COMP3161/9164
Concepts of Programming Languages

Natural Deduction and Rule Induction

Johannes Åman Pohjola
UNSW
Term 3 2022

Formalisation

To talk about languages in a mathematically precise way, we need to formalise them.

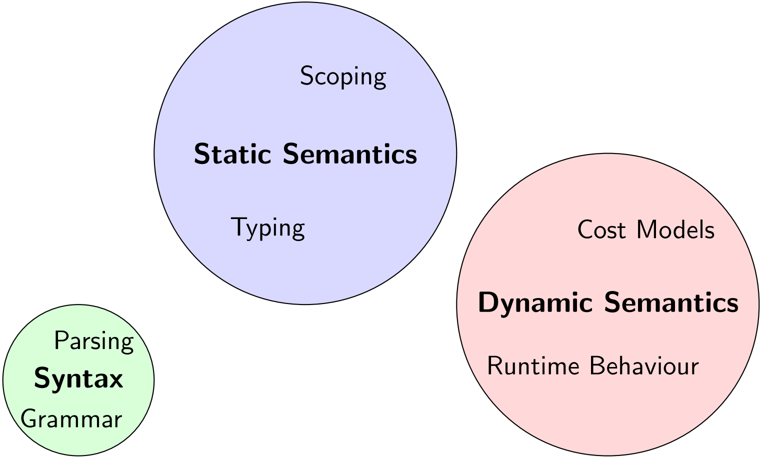
Formalisation

Formalisation is the process of giving a language a formal, mathematical description.

Typically, we describe the language in another language, called the *meta-language*. For implementations, it may be a programming language such as Haskell. For formalisations it is usually a minimal logic called a *meta-logic*.

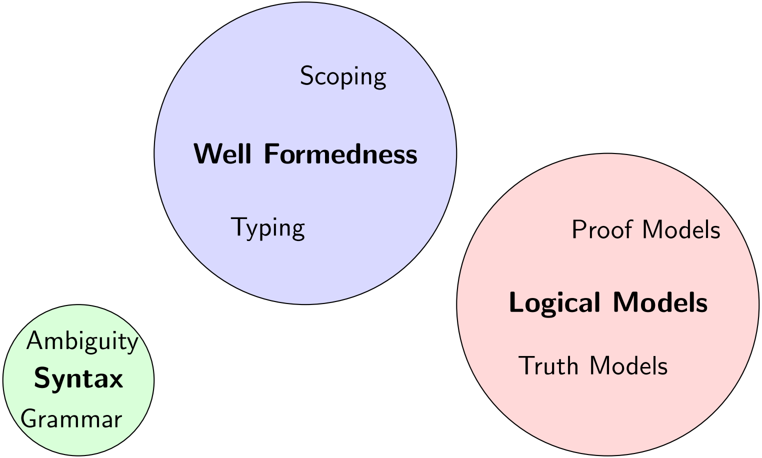
Learning from History

What sort of meta logic should we use? There are a number of things to formalise:



Learning from History

Logicians in the early 20th century had much the same desire to formalise *logics*.



Learning from History

In this course, we will use a meta-logic based on *Natural Deduction* and inductive inference rules, originally invented for formalising logics by Gerhard Gentzen in the mid 1930s.

Der Kalkül des natürlichen Schließens.

$$\frac{\mathfrak{A} \quad \mathfrak{B}}{\mathfrak{A} \,\&\, \mathfrak{B}} \qquad \frac{\mathfrak{A} \,\&\, \mathfrak{B}}{\mathfrak{A}} \quad \frac{\mathfrak{A} \,\&\, \mathfrak{B}}{\mathfrak{B}}$$

Judgements

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

Example (Informal Judgements)

- $3 + 4 \times 5$ is a valid arithmetic expression.
- The string *madam* is a palindrome.
- The string *snooze* is a palindrome
  $\Longrightarrow$ Judgements do not have to hold.

Unary Judgements

Formally, we denote the judgement that a property A holds for an object s by writing $s\ \mathsf{A}$.

Typically, s is a string when describing syntax, and s is a term when describing semantics.

Proving Judgements

We define how a judgement may be proven by providing a set of *inference rules*.

Inference Rules

An inference rule is written as:

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

This states that in order to prove judgement J (the *conclusion*), it suffices to prove all judgements J_1 through to J_n (the *premises*).

Rules with no premises are called *axioms*. Their conclusions always hold.

Examples

Example (Natural Numbers)

$$\boxed{n\ \mathsf{Nat}}$$

$$\frac{}{0\ \mathsf{Nat}}N_1$$

0 is a natural number

$$\frac{n\ \mathsf{Nat}}{(\mathsf{S}\ n)\ \mathsf{Nat}}N_2$$

if n is a natural number, then the successor of n is a natural number.

What terms are in the set $\{n \mid n\ \mathsf{Nat}\}$?

$$\{0, (\mathsf{S}\ 0), (\mathsf{S}\ (\mathsf{S}\ 0)), (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ 0))), \ldots\}$$

Examples

Example (Even and Odd Numbers)

$$\boxed{n\ \mathsf{Even}} \qquad \boxed{n\ \mathsf{Odd}}$$

$$\frac{}{0\ \mathsf{Even}}\,E_1 \qquad \frac{n\ \mathsf{Even}}{(\mathsf{S}\ (\mathsf{S}\ n))\ \mathsf{Even}}\,E_2 \qquad \frac{n\ \mathsf{Even}}{(\mathsf{S}\ n)\ \mathsf{Odd}}\,O_1$$

The Proof Video Game

To show that a judgement s A holds:

1. Find a rule whose conclusion matches s A.
2. The preconditions of the applied rules become new proof obligations.
3. Rinse and repeat until all obligations are proven up to axioms.

Examples

Example (Even and Odd Numbers)

$\boxed{n \text{ Even}}$ $\boxed{n \text{ Odd}}$

$$\frac{}{0\ \mathsf{Even}}E_1 \qquad \frac{n\ \mathsf{Even}}{(\mathsf{S}\ (\mathsf{S}\ n))\ \mathsf{Even}}E_2 \qquad \frac{n\ \mathsf{Even}}{(\mathsf{S}\ n)\ \mathsf{Odd}}O_1$$

$$\cfrac{\cfrac{\cfrac{\cfrac{}{0\ \mathsf{Even}}E_1}{(\mathsf{S}\ (\mathsf{S}\ 0))\ \mathsf{Even}}E_2}{(\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ 0))))\ \mathsf{Even}}E_2}{(\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ (\mathsf{S}\ 0)))))\ \mathsf{Odd}}O_1$$

Defining Languages

Example (Bracket Matching Language)

$$\mathsf{M} ::= \varepsilon \mid \mathsf{MM} \mid (\ \mathsf{M}\ )$$

Examples of strings: ε, (), (()), ()(), (()()), ...

Three rules:

Axiom	The empty string is in M
Juxtaposition	Any two strings in M can be concatenated to give a new string in M
Nesting	Any string in M can be surrounded by parentheses, giving a new string in M

With Rules

The Language M

$$\boxed{s \ \mathsf{M}}$$

$$\frac{}{\varepsilon \ \mathsf{M}} M_E \qquad \frac{s \ \mathsf{M}}{(s) \ \mathsf{M}} M_N \qquad \frac{s_1 \ \mathsf{M} \qquad s_2 \ \mathsf{M}}{s_1 s_2 \ \mathsf{M}} M_J$$

$$\frac{\dfrac{\dfrac{}{\varepsilon \ \mathsf{M}} M_E}{() \ \mathsf{M}} M_N \qquad \dfrac{\dfrac{\dfrac{}{\varepsilon \ \mathsf{M}} M_E}{() \ \mathsf{M}} M_N}{(()) \ \mathsf{M}} M_N}{()(()) \ \mathsf{M}} M_J$$

Getting Stuck

If we had started with rule M_N instead, we would have gotten stuck:

$$\dfrac{\dfrac{\color{red}{???}}{)\,(\,(\,)\ \ \mathrm{M}}}{(\,)\,(\,(\,)\,)\ \ \mathrm{M}}\,M_N$$

Takeaway

Getting stuck does not mean what you're trying to prove is false!

Derivability

Consider the following rule:

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

Does adding this rule change M? (i.e. is it not *admissible* to M)? No, because we could always use rule M_N twice instead. Rules that are compositions of existing rules are called *derivable*:

$$\cfrac{\cfrac{s \ \mathsf{M}}{(s) \ \mathsf{M}}\,M_N}{(\,(s)\,) \ \mathsf{M}}\,M_N$$

We can prove rules as well as judgements, by deriving the conclusion of the rule while taking the premises as local axioms.

Derivability

Is this rule derivable?

$$\frac{s\ \mathsf{M}}{(s)s\ \mathsf{M}}$$

We can derive it like so:

$$\dfrac{\dfrac{\dfrac{}{s\ \mathsf{M}}}{(s)\ \mathsf{M}}\,M_N \qquad \dfrac{}{s\ \mathsf{M}}}{(s)s\ \mathsf{M}}\,M_J$$

Derivability

Is this rule derivable?

$$\frac{(s)\ \mathsf{M}}{s\ \mathsf{M}}\,Q$$

It is not admissible, let alone derivable, as it adds strings to M:

$$\dfrac{\dfrac{\dfrac{}{\varepsilon\ \mathsf{M}}\,M_E}{()\ \mathsf{M}}\,M_N \qquad \dfrac{\dfrac{}{\varepsilon\ \mathsf{M}}\,M_E}{()\ \mathsf{M}}\,M_N}{\dfrac{()()\ \mathsf{M}}{)(\ \mathsf{M}}\,Q}\,M_J$$

Derivability

Is this rule admissible? If so, is it derivable?

$$\frac{()s\ \mathsf{M}}{s\ \mathsf{M}}$$

- It is admissible, as it doesn't let us prove any new judgements about M.
- It is not derivable, as it is not made up of the composition of existing rules.
- We will see how to prove these sorts of rules are admissible later on.

Hypothetical Derivations

We can write a rule in a horizontal format as well:

$$\frac{A}{B} \text{ is the same as } A \vdash B$$

This allows us to neatly make rules premises of other rules, called *hypothetical derivations*:

Example

$$\frac{A \vdash B}{C}$$

Read as: *If assuming A we can derive B, then we can derive C.*

Specifying Logic

With hypotheticals we can specify logic, which was the original purpose of natural deduction. Let $A\ \mathsf{True}$ be the judgement that the proposition A is true.

Example (And and Implies)

$$\frac{A\ \mathsf{True} \qquad B\ \mathsf{True}}{A \land B\ \mathsf{True}}\land_I \qquad \frac{A \land B\ \mathsf{True}}{A\ \mathsf{True}}\land_{E1} \qquad \frac{A \land B\ \mathsf{True}}{B\ \mathsf{True}}\land_{E2}$$

$$\frac{A\ \mathsf{True} \vdash B\ \mathsf{True}}{A \Rightarrow B\ \mathsf{True}}\Rightarrow_I \qquad \frac{A \Rightarrow B\ \mathsf{True} \qquad A\ \mathsf{True}}{B\ \mathsf{True}}\Rightarrow_E$$

Specifying Logic, Continued

Example (Or, True, False and Not)

$$\frac{A \text{ True}}{A \vee B \text{ True}} \vee_{I1} \qquad \frac{B \text{ True}}{A \vee B \text{ True}} \vee_{I2}$$

$$\frac{A \text{ True} \vdash C \text{ True} \qquad B \text{ True} \vdash C \text{ True} \qquad A \vee B \text{ True}}{C \text{ True}} \vee_{E}$$

$$\frac{}{\top \text{ True}} \top_{I} \qquad \frac{\bot \text{ True}}{A \text{ True}} \bot_{E}$$

$$\frac{A \text{ True} \vdash \bot \text{ True}}{\neg A \text{ True}} \neg_{I} \qquad \frac{\neg A \text{ True} \qquad A \text{ True}}{B \text{ True}} \neg_{E}$$

Minimal Definitions

$$\boxed{s \ \mathsf{M}}$$

$$\frac{}{\varepsilon \ \mathsf{M}} M_E \qquad \frac{s \ \mathsf{M}}{(s) \ \mathsf{M}} M_N \qquad \frac{s_1 \ \mathsf{M} \qquad s_2 \ \mathsf{M}}{s_1 s_2 \ \mathsf{M}} M_J$$

The above rules are the smallest set of rules to define every string in M.

Therefore

If we know that a string satisfies s M, it must have been through a (finite) derivation using these rules.

This is called an *inductive definition* of M.

Rule Induction

Suppose we want to show that a property $P(s)$ of strings s holds for any string s M. We will use *rule induction*.

If we show that

$$\frac{}{\varepsilon\ \mathsf{M}}M_E \qquad P(\varepsilon) \text{ holds, and}$$

$$\frac{s\ \mathsf{M}}{(s)\ \mathsf{M}}M_N \qquad P(s) \text{ implies } P((s)), \text{ and}$$

$$\frac{s_1\ \mathsf{M} \quad s_2\ \mathsf{M}}{s_1 s_2\ \mathsf{M}}M_J \qquad P(s_1) \text{ and } P(s_2) \text{ implies } P(s_1 s_2)$$

Then we have shown $P(s)$ for all s M.

These assumptions are called *inductive hypotheses*.

Rule Induction

Example (Counting Parens)

Let $op(s)$ denote the number of opening parentheses in s, and $cl(s)$ denote the number of closing parentheses. We shall prove that

$$s \ \mathrm{M} \implies op(s) = cl(s)$$

by doing rule induction on $s \ \mathrm{M}$.

Rule Induction

Example (Counting Parens)

$$\frac{}{\varepsilon \ \mathsf{M}} M_E$$

$$\frac{s \ \mathsf{M}}{(s) \ \mathsf{M}} M_N$$

$$\frac{s_1 \ \mathsf{M} \qquad s_2 \ \mathsf{M}}{s_1 s_2 \ \mathsf{M}} M_J$$

Base Case: $op(\varepsilon) = 0 = cl(\varepsilon)$

Inductive Case: Assuming I.H:

$$op(s) = cl(s)$$

$$op((s)) = op(s) + 1 = cl(s) + 1 = cl((s))$$

Inductive Case: Assuming I.Hs:

$op(s_1) = cl(s_1)$ and $op(s_2) = cl(s_2)$

$$op(s_1 s_2) = op(s_1) + op(s_2) = cl(s_1 s_2)$$

Rule Induction in General

Rule Induction Method

Given a set of rules R, we may prove a property P inductively for all judgements that can be inferred with R by showing, for each rule of the form

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

that if P holds for each of $J_1 \ldots J_n$, then P holds for J.

Therefore, axioms are the base cases of the induction, all other rules form inductive cases, and the premises of each rule give rise to inductive hypotheses.

Structural Induction

Conventional *structural induction* such as that on natural numbers, which we have encountered before, is a special case of rule induction.

Natural Number Induction

To show a property $P(n)$ for all $n \in \mathbb{N}$, it suffices to:

$$\frac{}{0\ \mathsf{Nat}}$$ Show that $P(0)$ holds, and

$$\frac{n\ \mathsf{Nat}}{(\mathsf{S}\ n)\ \mathsf{Nat}}$$ Assuming $P(n)$, show $P(n+1)$.

Another Example

Recall our definition of even numbers:

$$\boxed{n \text{ Even}}$$

$$\frac{}{0 \text{ Even}}E_1 \qquad \frac{n \text{ Even}}{(\mathsf{S}\ (\mathsf{S}\ n))\ \text{Even}}E_2$$

We could define odd numbers differently:

$$\boxed{n \text{ Odd}'}$$

$$\frac{}{(\mathsf{S}\ 0)\ \text{Odd}'}O_1' \qquad \frac{n \text{ Odd}'}{(\mathsf{S}\ (\mathsf{S}\ n))\ \text{Odd}'}O_2$$

Let's prove the original Odd rule, but for Odd′ (to "whiteboard"):

$$\frac{n \text{ Even}}{(\mathsf{S}\ n)\ \text{Odd}'}$$

Arithmetic

Example (Arithmetic Expression)

$$\mathsf{Arith} ::= i \mid \mathsf{Arith} \times \mathsf{Arith} \mid \mathsf{Arith} + \mathsf{Arith} \mid (\mathsf{Arith}) \qquad (i \in \mathbb{Z})$$

$$\frac{i \in \mathbb{Z}}{i \ \mathsf{Arith}}L \quad \frac{a\ \mathsf{Arith} \qquad b\ \mathsf{Arith}}{a \times b\ \mathsf{Arith}}P \quad \frac{a\ \mathsf{Arith} \qquad b\ \mathsf{Arith}}{a + b\ \mathsf{Arith}}S \quad \frac{a\ \mathsf{Arith}}{(a)\ \mathsf{Arith}}$$

We can infer $1 + 2 \times 3\ \mathsf{Arith}$ in two different ways.

Ambiguity

Arith is *ambiguous*, which means that there are multiple ways to derive the same judgement.

For syntax, this is a big problem, as different interpretations of syntax can lead to semantic inconsistency:

$$\dfrac{\dfrac{1 \in \mathbb{Z}}{1 \text{ Arith}} \quad \dfrac{\dfrac{2 \in \mathbb{Z}}{2 \text{ Arith}} \quad \dfrac{3 \in \mathbb{Z}}{3 \text{ Arith}}}{2 \times 3 \text{ Arith}}}{1 + 2 \times 3 \text{ Arith}} \qquad \dfrac{\dfrac{\dfrac{1 \in \mathbb{Z}}{1 \text{ Arith}} \quad \dfrac{2 \in \mathbb{Z}}{2 \text{ Arith}}}{1 + 2 \text{ Arith}} \quad \dfrac{3 \in \mathbb{Z}}{3 \text{ Arith}}}{1 + 2 \times 3 \text{ Arith}}$$

Second Attempt

We want to specify Arith in such a way that enforces order of operations.

Here we will use multiple judgements:

Example (Arithmetic Expression)

$$\begin{array}{lcl} \text{Atom} & ::= & i \mid (\text{SExp}) \quad (i \in \mathbb{Z}) \\ \text{PExp} & ::= & \text{Atom} \mid \text{PExp} \times \text{PExp} \\ \text{SExp} & ::= & \text{PExp} \mid \text{SExp} + \text{SExp} \end{array}$$

$$\frac{i \in \mathbb{Z}}{i\ \text{Atom}} \qquad \frac{a\ \text{SExp}}{(a)\ \text{Atom}} \qquad \frac{e\ \text{Atom}}{e\ \text{PExp}} \qquad \frac{e\ \text{PExp}}{e\ \text{SExp}}$$

$$\frac{a\ \text{PExp} \qquad b\ \text{PExp}}{a \times b\ \text{PExp}} \qquad \frac{a\ \text{SExp} \qquad b\ \text{SExp}}{a + b\ \text{SExp}}$$

Consider: Is there still any ambiguity here?

More ambiguity

$$
\dfrac{\dfrac{\dfrac{1 \in \mathbb{Z}}{1\ \mathsf{Atom}}}{1\ \mathsf{PExp}} \quad \dfrac{\dfrac{\dfrac{2 \in \mathbb{Z}}{2\ \mathsf{Atom}}}{2\ \mathsf{PExp}} \quad \dfrac{\dfrac{3 \in \mathbb{Z}}{3\ \mathsf{Atom}}}{3\ \mathsf{PExp}}}{2 \times 3\ \mathsf{PExp}}}{1 \times 2 \times 3\ \mathsf{PExp}}
\qquad
\dfrac{\dfrac{\dfrac{\dfrac{1 \in \mathbb{Z}}{1\ \mathsf{Atom}}}{1\ \mathsf{PExp}} \quad \dfrac{\dfrac{2 \in \mathbb{Z}}{2\ \mathsf{Atom}}}{2\ \mathsf{PExp}}}{1 \times 2\ \mathsf{PExp}} \quad \dfrac{\dfrac{3 \in \mathbb{Z}}{3\ \mathsf{Atom}}}{3\ \mathsf{PExp}}}{1 \times 2 \times 3\ \mathsf{PExp}}
$$

This ambiguity seems harmless, but it would not be harmless for some other operations. Which ones? Operators that are not *associative*.

We have to specify the *associativity* of operators. How?

Associativities

Operators have various *associativity* constraints:

Associative	All associativities are equal.
Left-Associative	$A \odot B \odot C = (A \odot B) \odot C$
Right-Associative	$A \odot B \odot C = A \odot (B \odot C)$

Try to think of some examples!

Enforcing associativity

We force the grammar to accept a smaller set of expressions on one side of the operator only. Show how this works on the "whiteboard".

Example (Arithmetic Expression)

$$
\begin{array}{lcl}
\text{Atom} & ::= & i \mid (\text{SExp}) \quad (i \in \mathbb{Z}) \\
\text{PExp} & ::= & \text{Atom} \mid \text{Atom} \times \text{PExp} \\
\text{SExp} & ::= & \text{PExp} \mid \text{PExp} + \text{SExp}
\end{array}
$$

$$
\frac{i \in \mathbb{Z}}{i\ \text{Atom}} \qquad \frac{a\ \text{SExp}}{(a)\ \text{Atom}} \qquad \frac{e\ \text{Atom}}{e\ \text{PExp}} \qquad \frac{e\ \text{PExp}}{e\ \text{SExp}}
$$

$$
\frac{a\ \text{Atom} \qquad b\ \text{PExp}}{a \times b\ \text{PExp}} \qquad \frac{a\ \text{PExp} \qquad b\ \text{SExp}}{a + b\ \text{SExp}}
$$

Here we made multiplication and addition right associative. How would we do left?

Bring Back Parentheses

The Parenthetical Language

$$\boxed{s \; \mathsf{M}}$$

$$\frac{}{\varepsilon \; \mathsf{M}} M_E \qquad \frac{s \; \mathsf{M}}{(\, s \,) \; \mathsf{M}} M_N \qquad \frac{s_1 \; \mathsf{M} \qquad s_2 \; \mathsf{M}}{s_1 s_2 \; \mathsf{M}} M_J$$

Is this language ambiguous? to "whiteboard"

Ambiguity in Parentheses

Not only is it ambiguous, it is infinitely so. Strings like ()()() could be split at two different locations by rule M_J, but if we use ε, then even the string () is ambiguous:

$$\dfrac{\dfrac{}{\varepsilon\ \mathrm{M}}\,M_E}{()\ \mathrm{M}}\,M_N \qquad \dfrac{\dfrac{}{\varepsilon\ \mathrm{M}}\,M_E \quad \dfrac{\dfrac{}{\varepsilon\ \mathrm{M}}\,M_E}{()\ \mathrm{M}}\,M_N}{()\ \mathrm{M}}\,M_J$$

$$\dfrac{\dfrac{}{\varepsilon\ \mathrm{M}}\,M_E \quad \dfrac{\dfrac{}{\varepsilon\ \mathrm{M}}\,M_E \quad \dfrac{\dfrac{}{\varepsilon\ \mathrm{M}}\,M_E}{()\ \mathrm{M}}\,M_N}{()\ \mathrm{M}}\,M_J}{()\ \mathrm{M}}\,M_J$$

We will eliminate the ambiguity by once again splitting M into two judgements, N and L.

The crucial observation is that terms in M are a list (L) of terms nested within parentheses (N).

Example (Unambiguous Parentheses)

$$\boxed{s\ \mathsf{L}} \qquad \boxed{s\ \mathsf{N}}$$

$$\frac{}{\varepsilon\ \mathsf{L}}L_E \qquad \frac{s\ \mathsf{L}}{(\,s\,)\ \mathsf{N}}N_N \qquad \frac{s_1\ \mathsf{N} \qquad s_2\ \mathsf{L}}{s_1 s_2\ \mathsf{L}}L_J$$

Proving Equivalence

Now we shall prove $\mathsf{M} = \mathsf{L}$. There are two cases, each dispatched with rule induction:

$$\frac{s\ \mathsf{M}}{s\ \mathsf{L}} \qquad \frac{s\ \mathsf{L}}{s\ \mathsf{M}}$$

The first case requires proving a *lemma*. The second requires *simultaneous induction*.
These proofs will be carried out on the "board".