Chapter 7

Equality

Reasoning with equality in first order logic can be accomplished axiometrically. 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 inefficient 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 $s \equiv s$ for any term $s$.

\[
\frac{}{s \equiv s} \equiv 1
\]

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 $s \equiv t$ we can replace any number of occurrences of $s$ in a true proposition and obtain another true proposition.

\[
\frac{s \equiv t \quad [s/x]A}{[t/x]A} \equiv E_1
\]
Symmetrically, we can also replace occurrences of \( t \) by \( s \).

\[
\frac{s \triangleq t}{[t/x]A \triangleq E_2}
\]

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 \( \triangleq E_1 \):

\[
\begin{align*}
& s \triangleq t & & \triangleq I \\
& s \triangleq s & & \triangleq E_1 \\
\hline
& t \triangleq s & & [t/x]A \\
& [s/x]A & & \triangleq E_1
\end{align*}
\]

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:

\[
\begin{align*}
& s \triangleq s & & \triangleq I \\
& \frac{s \triangleq t}{[s/x]A} & & \triangleq E_1 \\
\hline
& \vdash [s/x]A & & \Rightarrow_R \\
& \frac{[s/x]A \triangleq E_1}{[s/x]A}
\end{align*}
\]

and the reduction for \( \Rightarrow E_2 \) is identical.

Second, we have to verify local completeness. There are two symmetric expansions

\[
\begin{align*}
& \frac{\frac{D}{s \triangleq t}}{\Rightarrow E} \\
& \frac{D}{s \triangleq t} \\
& \frac{D}{s \triangleq t} \\
& \frac{\frac{D}{s \triangleq t}}{\Rightarrow E} \\
& \frac{D}{s \triangleq t} \\
& \frac{\frac{D}{s \triangleq t}}{\Rightarrow E} \\
& \frac{D}{s \triangleq t}
\end{align*}
\]

and

\[
\begin{align*}
& \frac{s \triangleq t}{} \\
& \frac{t \triangleq t}{} \\
& \frac{t \triangleq t}{} \\
\end{align*}
\]

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 \( \Rightarrow E_2 \) rule) does not imply global completeness.
7.1 Natural Deduction

Next we define normal and extraction derivations. These properties are given by the inherent role of introduction and elimination rules.

\[
\begin{align*}
  \frac{s \Downarrow s \uparrow}{s \Downarrow} \triangleq I \\
  \frac{s \Downarrow t \Downarrow \left[ s/x \right] A \uparrow}{\left[ t/x \right] A \uparrow} \triangleq E_1 \\
  \frac{s \Downarrow t \Downarrow \left[ t/x \right] A \uparrow}{\left[ s/x \right] A \uparrow} \triangleq E_2
\end{align*}
\]

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 \( s \Downarrow t \Downarrow \left[ s/x \right] A \uparrow \) is not normal:

\[
\begin{align*}
  \frac{s \Downarrow t \Downarrow}{s \Downarrow s \uparrow} \triangleq I \\
  \frac{s \Downarrow t \Downarrow \left[ t/x \right] A \uparrow}{t \Downarrow s? \ \left[ s/x \right] A \uparrow} \triangleq E_1
\end{align*}
\]

The judgment marked with ? should be \( t \Downarrow s \uparrow \) considering it is the conclusion of an equality elimination inference, and it should be \( t \Downarrow s \Downarrow \) 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.

**Intro Terms**  
\[
I ::= \ldots \mid \text{refl} \quad \text{for } \Downarrow I
\]

**Elim Terms**  
\[
E ::= \ldots \mid \text{subst}_{1}^{\lambda x.A} E I \quad \text{for } \Downarrow E_1 \mid \text{subst}_{2}^{\lambda x.A} E I \quad \text{for } \Downarrow E_2
\]

The typing rules are straightforward. Recall that we localize the hypothesize to make the rules more explicit.

\[
\begin{align*}
  \Gamma \vdash \text{refl} : s \Downarrow s \uparrow \Downarrow I \\
  \Gamma \vdash E : s \Downarrow t \Downarrow \quad \Gamma \vdash \left[ s/x \right] A \uparrow \\
  \Gamma \vdash \text{subst}_{1}^{\lambda x.A} E I : \left[ t/x \right] A \uparrow \Downarrow E_1 \\
  \Gamma \vdash E : s \Downarrow t \Downarrow \quad \Gamma \vdash \left[ t/x \right] A \uparrow \\
  \Gamma \vdash \text{subst}_{2}^{\lambda x.A} E I : \left[ s/x \right] A \uparrow \Downarrow E_2
\end{align*}
\]
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 $\Gamma \vdash I : A$ 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):

2. Given $\Gamma \vdash E : A$ or not.

First, it is clear that the constant refl for equality introduction does not need to carry any terms, since $s = s$ is given.

Second, to check $\text{subst} \lambda x.A \Gamma \vdash I$ against $A'$ we first synthesize the type of $E$ obtaining $s = t$ 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.

\[
\frac {\Gamma \rightarrow s \vdash s \rightarrow} {\text{R}}
\]

\[
\frac {\Gamma, s \vdash t \rightarrow [s/x]A \text{ \ and } \Gamma, s \vdash t \rightarrow [t/x]A \text{ \ and } \Gamma, s \vdash t \rightarrow [s/x]A \text{ \ and } \Gamma, s \vdash t \rightarrow [s/x]A} {\text{L}_1}
\]

The proof for admissibility of cut in this calculus runs into difficulties when the cut formula was changed in the application of the $\vdash \text{L}_1$ or $\vdash \text{L}_2$ rules. Consider, for example, the cut between

\[
\begin{align*}
\frac {\frac {\gamma, s \vdash t \rightarrow [s/x]A \text{ \ and } \gamma, s \vdash t \rightarrow [t/x]A \text{ \ and } \gamma, s \vdash t \rightarrow [s/x]A \rightarrow C} {\text{E}}}
\end{align*}
\]

If $[t/x]A$ is the principal formula of the last inference in $E$, we would normally apply the induction hypothesis to $D_1$ and $E$, in effect pushing the cut past the last inference in $D$. 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 syntactic category and two new judgments. $E$ stands for a basic proposition, which is either an atomic proposition $P$ or an equation $s \equiv t$.

\[
\Gamma \vdash E \quad E \text{ has an equational derivation from } \Gamma \\
\Gamma \Rightarrow A \quad A \text{ has a regular derivation from } \Gamma
\]

Equational derivations are defined as follows.

\[
\begin{align*}
\text{init} & : \Gamma, P \vdash E \Rightarrow P \\
\text{R} & : \Gamma, s \equiv t \Rightarrow [s/x]E \\
\text{L}_1 & : \Gamma, s \equiv t \Rightarrow [t/x]E
\end{align*}
\]

Regular derivations have all the inference rules of sequent derivations without equality (except for initial sequents) plus the following coercion.

\[
\begin{align*}
\text{eq} : \Gamma \Rightarrow E & \Rightarrow E \\
\text{R} : \Gamma \Rightarrow E & \Rightarrow E
\end{align*}
\]

Regular derivations are sound and complete with respect to the unrestricted calculus. Soundness is direct.

**Theorem 7.1 (Soundness of Regular Derivations)**

1. If $\Gamma \Rightarrow E$ then $\Gamma \Rightarrow E$
2. If $\Gamma \Rightarrow A$ then $\Gamma \Rightarrow A$

**Proof:** By straightforward induction over the given derivations. \qed

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 statement of the lemma must actually be slightly more general by allowing substitution into hypotheses.

**Lemma 7.2 (Admissibility of Generalized Equality Rules)**

1. If $[s/x]\Gamma, s \equiv t \Rightarrow [s/x]A$ then $[t/x]\Gamma, s \equiv t \Rightarrow [t/x]A$.
2. If $[t/x]\Gamma, s \equiv t \Rightarrow [t/x]A$ then $[s/x]\Gamma, s \equiv t \Rightarrow [s/x]A$.
3. If $[s/x]\Gamma, s \equiv t \Rightarrow [s/x]A$ then $[t/x]\Gamma, s \equiv t \Rightarrow [t/x]A$.
4. If $[s/x]\Gamma, s \equiv t \Rightarrow [s/x]A$ then $[t/x]\Gamma, s \equiv t \Rightarrow [t/x]A$.

Draft of April 6, 2004
Proof: By induction on the structure of the given derivations \( S \) or \( E \), 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:

\[ S_1 \]

\[
\frac{[s/x] \Gamma, s \vdash t, [s/x] A_1 \Rightarrow [s/x] A_2}{[s/x] \Gamma, s \vdash t \Rightarrow [s/x] A_1 \supset [s/x] A_2} \]

\[
[t/x] \Gamma, s \vdash t, [t/x] A_1 \Rightarrow [t/x] A_2 \quad \text{By i.h. on } S_1
\]

\[
[t/x] \Gamma, s \vdash t \Rightarrow [t/x] A_1 \supset [t/x] A_2 \quad \text{By rule } \supset R
\]

Case:

\[ E \]

\[
\frac{[s/x] \Gamma, s \vdash t \Rightarrow [s/x] E}{[s/x] \Gamma, s \vdash t \Rightarrow [s/x] E} \]

\[
[t/x] \Gamma, s \vdash t \Rightarrow [t/x] E \quad \text{By i.h. (3) on } E
\]

\[
[t/x] \Gamma, s \vdash t \Rightarrow [t/x] E \quad \text{By rule } \Rightarrow
\]

Case:

\[ E = \text{init} \]

\[
\frac{[s/x] \Gamma’, [s/x] P_1, s \vdash t \Rightarrow [s/x] P_2}{[s/x] \Gamma’, [s/x] P_1, s \vdash t \Rightarrow [s/x] P_2} \]

We obtain the first equation below from the assumption that \( E \) is an initial sequent.

\[
[s/x] P_1 = [s/x] P_2 \quad \text{Given}
\]

\[
[t/x] \Gamma’, [t/x] P_1, s \vdash t \Rightarrow [t/x] P_1 \quad \text{By rule init}
\]

\[
[t/x] \Gamma’, [t/x] P_1, s \vdash t \Rightarrow [s/x] P_1 \quad \text{By rule } \vdash L_2
\]

\[
[t/x] \Gamma’, [t/x] P_1, s \vdash t \Rightarrow [s/x] P_2 \quad \text{Same, by given equality}
\]

\[
[t/x] \Gamma’, [t/x] P_1, s \vdash t \Rightarrow [t/x] P_2 \quad \text{By rule } \vdash L_1
\]

Case:

\[ E’ \]

\[
\frac{[s/x] \Gamma’, [s/x] q \vdash [s/x] r, s \vdash t \Rightarrow [s/x] q/y E’}{[s/x] \Gamma’, [s/x] q \vdash [s/x] r, s \vdash t \Rightarrow [s/x] E} \]

\[ \vdash L_1 \]

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 \( \vdash L_1 \).

Draft of April 6, 2004
7.2 Sequent Calculus

\[ [s/x]E = [[s/x]r/y]E' \]
\[ [s/x]\Gamma', [s/x]q \mid [s/x]r, s \doteq t \implies [s/x][q/y]E' \quad \text{Given} \]
\[ [t/x]\Gamma', [t/x]q \mid [t/x]r, s \doteq t \implies [t/x][q/y]E' \quad \text{By i.h. on } \mathcal{E}' \]
\[ [t/x]\Gamma', [t/x]q \mid [t/x]r, s \doteq t \implies [[t/x]q/y]E' \quad \text{Same, since } x \text{ not in } E' \]
\[ [t/x]\Gamma', [t/x]q \mid [t/x]r, s \doteq t \implies [[t/x]r/y]E' \quad \text{By rule } \doteq L_1 \]
\[ [t/x]\Gamma', [t/x]q \mid [t/x]r, s \doteq t \implies [[t/x]r/y]E' \quad \text{Same, since } x \text{ not in } E' \]
\[ [t/x]\Gamma', [t/x]q \mid [t/x]r, s \doteq t \implies [t/x][r/y]E' \quad \text{Same, by given equality} \]
\[ [t/x]\Gamma', [t/x]q \mid [t/x]r, s \doteq t \implies [t/x]E \quad \text{By rule } \doteq L_1 \]

Case:

\[ \mathcal{E}' = [s/x]E' \]
\[ [s/x]\Gamma, s \doteq t \implies [s/x]E' \]
\[ [s/x]\Gamma, s \doteq t \implies [s/x]E \quad \doteq L_1 \]

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 \( \doteq L_1 \) with the principal formula \( s \doteq t \).

\[ [s/x]E = [t/x]E' \quad \text{Given} \]
\[ [t/x]\Gamma, s \doteq t \implies [t/x]E' \quad \text{By i.h. on } \mathcal{E}' \]
\[ [t/x]\Gamma, s \doteq t \implies [s/x]E \quad \text{Same, by given equality} \]
\[ [t/x]\Gamma, s \doteq t \implies [t/x]E \quad \text{By rule } \doteq L_1 \]

\( \square \)

A second lemma is helpful to streamline the completeness proof.

**Lemma 7.3 (Atomic Initial Sequents)** \( \Gamma, A \vdash \R \Rightarrow \Gamma, A \vdash A \).

**Proof:** By induction on the structure of \( A \). This is related to repeated local expansion. We show a few of cases.

**Case:** \( A = P \).

\[ \Gamma, P \R \Rightarrow P \quad \text{By rule init} \]
\[ \Gamma, P \R \Rightarrow P \quad \text{By rule eq} \]

**Case:** \( A = (s \doteq t) \).

\[ \Gamma, s \doteq t \R \Rightarrow s \doteq s \quad \text{By rule } \doteq R \]
\[ \Gamma, s \doteq t \R \Rightarrow s \doteq t \quad \text{By rule } \doteq L_1 \]

*Draft of April 6, 2004*
Case: $A = A_1 \land A_2$.

\[
\begin{align*}
\Gamma', A_1 & \Rightarrow A_1 & \text{By i.h. on } A_1 \\
\Gamma, A_1 \land A_2 & \Rightarrow A_1 & \text{By rule } \& \land L_1 \\
\Gamma, A_2 & \Rightarrow A_2 & \text{By i.h. on } A_2 \\
\Gamma, A_1 \land A_2 & \Rightarrow A_2 & \text{By rule } \& \land L_2 \\
\Gamma, A_1 \land A_2 & \Rightarrow A_1 \land A_2 & \text{By rule } \& \land R \\
\end{align*}
\]

With these two lemmas, completeness is relatively simple.

**Theorem 7.4 (Completeness of Regular Derivations)**

*If* $\Gamma \Rightarrow A$ *then* $\Gamma \Rightarrow A$.

**Proof:** By induction on the structure of the given derivation $S$. We show some cases; most are straightforward.

**Case:**

\[
S_2
\]

\[
S = \quad \begin{array}{c}
\Gamma, A_1 \Rightarrow A_2 \\
\Gamma \Rightarrow A_1 \lor A_2 \lor R
\end{array}
\]

\[
\begin{align*}
\Gamma, A_1 & \Rightarrow A_2 & \text{By i.h. on } S_2 \\
\Gamma & \Rightarrow A_1 \lor A_2 & \text{By rule } \lor R \\
\end{align*}
\]

**Case:**

\[
\begin{array}{c}
\Gamma', A \Rightarrow A
\end{array}
\]

By Lemma 7.3

**Case:**

\[
S_1
\]

\[
S = \quad \begin{array}{c}
\Gamma', s \triangle t \Rightarrow [s/x]A \\
\Gamma', s \triangle t \Rightarrow [t/x]A \lor L_1
\end{array}
\]

\[
\begin{align*}
\Gamma', s \triangle t & \Rightarrow [s/x]A & \text{By i.h. on } S_1 \\
\Gamma', s \triangle t & \Rightarrow [t/x]A & \text{By Lemma 7.2}
\end{align*}
\]

$\square$

*Draft of April 6, 2004*
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 \( \Gamma \xrightarrow{E} E \) and \( \Gamma, E \xrightarrow{E} F \) then \( \Gamma \xrightarrow{E} F \).
2. If \( \Gamma \xrightarrow{E} E \) and \( \Gamma, E \xrightarrow{R} C \) then \( \Gamma \xrightarrow{R} C \).
3. If \( \Gamma \xrightarrow{R} A \) and \( \Gamma, A \xrightarrow{E} F \) then \( \Gamma \xrightarrow{R} F \).
4. If \( \Gamma \xrightarrow{R} A \) and \( \Gamma, A \xrightarrow{R} C \) then \( \Gamma \xrightarrow{R} C \).

**Proof:** We prove the properties in sequence, using earlier ones to in the proofs of later ones.

**Part (1):** Given

\[
\begin{align*}
\mathcal{E} & \xrightarrow{E} E \quad \text{and} \quad \mathcal{F} = \Gamma, E \xrightarrow{E} F \\
\Gamma & \xrightarrow{E} F
\end{align*}
\]

we construct a derivation for \( \Gamma \xrightarrow{E} F \) 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:**

\[
\begin{align*}
\mathcal{E} & = \Gamma \xrightarrow{E} s \xrightarrow{E} s \\
\mathcal{F} & = \Gamma, s \xrightarrow{E} [s/x]F_1 \xrightarrow{E} F_1 \\
\Gamma & \xrightarrow{E} [s/x]F_1
\end{align*}
\]

By i.h. on \( \mathcal{E} \) and \( \mathcal{F}_1 \)

**Case:**

\[
\begin{align*}
\mathcal{E}_1 & = \Gamma', q \xrightarrow{E} |q/x|s' = |q/x|t' \\
\mathcal{F} & = \Gamma', q \xrightarrow{E} |r/x|s' = |r/x|t' \\
\Gamma', q & \xrightarrow{E} F
\end{align*}
\]

By i.h. on \( \mathcal{E}_1 \) and above
Part (2): Given

\[ \Gamma \vdash_{E} E \quad \text{and} \quad \Gamma, E \vdash_{R} C \]

we construct a derivation for \( \Gamma \vdash_{R} C \) 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 \( \vdash_{E} \) to \( \vdash_{R} \) in \( \mathcal{S} \) we appeal to Part (1).

Part (3): Given

\[ \Gamma \vdash_{R} A \quad \text{and} \quad \Gamma, A \vdash_{E} F \]

we construct a derivation for \( \Gamma \vdash_{E} F \) 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 \( \vdash_{E} \) to \( \vdash_{R} \) in \( \mathcal{S} \) we appeal to Part (1).

Part (4): Given

\[ \Gamma \vdash_{R} A \quad \text{and} \quad \Gamma, A \vdash_{R} C \]

we construct a derivation for \( \Gamma \vdash_{R} C \) 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. □