Chapter 1

Propositional Logic

The goal of this chapter is to develop the two principal notions of logic, namely propositions and proofs. There is no universal agreement about the proper foundations for these notions. The approach of constructive logic, which has been particularly successful for applications in computer science, is to understand the meaning of a proposition by understanding its proofs. This is an application to logic of the so-called *Principle of Verification*, first proposed by the philosopher L. Wittgenstein, and pursued by the philosophers of the Vienna Circle, including R. Carnap. According to this principle, the meaning of a proposition is determined by its method of verification. Indeed, inthe words of Martin-Löf [ML96, Page 27]:

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

In this chapter we apply this approach 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.

1.1 Judgments and Propositions

The cornerstone of Martin-Löf's constructive 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 may look out the window and see that it is raining. In logic, we are concerned with situation where the evidence is indirect: we deduce the judgment by making correct inferences from other evident judgments. In other words: a 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. In order to reason correctly, we therefore need a second judgment form "*A is a proposition*". But 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.

Returning to the first two judgments, let us try to explain the meaning of conjunction. We write *A prop* for the judgment "*A is a proposition*" and *A true* for the judgment "*A is true*" (presupposing that *A prop*). Given propositions A and B, we want to form the compound proposition "*A and B*", written more formally as $A \wedge B$. We express this in the following inference rule:

$$\frac{A\ \mathit{prop} \qquad B\ \mathit{prop}}{A \wedge B\ \mathit{prop}}\ \wedge F$$

This rule allows us to conclude that $A \wedge B$ *prop* if we already know that *A prop* and *B prop*. In this inference rule, A and B are *schematic variables*, and $\wedge F$ is the name of the rule (which is short for "conjunction formation"). The general form of an inference rule is

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

where the judgments $J_1, \ldots, J_n$ are called the *premises*, 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.

Once the rule of conjunction formation ($\wedge F$) has been specified, we know that $A \wedge B$ is a proposition, if A and B are. But we have not yet specified what it *means*, that is, what counts as a verification of $A \wedge B$. This is accomplished by the following inference rule:

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

Here the name $\wedge I$ stands for "conjunction introduction", since the conjunction is introduced in the conclusion. We take this as specifying the meaning of $A \wedge B$ completely. So what can be deduce 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:

$$\frac{A \wedge B\ \mathit{true}}{A\ \mathit{true}}\ \wedge E_L \qquad\qquad \frac{A \wedge B\ \mathit{true}}{B\ \mathit{true}}\ \wedge E_R$$

The name $\wedge E_L$ stands for "left conjunction elimination", since the conjunction in the premise has been eliminated in the conclusion. Similarly $\wedge E_R$ stands for "right conjunction elimination".

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 a second example we consider the proposition "*truth*" written as $\top$.

$$\frac{}{\top\ \mathit{prop}}\,\top F$$

Truth should always be true, 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.

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.

1.2 Hypothetical Judgments

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

$$\dfrac{\dfrac{A \wedge (B \wedge C)\ \mathit{true}}{B \wedge C\ \mathit{true}}\,\wedge E_R}{B\ \mathit{true}}\,\wedge E_L$$

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 $A \wedge (B \wedge C)$ 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 an *hypothetical derivation*. In general, we may have more than one assumption, so a hypothetical derivation 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. Note that we can always substitute a proof for any hypothesis J_i to eliminate the assumption. We call this the *substitution principle* for hypotheses.

Many mistakes in reasoning arise because dependencies on some hidden assumptions are ignored. When we need to be explicit, we write $J_1, \ldots, J_n \vdash J$ for the hypothetical judgment which is established by the hypothetical derivation above. We may refer to $J_1, \ldots, J_n$ as the antecedents and J as the succedent of the hypothetical judgment.

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,

$$\dfrac{\dfrac{A \wedge B\ \mathit{true}}{B\ \mathit{true}}\wedge E_R \qquad \dfrac{A \wedge B\ \mathit{true}}{A\ \mathit{true}}\wedge E_L}{B \wedge A\ \mathit{true}}\wedge I$$

can be seen a hypothetical derivation of $A \wedge B\ \mathit{true} \vdash B \wedge A\ \mathit{true}$.

With hypothetical judgments, we can now explain the meaning of implication "*A implies B*" or "*if A then B*" (more formally: $A \supset B$). First the formation rule:

$$\dfrac{A\ \mathit{prop} \qquad B\ \mathit{prop}}{A \supset B\ \mathit{prop}}\supset F$$

Next, the introduction rule: $A \supset B$ is true, if B is true under the assumption that A is true.

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

The tricky part of this rule is the label u. 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 $A \supset B\ \mathit{true}$ from the hypothesis $A\ \mathit{true}$. But the assumption $A\ \mathit{true}$ is introduced in the process of proving $A \supset B\ \mathit{true}$; the conclusion should not depend on it! 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.

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

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A\ true}\,u \qquad \dfrac{}{B\ true}\,w}{A \wedge B\ true}\wedge I}{B \supset (A \wedge B)\ true}\supset I^{w}}{A \supset (B \supset (A \wedge B))\ true}\supset I^{u}$$

Note that this derivation is not hypothetical (it does not depend on any assumptions). The assumption $A\ true$ labeled u is discharged in the last inference, and the assumption $B\ true$ labeled w is discharged in the second-to-last inference. It is critical that a discharged hypothesis is no longer available for reasoning, and that all labels introduced in a derivation are distinct.

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 $B\ true$.

$$\dfrac{A \supset B\ true \qquad A\ true}{B\ true}\supset E$$

This completes the rule concerning implication.

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

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \wedge B\ true}\,u}{B\ true}\wedge E_R \qquad \dfrac{\dfrac{}{A \wedge B\ true}\,u}{A\ true}\wedge E_L}{B \wedge A\ true}\wedge I}{(A \wedge B) \supset (B \wedge A)\ true}\supset I^{u}$$

When we construct such a derivation, we generally proceed by a combination of bottom-up and top-down reasoning. The next example is a distributivity law, 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.

$$\dfrac{\vdots}{(A \supset (B \wedge C)) \supset ((A \supset B) \wedge (A \supset C))\ true}$$

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

$$\dfrac{\dfrac{}{A \supset (B \wedge C)\ \mathit{true}}\,u \\ \vdots \\ (A \supset B) \wedge (A \supset C)\ \mathit{true}}{(A \supset (B \wedge C)) \supset ((A \supset B) \wedge (A \supset C))\ \mathit{true}}\,\supset I^u$$

Next, we use the conjunction introduction rule bottom-up.

$$\dfrac{\dfrac{\dfrac{}{A \supset (B \wedge C)\ \mathit{true}}\,u \\ \vdots \\ A \supset B\ \mathit{true}}{\dfrac{}{(A \supset B) \wedge (A \supset C)\ \mathit{true}}\,\wedge I} \qquad \dfrac{\dfrac{}{A \supset (B \wedge C)\ \mathit{true}}\,u \\ \vdots \\ A \supset C\ \mathit{true}}{(A \supset (B \wedge C)) \supset ((A \supset B) \wedge (A \supset C))\ \mathit{true}}\,\supset I^u$$

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

$$\dfrac{\dfrac{\dfrac{}{A \supset (B \wedge C)\ \mathit{true}}\,u \\ \vdots \\ B\ \mathit{true}}{A \supset B\ \mathit{true}}\,\supset I^w \qquad \dfrac{\dfrac{}{A \supset (B \wedge C)\ \mathit{true}}\,u \\ \vdots \\ A \supset C\ \mathit{true}}{(A \supset B) \wedge (A \supset C)\ \mathit{true}}\,\wedge I}{(A \supset (B \wedge C)) \supset ((A \supset B) \wedge (A \supset C))\ \mathit{true}}\,\supset I^u$$

Note that the hypothesis $A\ \mathit{true}$ is available only in the left branch, but 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.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \supset (B \wedge C)\ \mathit{true}}\,u \qquad \dfrac{}{A\ \mathit{true}}\,w}{B \wedge C\ \mathit{true}}\,\supset E \\ \vdots \\ B\ \mathit{true}}{A \supset B\ \mathit{true}}\,\supset I^w \qquad \dfrac{\dfrac{}{A \supset (B \wedge C)\ \mathit{true}}\,u \\ \vdots \\ A \supset C\ \mathit{true}}{(A \supset B) \wedge (A \supset C)\ \mathit{true}}\,\wedge I}{(A \supset (B \wedge C)) \supset ((A \supset B) \wedge (A \supset C))\ \mathit{true}}\,\supset I^u$$

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

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

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

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \supset (B \wedge C)\ true}\,u \quad \dfrac{}{A\ true}\,w}{B \wedge C\ true}\supset E}{B\ true}\wedge E_L}{A \supset B\ true}\supset I^w \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{A \supset (B \wedge C)\ true}\,u \quad \dfrac{}{A\ true}\,v}{B \wedge C\ true}\supset E}{C\ true}\wedge E_R}{A \supset C\ true}\supset I^v}{(A \supset B) \wedge (A \supset C)\ true}\wedge I$$
$$\dfrac{(A \supset B) \wedge (A \supset C)\ true}{(A \supset (B \wedge C)) \supset ((A \supset B) \wedge (A \supset C))\ true}\supset I^u$$

1.3 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.

$$\dfrac{A\ prop \qquad B\ prop}{A \vee B\ prop}\vee F$$

Disjunction is characterized by two introduction rules: $A \vee B$ is true, if either A or B is true.

$$\dfrac{A\ true}{A \vee B\ true}\vee I_L \qquad\qquad \dfrac{B\ true}{A \vee B\ true}\vee I_R$$

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

$$\dfrac{A \vee B\ true}{A\ true}\vee E_L?$$

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 derive the

truth of *every* proposition A as follows:

$$\dfrac{\dfrac{\dfrac{}{B\ true}\,u}{B \supset B\ true}\,\supset I^u \qquad \dfrac{\dfrac{\dfrac{}{B \supset B\ true}\,w}{A \vee (B \supset B)\ true}\,\vee I_R}{A\ true}\,\vee E_L?}{A\ true}\,\supset I^w \quad \supset E$$

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:

$$\dfrac{\begin{array}{ccc} & \dfrac{}{A\ true}\,u & \dfrac{}{B\ true}\,w \\ & \vdots & \vdots \\ A \vee B\ true & C\ true & C\ true \end{array}}{C\ true}\,\vee E^{u,w}$$

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.

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.

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

We begin with an implication introduction.

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

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.

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

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.

$$\dfrac{\dfrac{}{A \vee B\ true}\,u \qquad \dfrac{\dfrac{}{A\ true}\,v}{B \vee A\ true}\,\vee I_R \qquad \dfrac{\dfrac{}{B\ true}\,w}{B \vee A\ true}\,\vee I_L}{\dfrac{B \vee A\ true}{(A \vee B) \supset (B \vee A)\ true}\,\supset I^u}\,\vee E^{v,w}$$

This concludes the discussion of disjunction. Falsehood (written as $\bot$, sometimes called absurdity) is a proposition that should have no proof! Therefore there are no introduction rules, although we of course have the standard formation rule.

$$\dfrac{}{\bot\ prop}\,\bot F$$

Since there cannot be a proof of $\bot\ true$, it is sound to conclude the truth of any arbitrary proposition if we know $\bot\ true$. This justifies the elimination rule

$$\dfrac{\bot\ true}{C\ true}\,\bot E$$

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 $\bot E$ rule above.

From this is might seem that falsehood it useless: we can never prove it. This is correct, except that we might reason from contradictory hypotheses! We will see some examples when we discuss negation, since we may think of the proposition "*not* A" (written $\neg A$) as $A \supset \bot$. In other words, $\neg A$ is true precisely if the assumption $A\ true$ is contradictory because we could derive $\bot\ true$.