Mechanized semantics
Xavier Leroy

To cite this version:

HAL Id: inria-00529848
https://inria.hal.science/inria-00529848
Submitted on 26 Oct 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers. L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Mechanized semantics

with applications to program proof and compiler verification

Xavier LEROY
INRIA Paris-Rocquencourt

Abstract. The goal of this lecture is to show how modern theorem provers—in this case, the Coq proof assistant—can be used to mechanize the specification of programming languages and their semantics, and to reason over individual programs and over generic program transformations, as typically found in compilers. The topics covered include: operational semantics (small-step, big-step, definitional interpreters); a simple form of denotational semantics; axiomatic semantics and Hoare logic; generation of verification conditions, with application to program proof; compilation to virtual machine code and its proof of correctness; an example of an optimizing program transformation (dead code elimination) and its proof of correctness.

Introduction

The semantics of a programming language describe mathematically the meaning of programs written in this language. An example of use of semantics is to define a programming language with much greater precision than standard language specifications written in English. (See for example the definition of Standard ML [38].) In turn, semantics enable us to formally verify some programs, proving that they satisfy their specifications. Finally, semantics are also necessary to establish the correctness of algorithms and implementations that operate over programs: interpreters, compilers, static analyzers (including type-checkers and bytecode verifiers), program provers, refactoring tools, etc.

Semantics for nontrivial programming languages can be quite large and complex, making traditional, on-paper proofs using these semantics increasingly painful and unreliable. Automatic theorem provers and especially interactive proof assistants have great potential to alleviate these problems and scale semantic-based techniques all the way to realistic programming languages and tools. Popular proof assistants that have been successfully used in this area include ACL2, Coq, HOL4, Isabelle/HOL, PVS and Twelf.

The purpose of this lecture is to introduce students to this booming field of mechanized semantics and its applications to program proof and formal verification of programming tools such as compilers. Using the prototypical IMP imperative language as a concrete example, we will:

- mechanize various forms of operational and denotational semantics for this language and prove their equivalence (sections 1 and 2);
- introduce axiomatic semantics (Hoare logic) and show how to provide machine assistance for proving IMP programs using a verification condition generator (section 3);
- define a non-optimizing compiler from IMP to a virtual machine (a small subset of the Java virtual machine) and prove the correctness of this compiler via a semantic preservation argument (section 4);
- illustrate optimizing compilation through the development and proof of correctness of a dead code elimination pass (section 5).

We finish with examples of recent achievements and ongoing challenges in this area (section 6).

We use the Coq proof assistant to specify semantics and program transformations, and conduct all proofs. The best reference on Coq is Bertot and Castéran’s book [13], but for the purposes of this lecture, Bertot’s short tutorial [11] is largely sufficient. The Coq software and documentation is available as free software at http://coq.inria.fr/. By lack of time, we will not attempt to teach how to conduct interactive proofs in Coq (but see the two references above). However, we hope that by the end of this lecture, students will be familiar enough with Coq’s specification language to be able to read the Coq development underlying this lecture, and to write Coq specifications for problems of their own interest.

The reference material for this lecture is the Coq development available at http://gallium.inria.fr/~xleroy/courses/Marktoberdorf-2009/. These notes explain and recapitulate the definitions and main results using ordinary mathematical syntax, and provides bibliographical references. To help readers make the connection with the Coq development, the Coq names for the definitions and theorems are given as bracketed notes, [like this]. In the PDF version of the present document, available at the Web site above, these notes are hyperlinks pointing directly to the corresponding Coq definitions and theorems in the development.
1. Symbolic expressions

1.1. Syntax

As a warm-up exercise, we start by formalizing the syntax and semantics of a simple language of expressions comprising variables \(x, y, \ldots\), integer constants \(n\), and two operators + and −.

Expressions: [expr]
\[
e ::= x \mid n \mid e_1 + e_2 \mid e_1 - e_2
\]

The Coq representation of expressions is as an inductive type, similar to an ML or Haskell datatype.

Definition ident := nat.
Inductive expr : Type :=
| Evar: ident -> expr
| Econst: Z -> expr
| Eadd: expr -> expr -> expr
| Esub: expr -> expr -> expr.

\(\text{nat}\) and \(\text{Z}\) are predefined types for natural numbers and integers, respectively. Each case of the inductive type is a function that constructs terms of type \(\text{expr}\). For instance, \(\text{Evar}\) applied to the name of a variable produces the representation of the corresponding expression; and \(\text{Eadd}\) applied to the representations of two subexpressions \(e_1\) and \(e_2\) returns the representation of the expression \(e_1 + e_2\). Moreover, all terms of type \(\text{expr}\) are finitely generated by repeated applications of the 4 constructor functions; this enables definitions by pattern matching and reasoning by case analysis and induction.

1.2. Denotational semantics

The simplest and perhaps most natural way to specify the semantics of this language is as a function \([e] s\) that associates an integer value to the expression \(e\) in the state \(s\). States associate values to variables.

\[
[x] s = s(x) \quad [n] s = n
\]
\[
[e_1 + e_2] s = [e_1] s + [e_2] s \quad [e_1 - e_2] s = [e_1] s - [e_2] s
\]

In Coq, this denotational semantics is presented as a recursive function \([\text{eval}\_\text{expr}]\).

Definition state := ident -> Z.
Fixpoint eval_expr (s: state) (e: expr) {struct e} : Z :=
machine e with
| Evar x => s x
| Econst n => n
| Eadd e1 e2 => eval_expr s e1 + eval_expr s e2
| Esub e1 e2 => eval_expr s e1 - eval_expr s e2
end.
Fixpoint marks a recursive function definition. The struct e annotation states that it is structurally recursive on its e parameter, and therefore guaranteed to terminate. The match...with construct represents pattern-matching on the shape of the expression e.

1.3. Using the denotational semantics

The eval_expr function can be used as an interpreter, to evaluate expressions in a known environment. For example:

Eval compute in (let x : ident := O in let s : state := fun y => if eq_ident y x then 12 else 0 in eval_expr s (Eadd (Evar x) (Econst 1))).

Coq prints “13 : Z”. For additional performance, efficient executable Caml code can also be generated automatically from the Coq definition of eval_expr using the extraction mechanism of Coq.

Another use of eval_expr is to reason symbolically over expressions in arbitrary states. Consider the following claim:

Remark expr_add_pos:
  forall s x, s x >= 0 -> eval_expr s (Eadd (Evar x) (Econst 1)) > 0.

Using the simpl tactic of Coq, the goal reduces to a purely arithmetic statement:

forall s x, s x >= 0 -> s x + 1 > 0.

which can be proved by standard arithmetic (the omega tactic).

Finally, the denotation function eval_expr can also be used to prove “meta” properties of the semantics. For example, we can easily show that the denotation of an expression is insensitive to values of variables not mentioned in the expression.

Lemma eval_expr_domain:
  forall s1 s2 e, (forall x, is_free x e -> s1 x = s2 x) -> eval_expr s1 e = eval_expr s2 e.

The proof is a simple induction on the structure of e. The predicate is_free, stating whether a variable occurs in an expression, is itself defined as a recursive function:

Fixpoint is_free (x: ident) (e: expr) {struct e} : Prop :=
  match e with
  | Evar y => x = y
  | Econst n => False
  | Eadd e1 e2 => is_free x e1 \ is_free x e2
  | Esub e1 e2 => is_free x e1 \ is_free x e2
  end.

As the Prop annotation indicates, the result of this function is not a data type but a logical formula.
1.4. Variants

The denotational semantics we gave above interprets the + and - operators as arithmetic over mathematical integer. We can easily interpret them differently, for instance as signed, modulo $2^{32}$ arithmetic (as in Java):

```coq
Fixpoint eval_expr (s: state) (e: expr) {struct e} : Z :=
  match e with
  | Evar x => s x
  | Econst n => normalize n
  | Eadd e1 e2 => normalize (eval_expr s e1 + eval_expr s e2)
  | Esub e1 e2 => normalize (eval_expr s e1 - eval_expr s e2)
  end.
```

Here, normalize $n$ is $n$ reduced modulo $2^{32}$ to the interval $[-2^{31}, 2^{31})$.

We can also account for undefined expressions. In practical programming languages, the value of an expression can be undefined for several reasons: if it mentions a variable that was not previously defined; in case of overflow during an arithmetic operation; in case of an integer division by 0; etc. A simple way to account for undefinedness is to use the option type, as defined in Coq’s standard library. This is a two-constructor inductive type with None meaning “undefined” and Some $n$ meaning “defined and having value $n$”.

```coq
Definition state := ident -> option Z.
Fixpoint eval_expr (s: state) (e: expr) {struct e} : option Z :=
  match e with
  | Evar x => s x
  | Econst n => Some n
  | Eadd e1 e2 =>
    match eval_expr s e1, eval_expr s e2 with
    | Some n1, Some n2 => Some (n1 + n2)
    | _, _ => None
    end
  | Esub e1 e2 =>
    match eval_expr s e1, eval_expr s e2 with
    | Some n1, Some n2 => Some (n1 - n2)
    | _, _ => None
    end.
  end.
```

1.5. Summary

The approach we followed in this section—denotational semantics represented as a Coq recursive function—is natural and convenient, but limited by a fundamental aspect of Coq: all functions must be terminating, so that they are defined everywhere by construction. The termination guarantee can come either by the fact that they are structurally recursive (recursive calls are only done on strict sub-terms of the argument, as in the case of eval_expr), or by Noetherian recursion on a well-founded ordering. Consequently, the approach followed in this section cannot be used to give semantics to languages featuring general loops or
general recursion. As we now illustrate with the IMP language, we need to move away from functional presentations of the semantics (where a function computes a result given a state and a term) and adopt relational presentations instead (where a ternary predicate relates a state, a term, and a result).

2. The IMP language and its semantics

2.1. Syntax

The IMP language is a very simple imperative language with structured control. Syntactically, it extends the language of expressions from section 1 with boolean expressions (conditions) and commands (statements):

Expressions: \([expr]\)
\[ e ::= x | n | e_1 + e_2 | e_1 - e_2 \]

Boolean expressions: \([bool\ expr]\)
\[ b ::= e_1 = e_2 | e_1 < e_2 \]

Commands: \([cmd]\)
\[ c ::= \text{skip} | x := e | \text{if } b \text{ then } c_1 \text{ else } c_2 | \text{while } b \text{ do } c \text{ done} \]

The semantics of boolean expressions is given in the denotational style of section 1, as a function from states to booleans \([\text{eval} bool\ expr]\).

\[
\begin{align*}
[e_1 = e_2] s &= \begin{cases} 
  \text{true} & \text{if } [e_1] s = [e_2] s; \\
  \text{false} & \text{otherwise.}
\end{cases} \\
[e_1 < e_2] s &= \begin{cases} 
  \text{true} & \text{if } [e_1] s < [e_2] s; \\
  \text{false} & \text{otherwise.}
\end{cases}
\end{align*}
\]

2.2. Reduction semantics

A standard way to give semantics to languages such as IMP, where programs may not terminate, is reduction semantics, popularized by Plotkin under the name “structural operational semantics” [49], and also called “small-step semantics”. It builds on a reduction relation \((c, s) \rightarrow (c', s')\), meaning: in initial state \(s\), the command \(c\) performs one elementary step of computation, resulting in modified state \(s'\) and residual computations \(c'\). [red]

\[
\begin{align*}
(x := e, s) &\rightarrow (\text{skip}, s[x \leftarrow [e] s]) \quad \text{(red_assign)} \\
(c_1, s) &\rightarrow (c'_1, s) \quad \text{(red_seq_left)} \\
((c_1; c_2), s) &\rightarrow ((c'_1; c_2), s') \quad \text{(red_seq_skip)} \\
([b] s = \text{true}) &\rightarrow ((\text{if } b \text{ then } c_1 \text{ else } c_2), s) \rightarrow (c_1, s) \quad \text{(red_if_true)}
\end{align*}
\]
The Coq translation of such a definition by inference rules is called an inductive predicate. Such predicates build on the same inductive definition mechanisms that we already use to represent abstract syntax trees, but the resulting logical object is a proposition (sort Prop) instead of a data type (sort Type). The general recipe for translating inference rules to an inductive predicate is as follows. First, write each axiom and rule as a proper logical formula, using implications and universal quantification over free variables. For example, the rule red_seq_left becomes

\[
\forall c_1, c_2, s, c_1', s'. \quad \text{red} (c_1, s) (c_1', s') \rightarrow \text{red} (\text{Cseq } c_1, c_2, s) (\text{Cseq } c_1', c_2', s').
\]

Second, give a name to each rule. (These names are called “constructors”, by analogy with data type constructors.) Last, wrap these named rules in an inductive predicate definition like the following.

Inductive red: (cmd * state) -> (cmd * state) -> Prop :=
| red_assign: forall x e s, red (Cassign x e, s) (Cskip, update s x (eval_expr s e))
| red_seq_left: forall c1, c2, s, c1', s'. \text{red} (c1, s) (c1', s') \rightarrow \text{red} (\text{Cseq } c1, c2, s) (\text{Cseq } c1', c2', s')
| red_seq_skip: forall c, s, red (Cseq Cskip c, s) (c, s)
| red_if_true: forall s, b, c1, c2, \text{eval_bool_expr } s b = \text{true} \rightarrow \text{red} (\text{Cifthenelse } b c1, c2, s) (c1, s)
| red_if_false: forall s, b, c1, c2, \text{eval_bool_expr } s b = \text{false} \rightarrow \text{red} (\text{Cifthenelse } b c1, c2, s) (c2, s)
| red_while_true: forall s, b, c, \text{eval_bool_expr } s b = \text{true} \rightarrow \text{red} (\text{Cwhile } b c, s) (\text{Cseq } c (\text{Cwhile } b c), s)
| red_while_false: forall s, b, c, \text{eval_bool_expr } s b = \text{false} \rightarrow \text{red} (\text{Cwhile } b c, s) (\text{Cskip}, s).

Each constructor of the definition is a theorem that lets us conclude \text{red} (c, s) (c', s') when the corresponding premises hold. Moreover, the proposition \text{red} (c, s) (c', s') holds only if it was derived by applying these theorems.
a finite number of times (smallest fixpoint). This provides us with powerful reasoning principles: by case analysis on the last rule used, and by induction on a derivation. Consider for example the determinism of the reduction relation:

**Lemma red_deterministic:**
forall cs cs1, red cs cs1 -> forall cs2, red cs cs2 -> cs1 = cs2.

It is easily proved by induction on a derivation of red cs cs1 and a case analysis on the last rule used to conclude red cs cs2.

From the one-step reduction relation, we can define the the behavior of a command c in an initial state s is obtained by forming sequences of reductions starting at c, s:

- Termination with final state s’, written \((c, s) \downarrow s’\): finite sequence of reductions to skip. [terminates]
  \[(c, s) \Rightarrow (\text{skip}, s')\]

- Divergence, written \((c, s) \uparrow\): infinite sequence of reductions. [diverges]
  \[\forall c', \forall s', (c, s) \Rightarrow (c', s') \Rightarrow \exists c'', \exists s'', (c', s') \Rightarrow (c'', s'')\]

- Going wrong, written \((c, s) \Rightarrow \text{wrong}\): finite sequence of reductions to an irreducible state that is not skip. [goes wrong]
  \[(c, s) \Rightarrow \cdots \Rightarrow (c', s') \not\Rightarrow \text{with } c \neq \text{skip}\]

### 2.3. Natural semantics

An alternative to structured operational semantics is Kahn’s natural semantics [26], also called big-step semantics. Instead of describing terminating executions as sequences of reductions, natural semantics aims at giving a direct axiomatization of executions using inference rules.

To build intuitions for natural semantics, consider a terminating reduction sequence for the command \(c; c'\).

\[(c; c'), s \rightarrow (c_1; c'), s_1) \rightarrow \cdots \rightarrow (\text{skip}; c'), s_2) \rightarrow (c', s_2) \rightarrow \cdots \rightarrow (\text{skip}, s_3)\]

It contains a terminating reduction sequence for \(c\), of the form \((c, s) \Rightarrow (\text{skip}, s_2)\), followed by another terminating sequence for \((c', s_2)\).

The idea of natural semantics is to write inference rules that follow this structure and define a predicate \(c, s \Rightarrow s'\), meaning “in initial state \(s\), the command \(c\) terminates with final state \(s'\)”. [exec]

\[
\begin{align*}
skip &\Rightarrow s & (\text{exec_skip}) \\
\text{exec_assign} &\quad x := e, s \Rightarrow s[x \leftarrow [e] s] \\
\text{exec_seq} &\quad c_1; c_2, s \Rightarrow s_2 \quad (c_1, s \Rightarrow s_1 \quad c_2, s \Rightarrow s_2) \\
\text{exec_if} &\quad (\text{if } b \text{ then } c_1 \text{ else } c_2), s \Rightarrow s' \quad (c_1, s \Rightarrow s' \text{ if } [b] s = \text{true} \quad c_2, s \Rightarrow s' \text{ if } [b] s = \text{false})
\end{align*}
\]
\[
\begin{align*}
\text{\{b\} } s &= \text{false} \quad \text{(exec\_while\_stop)} \\
\text{while } b \text{ do } c \text{ done}, s &\Rightarrow s
\end{align*}
\]

\[
\begin{align*}
\text{\{b\} } s &= \text{true} \quad c, s \Rightarrow s_1 \quad \text{while } b \text{ do } c \text{ done}, s_1 &\Rightarrow s_2 \\
\text{while } b \text{ do } c \text{ done}, s &\Rightarrow s_2
\end{align*}
\]

We now have two different semantics for the same language. A legitimate question to ask is whether they are equivalent: do both semantics predict the same “terminates / diverges / goes wrong” behaviors for any given program? Such an equivalence result strengthens the confidence we have in both semantics. Moreover, it enables us to use whichever semantics is more convenient to prove a property of interest. We first show an implication from natural semantics to terminating reduction sequences.

**Theorem 1** [exec\_terminates] If \( c, s \Rightarrow s' \), then \( (c, s) \xrightarrow{\ast} (\text{skip}, s') \).

The proof is a straightforward induction on a derivation of \( c, s \Rightarrow s' \) and case analysis on the last rule used. Here is a representative case: \( c_1;c_2, s \Rightarrow s' \). By hypothesis, \( c_1; c_2, s \Rightarrow s' \). By inversion, we know that \( c_1, s \Rightarrow s_1 \) and \( c_2, s_1 \Rightarrow s' \) for some intermediate state \( s_1 \). Applying the induction hypothesis twice, we obtain \( (c_1, s) \xrightarrow{\ast} (\text{skip}, s_1) \) and \( (c_2, s_1) \xrightarrow{\ast} (\text{skip}, s') \). A context lemma (proved separately by induction) shows that \( ((c_1;c_2), s) \xrightarrow{\ast} ((\text{skip}; c_2), s_1) \). To obtain the expected result, all we need to do is to assemble the reduction sequences together, using the transitivity of \( \xrightarrow{\ast} \):

\[
((c_1;c_2), s) \xrightarrow{\ast} ((\text{skip}; c_2), s_1) \xrightarrow{\ast} (c_2, s_1) \xrightarrow{\ast} (\text{skip}, s')
\]

The converse implication (from terminating reduction sequences to natural semantics) is more difficult. The idea is to consider mixed executions that start with some reduction steps and finish in one big step using the natural semantics:

\[
(c_1, s_1) \rightarrow \cdots \rightarrow (c_i, s_i) \Rightarrow s'
\]

We first show that the last reduction step can always be “absorbed” by the final big step:

**Lemma 2** [red\_preserves\_exec] If \( (c, s) \rightarrow (c', s') \) and \( c', s' \Rightarrow s'' \), then \( c, s \Rightarrow s'' \).

Combining this lemma with an induction on the sequence of reduction, we obtain the desired semantic implication:

**Theorem 3** [terminates\_exec] If \( (c, s) \xrightarrow{\ast} (\text{skip}, s') \), then \( c, s \Rightarrow s' \).

### 2.4 Natural semantics for divergence

Kahn-style natural semantics correctly characterize programs that terminate, either normally (as in section 2.3) or by going wrong (through the addition of so-called error rules). For a long time it was believed that natural semantics is un-
able to account for divergence. As observed by Grall and Leroy [32], this is not true: diverging executions can also be described in the style of natural semantics, provided a coinductive definition (greatest fixpoint) is used. Define the infinite execution relation $c, s \Rightarrow \infty$ (from initial state $s$, the command $c$ diverges).

\[
\begin{align*}
  & c_1, s \Rightarrow \infty & \text{(execinf\_seq\_left)} \\
  & c_1; c_2, s \Rightarrow \infty &
\end{align*}
\]

\[
\begin{align*}
  & c_1, s \Rightarrow s_1 & c_2, s_1 \Rightarrow \infty & \text{(execinf\_seq\_right)} \\
  & c_1; c_2, s \Rightarrow \infty &
\end{align*}
\]

\[
\begin{align*}
  & c_1, s \Rightarrow \infty \text{ if } [b] s = \text{true} \\
  & c_2, s \Rightarrow \infty \text{ if } [b] s = \text{false} & \text{(execinf\_if)} \\
  & \text{if } b \text{ then } c_1 \text{ else } c_2, s \Rightarrow \infty \\
  & \text{[b] } s = \text{true} & c, s \Rightarrow \infty & \text{(execinf\_while\_body)} \\
  & \text{while } b \text{ do } c \text{ done}, s \Rightarrow \infty &
\end{align*}
\]

\[
\begin{align*}
  & [b] s = \text{true} & c, s \Rightarrow s_1 & \text{while } b \text{ do } c \text{ done}, s_1 \Rightarrow \infty & \text{(execinf\_while\_loop)} \\
  & \text{while } b \text{ do } c \text{ done}, s \Rightarrow \infty &
\end{align*}
\]

As denoted by the double horizontal bars, these rules must be interpreted coinductively as a greatest fixpoint [32, section 2]. Equivalently, the coinductive interpretation corresponds to conclusions of possibly infinite derivation trees, while the inductive interpretation corresponds to finite derivation trees. Coq provides built-in support for coinductive definitions of data types and predicates.

As in section 2.3 and perhaps even more so here, we need to prove an equivalence between the $c, s \Rightarrow \infty$ predicate and the existence of infinite reduction sequences. One implication follows from the decomposition lemma below:

**Lemma 4** [execinf\_red\_step] If $c, s \Rightarrow \infty$, there exists $c'$ and $s'$ such that $(c, s) \Rightarrow (c', s')$ and $c', s' \Rightarrow \infty$.

A simple argument by coinduction, detailed in [32], then concludes the expected implication:

**Theorem 5** [execinf\_diverges] If $c, s \Rightarrow \infty$, then $(c, s) \uparrow$.

The reverse implication uses two inversion lemmas:

- If $((c_1; c_2), s) \uparrow$, either $(c_1, s) \uparrow$ or there exists $s'$ such that $(c_1, s) \Rightarrow (\text{skip}, s')$ and $(c_2, s') \uparrow$.

- If $(\text{while } b \text{ do } c \text{ done}, s) \uparrow$, then $[b] s = \text{true}$ and either $(c, s) \uparrow$ or there exists $s'$ such that $(c, s) \Rightarrow (\text{skip}, s')$ and $(\text{while } b \text{ do } c \text{ done}, s') \uparrow$.

These lemmas follow from determinism of the $\Rightarrow$ relation and the seemingly obvious fact that any reduction sequence is either infinite or stops, after finitely many reductions, on an irreducible configuration:
∀c, s, (c, s) ↗ ∨ ∃c′, ∃s′, (c, s) → (c′, s′) ∧ (c′, s′) ↘

The property above cannot be proved in Coq’s constructive logic: such a constructive proof would be, in essence, a program that decides the halting problem. However, we can add the law of excluded middle (∀P, P ∨ ¬P) to Coq as an axiom, without breaking logical consistency. The fact above can easily be proved from the law of excluded middle.

**Theorem 6 [diverges_execinf]** If (c, s) ↗, then c, s ⇒ ∞.

### 2.5. Definitional interpreter

As mentioned at the end of section 1, we cannot write a Coq function with type cmd → state → state that would execute a command and return its final state whenever the command terminates: this function would not be total. We can, however, define a Coq function I(n, c, s) that executes c in initial state s, taking as extra argument a natural number n used to bound the amount of computation performed. This function returns either ⌊s′⌋ (termination with state s′) or ⊥ (insufficient recursion depth).

\[ I(0, c, s) = \perp \]
\[ I(n + 1, \text{skip}, s) = [s] \]
\[ I(n + 1, x := e, s) = [s[x ← [e] s]] \]
\[ I(n + 1, (c_1 ; c_2), s) = I(n, c_1, s) \triangleright (\lambda s'. I(n, c_2, s')) \]
\[ I(n + 1, (\text{if } b \text{ then } c_1 \text{ else } c_2), s) = I(n, c_1, s) \text{ if } [b] s = \text{true} \]
\[ I(n + 1, (\text{if } \neg b \text{ then } c_1 \text{ else } c_2), s) = I(n, c_2, s) \text{ if } [b] s = \text{false} \]
\[ I(n + 1, (\text{while } b \text{ do } c \text{ done}), s) = [s] \text{ if } [b] s = \text{false} \]
\[ I(n + 1, (\text{while } \neg b \text{ do } c \text{ done}), s) = I(n, c, s) \triangleright (\lambda s'. I(n, \text{while } b \text{ do } c \text{ done}, s')) \]

The “bind” operator \(\triangleright\), reminiscent of monads in functional programming, is defined by \(\perp \triangleright f = \perp\) and \([s] \triangleright f = f(s)\).

A crucial property of this definitional interpreter is that it is monotone with respect to the maximal recursion depth n. Evaluation results are ordered by taking \(\perp \leq [s]\) [resJe].

**Lemma 7 [interp_mon]** (Monotonicity of I.) If \(n \leq m\), then \(I(n, c, s) \leq I(m, c, s)\).

Exploiting this property, we can show partial correctness results of the definitional interpreter with respect to the natural semantics:

**Lemma 8 [interp_exec]** If \(I(n, c, s) = [s']\), then \(c, s \Rightarrow s'\).

**Lemma 9 [exec_interp]** If \(c, s \Rightarrow s'\), there exists an \(n\) such that \(I(n, c, s) = [s']\).

**Lemma 10 [execinf_interp]** If \(c, s \Rightarrow \infty\), then \(I(n, c, s) = \perp\) for all \(n\).
2.6. Denotational semantics

A simple form of denotational semantics [41] can be obtained by “letting \( n \) goes to infinity” in the definitional interpreter.

Lemma 11 \([\text{interp}\limdep]\) For every \( c \), there exists a function \([c]\) from states to evaluation results such that \( \forall s, \exists m, \forall n \geq m, I(n,c,s) = [c] s \).

Again, this result cannot be proved in Coq’s constructive logic and requires the axiom of excluded middle and an axiom of description.

This denotation function \([c]\) satisfies the equations of denotational semantics:

\[
\begin{align*}
[\text{skip}] s &= [s] \\
[x := e] s &= [s][x \leftarrow [e] s] \\
[c_1;c_2] s &= [c_1] s \triangleright (\lambda s'. [c_2] s') \\
\text{if } b \text{ then } c_1 \text{ else } c_2 \text{ s} &= [c_1] s \text{ if } [b] s = \text{true} \\
\text{if } b \text{ then } c_1 \text{ else } c_2 \text{ s} &= [c_2] s \text{ if } [b] s = \text{false} \\
\text{while } b \text{ do } c \text{ done} s &= [c] s \text{ if } [b] s = \text{false} \\
\text{while } b \text{ do } c \text{ done} s &= [c] s \triangleright (\lambda s'. \text{while } b \text{ do } c \text{ done} s') \text{ if } [b] s = \text{true}
\end{align*}
\]

Moreover, \([\text{while } b \text{ do } c \text{ done}]\) is the smallest function from states to results that satisfies the last two equations.

Using these properties of \([c]\), we can show full equivalence between the denotational and natural semantics.

Theorem 12 \([\text{denot}\exec] [\text{exec}\denot] c, s \Rightarrow s' \text{ if and only if } [c] s = [s']\).

Theorem 13 \([\text{denot}\execinf] [\text{execinf}\denot] c, s \Rightarrow \infty \text{ if and only if } [c] s = \perp\).

2.7. Further reading

The material presented in this section is inspired by Nipkow [44] (in Isabelle/HOL, for the IMP language) and by Grall and Leroy [32] (in Coq, for the call-by-value \(\lambda\)-calculus).

We followed Plotkin’s “SOS” presentation [49] of reduction semantics, characterized by structural inductive rules such as \([\text{red}\seq\text{left}]\). An alternate presentation, based on reduction contexts, was introduced by Wright and Felleisen [54] and is very popular to reason about type systems [48].


The definitional interpreter approach was identified by Reynolds in 1972. See [50] for a historical perspective.

3. Axiomatic semantics and program verification

Operational semantics as in section 2 focuses on describing actual executions of programs. In contrast, axiomatic semantics (also called Hoare logic) focuses on verifying logical assertions between the values of programs at various program points. It is the most popular approach to proving the correctness of imperative programs.

3.1. Weak Hoare triples and their rules

Following Hoare’s seminal work [24], we consider logical formulas of the form \{P\} c \{Q\}, meaning “if precondition P holds, the command c does not go wrong, and if it terminates, the postcondition Q holds”. Here, P and Q are arbitrary predicates over states. A formula \{P\} c \{Q\} is called a weak Hoare triple (by opposition with strong Hoare triples discussed in section 3.4, which guarantee termination as well). We first define some useful operations over predicates:

\[
P[x ← e] \overset{\text{def}}{=} \lambda s. P(s[x ← e]) \quad P \land Q \overset{\text{def}}{=} \lambda s. P(s) \land Q(s) \quad P ∨ Q \overset{\text{def}}{=} \lambda s. P(s) ∨ Q(s)
\]

\[
b true \overset{\text{def}}{=} \lambda s. [b] s = true \quad P \implies Q \overset{\text{def}}{=} \forall s, P(s) ⇒ Q(s)
\]

\[
b false \overset{\text{def}}{=} \lambda s. [b] s = false \quad P =⇒ P' \overset{\text{def}}{=} \lambda s. P(s) =⇒ P'(s)
\]

The axiomatic semantics, that is, the set of legal triples \{P\} c \{Q\}, is defined by the following inference rules: [triple]

\[
\{P\} \text{ skip } \{P\} \quad \{P[x ← e]\} x := e \{P\} \quad \{P\} c_1 \{Q\} \quad \{Q\} c_2 \{R\} \quad \{b true \land P\} c_1 \{Q\} \quad \{b false \land P\} c_2 \{Q\} \quad \{P\} \text{ if } b \text{ then } c_1 \text{ else } c_2 \{Q\} \quad \{b true \land P\} c \{P\} \quad \{P\} \text{ while } b \text{ do } c \text{ done } \{b false \land P\} \quad P \implies P' \quad \{P'\} c \{Q'\} \quad Q' \implies Q \quad \{P\} c \{Q\}
\]

Example. The triple \{a = bq + r\} r := r - b; q := q + 1 \{a = bq + r\} is derivable from rules \text{triple}_\text{assign}, \text{triple}_\text{seq} and \text{triple}_\text{consequence} because the following logical equivalences hold:

\[
(a = bq + r)[q ← q + 1] ↔ a = b(q + 1) + r
\]

\[
(a = b(q + 1) + r)[r ← r - b] ↔ a = b(q + 1) + (r - b) = bq + r
\]
3.2. Soundness of the axiomatic semantics

Intuitively, a weak Hoare triple \( \{ P \} c \{ Q \} \) is valid if for all initial states \( s \) such that \( P s \) holds, either \((c, s)\) diverges or it terminates in a state \( s' \) such that \( Q s' \) holds. We capture the latter condition by the predicate \((c, s)\) finally \( Q \), defined coinductively as:

\[
Q(s) \quad \text{finally\_{done}}
\]

\[
(s, s) \quad \text{finally\_Q}
\]

\[
(c, s) \rightarrow (c', s') \quad (c', s') \quad \text{finally\_Q}
\]

\[
(c, s) \quad \text{finally\_Q}
\]

In an inductive interpretation, rule finally_step could only be applied a finite number of steps, and therefore \((c, s)\) finally \( Q \) would be equivalent to \( \exists s'. \quad (c, s) \rightarrow (\text{skip}, s') \land Q(s') \). In the coinductive interpretation, rule finally_step can also be applied infinitely many times, capturing diverging executions as well.

The semantic interpretation \([\{ P \} c \{ Q \}]\) of a triple is, then, the proposition

\[
\forall s, \quad P s \implies (c, s) \quad \text{finally\_Q}
\]

We now proceed to show that if \( \{ P \} c \{ Q \} \) is derivable, the proposition \([\{ P \} c \{ Q \}]\) above holds. We start by some lemmas about the finally predicate.

**Lemma 14** [finally_seq] If \((c_1, s)\) finally \( Q \) and \([\{ Q \} c_2 \{ R \}]\), then \((c_1; c_2, s)\) finally \( R \).

**Lemma 15** [finally_while] If \([\{ b \text{ true} \land P \} c \{ P \}]\) then \([\{ P \} \text{ while } b \text{ do } c \text{ done } \{ b \text{ false} \land P \}]\).

**Lemma 16** [finally_consequence] If \((c, s)\) finally \( Q \) and \( Q \implies Q' \), then \((c, s)\) finally \( Q' \).

We can then prove the expected soundness result by a straightforward induction on a derivation of \( \{ P \} c \{ Q \} \):

**Theorem 17** [triple_correct] If \( \{ P \} c \{ Q \} \) can be derived by the rules of axiomatic semantics, then \([\{ P \} c \{ Q \}]\) holds.

3.3. Generation of verification conditions

In this section, we enrich the syntax of IMP commands with an annotation on while loops (to give the loop invariant) and an assert\((P)\) command to let the user provide assertions.
Annotated commands:

\[
c ::= \text{while } b \text{ do } \{P\} \text{ done} \quad \text{loop with invariant}
\]

\[
| \text{assert}(P) \quad \text{explicit assertion}
\]

\[
| \ldots \quad \text{other commands as in IMP}
\]

Annotated commands can be viewed as regular commands by erasing the \{P\} annotation on loops and turning assert\( (P) \) to skip. [erase]

The \text{wp} function computes the weakest (liberal) precondition for \(c\) given a postcondition \(Q\). [wp]

\[
\text{wp}(\text{skip}, Q) = Q
\]

\[
\text{wp}(x := e, Q) = Q[x \leftarrow e]
\]

\[
\text{wp}((e_1; e_2), Q) = \text{wp}(e_1, \text{wp}(e_2, Q))
\]

\[
\text{wp}((\text{if } b \text{ then } c_1 \text{ else } c_2), Q) = (b \text{ true } \land \text{wp}(c_1, Q)) \lor (b \text{ false } \land \text{wp}(c_2, Q))
\]

\[
\text{wp}((\text{while } b \text{ do } \{P\} \text{ done}), Q) = P
\]

With the same arguments, the \text{vcg} function (verification condition generator) computes a conjunction of implications that must hold for the triple \{\text{wp}(c, Q)\} \text{ c } \{Q\} to hold. [vcg]

\[
\text{vcg}(\text{skip}, Q) = T
\]

\[
\text{vcg}(x := e, Q) = T
\]

\[
\text{vcg}((e_1; e_2), Q) = \text{vcg}(e_1, \text{vcg}(e_2, Q)) \land \text{vcg}(e_2, Q)
\]

\[
\text{vcg}((\text{if } b \text{ then } c_1 \text{ else } c_2), Q) = \text{vcg}(c_1, Q) \land \text{vcg}(c_2, Q)
\]

\[
\text{vcg}((\text{while } b \text{ do } \{P\} \text{ done}), Q) = \text{vcg}(c, P)
\]

\[
\land (b \text{ false } \land P \implies Q)
\]

\[
\land (b \text{ true } \land P \implies \text{wp}(c, P))
\]

\[
\text{vcg}(\text{assert}(P), Q) = P \implies Q
\]

Lemma 18 [vcg_correct] If \text{vcg}(c, Q) holds, then \{\text{wp}(c, Q)\} \text{ c } \{Q\} can be derived by the rules of axiomatic semantics.

The derivation of a Hoare triple \{P\} \text{ c } \{Q\} can therefore be reduced to the computation of the following \text{vcgen}(P, c, Q) logical formula, and its proof. [vcgen]

\[
\text{vcgen}(P, c, Q) \overset{\text{def}}{=} (P \implies \text{wp}(c, Q)) \land \text{vcg}(c, Q)
\]

Theorem 19 [vcgen_correct] If \text{vcgen}(P, c, Q) holds, then \{P\} \text{ c } \{Q\} can be derived by the rules of axiomatic semantics.
Example. Consider the following annotated IMP program $c$:

```plaintext
r := a; q := 0;
while b < r+1 do {I} r := r - b; q := q + 1 done
```

and the following precondition $P$, loop invariant $I$ and postcondition $Q$:

$$
P \overset{\text{def}}{=} \lambda s. s(a) \geq 0 \land s(b) > 0
$$

$$
I \overset{\text{def}}{=} \lambda s. s(r) \geq 0 \land s(b) > 0 \land s(a) = s(b) \times s(q) + s(r)
$$

$$
Q \overset{\text{def}}{=} \lambda s. s(q) = s(a)/s(b)
$$

To prove that $\{ P \} c \{ Q \}$, we apply theorem 19, then ask Coq to compute and simplify the formula $\text{vcgen}(P, c, Q)$. We obtain the conjunction of three implications:

1. $s(a) \geq 0 \land s(b) > 0 \implies s(a) \geq 0 \land s(b) > 0 \land s(a) = s(b) \times 0 + s(a)$
2. $\neg (s(b) < s(r) + 1) \land s(r) \geq 0 \land s(b) > 0 \land s(a) = s(b) \times s(q) + s(r) \implies s(q) = s(a)/s(b)$
3. $s(b) < s(r) + 1 \land s(r) \geq 0 \land s(b) > 0 \land s(a) = s(b) \times s(q) + s(r) \implies s(r) - s(b) \geq 0 \land s(b) > 0 \land s(a) = s(b) \times (s(q) + 1) + (s(r) - s(b))$

which are easy to prove by purely arithmetic reasoning.

3.4. Strong Hoare triples

The axiomatic semantics we have seen so far enables us to prove partial correctness properties of programs, but not their termination. To prove termination as well, we need to use strong Hoare triples $[P] c [Q]$, meaning “if precondition $P$ holds, the command $c$ terminates and moreover the postcondition $Q$ holds”.

The rules defining valid strong Hoare triples are similar to those for weak triples, with the exception of the while rule, which contains additional requirements that ensure termination of the loop. [Triple]

$$
[P] \text{skip} [P] \quad \text{(Triple.skip)}
$$

$$
[P] c_1 [Q] \quad [Q] c_2 [R] \quad \text{(Triple.seq)}
$$

$$
[b \text{ true } \land P] c_1 [Q] \quad [b \text{ false } \land P] c_2 [Q] \quad \text{(Triple.if)}
$$

$$
(\forall v \in \mathbb{Z} \ [b \text{ true } \land e_m = v \land P] \ c \ [0 \leq e_m < v \land P]) \quad \text{(Triple.while)}
$$

$$
[P] \text{ while } b \text{ do } c \text{ done } [b \text{ false } \land P] \quad \text{(Triple.while)}
$$

$$
P \Rightarrow P' \quad [P'] c [Q'] \quad Q' \Rightarrow Q \quad \text{(Triple.consequence)}
$$
In the Triple\_while rule, $e_m$ stands for an expression whose value should decrease but remain nonnegative at each iteration. The precondition $e_m = v$ and the postcondition $0 \leq e_m < v$ capture this fact:

$$e_m = v \overset{\text{def}}{=} \lambda s. \left[ e_m \right] s = v \quad 0 \leq e_m < v \overset{\text{def}}{=} \lambda s. 0 \leq \left[ e_m \right] s < v$$

The $v$ variable therefore denotes the value of the measure expression at the beginning of the loop body. Since it is not statically known in general, rule Triple\_while quantifies universally over every possible $v \in \mathbb{Z}$. Conceptually, rule Triple\_while has infinitely many premises, one for each possible value of $v$. Such infinitely branching inference rules cause no difficulty in Coq.

Note that the Triple\_while rule above is not powerful enough to prove termination for some loops that occur in practice, for example if the termination argument is based on a lexicographic ordering. A more general version of the rule could involve an arbitrary well-founded ordering between states.

The semantic interpretation $\left[ \left[ P \right] c \left[ Q \right] \right]$ of a strong Hoare triple is the proposition

$$\forall s, \ P s \implies \exists s', (c, s \Rightarrow s') \land Q(s') \quad \text{[sem\_Triple]}$$

As previously done for weak triples, we now prove the soundness of the inference rules for strong triples with respect to this semantic interpretation.

**Theorem 20** [Triple\_correct] If $\left[ P \right] c \left[ Q \right]$ can be derived by the rules of axiomatic semantics, then $\left[ \left[ P \right] c \left[ Q \right] \right]$ holds.

The proof is by an outer induction on a derivation of $\left[ P \right] c \left[ Q \right]$ followed, in the while case, by an inner induction on the value of the associated measure expression.

### 3.5. Further reading

The material in this section follows Nipkow [44] (in Isabelle/HOL) and Bertot [12] (in Coq), themselves following Gordon [37].

Separation logic [45,51] extends axiomatic semantics with a notion of local reasoning: assertions carry a domain (in our case, a set of variable; in pointer programs, a set of store locations) and the logic enforces that nothing outside the domain of the triple changes during execution. Examples of mechanized separation logics include Marti et al. [35] in Coq, Tuch et al. [53] in Isabelle/HOL, Appel and Blazy [5] in Coq, and Myreen and Gordon [43] in HOL4.

The generation of verification conditions (section 3.3) is an instance of a more general technique known as “proof by reflection”, which aims at replacing deduction steps by computations [13, chap. 16]. The derivation of $\left\{ P \right\} c \left\{ Q \right\}$ from the rules of section 3.1 (a nonobvious process involving nondeterministic proof search) is replaced by the computation of $\text{vcgen}(P, c, Q)$ (a trivial evaluation of a recursive function application). Proofs by reflection can tremendously speed up the verification of combinatorial properties, as illustrated by Gonthier and Werner’s mechanized proof of the 4-color theorem [22].
4. Compilation to a virtual machine

There are several ways to execute programs:

- Interpretation: a program (the interpreter) traverses the abstract syntax tree of the program to be executed, performing the intended computations on the fly.
- Compilation to native code: before execution, the program is translated to a sequence of machine instructions. These instructions are those of a real microprocessor and are executed in hardware.
- Compilation to virtual machine code: before execution, the program is translated to a sequence of instructions, These instructions are those of a virtual machine. They do not correspond to that of an existing hardware processor, but are chosen close to the basic operations of the source language. Then, the virtual machine code is either interpreted (more efficiently than source-level interpretation) or further translated to real machine code.

In this section, we study the compilation of the IMP language to an appropriate virtual machine.

4.1. The IMP virtual machine

A state of the machine is composed of:

- A fixed code $C$ (a list of instructions).
- A variable program counter $pc$ (an integer position in $C$).
- A variable stack $\sigma$ (a list of integers).
- A store $s$ (mapping variables to integers).

The instruction set is as follows:

\begin{align*}
i & ::= const(n) & \text{push } n \text{ on stack} \\
& | var(x) & \text{push value of } x \\
& | setvar(x) & \text{pop value and assign it to } x \\
& | add & \text{pop two values, push their sum} \\
& | sub & \text{pop two values, push their difference} \\
& | branch(\delta) & \text{unconditional jump} \\
& | bne(\delta) & \text{pop two values, jump if } \neq \\
& | bge(\delta) & \text{pop two values, jump if } \geq \\
& | halt & \text{end of program}
\end{align*}

In branch instructions, $\delta$ is an offset relative to the next instruction.

The dynamic semantics of the machine is given by the following one-step transition relation $\delta$. $C(pc)$ is the instruction at position $pc$ in $C$, if any.
The code \( \text{comp}(e) \) for an expression evaluates \( e \) and pushes its value on top of the stack \([\text{compile-exp}]\). It executes linearly (no branches) and leaves the store unchanged. (This is the familiar translation from algebraic notation to reverse Polish notation.)

\[
\begin{align*}
\text{comp}(x) & = \text{var}(x) \\
\text{comp}(n) & = \text{const}(n) \\
\text{comp}(e_1 + e_2) & = \text{comp}(e_1); \text{comp}(e_2); \text{add} \\
\text{comp}(e_1 - e_2) & = \text{comp}(e_1); \text{comp}(e_2); \text{sub}
\end{align*}
\]
The code \( \text{comp}(b, \delta) \) for a boolean expression falls through if \( b \) is true, and branches to offset \( \delta \) if \( b \) is false.

\[
\begin{align*}
\text{comp}(e_1 = e_2, \delta) &= \text{comp}(e_1); \text{comp}(e_2); \text{bne}(\delta) \\
\text{comp}(e_1 < e_2, \delta) &= \text{comp}(e_1); \text{comp}(e_2); \text{bge}(\delta)
\end{align*}
\]

The code \( \text{comp}(c) \) for a command \( c \) updates the state according to the semantics of \( c \), while leaving the stack unchanged.

\[
\begin{align*}
\text{comp}(\text{skip}) &= \varepsilon \\
\text{comp}(x := e) &= \text{comp}(e); \text{setvar}(x) \\
\text{comp}(c_1; c_2) &= \text{comp}(c_1); \text{comp}(c_2) \\
\text{comp}(\text{if } b \text{ then } c_1 \text{ else } c_2) &= \text{comp}(b); |C_1| + 1; C_1; \text{branch}(|C_2|); C_2 \\
&\quad \text{where } C_1 = \text{comp}(c_1) \text{ and } C_2 = \text{comp}(c_2) \\
\text{comp}(\text{while } b \text{ do } c \text{ done}) &= B; C; \text{branch}(-(|B| + |C| + 1)) \\
&\quad \text{where } C = \text{comp}(c) \text{ and } B = \text{comp}(b, |C| + 1)
\end{align*}
\]

\(|C|\) is the length of a list of instructions \( C \). The mysterious offsets in branch instructions are depicted in figure 2.

Finally, the compilation of a program \( c \) is \( \text{compile}(c) = \text{comp}(c); \text{halt} \).

Combining the compilation scheme with the semantics of the virtual machine, we obtain a new way to execute a program \( c \) in initial state \( s \): start the machine in code \( \text{comp}(c) \) and state \((0, \varepsilon, s)\) (program counter at first instruction of \( \text{comp}(c) \); empty stack; state \( s \)), and observe its behavior. Does this behavior agree with the behavior of \( c \) predicted by the semantics of section 2?

4.3. Notions of semantic preservation

Consider two programs \( P_1 \) and \( P_2 \), possibly in different languages. (For example, \( P_1 \) is an IMP command and \( P_2 \) a sequence of VM instructions.) Under which conditions can we say that \( P_2 \) preserves the semantics of \( P_1 \)?
To make this question precise, we assume given operational semantics for the
two languages that associate to $P_1, P_2$ sets $B(P_1), B(P_2)$ of observable behaviors.
In our case, observable behaviors are: termination on a final state $s$, divergence,
and “going wrong”. The set $B(P)$ contains exactly one element if $P$ has deter-
ministic semantics, two or more otherwise.

Here are several possible formal characterizations of the informal claim that
$P_2$ preserves the semantics of $P_1$.

- Bisimulation (equivalence): $B(P_1) = B(P_2)$
- Backward simulation (refinement): $B(P_1) \supseteq B(P_2)$
- Backward simulation for correct source programs: if $$\text{wrong} \notin B(P_1)$$ then $B(P_1) \supseteq B(P_2)$
- Forward simulation: $B(P_1) \subseteq B(P_2)$
- Forward simulation for correct source programs: if $$\text{wrong} \notin B(P_1)$$ then $B(P_1) \subseteq B(P_2)$

Bisimulation is the strongest notion of semantic preservation, ensuring that
the two programs are indistinguishable. It is often too strong in practice. For
example, the C language has non-deterministic semantics because the evaluation
order for expressions is not fully specified; yet, C compilers choose one partic-
ular evaluation order while generating deterministic machine code; therefore, the
generated code has fewer behaviors than the source code. This intuition corre-
sponds to the backward simulation property defined above: all behaviors of $P_2$
are possible behaviors of $P_1$, but $P_1$ can have more behaviors.

In addition to reducing nondeterminism, compilers routinely optimize away
“going wrong” behaviors. For instance, the source program $P_1$ contains an integer
division $z := x/y$ that can go wrong if $y = 0$, but the compiler eliminated this
division because $z$ is not used afterwards, therefore generating a program $P_2$ that
does not go wrong if $y = 0$. This additional degree of liberty is reflected in the
“backward simulation for correct source programs” above.

Finally, the two “forward simulation” properties reverse the roles of $P_1$ and
$P_2$, expressing the fact that any (non-wrong) behavior of the source program $P_1$
is a possible behavior of the compiled code $P_2$. Such forward simulation proper-
ties are generally much easier to prove than backward simulations, but provide
apparently weaker guarantees: $P_2$ could have additional behaviors, not exhibited
by $P_1$, that are undesirable, such as “going wrong”. This cannot happen, however,
if $P_2$ has deterministic semantics.

Lemma 21 (Simulation and determinism.) If $P_2$ has deterministic semantics, then
“forward simulation for correct programs” implies “backward simulation for cor-
rect programs”.

In conclusion, for deterministic languages such as IMP and IMP virtual ma-
chine code, “forward simulation for correct programs” is an appropriate notion of
semantic preservation to prove the correctness of compilers and program trans-
formations.
4.4. Semantic preservation for the compiler

Recall the informal specification for the code $\text{comp}(e)$ generated by the compilation of expression $e$: it should evaluate $e$ and push its value on top of the stack, execute linearly (no branches), and leave the store unchanged. Formally, we should have $\text{comp}(e) : (0, \sigma, s) \rightarrow ([\text{comp}(e)], ([e], \sigma, s))$ for all stacks $\sigma$ and stores $s$.

Note that $pc = |\text{comp}(e)|$ means that the program counter is one past the last instruction in the sequence $\text{comp}(e)$. To enable a proof by induction, we need to strengthen this result and consider codes of the form $C_1;\text{comp}(e); C_2$, where the code for $e$ is bracketed by two arbitrary code sequences $C_1$ and $C_2$. The program counter, then, should go from $|C_1|$ (pointing to the first instruction of $\text{comp}(e)$) to $|C_1| + |\text{comp}(e)|$ (pointing one past the last instruction of $\text{comp}(e)$, or equivalently to the first instruction of $C_2$).

**Lemma 22 [compile_expr_correct]** For all instruction sequences $C_1, C_2$, stacks $\sigma$ and states $s$, $$C_1;\text{comp}(e); C_2 \vdash ([C_1], \sigma, s) \rightarrow ([C_1] + |\text{comp}(e)|, [e] \sigma, s)$$

The proof is a simple induction on the structure of $e$. Here is a representative case: $e = e_1 + e_2$. Write $v_1 = [e_1]$ and $v_2 = [e_2]$ $s$. The code $C$ is $C_1;\text{comp}(e_1);\text{comp}(e_2); \text{add}; C_2$. Viewing $C$ as $C_1;\text{comp}(e_1); (\text{comp}(e_2); \text{add}; C_2)$, we can apply the induction hypothesis to $e_1$, obtaining the transitions

$$([C_1], \sigma, s) \rightarrow ([C_1] + |\text{comp}(e_1)|, v_1, \sigma, s)$$

Likewise, viewing $C$ as $(C_1;\text{comp}(e_1));\text{comp}(e_2); (\text{add}; C_2)$, we can apply the induction hypothesis to $e_2$, obtaining

$$([C_1;\text{comp}(e_1)], v_1, \sigma, s) \rightarrow ([C_1;\text{comp}(e_1)] + |\text{comp}(e_2)|, v_2, v_1, \sigma, s)$$

Combining these two sequences with an $\text{add}$ transition, we obtain

$$([C_1], \sigma, s) \rightarrow ([C_1;\text{comp}(e_1);\text{comp}(e_2)] + 1, (v_1 + v_2), \sigma, s)$$

which is the desired result.

The statement and proof of correctness for the compilation of boolean expressions is similar. Here, the stack and the store are left unchanged, and control is transferred either to the end of the generated instruction sequence or to the given offset relative to this end, depending on the truth value of the condition.

**Lemma 23 [compile_bool_expr_correct]** For all instruction sequences $C_1, C_2$, stacks $\sigma$ and states $s$, $$C_1;\text{comp}(b, \delta); C_2 \vdash ([C_1], \sigma, s) \rightarrow (pc, \sigma, s)$$

with $pc = |C_1| + |\text{comp}(b)|$ if $[b]$ $s = \text{true}$ and $pc = |C_1| + |\text{comp}(b)| + \delta$ otherwise.
To show semantic preservation between an IMP command and its compiled code, we prove a “forward simulation for correct programs” result. We therefore have two cases to consider: (1) the command terminates normally, and (2) the command diverges. In both cases, we use the natural semantics to conduct the proof, since its compositional nature is a good match for the compositional nature of the compilation scheme.

**Theorem 24** [compile \textunderscore cmd \textunderscore correct \textunderscore terminating] Assume \( c, s \Rightarrow s' \). Then, for all instruction sequences \( C_1, C_2 \) and stack \( \sigma \),

\[
C_1; \text{comp}(c); C_2 \vdash (|C_1|, \sigma, s) \xrightarrow{*} (|C_1| + |\text{comp}(c)|, \sigma, s')
\]

The proof is by induction on a derivation of \( c, s \Rightarrow s' \) and uses the same techniques as that of lemma 22.

For the diverging case, we need the following special-purpose coinduction principle.

**Lemma 25** Let \( X \) be a set of (machine code, machine state) pairs such that

\[
\forall (C, S) \in X, \exists S', (C, S') \in X \land C \vdash S \xrightarrow{*} S'.
\]

Then, for all \((C, S) \in X\), we have \( C \vdash S \uparrow \) (there exists an infinite sequence of transitions starting from \( S \)).

The following theorem follows from the coinduction principle above applied to the set

\[
X = \{ (C_1; \text{comp}(c); C_2, (|C_1|, \sigma, s)) \mid c, s \Rightarrow \infty \}.
\]

**Theorem 26** [compile \textunderscore cmd \textunderscore correct \textunderscore diverging] Assume \( c, s \Rightarrow \infty \). Then, for all instruction sequences \( C_1, C_2 \) and stacks \( \sigma \),

\[
C_1; \text{comp}(c); C_2 \vdash (|C_1|, \sigma, s) \uparrow
\]

This completes the proof of forward simulation for correct programs.

4.5. Further reading

The virtual machine used in this section matches a small subset of the Java Virtual Machine [34]. Other examples of mechanized verification of nonoptimizing compilers producing virtual machine code include Bertot [10] (for the IMP language), Klein and Nipkow [29] (for a subset of Java), and Grall and Leroy [32] (for call-by-value \( \lambda \)-calculus). The latter two show forward simulation results; Bertot shows both forward and backward simulation, and concludes that backward simulation is considerably more difficult to prove. Other examples of difficult backward simulation arguments (not mechanized) can be found in [23], for call-by-name and call-by-value \( \lambda \)-calculus.
Lemma 22 (correctness of compilation of arithmetic expression to stack machine code) is historically important: it is the oldest published compiler correctness proof (McCarthy and Painter [36], in 1967) and the oldest mechanized compiler correctness proof (Milner and Weyhrauch, [39], in 1972). Since then, a great many correctness proofs for compilers and compilation passes have been published, some of them being mechanized: Dave’s bibliography [19] lists 99 references up to 2002.

5. An example of optimizing program transformation: dead code elimination

Compilers are typically structured as a sequence of program transformations, also called passes. Some passes translate from one language to another, lower-level language, closer to machine code. The compilation scheme of section 4 is a representative example. Other passes are optimizations: they rewrite the program to an equivalent, but more efficient program. For example, the optimized program runs faster, or is smaller.

In this section, we study a representative optimization: dead code elimination. The purpose of this optimization, performed on the IMP source language, is to remove assignments \( x := e \) (turning them into \texttt{skip} instructions) such that the value of \( x \) is not used in the remainder of the program. This reduces both the execution time and the code size.

Example. Consider the command \( x := 1; y := y + 1; x := 2 \). The assignment \( x := 1 \) can always be eliminated since \( x \) is not referenced before being redefined by \( x := 2 \).

To detect the fact that the value of a variable is not used later, we need a static analysis known as \textit{liveness analysis}.

5.1. Liveness analysis

A variable is \textit{dead} at a program point if its value is not used later in the execution of the program: either the variable is never mentioned again, or it is always redefined before further use. A variable is \textit{live} if it is not dead.

Given a set \( A \) of variables live “after” a command \( c \), the function \( \text{live}(c, A) \) over-approximates the set of variables live “before” the command \( [\text{live}] \). It proceeds by a form of reverse execution of \( c \), conservatively assuming that conditional branches can go both ways. \( FV \) computes the set of variables referenced in an expression \( \text{fv} \). 

\[
\begin{align*}
\text{live}(&\text{skip}, A) = A \\
\text{live}(x := e, A) = \begin{cases} (A \setminus \{x\}) \cup FV(e) & \text{if } x \in A; \\
A & \text{if } x \notin A. \end{cases} \\
\text{live}(c_1; c_2, A) = \text{live}(c_1, \text{live}(c_2, A)) \\
\text{live}(&\text{if } b \text{ then } c_1 \text{ else } c_2, A) = FV(b) \cup \text{live}(c_1, A) \cup \text{live}(c_2, A) \\
\text{live}(\text{while } b \text{ do } c \text{ done}, A) = \text{fix}(\lambda X. A \cup FV(b) \cup \text{live}(c, X))
\end{align*}
\]
Fix $F$ is a function from sets of variables to sets of variables, $\text{fix}(F)$ is supposed to compute a post-fixpoint of $F$, that is, a set $X$ such that $F(X) \subseteq X$. Typically, $F$ is iterated $n$ times, starting from the empty set, until we reach an $n$ such that $F^{n+1}(\emptyset) \subseteq F^n(\emptyset)$. Ensuring termination of such an iteration is, in general, a difficult problem. (See section 5.4 for discussion.) To keep things simple, we bound arbitrarily to $N$ the number of iterations, and return a default over-approximation if a post-fixpoint cannot be found within $N$ iterations:

$$\text{fix}(F, \text{default}) = \begin{cases} F^n(\emptyset) & \text{if } \exists n \leq N, F^{n+1}(\emptyset) \subseteq F^n(\emptyset); \\ \text{default} & \text{otherwise} \end{cases}$$

Here, a suitable default is $A \cup FV(\text{while } b \text{ do } c \text{ done})$, the set of variables live “after” the loop or referenced within the loop.

$$\text{live}(\text{while } b \text{ do } c \text{ done}, A) = \text{fix}(\lambda X. A \cup FV(b) \cup \text{live}(c, X), A \cup FV(\text{while } b \text{ do } c \text{ done}))$$

**Lemma 27 [live_while_charact]** Let $A' = \text{live}(\text{while } b \text{ do } c \text{ done}, A)$. Then:

$$FV(b) \subseteq A' \quad A \subseteq A' \quad \text{live}(c, A') \subseteq A'$$

### 5.2. Dead code elimination

The program transformation that eliminates dead code is, then: [dce]

$$\text{dce}(\text{skip}, A) = \text{skip}$$

$$\text{dce}(x := e, A) = \begin{cases} x := e & \text{if } x \in A; \\ \text{skip} & \text{if } x \notin A \end{cases}$$

$$\text{dce}(c_1; c_2, A) = \text{dce}(c_1, \text{live}(c_2, A)); \text{dce}(c_2, A)$$

$$\text{dce}((\text{if } b \text{ then } c_1 \text{ else } c_2), A) = \text{if } b \text{ then } \text{dce}(c_1, A) \text{ else } \text{dce}(c_2, A)$$

$$\text{dce}(\text{while } b \text{ do } c \text{ done}, A) = \text{while } b \text{ do } \text{dce}(c, A) \text{ done}$$

**Example.** Consider again the “Euclidean division” program $c$:

$$r := a; q := 0; \text{ while } b < r+1 \text{ do } r := r - b; q := q + 1 \text{ done}$$

If $q$ is not live “after” ($q \notin A$), it is not live throughout this program either. Therefore, $\text{dce}(c, A)$ produces

$$r := a; \text{ skip}; \text{ while } b < r+1 \text{ do } r := r - b; \text{ skip } \text{ done}$$

The useless computations of $q$ have been eliminated entirely, in a process similar to program slicing. In contrast, if $q$ is live “after” ($q \in A$), all computations are necessary and $\text{dce}(c, A)$ returns $c$ unchanged.
5.3. Correctness of the transformation

We show a “forward simulation for correct programs” property:

- If \( c, s \Downarrow s' \), then \( \text{dce}(c, A), s \Downarrow s'' \) for some \( s'' \) related to \( s' \).
- If \( c, s \Uparrow \), then \( \text{dce}(c, A), s \Uparrow \).

However, the program \( \text{dce}(c, A) \) performs fewer assignments than \( c \), therefore the final states can differ on the values of dead variables. We define agreement between two states \( s, s' \) with respect to a set of live variables \( A \).

\[
\text{agree} \quad s \approx s' : A \quad \overset{\text{def}}{=} \quad \forall x \in A, \ s(x) = s'(x)
\]

Lemma 28 [eval_expr_agree] [eval_bool_expr_agree] Assume \( s \approx s' : A \). If \( \text{FV}(e) \subseteq A \), then \( \llbracket e \rrbracket s \approx \llbracket e \rrbracket s' \). If \( \text{FV}(b) \subseteq A \), then \( \llbracket b \rrbracket s \approx \llbracket b \rrbracket s' \).

The following two key lemmas show that agreement is preserved by parallel assignment to a live variable, or by unilateral assignment to a dead variable. The latter case corresponds to the replacement of \( x := e \) by \( \text{skip} \).

Lemma 29 [agree_update_live] (Assignment to a live variable.) If \( s \approx s' : A \setminus \{x\} \), then \( s[x \leftarrow v] \approx s'[x \leftarrow v] : A \).

Lemma 30 [agree_update_dead] (Assignment to a dead variable.) If \( s \approx s' : A \) and \( x \notin A \), then \( s[x \leftarrow v] \approx s' : A \).

Using these lemmas, we can show forward simulation diagrams both for terminating and diverging commands \( c \). In both cases, we assume agreement on the variables live “before” \( c \), namely \( \text{live}(c, A) \).

Theorem 31 [dce_correct_terminating] If \( c, s \Rightarrow s' \) and \( s \approx s_1 : \text{live}(c, A) \), then there exists \( s'_1 \) such that \( \text{dce}(c, A), s_1 \Rightarrow s'_1 \) and \( s' \approx s'_1 : A \).

Theorem 32 [dce_correct_diverging] If \( c, s \Rightarrow \infty \) and \( s \approx s_1 : \text{live}(c, A) \), then \( \text{dce}(c, A), s_1 \Rightarrow \infty \).

5.4. Further reading

Dozens of compiler optimizations are known, each targeting a particular class of inefficiencies. See Appel [3] for an introduction to optimization, and Muchnick [42] for a catalog of classic optimizations.

The results of liveness analysis can be exploited to perform register allocation (a crucial optimization performance-wise), following Chaitin’s approach [17] [3, chap. 11]: coloring of an interference graph. A mechanized proof of correctness for graph coloring-based register allocation, extending the proof given in this section, is described by Leroy [31,30].

Liveness analysis is an instance of a more general class of static analyses called dataflow analyses [3, chap. 17], themselves being a special case of abstract interpretation. Bertot et al. [14] and Leroy [30] prove, in Coq, the correctness of
several optimizations based on dataflow analyses, such as constant propagation
and common subexpression elimination. Cachera et al. [16] present a reusable Coq
framework for dataflow analyses.

Dataflow analyses are generally carried on an unstructured representation
of the program called the control-flow graph. Dataflow equations are set up between
the nodes of this graph, then solved by one global fixpoint iteration, often based
on Kildall’s worklist algorithm [27]. This is more efficient than the approach we
described (computing a local fixpoint for each loop), which can be exponential
in the nesting degree of loops. Kildall’s worklist algorithm has been mechanically
verified many times [14,18,29].

The effective computation of fixpoints is a central issue in static analysis.
Theorems such as Knaster-Tarski’s show the existence of fixpoints in many cases,
and can be mechanized [47,15], but fail to provide effective algorithms. Noetherian
recursion can be used if the domain of the analysis is well founded (no infinite
chains) [13, chap. 15], but this property is difficult to ensure in practice [16]. The
shortcut we took in this section (bounding arbitrarily the number of iterations)
is inelegant but a reasonable engineering compromise.

6. State of the art and current trends

While this lecture was illustrated using “toy” languages and machines, the tech-
niques we presented, based on operational and axiomatic semantics and on their
mechanization using proof assistants, do scale to realistic programming languages
and systems. Here are some recent achievements using similar techniques, in re-
verse chronological order.

- The verification of the seL4 secure micro-kernel (http://nicta.com.au/
  research/projects/14.verified/) [28].
- The CompCert verified compiler: a realistic, moderately-optimizing com-
piler for a large subset of the C language down to PowerPC and ARM
assembly code. (http://compcert.inria.fr/) [31].
- The Verisoft project (http://www.verisoft.de/), which aims at the end-
to-end formal verification of a complete embedded system, from hardware
to application.
- Formal specifications of the Java / Java Card virtual machines and mech-
anized verifications of the Java bytecode verifier: Ninja [29], Jakarta [7],
Bicolano (http://mobius.inria.fr/twiki/bin/view/Bicolano), and the Kestrel Institute project (http://www.kestrel.edu/home/projects/
java/).
- Formal verification of the ARM6 processor micro-architecture against the
ARM instruction set specification [21]
- The “foundational” approach to Proof-Carrying Code [4].
- The CLI stack: a formally verified microprocessor and compiler from
an assembly-level language (http://www.cs.utexas.edu/~moore/
best-ideas/piton/index.html) [40].

Here are some active research topics in this area.
Combining static analysis and program proof. Static analysis can be viewed as the automatic generation of logical assertions, enabling the results of static analysis to be verified a posteriori using a program logic, and facilitating the annotation of existing code with logical assertions.

Proof-preserving compilation. Given a source program annotated with assertions and a proof in axiomatic semantics, can we produce machine code annotated with the corresponding assertions and the corresponding proof? [8,33].

Binders and $\alpha$-conversion. A major obstacle to the mechanization of rich language semantics and advanced type systems is the handling of bound variables and the fact that terms containing binders are equal modulo $\alpha$-conversion of bound variables. The POPLmark challenge explores this issue [6].

Shared-memory concurrency. Shared-memory concurrency raises major semantic difficulties, ranging from formalizing the “weakly-consistent” memory models implemented by today’s multicore processors [52] to mechanizing program logics appropriate for proving concurrent programs correct [20,25].

Progressing towards fully-verified development and verification environments for high-assurance software. Beyond verifying compilers and other code generation tools, we’d like to gain formal assurance in the correctness of program verification tools such as static analyzers and program provers.

References


