Automated Theorem Proving

Frank Pfenning
Carnegie Mellon University

Draft of Spring 2004

Material for the course *Automated Theorem Proving* at Carnegie Mellon University, Fall 1999, revised Spring 2004. This includes revised excerpts from the course notes on *Linear Logic* (Spring 1998) and *Computation and Deduction* (Spring 1997). Material for this course is available at
`http://www.cs.cmu.edu/~fp/courses/atp/`.

Please send comments to `fp@cs.cmu.edu`

This material is in rough draft form and is likely to contain errors. Furthermore, citations are in no way adequate or complete. Please do not cite or distribute this document.

This work was supported by NSF Grants CCR-9303383, CCR-9619684, CCR-0306313, and CCR-0325808.

Contents

Chapter 1

Introduction

Logic is a science studying the principles of reasoning and valid inference. Automated deduction is concerned with the mechanization of formal reasoning, following the laws of logic. The roots of the field go back to the end of the last century when Frege developed his *Begriffsschrift*[1], the first comprehensive effort to develop a formal language suitable as a foundation for mathematics. Alas, Russell discovered a paradox which showed that Frege's system was *inconsistent*, that is, the truth of every proposition can be derived in it. Russell then devised his own system based on a *type theory* and he and Whitehead demonstrated in the monumental *Principia Mathematica* how it can serve as a foundation of mathematics. Later, Hilbert developed a simpler alternative, the *predicate calculus*. Gentzen's formulation of the predicate calculus in a system of *natural deduction* provides a major milestone for the field. In natural deduction, the meaning of each logical connective is explained via inference rules, an approach later systematically refined by Martin-Löf. This is the presentation we will follow in these notes.

Gentzen's seminal work also contains an early consistency proof for a formal logical system. As a technical device he introduced the *sequent calculus* and showed that it derives the same theorems as natural deduction. The famous *Hauptsatz*[2] establishes that all proofs in the sequent calculus can be found according to a simple strategy. It is immediately evident that there are many propositions which have no proof according to this strategy, thereby guaranteeing consistency of the system.

Most search strategies employed by automated deduction systems are either directly based on or can be derived from the sequent calculus. We can broadly classify procedures as either working backwards from the proposed theorem toward the axioms, or forward from the axioms toward the theorem. Among the backward searching procedures we find tableaux, connection methods, matrix methods and some forms of resolution. Among the forward searching procedures we find classical resolution and the inverse method. The prominence of

[1] literally translated as *concept notation*

[2] literally just "main theorem", often called the *cut elimination theorem*

resolution among these methods is no accident, since Robinson's seminal paper represented a major leap forward in the state of the art. It is natural to expect that a combination of forward and backward search could improve the efficiency of theorem proving system. Such a combination, however, has been elusive up to now, due to the largely incompatible basic choices in design and implementation of the two kinds of search procedures.

In this course we study both types of procedures. We investigate high-level questions, such as how these procedures relate to the basic sequent calculus. We also consider low-level issues, such as techniques for efficient implementation of the basic inference engine.

There is one further dimension to consider: which *logic* do we reason in? In philosophy, mathematics, and computer science many different logics are of interest. For example, there are classical logic, intuitionistic logic, modal logic, relevance logic, higher-order logic, dynamic logic, temporal logic, linear logic, belief logic, and lax logic (to mention just a few). While each logic requires its own considerations, many techniques are shared. This can be attributed in part to the common root of different logics in natural deduction and the sequent calculus. Another reason is that low-level efficiency improvements are relatively independent of higher-level techniques.

For this course we chose intuitionistic logic for a variety of reasons. First, intuitionistic propositions correspond to logical specifications and proofs to functional programs, which means intuitionistic logic is of central interest in the study of programming languages. Second, intuitionistic logic is more complex than classical logic and exhibits phenomena obscured by special properties which apply only to classical logic. Third, there are relatively straightforward interpretations of classical in intuitionistic logic which permits us to study logical interpretations in connection with theorem proving procedures.

The course is centered around a project, namely the joint design and implementation of a succession of theorem provers for intuitionistic logic. We start with natural deduction, followed by a sequent calculus, and a simple tableau prover. Then we turn toward the inverse method and introduce successive refinements consisting of both high-level and low-level optimizations.[3] The implementation component is important to gain a deeper understanding of the techniques introduced in our abstract study.

The goal of the course is to give students a thorough understanding of the central techniques in automated theorem proving. Furthermore, they should understand the systematic development of these techniques and their correctness proofs, thereby enabling them to transfer methods to different logics or applications. We are less interested here in an appreciation of the pragmatics of highly efficient implementations or performance tuning.

[3] The precise order and extent of the improvements possible in a one-semester graduate course has yet to be determined.

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.

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

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:

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

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

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

and symmetrically

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

The new judgment

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

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.

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

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*.

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

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

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

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.

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

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

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

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

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

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.

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

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

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

The other reduction is symmetric.

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

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.

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

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 $\neg A$.

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

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:

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

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.

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

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

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

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.

$$\begin{array}{c}\mathcal{D} \\ \top\ \mathit{true}\end{array} \qquad \Longrightarrow_E \qquad \dfrac{}{\top\ \mathit{true}}\,\top\mathrm{I}$$

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.

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

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.

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

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.

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

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) ∀I inference followed by ∀E leads to the the assumption $[b/a]P(a)$ which is equal to $P(b)$. The resulting derivation

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

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.

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

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

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

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.

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

The restriction is similar to the one for ∀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.

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

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.

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

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.

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

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

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

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

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	Elimination Rules
$\dfrac{A\ \mathit{true} \qquad B\ \mathit{true}}{A \wedge B\ \mathit{true}}\wedge\mathrm{I}$	$\dfrac{A \wedge B\ \mathit{true}}{A\ \mathit{true}}\wedge\mathrm{E_L} \qquad \dfrac{A \wedge B\ \mathit{true}}{B\ \mathit{true}}\wedge\mathrm{E_R}$
$\dfrac{A\ \mathit{true}}{A \vee B\ \mathit{true}}\vee\mathrm{I_L} \qquad \dfrac{B\ \mathit{true}}{A \vee B\ \mathit{true}}\vee\mathrm{I_R}$	$\dfrac{A \vee B\ \mathit{true} \qquad \begin{array}{c}\overline{A\ \mathit{true}}^{\,u} \\ \vdots \\ C\ \mathit{true}\end{array} \qquad \begin{array}{c}\overline{B\ \mathit{true}}^{\,w} \\ \vdots \\ C\ \mathit{true}\end{array}}{C\ \mathit{true}}\vee\mathrm{E}^{u,w}$
$\dfrac{\begin{array}{c}\overline{A\ \mathit{true}}^{\,u} \\ \vdots \\ B\ \mathit{true}\end{array}}{A \supset B\ \mathit{true}}\supset\mathrm{I}^{u}$	$\dfrac{A \supset B\ \mathit{true} \qquad A\ \mathit{true}}{B\ \mathit{true}}\supset\mathrm{E}$
$\dfrac{\begin{array}{c}\overline{A\ \mathit{true}}^{\,u} \\ \vdots \\ p\ \mathit{true}\end{array}}{\neg A\ \mathit{true}}\neg\mathrm{I}^{p,u}$	$\dfrac{\neg A\ \mathit{true} \qquad A\ \mathit{true}}{C\ \mathit{true}}\neg\mathrm{E}$
$\dfrac{}{\top\ \mathit{true}}\top\mathrm{I}$	*no* $\top$ *elimination*
no $\bot$ *introduction*	$\dfrac{\bot\ \mathit{true}}{C\ \mathit{true}}\bot\mathrm{E}$
$\dfrac{[a/x]A\ \mathit{true}}{\forall x.\ A\ \mathit{true}}\forall\mathrm{I}^{a}$	$\dfrac{\forall x.\ A\ \mathit{true}}{[t/x]A\ \mathit{true}}\forall\mathrm{E}$
$\dfrac{[t/x]A\ \mathit{true}}{\exists x.\ A\ \mathit{true}}\exists\mathrm{I}$	$\dfrac{\exists x.\ A\ \mathit{true} \qquad \begin{array}{c}\overline{[a/x]A\ \mathit{true}}^{\,u} \\ \vdots \\ C\ \mathit{true}\end{array}}{C\ \mathit{true}}\exists\mathrm{E}^{a,u}$

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	Elimination Rules
$\dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,\wedge\mathrm{I}$	$\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\,\wedge\mathrm{E}_\mathrm{L} \qquad \dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\,\wedge\mathrm{E}_\mathrm{R}$
$\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,\vee\mathrm{I}_\mathrm{L} \qquad \dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\,\vee\mathrm{I}_\mathrm{R}$	$\dfrac{\Gamma \vdash A \vee B \qquad \Gamma, u{:}A \vdash C \qquad \Gamma, w{:}B \vdash C}{\Gamma \vdash C}\,\vee\mathrm{E}^{u,w}$
$\dfrac{\Gamma, u{:}A \vdash B}{\Gamma \vdash A \supset B}\,\supset\mathrm{I}^u$	$\dfrac{\Gamma \vdash A \supset B \qquad \Gamma \vdash A}{\Gamma \vdash B}\,\supset\mathrm{E}$
$\dfrac{\Gamma, u{:}A \vdash p}{\Gamma \vdash \neg A}\,\neg\mathrm{I}^{p,u}$	$\dfrac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash C}\,\neg\mathrm{E}$
$\dfrac{}{\Gamma \vdash \top}\,\top\mathrm{I}$	*no $\top$ elimination*
no $\bot$ introduction	$\dfrac{\Gamma \vdash \bot}{\Gamma \vdash C}\,\bot\mathrm{E}$
$\dfrac{\Gamma \vdash [a/x]A}{\Gamma \vdash \forall x.\ A}\,\forall\mathrm{I}^a$	$\dfrac{\Gamma \vdash \forall x.\ A}{\Gamma \vdash [t/x]A}\,\forall\mathrm{E}$
$\dfrac{\Gamma \vdash [t/x]A}{\Gamma \vdash \exists x.\ A}\,\exists\mathrm{I}$	$\dfrac{\Gamma \vdash \exists x.\ A \qquad \Gamma, u{:}[a/x]A \vdash C}{\Gamma \vdash C}\,\exists\mathrm{E}^{a,u}$

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

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

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

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

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.

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

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.

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

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

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 $\top$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

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

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.

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

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.

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

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

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

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

$$\frac{\Gamma \triangleright M : \tau \rightarrow \sigma \qquad \Gamma \triangleright N : \tau}{\Gamma \triangleright M\, N : \sigma}\,\mathsf{app}$$

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

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

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

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

$$A \ @\ t.$$

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

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

2. Add the following elimination rule for truth.

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

3. Add the following introduction rule for falsehood.

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

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:

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

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.

Chapter 3

Sequent Calculus

In this chapter we develop the sequent calculus as a formal system for proof search in natural deduction. The sequent calculus was originally introduced by Gentzen [Gen35], primarily as a technical device for proving consistency of predicate logic. Our goal of describing a proof search procedure for natural deduction predisposes us to a formulation due to Kleene [Kle52] called G_3.

We introduce the sequent calculus in two steps. The first step is based on the simple strategy of building a natural deduction by using introduction rules bottom-up and elimination rules top-down. The result is an intercalation calculus which applies both to intuitionistic and classical logic [Byr99]. The second step consists of reformulating the rules for intercalation so that both forms of rules work bottom-up, resulting in the sequent calculus.

We also show how intercalation derivations lead to more compact proof terms, and how to extract proof terms from sequent calculus derivations.

3.1 Intercalation

A simple strategy in the search for a natural deduction is to use introduction rules reasoning bottom-up (from the proposed theorem towards the hypotheses) and the elimination rules top-down (from the assumptions towards the proposed theorem). When they meet in the middle we have found a *normal* deduction. Towards the end of this chapter we show that this strategy is in fact complete: if a proposition A has a natural deduction then it has a normal deduction. First, however, we need to make this strategy precise.

A general technique for representing proof search strategies is to introduce new judgments which permit only those derivations which can be found by the intended strategy. We then prove the correctness of the new, restricted judgments by appropriate soundness and completeness theorems.

In this case, we introduce two judgments:

$A \Uparrow$ Proposition A has a normal deduction, and
$A \downarrow$ Proposition A is extracted from a hypothesis.

They are defined by restricting the rules of natural deduction according to their status as introduction or elimination rules. Hypotheses can be trivially extracted. Therefore the necessary hypothetical judgments (in localized form, see Section 2.3) are
$u_1{:}A_1 \downarrow, \ldots, u_n{:}A_n \downarrow\ \vdash A \Uparrow$ and
$u_1{:}A_1 \downarrow, \ldots, u_n{:}A_n \downarrow\ \vdash A \downarrow$.
We write $\Gamma^{\downarrow}$ for a context of the form shown above.

Hypotheses. The general rule for hypotheses simply reflects the nature of hypothetical judgments.

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

Coercion. The bottom-up and top-down derivations must be able to meet in the middle.

$$\frac{\Gamma^{\downarrow} \vdash A \downarrow}{\Gamma^{\downarrow} \vdash A \Uparrow}\, {\downarrow}{\Uparrow}$$

Looked at another way, this rule allows us to coerce any extraction derivation to a normal deduction. Of course, the opposite coercion would contradict the intended strategy.

Conjunction. The rules for conjunction exhibit no unexpected features: the introduction rule is classified as a bottom-up rule, the elimination rule is classified as a top-down rule.

$$\frac{\Gamma^{\downarrow} \vdash A \Uparrow \qquad \Gamma^{\downarrow} \vdash B \Uparrow}{\Gamma^{\downarrow} \vdash A \wedge B \Uparrow}\, \wedge\mathrm{I}$$

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

Truth. For truth, there is only an introduction rule which is classified as normal.

$$\frac{}{\Gamma^{\downarrow} \vdash \top \Uparrow}\, \top\mathrm{I}$$

Implication. The introduction rule for implication is straightforward. In the elimination rule we require that the the second premise is normal. It is only the first premise (whose primary connective is eliminated in this rule) which must be extracted from a hypothesis.

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

Disjunction. The introduction rules for disjunction are straightforward. For the elimination rule, again the premise with the connective which is eliminated must have a top-down derivation. The new assumptions in each branch also are top-down derivations. Overall, for the derivation to be normal we must require the derivations of both premises to be normal.

$$\frac{\Gamma^{\downarrow} \vdash A \Uparrow}{\Gamma^{\downarrow} \vdash A \vee B \Uparrow}\,\vee\mathrm{I_L} \qquad \frac{\Gamma^{\downarrow} \vdash B \Uparrow}{\Gamma^{\downarrow} \vdash A \vee B \Uparrow}\,\vee\mathrm{I_R}$$

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

It would also be consistent to allow the derivations of C to be extractions, but it is not necessary to obtain a complete search procedure and complicates the relation to the sequent calculus (see Exercise 3.1).

Falsehood. Falsehood corresponds to a disjunction with no alternatives. Therefore there is no introduction rule, and the elimination rule has no cases. This consideration yields

$$\frac{\Gamma^{\downarrow} \vdash \bot \downarrow}{\Gamma^{\downarrow} \vdash C \Uparrow}\,\bot\mathrm{E}.$$

For this rule, it does not appear to make sense to allow the conclusion as having been constructed top-down, since the proposition C would be completely unrestricted.

Negation. Negation combines elements from implication and falsehood, since we may think of $\neg A$ as $A \supset \bot$.

$$\frac{\Gamma^{\downarrow}, u{:}A \downarrow\ \vdash p \Uparrow}{\Gamma^{\downarrow} \vdash \neg A \Uparrow}\,\neg\mathrm{I}^{p,u} \qquad \frac{\Gamma^{\downarrow} \vdash \neg A \downarrow \qquad \Gamma^{\downarrow} \vdash A \Uparrow}{\Gamma^{\downarrow} \vdash C \Uparrow}\,\neg\mathrm{E}$$

Universal Quantification. Universal quantification does not introduce any new considerations.

$$\frac{\Gamma^{\downarrow} \vdash [a/x]A \Uparrow}{\Gamma^{\downarrow} \vdash \forall x.\ A \Uparrow}\,\forall\mathrm{I}^{a} \qquad \frac{\Gamma^{\downarrow} \vdash \forall x.\ A \downarrow}{\Gamma^{\downarrow} \vdash [t/x]A \downarrow}\,\forall\mathrm{E}$$

Existential Quantification. Existential quantification is similar to disjunction and a more lenient view of extraction is possible here, too (see Exercise 3.1).

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

It is quite easy to see that normal and extraction derivations are sound with respect to natural deduction. In order to state and prove this theorem, we introduce some conventions. Given a context

$$\Gamma^{\downarrow} = u_1{:}A_1 \downarrow, \ldots, u_n{:}A_n \downarrow$$

we denote

$$u_1{:}A_1, \ldots, u_n{:}A_n$$

by Γ and vice versa.

Theorem 3.1 (Soundness of Normal Deductions)

1. *If* $\Gamma^{\downarrow} \vdash A \Uparrow$ *then* $\Gamma \vdash A$*, and*
2. *if* $\Gamma^{\downarrow} \vdash A \downarrow$ *then* $\Gamma \vdash A$.

Proof: By induction on the structure of the given derivations. We show only three cases, since the proof is absolutely straightforward.

Case:

$$\mathcal{E} = \frac{}{\Gamma_1^{\downarrow}, u{:}A \downarrow, \Gamma_2^{\downarrow} \vdash A \downarrow}\, u$$

The we construct directly $\Gamma_1, u{:}A, \Gamma_2 \vdash A$.

Case:

$$\mathcal{N} = \frac{\begin{array}{c}\mathcal{E}\\ \Gamma^{\downarrow} \vdash A \downarrow\end{array}}{\Gamma^{\downarrow} \vdash A \Uparrow}\, {\downarrow\Uparrow}$$

Then $\Gamma \vdash A$ by induction hypothesis on $\mathcal{E}$.

Case:

$$\mathcal{N} = \frac{\begin{array}{c}\mathcal{N}_2\\ \Gamma^{\downarrow}, u{:}A_1 \downarrow\ \vdash A_2 \Uparrow\end{array}}{\Gamma^{\downarrow} \vdash A_1 \supset A_2 \Uparrow}\, {\supset}\mathrm{I}^u$$

$\Gamma, u{:}A_1 \vdash A_2$ By i.h. on $\mathcal{N}_2$

$\Gamma \vdash A_1 \supset A_2$ By rule $\supset$I

□

When trying to give a translation in the other direction we encounter a difficulty: certain patterns of inference cannot be annotated directly. For example, consider

$$\cfrac{\cfrac{\begin{array}{c}\mathcal{D}\\ \Gamma \vdash A\end{array} \qquad \begin{array}{c}\mathcal{E}\\ \Gamma \vdash B\end{array}}{\Gamma \vdash A \wedge B}\, \wedge\mathrm{I}}{\Gamma \vdash A}\, \wedge\mathrm{E_L}.$$

If we try to classify each judgment, we obtain a conflict:

$$\dfrac{\dfrac{\begin{array}{c}\mathcal{D}'\\ \Gamma \vdash A \Uparrow\end{array} \qquad\qquad \begin{array}{c}\mathcal{E}'\\ \Gamma \vdash B \Uparrow\end{array}}{\Gamma \vdash A \wedge B\ ?}\,\wedge\mathrm{I}}{\Gamma \vdash A \downarrow}\,\wedge\mathrm{E_L}.$$

In this particular case, we can avoid the conflict: in order to obtain the derivation of $A \Uparrow$ we can just translate the derivation $\mathcal{D}$ and avoid the final two inferences! In general, we can try to apply local reductions to the given original derivation until no situations of the form above remain. This approach is called *normalization*. It is not easy to prove that normalization terminates, and the situation is complicated by the fact that the local reductions alone do not suffice to transform an arbitrary natural deduction into normal form (see Exercise 3.2).

Here, we follow an alternative approach to prove completeness of normal deductions. First, we temporarily augment the system with another rule which makes the translation from natural deductions immediate. Then we relate the resulting system to a sequent calculus and show that the additional rule was redundant.

A candidate for the additional rule is easy to spot: we just add the missing coercion from normal to extraction deductions. Since all rules are present, we can just coerce back and forth as necessary in order to obtain a counterpart for any natural deduction in this extended system. Of course, the resulting derivations are no longer normal, which we indicate by decorating the turnstile with a "+". The judgments $\Gamma^{\downarrow} \vdash^{+} A \Uparrow$ and $\Gamma^{\downarrow} \vdash^{+} A \downarrow$ are defined by all counterparts of all rules which define normal and extracting derivations, plus the rule

$$\dfrac{\Gamma^{\downarrow} \vdash^{+} A \Uparrow}{\Gamma^{\downarrow} \vdash^{+} A \downarrow}\,{\Uparrow\downarrow}$$

Now the annotation in the example above can be completed.

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}\mathcal{D}'\\ \Gamma \vdash^{+} A \Uparrow\end{array} \qquad\qquad \begin{array}{c}\mathcal{E}'\\ \Gamma \vdash^{+} B \Uparrow\end{array}}{\Gamma \vdash^{+} A \wedge B \Uparrow}\,\wedge\mathrm{I}}{\Gamma \vdash^{+} A \wedge B \downarrow}\,{\Uparrow\downarrow}}{\Gamma \vdash^{+} A \downarrow}\,\wedge\mathrm{E_L}$$

Both soundness and completeness of the extended calculus with respect to natural deduction is easy to see.

Theorem 3.2 (Soundness of Annotated Deductions)

1. *If* $\Gamma^{\downarrow} \vdash^{+} A \Uparrow$ *then* $\Gamma \vdash A$*, and*

2. *if* $\Gamma^{\downarrow} \vdash^{+} A \downarrow$ *then* $\Gamma \vdash A$.

Proof: By simultaneous induction over the structure of the given derivations. □

The constructive proof of the completeness theorem below will contain an algorithm for annotating a given natural deduction.

Theorem 3.3 (Completeness of Annotated Deductions)

1. *If* $\Gamma \vdash A$ *then* $\Gamma^{\downarrow} \vdash^{+} A \Uparrow$*, and*
2. *if* $\Gamma \vdash A$ *then* $\Gamma^{\downarrow} \vdash^{+} A \downarrow$.

Proof: By induction over the structure of the given derivation. We show only two cases.

Case:

$$\mathcal{D} = \cfrac{\begin{array}{c}\mathcal{D}\\ \Gamma \vdash B \supset A\end{array} \qquad \begin{array}{c}\mathcal{E}\\ \Gamma \vdash B\end{array}}{\Gamma \vdash A}\,{\supset}\mathrm{E}$$

$\Gamma^{\downarrow} \vdash^{+} B \supset A \downarrow$	By i.h. (2) on $\mathcal{D}$
$\Gamma^{\downarrow} \vdash^{+} B \Uparrow$	By i.h. (1) on $\mathcal{E}$
$\Gamma^{\downarrow} \vdash^{+} A \downarrow$	By rule $\supset$E, proving (2)
$\Gamma^{\downarrow} \vdash^{+} A \Uparrow$	By rule $\downarrow\Uparrow$, proving (1)

Case:

$$\mathcal{D} = \cfrac{\begin{array}{c}\mathcal{D}_2\\ \Gamma, u{:}A_1 \vdash A_2\end{array}}{\Gamma \vdash A_1 \supset A_2}\,{\supset}\mathrm{I}^{u}$$

$\Gamma^{\downarrow}, u{:}A_1 \downarrow \vdash^{+} A_2 \Uparrow$	By i.h. (1) on $\mathcal{D}_2$
$\Gamma^{\downarrow} \vdash^{+} A_1 \supset A_2 \Uparrow$	By rule $\supset\mathrm{I}^{u}$, proving (1)
$\Gamma^{\downarrow} \vdash^{+} A_1 \supset A_2 \downarrow$	By rule $\Uparrow\downarrow$, proving (2)

□

Even though natural deductions and annotated deductions are very similar, they are not in bijective correspondence. For example, in an annotated deduction we can simply alternate the two coercions an arbitrary number of times. Under the translation to natural deduction, all of these are identified.

Before we introduce the sequent calculus, we make a brief excursion to study the impact of annotations on proof terms.

3.2 Compact Proof Terms

The proof terms introduced in Section 2.4 sometimes contain significant amounts of redundant information. The reason are the propositions which label λ-abstractions and also occur in the inl^A, inr^A, $\mu^p u{:}A$, $\cdot_A$, and abort^A constructs. For example, assume we are given a proof term $\lambda u{:}A.\ M$ and we are supposed to check if it represents a proof of $A' \supset B$. We then have to check that $A = A'$ and, moreover, the information is duplicated. The reason for this duplication was the intended invariant that every term proves a unique proposition. Under the interpretations of propositions as types, this means we can always synthesize a unique type for every valid term. However, we can improve this if we alternate between synthesizing a type and checking a term against a given type.

Therefore we introduce two classes of terms: those whose type can be synthesized, and those which can be checked against a type. Interestingly, this corresponds precisely with the annotations as introduction or elimination rules given above. We ignore negation again, thinking of $\neg A$ as $A \supset \bot$. We already discussed why the eliminations for disjunction and falsehood appear among the intro terms.

Intro Terms	I	$::=$	$\langle I_1, I_2 \rangle$	Conjunction
			$\mid \lambda u.\ I$	Implication
			$\mid \mathrm{inl}\, I \mid \mathrm{inr}\, I$	Disjunction
			$\mid (\,\textbf{case}\ E\ \textbf{of}\ \mathrm{inl}\, u_1 \Rightarrow I_1 \mid \mathrm{inr}\, u_2 \Rightarrow I_2)$	
			$\mid \langle\,\rangle$	Truth
			$\mid \mathrm{abort}\, E$	Falsehood
			$\mid E$	Coercion
Elim Terms	E	$::=$	u	Hypotheses
			$\mid E\, I$	Implication
			$\mid \mathrm{fst}\, E \mid \mathrm{snd}\, E$	Conjunction
			$\mid (I : A)$	Coercion

The presence of E as an intro term corresponds to the coercion $\downarrow\Uparrow$ which is present in normal deductions. The presence of $(I : A)$ as an elim term corresponds to the coercion $\Uparrow\downarrow$ which is present only in the extended system. Therefore, a normal deduction can be represented without any internal type information, while a general deduction requires information at the point where an introduction rule is directly followed by an elimination rule. It is easy to endow the annotated natural deduction judgments with the modified proof terms from above. We leave the details to Exercise 3.3. The two judgments are $\Gamma^{\downarrow} \vdash^{+} I : A \Uparrow$ and $\Gamma^{\downarrow} \vdash^{+} E : A \downarrow$.

Now we can prove the correctness of bi-directional type-checking.

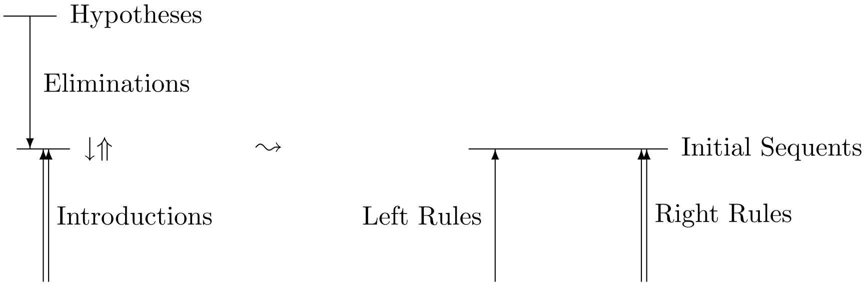
Theorem 3.4 (Bi-Directional Type-Checking)

1. *Given $\Gamma^{\downarrow}$, I, and A. Then either $\Gamma^{\downarrow} \vdash^{+} I : A \Uparrow$ or not.*
2. *Given $\Gamma^{\downarrow}$ and E. Then either there is a unique A such that $\Gamma^{\downarrow} \vdash^{+} E : A \downarrow$ or there is no such A.*

Proof: See Exercise 3.3. □

3.3 Sequent Calculus

In Section 3.1 we introduced normal deductions which embody the strategy that proof search should proceed only bottom-up via introduction rules and top-down via elimination rules. The bi-directional nature of this calculus makes it somewhat unwieldy when it comes to the study of meta-theoretic properties and, in particular, complicates its completeness proof. In this section we develop a closely related calculus in which all proof search steps proceed bottom-up. Pictorially, we would like to flip the elimination rules upside-down.



This transformation turns introduction rules into so-called right rules, and upside-down elimination rules into so-called left rules. We have two judgments, *A left* (*A* is a proposition on the left) and *A right* (*A* is a proposition on the right). They are assembled into the form of a hypothetical judgment

$$u_1{:}A_1\ \mathit{left}, \ldots, u_n{:}A_n\ \mathit{left} \vdash A\ \mathit{right}.$$

We call such a hypothetical judgment a *sequent.*

Note that the proposition A on the right directly corresponds to the proposition whose truth is established by a natural deduction. On the other hand, propositions on the left do *not* directly correspond to hypotheses in natural deduction, since in general they include hypotheses and propositions derived from them by elimination rules.

Keeping this intuition in mind, the inference rules for sequents can now be constructed mechanically from the rules for normal and extracting derivations. To simplify the notation, we denote the sequent above by

$$A_1, \ldots, A_n \Longrightarrow A$$

where the judgments *left* and *right* are implied by the position of the propositions. Moreover, labels u_i are suppressed until we introduce proof terms. Finally, left rules may be applied to any left proposition. Since the order of the left propositions is irrelevant, we write Γ, A instead of the more pedantic Γ, A, Γ'.

Initial Sequents. These correspond to the coercion from extraction to normal derivations, and *not* to the use of hypotheses in natural deductions.

$$\frac{}{\Gamma, A \Longrightarrow A}\,\mathrm{init}$$

Conjunction. The right and left rules are straightforward and provide a simple illustration of the translation, in particular in the way the elimination rules are turned upside-down.

$$\frac{\Gamma \Longrightarrow A \qquad \Gamma \Longrightarrow B}{\Gamma \Longrightarrow A \wedge B}\,\wedge\mathrm{R}$$

$$\frac{\Gamma, A \wedge B, A \Longrightarrow C}{\Gamma, A \wedge B \Longrightarrow C}\,\wedge\mathrm{L}_1 \qquad \frac{\Gamma, A \wedge B, B \Longrightarrow C}{\Gamma, A \wedge B \Longrightarrow C}\,\wedge\mathrm{L}_2$$

In the introduction rule (read bottom-up), we propagate Γ to both premises. This reflects that in natural deduction we can use any available assumption freely in both subdeductions. Furthermore, in the elimination rule the hypothesis $A \wedge B$ *left* persists. This reflects that assumptions in natural deduction may be used more than once. Later we analyze which of these hypotheses are actually needed and eliminate some redundant ones. For now, however, they are useful because they allow us to give a very direct translation to and from normal natural deductions.

Implication. The right rule for implication is straightforward. The left rule requires some thought. Using an extracted implication $A \supset B$ gives rise to two subgoals: we have to find a normal proof of A, but we also still have to prove our overall goal, now with the additional extracted proposition B.

$$\frac{\Gamma, A \Longrightarrow B}{\Gamma \Longrightarrow A \supset B}\,{\supset}\mathrm{R} \qquad \frac{\Gamma, A \supset B \Longrightarrow A \qquad \Gamma, A \supset B, B \Longrightarrow C}{\Gamma, A \supset B \Longrightarrow C}\,{\supset}\mathrm{L}$$

Disjunction. This introduces no new considerations.

$$\frac{\Gamma \Longrightarrow A}{\Gamma \Longrightarrow A \vee B}\,\vee\mathrm{R}_1 \qquad \frac{\Gamma \Longrightarrow B}{\Gamma \Longrightarrow A \vee B}\,\vee\mathrm{R}_2$$

$$\frac{\Gamma, A \vee B, A \Longrightarrow C \qquad \Gamma, A \vee B, B \Longrightarrow C}{\Gamma, A \vee B \Longrightarrow C}\,\vee\mathrm{L}$$

Negation. Negation requires a judgment parametric in a proposition. Sometimes, this is encoded as an empty right-hand side (see Exercise 3.6).

$$\frac{\Gamma, A \Longrightarrow p}{\Gamma \Longrightarrow \neg A}\,\neg\mathrm{R}^p \qquad \frac{\Gamma, \neg A \Longrightarrow A}{\Gamma, \neg A \Longrightarrow C}\,\neg\mathrm{L}$$

Truth. By our general method, there is no left rule, only a right rule which models the introduction rule.

$$\frac{}{\Gamma \Longrightarrow \top}\ \top\mathrm{R}$$

Falsehood. Again by our general method, there is no right rule, only a left rule which models the (upside-down) elimination rule.

$$\frac{}{\Gamma, \bot \Longrightarrow C}\ \bot\mathrm{L}$$

Universal Quantification. These require only a straightforward transcription, with the appropriate translation of the side condition.

$$\frac{\Gamma \Longrightarrow [a/x]A}{\Gamma \Longrightarrow \forall x.\ A}\ \forall\mathrm{R}^a \qquad \frac{\Gamma, \forall x.\ A, [t/x]A \Longrightarrow C}{\Gamma, \forall x.\ A \Longrightarrow C}\ \forall\mathrm{L}$$

Existential Quantification. Again, the rules can be directly constructed from the introduction and elimination rule of natural deduction.

$$\frac{\Gamma \Longrightarrow [t/x]A}{\Gamma \Longrightarrow \exists x.\ A}\ \exists\mathrm{R} \qquad \frac{\Gamma, \exists x.\ A, [a/x]A \Longrightarrow C}{\Gamma, \exists x.\ A \Longrightarrow C}\ \exists\mathrm{L}^a$$

The intended theorem describing the relationship between sequent calculus and natural deduction states that $\Gamma^{\downarrow} \vdash A \Uparrow$ if and only if $\Gamma \Longrightarrow A$. *Prima facie* is unlikely that we can prove either of these directions without further generalization, since the judgments $\Gamma^{\downarrow} \vdash A \Uparrow$ and $\Gamma^{\downarrow} \vdash A \downarrow$ are mutually recursive, and the statement above does not even mention the latter.

In preparation for the upcoming proof, we recall the general property of hypothetical judgments, namely that we can substitute a derivation of the appropriate judgment for a hypothesis. When applied to normal and extracting derivations, this yields the following property.

Lemma 3.5 (Substitution Property for Extractions)

1. *If* $\Gamma_1^{\downarrow}, u{:}A \downarrow, \Gamma_2^{\downarrow} \vdash C \Uparrow$ *and* $\Gamma_1^{\downarrow} \vdash A \downarrow$ *then* $\Gamma_1^{\downarrow}, \Gamma_2^{\downarrow} \vdash C \Uparrow$.

2. *If* $\Gamma_1^{\downarrow}, u{:}A \downarrow, \Gamma_2^{\downarrow} \vdash C \downarrow$ *and* $\Gamma_1^{\downarrow} \vdash A \downarrow$ *then* $\Gamma_1^{\downarrow}, \Gamma_2^{\downarrow} \vdash C \downarrow$.

Proof: By induction on the structure of the given derivations of $C \Uparrow$ and $C \downarrow$. In the case where the hypothesis is used we employ weakening, that is, we adjoin the additional hypotheses $\Gamma_2^{\downarrow}$ to every judgment in the derivation of $\Gamma_1^{\downarrow} \vdash A \downarrow$. □

Using this lemma, a direct proof goes through (somewhat surprisingly).

Theorem 3.6 (Soundness of Sequent Calculus)
If $\Gamma \Longrightarrow C$ *then* $\Gamma^{\downarrow} \vdash C \Uparrow$.

Proof: By induction on the structure of the given derivation $\mathcal{S}$. We show a few representative cases.

Case: Initial sequents.

$$\frac{}{\Gamma, C \Longrightarrow C}\,\text{init}$$

$$\begin{array}{ll}
\Gamma^{\downarrow}, u{:}C \downarrow\ \vdash C \downarrow & \text{By hypothesis } u \\
\Gamma^{\downarrow}, u{:}C \downarrow\ \vdash C \Uparrow & \text{By rule } {\downarrow}{\Uparrow}
\end{array}$$

This case confirms that initial sequents correspond to the coercion from extractions to normal deductions.

Case: Implication right rule.

$$\frac{\begin{array}{c}\mathcal{S}_2\\ \Gamma, C_1 \Longrightarrow C_2\end{array}}{\Gamma \Longrightarrow C_1 \supset C_2}\,{\supset}\text{R}$$

$$\begin{array}{ll}
\Gamma^{\downarrow}, u{:}C_1 \downarrow\ \vdash C_2 \Uparrow & \text{By i.h. on } \mathcal{S}_2 \\
\Gamma^{\downarrow} \vdash C_1 \supset C_2 \Uparrow & \text{By rule } {\supset}\text{I}^u
\end{array}$$

This case exemplifies how right rules correspond directly to introduction rules.

Case: Implication left rule.

$$\frac{\begin{array}{c}\mathcal{S}_1\\ \Gamma, A_1 \supset A_2 \Longrightarrow A_1\end{array} \qquad \begin{array}{c}\mathcal{S}_2\\ \Gamma, A_1 \supset A_2, A_2 \Longrightarrow C\end{array}}{\Gamma, A_1 \supset A_2 \Longrightarrow C}\,{\supset}\text{L}$$

$$\begin{array}{ll}
\Gamma^{\downarrow}, u{:}A_1 \supset A_2 \downarrow\ \vdash A_1 \Uparrow & \text{By i.h. on } \mathcal{S}_1 \\
\Gamma^{\downarrow}, u{:}A_1 \supset A_2 \downarrow\ \vdash A_1 \supset A_2 \downarrow & \text{By hypothesis } u \\
\Gamma^{\downarrow}, u{:}A_1 \supset A_2 \downarrow\ \vdash A_2 \downarrow & \text{By rule } {\supset}\text{E} \\
\Gamma^{\downarrow}, u{:}A_1 \supset A_2 \downarrow, w{:}A_2 \downarrow\ \vdash C \Uparrow & \text{By i.h. on } \mathcal{S}_2 \\
\Gamma^{\downarrow}, u{:}A_1 \supset A_2 \downarrow\ \vdash C \Uparrow & \text{By substitution property (Lemma 3.5)}
\end{array}$$

This case illustrates how left rules correspond to elimination rules. The general pattern is that the result of applying the appropriate elimination rule is substituted for a hypothesis.

□

The proof of completeness is somewhat trickier—we first need to generalize the induction hypothesis. Generalizing a desired theorem so that a direct inductive proof is possible often requires considerable ingenuity and insight into the problem. In this particular case, the generalization is of medium difficulty.

The reader who has not seen the proof is invited to test his understanding by carrying out the generalization and proof himself before reading on.

The nature of a sequent as a hypothetical judgment gives rise to several general properties we will take advantage of. We make two of them, weakening and contraction, explicit in the following lemma.

Lemma 3.7 (Structural Properties of Sequents)

1. *(Weakening) If* $\Gamma \Longrightarrow C$ *then* $\Gamma, A \Longrightarrow C$.
2. *(Contraction) If* $\Gamma, A, A \Longrightarrow C$ *then* $\Gamma, A \Longrightarrow C$.

Proof: First, recall our general convention that we consider the hypotheses of a sequent modulo permutation. We prove each property by a straightforward induction over the structure of the derivation. In the case of weakening we adjoin an unused hypothesis $A\,\mathit{left}$ to each sequent in the derivation. In the case of contraction we replace any use of either of the two hypotheses by a common hypothesis. □

The theorem below only establishes the completeness of sequent derivations with respect to normal deductions. That is, at this point we have not established the completeness of sequents with respect to arbitrary natural deductions which is more difficult.

Theorem 3.8 (Completeness of Sequent Derivations)

1. *If* $\Gamma^{\downarrow} \vdash C \Uparrow$ *then* $\Gamma \Longrightarrow C$.
2. *If* $\Gamma^{\downarrow} \vdash A \downarrow$ *and* $\Gamma, A \Longrightarrow C$ *then* $\Gamma \Longrightarrow C$.

Proof: By induction on the structure of the given derivations $\mathcal{I}$ and $\mathcal{E}$. We show some representative cases.

Case: Use of hypotheses.

$$\mathcal{E} = \cfrac{}{\Gamma_1^{\downarrow}, u{:}A \downarrow, \Gamma_2^{\downarrow} \vdash A \downarrow}\, u$$

$\Gamma_1, A, \Gamma_2, A \Longrightarrow C$ Assumption
$\Gamma_1, A, \Gamma_2 \Longrightarrow C$ By contraction (Lemma 3.7)

Case: Coercion.

$$\mathcal{I} = \cfrac{\begin{matrix}\mathcal{E}\\ \Gamma^{\downarrow} \vdash C \downarrow\end{matrix}}{\Gamma^{\downarrow} \vdash C \Uparrow}\, {\downarrow}{\Uparrow}$$

$\Gamma, C \Longrightarrow C$ By rule init
$\Gamma \Longrightarrow C$ By i.h. on $\mathcal{E}$

Case: Implication introduction.

$$\mathcal{I} = \dfrac{\overset{\mathcal{I}_2}{\Gamma^{\downarrow}, u{:}C_1 \downarrow\, \vdash C_2 \Uparrow}}{\Gamma^{\downarrow} \vdash C_1 \supset C_2 \Uparrow}\,{\supset}\mathrm{I}^u$$

$\Gamma, C_1 \Longrightarrow C_2$	By i.h. on $\mathcal{I}_2$
$\Gamma \Longrightarrow C_1 \supset C_2$	By rule ${\supset}$R

Case: Implication elimination.

$$\mathcal{E} = \dfrac{\overset{\mathcal{E}_2}{\Gamma^{\downarrow} \vdash A_1 \supset A_2 \downarrow} \qquad \overset{\mathcal{I}_1}{\Gamma^{\downarrow} \vdash A_1 \Uparrow}}{\Gamma^{\downarrow} \vdash A_2 \downarrow}\,{\supset}\mathrm{E}$$

$\Gamma, A_2 \Longrightarrow C$	Assumption
$\Gamma, A_1 \supset A_2, A_2 \Longrightarrow C$	By weakening (Lemma 3.7)
$\Gamma \Longrightarrow A_1$	By i.h. on $\mathcal{I}_1$
$\Gamma, A_1 \supset A_2 \Longrightarrow A_1$	By weakening (Lemma 3.7)
$\Gamma, A_1 \supset A_2 \Longrightarrow C$	By rule ${\supset}$L
$\Gamma \Longrightarrow C$	By i.h. on $\mathcal{E}_2$

□

In order to establish soundness and completeness with respect to arbitrary natural deductions we establish a connection to annotated natural deductions. Recall that this is an extension of normal deductions which we showed sound and complete with respect to arbitrary natural deduction in Theorems 3.2 and 3.3. We related annotated natural deductions to the sequent calculus by adding a rule called cut.

We write the extended judgment of sequent derivations with cut as $\Gamma \stackrel{+}{\Longrightarrow} C$. It is defined by copies of all the rules for $\Gamma \Longrightarrow C$, plus the rule of cut:

$$\dfrac{\Gamma \stackrel{+}{\Longrightarrow} A \qquad \Gamma, A \stackrel{+}{\Longrightarrow} C}{\Gamma \stackrel{+}{\Longrightarrow} C}\,\mathrm{cut}$$

Thought of from the perspective of bottom-up proof construction, this rule corresponds to proving and then assuming a lemma A during a derivation.

Theorem 3.9 (Soundness of Sequent Calculus with Cut)
If $\Gamma \stackrel{+}{\Longrightarrow} C$ *then* $\Gamma^{\downarrow} \vdash^{+} C \Uparrow$.

Proof: As in Theorem 3.6 by induction on the structure of the given derivation $\mathcal{S}$, with one additional case.

Case: Cut.

$$\mathcal{S} = \frac{\overset{\mathcal{S}_1}{\Gamma \Longrightarrow A} \qquad \overset{\mathcal{S}_2}{\Gamma, A \Longrightarrow C}}{\Gamma \Longrightarrow C}\,\text{cut}$$

$\Gamma^{\downarrow} \vdash^{+} A \Uparrow$	By i.h. on $\mathcal{S}_1$
$\Gamma^{\downarrow} \vdash^{+} A \downarrow$	By rule $\Uparrow\downarrow$
$\Gamma^{\downarrow}, u{:}A \downarrow \ \vdash^{+} C \Uparrow$	By i.h. on $\mathcal{S}_2$
$\Gamma^{\downarrow} \vdash^{+} C \Uparrow$	By substitution (Lemma 3.5, generalized)

We see that, indeed, cut corresponds to the coercion from normal to extraction derivations.

□

Theorem 3.10 (Completeness of Sequent Calculus with Cut)

1. *If* $\Gamma^{\downarrow} \vdash^{+} C \Uparrow$ *then* $\Gamma \overset{+}{\Longrightarrow} C$.

2. *If* $\Gamma^{\downarrow} \vdash^{+} A \downarrow$ *and* $\Gamma, A \overset{+}{\Longrightarrow} C$ *then* $\Gamma \overset{+}{\Longrightarrow} C$.

Proof: As in the proof of Theorem 3.10 with one additional case.

Case: Coercion from normal to extraction derivations.

$$\mathcal{E} = \frac{\overset{\mathcal{I}}{\Gamma^{\downarrow} \vdash^{+} A \Uparrow}}{\Gamma^{\downarrow} \vdash^{+} A \downarrow}\,\Uparrow\downarrow$$

$\Gamma \Longrightarrow A$	By i.h. on $\mathcal{I}$
$\Gamma, A \Longrightarrow C$	By assumption
$\Gamma \Longrightarrow C$	By rule cut

□

The central property of the sequent calculus is that the cut rule is redundant. That is, if $\Gamma \overset{+}{\Longrightarrow} C$ then $\Gamma \Longrightarrow C$. This so-called cut elimination theorem (Gentzen's *Hauptsatz* [Gen35]) is one of the central theorems of logic. As an immediately consequence we can see that not every proposition has a proof, since no rule is applicable to derive $\cdot \Longrightarrow \bot$. In the system with cut, a derivation of this sequent might end in the cut rule and consistency is not at all obvious. The proof of cut elimination and some of its many consequences are the subject of the next section.

3.4 Cut Elimination

This section is devoted to proving that the rule of cut is redundant in the sequent calculus. First we prove that cut is *admissible*: whenever the premises of the cut rule are derivable in the sequent calculus *without cut*, then the conclusion is. It is a simple observation that adding an admissible rule to a deductive system does not change the derivable judgments. Formally, this second step is an induction over the structure of a derivation that may contain cuts, proving that if $\Gamma \overset{+}{\Longrightarrow} C$ then $\Gamma \Longrightarrow C$.

There is a stronger property we might hope to prove for cut: it could be a *derived* rule of inference. Derived rules have a direct deduction of the conclusion from the premises within the given system. For example,

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B \qquad \Gamma \vdash C}{\Gamma \vdash A \wedge (B \wedge C)}$$

is a derived rule, as evidenced by the following deduction:

$$\frac{\Gamma \vdash A \qquad \dfrac{\Gamma \vdash B \qquad \Gamma \vdash C}{\Gamma \vdash B \wedge C}\wedge\mathrm{I}}{\Gamma \vdash A \wedge (B \wedge C)}\wedge\mathrm{I}.$$

Derived rules have the property that they remain valid under all extensions of a given system. Admissible rules, on the other hand, have to be reconsidered when new connectives or inference rules are added to a system, since these rules may invalidate the proof of admissibility.

It turns out that cut is only admissible, but not derivable in the sequent calculus. Therefore, we will prove the following theorem:

If $\Gamma \Longrightarrow A$ *and* $\Gamma, A \Longrightarrow C$ *then* $\Gamma \Longrightarrow C$.

We call A the *cut formula*. Also, each left or right rule in the sequent calculus focuses on an occurrence of a proposition in the conclusion, called the *principal formula* of the inference.

The proof combines two ideas: induction over the structure of the cut formula with induction over the structures of the two given derivations. They are combined into one nested induction: an outer induction over the structure of the cut formula and an inner induction over the structure of the derivations of the premises. The outer induction over the structure of the cut formula is related to local reductions in natural deduction (see Exercise 3.7).

Theorem 3.11 (Admissibility of Cut)
If $\Gamma \Longrightarrow A$ *and* $\Gamma, A \Longrightarrow C$ *then* $\Gamma \Longrightarrow C$.

Proof: By nested inductions on the structure of A, the derivation $\mathcal{D}$ of $\Gamma \Longrightarrow A$ and $\mathcal{E}$ of $\Gamma, A \Longrightarrow C$. More precisely, we appeal to the induction hypothesis either with a strictly smaller cut formula, or with an identical cut formula and two derivations, one of which is strictly smaller while the other stays the same. The proof is constructive, which means we show how to transform

$$\begin{array}{c}\mathcal{D}\\ \Gamma \Longrightarrow A\end{array} \quad\text{and}\quad \begin{array}{c}\mathcal{E}\\ \Gamma, A \Longrightarrow C\end{array} \quad\text{to}\quad \begin{array}{c}\mathcal{F}\\ \Gamma \Longrightarrow C.\end{array}$$

The proof is divided into several classes of cases. More than one case may be applicable, which means that the algorithm for constructing the derivation of $\Gamma \Longrightarrow C$ from the two given derivations is naturally non-deterministic.

Case: $\mathcal{D}$ is an initial sequent.

$$\mathcal{D} = \frac{}{\Gamma', A \Longrightarrow A}\,\text{init}$$

$\Gamma = \Gamma', A$	This case
$\Gamma', A, A \Longrightarrow C$	Derivation $\mathcal{E}$
$\Gamma', A \Longrightarrow C$	By contraction (Lemma 3.7)
$\Gamma \Longrightarrow C$	By equality

Case: $\mathcal{E}$ is an initial sequent using the cut formula.

$$\mathcal{E} = \frac{}{\Gamma, A \Longrightarrow A}\,\text{init}$$

$C = A$	This case
$\Gamma \Longrightarrow A$	Derivation $\mathcal{D}$

Case: $\mathcal{E}$ is an initial sequent not using the cut formula.

$$\mathcal{E} = \frac{}{\Gamma', C, A \Longrightarrow C}\,\text{init}$$

$\Gamma = \Gamma', C$	This case
$\Gamma', C \Longrightarrow C$	By rule init
$\Gamma \Longrightarrow C$	By equality

Case: A is the principal formula of the final inference in both $\mathcal{D}$ and $\mathcal{E}$. There are a number of subcases to consider, based on the last inference in $\mathcal{D}$ and $\mathcal{E}$. We show some of them.

Subcase:

$$\mathcal{D} = \frac{\begin{array}{c}\mathcal{D}_1\\ \Gamma \Longrightarrow A_1\end{array} \qquad \begin{array}{c}\mathcal{D}_2\\ \Gamma \Longrightarrow A_2\end{array}}{\Gamma \Longrightarrow A_1 \wedge A_2}\,\wedge\text{R}$$

$$\text{and}\mathcal{E} = \frac{\begin{array}{c}\mathcal{E}_1\\ \Gamma, A_1 \wedge A_2, A_1 \Longrightarrow C\end{array}}{\Gamma, A_1 \wedge A_2 \Longrightarrow C}\,\wedge\text{L}_1$$

$\Gamma, A_1 \Longrightarrow C$ By i.h. on $A_1 \wedge A_2$, $\mathcal{D}$ and $\mathcal{E}_1$
$\Gamma \Longrightarrow C$ By i.h. on A_1 from above and $\mathcal{D}_1$

Actually we have ignored a detail: in the first appeal to the induction hypothesis, $\mathcal{E}_1$ has an additionaly hypothesis (A_1 *left*) and therefore does not match the statement of the theorem precisely. However, we can always weaken $\mathcal{D}$ to include this additional hypothesis without changing the structure of $\mathcal{D}$ (see the proof of Lemma 3.7) and then appeal to the induction hypothesis. We will not be explicit about these trivial weakening steps in the remaining cases.

Subcase:

$$\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}_2\\ \Gamma, A_1 \Longrightarrow A_2\end{array}}{\Gamma \Longrightarrow A_1 \supset A_2}\supset\!\mathrm{R}$$

$$\text{and} \quad \mathcal{E} = \dfrac{\begin{array}{c}\mathcal{E}_1\\ \Gamma, A_1 \supset A_2 \Longrightarrow A_1\end{array} \qquad \begin{array}{c}\mathcal{E}_2\\ \Gamma, A_1 \supset A_2, A_2 \Longrightarrow C\end{array}}{\Gamma, A_1 \supset A_2 \Longrightarrow C}\supset\!\mathrm{L}$$

$\Gamma \Longrightarrow A_1$ By i.h. on $A_1 \supset A_2$, $\mathcal{D}$ and $\mathcal{E}_1$
$\Gamma \Longrightarrow A_2$ By i.h. on A_1 from above and $\mathcal{D}_2$
$\Gamma, A_2 \Longrightarrow C$ By i.h. on $A_1 \supset A_2$, $\mathcal{D}$ and $\mathcal{E}_2$
$\Gamma \Longrightarrow C$ By i.h. on A_2 from above

Subcase:

$$\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma, A_1 \Longrightarrow p\end{array}}{\Gamma \Longrightarrow \neg A_1}\neg\mathrm{R}^p$$

$$\text{and} \quad \mathcal{E} = \dfrac{\begin{array}{c}\mathcal{E}_1\\ \Gamma, \neg A_1 \Longrightarrow A_1\end{array}}{\Gamma, \neg A_1 \Longrightarrow C}\neg\mathrm{L}$$

$\Gamma \Longrightarrow A_1$ By i.h. on $\mathcal{D}$ and $\mathcal{E}_1$
$\Gamma, A_1 \Longrightarrow C$ By substitution for parameter C in $\mathcal{D}_1$
$\Gamma \Longrightarrow C$ By i.h. on A_1 from above

Note that the condition that p be a new parameter in $\mathcal{D}_1$ is necessary to guarantee that in the substitution step above we have $[C/p]A_1 = A_1$ and $[C/p]\Gamma = \Gamma$.

Subcase:

$$\mathcal{D} = \cfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma \Longrightarrow [t/x]A_1\end{array}}{\Gamma \Longrightarrow \exists x.\ A_1}\,\exists\mathrm{R}$$

$$\text{and}\quad \mathcal{E} = \cfrac{\begin{array}{c}\mathcal{E}_1\\ \Gamma, \exists x.\ A_1, [a/x]A_1 \Longrightarrow C\end{array}}{\Gamma, \exists x.\ A_1 \Longrightarrow C}\,\exists\mathrm{L}^a$$

$\Gamma, [t/x]A_1 \Longrightarrow C$	By substitution for parameter a in $\mathcal{E}_1$
$\Gamma, [t/x]A_1 \Longrightarrow C$	By i.h. on $\exists x.\ A_1$, $\mathcal{D}$ and $[t/a]\mathcal{E}_1$
$\Gamma \Longrightarrow C$	By i.h. on $[t/x]A_1$ from $\mathcal{D}_1$ and above

Note that this case requires that $[t/x]A_1$ is considered smaller than $\exists x.\ A_1$. Formally, this can be justified by counting the number of quantifiers and connectives in a proposition and noting that the term t does not contain any. A similar remark applies to check that $[t/a]\mathcal{E}_1$ is smaller than $\mathcal{E}$. Also note how the side condition that a must be a new parameter in the $\exists$L rule is required in the substitution step to conclude that $[t/a]\Gamma = \Gamma$, $[t/a][a/x]A_1 = [t/x]A_1$, and $[t/a]C$.

Case: A is not the principal formula of the last inference in $\mathcal{D}$. In that case $\mathcal{D}$ must end in a left rule and we can appeal to the induction hypothesis on one of its premises. We show some of the subcases.

Subcase:

$$\mathcal{D} = \cfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma', B_1 \wedge B_2, B_1 \Longrightarrow A\end{array}}{\Gamma', B_1 \wedge B_2 \Longrightarrow A}\,\wedge\mathrm{L}_1$$

$\Gamma = \Gamma', B_1 \wedge B_2$	This case
$\Gamma', B_1 \wedge B_2, B_1 \Longrightarrow C$	By i.h. on A, $\mathcal{D}_1$ and $\mathcal{E}$
$\Gamma', B_1 \wedge B_2 \Longrightarrow C$	By rule $\wedge\mathrm{L}_1$
$\Gamma \Longrightarrow C$	By equality

Subcase:

$$\mathcal{D} = \cfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma', B_1 \supset B_2 \Longrightarrow B_1\end{array} \qquad \begin{array}{c}\mathcal{D}_2\\ \Gamma', B_1 \supset B_2, B_2 \Longrightarrow A\end{array}}{\Gamma', B_1 \supset B_2 \Longrightarrow A}\,\supset\mathrm{L}$$

$\Gamma = \Gamma', B_1 \supset B_2$	This case
$\Gamma', B_1 \supset B_2, B_2 \Longrightarrow C$	By i.h. on A, $\mathcal{D}_2$ and $\mathcal{E}$
$\Gamma', B_2 \supset B_2 \Longrightarrow C$	By rule $\supset$L on $\mathcal{D}_1$ and above
$\Gamma \Longrightarrow C$	By equality

Case: A is not the principal formula of the last inference in $\mathcal{E}$. This overlaps with the previous case, since A may not be principal on either side. In this case, we appeal to the induction hypothesis on the subderivations of $\mathcal{E}$ and directly infer the conclusion from the results. We show some of the subcases.

Subcase:

$$\mathcal{E} = \dfrac{\begin{matrix}\mathcal{E}_1 \\ \Gamma, A \Longrightarrow C_1\end{matrix} \qquad \begin{matrix}\mathcal{E}_2 \\ \Gamma, A \Longrightarrow C_2\end{matrix}}{\Gamma, A \Longrightarrow C_1 \wedge C_2} \wedge\mathrm{R}$$

$C = C_1 \wedge C_2$	This case
$\Gamma \Longrightarrow C_1$	By i.h. on A, $\mathcal{D}$ and $\mathcal{E}_1$
$\Gamma \Longrightarrow C_2$	By i.h. on A, $\mathcal{D}$ and $\mathcal{E}_2$
$\Gamma \Longrightarrow C_1 \wedge C_2$	By rule $\wedge$R on above

Subcase:

$$\mathcal{E} = \dfrac{\begin{matrix}\mathcal{E}_1 \\ \Gamma', B_1 \wedge B_2, B_1, A \Longrightarrow C\end{matrix}}{\Gamma', B_1 \wedge B_1, A \Longrightarrow C} \wedge\mathrm{L}_1$$

$\Gamma = \Gamma', B_1 \wedge B_2$	This case
$\Gamma', B_1 \wedge B_2, B_1 \Longrightarrow C$	By i.h. on A, $\mathcal{D}$ and $\mathcal{E}_1$
$\Gamma', B_1 \wedge B_2 \Longrightarrow C$	By rule $\wedge\mathrm{L}_1$ from above

□

As mentioned above, it is a general property of deductive system that adding an admissible rule does not change the derivable judgments. We show the argument in this special case.

Theorem 3.12 (Cut Elimination)
If $\Gamma \overset{+}{\Longrightarrow} C$ *then* $\Gamma \Longrightarrow C$.

Proof: In each case except cut we simply appeal to the induction hypotheses and reapply the same rule on the resulting cut-free derivations. So we write out only the case of cut.

Case:

$$\mathcal{D}^+ = \dfrac{\begin{matrix}\mathcal{D}_1^+ \\ \Gamma \overset{+}{\Longrightarrow} A\end{matrix} \qquad \begin{matrix}\mathcal{D}_2^+ \\ \Gamma, A \overset{+}{\Longrightarrow} C\end{matrix}}{\Gamma \overset{+}{\Longrightarrow} C} \mathrm{cut}$$

$\Gamma \Longrightarrow A$	By i.h. on $\mathcal{D}_1^+$
$\Gamma, A \Longrightarrow C$	By i.h. on $\mathcal{D}_2^+$
$\Gamma \Longrightarrow C$	By admissibility of cut (Theorem 3.11)

□

3.5 Applications of Cut Elimination

The cut elimination theorem is the final piece needed to complete our study of natural deduction and normal natural deduction and at the same time the springboard to the development of efficient theorem proving procedures. Our proof in the previous section is constructive and therefore contains an algorithm for cut elimination. Because the cases are not mutually exclusive, the algorithm is non-deterministic. However, the resulting derivation should always be the same. While this property does not quite hold, the different derivations can be shown to be equivalent in a natural sense. This is called the *confluence* property for intuitionistic cut elimination modulo commutative conversions. It it is not implicit in our proof, but has to be established separately. On the other hand, our proof shows that any possible execution of the cut-elimination algorithm terminates. This is called the *strong normalization* property for the sequent calculus.

By putting the major results of this chapter together we can now prove the normalization theorem for natural deduction.

Theorem 3.13 (Normalization for Natural Deduction)
If $\Gamma \vdash A$ *then* $\Gamma^{\downarrow} \vdash A \Uparrow$.

Proof: Direct from previous theorems.

$\Gamma \vdash A$	Assumption
$\Gamma^{\downarrow} \vdash^{+} A \Uparrow$	By completeness of annotated deductions (Theorem 3.3)
$\Gamma \overset{+}{\Longrightarrow} A$	By completeness of sequent calculus with cut (Theorem 3.10)
$\Gamma \Longrightarrow A$	By cut elimination (Theorem 3.12)
$\Gamma^{\downarrow} \vdash A \Uparrow$	By soundness of sequent calculus (Theorem 3.6)

□

Among the other consequences of cut elimination are consistency and various independence results.

Corollary 3.14 (Consistency) *There is no deduction of* $\vdash \bot$.

Proof: Assume there is a deduction $\vdash \bot$. By the results of this chapter then $\cdot \Longrightarrow \bot$. However, this sequent cannot be the conclusion of any inference rule in the (cut-free) sequent calculus. Therefore $\vdash \bot$ cannot be derivable. □

In the same category are the following two properties. As in the proof above, we analyze the inference rules which may have led to a given conclusion. This proof technique is called *inversion.*

Corollary 3.15 (Disjunction and Existential Property)

1. *If* $\vdash A \vee B$ *then either* $\vdash A$ *or* $\vdash B$.
2. *If* $\vdash \exists x.\ A$ *then* $\vdash [t/x]A$ *for some* t.

Proof: Direct by inversion on possible sequent derivations in both cases.

1. Assume $\vdash A \vee B$. Then $\cdot \Longrightarrow A \vee B$. By inversion, either $\cdot \Longrightarrow A$ or $\cdot \Longrightarrow B$. Therefore $\vdash A$ or $\vdash B$.
2. Assume $\exists x.\ A$. then $\cdot \Longrightarrow \exists x.\ A$. By inversion, $\cdot \Longrightarrow [t/x]A$ for some t. Hence $\vdash [t/x]A$.

□

Note that the disjunction and existential properties rely on a judgment without hypotheses. For example, we have $B \vee A \Longrightarrow A \vee B$, but neither $B \vee A \Longrightarrow A$ for $B \vee A \Longrightarrow B$ hold.

The second class of properties are *independence* results which demonstrate that certain judgments are not derivable. As a rule, these are parametric judgments some instances of which may be derivable. For example, we will show that the law of excluded middle is independent. Nonetheless, there are some propositions A for which we can show $\vdash A \vee \neg A$ (for example, take $A = \bot$).

Corollary 3.16 (Independence of Excluded Middle)
There is no deduction of $\vdash A \vee \neg A$ for arbitrary A.

Proof: Assume there is a deduction of $\vdash A \vee \neg A$. By the result of this section then $\cdot \Longrightarrow A \vee \neg A$. By inversion now either $\cdot \Longrightarrow A$ or $\cdot \Longrightarrow \neg A$. The former judgment (which is parametric in A) has no derivation. By inversion, the latter can only be infered from $A \Longrightarrow p$ for a new parameter p. But there is no inference rule with this conclusion, and hence there cannot be a deduction of $\vdash A \vee \neg A$. □

3.6 Proof Terms for Sequent Derivations

In this section we address the question of how to assign proof terms to sequent calculus derivations. There are essentially two possibilities: we can either develop a new proof term calculus specifically for sequent derivations, or we can directly assign natural deduction proof terms. The former approach can be found, for example, in [Pfe95]. The latter is more appropriate for our purposes here, since we view natural deductions as defining truth and since we already devised methods for compact representations in Section 3.2.

We define a new judgment, $\Gamma \Longrightarrow I : A$, maintaining that $\Gamma \vdash I : A$. For this purpose we abandon the previous convention of omitting labels for hypotheses, since proof terms need to refer to them. On the other hand, we still consider assumptions modulo permutations in order to simplify notation. We use the compact proof terms here only for simplicity.

The proof terms to be assigned to each inference rule can be determined by a close examination of the soundness proof for the sequent calculus (Theorem 3.6). Since that proof is constructive, it contains an algorithm for translating a sequent derivation to a normal natural deduction. We just have to write down the corresponding proof terms.

Initial Sequents. These are straightforward.

$$\frac{}{\Gamma, u{:}A \Longrightarrow u : A}\,\text{init}$$

Note that there may be several hypotheses A with different labels. In the shorthand notation without labels before, it is ambiguous which one was used.

Conjunction. The right rule is straightforward, since it is isomorphic to the introduction rule for natural deduction. The left rules require a substitution to be carried out, just as in the proof of Theorem 3.6.

$$\frac{\Gamma \Longrightarrow I : A \qquad \Gamma \Longrightarrow J : B}{\Gamma \Longrightarrow \langle I, J\rangle : A \wedge B}\,{\wedge}\text{R}$$

$$\frac{\Gamma, u{:}A \wedge B, w{:}A \Longrightarrow I : C}{\Gamma, u{:}A \wedge B \Longrightarrow [\text{fst}\, u/w]I : C}\,{\wedge}\text{L}_1 \qquad \frac{\Gamma, u{:}A \wedge B, w{:}B \Longrightarrow I : C}{\Gamma, u{:}A \wedge B \Longrightarrow [\text{snd}\, u/w]I : C}\,{\wedge}\text{L}_2$$

There are two potential efficiency problems in the proof term assignment for the left rule. The first is that if w is used many times in I, then $\text{fst}\, u$ or $\text{snd}\, u$ may be replicated many times, leading to a large proof. The second is that when a number of successive left rules are encountered, the term I we substitute into will be traversed many times. These problems can be avoided in several ways (see Exercise **??**).

Implication. The pattern of the previous right and left rules continues here.

$$\frac{\Gamma, u{:}A \Longrightarrow I : B}{\Gamma \Longrightarrow \lambda u.\, I : A \supset B}\,{\supset}\text{R}$$

$$\frac{\Gamma, u{:}A \supset B \Longrightarrow J : A \qquad \Gamma, u{:}A \supset B, w{:}B \Longrightarrow I : C}{\Gamma, u{:}A \supset B \Longrightarrow [u\, J/w]I : C}\,{\supset}\text{L}$$

Disjunction. This introduces no new considerations.

$$\frac{\Gamma \Longrightarrow I : A}{\Gamma \Longrightarrow \text{inl}\, I : A \vee B}\,{\vee}\text{R}_1 \qquad \frac{\Gamma \Longrightarrow J : B}{\Gamma \Longrightarrow \text{inr}\, J : A \vee B}\,{\vee}\text{R}_2$$

$$\frac{\Gamma, u{:}A \vee B, v{:}A \Longrightarrow I : C \qquad \Gamma, u{:}A \vee B, w{:}B \Longrightarrow J : C}{\Gamma, u{:}A \vee B \Longrightarrow (\,\textbf{case}\ u\ \textbf{of}\ \text{inl}\, v \Rightarrow I \mid \text{inr}\, w \Rightarrow J) : C}\,{\vee}\text{L}$$

Negation. This is similar to implication.[1]

$$\frac{\Gamma, u{:}A \Longrightarrow I : p}{\Gamma \Longrightarrow \mu^p u.\, I : \neg A}\,\neg\text{R}^p \qquad \frac{\Gamma, u{:}\neg A \Longrightarrow I : A}{\Gamma, u{:}\neg A \Longrightarrow u \cdot I : C}\,\neg\text{L}$$

[1] [*add to compact proof term section?*]

Truth. This is trivial, since there is no left rule.

$$\frac{}{\Gamma \Longrightarrow \langle\,\rangle : \top}\,\top\mathrm{R}$$

Falsehood. Again, this is immediate.

$$\frac{}{\Gamma, u{:}\bot \Longrightarrow \mathrm{abort} u : C}\,\bot\mathrm{L}$$

To treat the quantifiers we extend our proof term calculus to handle the quantifier rules. We overload the notation by reusing λ-abstraction and pairing. There is no ambiguity, because the proof term for universal quantification binds a term variable x (rather than a proof variable u), and the first component of the pair for existential quantification is a first-order term, rather than a proof term as for conjunction.

First, we show the assignment of these terms to natural deductions, then to the sequent calculus.

Universal Quantification. The proof term for a universal quantifier $\forall x.\ A$ is a function from a term t to a proof of $[t/x]A$. The elimination term applies this function.

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

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

The local reductions and expansions just mirror the corresponding operations on natural deductions.

$$\begin{array}{lll} (\lambda x.\ M)\,t & \longrightarrow_R & [t/x]M \\ M : \forall x.\ A & \longrightarrow_E & \lambda x.\ M\,x \quad (x \text{ not free in } M) \end{array}$$

Existential Quantification. The proof term for an existential $\exists x.\ A$ is a pair consisting of a witness term t and the proof of $[t/x]A$.

$$\frac{\Gamma \vdash M : [t/x]A}{\Gamma \vdash \langle t, M\rangle : \exists x.\ A}\,\exists\mathrm{I}$$

$$\frac{\Gamma \vdash M : \exists x.\ A \qquad \Gamma, u{:}[a/x]A \vdash [a/x]N : C}{\Gamma \vdash \mathbf{let}\ \langle x, u\rangle = M\ \mathbf{in}\ N : C}\,\exists\mathrm{E}^{a,u}$$

The local reduction for the existential quantifier has to perform two substitutions, just as on natural deductions.

$$\begin{array}{rll} \mathbf{let}\ \langle x, u\rangle = \langle t, M\rangle\ \mathbf{in}\ N & \longrightarrow_R & [M/u][t/x]N \\ M : \exists x.\ A & \longrightarrow_E & \mathbf{let}\ \langle x, u\rangle = M\ \mathbf{in}\ \langle x, u\rangle \end{array}$$

It is once again easy to see how to divide the proof terms into introduction and elimination forms. We only show the resulting definition of compact proof terms.

$$\begin{array}{llll}
\text{Intro Terms} & I & ::= & \ldots \\
 & & & \mid \lambda x.\, I \qquad\qquad\qquad \text{Universal Quantification} \\
 & & & \mid \langle t, I\rangle \qquad\qquad\quad\;\, \text{Existential Quantification} \\
 & & & \mid \textbf{let } \langle x, u\rangle = E \textbf{ in } I \\
\text{Elim Terms} & E & ::= & \ldots \mid E\, t \qquad\qquad\quad \text{Universal Quantification}
\end{array}$$

On sequent calculus derivations, we follow the same strategy as in the preceding propositional rules.

Universal Quantification.

$$\frac{\Gamma \Longrightarrow [a/x]I : [a/x]A}{\Gamma \Longrightarrow \lambda x.\, I : \forall x.\, A}\forall\mathrm{R}^a \qquad \frac{\Gamma, u{:}\forall x.\, A, w{:}[t/x]A \Longrightarrow I : C}{\Gamma, u{:}\forall x.\, A \Longrightarrow [u\, t/w]I : C}\forall\mathrm{L}$$

Existential Quantification.

$$\frac{\Gamma \Longrightarrow I : [t/x]A}{\Gamma \Longrightarrow \langle t, I\rangle : \exists x.\, A}\exists\mathrm{R} \qquad \frac{\Gamma, u{:}\exists x.\, A, w{:}[a/x]A \Longrightarrow [a/x]I : C}{\Gamma, u{:}\exists x.\, A \Longrightarrow (\textbf{let } \langle x, w\rangle = u \textbf{ in } I) : C}\exists\mathrm{L}^a$$

3.7 Classical Sequent Calculus

We briefly mentioned in Section 2.2 that there are several ways to add a rule or axiom schema to natural deduction to obtain a classical interpretation of the connectives. As the example of $A \vee \neg A$ illustrates, this changes the interpretation of the propositions and our method of explaining the meaning of a proposition via its introduction and elimination rules fails. In this section we explore an alternative, judgmental approach to classical logic. Rather than starting from natural deduction we start from the sequent calculus, because Gentzen [Gen35] has already proposed a sequent calculus for classical logic that has a strong subformula property and thereby satisfies at least the requirement that the meaning of a proposition (if we can define what that means) depends only on the meaning of its constituents.

Recall the basic judgment form for the (intuitionistic) sequent calculus,

$$u_1{:}A_1\; \mathit{left}, \ldots, u_n{:}A_n\; \mathit{left} \vdash A\; \mathit{right},$$

which arises by splitting the basic judgment A *true* into $A\,\mathit{left}$ (truth as an assumption, only in the antecedent) and $A\,\mathit{right}$ (truth as a conclusion, only in the succedent), which we abbreviated as

$$A_1, \ldots, A_n \Longrightarrow A$$

In order to formulate classical logic, we add a new basic judgment, A *false*, which we use only as an assumption. Furthermore, we have the judgment of contradiction, *contr*, expressing that a collection of assumptions is contradictory. The hypothetical judgment form we consider is

$$u_1{:}A_1\ \mathit{true}, \ldots, u_n{:}A_n\ \mathit{true}, z_1{:}B_1\ \mathit{false}, \ldots, z_m{:}B_m\ \mathit{false} \vdash \mathit{contr}$$

stating that the assumptions about truth and falsehood are contradictory. The basic **rule of contradiction** relating truth and falsehood is

$$\frac{}{\Psi, u{:}A\ \mathit{true}, z{:}A\ \mathit{false} \vdash \mathit{contr}}\ \text{contra}$$

which states that a proposition cannot be simultaneously true and false. There are further unused assumptions about truth and falsehood are allowed in Ψ. Interestingly, many theorem proving procedures for classical logic are presented in this style: instead of proving a proposition we derive a contradiction from the negated assumptions. Perhaps our analysis provides some hints why this is indeed the right view of classical logic.

Conversely, we have a principle that states any proposition A must be either true or false.

Principle of excluded middle.
If $\Psi, u{:}A\ \mathit{true} \vdash \mathit{contr}$ and $\Psi, z{:}A\ \mathit{false} \vdash \mathit{contr}$ then $\Psi \vdash \mathit{contr}$.

The argument for this principle, from the rule of contradiction, goes as follows: if the assumption A *true* is contradictory, then either A must be false (assuming Ψ) or Ψ itself is contradictory. In the latter case we are done. But if A *false* follows from Ψ then we can discharge the assumption that A is false from the second given derivation.

It is important that this principle must hold for the logic, rather than being assumed as an inference rule. This means that the law of excluded middle is not an arbitrary assumption, but arises from the nature of falsehood as the opposite of truth in a systematic way, at the level of judgments.

We abbreviate the the judgment

$$u_1{:}A_1\ \mathit{true}, \ldots, u_n{:}A_n\ \mathit{true}, z_1{:}B_1\ \mathit{false}, \ldots, z_m{:}B_m\ \mathit{false} \vdash \mathit{contr}$$

as

$$A_1, \ldots, A_n \# B_1, \ldots, B_m.$$

We have to keep in mind that A_i are assumptions about truth, and B_j are assumptions about falsehood, with the overall goal to derive a contradiction.

In the literature one finds two other common notations for this judgment, first and foremost Gentzen's multiple-conclusion sequent calculus.

$$A_1, \ldots, A_n \Longrightarrow B_1, \ldots, B_m$$

Gentzen observed that we can capture the difference between classical and intuitionistic reasoning by either allowing or disallowing multiple conclusions. However, the only way we have been able to explain this from the judgmental point of view is in the manner indicated above. The other notation sometimes used, in the presentation of tableaux, resolution and other theorem proving techniques is

$$A_1^\top, \ldots A_n^\top, B_1^\perp, \ldots, B_m^\perp$$

where we mark assumption A *true* as $A^\top$ and assumptions B *false* as $B^\perp$ instead of segregating them in the manner of a sequent calculus. There is no essential difference between these notations as long as we keep in mind their correct interpretation.

We first restate our judgmental rules and principles in the new notation, using Γ for truth assumptions and Δ for falsehood assumptions.

Rule of Contradiction.

$$\frac{}{\Gamma, A \mathrel{\#} A, \Delta}\,\text{contra}$$

Principle of Excluded Middle.

If $\Gamma \mathrel{\#} A, \Delta$ and $\Gamma, A \mathrel{\#} \Delta$ then $\Gamma \mathrel{\#} \Delta$.

We also have the expected weakening and contraction properties, both for truth and falsehood, which follow from the general nature of hypothetical reasoning. For a multiple-conclusion view of sequents, these are much more difficult to explain.

Since we do not change the meaning of truth (or the meaning of the connectives), all the left rules from the intuitionistic sequent calculus carry over to analogous rules here. We have to derive the rules for assumptions A *false* from the principle of excluded middle (which was in turn justified by the rule of contradiction that defined falsehood).

Conjunction. The (left) rules for truth are as usual. We write the names of the rules as T in this context.

$$\frac{\Gamma, A \wedge B, A \mathrel{\#} \Delta}{\Gamma, A \wedge B \mathrel{\#} \Delta}\,\wedge\mathrm{T}_1 \qquad \frac{\Gamma, A \wedge B, B \mathrel{\#} \Delta}{\Gamma, A \wedge B \mathrel{\#} \Delta}\,\wedge\mathrm{T}_2$$

To determine the rules for falsehood we have to think about what we can conclude from the assumption that $A \wedge B$ *false*. If $A \wedge B$ is false, then either A or B must be false, so we must be able to obtain a contradiction in both cases.

$$\frac{\Gamma \mathrel{\#} A, A \wedge B, \Delta \qquad \Gamma \mathrel{\#} B, A \wedge B, \Delta}{\Gamma \mathrel{\#} A \wedge B, \Delta}\,\wedge\mathrm{F}$$

We use F to mark rules operating on falsehood assumptions.

The fact that the truth and falsehood rules mesh in a way predicted by the principle of excluded middle is the subject of Theorem 3.17. Intuitively, we should verify that if we use excluded middle for a conjunction we can reduce it to uses on excluded middle for the conjuncts.

Truth. Truth is straightforward: there is no left rule and the rule for $\top$ *false* simply succeeds.

$$\frac{}{\Gamma \mathrel{\#} \top, \Delta}\,\top F$$

Disjunction. The left rule becomes the rule for truth assumptions.

$$\frac{\Gamma, A \vee B, A \mathrel{\#} \Delta \qquad \Gamma, A \vee B, B \mathrel{\#} \Delta}{\Gamma, A \vee B \mathrel{\#} \Delta}\,\vee T$$

How can we proceed if we know that $A \vee B$ *false*? Intuitively, it means that both A and B must be false.

$$\frac{\Gamma \mathrel{\#} A, A \vee B, \Delta}{\Gamma \mathrel{\#} A \vee B, \Delta}\,\vee F_1 \qquad \frac{\Gamma \mathrel{\#} B, A \vee B, \Delta}{\Gamma \mathrel{\#} A \vee B, \Delta}\,\vee F_2$$

Falsehood. This is dual to truth: there is a left rule but no rule for $\bot$ *false*, which provides no information.

$$\frac{}{\Gamma, \bot \mathrel{\#} \Delta}\,\bot T$$

Implication. We can use an assumption $A \supset B$ *true* only by proving A *true* (which licenses us to assume B *true*). Unfortunately, our classical sequent calculus does not allow us to derive the truth of any proposition, only contradictions. This means we cannot give a judgmental explanation of the constructive implication in the classical sequent calculus without destroying its meaning. However, there is a classical form of implication $A \Rightarrow B$ meaning that either A is false or B is true. This leads to the following rules for this new classical connective

$$\frac{\Gamma, A \Rightarrow B \mathrel{\#} A, \Delta \qquad \Gamma, A \Rightarrow B, B \mathrel{\#} \Delta}{\Gamma, A \Rightarrow B \mathrel{\#} \Delta}\,{\Rightarrow}T \qquad \frac{\Gamma, A \mathrel{\#} B, A \Rightarrow B, \Delta}{\Gamma \mathrel{\#} A \Rightarrow B, \Delta}\,{\Rightarrow}F$$

Negation. As for implication, we cannot formulate a rule for constructive negation in the classical sequent calculus. Instead, we have a new form of negation that flips between truth and falsehood. That is, $\sim A$ is true if A is false and $\sim A$ is false if A is true. We obtain the following rules

$$\frac{\Gamma, \sim A \mathrel{\#} A, \Delta}{\Gamma, \sim A \mathrel{\#} \Delta}\,{\sim}T \qquad \frac{\Gamma, A \mathrel{\#} \sim A, \Delta}{\Gamma \mathrel{\#} \sim A, \Delta}\,{\sim}F$$

We conclude that the difference between intuitionistic and classical logic does not lie in the nature of conjunction or disjunction, but in the nature of implication and negation. Moreover, if we accept that a notion of falsehood of a proposition as being contradictory with its truth, then the principle of excluded middle seems fully justified for proofs of contradiction. This does not answer any question about a possible computational interpretation of classical logic or about a faithful system of natural deduction or about a possible integration of intuitionistic and classical logic in a single system.

Theorem 3.17 (Principle of Excluded Middle)
If $\Gamma \# A, \Delta$ *and* $\Gamma, A \# \Delta$ *then* $\Gamma \# \Delta$

Proof: By induction on the structure of A and, for each A simultaneously on the structure of the two given derivations. This means, as for the proof of the admissibility of cut (Theorem 3.11), we can appeal to the induction hypothesis on a smaller formulas and arbitrary derivations, or on the same formula such that one of the derivations gets smaller and the other one remains the same.

The division into cases, and the idea of the proof in each case is quite similar to the admissibility of cut, so we elide any details here. □

At this point it might seem like intuitionistic logic and classical logic are simply different, with classical logic somewhat impoverished. It only appears to have conjunction, disjunction, and a form of negation, while intuitionistic logic also has a constructive implication that does not appear expressible in classical logic.

However, the situation is more complicated. It turns out that there is a uniform way to translate classical logic to intuitionistic logic that preserves truth. This means intuitionistic logic can simulate A *false*, contradiction, and negation. The idea is due to Kolmogorov [**?**] who, however, did not prove its correctness in the modern sense.

The translation A^o maps atomic formulas to themselves, classical negation to intuitionistic negation, and prefixes any other subformula by a double negation. Some optimization are possible, but not necessary.

$$\begin{array}{rcl}
P^o & = & P \\
(A \wedge B)^o & = & \neg\neg A^o \wedge \neg\neg B^o \\
(\top)^o & = & \top \\
(A \vee B)^o & = & \neg\neg A^o \vee \neg\neg B^o \\
(\bot)^o & = & \bot \\
(\sim A)^o & = & \neg A^o \\
(A \Rightarrow B)^o & = & \neg\neg A^o \supset \neg\neg B^o
\end{array}$$

Then we interpret A *false* and $\neg A^o$ *true*. We also write Γ^o for translating each formula A in Γ to A^o, and $\neg\Gamma$ for applying $\neg$ to each formula in Γ.

Lemma 3.18
If $\Gamma \# \Delta$ *then* $\Gamma^o, \neg\Delta^o \Longrightarrow p$ *for a parameter* p *not in* Γ *or* Δ.

Proof: Part (1) follows by induction on the derivation $\mathcal{D}$ of $\Gamma \# \Delta$. Each case is straightforward; we show some representative ones. After the first case, we silently apply weakening when necessary. The proofs in each case may be easier to think about if we read them from the last line upwards.

Case:

$$\mathcal{D} = \frac{}{\Gamma_1, A \mathrel{\#} A, \Delta_1}\,\text{contra}$$

$\Gamma_1^o, A^o, \Delta_1^o \Longrightarrow A^o$ By rule init
$\Gamma_1^o, A^o, \neg A^o, \Delta_1^o \Longrightarrow A^o$ By weakening
$\Gamma_1^o, A^o, \neg A^o, \Delta_1^o \Longrightarrow p$ By rule $\neg$L

Case:

$$\mathcal{D} = \frac{\begin{array}{c}\mathcal{D}_1\\ \Gamma_1, A \wedge B, A \mathrel{\#} \Delta\end{array}}{\Gamma_1, A \wedge B \mathrel{\#} \Delta}\,\wedge\mathrm{T}_1$$

$\Gamma_1^o, \neg\neg A^o \wedge \neg\neg B^o, A^o, \neg\Delta^o \Longrightarrow p$ By i.h. on $\mathcal{D}_1$
$\Gamma_1^o, \neg\neg A^o \wedge \neg\neg B^o, \neg\Delta^o \Longrightarrow \neg A^o$ By rule $\neg$R
$\Gamma_1^o, \neg\neg A^o \wedge \neg\neg B^o, \neg\neg A^o, \neg\Delta^o \Longrightarrow p$ By rule $\neg$L
$\Gamma_1^o, \neg\neg A^o \wedge \neg\neg B^o, \neg\Delta^o \Longrightarrow p$ By rule $\wedge\mathrm{L}_1$
$\Gamma_1^o, (A \wedge B)^o, \neg\Delta^o \Longrightarrow p$ By defn of $()^o$

Case:

$$\mathcal{D} = \frac{\begin{array}{c}\mathcal{D}_1\\ \Gamma \mathrel{\#} A, A \wedge B, \Delta_1\end{array} \qquad \begin{array}{c}\mathcal{D}_2\\ \Gamma \mathrel{\#} B, A \wedge B, \Delta_1\end{array}}{\Gamma \mathrel{\#} A \wedge B, \Delta_1}\,\wedge\mathrm{F}$$

$\Gamma^o, \neg A^o, \neg(A \wedge B)^o, \neg\Delta_1^o \Longrightarrow p$ By i.h. on $\mathcal{D}_1$
$\Gamma^o, \neg(A \wedge B)^o, \neg\Delta_1^o \Longrightarrow \neg\neg A^o$ By rule $\neg$R
$\Gamma^o, \neg B^o, \neg(A \wedge B)^o, \neg\Delta_1^o \Longrightarrow p$ By i.h. on $\mathcal{D}_2$
$\Gamma^o, \neg(A \wedge B)^o, \neg\Delta_1^o \Longrightarrow \neg\neg B^o$ By rule $\neg$R
$\Gamma^o, \neg(A \wedge B)^o, \neg\Delta_1^o \Longrightarrow \neg\neg A^o \wedge \neg\neg B^o$ By rule $\wedge$R
$\Gamma^o, \neg(A \wedge B)^o, \neg\Delta_1^o \Longrightarrow (A \wedge B)^o$ By defn. of $()^o$
$\Gamma^o, \neg(A \wedge B)^o, \neg\Delta_1^o \Longrightarrow p$ By rule $\neg$L

□

For part (2), an induction over the structure of the given deduction will not work, because subdeductions will not necessarily have a conclusion of the same form. Instead we employ a simpler backward translation, $()^e$ and show that if $\Gamma \Longrightarrow C$ then $\Gamma^e \mathrel{\#} C^e$

$$\begin{array}{rcl}
P^e & = & P\\
(A \wedge B)^e & = & A^e \wedge B^e\\
(\top)^e & = & \top\\
(A \vee B)^e & = & A^e \vee B^e\\
(\bot)^e & = & \bot\\
(\neg A)^e & = & {\sim}A^e\\
(A \supset B)^e & = & A^e \Rightarrow B^e
\end{array}$$

Because the double-negation translation $()^o$ inserts double negations and the backward translation $()^e$ keeps the structure of the formula intact, if we translate back and forth we obtain an equivalent proposition.

Lemma 3.19
$A \# (A^o)^e$ and $(A^o)^e \# A$ for any (classical) proposition A.

Proof: By induction on the structure of A. We show two cases, eliding appeals to weakening.

Case: $A = P$. Then $(A^o)^e = (P^o)^e = P$ and $P \# P$ by rule contra.

Case: $A = A_1 \wedge A_2$.

$A_1 \# (A_1^o)^e$	By i.h. on A_1
$A_1 \wedge A_2 \# (A_1^o)^e$	By $\wedge T_1$
$A_1 \wedge A_2, {\sim}(A_1^o)^e \# \cdot$	By ${\sim}$T
$A_1 \wedge A_2 \# {\sim}{\sim}(A_1^o)^e$	By ${\sim}$F
$A_2 \# (A_2^o)^e$	By i.h. on A_2
$A_1 \wedge A_2 \# (A_2^o)^e$	By $\wedge T_2$
$A_1 \wedge A_2, {\sim}(A_2^o)^e \# \cdot$	By ${\sim}$T
$A_1 \wedge A_2 \# {\sim}{\sim}(A_2^o)^e$	By ${\sim}$F
$A_1 \wedge A_2 \# {\sim}{\sim}(A_1^o)^e \wedge {\sim}{\sim}(A_2^o)^e$	By $\wedge$F
$A_1 \wedge A_2 \# (\neg\neg A_1^o \wedge \neg\neg A_2^o)^e$	By defn. of $()^e$
$A_1 \wedge A_2 \# ((A_1 \wedge A_2)^o)^e$	By defn. of $()^o$

□

The truth and falsehood rules of the classical sequent calculus can simulate the left and right rules of the intuitionistic sequent calculus on corresponding propositions.

Lemma 3.20 *If $\Gamma \Longrightarrow C$ then $\Gamma^e \# C^e$.*

Proof: By induction on the structure of the given derivation $\mathcal{D}$. We show some representative cases.

Case:

$$\mathcal{D} = \dfrac{}{\Gamma_1, C \Longrightarrow C}\,\text{init}$$

$\Gamma_1^e, C^e \# C^e$	By rule contra

Case:

$$\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}_1 \\ \Gamma, A \Longrightarrow B\end{array}}{\Gamma \Longrightarrow A \supset B}\,{\supset}\text{R}$$

$$\begin{array}{lr}
\Gamma^e, A^e \,\#\, B^e & \text{By i.h. on } \mathcal{D}_1 \\
\Gamma^e, A^e \,\#\, B^e, A^e \Rightarrow B^e & \text{By weakening} \\
\Gamma^e \,\#\, A^e \Rightarrow B^e & \text{By rule} \Rightarrow\!\text{F} \\
\Gamma^e \,\#\, (A \supset B)^e & \text{By defn. of } ()^e
\end{array}$$

Case:

$$\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}_1 \\ \Gamma_1, A \supset B \Longrightarrow A\end{array} \qquad \begin{array}{c}\mathcal{D}_2 \\ \Gamma_1, A \supset B, B \Longrightarrow C\end{array}}{\Gamma_1, A \supset B \Longrightarrow C} \supset\!\text{L}$$

$$\begin{array}{lr}
\Gamma_1^e, A^e \Rightarrow B^e \,\#\, A^e & \text{By i.h. on } \mathcal{D}_1 \\
\Gamma_1^e, A^e \Rightarrow B^e \,\#\, A^e, C^e & \text{By weakening} \\
\Gamma_1^e, A^e \Rightarrow B^e, B^e \,\#\, C^e & \text{By i.h. on } \mathcal{D}_2 \\
\Gamma_1^e, A^e \Rightarrow B^e \,\#\, C^e & \text{By rule} \Rightarrow\!\text{F} \\
\Gamma_1^e, (A \supset B)^e \,\#\, C^e & \text{By defn. of } ()^e
\end{array}$$

□

Theorem 3.21 (Interpretation of Classical in Intuitionistic Logic) *$\Gamma \,\#\, \Delta$ iff $\Gamma^o, \neg\Delta^o \Longrightarrow p$ for a parameter p not in Γ or Δ.*

Proof: The forward direction is precisely the subject of Lemma 3.18.

In the backward direction, we know from Lemma 3.20, that $(\Gamma^o)^e, {\sim}(\Delta^o)^e \,\#\, p$. The we repeatedly use $\sim$T to conclude $(\Gamma^o)^e \,\#\, {\sim}{\sim}(\Delta^o)^e, p$. This derivation is parametric in p, so we instantiate p with $\bot$ and then use the law of excluded middle with the one-step derivation of $(\Gamma^o)^e, \bot \,\#\, {\sim}{\sim}(\Delta^o)^e$ to conclude $(\Gamma^o)^e \,\#\, (\Delta^o)^e$. Now we can repeatedly apply excluded middle, first with ${\sim}{\sim}A \,\#\, A$, then using Lemma 3.19, to arrive at $\Gamma \,\#\, \Delta$. □

3.8 Exercises

Exercise 3.1 Consider a system of normal deduction where the elimination rules for disjunction and existential are allowed to end in an extraction judgment.

$$\dfrac{\Gamma^{\downarrow} \vdash A \vee B \downarrow \qquad \Gamma^{\downarrow}, u{:}A \downarrow\; \vdash C \downarrow \qquad \Gamma^{\downarrow}, w{:}B \downarrow\; \vdash C \downarrow}{\Gamma^{\downarrow} \vdash C \downarrow} \vee\text{E}^{u,w}$$

$$\dfrac{\Gamma^{\downarrow} \vdash \exists x.\, A \downarrow \qquad \Gamma^{\downarrow}, u{:}[a/x]A \downarrow\; \vdash C \downarrow}{\Gamma^{\downarrow} \vdash C \downarrow} \exists\text{E}^{a,u}$$

Discuss the relative merits of allowing or disallowing these rules and show how they impact the subsequent development in this Chapter (in particular, bidirectional type-checking and the relationship to the sequent calculus).

Exercise 3.2

1. Give an example of a natural deduction which is *not* normal (in the sense defined in Section 3.1), yet contains no subderivation which can be locally reduced.

2. Generalizing from the example, devise additional rules of reduction so that any natural deduction which is not normal can be reduced. You should introduce no more and no fewer rules than you need for this purpose.

3. Prove that your rules satisfy the specification in part (2).

Exercise 3.3 Write out the rules defining the judgments $\Gamma^{\downarrow} \vdash^{+} I : A \Uparrow$ and $\Gamma^{\downarrow} \vdash^{+} E : A \downarrow$ and prove Theorem 3.4. Make sure to carefully state the induction hypothesis (if it is different from the statement of the theorem) and consider all the cases.

Exercise 3.4 Fill in the missing subcases in the proof of the admissibility of cut (Theorem 3.11) where A is the principal formula in both $\mathcal{D}$ and $\mathcal{E}$.

Exercise 3.5 Consider an extension of intuitionistic logic by a universal quantifier over propositions, written as $\forall^2 p.\ A$, where p is variable ranging over propositions.

1. Show introduction and elimination rules for $\forall^2$.

2. Extend the calculus of normal and extraction derivations.

3. Show left and right rules of the sequent calulus for $\forall^2$.

4. Extend the proofs of soundness and completeness for the sequent calculus and sequent calculus with cut to accomodate the new rules.

5. Point out why the proof for admissibility of cut does not extend to this logic.

Exercise 3.6 Gentzen's original formulation of the sequent calculus for intuitionistic logic permitted the right-hand side to be empty. The introduction rule for negation then has the form

$$\frac{\Gamma, A \Longrightarrow}{\Gamma \Longrightarrow \neg A}\neg\mathrm{R}.$$

Write down the corresponding left rule and detail the changes in the proof for admissibility of cut. Can you explain sequents with empty right-hand sides as judgments?

Exercise 3.7 The algorithm for cut elimination implicit in the proof for admissibility of cut can be described as a set of reduction rules on sequent derivations containing cut.

1. Write out all reduction rules on the fragment containing only implication.
2. Show the extracted proof term before and after each reduction.
3. If possible, formulate a strategy of reduction on proof terms for natural deduction which directly models cut elimination under our translation.
4. Either formulate and prove a theorem about the connection of the strategies for cut elimination and reduction, or show by example why such a connection is difficult or impossible.

Exercise 3.8

1. Prove that we can restrict initial sequents in the sequent calculus to have the form $\Gamma, P \Longrightarrow P$ where P is an atomic proposition without losing completeness.
2. Determine the corresponding restriction in normal and extraction derivations and prove that they preserve completeness.
3. If you see a relationship between these properties and local reductions or expansions, explain. If you can cast it in the form of a theorem, do so and prove it.

Exercise 3.9 For each of the following propositions, prove that they are derivable in classical logic using the law of excluded middle. Furthermore, prove that they are not true in intuitionistic logic for arbitrary A, B, and C.

1. $((A \supset B) \supset A) \supset A$.
2. Any entailment in Exercise 2.8 which is only classically, but not intuitionistically true.

Chapter 4

Focused Derivations

The sequent calculus as presented in the previous chapter is an excellent foundation for proof search strategies, but it is not yet practical. For a typical sequent there are many choices, such as which left or right rule to use to reduce the goal in the bottom-up construction of a proof. After one step, similar choices arise again, and so on. Without techniques to eliminate some of this non-determinism one would be quickly overwhelmed with multiple choices.

In this chapter we present two techniques to reduce the amount of non-determinism in search. The first are *inversion properties* which hold when the premises of an inference rule are derivable if and only if the conclusion is. This means that we do not lose completeness when applying an invertible rule as soon as it is applicable. The second are *focusing properties* which allow us to chain together non-invertible inference rules with consecutive principal formulas, once again without losing completeness.

While inversion and focusing are motivated by bottom-up proof search, they generally reduce the number of derivations in the search space. For this reason they also apply in top-down search procedures such as the inverse method introduced in Chapter 5.

4.1 Inversion

The simplest way to avoid non-determinism is to consider those propositions on the left or right for which there is a unique way to apply a corresponding left or right rule. For example, to prove $A \wedge B$ we can immediately apply the right rule without losing completeness. On the other hand, to prove $A \vee B$ we can not immediately apply a left rule. As a counterexample consider $B \vee A \Longrightarrow A \vee B$, where we first need to apply a left rule.

On a given sequent, a number of invertible rules may be applicable. However, the order of this choice does not matter. In other words, we have replaced *don't-know* non-determinism by *don't-care* non-determinism.

Determining the invertibility of left rules in order to support this strategy requires some additional considerations. The pure inversion property states that the premises should be derivable if and only if the conclusion is. However, in left rule the principal formula is still present in the premises, which means we can continue to apply the same left rule over and over again leading to non-termination. So we require in addition that the principal formula of a left rule is no longer needed, thereby guaranteeing the termination of the inversion phase of the search.

Theorem 4.1 (Inversion)

1. *If* $\Gamma \Longrightarrow A \wedge B$ *then* $\Gamma \Longrightarrow A$ *and* $\Gamma \Longrightarrow B$*.*
2. *If* $\Gamma \Longrightarrow A \supset B$ *then* $\Gamma, A \Longrightarrow B$*.*
3. *If* $\Gamma \Longrightarrow \forall x.\ A$ *then* $\Gamma \Longrightarrow [a/x]A$ *for a new individual parameter* a*.*
4. *If* $\Gamma \Longrightarrow \neg A$ *then* $\Gamma, A \Longrightarrow p$ *for a new propositional parameter* p*.*
5. *If* $\Gamma, A \wedge B \Longrightarrow C$ *then* $\Gamma, A, B \Longrightarrow C$*.*
6. *If* $\Gamma, \top \Longrightarrow C$ *then* $\Gamma \Longrightarrow C$*.*
7. *If* $\Gamma, A \vee B \Longrightarrow C$ *then* $\Gamma, A \Longrightarrow C$ *and* $\Gamma, B \Longrightarrow C$*.*
8. *If* $\Gamma, \exists x.\ A \Longrightarrow C$ *then* $\Gamma, [a/x]A \Longrightarrow C$ *for a new individual parameter* a*.*

Proof: By induction over the structure of the given derivations. Parts (5) and (6) are somewhat different in that they extract an inversion property from two and zero left rules, respectively. The proof is nonetheless routine.

Alternatively, we can take advantage of the admissibility of cut to avoid another inductive proof. For example, to show the first property, we can reason as follows:

$\Gamma \Longrightarrow A \wedge B$	Assumption
$\Gamma, A \wedge B, A \Longrightarrow A$	By rule init
$\Gamma, A \wedge B \Longrightarrow A$	By rule $\wedge\mathrm{L}_1$
$\Gamma \Longrightarrow A$	By admissibility of cut (Theorem 3.11)

See also Exercise 4.1. □

The rules $\top$R and $\bot$L are a special case: they can be applied eagerly without losing completeness, but these rules have no premises and therefore do not admit a theorem of the form above. None of the other rules permit an inversion property, as the following counterexamples show. These counterexamples can easily be modifed so that they are not initial sequents.

1. $A \vee B \Longrightarrow A \vee B$ (both $\vee\mathrm{R}_1$ or $\vee\mathrm{R}_2$ lead to an unprovable sequent).
2. $\bot \Longrightarrow \bot$ (no right rule applicable).
3. $\exists x.\ A \Longrightarrow \exists x.\ A$ ($\exists$R leads to an unprovable sequent).

4. $A \supset B \Longrightarrow A \supset B$ ($\supset$L leads to an unprovable sequent).

5. $\neg A \Longrightarrow \neg A$ ($\neg$L leads to an unprovable sequent).

6. $\forall x.\ A \Longrightarrow \forall x.\ A$ ($\forall$L leads to an unprovable sequent if we erase the original copy of $\forall x.\ A$).

Now we can write out a pure inversion strategy in the form of an inference system. One difficulty with such a system is that the don't-care non-determinism is not directly visible and has to be remarked on separately. We also refer to don't-care non-determinism as *conjunctive non-determinism*: eventually, all applicable rules have to be applied, but their order is irrelevant as far as provability is concerned.

First, we distinguish those kinds of propositions for which either the left or the right rule is *not* invertible. We call them *synchronous* propositions (either on the left or on the right).[1] The remaining propositions are called *asynchronous*. This terminology comes from the study of concurrency where an asynchronously computing processes proceed independently of all other processes, while a synchronously computing process may have to wait for other processes.

$$\begin{array}{rcll}
\text{Left synchronous propositions} & L & ::= & P \mid A_1 \supset A_2 \mid \forall x.\ A \\
\text{Right synchronous propositions} & R & ::= & P \mid A_1 \vee A_2 \mid \bot \mid \exists x.\ A \\
\text{Passive antecedents} & \Delta & ::= & \cdot \mid \Delta, L
\end{array}$$

Note that we will revise this classification in Section 4.3. Sequents are composed of four judgments: left and right propositions, each of which may be active or passive. In order to simplify the notation, we collect like judgments into zones, keeping in mind that there can only be one proposition on the right. The active propositions that are decomposed asynchronously will be written in the center, the synchronous ones move to the outside for later consideration.

Sequents are written as

$$\Delta; \Omega \Longrightarrow A; \cdot \quad \text{and} \quad \Delta; \Omega \Longrightarrow \cdot; R$$

where the outer zones containing Δ or R are passive and the inner zones containing Ω or A are active. We still think of Δ as unordered, but it is important that Ω is ordered in order to avoid spurious non-deterministic choices. We must always work on its right end. We break down the principal connectives of asynchronous propositions eagerly, moving synchronous propositions into the passive zones, until all asynchronous connectives have been decomposed. At that point we have to choose one of the passive (synchronous) propositions. If this attempt fails we have to backtrack and try other choices.

In order to prove a sequent $\Gamma \Longrightarrow A$, we initialize our inversion-based procedure with the sequent $\cdot; \Gamma \Longrightarrow A; \cdot$, where the order we choose for the elements of Γ is irrelevant.

[1] For the moment, we do not consider negation explicitly—think of it as defined.

Right Asynchronous Propositions. First, we decompose the right asynchronous connectives.

$$\frac{\Delta; \Omega \Longrightarrow A; \cdot \qquad \Delta; \Omega \Longrightarrow B; \cdot}{\Delta; \Omega \Longrightarrow A \wedge B; \cdot} \wedge\mathrm{R} \qquad \frac{}{\Delta; \Omega \Longrightarrow \top} \top\mathrm{R}$$

$$\frac{\Delta; \Omega, A \Longrightarrow B; \cdot}{\Delta; \Omega \Longrightarrow A \supset B; \cdot} \supset\mathrm{R} \qquad \frac{\Delta; \Omega \Longrightarrow [a/x]A; \cdot}{\Delta; \Omega \Longrightarrow \forall x.\, A; \cdot} \forall\mathrm{R}^a$$

$$\frac{\Delta; \Omega \Longrightarrow \cdot; R}{\Delta; \Omega \Longrightarrow R; \cdot} R\mathrm{R}$$

The last rule moves the right synchronous proposition into the passive zone.

Left Asynchronous Propositions. When the proposition on the right is passive, we break down the left asynchronous connectives in the active zone on the left. Recall that Ω is considered in order, so there is no non-determinism.

$$\frac{\Delta; \Omega, A, B \Longrightarrow \cdot; R}{\Delta; \Omega, A \wedge B \Longrightarrow \cdot; R} \wedge\mathrm{L} \qquad \frac{\Delta; \Omega \Longrightarrow \cdot; R}{\Delta; \Omega, \top \Longrightarrow \cdot; R} \top\mathrm{L}$$

$$\frac{\Delta; \Omega, A \Longrightarrow \cdot; R \qquad \Delta; \Omega, B \Longrightarrow \cdot; R}{\Delta; \Omega, A \vee B \Longrightarrow \cdot; R} \vee\mathrm{L} \qquad \frac{}{\Delta; \Omega, \bot \Longrightarrow \cdot; R} \bot\mathrm{L}$$

$$\frac{\Delta; \Omega, [a/x]A \Longrightarrow \cdot; R}{\Delta; \Omega, \exists x.\, A \Longrightarrow \cdot; R} \exists\mathrm{L}^a$$

$$\frac{\Delta, L; \Omega \Longrightarrow \cdot; R}{\Delta; \Omega, L \Longrightarrow \cdot; R} L\mathrm{L}$$

The last rule allows us to move synchronous propositions into the passive zone.

Right Synchronous Propositions. The active rules always terminate when applied in a bottom-up fashion during proof search (see Lemma 4.7). Now a don't-know non-deterministic choice arises: either we apply a right rule to infer R or a left rule to one of the passive assumptions in Δ. We also refer to don't-know non-determinism as *disjunctive non-determinism* since we have to pick one of several possibilities.

$$\frac{\Delta; \cdot \Longrightarrow A; \cdot}{\Delta; \cdot \Longrightarrow \cdot; A \vee B} \vee\mathrm{R}_1 \qquad \frac{\Delta; \cdot \Longrightarrow B; \cdot}{\Delta; \cdot \Longrightarrow \cdot; A \vee B} \vee\mathrm{R}_2$$

$$\textit{no right rule for } \bot \qquad \frac{\Delta; \cdot \Longrightarrow [t/x]A; \cdot}{\Delta; \cdot \Longrightarrow \cdot; \exists x.\, A} \exists\mathrm{R}$$

In the last case we would have to guess the t, but in practice the t is determined by unification as indicated in Section 4.4.

Left Synchronous Propositions. Left synchronous propositions may be needed more than once, so they are duplicated in the application of the left rules.

$$\frac{\Delta, A \supset B; \cdot \Longrightarrow A; \cdot \qquad \Delta, A \supset B; B \Longrightarrow \cdot; R}{\Delta, A \supset B; \cdot \Longrightarrow \cdot; R} {\supset}\mathrm{L}$$

$$\frac{\Delta, \forall x.\ A; [t/x]A \Longrightarrow \cdot; R}{\Delta, \forall x.\ A; \cdot \Longrightarrow \cdot; R} \forall\mathrm{L}$$

Initial Sequents. This leaves the question of initial sequents, which is easily handled by allowing an passive atomic proposition on the left to match a passive atomic proposition on the right.

$$\frac{}{\Delta, P; \cdot \Longrightarrow \cdot; P} \mathrm{init}$$

The judgments $\Delta; \Omega \Longrightarrow A; \cdot$ and $\Delta; \Omega \Longrightarrow \cdot; R$ are hypothetical in Δ, but *not* hypothetical in Ω in the usual sense. This is because proposition in Ω do not persist, because they have to be empty in the initial sequents, and because they must be considered in order. In other words, contraction, weakening, and exchange are not available for Ω. These turn out to be admissible, but the structure of the proof is changed globally. Therefore we consider it an *ordered hypothetical judgment* where each hypothesis must be used exactly once in a derivation, in the given order. We do not formalize this notion any further, but just remark that appropriate versions of the substitution property can be devised to explain its meaning.

First, the soundness theorem is straightforward, since inversion proofs merely eliminate some disjunctive non-determinism.

Theorem 4.2 (Soundness of Inversion Proofs)
If $\Delta; \Omega \Longrightarrow A; \cdot$ *or* $\Delta; \Omega \Longrightarrow \cdot; A$ *then* $\Delta, \Omega \Longrightarrow A$.

Proof: By a straightforward induction over the given derivation, applying weakening in some cases. □

The completeness theorem requires a number of inversion lemmas. For a possible alternative path, see Exercise 4.2. The first set of results expresses the invertibility of the rules concerning the active propositions. That is, we can immediately apply any invertible rule witout losing completeness. The second set of results expresses the opposite: we can always postpone the non-invertible rules until all invertible rules have been applied.

We use the notation $\Delta; \Omega \Longrightarrow \rho$ to stand for $\Delta; \Omega \Longrightarrow A; \cdot$ or $\Delta; \Omega \Longrightarrow \cdot; R$.

Lemma 4.3 (Inversion on Asynchronous Connectives)

1. $\Delta; \Omega \Longrightarrow A \wedge B; \cdot$ *iff* $\Delta; \Omega \Longrightarrow A; \cdot$ *and* $\Delta; \Omega \Longrightarrow B; \cdot$.

2. $\Delta; \Omega \Longrightarrow A \supset B; \cdot$ *iff* $\Delta; \Omega, A \Longrightarrow B; \cdot$.

3. $\Delta; \Omega \Longrightarrow \forall x.\, A; \cdot$ *iff* $\Delta; \Omega \Longrightarrow [a/x]A; \cdot$ *for any new parameter* a.

4. $\Delta; \Omega \Longrightarrow R; \cdot$ *iff* $\Delta; \Omega \Longrightarrow \cdot; R$ *for* R *right synchronous.*

5. $\Delta; \Omega_1, A \wedge B, \Omega_2 \Longrightarrow \rho$ *iff* $\Delta; \Omega_1, A, B, \Omega_2 \Longrightarrow \rho$.

6. $\Delta; \Omega_1, \top, \Omega_2 \Longrightarrow \rho$ *iff* $\Delta; \Omega_1, \Omega_2 \Longrightarrow \rho$.

7. $\Delta; \Omega_1, A \vee B, \Omega_2 \Longrightarrow \rho$ *iff* $\Delta; \Omega_1, A, \Omega_2 \Longrightarrow \rho$ *and* $\Delta; \Omega_1, B, \Omega_2 \Longrightarrow \rho$.

8. $\Delta; \Omega_1, \exists x.A, \Omega_2 \Longrightarrow \rho$ *iff* $\Delta; \Omega_1, [a/x]A, \Omega_2 \Longrightarrow \rho$ *for any new param.* a.

9. $\Delta; \Omega_1, L, \Omega_2 \Longrightarrow \rho$ *iff* $\Delta, L; \Omega_1, \Omega_2 \Longrightarrow \rho$ *for* L *left synchronous.*

Proof: In each direction the result is either immediate by a rule, by inversion, or follows by a straightforward induction on the structure of the given derivation. □

The dual lemma shows that rules acting on synchronous propositions can be postponed until after the asynchronous rules. We define the *active size* of a sequent $\Delta; \Omega \Longrightarrow A; \cdot$ or $\Delta; \Omega \Longrightarrow \cdot; R$ as the number of logical quantifiers, connectives, constants, and atomic propositions in Ω and A. Note that the active size of a sequent is 0 if and only if it has the form $\Delta; \cdot \Longrightarrow \cdot; R$.

Lemma 4.4 (Postponement of Synchronous Connectives)

1. *If* $\Delta; \Omega \Longrightarrow A; \cdot$ *or* $\Delta; \Omega \Longrightarrow \cdot; A$ *then* $\Delta; \Omega \Longrightarrow \cdot; A \vee B$.

2. *If* $\Delta; \Omega \Longrightarrow B; \cdot$ *or* $\Delta; \Omega \Longrightarrow \cdot; B$ *then* $\Delta; \Omega \Longrightarrow \cdot; A \vee B$.

3. *If* $\Delta; \Omega \Longrightarrow [t/x]A; \cdot$ *or* $\Delta; \Omega \Longrightarrow \cdot; [t/x]A$ *then* $\Delta; \Omega \Longrightarrow \cdot; \exists x.\, A$.

4. *If* $(\Delta, A \supset B); (\Omega_1, \Omega_2) \Longrightarrow A; \cdot$ *and* $(\Delta, A \supset B); (\Omega_1, B, \Omega_2) \Longrightarrow \rho$ *then* $(\Delta, A \supset B); (\Omega_1, \Omega_2) \Longrightarrow \rho$.

5. *If* $(\Delta, \forall x.\, A); (\Omega_1, [t/x]A, \Omega_2) \Longrightarrow \rho$ *then* $(\Delta, \forall x.\, A); (\Omega_1, \Omega_2) \Longrightarrow \rho$.

Proof: By induction on the active size of the given sequent. For the right rules (parts (1), (2), and (3)), the base cases are $\Omega = \cdot$, in which case the conclusion follows directly by a rule. For the left rules, the base case is $\Omega = \cdot$ and $\rho = \cdot; R$, in which case the conclusion follows directly by a rule. In all other case we apply inversion to an element of Ω (Lemma 4.3) or C (if $\rho = C; \cdot$) and appeal to the induction hypothesis. Since the right-hand sides of the inversion principles have smaller active size than the left-hand sides, we are correct in applying the induction hypothesis. We show two cases in the proof of part (4).

Case: $\Omega = \cdot$ and $\rho = \cdot; R$.

$(\Delta, A \supset B); B \Longrightarrow \cdot; R$	Assumption
$(\Delta, A \supset B); \cdot \Longrightarrow A; \cdot$	Assumption
$(\Delta, A \supset B); \cdot \Longrightarrow \cdot; R$	By rule $\supset$L

Case: $\Omega = \Omega', C \vee D$.

$(\Delta, A \supset B); \Omega', C \vee D, B \Longrightarrow \rho$	Assumption
$(\Delta, A \supset B); \Omega', C, B \Longrightarrow \rho$ and	
$(\Delta, A \supset B); \Omega', D, B \Longrightarrow \rho$	By inversion
$(\Delta, A \supset B); \Omega', C \vee D \Longrightarrow A; \cdot$	Assumption
$(\Delta, A \supset B); \Omega', C \Longrightarrow A; \cdot$ and	
$(\Delta, A \supset B); \Omega', D \Longrightarrow A; \cdot$	By inversion
$(\Delta, A \supset B); \Omega', C \Longrightarrow \rho$	By i.h. on Ω', C
$(\Delta, A \supset B); \Omega', D \Longrightarrow \rho$	By i.h. on Ω', D
$(\Delta, A \supset B); \Omega', C \vee D \Longrightarrow \rho$	By rule $\vee$L

□

For the proof of completeness, and also to permit some optimizations in the search procedure, we need to show that weakening and contraction for propositions in Ω are admissible, at the price of possibly lengthening the derivation. Note that weakening and contraction for Δ is trivial, since inversion sequents *are* hypothetical in Δ.

Lemma 4.5 (Structural Properties of Inversion Sequents)

1. *If* $\Delta; \Omega \Longrightarrow \rho$ *then* $(\Delta, A); \Omega \Longrightarrow \rho$.
2. *If* $(\Delta, A, A); \Omega \Longrightarrow \rho$ *then* $(\Delta, A); \Omega \Longrightarrow \rho$.
3. *If* $\Delta; (\Omega_1, \Omega_2) \Longrightarrow \rho$ *then* $\Delta; (\Omega_1, A, \Omega_2) \Longrightarrow \rho$.
4. *If* $\Delta; (\Omega_1, A, A, \Omega_2) \Longrightarrow \rho$ *then* $\Delta; (\Omega_1, A, \Omega_2) \Longrightarrow \rho$.

Proof: Parts (1) and (2) follow as usual by straightforward structural inductions over the given derivations. Parts (3) and (4) follow by induction on the structure of A, taking advantage of the inversion properties for asynchronous propositions (Lemma 4.3) and parts (1) and (2) for synchronous propositions. □

Theorem 4.6 (Completeness of Inversion Proofs)
If $\Omega \Longrightarrow A$ *then* $\cdot; \Omega \Longrightarrow A; \cdot$.

Proof: By induction on the structure of the given sequent derivation $\mathcal{S}$, taking advantage of the inversion, postponement, and structural properties proven in this section. We think of the ordinary left rules of the sequent calculus as operating on some proposition in the middle of Ω, rather than explicitly dealing with exchange. We consider in turn: invertible right rules, invertible left rules, initial sequents, non-invertible right rules and non-invertible left rules.

Case:

$$\mathcal{S} = \dfrac{\begin{array}{cc}\mathcal{S}_1 & \mathcal{S}_2\\ \Omega \Longrightarrow A_1 & \Omega \Longrightarrow A_2\end{array}}{\Omega \Longrightarrow A_1 \wedge A_2}\,\wedge\mathrm{R}$$

$$\begin{array}{ll}
\cdot;\Omega \Longrightarrow A_1;\cdot & \text{By i.h. on } \mathcal{S}_1\\
\cdot;\Omega \Longrightarrow A_2;\cdot & \text{By i.h. on } \mathcal{S}_2\\
\cdot;\Omega \Longrightarrow A_1 \wedge A_2;\cdot & \text{By Lemma 4.3(1)}
\end{array}$$

Cases: The right invertible rules $\supset$R and $\forall$R and also the case for $\top$R are similar to the case for $\wedge$R.

Case:

$$\mathcal{S} = \dfrac{\begin{array}{cc}\mathcal{S}_1 & \mathcal{S}_2\\ \Omega_1, B_1 \vee B_2, B_1, \Omega_2 \Longrightarrow A & \Omega_1, B_1 \vee B_2, B_2, \Omega_2 \Longrightarrow A\end{array}}{\Omega_1, B_1 \vee B_2, \Omega_2 \Longrightarrow A}\,\vee\mathrm{L}$$

$$\begin{array}{ll}
\cdot;\Omega_1, B_1 \vee B_2, B_1, \Omega_2 \Longrightarrow A;\cdot & \text{By i.h. on } \mathcal{S}_1\\
\cdot;\Omega_1, B_1 \vee B_2, B_2, \Omega_2 \Longrightarrow A;\cdot & \text{By i.h. on } \mathcal{S}_2\\
\cdot;\Omega_1, B_1 \vee B_2, B_1 \vee B_2, \Omega_2 \Longrightarrow A;\cdot & \text{By Lemma 4.3(7)}\\
\cdot;\Omega_1, B_1 \vee B_2, \Omega_2 \Longrightarrow A;\cdot & \text{By contraction (Lemma 4.5)}
\end{array}$$

Cases: The left invertible rule $\exists$L and also the case for $\bot$L are similar to the case for $\vee$L.

Case:

$$\mathcal{S} = \dfrac{\begin{array}{c}\mathcal{S}_1\\ \Omega_1, B_1 \wedge B_2, B_1, \Omega_2 \Longrightarrow A\end{array}}{\Omega_1, B_1 \wedge B_2, \Omega_2 \Longrightarrow A}\,\wedge\mathrm{L}_1$$

$$\begin{array}{ll}
\cdot;\Omega_1, B_1 \wedge B_2, B_1, \Omega_2 \Longrightarrow A;\cdot & \text{By i.h. on } \mathcal{S}_1\\
\cdot;\Omega_1, B_1 \wedge B_2, B_1, B_2, \Omega_2 \Longrightarrow A;\cdot & \text{By weakening (Lemma 4.5)}\\
\cdot;\Omega_1, B_1 \wedge B_2, B_1 \wedge B_2, \Omega_2 \Longrightarrow A & \text{By Lemma 4.3(5)}\\
\cdot;\Omega_1, B_1 \wedge B_2, \Omega_2 \Longrightarrow A & \text{By contraction (Lemma 4.5)}
\end{array}$$

Case: The case for $\wedge\mathrm{L}_2$ is symmetric to $\wedge\mathrm{L}_1$. Note that there is no left rule for $\top$ in the sequent calculus, so the $\top$L rule on inversion sequents arises only from weakening (see the following case).

Case:

$$\mathcal{S} = \dfrac{}{\Omega_1, P, \Omega_2 \Longrightarrow P}\,\mathrm{init}$$

$P; \cdot \Longrightarrow \cdot; P$	By rule init
$\cdot; P \Longrightarrow \cdot; P$	By rule LL
$\cdot; P \Longrightarrow P; \cdot$	By rule RR
$\cdot; \Omega_1, P, \Omega_2 \Longrightarrow P; \cdot$	By weakening (Lemma 4.5)

Case:

$$\mathcal{S} = \cfrac{\begin{matrix}\mathcal{S}_1 \\ \Omega \Longrightarrow A_1\end{matrix}}{\Omega \Longrightarrow A_1 \vee A_2}\,\vee\mathrm{R}_1$$

$\cdot; \Omega \Longrightarrow A_1; \cdot$	By i.h. on $\mathcal{S}_1$
$\cdot; \Omega \Longrightarrow \cdot; A_1 \vee A_2$	By postponement (Lemma 4.4)
$\cdot; \Omega \Longrightarrow A_1 \vee A_2; \cdot$	By rule RR

Cases: The cases for the non-invertible right rules $\vee\mathrm{R}_2$ and $\exists\mathrm{R}$ are similar to $\vee\mathrm{R}_1$.

Case:

$$\mathcal{S} = \cfrac{\begin{matrix}\mathcal{S}_1 \\ \Omega_1, B_1 \supset B_2, \Omega_2 \Longrightarrow B_1\end{matrix} \qquad \begin{matrix}\mathcal{S}_2 \\ \Omega_1, B_1 \supset B_2, B_2, \Omega_2 \Longrightarrow A\end{matrix}}{\Omega_1, B_1 \supset B_2, \Omega_2 \Longrightarrow A}\,{\supset}\mathrm{L}$$

$\cdot; \Omega_1, B_1 \supset B_2, \Omega_2 \Longrightarrow B_1; \cdot$	By i.h. on $\mathcal{S}_1$
$B_1 \supset B_2; \Omega_1, \Omega_2 \Longrightarrow B_1; \cdot$	By inversion (Lemma 4.3(9))
$\cdot; \Omega_1, B_1 \supset B_2, B_2, \Omega_2 \Longrightarrow A; \cdot$	By i.h. on $\mathcal{S}_2$
$B_1 \supset B_2; \Omega_1, B_2, \Omega_2 \Longrightarrow A; \cdot$	By inversion (Lemma 4.3(9))
$B_1 \supset B_2; \Omega_1, \Omega_2 \Longrightarrow A; \cdot$	By postponement (Lemma 4.4)
$\cdot; \Omega_1, B_1 \supset B_2, \Omega_2 \Longrightarrow A; \cdot$	By Lemma 4.3(9)

Case: The cases for the non-invertible left rule $\forall\mathrm{L}$ is similar to $\supset$L.

□

We can also show that the active rules always terminate, which is important for the algorithm.

Lemma 4.7 (Termination of Active Rules)
Given a goal $\Delta; \Omega \Longrightarrow \rho$. Any sequence of applications of active rules terminates.

Proof: By induction on the active size of the given sequent. □

Next we describe a non-deterministic algorithm for proof search. There are a number of ways to eliminate the remaining disjunctive non-determinism. Typical is depth-first search, made complete by iterative deepening. The choice of the term t in the rules $\exists$R and $\forall$L is later solved by introducing free variables and equational constraints into the search procedures which are solved by unification (see Section 4.4). Many futher refinements and improvements are possible on this procedures, but not discussed here.

Given a goal $\Delta; \Omega \Longrightarrow \rho$.

1. If $\Omega = \cdot$ and $\rho = \cdot; P$ succeed if P is in Δ.

2. If $\Omega = \cdot$ and $\rho = \cdot; R$, but the previous case does not apply, guess an inference rule to reduce the goal. In the cases of ∃R and ∀L we also have to guess a term t. Solve each subgoal by recursively applying the procedure. This case represents a disjunctive choice (don't know non-determinism). If no rule applies, we fail.

3. If Ω is non-empty or $\rho = A; \cdot$, use the unique applicable active rule and solve each of the subgoals by recursively applying the procedure.

This search procedure is clearly sound, because the inversion proof system is sound (Theorem 4.2). Furthermore, if there is a derivation the procedure will (in principle) always terminate and find some derivation if it guesses correctly in step (2).

4.2 Backchaining

While the inversion properties from the previous section are critical for constructing efficient theorem provers, they far from sufficient. The difficulty is that many non-deterministic choices remain. In this section we discuss a particular strategy called *backchaining* which has applications outside of theorem proving, for example, in logic programming. We restrict ourselves to *Horn logic*, a particularly simple logic that is useful in many circumstances. In the next section we describe *focusing*, which is the generalization of backchaining to full intuitionistic logic.

In many theorem proving problems we are in a situation where we have a number of propositions describing a *theory* and then a proposition we would like to prove with respect to that theory. Theories are often given in the form of propositions $\forall x_1 \ldots \forall x_n.\, P_1 \wedge \ldots \wedge P_k \supset P$. These hypotheses are synchronous (in the sense of the previous section), that is, we have to choose between them when trying to prove some atomic proposition Q. Backchaining rests on two observations. The first is that search remains complete if we only try to use those assumptions where P and Q can be made equal by instantiating $x_1, \ldots, x_n$ with appropriate terms. The second is that once we decide which assumption to use, we can apply a whole sequence of left rules (here ∀L and ⊃L) without considering any other synchronous assumption.

Both of these observation are of crucial importance. The first cuts down on the number of assumptions we may use. The second drastically reduces the non-determinism. To see the latter, consider a theory with m clauses defining a predicate p and that ach clause has n universal quantifiers. With backchaining (and unification, see Section 4.4) we create one choice with m alternatives. With just the inversion strategy, we have m choices in the first step, then $m+1$ choices in the second step after instantiating one quantifier, and so on, yielding

$m(m+1)\cdots(m+p)$ choices. As the main theorem of this section and the next shows, these choices are redundant.

We first define Horn clauses in a form that is slightly more general than what is usually given in the literature.

$$\begin{array}{rcll}
\text{Horn clauses} & D & ::= & P \mid G \supset D \mid \forall x.\, D \\
\text{Horn goals} & G & ::= & P \mid G_1 \wedge G_1 \mid \top \\[1ex]
\text{Horn theories} & \Delta & ::= & \cdot \mid \Delta, D
\end{array}$$

Some further generalizations are possible; important for us is the absence of implications and universal quantification in goals as well as existential, disjunction, and falsehood in clauses.

A theorem proving problem in Horn logic is stated as

$$\Delta \Longrightarrow G$$

where Δ is a Horn theory and G is a Horn goal, that is, a conjunction of atomic propositions.

As two simple examples of Horn theories we consider even and odd numbers, and graph reachability.

For even/odd number we have constants $\mathsf{0}$ and s to represent the natural numbers in unary form. As usual, we abbreviate $\mathsf{0}()$ with just $\mathsf{0}$.

$$\begin{array}{l}
\mathsf{even}(\mathsf{0}), \\
\forall x.\, \mathsf{even}(x) \supset \mathsf{odd}(\mathsf{s}(x)), \\
\forall x.\, \mathsf{odd}(x) \supset \mathsf{even}(\mathsf{s}(x))
\end{array}$$

For reachability in a directed graph we assume we have a constant for each node in the graph and an assumption $\mathsf{edge}(a, b)$ for each edge from node a to node b. In addition we assume

$$\begin{array}{l}
\forall x.\, \forall y.\, \mathsf{edge}(x, y) \supset \mathsf{reach}(x, y), \\
\forall x.\, \forall y.\, \forall z.\, \mathsf{reach}(x, y) \wedge \mathsf{reach}(y, z) \supset \mathsf{reach}(x, z)
\end{array}$$

In the even/odd example, we would like for backchaining to reduce the goal $\mathsf{even}(\mathsf{s}(\mathsf{s}(\mathsf{0})))$ to the subgoal $\mathsf{odd}(\mathsf{s}(\mathsf{0}))$. In this case this reduction should be essentially deterministic, because only the last clause could match the goal. We formalize backchaining with the following two judgments.

$$\begin{array}{ll}
\Delta \overset{u}{\Longrightarrow} G & \text{Horn theory } \Delta \text{ proves } G \text{ uniformly} \\
\Delta; D \overset{u}{\Longrightarrow} P & \text{Backchaining on Horn clause } D \text{ proves } P
\end{array}$$

First the rules of uniform proof, which are rather simple. The critical one is the last, which selects a Horn clause from Δ for backchaining.

$$\frac{\Delta \overset{u}{\Longrightarrow} G_1 \qquad \Delta \overset{u}{\Longrightarrow} G_2}{\Delta \overset{u}{\Longrightarrow} G_1 \wedge G_2}\,\wedge\mathrm{R} \qquad\qquad \frac{}{\Delta \overset{u}{\Longrightarrow} \top}\,\top\mathrm{R}$$

$$\frac{\Delta; D \overset{u}{\Longrightarrow} P \qquad (D \text{ in } \Delta)}{\Delta \overset{u}{\Longrightarrow} P}\,\mathrm{select}$$

The rules for backchaining consider the possible forms of the Horn clause, decomposing it by a left rule. When using this as a proof search procedure by interpreting it bottom-up, we imagine using unification variables instead of guessing terms, and solving left-most premises first.

$$\frac{}{\Delta; P \overset{u}{\Longrightarrow} P}\,\text{init} \qquad (\Delta; P \overset{u}{\Longrightarrow} Q \text{ fails for } P \neq Q)$$

$$\frac{\Delta; D \overset{u}{\Longrightarrow} P \qquad \Delta \overset{u}{\Longrightarrow} G}{\Delta; G \supset D \overset{u}{\Longrightarrow} P}\,{\supset}\text{L} \qquad \frac{\Delta; [t/x]D \overset{u}{\Longrightarrow} P}{\Delta; \forall x.\, D \overset{u}{\Longrightarrow} P}\,\forall\text{L}$$

It is not difficult to see that this indeed captures the intended proof search strategy for backchaining. It is also rather straightforward to prove it sound and complete.

Theorem 4.8 (Soundness of Uniform Proofs in Horn Theories)

1. *If* $\Delta \overset{u}{\Longrightarrow} G$ *then* $\Delta \Longrightarrow G$.
2. *If* $\Delta; D \overset{u}{\Longrightarrow} G$ *then* $\Delta, D \Longrightarrow G$.

Proof: By straightforward induction over the given derivations. In the case of the select rule, we require the admissibility of contraction in the sequent calculus. □

For the completeness direction we need a postponement lemma, similar to the case of inversion proofs. This lemma demonstrates that the left rules of the sequent calculus are admissible for the passive propositions of uniform sequents.

Lemma 4.9 (Postponement for Uniform Proofs)

1. *If* $\Delta, G \supset D, D; D' \overset{u}{\Longrightarrow} P$ *and* $\Delta, G \supset D \overset{u}{\Longrightarrow} G$ *then* $\Delta, G \supset D; D' \overset{u}{\Longrightarrow} P$
2. *If* $\Delta, G \supset D, D \overset{u}{\Longrightarrow} G'$ *and* $\Delta, G \supset D \overset{u}{\Longrightarrow} G$ *then* $\Delta, G \supset D \overset{u}{\Longrightarrow} G'$
3. *If* $\Delta, \forall x.\, D, [t/x]D; D' \overset{u}{\Longrightarrow} P$ *then* $\Delta, \forall x.\, D; D' \overset{u}{\Longrightarrow} P$
4. *If* $\Delta, \forall x.\, D, [t/x]D \overset{u}{\Longrightarrow} G'$ *then* $\Delta, \forall x.\, D \overset{u}{\Longrightarrow} G'$

Proof: By straightforward inductions over the first given derivation. □

Theorem 4.10 (Completness of Uniform Proofs in Horn Theories)

1. *If* $\Delta \Longrightarrow G$ *then* $\Delta \overset{u}{\Longrightarrow} G$.
2. *If* $\Delta \Longrightarrow P$ *then there is a* D *in* Δ *such that* $\Delta; D \overset{u}{\Longrightarrow} P$.

Proof: Part (1) follows by inversion properties of the sequent calculus. We show one case of Part (2).

Case:

$$\mathcal{S} = \cfrac{\begin{array}{cc} \mathcal{S}_1 & \mathcal{S}_2 \\ \Delta', G \supset D \Longrightarrow G & \Delta', G \supset D, D \Longrightarrow P \end{array}}{\Delta', G \supset D \Longrightarrow P} \supset\!L$$

$\Delta', G \supset D, D; D' \overset{u}{\Longrightarrow} P$ for some D' in $\Delta', G \supset D, D$	By i.h. on $\mathcal{S}_2$
$\Delta', G \supset D \overset{u}{\Longrightarrow} G$	By i.h. on $\mathcal{S}_1$
$\Delta', G \supset D; D' \overset{u}{\Longrightarrow} P$	By Lemma 4.9
If D' in $\Delta', G \supset D$ we are done	
If $D' = D$:	
$\Delta', G \supset D; G \supset D \overset{u}{\Longrightarrow} P$	By rule $\supset$L

□

Horn theories have a number of important properties. Some of these stem from the fact that during proof search, the collection of assumptions Δ never changes, nor will there ever be any new parameters introduced. This allows us to give an *inductive* interpretation to the set of clauses. For example, we could reason inductively about properties of even numbers, rather than just reason in first-order logic.

A related property is that Horn clauses can be seen to define *inference rules.* For example, we can translate the theory defining the even and odd numbers into the rules

$$\cfrac{}{\mathsf{even}(0)} \qquad \cfrac{\mathsf{even}(t)}{\mathsf{odd}(\mathsf{s}(t))} \qquad \cfrac{\mathsf{odd}(t)}{\mathsf{even}(\mathsf{s}(t))}$$

In fact, one can see the uniform proof system and backchaining as implementing precisely these rules. In other words, we can also *compile* a Horn theory into a set of inference rules and then prove Horn goals from no assumptions, but using the additional rules.

This view is also interesting in that it provides the basis for a forward-reasoning procedure for Horn logic that resembles the inverse method. However, all sequents we ever consider have an empty left-hand side! That is, from some atomic facts, using unary inference rules (possibly with multiple premises), we derive further facts. We illustrate this way of proceeding using our second Horn theory which implements a particular graph. First, we turning the theory

$$\begin{array}{l} \forall x.\, \forall y.\, \mathsf{edge}(x,y) \supset \mathsf{reach}(x,y), \\ \forall x.\, \forall y.\, \forall z.\, \mathsf{reach}(x,y) \wedge \mathsf{reach}(y,z) \supset \mathsf{reach}(x,z) \end{array}$$

into the inference rules

$$\cfrac{\mathsf{edge}(s,t)}{\mathsf{reach}(s,t)} \qquad \cfrac{\mathsf{reach}(s,t) \qquad \mathsf{reach}(t,u)}{\mathsf{reach}(s,u)}$$

Second, assume we start with facts

$$\mathsf{edge}(a,b), \mathsf{edge}(b,c)$$

Applying all possible rules we obtain

$$\begin{array}{l}\mathsf{edge}(a,b), \mathsf{edge}(b,c),\\ \mathsf{reach}(a,b), \mathsf{reach}(b,c)\end{array}$$

After one more step we have

$$\begin{array}{l}\mathsf{edge}(a,b), \mathsf{edge}(b,c),\\ \mathsf{reach}(a,b), \mathsf{reach}(b,c),\\ \mathsf{reach}(a,c)\end{array}$$

Now applying any more rules does not add any more facts: the set of facts is *saturated*. We can now see if the goal (e.g., $\mathsf{reach}(c,a)$) is in the saturated set or not. If yes it is true, if not it cannot be derived from the given facts.

The above strategy can be generalized to the case of facts with free variables (which are universally interpreted) and is known under the name of *unit resolution*.

It is interesting that the forward chaining strategy works particularly well for Horn theories such as for reach which can easily be seen to be terminating. This is because no new terms are constructed during the inferences. On the other hand, the backward chaining strategy we exemplified using even and odd can easily be seen to be terminating in the backward directions because the term involved get smaller.

As far as I know, it is still an open research problem how backward chaining and forward chaining (here illustrated with unit resolution) can be profitably combined. Also, the relationship between the inverse method and unit (or general) resolution is unclear in the sense that we do not know of a proposal that effectively combines these strategies.

4.3 Focusing

The search procedure based on inversion developed in Section 4.1 still has an unacceptable amount of don't know non-determinism. For the Horn fragment, we addressed this issue in Section 4.2; here we combine backchaining with inversion in order to obtain a method that works for full intuitionistic logic.

We first recall the problem with the inversion strategy. The problem lies in the undisciplined use and proliferation of assumptions whose left rule is not invertible.

In a typical situation we have some universally quantified implications as assumptions. For example, Δ could be

$$\begin{array}{l}\forall x_1.\, \forall y_1.\, \forall z_1.\, P_1(x_1,y_1,z_1) \supset Q_1(x_1,y_1,z_1) \supset R_1(x_1,y_1,z_1),\\ \forall x_2.\, \forall y_2.\, \forall z_2.\, P_2(x_2,y_2,z_2) \supset Q_2(x_2,y_2,z_2) \supset R_2(x_2,y_2,z_2)\end{array}$$

If the right-hand side is passive, we now have to apply ∀L to one of the two assumptions. We assume we guess the first one and that we can guess an appropriate term t_1. After the ∀L rule and a left transition, we are left with

$$\begin{array}{l}\forall x_1.\, \forall y_1.\, \forall z_1.\, P_1(x_1, y_1, z_1) \supset Q_1(x_1, y_1, z_1) \supset R_1(x_1, y_1, z_1),\\ \forall x_2.\, \forall y_2.\, \forall z_2.\, P_2(x_2, y_2, z_2) \supset Q_2(x_2, y_2, z_2) \supset R_2(x_2, y_2, z_2),\\ \forall y_1.\, \forall z_1.\, P_1(t_1, y_1, z_1) \supset Q_1(t_1, y_1, z_1) \supset R_1(t_1, y_1, z_1).\end{array}$$

Again, we are confronted with a don't know non-deterministic choice, now between 3 possibilities. One can see that the number of possible choices quickly explodes. We can observe that the pattern above does not coincide with mathematical practice. Usually one applies an assumption or lemma of the form above by instantiating all the quantifiers and all preconditions at once. This strategy called *focusing* is a refinement of the inversion strategy.

Roughly, when all propositions in a sequent are synchronous, we *focus* either on an assumption or the proposition we are trying to prove and then apply a sequence of non-invertible rules to the chosen proposition. This phase stops when either an invertible connective or an atomic proposition is reached.

The focusing strategy is defined by four judgments

$\Delta; \Omega \overset{a}{\Longrightarrow} A; \cdot$	Decompose right asynchronous proposition
$\Delta; \Omega \overset{a}{\Longrightarrow} \cdot; R$	Decompose left asynchronous propositions
$\Delta; A \overset{s}{\Longrightarrow} \cdot; R$	Focus on left synchronous proposition
$\Delta; \cdot \overset{s}{\Longrightarrow} A; \cdot$	Focus on right synchronous proposition

The first two judgment are very similar to the inversion strategy. When we have the situation $\Delta; \cdot \overset{a}{\Longrightarrow} \cdot; R$ where Δ consists of left synchronous propositions and R is right synchronous, we focus either on R or on some proposition L in Δ and chain together inferences on the those propositions.

As in the inversion judgment, the proposition on the outside of the four zones are passive, while the ones on the inside are actively decomposed.

For the strategy to be maximally effective, we slightly generalize our classification of connectives, permitting conjunction and truth to be viewed as either synchronous or asynchronous, depending on what is convenient. This allows us to extend the phases maximally, removing as much non-determinism as possible.

	Asynchronous	Synchronous
Right	$\wedge, \top, \supset, \forall$	$\wedge, \top, \vee, \bot, \exists$
Left	$\wedge, \top, \vee, \bot, \exists$	$\wedge, \top, \supset, \forall$

We now use R for propositions that are *not* right asynchronous $(\vee, \bot, \exists, P)$ and L for propositions that are *not* left asynchronous $(\supset, \forall, P)$.

Except for the special status of conjunction and truth, each connective has unique and complementary status on the left and on the right. Andreoli's original analysis [And92] was carried out in linear logic, which did not show these anomalies. This is because there are two forms of conjunction (additive and multiplicative), each with a unique status.

We first repeat the inversion rules which constitute an asynchronous phase during search.

Right Asynchronous Propositions. First, we decompose the right asynchronous connectives.

$$\frac{\Delta;\Omega \overset{a}{\Longrightarrow} A;\cdot \qquad \Delta;\Omega \overset{a}{\Longrightarrow} B;\cdot}{\Delta;\Omega \overset{a}{\Longrightarrow} A \wedge B;\cdot}\,\wedge\mathrm{R} \qquad \frac{}{\Delta;\Omega \overset{a}{\Longrightarrow} \top;\cdot}\,\top\mathrm{R}$$

$$\frac{\Delta;\Omega, A \overset{a}{\Longrightarrow} B;\cdot}{\Delta;\Omega \overset{a}{\Longrightarrow} A \supset B;\cdot}\,\supset\mathrm{R} \qquad \frac{\Delta;\Omega \overset{a}{\Longrightarrow} [a/x]A;\cdot}{\Delta;\Omega \overset{a}{\Longrightarrow} \forall x.\ A;\cdot}\,\forall\mathrm{R}^{a}$$

$$\frac{\Delta;\Omega \overset{a}{\Longrightarrow} \cdot;R \quad (R = A \vee B, \bot, \exists x.\ A, P)}{\Delta;\Omega \overset{a}{\Longrightarrow} R;\cdot}\,R\mathrm{R}$$

Left Asynchronous Propositions. Next we break down the left asynchronous propositions. Recall that Ω is considered in order, so the rules are deterministic.

$$\frac{\Delta;\Omega, A, B \overset{a}{\Longrightarrow} \cdot;R}{\Delta;\Omega, A \wedge B \overset{a}{\Longrightarrow} \cdot;R}\,\wedge\mathrm{L} \qquad \frac{\Delta;\Omega \overset{a}{\Longrightarrow} \cdot;R}{\Delta;\Omega, \top \overset{a}{\Longrightarrow} \cdot;R}\,\top\mathrm{L}$$

$$\frac{\Delta;\Omega, A \overset{a}{\Longrightarrow} \cdot;R \qquad \Delta;\Omega, B \overset{a}{\Longrightarrow} \cdot;R}{\Delta;\Omega, A \vee B \overset{a}{\Longrightarrow} \cdot;R}\,\vee\mathrm{L} \qquad \frac{}{\Delta;\Omega, \bot \overset{a}{\Longrightarrow} \cdot;R}\,\bot\mathrm{L}$$

$$\frac{\Delta;\Omega, [a/x]A \overset{a}{\Longrightarrow} \cdot;R}{\Delta;\Omega, \exists x.\ A \overset{a}{\Longrightarrow} \cdot;R}\,\exists\mathrm{L}^{a}$$

$$\frac{\Delta, L;\Omega \overset{a}{\Longrightarrow} \cdot;R \quad (L = A \supset B, \forall x.\ A, P)}{\Delta;\Omega, L \overset{a}{\Longrightarrow} \cdot;R}\,L\mathrm{L}$$

Focus. Next we need to decide which proposition among Δ and R to focus on. While we allow focusing on an atomic assumption, focusing on the succedent requires it to be non-atomic. The reason is our handling of initial sequents. For uniformity we also include $\bot$, even though focusing on it will fail in the next step.

$$\frac{(\Delta, L); L \overset{s}{\Longrightarrow} \cdot;R}{(\Delta, L);\cdot \overset{a}{\Longrightarrow} \cdot;R}\,\mathrm{focus}L \qquad \frac{\Delta;\cdot \overset{s}{\Longrightarrow} R;\cdot \quad (R = A \vee B, \bot, \exists x.\ A)}{\Delta;\cdot \overset{a}{\Longrightarrow} \cdot;R}\,\mathrm{focus}R$$

Right Synchronous Propositions. The non-invertible rules on the right maintain the focus on principal formula of the inference. When we have reduced the right-hand side to an asynchronous (but not synchronous) or atomic proposition, we blur our focus and initiate an asynchronous phase.

$$\frac{\Delta; \cdot \overset{s}{\Longrightarrow} A; \cdot}{\Delta; \cdot \overset{s}{\Longrightarrow} A \vee B; \cdot}\,\vee\mathrm{R}_1 \qquad \frac{\Delta; \cdot \overset{s}{\Longrightarrow} B; \cdot}{\Delta; \cdot \overset{s}{\Longrightarrow} A \vee B; \cdot}\,\vee\mathrm{R}_2$$

$$\text{no right focus rule for } \bot \qquad \frac{\Delta; \cdot \overset{s}{\Longrightarrow} [t/x]A; \cdot}{\Delta; \cdot \overset{s}{\Longrightarrow} \exists x.\ A; \cdot}\,\exists\mathrm{R}$$

$$\frac{\Delta; \cdot \overset{a}{\Longrightarrow} A; \cdot \quad (A = B \supset C, \forall x.\ B, P)}{\Delta; \cdot \overset{s}{\Longrightarrow} A; \cdot}\,\mathrm{blur}R$$

Left Synchronous Propositions. The non-invertible rules on the left also maintain their focus on the principal formula of the inference. When we have reached an asynchronous (but not synchronous) proposition, we blur our focus and initiate an asynchrounous phase.

$$\frac{\Delta; B \overset{s}{\Longrightarrow} \cdot; R \qquad \Delta; \cdot \overset{s}{\Longrightarrow} A; \cdot}{\Delta; A \supset B \overset{s}{\Longrightarrow} \cdot; R}\,\supset\mathrm{L} \qquad \frac{\Delta; [t/x]A \overset{s}{\Longrightarrow} \cdot; R}{\Delta; \forall x.\ A \overset{s}{\Longrightarrow} \cdot; R}\,\forall\mathrm{L}$$

$$\frac{\Delta; A \overset{s}{\Longrightarrow} \cdot; R}{\Delta; A \wedge B \overset{s}{\Longrightarrow} \cdot; R}\,\wedge\mathrm{L}_1 \qquad \frac{\Delta; B \overset{s}{\Longrightarrow} \cdot; R}{\Delta; A \wedge B \overset{s}{\Longrightarrow} \cdot; R}\,\wedge\mathrm{L}_2$$

$$\text{no rule for } \top\mathrm{L} \qquad \frac{\Delta; A \overset{a}{\Longrightarrow} \cdot; R \quad (A = B \vee C, \bot, \exists x.\ B)}{\Delta; A \overset{s}{\Longrightarrow} \cdot; R}\,\mathrm{blur}L$$

$$\frac{}{\Delta; P \overset{s}{\Longrightarrow} \cdot; P}\,\mathrm{init} \qquad \text{no rule for } \Delta; P \overset{s}{\Longrightarrow} \cdot; Q \text{ for } P \neq Q$$

Note that the second premise of the ⊃L rule is still a focused sequent. From a practical point of view it is important to continue with the focusing steps in the first premise before attempting to prove the second premise, because the decomposition of B may ultimately fail when an atomic proposition is reached. Such a failure would render the possibly difficult proof of A useless.

There is a slight, but important asymmetry in the initial sequents: we require that we have focused on the left proposition.

If one shows only applications of the decision rules in a derivation, the format is very close to *assertion-level proofs* as proposed by Huang [Hua94]. His motivation was the development of a formalism appropriate for the presentation of mathematical proofs in a human-readable form. This provides independent evidence for the value of focusing proofs. Focusing derivations themselves were developed by Andreoli [And92] in the context of classical linear logic. An adaptation to intuitionistic linear logic was given by Howe [How98] which is related the calculus LJT devised by Herbelin [Her95]. Herbelin's goal was to devise a sequent calculus whose derivations are in bijective correspondence to normal natural deductions. Due to the $\vee$, $\bot$ and $\exists$ elimination rules, this is not the case here.

The search procedure which works with focusing sequents is similar to the one for inversion. After the detailed development of inversion proofs, we will not repeat or extend the development here, but refer the interested reader to the literature. The techniques are very similar to the ones shown in Section 4.1.

4.4 Unification

When proving a proposition of the form $\exists x.\ A$ by its right rule in the sequent or focusing calculus, we must supply a term t and then prove $[t/x]A$. The domain of quantification may include infinitely many terms (such as the natural numbers), so this choice cannot be resolved simply by trying all possible terms t. Similarly, when we use a hypothesis of the form $\forall x.\ A$ we must supply a term t to substitute for x. We refer to this a *existential non-determinism*.

Fortunately, there is a technique called *unification* which is sound and complete for syntactic equality between terms. The basic idea is quite simple: we postpone the choice of t and instead substitute a new *existential variable* (often called *meta-variable* or *logic variable*) X for x and continue with the bottom-up construction of a derivation. When we reach initial sequents we check if there is a substitution for the existential variables such that the hypothesis matches the conclusion. If so, we apply this instantiation globally to the partial derivation and continue to search for proofs of other subgoals. Finding an instantiation for existential variables under which two propositions or terms match is called *unification*. It is decidable if a unifying substitution or *unifier* exists, and if so, we can effectively compute it in linear time. Moreover, we can do so with a minimal commitment and we do not need to choose between various possible unifiers.

Because of its central importance in both backward- and forward-directed search, unification has been thoroughly investigated. Herbrand [Her30] is given credit for the first description of a unification algorithm in a footnote of his thesis, but it was not until 1965 that it was introduced into automated deduction through the seminal work by Alan Robinson [Rob65, Rob71]. The first algorithms were exponential, and later almost linear [Hue76, MM82] and linear algorithms [MM76, PW78] were discovered. In the practice of theorem proving, generally variants of Robinson's algorithm are still used, due to its low constant overhead on the kind of problems encountered in practice. For further discussion and a survey of unification, see [Kni89]. We describe a variant of Robinson's algorithm.

Before we describe the unification algorithm itself, we relate it to the problem of proof search. We use here the sequent calculus with atomic initial sequents, but it should be clear that precisely the same technique of *residuation* applies to focused derivations. We enrich the judgment $\Gamma \overset{-}{\Longrightarrow} A$ by a *residual proposition*

F such that

1. if $\Gamma \overset{-}{\Longrightarrow} A$ then $\Gamma \overset{-}{\Longrightarrow} A \setminus F$ and F is true, and

2. if $\Gamma \overset{-}{\Longrightarrow} A \setminus F$ and F is true then $\Gamma \overset{-}{\Longrightarrow} A$.

Generally, we cannot prove such properties directly by induction, but we need to generalize them, exhibiting the close relationship between the derivations of the sequents and residual formulas F.

Residual formulas F are amenable to specialized procedures such as unification, since they are drawn from a simpler logic or deductive system than the general propositions A. In practice they are often solved *incrementally* rather than collected throughout a derivation and only solved at the end. This is important for the early detection of failures during proof search. Incremental solution of residual formulas is the topic of Exercise **??**.

What do we need in the residual propositions so that existential choices and equalities between atomic propositions can be expressed? The basic proposition is one of equality between atomic propositions, $P_1 \doteq P_2$. We also have conjunction $F_1 \wedge F_2$, since equalities may be collected from several subgoals, and $\top$ if there are no residual propositions to be proven. Finally, we need the existential quantifier $\exists x.\ F$ to express the scope of existential variables, and $\forall x.\ F$ to express the scope of parameters introduced in a derivation. We add equality between terms, since it is required to describe the unification algorithm itself. We refer to the logic with these connectives as *unification logic*, defined via a deductive system.

$$\textit{Formulas} \quad F \quad ::= \quad P_1 \doteq P_2 \mid t_1 \doteq t_2 \mid F_1 \wedge F_2 \mid \top \mid \exists x.\ F \mid \forall x.\ F$$

The main judgment "*F is valid*", written $\models F$, is defined by the following rules, which are consistent with, but more specialized than the rules for these connectives in intuitionistic natural deduction (see Exercise **??**).

$$\frac{}{\models P \doteq P}\ {\doteq}\mathrm{I} \qquad\qquad \frac{}{\models t \doteq t}\ {\doteq}\mathrm{I}'$$

$$\frac{\models F_1 \qquad \models F_2}{\models F_1 \wedge F_2}\ {\wedge}\mathrm{I} \qquad\qquad \frac{}{\models \top}\ \top\mathrm{I}$$

$$\frac{\models [t/x]F}{\models \exists x.\ F}\ \exists\mathrm{I} \qquad\qquad \frac{\models [a/x]F}{\models \forall x.\ F}\ \forall\mathrm{I}^a$$

The $\forall\mathrm{I}^a$ rule is subject to the usual proviso that a is a new parameter not occurring in $\forall x.\ F$. There are no elimination rules, since we do not need to consider hypotheses about the validity of a formula F which is the primary reason for the simplicity of theorem proving in the unification logic.

We enrich the sequent calculus with residual formulas from the unification logic, postponing all existential choices. Recall that in practice we merge residuation and solution in order to discover unprovable residual formulas as soon as possible. This merging of the phases is not represented in our system.

Initial Sequents. Initial sequents residuate an equality between its principal propositions. Any solution to the equation will unify P' and P, which means that this will translate to a correct application of the initial sequent rule in the original system.

$$\frac{}{\Gamma, P' \stackrel{-}{\Longrightarrow} P \setminus P' \doteq P}\,\mathrm{init}$$

Propositional Connectives. We just give a few sample rules for the connectives which do not involve quantifiers, since all of them simply propagate or combine unification formulas, regardless whether they are additive, multiplicative, or exponential.

$$\frac{\Gamma, A \stackrel{-}{\Longrightarrow} B \setminus F}{\Gamma \stackrel{-}{\Longrightarrow} A \supset B \setminus F}\,{\supset}\mathrm{R} \qquad \frac{}{\Gamma \stackrel{-}{\Longrightarrow} \top \setminus \top}\,\top\mathrm{R}$$

$$\frac{\Gamma, A \supset B \stackrel{-}{\Longrightarrow} A \setminus F_1 \qquad \Gamma, A \supset B, B \stackrel{-}{\Longrightarrow} C \setminus F_2}{\Gamma, A \supset B \stackrel{-}{\Longrightarrow} C \setminus F_1 \wedge F_2}\,{\supset}\mathrm{L}$$

Quantifiers. These are the critical rules. Since we residuate the existential choices entirely, the ∃R and ∀L rules instantiate a quantifier by a new *parameter*, which is existentially quantified in the residual formula in both cases. Similarly, the ∀R and ∃L rule introduce a parameter which is universally quantified in the residual formula.

$$\frac{\Gamma \stackrel{-}{\Longrightarrow} [a/x]A \setminus [a/x]F}{\Gamma \stackrel{-}{\Longrightarrow} \forall x.\, A \setminus \forall x.\, F}\,\forall\mathrm{R}^a \qquad \frac{\Gamma, \forall x.\, A, [a/x]A \stackrel{-}{\Longrightarrow} C \setminus [a/x]F}{\Gamma, \forall x.\, A \stackrel{-}{\Longrightarrow} C \setminus \exists x.\, F}\,\forall\mathrm{L}^a$$

$$\frac{\Gamma \stackrel{-}{\Longrightarrow} [a/x]A \setminus [a/x]F}{\Gamma \stackrel{-}{\Longrightarrow} \exists x.\, A \setminus \exists x.\, F}\,\exists\mathrm{R}^a \qquad \frac{\Gamma, \exists x.\, A, [a/x]A \stackrel{-}{\Longrightarrow} C \setminus [a/x]F}{\Gamma, \exists x.\, A \stackrel{-}{\Longrightarrow} C \setminus \forall x.\, A}\,\exists\mathrm{L}^a$$

The soundness of residuating equalities and existential choices in this manner is straightforward.

Theorem 4.11 (Soundness of Equality Residuation)
If $\Gamma \stackrel{-}{\Longrightarrow} A \setminus F$ *and* $\models F$ *then* $\Gamma \stackrel{-}{\Longrightarrow} A$.

Proof: By induction on the structure of the given derivation $\mathcal{R}$. We show the critical cases. Note how in the case of the $\exists$R rule the derivation of $\models \exists x.\ F$ provides the essential witness term t.

Case:

$$\mathcal{R} = \dfrac{}{\Gamma, P' \overset{-}{\Longrightarrow} P \setminus P' \doteq P}\ \text{init}$$

$\models P' \doteq P$	By assumption
$P' = P$	By inversion
$\Gamma, P' \overset{-}{\Longrightarrow} P$	By rule init

Case:

$$\mathcal{R} = \dfrac{\begin{array}{c}\mathcal{R}_1\\ \Gamma \overset{-}{\Longrightarrow} [a/x]A_1 \setminus [a/x]F_1\end{array}}{\Gamma \overset{-}{\Longrightarrow} \exists x.\ A_1 \setminus \exists x.\ F_1}\ \exists\text{R}^a$$

$\models \exists x.\ F_1$	By assumption
$\models [t/x]F_1$ for some t	By inversion
$\Gamma \overset{-}{\Longrightarrow} [t/x]A_1 \setminus [t/x]F_1$	By substitution for parameter a
$\Gamma \overset{-}{\Longrightarrow} [t/x]A_1$	By i.h.
$\Gamma \overset{-}{\Longrightarrow} \exists x.\ A_1$	By rule $\exists$R

Case:

$$\mathcal{R} = \dfrac{\begin{array}{c}\mathcal{R}_1\\ \Gamma \overset{-}{\Longrightarrow} [a/x]A_1 \setminus [a/x]F_1\end{array}}{\Gamma \overset{-}{\Longrightarrow} \forall x.\ A_1 \setminus \forall x.\ F_1}\ \forall\text{R}^a$$

$\models \forall x.\ F_1$	By assumption
$\models [b/x]F_1$ for a new parameter b	By inversion
$\models [a/x]F_1$	By substitititution of a for b
$\Gamma \overset{-}{\Longrightarrow} [a/x]A_1$	By i.h.
$\Gamma \overset{-}{\Longrightarrow} \forall x.\ A_1$	By rule $\forall$R

□

The opposite direction is more difficult. The desired theorem:

If $\Gamma \overset{-}{\Longrightarrow} A$ *then* $\Gamma \overset{-}{\Longrightarrow} A \setminus F$ *for some* F *with* $\models F$

cannot be proved directly by induction, since the premisses of the two derivations are different in the $\exists$R and $\forall$L rules. However, one can be obtained from the other by substituting terms for parameters. Since this must be done simultaneously, we introduce a new notation.

$$\textit{Parameter Substitution} \quad \rho \quad ::= \quad \cdot \mid \rho, t/a$$

We assume all the parameters a substituted for by ρ are distinct to avoid ambiguity. We write $A[\rho]$, $F[\rho]$, and $\Gamma[\rho]$, for the result of applying the substitution ρ to a proposition, formula, or context, respectively.

Lemma 4.12 *If* $\Gamma \overset{-}{\Longrightarrow} A$ *where* $A = A'[\rho]$, $\Gamma = \Gamma'[\rho]$ *then* $\Gamma' \overset{-}{\Longrightarrow} A' \setminus F$ *for some* F *such that* $\models F[\rho]$.

Proof: The proof proceeds by induction on the structure of the given derivation $\mathcal{D}$. We show only two cases, the second of which required the generalization of the induction hypothesis.

Case:

$$\mathcal{D} = \dfrac{}{\Gamma_1, P \overset{-}{\Longrightarrow} P}\,\text{init}$$

$\Gamma_1 = \Gamma'_1[\rho]$, $P = P'[\rho]$, and $P = P''[\rho]$	Assumption
$\Gamma'_1, P' \overset{-}{\Longrightarrow} P'' \setminus P' \doteq P''$	By rule init
$\models P'[\rho] \doteq P''[\rho]$	By rule $\doteq$I

Case:

$$\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}_1 \\ \Gamma \overset{-}{\Longrightarrow} [t/x]A_1\end{array}}{\Gamma \overset{-}{\Longrightarrow} \exists x.\ A_1}\,\exists\text{R}$$

$\exists x.\ A_1 = A'[\rho]$	Assumption
$A' = \exists x.\ A'_1$ for a new parameter a with	
$[a/x]A_1 = ([a/x]A'_1)[\rho, a/a]$	By definition of substitution
$[t/x]A_1 = ([a/x]A'_1)[\rho, t/a]$	By substitution for parameter a
$\Gamma = \Gamma'[\rho]$	Assumption
$\Gamma'[\rho] = \Gamma'[\rho, t/a]$	Since a is new
$\Gamma' \overset{-}{\Longrightarrow} [a/x]A'_1 \setminus [a/x]F_1$, and	
$\models ([a/x]F_1)[\rho, t/a]$	By i.h.
$\Gamma' \overset{-}{\Longrightarrow} \exists x.\ A'_1 \setminus \exists x.\ F_1$	By rule $\exists$R
$\models (\exists x.\ F_1)[\rho]$	By rule $\exists$R and definition of substitution

□

Theorem 4.13 (Completeness of Equality Residuation)
If $\Gamma \overset{-}{\Longrightarrow} A$ *then* $\Gamma \overset{-}{\Longrightarrow} A \setminus F$ *for some* F *and* $\models F$.

Proof: From Lemma 4.12 with $A' = A$, $\Gamma' = \Gamma$, and ρ the identity substitution on the parameters in Γ and A. □

Next we describe an algorithm for proving residuated formulas, that is, an algorithm for unification. We do this in two steps: first we solve the problem in the fragment without parameters and universal quantifiers and then we extend the solution to the general case.

There are numerous ways of describing unification algorithsm in the literature. We view it here as a process of transformation on a collection of constraints. In the first instance we consider global unification, where we are given a single constraint formula (as generated by equality residuation, for example) and we have to determine if it is true. Later, we will generalize the view in order just partially transform the constraints to a normal form which is easily seen to have most general solutions. This latter view will be particularly useful when constraints are generated incrementally during proof search.

A collection of equational constraints is simply a collection of formulas in the unification logic or an indication that the constraints are inconsistent (#).

$$\text{Constraints} \quad C \quad ::= \quad \cdot \mid F, C \mid \#$$

We will freely exchange formulas among the constraints, just as we freely exchange assumptions in the sequent calculus. The empty constraint "·" corresponds to success, a contradiction to failure of proving the unification formula. Constraints may contain free *unification variables* X which are interpreted existentially. They are also known as *existential variables* or *logic variables.* Note that unification variables are never bound. We group the rules into several classes. The first, breaks down the structure of the formulas in C.

$$\begin{array}{lll}
F_1 \wedge F_2, C & \mapsto & F_1, F_2, C \\
\top, C & \mapsto & C \\
\exists x.\, F, C & \mapsto & [X/x]F, C \quad \text{where } X \text{ not free in } F \text{ or } C
\end{array}$$

The second group of rules breaks down equalities into simpler equalities.

$$\begin{array}{lllr}
p(t_1, \ldots, t_n) \doteq p(s_1 \ldots, s_n), C & \mapsto & t_1 \doteq s_1, \ldots, t_n \doteq s_n, C & \\
f(t_1, \ldots, t_n) \doteq f(s_1 \ldots, s_n), C & \mapsto & t_1 \doteq s_1, \ldots, t_n \doteq s_n, C & \\
p(t_1, \ldots, t_n) \doteq q(s_1 \ldots, s_n), C & \mapsto & \# & \text{where } p \neq q \\
f(t_1, \ldots, t_n) \doteq g(s_1 \ldots, s_n), C & \mapsto & \# & \text{where } f \neq g
\end{array}$$

Note that equations of predicate or function symbols without arguments ($n = 0$) will either be simply removed or be inconsistent.

Finally, we will be left with equations where one of the two sides is a unification variable (we are not yet considering parameters). In that case, we must consider the right-hand side and distinguish several cases:

$$\begin{array}{llll}
X \doteq X, C & \mapsto & C & \\
X \doteq t, C & \mapsto & [t/X]C & \text{provided } X \text{ not free in } t \\
t \doteq X, C & \mapsto & [t/X]C & \text{provided } X \text{ not free in } t \\
X \doteq t, C & \mapsto & \# & \text{if } t \neq X \text{ and } X \text{ free in } t \\
t \doteq X, C & \mapsto & \# & \text{if } t \neq X \text{ and } X \text{ free in } t
\end{array}$$

The conditions on these rules are necessary in order to recognize cases such as $X \doteq f(X)$, which has no solution: No matter which term we substitute for X, the right-hand side will always have one more function symbol than the left-hand side, so the equation cannot be satisfied. We refer to the condition "*X not free in t*" as the *occurs-check*.

Note that the whole algorithm depends critically on the function symbols being uninterpreted. As a trivial example, consider $+(3,4) \doteq +(2,5)$ on which the above algorithm would fail. Slighly trickier is something like $X \doteq -(-(X))$ which is true for any integer X, but violates the occurs-check.

As a first step in the correctness proof we can verify that a unification will always terminate.

Lemma 4.14 (Termination of Unification) *Any sequence of reductions $C \mapsto C' \mapsto C'' \ldots$ must terminate and yield either $\#$ or the empty set of constraints $(\cdot)$.*

Proof: By nested induction, first on the number of variables (unification variables X or bound variables $\exists x$) in C, second on the total size of the constraint, counting quantifiers, logical connectives, and variables occurrences.

The first set of rules for structural decomposition and the rule for eliminating $X \doteq X$ decreases the size of the constraints, without increasing the number of variables. The set of rules for variables (except for $X \doteq X$) reduces the number of variables in C by substitution for all occurrences of a variable (possibly increasing the total size of the constraint). □

In order to show the correctness of the unification algorithm, we would like to show that each step preserves provability. That is, if $C \mapsto C'$ then C is provable iff C' is provable. However, a difficulty arises in the case of existential quantification, since we step from $\exists x.\ F$ to $[X/x]F$ and we have not defined what it means for a formula with a unification variable to be provable. Intuitively, it should mean that not the formula itself, but some instance of it is provable. Hence we define that a constraint is *satisfiable* to mean that there is an instance that is provable. In order to define the concept of an *instance* we define simultaneous substitution for the unification variables of a term.

The second concept we need is that of a *substitution* for existential variables. We use a new notation, because this form of substitution is quite different from substitutions for bound variables x or parameters a.

$$\textit{Substitutions} \quad \theta \quad ::= \quad \cdot \mid \theta, t/X$$

We require that all variables X defined by a substitution are distinct. We write $\mathrm{dom}(\theta)$ for the variables defined by a substitution and $\mathrm{cod}(\theta)$ for all the variables occuring in the terms t. For a ground substitution $\mathrm{cod}(\theta)$ is empty. For the technical development it is convenient to assume that the domain and co-domain of a substitution share no variables. This rules out "circular" substitutions such as $f(X)/X$ and it also disallows identity substitutions X/X. The latter restriction can be dropped, but it does no harm and is closer to the implementation.

As for contexts, we consider the order of the definitions in a substitution to be irrelevant.

We write $t[\theta]$, $A[\theta]$, and $\Gamma[\theta]$ for the application of a substitution to a term, proposition, or context. This is defined to be the identity on existential variables that are not explicitly defined in the substitution.

We also need an operation of composition, written as $\theta_1 \circ \theta_2$ with the property that $t[\theta_1 \circ \theta_2] = (t[\theta_1])[\theta_2]$ and similarly for propositions and contexts. Composition is defined by

$$\begin{aligned} (\cdot) \circ \theta_2 &= \theta_2 \\ (\theta_1, t/X) \circ \theta_2 &= (\theta_1 \circ \theta_2), t[\theta_2]/X \end{aligned}$$

In order for composition to be well-defined and have the desired properties we require that $\mathrm{dom}(\theta_1)$, $\mathrm{dom}(\theta_2)$ and $\mathrm{cod}(\theta_2)$ are disjoint, but of course variables in the co-domain of θ_1 can be defined by θ_2.

Now we define that *constraint* $C = F_1, \ldots, F_n$ *is satisfiable* if there exists a substitution θ for unification variables in C such that $\models F_i[\theta]$ for all $1 \leq i \leq n$. We write C *sat* if C is satisfiable.

Theorem 4.15 (Preservation of Satisfiability)
If $C \mapsto C'$ *then* C *sat iff* C' *sat*

Proof: In both directions, the proof is by cases on the definition of $C \mapsto C'$. We show a three cases from left-to-right. The other cases and opposite direction are similar.

Assume $C \mapsto C'$ and C *sat*. We have to show the C' *sat*.

Case: $\exists x.\ F, C_1 \mapsto [X/x]F, C_1$.

$\exists x.\ F, C_1$ *sat*	Assumption
For some θ, $\models (\exists x.\ F)[\theta]$	
and $\models F_1[\theta]$ for every F_1 in C_1	By defn. of *sat*
$\models \exists x.\ (F[\theta])$	By defn. of substitution
$\models [t/x](F[\theta])$	By inversion
$\models ([t/x]F)[\theta]$	By props. of substitution
$\models ([X/x]F)[\theta, t/X]$	Since X not in F or t
$\models F_1[\theta, t/X]$ for any F_1 in C_1	Since X not in C_1
$[X/x]F, C_1$ *sat*	By defn. of *sat*

Case: $X \doteq t, C_1 \mapsto [t/X]C_1$ where X not in t.

$X \doteq t, C_1$ *sat*	Assumption
For some θ, $\models (X \doteq t)[\theta]$	
and $\models F_1[\theta]$ for every F_1 in C_1	By defn. of *sat*
$\models X[\theta] \doteq t[\theta]$	By defn. of substitution
$X[\theta] = t[\theta]$	By inversion
$\theta = (\theta', t[\theta]/X)$	By defn. of substitution

$t[\theta]/X = t[\theta']/X$	Since X not in t
$\models F_1[\theta', t[\theta']/X]$ for any F_1 in C_1	From above
$\models ([t/X]F_1)[\theta']$	By props. of substitution
$[t/X]C_1$ *sat*	By defn. of *sat*

Case: $X \doteq t, C_1 \mapsto \#$ where X in t, $X \neq t$.

$X \doteq t, C_1$ *sat*	Assumption
$\models (X \doteq t)[\theta]$ for some θ	By defn. of *sat*
$\models X[\theta] \doteq t[\theta]$	By defn. of substitution
$X[\theta] = t[\theta]$	By inversion
$X[\theta] = f(\ldots X \ldots)[\theta]$	Since X in t, $X \neq t$
$X[\theta] = f(\ldots X[\theta] \ldots)$	By defn. of substitution
Contradiction	Right-hand side has more function symbols than left-hand side

This case is impossible

□

The argument above requires some elementary reasoning about substitution. Those proofs are usually straightforward by induction on the structure of the term we substitute in, as long as the right condition on occurrences of variables are known.

Termination of unification together with preservation of satisfiability gives us the correctness of unification as a procedure.

4.5 Unification with Parameters

The generalization of the algorithm above to account for universal quantifiers and parameters is not completely straightforward. The difficulty is that $\forall x.\ \exists y.\ y \doteq x$ is valid, while $\exists y.\ \forall x.\ y \doteq x$ is not. In unification logic, the fact that the second cannot be derived is due to the parameter restriction.

$$\dfrac{\dfrac{\dfrac{}{\models a \doteq a}\,{\doteq}\mathrm{I}}{\models \forall x.\ a \doteq x}\,\forall\mathrm{I}^a??}{\models \exists y.\ \forall x.\ y \doteq x}\,\exists\mathrm{I}$$

In this derivation, the application of $\forall\mathrm{I}^a$ is incorrect. However, if we had a way to postpone choosing the instantiation for y, say, by supplying an existential variable instead, then the situation is far less clear.

$$\dfrac{\dfrac{\dfrac{\text{“}a/Y\text{”??}}{\models Y \doteq a}\,{\doteq}\mathrm{I}}{\models \forall x.\ Y \doteq x}\,\forall\mathrm{I}^a??}{\models \exists y.\ \forall x.\ y \doteq x}\,\exists\mathrm{I}$$

In this derivation, it is the substitution of a for Y which will invalidate the derivation at the $\forall\mathrm{I}^a$ rule application. Up to that point we could not really fail. Written in our transformation notation:

$$\begin{array}{ll} & \exists y.\, \forall x.\, y \doteq x \\ \mapsto & \forall x.\, Y \doteq x \\ \mapsto & Y \doteq a \\ \mapsto^{??} & \cdot \end{array}$$

From this very simple example it seems clear that we need to prohibit final step: Y may not be instantiated with a term that mentions parameter a. There are two approaches to encoding this restriction. More or less standard in theorem proving is *Skolemization* which we pursue in Exercise 4.3. The dual solution notes for each existential variable which parameters may occur in its substitution term. In the example above, Y was introduced at a point where a did not yet occur, so the substitution of a for Y should be rejected.

In order to describe this concisely, we add a *parameter context* Ψ to the judgment which lists distinct parameters.

$$\textit{Parameter Context} \quad \Psi \quad ::= \quad \cdot \mid \Psi, a$$

We annotate each judgment with the parameter context and introduce the new judgment "*t is closed with respect to Ψ*", written as $\Psi \models t\ \mathit{term}$. It is defined by the following rules.

$$\frac{}{\Psi_1, a, \Psi_2 \vdash a\ \mathit{term}}\,\mathrm{parm} \qquad \frac{\Psi \vdash t_1\ \mathit{term} \ \cdots\ \Psi \vdash t_n\ \mathit{term}}{\Psi \vdash f(t_1, \ldots, t_n)\ \mathit{term}}\,\mathrm{root}$$

We modify the validity judgment for unification formulas to guarantee this condition.

$$\frac{\Psi \vdash t\ \mathit{term} \qquad \Psi \models [t/x]F}{\Psi \models \exists x.\, F}\,\exists\mathrm{I} \qquad \frac{\Psi, a \models [a/x]F}{\Psi \models \forall x.\, F}\,\forall\mathrm{I}^a$$

Now the state of the unification algorithm (that is, the current set of constraints) must record the parameter context. We write this as $\Psi \rhd C$. Ψ is simply carried along from left to right in most transformations.

$$\begin{array}{lcll}
(\Psi \rhd F_1 \wedge F_2, C) & \mapsto & (\Psi \rhd F_1, F_2, C) & \\
(\Psi \rhd \top, C) & \mapsto & (\Psi \rhd C) & \\
(\Psi \rhd f(t_1, \ldots, t_n) \doteq f(s_1 \ldots, s_n), C) & \mapsto & (\Psi \rhd t_1 \doteq s_1, \ldots, t_n \doteq s_n, C) & \\
(\Psi \rhd f(t_1, \ldots, t_n) \doteq g(s_1 \ldots, s_n), C) & \mapsto & (\Psi \rhd \#) & \text{where } f \neq g \\
(\Psi \rhd a \doteq a, C) & \mapsto & (\Psi \rhd C) & \\
(\Psi \rhd a \doteq b, C) & \mapsto & (\Psi \rhd \#) & \text{where } a \neq b \\
(\Psi \rhd a \doteq f(t_1, \ldots, t_n)) & \mapsto & (\Psi \rhd \#) & \\
(\Psi \rhd f(t_1, \ldots, t_n) \doteq a) & \mapsto & (\Psi \rhd \#) &
\end{array}$$

The notion of an existential variable must now be generalized to track the set of parameters its substituend may depend on. We write X_Δ for a unification variable X that may depend on all the parameters in Δ, but no others. All occurrences of a variable X must be annotated with the same Δ—we think of Δ as an intrinsic property of X.

$$\begin{array}{lcll}
(\Psi \rhd \forall x.\ F, C) & \mapsto & (\Psi, a \rhd [a/x]F, C) & \text{where } a \text{ not in } \Psi,\ F, \text{ or } C \\
(\Psi \rhd \exists x.\ F, C) & \mapsto & (\Psi \rhd [X_\Psi/x]F, C) & \text{where } X \text{ not free in } F \text{ or } C
\end{array}$$

An equation $X_\Psi \doteq t$ could now be solved immediately, if all parameters of t are contained in Ψ and X does not occur in t. A first attempt at such a rule would be

$$(\Psi \rhd X_\Delta \doteq t, C) \quad \mapsto \quad (\Psi \rhd [t/X]C) \quad \text{where } \Delta \vdash t \ \textit{term} \text{ and } X \text{ not free in } t$$

However, in general t will not be closed so we cannot prove that $\Delta \vdash t$ *term*. For example, consider the constraint

$$a \rhd X_{\cdot} \doteq f(Y_a) \wedge Y_a \doteq a$$

where X cannot depend on any parameters and Y can depend on a. This should have no solution, since $X_{\cdot}$ would have to be equal to $f(a)$, which is not permissible. On the other hand,

$$a \rhd X_{\cdot} \doteq f(Y_a) \wedge Y_a \doteq c$$

for a constant c has a solution where Y_a is c and $X_{\cdot}$ is $f(c)$. So when we process an equation $X_\Delta = t$ we need to restrict any variable in t so it can depend only on the parameters in Δ. In the example above, we would substitute $Y'_{\cdot}$ for Y_a.

In order to describe this restriction, we introduce a new form of constraints which expresses the judgment $\Delta \vdash t$ *term* in the presence of unification variables. We write it as $t \mid_\Delta$, thinking of it as the restriction of t to Δ. It is implemented by the following transformations.

$$\begin{array}{lcll}
(\Psi \rhd f(t_1, \ldots, t_n) \mid_\Delta, C) & \mapsto & (\Psi \rhd t_1 \mid_\Delta, \ldots, t_n \mid_\Delta, C) & \\
(\Psi \rhd a \mid_\Delta, C) & \mapsto & (\Psi \rhd C) & \text{if } a \in \Delta \\
(\Psi \rhd a \mid_\Delta, C) & \mapsto & (\Psi \rhd \#) & \text{if } a \notin \Delta \\
(\Psi \rhd Y_{\Delta'} \mid_\Delta, C) & \mapsto & (\Psi \rhd [Y_{\Delta' \cap \Delta}/Y]C) &
\end{array}$$

the collection of the above four rules implement a process called *pruning*. Now we can finally write down the correct rule for existential variables.

$$(\Psi \rhd X_\Delta \doteq t, C) \quad \mapsto \quad (\Psi \rhd t \mid_\Delta, [t/X]C) \quad \text{provided } X \text{ not free in } t$$

From an implementation point of view, it makes sense to first solve $t \mid_\Delta$ before substitution t for X. In fact, it is probably beneficial to combine it with the occurs-check to the term t need only be traversed once.

The soundness and completeness theorems from above extend to the problem with parameters, but become more difficult. The principal new notion we need is an *admissible substitution* θ which has the property that for every existential variable X_Δ we have $\Delta \vdash X[\theta]$ *term* (see Exercise 4.4).

The ML implementation takes advantage of the fact that whenever a variable must be restricted, one of the two contexts is a prefix of the other. This is because every equation in a formula F lies beneath a path of possibly alternating quantifiers, a so-called *mixed quantifier prefix*. When we apply the rules above algorithmically, we instantiate each existentially quantified variable with a new free existential variable which depends on all parameters which were introduced for the universally quantified variables to its left. Clearly, then, for any two variables in the same equation, one context is a prefix of the other. Our ML implementation does take advantage of this observation by simplifying the intersection operation.

We can take this optimization a step further and only record with an integer (a kind of time stamp), which parameters an existential variable may depend on. This improves the efficiency of the algorithm even further, since we only need to calculate the minimum of two integers instead of intersecting two contexts during restriction. In the ML code for this class, we did not optimize to this extent.

4.6 Exercises

Exercise 4.1 Give an alternative proof of the inversion properties (Theorem 4.1) which does not use induction, but instead relies on admissibility of cut in the sequent calculus (Theorem 3.11).

Exercise 4.2 Formulate one or several cut rules directly on inversion sequents as presented in Section 4.1 and prove that they are admissible. Does this simplify the development of the completeness result for inversion proofs? Show how admissibility might be used, or illustrate why it is not much help.

Exercise 4.3 An alternative to indexing unification variables with the parameters they may depend on is *Skolemization*. Instead of changing the notion of unification variable, we change the notion of parameter, replacing it by a so-called *Skolem function*. The two quantifier rules become

$$\begin{array}{lcll}
\forall x.\, F, C & \mapsto & [f(X_1, \ldots, X_n)/x]F, C & \text{where } f \text{ not in } F\text{, or } C\text{, and } X_1, \ldots, X_n \\
 & & & \text{are all free unification variables in } F \\
\exists x.\, F, C & \mapsto & [X/x]F, C & \text{where } X \text{ not free in } F \text{ or } C
\end{array}$$

Now, incorrect dependencies are avoided due to the occurs-check. Reconsider our simple example:

$$\begin{array}{ll}
 & \exists y.\, \forall x.\, y \doteq x \\
\mapsto & \forall x.\, Y \doteq x \\
\mapsto & Y \doteq f(Y) \\
\mapsto & \#
\end{array}$$

Skolemization is attractive because it allows us to use a simpler algorithm for unification. Moreover, in some logics such as classical logic it can be applied statically, before we ever attempt to prove the proposition, completely eliminating parameters from consideration. On the other hand, Skolemization is unsound in some higher-order logics. Also, it is more difficult to recover a proof of proposition if we Skolemize during search.

Prove the correctness of the unification algorithm for the full unification logic (including universal quantifiers) which employs Skolemization.

Exercise 4.4 Extend the proofs of termination and preservation of satisfiability from the purely existential case in Section 4.4 to allow for the presence of parameters as sketched in Section 4.5. An important concept will likely be that of *admissible substitution* θ which has the property that for every existential variable X_Δ we have $\Delta \vdash X[\theta]$ *term*. You should be careful to make a precise connection between the constraint $t \mid_\Delta$ and the judgment $\Delta \vdash t$ *term* (where the latter is not defined for unification variables).

Chapter 5

The Inverse Method

After the definition of logic via natural deduction, we have developed a succession of techniques for theorem proving based on sequent calculi. We considered a sequent $\Gamma \Longrightarrow C$ as a goal, to be solved by backwards-directed search which was modeled by the bottom-up construction of a derivation. The critical choices were disjunctive non-determinism (resolved by guessing and backtracking) and existential non-determinism (resolved by introducing existential variables and unification). The limiting factor in more refined theorem provers based on this method is generally the number of disjunctive choices which have to be made. It is complicated by the fact that existential variables are global in a partial derivation, which means that choices in one conjunctive branch have effects in other branches. This effects redundancy elimination, since subgoals are not independent of each other.

The diametrically opposite approach would be to work forward from the initial sequents until the goal sequent is reached. If we guarantee a fair strategy in the selection of axioms and inference rules, every goal sequent can be derived this way. Without further improvements, this is clearly infeasible, since there are too many derivations for us to hope that we can find one for the goal sequent in this manner.

The *inverse method* is based on the property that in a cut-free derivation of a goal sequent, we only need to consider subformulas of the goal and their substitution instances. For example, when we have derived both A and B in the forward direction, we only derive their conjunction $A \wedge B$ if $A \wedge B$ is a subformula of the goal sequent.

The nature of forward search under these restrictions is quite different from the backward search. Since we always add new consequences to the sequents already derived, knowledge grows monotonically and no disjunctive non-determinism arises. Similarly for existential non-determinism, if we keep sequents in their maximally general form. On the other hand, there is a potentially very large amount of conjunctive non-determinism, since we have to apply all applicable rules to all sequents in a fair manner in order to guarantee completeness. The critical factor in forward search is to limit conjunctive non-determinism. We can view this as redundancy elimination: among the many ways that a given sequent may be derived, we try to actually consider a few as possible. The techniques developed in the preceding chapters, with some modifications, can be applied in this new setting.

Historically, the inverse method is due to Maslov [Mas64]. It has been adapted to intuitionistic and other non-classical logics by Voronkov [Vor92], Mints [Min94], and Tammet [Tam96, Tam97].

5.1 Forward Sequent Calculus

As a first step towards the inverse method, we write out a sequent calculus appropriate for forward search. This stems from a basic reinterpretation of a sequent during search. Previously, $\Gamma \Longrightarrow C$ expressed that we may use all hypotheses in Γ to prove that C is true. Now we will think of $\Gamma \longrightarrow C$ to mean that we needed all the hypotheses in Γ in order to prove that C is true.

This means that weakening is no longer valid for sequents $\Gamma \longrightarrow C$ and we have to take special care when we formulate correctness theorems. Secondly, we do not need to keep duplicate assumptions, so we view Γ in the sequent $\Gamma \longrightarrow C$ as a *set* of assumptions. We write $\Gamma_1 \cup \Gamma_2$ for the union of two sets of assumptions, and Γ, A stands for $\Gamma \cup \{A\}$.[1]

Initial Sequents. Previously, we allowed $\Gamma, A \Longrightarrow A$, since the assumptions in Γ can be used, but are just not needed in this case. In the forward calculus, initial sequents

$$\frac{}{A \longrightarrow A}\,\text{init}$$

express that only the hypothesis A is needed to derive the truth of A and nothing else.

Conjunction. In the right rule for conjunction, we previously concluded $\Gamma \Longrightarrow A \wedge B$ from $\Gamma \Longrightarrow A$ and $\Gamma \Longrightarrow B$. This expressed that all assumptions Γ are available in both branches. Now we need to take the union of the two sets of assumptions, expressing that both are needed to prove the conclusion.

$$\frac{\Gamma_1 \longrightarrow A \qquad \Gamma_2 \longrightarrow B}{\Gamma_1 \cup \Gamma_2 \longrightarrow A \wedge B}\,\wedge\text{R}$$

On the left rules, so such considerations arise.

$$\frac{\Gamma, A \longrightarrow C}{\Gamma, A \wedge B \longrightarrow C}\,\wedge\text{L}_1 \qquad \frac{\Gamma, B \longrightarrow C}{\Gamma, A \wedge B \longrightarrow C}\,\wedge\text{L}_2$$

Note that if $A \wedge B$ is already present in Γ in the two left rules, it will not be added again.

[1] In the language of judgments, $\Gamma \longrightarrow A$ is a *strict hypothetical judgment.*

Truth. As in the backward sequent calculus, there is only a right rule. Unlike the backward sequent calculus, it does not permit any hypotheses.

$$\frac{}{\cdot \longrightarrow \top}\top R$$

Implication. In the backward sequent calculus, the right rule for implication has the form

$$\frac{\Gamma, A \Longrightarrow B}{\Gamma \Longrightarrow A \supset B}\supset R.$$

In the forward direction this would not be sufficient, because it would allow us to conclude $A \supset B$ only if A is actually needed in the proof of B. To account for this case, we introduce two separate rules.

$$\frac{\Gamma, A \longrightarrow B}{\Gamma \longrightarrow A \supset B}\supset R_1 \qquad \frac{\Gamma \longrightarrow B}{\Gamma \longrightarrow A \supset B}\supset R_2$$

Another, more efficient possibility combines these rules into one which removes A from the context of the premise if it is there and otherwise leaves it unchanged (see Section **??**). In the left rule we have to take a union as in the right rule for conjunction.

$$\frac{\Gamma_1 \longrightarrow A \qquad \Gamma_2, B \longrightarrow C}{\Gamma_1 \cup \Gamma_2, A \supset B \longrightarrow C}\supset L$$

Note that the principal proposition $A \supset B$ does not occur in the premises. However, it might occur in Γ_1 or Γ_2, in which case it is not added again in the conclusion.

Disjunction. This introduces no new considerations.

$$\frac{\Gamma \longrightarrow A}{\Gamma \longrightarrow A \vee B}\vee R_1 \qquad \frac{\Gamma \longrightarrow B}{\Gamma \longrightarrow A \vee B}\vee R_2$$

$$\frac{\Gamma_1, A \longrightarrow C \qquad \Gamma_2, B \longrightarrow C}{\Gamma_1, \Gamma_2, A \vee B \longrightarrow C}\vee L$$

Falsehood. There is only a left rule.

$$\frac{}{\bot \longrightarrow C}\bot L$$

We postpone the consideration of negation and quantifiers.

The soundness of the forward sequent calculus is easy to establish.

Theorem 5.1 (Soundness of Forward Sequent Calculus)
If $\Gamma \longrightarrow C$ *then* $\Gamma \Longrightarrow C$

Proof: By induction on the structure of the derivation $\mathcal{F}$ of $\Gamma \longrightarrow C$. We show only some of the cases, since the patterns are very similar in the remaining ones. In order to avoid confusion, we write Γ, A and $\Gamma \cup \{A\}$ for forward sequents to be more explicit about possible contractions.

Case:

$$\mathcal{F} = \frac{}{C \longrightarrow C}\,\text{init}$$

$C \Longrightarrow C$	By rule init

Case:

$$\mathcal{F} = \frac{\begin{array}{c}\mathcal{F}_1\\ \Gamma_1 \longrightarrow C_1\end{array} \qquad \begin{array}{c}\mathcal{F}_2\\ \Gamma_2 \longrightarrow C_2\end{array}}{\Gamma_1 \cup \Gamma_2 \longrightarrow C_1 \wedge C_2}\,\wedge\text{R}$$

$\Gamma_1 \Longrightarrow C_1$	By i.h. on $\mathcal{F}_1$
$\Gamma_1 \cup \Gamma_2 \Longrightarrow C_1$	By weakening
$\Gamma_2 \Longrightarrow C_2$	By i.h. on $\mathcal{F}_2$
$\Gamma_1 \cup \Gamma_2 \Longrightarrow C_2$	By weakening
$\Gamma_1 \cup \Gamma_2 \Longrightarrow C_1 \wedge C_2$	By rule $\wedge$R

Case:

$$\mathcal{F} = \frac{\begin{array}{c}\mathcal{F}_1\\ \Gamma_1 \longrightarrow A\end{array} \qquad \begin{array}{c}\mathcal{F}_2\\ \Gamma_2, B \longrightarrow C\end{array}}{\Gamma_1 \cup \Gamma_2 \cup \{A \supset B\} \longrightarrow C}\,\supset\text{L}$$

$\Gamma_1 \Longrightarrow A$	By i.h. on $\mathcal{F}_1$
$\Gamma_1 \cup \Gamma_2, A \supset B \Longrightarrow A$	By weakening
$\Gamma_2, B \Longrightarrow C$	By i.h. on $\mathcal{F}_2$
$\Gamma_1 \cup \Gamma_2, A \supset B, B \Longrightarrow C$	By weakening
$\Gamma_1 \cup \Gamma_2, A \supset B \Longrightarrow C$	By rule $\supset$L
$\Gamma_1 \cup \Gamma_2 \cup \{A \supset B\} \Longrightarrow C$	By contraction (if needed)

□

Completeness is more difficult. In fact, it is false! For example, for atomic propositions P and Q we can not derive $P, Q \Longrightarrow P$. Fortunately, the absence of weakening is the only source of difficulty and can easily be taken into account.

Theorem 5.2 (Completeness of Forward Sequent Calculus)
If $\Gamma \Longrightarrow C$ then $\Gamma' \longrightarrow C$ for some $\Gamma' \subseteq \Gamma$.

Proof: By induction on the structure of $\mathcal{S}$ for $\Gamma \Longrightarrow C$.

Case:

$$\mathcal{S} = \dfrac{}{\Gamma_1, C \Longrightarrow C}\,\text{init}$$

$$\begin{array}{lr}
C \longrightarrow C & \text{By rule init} \\
\{C\} \subseteq \Gamma_1, C & \text{By definition of } \subseteq
\end{array}$$

Case:

$$\mathcal{S} = \dfrac{\begin{array}{c}\mathcal{S}_1 \\ \Gamma, A \Longrightarrow B\end{array}}{\Gamma \Longrightarrow A \supset B}\,{\supset}\text{R}$$

$$\begin{array}{lr}
\Gamma'' \longrightarrow B \text{ for some } \Gamma'' \subseteq \Gamma, A & \text{By i.h. on } \mathcal{S}_1 \\
\Gamma'' = \Gamma', A \text{ and } \Gamma' \subseteq \Gamma & \text{First subcase} \\
\Gamma' \longrightarrow A \supset B & \text{By rule } {\supset}\text{R}_1 \\
\Gamma'' \subseteq \Gamma & \text{Second subcase} \\
\Gamma'' \longrightarrow A \supset B & \text{By rule } {\supset}\text{R}_2
\end{array}$$

Case:

$$\mathcal{S} = \dfrac{\begin{array}{c}\mathcal{S}_1 \\ \Gamma_1, A \supset B \Longrightarrow A\end{array} \qquad \begin{array}{c}\mathcal{S}_2 \\ \Gamma_1, A \supset B, B \Longrightarrow C\end{array}}{\Gamma_1, A \supset B \Longrightarrow C}\,{\supset}\text{L}$$

$$\begin{array}{lr}
\Gamma'_1 \longrightarrow A \text{ for some } \Gamma'_1 \subseteq \Gamma_1, A \supset B & \text{By i.h. on } \mathcal{S}_1 \\
\Gamma'_2 \longrightarrow C \text{ for some } \Gamma'_2 \subseteq \Gamma_1, A \supset B, B & \text{By i.h. on } \mathcal{S}_2 \\
\Gamma'_2 = \Gamma''_2, B \text{ and } \Gamma''_2 \subseteq \Gamma_1, A \supset B & \text{First subcase} \\
\Gamma'_1 \cup \Gamma''_2 \cup \{A \supset B\} \longrightarrow C & \text{By rule } {\supset}\text{L} \\
\Gamma'_1 \cup \Gamma''_2 \cup \{A \supset B\} \subseteq \Gamma_1 \cup \{A \supset B\} & \text{By properties of } \subseteq \\
\Gamma'_2 \subseteq \Gamma_1, A \supset B & \text{Second subcase} \\
\Gamma' = \Gamma'_2 \text{ satisfies claim} &
\end{array}$$

□

5.2 Negation and Empty Succedents

In the backward sequent calculus, the rules for negation

$$\dfrac{\Gamma, A \Longrightarrow p}{\Gamma \Longrightarrow \neg A}\,\neg\text{R}^p \qquad \dfrac{\Gamma, \neg A \Longrightarrow A}{\Gamma, \neg A \Longrightarrow C}\,\neg\text{L}$$

require propositional parameters p. In Gentzen's original formulation of the sequent calculus he avoided this complication by allowing an empty right-hand side. A sequent of the form

$$\Gamma \Longrightarrow \cdot$$

can then be interpreted as

$$\Gamma \Longrightarrow p \qquad \text{for a parameter } p \text{ not in } \Gamma$$

As a result we can substitute an arbitrary proposition for the right-hand side (the defining property for parametric judgments) and obtain an evident judgment. In the sequent calculus with empty right-hand sides, this can be accomplished by weakening on the right:

If $\Gamma \Longrightarrow \cdot$ then $\Gamma \Longrightarrow C$ for any proposition C.

When the right-hand side can be empty or a singleton we write $\Gamma \Longrightarrow \gamma$, where $\gamma = C$ or $\gamma = \cdot$.

In a forward sequent calculus we can take advantage of this in order to avoid overcommitment in the rules for negation and falsehood. We first show the forward rules for negation; then we reexamine all the previous rules.

Negation. We just take advantage of the new form of judgment, avoiding, for example, a commitment to a particular proposition C in the $\neg$L rule.

$$\frac{\Gamma, A \longrightarrow \cdot}{\Gamma \longrightarrow \neg A}\neg\text{R} \qquad \frac{\Gamma \longrightarrow A}{\Gamma, \neg A \longrightarrow \cdot}\neg\text{L}$$

Interestingly, we do not need a second right rule for negation as for implication (see Exercise **??**).

Falsehood. Falsehood can similarly benefit from avoiding commitment. Note that previously the rule stated $\bot \longrightarrow C$, although there are many possible choices for C. Now we just replace this by

$$\frac{}{\bot \longrightarrow \cdot}\bot\text{L}$$

There still is no right rule.

Initial Sequents. They do not change.

$$\frac{}{A \longrightarrow A}\text{init}$$

Conjunction. The right rule requires no change.

$$\frac{\Gamma_1 \longrightarrow A \qquad \Gamma_2 \longrightarrow B}{\Gamma_1 \cup \Gamma_2 \longrightarrow A \wedge B}\wedge\text{R}$$

On the left rules simply need to allow for an empty right-hand side.

$$\frac{\Gamma, A \longrightarrow \gamma}{\Gamma, A \wedge B \longrightarrow \gamma}\wedge\text{L}_1 \qquad \frac{\Gamma, B \longrightarrow \gamma}{\Gamma, A \wedge B \longrightarrow \gamma}\wedge\text{L}_2$$

Truth. Does not change.

$$\frac{}{\cdot \longrightarrow \top}\,\top\text{R}$$

Implication. The possibility of empty right-hand sides requires a third right rule for implication. Again, in an implementation the three rules might be combined into a more efficient one.

$$\frac{\Gamma, A \longrightarrow B}{\Gamma \longrightarrow A \supset B}\,{\supset}\text{R}_1 \qquad \frac{\Gamma \longrightarrow B}{\Gamma \longrightarrow A \supset B}\,{\supset}\text{R}_2 \qquad \frac{\Gamma, A \longrightarrow \cdot}{\Gamma \longrightarrow A \supset B}\,{\supset}\text{R}_3$$

$$\frac{\Gamma_1 \longrightarrow A \qquad \Gamma_2, B \longrightarrow \gamma}{\Gamma_1 \cup \Gamma_2, A \supset B \longrightarrow \gamma}\,{\supset}\text{L}$$

Disjunction. The rule for disjunction on the right remains the same, but the left rule now has to account for several possibilities, depending on whether the right-hand sides of the premises are empty. Essentially, we take the union of the right-hand sides of the two premises, except that the result must be a singleton or empty for the sequent to be well-formed.

$$\frac{\Gamma \longrightarrow A}{\Gamma \longrightarrow A \vee B}\,\vee\text{R}_1 \qquad \frac{\Gamma \longrightarrow B}{\Gamma \longrightarrow A \vee B}\,\vee\text{R}_2$$

$$\frac{\Gamma_1, A \longrightarrow \gamma_1 \qquad \Gamma_2, B \longrightarrow \gamma_2}{\Gamma_1 \cup \Gamma_2, A \vee B \longrightarrow \gamma_1 \cup \gamma_2}\,\vee\text{L}$$

In detail, either γ_1 or γ_2 is empty, or $\gamma_1 = \gamma_2 = C = \gamma_1 \cup \gamma_2$. The rule does not apply otherwise.

The statement of the soundness theorem does not change much with empty succedents.

Theorem 5.3 (Soundness of Forward Sequent Calculus)

1. *If* $\Gamma \longrightarrow C$ *then* $\Gamma \Longrightarrow C$*, and*

2. *if* $\Gamma \longrightarrow \cdot$ *then* $\Gamma \Longrightarrow C$ *for all* C*.*

Proof: By induction on the derivation $\mathcal{F}$ of $\Gamma \longrightarrow \gamma$. □

In the completeness theorem, we now need to allow possible weakening on the left or on the right.

Theorem 5.4 (Completeness of Forward Sequent Calculus)

1. *If* $\Gamma \Longrightarrow C$ *then* $\Gamma' \longrightarrow C$ *or* $\Gamma' \longrightarrow \cdot$ *for some* $\Gamma' \subseteq \Gamma$*.*

Proof: By induction on the derivation $\mathcal{S}$ of $\Gamma \Longrightarrow C$. □

5.3 The Subformula Property

It is a general property of cut-free sequent calculi that all propositions occurring in a derivation are subformulas of the endsequent. In the forward direction we can therefore restrict the application of a rule to the case where the principal formula in the conclusion is a subformula of the goal sequent. We refine this property further by tracking positive and negative subformula occurrences. We then restrict left rule to introduce only negative subformulas of the goal sequent and right rules to positive subformulas of the goal sequent. To this end we introduce signed formulas.

$$\begin{array}{lll} \text{Positive} & A^+ & ::= & P^+ \mid A_1^+ \wedge A_2^+ \mid A_1^- \supset A_2^+ \mid A_1^+ \vee A_2^+ \mid \top^+ \mid \bot^+ \mid \neg A^- \\ \text{Negative} & A^- & ::= & P^- \mid A_1^- \wedge A_2^- \mid A_1^+ \supset A_2^- \mid A_1^- \vee A_2^- \mid \top^- \mid \bot^- \mid \neg A^+ \end{array}$$

It is obvious that every proposition can be annotated both positively and negatively, and that such an annotation is unique. We write Γ^- for a context $A_1^-, \ldots, A_n^-$ and γ^+ for an empty succedent or C^+. All inference rules for the sequent calculus can be annotated so that for a goal sequent $\Gamma^- \longrightarrow \gamma^+$, each sequent arising in the derivation has the same form, with only negative propositions on the left and positive propositions on the right (see Exercise 5.1). We say that A is a subformula of Γ or γ if A is a subformula of an element of Γ or γ, respectively, and similarly for signed propositions.

Theorem 5.5 (Signed Subformula Property)
Given a derivation $\mathcal{S}$ of $\Gamma^- \longrightarrow \gamma^+$. Then each sequent in $\mathcal{S}$ has the form $A_1^-, \ldots, A_n^- \longrightarrow B^+$ or $A_1^-, \ldots, A_n^- \longrightarrow \cdot$ where all A_i^- and B^+ are signed subformulas of Γ^- or γ^+.

Proof: By straightforward induction on the structure of $\mathcal{S}$. □

Note that this is a very strong theorem, since it asserts not only that every provable goal sequent has a derivation consisting of subformulas, but that *all* derivations of a provable sequent consist only of subformulas. A sequent not consisting of subformulas cannot contribute to a derivation of a goal sequent in the (cut-free) forward sequent calculus.

The subformula property immediately gives rise to a procedure for forward theorem proving. We start with all initial sequents of the form $A^- \longrightarrow A^+$ where both A^- and A^+ are signed subformulas of the goal sequent. We also have to add $\cdot \longrightarrow \top^+$ and $\bot^- \longrightarrow \cdot$ if $\top^+$ or $\bot^-$ are subformulas of the goal sequent, respectively.

Then we apply all possible inference rules where the principal proposition in the conclusion is a subformula of the goal sequent. We stop with success when we have generated the goal sequent, or if the goal sequent can be obtained from a generated sequent by weakening. We fail if any possible way of applying inference rules yields only sequents already in the database. In that case the goal sequent cannot be derivable if we have not encountered it (or a strengthened form of it) already.

We now show an example derivation in a linearized format. The goal sequent is $A \supset (B \supset C) \longrightarrow ((A \wedge B) \supset C)$. After signing each subformula we obtain

$$(A^+ \supset (B^+ \supset C^-)^-)^- \longrightarrow (((A^- \wedge B^-)^-) \supset C^+)^+$$

If show only the top-level sign, this leads to the following list of signed subformulas.

$$\begin{array}{l} A^+, B^+, C^-, A^-, B^-, C^+, \\ (B \supset C)^-, (A \wedge B)^-, \\ (A \supset (B \supset C))^-, ((A \wedge B) \supset C)^+ \end{array}$$

This means we have both positive and negative occurrences of A, B, and C and we have to consider three initial sequents.

1	$A^- \longrightarrow A^+$	init
2	$B^- \longrightarrow B^+$	init
3	$C^- \longrightarrow C^+$	init
4	$(A \wedge B)^- \longrightarrow A^+$	$\wedge\mathrm{L}_1$ 1
5	$(A \wedge B)^- \longrightarrow B^+$	$\wedge\mathrm{L}_1$ 2
6	$(A \wedge B)^-, (B \supset C)^- \longrightarrow C^+$	$\supset$L 5 3
7	$(A \wedge B)^-, (A \supset (B \supset C))^- \longrightarrow C^+$	$\supset$L 4 6
8	$(A \supset (B \supset C))^- \longrightarrow ((A \wedge B) \supset C)^+$	$\supset\mathrm{R}_1$ 7

We use the horizontal lines to indicate iterations of an algorithm which derives all possible new consequences from the sequents already established. We have elided those sequents that do not contribute to the final derivation. For example, in the first step we can use $\supset\mathrm{R}_2$ to conclude $C^- \longrightarrow ((A \wedge B) \supset C)^+$, from $C^- \longrightarrow C^+$, since the succedent is a positive subformula of the goal sequent.

Note that the inference of line 7 contains an implicit contraction, since $(A \wedge B)^-$ is an assumption in both premises (4 and 6).

5.4 Naming Subformulas

Without any further optimizations, the check if a given inference rule should be used in the forward direction is complicated, since we have to repeatedly scan the goal sequent for subformula occurrences. An integral part of the inverse method is to avoid this scan by introducing names for non-atomic subformulas and then specialize the inference rules to work only the names. We will not be formal about this optimization, since we view it as an implementation technique, but not an improvement of a logical nature. By expanding all newly defined names we obtain a derivation as in the previous section.

We return to the previous example to illustrate the technique. The goal sequent is $A \supset (B \supset C) \longrightarrow (A \wedge B) \supset C$. After naming each subformula we obtain the signed atomic propositions

$$A^+, B^+, C^-, A^-, B^-, C^+,$$

and the new names

$$\begin{array}{rcl}
L_1^- & = & B^+ \supset C^- \\
L_2^- & = & A^- \wedge B^- \\
L_3^- & = & A^+ \supset L_1^- \\
L_4^+ & = & L_2^- \supset C^+
\end{array}$$

We can now write out the general sequent calculus inference rules, specialized to the above labels. Since the goal sequent contains no negative occurrence of negation or falsehood, we may restrict the right-hand sides of all rules to be non-empty. This means only two implication right rules are necessary instead of three for L_4^+.

$$\frac{\Gamma_1 \longrightarrow B^+ \qquad \Gamma_2, C^- \longrightarrow \gamma}{\Gamma_1 \cup \Gamma_2, L_1^- \longrightarrow \gamma} \supset\!\mathrm{L}\ (L_1^-)$$

$$\frac{\Gamma, A^- \longrightarrow \gamma}{\Gamma, L_2^- \longrightarrow \gamma} \wedge\mathrm{L}_1\ (L_2^-) \qquad \frac{\Gamma, B^- \longrightarrow \gamma}{\Gamma, L_2^- \longrightarrow \gamma} \wedge\mathrm{L}_2\ (L_2^-)$$

$$\frac{\Gamma_1 \longrightarrow A^+ \qquad \Gamma_2, L_1^- \longrightarrow \gamma}{\Gamma_1 \cup \Gamma_2, L_3^- \longrightarrow \gamma} \supset\!\mathrm{L}\ (L_3^-)$$

$$\frac{\Gamma, L_2^- \longrightarrow C^+}{\Gamma \longrightarrow L_4^+} \supset\!\mathrm{R}_1\ (L_4^+) \qquad \frac{\Gamma \longrightarrow C^+}{\Gamma \longrightarrow L_4^+} \supset\!\mathrm{R}_2\ (L_4^+)$$

In its labeled form, the derivation above looks as follows.

1	$A^- \longrightarrow A^+$	init
2	$B^- \longrightarrow B^+$	init
3	$C^- \longrightarrow C^+$	init
4	$L_2^- \longrightarrow A^+$	$\wedge\mathrm{L}_1$ 1
5	$L_2^- \longrightarrow B^+$	$\wedge\mathrm{L}_1$ 2
6	$L_2^-, L_1^- \longrightarrow C^+$	$\supset$L 5 3
7	$L_2^-, L_3^- \longrightarrow C^+$	$\supset$L 4 6
8	$L_3^- \longrightarrow L_4^+$	$\supset\mathrm{R}_1$ 7

In the algorithm for labeling subterms we can avoid some redundancy if we give identical subterms the same label. However, this is not required for soundness and completeness, it only trims the search space.

Another choice arises for initial sequents. As in backwards search, we may restrict ourselves to atomic initial sequents or we may allow arbitrary labeled subformulas as long as they occur both negatively and positively. Tammet [Tam96] reports that allowing non-atomic initial sequents led to significant speed-up on a certain class of test problems. Of course, in their named form, even non-atomic sequents have the simple form $L^- \longrightarrow L^+$ for a label L.

5.5 Forward Subsumption

For the propositional case, we can obtain a decision procedure from the inverse method. We stop with success if we have reached the goal sequent (or a strengthened form of it) and with failure if any possible application of an inference rule leads to a sequent that is already present. This means we should devise a data structure or algorithm which allows us to check easily if the conclusion of an inference rule application is already present in the database of derived sequents. This check for equality should allow for permutations of hypotheses.

We can improve this further by not just checking equality modulo permutations, but taking weakening into account. For example, if we have derived $L_1^-, L_2^- \longrightarrow L_4^+$ then the sequent $L_1^-, L_2^-, L_3^- \longrightarrow L_4^+$ is redundant and could simply be obtained from the previous sequent by weakening. Similarly, $L_1^- \longrightarrow \cdot$ has more information than $L_1^- \longrightarrow L_2^+$, so the latter clause does not need to be kept if we have the former clause. Note that we already need this form of weakening to determine success if the goal sequent has assumptions. We say the a sequent S subsumes a sequent S' (written as $S \leq S'$) if S' can be obtains from S by weakening on the right and left.

In the propositional case, there is a relatively simple way to implement subsumption. We introduce a total ordering among all atomic propositions and also the new literals introduced during the naming process. Then we keep the antecedents of each sequent as an ordered list of atoms and literals. The union operation required in the implementation of inference rules with two premises, and the subset test required for subsumption can now both be implemented efficiently.

The reverse, called *backward subsumption* discards a previously derived sequent S if the new sequent S' subsumes S. Generally, backward subsumption is considered less fundamentally important. For example, it is not necessary to obtain a decision procedure for the propositional case. Implementations generally appear to be optimized for efficient forward subsumption.

[*the remainder of this section is speculative*]

However, it seems possible to exploit backward subsumption in a stronger way. Instead of simply deleting the subsumed sequent, we could strengthen its consequences, essentially by replaying the rules applied to it on the stronger sequent.

5.6 Proof Terms for the Inverse Method

The simplicity of the proof for the completeness theorem (Theorem 5.4) indicates that a proof term assignment should be relatively straightforward. The implicit contraction necessary when taking the union of two sets of antecedents presents the only complication. A straightforward solution seems to be to label each antecedent not with just a single variable, but with a set of variables. When taking the union of two sets of antecedents, we also need to take the union of the corresponding label sets. But this would require globally different variables for labeling antecedents in order to avoid interference between the premises of two-premise rules. Another possibility would be to assign a unique label to each negative subformula of the goal sequent and simply use this label in the proof term. This strategy will have to be reexamined in the first-order case, since a given literal may appear with different arguments.

Note that proof term assignment in the forward sequent calculus can be done *on-line* or *off-line*. In the on-line method we construct an appropriate proof term for each sequent at each inference step in a partial derivation. In the off-line method we keep track of the minimal information so we can recover the actual sequence of inference steps to arrive a the final conclusion. From this we reconstruct a proof term only once a complete sequent derivation has been found.

The on-line method would be preferable if we could use the proof term information to guide further inferences or subsumption; otherwise the off-line method is preferable since the overhead is reduced to a a validation phase once a proof has been found.

5.7 Forward Sequent Calculus for First-Order Logic

Generalizing the basic ideas of the inverse method as introduced in the preceding sections requires unification (see Section 4.4), although it is employed in a different way than in backward search. The underlying method can be traced directly to Robinson's original work on resolution [Rob65], and precise connections to classical resolution have been established in the literature [Tam97].

The extension of the forward sequent calculus to the first-order case is straightforward.

$$\frac{\Gamma, [t/x]A \longrightarrow \gamma}{\Gamma, \forall x.\ A \longrightarrow \gamma}\,\forall\mathrm{L} \qquad \frac{\Gamma \longrightarrow [a/x]A}{\Gamma \longrightarrow \forall x.\ A}\,\forall\mathrm{R}^a$$

$$\frac{\Gamma, [a/x]A \longrightarrow \gamma}{\Gamma, \exists x.\ A \longrightarrow \gamma}\,\exists\mathrm{L}^a \qquad \frac{\Gamma \longrightarrow [t/x]A}{\Gamma \longrightarrow \exists x.\ A}\,\exists\mathrm{R}$$

Recall the restriction on the $\forall$R and $\exists$L rules: the derivation of premise must be parametric in a. That is, a may not occur in Γ or A. Soundness and completeness of this calculus with respect to the backward sequent calculus extends in a straightforward way.

These rules suggest an extension of the subformula property. We write $A < B$ for A *is an immediate subformula of* B, $^\pm$ for an arbitrary sign ($^+$ or $^-$) and

$^{\mp}$ for its complement.

$$\begin{array}{ll}
A^{\pm} < (A \wedge B)^{\pm} & B^{\pm} < (A \wedge B)^{\pm} \\
A^{\pm} < (A \vee B)^{\pm} & B^{\pm} < (A \vee B)^{\pm} \\
A^{\mp} < (A \supset B)^{\pm} & B^{\pm} < (A \supset B)^{\pm} \\
{[a/x]}A^{+} < (\forall x.\, A)^{+} & \text{for all parameters } a \\
{[t/x]}A^{-} < (\forall x.\, A)^{-} & \text{for all terms } t \\
{[t/x]}A^{+} < (\exists x.\, A)^{+} & \text{for all terms } t \\
{[a/x]}A^{-} < (\exists x.\, A)^{-} & \text{for all parameters } a
\end{array}$$

We write $A <^* B$ for the reflexive and transitive closure of the immediate subformula relation. Also, we write $A <^* \Gamma$ if there is a formula B in Γ such that $A <^* B$, and $\Delta <^* \Gamma$ if for every A in Δ, $A <^* \Gamma$.

The signed subformula property (Theorem 5.5) directly extends to the first-order case, using the definitions above:

> *For all sequents* $\Delta^- \longrightarrow A^+$ *or* $\Delta^- \longrightarrow \cdot$ *in a derivation of* $\Gamma^- \longrightarrow C^+$ *or* $\Gamma^- \longrightarrow \cdot$ *we have* $\Delta^-, A^+ <^* \Gamma^-, C^+$.

Before formalizing the first-order inverse method, we now go through several examples which show how to take advantage of this extended subformula property in order to construct a search algorithm.

The first example is

$$(\forall x.\, P(x) \supset P(g(x))) \longrightarrow P(c) \supset P(g(g(c)))$$

for a unary predicate P, function f and constant c. We begin by enumerating and naming subformulas. First, the atomic subformulas, from left to right.

$$\begin{array}{lll}
(i) & P(\underline{t})^{+} & \text{for all terms } \underline{t} \\
(ii) & P(g(\underline{s}))^{-} & \text{for all terms } \underline{s} \\
(iii) & P(c)^{-} & \\
(iv) & P(g(g(c)))^{+} &
\end{array}$$

Now, we have to consider all initial sequents $Q \longrightarrow Q$ where Q is a subformula of the goal sequent above. To this end we *unify* positive and negative atomic propositions, treating $\underline{t}$ and $\underline{s}$ as variables, since they stand for arbitrary terms. We obtain:

$$\begin{array}{lll}
1. & P(g(\underline{s}))^{-} \longrightarrow P(g(\underline{s}))^{+} & \text{for all term } \underline{s}, \text{ from } (ii) \text{ and } (i) \\
2. & P(g(g(c)))^{-} \longrightarrow P(g(g(c)))^{+} & \text{from } (ii) \text{ and } (iv) \\
3. & P(c)^{-} \longrightarrow P(c)^{+} & \text{from } (iii) \text{ and } (i)
\end{array}$$

Note that the sequent (1) above represents a schematic judgment in the same way that inferences rules are schematic, where $\underline{s}$ is a schematic variable ranging over arbitrary terms. This will be true not only of the initial sequents, but of the sequents we derive. This is one of the major generalizations from the propositional case of the inverse method.

We can see that the initial sequents described in line (1) includes those in line (2), since we can use $g(c)$ for $\underline{s}$. This is an extended form of subsumption: not only do we check is one sequent can be weakened to another, but we also have to allow for instantiation of variables ($\underline{s}$, in this case).

Next, we introduce names for compound subformulas.

$$\begin{array}{lcll}
L_1(\underline{t})^- & = & P(\underline{t})^+ \supset P(g(\underline{t}))^- & \text{for terms } \underline{t} \\
L_2^- & = & \forall x.\, L_1(x)^- & \\
L_3^+ & = & P(c)^- \supset P(g(g(c)))^+ &
\end{array}$$

From the general forward sequent rules, we can now construct versions of the inference rules specialized to subformulas of the goal sequent.

$$\frac{\Gamma_1 \longrightarrow P(\underline{t})^+ \qquad \Gamma_2, P(g(\underline{t}))^- \longrightarrow \gamma}{\Gamma_1 \cup \Gamma_2, L_1(\underline{t})^- \longrightarrow \gamma} \supset\!\mathrm{L}$$

$$\frac{\Gamma, L_1(t)^- \longrightarrow \gamma}{\Gamma, L_2^- \longrightarrow \gamma} \forall\mathrm{L}$$

$$\frac{\Gamma, P(c)^- \longrightarrow P(g(g(c)))^+}{\Gamma \longrightarrow L_3^+} \supset\!\mathrm{R}_1$$

$$\frac{\Gamma \longrightarrow P(g(g(c)))^+}{\Gamma \longrightarrow L_3^+} \supset\!\mathrm{R}_2 \qquad \frac{\Gamma, P(c)^- \longrightarrow \cdot}{\Gamma \longrightarrow L_3^+} \supset\!\mathrm{R}_3$$

The notation distinguishes the cases where an arbitrary term t is involved in the rule because of the principal connective (in the $\forall$L rule) and where an arbitrary term $\underline{t}$ is involved because of subformula considerations (in the $\supset$L rule).

We can now use these rules, starting from the remaining two initial sequents to derive the goal sequent $L_2^- \longrightarrow L_3^+$. We omit some, but not all sequents that could be generated, but do not contribute to the final derivation.

1.	$P(g(\underline{s}))^- \longrightarrow P(g(\underline{s}))^+$	init, for all terms $\underline{s}$
3.	$P(c)^- \longrightarrow P(c)^+$	init
4.	$P(c)^-, L_1(c)^- \longrightarrow P(g(c))^+$	$\supset$L 3 1$[c/\underline{s}]$
5.	$P(g(\underline{t}))^-, L_1(g(\underline{t}))^- \longrightarrow P(g(g(\underline{t})))^-$	$\supset$L 1$[\underline{t}/\underline{s}]$ 1$[g(\underline{t})/\underline{s}]$, for all $\underline{t}$
6.	$P(g(g(c)))^- \longrightarrow L_3^+$	$\supset$R$_2$ 1$[g(c)/\underline{s}]$
7.	$P(g(\underline{t}))^-, L_2^- \longrightarrow P(g(g(\underline{t})))^+$	$\forall$L 5, for all $\underline{t}$
8.	$P(c)^-, L_2^-, L_1(c)^- \longrightarrow P(g(g(c)))^+$	$\supset$L 3 7$[c/\underline{t}]$
9.	$P(c)^-, L_2^- \longrightarrow P(g(g(c)))^+$	$\forall$L 8, with contraction
10.	$L_2^- \longrightarrow L_3^+$	$\supset$R$_1$ 9

Inference previously involved matching a sequents against the premises of an inference rule. As this example shows, we now have to *unify* derived sequents with the premises of the inference rules. The schematic variables in the sequent as well as in the inference rule may be instantiated in this process, thereby determining the most general conclusion. It is important in this process to note that the scope of each schematic variable includes only a particular sequent or inference rule. Schematic variables called $\underline{t}$ in different sequents are different—usually this is accounted for by systematically renaming variables before starting unification.

The example above does not involve any parameters, only schematic variables. We now consider another example involving parameters,

$$\exists y.\, \forall x.\, P(x,y) \longrightarrow \forall x.\, \exists y.\, P(x,y)$$

for a binary predicate P. Clearly, this judgment should be derivable. Again, we first generate positive and negative atomic subformulas.

$$\begin{array}{lll} (i) & P(\underline{t},\underline{a})^- & \text{for all terms } \underline{t} \text{ and parameters } \underline{a} \\ (ii) & P(\underline{b},\underline{s})^+ & \text{for all parameters } \underline{b} \text{ and terms } \underline{s} \end{array}$$

Because of the negative existential and positive universal quantification the allowed instances of the atomic subformulas are restricted to parameters in certain places. However, it should be understood that $\underline{a}$ in line (i) is only a schematic variable ranging over parameters and may be instantiated to different parameters for different uses of a negative formula $P(\_,\_)^-$.

Next we generate all possible atomic initial sequents. This means we have to look for common instances of the positive and negative atomic formulas schemas listed above. The only possible instances have the form

$$1. \quad P(\underline{b},\underline{a})^- \longrightarrow P(\underline{b},\underline{a})^+ \quad \text{for all parameters } \underline{b} \text{ and terms } \underline{s}$$

Now we list the possible compound subformulas.

$$\begin{array}{lcll} L_1(\underline{a})^- & = & \forall x.\, P(x,\underline{a})^- & \text{for parameters } \underline{a} \\ L_2^- & = & \exists y.\, L_1(y)^- & \\ L_3(\underline{b})^+ & = & \exists y.\, P(\underline{b},y)^+ & \text{for parameters } \underline{b} \\ L_4^+ & = & \forall x.\, L_3(x)^+ & \end{array}$$

The specialized inference rules read:

$$\frac{\Gamma, P(t,\underline{a})^- \longrightarrow \gamma}{\Gamma, L_1(\underline{a})^- \longrightarrow \gamma}\,\forall\mathrm{L} \qquad \frac{\Gamma, L_1(a)^- \longrightarrow \gamma}{\Gamma, L_2^- \longrightarrow \gamma}\,\exists\mathrm{L}^a$$

$$\frac{\Gamma \longrightarrow P(\underline{b},s)^+}{\Gamma \longrightarrow L_3(\underline{b})^+}\,\exists\mathrm{R} \qquad \frac{\Gamma \longrightarrow L_3(b)^+}{\Gamma \longrightarrow L_4^+}\,\forall\mathrm{R}^b$$

Note that the $\exists$L and $\forall$R rules have parametric premises, which means we have to enforce the side condition that parameter a or b do not occur elsewhere in the premises of these two rules, respectively. The derivation takes the following simple form. We omit signs for brevity, and it should be understood that $\underline{b}$ and $\underline{a}$ are quantified *locally* in each sequent.

1.	$P(\underline{b},\underline{a}) \longrightarrow P(\underline{b},\underline{a})$	init	
2.	$L_1(\underline{a}) \longrightarrow P(\underline{b},\underline{a})$	$\forall$L 1	
3.	$P(\underline{b},\underline{a}) \longrightarrow L_3(\underline{b})$	$\exists$R 1	
4.	$L_1(\underline{a}) \longrightarrow L_3(\underline{b})$	$\exists$R 2	
5.	$L_1(\underline{a}) \longrightarrow L_3(\underline{b})$	$\forall$L 3	(subsumed by 4)
6.	$L_2 \longrightarrow L_3(\underline{b})$	$\exists\mathrm{L}^a$ 4	
7.	$L_1(\underline{a}) \longrightarrow L_4$	$\forall\mathrm{R}^b$ 4	
8.	$L_2 \longrightarrow L_4$	$\forall\mathrm{R}^b$ 6	or $\exists\mathrm{L}^a$ 7

Note that the ∃L and ∀R rule are not applicable to sequents (2) or (3), because the side conditions on the parameters would be violated.

Next we consider the converse, which should *not* be derivable.

$$\forall x.\, \exists y.\, P(x,y) \longrightarrow \exists y.\, \forall x.\, P(x,y)$$

Again, we first generate the atomic subformulas.

(i)	$P(\underline{t},\underline{a})^-$	for all terms $\underline{t}$ and parameters $\underline{a}$
(ii)	$P(\underline{b},\underline{s})^+$	for all parameters $\underline{b}$ and terms $\underline{s}$

Then the possible initial sequents.

1. $P(\underline{b},\underline{a})^- \longrightarrow P(\underline{b},\underline{a})^+$ for all parameters $\underline{b}$ and terms $\underline{a}$

Then, the compound subformulas.

$$\begin{array}{lcll} L_1(\underline{t})^- & = & \exists y.\, P(\underline{t},y)^- & \text{for terms } \underline{t} \\ L_2^- & = & \forall x.\, L_1(x)^- & \\ L_3(\underline{s})^+ & = & \forall x.\, P(x,\underline{s})^+ & \text{for terms } \underline{s} \\ L_4^+ & = & \exists y.\, L_3(y)^+ & \end{array}$$

From this we derive the specialized rules of inference.

$$\frac{\Gamma, P(\underline{t},a)^- \longrightarrow \gamma}{\Gamma, L_1(\underline{t})^- \longrightarrow \gamma}\,\exists\mathrm{L}^a \qquad \frac{\Gamma, L_1(t)^- \longrightarrow \gamma}{\Gamma, L_2^- \longrightarrow \gamma}\,\forall\mathrm{L}$$

$$\frac{\Gamma \longrightarrow P(b,\underline{s})^+}{\Gamma \longrightarrow L_3(\underline{s})^+}\,\forall\mathrm{R} \qquad \frac{\Gamma \longrightarrow L_3(s)^+}{\Gamma \longrightarrow L_4^+}\,\exists\mathrm{R}$$

Given an initial sequent

1. $P(\underline{b},\underline{a})^- \longrightarrow P(\underline{b},\underline{a})^+$ for all parameters $\underline{b}$ and terms $\underline{a}$

we see that no inference rules are applicable, because the side condition on parameter occurrences would be violated. Therefore the goal sequent cannot be derivable.

5.8 Factoring

The examples in the previous section suggest the following algorithm:

1. Determine all signed schematic atomic subformulas of the given goal sequent.
2. Unify positive and negative atomic subformulas after renaming variables so they have none in common. This yields a set of initial sequents from which subsumed copies should be eliminated.
3. Name all signed compound subformulas as new predicates on their free variables.
4. Specialize the inference rules to these subformulas.
5. Starting from the initial sequents, apply the specialized inference rules in a fair way by unifying (freshly renamed) copies of sequents derived so far with premises of the inference rules, generating most general conclusions as a new schematic sequents.
6. Stop with success when the goal sequent has been derived.

Perhaps somewhat surprisingly, this method is incomplete using only the rules given so far. As a counterexample, consider

$$\cdot \longrightarrow \exists x.\, P(x) \supset P(x) \wedge P(c)$$

for a unary predicate P and constant c. Initial sequents:

$$\begin{array}{lll} 1. & P(\underline{t}) \longrightarrow P(\underline{t}) & \text{for all terms } t \\ 2. & P(c) \longrightarrow P(c) & \text{(subsumed by (1))} \end{array}$$

Signed subformulas:

$$\begin{array}{lcl} L_1^+(\underline{s}) & = & P(\underline{s})^+ \wedge P(c)^+ \\ L_2^+(\underline{s}) & = & P(\underline{s})^- \supset L_1(\underline{s})^+ \\ L_3^+ & = & \exists x.\, L_2^+(x) \end{array}$$

Specialized rules (omitting polarities and the irrelevant $\supset$R$_3$):

$$\frac{\Gamma_1 \longrightarrow P(\underline{s}) \qquad \Gamma_2 \longrightarrow P(c)}{\Gamma_1 \cup \Gamma_2 \longrightarrow L_1} \wedge\mathrm{I}$$

$$\frac{\Gamma, P(\underline{s}) \longrightarrow L_1(\underline{s})}{\Gamma \longrightarrow L_2(\underline{s})} \supset\mathrm{R}_1 \qquad \frac{\Gamma \longrightarrow L_1(\underline{s})}{\Gamma \longrightarrow L_2(\underline{s})} \supset\mathrm{R}_2$$

$$\frac{\Gamma \longrightarrow L_2(t)}{\Gamma \longrightarrow L_3} \exists\mathrm{R}$$

Initially, we can only apply $\wedge$I, after renaming a copy of (1).

$$\begin{array}{lll}
1. & P(\underline{t}) \longrightarrow P(\underline{t}) & \text{init, for all terms } \underline{t} \\
3. & P(\underline{t}), P(c) \longrightarrow L_1(\underline{t}) & \wedge\text{R}\, 1[\underline{t}/\underline{t}]\ 1[c/\underline{t}], \text{for all terms } \underline{t}
\end{array}$$

Now there are two ways to apply the $\supset\text{R}_1$ rule, but either $P(\underline{t})$ or $P(c)$ is left behind as an assumption, and the goal sequent cannot be derived.

The problem is that even though the sequent

$$P(c) \longrightarrow L_1(c)$$

should be derivable, it is only the contraction of an instance of sequent (3). We therefore extend the system with an explicit rule which permits contraction after instantiation, called *factoring*. That is, after we derive a new sequent, we consider possible most general unifiers among antecedents of the sequent and add the results (while continuing to check for subsumption).

In the example above, we proceed as follows:

$$\begin{array}{lll}
1. & P(\underline{t}) \longrightarrow P(\underline{t}) & \text{init, for all terms } \underline{t} \\
3. & P(\underline{t}), P(c) \longrightarrow L_1(\underline{t}) & \wedge\text{R}\ 1[\underline{t}/\underline{t}]\ 1[c/\underline{t}], \text{for all terms } \underline{t} \\
4. & P(c) \longrightarrow L_1(c) & \mathit{factor}\, 3[c/\underline{t}] \\
5. & \cdot \longrightarrow L_2(c) & \supset\text{R}_1\ 4 \\
6. & \cdot \longrightarrow L_3 & \exists\text{R}
\end{array}$$

Usually, this is done eagerly for each rule which unions assumptions and therefore might allow new factors to be derived. It is also possible to delay this until the rules which require factoring (such as $\supset$R), but this might require factoring to be done repeatedly and may prohibit some subsumption.

In our inference rule notation, where unification of sequents with premises of rules is implicit, this factoring rule would simply look like a contraction.

$$\frac{\Gamma, A, A \longrightarrow C}{\Gamma, A \longrightarrow C}\,\text{contract}$$

Previously, this was implicit, since we maintained assumptions as sets.

5.9 Inverse Focusing

In the system presented so far the non-determinism in forward reasoning is still unacceptable, despite the use of subsumption. We can now analyze the rules in a way that is analogous to Chapter 4, taking advantage of inversion and focusing properties. This eliminates many derivations, significantly improving overall efficiency at a high level of abstraction. Similar optimizations have been proposed by Tammet [Tam96] and Mints [Min94], although the exact relationship between these system and the one presented below have yet to be investigated. The work here exploits Andreoli's observation [**?**] that focused derivations correspond to interpreting propositions as derived rules of inference. Much of this section, however, is speculative in the sense that no formal properties have been proven.

Our overall strategy is to restrict the inverse method further so that it can find only focused proofs.

Given a sequent $\Gamma \Longrightarrow A$, use ordinary backward reasoning to decompose $\cdot; \Gamma \overset{a}{\Longrightarrow} A; \cdot$ into a collection of subgoals, all of which have the form $\Delta; \cdot \overset{a}{\Longrightarrow} \cdot; R$. Note that this set is uniquely determined (modulo names of parameters that may be introduced). We prove each of the subgoals completely independently.

We call sequents of the form $\Delta; \cdot \overset{a}{\Longrightarrow} \cdot; R$ *stable sequents*. Recall that Δ consists only of left synchronous propositions (P, $A \supset B$, $\forall x.\ A$) and R only of right synchronous propositions (P, $A \vee B$, $\bot$, $\exists x.\ A$). In our version of the inverse method, we only generate stable sequents, so we write them as $\Delta \longrightarrow R$. Furthermore, instead of naming all subformulas, we only name the subformulas that could occur in stable sequents in the search for a proof of the given proposition.

As a first example, consider proving $(A \supset (B \supset C)) \supset ((A \wedge B) \supset C)$. Here, A, B, and C are considered atomic formulas. We begin by decomposing all top-level asynchronous connectives.

$$\begin{array}{l}
B, A, A \supset (B \supset C); \cdot \overset{a}{\Longrightarrow} \cdot; C \\
B, A; A \supset (B \supset C) \overset{a}{\Longrightarrow} \cdot; C \\
B; A \supset (B \supset C), A \overset{a}{\Longrightarrow} \cdot; C \\
\cdot; A \supset (B \supset C), A, B \overset{a}{\Longrightarrow} \cdot; C \\
\cdot; A \supset (B \supset C), A \wedge B \overset{a}{\Longrightarrow} \cdot; C \\
\cdot; A \supset (B \supset C), A \wedge B \overset{a}{\Longrightarrow} C; \cdot \\
\cdot; A \supset (B \supset C) \overset{a}{\Longrightarrow} (A \wedge B) \supset C; \cdot \\
\cdot; \cdot \overset{a}{\Longrightarrow} (A \supset (B \supset C)) \supset ((A \wedge B) \supset C); \cdot
\end{array}$$

Next we consider how a bottom-up proof search could proceed: it could focus on any of the three propositions in the premise, but not on the conclusion (since C is atomic).

Focusing on B or A succeeds only if the conclusion is B and A, respectively. This leads to the initial sequents

$$\begin{array}{c}
A \longrightarrow A \\
B \longrightarrow B
\end{array}$$

If we focus on $A \supset (B \supset C)$, in a situation where have some unknown Δ and R, the proof fragment would have to look as follows:

$$\begin{array}{lll}
(1) & \Delta; \cdot \overset{a}{\Longrightarrow} \cdot; A & \\
(2) & \Delta; \cdot \overset{s}{\Longrightarrow} A; \cdot & \text{blur}R\ 1 \\
(3) & \Delta; \cdot \overset{a}{\Longrightarrow} \cdot; B & \\
(4) & \Delta; \cdot \overset{s}{\Longrightarrow} B; \cdot & \text{blur}R\ 3 \\
(5) & \Delta; C \overset{s}{\Longrightarrow} \cdot; R & \\
(6) & \Delta; B \supset C \overset{s}{\Longrightarrow} \cdot; R & {\supset}\text{L}\ 5\ 4 \\
(7) & \Delta; A \supset (B \supset C) \overset{s}{\Longrightarrow} \cdot; R & {\supset}\text{L}\ 6\ 2
\end{array}$$

Here (1) and (3) are stable sequents, but what about (5)? The only rule that applies is init, for $C = R$. This means any use of focusing with the hypothesis $A \supset (B \supset C)$ will reduce the goal of proving C to the goal of proving A and B. Writing is as a derived rule (and changing it to the forward direction)

$$\frac{\Delta_1 \longrightarrow A \qquad\quad \Delta_2 \longrightarrow B}{\Delta_1, \Delta_2, A \supset (B \supset C) \longrightarrow C}$$

Next we observe that B, A, and $A \supset (B \supset C)$ would occur in any (bottom-up) focused sequent that is part of the proof search tree. We call such assumptions *global* and do not explicitly write them in our sequents. As a result we have exactly two axioms and one rule of inference.

$$\cdot \longrightarrow A$$

$$\cdot \longrightarrow B$$

$$\frac{\Delta_1 \longrightarrow A \qquad\quad \Delta_2 \longrightarrow B}{\Delta_1, \Delta_2 \longrightarrow C}$$

The overall goal is to prove $\cdot \longrightarrow C$, which follows in one inference. We also observe that Δ_1 and Δ_2 in the sole inference rule will always be empty, since all initial sequents have an empty right-hand side, and all inference rules (only one, here) preserve this property. We claim, without substantiating it, that this is true for any Horn theory.

As a second example, consider $((A \vee C) \wedge (B \supset C)) \supset ((A \supset B) \supset C)$. First, we decompose the asynchronous connectives, which yields two independent theorems to prove.

$$\begin{array}{l} A \supset B, B \supset C, A; \cdot \overset{a}{\Longrightarrow} \cdot; C \\ A \supset B, B \supset C, C; \cdot \overset{a}{\Longrightarrow} \cdot; C \end{array}$$

The second one is trivial. For the first one, focusing on the three possible assumptions, and deleting global assumptions, yields one starting sequent and two rules of inference.

$$\cdot \longrightarrow A$$

$$\frac{\Delta \longrightarrow B}{\Delta \longrightarrow C} \qquad\quad \frac{\Delta \longrightarrow A}{\Delta \longrightarrow B}$$

Now $\cdot \longrightarrow C$ follows in two (forced) steps.

As an example of an unprovable sequent, consider the reverse implication $((A \supset B) \supset C) \supset ((A \vee C) \wedge (B \supset C))$. Asynchronous decomposition yields two independent stable sequents to be proven.

$$\begin{array}{l} (A \supset B) \supset C; \cdot \overset{a}{\Longrightarrow} \cdot; A \vee C \\ B, (A \supset B) \supset C; \cdot \overset{a}{\Longrightarrow} \cdot; C \end{array}$$

Analysing the first one, we apply synchronous decomposition on the right and on the left. On the right we have two possible derivation fragments.

$$\dfrac{\dfrac{\dfrac{\Delta; \cdot \overset{a}{\Longrightarrow} \cdot; A}{\Delta; \cdot \overset{s}{\Longrightarrow} A; \cdot}}{\Delta; \cdot \overset{s}{\Longrightarrow} A \vee C; \cdot}}{\Delta; \cdot \overset{a}{\Longrightarrow} \cdot; A \vee C} \qquad \dfrac{\dfrac{\dfrac{\Delta; \cdot \overset{a}{\Longrightarrow} \cdot; C}{\Delta; \cdot \overset{s}{\Longrightarrow} C; \cdot}}{\Delta; \cdot \overset{s}{\Longrightarrow} A \vee C; \cdot}}{\Delta; \cdot \overset{a}{\Longrightarrow} \cdot; A \vee C}$$

This yields two derived rules of inference in the forward direction.

$$\dfrac{\Delta \longrightarrow A}{\Delta \longrightarrow A \vee C} \qquad \dfrac{\Delta \longrightarrow C}{\Delta \longrightarrow A \vee C}$$

Focusing on the left-hand side instead, we obtain:

$$\dfrac{\Delta; C \overset{s}{\Longrightarrow} \cdot; R \qquad \dfrac{\dfrac{\Delta, A; \cdot \overset{a}{\Longrightarrow} \cdot; B}{\Delta; \cdot \overset{a}{\Longrightarrow} A \supset B; \cdot}\,\text{3 steps}}{\Delta; \cdot \overset{s}{\Longrightarrow} A \supset B; \cdot}}{\Delta; (A \supset B) \supset C \overset{s}{\Longrightarrow} \cdot; R}$$

The leftmost open premise forces $R = C$, so we obtain the rule

$$\dfrac{\Delta, A \longrightarrow B}{\Delta \longrightarrow C}$$

We have to be careful when applying this rule, because A may not acutally be present on the left-hand side (or, if we consider empty succedents, B on the right-hand side). We should mark A and B as optional (although at least one of them must be there, otherwise the rule makes no progress and the conclusion is subsumed by the premise). We indicate this with square brackets.

$$\dfrac{\Delta, [A] \longrightarrow [B]}{\Delta \longrightarrow C}$$

Because focusing on $(A \supset B) \supset C$ adds A as a new assumption, and B as a new conclusion we need to iterate the process of deriving rules. B in the conclusion yields no rule (we cannot focus on an atomic succedent), but A in the premise does because we also have a positive occurrence of A in a prior rule, which yields the initial sequent

$$A \longrightarrow A$$

Summarizing the situation, we have

$$\frac{\Delta \longrightarrow A}{\Delta \longrightarrow A \vee C} \qquad \frac{\Delta \longrightarrow C}{\Delta \longrightarrow A \vee C}$$

$$\frac{\Delta, [A] \longrightarrow [B]}{\Delta \longrightarrow C}$$

$$A \longrightarrow A$$

Forward reasoning saturates after one step, without proving C, which means that this sequent we started with is unprovable. This means the original formula is (intuitionistically) unprovable. However, we can still consider the second subgoal

$$B, (A \supset B) \supset C; \cdot \overset{a}{\Longrightarrow} \cdot; C$$

Applying a similiar analysis to before, we obtain:

$$\frac{\Delta, [A] \longrightarrow [B]}{\Delta \longrightarrow C}$$

$$B \longrightarrow B$$

After one step we obtain $\cdot \longrightarrow C$ (applying the only rule without matching A), which is what we needed to prove. So this subgoal is indeed provable.

Next we consider a first-order example, $(\forall x.\, A(x) \supset C) \supset ((\exists x.\, A(x)) \supset C)$, where x not free in C. First, we decompose the asynchronous connectives.

$$\begin{array}{l}
A(b), \forall x.\, A(x) \supset C; \cdot \overset{a}{\Longrightarrow} \cdot; C \\
A(b); \forall x.\, A(x) \supset C \overset{a}{\Longrightarrow} \cdot; C \\
\cdot; \forall x.\, A(x) \supset C, A(b) \overset{a}{\Longrightarrow} \cdot; C \\
\cdot; \forall x.\, A(x) \supset C, \exists x.\, A(x) \overset{a}{\Longrightarrow} \cdot; C \\
\cdot; \forall x.\, A(x) \supset C, \exists x.\, A(x) \overset{a}{\Longrightarrow} C; \cdot \\
\cdot; \forall x.\, A(x) \supset C \overset{a}{\Longrightarrow} (\exists x.\, A(x)) \supset C; \cdot \\
\cdot; \cdot \overset{a}{\Longrightarrow} (\forall x.\, A(x) \supset C) \supset ((\exists x.\, A(x)) \supset C); \cdot
\end{array}$$

In the resulting stable sequent we have a new parameter b. Since it will be available in any sequent of its proof, we can consider it as a parameter with global scope (that is, a constant). Focusing on $A(b)$ (and erasing the global assumption $A(b)$) yields the initial sequent

$$\cdot \longrightarrow A(b)$$

Focusing on the implication yields

$$\dfrac{\dfrac{\Delta; C \overset{s}{\Longrightarrow} \cdot; R \qquad \dfrac{\Delta; \cdot \overset{a}{\Longrightarrow} \cdot; A(t)}{\Delta; \cdot \overset{s}{\Longrightarrow} A(t); \cdot}}{\Delta; A(t) \supset C \overset{s}{\Longrightarrow} \cdot; R}}{\Delta; \forall x.\, A(x) \supset C \overset{s}{\Longrightarrow} \cdot; R}$$

The left-most open goal forces $R = C$, and we obtain the rule

$$\frac{\Delta \longrightarrow A(t)}{\Delta \longrightarrow C}$$

Note that this rule is schematic in t. Now we obtain our overall goal C in one step, using b for t.

It does not show up very prominently in our examples, but for completeness of this method it is critical that we continue the construction of derived rules with the new subformulas that arise when focusing on any proposition in a stable sequent ends in a collection of new stable sequent.

So, given a stable sequent to start with, we pick a synchronous proposition on the left or right. We iterate synchronous decomposition, obtaining asynchronous subgoals. Those asynchronous subgoals are now decomposed in turn, until we have again all stable sequents. The new propositions in these stable sequents must be named, and then recursively analyzed in the same way.

We must also take care to allow some formula occurrences in the premises of the derived rule to be absent from the sequents they are matched against. We only sketched this here in one of the examples. Finally, we conjecture that it is sufficient to consider contraction (factoring) on stable sequents.

5.10 Exercises

Exercise 5.1 Show the forward sequent calculus on signed propositions and prove that if $\Gamma \longrightarrow A$ then $\Gamma^- \longrightarrow A^+$.

Exercise 5.2 In the exercise we explore add the connective $A \equiv B$ as a primitive to inverse method.

1. Following Exercise 2.6, introduce appropriate left and right rules to the backward sequent calculus.

2. Transform the rules to be appropriate for the forward sequent calculus.

3. Extend the notion of positive and negative subformula.

4. Extend the technique of subformula naming and inference rule specialization.

5. Show inverse derivations for each of the following.
   (a) Reflexivity: $\longrightarrow A \equiv A$.
   (b) Symmetry: $A \equiv B \longrightarrow B \equiv A$.
   (c) Transitivity: $A \equiv B, B \equiv C \longrightarrow A \equiv C$.
6. Compare your technique with thinking of $A \equiv B$ as a syntactic abbreviation for $(A \supset B) \wedge (B \supset A)$. Do you see significant advantages or disadvantages of your method?

Chapter 6

Labeled Deduction

Starting from a system of natural deduction for the definition of intuitionistic logic, we have made a remarkable journey, including the sequent calculus, focusing, and the inverse method. Many, if not all of the idea are shared between many reasonable and useful logics: intuitionistic logic, classical logic, linear logic, modal logic, temporal logic, and probably many more. In this chapter we see another surprisingly robust idea: labeled deduction. There are many views of labeled deduction. One of the most general is that we relativize our notion of truth. While intuistionistic logic is based on a single unary judgment, namely $A\,\mathit{true}$, labeled deduction is based on binary judgments of the form $A\,\mathit{true}[p]$, where p is a *label* or *world*. We may read $A\,\mathit{true}[p]$ as "*A is true at world p.*"

The uses of a relativized notions of truth are many; we concentrate here only on a single one. The motivation comes from developing a sequent calculus for intuitionistic logic in which all rules are invertible. Alternatively, it can be seen as a means of interpreting intuitionistic logic in classical logic (we have already seen the opposite). Wallen's book [Wal90] is the seminal work in this area with respect to automated deduction and is still fresh after more than a decade. A newer reference is Waaler's article in Handbook of Automated Reasoning [Waa01]. Often cited is also Fitting's book [Fit83], but it seems to be difficult to obtain.

6.1 Multiple Conclusions

One of the problems with focusing is that disjunction on the right-hand side is opaque: if we have a conclusion $A \vee B$ may have to try to prove A or B and then backtrack to prove the other without sharing of information between the attempts. Moreover, while focusing on a left synchronous formula, we completely ignore the shape of the succedent. An idea to remedy this situation is to replace $A \vee B$ by A, B on the right-hand side, postponing the choice between A and B. It is difficult to give a satisfactory judgmental reading of multiple propositions on the right, but let us suspend this issue and simply read A, B on the right as a *postponed choice* between A and B.

Our basic judgment form is now

$$\Gamma \overset{m}{\Longrightarrow} \Delta$$

to be read as "*Under assumptions* Γ *prove one of* Δ*,*" although it will not be the case that there is always one element in Δ that we can actually prove. Initial sequents, conjunction, and disjunction are as in the judgment for classical logic, $\Gamma \mathrel{\#} \Delta$, in which Γ are assumptions about truth and Δ assumptions about falsehood.

$$\frac{}{\Gamma, P \overset{m}{\Longrightarrow} P, \Delta}\,\text{init}$$

$$\frac{\Gamma, A, B \overset{m}{\Longrightarrow} \Delta}{\Gamma, A \wedge B \overset{m}{\Longrightarrow} \Delta}\,\wedge\text{L} \qquad \frac{\Gamma \overset{m}{\Longrightarrow} A, \Delta \qquad \Gamma \overset{m}{\Longrightarrow} B, \Delta}{\Gamma \overset{m}{\Longrightarrow} A \wedge B, \Delta}\,\wedge\text{R}$$

$$\frac{\Gamma, A \overset{m}{\Longrightarrow} \Delta \qquad \Gamma, B \overset{m}{\Longrightarrow} \Delta}{\Gamma, A \vee B \overset{m}{\Longrightarrow} \Delta}\,\vee\text{L} \qquad \frac{\Gamma \overset{m}{\Longrightarrow} A, B, \Delta}{\Gamma \overset{m}{\Longrightarrow} A \vee B, \Delta}\,\vee R$$

Since we have already observed that conjunction and disjunction are really the same for intuitionistic and classical logic, perhaps the rules above do not come as a suprise. But how to we salvage the intuitionistic nature of the logic? Consider the problem of $(A \supset B) \vee A$, which is classically true for all A and B, but not intuitionistically. The classical proof is

$$\frac{\dfrac{\dfrac{}{A \mathrel{\#} B, A}\,\text{init}}{\cdot \mathrel{\#} (A \supset B), A}\,{\supset}F}{\cdot \mathrel{\#} (A \supset B) \vee A}\,\vee F$$

If we try to interpret this proof intuitionistically, replacing $\#$ by $\overset{m}{\Longrightarrow}$, we see that the right rule for implication looks very suspicious: the scope of the assumption A should be B (since we say: $A \supset B$), and yet it appears to include the other disjunct, A. In this way we avoid ever producing evidence for one of the propositions on the right: we exploit one to prove the other.

To avoid this counterexample, we have to change the implication right rule to be the following:

$$\frac{\Gamma, A \supset B \overset{m}{\Longrightarrow} A, \Delta \qquad \Gamma, B \overset{m}{\Longrightarrow} \Delta}{\Gamma, A \supset B \overset{m}{\Longrightarrow} \Delta}\,{\supset}\text{L} \qquad \frac{\Gamma, A \overset{m}{\Longrightarrow} B}{\Gamma \overset{m}{\Longrightarrow} A \supset B, \Delta}\,{\supset}\text{R}$$

The crucial point is that before we can use $\supset$R we have to commit a choice to preserve the scope of the new assumption A. This sequent calculus admits weakening and contraction on both sides and a cut elimination theorem. It is also sound and complete, although a theorem to that effect must be formulated carefully.

Before that, we can add the logical constants for truth and falsehood.

$$\frac{\Gamma \overset{m}{\Longrightarrow} \Delta}{\Gamma, \top \overset{m}{\Longrightarrow} \Delta}\top L \qquad \frac{}{\Gamma \overset{m}{\Longrightarrow} \top, \Delta}\top R$$

$$\frac{}{\Gamma, \bot \overset{m}{\Longrightarrow} \Delta}\bot L \qquad \frac{\Gamma \overset{m}{\Longrightarrow} \Delta}{\Gamma \overset{m}{\Longrightarrow} \bot, \Delta}\bot R$$

Negation can be derived from implication and falsehood.

$$\frac{\Gamma, \neg A \overset{m}{\Longrightarrow} A, \Delta}{\Gamma, \neg A \overset{m}{\Longrightarrow} \Delta}\neg L \qquad \frac{\Gamma, A \overset{m}{\Longrightarrow} \cdot}{\Gamma \overset{m}{\Longrightarrow} \neg A, \Delta}\neg R$$

Note that $\neg$R makes a commitment, erasing Δ, as for implication.

The first, natural idea at soundness would state that if $\Gamma \overset{m}{\Longrightarrow} \Delta$, then there is a proposition C in Δ such that $\Gamma \Longrightarrow C$. This, unfortunately, is false, as can be seen from $A \vee B \overset{m}{\Longrightarrow} B, A$ is is provable and, yet, neither B or A by itself follows from $A \vee B$. We write $\bigvee(A_1, \ldots, A_n)$ for $A_1 \vee \cdots \vee A_n$ which is interpreted as $\bot$ if $n = 0$.

Theorem 6.1 (Soundness of Multiple-Conclusion Sequent Calculus) *If* $\Gamma \overset{m}{\Longrightarrow} \Delta$ *then* $\Gamma \Longrightarrow \bigvee \Delta$.

Proof: By induction on the given derivation. Most cases are immediate. We show only the implication cases.

Case:

$$\mathcal{D} = \frac{\begin{array}{c}\mathcal{D}_1\\ \Gamma, A \overset{m}{\Longrightarrow} B\end{array}}{\Gamma \overset{m}{\Longrightarrow} A \supset B, \Delta}\supset R$$

$\Gamma, A \Longrightarrow B$	By i.h.
$\Gamma \Longrightarrow A \supset B$	By rule $\supset$R
$\Gamma \Longrightarrow (A \supset B) \vee \bigvee \Delta$	By repeated $\vee R$

Case:

$$\mathcal{D} = \frac{\begin{array}{c}\mathcal{D}_1\\ \Gamma, A \supset B \overset{m}{\Longrightarrow} A, \Delta\end{array} \qquad \begin{array}{c}\mathcal{D}_2\\ \Gamma, B \overset{m}{\Longrightarrow} \Delta\end{array}}{\Gamma, A \supset B \overset{m}{\Longrightarrow} \Delta}\supset L$$

$\Gamma, A \supset B \Longrightarrow A \vee C$ for $C = \bigvee \Delta$	By i.h.
$\Gamma, B \Longrightarrow C$	By i.h.
$\Gamma \Longrightarrow B \supset C$	By rule $\supset$R
$\Gamma, A \supset B, B \supset C, A \vee C \Longrightarrow C$	Direct proof
$\Gamma, A \supset B, B \supset C \Longrightarrow C$	By admissibility of cut
$\Gamma, A \supset B \Longrightarrow C$	By admissibility of cut

□

Theorem 6.2 (Completness of Multiple-Conclusion Sequent Calculus) *If* $\Gamma \Longrightarrow A$ *then* $\Gamma \overset{m}{\Longrightarrow} A$

Proof: By induction on the given derivation. Most cases are immediate. In the case of $\vee R$ we need to apply weakening after the induction hypothesis. □

6.2 Propositional Labeled Deduction

The next problem is to avoid or at least postpone the choice associated with the $\supset$R rule. However, it is clear we cannot simply leave Δ around, since this would yield classical logic, as the example in the previous section demonstrates. Instead we label assumptions and conclusion in such a way that the new assumption A will be prohibited from being used in the proof of any proposition in the conclusion except for its natural scope, B. In other words, we enforce scoping by labeling. We need *label parameters* $a, b, \ldots$ and *labels*, where a label is simply a sequence of label parameters.

$$\text{Labels} \quad p, q \quad ::= \quad a_1\, a_2 \ldots a_n$$

We use ϵ to denote the empty sequence of labels. An assumption A *true*$[p]$ is supposed to be available to prove any conclusion B *true*$[pq]$, that is, the scope of any label includes any extension of that label. We abbreviate A *true*$[p]$ as $A[p]$. Initial sequents then have the form

$$\frac{}{\Gamma, A[p] \Longrightarrow A[pq], \Delta}\,\text{init}$$

In the implication right rule we create a new scope, by introducing a new label parameter.

$$\frac{\Gamma, A[pa] \Longrightarrow B[pa], \Delta}{\Gamma \Longrightarrow (A \supset B)[p], \Delta}\,\supset\!\text{R}^a$$

Important is that the parameter a must be new. Therefore, for no conlusion $C[q]$ in Δ could q be an extension of pa. Effectively, the scope of $A[pa]$ excludes Δ.

Revisiting an earlier example (and anticipating that $\vee$ propagates its labels to both subformulas), we see that it is not provable because ϵ is not an extension of a.

$$\dfrac{\dfrac{\dfrac{}{A[a] \Longrightarrow B[a], A[\epsilon]}\,?}{\cdot \Longrightarrow (A \supset B)[\epsilon], A[\epsilon]}\,{\supset}\mathrm{R}^a}{\cdot \Longrightarrow (A \supset B) \vee A[\epsilon]}\,\vee R$$

The implication left rule incorporates the fact that an assumption $(A \supset B)[p]$ is available in any extension of p. When we apply ⊃L we have to choose the world in which we can show $A[pq]$. It is in this world that we can assume $B[pq]$.

$$\dfrac{\Gamma, (A \supset B)[p] \Longrightarrow A[pq] \qquad \Gamma, B[pq] \Longrightarrow \Delta}{\Gamma, (A \supset B)[p] \Longrightarrow \Delta}\,{\supset}\mathrm{L}$$

As an example, consider the beginning of the proof of transitivity.

$$\dfrac{\dfrac{\dfrac{A \supset B[a], B \supset C[ab], A[abc] \Longrightarrow C[abc]}{A \supset B[a], B \supset C[ab] \Longrightarrow A \supset C[ab]}\,{\supset}\mathrm{R}^c}{A \supset B[a] \Longrightarrow (B \supset C) \supset A \supset C[a]}\,{\supset}\mathrm{R}^b}{\Longrightarrow (A \supset B) \supset (B \supset C) \supset (A \supset C)[\epsilon]}\,{\supset}\mathrm{R}^a$$

At this point we have to apply implication left to either $A \supset B[a]$ or $B \supset C[ab]$. The difficulty is to guess at which extended label to apply it. If we apply the ⊃L rule to $A \supset B[a]$ we can we see we must be able to prove $A[aq]$ for some q. But we have available only $A[abc]$, so q must be an extension of bc.

$$\dfrac{\dfrac{}{A \supset B[a], B \supset C[ab], A[abc] \Longrightarrow A[abc]}\,\mathrm{init} \qquad B \supset C[ab], A[abc], B[abc] \Longrightarrow C[abc]}{A \supset B[a], B \supset C[ab], A[abc] \Longrightarrow C[abc]}\,{\supset}\mathrm{L}$$

We continue in the right premise with another implication left rule, this time choosing $q = c$ so we can prove $B[abq]$.

$$\dfrac{\dfrac{}{B \supset C[ab], A[abc], B[abc] \Longrightarrow B[abc]}\,\mathrm{init} \qquad \dfrac{}{A[abc], B[abc], C[abc] \Longrightarrow C[abc]}\,\mathrm{init}}{B \supset C[ab], A[abc], B[abc] \Longrightarrow C[abc]}\,{\supset}\mathrm{L}$$

In the rules for remaining propositional connectives, the labels do not change because no new scope is introduced.

$$\dfrac{\Gamma, A[p], B[p] \Longrightarrow \Delta}{\Gamma, (A \wedge B)[p] \Longrightarrow \Delta}\,\wedge\mathrm{L} \qquad \dfrac{\Gamma \Longrightarrow A[p], \Delta \qquad \Gamma \Longrightarrow B[p], \Delta}{\Gamma \Longrightarrow (A \wedge B)[p], \Delta}\,\wedge\mathrm{R}$$

$$\dfrac{\Gamma, A[p] \Longrightarrow \Delta \qquad \Gamma, B[p] \Longrightarrow \Delta}{\Gamma, (A \vee B)[p] \Longrightarrow \Delta}\,\vee\mathrm{L} \qquad \dfrac{\Gamma \Longrightarrow A[p], B[p], \Delta}{\Gamma \Longrightarrow (A \vee B)[p], \Delta}\,\vee R$$

Truth and falsehood are also straightforward.

$$\frac{\Gamma \Longrightarrow \Delta}{\Gamma, \top[p] \Longrightarrow \Delta}\,\top\mathrm{L} \qquad \frac{}{\Gamma \Longrightarrow \top[p], \Delta}\,\top\mathrm{R}$$

$$\frac{}{\Gamma, \bot[p] \Longrightarrow \Delta}\,\bot\mathrm{L} \qquad \frac{\Gamma \Longrightarrow \Delta}{\Gamma \Longrightarrow \bot[p], \Delta}\,\bot\mathrm{R}$$

A way to think about the $\bot$L rule is to consider that $\bot[p]$ entails the empty right-hand side from which we can generate Δ by weakening. So it makes sense even if all the worlds in Δ are out of the scope defined by p. We can determine the laws for negation from considerations for implication and falsehood.

$$\frac{\Gamma, (\neg A)[p] \Longrightarrow A[pq], \Delta}{\Gamma, (\neg A)[p] \Longrightarrow \Delta}\,\neg\mathrm{L} \qquad \frac{\Gamma, A[pa] \Longrightarrow \Delta}{\Gamma \Longrightarrow (\neg A)[p], \Delta}\,\neg\mathrm{R}^a$$

The $\neg$R rule is subject to the proviso that a does not appear in the conclusion.

Showing the soundness and completeness of labeled deduction is not a trivial enterprise; we show here only completeness. A critical notion is that of a *monotone sequent*. We write $p \preceq q$ if there exists a p' such that $p\,p' = q$ and say *p is a prefix of q*. We say a sequent $A_1[p_1], \ldots, A_n[p_n] \Longrightarrow C_1[q_1], \ldots, C_m[q_m]$ is *monotone at q* if $q_j = q$ for all $1 \leq j \leq m$ and every p_i is a prefix of q, that is, $p_i \preceq q$ for all $1 \leq i \leq m$.

Theorem 6.3 (Completeness of Labeled Deduction) *If $\Gamma \overset{m}{\Longrightarrow} \Delta$ is derivable then for any monotone labeling $\Gamma' \Longrightarrow \Delta'$ of $\Gamma \overset{m}{\Longrightarrow} \Delta$, we have that $\Gamma' \Longrightarrow \Delta'$ is derivable.*

Proof: By induction on the structure of the given derivation. We show a few cases.

Case:

$$\mathcal{D} = \frac{}{\Gamma, P \overset{m}{\Longrightarrow} P, \Delta}\,\mathrm{init}$$

$\Gamma', P[p] \Longrightarrow P[q], \Delta'$ monotone at q	Assumption
$p \preceq q$	By defn. of monotonicity
$\Gamma', P[p] \Longrightarrow P[q], \Delta'$	By rule init

Case:

$$\mathcal{D} = \frac{\begin{matrix}\mathcal{D}_1 \\ \Gamma, A \overset{m}{\Longrightarrow} B\end{matrix}}{\Gamma \overset{m}{\Longrightarrow} A \supset B, \Delta}\,\supset\mathrm{R}$$

$\Gamma' \Longrightarrow (A \supset B)[q], \Delta'$ monotone at q	Assumption
$\Gamma', A[qa] \Longrightarrow B[qa]$ monotone at qa for a new a	By defn. of monotonicity
$\Gamma', A[qa] \Longrightarrow B[qa]$ derivable	By i.h.
$\Gamma' \Longrightarrow (A \supset B)[q]$ derivable	By rule $\supset\mathrm{R}^a$
$\Gamma' \Longrightarrow (A \supset B)[q], \Delta'$ derivable	By weakening

Case:

$$\mathcal{D} = \dfrac{\begin{array}{c}\mathcal{D}_1\\ \Gamma, A \supset B \overset{m}{\Longrightarrow} A, \Delta\end{array} \qquad \begin{array}{c}\mathcal{D}_2\\ \Gamma, B \overset{m}{\Longrightarrow} \Delta\end{array}}{\Gamma, A \supset B \overset{m}{\Longrightarrow} \Delta} \supset\!\mathrm{L}$$

$\Gamma', A \supset B[p] \Longrightarrow \Delta'$ monotone at q	Assumption
$\Gamma', A \supset B[p] \Longrightarrow A[q], \Delta'$ monotone at q	By defn. of monotonicity
$\Gamma', A \supset B[p] \Longrightarrow A[q], \Delta'$ derivable	By i.h.
$\Gamma', B[q] \Longrightarrow \Delta'$ monotone at q	By defn. of monotonicity
$\Gamma', B[q] \Longrightarrow \Delta'$ derivable	By i.h.
$\Gamma', (A \supset B)[p] \Longrightarrow \Delta'$	By rule ⊃L and $p \preceq q$

□

The soundness proof is considerably more difficult. Standard techniques are via so-called Kripke models or by direct translation from matrix proofs to the sequent calculus. On of the problems is that the (unlabeled) proof will generally have to proceed with a different order of the inferences than the labeled proof. The interested reader is refered to Wallen [Wal90], Waaler [Waa01], and Schmitt et al. [KS00, SLKN01].

6.3 First-Order Labeled Deduction

In first-order intuitionistic logic, it is not just the implication that introduces a new scope, but also universal quantification. This means we have to change both the multiple-conclusion sequent calculus and the labeled deduction system. The changes in the multiple-conclusion calculus is quite straightforward; the change to the labeled calculus are more extensive. We show here only the rules, but not any proofs. The reader is refered to the literature cited at the beginning of this chapter for details.

$$\dfrac{\Gamma, \forall x.\, A(x), A(t) \overset{m}{\Longrightarrow} \Delta}{\Gamma, \forall x.\, A(x) \overset{m}{\Longrightarrow} \Delta}\forall\mathrm{L} \qquad \dfrac{\Gamma \overset{m}{\Longrightarrow} A(b)}{\Gamma \overset{m}{\Longrightarrow} \forall x.\, A(x), \Delta}\forall\mathrm{R}^b$$

$$\dfrac{\Gamma, A(b) \overset{m}{\Longrightarrow} \Delta}{\Gamma, \exists x.\, A(x) \overset{m}{\Longrightarrow} \Delta}\exists\mathrm{L}^b \qquad \dfrac{\Gamma \overset{m}{\Longrightarrow} A(t), \exists x.\, A(x), \Delta}{\Gamma \overset{m}{\Longrightarrow} \exists x.\, A(x), \Delta}\exists\mathrm{R}$$

The side condition on $\forall\mathrm{R}^b$ and $\exists\mathrm{L}^b$ is the usual: b must not occur in the conclusion. Note that Δ is erased in the premise of ∀R, and that an extra copy of $\exists x.\, A(x)$ is kept in the ∃R rule.

The fact that universal quantification creates a new scope means that in the labeled deductive systems, terms must now also be labeled. We have a new judgment t *term*$[p]$ which means t *is a well-formed term at* p. We may abbreviate this as $t[p]$. We introduce a new set of assumptions in order to track the labels at which they have been introduced.

$$\text{Labeled Parameter Contexts} \quad \Sigma \quad ::= \quad \cdot \mid \Sigma, a\ \mathit{term}[p]$$

We have two principal judgments.

$$\begin{array}{c} \Sigma; \Gamma \Longrightarrow \Delta \\ \Sigma \vdash t\ \mathit{term}[p] \end{array}$$

The first just adds an explicit parameter context to a sequent, the second test whether terms are well-formed. The latter is defined by the following rules:

$$\frac{a\ \mathit{term}[p] \text{ in } \Sigma}{\Sigma \vdash a\ \mathit{term}[pq]}\,\text{parm} \qquad \frac{\Sigma \vdash t_i\ \mathit{term}[p] \quad \text{for all } 1 \leq i \leq n}{\Sigma \vdash f(t_1, \ldots t_n)\ \mathit{term}[p]}\,\text{func}$$

As propositional assumptions, term assumptions remain valid in future worlds (allowing pq in the parameter rule). In the rules for $\Sigma; \Gamma \Longrightarrow \Delta$, Σ is carried through from conclusion to premises in all rules except those containing quantifiers. The new rules for quantifiers are:

$$\frac{\Sigma \vdash t[pq] \qquad \Sigma; \Gamma, \forall x.\ A(x)[p], A(t)[pq] \Longrightarrow \Delta}{\Sigma; \Gamma, \forall x.\ A(x)[p] \Longrightarrow \Delta}\,\forall\text{L}$$

$$\frac{\Sigma, b[pa]; \Gamma \Longrightarrow A(b)[pa], \Delta}{\Sigma; \Gamma \Longrightarrow \forall x.\ A(x)[p], \Delta}\,\forall\text{R}^{b,a}$$

$$\frac{\Sigma, b[p]; \Gamma, A(b)[p] \Longrightarrow \Delta}{\Sigma; \Gamma, \exists x.\ A(x)[p] \Longrightarrow \Delta}\,\exists\text{L}^{b}$$

$$\frac{\Sigma \vdash t[p] \qquad \Sigma; \Gamma \Longrightarrow A(t)[p], \exists x.\ A(x)[p], \Delta}{\Sigma; \Gamma \Longrightarrow \exists x.\ A(x)[p], \Delta}\,\exists\text{R}$$

6.4 Matrix Methods

The system of labeled deduction, if propositional or first-order, still has non-invertible rules. Specifically, implication and universal quantification on the left are synchronous, as well as existential quantification on right. These propositions may have to wait for a label or term parameter to be introduced before they can be decomposed.

In order to postpone these choices we can introduce free variables, standing both for labels and terms, and employ unification (again, both for labels and terms) for possibly initial sequents. These kinds of algorithms are usually described as so-called *matrix methods*, *connections methods*, or *mating methods*, originally developed for classical logic.

This is a large subject, and we forego a special treatment here. A good introduction, with further pointers to the literature, can be found in Waaler's article [Waa01] in the *Handbook of Automated Reasoning.* Highly recommended is also Wallen's book [Wal90], although it does not fully address some of the more difficult aspects of the implementation such as label unification.

Chapter 7

Equality

Reasoning with equality in first order logic can be accomplished *axiomatically.* That is, we can simply add reflexivity, symmetry, transitivity, and congruence rules for each predicate and function symbol and use the standard theorem proving technology developed in the previous chapters. This approach, however, does not take strong advantage of inherent properties of equality and leads to a very large and inefficent search space.

While there has been a deep investigation of equality reasoning in classical logic, much less is known for intuitionistic logic. Some recent references are [Vor96, DV99].

In this chapter we develop some of the techniques of equational reasoning, starting again from first principles in the definition of logic. We therefore recapitulate some of the material in earlier chapters, now adding equality as a new primitive predicate symbol.

7.1 Natural Deduction

We characterize equality by its introduction rule, which simply states that $s \doteq s$ for any term s.

$$\frac{}{s \doteq s} \doteq \mathrm{I}$$

We have already seen this introduction rule in unification logic in Section 4.4. In the context of unification logic, however, we did not consider hypothetical judgments, so we did not need or specify elimination rules for equality.

If we know $s \doteq t$ we can replace any number of occurrences of s in a true proposition and obtain another true proposition.

$$\frac{s \doteq t \qquad [s/x]A}{[t/x]A} \doteq \mathrm{E}_1$$

Symmetrically, we can also replace occurrences of t by s.

$$\frac{s \doteq t \qquad [t/x]A}{[s/x]A}\doteq \mathrm{E}_2$$

It might seem that this second rule is redundant, and in some sense it is. In particular, it is a *derivable* rule of the calculus with only $\doteq \mathrm{E}_1$:

$$\frac{\dfrac{s \doteq t \qquad \dfrac{}{s \doteq s}\doteq \mathrm{I}}{t \doteq s}\doteq \mathrm{E}_1 \qquad [t/x]A}{[s/x]A}\doteq \mathrm{E}_1$$

However, this deduction is not *normal* (as defined below), and without the second elimination rule the normalization theorem would not hold and cut elimination in the sequent calculus would fail. We continue this discussion below, after introducing normal derivations.

Next, we check the local soundness and completeness of the rules. First, local soundness:

$$\frac{\dfrac{}{s \doteq s}\doteq \mathrm{I} \qquad \begin{matrix}\mathcal{D}\\ [s/x]A\end{matrix}}{\vdash [s/x]A}\doteq \mathrm{E}_1 \qquad \Longrightarrow_R \qquad \begin{matrix}\mathcal{D}\\ [s/x]A\end{matrix}$$

and the reduction for $\doteq \mathrm{E}_2$ is identical.

Second, we have to verify local completeness. There are two symmetric expansions

$$\begin{matrix}\mathcal{D}\\ s \doteq t\end{matrix} \qquad \Longrightarrow_E \qquad \frac{\begin{matrix}\mathcal{D}\\ s \doteq t\end{matrix} \qquad \dfrac{}{s \doteq s}\doteq \mathrm{I}}{s \doteq t}\doteq \mathrm{E}_1$$

and

$$\begin{matrix}\mathcal{D}\\ s \doteq t\end{matrix} \qquad \Longrightarrow_E \qquad \frac{\begin{matrix}\mathcal{D}\\ s \doteq t\end{matrix} \qquad \dfrac{}{t \doteq t}\doteq \mathrm{I}}{s \doteq t}\doteq \mathrm{E}_2$$

witnessing local completeness.

Note that the second is redundant in the sense that for local completeness we only need to show that there is *some* way to apply elimination rules so that we can reconstitute the connective by introduction rules. This is an interesting example where local completeness (in the absence of the $\doteq \mathrm{E}_2$ rule) does not imply global completeness.

Next we define normal and extraction derivations. These properties are given by the inherent role of introduction and elimination rules.

$$\frac{}{s \doteq s \Uparrow}\doteq\mathrm{I}$$

$$\frac{s \doteq t \downarrow \qquad [s/x]A \Uparrow}{[t/x]A \Uparrow}\doteq\mathrm{E}_1 \qquad \frac{s \doteq t \downarrow \qquad [t/x]A \Uparrow}{[s/x]A \Uparrow}\doteq\mathrm{E}_2$$

The elimination rule is similar to the rules for disjunction in the sense that there is a side derivation whose conclusion is copied from the premise to the conclusion of the elimination rule. In the case of disjunction, the copy is identical; here, some copies of s are replaced by t or vice versa.

Now we can see, why the derivation of $\doteq\mathrm{E}_2$ is not normal:

$$\frac{\dfrac{s \doteq t \downarrow \qquad \dfrac{}{s \doteq s \Uparrow}\doteq\mathrm{I}}{t \doteq s ?}\doteq\mathrm{E}_1 \qquad [t/x]A \Uparrow}{[s/x]A \Uparrow}\doteq\mathrm{E}_1$$

The judgment marked with ? should be $t \doteq s \Uparrow$ considering it is the conclusion of an equality elimination inference, and it should be $t \doteq s \downarrow$ considering it is the left premise of an equality elimination. Since no coercion from $\Uparrow$ to $\downarrow$ is available for normal derivations the deduction above cannot be annotated.

We assign proof terms only in their compact form (see Section 3.2). This means we have to analyse how much information is needed in the proof term to allow bi-directional type checking. Recall that we have introduction terms I and elimination terms E and that introduction terms are checked against a given type, while elimination term must carry enough information so that their type is unique. Following these considerations leads to the following new terms.

$$\begin{array}{llll}
\text{Intro Terms} & I & ::= & \ldots \mid \mathrm{refl} & \text{for } \doteq\mathrm{I} \\
\text{Elim Terms} & E & ::= & \ldots \mid \mathrm{subst}_1^{\lambda x.A}\, E\, I & \text{for } \doteq\mathrm{E}_1 \\
 & & & \mid \mathrm{subst}_2^{\lambda x.A}\, E\, I & \text{for } \doteq\mathrm{E}_2
\end{array}$$

The typing rules are straightforward. Recall that we localize the hypothesize to make the rules more explicit.

$$\frac{}{\Gamma^{\downarrow} \vdash \mathrm{refl} : s \doteq s \Uparrow}\doteq\mathrm{I}$$

$$\frac{\Gamma^{\downarrow} \vdash E : s \doteq t \downarrow \qquad \Gamma^{\downarrow} \vdash I : [s/x]A \Uparrow}{\Gamma^{\downarrow} \vdash \mathrm{subst}_1^{\lambda x.A}\, E\, I : [t/x]A \Uparrow}\doteq\mathrm{E}_1$$

$$\frac{\Gamma^{\downarrow} \vdash E : s \doteq t \downarrow \qquad \Gamma^{\downarrow} \vdash I : [t/x]A \Uparrow}{\Gamma^{\downarrow} \vdash \mathrm{subst}_2^{\lambda x.A}\, E\, I : [s/x]A \Uparrow}\doteq\mathrm{E}_2$$

We record the proposition A and an indication of the bound variable x in order to provide enough information for bi-direction type checking. Recall the desired property (Theorem 3.4):

1. *Given $\Gamma^{\downarrow}$, I, and A. Then either $\Gamma^{\downarrow} \vdash I : A \Uparrow$ or not.*
2. *Given $\Gamma^{\downarrow}$ and E. Then either there is a unique A such that $\Gamma^{\downarrow} \vdash E : A \downarrow$ or there is no such A.*

First, it is clear that the constant refl for equality introduction does not need to carry any terms, since $s \doteq s$ is given.

Second, to check $\mathrm{subst}_1^{\lambda x.A}\, E\, I$ against A' we first synthesize the type of E obtaining $s \doteq t$ and thereby s and t. Knowing t and A' does not determine A (consider, for example, $[t/x]A = q(t,t)$ which allows $A = q(x,x)$, $A = q(x,t)$, $A = q(t,x)$ and $A = q(t,t)$). However, A is recorded explicitly in the proof term, together with the variable x. Therefore we can now check whether the given type $[t/x]A$ is equal to A'. If that succeeds we have to check the introduction term I against $[s/x]A$ to verify the correctness of the whole term.

7.2 Sequent Calculus

The rules for the sequent calculus are determined by the definition of normal deduction as in Chapter 3. Introduction rules are turned into right rules; elimination rules into left rules.

$$\frac{}{\Gamma \Longrightarrow s \doteq s} \doteq\mathrm{R}$$

$$\frac{\Gamma, s \doteq t \Longrightarrow [s/x]A}{\Gamma, s \doteq t \Longrightarrow [t/x]A} \doteq\mathrm{L}_1 \qquad \frac{\Gamma, s \doteq t \Longrightarrow [t/x]A}{\Gamma, s \doteq t \Longrightarrow [s/x]A} \doteq\mathrm{L}_2$$

The proof for admissibility of cut in this calculus runs into difficulties when the cut formula was changed in the application of the $\doteq\mathrm{L}_1$ or $\doteq\mathrm{L}_2$ rules. Consider, for example, the cut between

$$\mathcal{D} = \frac{\begin{matrix}\mathcal{D}_1\\ \Gamma, s \doteq t \Longrightarrow [s/x]A\end{matrix}}{\Gamma, s \doteq t \Longrightarrow [t/x]A} \doteq\mathrm{L}_1 \qquad \text{and} \qquad \begin{matrix}\mathcal{E}\\ \Gamma, s \doteq t, [t/x]A \Longrightarrow C\end{matrix}$$

If $[t/x]A$ is the principal formula of the last inference in $\mathcal{E}$, we would normally apply the induction hypothesis to $\mathcal{D}_1$ and $\mathcal{E}$, in effect pushing the cut past the last inference in $\mathcal{D}$. We cannot do this here, since $[s/x]A$ and $[t/x]A$ do not match. None of the rules in the sequent calculus without equality changed the conclusion in a left rule, so this situation did not arise before.

The simplest remedy seems to be to restrict the equality rules so they must be applied last in the bottom-up construction of a proof, and only to atomic formulas or other equalities. In this way, they cannot interfere with other inferences—they have been pushed up to the leaves of the derivation. This restriction is interesting for other purposes as well, since it allows us to separate equality reasoning from logical reasoning during the proof search process.

We introduce one new syntactice category and two new judgments. E stands for a *basic proposition*, which is either an atomic proposition P or an equation $s \doteq t$.

$$\begin{array}{ll} \Gamma \xRightarrow{\text{E}} E & E \text{ has an equational derivation from } \Gamma \\ \Gamma \xRightarrow{\text{R}} A & A \text{ has a regular derivation from } \Gamma \end{array}$$

Equational derivations are defined as follows.

$$\frac{}{\Gamma, P \xRightarrow{\text{E}} P}\,\text{init} \qquad \frac{}{\Gamma \xRightarrow{\text{E}} s \doteq s}\,\doteq\text{R}$$

$$\frac{\Gamma, s \doteq t \xRightarrow{\text{E}} [s/x]E}{\Gamma, s \doteq t \xRightarrow{\text{E}} [t/x]E}\,\doteq\text{L}_1 \qquad \frac{\Gamma, s \doteq t \xRightarrow{\text{E}} [s/x]E}{\Gamma, s \doteq t \xRightarrow{\text{E}} [t/x]E}\,\doteq\text{L}_1$$

Regular derivations have all the inference rules of sequent derivations without equality (except for initial sequents) plus the following coercion.

$$\frac{\Gamma \xRightarrow{\text{E}} E}{\Gamma \xRightarrow{\text{R}} E}\,\text{eq}$$

Regular derivations are sound and complete with respect to the unrestricted calculus. Soundness is direct.

Theorem 7.1 (Soudness of Regular Derivations)

1. *If* $\Gamma \xRightarrow{\text{E}} E$ *then* $\Gamma \Longrightarrow E$
2. *If* $\Gamma \xRightarrow{\text{R}} A$ *then* $\Gamma \Longrightarrow A$

Proof: By straightforward induction over the given derivations. □

In order to prove completeness we need a lemma which states that the unrestricted left equality rules are admissible in the restricted calculus. Because new assumptions are made, the statment of the lemma must actually be slightly more general by allowing substitution into hypotheses.

Lemma 7.2 (Admissibility of Generalized Equality Rules)

1. *If* $[s/x]\Gamma, s \doteq t \xRightarrow{\text{R}} [s/x]A$ *then* $[t/x]\Gamma, s \doteq t \xRightarrow{\text{R}} [t/x]A$.
2. *If* $[t/x]\Gamma, s \doteq t \xRightarrow{\text{R}} [t/x]A$ *then* $[s/x]\Gamma, s \doteq t \xRightarrow{\text{R}} [s/x]A$.
3. *If* $[s/x]\Gamma, s \doteq t \xRightarrow{\text{E}} [s/x]A$ *then* $[t/x]\Gamma, s \doteq t \xRightarrow{\text{E}} [t/x]A$.
4. *If* $[s/x]\Gamma, s \doteq t \xRightarrow{\text{E}} [s/x]A$ *then* $[t/x]\Gamma, s \doteq t \xRightarrow{\text{E}} [t/x]A$.

Proof: By induction on the structure of the given derivations $\mathcal{S}$ or $\mathcal{E}$, where the second and fourth parts are completely symmetric to the first and third part. In most cases this follows directly from the induction hypothesis. We show a few characteristic cases.

Case:

$$\mathcal{S} = \dfrac{\begin{array}{c}\mathcal{S}_1 \\ [s/x]\Gamma, s \doteq t, [s/x]A_1 \overset{\text{R}}{\Longrightarrow} [s/x]A_2\end{array}}{[s/x]\Gamma, s \doteq t \overset{\text{R}}{\Longrightarrow} [s/x]A_1 \supset [s/x]A_2} \supset\!\text{R}$$

$[t/x]\Gamma, s \doteq t, [t/x]A_1 \overset{\text{R}}{\Longrightarrow} [t/x]A_2$ By i.h. on $\mathcal{S}_1$

$[t/x]\Gamma, s \doteq t \overset{\text{R}}{\Longrightarrow} [t/x]A_1 \supset [t/x]A_2$ By rule $\supset$R

Case:

$$\mathcal{S} = \dfrac{\begin{array}{c}\mathcal{E} \\ [s/x]\Gamma, s \doteq t \overset{\text{E}}{\Longrightarrow} [s/x]E\end{array}}{[s/x]\Gamma, s \doteq t \overset{\text{R}}{\Longrightarrow} [s/x]E} \text{eq}$$

$[t/x]\Gamma, s \doteq t \overset{\text{E}}{\Longrightarrow} [t/x]E$ By i.h. (3) on $\mathcal{E}$

$[t/x]\Gamma, s \doteq t \overset{\text{R}}{\Longrightarrow} [t/x]E$ By rule eq

Case:

$$\mathcal{E} = \dfrac{}{[s/x]\Gamma', [s/x]P_1, s \doteq t \overset{\text{E}}{\Longrightarrow} [s/x]P_2} \text{init}$$

We obtain the first equation below from the assumption that $\mathcal{E}$ is an initial sequent.

$[s/x]P_1 = [s/x]P_2$ Given

$[t/x]\Gamma', [t/x]P_1, s \doteq t \overset{\text{E}}{\Longrightarrow} [t/x]P_1$ By rule init

$[t/x]\Gamma', [t/x]P_1, s \doteq t \overset{\text{E}}{\Longrightarrow} [s/x]P_1$ By rule $\doteq$L$_2$

$[t/x]\Gamma', [t/x]P_1, s \doteq t \overset{\text{E}}{\Longrightarrow} [s/x]P_2$ Same, by given equality

$[t/x]\Gamma', [t/x]P_1, s \doteq t \overset{\text{E}}{\Longrightarrow} [t/x]P_2$ By rule $\doteq$L$_1$

Case:

$$\mathcal{E} = \dfrac{\begin{array}{c}\mathcal{E}' \\ [s/x]\Gamma', [s/x]q \doteq [s/x]r, s \doteq t \overset{\text{E}}{\Longrightarrow} [[s/x]q/y]E'\end{array}}{[s/x]\Gamma', [s/x]q \doteq [s/x]r, s \doteq t \overset{\text{E}}{\Longrightarrow} [s/x]E} \doteq\text{L}_1$$

Note that we wrote the premise so that E' does contain an occurrence of x. We obtain the first equation below from the form of the inference rule $\doteq$L$_1$.

$$\begin{array}{lr}
[s/x]E = [[s/x]r/y]E' & \text{Given} \\
[s/x]\Gamma', [s/x]q \doteq [s/x]r, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} [s/x][q/y]E' & \text{Same as } \mathcal{E}' \text{ (} x \text{ not in } E'\text{)} \\
[t/x]\Gamma', [t/x]q \doteq [t/x]r, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} [t/x][q/y]E' & \text{By i.h. on } \mathcal{E}' \\
[t/x]\Gamma', [t/x]q \doteq [t/x]r, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} [[t/x]q/y]E' & \text{Same, since } x \text{ not in } E' \\
[t/x]\Gamma', [t/x]q \doteq [t/x]r, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} [[t/x]r/y]E' & \text{By rule } \doteq \mathrm{L}_1 \\
[t/x]\Gamma', [t/x]q \doteq [t/x]r, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} [t/x][r/y]E' & \text{Same, since } x \text{ not in } E' \\
[t/x]\Gamma', [t/x]q \doteq [t/x]r, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} [s/x][r/y]E' & \text{By rule } \doteq \mathrm{L}_2 \\
[t/x]\Gamma', [t/x]q \doteq [t/x]r, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} [[s/x]r/y]E' & \text{Same, since } x \text{ not in } E' \\
[t/x]\Gamma', [t/x]q \doteq [t/x]r, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} [s/x]E & \text{Same, by given equality} \\
[t/x]\Gamma', [t/x]q \doteq [t/x]r, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} [t/x]E & \text{By rule } \doteq \mathrm{L}_1
\end{array}$$

Case:

$$\mathcal{E} = \dfrac{\begin{array}{c}\mathcal{E}' \\ [s/x]\Gamma, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} [s/x]E'\end{array}}{[s/x]\Gamma, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} [s/x]E} \doteq \mathrm{L}_1$$

Note that we wrote the premise so that E' does contain an occurrence of x. We obtain the first line below from the shape of the conclusion in the inference rule $\doteq \mathrm{L}_1$ with the principal formula $s \doteq t$.

$$\begin{array}{lr}
[s/x]E = [t/x]E' & \text{Given} \\
[t/x]\Gamma, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} [t/x]E' & \text{By i.h. on } \mathcal{E}' \\
[t/x]\Gamma, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} [s/x]E & \text{Same, by given equality} \\
[t/x]\Gamma, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} [t/x]E & \text{By rule } \doteq \mathrm{L}_1
\end{array}$$

□

A second lemma is helpful to streamline the completeness proof.

Lemma 7.3 (Atomic Initial Sequents) $\Gamma, A \overset{\mathrm{R}}{\Longrightarrow} A$.

Proof: By induction on the structure of A. This is related to repeated local expansion. We show a few of cases.

Case: $A = P$.

$$\begin{array}{lr}
\Gamma, P \overset{\mathrm{E}}{\Longrightarrow} P & \text{By rule init} \\
\Gamma, P \overset{\mathrm{R}}{\Longrightarrow} P & \text{By rule eq}
\end{array}$$

Case: $A = (s \doteq t)$.

$$\begin{array}{lr}
\Gamma, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} s \doteq s & \text{By rule } \doteq \mathrm{R} \\
\Gamma, s \doteq t \overset{\mathrm{E}}{\Longrightarrow} s \doteq t & \text{By rule } \doteq \mathrm{L}_1
\end{array}$$

Case: $A = A_1 \wedge A_2$.

$\Gamma, A_1 \overset{\mathrm{R}}{\Longrightarrow} A_1$ By i.h. on A_1

$\Gamma, A_1 \wedge A_2 \overset{\mathrm{R}}{\Longrightarrow} A_1$ By rule $\wedge\mathrm{L}_1$

$\Gamma, A_2 \overset{\mathrm{R}}{\Longrightarrow} A_2$ By i.h. on A_2

$\Gamma, A_1 \wedge A_2 \overset{\mathrm{R}}{\Longrightarrow} A_2$ By rule $\wedge\mathrm{L}_2$

$\Gamma, A_1 \wedge A_2 \overset{\mathrm{R}}{\Longrightarrow} A_1 \wedge A_2$ By rule $\wedge\mathrm{R}$

□

With these two lemmas, completeness is relatively simple.

Theorem 7.4 (Completeness of Regular Derivations)
If $\Gamma \Longrightarrow A$ *then* $\Gamma \overset{\mathrm{R}}{\Longrightarrow} A$.

Proof: By induction on the structure of the given derivation $\mathcal{S}$. We show some cases; most are straightforward.

Case:

$$\mathcal{S} = \dfrac{\begin{array}{c}\mathcal{S}_2\\ \Gamma, A_1 \Longrightarrow A_2\end{array}}{\Gamma \Longrightarrow A_1 \supset A_2}\supset\mathrm{R}$$

$\Gamma, A_1 \overset{\mathrm{R}}{\Longrightarrow} A_2$ By i.h. on $\mathcal{S}_2$

$\Gamma \overset{\mathrm{R}}{\Longrightarrow} A_1 \supset A_2$ By rule $\supset\mathrm{R}$

Case:

$$\mathcal{S} = \dfrac{}{\Gamma', A \Longrightarrow A}\mathrm{init}$$

$\Gamma', A \overset{\mathrm{R}}{\Longrightarrow} A$ By Lemma 7.3

Case:

$$\mathcal{S} = \dfrac{\begin{array}{c}\mathcal{S}_1\\ \Gamma', s \doteq t \Longrightarrow [s/x]A\end{array}}{\Gamma', s \doteq t \Longrightarrow [t/x]A}\doteq\mathrm{L}_1$$

$\Gamma', s \doteq t \overset{\mathrm{R}}{\Longrightarrow} [s/x]A$ By i.h. on $\mathcal{S}_1$

$\Gamma', s \doteq t \overset{\mathrm{R}}{\Longrightarrow} [t/x]A$ By Lemma 7.2

□

Regular derivations are the basis for proof search procedures. Furthermore, we can prove admissibility of cut, essentially following the same argument as in the system without equality for regular derivations. On equality derivations, we have to employ a new argument.

Theorem 7.5 (Admissibility of Cut with Equality)

1. *If* $\Gamma \overset{\mathrm{E}}{\Longrightarrow} E$ *and* $\Gamma, E \overset{\mathrm{E}}{\Longrightarrow} F$ *then* $\Gamma \overset{\mathrm{E}}{\Longrightarrow} F$.
2. *If* $\Gamma \overset{\mathrm{E}}{\Longrightarrow} E$ *and* $\Gamma, E \overset{\mathrm{R}}{\Longrightarrow} C$ *then* $\Gamma \overset{\mathrm{R}}{\Longrightarrow} C$.
3. *If* $\Gamma \overset{\mathrm{R}}{\Longrightarrow} A$ *and* $\Gamma, A \overset{\mathrm{E}}{\Longrightarrow} F$ *then* $\Gamma \overset{\mathrm{R}}{\Longrightarrow} F$.
4. *If* $\Gamma \overset{\mathrm{R}}{\Longrightarrow} A$ *and* $\Gamma, A \overset{\mathrm{R}}{\Longrightarrow} C$ *then* $\Gamma \overset{\mathrm{R}}{\Longrightarrow} C$.

Proof: We prove the properties in sequence, using earlier ones to in the proofs of later ones.

Part (1): Given

$$\begin{array}{c}\mathcal{E}\\ \Gamma \overset{\mathrm{E}}{\Longrightarrow} E\end{array} \qquad \text{and} \qquad \begin{array}{c}\mathcal{F}\\ \Gamma, E \overset{\mathrm{E}}{\Longrightarrow} F\end{array}$$

we construct a derivation for $\Gamma \overset{\mathrm{E}}{\Longrightarrow} F$ by nested induction on the structure of $\mathcal{E}$ and $\mathcal{F}$. That is, in appeals to the induction hypothesis, $\mathcal{E}$ may be smaller (in which case $\mathcal{F}$ may be arbitrary), or $\mathcal{E}$ stays the same and $\mathcal{F}$ gets smaller.

Cases: If E is a side formula of the last inference in $\mathcal{F}$ we appeal to the induction hypothesis on the premise and reapply the inference on the result. If $\mathcal{F}$ is an initial sequent we can directly construct the desired derivation. In the remaining cases, we assume E is the principal formula of the last inference in $\mathcal{F}$.

Case:

$$\mathcal{E} = \frac{}{\Gamma \overset{\mathrm{E}}{\Longrightarrow} s \doteq s}\,{\doteq}\mathrm{R} \qquad \text{and} \qquad \mathcal{F} = \frac{\begin{array}{c}\mathcal{F}_1\\ \Gamma, s \doteq s \overset{\mathrm{E}}{\Longrightarrow} [s/x]F_1\end{array}}{\Gamma, s \doteq s \overset{\mathrm{E}}{\Longrightarrow} [s/x]F_1}\,{\doteq}\mathrm{L}_1$$

$\Gamma \Longrightarrow [s/x]F_1$ By i.h. on $\mathcal{E}$ and $\mathcal{F}_1$

Case:

$$\mathcal{E} = \frac{\begin{array}{c}\mathcal{E}_1\\ \Gamma', q \doteq r \overset{\mathrm{E}}{\Longrightarrow} [q/x]s' = [q/x]t'\end{array}}{\Gamma', q \doteq r \overset{\mathrm{E}}{\Longrightarrow} [r/x]s' \doteq [r/x]t'}\,{\doteq}\mathrm{L}_1$$

$\Gamma', q \doteq r, [r/x]s' \doteq [r/x]t' \overset{\mathrm{E}}{\Longrightarrow} F$ $\mathcal{F}$, in this case

$\Gamma', q \doteq r, [q/x]s' \doteq [q/x]t' \overset{\mathrm{E}}{\Longrightarrow} F$ By Lemma 7.2

$\Gamma', q \doteq r \overset{\mathrm{E}}{\Longrightarrow} F$ By i.h. on $\mathcal{E}_1$ and above

Part (2): Given

$$\begin{array}{c}\mathcal{E}\\ \Gamma \overset{\mathrm{E}}{\Longrightarrow} E\end{array} \qquad \text{and} \qquad \begin{array}{c}\mathcal{S}\\ \Gamma, E \overset{\mathrm{R}}{\Longrightarrow} C\end{array}$$

we construct a derivation for $\Gamma \overset{\mathrm{R}}{\Longrightarrow} C$ by induction over the structure of $\mathcal{S}$. Since E is either atomic or an equality, it cannot be the principal formula of an inference in $\mathcal{S}$. When we reach a coercion from $\overset{\mathrm{E}}{\Longrightarrow}$ to $\overset{\mathrm{R}}{\Longrightarrow}$ in $\mathcal{S}$ we appeal to Part (1).

Part (3): Given

$$\begin{array}{c}\mathcal{S}\\ \Gamma \overset{\mathrm{R}}{\Longrightarrow} A\end{array} \qquad \text{and} \qquad \begin{array}{c}\mathcal{F}\\ \Gamma, A \overset{\mathrm{E}}{\Longrightarrow} F\end{array}$$

we construct a derivation for $\Gamma \overset{\mathrm{E}}{\Longrightarrow} F$ by nested induction on the structure of $\mathcal{F}$ and $\mathcal{S}$. If A is the principal formula of an inference in $\mathcal{F}$ then A must be atomic or an equality. In the former case we can derive the desired conclusion directly; in the latter case we proceed by induction over $\mathcal{S}$. Since A is an equality, it cannot be the principal formula of an inference in $\mathcal{S}$. When we reach a coercion for $\overset{\mathrm{E}}{\Longrightarrow}$ to $\overset{\mathrm{R}}{\Longrightarrow}$ in $\mathcal{S}$ we appeal to Part (1).

Part (4): Given

$$\begin{array}{c}\mathcal{S}\\ \Gamma \overset{\mathrm{R}}{\Longrightarrow} A\end{array} \qquad \text{and} \qquad \begin{array}{c}\mathcal{T}\\ \Gamma, A \overset{\mathrm{R}}{\Longrightarrow} C\end{array}$$

we construct a derivation for $\Gamma \overset{\mathrm{R}}{\Longrightarrow} C$ by nested induction on the structure of A, and the derivations $\mathcal{S}$ and $\mathcal{T}$ as in the proof of admissibility of cut without equality (Theorem 3.11). When we reach coercions from equality derivations we appeal to Parts 3 or 2. □

Bibliography

[And92] Jean-Marc Andreoli. Logic programming with focusing proofs in linear logic. *Journal of Logic and Computation*, 2(3):197–347, 1992.

[Byr99] John Byrnes. *Proof Search and Normal Forms in Natural Deduction*. PhD thesis, Department of Philosophy, Carnegie Mellon University, May 1999.

[Cur30] H.B. Curry. Grundlagen der kombinatorischen Logik. *American Journal of Mathematics*, 52:509–536, 789–834, 1930.

[DV99] Anatoli Degtyarev and Andrei Voronkov. Equality reasoning in sequent-based calculi. In Alan Robinson and Andrei Voronkov, editors, *Handbook of Automated Reasoning*. Elsevier Science Publishers, 1999. In preparation.

[Fit83] Melvin Fitting. *Proof Methods for Modal and Intuitionistic Logics*. D.Reidel Publishing Co., Dordrecht, 1983.

[Gen35] Gerhard Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210, 405–431, 1935. Translated under the title *Investigations into Logical Deductions* in [Sza69].

[Her30] Jacques Herbrand. Recherches sur la théorie de la démonstration. *Travaux de la Société des Sciences et de Lettres de Varsovic*, 33, 1930.

[Her95] Hugo Herbelin. *Séquents qu'on calcule*. PhD thesis, Universite Paris 7, January 1995.

[Hil22] David Hilbert. Neubegründung der Mathematik (erste Mitteilung). In *Abhandlungen aus dem mathematischen Seminar der Hamburgischen Universität*, pages 157–177, 1922. Reprinted in [Hil35].

[Hil35] David Hilbert. *Gesammelte Abhandlungen*, volume 3. Springer-Verlag, Berlin, 1935.

[How69] W. A. Howard. The formulae-as-types notion of construction. Unpublished manuscript, 1969. Reprinted in To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism, 1980.

[How98] Jacob M. Howe. *Proof Search Issues in Some Non-Classical Logics*. PhD thesis, University of St. Andrews, Scotland, 1998.

[Hua94] Xiarong Huang. *Human Oriented Proof Presentation: A Reconstructive Approach*. PhD thesis, Universität des Saarlandes, Saarbrücken, Germany, 1994. Published by infix, St. Augustin, Germany, Dissertationen zur Künstlichen Intelligenz, Volume 112, 1996.

[Hue76] Gérard Huet. *Résolution d'équations dans des langages d'ordre* $1, 2, \ldots, \omega$. PhD thesis, Université Paris VII, September 1976.

[Kle52] Stephen Cole Kleene. *Introduction to Metamathematics*. North-Holland, 1952.

[Kni89] Kevin Knight. Unification: A multi-disciplinary survey. *ACM Computing Surveys*, 2(1):93–124, March 1989.

[KS00] Christoph Kreitz and Stephan Schmitt. A uniform procedure for converting matrix proofs into sequent-style systems. *Information and Computation*, 162(1–2):226–254, 2000.

[LS86] Joachim Lambek and Philip J. Scott. *Introduction to Higher Order Categorical Logic*. Cambridge University Press, Cambridge, England, 1986.

[Mas64] S. Maslov. The inverse method of establishing deducibility in the classical predicate calculus. *Soviet Mathematical Doklady*, 5:1420–1424, 1964.

[Min94] G. Mints. Resolution strategies for the intuitionistic logic. In *Constraint Programming*, pages 289–311. NATO ASI Series F, Springer-Verlag, 1994.

[ML85a] Per Martin-Löf. On the meanings of the logical constants and the justifications of the logical laws. Technical Report 2, Scuola di Specializzazione in Logica Matematica, Dipartimento di Matematica, Università di Siena, 1985.

[ML85b] Per Martin-Löf. Truth of a proposition, evidence of a judgement, validity of a proof. Notes to a talk given at the workshop *Theory of Meaning*, Centro Fiorentino di Storia e Filosofia della Scienza, June 1985.

[ML94] Per Martin-Löf. Analytic and synthetic judgements in type theory. In Paolo Parrini, editor, *Kant and Contemporary Epistemology*, pages 87–99. Kluwer Academic Publishers, 1994.

[MM76] Alberto Martelli and Ugo Montanari. Unification in linear time and space: A structured presentation. Internal Report B76-16, Istituto di Elaborazione delle Informazione, Consiglio Nazionale delle Ricerche, Pisa, Italy, July 1976.

[MM82] Alberto Martelli and Ugo Montanari. An efficient unification algorithm. *ACM Transactions on Programming Languages and Systems*, 4(2):258–282, April 1982.

[Par92] Michel Parigot. $\lambda\mu$-calculus: An algorithmic interpretation of classical natural deduction. In A. Voronkov, editor, *Proceedings of the International Conference on Logic Programming and Automated Reasoning*, pages 190–201, St. Petersburg, Russia, July 1992. Springer-Verlag LNCS 624.

[Pfe95] Frank Pfenning. Structural cut elimination. In D. Kozen, editor, *Proceedings of the Tenth Annual Symposium on Logic in Computer Science*, pages 156–166, San Diego, California, June 1995. IEEE Computer Society Press.

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

[PW78] M. S. Paterson and M. N. Wegman. Linear unification. *Journal of Computer and System Sciences*, 16(2):158–167, April 1978.

[Rob65] J. A. Robinson. A machine-oriented logic based on the resolution principle. *Journal of the ACM*, 12(1):23–41, January 1965.

[Rob71] J. A. Robinson. Computational logic: The unification computation. *Machine Intelligence*, 6:63–72, 1971.

[SLKN01] Stephan Schmitt, Lori Lorigo, Christoph Kreitz, and Alexey Nogin. Jprover: Integrating connection-based theorem proving into interactive proof assistants. In R.Goré, A.Leitsch, and T.Nipkow, editors, *Proceedings of the International Joint Conference on Automated Reasoning (IJCAR'01)*, pages 421–426, Siena, Italy, June 2001. Springer Verlag LNAI 2083.

[Sza69] M. E. Szabo, editor. *The Collected Papers of Gerhard Gentzen.* North-Holland Publishing Co., Amsterdam, 1969.

[Tam96] T. Tammet. A resolution theorem prover for intuitionistic logic. In M. McRobbie and J. Slaney, editors, *Proceedings of the 13th International Conference on Automated Deduction (CADE-13)*, pages 2–16, New Brunswick, New Jersey, 1996. Springer-Verlag LNCS 1104.

[Tam97] T. Tammet. Resolution, inverse method and the sequent calculus. In A. Leitsch G. Gottlog and D. Mundici, editors, *Proceedings of the 5th Kurt Gödel Colloquium on Computational Logic and Proof Theory (KGC'97)*, pages 65–83, Vienna, Austria, 1997. Springer-Verlag LNCS 1289.

[Vor92] Andrei Voronkov. Theorem proving in non-standard logics based on the inverse method. In D. Kapur, editor, *Proceedings of the 11th International Conference on Automated Deduction*, pages 648–662, Saratoga Springs, New York, 1992. Springer-Verlag LNCS 607.

[Vor96] Andrei Voronkov. Proof-search in intuitionistic logic with equality, or back to simultaneous rigid e-unification. In M.A. McRobbie and J.K. Slaney, editors, *Proceedings of the 13th International Conference on Automated Deduction*, pages 32–46, New Brunswick, New Jersey, July/August 1996. Springer-Verlag LNAI 1104.

[Waa01] Arild Waaler. Connections in nonclassical logics. In Alan Robinson and Andrei Voronkov, editors, *Handbook of Automated Reasoning*, volume 2, chapter 22, pages 1487–1578. Elsevier Science and MIT Press, 2001.

[Wal90] Lincoln A. Wallen. *Automated Deduction in Non-Classical Logics*. MIT Press, 1990.