Utrecht University

Revision:
Judgements, Inference Rules & Proofs

Concepts of Programming Language Design 2024/2025

Gabriele Keller
Tom Smeding

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
- the number *3* is even

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

formally, s is an element of a universe $\boldsymbol{U}$ (a set) where

- $\boldsymbol{A} \subseteq \boldsymbol{U}$ and $s \in \boldsymbol{A}$

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

$$\frac{J_1, \; J_2 \; \dots \; J_n}{J}$$

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 `5` is a natural number, we write $\dfrac{}{\texttt{5}\ \textit{Nat}}$
- Inference rules to define this judgement
  - "`0` is a natural number" (axiom) $\dfrac{}{\texttt{0}\ \textit{Nat}}\ (\textit{Nat-1})$
  - "if x is a natural number, then `(s` x`)` is a natural number (*s* for *successor*)

$$\frac{x\ \textit{Nat}}{(\texttt{s}\ x)\ \textit{Nat}}\ (\textit{Nat-2})$$

★ this set of rules characterises the set of syntactic objects

$$\textit{Nat} = \{\texttt{0}, (\texttt{s 0}), (\texttt{s(s 0)}), (\texttt{s(s(s 0)))}, \ldots\}$$

Utrecht University

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
  - ★ "`0` is even" (axiom)

$$\frac{}{\texttt{0}\ \textit{\textbf{Even}}}$$

  - ★ "if n is even, then `s(s(`n`))` is even"

$$\frac{n\ \textit{\textbf{Even}}}{(\texttt{s}(\texttt{s}\ n))\ \textit{\textbf{Even}}}$$

  - ★ "if n is even, then `(s `n`)` is odd"

$$\frac{n\ \textit{\textbf{Even}}}{(\texttt{s}\ n)\ \textit{\textbf{Odd}}}$$

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` $\mathit{divides}$ `16` (binary relationship)
  - `ail` $\mathit{is\ a\ substring\ of}$ `mail` (binary)
  - `3` plus `5` equals `8` (tertiary)
- Infix notation to denote binary relations
  - `4` div `16`
  - `ail` substr `mail`

Utrecht University

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 an **equivalence relation.**

Utrecht University

Relations

- Example
  - how can we define the ’less than’ relation on natural numbers inductively?
  - $< \;\subseteq\; \boldsymbol{Nat} \times \boldsymbol{Nat}$

$$\frac{n\ \boldsymbol{Nat}}{0 < (\mathtt{s}\ n)} \qquad\qquad \frac{n < m}{(\mathtt{s}\ n) < (\mathtt{s}\ m)}$$

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 $s\ \boldsymbol{A}$ holds

  1) find a rule whose conclusion matches $s\ \boldsymbol{A}$

  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 0))))` is even
- Let's start informally
  - `(s(s(s(s 0))))` is even if `(s(s 0))` is even
  - `(s(s 0))` is even if `0` is even
  - `0` is even
- Note: the preconditions of the rules we use become proof obligations

Derivation Tree

$$\frac{}{\texttt{0}\ \textit{\textbf{Even}}}\ (\textit{Even-1}) \qquad\qquad \frac{n\ \textit{\textbf{Even}}}{\texttt{(s(s}\ n\texttt{))}\ \textit{\textbf{Even}}}\ (\textit{Even-2})$$

$$\cfrac{\cfrac{\cfrac{}{\texttt{0}\ \textit{\textbf{Even}}}\ (\textit{Even-1})}{\texttt{(s(s}\ \boxed{\texttt{0}}\texttt{))}\ \textit{\textbf{Even}}}\ (\textit{Even-2})}{\texttt{(s(s}\underbrace{\texttt{(s(s 0))}}_{n}\texttt{))}\ \textit{\textbf{Even}}}\ (\textit{Even-2})$$

Or as regular proof, listing proof assumptions, goals, and steps:

$$\frac{}{\texttt{0}\ \textit{\textbf{Even}}}\ (\textit{Even-1})$$

$$\frac{n\ \textit{\textbf{Even}}}{\texttt{(s(s}\ n\texttt{))}\ \ \textit{\textbf{Even}}}\ (\textit{Even-2})$$

Proof:

[G] `(s(s(s(s 0))))` ***Even***

Begin

1. $\{$*Even-1*, *Even-2*$\}$ `(s(s 0))` ***Even***
2. $\{1,$ *Even-2*$\}$ `(s(s(s(s 0))))` ***Even***

End

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)
- Definition as BNF (Backus–Naur form)
  - $M ::= \ \varepsilon \mid MM \mid (M)$

Utrecht University

Grammars as inference rules

Definition by inference rules

(1) the empty string is in $\boldsymbol{M}$

$$\frac{}{\varepsilon \quad \boldsymbol{M}} \quad (M\text{-}1)$$

(2) if s_1 and s_2 are in $\boldsymbol{M}$, so is $s_1 s_2$ (concatenation)

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

(3) if s is in $\boldsymbol{M}$, so is (s)

$$\frac{s \ \boldsymbol{M}}{(s) \ \boldsymbol{M}} \quad (M\text{-}3)$$

Utrecht University

Side note: colour scheme

the name of the rule we define here:

variables/placeholders for objects of the judgement

$$\frac{}{\epsilon\ M} \quad (M\text{-}1)$$

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

$$\frac{s\ M}{\texttt{(}s\texttt{)}\ M} \quad (M\text{-}3)$$

`part of the term/string`

the name (or symbol) of the judgement

Natural deduction

- Show that $\texttt{()}\ \texttt{(())}\ \boldsymbol{M}$

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

$$\dfrac{}{\varepsilon\ \boldsymbol{M}}\quad(M\text{-}1)$$

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

$$\dfrac{s\ \boldsymbol{M}}{\texttt{(}s\texttt{)}\ \boldsymbol{M}}\quad(M\text{-}3)$$

- 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?

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

  - 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?

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

  - 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?

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

  - not admissible: we could derive $\texttt{)(} \;\; M$ using this rule!

Overview

- What we covered so far:
  - definitions of sets/properties using judgements
  - using inference rules to describe the elements of a set
  - how to formally show that a particular object is an element of such a set using natural deduction
  - derivable, admissible and inadmissible rules
- Today
  - proofs by rule (natural) induction
  - simultaneous inductive definitions

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 the set of perfectly matched parentheses:
  - 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?

Utrecht University

Rule Induction (structural induction)

$$\frac{}{\varepsilon \;\; \boldsymbol{M}} \quad (M\text{-}1)$$

$$\frac{s_1 \;\; \boldsymbol{M} \qquad s_2 \;\; \boldsymbol{M}}{s_1 s_2 \;\; \boldsymbol{M}} \quad (M\text{-}2)$$

$$\frac{s \;\; \boldsymbol{M}}{(\, s \,) \;\; \boldsymbol{M}} \quad (M\text{-}3)$$

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

show that

if *P* holds for the objects in J_1 to J_n, then P holds for the object in 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 Hypotheses

Rule Induction over Natural Numbers

- We have two rules which define the natural numbers:

$$\frac{}{\texttt{0}\ \boldsymbol{Nat}}\ (\mathit{Nat\text{-}1})$$

$$\frac{x\ \boldsymbol{Nat}}{(\texttt{s}\ x)\ \boldsymbol{Nat}}\ (\mathit{Nat\text{-}2})$$

Therefore, if we can show that a property $\boldsymbol{P}$

holds for `0` and

holds for $(\texttt{s}\ n)$ if (under the assumption that) it holds for $\boldsymbol{n}$

we have shown that it holds for any n in $\boldsymbol{Nat}$

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

Utrecht University

Rule Induction over Natural Numbers

- In other words: we have

$$\frac{}{\texttt{0}\ \boldsymbol{Nat}}\ (\textit{Nat-1})$$

$$\frac{x\ \boldsymbol{Nat}}{(\texttt{s}\ x)\ \boldsymbol{Nat}}\ (\textit{Nat-2})$$

- If we can prove that the following rules hold:

$$\frac{}{\texttt{0}\ \boldsymbol{P}}\ (\textit{P-1})$$

$$\frac{x\ \boldsymbol{P}}{(\texttt{s}\ x)\ \boldsymbol{P}}\ (\textit{P-2})$$

- then we know that for every $x\ \boldsymbol{Nat}$ there has to be a proof of the form

$$\begin{array}{c} \overline{\phantom{x\ \boldsymbol{Nat}}}\ (\textit{Nat-1}) \\ \vdots \\ \overline{x\ \boldsymbol{Nat}}\ (\textit{Nat-2}) \end{array}$$

which can be rewritten to

$$\begin{array}{c} \overline{\phantom{x\ \boldsymbol{P}}}\ (\textit{P-1}) \\ \vdots \\ \overline{x\ \boldsymbol{P}}\ (\textit{P-2}) \end{array}$$

by replacing every $\boldsymbol{Nat}$ judgement with a $\boldsymbol{P}$ judgement

- therefore any object $\boldsymbol{Nat}$ in has to also be in $\boldsymbol{P}$

Utrecht University

Rule Induction over M

- Same for $\boldsymbol{M}$:

$$\frac{}{\varepsilon \quad \boldsymbol{M}} \quad (M\text{-}1)$$

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

$$\frac{s \ \boldsymbol{M}}{(s) \ \boldsymbol{M}} \quad (M\text{-}3)$$

- If we can show that these rules hold:

$$\frac{}{\varepsilon \quad \boldsymbol{P}} \quad (P\text{-}1)$$

$$\frac{s_1 \ \boldsymbol{P} \qquad s_2 \ \boldsymbol{P}}{s_1 s_2 \ \boldsymbol{P}} \quad (P\text{-}2)$$

$$\frac{s \ \boldsymbol{P}}{(s) \ \boldsymbol{P}} \quad (P\text{-}3)$$

- Then $s \ \boldsymbol{M}$ implies $s \ \boldsymbol{P}$ because we can rewrite any proof for $s \ \boldsymbol{M}$ in one for $s \ \boldsymbol{P}$

Rule induction example

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

- let $open(s)$ be the number of left parens and $close(s)$ the number of right parens

$$
\begin{aligned}
open(\epsilon) &= 0 && (open\text{-}1)\\
open(\,(\,s) &= 1 + open(s) && (open\text{-}2)\\
open(\,)\,s) &= open(s) && (open\text{-}3)\\
open(s_1 s_2) &= open(s_1) + open(s_2) && (open\text{-}4)
\end{aligned}
$$

$$
\begin{aligned}
close(\epsilon) &= 0 && (close\text{-}1)\\
close(\,(\,s) &= close(s) && (close\text{-}2)\\
close(\,)\,s) &= 1 + close(s) && (close\text{-}3)\\
close(s_1 s_2) &= close(s_1) + close(s_2) && (close\text{-}4)
\end{aligned}
$$

- Show that if $s\ M$ holds then $open(s) = close(s)$

Utrecht University

Rule induction example

- Proof outline: we have to consider three cases (one case per rule). If $s\ \boldsymbol{M}$ was inferred using
  - Rule (M-1), then $s = \varepsilon$
  - Rule (M-2), then $s = s_1 s_2$, for some $s_1\ \boldsymbol{M}$ and $s_2\ \boldsymbol{M}$
  - Rule (M-3), then $s = \texttt{(}s_1\texttt{)}$ for some $s_1\ \boldsymbol{M}$

- That is, we need to show that these three rules/lemmata hold:

$$open\ (\varepsilon) = \overline{close\ (\varepsilon)} \quad (lemma\ 1)$$

$$\frac{}{\varepsilon\ \boldsymbol{M}}\ (M\text{-}1)$$

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

$$\frac{s\ \boldsymbol{M}}{\texttt{(}s\texttt{)}\ \boldsymbol{M}}\ (M\text{-}3)$$

Utrecht University

Rule induction example

- Proof outline: we have to consider three cases (one case per rule). If s $\boldsymbol{M}$ was inferred using
  - Rule (M-1), then $s = \varepsilon$
  - Rule (M-2), then $s = s_1 s_2$, for some s_1 $\boldsymbol{M}$ and s_2 $\boldsymbol{M}$
  - Rule (M-3), then $s =$ (s_1) for some s_1 $\boldsymbol{M}$

- That is, we need to show that these three rules/lemmata hold:

$$\frac{}{open\ (\varepsilon) = close\ (\varepsilon)}\quad (lemma\ 1) \qquad\qquad \frac{}{\varepsilon\ \ \boldsymbol{M}}\quad (M\text{-}1)$$

$$\frac{open\ (s_1) = close\ (s_1) \qquad open\ (s_2) = close\ (s_2)}{open\ (s_1 s_2) = close\ (s_1 s_2)}\quad (lemma\ 2) \qquad\qquad \frac{s_1\ \boldsymbol{M} \qquad s_2\ \boldsymbol{M}}{s_1 s_2\ \boldsymbol{M}}\quad (M\text{-}2)$$

$$\frac{s\ \boldsymbol{M}}{(\,s\,)\ \ \boldsymbol{M}}\quad (M\text{-}3)$$

Rule induction example

- Proof outline: we have to consider three cases (one case per rule). If $s\ \boldsymbol{M}$ was inferred using
  - Rule $(M\text{-}1)$, then $s = \varepsilon$
  - Rule $(M\text{-}2)$, then $s = s_1 s_2$, for some $s_1\ \boldsymbol{M}$ and $s_2\ \boldsymbol{M}$
  - Rule $(M\text{-}3)$, then $s = (s_1)$ for some $s_1\ \boldsymbol{M}$

- That is, we need to show that these three rules/lemmata hold:

$$\frac{}{open\ (\varepsilon) = close\ (\varepsilon)}\ (lemma\ 1) \qquad \frac{}{\varepsilon\ \boldsymbol{M}}\ (M\text{-}1)$$

$$\frac{open\ (s_1) = close\ (s_1) \qquad open\ (s_2) = close\ (s_2)}{open\ (s_1 s_2) = close\ (s_1 s_2)}\ (lemma\ 2) \qquad \frac{s_1\ \boldsymbol{M} \qquad s_2\ \boldsymbol{M}}{s_1 s_2\ \boldsymbol{M}}\ (M\text{-}2)$$

$$\frac{open\ (s) = close\ (s)}{open\ ((s)) = close\ ((s))}\ (lemma\ 3) \qquad \frac{s\ \boldsymbol{M}}{(s)\ \boldsymbol{M}}\ (M\text{-}3)$$

Proof

Subproof for Rule (1):

[G] $open\ (\varepsilon) = close\ (\varepsilon)$

$$
\begin{aligned}
open(\epsilon) &= 0 && (open\text{-}1)\\
open(\,(\,s) &= 1 + open(s) && (open\text{-}2)\\
open(\,)\,s) &= open(s) && (open\text{-}3)\\
open(s_1 s_2) &= open(s_1) + open(s_2) && (open\text{-}4)
\end{aligned}
$$

$$
\begin{aligned}
close(\epsilon) &= 0 && (close\text{-}1)\\
close(\,(\,s) &= close(s) && (close\text{-}2)\\
close(\,)\,s) &= 1 + close(s) && (close\text{-}3)\\
close(s_1 s_2) &= close(s_1) + close(s_2) && (close\text{-}4)
\end{aligned}
$$

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

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

$$\frac{s\ M}{(\,s\,)\ M} \quad (M\text{-}3)$$

Utrecht University

Proof

- Subproof case for Rule (2):

[IH1] $open\ (s_1) = close\ (s_1)$

[IH2] $open\ (s_2) = close\ (s_2)$

[G] $open\ (s_1 s_2) = close\ (s_1 s_2)$

$$
\begin{aligned}
open(\epsilon) &= 0 && (open\text{-}1)\\
open(\texttt{(}s) &= 1 + open(s) && (open\text{-}2)\\
open(\texttt{)}s) &= open(s) && (open\text{-}3)\\
open(s_1 s_2) &= open(s_1) + open(s_2) && (open\text{-}4)
\end{aligned}
$$

$$
\begin{aligned}
close(\epsilon) &= 0 && (close\text{-}1)\\
close(\texttt{(}s) &= close(s) && (close\text{-}2)\\
close(\texttt{)}s) &= 1 + close(s) && (close\text{-}3)\\
close(s_1 s_2) &= close(s_1) + close(s_2) && (close\text{-}4)
\end{aligned}
$$

$$\frac{}{\varepsilon \;\; M} \quad (M\text{-}1)$$

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

$$\frac{s \; M}{\texttt{(}\, s \,\texttt{)} \; M} \quad (M\text{-}3)$$

Utrecht University

Proof

- Subproof case for Rule (3):

  [IH] $open\ (s) = close\ (s)$

  [G] $open\ ((s)) = close\ ((s))$

$$
\begin{aligned}
open(\epsilon) &= 0 && (open\text{-}1)\\
open((s) &= 1 + open(s) && (open\text{-}2)\\
open()s) &= open(s) && (open\text{-}3)\\
open(s_1 s_2) &= open(s_1) + open(s_2) && (open\text{-}4)
\end{aligned}
$$

$$
\begin{aligned}
close(\epsilon) &= 0 && (close\text{-}1)\\
close((s) &= close(s) && (close\text{-}2)\\
close()s) &= 1 + close(s) && (close\text{-}3)\\
close(s_1 s_2) &= close(s_1) + close(s_2) && (close\text{-}4)
\end{aligned}
$$

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

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

$$\frac{s\ M}{(s)\ M}\quad (M\text{-}3)$$

Simultaneous Inductive Definitions

- Consider the following grammar (in BNF)

$$\boldsymbol{Expr} \rightarrow \boldsymbol{Int} \mid (\ \boldsymbol{Expr}\ ) \mid \boldsymbol{Expr} + \boldsymbol{Expr} \mid \boldsymbol{Expr} * \boldsymbol{Expr}$$

where $\boldsymbol{Int}$ is the set of integer constants

- It corresponds to the following inference rules

$$\frac{i \in \boldsymbol{Int}}{i\ \boldsymbol{Expr}} \quad (E\text{-}1)$$

$$\frac{e\ \boldsymbol{Expr}}{(e)\ \boldsymbol{Expr}} \quad (E\text{-}2)$$

$$\frac{e_1\ \boldsymbol{Expr} \quad e_2\ \boldsymbol{Expr}}{e_1 + e_2\ \boldsymbol{Expr}} \quad (E\text{-}3)$$

$$\frac{e_1\ \boldsymbol{Expr} \quad e_2\ \boldsymbol{Expr}}{e_1 * e_2\ \boldsymbol{Expr}} \quad (E\text{-}4)$$

Utrecht University

Simultaneous Inductive Definitions

- Infer `1 + 2 * 3` $\boldsymbol{Expr}$

$$\frac{}{\texttt{1+2*3} \quad \boldsymbol{Expr}} \qquad\qquad \frac{}{\texttt{1+2*3} \quad \boldsymbol{Expr}}$$

- The grammar is ambiguous!
  - we usually 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

    `1 * 2 * 3 = (1 * 2) * 3`

  - multiplication has a higher precedence than addition

Utrecht University

Simultaneous Inductive Definitions

- Alternative inference rules

What should $e1$ and $e2$ look like so that we can split at that + symbol?

can be any kind of arith. expr

can be any kind of arith. expr but not a sum!

$$e_1 \quad + \quad e_2$$

$$\boldsymbol{SExpr} \qquad \boldsymbol{PExpr}$$

$$\frac{e_1\ \boldsymbol{SExpr} \qquad e_2\ \boldsymbol{PExpr}}{e_1 + e_2\ \ \boldsymbol{SExpr}}$$

Simultaneous Inductive Definitions

- Alternative inference rules

can be any kind of arith. expr but not a sum

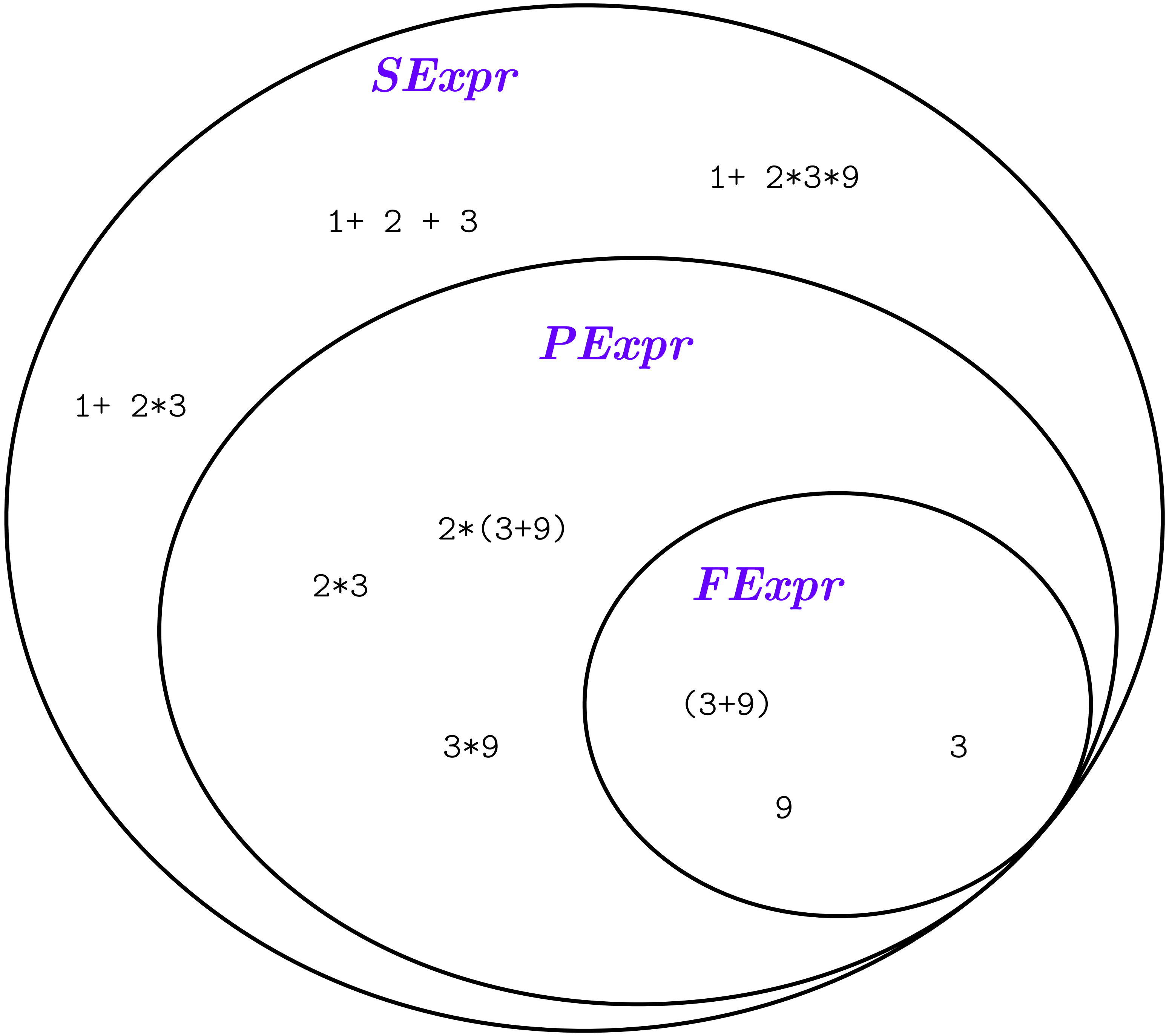
$e_1 \quad * \quad e_2$

only number or parenthesised expression

$\boldsymbol{PExpr} \qquad \boldsymbol{FExpr}$

$$\frac{e_1\ \boldsymbol{PExpr} \qquad e_2\ \boldsymbol{FExpr}}{e_1 * e_2\ \ \boldsymbol{PExpr}}$$

Simultaneous Inductive Definitions



Utrecht University

Simultaneous Inductive Definitions

- Alternative inference rules

$$\frac{e_1\ \boldsymbol{SExpr} \quad e_2\ \boldsymbol{PExpr}}{e_1 + e_2\ \boldsymbol{SExpr}}\ (S\text{-}1)$$

$$\frac{e\ \boldsymbol{PExpr}}{e\ \boldsymbol{SExpr}}\ (S\text{-}2)$$

$$\frac{e_1\ \boldsymbol{PExpr} \quad e_2\ \boldsymbol{FExpr}}{e_1 * e_2\ \boldsymbol{PExpr}}\ (P\text{-}1)$$

$$\frac{e\ \boldsymbol{FExpr}}{e\ \boldsymbol{PExpr}}\ (P\text{-}2)$$

$$\frac{e\ \boldsymbol{SExpr}}{(e)\ \boldsymbol{FExpr}}\ (F\text{-}1)$$

$$\frac{n \in \boldsymbol{Int}}{n\ \boldsymbol{FExpr}}\ (F\text{-}2)$$

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

Utrecht University

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 $\boldsymbol{SExpr}$, 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`)`

$$\frac{e_1\ \boldsymbol{SExpr} \quad e_2\ \boldsymbol{PExpr}}{e_1\ \texttt{+}\ e_2\ \boldsymbol{SExpr}}$$

$$\frac{e\ \boldsymbol{PExpr}}{e\ \boldsymbol{SExpr}}$$

$$\frac{e_1\ \boldsymbol{PExpr} \quad e_2\ \boldsymbol{FExpr}}{e_1\ \texttt{*}\ e_2\ \boldsymbol{PExpr}}$$

$$\frac{e\ \boldsymbol{FExpr}}{e\ \boldsymbol{PExpr}}$$

$$\frac{e\ \boldsymbol{SExpr}}{\texttt{(}e\texttt{)}\ \boldsymbol{FExpr}}$$

$$\frac{n \in \boldsymbol{Int}}{n\ \boldsymbol{FExpr}}$$

Ambiguous Grammars

M is also ambiguous:

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

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

$$\frac{s\ M}{(s)\ M}\ (M\text{-}3)$$

empty string problem (ε = ε ε = ε ε ε = ...)

Example: derive () M

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

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

Ambiguous Grammars

- How can we solve this?
  - we regard the expressions as a possibly empty list $\boldsymbol{L}$ of nested parenthesised expressions $\boldsymbol{N}$

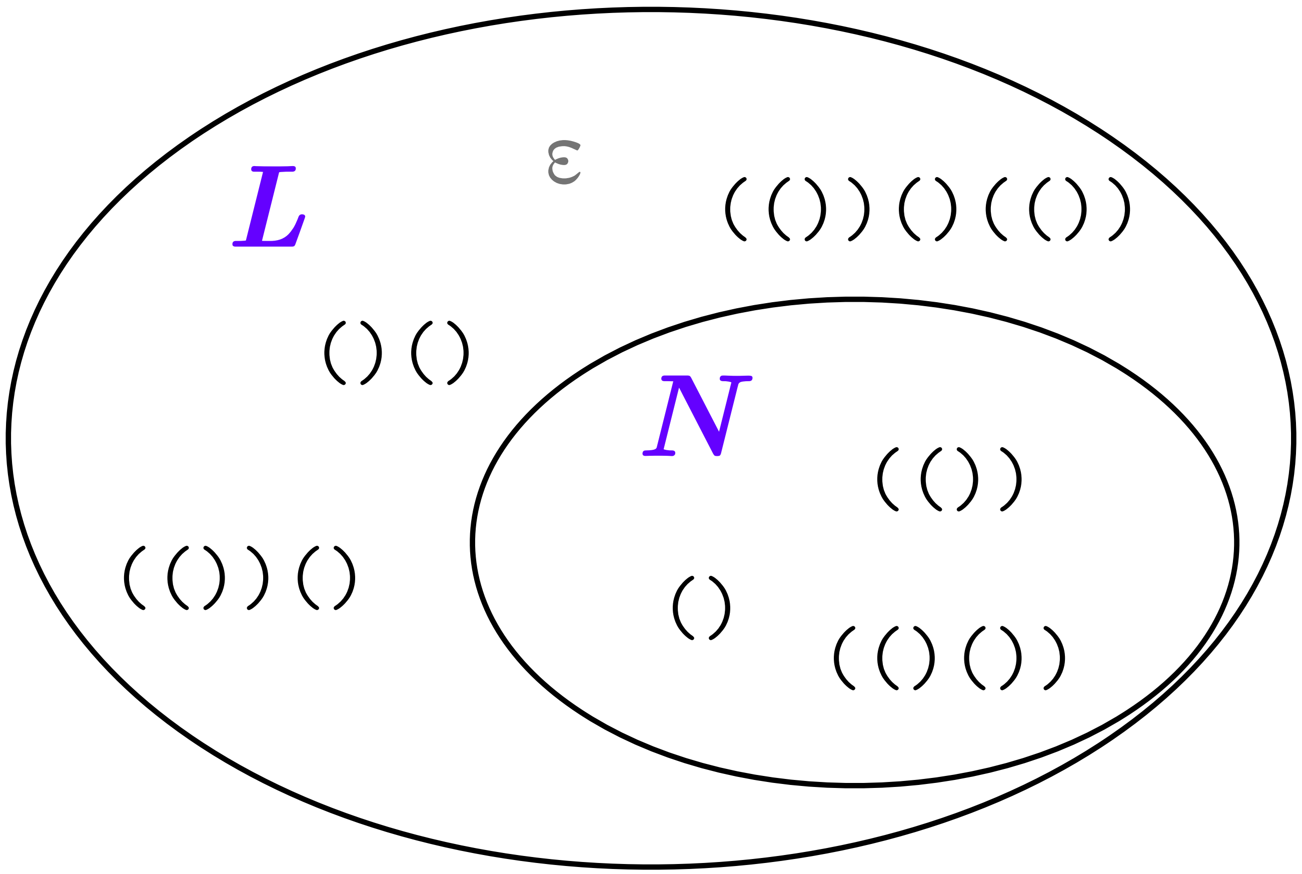
$$\frac{}{\epsilon\ \boldsymbol{L}}\qquad (L\text{-}1)$$

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

$$\frac{s\ \boldsymbol{L}}{(s)\ \boldsymbol{N}}\qquad (N\text{-}1)$$

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

Ambiguous Grammars



$\boldsymbol{N}$ is a subset of $\boldsymbol{L}$, as

$$\frac{s\ \boldsymbol{N}}{s\ \boldsymbol{L}}$$

is derivable

Ambiguous Grammars

- do both set of rules really define the same language? Is $\boldsymbol{L} = \boldsymbol{M}$?

- we need to show that they are indeed the same, we need to show that $s\ \boldsymbol{M}$ if and only if (iff) $s\ \boldsymbol{L}$:

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

(2) $s\ \boldsymbol{L}$ implies $s\ \boldsymbol{M}$ (*i.e.*, $\boldsymbol{L} \subseteq \boldsymbol{M}$)

$$\frac{}{\epsilon\ \boldsymbol{L}}\ (L\text{-}1) \qquad \frac{}{\varepsilon\ \ \boldsymbol{M}}\ (M\text{-}1)$$

$$\frac{s_1\ \boldsymbol{N} \quad s_2\ \boldsymbol{L}}{s_1 s_2\ \boldsymbol{L}}\ (L\text{-}2) \qquad \frac{s_1\ \boldsymbol{M} \quad s_2\ \boldsymbol{M}}{s_1 s_2\ \boldsymbol{M}}\ (M\text{-}2)$$

$$\frac{s\ \boldsymbol{L}}{(s)\ \boldsymbol{N}}\ (N\text{-}1) \qquad \frac{s\ \boldsymbol{M}}{(s)\ \boldsymbol{M}}\ (M\text{-}3)$$

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) $s = s_1 s_2$ for some $s_1\ M$ and $s_2\ M$ (induction step 1)

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

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

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

$$\frac{s\ L}{(s)\ N}\ (N\text{-}1) \qquad \frac{s\ M}{(s)\ M}\ (M\text{-}3)$$

Utrecht University

Proving $\boldsymbol{L} = \boldsymbol{M}$

- Proof that s $\boldsymbol{M}$ implies s $\boldsymbol{L}$ ($\boldsymbol{M} \subseteq \boldsymbol{L}$)

- Subproof 1 : $s = \varepsilon$

  Proof

  [A] ε $\boldsymbol{M}$

  [G] ε $\boldsymbol{L}$

  Begin

  1. {L-1} ε $\boldsymbol{L}$

  End

Proving $L = M$

- Proof that s M implies s L $(M \subseteq L)$

- Subproof 3 : $s = (s_1)$ for some string s_1 M

Proof

[IH] s_1 L

[G] (s_1) L

Begin

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

End

Proving $\boldsymbol{L} = \boldsymbol{M}$

- Proof that s $\boldsymbol{M}$ implies s $\boldsymbol{L}$ ($\boldsymbol{M} \subseteq \boldsymbol{L}$)

  - Subproof 2 : $s = s_1 s_2$ for some strings s_1 $\boldsymbol{M}$ and s_2 $\boldsymbol{M}$

Proof
[IH-1] s_1 $\boldsymbol{L}$
[IH-2] s_2 $\boldsymbol{L}$
[G] s_1 s_2 $\boldsymbol{L}$
Begin

doesn't work - we can't be sure that s_1 is actually in $\boldsymbol{N}$!

$$\text{(L-2)}\ \dfrac{\dfrac{????}{s_1\ \boldsymbol{N}} \qquad \dfrac{}{s_2\ \boldsymbol{L}}\ \text{(IH-2)}}{s_1 s_2\ \boldsymbol{L}}$$

Proving $\boldsymbol{L} = \boldsymbol{M}$

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

$$\frac{s_1 \; \boldsymbol{L} \qquad s_2 \; \boldsymbol{L}}{s_1 s_2 \; \boldsymbol{L}}$$

$$\frac{}{\epsilon \; \boldsymbol{L}} \quad (L\text{-}1) \qquad\qquad \frac{}{\varepsilon \; \boldsymbol{M}} \quad (M\text{-}1)$$

$$\frac{s_1 \; \boldsymbol{N} \qquad s_2 \; \boldsymbol{L}}{s_1 s_2 \; \boldsymbol{L}} \quad (L\text{-}2) \qquad\qquad \frac{s_1 \; \boldsymbol{M} \qquad s_2 \; \boldsymbol{M}}{s_1 s_2 \; \boldsymbol{M}} \quad (M\text{-}2)$$

$$\frac{s \; \boldsymbol{L}}{(s) \; \boldsymbol{N}} \quad (N\text{-}1) \qquad\qquad \frac{s \; \boldsymbol{M}}{(s) \; \boldsymbol{M}} \quad (M\text{-}3)$$

Proving $\boldsymbol{L} = \boldsymbol{M}$

- How can we prove this by rule induction?

$$\frac{s_1\ \boldsymbol{L} \qquad s_2\ \boldsymbol{L}}{s_1 s_2\ \boldsymbol{L}}$$

- There are two options - we can either prove it if by induction over s_1 or s_2
- As it was s_1 which caused the problem, it indicates that we should do induction over s_1

- Prove:

for all s $\boldsymbol{L}$ and all t $\boldsymbol{L}$:

$$\frac{s\ \boldsymbol{L} \qquad t\ \boldsymbol{L}}{st\ \boldsymbol{L}}$$

- Subproof 1 : $s = \varepsilon$

Proof

[A] t $\boldsymbol{L}$

[G] εt $\boldsymbol{L}$

Begin

1. {A, $\varepsilon t = t$} εt $\boldsymbol{L}$

End

$$\frac{}{\epsilon\ \boldsymbol{L}} \qquad (\textit{L-1})$$

$$\frac{s_1\ \boldsymbol{N} \qquad s_2\ \boldsymbol{L}}{s_1 s_2\ \boldsymbol{L}} \qquad (\textit{L-2})$$

$$\frac{s\ \boldsymbol{L}}{(s)\ \boldsymbol{N}} \qquad (\textit{N-1})$$

- Prove:

for all $s\ \boldsymbol{L}$ and all $t\ \boldsymbol{L}$:
$$\frac{s\ \boldsymbol{L} \qquad t\ \boldsymbol{L}}{st\ \boldsymbol{L}}$$

$$\frac{}{\epsilon\ \boldsymbol{L}}\ (L\text{-}1)$$

$$\frac{s_1\ \boldsymbol{N} \qquad s_2\ \boldsymbol{L}}{s_1 s_2\ \boldsymbol{L}}\ (L\text{-}2)$$

$$\frac{s\ \boldsymbol{L}}{(s)\ \boldsymbol{N}}\ (N\text{-}1)$$

- Subproof 2 : $s = s_1 s_2$, *with* $s_1\ \boldsymbol{N}$ *and* $s_2\ \boldsymbol{L}$

Proof

[A1] $s_1\ \boldsymbol{N}$

[A2] $s_2\ \boldsymbol{L}$

[IH] for all $t'\ \boldsymbol{L}$:
$$\frac{s_2\ \boldsymbol{L} \qquad t'\ \boldsymbol{L}}{s_2 t'\ \boldsymbol{L}}$$

[G] for all $t'\ \boldsymbol{L}$:
$$\frac{s_1 s_2\ \boldsymbol{L} \qquad t'\ \boldsymbol{L}}{s_1 s_2 t'\ \boldsymbol{L}}$$

Begin

Subproof

[A3] $t'\ \boldsymbol{L}$

[G] $s_1 s_2 t'\ \boldsymbol{L}$

$$\dfrac{\dfrac{}{s_1\ \boldsymbol{N}}\,(A1) \qquad \dfrac{\dfrac{}{s_2\ \boldsymbol{L}}\,(A2) \qquad \dfrac{}{t'\ \boldsymbol{L}}\,(A3)}{s_2 t'\ \boldsymbol{L}}\,(IH)}{s_1 s_2 t'\ \boldsymbol{L}}\,(L\text{-}2)$$

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 case distinction over s_1
  - we still need to show that if s L, *then* s M