Concepts of Programming Languages

Judgements, Inference Rules & Proofs

Lecturer: Gabriele Keller
Tutor: Liam O’Connor
University of New South Wales
School of Computer Sciences & Engineering
Sydney, Australia

COMP 3161/9161

Our Toolbox

- Formalisation of programming languages (PLs)
  - ★ to reason about PLs, we need a language in which we can describe PLs and their properties
  - ★ a language to talk about other languages is called a meta-language
  - ★ to be sufficiently precise, we need a formal language
- This is what we need to be able to describe:
  - ★ language grammar *syntax*
  - ★ scoping rules *static semantics*
  - ★ type systems *static semantics*
  - ★ execution behaviour *dynamic semantics*

Fortunately, we can use natural deduction/inference rules for all of these tasks!!

Judgements and Inference Rules

Definition: *Judgement*

A *judgement* is a statement asserting a certain property for an object

Examples

- ★ 3+4*5 is a valid arithmetic expression
- ★ the string *"madam"* is a palindrome
- ★ 0.21312423 is a floating point value

A formal notation: we denote that property A holds for object s by writing $s\ A$

- ★ formally, s is an element of a universe U (a set) where
  - $A \subseteq U$ and $s \in A$
  - in our case, U will usually be the set of strings or terms

Inference Rules

Definition: *Inference Rules*

Given judgements J, J_1, J_2 up to J_n, an inference rule is an implication of the form:

If J_1, J_2, up to J_n are inferable, then J is inferable

A formal notation: we denote an inference rule formally by writing

$$\frac{J_{,1},\ J_2\ \ldots\ J_n}{J}$$

Terminology:

- We call J_1 to J_n the premises of the rule and
- J its conclusion
- If a rule has no premise, it is called an axiom

Examples

- Using inference rules to define the set of natural numbers
  - ★ to assert that n is a natural number, we write n ***nat***
- Inference rules to define this judgement
  - ★ "0 is a natural number" (axiom)

$$\frac{}{0\ \textbf{\textit{nat}}}$$

  - ★ "if n is a natural number, then $s(n)$ is a natural number (s for *successor*)

$$\frac{n\ \textbf{\textit{nat}}}{s(n)\ \textbf{\textit{nat}}}$$

  - ★ this set of rules characterises the set of syntactic objects

$$\textbf{\textit{nat}} = \{0, s(0), s(s(0)), s(s(s(0))), ...\}$$

Examples

- Using inference rules to define the set of even and odd natural numbers
  - ★ n ***even*** and n ***odd***
- Inference rules used to define the judgement
  - ★ “o is even” (axiom)

$$\frac{}{o\ \textbf{\textit{even}}}$$

  - ★ “if n is even, then $s(s(n))$ is even”

$$\frac{n\ \textbf{\textit{even}}}{s(s(n))\ \textbf{\textit{even}}}$$

  - ★ “if n is even, then $s(n)$ is odd”

$$\frac{n\ \textbf{\textit{even}}}{s(n)\ \textbf{\textit{odd}}}$$

Proofs by natural deduction

- What we covered:
  - ★ definitions of sets/properties using judgements
  - ★ using inference rules to describe the elements of a set
- What we want to do
  - ★ how can we formally show that an object is an element of such a set?
    - a natural number is odd or even
    - a program is valid in a particular language
- Natural deduction: to show that *s A* holds
  1) find a rule whose conclusion matches *s A*
  2) show that the precondition of the rule holds
  3) continue until all preconditions have been reduced to axioms

Natural deduction

- Example: show that $s(s(s(s(o))))$ is even
- Let's start informally
  - ★ $s(s(s(s(o))))$ is even if $s(s(o))$ is even
  - ★ $s(s(o))$ is even if o is even
  - ★ o is even
- Note: the preconditions of the rules we use become proof obligations

Grammars as inference rules

- Example: take the set of properly matched parentheses

  $M = \{\varepsilon,\ (\,),\ (\,(\,)\,),\ (\,)\,(\,),\ (\,(\,)\,(\,)\,), (\,)\,(\,)\,(\,), \ldots\}$

- Informally
  - the empty string (denoted by ε) is in *M*
  - if s_1 and s_2 are in *M*, so is $s_1 s_2$ (concatenation)
  - if *s* is in *M*, so is **(***s***)**
- Formal definition as EBNF
  - $M \rightarrow \varepsilon \mid MM \mid \mathbf{(}M\mathbf{)}$

Grammars as inference rules

Definition by inference rules

(1) the empty string is in *M*

$$(1)\quad \frac{}{\varepsilon \quad M}$$

(2) if s_1 and s_2 are in *M*, so is $s_1 s_2$ (concatenation)

$$(2)\quad \frac{s_1\ M \qquad s_2\ M}{s_1 s_2\ M}$$

(3) if s is in *M*, so is **(**s**)**

$$(3)\quad \frac{s\ M}{\mathbf{(}s\mathbf{)}\ M}$$

Natural deduction

- Show that **() (())** *M*

$$\dfrac{\dfrac{\dfrac{}{\boldsymbol{\varepsilon}\ M}\,(1)}{\mathbf{()}\ M}\,(3) \qquad \dfrac{\dfrac{\dfrac{}{\boldsymbol{\varepsilon}\ M}\,(1)}{\mathbf{()}\ M}\,(3)}{\mathbf{(())}\ M}\,(3)}{\underbrace{\mathbf{()}}_{s_1}\,\underbrace{\mathbf{(())}}_{s_2}\ M}\,(2)$$

$$(1)\quad \dfrac{}{\varepsilon\ \ M}$$

$$(2)\quad \dfrac{s_1\ M \qquad s_2\ M}{s_1 s_2\ M}$$

$$(3)\quad \dfrac{s\ M}{\mathbf{(}s\mathbf{)}\ M}$$

- But what happens if we start with Rule (3) instead?
    - if we're running into a `dead end' trying to prove a judgement, it doesn't mean that this judgement is not derivable

Admissible and derivable rules

- What happens if we add the following rule to the system?

$$\frac{s \quad M}{\mathbf{((}s\mathbf{))}\ M}$$

  - this rule is derivable wrt to the original three - it's the same as applying Rule (3) twice - adding it to the rules would not add any new objects to *M*
- And this?

$$\frac{\mathbf{()}s \quad M}{s\ M}$$

  - this rule is admissible wrt to the original three rules, because it doesn't add any new objects to M, but it is not derivable (not just a combination of the original rules)
- And this?

$$\frac{\mathbf{(}s\mathbf{)} \quad M}{s\ M}$$

  - not admissible: we could derive **)(** M using this rule!

UNSW
THE UNIVERSITY OF NEW SOUTH WALES
SYDNEY • AUSTRALIA

Rule Induction

- We call a set of inference rules an inductive definition of a judgement if the rules are exhaustive; i.e,
  - ★ if a judgement holds, it can be inferred from the rules, and
  - ★ if a judgement can be inferred, it holds
- Example: Rules (1)-(3) of *M* are an inductive definition of *M*:
  - for every string s of properly matched parenthesis, we can infer *s M*
  - whenever we can infer *s M*, s really is a string of properly matched parentheses
- If we want to show that a property holds for every element of an inductively defined set, how can we do this?
  - ★ every string *s* in *M* has the same number of opening and closing parentheses

Rule Induction (structural induction)

(1)

$$(1)\ \frac{}{\varepsilon\ \ M}$$

(2)

$$(2)\ \frac{s_1\ M \quad s_2\ M}{s_1 s_2\ M}$$

(3)

$$(3)\ \frac{s\ M}{(\,s\,)\ M}$$

Rule Induction

Definition: *Rule Induction*

Given a set of rules R, we can prove inductively that a property P holds for all judgements that can be inferred from R:

For each rule of the form

$$\frac{J_1,\ J_2,\ \ldots\ ,J_n}{J}$$

show that

if P holds for J_1 to J_n, then P holds for J.

Base cases and induction steps:

- axioms form the base case of the induction
- all other rules form the induction steps
- the J_i become the Induction Hypothesis

Rule Induction over Natural Numbers

- We have two rules which define the natural numbers:

$$\frac{}{o\ \textbf{\textit{nat}}}$$

$$\frac{n\ \textbf{\textit{nat}}}{s(n)\ \textbf{\textit{nat}}}$$

- Therefore, if we can show that a property *P*
  - holds for o and
  - holds for $s(n)$ if (under the assumption that) it holds for n

  we have shown that it holds for any n in ***nat***

Induction over natural numbers is just a special case of rule induction!

Rule induction example

- Show that: if $s\ M$ is inferable by rules (1)-(3), then s has the same number of opening and closing parenthesis

- Formalise the property:

  ★ let $pl(s)$ be the number of left parens and $pr(s)$ the number of right parens , then we have to show that

$$pl(s) = pr(s) \text{ for all } s\ M$$

- Proof outline: we have to consider three cases (one case per rule). If $s\ M$ was inferred using

  - Rule (1), then $s = \varepsilon$
  - Rule (2), then $s = s_1 s_2$, for some $s_1\ M$ and $s_2\ M$
  - Rule (3), then $s = \mathbf{(}s_1\mathbf{)}$ for some $s_1\ M$

Proof

- Proof case for Rule (1)
  - ★ Rule (1) is an axiom ⇒ base case (usually easy to prove)
    - as $s = \varepsilon$, we have $pl(s) = 0 = pr(s)$
- Proof case for Rule (2)
  - ★ need to show that
    - if $pl(s_1) = pr(s_2)$, and $pl(s_2) = pr(s_2)$, then $pl\ (s_1 s_2) = pr\ (s_1 s_2)$
- Proof case for Rule (3)
  - ★ need to show that
    - if $pl(s_1) = pr(s_1)$, then $pl(\mathbf{(}s_1\mathbf{)}) = pr(\mathbf{(}s_1\mathbf{)})$

Simultaneous Inductive Definitions

- As an example, consider the following grammar

$$Expr \to Int \mid \textbf{(}\ Expr\ \textbf{)} \mid Expr\ \textbf{+}\ Expr \mid Expr\ \textbf{*}\ Expr$$

where *Int* is an integer constant

- It corresponds to the following inference rules

$$\frac{}{i\ Expr}\ i \in Int \qquad \frac{e\ Expr}{\textbf{(}e\textbf{)}\ Expr}$$

$$\frac{e_1\ Expr \quad e_2\ Expr}{e_1 \textbf{ + } e_2\ \ Expr} \qquad \frac{e_1\ Expr \quad e_2\ Expr}{e_1 \textbf{ * } e_2\ \ Expr}$$

Simultaneous Inductive Definitions

- Infer **1 + 2 * 3** *Expr*

$$\dfrac{\dfrac{\mathbf{1}\ \mathit{Int}}{\mathbf{1}\ \mathit{Expr}} \qquad \dfrac{\dfrac{\mathbf{2}\ \mathit{Int}}{\mathbf{2}\ \mathit{Expr}} \quad \dfrac{\mathbf{3}\ \mathit{Int}}{\mathbf{3}\ \mathit{Expr}}}{\mathbf{2*3}\ \mathit{Expr}}}{\mathbf{1+2*3}\ \mathit{Expr}}
\qquad\qquad
\dfrac{\dfrac{\dfrac{\mathbf{1}\ \mathit{Int}}{\mathbf{1}\ \mathit{Expr}} \quad \dfrac{\mathbf{2}\ \mathit{Int}}{\mathbf{2}\ \mathit{Expr}}}{\mathbf{1+2}\ \mathit{Expr}} \qquad \dfrac{\mathbf{3}\ \mathit{Int}}{\mathbf{3}\ \mathit{Expr}}}{\mathbf{1+2*3}\ \mathit{Expr}}$$

- The grammar is ambiguous!
  - we don’t want ambiguous grammars, as they lead to ambiguous interpretations of the program
- We need alternative inference rules to reflect the fact that
  - addition and multiplication are left associative
  - multiplication has a higher precedence than addition

Simultaneous Inductive Definitons

- Alternative inference rules

$$\frac{e_1\ SExpr \quad e_2\ PExpr}{e_1 + e_2\ \ SExpr} \qquad \frac{e\ PExpr}{e\ SExpr}$$

$$\frac{e_1\ PExpr \quad e_2\ FExpr}{e_1 * e_2\ \ PExpr} \qquad \frac{e\ FExpr}{e\ PExpr}$$

$$\frac{}{i\ FExpr}\ i \in Int \qquad \frac{e\ SExpr}{(e)\ FExpr}$$

  - SExpr corresponds to Expr in the previous definition
  - FExpr and PExpr are auxiliary symbols to define SExpr
    - $FExpr \subseteq PExpr \subseteq SExpr$
  - Simultaneous inductive definition: SExpr depends on PExpr, PExpr on FExpr, which in turn depends on SExpr

UNSW THE UNIVERSITY OF NEW SOUTH WALES SYDNEY • AUSTRALIA

Rule Induction and Simultaneous Inductive Definitions

- The principle of rule induction extends to simultaneous inductive definitions
- To prove a property P of a term in $SExpr$, we need to show that
  - it holds for all integer values
  - if it holds for two terms e_1 and e_2, it holds for e_1 **+** e_2
  - if it holds for two terms e_1 and e_2, it holds for e_1 ***** e_2
  - if it holds for a term e, it holds for **(**e**)**

$$\frac{e_1\ SExpr \qquad e_2\ PExpr}{e_1 \mathbin{\mathbf{+}} e_2\ \ SExpr} \qquad \frac{e\ PExpr}{e\ SExpr}$$

$$\frac{e_1\ PExpr \qquad e_2\ FExpr}{e_1 \mathbin{\mathbf{*}} e_2\ \ PExpr} \qquad \frac{e\ FExpr}{e\ PExpr}$$

$$\frac{}{i\ FExpr}\ i \in Int \qquad \frac{e\ SExpr}{\mathbf{(}e\mathbf{)}\ FExpr}$$

Ambiguous Grammars

- M is also ambiguous:
  - ★ empty string problem (ε = ε ε = ε ε ε = ...)

$$\text{(M-1)}\ \frac{}{\varepsilon\ M} \qquad \text{(M-2)}\ \frac{s_1\ M \quad s_2\ M}{s_1 s_2\ M} \qquad \text{(M-3)}\ \frac{s\ M}{\mathbf{(}s\mathbf{)}\ M}$$

- Example: derive **()** *M*

$$\text{(M-3)}\ \dfrac{\text{(M-1)}\ \dfrac{}{\varepsilon\ M}}{\mathbf{(}\varepsilon\mathbf{)}\ M}$$

$$\text{(M-3)}\ \dfrac{\text{(M-2)}\ \dfrac{\text{(M-1)}\ \dfrac{}{\varepsilon\ M} \qquad \dfrac{}{\varepsilon\ M}\ \text{(M-1)}}{\varepsilon\ \varepsilon\ \ M}}{\mathbf{(}\varepsilon\ \varepsilon\mathbf{)}\ M}$$

Ambiguos Grammars

- How can we solve this?
  - ★ we regard the expressions as a possibly empty list *L* of nested parenthesised expressions *N*

$$(\text{L-1})\ \frac{}{\varepsilon\ L} \qquad (\text{L-2})\ \frac{s_1\ N \quad s_2\ L}{s_1 s_2\ L} \qquad (\text{N-1})\ \frac{s\ L}{\mathbf{(}s\mathbf{)}\ N}$$

- L corresponds to M in the previous definition, N is just an auxiliary construct
- L is defined in terms on N, and vice versa
- this is another example of a simultaneous inductive definition

Ambiguos Grammars

- do both set of rules really define the same language? Is $L = M$?
- we need to show that they are indeed the same, we need to show that *s M* if and only if (iff) *s L*:

  (1) *s M* implies *s L* (*i.e., $M \subseteq L$*)

  (2) *s L* implied *s M* (*i.e., $L \subseteq M$*)

- *we can't derive it directly from the given rules*

$$\text{(L-1)}\ \frac{}{\varepsilon} \qquad \text{(L-2)}\ \frac{s_1\ N \quad s_2\ L}{s_1 s_2\ L} \qquad \text{(N-1)}\ \frac{s\ L}{\mathbf{(}s\mathbf{)}\ N}$$

$$\text{(M-1)}\ \frac{}{\varepsilon} \qquad \text{(M-2)}\ \frac{s_1\ M \quad s_2\ M}{s_1 s_2\ M} \qquad \text{(M-3)}\ \frac{s\ M}{\mathbf{(}s\mathbf{)}\ M}$$

Proving L = M

- we can use rule induction
- Part (1) of proof: show that $s\ M$ implies $s\ L$ ($M \subseteq L$)
- one case per inference rule of M

(1) $s = \varepsilon$ (base case)

(2) $s = \mathbf{(}s_1\mathbf{)}$ for some string $s_1\ M$ (induction step 1)

(3) $s = s_1 s_2$ for some $s_1\ M$ and $s_2\ M$ (induction step 2)

(L-1) $\dfrac{}{\varepsilon}$ (L-2) $\dfrac{s_1\ N \quad s_2\ L}{s_1 s_2\ L}$ (N-1) $\dfrac{s\ L}{\mathbf{(}s\mathbf{)}\ N}$

(M-1) $\dfrac{}{\varepsilon}$ (M-2) $\dfrac{s_1\ M \quad s_2\ M}{s_1 s_2\ M}$ (M-3) $\dfrac{s\ M}{\mathbf{(}s\mathbf{)}\ M}$

Proving L = M

- Part (1), Case (1): $s = \varepsilon$

$$\text{(L-1)}\ \frac{}{\varepsilon\ L}$$

- Part (1), Case (2): $s = \mathbf{(}s_1\mathbf{)}$ for some string $s_1\ M$

  ★ Induction hypothesis: $s_1\ L$

$$\text{(L-2)}\ \frac{\text{(N-1)}\ \dfrac{\text{(I.H.)}\ \dfrac{}{s_1\ L}}{\mathbf{(}s_1\mathbf{)}\ N} \qquad \dfrac{}{\varepsilon\ L}\ \text{(L-1)}}{\mathbf{(}s_1\mathbf{)}\ L}$$

$$\text{(L-1)}\ \frac{}{\varepsilon} \qquad \text{(L-2)}\ \frac{s_1\ N \quad s_2\ L}{s_1 s_2\ L} \qquad \text{(N-1)}\ \frac{s\ L}{\mathbf{(}s\mathbf{)}\ N}$$

$$\text{(M-1)}\ \frac{}{\varepsilon} \qquad \text{(M-2)}\ \frac{s_1\ M \quad s_2\ M}{s_1 s_2\ M} \qquad \text{(M-3)}\ \frac{s\ M}{\mathbf{(}s\mathbf{)}\ M}$$

Proving L = M

- Part (1), Case (3): $s = s_1 s_2$ for some $s_1\ M$, $s_2\ M$
  - ★ Induction hypothesis 1: $s_1\ L$
  - ★ Induction hypothesis 2: $s_2\ L$

doesn't work - we can't be sure that s_1 is actually in N!

$$\text{(L-2)}\ \frac{\dfrac{????}{s_1\ N} \qquad \dfrac{}{s_2\ L}\ \text{(I.H.-2)}}{s_1 s_2\ L}$$

$$\text{(L-1)}\ \frac{}{\varepsilon} \qquad \text{(L-2)}\ \frac{s_1\ N \quad s_2\ L}{s_1 s_2\ L} \qquad \text{(N-1)}\ \frac{s\ L}{(s)\ N}$$

$$\text{(M-1)}\ \frac{}{\varepsilon} \qquad \text{(M-2)}\ \frac{s_1\ M \quad s_2\ M}{s_1 s_2\ M} \qquad \text{(M-3)}\ \frac{s\ M}{(s)\ M}$$

Proving L = M

- To summarise, we have
  - ★ s_1 L (I.H.-1)
  - ★ s_2 L (I.H.-2), and need to show that this implies
  - ★ $s_1 s_2$ L
- unfortunately, we can't directly derive it from any of the rules we have
- can we use rule induction to prove the lemma:

$$\frac{s_1\ L \quad s_2\ L}{s_1 s_2\ L}$$

(L-1) $\dfrac{}{\varepsilon\ L}$ (L-2) $\dfrac{s_1\ N \quad s_2\ L}{s_1 s_2\ L}$ (N-1) $\dfrac{s\ L}{(s)\ N}$

- Prove: $\dfrac{s\ L \quad t\ L}{st\ L}$
- To do this, we assume

  (A-1) $s\ L$

  (A-2) $t\ L$, and show that this implies st L
- Induction over s
  - base case: $s = \varepsilon$
  - inductive step: $s = s_1 s_2$ for (A-3) $s_1\ N$, and (A-4) $s_2\ L$

$$\text{(I.H.)} \quad \frac{s_2\ L \quad t\ L}{s_2 s\ L}$$

for a fixed s_2 and any t

$$\dfrac{\dfrac{}{s_1\ N}\,\text{(A-3)} \qquad \dfrac{\dfrac{}{s_2\ L}\,\text{(A-4)} \quad \dfrac{}{t\ L}\,\text{(A-2)}}{s_2 t\ L}\,\text{(I.H.)}}{s_1 s_2 t\ L}\,\text{(L-2)}$$

$$\text{(L-1)}\ \frac{}{\varepsilon} \qquad \text{(L-2)}\ \frac{s_1\ N \quad s_2\ L}{s_1 s_2\ L} \qquad \text{(N-1)}\ \frac{s\ L}{\mathbf{(}s\mathbf{)}\ N}$$

$$\text{(M-1)}\ \frac{}{\varepsilon} \qquad \text{(M-2)}\ \frac{s_1\ M \quad s_2\ M}{s_1 s_2\ M} \qquad \text{(M-3)}\ \frac{s\ M}{\mathbf{(}s\mathbf{)}\ M}$$

Proving L = M

- summary so far:
  - ★ we showed that if *s M, then s L* by rule induction over s
    - base case was easy
    - for the inductive step, we first had to prove the lemma

$$\frac{s_1\ L \quad s_2\ L}{s_1 s_2\ L}$$

      using induction over s_1

  - ★ we still need to show that *if s L then s M*

Judgements revisited

- A judgement states that a certain property holds for a specific object (which corresponds to a set membership)
- More generally, judgements express a relationship between a number of objects (*n*-ary relations)
- Examples:
  - ★ *4 divides 16* (binary relationship)
  - ★ `ail` *is a substring of* `mail` (binary)
  - ★ *3 plus 5 equals 8* (tertiary)
- Infix notation to denote binary relations
  - ★ 4 *div* 16
  - ★ `ail` *substr* `mail`

Relations

Definition: A binary relation $\boldsymbol{R}$ is

symmetric, iff for all a, b, $a\boldsymbol{R}b$ implies $b\boldsymbol{R}a$

reflexive, iff for all a, $a\boldsymbol{R}a$ holds

transitive, iff for all a, b, c, $a\boldsymbol{R}b$ and $b\boldsymbol{R}c$ implies $a\boldsymbol{R}c$

.

Definition:

A relation which is symmetric, reflexive, and transitive is called equivalence relation.