

Liam O'Connor

CSE, UNSW (and data61)

Semester 2 2018



Formalisation

To talk about languages in a mathematical way, we need to **formalise** them.

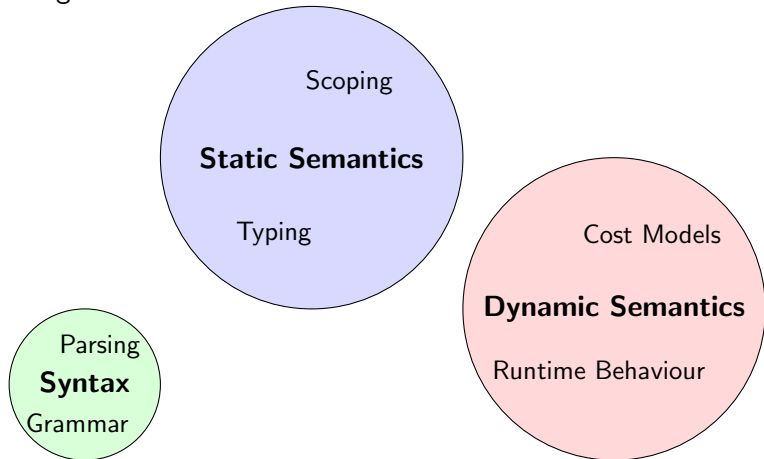
Formalisation

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**, but for formalisations it is usually a minimal logic called a *meta-logic*.

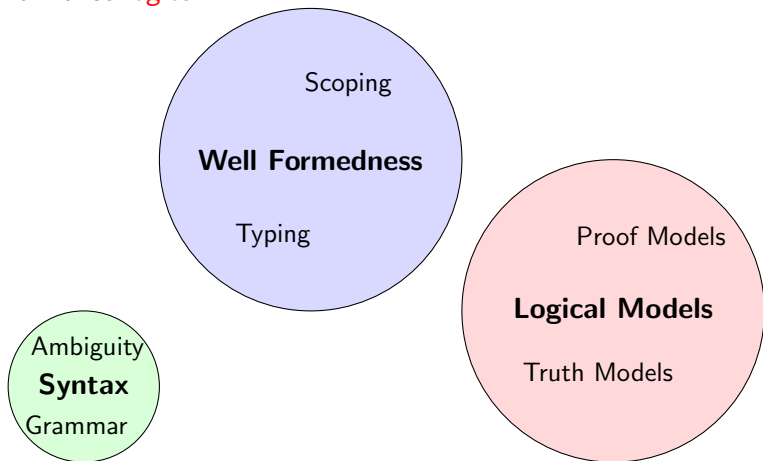
Learning from History

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.

$$\frac{\mathcal{A} \quad \mathcal{B}}{\mathcal{A} \& \mathcal{B}} \qquad
 \frac{\mathcal{A} \& \mathcal{B}}{\mathcal{A}} \qquad
 \frac{\mathcal{A} \& \mathcal{B}}{\mathcal{B}}$$

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
- ⇒ 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* **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:

$$\frac{J_1 \quad J_2 \quad \dots \quad J_n}{J}$$

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)

$$n \text{ Nat}$$

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

0 is a natural number

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

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

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

$$\{0, (S 0), (S (S 0)), (S (S (S 0))), \dots\}$$

Examples

Example (Even and Odd Numbers)

$$\begin{array}{ccc}
 \frac{}{0 \text{ Even}} E_1 & \frac{\boxed{n \text{ Even}}}{(S (S n)) \text{ Even}} E_2 & \frac{\boxed{n \text{ Even}}}{(S n) \text{ Odd}} O_1
 \end{array}$$

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)

$$\begin{array}{ccc}
 \boxed{n \text{ Even}} & \boxed{n \text{ Odd}} & \\
 \frac{}{0 \text{ Even}} E_1 & \frac{n \text{ Even}}{(S (S n)) \text{ Even}} E_2 & \frac{n \text{ Even}}{(S n) \text{ Odd}} O_1
 \end{array}$$

$$\frac{\frac{\frac{\frac{\frac{}{0 \text{ Even}} E_1}{(S (S 0)) \text{ Even}} E_2}{(S (S (S (S 0)))) \text{ Even}} E_2}{(S (S (S (S (S 0)))) \text{ Odd}} O_1$$

Defining Languages

Example (Bracket Matching Language)

$$\mathbf{M} ::= \varepsilon \mid \mathbf{M}\mathbf{M} \mid (\mathbf{M})$$

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

Three rules:

Axiom The empty string is in **M**

Nesting Any string in **M** can be surrounded by parentheses, giving a new string in **M**

Juxtaposition Any two strings in **M** can be concatenated to give a new string in **M**

With Rules

The Language \mathcal{M}

$$\begin{array}{c}
 \boxed{s \mathcal{M}} \\
 \\
 \frac{}{\varepsilon \mathcal{M}} M_E \qquad \frac{s \mathcal{M}}{(s) \mathcal{M}} M_N \qquad \frac{s_1 \mathcal{M} \quad s_2 \mathcal{M}}{s_1 s_2 \mathcal{M}} M_J
 \end{array}$$

$$\frac{\frac{\frac{}{\varepsilon \mathcal{M}} M_E}{() \mathcal{M}} M_N \quad \frac{\frac{\frac{}{\varepsilon \mathcal{M}} M_E}{() \mathcal{M}} M_N}{(() \mathcal{M})} M_N}{() (()) \mathcal{M}} M_J$$

Getting Stuck

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

$$\frac{\text{???}}{\frac{) ((\mathbf{M}}{((() \mathbf{M}} M_N}$$

Takeaway

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

Derivability

Consider the following rule:

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

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

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

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?

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

We can derive it like so:

$$\frac{\frac{\overline{s \mathbf{M}}}{(s) \mathbf{M}} M_N \quad \overline{s \mathbf{M}}}{(s) s \mathbf{M}} M_J$$

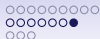
Derivability

Is this rule derivable?

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

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

$$\frac{\frac{\frac{\frac{\frac{}{\varepsilon \mathbf{M}}{M_E}}{() \mathbf{M}}{M_N}}{() () \mathbf{M}}{M_J}}{) (\mathbf{M}}}{Q}}$$



Derivability

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

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

- 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 **True** be the judgement that the proposition A is true.

Example (And and Implies)

$$\begin{array}{c}
 \frac{A \text{ True} \quad B \text{ True}}{A \wedge B \text{ True}} \wedge_I \quad \frac{A \wedge B \text{ True}}{A \text{ True}} \wedge_{E1} \quad \frac{A \wedge B \text{ True}}{B \text{ True}} \wedge_{E2} \\
 \\
 \frac{A \text{ True} \vdash B \text{ True}}{A \Rightarrow B \text{ True}} \Rightarrow_I \quad \frac{A \Rightarrow B \text{ True} \quad A \text{ True}}{B \text{ True}} \Rightarrow_E
 \end{array}$$

Specifying Logic, Continued

Example (Or, True, False and Not)

$$\begin{array}{c}
 \frac{A \text{ True}}{A \vee B \text{ True}} \vee I_1 \quad \frac{B \text{ True}}{A \vee B \text{ True}} \vee I_2 \\
 \\
 \frac{A \text{ True} \vdash C \text{ True} \quad B \text{ True} \vdash C \text{ True} \quad A \vee B \text{ True}}{C \text{ True}} \vee E \\
 \\
 \frac{}{\top \text{ True}} \top I \quad \frac{\perp \text{ True}}{A \text{ True}} \perp E \\
 \\
 \frac{A \text{ True} \vdash \perp \text{ True}}{\neg A \text{ True}} \neg I \quad \frac{\neg A \text{ True} \quad A \text{ True}}{B \text{ True}} \neg E
 \end{array}$$

Minimal Definitions

$$\begin{array}{c}
 \boxed{s \ M} \\
 \frac{}{\varepsilon \ M} M_E \qquad \frac{s \ M}{(s) \ M} M_N \qquad \frac{s_1 \ M \quad s_2 \ M}{s_1 s_2 \ M} M_J
 \end{array}$$

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

Therefore

If we know that a string $s \ M$, it must have been through one of 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 $s \mathbf{M}$. We will use *rule induction*.

If we show that

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

$P(\varepsilon)$ holds, and

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

$P(s)$ implies $P((s))$, and

$$\frac{s_1 \mathbf{M} \quad s_2 \mathbf{M}}{s_1 s_2 \mathbf{M}} M_J$$

$P(s_1)$ and $P(s_2)$ implies $P(s_1 s_2)$

Then we have shown $P(s)$ for all $s \mathbf{M}$.

These assumptions are called *inductive hypotheses*.

Rule Induction

Example (Counting Prens)

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

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

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

Rule Induction

Example (Counting Prens)

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

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

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

Inductive Case: Assuming I.H:

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

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

$$\frac{s_1 \mathbf{M} \quad s_2 \mathbf{M}}{s_1 s_2 \mathbf{M}} M_J$$

Inductive Case: Assuming I.Hs:

$$op(s_1) = cl(s_1) \text{ and } op(s_2) = cl(s_2)$$

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

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

$$\frac{J_1 \quad J_2 \quad \dots \quad J_n}{J}$$

that if P holds for each of $J_1 \dots J_n$, 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 you may 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:

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

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

Another Example

Recall our definition of even numbers:

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

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

We could define odd numbers differently:

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

$$\frac{}{(S 0) \text{ Odd}'} O'_1 \qquad \frac{n \text{ Odd}'}{(S (S n)) \text{ Odd}'} O'_2$$

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

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