved with general recursion.

A variation of the theorem of Knaster-Tarski

Theorem 1 *Let (W, \leq) be a partially ordered set. Let $f : W \rightarrow W$ be a monotone function. Let V be a subset of W which is closed under least upper bounds in W (i.e. every subset of V has a least upper bound in W which is in V), and which is invariant under f ($\forall v \in V f.v \in V$). Then V contains a fixed point v_0 of f , which satisfies $v_0 \leq w$ for every $w \in W$ with $f.w \leq w$. In particular, v_0 is the smallest fixed point of f in W .*

Proof

Let $U = \{u \in V \mid \forall w \in W (f.w \leq w \Rightarrow u \leq w)\}$.

Let v_0 be the least upper bound of U in W . $v_0 \in V$.

$$\forall w \in W$$

$$f.w \leq w$$

$$\Rightarrow \forall u \in U u \leq w$$

$$\Rightarrow v_0 \leq w$$

$$\Rightarrow f.v_0 \leq f.w \leq w$$

Thus, $v_0 \in U$ and $f.v_0 \in U$. Since v_0 is the least upper bound of U , $f.v_0 \leq v_0$ and $f.(f.v_0) \leq f.v_0$.

We deduce from $v_0 \in U$ and the last inequality: $v_0 \leq f.v_0$, which concludes the proof.

□

Predicates

Let E be a set of states, describing for instance the values of the variables of a program. A *predicate* is a boolean function defined on E which gives conditions on the state of the system.

true and *false* denote respectively the true and false predicate: every state satisfies *true* and no state satisfies *false*.

Given two predicates P and R , the predicates $P \wedge Q$, $P \vee Q$, $\neg P$, $P \Rightarrow Q$ are defined in an obvious way.

Predicate-transformers wp and wlp

Given a command (i.e. a program) p and a predicate R , $wp.p.R$ is the weakest precondition such that any execution of p from a state satisfying it will terminate and lead to a state which satisfies R .

Given a command p and a predicate R , $wlp.p.R$ is the weakest precondition such that any terminating execution of p from a state satisfying it will lead to a state which satisfies R .

wp and wlp are called *predicate-transformers*.

Intuitive properties of wp and wlp

- $wp.t.x = wp.t.true \wedge wlp.t.x$

- $wlp.t. \left(\bigwedge_{y \in Y} y \right) = \bigwedge_{y \in Y} (wlp.t.y)$

- $wp.t.false = false$

This is the so-called *Law of the Excluded Miracle*. It is only postulated by Dijkstra and we will afterwards allow exceptions to it.

- $wp.(p; q).x = wp.p.(wp.q.x)$ or $wp.(p; q) = (wp.p) \circ (wp.q)$

Commands

Let S be a set of statements (e.g. assignments) whose semantics is assumed to be known, in terms of the predicate transformers wp and wlp . Let H be a set of procedure names. $A = H \cup S$ is the set of *simple commands*. A^* is the set of words over A , the concatenation operator being denoted by $;$. An element of A^* is called a command.

Any function defined on A with values in X^X for some set X , such as wp and wlp , is extended to A^* by the rules:

$$w.\varepsilon = id_X$$

$$w.(p; q) = (w.p) \circ (w.q)$$

The Semantic Domain

Let (X, \leq) be a complete partially ordered set. 1 is the biggest element of X and 0 is the smallest one. We may interpret X as a set of predicates over some states space. In this case, 1 is identified with *true* and 0 is identified with *false*. We keep the analogy with predicates by denoting \wedge and \vee the greatest lower bound and the least upper bound. \neg denotes an arbitrary function: $X \rightarrow X$.

Let M be the set of monotone functions $X \rightarrow X$.

Let $W = X^A$. As seen before, any element of W may be extended to an element of X^{A^*} . We will not in the following make the difference between an element of W and its extension.

Declaration of procedures

Every procedure h , $h \in H$ has a declaration as following:

$$h ::= (b_j \rightarrow r_j)_{j \in J_h}$$

J_h is a set (not necessarily finite) of indices. For all j , b_j is a predicate and r_j is a command.

Intuitively, r_j will be executed if the initial state satisfies b_j (if several b_j are satisfied, one of them is arbitrarily chosen: there may be nondeterminism).

Semantic functions

$w \in W$ is a *semantic function* if it satisfies :

$$\forall h \in H, \forall x \in X, w.h.x = \bigwedge_{j \in J_h} (\neg b_j \vee w.r_j.x)$$

If we want to extend in a natural way wp and wlp to procedure calls, these two functions must be semantic functions: to be in the state x after a terminating execution of h , you have to be in $wp.r_j.x$ for every j such that the initial state satisfies r_j .

Partial and total declarations and commands

If there exists no j such that b_j is satisfied for some state x , the execution of h on x fails and h is said to be *partial*. By convention, we have in such a case $x \in wp.h.false$ and the law of the excluded miracle is not verified any longer.

In a similar way, any command may be partial: in particular, statements, whose semantics is supposed to be known, may be partial.

A non-partial command is said to be *total*.

Towards a fixpoint definition of wp and wlp (1)

In the following, we assume that wp and wlp are only defined on S and we are looking for a formal definition of their extensions on A^* .

Let $wg \in M^S$.

We define $F.wg \in W^W$ by:

$$\forall w \in W, \forall s \in S, \forall h \in H, \forall x \in X \\ (F.wg.w.s.x = wg.s.x) \wedge \left(F.wg.w.h.x = \left(\bigwedge_{j \in J_h} \neg b_j \vee w.r_j.x \right) \right)$$

The purpose is to give a definition of the extensions of wp and wlp as fixpoints of $F.wp$ and $F.wlp$.

Towards a fixpoint definition of wp and wlp (2)

We define a partial order on W :

$$\forall (w, w') \in W^2, w \preceq w' \Leftrightarrow (\forall a \in A, \forall x \in X, w.a.x \leq w'.a.x)$$

(W, \preceq) is complete. w_0 and w_1 , which are defined below, are respectively the greatest lower bound and the least upper bound of a subset U of W .

$$w_0.a.x = \bigwedge_{u \in U} u.a.x \quad w_1.a.x = \bigvee_{u \in U} u.a.x$$

The verifications that w_0 and w_1 are elements of W and that they are the extreme bounds of U are easy.

Towards a fixpoint definition of wp and wlp (3)

We show now that the formula defining \preceq still stands for commands in A^* :

$$\forall (w, w') \in W^2, w \preceq w' \Leftrightarrow (\forall t \in A^*, \forall x \in X, w.t.x \leq w'.t.x)$$

We prove it by induction on the length of t . The base case is obvious. As for the induction step just uses the monotony of $w.a$ with $w \in W$ and $a \in A$.

Theorem 2 *For any function $wg \in M^S$, $F.wg$ is monotone.*

Proof

Let $(w, w') \in W^2, w \preceq w'$

$$\forall s \in S, \forall h \in H, \forall x \in X$$

$$F.wg.s.x = wg.s.x = F.wg.s'.x$$

$$F.wg.w.h.x = \left(\bigwedge_{j \in J_h} \neg b_j \vee w.r_j.x \right) \leq \left(\bigwedge_{j \in J_h} \neg b_j \vee w'.r_j.x \right) = F.wg.w'.h.x$$

The inequality stands because \vee and \bigwedge are monotone functions.

Thus, $F.wg.w \preceq F.wg.w'$ and F is monotone.

□

Fixpoint definition of wp and wlp

As $F.wg$ is for any wg a monotone function over a complete partially ordered set, we can use the Knaster-Tarski theorem.

The extensions of wp and wlp , which we still denote wp and wlp , are defined as following:

- wp is the smallest fixed point of $F.wp$.
- wlp is the greatest fixed point of $F.wlp$.

The fact that they are fixpoints of a $F.w$ for some w guarantees that they are semantic functions.

The Law of the Excluded Miracles

Theorem 3 *All comands are total if and only if all statements and all declarations are total.*

Proof

First let all commands be total. It suffices to prove that all declarations are total.

$$\begin{aligned} & wp.h.0 = 0 \\ \Rightarrow & F.wp.wp.0 = 0 \\ \Rightarrow & \bigwedge_{j \in J_h} \neg b_j \vee wp.r_j.0 = 0 \\ \Rightarrow & \bigwedge_{j \in J_h} \neg b_j = 0 \end{aligned}$$

For the converse, let $u \in W$ be defined by:

$$\forall a \in A, u.a.0 = 0$$

$$\forall a \in A, \forall x \in X, x \neq 0 \Rightarrow u.a.x = 1$$

We have:

$$\forall w \in W, w \preceq u \Leftrightarrow (\forall a \in A, w.a.0 = 0)$$

We observe that:

$$\begin{aligned} & \forall t \in A^*, wp.t.0 = 0 \\ \Leftrightarrow & \forall a \in A, wp_a.0 = 0 \\ \Leftrightarrow & wp \preceq u \\ \Leftrightarrow & F.wp.u \preceq u \\ \Leftrightarrow & \forall a \in A, F.wp.u.a.0 = 0 \\ \Leftrightarrow & (\forall s \in S, wp.s.0 = 0) \wedge (\forall h \in H, \bigwedge_{J_h} \neg b_j \vee u.r_j.0 = 0) \\ \Leftrightarrow & (\forall s \in S, wp.s.0 = 0) \wedge (\forall h \in H, \bigwedge_{J_h} \neg b_j = 0) \end{aligned}$$

□

Assumptions

We assume the definitions of wp and wlp satisfy (we already saw they were intuitive properties):

- $\forall s \in S, \forall x \in X, wp.s.x = wp.s.1 \wedge wp.s.x$

- $\forall s \in S, \forall Y \in \mathcal{P}(X), wlp.s. \left(\bigwedge_{y \in Y} y \right) = \bigwedge_{y \in Y} wlp.s.y$

Furthermore, we assume that (X, \vee, \wedge, \neg) is a complete boolean lattice. In particular, we have the usual distributivity laws between \wedge and \vee and the laws of De Morgan.

Determinacy

A command t is said to be *deterministic* if and only if:

$$\forall x \in X, \neg wp.t.x \leq wlp.t.(\neg x)$$

Informally, a command is deterministic if, when started on a state not leading to a state verifying x , it will not terminate or will terminate on a state satisfying $\neg x$.

A procedure h is said to be *deterministic* if and only if:

$$\forall i, j \in J_h, i \neq j \rightarrow b_i \wedge b_j = 0$$

Properties of wp and wlp

Theorem 4

$$\forall t \in A^*, \forall Y \in \mathcal{P}(X), wlp.t. \left(\bigwedge_{y \in Y} y \right) = \bigwedge_{y \in Y} wlp.t.y$$

Theorem 5

$$\forall t \in A^*, \forall x \in X, wp.s.x = wp.t.1 \wedge wp.t.x$$

Theorem 6 *Let all statements and all declarations be deterministic. Then all commands are deterministic.*

The overall pattern of the proofs of these three theorems is the same. Only the calculus details change, but there are no big difficulties. Therefore, we will only give the proof of the last one.

Proof

We suppose that all statements and all declarations are deterministic.

Let $W' = \{w \in W \mid \forall a \in A, \forall x \in X, \neg(wp.a.x) \leq w.a.(\neg x)\}$. We prove in the lemma 1 that $W' = \{w \in W \mid \forall t \in A^*, \forall x \in X, \neg(wp.t.x) \leq w.t.(\neg x)\}$.

What we must prove is then that $wlp \in W'$.

wlp is the biggest fixpoint of $F.wlp$ in W . In the lemma 2, we prove that W' is closed under greatest lower bounds and in lemma 3 that W' is invariant under $F.wlp$. We can thus use the variation of the Knaster-Tarski theorem, which gives us the result we looked for.

□

Lemma 1 $\forall w \in W', \forall t \in A^*, \forall x \in X \neg(wp.t.x) \leq w.t.(\neg x)$

Proof

It is a simple induction on the length of the string t which uses the monotony of $w.a$ for $a \in A$.

□

Lemma 2 *W' is closed under greatest lower bounds in W .*

Proof

Since W is complete, every subset of W' has a greatest lower bound. Let U be a subset of W' and w be the greatest lower bound of U .

$$\forall u \in U \neg(wp.a.x) \leq w.a.(\neg x)$$

Hence:

$$\neg(wp.a.x) \leq u.a.(\neg x)$$

□

Lemma 3 *W is invariant under F.wlp.*

Proof

Let $w \in W'$.

$$F.wlp.w \in W'$$

$$\Leftrightarrow (\forall x \in X, \forall s \in S, \neg(wp.s.x) \leq wlp.s.(\neg x))$$

$$\wedge (\forall x \in X, \forall h \in H, \neg(F.wp.wp.h.x) \leq F.wlp.w.h.(\neg x))$$

The first condition is satisfied because all statements are deterministic. Then:

$$\begin{aligned}
& \neg(F.wp.wp.h.x) \leq F.wlp.w.h.(\neg x) \\
\Leftarrow & \neg \left(\bigwedge_{i \in J_h} \neg b_i \vee wp.r_i.x \right) \leq \left(\bigwedge_{j \in J_h} \neg b_j \vee w.r_j.(\neg x) \right) \\
\Leftarrow & \left(\bigvee_{i \in J_h} b_i \wedge \neg(wp.r_i.x) \right) \leq \left(\bigwedge_{j \in J_h} \neg b_j \vee w.r_j.(\neg x) \right) \\
\Leftarrow & \forall i, j \in J_h, (b_i \wedge \neg(wp.r_i.x)) \leq (\neg b_j \vee w.r_j.(\neg x)) \\
\Leftarrow & (\forall i, j \in J_h, b_i \leq \neg b_j) \wedge (\forall j \in J_h, \neg(wp.r_j.x) \leq w.r_j.(\neg x)) \\
\Leftarrow & \forall i, j \in J_h, i \neq j \Rightarrow b_i \wedge b_j = 0
\end{aligned}$$

□

Hoare Triples

A *Hoare Triple* is a triple $\langle x, h, y \rangle$ with $x, y \in X$ and $h \in H$.

If T is a set of Hoare triples, we say that $w \in W$ satisfies T and we denote $w \models T$ if and only if:

$$\forall \langle x, h, y \rangle \in T, x \leq w.h.y$$

Let $WLP = \{w \in W \mid \forall s \in S, w.s = wlp.s\}$

Theorem 7 *Let T be a set of Hoare triples such that:*

$$\forall w \in WLP, w \models T \Rightarrow F.wlp.w \models T$$

Then $wlp \models T$.