Chapter 2

Natural Deduction

> Ich wollte zunächst einmal einen Formalismus aufstellen, der dem wirklichen Schließen möglichst nahe kommt. So ergab sich ein „Kalkül des natürlichen Schließens“.[1]
>
> — Gerhard Gentzen
> *Untersuchungen über das logische Schließen* [Gen35]

In this chapter we explore ways to define logics, or, which comes to the same thing, ways to give meaning to logical connectives. Our fundamental notion is that of a *judgment* based on *evidence*. For example, we might make the judgment "*It is raining*" based on visual evidence. Or we might make the judgment "'*A implies A' is true for any proposition A*" based on a derivation. The use of the notion of a judgment as conceptual prior to the notion of proposition has been advocated by Martin-Löf [ML85a, ML85b]. Certain forms of judgments frequently recur and have therefore been investigated in their own right, prior to logical considerations. Two that we will use are *hypothetical judgments* and *parametric jugments* (the latter are sometimes called *general judgments* or *schematic judgments*).

A hypothetical judgment has the form "J_2 *under hypothesis* J_1". We consider this judgment evident if we are prepared to make the judgment J_2 once provided with evidence for J_1. Formal evidence for a hypothetical judgment is a *hypothetical derivation* where we can freely use the hypothesis J_1 in the derivation of J_2. Note that hypotheses need not be used, and could be used more than once.

A parametric judgment has the form "J *for any* a" where a is a *parameter* which may occur in J. We make this judgment if we are prepared to make the judgment $[O/a]J$ for arbitrary objects O of the right category. Here $[O/a]J$ is our notation for substituting the object O for parameter a in the judgment J. Formal evidence for a parametric judgment J is a *parametric derivation* with free occurrences of the parameter a.

[1] First I wanted to construct a formalism which comes as close as possible to actual reasoning. Thus arose a "calculus of natural deduction".

Formal evidence for a judgment in form of a derivation is usually written in two-dimensional notation:

$$\begin{array}{c} \mathcal{D} \\ J \end{array}$$

if $\mathcal{D}$ is a derivation of J. For the sake of brevity we sometimes use the alternative notation $\mathcal{D} :: J$. A hypothetical judgment is written as

$$\begin{array}{c} \overline{J_1}\,u \\ \vdots \\ J_2 \end{array}$$

where u is a label which identifies the hypothesis J_1. We use the labels to guarantee that hypotheses which are introduced during the reasoning process are not used outside their scope.

The separation of the notion of judgment and proposition and the corresponding separation of the notion of evidence and proof sheds new light on various styles that have been used to define logical systems.

An axiomatization in the style of Hilbert [Hil22], for example, arises when one defines a judgment "*A is true*" without the use of hypothetical judgments. Such a definition is highly economical in its use of judgments, which has to be compensated by a liberal use of implication in the axioms. When we make proof structure explicit in such an axiomatization, we arrive at combinatory logic [Cur30].

A categorical logic [LS86] arises (at least in the propositional case) when the basic judgment is not truth, but entailment "*A entails B*". Once again, presentations are highly economical and do not need to seek recourse in complex judgment forms (at least for the propositional fragment). But derivations often require many hypotheses, which means that we need to lean rather heavily on conjunction here. Proofs are realized by morphisms which are an integral part of the machinery of category theory.

While these are interesting and in many ways useful approaches to logic specification, neither of them comes particularly close to capturing the practice of mathematical reasoning. This was Gentzen's point of departure for the design of a system of *natural deduction* [Gen35]. From our point of view, this system is based on the simple judgment "*A is true*", but relies critically on hypothetical and parametric judgments. In addition to being extremely elegant, it has the great advantage that one can define all logical connectives without reference to any other connective. This principle of modularity extends to the meta-theoretic study of natural deduction and simplifies considering fragments and extension of logics. Since we will consider many fragments and extension, this *orthogonality* of the logical connectives is a critical consideration. There is another advantage to natural deduction, namely that its proofs are isomorphic to the terms in a λ-calculus via the so-called Curry-Howard isomorphism [How69], which establishes many connections to functional programming.

Finally, we arrive at the *sequent calculus* (also introduced by Gentzen in his seminal paper [Gen35]) when we split the single judgment of truth into two: "*A is an assumption*" and "*A is true*". While we still employ the machinery of parametric and hypothetical judgments, we now need an explicit rule to state that "*A is an assumption*" is sufficient evidence for "*A is a true*". The reverse, namely that if "*A is true*" then "*A may be used as an assumption*" is the Cut rule which he proved to be redundant in his *Hauptsatz*. For Gentzen the sequent calculus was primarily a technical device to prove consistency of his system of natural deduction, but it exposes many details of the fine structure of proofs in such a clear manner that many logic presentations employ sequent calculi. The laws governing the structure of proofs, however, are more complicated than the Curry-Howard isomorphism for natural deduction might suggest and are still the subject of study [Her95, Pfe95].

We choose natural deduction as our definitional formalism as the purest and most widely applicable. Later we justify the sequent calculus as a calculus of proof search for natural deduction and explicitly relate the two forms of presentation.

We begin by introducing natural deduction for intuitionistic logic, exhibiting its basic principles.

2.1 Intuitionistic Natural Deduction

The system of natural deduction we describe below is basically Gentzen's system NJ [Gen35] or the system which may be found in Prawitz [Pra65]. The calculus of natural deduction was devised by Gentzen in the 1930's out of a dissatisfaction with axiomatic systems in the Hilbert tradition, which did not seem to capture mathematical reasoning practices very directly. Instead of a number of axioms and a small set of inference rules, valid deductions are described through inference rules only, which at the same time explain the meaning of the logical quantifiers and connectives in terms of their proof rules.

A language of (first-order) *terms* is built up from *variables* x, y, *etc.*, *function symbols* f, g, *etc.*, each with a unique arity, and *parameters* a, b, *etc.* in the usual way.

$$\textit{Terms} \quad t \quad ::= \quad x \mid a \mid f(t_1, \ldots, t_n)$$

A constant c is simply a function symbol with arity 0 and we write c instead of $c()$. Exactly which function symbols are available is left unspecified in the general development of predicate logic and only made concrete for specific theories, such as the theory of natural numbers. However, variables and parameters are always available. We will use t and s to range over terms.

The language of *propositions* is built up from *predicate symbols* P, Q, *etc.* and terms in the usual way.

$$\begin{array}{lcl} \textit{Propositions} \quad A & ::= & P(t_1, \ldots, t_n) \mid A_1 \wedge A_2 \mid A_1 \supset A_2 \mid A_1 \vee A_2 \mid \neg A \\ & & \mid \bot \mid \top \mid \forall x.\ A \mid \exists x.\ A \end{array}$$

A propositional constant P is simply a predicate symbol with no arguments and we write P instead of $P()$. We will use A, B, and C to range over propositions. Exactly which predicate symbols are available is left unspecified in the general development of predicate logic and only made concrete for specific theories.

The notions of *free* and *bound* variables in terms and propositions are defined in the usual way: the variable x is bound in propositions of the form $\forall x.\ A$ and $\exists x.\ A$. We use parentheses to disambiguate and assume that $\wedge$ and $\vee$ bind more tightly than $\supset$. It is convenient to assume that propositions have no free individual variables; we use parameters instead where necessary. Our notation for substitution is $[t/x]A$ for the result of substituting the term t for the variable x in A. Because of the restriction on occurrences of free variables, we can assume that t is free of individual variables, and thus capturing cannot occur.

The main judgment of natural deduction is "C *is true*" written as C *true*, from hypotheses A_1 *true*$, \ldots,$ A_n *true*. We will model this as a hypothetical judgment. This means that certain structural properties of derivations are tacitly assumed, independently of any logical inferences. In essence, these assumptions explain what hypothetical judgments are.

Hypothesis. If we have a hypothesis A *true* than we can conclude A *true*.

Weakening. Hypotheses need not be used.

Duplication. Hypotheses can be used more than once.

Exchange. The order in which hypotheses are introduced is irrelevant.

In natural deduction each logical connective and quantifier is characterized by its *introduction rule(s)* which specifies how to infer that a conjunction, disjunction, *etc.* is true. The *elimination rule* for the logical constant tells what other truths we can deduce from the truth of a conjunction, disjunction, *etc.* Introduction and elimination rules must match in a certain way in order to guarantee that the rules are meaningful and the overall system can be seen as capturing mathematical reasoning.

The first is a *local soundness* property: if we introduce a connective and then immediately eliminate it, we should be able to erase this detour and find a more direct derivation of the conclusion without using the connective. If this property fails, the elimination rules are too strong: they allow us to conclude more than we should be able to know.

The second is a *local completeness* property: we can eliminate a connective in a way which retains sufficient information to reconstitute it by an introduction rule. If this property fails, the elimination rules are too weak: they do not allow us to conclude everything we should be able to know.

We provide evidence for local soundness and completeness of the rules by means of *local reduction* and *expansion* judgments, which relate proofs of the same proposition.

One of the important principles of natural deduction is that each connective should be defined only in terms of inference rules without reference to other logical connectives or quantifiers. We refer to this as *orthogonality* of the connectives. It means that we can understand a logical system as a whole by understanding each connective separately. It also allows us to consider fragments and extensions directly and it means that the investigation of properties of a logical system can be conducted in a modular way.

We now show the introduction and elimination rules, local reductions and expansion for each of the logical connectives in turn. The rules are summarized on page 2.1.

Conjunction. $A \wedge B$ should be true if both A and B are true. Thus we have the following introduction rule.

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

If we consider this as a complete definition, we should be able to recover both A and B if we know $A \wedge B$. We are thus led to two elimination rules.

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

To check our intuition we consider a deduction which ends in an introduction followed by an elimination:

$$\frac{\dfrac{\begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array} \qquad \begin{array}{c}\mathcal{E}\\ B\ \mathit{true}\end{array}}{A \wedge B\ \mathit{true}}\wedge\mathrm{I}}{A\ \mathit{true}}\wedge\mathrm{E_L}$$

Clearly, it is unnecessary to first introduce the conjunction and then eliminate it: a more direct proof of the same conclusion from the same (or fewer) assumptions would be simply

$$\begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array}$$

Formulated as a transformation or *reduction* between derivations we have

$$\frac{\dfrac{\begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array} \qquad \begin{array}{c}\mathcal{E}\\ B\ \mathit{true}\end{array}}{A \wedge B\ \mathit{true}}\wedge\mathrm{I}}{A\ \mathit{true}}\wedge\mathrm{E_L} \quad \Longrightarrow_R \quad \begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array}$$

and symmetrically

$$\frac{\dfrac{\begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array} \qquad \begin{array}{c}\mathcal{E}\\ B\ \mathit{true}\end{array}}{A \wedge B\ \mathit{true}}\wedge\mathrm{I}}{B\ \mathit{true}}\wedge\mathrm{E_R} \quad \Longrightarrow_R \quad \begin{array}{c}\mathcal{E}\\ B\ \mathit{true}\end{array}$$

The new judgment

$$\begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array} \Longrightarrow_R \begin{array}{c}\mathcal{E}\\ A\ \mathit{true}\end{array}$$

relates derivations with the same conclusion. We say $\mathcal{D}$ *locally reduces to* $\mathcal{E}$. Since local reductions are possible for both elimination rules for conjunction, our rules are locally sound. To show that the rules are locally complete we show how to reintroduce a conjunction from its components in the form of a local expansion.

$$\begin{array}{c}\mathcal{D}\\ A \wedge B\ \mathit{true}\end{array} \Longrightarrow_E \dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ A \wedge B\ \mathit{true}\end{array}}{A\ \mathit{true}}\wedge\mathrm{E_L} \qquad \dfrac{\begin{array}{c}\mathcal{D}\\ A \wedge B\ \mathit{true}\end{array}}{B\ \mathit{true}}\wedge\mathrm{E_R}}{A \wedge B\ \mathit{true}}\wedge\mathrm{I}$$

Implication. To derive $A \supset B$ *true* we assume A *true* and then derive B *true*. Written as a hypothetical judgment:

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

We must be careful that the hypothesis A *true* is available only in the derivation above the premiss. We therefore label the inference with the name of the hypothesis u, which must not be used already as the name for a hypothesis in the derivation of the premiss. We say that the hypothesis A *true* labelled u is *discharged* at the inference labelled $\supset\mathrm{I}^u$. A derivation of $A \supset B$ *true* describes a construction by which we can transform a derivation of A *true* into a derivation of B *true*: we substitute the derivation of A *true* wherever we used the assumption A *true* in the hypothetical derivation of B *true*. The elimination rule expresses this: if we have a derivation of $A \supset B$ *true* and also a derivation of A *true*, then we can obtain a derivation of B *true*.

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

The local reduction rule carries out the substitution of derivations explained above.

$$\dfrac{\dfrac{\begin{array}{c}\overline{A\ \mathit{true}}\,u\\ \mathcal{D}\\ B\ \mathit{true}\end{array}}{A \supset B\ \mathit{true}}\supset\mathrm{I}^u \qquad \begin{array}{c}\mathcal{E}\\ A\ \mathit{true}\end{array}}{B\ \mathit{true}}\supset\mathrm{E} \Longrightarrow_R \begin{array}{c}\dfrac{\mathcal{E}}{A\ \mathit{true}}\,u\\ \mathcal{D}\\ B\ \mathit{true}\end{array}$$

The final derivation depends on all the hypotheses of $\mathcal{E}$ and $\mathcal{D}$ except u, for which we have substituted $\mathcal{E}$. An alternative notation for this substitution of derivations for hypotheses is $[\mathcal{E}/u]\mathcal{D} :: B\ \mathit{true}$. The local reduction described above may significantly increase the overall size of the derivation, since the deduction $\mathcal{E}$ is substituted for each occurrence of the assumption labeled u in $\mathcal{D}$ and may thus be replicated many times. The local expansion simply rebuilds the implication.

$$\begin{array}{c}\mathcal{D}\\ A \supset B\ \mathit{true}\end{array} \quad \Longrightarrow_E \quad \dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ A \supset B\ \mathit{true}\end{array} \qquad \dfrac{}{A\ \mathit{true}}u}{B\ \mathit{true}}\supset\!E}{A \supset B\ \mathit{true}}\supset\!I^u$$

Disjunction. $A \vee B$ should be true if either A is true or B is true. Therefore we have two introduction rules.

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

If we have a hypothesis $A \vee B\ \mathit{true}$, we do not know how it might be inferred. That is, a proposed elimination rule

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

would be incorrect, since a deduction of the form

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{E}\\ B\ \mathit{true}\end{array}}{A \vee B\ \mathit{true}}\vee I_R}{A\ \mathit{true}}?$$

cannot be reduced. As a consequence, the system would be *inconsistent*: if we have at least one theorem (B, in the example) we can prove every formula (A, in the example). How do we use the assumption $A \vee B$ in informal reasoning? We often proceed with a proof by cases: we prove a conclusion C under the assumption A and also show C under the assumption B. We then conclude C, since either A or B by assumption. Thus the elimination rule employs two hypothetical judgments.

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

Now one can see that the introduction and elimination rules match up in two reductions. First, the case that the disjunction was inferred by $\vee\mathrm{I_L}$.

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ A\ \mathit{true}\end{array}}{A \vee B\ \mathit{true}}\vee\mathrm{I_L} \quad \begin{array}{c}\overline{A\ \mathit{true}}^{\,u}\\ \mathcal{E}_1\\ C\ \mathit{true}\end{array} \quad \begin{array}{c}\overline{B\ \mathit{true}}^{\,w}\\ \mathcal{E}_2\\ C\ \mathit{true}\end{array}}{C\ \mathit{true}}\vee\mathrm{E}^{u,w} \quad \Longrightarrow_R \quad \begin{array}{c}\dfrac{\mathcal{D}}{A\ \mathit{true}}u\\ \mathcal{E}_1\\ C\ \mathit{true}\end{array}$$

The other reduction is symmetric.

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ B\ \mathit{true}\end{array}}{A \vee B\ \mathit{true}}\vee\mathrm{I_R} \quad \begin{array}{c}\overline{A\ \mathit{true}}^{\,u}\\ \mathcal{E}_1\\ C\ \mathit{true}\end{array} \quad \begin{array}{c}\overline{B\ \mathit{true}}^{\,w}\\ \mathcal{E}_2\\ C\ \mathit{true}\end{array}}{C\ \mathit{true}}\vee\mathrm{E}^{u,w} \quad \Longrightarrow_R \quad \begin{array}{c}\dfrac{\mathcal{D}}{B\ \mathit{true}}w\\ \mathcal{E}_2\\ C\ \mathit{true}\end{array}$$

As in the reduction for implication, the resulting derivation may be longer than the original one. The local expansion is more complicated than for the previous connectives, since we first have to distinguish cases and then reintroduce the disjunction in each branch.

$$\begin{array}{c}\mathcal{D}\\ A \vee B\ \mathit{true}\end{array} \quad \Longrightarrow_E \quad \dfrac{\begin{array}{c}\mathcal{D}\\ A \vee B\ \mathit{true}\end{array} \quad \dfrac{\overline{A\ \mathit{true}}^{\,u}}{A \vee B\ \mathit{true}}\vee\mathrm{I_L} \quad \dfrac{\overline{B\ \mathit{true}}^{\,w}}{A \vee B\ \mathit{true}}\vee\mathrm{I_R}}{A \vee B\ \mathit{true}}\vee\mathrm{E}^{u,w}$$

Negation. In order to derive $\neg A$ we assume A and try to derive a contradiction. Thus it seems that negation requires falsehood, and, indeed, in most literature on constructive logic, $\neg A$ is seen as an abbreviation of $A \supset \bot$. In order to give a self-contained explanation of negation by an introduction rule, we employ a judgment that is parametric in a propositional parameter p: If we can derive *any* p from the hypothesis A we conclude $\neg A$.

$$\dfrac{\begin{array}{c}\overline{A\ \mathit{true}}^{\,u}\\ \vdots\\ p\ \mathit{true}\end{array}}{\neg A\ \mathit{true}}\neg\mathrm{I}^{p,u} \qquad \dfrac{\neg A\ \mathit{true} \quad A\ \mathit{true}}{C\ \mathit{true}}\neg\mathrm{E}$$

The elimination rule follows from this view: if we know $\neg A$ *true* and A *true* then we can conclude any formula C is true. In the form of a local reduction:

$$\dfrac{\dfrac{\begin{matrix}\overline{A\ \mathit{true}}\,u\\ \mathcal{D}\\ p\ \mathit{true}\end{matrix}}{\neg A\ \mathit{true}}\,\neg\mathrm{I}^{p,u} \qquad \begin{matrix}\mathcal{E}\\ A\ \mathit{true}\end{matrix}}{C\ \mathit{true}}\,\neg\mathrm{E} \quad \Longrightarrow_R \quad \begin{matrix}\dfrac{\mathcal{E}}{A\ \mathit{true}}\,u\\ {[C/p]\mathcal{D}}\\ C\ \mathit{true}\end{matrix}$$

The substitution $[C/p]\mathcal{D}$ is valid, since $\mathcal{D}$ is parametric in p. The local expansion is similar to the case for implication.

$$\begin{matrix}\mathcal{D}\\ \neg A\ \mathit{true}\end{matrix} \quad \Longrightarrow_E \quad \dfrac{\dfrac{\begin{matrix}\mathcal{D}\\ \neg A\ \mathit{true}\end{matrix} \qquad \overline{A\ \mathit{true}}\,u}{p\ \mathit{true}}\,\neg\mathrm{E}}{\neg\ \mathit{true}A}\,\neg\mathrm{I}^{p,u}$$

Truth. There is only an introduction rule for $\top$:

$$\overline{\top\ \mathit{true}}\,\top\mathrm{I}$$

Since we put no information into the proof of $\top$, we know nothing new if we have an assumption $\top$ and therefore we have no elimination rule and no local reduction. It may also be helpful to think of $\top$ as a 0-ary conjunction: the introduction rule has 0 premisses instead of 2 and we correspondingly have 0 elimination rules instead of 2. The local expansion allows the replacement of any derivation of $\top$ by $\top$I.

$$\begin{matrix}\mathcal{D}\\ \top\ \mathit{true}\end{matrix} \quad \Longrightarrow_E \quad \overline{\top\ \mathit{true}}\,\top\mathrm{I}$$

Falsehood. Since we should not be able to derive falsehood, there is no introduction rule for $\bot$. Therefore, if we can derive falsehood, we can derive everything.

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

Note that there is no local reduction rule for $\bot$E. It may be helpful to think of $\bot$ as a 0-ary disjunction: we have 0 instead of 2 introduction rules and we correspondingly have to consider 0 cases instead of 2 in the elimination rule. Even though we postulated that falsehood should not be derivable, falsehood could clearly be a consequence of contradictory assumption. For example, $A \wedge$

$\neg A \supset \bot$ *true* is derivable. While there is no local reduction rule, there still is a local expansion in analogy to the case for disjunction.

$$\begin{array}{c} \mathcal{D} \\ \bot\ \mathit{true} \end{array} \quad \Longrightarrow_E \quad \dfrac{\begin{array}{c} \mathcal{D} \\ \bot\ \mathit{true} \end{array}}{\bot\ \mathit{true}}\,\bot\mathrm{E}$$

Universal Quantification. Under which circumstances should $\forall x.\ A$ be true? This clearly depends on the domain of quantification. For example, if we know that x ranges over the natural numbers, then we can conclude $\forall x.\ A$ if we can prove $[0/x]A$, $[1/x]A$, *etc.* Such a rule is not effective, since it has infinitely many premisses. Thus one usually retreats to rules such as induction. However, in a general treatment of predicate logic we would like to prove statements which are true for *all* domains of quantification. Thus we can only say that $\forall x.\ A$ should be provable if $[a/x]A$ is provable for a new parameter a about which we can make no assumption. Conversely, if we know $\forall x.\ A$, we know that $[t/x]A$ for any term t.

$$\dfrac{[a/x]A\ \mathit{true}}{\forall x.\ A\ \mathit{true}}\,\forall\mathrm{I}^a \qquad\qquad \dfrac{\forall x.\ A\ \mathit{true}}{[t/x]A\ \mathit{true}}\,\forall\mathrm{E}$$

The label a on the introduction rule is a reminder the parameter a must be "new", that is, it may not occur in any undischarged assumption in the proof of $[a/x]A$ or in $\forall x.\ A$ itself. In other words, the derivation of the premiss must be parametric in a. The local reduction carries out the substitution for the parameter.

$$\dfrac{\dfrac{\begin{array}{c} \mathcal{D} \\ [a/x]A\ \mathit{true} \end{array}}{\forall x.\ A\ \mathit{true}}\,\forall\mathrm{I}}{[t/x]A\ \mathit{true}}\,\forall\mathrm{E} \quad \Longrightarrow_R \quad \begin{array}{c} [t/a]\mathcal{D} \\ [t/x]A\ \mathit{true} \end{array}$$

Here, $[t/a]\mathcal{D}$ is our notation for the result of substituting t for the parameter a throughout the deduction $\mathcal{D}$. For this substitution to preserve the conclusion, we must know that a does not already occur in A. Similarly, we would change the hypotheses if a occurred free in any of the undischarged hypotheses of $\mathcal{D}$. This might render a larger proof incorrect. As an example, consider the formula $\forall x.\ \forall y.\ P(x) \supset P(y)$ which should clearly not be true for all predicates P. The following is *not* a deduction of this formula.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{P(a)\ \mathit{true}}\;u}{\forall x.\ P(x)\ \mathit{true}}\;\forall\mathrm{I}^a?}{P(b)\ \mathit{true}}\;\forall\mathrm{E}}{P(a) \supset P(b)\ \mathit{true}}\;{\supset}\mathrm{I}^u}{\forall y.\ P(a) \supset P(y)\ \mathit{true}}\;\forall\mathrm{I}^b}{\forall x.\ \forall y.\ P(x) \supset P(y)\ \mathit{true}}\;\forall\mathrm{I}^a$$

The flaw is at the inference marked with "?," where a is free in the hypothesis labelled u. Applying a local proof reduction to the (incorrect) $\forall$I inference followed by $\forall$E leads to the the assumption $[b/a]P(a)$ which is equal to $P(b)$. The resulting derivation

$$\dfrac{\dfrac{\dfrac{\overline{P(b)\ \mathit{true}}\;u}{P(a) \supset P(b)\ \mathit{true}}\;{\supset}\mathrm{I}^u}{\forall y.\ P(a) \supset P(y)\ \mathit{true}}\;\forall\mathrm{I}^b}{\forall x.\ \forall y.\ P(x) \supset P(y)\ \mathit{true}}\;\forall\mathrm{I}^a$$

is once again incorrect since the hypothesis labelled u should read $P(a)$, not $P(b)$.

The local expansion for universal quantification is much simpler.

$$\begin{array}{c}\mathcal{D}\\ \forall x.\ A\ \mathit{true}\end{array} \quad \Longrightarrow_E \quad \dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ \forall x.\ A\ \mathit{true}\end{array}}{[a/x]A\ \mathit{true}}\;\forall\mathrm{E}}{\forall x.\ A\ \mathit{true}}\;\forall\mathrm{I}^a$$

Existential Quantification. We conclude that $\exists x.\ A$ is true when there is a term t such that $[t/x]A$ is true.

$$\dfrac{[t/x]A\ \mathit{true}}{\exists x.\ A\ \mathit{true}}\;\exists\mathrm{I}$$

When we have an assumption $\exists x.\ A$ we do not know for which t it is the case that $[t/x]A$ holds. We can only assume that $[a/x]A$ holds for some parameter a about which we know nothing else. Thus the elimination rule resembles the one for disjunction.

$$\dfrac{\exists x.\,A\ \mathit{true} \qquad \begin{array}{c}\overline{[a/x]A\ \mathit{true}}^{\,u}\\ \vdots\\ C\ \mathit{true}\end{array}}{C\ \mathit{true}}\ \exists\mathrm{E}^{a,u}$$

The restriction is similar to the one for $\forall$I: the parameter a must be new, that is, it must not occur in $\exists x.\ A$, C, or any assumption employed in the derivation of the second premiss. In the reduction rule we have to perform two substitutions: we have to substitute t for the parameter a and we also have to substitute for the hypothesis labelled u.

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}\\ [t/x]A\ \mathit{true}\end{array}}{\exists x.\,A}\ \exists\mathrm{I} \qquad \begin{array}{c}\overline{[a/x]A\ \mathit{true}}^{\,u}\\ \mathcal{E}\\ C\ \mathit{true}\end{array}}{C\ \mathit{true}}\ \exists\mathrm{E}^{a,u} \quad \Longrightarrow_R \quad \begin{array}{c}\dfrac{\mathcal{D}}{[t/x]A\ \mathit{true}}\ u\\ [t/a]\mathcal{E}\\ C\ \mathit{true}\end{array}$$

The proviso on occurrences of a guarantees that the conclusion and hypotheses of $[t/a]\mathcal{E}$ have the correct form. The local expansion for existential quantification is also similar to the case for disjunction.

$$\begin{array}{c}\mathcal{D}\\ \exists x.\,A\ \mathit{true}\end{array} \quad \Longrightarrow_E \quad \dfrac{\begin{array}{c}\mathcal{D}\\ \exists x.\,A\ \mathit{true}\end{array} \qquad \dfrac{\overline{[a/x]A\ \mathit{true}}^{\,u}}{\exists x.\,A\ \mathit{true}}\ \exists\mathrm{I}}{\exists x.\,A\ \mathit{true}}\ \exists\mathrm{E}^{a,u}$$

Here is a simple example of a natural deduction. We attempt to show the process by which such a deduction may have been generated, as well as the final deduction. The three vertical dots indicate a gap in the derivation we are trying to construct, with hypotheses and their consequences shown above and the desired conclusion below the gap.

$$\begin{array}{c}\vdots\\ A \wedge (A \supset B) \supset B\ \mathit{true}\end{array} \quad \rightsquigarrow \quad \dfrac{\begin{array}{c}\overline{A \wedge (A \supset B)\ \mathit{true}}^{\,u}\\ \vdots\\ B\ \mathit{true}\end{array}}{A \wedge (A \supset B) \supset B\ \mathit{true}}\ {\supset}\mathrm{I}^{u}$$

$$\rightsquigarrow \quad \dfrac{\begin{array}{c} \dfrac{\dfrac{}{A \wedge (A \supset B)\ \mathit{true}}\,u}{A\ \mathit{true}}\,\wedge\mathrm{E_L} \\ \vdots \\ B\ \mathit{true}\end{array}}{A \wedge (A \supset B) \supset B\ \mathit{true}}\,\supset\mathrm{I}^u \quad \rightsquigarrow \quad \dfrac{\begin{array}{c} \dfrac{\dfrac{}{A \wedge (A \supset B)\ \mathit{true}}\,u}{A\ \mathit{true}}\,\wedge\mathrm{E_L} \qquad \dfrac{\dfrac{}{A \wedge (A \supset B)\ \mathit{true}}\,u}{A \supset B\ \mathit{true}}\,\wedge\mathrm{E_R} \\ \vdots \\ B\ \mathit{true}\end{array}}{A \wedge (A \supset B) \supset B\ \mathit{true}}\,\supset\mathrm{I}^u$$

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

$$\rightsquigarrow \quad \dfrac{\dfrac{\dfrac{\dfrac{}{A \wedge (A \supset B)\ \mathit{true}}\,u}{A \supset B\ \mathit{true}}\,\wedge\mathrm{E_R} \qquad \dfrac{\dfrac{}{A \wedge (A \supset B)\ \mathit{true}}\,u}{A\ \mathit{true}}\,\wedge\mathrm{E_L}}{B\ \mathit{true}}\,\supset\mathrm{E}}{A \wedge (A \supset B) \supset B\ \mathit{true}}\,\supset\mathrm{I}^u$$

The symbols A and B in this derivation stand for arbitrary propositions; we can thus established a judgment parametric in A and B. In other words, every instance of this derivation (substituting arbitrary propositions for A and B) is a valid derivation.

Below is a summary of the rules of intuitionistic natural deduction.

Introduction Rules

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

$$\frac{A\ \mathit{true}}{A \vee B\ \mathit{true}}\ \vee\mathrm{I}_{\mathrm{L}} \qquad \frac{B\ \mathit{true}}{A \vee B\ \mathit{true}}\ \vee\mathrm{I}_{\mathrm{R}}$$

$$\frac{\begin{array}{c}\overline{A\ \mathit{true}}^{\,u}\\ \vdots\\ B\ \mathit{true}\end{array}}{A \supset B\ \mathit{true}}\ \supset\mathrm{I}^{u}$$

$$\frac{\begin{array}{c}\overline{A\ \mathit{true}}^{\,u}\\ \vdots\\ p\ \mathit{true}\end{array}}{\neg A\ \mathit{true}}\ \neg\mathrm{I}^{p,u}$$

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

no $\bot$ *introduction*

$$\frac{[a/x]A\ \mathit{true}}{\forall x.\ A\ \mathit{true}}\ \forall\mathrm{I}^{a}$$

$$\frac{[t/x]A\ \mathit{true}}{\exists x.\ A\ \mathit{true}}\ \exists\mathrm{I}$$

Elimination Rules

$$\frac{A \wedge B\ \mathit{true}}{A\ \mathit{true}}\ \wedge\mathrm{E}_{\mathrm{L}} \qquad \frac{A \wedge B\ \mathit{true}}{B\ \mathit{true}}\ \wedge\mathrm{E}_{\mathrm{R}}$$

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

$$\frac{A \supset B\ \mathit{true} \qquad A\ \mathit{true}}{B\ \mathit{true}}\ \supset\mathrm{E}$$

$$\frac{\neg A\ \mathit{true} \qquad A\ \mathit{true}}{C\ \mathit{true}}\ \neg\mathrm{E}$$

no $\top$ *elimination*

$$\frac{\bot\ \mathit{true}}{C\ \mathit{true}}\ \bot\mathrm{E}$$

$$\frac{\forall x.\ A\ \mathit{true}}{[t/x]A\ \mathit{true}}\ \forall\mathrm{E}$$

$$\frac{\exists x.\ A\ \mathit{true} \qquad \begin{array}{c}\overline{[a/x]A\ \mathit{true}}^{\,u}\\ \vdots\\ C\ \mathit{true}\end{array}}{C\ \mathit{true}}\ \exists\mathrm{E}^{a,u}$$

2.2 Classical Logic

The inference rules so far only model *intuitionistic logic*, and some classically true propositions such as $A \vee \neg A$ (for an arbitrary A) are not derivable, as we will see in Section 3.5. There are three commonly used ways one can construct a system of *classical natural deduction* by adding one additional rule of inference. $\bot_C$ is called *Proof by Contradiction* or *Rule of Indirect Proof*, $\neg\neg_C$ is the *Double Negation Rule*, and XM is referred to as *Excluded Middle*.

$$\dfrac{\begin{array}{c}\overline{\neg A}\,u \\ \vdots \\ \bot\end{array}}{A}\,\bot_C^u \qquad \dfrac{\neg\neg A}{A}\,\neg\neg_C \qquad \dfrac{}{A \vee \neg A}\,\mathrm{XM}$$

The rule for classical logic (whichever one chooses to adopt) breaks the pattern of introduction and elimination rules. One can still formulate some reductions for classical inferences, but natural deduction is at heart an intuitionistic calculus. The symmetries of classical logic are much better exhibited in sequent formulations of the logic. In Exercise 2.3 we explore the three ways of extending the intuitionistic proof system and show that they are equivalent.

Another way to obtain a natural deduction system for classical logic is to allow multiple conclusions (see, for example, Parigot [Par92]).

2.3 Localizing Hypotheses

In the formulation of natural deduction from Section 2.1 correct use of hypotheses and parameters is a global property of a derivation. We can localize it by annotating each judgment in a derivation by the available parameters and hypotheses. We give here a formulation of natural deduction for intuitionistic logic with localized hypotheses, but not parameters. For this we need a notation for hypotheses which we call a *context*.

$$\textit{Contexts} \quad \Gamma \quad ::= \quad \cdot \mid \Gamma, u{:}A$$

Here, "$\cdot$" represents the empty context, and $\Gamma, u{:}A$ adds hypothesis A *true* labelled u to Γ. We assume that each label u occurs at most once in a context in order to avoid ambiguities. The main judgment can then be written as $\Gamma \vdash A$, where

$$\cdot, u_1{:}A_1, \ldots, u_n{:}A_n \vdash A$$

stands for

$$\begin{array}{c}\overline{A_1\ \textit{true}}\,u_1 \quad \ldots \overline{A_n\ \textit{true}}\,u_n \\ \vdots \\ A\ \textit{true}\end{array}$$

in the notation of Section 2.1.

We use a few important abbreviations in order to make this notation less cumbersome. First of all, we may omit the leading "$\cdot$" and write, for example, $u_1{:}A_1, u_2{:}A_2$ instead of $\cdot, u_1{:}A_1, u_2{:}A_2$. Secondly, we denote concatenation of contexts by overloading the comma operator as follows.

$$\begin{array}{rcl} \Gamma, \cdot & = & \Gamma \\ \Gamma, (\Gamma', u{:}A) & = & (\Gamma, \Gamma'), u{:}A \end{array}$$

With these additional definitions, the localized version of our rules are as follows.

Introduction Rules

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge\mathrm{I}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee\mathrm{I_L} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee\mathrm{I_R}$$

$$\frac{\Gamma, u{:}A \vdash B}{\Gamma \vdash A \supset B} \supset\mathrm{I}^u$$

$$\frac{\Gamma, u{:}A \vdash p}{\Gamma \vdash \neg A} \neg\mathrm{I}^{p,u}$$

$$\frac{}{\Gamma \vdash \top} \top\mathrm{I}$$

no $\perp$ introduction

$$\frac{\Gamma \vdash [a/x]A}{\Gamma \vdash \forall x.\ A} \forall\mathrm{I}^a$$

$$\frac{\Gamma \vdash [t/x]A}{\Gamma \vdash \exists x.\ A} \exists\mathrm{I}$$

Elimination Rules

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge\mathrm{E_L} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge\mathrm{E_R}$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, u{:}A \vdash C \qquad \Gamma, w{:}B \vdash C}{\Gamma \vdash C} \vee\mathrm{E}^{u,w}$$

$$\frac{\Gamma \vdash A \supset B \qquad \Gamma \vdash A}{\Gamma \vdash B} \supset\mathrm{E}$$

$$\frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash C} \neg\mathrm{E}$$

no $\top$ elimination

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash C} \perp\mathrm{E}$$

$$\frac{\Gamma \vdash \forall x.\ A}{\Gamma \vdash [t/x]A} \forall\mathrm{E}$$

$$\frac{\Gamma \vdash \exists x.\ A \qquad \Gamma, u{:}[a/x]A \vdash C}{\Gamma \vdash C} \exists\mathrm{E}^{a,u}$$

We also have a new rule for hypotheses which was an implicit property of the hypothetical judgments before.

$$\frac{}{\Gamma_1, u{:}A, \Gamma_2 \vdash A}\, u$$

Other general assumptions about hypotheses, namely that they may be used arbitrarily often in a derivation and that their order does not matter, are indirectly reflected in these rules. Note that if we erase the context Γ from the judgments throughout a derivation, we obtain a derivation in the original notation.

When we discussed local reductions in order to establish local soundness, we used the notation

$$\begin{array}{c} \dfrac{\mathcal{D}}{A\ \mathit{true}}\,u \\ \mathcal{E} \\ C\ \mathit{true} \end{array}$$

for the result of substituting the derivation $\mathcal{D}$ of A *true* for all uses of the hypothesis A *true* labelled u in $\mathcal{E}$. We would now like to reformulate the property with localized hypotheses. In order to prove that the (now explicit) hypotheses behave as expected, we use the principle of *structural induction* over derivations. Simply put, we prove a property for all derivations by showing that, whenever it holds for the premisses of an inference, it holds for the conclusion. Note that we have to show the property outright when the rule under consideration has no premisses. Such rules are the base cases for the induction.

Theorem 2.1 (Structural Properties of Hypotheses) *The following properties hold for intuitionistic natural deduction.*

1. *(Exchange) If* $\Gamma_1, u_1{:}A, \Gamma_2, u_2{:}B, \Gamma_3 \vdash C$ *then* $\Gamma_1, u_2{:}B, \Gamma_2, u_1{:}A, \Gamma_3 \vdash C$.
2. *(Weakening) If* $\Gamma_1, \Gamma_2 \vdash C$ *then* $\Gamma_1, u{:}A, \Gamma_2 \vdash C$.
3. *(Contraction) If* $\Gamma_1, u_1{:}A, \Gamma_2, u_2{:}A, \Gamma_3 \vdash C$ *then* $\Gamma_1, u{:}A, \Gamma_2, \Gamma_3 \vdash C$.
4. *(Substitution) If* $\Gamma_1, u{:}A, \Gamma_2 \vdash C$ *and* $\Gamma_1 \vdash A$ *then* $\Gamma_1, \Gamma_2 \vdash C$.

Proof: The proof is in each case by straightforward induction over the structure of the first given derivation.

In the case of exchange, we appeal to the inductive assumption on the derivations of the premisses and construct a new derivation with the same inference rule. Algorithmically, this means that we exchange the hypotheses labelled u_1 and u_2 in every judgment in the derivation.

In the case of weakening and contraction, we proceed similarly, either adding the new hypothesis $u{:}A$ to every judgment in the derivation (for weakening), or replacing uses of u_1 and u_2 by u (for contraction).

For substitution, we apply the inductive assumption to the premisses of the given derivation $\mathcal{D}$ until we reach hypotheses. If the hypothesis is different from u we can simply erase $u{:}A$ (which is unused) to obtain the desired derivation. If the hypothesis is $u{:}A$ the derivation looks like

$$\mathcal{D} = \dfrac{}{\Gamma_1, u{:}A, \Gamma_2 \vdash A}\,u$$

so $C = A$ in this case. We are also given a derivation $\mathcal{E}$ of $\Gamma_1 \vdash A$ and have to construct a derivation $\mathcal{F}$ of $\Gamma_1, \Gamma_2 \vdash A$. But we can just repeatedly apply weakening to $\mathcal{E}$ to obtain $\mathcal{F}$. Algorithmically, this means that, as expected, we substitute the derivation $\mathcal{E}$ (possibly weakened) for uses of the hypotheses $u{:}A$ in $\mathcal{D}$. Note that in our original notation, this weakening has no impact, since unused hypotheses are not apparent in a derivation. □

It is also possible to localize the derivations themselves, using *proof terms*. As we will see in Section 2.4, these proof terms form a λ-calculus closely related to functional programming. When parameters, hypotheses, and proof terms are all localized our main judgment becomes decidable. In the terminology of Martin-Löf [ML94], the main judgment is then *analytic* rather than *synthetic*. We no longer need to go outside the judgment itself in order to collect evidence for it: An analytic judgment encapsulates its own evidence.

2.4 Proof Terms

The basic judgment of the system of natural deduction is the derivability of a formula A, written as $\vdash A$. It has been noted by Howard [How69] that there is a strong correspondence between (intuitionistic) derivations and λ-terms. The formulas A then act as types classifying λ-terms. In the propositional case, this correspondence is an isomorphism: formulas are isomorphic to types and derivations are isomorphic to simply-typed λ-terms. These isomorphisms are often called the *propositions-as-types* and *proofs-as-programs* paradigms.

If we stopped at this observation, we would have obtained only a fresh interpretation of familiar deductive systems, but we would not be any closer to the goal of providing a language for reasoning about properties of programs. However, the correspondences can be extended to first-order and higher-order logics. Interpreting first-order (or higher-order) formulas as types yields a significant increase in expressive power of the type system. However, maintaining an isomorphism during the generalization to first-order logic is somewhat unnatural and cumbersome. One might expect that a proof contains more information than the corresponding program. Thus the literature often talks about *extracting programs from proofs* or *contracting proofs to programs*. We do not discuss program extraction further in these notes.

We now introduce a notation for derivations to be carried along in deductions. For example, if M represents a proof of A and N represents a proof of B, then the pair $\langle M, N \rangle$ can be seen as a representation of the proof of $A \wedge B$ by $\wedge$-introduction. We write $\Gamma \vdash M : A$ to express the judgment M *is a proof term for* A *under hypotheses* Γ. We also repeat the local reductions and expansions from the previous section in the new notation. For local expansion we state the proposition whose truth must established by the proof term on the left-hand side. This expresses restrictions on the application of the expansion rules.

Conjunction. The proof term for a conjunction is simply the pair of proofs of the premisses.

$$\frac{\Gamma \vdash M : A \qquad \Gamma \vdash N : B}{\Gamma \vdash \langle M, N\rangle : A \wedge B}\wedge\mathrm{I}$$

$$\frac{\Gamma \vdash M : A \wedge B}{\Gamma \vdash \mathrm{fst}\, M : A}\wedge\mathrm{E_L} \qquad \frac{\Gamma \vdash M : A \wedge B}{\Gamma \vdash \mathrm{snd}\, M : B}\wedge\mathrm{E_R}$$

The local reductions now lead to two obvious local reductions of the proof terms. The local expansion is similiarly translated.

$$\begin{array}{rcl} \mathrm{fst}\,\langle M, N\rangle & \longrightarrow_R & M \\ \mathrm{snd}\,\langle M, N\rangle & \longrightarrow_R & N \\ M : A \wedge B & \longrightarrow_E & \langle \mathrm{fst}\, M, \mathrm{snd}\, M\rangle \end{array}$$

Implication. The proof of an implication $A \supset B$ will be represented by a function which maps proofs of A to proofs of B. The introduction rule explicitly forms such a function by λ-abstraction and the elimination rule applies the function to an argument.

$$\frac{\Gamma, u{:}A \vdash M : B}{\Gamma \vdash (\lambda u{:}A.\ M) : A \supset B}\supset\mathrm{I}^u \qquad \frac{\Gamma \vdash M : A \supset B \qquad \Gamma \vdash N : A}{\Gamma \vdash M\, N : B}\supset\mathrm{E}$$

The binding of the variable u in the conclusion of $\supset$I correctly models the intuition that the hypothesis is discharged and not available outside deduction of the premiss. The abstraction is labelled with the proposition A so that we can later show that the proof term uniquely determines a natural deduction. If A were not given then, for example, $\lambda u.\ u$ would be ambigous and serve as a proof term for $A \supset A$ for any formula A. The local reduction rule is β-reduction; the local expansion is η-expansion.

$$\begin{array}{rcl} (\lambda u{:}A.\ M)\, N & \longrightarrow_R & [N/u]M \\ M : A \supset B & \longrightarrow_E & \lambda u{:}A.\ M\, u \end{array}$$

In the reduction rule, bound variables in M that are free in N must be renamed in order to avoid variable capture. In the expansion rule u must be new—it may not already occur in M.

Disjunction. The proof term for disjunction introduction is the proof of the premiss together with an indication whether it was inferred by introduction on the left or on the right. We also annotate the proof term with the formula which did not occur in the premiss so that a proof term always proves exactly one proposition.

$$\frac{\Gamma \vdash M : A}{\Gamma \vdash \mathrm{inl}^B\, M : A \vee B}\vee\mathrm{I_L} \qquad \frac{\Gamma \vdash N : B}{\Gamma \vdash \mathrm{inr}^A\, N : A \vee B}\vee\mathrm{I_R}$$

The elimination rule corresponds to a case construction.

$$\frac{\Gamma \vdash M : A \vee B \qquad \Gamma, u{:}A \vdash N_1 : C \qquad \Gamma, w{:}B \vdash N_2 : C}{\Gamma \vdash (\,\mathbf{case}\ M\ \mathbf{of}\ \mathrm{inl}\,u \Rightarrow N_1 \mid \mathrm{inr}\,w \Rightarrow N_2\,) : C} \vee\mathrm{E}^{u,w}$$

Since the variables u and w label assumptions, the corresponding proof term variables are *bound* in N_1 and N_2, respectively. The two reduction rules now also look like rules of computation in a λ-calculus.

$$\begin{array}{lcl}\mathbf{case}\ \mathrm{inl}^B\,M\ \mathbf{of}\ \mathrm{inl}\,u \Rightarrow N_1 \mid \mathrm{inr}\,w \Rightarrow N_2 & \longrightarrow_R & [M/u]N_1 \\ \mathbf{case}\ \mathrm{inr}^A\,M\ \mathbf{of}\ \mathrm{inl}\,u \Rightarrow N_1 \mid \mathrm{inr}\,w \Rightarrow N_2 & \longrightarrow_R & [M/w]N_2\end{array}$$

$$M : A \vee B \quad \longrightarrow_E \quad \mathbf{case}\ M\ \mathbf{of}\ \mathrm{inl}\,u \Rightarrow \mathrm{inl}^B\,u \mid \mathrm{inr}\,w \Rightarrow \mathrm{inr}^A\,w$$

The substitution of a deduction for a hypothesis is represented by the substitution of a proof term for a variable.

Negation. This is similar to implication. Since the premise of the rule is parametric in p the corresponding proof constructor must bind a propositional variable p, indicated by μ^p. Similarly, the elimination construct must record the formula to maintain the property that every valid term proves exactly one proposition. This is indicated as a subscript C to the infix operator "$\cdot$".

$$\frac{\Gamma, u{:}A \vdash M : p}{\Gamma \vdash \mu^p u{:}A.\ M : \neg A} \neg\mathrm{I}^{p,u} \qquad\qquad \frac{\Gamma \vdash M : \neg A \qquad \Gamma \vdash N : A}{\Gamma \vdash M \cdot_C N : C} \neg\mathrm{E}$$

The reduction performs formula and proof term substitutions.

$$\begin{array}{rcl}(\mu^p u{:}A.\ M) \cdot_C N & \longrightarrow_R & [N/u][C/p]M \\ M : \neg A & \longrightarrow_E & \mu^p u{:}A.\ M \cdot_p u\end{array}$$

Truth. The proof term for $\top\mathrm{I}$ is written $\langle\,\rangle$.

$$\frac{}{\Gamma \vdash \langle\,\rangle : \top} \top\mathrm{I}$$

Of course, there is no reduction rule. The expansion rule reads

$$M : \top \quad \longrightarrow_E \quad \langle\,\rangle$$

Falsehood. Here we need to annotate the proof term abort with the formula being proved to avoid ambiguity.

$$\frac{\Gamma \vdash M : \bot}{\Gamma \vdash \mathrm{abort}^C\,M : C} \bot\mathrm{E}$$

Again, there is no reduction rule, only an expansion rule.

$$M : \bot \quad \longrightarrow_E \quad \mathrm{abort}^{\bot}\,M$$

In summary, we have

$$
\begin{array}{llcll}
\text{Terms} & M & ::= & u & \textit{Hypotheses} \\
& & \mid & \langle M_1, M_2\rangle \mid \mathrm{fst}\, M \mid \mathrm{snd}\, M & \textit{Conjunction} \\
& & \mid & \lambda u{:}A.\ M \mid M_1\, M_2 & \textit{Implication} \\
& & \mid & \mathrm{inl}^A\, M \mid \mathrm{inr}^A\, M & \textit{Disjunction} \\
& & \mid & (\,\mathbf{case}\ M\ \mathbf{of}\ \mathrm{inl}\, u_1 \Rightarrow M_1 \mid \mathrm{inr}\, u_2 \Rightarrow M_2) & \\
& & \mid & \mu^p u{:}A.\ M \mid M_1 \cdot_A M_2 & \textit{Negation} \\
& & \mid & \langle\,\rangle & \textit{Truth} \\
& & \mid & \mathrm{abort}^A\, M & \textit{Falsehood}
\end{array}
$$

and the reduction rules

$$
\begin{array}{rcc}
\mathrm{fst}\,\langle M, N\rangle & \longrightarrow_R & M \\
\mathrm{snd}\,\langle M, N\rangle & \longrightarrow_R & N \\
(\lambda u{:}A.\ M)\, N & \longrightarrow_R & [N/u]M \\
\mathbf{case}\ \mathrm{inl}^B\, M\ \mathbf{of}\ \mathrm{inl}\, u \Rightarrow N_1 \mid \mathrm{inr}\, w \Rightarrow N_2 & \longrightarrow_R & [M/u]N_1 \\
\mathbf{case}\ \mathrm{inr}^A\, M\ \mathbf{of}\ \mathrm{inl}\, u \Rightarrow N_1 \mid \mathrm{inr}\, w \Rightarrow N_2 & \longrightarrow_R & [M/w]N_2 \\
(\mu^p u{:}A.\ M) \cdot_C N & \longrightarrow_R & [N/u][C/p]M \\
\textit{no rule for truth} & & \\
\textit{no rule for falsehood} & &
\end{array}
$$

The expansion rules are given below.

$$
\begin{array}{rcl}
M : A \wedge B & \longrightarrow_E & \langle \mathrm{fst}\, M, \mathrm{snd}\, M\rangle \\
M : A \supset B & \longrightarrow_E & \lambda u{:}A.\ M\, u \\
M : A \vee B & \longrightarrow_E & \mathbf{case}\ M\ \mathbf{of}\ \mathrm{inl}\, u \Rightarrow \mathrm{inl}^B\, u \mid \mathrm{inr}\, w \Rightarrow \mathrm{inr}^A\, w \\
M : \neg A & \longrightarrow_E & \mu^p u{:}A.\ M \cdot_p u \\
M : \top & \longrightarrow_E & \langle\,\rangle \\
M : \bot & \longrightarrow_E & \mathrm{abort}^\bot\, M
\end{array}
$$

We can now see that the formulas act as types for proof terms. Shifting to the usual presentation of the typed λ-calculus we use τ and σ as symbols for types, and $\tau \times \sigma$ for the product type, $\tau \to \sigma$ for the function type, $\tau + \sigma$ for the disjoint sum type, 1 for the unit type and 0 for the empty or void type. Base types b remain unspecified, just as the basic propositions of the propositional calculus remain unspecified. Types and propositions then correspond to each other as indicated below.

$$
\begin{array}{rcl}
\text{Types}\ \tau & ::= & b \mid \tau_1 \times \tau_2 \mid \tau_1 \to \tau_2 \mid \tau_1 + \tau_2 \mid 1 \mid 0 \\
\text{Propositions}\ A & ::= & p \mid A_1 \wedge A_2 \mid A_1 \supset A_2 \mid A_1 \vee A_2 \mid \top \mid \bot
\end{array}
$$

We omit here the negation type which is typically not used in functional programming and thus does not have a well-known counterpart. We can think of $\neg A$ as corresponding to $\tau \to 0$, where τ corresponds to A. We now summarize and restate the rules above, using the notation of types instead of propositions (omitting only the case for negation). Note that contexts Γ now declare variables with their types, rather than hypothesis labels with their proposition.

$\Gamma \rhd M : \tau$ *Term M has type τ in context Γ*

$$\frac{\Gamma \rhd M : \tau \qquad \Gamma \rhd N : \sigma}{\Gamma \rhd \langle M, N \rangle : \tau \times \sigma}\,\mathsf{pair}$$

$$\frac{\Gamma \rhd M : \tau \times \sigma}{\Gamma \rhd \mathrm{fst}\, M : \tau}\,\mathsf{fst} \qquad \frac{\Gamma \rhd M : \tau \times \sigma}{\Gamma \rhd \mathrm{snd}\, M : \sigma}\,\mathsf{snd}$$

$$\frac{\Gamma, u{:}\tau \rhd M : \sigma}{\Gamma \rhd (\lambda u{:}\tau.\ M) : \tau \to \sigma}\,\mathsf{lam} \qquad \frac{u : \tau \text{ in } \Gamma}{\Gamma \rhd u : \tau}\,\mathsf{var}$$

$$\frac{\Gamma \rhd M : \tau \to \sigma \qquad \Gamma \rhd N : \tau}{\Gamma \rhd M\, N : \sigma}\,\mathsf{app}$$

$$\frac{\Gamma \rhd M : \tau}{\Gamma \rhd \mathrm{inl}^{\sigma}\, M : \tau + \sigma}\,\mathsf{inl} \qquad \frac{\Gamma \rhd N : \sigma}{\Gamma \rhd \mathrm{inr}^{\tau}\, N : \tau + \sigma}\,\mathsf{inr}$$

$$\frac{\Gamma \rhd M : \tau + \sigma \qquad \Gamma, u{:}\tau \rhd N_1 : \nu \qquad \Gamma, w{:}\sigma \rhd N_2 : \nu}{\Gamma \rhd (\,\mathbf{case}\ M\ \mathbf{of}\ \mathrm{inl}\, u \Rightarrow N_1 \mid \mathrm{inr}\, w \Rightarrow N_2) : \nu}\,\mathsf{case}$$

$$\frac{}{\Gamma \rhd \langle\,\rangle : 1}\,\mathsf{unit} \qquad \frac{\Gamma \rhd M : 0}{\Gamma \rhd \mathrm{abort}^{\nu}\, M : \nu}\,\mathsf{abort}$$

2.5 Exercises

Exercise 2.1 Prove the following by natural deduction using only intuitionistic rules when possible. We use the convention that $\supset$, $\wedge$, and $\vee$ associate to the right, that is, $A \supset B \supset C$ stands for $A \supset (B \supset C)$. $A \equiv B$ is a syntactic abbreviation for $(A \supset B) \wedge (B \supset A)$. Also, we assume that $\wedge$ and $\vee$ bind more tightly than $\supset$, that is, $A \wedge B \supset C$ stands for $(A \wedge B) \supset C$. The scope of a quantifier extends as far to the right as consistent with the present parentheses. For example, $(\forall x.\ P(x) \supset C) \wedge \neg C$ would be disambiguated to $(\forall x.\ (P(x) \supset C)) \wedge (\neg C)$.

1. $\vdash A \supset B \supset A$.
2. $\vdash A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$.
3. (Peirce's Law). $\vdash ((A \supset B) \supset A) \supset A$.
4. $\vdash A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$.
5. $\vdash A \supset (A \wedge B) \vee (A \wedge \neg B)$.
6. $\vdash (A \supset \exists x.\ P(x)) \equiv \exists x.\ (A \supset P(x))$.
7. $\vdash ((\forall x.\ P(x)) \supset C) \equiv \exists x.\ (P(x) \supset C)$.

8. $\vdash \exists x.\, \forall y.\, (P(x) \supset P(y))$.

Exercise 2.2 We write $A \vdash B$ if B follows from hypothesis A and $A \dashv\vdash B$ for $A \vdash B$ and $B \vdash A$. Which of the following eight parametric judgments are derivable intuitionistically?

1. $(\exists x.\, A) \supset B \dashv\vdash \forall x.\, (A \supset B)$
2. $A \supset (\exists x.\, B) \dashv\vdash \exists x.\, (A \supset B)$
3. $(\forall x.\, A) \supset B \dashv\vdash \exists x.\, (A \supset B)$
4. $A \supset (\forall x.\, B) \dashv\vdash \forall x.\, (A \supset B)$

Provide natural deductions for the valid judgments. You may assume that the bound variable x does not occur in B (items 1 and 3) or A (items 2 and 4).

Exercise 2.3 Show that the three ways of extending the intuitionistic proof system for classical logic are equivalent, that is, the same formulas are deducible in all three systems.

Exercise 2.4 Assume we had omitted disjunction and existential quantification and their introduction and elimination rules from the list of logical primitives. In the classical system, give a definition of disjunction and existential quantification (in terms of other logical constants) and show that the introduction and elimination rules now become *admissible rules of inference*. A rule of inference is *admissible* if any deduction using the rule can be transformed into one without using the rule.

Exercise 2.5 Assume we would like to design a system of natural deduction for a simple temporal logic. The main judgment is now "*A is true at time t*" written as

$$A \mathbin{@} t.$$

1. Explain how to modify the given rules for natural deduction to this more general judgment and show the rules for implication and universal quantification.

2. Write out introduction and elimination rules for the temporal operator $\bigcirc A$ which should be true if A is true at the next point in time. Denote the "next time after t" by $t + 1$.

3. Show the local reductions and expansions which show the local soundness and completness of your rules.

4. Write out introduction and elimination rules for the temporal operator $\Box A$ which should be true if A is true at all times.

5. Show the local reductions and expansions.

Exercise 2.6 Design introduction and elimination rules for the connectives

1. $A \equiv B$, usually defined as $(A \supset B) \wedge (B \supset A)$,

2. $A \mid B$ (exclusive or), usually defined as $(A \wedge \neg B) \vee (\neg A \wedge B)$,

without recourse to other logical constants or operators. Also show the corresponding local reductions and expansions. For each of the following proposed connectives, write down appropriate introduction and eliminations rules and show the local reductions and expansion or indicate that no such rule may exist.

3. $A \overline{\wedge} B$ for $\neg(A \wedge B)$,

4. $A \overline{\vee} B$ for $\neg(A \vee B)$,

5. $A \overline{\supset} B$ for $\neg(A \supset B)$,

6. $+A$ for $\neg\neg A$,

7. $\exists^* x.\ A$ for $\neg \forall x.\ \neg A$,

8. $\forall^* x.\ A$ for $\neg \exists x.\ \neg A$,

9. $A \Rightarrow B \mid C$ for $(A \supset B) \wedge (\neg A \supset C)$.

Exercise 2.7 A given introduction rule does not necessarily uniquely determine matching elimination rules and vice versa. Explore if the following alternative rules are also sound and complete.

1. Replace the two elimination rules for conjunction by

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

2. Add the following elimination rule for truth.

$$\frac{\top\ \mathit{true} \qquad C\ \mathit{true}}{C\ \mathit{true}} \top \mathrm{E}$$

3. Add the following introduction rule for falsehood.

$$\frac{p\ \mathit{true}}{\bot\ \mathit{true}} \bot \mathrm{I}^{p}$$

Consider if any other of the standard connectives might permit alternative introduction or elimination rules which preserve derivability.

Exercise 2.8 For each of 14 following proposed entailments either write out a proof term for the corresponding implication or indicate that it is not derivable.

1. $A \supset (B \supset C) \dashv\vdash (A \wedge B) \supset C$
2. $A \supset (B \wedge C) \dashv\vdash (A \supset B) \wedge (A \supset C)$
3. $A \supset (B \vee C) \dashv\vdash (A \supset B) \vee (A \supset C)$
4. $(A \supset B) \supset C \dashv\vdash (A \vee C) \wedge (B \supset C)$
5. $(A \vee B) \supset C \dashv\vdash (A \supset C) \wedge (B \supset C)$
6. $A \wedge (B \vee C) \dashv\vdash (A \wedge B) \vee (A \wedge C)$
7. $A \vee (B \wedge C) \dashv\vdash (A \vee B) \wedge (A \vee C)$

Exercise 2.9 The de Morgan laws of classical logic allow negation to be distributed over other logical connectives. Investigate which directions of the de Morgan equivalences hold in intuitionistic logic and give proof terms for the valid entailments.

1. $\neg(A \wedge B) \dashv\vdash \neg A \vee \neg B$
2. $\neg(A \vee B) \dashv\vdash \neg A \wedge \neg B$
3. $\neg(A \supset B) \dashv\vdash A \wedge \neg B$
4. $\neg(\neg A) \dashv\vdash A$
5. $\neg\top \dashv\vdash \bot$
6. $\neg\bot \dashv\vdash \top$
7. $\neg\forall x.\ A \dashv\vdash \exists x.\ \neg A$
8. $\neg\exists x.\ A \dashv\vdash \forall x.\ \neg A$

Exercise 2.10 An alternative approach to negation is to introduce another judgment, A *is false*, and develop a system of evidence for this judgment. For example, we might say that $A \wedge B$ is false if either A is false or B is false. Similarly, $A \vee B$ is false if both A and B are false. Expressed as inference rules:

$$\frac{A\ \mathit{false}}{A \wedge B\ \mathit{false}} \qquad \frac{B\ \mathit{false}}{A \wedge B\ \mathit{false}} \qquad\qquad \frac{A\ \mathit{false} \qquad B\ \mathit{false}}{A \vee B\ \mathit{false}}$$

1. Write out a complete set of rules defining the judgment A *false* for the conjunction, implication, disjunction, truth, and falsehood.
2. Verify local soundness and completeness of your rules, if these notions make sense.

3. Now we define that $\neg A$ *true* if A *false*. Complete the set of rules and verify soundness and completeness if appropriate.

4. Does your system satisfy that every proposition A is either true or false? If so, prove it. Otherwise, show a counterexample.

5. Compare this notion of negation with the standard notion in intuitionistic logic.

6. Extend your system to include universal and existential quantification (if possible) and discuss its properties.