1 Background

In the early 1900s, the principal efforts towards foundations for mathematical and logical reasoning—mathematical logic—focused on developing sets of axioms. Axioms are similar to rules in having meta-variables that can be instantiated (to logical formulas, for example), but differ from rules in having no premises as such. Instead, the premises are encoded as the conditions of implications. For example, the axiom

\[ A \supset (B \supset A) \]

says that if \( A \), then: if \( B \), then \( A \). More clearly, it can be read “if \( A \) and \( B \), then \( A \).” The first occurrence of \( A \) plays the role of a premise, as does the \( B \); the second occurrence of \( A \) plays the role of the conclusion.

Such axioms (the above is an image from Gentzen’s thesis, based on work by Hilbert and Glivenko) were not user-friendly: the process of instantiating axioms doesn’t line up well with the reasoning that mathematicians actually do.

Gentzen’s work has several advantages over axiom systems like the above.

First, rules clearly distinguish the premises from the conclusion. I think this is a relatively small advantage, because with some practice the premises are easy to see.

Second, each of Gentzen’s rules of natural deduction has a close analogue to actual mathematical reasoning, whereas axiom systems necessarily include “administrative” axioms like \( A \supset (B \supset A) \). This closeness arises by modelling assumptions; while natural deduction’s particular style of modelling assumptions is somewhat awkward, Gentzen also developed sequent calculus which models assumptions in a different way.

Third, along with rules Gentzen developed derivations. Rather than searching through a proof of \( A \land B \) for the parts contributing to \( A \) and the parts contributing to \( B \), a derivation proving \( A \land B \)
§1 Background

clearly separates the proof of $A$ from the proof of $B$. This compositionality makes derivations easier
to deal with as mathematical objects, and—from a computational standpoint—as data structures.

However, a disadvantage of derivations is that they are space-inefficient. (It was once fashion-
able for PL researchers to include large derivations in their papers; these usually required a figure in
“landscape” orientation.) Moreover, they do not resemble traditional mathematical proofs. Some
descendants of natural deduction, such as Fitch systems, adopt many of Gentzen’s rules (and his
rule notation) but use a line-by-line proof format rather than derivations. Such descendants seem
to be a good way to teach logic, and a good way to write careful and detailed proofs, but for our
purposes we need to handle proofs as objects (data structures) in their own right.

2 Introduction and elimination

A feature of natural deduction (inherited by type systems!) is that the rules can be systematically
designed, or at least systematically organized. The rules for each connective, such as $\land$ or $\lor$, can be
categorized as (1) rules that introduce the connective, and (2) rules that eliminate the connective.
(The number of rules in each category depends on the connective; one very common connective
has zero elimination rules.)

In addition, the rules of natural deduction are orthogonal: the rules to introduce and eliminate
$\land$ only mention $\land$, not $\lor$ or any other connective. This makes natural deduction, and type systems
based on it, easier to extend: to incorporate a connective, we only have to design its introduction
and elimination rules—which may not be easy but can be done without regard for any other
connectives. The rules for each connective are a kind of “module” in the rule system.
§2 Introduction and elimination

3 Natural deduction

atomic formulas  P, Q
formulas  A, B, C ::=
  P  atomic formula
  A ⊃ B  implication
  A ∨ B  conjunction (and)
  A ∧ B  disjunction (or)
  ∀a : nat. A  universal quantification
  ∃a : nat. A  existential quantification

\[ A \text{ true} \]

\[
\frac{A \text{ true} \quad B \text{ true}}{A \land B \text{ true}} \quad \land \text{Intro} \quad \frac{A \land B \text{ true}}{A \text{ true}} \quad \land \text{Elim1} \quad \frac{A \land B \text{ true}}{B \text{ true}} \quad \land \text{Elim2}
\]

\[ x[A \text{ true}] \]

\[ \vdots \]

\[
\frac{B \text{ true}}{(A \supset B) \text{ true}} \quad \supset \text{Intro} \]

\[
\frac{A \supset B \text{ true} \quad A \text{ true}}{B \text{ true}} \quad \supset \text{Elim}
\]

Rule \( \supset \text{Elim} \) is modus ponens, but rule \( \supset \text{Intro} \) requires an assumption. The assumption “floats” above the subderivation in which it is available; it is available between the floating assumption \( x[A \text{ true}] \) to its point of introduction, marked with the superscript \( x \) next to the rule name. I have highlighted the \( x \) in the rule, but we may have to work without highlighting.

This notation for assumptions is somewhat unfriendly: it’s easy to lose track of the scope of the assumption. But this notation may be closer to ordinary mathematical reasoning, and it’s historically important, so we’ll keep using it for now.

Disjunction usually causes more trouble than conjunction, and this certainly holds for natural deduction. However, there is a duality between conjunction and disjunction. In Boolean logic, you can get a feeling for this by comparing the truth table for AND with the truth table for OR, after swapping “true” and “false” in one of them. In natural deduction, this opposition between conjunction and disjunction shows itself in a similarity between the elimination rules for \( \land \), which are \( \land \text{Elim1}/\land \text{Elim2} \), and the introduction rules for \( \lor \):

\[
\frac{A \text{ true}}{A \lor B \text{ true}} \quad \lor \text{Intro1} \quad \frac{B \text{ true}}{A \lor B \text{ true}} \quad \lor \text{Intro2}
\]

Observe that \( \lor \text{Intro1} \) is \( \land \text{Elim1} \) turned upside down, with \( \land \) changed to \( \lor \).

Sadly, flipping the introduction rule \( \land \text{Intro} \) upside down doesn’t give us a good \( \lor \)-elimination rule:

\[
\frac{A \lor B \text{ true}}{A \text{ true} \quad B \text{ true}} \quad ?? \lor \text{Elim} ??
\]

This rule seems to have two conclusions. People sometimes write more than one conclusion as a concise notation for two rules with identical premises—we could combine \( \land \text{Elim1} \) and \( \land \text{Elim2} \), for example. But it’s certainly not true that, from “\( A \) or \( B \)”, we should get \( A \) and \( B \).
Instead, our $\lor$Elim rule will reason by cases. If $A \lor B$ then either $A$, or $B$. As we can split a proof into cases according to a given grammar (“Case $e = n\ldots Case e = (+e_1e_2)$”), we can have subderivations with different assumptions.

$$
\begin{align*}
\begin{array}{c}
x[A \text{ true}] \\
y[B \text{ true}] \\
\vdots \\
A \lor B \text{ true} \\
\end{array} & \quad \begin{array}{c}
\vdots \\
C \text{ true} \\
C \text{ true} \\
\end{array} \\
\hline
C \text{ true} & \lor\text{Elim}^{x,y}
\end{align*}
$$

To understand why the conclusion of $\lor$Elim should be $C \text{ true}$, where $C$ is any formula, it may help to think about case analysis in a (line-by-line) proof: we can case-analyze regardless of what our goal is. We might be trying to show that $v = 0$, or that $v_1 = v_2$, or that $e \Downarrow v$; whatever the goal, case analysis works the same way. The only requirement is that each case must show the same goal: if we want to show $v = 0$ we need to show $v = 0$ assuming $e = n$, and $v = 0$ assuming $e = (+e_1e_2)$.

### 3.1 Example!

$$
\begin{align*}
z[A_1 \lor A_2 \text{ true}] \\
x[A_1 \text{ true}] \\
y[A_2 \text{ true}] \\
\hline
\begin{array}{c}
A_1 \lor A_2 \text{ true} \\
\end{array} & \quad \begin{array}{c}
A_1 \text{ true} \\
\lor\text{Intro}^x \\
A_2 \lor A_1 \text{ true} \\
\lor\text{Intro}^y \\
A_2 \lor A_1 \text{ true} \\
\hline
\lor\text{Intro}^{x,y}
\end{array}
\end{align*}
$$

$$
\begin{align*}
\begin{array}{c}
A_1 \text{ true} \\
\lor\text{Intro}^x \\
A_2 \lor A_1 \text{ true} \\
\hline
A_2 \lor A_1 \text{ true} \\
\lor\text{Intro}^{x,y}
\end{array} & \quad \begin{array}{c}
A_2 \lor A_1 \text{ true} \\
\lor\text{Intro}^{x,y}
\end{array}
\end{align*}
$$

$$
\begin{align*}
\begin{array}{c}
A_1 \lor A_2 \text{ true} \\
\end{array} & \quad \begin{array}{c}
A_2 \lor A_1 \text{ true} \\
\hline
\lor\text{Intro}^{x,y}
\end{array}
\end{align*}
$$

$$
\begin{align*}
\begin{array}{c}
A_1 \lor A_2 \text{ true} \\
\end{array} & \quad \begin{array}{c}
A_2 \lor A_1 \text{ true} \\
\hline
\lor\text{Intro}^{x,y}
\end{array}
\end{align*}
$$

$$
\begin{align*}
\begin{array}{c}
A_1 \lor A_2 \text{ true} \\
\end{array} & \quad \begin{array}{c}
A_2 \lor A_1 \text{ true} \\
\hline
\lor\text{Intro}^{x,y}
\end{array}
\end{align*}
$$

$$
\begin{align*}
\begin{array}{c}
A_1 \lor A_2 \text{ true} \\
\end{array} & \quad \begin{array}{c}
A_2 \lor A_1 \text{ true} \\
\hline
\lor\text{Intro}^{x,y}
\end{array}
\end{align*}
$$

$$
\begin{align*}
\begin{array}{c}
A_1 \lor A_2 \text{ true} \\
\end{array} & \quad \begin{array}{c}
A_2 \lor A_1 \text{ true} \\
\hline
\lor\text{Intro}^{x,y}
\end{array}
\end{align*}
$$
§3 Natural deduction

(In 2018, this was roughly the dividing line between the January 25th and January 30th lectures.)

4 Natural deduction, extended

atomic formulas \( P, Q \) 
formulas \( A, B, C \) ::=
| \( P \) atomic formula  
| \( A \supset B \) implication  
| \( A \land B \) conjunction (and)  
| \( A \lor B \) disjunction (or)  
| \( \forall a : \text{nat. } A \) universal quantification  
| \( \exists a : \text{nat. } A \) existential quantification  
| \( \text{True} \) truth

4.1 True

To design rules for the formula True, it may be helpful to view it as an “and” of nothing—a 0-ary conjunction. Since \( \land \) is a binary (2-ary) conjunction whose introduction rule \( \land \text{Intro} \) has two premises, following that structure leads to the rule TrueIntro, which has zero premises. This seems consistent with an intuitive understanding of True: since True has no subformulas, its truth does not depend on the truth of the subformulas (unlike \( \land \) where \( A \land B \) is true only if \( A \) and \( B \) are true).

For the elimination rule(s), we can also argue by analogy to \( \land \). However, the argument feels a little different from the argument for the introduction rule.

\[
\frac{A \land B \text{ true}}{A \text{ true} \ \land \text{Elim1}} \quad \frac{A \land B \text{ true}}{B \text{ true} \ \land \text{Elim2}}
\]

\[
\frac{\text{x}[A \text{ true}]}{B \text{ true} \ \lor \text{Intro1}} \quad \frac{A \supset B \text{ true}}{A \text{ true} \ \supset \text{Elim}} \quad \frac{\text{x}[A \text{ true}]}{B \text{ true} \ \supset \text{Elim}} \quad \frac{\text{y}[B \text{ true}]}{C \text{ true} \ \lor \text{Elim}^x,y}
\]

\[
\frac{A \lor B \text{ true}}{C \text{ true} \ \lor \text{Intro2}} \quad \frac{A \lor B \text{ true}}{C \text{ true} \ \lor \text{Elim}^x,y}
\]

\[
\frac{C \text{ true}}{\text{True true} \ \text{TrueIntro}} \quad \quad \text{no elimination rules for True}
\]
The trick is to find something about the above rules related to the number two. But the only thing related to two within $\land$Elim1 and $\land$Elim2 is the formula $A \land B$ itself: each rule has one premise. Instead, we must step back and observe that the number of elimination rules is two. Since $\land$ is 2-ary and True is 0-ary, this suggests that we should have zero elimination rules for True!

We can justify this by analogy to $\land$, but more intuitively: the formula $A \land B$ combines two facts ($A$ is true and $B$ is true), leading to two elimination rules, each extracting one of those two facts. But no facts are needed to justify True. Therefore, no facts can be extracted. Perhaps we could argue that True itself could be extracted:

\[
\begin{array}{c}
\text{True} \\
\text{true} \\
\text{True} \\
\text{true}
\end{array}
\]

But this rule is admissible (that is, redundant): we already have TrueIntro, which has the same conclusion. (Any rule with a premise that is identical to its conclusion is admissible.)

Allowing rules to have multiple conclusions is something that I'm trying to avoid, because it can be confusing, but allowing that leads to another argument for having no elimination rules. If we allow multiple conclusions then we can combine $\land$Elim1 and $\land$Elim2:

\[
\begin{array}{c}
A \land B \\
\text{true}
\end{array}
\quad
\begin{array}{c}
A \\
\text{true}
\end{array}
\quad
\begin{array}{c}
B \\
\text{true}
\end{array}
\]

$\land$Elim-combined

Since this rule has two conclusions, TrueElim should have zero conclusions. But a rule with no conclusions isn’t a rule; even if we tried to bend the definition to allow it, it can’t conclude anything because it has no conclusion.

\section{Harmony}

The above arguments for designing rules for True have “intensional flavour”: we argued for our design based on existing internal features—our rules for $\land$—of the system (and then checked the resulting rules against our intuitive understanding of True).

This seems to run against Carnap’s aphorism, “In logic, there are no morals.” It suggests that we have some constraints around how the parts of the system fit together.

While I argued (in lecture, not written up here yet) by analogy to true as an identity element for $\land$, that wasn’t strictly necessary. Whether or not we believe that $\land$ comports with common usage of the word “and”, we can ask: If $\land$ is the 2-ary version of something, what is the 0-ary version? We can choose to call that 0-ary version “True”, or “tonk”, or even “False” (if we enjoy confusion).

One intensional quality-assurance tool doesn’t even need to compare the rules for different connectives: harmony checks that the introduction rules and elimination rules for a single connective match (are in harmony with) each other. Harmony has two parts:

- **Local soundness** holds when the results of applying elimination rules were already used in the introduction rule. On a high level, facts go into an introduction rule; the elimination rules should produce only those facts.

- **Local completeness** holds when the elimination rules can be used to recover all of the facts that went into the introduction.
§5 Harmony

Checking that rules satisfy these two parts of harmony gives us some protection against two possible design mistakes: neglecting to add a necessary rule, and adding a rule that is too powerful. Specifically:

- If local soundness is violated, either an elimination rule is wrong (it is producing something outside the “inputs” to the introduction rule), or we forgot an introduction rule.
- If local completeness is violated, either we forgot an elimination rule, or an introduction rule is wrong.

It's probably easiest to grasp these ideas by considering some relatively clear mistakes in designing rules for conjunction.

\[
\text{A true} \quad \text{B true} \quad \text{\(\land\) Intro} \quad \text{A \land B true} \quad \text{\(\land\) Elim1}
\]

Suppose the above two rules were our only rules for \(\land\). Local soundness holds, because our (only) elimination rule \(\land\)Elim1 produces A true, which “went into” our use of \(\land\)Intro:

\[
\text{A true} \quad \text{B true} \quad \text{\(\land\) Intro} \quad \text{A \land B true} \quad \text{\(\land\) Elim1}
\]

But local completeness fails, because our single elimination rule can't recover the information B true. Checking local completeness ensures that we remember to include both elimination rules.

On the other hand, suppose we have both elimination rules but forget one of the premises of \(\land\)Intro.

\[
\text{A true} \quad \text{\(\land\) Intro??} \quad \text{A \land B true} \quad \text{\(\land\) Elim1} \quad \text{A \land B true} \quad \text{\(\land\) Elim2}
\]

Checking local soundness will reveal the problem:

\[
\text{A true} \quad \text{\(\land\) Intro??} \quad \text{A \land B true} \quad \text{\(\land\) Elim2}
\]

The rule \(\land\)Elim2 derives B true, but B true didn't go into our (wrong) introduction rule \(\land\)Intro??, so \(\land\)Elim2 is locally unsound with respect to \(\land\)Intro??.

Local soundness and local completeness are not quite the same as soundness and completeness between different systems, but they are similar in that they depend on keeping something in a “fixed position” and comparing other stuff to the fixed thing: Ordinary soundness takes some system as ground truth, and checks that another system stays within that ground truth; ordinary completeness asks whether another system covers everything within that ground truth. Local soundness keeps the introduction rules stationary, and ensures that the elimination rules stay “within the scope” of the introduction rules. Local completeness also keeps the introduction rules stationary, and checks that the elimination rules can recover all of the information used by the introduction rules.
§5 Harmony

Let’s check that our rules for \( \supset \) satisfy local soundness and local completeness.

\[
\begin{array}{c}
\text{x[A true]} \\
\vdots \\
B \text{ true} \\
\hline
(A \supset B) \text{ true} \\
\end{array}
\quad \frac{\text{ Intro} \times}{\text{ A \supset B \ true} \quad \text{ A true} \quad \text{ Elim}}
\]

5.1 Local soundness for \( \supset \)

For each elimination rule for \( \supset \), we ask if that rule is locally sound. We have one elimination rule for \( \supset \); is it locally sound?

\[
\begin{array}{c}
\text{x[A true]} \\
\vdots \\
B \text{ true} \\
\hline
(A \supset B) \text{ true} \\
\end{array}
\quad \frac{\text{ Intro} \times}{\text{ A true} \quad \text{ Elim}}
\]

This is a little more complicated than \( \land \), because \( \supset \) Elim has a second premise \( A \text{ true} \). We can apply \( \supset \) Elim only when \( A \text{ true} \). So the question becomes: did the information

“assuming \( A \text{ true} \) [the other premise of \( \supset \) Elim], it holds that \( B \text{ true} \) [the conclusion of \( \supset \) Elim]”

go into the application of \( \supset \) Intro? Yes, because the (only) premise of \( \supset \) Intro derived \( B \text{ true} \) under the assumption \( A \text{ true} \).

5.2 Local completeness for \( \supset \)

For local completeness, we ask whether all the information going into \( \supset \) Intro can be recovered using one of the elimination rules for \( \supset \). Since there is only one elimination rule, we ask whether the information going into \( \supset \) Intro can be recovered using \( \supset \) Elim. That information was

“assuming \( A \text{ true} \) [the assumption within the premise of \( \supset \) Intro], it holds that \( B \text{ true} \) [the premise of \( \supset \) Intro].”

(This is the same piece of information that we used in local soundness, but only because our rules really do satisfy local soundness and local completeness!) The argument for local completeness goes like this:

1. Assume we have a derivation of \( A \supset B \text{ true} \) whose concluding rule is \( \supset \) Intro.

2. Assume \( A \text{ true} \).
3. Our goal is to derive B true.

4. Applying rule \( \supset \text{Elim} \) to \( A \supset B \) true and \( A \) true gives \( B \) true.

Note that if we had forgotten to write \( \supset \text{Elim} \), we could not take the last step of this argument.

5.3 Local soundness for True

For each elimination rule for True, we ask if that rule is locally sound. We have no elimination rules for True, so there is nothing to check.

5.4 Local completeness for True

For local completeness, we ask whether all the information going into \( \text{TrueIntro} \) can be recovered using one of the elimination rules for True. But \( \text{TrueIntro} \) has no premises, so no information went into it. So there is nothing to check.

5.5 Local soundness for \( \lor \)

For each elimination rule for \( \lor \), we ask if that rule is locally sound. We have only one elimination rule for \( \lor \), but it is somewhat complicated:

\[
\begin{array}{c}
\vdots \\
A \lor B \text{ true} \\
\vdots \\
\text{C true} \\
\text{C true} \\
\text{C true} \\
\end{array}
\]

Since we have more than one introduction rule for \( \lor \), we don’t know which of them was used to derive \( A \lor B \) true, so I have included some “…”.

For \( \supset \) we assumed the other (second) premise of \( \supset \text{Elim} \). So here, we assume the other (second and third) premises of \( \lor \text{Elim} \):

- Second premise of \( \lor \text{Elim} \): “assuming \( A \) true, then \( C \) true.”
- Third premise of \( \lor \text{Elim} \): “assuming \( B \) true, then \( C \) true.”

We also assume the first premise, the derivation of \( A \lor B \) true by one of the \( \lor \)-introduction rules. Consider cases of which introduction rule was used. Our goal is to show \( C \) true.

- Case: \( \lor \text{Intro1} \) was used.
  By inversion on \( \lor \text{Intro1} \), \( A \) true.
  We know (“Second premise of \( \lor \text{Elim} \)” that, if \( A \) true, then \( C \) true. Since we know \( A \) true, we know \( C \) true.

- Case: \( \lor \text{Intro2} \) was used.
  By inversion on \( \lor \text{Intro2} \), \( B \) true.
  We know (“Third premise of \( \lor \text{Elim} \)” that, if \( B \) true, then \( C \) true. Since we know \( B \) true, we know \( C \) true.
5 Harmony

5.6 Local completeness for $\lor$

Arguing local completeness for $\lor$ is tricky, because $\lor$Elim does not literally produce the information that went into the introduction rule. Instead, it splits into two cases, each working towards a common goal $C$ true, where $C$ may not be the same as $A$ or $B$. Instead of trying to get the literal information $A$ true (or $B$ true), we must consider what we could deduce if we knew that either $A$ true holds or $B$ true holds.

1. Assume, as usual, $A \lor B$ true by one of the introduction rules for $\lor$; this is the first premise of $\lor$Elim.

2. Also assume, as usual, the remaining premises of $\lor$Elim.

3. Suppose that $C'$ is a formula that can be deduced assuming $A$, and can be deduced assuming $B$. Our goal is now to use $\lor$Elim to derive $C'$ true.

4. We want to apply $\lor$Elim. We don't get to choose $A$ and $B$; they are determined by the pre-existing derivation of $A \lor B$ true. However, we can choose $C$.

5. Let $C$ be $C'$.

6. Either $\lor$Intro1 was used to derive $A \lor B$ true, or $\lor$Intro2 was used to derive it.

   • Case: $\lor$Intro1 was used.
     By inversion on $\lor$Intro1, $A$ true.
     The second premise of $\lor$Elim is that $C'$ true under the assumption $A$ true. That is, $C'$ true can be deduced from $A$ true.

   • Case: $\lor$Intro2 was used.
     By inversion on $\lor$Intro2, $B$ true.
     The second premise of $\lor$Elim is that $C'$ true under the assumption $B$ true. That is, $C'$ true can be deduced from $B$ true.

7. By rule $\lor$Elim, $C'$ true.

The business about $C'$ is needed to reject a possible bug in $\lor$Elim: an insufficiently general conclusion. Consider this specialized version of $\lor$Elim, which can express our example in Section 3.1 but nothing else:

\[
\begin{array}{c}
   x[A \text{ true}] & y[B \text{ true}] \\
   : & : \\
   A \lor B \text{ true} & B \lor A \text{ true} & B \lor A \text{ true} \\
   & B \lor A \text{ true} \\
\end{array}
\]

If $\lor$Elim-swap were our only elimination rule for $\lor$, step 5—Let $C$ be $C'$—would work only in the special case of $C' = B \lor A$. Since $\lor$Elim-swap cannot derive other conclusions, including—for example—$(A \lor B) \lor A$, our argument fails, as it should: $\lor$Elim-swap is incomplete because it doesn't work for most possible $C'$.

Note that $\lor$Elim-swap is locally sound: it works for only one conclusion, but for that conclusion, it does not go beyond the premise of the introduction rule.


§5 Harmony

■ Exercise 1. Consider the connective tonk, due to A.N. Prior (1960), who argued (tongue-in-cheek) that tonk would succeed based on its “extreme convenience”. Translated to our notation, Prior gave two rules for tonk:

\[
\frac{A \text{ true}}{(A \text{ tonk } B) \text{ true}} \quad \frac{(A \text{ tonk } B) \text{ true}}{B \text{ true}}
\]

Essentially, this connective steals one of the introduction rules for $\lor$ and one of the elimination rules for $\land$.

Argue that local soundness for tonk does not hold.
6 Quantifiers and falsehood

For quantifiers, we need some notation that substitutes a specific natural number for the quantified variable. Suppose we have
\[ \forall \, a : \text{nat.} \, (\text{even}(a) \lor \text{odd}(a)) \]
and we want to know that the natural number 5 is either even or odd. We can get
\[ (\text{even}(5) \lor \text{odd}(5)) \]
by looking for \( a \) (the quantified variable) throughout the body of the quantifier, and wherever we find \( a \), replacing it with 5.
\[ \forall \, a : \text{nat.} \, (\text{even}(a) \lor \text{odd}(a)) \]
body of the quantifier

We will write this use of substitution as
\[ [5/a](\text{even}(a) \lor \text{odd}(a)) \]
or more generally,
\[ [n/a]A = A \text{ with } n \text{ replacing each occurrence of } a \]

Substitution is a meta-level operation, like writing \( n_1 + n_2 \) in the rule eval-add. As with addition, it would be better to formally define what \([n/a]A\) means. However, the full definition of substitution has some “interesting” parts, which I don’t want to explain just yet.

If you’re curious about what the interesting parts might be, consider what should happen if we substitute 5 for \( b \) in the following:
\[ (b > 2) \land \left( \text{prime}(a) \supset (\exists \, b : \text{nat.} \, (b > a) \land \text{prime}(b)) \right) \]

6.1 Mnemonic device

The PL research community has not converged on one standard notation for substitution. I have a number of reasons for preferring the notation above, which I won’t bore you with. A shortcoming of my preferred notation is that the order of \( n \) (the thing replacing the variable) and \( a \) (the variable being replaced) is not immediately clear. Here is a memory trick (more snobbily, a mnemonic device):

If we look for all occurrences of \( a \) throughout \( a \), and replace \( a \) with 5, we write that as
\[ [5/a]a = 5 \]

If we creatively reinterpret \( 5/a \) as a fraction and reinterpret substitution as multiplication, we can “cancel” the \( a \):
\[ \frac{5}{a} \cdot a = \frac{5 \cdot a}{a} = 5 \]
### 6.2 Substitution as renaming

We don't have to substitute a constant natural number like 5. We could also substitute a variable.

\[
\left[ a'/a \right] ((b > a) \land \text{prime}(b)) = ((b > a') \land \text{prime}(b))
\]

We could then substitute a constant for \( a' \):

\[
\left[ 2/a' \right] \left[ a'/a \right] ((b > a) \land \text{prime}(b)) = \left[ 2/a' \right] ((b > a') \land \text{prime}(b)) = ((b > 2) \land \text{prime}(b))
\]

A nice feature of this notation is that such “double substitutions” have the same variable in the centre: “2 replaces \( a' \) which replaces \( a \), so 2 is replacing \( a \)”, or (reading right to left) “replace \( a \) with \( a' \), then replace \( a' \) with 2”.
§6 Quantifiers and falsehood

6.3 Natural deduction, extended again (2018–02–01)

atomic formulas
P, Q
formulas
A, B, C ::= P atomic formula
A ⊃ B implication
A ∧ B conjunction (and)
A ∨ B disjunction (or)
∀a : nat. A universal quantification
∃a : nat. A existential quantification
True truth
False falsehood

[A true] A is true

x [A true]

B true ⊃Intro\scriptstyle x

(A ⊃ B) true ⊃Elim

True true TrueIntro

no elimination rules for True

A true B true ∧Intro

A ∧ B true ∧Elim1 A ∧ B true ∧Elim2

x[a] : nat

B true ∀Intro\scriptstyle x

(∀a : nat. B) true n : nat ∀Elim

[n/a]B true

x[A true]
y[B true]

C true ∨Elim\scriptstyle x,y

no introduction rules for False

False true FalseElim

x[a] : nat

y[B true]

C true ∃Intro

(∃a : nat. B) true C true ∃Elim\scriptstyle x,y

lec6–8, J. Dunfield, CISC 465/865 Winter 2020: 2020/1/28
6 Quantifiers and falsehood

6.3.1 Motivation for the new rules

Here we have added rules for $\forall$, $\exists$, and $\text{False}$. In class, I motivated the design through various symmetries:

- True is a 0-ary conjunction, $\land$ is a 2-ary (binary) conjunction, $\forall$ is an $\infty$-ary (infinitary) conjunction.
- False is a 0-ary disjunction, $\lor$ is a 2-ary (binary) disjunction, $\exists$ is an $\infty$-ary (infinitary) disjunction.

For $\forall\text{Intro}$, the 2 premises of $\land\text{Intro}$ for the 2-ary $\land$ became “infinite premises”, one for each natural number.

\[
\begin{array}{l}
[0/a]B \text{ true} & [1/a]B \text{ true} & [2/a]B \text{ true} & \cdots \\
\hline
(\forall a : \text{nat.} B) \text{ true}
\end{array}
\]

Our actual $\forall\text{Intro}$ rule represents this infinite set of premises as one premise with an assumption that $a$ is a natural number.

For $\forall\text{Elim}$, the 2 elimination rules of $\land\text{Elim}$ for the 2-ary $\land$ became an infinite number of elimination rules.

\[
\begin{array}{l}
(\forall a : \text{nat.} B) \text{ true} & \forall\text{Elim0} (\forall a : \text{nat.} B) \text{ true} & \forall\text{Elim1} (\forall a : \text{nat.} B) \text{ true} & \forall\text{Elim2} (\forall a : \text{nat.} B) \text{ true} & \cdots \\
\hline
[0/a]B \text{ true} & [1/a]B \text{ true} & [2/a]B \text{ true}
\end{array}
\]

Since we cannot directly write all the rules in the infinite set $\{\forall\text{Elim0}, \forall\text{Elim1}, \forall\text{Elim2}, \forall\text{Elim3}, \ldots\}$, we replaced them with one rule that requires a specific $n$:

\[
\begin{array}{l}
(\forall a : \text{nat.} B) \text{ true} & n : \text{nat} \\
\hline
[n/a]B \text{ true}
\end{array}
\]

If we choose $n = 0$, our $\forall\text{Elim}$ does the same thing as $\forall\text{Elim0}$; if we choose $n = 1$, it does the same thing as $\forall\text{Elim1}$, and so forth.

Moving on to $\exists$, I waved my hands about duality between $\forall$ and $\exists$—which suggests that aspects of $\forall\text{Intro}$, should find their way into $\exists$’s elimination rule, and that aspects of $\forall\text{Elim}$ should show up in $\exists$’s introduction rule. I also (perhaps more clearly) used our rules for 2-ary disjunction $\lor$ to inform the rules for the infinitary disjunction $\exists$.

Thus, the 2 introduction rules for the 2-ary $\lor$ became an infinite number of introduction rules

\[
\begin{array}{l}
(\exists a : \text{nat.} B) \text{ true} & \exists\text{Intro0} (\exists a : \text{nat.} B) \text{ true} & \exists\text{Intro1} (\exists a : \text{nat.} B) \text{ true} & \exists\text{Intro2} (\exists a : \text{nat.} B) \text{ true} & \cdots \\
\hline
[0/a]B \text{ true} & [1/a]B \text{ true} & [2/a]B \text{ true}
\end{array}
\]

which we coalesced into $\exists\text{Intro}$, noting that since the elimination rule for $\forall$ has a premise $n : \text{nat}$, duality between $\forall$ and $\exists$ suggests that the introduction rule for $\exists$ should also assume $a : \text{nat}$ within a premise.

Our elimination rule for $\exists$ has similar structure to our elimination rule for $\lor$. We arrived at that structure by, first, replicating the two $C \text{ true}$ premises of $\lor$ into an infinite set gives

\[
\begin{array}{l}
y_0[0/a]B \text{ true} & y_1[1/a]B \text{ true} & y_2[2/a]B \text{ true} \\
\vdots & \vdots & \vdots \\
(\exists a : \text{nat.} B) \text{ true} & C \text{ true} & C \text{ true} & C \text{ true} & \cdots \\
\hline
C \text{ true}
\end{array}
\]

Our actual $\exists\text{Elim}$ rule represents this infinite set of premises as one premise under the assumption $a : \text{nat}$.

lec6–8, J. Dunfield, CISC 465/865 Winter 2020: 2020/1/28
6 Quantifiers and falsehood

6.4 Historical notes (optional reading)

6.4.1 Assumptions and substitution

In Gentzen’s natural deduction system (“NJ”, essentially a misprint of “NI”), the assumptions \( x [a : \text{nat}] \) are not written out. Moreover, Gentzen’s rules rename the variable in the quantifier (e.g. the \( a \) in \( \forall a : \text{nat}. B \)) to a new variable \( a' \): Instead of assuming \( a : \text{nat} \) and \( B \) true, Gentzen assumes \([a'/a]B \) true and calls the new variable \( a' \) an Eigenvariable. (Eigen is German for “own”: the eigenvariable “belongs” to the particular application of the rule.)

This “extra” substitution is painless in Gentzen’s notation, because he wrote quantifiers differently: instead of \( \forall a : \text{nat}. A \), with \( \forall a : \text{nat}. \text{prime}(a) \) as a concrete example, he wrote (roughly) \( \forall a : \text{nat}. A(a) \). Then the substitution of \( a' \) for \( a \) in the body \( A(a) \) of the quantifier can be written as \( A(a') \). If this course were entirely about natural deduction, I might have used Gentzen’s notation since it is more compact than square-bracket substitutions, but Gentzen’s notation is not suited for code in programming languages. By using square-bracket substitution, we can use the same notation consistently.

6.4.2 Judgment form

Gentzen did not write \texttt{true} in judgments or derivations. For example, Gentzen’s original \( \land \text{Intro} \) looked like this:

\[
\begin{array}{c}
\text{A} \\
\text{B}
\end{array} \quad \rightarrow
\begin{array}{c}
\text{A} \\
\text{B}
\end{array} \\ 
\begin{array}{c}
\text{A} \land \text{B}
\end{array} \quad \land \text{I}
\]

6.4.3 Included connectives

Apart from such notational differences, Gentzen’s NJ differs from our development in several ways:

- NJ does not include \texttt{True}. Without \texttt{True}, I think our FalseElim would seem less plausible.
- NJ does include negation, which still lurks on our horizon. Also, while Gentzen has our exact FalseElim, he calls it a negation elimination rule... because he \textit{does} have a way to derive False through a negation-elimination rule.

6.4.4 Local soundness

For Gentzen [1934] §5.13), the introduction rules for a connective are its definition. He informally explained (without using the term) an example of local soundness (for \( \supset \)), noting that “we need not go into the ‘informal sense’ of the \( \supset \)-symbol”: local soundness is an intensional (internal) property of the rules. Later, the view that introduction rules define a connective became known as verificationism (we “verify” that \( A \land B \) true is derivable by applying the introduction rule for \( \land \)). An opposing view, known as pragmatism, regards the elimination rules as “the” definition: the meaning of \( A \land B \) true is what you can do with it.

References