ConstLog: Constructive Logic

Lecture Notes on Natural Deduction

Frank Pfenning André Platzer

Carnegie Mellon University || Karlsruhe Institute of Technology

Lecture 2

1 Introduction

The goal of this chapter is to develop the two principal notions of logic, namely *propositions* and *proofs*. Ironically, there is no universal agreement about the proper foundations for these notions. The classical logic approach of defining the meaning of logical operators by induction as a function on truth values does not work for constructive logic. One approach, which has been particularly successful for applications in computer science, is to understand the meaning of a proposition by understanding its proofs. In the words of Martin-Löf [ML96, Page 27]:

> *The meaning of a proposition is determined by [. . .] what counts as a verification of it.*

A *verification* may be understood as a certain kind of proof that only examines the constituents of a proposition, which we will formalize in a later lecture. For today's lecture, we will define proofs. This is analyzed in greater detail by Dummett [Dum91] although with less direct connection to computer science. The system of inference rules that arises from this point of view is *natural deduction*, first proposed by Gentzen [Gen35] and studied in depth by Prawitz [Pra65].

We follow Martin-Löf's approach, in a rich philosophical tradition, to explain the basic propositional connectives. We will see later that universal and existential quantifiers and types such as natural numbers, lists, or trees naturally fit into the same framework.

We will define the meaning of the usual connectives of propositional logic (conjunction, implication, disjunction) by rules that allow us to infer when they should be true, so-called *introduction rules*. From these, we derive rules for the use of propositions, so-called *elimination rules*. The resulting system of *natural deduction* is the foundation of intuitionistic logic which has direct connections to functional programming and logic programming.

2 Judgments and Propositions

The cornerstone of Martin-Löf's foundation of logic is a clear separation of the notions of judgment and proposition. A *judgment* is something we may know, that is, an object of knowledge. A judgment is *evident* if we in fact know it.

We make a judgment such as "*it is raining*", because we have evidence for it. In everyday life, such evidence is often immediate: we look out the window and see that it is, indeed, raining. In logic, we deal with situations where the evidence is undeniable but indirect: we deduce the judgment by making correct inferences from other evident judgments. In other words: *a logical judgment is evident if we have a proof for it*.

The most important judgment form in logic is "*A is true*", where A is a proposition After all it makes a big difference whether a proposition is just a proposition or whether it is actually true. There are many others that have been studied extensively. For example, "*A is false*", "*A is true at time t*" (from temporal logic), "*A is necessarily true*" (from modal logic), "*program M has type τ*" (from programming languages), etc. or even just "*A is a well-formed proposition*".

Returning to the first judgment, let us try to explain the meaning of conjunction. We write A *true* for the judgment "*A is true*" (presupposing that A is a proposition. Given propositions A and B, we can form the compound proposition "*A and B*", written more formally as $A \wedge B$. But we have not yet specified what conjunction *means*, that is, what counts as a verification of $A \wedge B$. This is accomplished by the following inference rule:

$$\frac{A\ \mathit{true} \quad B\ \mathit{true}}{A \wedge B\ \mathit{true}}\ \wedge I$$

Here the name $\wedge I$ on the rule bar stands for "conjunction introduction", since the conjunction is introduced in the conclusion.

This rule allows us to conclude that $A \wedge B$ *true* if we already know that A *true* and B *true*. In this inference rule, A and B are *schematic variables*, and $\wedge I$ is the name of the rule. Intuitively, the $\wedge I$ rule says that a proof of $A \wedge B$ *true* consists of a proof of A *true* together with a proof of B *true*.

The general form of an inference rule is

$$\frac{J_1\ \dots\ J_n}{J}\ \mathit{name}$$

where the judgments $J_1, \dots, J_n$ are called the *premises*, and the judgment J is called the *conclusion*. In general, we will use letters J to stand for judgments, while A, B, and C are reserved for propositions.

We take conjunction introduction as specifying the meaning of $A \wedge B$ completely. So what can be deduced if we know that $A \wedge B$ is true? By the above rule, to have a verification for $A \wedge B$ means to have verifications for A and B. Hence the following two rules are justified:

$$\frac{A \wedge B\ \mathit{true}}{A\ \mathit{true}}\ \wedge E_1 \qquad\qquad \frac{A \wedge B\ \mathit{true}}{B\ \mathit{true}}\ \wedge E_2$$

The name $\wedge E_1$ stands for "first/left conjunction elimination", since the conjunction in the premise has been eliminated in the conclusion. Similarly $\wedge E_2$ stands for "second/right conjunction elimination". Intuitively, the $\wedge E_1$ rule says that A *true* follows if we have a proof of $A \wedge B$ *true*, because "we must have had a proof of A *true* to justify $A \wedge B$ *true*".

We will later see what precisely is required in order to guarantee that the formation, introduction, and elimination rules for a connective fit together correctly. For now, we will informally argue the correctness of the elimination rules, as we did for the conjunction elimination rules.

As a second example we consider the proposition "*truth*" written as $\top$. Truth should always be true, unconditionally, which means its introduction rule has no premises.

$$\frac{}{\top\ \mathit{true}}\ \top I$$

Consequently, we have no information if we know $\top$ *true*, so there is no elimination rule. "No information comes out of $\top$ *true* if none went in."

A conjunction of two propositions is characterized by one introduction rule with *two* premises, and *two* corresponding elimination rules. We may think of truth as a conjunction of *zero* propositions. By analogy it should then have one introduction rule with *zero* premises, and *zero* corresponding elimination rules. This is precisely what we wrote out above.

3 Hypothetical Judgments

Consider the following derivation, for arbitrary propositions A, B, and C:

$$\cfrac{\cfrac{A \wedge (B \wedge C)\ \mathit{true}}{B \wedge C\ \mathit{true}}\ \wedge E_2}{B\ \mathit{true}}\ \wedge E_1$$

Have we actually proved anything here? At first glance it seems that cannot be the case: B is an arbitrary proposition; clearly we should not be able to prove that it is true. Upon closer inspection we see that all inferences are correct, but the first judgment $A \wedge (B \wedge C)$ *true* has not been justified. We can extract the following knowledge:

From the assumption that $A \wedge (B \wedge C)$ is true, we deduce that B must be true.

This is an example of a *hypothetical judgment*, and the figure above is a *hypothetical deduction* from the assumption $A \wedge (B \wedge C)$ *true*. In general, we may have multiple assumptions, so a hypothetical deduction has the form

$$\begin{array}{c} J_1 \quad \cdots \quad J_n \\ \vdots \\ J \end{array}$$

where the judgments $J_1, \ldots, J_n$ are unproven assumptions, and the judgment J is the conclusion. All instances of the inference rules are hypothetical judgments as well (albeit possibly with 0 assumptions if the inference rule has no premises).

Many mistakes in reasoning arise because dependencies on some hidden assumptions are ignored. When we need to be explicit, we will write $J_1, \ldots, J_n \vdash J$ for the hypothetical judgment which is established by the hypothetical deduction above. We may refer to $J_1, \ldots, J_n$ as the *antecedents* and J as the *succedent* of the hypothetical judgment. For example, the hypothetical judgment $A \wedge (B \wedge C)\ \mathit{true} \vdash B\ \mathit{true}$ is proved by the above hypothetical deduction that $B\ \mathit{true}$ indeed follows from the hypothesis $A \wedge (B \wedge C)\ \mathit{true}$ using inference rules.

Substitution Principle for Hypotheses: We can always substitute a proof for any hypothesis J_i to eliminate the assumption, because the proof justifies J_i (possibly from other assumptions). Into the above hypothetical deduction, a proof of its hypothesis J_i

$$\begin{array}{c} K_1 \quad \cdots \quad K_m \\ \vdots \\ J_i \end{array}$$

can be substituted in for J_i to obtain the hypothetical deduction

$$\begin{array}{ccccc} & & K_1 \quad \cdots \quad K_m & & \\ & & \vdots & & \\ J_1 & \cdots & J_i & \cdots & J_n \\ & & \vdots & & \\ & & J & & \end{array}$$

This hypothetical deduction concludes J from the unproven assumptions $J_1, \ldots, J_{i-1}, K_1, \ldots, K_m, J_{i+1}, \ldots, J_n$ and justifies the hypothetical judgment

$$J_1, \ldots, J_{i-1}, K_1, \ldots, K_m, J_{i+1}, \ldots, J_n \vdash J$$

That is, into the hypothetical judgment $J_1, \ldots, J_n \vdash J$, we can always substitute a derivation of the judgment J_i that was used as a hypothesis to obtain a derivation which no longer depends on the assumption J_i. A hypothetical deduction with 0 assumptions is a *proof* of its conclusion J.

One has to keep in mind that hypotheses may be used more than once, or not at all. For example, for arbitrary propositions A and B,

$$\dfrac{\dfrac{A \wedge B\ \mathit{true}}{B\ \mathit{true}}\ \wedge E_2 \qquad \dfrac{A \wedge B\ \mathit{true}}{A\ \mathit{true}}\ \wedge E_1}{B \wedge A\ \mathit{true}}\ \wedge I$$

can be seen a hypothetical derivation of $A \wedge B\ \mathit{true} \vdash B \wedge A\ \mathit{true}$. Similarly, a minor variation of the first proof in this section is a hypothetical derivation for the hypothetical judgment $A \wedge (B \wedge C)\ \mathit{true} \vdash B \wedge A\ \mathit{true}$ that uses the hypothesis twice.

With hypothetical judgments, we can now explain the meaning of implication "A *implies* B" or "*if* A *then* B" (more formally: $A \supset B$). The introduction rule reads: $A \supset B$ is true, if B is true under the assumption that A is true.

$$\dfrac{\begin{array}{c}\overline{A\ \mathit{true}}\ u \\ \vdots \\ B\ \mathit{true}\end{array}}{A \supset B\ \mathit{true}}\ \supset\! I^u$$

The tricky part of this rule is the label u and its bar. If we omit this annotation, the rule would read

$$\dfrac{\begin{array}{c}A\ \mathit{true} \\ \vdots \\ B\ \mathit{true}\end{array}}{A \supset B\ \mathit{true}}\ \supset\! I$$

which would be *incorrect*: it looks like a derivation of $A \supset B$ *true* from the hypothesis A *true*. But since the assumption A *true* is *introduced* in the process of proving $A \supset B$ *true*; the conclusion $A \supset B$ *true* should not depend on it! Certainly, whether the implication $A \supset B$ is true is independent of the question whether A itself is actually true. Therefore we label uses of the assumption with a *new* name u, and the corresponding inference which introduced this assumption into the derivation with the same label u.

The rule makes intuitive sense, a proof justifying $A \supset B$ *true* assumes, hypothetically, the left-hand side of the implication so assumes A *true*, and uses this to show the right-hand side of the implication by proving B *true*. The proof of $A \supset B$ *true* constructs a proof of B *true* from the additional assumption that A *true*, which may be used in the proof.

As a concrete example, consider the following proof of $A \supset (B \supset (A \wedge B))$.

$$\dfrac{\dfrac{\dfrac{\overline{A\ \mathit{true}}\ u \quad \overline{B\ \mathit{true}}\ w}{A \wedge B\ \mathit{true}}\ \wedge I}{B \supset (A \wedge B)\ \mathit{true}}\ \supset\! I^w}{A \supset (B \supset (A \wedge B))\ \mathit{true}}\ \supset\! I^u$$

This derivation is *not* hypothetical (it does not depend on any assumptions). The assumption A *true* labeled u is *discharged* in the last inference introducing label u, and the assumption B *true* labeled w is discharged in the second-to-last inference introducing label w. It is critical that discharged hypotheses are no longer available for reasoning anywhere else, and that all labels introduced in a derivation are distinct to avoid incorrect arguments with incorrect scoping. Correct scoping of hypothesis labels is just as important as correct scoping of function parameters, a similarity that later lectures will explore.

Finally, we consider what the elimination rule for implication should say. By the only introduction rule, having a proof of $A \supset B$ *true* means that we have a hypothetical proof of B *true* from A *true*. By the substitution principle, if we also have a proof of A *true* then we get a proof of B *true*.

$$\frac{A \supset B \; true \quad A \; true}{B \; true} \supset E$$

This completes the rules concerning implication.

With the rules so far, we can write out proofs of simple properties concerning conjunction and implication. The first expresses the interaction law that conjunction is commutative—intuitively, an obvious property.

$$\dfrac{\dfrac{\dfrac{}{A \wedge B \; true}\,u}{B \; true}\wedge E_2 \quad \dfrac{\dfrac{}{A \wedge B \; true}\,u}{A \; true}\wedge E_1}{\dfrac{B \wedge A \; true}{(A \wedge B) \supset (B \wedge A) \; true}\supset I^u}\wedge I$$

When we construct such a derivation, we generally proceed by a combination of bottom-up and top-down reasoning. The next example is the interaction law of distributivity, allowing us to move implications over conjunctions. This time, we show the partial proofs in each step. Of course, other sequences of steps in proof constructions are also possible.

$$\begin{array}{c} \vdots \\ (A \supset (B \wedge C)) \supset ((A \supset B) \wedge (A \supset C)) \; true \end{array}$$

First, we use the implication introduction rule bottom-up.

$$\dfrac{\begin{array}{c} \dfrac{}{A \supset (B \wedge C) \; true}\,u \\ \vdots \\ (A \supset B) \wedge (A \supset C) \; true \end{array}}{(A \supset (B \wedge C) \supset ((A \supset B) \wedge (A \supset C)) \; true} \supset I^u$$

Next, we use the conjunction introduction rule bottom-up, copying the available assumptions to both branches in the scope.

$$\dfrac{\dfrac{\begin{array}{c} \dfrac{}{A \supset (B \wedge C) \; true}\,u \\ \vdots \\ A \supset B \; true \end{array} \quad \begin{array}{c} \dfrac{}{A \supset (B \wedge C) \; true}\,u \\ \vdots \\ A \supset C \; true \end{array}}{(A \supset B) \wedge (A \supset C) \; true} \wedge I}{(A \supset (B \wedge C)) \supset ((A \supset B) \wedge (A \supset C)) \; true} \supset I^u$$

We now pursue the left branch, again using implication introduction bottom-up.

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{u}
\UnaryInfC{$A \supset (B \wedge C)\ \mathit{true}$}
\AxiomC{}
\RightLabel{w}
\UnaryInfC{$A\ \mathit{true}$}
\noLine
\BinaryInfC{$\vdots$}
\noLine
\UnaryInfC{$B\ \mathit{true}$}
\RightLabel{$\supset\! I^w$}
\UnaryInfC{$A \supset B\ \mathit{true}$}
\AxiomC{}
\RightLabel{u}
\UnaryInfC{$A \supset (B \wedge C)\ \mathit{true}$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$A \supset C\ \mathit{true}$}
\RightLabel{$\wedge I$}
\BinaryInfC{$(A \supset B) \wedge (A \supset C)\ \mathit{true}$}
\RightLabel{$\supset\! I^u$}
\UnaryInfC{$(A \supset (B \wedge C)) \supset ((A \supset B) \wedge (A \supset C))\ \mathit{true}$}
\end{prooftree}
$$

Note that the hypothesis A *true* is available only in the left branch and not in the right one: it is discharged at the inference $\supset\! I^w$. We now switch to top-down reasoning, taking advantage of implication elimination.

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{u}
\UnaryInfC{$A \supset (B \wedge C)\ \mathit{true}$}
\AxiomC{}
\RightLabel{w}
\UnaryInfC{$A\ \mathit{true}$}
\RightLabel{$\supset\! E$}
\BinaryInfC{$B \wedge C\ \mathit{true}$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$B\ \mathit{true}$}
\RightLabel{$\supset\! I^w$}
\UnaryInfC{$A \supset B\ \mathit{true}$}
\AxiomC{}
\RightLabel{u}
\UnaryInfC{$A \supset (B \wedge C)\ \mathit{true}$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$A \supset C\ \mathit{true}$}
\RightLabel{$\wedge I$}
\BinaryInfC{$(A \supset B) \wedge (A \supset C)\ \mathit{true}$}
\RightLabel{$\supset\! I^u$}
\UnaryInfC{$(A \supset (B \wedge C)) \supset ((A \supset B) \wedge (A \supset C))\ \mathit{true}$}
\end{prooftree}
$$

Now we close the gap in the left-hand side by conjunction elimination.

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{u}
\UnaryInfC{$A \supset (B \wedge C)\ \mathit{true}$}
\AxiomC{}
\RightLabel{w}
\UnaryInfC{$A\ \mathit{true}$}
\RightLabel{$\supset\! E$}
\BinaryInfC{$B \wedge C\ \mathit{true}$}
\RightLabel{$\wedge E_1$}
\UnaryInfC{$B\ \mathit{true}$}
\RightLabel{$\supset\! I^w$}
\UnaryInfC{$A \supset B\ \mathit{true}$}
\AxiomC{}
\RightLabel{u}
\UnaryInfC{$A \supset (B \wedge C)\ \mathit{true}$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$A \supset C\ \mathit{true}$}
\RightLabel{$\wedge I$}
\BinaryInfC{$(A \supset B) \wedge (A \supset C)\ \mathit{true}$}
\RightLabel{$\supset\! I^u$}
\UnaryInfC{$(A \supset (B \wedge C)) \supset ((A \supset B) \wedge (A \supset C))\ \mathit{true}$}
\end{prooftree}
$$

The right premise of the conjunction introduction can be filled in analogously. We skip the intermediate steps and only show the final derivation.

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{u}
\UnaryInfC{$A \supset (B \wedge C)\ \mathit{true}$}
\AxiomC{}
\RightLabel{w}
\UnaryInfC{$A\ \mathit{true}$}
\RightLabel{$\supset\! E$}
\BinaryInfC{$B \wedge C\ \mathit{true}$}
\RightLabel{$\wedge E_1$}
\UnaryInfC{$B\ \mathit{true}$}
\RightLabel{$\supset\! I^w$}
\UnaryInfC{$A \supset B\ \mathit{true}$}
\AxiomC{}
\RightLabel{u}
\UnaryInfC{$A \supset (B \wedge C)\ \mathit{true}$}
\AxiomC{}
\RightLabel{v}
\UnaryInfC{$A\ \mathit{true}$}
\RightLabel{$\supset\! E$}
\BinaryInfC{$B \wedge C\ \mathit{true}$}
\RightLabel{$\wedge E_2$}
\UnaryInfC{$C\ \mathit{true}$}
\RightLabel{$\supset\! I^v$}
\UnaryInfC{$A \supset C\ \mathit{true}$}
\RightLabel{$\wedge I$}
\BinaryInfC{$(A \supset B) \wedge (A \supset C)\ \mathit{true}$}
\RightLabel{$\supset\! I^u$}
\UnaryInfC{$(A \supset (B \wedge C)) \supset ((A \supset B) \wedge (A \supset C))\ \mathit{true}$}
\end{prooftree}
$$

Note how important the correct scoping of assumptions is. The assumptions labeled w and v are both assuming the same A *true*. But the assumption labeled w cannot be used in the proof of $A \supset C$ *true*. Otherwise, we could incorrectly prove $(A \supset (B \wedge C)) \supset ((A \supset B) \wedge C)$, which would claim to construct C out of nothing from a mere function turning A into $B \wedge C$.

4 Disjunction and Falsehood

So far we have explained the meaning of conjunction, truth, and implication. The disjunction "A *or* B" (written as $A \vee B$) is more difficult, but does not require any new judgment forms. Disjunction is characterized by two introduction rules: $A \vee B$ is true, if either A is true or B is true.

$$\frac{A\ \mathit{true}}{A \vee B\ \mathit{true}}\ \vee I_1 \qquad\qquad \frac{B\ \mathit{true}}{A \vee B\ \mathit{true}}\ \vee I_2$$

Now it would be incorrect to have an elimination rule such as

$$\frac{A \vee B\ \mathit{true}}{A\ \mathit{true}}\ \vee E_1?$$

because even if we know that $A \vee B$ is true, we do not know whether the disjunct A or the disjunct B is true. Concretely, with such a rule we could unsoundly derive the truth of *every* proposition A as follows:

$$\frac{\dfrac{\dfrac{}{\top\ \mathit{true}}\ \top I}{A \vee \top\ \mathit{true}}\ \vee I_2}{A\ \mathit{true}}\ \vee E_1?$$

Thus we take a different approach. If we know that $A \vee B$ is true, we must consider two cases: A *true* and B *true*. If we can prove a conclusion C *true* in both cases, then C must be true! Written as an inference rule:

$$\frac{A \vee B\ \mathit{true} \qquad \begin{array}{c}\overline{A\ \mathit{true}}\ u \\ \vdots \\ C\ \mathit{true}\end{array} \qquad \begin{array}{c}\overline{B\ \mathit{true}}\ w \\ \vdots \\ C\ \mathit{true}\end{array}}{C\ \mathit{true}}\ \vee E^{u,w}$$

If we know that $A \vee B$ *true* then we also know C *true*, if that follows both in the case where $A \vee B$ *true* because A is true and in the case where $A \vee B$ *true* because B is true. Note that we use once again the mechanism of hypothetical judgments. In the proof of the second premise we may use the assumption A *true* labeled u, in the proof of the third premise we may use the assumption B *true* labeled w. Both are discharged at the disjunction elimination rule. Of course, labels u and w must be new and different.

Let us justify the conclusion of this rule more explicitly. By the first premise we know $A \vee B$ *true*. The premises of the two possible introduction rules are A *true* and B *true*. In case A *true* we conclude C *true* by the substitution principle and the second premise: we substitute the proof of $A\ true$ for any use of the assumption labeled u in the hypothetical derivation. The case for B *true* is symmetric, using the hypothetical derivation in the third premise.

Because of the complex nature of the elimination rule, reasoning with disjunction is more difficult than with implication and conjunction. As a simple example, we prove the commutativity of disjunction.

$$\begin{array}{c} \vdots \\ (A \vee B) \supset (B \vee A)\ \mathit{true} \end{array}$$

We begin with an implication introduction.

$$\dfrac{\begin{array}{c} \overline{A \vee B\ \mathit{true}}^{\;u} \\ \vdots \\ B \vee A\ \mathit{true} \end{array}}{(A \vee B) \supset (B \vee A)\ \mathit{true}} \supset\! I^u$$

At this point we cannot use either of the two disjunction introduction rules. The problem is that neither B nor A follow from our assumption $A \vee B$! So first we need to distinguish the two cases via the rule of disjunction elimination.

$$\dfrac{\dfrac{\overline{A \vee B\ \mathit{true}}^{\;u} \quad \begin{array}{c} \overline{A\ \mathit{true}}^{\;v} \\ \vdots \\ B \vee A\ \mathit{true} \end{array} \quad \begin{array}{c} \overline{B\ \mathit{true}}^{\;w} \\ \vdots \\ B \vee A\ \mathit{true} \end{array}}{B \vee A\ \mathit{true}} \vee E^{v,w}}{(A \vee B) \supset (B \vee A)\ \mathit{true}} \supset\! I^u$$

The assumption labeled u is still available for each of the two proof obligations, but we have omitted it, since it is no longer needed.

Now each gap can be filled in directly by the two disjunction introduction rules.

$$\dfrac{\dfrac{\overline{A \vee B\ \mathit{true}}^{\;u} \quad \dfrac{\overline{A\ \mathit{true}}^{\;v}}{B \vee A\ \mathit{true}} \vee I_2 \quad \dfrac{\overline{B\ \mathit{true}}^{\;w}}{B \vee A\ \mathit{true}} \vee I_1}{B \vee A\ \mathit{true}} \vee E^{v,w}}{(A \vee B) \supset (B \vee A)\ \mathit{true}} \supset\! I^u$$

This concludes the discussion of disjunction. Falsehood (written as $\perp$, sometimes called absurdity or falsum) is a proposition that should have no proof! Therefore there, crucially, are no introduction rules for $\perp$.

Since there cannot be a proof of $\perp$ *true* (it has no introduction rule), it is sound to conclude the truth of any arbitrary proposition C if we know $\perp$ *true*. This justifies the elimination rule

$$\frac{\perp\ \textit{true}}{C\ \textit{true}}\ \perp E$$

We can also think of falsehood as a disjunction between zero alternatives. By analogy with the binary disjunction, we therefore have zero introduction rules, and an elimination rule in which we have to consider zero cases. This is precisely the $\perp E$ rule above.

From this it might seem that falsehood it useless: we can never prove it. This is correct, except that we might reason from contradictory hypotheses! Even if $\perp$ *true* cannot be proved, $\perp \supset \perp$ *true* can be proved. We will see some examples when we discuss negation, since we consider the proposition "*not* A" (written $\neg A$) as an abbreviation for $A \supset \perp$. In other words, $\neg A$ is true precisely if the assumption A *true* is contradictory because we could derive $\perp$ *true*. That is, a proof of the impossible $\perp$ *true* can be constructed from any proof of A *true*.

5 Natural Deduction

The judgments, propositions, and inference rules we have defined so far collectively form a system of *natural deduction*. It is a minor variant of a system introduced by Gentzen [Gen35] and studied in depth by Prawitz [Pra65]. One of Gentzen's main motivations was to devise rules that model mathematical reasoning as directly as possible, although clearly in much more detail than in a typical mathematical argument.

The specific interpretation of the truth judgment underlying these rules is *intuitionistic* or *constructive*. This differs from the *classical* or *Boolean* interpretation of truth. For example, classical logic accepts the proposition $A \vee (A \supset B)$ as true for arbitrary A and B, although in the system we have presented so far this would have no proof. Classical logic is based on the principle that every proposition must be true or false. If we distinguish these cases we see that $A \vee (A \supset B)$ should be accepted, because in case that A is true, the left disjunct holds; in case A is false, the right disjunct holds. In contrast, intuitionistic logic is based on explicit evidence, and evidence for a disjunction requires evidence for one of the disjuncts. We will return to classical logic and its relationship to intuitionistic logic later; for now our reasoning remains intuitionistic since, as we will see, it has a direct connection to functional computation, which classical logic lacks.

We summarize the rules of inference for the truth judgment of intuitionistic propositional logic introduced so far in Figure 1.

6 Notational Definition

So far, we have defined the meaning of the logical connectives by their introduction rules, which is the so-called *verificationist* approach. Another common way to define a logical connective is by a *notational definition*. A notational definition gives the meaning

Introduction Rules **Elimination Rules**

$$\dfrac{A\ \mathit{true} \quad B\ \mathit{true}}{A \wedge B\ \mathit{true}}\ \wedge I \qquad\qquad \dfrac{A \wedge B\ \mathit{true}}{A\ \mathit{true}}\ \wedge E_1 \quad \dfrac{A \wedge B\ \mathit{true}}{B\ \mathit{true}}\ \wedge E_2$$

$$\dfrac{}{\top\ \mathit{true}}\ \top I \qquad\qquad \mathit{no}\ \top E\ \mathit{rule}$$

$$\begin{array}{c} \overline{A\ \mathit{true}}^{\,u} \\ \vdots \\ B\ \mathit{true} \\ \hline A \supset B\ \mathit{true} \end{array}\ \supset I^u \qquad\qquad \dfrac{A \supset B\ \mathit{true} \quad A\ \mathit{true}}{B\ \mathit{true}}\ \supset E$$

$$\dfrac{A\ \mathit{true}}{A \vee B\ \mathit{true}}\ \vee I_1 \quad \dfrac{B\ \mathit{true}}{A \vee B\ \mathit{true}}\ \vee I_2 \qquad \begin{array}{ccc} & \overline{A\ \mathit{true}}^{\,u} & \overline{B\ \mathit{true}}^{\,w} \\ & \vdots & \vdots \\ A \vee B\ \mathit{true} & C\ \mathit{true} & C\ \mathit{true} \\ \hline & C\ \mathit{true} & \end{array}\ \vee E^{u,w}$$

$$\mathit{no}\ \bot I\ \mathit{rule} \qquad\qquad \dfrac{\bot\ \mathit{true}}{C\ \mathit{true}}\ \bot E$$

Figure 1: Rules for intuitionistic natural deduction

of the general form of a proposition in terms of another proposition whose meaning has already been defined. For example, we can define *logical equivalence*, written $A \equiv B$ as $(A \supset B) \wedge (B \supset A)$. This definition is justified, because we already understand implication and conjunction, so can understand $A \equiv B$ by expansion.

As mentioned above, another common notational definition in intuitionistic logic is the definition $\neg A = (A \supset \bot)$. Several other, more direct definitions of intuitionistic negation also exist, and we will see some of them later in the course. Perhaps the most intuitive one is to say that $\neg A$ *true* if A *false*, but this requires the new judgment of falsehood.

Notational definitions can be convenient, but they can be a bit cumbersome at times. We sometimes give a notational definition and then derive introduction and elimination rules for the connective from its notational definition. It should be understood that these rules, even if they may be called introduction or elimination rules, have a different status from those that define a connective. In this particular case, we get the *derived* *rules*:

$$
\cfrac{\cfrac{\overline{A\ \mathit{true}}\ u}{\vdots}\quad}{} \qquad
\frac{\begin{array}{c}\overline{A\ \mathit{true}}^{\,u}\\ \vdots \\ \bot\ \mathit{true}\end{array}}{\neg A\ \mathit{true}}\ \neg I^u
\qquad\qquad
\frac{\neg A\ \mathit{true} \quad A\ \mathit{true}}{\bot\ \mathit{true}}\ \neg E
$$

You should convince yourself that these are indeed derived rules under the notational definition of $\neg A$. They also *almost* have the form of introduction and elimination rules, except that we use $\bot$ to define $\neg A$, while previously we avoided using other connectives besides the one we are defining. When following the strict verificationist program, the use of other connectives or propositions that are not part of the original propositions should be frowned upon in introduction rules. The underlying reason is that this might ruin the entire verificationist program of understanding propositions in terms of how they can be verified. If the introduction rule of one operator is defined in terms of another operator, whose introduction rule is again defined in terms of the first operator, then this mutual recursion has not given meaning to either operator. Just imagine how much you learn about roses if you were to take "A rose is a rose is a rose" as their definition.

References

[Dum91] Michael Dummett. *The Logical Basis of Metaphysics*. Harvard University Press, Cambridge, Massachusetts, 1991. The William James Lectures, 1976.

[Gen35] Gerhard Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210, 405–431, 1935. English translation in M. E. Szabo, editor, *The Collected Papers of Gerhard Gentzen*, pages 68–131, North-Holland, 1969.

[ML96] Per Martin-Löf. On the meanings of the logical constants and the justifications of the logical laws. *Nordic Journal of Philosophical Logic*, 1(1):11–60, 1996. Notes for three lectures given in Siena, April 1983. URL: `http://www.hf.uio.no/ifikk/forskning/publikasjoner/tidsskrifter/njpl/vol1no1/meaning.pdf`.

[Pra65] Dag Prawitz. *Natural Deduction*. Almquist & Wiksell, Stockholm, 1965.