Isabelle’s Logics

Lawrence C. Paulson
Computer Laboratory
University of Cambridge
lcp@cl.cam.ac.uk

With Contributions by Tobias Nipkow and Markus Wenzel

25 October 2022

Markus Wenzel made numerous improvements. Sara Kalvala contributed Chap. 4. Philippe de Groote wrote the first version of the logic LK. Tobias Nipkow developed LCF and Cube. Martin Coen developed Modal with assistance from Rajeev Goré. The research has been funded by the EPSRC (grants GR/G53279, GR/H40570, GR/K57381, GR/K77051, GR/M75440) and by ESPRIT (projects 3245: Logical Frameworks, and 6453: Types), and by the DFG Schwerpunktprogramm Deduktion.
# Contents

## 1 Syntax definitions

## 2 Higher-Order Logic

2.1 Syntax ........................................... 5
   2.1.1 Types and overloading ................. 5
   2.1.2 Binders ................................... 8
   2.1.3 The let and case constructions ....... 9
2.2 Rules of inference .............................. 10
2.3 A formulation of set theory .................. 14
   2.3.1 Syntax of set theory .................... 14
   2.3.2 Axioms and rules of set theory ...... 17
   2.3.3 Properties of functions ............... 20
2.4 Simplification and substitution ............ 22
   2.4.1 Case splitting ......................... 23
2.5 Types .......................................... 23
   2.5.1 Product and sum types ................. 24
   2.5.2 The type of natural numbers, \textit{nat} ........ 26
   2.5.3 Numerical types and numerical reasoning .... 28
   2.5.4 The type constructor for lists, \textit{list} ........ 29
2.6 Datatype definitions ......................... 29
   2.6.1 Basics .................................... 32
   2.6.2 Defining datatypes ..................... 37
2.7 Old-style recursive function definitions .... 38
2.8 Example: Cantor’s Theorem .................. 42

## 3 First-Order Sequent Calculus

3.1 Syntax and rules of inference ............... 44
3.2 Automatic Proof ................................ 50
3.3 Tactics for the cut rule ..................... 50
3.4 Tactics for sequents ......................... 51
3.5 A simple example of classical reasoning .... 52
3.6 A more complex proof ......................... 53
3.7 *Unification for lists ....................... 55
CONTENTS

3.8 *Packaging sequent rules ........................................... 56
3.9 *Proof procedures .................................................. 57
  3.9.1 Method A ...................................................... 57
  3.9.2 Method B ...................................................... 58

4 Defining A Sequent-Based Logic .................................. 59
  4.1 Concrete syntax of sequences ................................. 59
  4.2 Basis .......................................................... 60
  4.3 Object logics ................................................... 60
  4.4 What’s in Sequents.thy ....................................... 61

5 Constructive Type Theory ......................................... 63
  5.1 Syntax .......................................................... 65
  5.2 Rules of inference .............................................. 69
  5.3 Rule lists ....................................................... 72
  5.4 Tactics for subgoal reordering .............................. 73
  5.5 Rewriting tactics .............................................. 73
  5.6 Tactics for logical reasoning ................................. 74
  5.7 A theory of arithmetic ....................................... 75
  5.8 The examples directory ..................................... 75
  5.9 Example: type inference .................................... 77
  5.10 An example of logical reasoning ............................. 78
  5.11 Example: deriving a currying functional .................. 81
  5.12 Example: proving the Axiom of Choice .................... 83
Several logics come with Isabelle. Many of them are sufficiently developed to serve as comfortable reasoning environments. They are also good starting points for defining new logics. Each logic is distributed with sample proofs, some of which are described in this document.

\textbf{HOL} is currently the best developed Isabelle object-logic, including an extensive library of (concrete) mathematics, and various packages for advanced definitional concepts (like (co-)inductive sets and types, well-founded recursion etc.). The distribution also includes some large applications.

\textbf{ZF} provides another starting point for applications, with a slightly less developed library than \textbf{HOL}. \textbf{ZF}’s definitional packages are similar to those of \textbf{HOL}. Untyped \textbf{ZF} set theory provides more advanced constructions for sets than simply-typed \textbf{HOL}. \textbf{ZF} is built on \textbf{FOL} (first-order logic), both are described in a separate manual \textit{Isabelle’s Logics: FOL and ZF} [12].

There are some further logics distributed with Isabelle:

\textbf{CCL} is Martin Coen’s Classical Computational Logic, which is the basis of a preliminary method for deriving programs from proofs [2]. It is built upon classical FOL.

\textbf{LCF} is a version of Scott’s Logic for Computable Functions, which is also implemented by the \texttt{lcf} system [13]. It is built upon classical FOL.

\textbf{HOLCF} is a version of \textbf{LCF}, defined as an extension of \textbf{HOL}. See [10] for more details on \textbf{HOLCF}.

\textbf{CTT} is a version of Martin-Löf’s Constructive Type Theory [11], with extensional equality. Universes are not included.

\textbf{Cube} is Barendregt’s \(\lambda\)-cube.

The directory \texttt{Sequents} contains several logics based upon the sequent calculus. Sequents have the form \(A_1, \ldots, A_m \vdash B_1, \ldots, B_n\); rules are applied using associative matching.

\textbf{LK} is classical first-order logic as a sequent calculus.

\textbf{Modal} implements the modal logics \(T\), \(S4\), and \(S43\).
ILL implements intuitionistic linear logic.

The logics CCL, LCF, Modal, ILL and Cube are undocumented. All object-logics’ sources are distributed with Isabelle (see the directory src). They are also available for browsing on the WWW at

http://www.cl.cam.ac.uk/Research/HVG/Isabelle/library/
https://isabelle.in.tum.de/library/

Note that this is not necessarily consistent with your local sources!

Do not read the Isabelle’s Logics manuals before reading Isabelle/HOL — The Tutorial or Introduction to Isabelle, and performing some Isabelle proofs. Consult the Reference Manual for more information on tactics, packages, etc.
Chapter 1

Syntax definitions

The syntax of each logic is presented using a context-free grammar. These grammars obey the following conventions:

- identifiers denote nonterminal symbols
- typewriter font denotes terminal symbols
- parentheses (…) express grouping
- constructs followed by a Kleene star, such as id* and (...)* can be repeated 0 or more times
- alternatives are separated by a vertical bar, |
- the symbol for alphanumeric identifiers is id
- the symbol for scheme variables is var

To reduce the number of nonterminals and grammar rules required, Isabelle’s syntax module employs priorities, or precedences. Each grammar rule is given by a mixfix declaration, which has a priority, and each argument place has a priority. This general approach handles infix operators that associate either to the left or to the right, as well as prefix and binding operators.

In a syntactically valid expression, an operator’s arguments never involve an operator of lower priority unless brackets are used. Consider first-order logic, where ∃ has lower priority than ∨, which has lower priority than ∧. There, \( P \land Q \lor R \) abbreviates \( (P \land Q) \lor R \) rather than \( P \land (Q \lor R) \). Also, \( \exists x . P \lor Q \) abbreviates \( \exists x . (P \lor Q) \) rather than \( (\exists x . P) \lor Q \). Note especially that \( P \lor (\exists x . Q) \) becomes syntactically invalid if the brackets are removed.

A binder is a symbol associated with a constant of type \( (\sigma \Rightarrow \tau') \Rightarrow \tau' \). For instance, we may declare \( \forall \) as a binder for the constant All, which has type \( (\alpha \Rightarrow \sigma) \Rightarrow o \). This defines the syntax \( \forall x . t \) to mean \( \text{All}(\lambda x . t) \). We can also write \( \forall x_1 \ldots x_m . t \) to abbreviate \( \forall x_1 \ldots \forall x_m . t \); this is possible for any constant provided that \( \tau \) and \( \tau' \) are the same type. The Hilbert description operator \( \varepsilon x . P x \) has type \( (\alpha \Rightarrow \text{bool}) \Rightarrow \alpha \) and normally binds only one
variable. ZF’s bounded quantifier $\forall x \in A . P(x)$ cannot be declared as a binder because it has type $[i, i \Rightarrow o] \Rightarrow o$. The syntax for binders allows type constraints on bound variables, as in

$$\forall (x::\alpha) (y::\beta) (z::\gamma) . Q(x, y, z)$$

To avoid excess detail, the logic descriptions adopt a semi-formal style. Infix operators and binding operators are listed in separate tables, which include their priorities. Grammar descriptions do not include numeric priorities; instead, the rules appear in order of decreasing priority. This should suffice for most purposes; for full details, please consult the actual syntax definitions in the .thy files.

Each nonterminal symbol is associated with some Isabelle type. For example, the formulae of first-order logic have type $o$. Every Isabelle expression of type $o$ is therefore a formula. These include atomic formulae such as $P$, where $P$ is a variable of type $o$, and more generally expressions such as $P(t, u)$, where $P$, $t$ and $u$ have suitable types. Therefore, ‘expression of type $o’ is listed as a separate possibility in the grammar for formulae.
Chapter 2

Higher-Order Logic

This chapter describes Isabelle’s formalization of Higher-Order Logic, a polymorphic version of Church’s Simple Theory of Types. HOL can be best understood as a simply-typed version of classical set theory. The monograph Isabelle/HOL — A Proof Assistant for Higher-Order Logic provides a gentle introduction on using Isabelle/HOL in practice. All of this material is mainly of historical interest!

2.1 Syntax

Figure 2.1 lists the constants (including infixes and binders), while Fig. 2.2 presents the grammar of higher-order logic. Note that $a \neq b$ is translated to $\neg(a = b)$.

HOL has no if-and-only-if connective; logical equivalence is expressed using equality. But equality has a high priority, as befitting a relation, while if-and-only-if typically has the lowest priority. Thus, $\neg\neg P = P$ abbreviates $\neg\neg(P = P)$ and not $(\neg\neg P) = P$. When using $=$ to mean logical equivalence, enclose both operands in parentheses.

2.1.1 Types and overloading

The universal type class of higher-order terms is called term. By default, explicit type variables have class term. In particular the equality symbol and quantifiers are polymorphic over class term.

The type of formulae, bool, belongs to class term; thus, formulae are terms. The built-in type fun, which constructs function types, is overloaded with arity (term, term) term. Thus, $\sigma \Rightarrow \tau$ belongs to class term if $\sigma$ and $\tau$ do, allowing quantification over functions.

HOL allows new types to be declared as subsets of existing types, either using the primitive typedef or the more convenient datatype (see §2.6).

Several syntactic type classes — plus, minus, times and power — permit overloading of the operators $+$, $-$, $\ast$, and $^\wedge$. They are overloaded to denote
## Higher-Order Logic

<table>
<thead>
<tr>
<th>name</th>
<th>meta-type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trueprop</td>
<td>bool \implies prop</td>
<td>coercion to prop</td>
</tr>
<tr>
<td>Not</td>
<td>bool \implies bool</td>
<td>negation (\neg)</td>
</tr>
<tr>
<td>True</td>
<td>bool</td>
<td>tautology (\top)</td>
</tr>
<tr>
<td>False</td>
<td>bool</td>
<td>absurdity (\bot)</td>
</tr>
<tr>
<td>If</td>
<td>bool, \alpha, \alpha \implies \alpha</td>
<td>conditional</td>
</tr>
<tr>
<td>Let</td>
<td>\alpha \implies \beta \implies \beta</td>
<td>let binder</td>
</tr>
</tbody>
</table>

### Constants

<table>
<thead>
<tr>
<th>symbol</th>
<th>name</th>
<th>meta-type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOME or \emptyset</td>
<td>Eps</td>
<td>(\alpha \implies bool) \implies \alpha</td>
<td>Hilbert description (\varepsilon)</td>
</tr>
<tr>
<td>ALL or !</td>
<td>All</td>
<td>(\alpha \implies bool) \implies bool</td>
<td>universal quantifier (\forall)</td>
</tr>
<tr>
<td>EX or ?</td>
<td>Ex</td>
<td>(\alpha \implies bool) \implies bool</td>
<td>existential quantifier (\exists)</td>
</tr>
<tr>
<td>EX! or ?!</td>
<td>Ex1</td>
<td>(\alpha \implies bool) \implies bool</td>
<td>unique existence (\exists!)</td>
</tr>
<tr>
<td>LEAST</td>
<td>Least</td>
<td>(\alpha :: ord \implies bool) \implies \alpha</td>
<td>least element</td>
</tr>
</tbody>
</table>

### Binders

<table>
<thead>
<tr>
<th>symbol</th>
<th>meta-type</th>
<th>priority</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\circ</td>
<td>[\beta \implies \gamma, \alpha \implies \beta] \implies (\alpha \implies \gamma)</td>
<td>Left 55</td>
<td>composition (\circ)</td>
</tr>
<tr>
<td>=</td>
<td>[\alpha, \alpha] \implies bool</td>
<td>Left 50</td>
<td>equality (=)</td>
</tr>
<tr>
<td>&lt;</td>
<td>[\alpha :: ord, \alpha] \implies bool</td>
<td>Left 50</td>
<td>less than (&lt;)</td>
</tr>
<tr>
<td>\leq</td>
<td>[\alpha :: ord, \alpha] \implies bool</td>
<td>Left 50</td>
<td>less than or equals (\leq)</td>
</tr>
<tr>
<td>&amp;</td>
<td>[bool, bool] \implies bool</td>
<td>Right 35</td>
<td>conjunction (\land)</td>
</tr>
<tr>
<td></td>
<td>\implies</td>
<td>Right 30</td>
<td>disjunction (\lor)</td>
</tr>
<tr>
<td>\rightarrow</td>
<td>[bool, bool] \implies bool</td>
<td>Right 25</td>
<td>implication (\rightarrow)</td>
</tr>
</tbody>
</table>

### Infixes

Figure 2.1: Syntax of HOL
term = expression of class term
| SOME id . formula | @ id . formula
| let id = term; ...; id = term in term
| if formula then term else term
| LEAST id . formula

formula = expression of type bool
| term = term
| term <= term
| term < term
| ~ formula
| formula & formula
| formula | formula
| formula --> formula
| ALL id id* . formula | ! id id* . formula
| EX id id* . formula | ? id id* . formula
| EX! id id* . formula | ?! id id* . formula

Figure 2.2: Full grammar for HOL
the obvious arithmetic operations on types \texttt{nat}, \texttt{int} and \texttt{real}. (With the \texttt{^} operator, the exponent always has type \texttt{nat}.) Non-arithmetic overloadings are also done: the operator - can denote set difference, while \texttt{^} can denote exponentiation of relations (iterated composition). Unary minus is also written as - and is overloaded like its 2-place counterpart; it even can stand for set complement.

The constant \texttt{0} is also overloaded. It serves as the zero element of several types, of which the most important is \texttt{nat} (the natural numbers). The type class \texttt{plus_ac0} comprises all types for which 0 and + satisfy the laws \( x + y = y + x, (x + y) + z = x + (y + z) \) and \( 0 + x = x \). These types include the numeric ones \texttt{nat}, \texttt{int} and \texttt{real} and also multisets. The summation operator \texttt{sum} is available for all types in this class.

Theory \texttt{Ord} defines the syntactic class \texttt{ord} of order signatures. The relations \texttt{<} and \leq are polymorphic over this class, as are the functions \texttt{mono}, \texttt{min} and \texttt{max}, and the \texttt{LEAST} operator. \texttt{Ord} also defines a subclass \texttt{order} of \texttt{ord} which axiomatizes the types that are partially ordered with respect to \leq. A further subclass \texttt{linorder} of \texttt{order} axiomatizes linear orderings. For details, see the file \texttt{Ord.thy}.

If you state a goal containing overloaded functions, you may need to include type constraints. Type inference may otherwise make the goal more polymorphic than you intended, with confusing results. For example, the variables \( i, j \) and \( k \) in the goal \( i \leq j \Rightarrow i \leq j + k \) have type \( \alpha :: \{ \texttt{ord}, \texttt{plus} \} \), although you may have expected them to have some numeric type, e.g. \texttt{nat}. Instead you should have stated the goal as \( (i :: \texttt{nat}) \leq j \Rightarrow i \leq j + k \), which causes all three variables to have type \texttt{nat}.

\!

If resolution fails for no obvious reason, try setting \texttt{show_types} to \texttt{true}, causing Isabelle to display types of terms. Possibly set \texttt{show_sorts} to \texttt{true} as well, causing Isabelle to display type classes and sorts.

Where function types are involved, Isabelle’s unification code does not guarantee to find instantiations for type variables automatically. Be prepared to use \texttt{res_inst_tac} instead of \texttt{resolve_tac}, possibly instantiating type variables. Setting \texttt{Unify.trace_types} to \texttt{true} causes Isabelle to report omitted search paths during unification.

\subsection{Binders}

Hilbert’s description operator \( \varepsilon x . P[x] \) stands for some \( x \) satisfying \( P \), if such exists. Since all terms in HOL denote something, a description is always meaningful, but we do not know its value unless \( P \) defines it uniquely. We may write descriptions as \texttt{Eps(\lambda x . P[x])} or use the syntax \texttt{SOME} \( x . \ P[x] \).
Existential quantification is defined by

\[ \exists x . P x \equiv P(\varepsilon x . P x) . \]

The unique existence quantifier, \( \exists! x . P \), is defined in terms of \( \exists \) and \( \forall \). An Isabelle binder, it admits nested quantifications. For instance, \( \exists! x y . P x y \) abbreviates \( \exists! x . \exists! y . P x y \); note that this does not mean that there exists a unique pair \((x, y)\) satisfying \( P x y \).

The basic Isabelle/HOL binders have two notations. Apart from the usual \texttt{ALL} and \texttt{EX} for \( \forall \) and \( \exists \), Isabelle/HOL also supports the original notation of Gordon’s HOL system: \(!\) and \(?\). In the latter case, the existential quantifier \texttt{must} be followed by a space; thus \texttt{?x} is an unknown, while \texttt{? x. f x=y} is a quantification. Both notations are accepted for input. The print mode “HOL” governs the output notation. If enabled (e.g. by passing option \texttt{-m HOL} to the \texttt{isabelle} executable), then \(!\) and \(?\) are displayed.

If \( \tau \) is a type of class \texttt{ord}, \( P \) a formula and \( x \) a variable of type \( \tau \), then the term \texttt{LEAST} \( x . P[x] \) is defined to be the least (w.r.t. \( \leq \)) \( x \) such that \( P x \) holds (see Fig. 2.4). The definition uses Hilbert’s \( \varepsilon \) choice operator, so \texttt{Least} is always meaningful, but may yield nothing useful in case there is not a unique least element satisfying \( P \).\footnote{Class \texttt{ord} does not require much of its instances, so \( \leq \) need not be a well-ordering, not even an order at all!}

\[ ! \] The low priority of binders means that they need to be enclosed in parenthesis when they occur in the context of other operations. For example, instead of \( P \land \forall x . Q \) you need to write \( P \land (\forall x . Q) \).

\subsection*{2.1.3 The let and case constructions}

Local abbreviations can be introduced by a \texttt{let} construct whose syntax appears in Fig. 2.2. Internally it is translated into the constant \texttt{Let}. It can be expanded by rewriting with its definition, \texttt{Let_def}.

HOL also defines the basic syntax

\[ \texttt{case e of c_1 \Rightarrow e_1 | \ldots | c_n \Rightarrow e_n} \]

as a uniform means of expressing \texttt{case} constructs. Therefore \texttt{case} and \texttt{of} are reserved words. Initially, this is mere syntax and has no logical meaning. By declaring translations, you can cause instances of the \texttt{case} construct to denote applications of particular case operators. This is what happens automatically for each \texttt{datatype} definition (see §2.6).
CHAPTER 2. HIGHER-ORDER LOGIC

refl \ t = (t::'a)

subst \[| s = t; P s |\] ==> P (t::'a)

ext \ (!!x::'a. (f x :: 'b) = g x) ==> (%x. f x) = (%x. g x)

impI \ (P ==> Q) ==> P-->Q

mp \[| P-->Q; P |\] ==> Q

iff \ (P-->Q) --> (Q-->P) --> (P=Q)

someI \ P(x::'a) ==> P(@x. P x)

True_or_False \ (P=True) | (P=False)

Figure 2.3: The HOL rules

Both if and case constructs have as low a priority as quantifiers, which requires additional enclosing parentheses in the context of most other operations. For example, instead of \ f x = if . . . then . . . else . . . you need to write \ f x = (if . . . then . . . else . . .).

2.2 Rules of inference

Figure 2.3 shows the primitive inference rules of HOL, with their ML names. Some of the rules deserve additional comments:

ext expresses extensionality of functions.

iff asserts that logically equivalent formulae are equal.

someI gives the defining property of the Hilbert ε-operator. It is a form of the Axiom of Choice. The derived rule some_equality (see below) is often easier to use.

True_or_False makes the logic classical.\(^2\)

HOL follows standard practice in higher-order logic: only a few connectives are taken as primitive, with the remainder defined obscurely (Fig. 2.4). Gordon’s HOL system expresses the corresponding definitions [6, page 270] using object-equality (=), which is possible because equality in higher-order logic may equate formulae and even functions over formulae. But theory HOL, like all other Isabelle theories, uses meta-equality (==) for definitions.

\(^2\)In fact, the ε-operator already makes the logic classical, as shown by Diaconescu; see Paulson [14] for details.
CHAPTER 2. HIGHER-ORDER LOGIC

```
True_def True   == ((%x::bool. x)=(%x. x))
All_def All     == (%P. P = (%x. True))
Ex_def Ex      == (%P. P(∃x. P x))
False_def False == (!P. P)
not_def not    == (%P. P-->False)
and_def op &   == (%P Q. !R. (P-->Q-->R) --> R)
or_def op |     == (%P Q. !R. (P-->R) --> (Q-->R) --> R)
Ex1_def Ex1    == (%P. (?) x. P x & (! y. P y --> y=x))
o_def op o     == (%(f::'b=>'c) g x::'a. f(g x))
if_def If P x y ==
    (%P x y. @z::'a.(P=True --> z=x) & (P=False --> z=y))
Let_def Let s f == f s
Least_def Least P == @x. P(x) & (ALL y. P(y) --> x <= y)
```

Figure 2.4: The HOL definitions

The definitions above should never be expanded and are shown for completeness only. Instead users should reason in terms of the derived rules shown below or, better still, using high-level tactics.

Some of the rules mention type variables; for example, refl mentions the type variable 'a. This allows you to instantiate type variables explicitly by calling res_inst_tac.

Some derived rules are shown in Figures 2.5 and 2.6, with their ML names. These include natural rules for the logical connectives, as well as sequent-style elimination rules for conjunctions, implications, and universal quantifiers.

Note the equality rules: ssusbst performs substitution in backward proofs, while box_equals supports reasoning by simplifying both sides of an equation.

The following simple tactics are occasionally useful:

- **strip_tac** \(i\) applies \(\text{allI}\) and \(\text{impI}\) repeatedly to remove all outermost universal quantifiers and implications from subgoal \(i\).

- **case_tac** "\(P\)" \(i\) performs case distinction on \(P\) for subgoal \(i\); the latter is replaced by two identical subgoals with the added assumptions \(P\) and \(\neg P\), respectively.

- **smp_tac** \(j\) \(i\) applies \(j\) times \(\text{spec}\) and then \(\text{mp}\) in subgoal \(i\), which is typically useful when forward-chaining from an induction hypothesis. As a generalization of **mp_tac**, if there are assumptions \(\forall \vec{x}. P\vec{x} \rightarrow Q\vec{x}\) and \(P\vec{a}\), (\(\vec{x}\) being a vector of \(j\) variables) then it replaces the universally quantified implication by \(Q\vec{a}\). It may instantiate unknowns. It fails if it can do nothing.
CHAPTER 2. HIGHER-ORDER LOGIC

\begin{itemize}
  \item sym \quad s=t \implies t=s
  \item trans \quad [\mid r=s; s=t \mid] \implies r=t
  \item ssubst \quad [\mid t=s; P s \mid] \implies P t
  \item box_equals \quad [\mid a=b; a=c; b=d \mid] \implies c=d
  \item arg_cong \quad x = y \implies f x = f y
  \item fun_cong \quad f = g \implies f x = g x
  \item cong \quad [\mid f = g; x = y \mid] \implies f x = g y
  \item not\_sym \quad t \neq s \implies s \neq t
\end{itemize}

\textbf{EQUALITY}

\begin{itemize}
  \item TrueI \quad True
  \item FalseE \quad False \implies P
  \item conjI \quad [\mid P; Q \mid] \implies P \& Q
  \item conjunct1 \quad [\mid P \& Q \mid] \implies P
  \item conjunct2 \quad [\mid P \& Q \mid] \implies Q
  \item conjE \quad [\mid P \& Q; [\mid P; Q \mid] \implies R \mid] \implies R
  \item disjI1 \quad P \implies P \mid Q
  \item disjI2 \quad Q \implies P \mid Q
  \item disjE \quad [\mid P \mid Q; P \implies R; Q \implies R \mid] \implies R
  \item notI \quad (P \implies False) \implies \neg P
  \item notE \quad [\mid \neg P; P \mid] \implies R
  \item impE \quad [\mid P \implies Q; P; Q \implies R \mid] \implies R
\end{itemize}

\textbf{PROPOSITIONAL LOGIC}

\begin{itemize}
  \item iffI \quad [\mid P \implies Q; Q \implies P \mid] \implies P=Q
  \item iffD1 \quad [\mid P=Q; P \mid] \implies Q
  \item iffD2 \quad [\mid P=Q; Q \mid] \implies P
  \item iffE \quad [\mid P=Q; [\mid P \implies Q; Q \implies P \mid] \implies R \mid] \implies R
\end{itemize}

\textbf{LOGICAL EQUIVALENCE}

Figure 2.5: Derived rules for HOL
### Quantifiers and descriptions

<table>
<thead>
<tr>
<th>Formula</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allI (!x. P x) ==&gt; !x. P x</td>
<td>All quantifier</td>
</tr>
<tr>
<td>spec !x. P x ==&gt; P x</td>
<td>Specification</td>
</tr>
<tr>
<td>allE [! x. P x; P x ==&gt; R</td>
<td>All elimination</td>
</tr>
<tr>
<td>all_dupE [! x. P x; [P x; !x. P x] ==&gt; R] ] ==&gt; R</td>
<td>All duplication elimination</td>
</tr>
<tr>
<td>exI P x ==&gt; ? x. P x</td>
<td>Existential introduction</td>
</tr>
<tr>
<td>exE [? x. P x; !x. P x ==&gt; Q</td>
<td>Existential elimination</td>
</tr>
<tr>
<td>ex1I [P a; !x. P x ==&gt; x=a ] ] ==&gt; ?! x. P x</td>
<td>Existential uniqueness introduction</td>
</tr>
<tr>
<td>ex1E [? ! x. P x; !x. [P x; ! y. P y --&gt; y=x ] ==&gt; R ] ] ==&gt; R</td>
<td>Existential uniqueness elimination</td>
</tr>
<tr>
<td>some_equality [P a; !x. P x ==&gt; x=a ] ] ==&gt; ($x. P x) = a</td>
<td>Some uniqueness equality</td>
</tr>
</tbody>
</table>

### Classical logic

<table>
<thead>
<tr>
<th>Formula</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccontr (-P ==&gt; False) ==&gt; P</td>
<td>Contradiction</td>
</tr>
<tr>
<td>classical (-P ==&gt; P) ==&gt; P</td>
<td>Classical logic</td>
</tr>
<tr>
<td>excluded_middle -P</td>
<td></td>
</tr>
<tr>
<td>disjCI (-Q ==&gt; P) ==&gt; P</td>
<td>Disjunction</td>
</tr>
<tr>
<td>exCI (! x. - P x ==&gt; P a) ==&gt; ? x. P x</td>
<td>Existential introduction</td>
</tr>
<tr>
<td>impCE [P--&gt;Q; - P ==&gt; R; Q ==&gt; R</td>
<td>Implication</td>
</tr>
<tr>
<td>iffCE [P=Q; [P;Q] ==&gt; R; [P; -Q</td>
<td>Implication</td>
</tr>
<tr>
<td>notnotD -P ==&gt; P</td>
<td>Notation</td>
</tr>
<tr>
<td>swap -P ==&gt; (-Q ==&gt; P)</td>
<td>Swap</td>
</tr>
</tbody>
</table>

### Conditionals

<table>
<thead>
<tr>
<th>Formula</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>if_P P ==&gt; (if P then x else y) = x</td>
<td>Conditional</td>
</tr>
<tr>
<td>if_not_P - P ==&gt; (if P then x else y) = y</td>
<td>Conditional</td>
</tr>
<tr>
<td>split_if P(if Q then x else y) = ((Q --&gt; P x) &amp; (~Q --&gt; P y))</td>
<td>Conditional</td>
</tr>
</tbody>
</table>

Figure 2.6: More derived rules
2.3 A formulation of set theory

Historically, higher-order logic gives a foundation for Russell and Whitehead’s theory of classes. Let us use modern terminology and call them sets, but note that these sets are distinct from those of ZF set theory, and behave more like ZF classes.

- Sets are given by predicates over some type $\sigma$. Types serve to define universes for sets, but type-checking is still significant.
- There is a universal set (for each type). Thus, sets have complements, and may be defined by absolute comprehension.
- Although sets may contain other sets as elements, the containing set must have a more complex type.

Finite unions and intersections have the same behaviour in HOL as they do in ZF. In HOL the intersection of the empty set is well-defined, denoting the universal set for the given type.

2.3.1 Syntax of set theory

HOL’s set theory is called Set. The type $\alpha$ set is essentially the same as $\alpha \Rightarrow \text{bool}$. The new type is defined for clarity and to avoid complications involving function types in unification. The isomorphisms between the two types are declared explicitly. They are very natural: Collect maps $\alpha \Rightarrow \text{bool}$ to $\alpha$ set, while op : maps in the other direction (ignoring argument order).

Figure 2.7 lists the constants, infixes, and syntax translations. Figure 2.8 presents the grammar of the new constructs. Infix operators include union and intersection ($A \cup B$ and $A \cap B$), the subset and membership relations, and the image operator $\Rightarrow$. Note that $a \neg: b$ is translated to $\neg(a \in b)$.

The $\{a_1, \ldots\}$ notation abbreviates finite sets constructed in the obvious manner using insert and $\{\}$:

$$ \{a, b, c\} \equiv \text{insert } a(\text{insert } b(\text{insert } c\{\})) $$

The set $\{x. \ P[x]\}$ consists of all $x$ (of suitable type) that satisfy $P[x]$, where $P[x]$ is a formula that may contain free occurrences of $x$. This syntax expands to $\text{Collect}(\lambda x. \ P[x])$. It defines sets by absolute comprehension, which is impossible in ZF; the type of $x$ implicitly restricts the comprehension.
CHAPTER 2. HIGHER-ORDER LOGIC

<table>
<thead>
<tr>
<th>name</th>
<th>meta-type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{}</td>
<td>α set</td>
<td>the empty set</td>
</tr>
<tr>
<td>insert</td>
<td>[α, α set] ⇒ α set</td>
<td>insertion of element</td>
</tr>
<tr>
<td>Collect</td>
<td>(α ⇒ bool) ⇒ α set</td>
<td>comprehension</td>
</tr>
<tr>
<td>INTER</td>
<td>[α set, α ⇒ β set] ⇒ β set</td>
<td>intersection over a set</td>
</tr>
<tr>
<td>UNION</td>
<td>[α set, α ⇒ β set] ⇒ β set</td>
<td>union over a set</td>
</tr>
<tr>
<td>Inter</td>
<td>(α set) set ⇒ α set</td>
<td>set of sets intersection</td>
</tr>
<tr>
<td>Union</td>
<td>(α set) set ⇒ α set</td>
<td>set of sets union</td>
</tr>
<tr>
<td>Pow</td>
<td>α set ⇒ (α set) set</td>
<td>powerset</td>
</tr>
<tr>
<td>range</td>
<td>(α ⇒ β) ⇒ β set</td>
<td>range of a function</td>
</tr>
<tr>
<td>Ball</td>
<td>[α set, α ⇒ bool] ⇒ bool</td>
<td>bounded quantifiers</td>
</tr>
</tbody>
</table>

**Constants**

<table>
<thead>
<tr>
<th>symbol</th>
<th>name</th>
<th>meta-type</th>
<th>priority</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INT</td>
<td>INTER1</td>
<td>(α ⇒ β set) ⇒ β set</td>
<td>10</td>
<td>intersection</td>
</tr>
<tr>
<td>UN</td>
<td>UNION1</td>
<td>(α ⇒ β set) ⇒ β set</td>
<td>10</td>
<td>union</td>
</tr>
</tbody>
</table>

**Binders**

<table>
<thead>
<tr>
<th>symbol</th>
<th>meta-type</th>
<th>priority</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>```</td>
<td>[α ⇒ β, α set] ⇒ β set</td>
<td>Left 90</td>
<td>image</td>
</tr>
<tr>
<td>Int</td>
<td>[α set, α set] ⇒ α set</td>
<td>Left 70</td>
<td>intersection (∩)</td>
</tr>
<tr>
<td>Un</td>
<td>[α set, α set] ⇒ α set</td>
<td>Left 65</td>
<td>union (∪)</td>
</tr>
<tr>
<td>:</td>
<td>[α, α set] ⇒ bool</td>
<td>Left 50</td>
<td>membership (∈)</td>
</tr>
<tr>
<td>&lt;=</td>
<td>[α set, α set] ⇒ bool</td>
<td>Left 50</td>
<td>subset (⊆)</td>
</tr>
</tbody>
</table>

**Infixes**

Figure 2.7: Syntax of the theory Set
CHAPTER 2. HIGHER-ORDER LOGIC

<table>
<thead>
<tr>
<th>external</th>
<th>internal</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a \sim b$</td>
<td>$\neg(a : b)$</td>
<td>not in</td>
</tr>
<tr>
<td>${a_1, \ldots}$</td>
<td>insert $a_1 \ldots {}$</td>
<td>finite set</td>
</tr>
<tr>
<td>${x. \ P[x]}$</td>
<td>Collect($\lambda x. P[x]$)</td>
<td>comprehension</td>
</tr>
<tr>
<td>$\text{INT } x:A. B[x]$</td>
<td>$\text{INTER } A \lambda x. B[x]$</td>
<td>intersection</td>
</tr>
<tr>
<td>$\text{UN } x:A. B[x]$</td>
<td>$\text{UNION } A \lambda x. B[x]$</td>
<td>union</td>
</tr>
<tr>
<td>$\text{ALL } x:A. P[x]$ or $! x:A. P[x]$</td>
<td>$\text{Ball } A \lambda x. P[x]$</td>
<td>bounded $\forall$</td>
</tr>
<tr>
<td>$\text{EX } x:A. P[x]$ or $? x:A. P[x]$</td>
<td>$\text{Bex } A \lambda x. P[x]$</td>
<td>bounded $\exists$</td>
</tr>
</tbody>
</table>

**Translations**

\[
\text{term} = \text{other terms...} \\
\{} \\
\{ \text{term} , \text{term}\}^* \} \\
\{ \text{id} . \text{formula} \} \\
\text{term} \sim \text{term} \\
\text{term} \text{Int} \text{term} \\
\text{term} \text{Un} \text{term} \\
\text{INT } \text{id:term} . \text{term} \\
\text{UN } \text{id:term} . \text{term} \\
\text{INT } \text{id id*} . \text{term} \\
\text{UN } \text{id id*} . \text{term}
\]

\[
\text{formula} = \text{other formulae...} \\
\text{term} : \text{term} \\
\text{term} \sim : \text{term} \\
\text{term} \leq \text{term} \\
\text{ALL } \text{id:term} . \text{formula} | ! \text{id:term} . \text{formula} \\
\text{EX } \text{id:term} . \text{formula} | ? \text{id:term} . \text{formula}
\]

**Full Grammar**

Figure 2.8: Syntax of the theory Set (continued)
The set theory defines two **bounded quantifiers**:

\[
\forall x \in A. P[x] \quad \text{abbreviates} \quad \forall x. x \in A \rightarrow P[x]
\]

\[
\exists x \in A. P[x] \quad \text{abbreviates} \quad \exists x. x \in A \land P[x]
\]

The constants \texttt{Ball} and \texttt{Bex} are defined accordingly. Instead of \texttt{Ball} \( A \ P \) and \texttt{Bex} \( A \ P \) we may write \texttt{ALL} \( x : A. \ P[x] \) and \texttt{EX} \( x : A. \ P[x] \). The original notation of Gordon’s HOL system is supported as well: \(!\) and \(?\).

Unions and intersections over sets, namely \( \bigcup_{x \in A} B[x] \) and \( \bigcap_{x \in A} B[x] \), are written \( \text{UN} \: x : A. \: B[x] \) and \( \text{INT} \: x : A. \: B[x] \).

Unions and intersections over types, namely \( \bigcup_x B[x] \) and \( \bigcap_x B[x] \), are written \( \text{UN} \: x. \: B[x] \) and \( \text{INT} \: x. \: B[x] \). They are equivalent to the previous union and intersection operators when \( A \) is the universal set.

The operators \( \bigcup A \) and \( \bigcap A \) act upon sets of sets. They are not binders, but are equal to \( \bigcup_{x \in A} x \) and \( \bigcap_{x \in A} x \), respectively.

### 2.3.2 Axioms and rules of set theory

Figure 2.9 presents the rules of theory \texttt{Set}. The axioms \texttt{mem_Collect_eq} and \texttt{Collect_mem_eq} assert that the functions \texttt{Collect} and \texttt{op :} are isomorphisms. Of course, \texttt{op :} also serves as the membership relation.
CollectI \[| P \ a \ | \implies \ a : \{x. P \ x\}\]
CollectD \[| a : \{x. P \ x\} \ | \implies P \ a\]
CollectE \[| a : \{x. P \ x\}; \ P a \implies W \ | \implies W\]
bballI \[|!!x. x:A \implies P \ x \ | \implies \forall x:A. P \ x\]
bbspec \[|\forall x:A. P \ x; \ x:A \ | \implies P \ x\]
bballE \[|\forall x:A. P \ x; \ P x \implies Q; \ \neg x:A \implies Q \ | \implies Q\]
bbexI \[| P x; \ x:A \ | \implies \exists x:A. P \ x\]
bbexCI \[|\exists x:A. \neg P x \implies P a; \ a:A \ | \implies \exists x:A. P \ x\]
bbexE \[|\exists x:A. P \ x; \ \forall x. [| x:A; P x \ | \implies Q \ | \implies Q\]

Comprehension and Bounded quantifiers

subsetI \[|\exists x:A \implies x:B) \implies A \subseteq B\]
subsetD \[| A \subseteq B; \ c:A \ | \implies c:B\]
subsetCE \[| A \subseteq B; \ \neg (c:A) \implies P; \ c:B \implies P \ | \implies P\]
subset_refl \[A \subseteq A\]
subset_trans \[| A=B; \ B=B \ | \implies A=C\]
equalityI \[| A \subseteq B; \ B \subseteq A \ | \implies A = B\]
equalityD1 \[A = B \implies A=B\]
equalityD2 \[A = B \implies B=A\]
equalityE \[| A = B; \ [| A=B; \ B=A \ | \implies P \ | \implies P\]
equalityCE \[| A = B; \ [| c:A; c:B \ | \implies P; \ [\neg c:A; \ \neg c:B \ | \implies P \ | \implies P\]

The subset and equality relations

Figure 2.10: Derived rules for set theory
emptyE  a : {} ==> P

insertI1  a : insert a B
insertI2  a : B ==> a : insert b B
insertE  [ | a : insert b A; a=b ==> P; a:A ==> P ] ==> P

ComplI  [ | c:A ==> False ] ==> c : -A
ComplD  [ | c : -A | ] ==> ~ c:A

UnI1  c:A ==> c : A Un B
UnI2  c:B ==> c : A Un B
UnCI  (~c:B ==> c:A) ==> c : A Un B
UnE  [ | c : A Un B; c:A ==> P; c:B ==> P ] ==> P

IntI  [ | c:A; c:B | ] ==> c : A Int B
IntD1  c : A Int B ==> c:A
IntD2  c : A Int B ==> c:B
IntE  [ | c : A Int B; [ | c:A; c:B | ] ==> P ] ==> P

UN_I  [ | a:A; b: B a | ] ==> b: (UN x:A. B x)
UN_E  [ | b: (UN x:A. B x); !!x.[ | x:A; b:B x | ] ==> R | ] ==> R

INT_I  (!!x. x:A ==> b : B x) ==> b : (INT x:A. B x)
INT_D  [ | b: (INT x:A. B x); a:A | ] ==> b: B a
INT_E  [ | b: (INT x:A. B x); b: B a ==> R; ~ a:A ==> R | ] ==> R

UnionI  [ | X:C; A:X | ] ==> A : Union C

InterI  [ | !!X. X:C ==> A:X | ] ==> A : Inter C
InterD  [ | A : Inter C; X:C | ] ==> A:X
InterE  [ | A : Inter C; A:X ==> R; ~ X:C ==> R | ] ==> R

PowI  A<=B ==> A: Pow B
PowD  A: Pow B ==> A<=B

imageI  [ | x:A | ] ==> f x : f``A
imageE  [ | b : f``A; !!x.[ | b=f x; x:A | ] ==> P | ] ==> P

rangeI  f x : range f
rangeE  [ | b : range f; !!x.[ | b=f x | ] ==> P | ] ==> P

Figure 2.11: Further derived rules for set theory
CHAPTER 2. HIGHER-ORDER LOGIC

All the other axioms are definitions. They include the empty set, bounded quantifiers, unions, intersections, complements and the subset relation. They also include straightforward constructions on functions: image (``) and range.

Figures 2.10 and 2.11 present derived rules. Most are obvious and resemble rules of Isabelle’s ZF set theory. Certain rules, such as subsetCE, bexCI and UnCI, are designed for classical reasoning; the rules subsetD, bexI, Un1 and Un2 are not strictly necessary but yield more natural proofs. Similarly, equalityCE supports classical reasoning about extensionality, after the fashion of iffCE. See the file HOL/Set.ML for proofs pertaining to set theory.

Figure 2.12 presents lattice properties of the subset relation. Unions form least upper bounds; non-empty intersections form greatest lower bounds. Reasoning directly about subsets often yields clearer proofs than reasoning about the membership relation. See the file HOL/subset.ML.

Figure 2.13 presents many common set equalities. They include commutative, associative and distributive laws involving unions, intersections and complements. For a complete listing see the file HOL/equalities.ML.

! Blast_tac proves many set-theoretic theorems automatically. Hence you seldom need to refer to the theorems above.

2.3.3 Properties of functions

Figure 2.14 presents a theory of simple properties of functions. Note that inv f uses Hilbert’s ε to yield an inverse of f. See the file HOL/Fun.ML for a complete listing of the derived rules. Reasoning about function composition
CHAPTER 2. HIGHER-ORDER LOGIC

Int_absorb \quad A \, \text{Int} \, A = A
Int_commute \quad A \, \text{Int} \, B = B \, \text{Int} \, A
Int_assoc \quad (A \, \text{Int} \, B) \, \text{Int} \, C = A \, \text{Int} \, (B \, \text{Int} \, C)
Int_Un_distrib \quad (A \, \text{Un} \, B) \, \text{Int} \, C = (A \, \text{Int} \, C) \, \text{Un} \, (B \, \text{Int} \, C)

Un_absorb \quad A \, \text{Un} \, A = A
Un_commute \quad A \, \text{Un} \, B = B \, \text{Un} \, A
Un_assoc \quad (A \, \text{Un} \, B) \, \text{Un} \, C = A \, \text{Un} \, (B \, \text{Un} \, C)
Un_Int_distrib \quad (A \, \text{Int} \, B) \, \text{Un} \, C = (A \, \text{Un} \, C) \, \text{Int} \, (B \, \text{Un} \, C)

Compl_disjoint \quad A \, \text{Int} \, (-A) = \{x. \text{False}\}
Compl_partition \quad A \, \text{Un} \, (-A) = \{x. \text{True}\}
double_complement \quad -(A) = A
Compl_Un \quad -(A \, \text{Un} \, B) = (-A) \, \text{Int} \, (-B)
Compl_Int \quad -(A \, \text{Int} \, B) = (-A) \, \text{Un} \, (-B)

Union_Un_distrib \quad \text{Union}(A \, \text{Un} \, B) = (\text{Union} A) \, \text{Un} \, (\text{Union} B)
Int_Union \quad A \, \text{Int} \, (\text{Union} B) = (\text{UN} C:B. \, A \, \text{Int} \, C)

Inter_Un_distrib \quad \text{Inter}(A \, \text{Un} \, B) = (\text{Inter} A) \, \text{Int} \, (\text{Inter} B)
Un_Inter \quad A \, \text{Un} \, (\text{Inter} B) = (\text{INT} C:B. \, A \, \text{Un} \, C)

Figure 2.13: Set equalities

<table>
<thead>
<tr>
<th>name</th>
<th>meta-type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inj</td>
<td>((\alpha \Rightarrow \beta) \Rightarrow \text{bool})</td>
<td>injective/surjective</td>
</tr>
<tr>
<td>surj</td>
<td>([\alpha \Rightarrow \beta, \alpha \text{ set}] \Rightarrow \text{bool})</td>
<td>injective over subset</td>
</tr>
<tr>
<td>inj_on</td>
<td>((\alpha \Rightarrow \beta) \Rightarrow (\beta \Rightarrow \alpha))</td>
<td>inverse function</td>
</tr>
</tbody>
</table>

| inj_def | inj f | \(== ! \ x \, y. \ f \, \text{x=f y ---> x=y}\) |
| surj_def| surj f| \(== ! y. \ ? \ x. \ y=f \ x\) |
| inj_on_def | inj_on f A | \(== !x:A. \ !y:A. \ f \, \text{x=f y ---> x=y}\) |
| inv_def | inv f | \(== \forall y. \ @x. \ f(x)=y\) |

Figure 2.14: Theory Fun
(the operator \( \circ \)) and the predicate \( \text{surj} \) is done simply by expanding the definitions.

There is also a large collection of monotonicity theorems for constructions on sets in the file \( \text{HOL/mono.ML} \).

### 2.4 Simplification and substitution

Simplification tactics such as \texttt{Asm_simp_tac} and \texttt{Full_simp_tac} use the default simpset \( \text{simpset()} \), which works for most purposes. A quite minimal simplification set for higher-order logic is \texttt{HOL_ss}; even more frugal is \texttt{HOL_basic_ss}. Equality (=), which also expresses logical equivalence, may be used for rewriting. See the file \texttt{HOL/simpdata.ML} for a complete listing of the basic simplification rules.

See the \textit{Reference Manual} for details of substitution and simplification.

Reducing \( a = b \land P(a) \) to \( a = b \land P(b) \) is sometimes advantageous. The left part of a conjunction helps in simplifying the right part. This effect is not available by default: it can be slow. It can be obtained by including \texttt{conj_cong} in a simpset, \texttt{addcongs [conj_cong]}.

By default only the condition of an \texttt{if} is simplified but not the \texttt{then} and \texttt{else} parts. Of course the latter are simplified once the condition simplifies to \texttt{True} or \texttt{False}. To ensure full simplification of all parts of a conditional you must remove \texttt{if_weak_cong} from the simpset, \texttt{delcongs [if_weak_cong]}.

If the simplifier cannot use a certain rewrite rule — either because of nontermination or because its left-hand side is too flexible — then you might try \texttt{stac}:

\texttt{stac thm i}, where \( \text{thm} \) is of the form \( \text{lhs} = \text{rhs} \), replaces in subgoal \( i \) instances of \( \text{lhs} \) by corresponding instances of \( \text{rhs} \). In case of multiple instances of \( \text{lhs} \) in subgoal \( i \), backtracking may be necessary to select the desired ones.

If \( \text{thm} \) is a conditional equality, the instantiated condition becomes an additional (first) subgoal.

HOL provides the tactic \texttt{hyp_subst_tac}, which substitutes for an equality throughout a subgoal and its hypotheses. This tactic uses HOL’s general substitution rule.
2.4.1 Case splitting

HOL also provides convenient means for case splitting during rewriting. Goals containing a subterm of the form if \( b \) then \( \ldots \) else \( \ldots \) often require a case distinction on \( b \). This is expressed by the theorem split_if:

\[
P(if \ ?b \ then \ ?x \ else \ ?y) = ((?b \rightarrow \ ?P(?x)) \land (\neg ?b \rightarrow \ ?P(?y)))
\]  

\((\ast)\)

For example, a simple instance of \((\ast)\) is

\[x \in (if \ x \in A \ then \ A \ else \ \{x\}) = ((x \in A \rightarrow x \in A) \land (x \notin A \rightarrow x \in \{x\}))\]

Because \((\ast)\) is too general as a rewrite rule for the simplifier (the left-hand side is not a higher-order pattern in the sense of the Reference Manual), there is a special infix function addsplits of type simpset * thm list -> simpset (analogous to addsimps) that adds rules such as \((\ast)\) to a simpset, as in

\[
\text{by(simp_tac (simpset() addsplits [split_if]) 1)};
\]

The effect is that after each round of simplification, one occurrence of if is split according to split_if, until all occurrences of if have been eliminated.

It turns out that using split_if is almost always the right thing to do. Hence split_if is already included in the default simpset. If you want to delete it from a simpset, use delsplits, which is the inverse of addsplits:

\[
\text{by(simp_tac (simpset() delsplits [split_if]) 1)};
\]

In general, addsplits accepts rules of the form

\[
P(c \ ?x_1 \ldots \ ?x_n) = rhs
\]

where \( c \) is a constant and \( rhs \) is arbitrary. Note that \((\ast)\) is of the right form because internally the left-hand side is \( ?P(\text{If } ?b \ ?x \ ?y) \). Important further examples are splitting rules for case expressions (see §2.5.4 and §2.6.1).

Analogous to Addsimps and Delsimps, there are also imperative versions of addsplits and delsplits

\[
\text{Addplits: thm list -> unit}
\]

\[
\text{Delsplits: thm list -> unit}
\]

for adding splitting rules to, and deleting them from the current simpset.

2.5 Types

This section describes HOL’s basic predefined types (\( \alpha \times \beta \), \( \alpha + \beta \), nat and \( \alpha \text{ list} \)) and ways for introducing new types in general. The most important type construction, the datatype, is treated separately in §2.6.
2.5.1 Product and sum types

<table>
<thead>
<tr>
<th>symbol</th>
<th>meta-type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pair</td>
<td>$[\alpha, \beta] \Rightarrow \alpha \times \beta$</td>
<td>ordered pairs $(a, b)$</td>
</tr>
<tr>
<td>fst</td>
<td>$\alpha \times \beta \Rightarrow \alpha$</td>
<td>first projection</td>
</tr>
<tr>
<td>snd</td>
<td>$\alpha \times \beta \Rightarrow \beta$</td>
<td>second projection</td>
</tr>
<tr>
<td>split</td>
<td>$[[\alpha, \beta] \Rightarrow \gamma, \alpha \times \beta] \Rightarrow \gamma$</td>
<td>generalized projection</td>
</tr>
<tr>
<td>Sigma</td>
<td>$[\alpha \text{ set}, \alpha \Rightarrow \beta \text{ set}] \Rightarrow (\alpha \times \beta)\text{ set}$</td>
<td>general sum of sets</td>
</tr>
</tbody>
</table>

**Sigma_def**  
$\Sigma A B := \text{UN } x:A. \ \text{UN } y:B. \ {(x,y)}$

**prod.inject**  
$((a,b) = (a',b')) = (a=a' \ & \ b=b')$

**Pair_inject**  
$[| (a, b) = (a',b'); \ [| a=a'; b=b' |] ==> R |] ==> R$

**prod.exhaust**  
$[| !!x y. \ p = (x,y) ==> Q |] ==> Q$

**fst_conv**  
$fst (a,b) = a$

**snd_conv**  
$snd (a,b) = b$

**surjective_pairing**  
$p = (fst p, snd p)$

**split**  
$\text{case_prod c (a,b) = c a b}$

**prod.split**  
$R(\text{case_prod c p}) = (! x y. \ p = (x,y) --> R(c x y))$

**SigmaI**  
$[| a:A; b:B a |] ==> (a,b) : \Sigma A B$

**SigmaE**  
$[| c:Sigma A B; !!x y.[| x:A; y:B x; c=(x,y) |] ==> P |] ==> P$

Figure 2.15: Type $\alpha \times \beta$

Theory Prod (Fig. 2.15) defines the product type $\alpha \times \beta$, with the ordered pair syntax $(a, b)$. General tuples are simulated by pairs nested to the right:

<table>
<thead>
<tr>
<th>external</th>
<th>internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\tau_1 \times \ldots \times \tau_n$</td>
<td>$\tau_1 \times (\ldots (\tau_{n-1} \times \tau_n) \ldots)$</td>
</tr>
<tr>
<td>$(t_1, \ldots, t_n)$</td>
<td>$(t_1, (\ldots, (t_{n-1}, t_n) \ldots)$</td>
</tr>
</tbody>
</table>

In addition, it is possible to use tuples as patterns in abstractions:

$\%(x,y). \ t \quad \text{stands for} \quad \text{split}(%(x,y). \ t)$

Nested patterns are also supported. They are translated stepwise:

$\%(x,y,z). \ t \quad \leadsto \quad \%(x, (y,z)). \ t$

$\leadsto \quad \text{case_prod}(%(x,%. \%(y,z). \ t))$

$\leadsto \quad \text{case_prod}(%(x. \text{ case_prod}(%(y z. \ t)))$

The reverse translation is performed upon printing.
The translation between patterns and split is performed automatically by the parser and printer. Thus the internal and external form of a term may differ, which can affects proofs. For example the term $(\%(x,y). (y,x))(a,b)$ requires the theorem split (which is in the default simpset) to rewrite to $(b,a)$.

In addition to explicit λ-abstractions, patterns can be used in any variable binding construct which is internally described by a λ-abstraction. Some important examples are

**Let:** let pattern = t in u  
**Quantifiers:** ALL pattern: A. P  
**Choice:** SOME pattern. P  
**Set operations:** UN pattern: A. B  
**Sets:** {pattern. P}

There is a simple tactic which supports reasoning about patterns:

\begin{align*}
\text{split-all-tac } i & \text{ replaces in subgoal } i \text{ all } !!\text{-quantified variables of product type by individual variables for each component. A simple example:}\nonumber
\end{align*}

1. \( !!p. (\%(x,y,z). (x, y, z)) p = p \)
   by(split-all-tac 1);
1. \( !!x xa ya. (\%(x,y,z). (x, y, z)) (x, xa, ya) = (x, xa, ya) \)

Theory **Prod** also introduces the degenerate product type **unit** which contains only a single element named () with the property

\begin{align*}
\text{unit_eq} & \quad u = ()
\end{align*}

Theory **Sum** (Fig. 2.16) defines the sum type \( \alpha + \beta \) which associates to the right and has a lower priority than \( \ast \): \( \tau_1 + \tau_2 + \tau_3 \ast \tau_4 \) means \( \tau_1 + (\tau_2 + (\tau_3 \ast \tau_4)) \).

The definition of products and sums in terms of existing types is not shown. The constructions are fairly standard and can be found in the respective theory files. Although the sum and product types are constructed manually for foundational reasons, they are represented as actual datatypes later.
2.5.2 The type of natural numbers, \textit{nat}

The theory \texttt{Nat} defines the natural numbers in a roundabout but traditional way. The axiom of infinity postulates a type \textit{ind} of individuals, which is non-empty and closed under an injective operation. The natural numbers are inductively generated by choosing an arbitrary individual for 0 and using the injective operation to take successors. This is a least fixedpoint construction.

Type \textit{nat} is an instance of class \texttt{ord}, which makes the overloaded functions of this class (especially < and \texttt{<=}, but also \texttt{min}, \texttt{max} and \texttt{LEAST}) available on \textit{nat}. Theory \texttt{Nat} also shows that \texttt{<=} is a linear order, so \textit{nat} is also an instance of class \texttt{linorder}.

Theory \texttt{NatArith} develops arithmetic on the natural numbers. It defines addition, multiplication and subtraction. Theory \texttt{Divides} defines division, remainder and the “divides” relation. The numerous theorems proved include commutative, associative, distributive, identity and cancellation laws. See Figs. 2.17 and 2.18. The recursion equations for the operators +, - and * on \textit{nat} are part of the default simpset.

Functions on \textit{nat} can be defined by primitive or well-founded recursion; see §2.7. A simple example is addition. Here, \texttt{op +} is the name of the infix operator +, following the standard convention.
CHAPTER 2. HIGHER-ORDER LOGIC

<table>
<thead>
<tr>
<th>symbol</th>
<th>meta-type</th>
<th>priority</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$\alpha$</td>
<td></td>
<td>zero</td>
</tr>
<tr>
<td>Suc</td>
<td>$nat \Rightarrow nat$</td>
<td></td>
<td>successor function</td>
</tr>
<tr>
<td>$\ast$</td>
<td>$[\alpha, \alpha] \Rightarrow \alpha$</td>
<td>Left 70</td>
<td>multiplication</td>
</tr>
<tr>
<td>$\div$</td>
<td>$[\alpha, \alpha] \Rightarrow \alpha$</td>
<td>Left 70</td>
<td>division</td>
</tr>
<tr>
<td>$\mod$</td>
<td>$[\alpha, \alpha] \Rightarrow \alpha$</td>
<td>Left 70</td>
<td>modulus</td>
</tr>
<tr>
<td>$\dvd$</td>
<td>$[\alpha, \alpha] \Rightarrow bool$</td>
<td>Left 70</td>
<td>“divides” relation</td>
</tr>
<tr>
<td>+</td>
<td>$[\alpha, \alpha] \Rightarrow \alpha$</td>
<td>Left 65</td>
<td>addition</td>
</tr>
<tr>
<td>-</td>
<td>$[\alpha, \alpha] \Rightarrow \alpha$</td>
<td>Left 65</td>
<td>subtraction</td>
</tr>
</tbody>
</table>

**Constants and infixes**

\[
\text{nat\_induct} \quad \text{[| } P \; 0; \; !\!n. \; P \; n \Longrightarrow P(\text{Suc} \; n) \; |] \; \Longrightarrow \; P \; n
\]

\[
\text{Suc\_not\_Zero} \quad \text{Suc} \; m \; = \; 0
\]

\[
\text{inj\_Suc} \quad \text{inj} \; \text{Suc}
\]

\[
\text{n\_not\_Suc\_n} \quad \text{n\_=}\text{Suc} \; n
\]

**Basic properties**

Figure 2.17: The type of natural numbers, $nat$

\[
\begin{align*}
0+n & = n \\
(Suc \; m)+n & = Suc(m+n)
\end{align*}
\]

\[
\begin{align*}
m-0 & = m \\
0-n & = n \\
Suc(m)-Suc(n) & = m-n
\end{align*}
\]

\[
\begin{align*}
0*n & = 0 \\
Suc(m)*n & = n \; + \; m*n
\end{align*}
\]

**mod\_less** \quad \text{m} \; < \; \text{n} \; \Longrightarrow \; \text{m} \; \text{mod} \; \text{n} \; = \; \text{m}

\[
\text{mod\_geq} \quad \text{[| } 0\; < \; \text{n} ; \; \neg m \; < \; \text{n} \; |] \; \Longrightarrow \; \text{m mod} \; \text{n} \; = \; (m-n) \; \text{mod} \; \text{n}
\]

**div\_less** \quad \text{m} \; < \; \text{n} \; \Longrightarrow \; \text{m} \; \text{div} \; \text{n} \; = \; 0

\[
\text{div\_geq} \quad \text{[| } 0\; < \; \text{n} ; \; \neg m \; < \; \text{n} \; |] \; \Longrightarrow \; \text{m div} \; \text{n} \; = \; Suc((m-n) \; \text{div} \; \text{n})
\]

Figure 2.18: Recursion equations for the arithmetic operators
There is also a \texttt{case} construct of the form
\begin{verbatim}
    case \_ of \_ => \_ \mid \_ => \_
\end{verbatim}
Note that Isabelle insists on precisely this format; you may not even change the order of the two cases. Both \texttt{primrec} and \texttt{case} are realized by a recursion operator \texttt{rec_nat}, which is available because \texttt{nat} is represented as a datatype.

Tactic \texttt{induct_tac "n" \_} performs induction on variable \texttt{n} in subgoal \texttt{\_}. There is also the derived theorem \texttt{less_induct}:\[
[| \mbox{!!n. [| !!m. m<n --> P m |] ==> P n |}] ==> P n
\]

2.5.3 Numerical types and numerical reasoning

The integers (type \texttt{int}) are also available in HOL, and the reals (type \texttt{real}) are available in the logic image \texttt{HOL-Complex}. They support the expected operations of addition (+), subtraction (-) and multiplication (*), and much else. Type \texttt{int} provides the \texttt{div} and \texttt{mod} operators, while type \texttt{real} provides real division and other operations. Both types belong to class \texttt{linorder}, so they inherit the relational operators and all the usual properties of linear orderings. For full details, please survey the theories in subdirectories \texttt{Integ}, \texttt{Real}, and \texttt{Complex}.

All three numeric types admit numerals of the form \texttt{sd\ldots d}, where \texttt{s} is an optional minus sign and \texttt{d\ldots d} is a string of digits. Numerals are represented internally by a datatype for binary notation, which allows numerical calculations to be performed by rewriting. For example, the integer division of \texttt{54342339} by \texttt{3452} takes about five seconds. By default, the simplifier cancels like terms on the opposite sites of relational operators (reducing \texttt{z+x<x+y} to \texttt{z<y}, for instance. The simplifier also collects like terms, replacing \texttt{x+y+x*3} by \texttt{4*x+y}.

Sometimes numerals are not wanted, because for example \texttt{n+3} does not match a pattern of the form \texttt{Suc \_ k}. You can re-arrange the form of an arithmetic expression by proving (via \texttt{subgoal_tac}) a lemma such as \texttt{n+3 = Suc (Suc (Suc n))}. As an alternative, you can disable the fancier simplifications by using a basic simpset such as \texttt{HOL_ss} rather than the default one, \texttt{simpset()}.

Reasoning about arithmetic inequalities can be tedious. Fortunately, HOL provides a decision procedure for \textit{linear arithmetic}: formulae involving addition and subtraction. The simplifier invokes a weak version of this
decision procedure automatically. If this is not sufficient, you can invoke the
full procedure Lin_Arith.tac explicitly. It copes with arbitrary formulae
involving $=$, $<$, $\leq$, $+$, $-$, $\text{Suc}$, $\text{min}$, $\text{max}$ and numerical constants. Other sub-
terms are treated as atomic, while subformulae not involving numerical types
are ignored. Quantified subformulae are ignored unless they are positive uni-
versal or negative existential. The running time is exponential in the number
of occurrences of $\text{min}$, $\text{max}$, and $-$ because they require case distinctions. If
$k$ is a numeral, then $\text{div } k$, $\text{mod } k$ and $k \text{ dvd}$ are also supported. The for-
ter two are eliminated by case distinctions, again blowing up the running
time. If the formula involves explicit quantifiers, Lin_Arith.tac may take
super-exponential time and space.

If Lin_Arith.tac fails, try to find relevant arithmetic results in the li-
brary. The theories Nat and NatArith contain theorems about $<$, $\leq$, $+$, $-$
and $\times$. Theory Divides contains theorems about $\text{div}$ and $\text{mod}$. Use Proof
General’s find button (or other search facilities) to locate them.

### 2.5.4 The type constructor for lists, list

Figure 2.19 presents the theory List: the basic list operations with their
types and syntax. Type $\alpha$ list is defined as a datatype with the constructors
$[]$ and $\#$. As a result the generic structural induction and case analysis
tactics induct_tac and cases_tac also become available for lists. A case
construct of the form

\[
\text{case } e \text{ of } [] \Rightarrow a \mid x\text{#xs} \Rightarrow b
\]

is defined by translation. For details see §2.6. There is also a case splitting
rule list.split

\[
P(\text{case } e \text{ of } [] \Rightarrow a \mid x\text{#xs} \Rightarrow f x xs) = \\
((e = [] \rightarrow P(a)) \land (\forall x xs. e = x\text{#xs} \rightarrow P(f x xs)))
\]

which can be fed to addsplits just like split_if (see §2.4.1).

List provides a basic library of list processing functions defined by prim-
itive recursion. The recursion equations are shown in Figs. 2.20 and 2.21.

### 2.6 Datatype definitions

Inductive datatypes, similar to those of ML, frequently appear in applica-
tions of Isabelle/HOL. In principle, such types could be defined by hand
via typedef, but this would be far too tedious. The datatype definition
### Constants and Infixes

<table>
<thead>
<tr>
<th>symbol</th>
<th>meta-type</th>
<th>priority</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[]</td>
<td>α list</td>
<td></td>
<td>empty list</td>
</tr>
<tr>
<td>#</td>
<td>[α, α list] ⇒ α list</td>
<td>Right 65</td>
<td>list constructor</td>
</tr>
<tr>
<td>null</td>
<td>α list ⇒ bool</td>
<td></td>
<td>emptiness test</td>
</tr>
<tr>
<td>hd</td>
<td>α list ⇒ α</td>
<td></td>
<td>head</td>
</tr>
<tr>
<td>tl</td>
<td>α list ⇒ α list</td>
<td></td>
<td>tail</td>
</tr>
<tr>
<td>last</td>
<td>α list ⇒ α</td>
<td></td>
<td>last element</td>
</tr>
<tr>
<td>butlast</td>
<td>α list ⇒ α list</td>
<td></td>
<td>drop last element</td>
</tr>
<tr>
<td>@</td>
<td>[α list, α list] ⇒ α list</td>
<td>Left 65</td>
<td>append</td>
</tr>
<tr>
<td>map</td>
<td>(α ⇒ β) ⇒ (α list ⇒ β list)</td>
<td></td>
<td>apply to all</td>
</tr>
<tr>
<td>filter</td>
<td>(α ⇒ bool) ⇒ (α list ⇒ α list)</td>
<td></td>
<td>filter functional</td>
</tr>
<tr>
<td>set</td>
<td>α list ⇒ α set</td>
<td></td>
<td>elements</td>
</tr>
<tr>
<td>mem</td>
<td>α ⇒ α list ⇒ bool</td>
<td>Left 55</td>
<td>membership</td>
</tr>
<tr>
<td>foldl</td>
<td>(β ⇒ α) ⇒ β ⇒ α list ⇒ β</td>
<td>iteration</td>
<td></td>
</tr>
<tr>
<td>concat</td>
<td>(α list)list ⇒ α list</td>
<td></td>
<td>concatenation</td>
</tr>
<tr>
<td>rev</td>
<td>α list ⇒ α list</td>
<td></td>
<td>reverse</td>
</tr>
<tr>
<td>length</td>
<td>α list ⇒ nat</td>
<td></td>
<td>length</td>
</tr>
<tr>
<td>!</td>
<td>α list ⇒ nat ⇒ α</td>
<td>Left 100</td>
<td>indexing</td>
</tr>
<tr>
<td>take, drop</td>
<td>nat ⇒ α list ⇒ α list</td>
<td>take/drop a prefix</td>
<td></td>
</tr>
<tr>
<td>takeWhile,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dropWhile</td>
<td>(α ⇒ bool) ⇒ α list ⇒ α list</td>
<td>take/drop a prefix</td>
<td></td>
</tr>
</tbody>
</table>

### Translations

**Figure 2.19:** The theory **List**
null [] = True
null (x#xs) = False

hd (x#xs) = x
tl (x#xs) = xs
tl [] = []

[] @ ys = ys
(x#xs) @ ys = x # xs @ ys

set [] = {}
set (x#xs) = insert x (set xs)

x mem [] = False
x mem (y#ys) = (if y=x then True else x mem ys)

concat([]) = []
concat(x#xs) = x @ concat(xs)

rev([]) = []
rev(x#xs) = rev(xs) @ [x]

length([]) = 0
length(x#xs) = Suc(length(xs))

xs!0 = hd xs
xs!(Suc n) = (tl xs)!n

Figure 2.20: Simple list processing functions
package of Isabelle/HOL (cf. [1]) automates such chores. It generates an appropriate `typedef` based on a least fixed-point construction, and proves freeness theorems and induction rules, as well as theorems for recursion and case combinators. The user just has to give a simple specification of new inductive types using a notation similar to ML or Haskell.

The current datatype package can handle both mutual and indirect recursion. It also offers to represent existing types as datatypes giving the advantage of a more uniform view on standard theories.

### 2.6.1 Basics

A general `datatype` definition is of the following form:

\[
\text{datatype } (\vec{\alpha}) t_1 = C_1^1 \tau_{1,1}^1 \ldots \tau_{1,m_1}^1 \mid \ldots \mid C_{k_1}^1 \tau_{k_1,1}^1 \ldots \tau_{k_1,m_{k_1}}^1 \\
\vdots \\
\text{and } (\vec{\alpha}) t_n = C_1^n \tau_{1,1}^n \ldots \tau_{1,m_n}^n \mid \ldots \mid C_{k_n}^n \tau_{k_n,1}^n \ldots \tau_{k_n,m_{k_n}}^n
\]

where \( \vec{\alpha} = (\alpha_1, \ldots, \alpha_h) \) is a list of type variables, \( C_i^j \) are distinct constructor names and \( \tau_{i,j}^{i'} \) are admissible types containing at most the type variables \( \alpha_1, \ldots, \alpha_h \). A type \( \tau \) occurring in a `datatype` definition is admissible if and only if
• $\tau$ is non-recursive, i.e. $\tau$ does not contain any of the newly defined type constructors $t_1, \ldots, t_n$, or

• $\tau = (\vec{\alpha})t_j$ where $1 \leq j \leq n$, or

• $\tau = (\tau'_1, \ldots, \tau'_k)t'$, where $t'$ is the type constructor of an already existing datatype and $\tau'_1, \ldots, \tau'_k$ are admissible types.

• $\tau = \sigma \rightarrow \tau'$, where $\tau'$ is an admissible type and $\sigma$ is non-recursive (i.e. the occurrences of the newly defined types are strictly positive).

If some $(\vec{\alpha})t_j'$ occurs in a type $\tau_{j,i}^j$ of the form

$$(\ldots, (\vec{\alpha})t_j' \ldots, \ldots)t'$$

this is called a nested (or indirect) occurrence. A very simple example of a datatype is the type \texttt{list}, which can be defined by

```ml
datatype 'a list = Nil
  | Cons 'a (\texttt{\textquotesingle}a list)
```

Arithmetic expressions \texttt{aexp} and boolean expressions \texttt{bexp} can be modelled by the mutually recursive datatype definition

```ml
datatype 'a aexp = If_then_else ('a bexp) ('a aexp) ('a aexp)
  | Sum ('a aexp) ('a aexp)
  | Diff ('a aexp) ('a aexp)
  | Var 'a
  | Num nat

and 'a bexp = Less ('a aexp) ('a aexp)
  | And ('a bexp) ('a bexp)
  | Or ('a bexp) ('a bexp)
```

The datatype \texttt{term}, which is defined by

```ml
datatype ('a, 'b) term = Var 'a
  | App 'b (((\texttt{\textquotesingle}a, \texttt{\textquotesingle}b) term) list)
```

is an example for a datatype with nested recursion. Using nested recursion involving function spaces, we may also define infinitely branching datatypes, e.g.

```ml
datatype 'a tree = Atom 'a | Branch "nat => 'a tree"
```

Types in HOL must be non-empty. Each of the new datatypes $(\vec{\alpha})t_j$ with $1 \leq j \leq n$ is non-empty if and only if it has a constructor $C_j^{i}$ with the following property: for all argument types $\tau_{i,i}^j$ of the form $(\vec{\alpha})t_j'$ the datatype $(\vec{\alpha})t_j'$ is non-empty.
CHAPTER 2. HIGHER-ORDER LOGIC

If there are no nested occurrences of the newly defined datatypes, obviously at least one of the newly defined datatypes \((\vec{\alpha})t_j\) must have a constructor \(C^j_i\) without recursive arguments, a base case, to ensure that the new types are non-empty. If there are nested occurrences, a datatype can even be non-empty without having a base case itself. Since list is a non-empty datatype, datatype \(t = C (t \text{ list})\) is non-empty as well.

Freeness of the constructors

The datatype constructors are automatically defined as functions of their respective type:

\[
C^j_i : \tau_{i,1}^j, \ldots, \tau_{i,m_i}^j \Rightarrow (\alpha_1, \ldots, \alpha_h) t_j
\]

These functions have certain freeness properties. They construct distinct values:

\[
C^j_i x_1 \ldots x_{m_i} \neq C^j_{i'} y_1 \ldots y_{m_{i'}} \quad \text{for all } i \neq i'.
\]

The constructor functions are injective:

\[
(C^j_i x_1 \ldots x_{m_i} = C^j_{i'} y_1 \ldots y_{m_{i'}}) = (x_1 = y_1 \land \ldots \land x_{m_i} = y_{m_{i'}})
\]

Since the number of distinctness inequalities is quadratic in the number of constructors, the datatype package avoids proving them separately if there are too many constructors. Instead, specific inequalities are proved by a suitable simplification procedure on demand.3

---

3This procedure, which is already part of the default simpset, may be referred to by the ML identifier DatatypePackage.distinct_simproc.
CHAPTER 2. HIGHER-ORDER LOGIC

Structural induction

The datatype package also provides structural induction rules. For datatypes without nested recursion, this is of the following form:

\[ \forall x_1 \ldots x_{m_1} \cdot \left[ P_{s_1^1} x_1^1 \ldots P_{s_1^m} x_1^m \right] \implies P_1 \left( C_1^1 x_1 \ldots x_{m_1} \right) \]

\[ \vdots \]

\[ \forall x_1 \ldots x_{m_{k_1}} \cdot \left[ P_{s_{k_1}^1} x_{k_1}^1 \ldots P_{s_{k_1}^m} x_{k_1}^m \right] \implies P_1 \left( C_{k_1}^1 x_1 \ldots x_{m_{k_1}} \right) \]

\[ \vdots \]

\[ \forall x_1 \ldots x_{m_n} \cdot \left[ P_{s_n^1} x_{n}^1 \ldots P_{s_n^m} x_{n}^m \right] \implies P_n \left( C_n^1 x_1 \ldots x_{m_n} \right) \]

\[ \vdots \]

\[ \forall x_1 \ldots x_{m_{k_n}} \cdot \left[ P_{s_{k_n}^1} x_{k_n}^1 \ldots P_{s_{k_n}^m} x_{k_n}^m \right] \implies P_n \left( C_{k_n}^1 x_1 \ldots x_{m_{k_n}} \right) \]

where

\[ Rec_i^j := \left\{ \left( r_{i_1}^j, s_{i_1}^j \right), \ldots, \left( r_{i_l}^j, s_{i_l}^j \right) \right\} = \left\{ (i', i'') \mid 1 \leq i' \leq m_{i'} \land 1 \leq i'' \leq n \land \tau_{i', i''} = (\alpha_1, \ldots, \alpha_h) t_{i''} \right\} \]

i.e. the properties \( P_i \) can be assumed for all recursive arguments.

For datatypes with nested recursion, such as the term example from above, things are a bit more complicated. Conceptually, Isabelle/HOL unfolds a definition like

\[
\text{datatype ('a,'b) term} = \text{Var 'a} \\
\hspace{1em} \mid \text{App 'b ((('a, 'b) term) list)}
\]

to an equivalent definition without nesting:

\[
\text{datatype ('a,'b) term} = \text{Var} \\
\hspace{1em} \mid \text{App 'b ((('a, 'b) term) list)}
\]

and \( ('a,'b) \text{ term_list} = \text{Nil} \)

\[ \mid \text{Cons} ('a,'b) \text{ term) ((('a,'b) term_list)} \]

Note however, that the type \( ('a,'b) \text{ term_list} \) and the constructors \text{Nil}' and \text{Cons}' are not really introduced. One can directly work with the original (isomorphic) type \( ('a, 'b) \text{ term) list} \) and its existing constructors \text{Nil}
and Cons. Thus, the structural induction rule for term gets the form
\[
\begin{align*}
\wedge x & . \; P_1 (\text{Var } x) \\
\wedge x_1 \; x_2 & . \; P_2 \; x_2 \implies P_1 (\text{App } x_1 \; x_2) \\
P_2 \; \text{Nil} & \\
\wedge x_1 \; x_2 & . \; [P_1 \; x_1; P_2 \; x_2] \implies P_2 (\text{Cons } x_1 \; x_2)
\end{align*}
\]

\[P_1 \; x_1 \wedge P_2 \; x_2\]

Note that there are two predicates \(P_1\) and \(P_2\), one for the type \((a, b)\) term and one for the type \((a, b)\) list.

For a datatype with function types such as \(a\) tree, the induction rule is of the form
\[
\begin{align*}
\wedge a & . \; P (\text{Atom } a) \\
\wedge ts & . \; (\forall x . \; P (ts \; x)) \implies P (\text{Branch } ts)
\end{align*}
\]

In principle, inductive types are already fully determined by freeness and structural induction. For convenience in applications, the following derived constructions are automatically provided for any datatype.

The case construct

The type comes with an ML-like case-construct:

\[
\text{case } e \text{ of } \begin{cases} 
C_1^j \; x_{1,1} \ldots x_{1,m_1^j} & \Rightarrow e_1 \\
\vdots \\
C_k^j \; x_{k,1} \ldots x_{k,m_k^j} & \Rightarrow e_k 
\end{cases}
\]

where the \(x_{i,j}\) are either identifiers or nested tuple patterns as in §2.5.1.

\!

All constructors must be present, their order is fixed, and nested patterns are not supported (with the exception of tuples). Violating this restriction results in strange error messages.

To perform case distinction on a goal containing a case-construct, the theorem \(t_j\text{.split}\) is provided:

\[
P(t_j\text{.case } f_1 \ldots f_k \; e) = (\forall x_1 \ldots x_{m_i^j} . \; e = C_i^j \; x_1 \ldots x_{m_i^j} \implies P(f_i \; x_1 \ldots x_{m_i^j})) \\
\wedge \ldots \wedge \\
(\forall x_1 \ldots x_{m_j^j} . \; e = C_k^j \; x_1 \ldots x_{m_j^j} \implies P(f_k \; x_1 \ldots x_{m_j^j}))
\]

where \(t_j\text{.case}\) is the internal name of the case-construct. This theorem can be added to a simpset via addsplits (see §2.4.1).
Case splitting on assumption works as well, by using the rule \( t_j.\text{split_asm} \) in the same manner. Both rules are available under \( t_j.\text{splits} \) (this name is not bound in ML, though).

By default only the selector expression (\( e \) above) in a case-construct is simplified, in analogy with if (see page 22). Only if that reduces to a constructor is one of the arms of the case-construct exposed and simplified. To ensure full simplification of all parts of a case-construct for datatype \( t \), remove \( t.\text{case_weak_cong} \) from the simpset, for example by \texttt{delcongs [thm "t.case_cong_weak"]}.

The function \texttt{size}

Theory \texttt{NatArith} declares a generic function \texttt{size} of type \( \alpha \Rightarrow \text{nat} \). Each datatype defines a particular instance of \texttt{size} by overloading according to the following scheme:

\[
\text{size}(C^{i_j}_{i_1} x_1 \ldots x_{m_j}) = \begin{cases} 
0 & \text{if } \text{Rec}^{i_j}_{i_1} = \emptyset \\
1 + \sum_{h=1}^{l_j} \text{size } x_{r_{i_1, h}} & \text{if } \text{Rec}^{i_j}_{i_1} = \{ (r_{i_1, 1}, s_{i, 1}), \ldots, (r_{i_1, l_j}, s_{i, l_j}) \}
\end{cases}
\]

where \( \text{Rec}^{i_j}_{i_1} \) is defined above. Viewing datatypes as generalised trees, the size of a leaf is 0 and the size of a node is the sum of the sizes of its subtrees + 1.

2.6.2 Defining datatypes

The theory syntax for datatype definitions is given in the Isabelle/Isar reference manual. In order to be well-formed, a datatype definition has to obey the rules stated in the previous section. As a result the theory is extended with the new types, the constructors, and the theorems listed in the previous section.

Most of the theorems about datatypes become part of the default simpset and you never need to see them again because the simplifier applies them automatically. Only induction or case distinction are usually invoked by hand.

\texttt{induct_tac "x" i} applies structural induction on variable \( x \) to subgoal \( i \), provided the type of \( x \) is a datatype.

\texttt{induct_tac "x_1 \ldots x_n" i} applies simultaneous structural induction on the variables \( x_1, \ldots, x_n \) to subgoal \( i \). This is the canonical way to prove properties of mutually recursive datatypes such as \texttt{aexp} and \texttt{bexp}, or datatypes with nested recursion such as \texttt{term}. 
In some cases, induction is overkill and a case distinction over all constructors of the datatype suffices.

\texttt{case_tac \"u\" i} performs a case analysis for the term \( u \) whose type must be a datatype. If the datatype has \( k_j \) constructors \( C_{i_1}^j, \ldots C_{i_k}^j \), subgoal \( i \) is replaced by \( k_j \) new subgoals which contain the additional assumption \( u = C_{i'}^j x_1 \ldots x_{m_{i'}}^j \) for \( i' = 1, \ldots, k_j \).

Note that induction is only allowed on free variables that should not occur among the premises of the subgoal. Case distinction applies to arbitrary terms.

For the technically minded, we exhibit some more details. Processing the theory file produces an ML structure which, in addition to the usual components, contains a structure named \( t \) for each datatype \( t \) defined in the file. Each structure \( t \) contains the following elements:

\begin{itemize}
  \item \texttt{val distinct : thm list}
  \item \texttt{val inject : thm list}
  \item \texttt{val induct : thm}
  \item \texttt{val exhaust : thm}
  \item \texttt{val cases : thm list}
  \item \texttt{val split : thm}
  \item \texttt{val split_asm : thm}
  \item \texttt{val recs : thm list}
  \item \texttt{val size : thm list}
  \item \texttt{val simps : thm list}
\end{itemize}

\texttt{distinct}, \texttt{inject}, \texttt{induct}, \texttt{size} and \texttt{split} contain the theorems described above. For user convenience, \texttt{distinct} contains inequalities in both directions. The reduction rules of the case-construct are in \texttt{cases}. All theorems from \texttt{distinct}, \texttt{inject} and \texttt{cases} are combined in \texttt{simps}. In case of mutually recursive datatypes, \texttt{recs}, \texttt{size}, \texttt{induct} and \texttt{simps} are contained in a separate structure named \( t_1 \ldots t_n \).

\section{Old-style recursive function definitions}

Old-style recursive definitions via \texttt{recdef} requires that you supply a well-founded relation that governs the recursion. Recursive calls are only allowed if they make the argument decrease under the relation. Complicated recursion forms, such as nested recursion, can be dealt with. Termination can even be proved at a later time, though having unsolved termination conditions around can make work difficult.\footnote{This facility is based on Konrad Slind’s TFL package [16]. Thanks are due to Konrad for implementing TFL and assisting with its installation.}
Using \texttt{recdef}, you can declare functions involving nested recursion and pattern-matching. Recursion need not involve datatypes and there are few syntactic restrictions. Termination is proved by showing that each recursive call makes the argument smaller in a suitable sense, which you specify by supplying a well-founded relation.

Here is a simple example, the Fibonacci function. The first line declares \texttt{fib} to be a constant. The well-founded relation is simply \(<\) (on the natural numbers). Pattern-matching is used here: 1 is a macro for \texttt{Suc 0}.

\begin{verbatim}
consts fib :: "nat => nat"
recdef fib "less_than"
  "fib 0 = 0"
  "fib 1 = 1"
  "fib (Suc(Suc x)) = (fib x + fib (Suc x))"
\end{verbatim}

With \texttt{recdef}, function definitions may be incomplete, and patterns may overlap, as in functional programming. The \texttt{recdef} package disambiguates overlapping patterns by taking the order of rules into account. For missing patterns, the function is defined to return a default value.

The well-founded relation defines a notion of “smaller” for the function’s argument type. The relation \(<\) is \textbf{well-founded} provided it admits no infinitely decreasing chains

\[ \cdots < x_n < \cdots < x_1. \]

If the function’s argument has type \(\tau\), then \(<\) has to be a relation over \(\tau\): it must have type \((\tau \times \tau)\text{set}\).

Proving well-foundedness can be tricky, so Isabelle/HOL provides a collection of operators for building well-founded relations. The package recognises these operators and automatically proves that the constructed relation is well-founded. Here are those operators, in order of importance:

- \textbf{less\_than} is “less than” on the natural numbers. (It has type \((\text{nat} \times \text{nat})\text{set}\), while \(<\) has type \([\text{nat}, \text{nat}] \Rightarrow \text{bool}\).

- \textbf{measure} \(f\), where \(f\) has type \(\tau \Rightarrow \text{nat}\), is the relation \(<\) on type \(\tau\) such that \(x < y\) if and only if \(f(x) < f(y)\). Typically, \(f\) takes the recursive function’s arguments (as a tuple) and returns a result expressed in terms of the function \texttt{size}. It is called a measure function. Recall that \texttt{size} is overloaded and is defined on all datatypes (see §2.6.1).

- \textbf{inv\_image} \(R f\) is a generalisation of \texttt{measure}. It specifies a relation such that \(x < y\) if and only if \(f(x)\) is less than \(f(y)\) according to \(R\), which must itself be a well-founded relation.
• $R_1^{\text{lex}} R_2$ is the lexicographic product of two relations. It is a
relation on pairs and satisfies $(x_1, x_2) < (y_1, y_2)$ if and only if $x_1$ is less
than $y_1$ according to $R_1$ or $x_1 = y_1$ and $x_2$ is less than $y_2$ according
to $R_2$.

• \texttt{finite_psubset} is the proper subset relation on finite sets.

We can use \texttt{measure} to declare Euclid’s algorithm for the greatest com-
mon divisor. The measure function, $\lambda(m, n) . n$, specifies that the recursion
terminates because argument $n$ decreases.

\begin{verbatim}
recdef gcd "measure ((%(m,n). n) ::nat*nat=>nat)"
  "gcd (m, n) = (if n=0 then m else gcd(n, m mod n))"
\end{verbatim}

The general form of a well-founded recursive definition is

\begin{verbatim}
recdef function rel
  congs congruence rules (optional)
  simpset simplification set (optional)
  reduction rules
\end{verbatim}

where

• \texttt{function} is the name of the function, either as an id or a string.

• \texttt{rel} is a HOL expression for the well-founded termination relation.

• \texttt{congruence rules} are required only in highly exceptional circumstances.

• The \texttt{simplification set} is used to prove that the supplied relation is
well-founded. It is also used to prove the termination conditions: assertions that arguments of recursive calls decrease under \texttt{rel}. By
default, simplification uses \texttt{simplset()}, which is sufficient to prove well-
fonndedness for the built-in relations listed above.

• \texttt{reduction rules} specify one or more recursion equations. Each left-hand
side must have the form $f \, t$, where $f$ is the function and $t$ is a tuple of
distinct variables. If more than one equation is present then $f$ is defined
by pattern-matching on components of its argument whose type is a
datatype.

The ML identifier $f$.\texttt{simps} contains the reduction rules as a list of
theorems.

With the definition of \texttt{gcd} shown above, Isabelle/HOL is unable to prove
one termination condition. It remains as a precondition of the recursion
theorems:
The theory HOL/ex/Primes illustrates how to prove termination conditions afterwards. The function Tfl.tgoalw is like the standard function goalw, which sets up a goal to prove, but its argument should be the identifier f.simps and its effect is to set up a proof of the termination conditions:

Tfl.tgoalw thy [] gcd.simps;
Level 0
  ! m n. n ~= 0 --> m mod n < n
  1. ! m n. n ~= 0 --> m mod n < n

This subgoal has a one-step proof using simp_tac. Once the theorem is proved, it can be used to eliminate the termination conditions from elements of gcd.simps. Theory HOL/Subst/Unify is a much more complicated example of this process, where the termination conditions can only be proved by complicated reasoning involving the recursive function itself.

Isabelle/HOL can prove the gcd function’s termination condition automatically if supplied with the right simpset.

recdef gcd "measure ((%(m,n). n) ::nat*nat=>nat)"
  simpset "simpset() addsimps [mod_less_divisor, zero_less_eq]"
  "gcd (m, n) = (if n=0 then m else gcd(n, m mod n))"

If all termination conditions were proved automatically, f.simps is added to the simpset automatically, just as in primrec. The simplification rules corresponding to clause $i$ (where counting starts at 0) are called f.$i$ and can be accessed as thms "f.$i"", which returns a list of theorems. Thus you can, for example, remove specific clauses from the simpset. Note that a single clause may give rise to a set of simplification rules in order to capture the fact that if clauses overlap, their order disambiguates them.

A recdef definition also returns an induction rule specialised for the recursive function. For the gcd function above, the induction rule is

gcd.induct;
"(!m n. n ~= 0 --> ?P n (m mod n) ==> ?P m n) ==> ?P ?u ?v" : thm

This rule should be used to reason inductively about the gcd function. It usually makes the induction hypothesis available at all recursive calls, leading to very direct proofs. If any termination conditions remain unproved, they will become additional premises of this rule.
2.8 Example: Cantor’s Theorem

Cantor’s Theorem states that every set has more subsets than it has elements. It has become a favourite example in higher-order logic since it is so easily expressed:

\[
\forall f :: \alpha \Rightarrow \alpha \Rightarrow bool . \exists S :: \alpha \Rightarrow bool . \forall x :: \alpha . f x \neq S
\]

Viewing types as sets, \( \alpha \Rightarrow bool \) represents the powerset of \( \alpha \). This version states that for every function from \( \alpha \) to its powerset, some subset is outside its range.

The Isabelle proof uses HOL’s set theory, with the type \( \alpha set \) and the operator \( range \).

context Set.thy;

The set \( S \) is given as an unknown instead of a quantified variable so that we may inspect the subset found by the proof.

Goal "?S ~: range (f :: 'a=>'a set)";

Next, we apply \texttt{equalityCE}, reasoning that since \(?S = f x\), we have \( ?c \in ?S \) if and only if \( ?c \in f x \) for any \( ?c \).

by (erule_tac [equalityCE] 1);

Now we use a bit of creativity. Suppose that \( ?S \) has the form of a comprehension. Then \( ?c \in \{ x . ?P x \} \) implies \( ?P ?c \). Destruct-resolution using \texttt{CollectD} instantiates \( ?S \) and creates the new assumption.
Forcing a contradiction between the two assumptions of subgoal 1 completes the instantiation of $S$. It is now the set $\{ x \cdot x \notin f x \}$, which is the standard diagonal construction.

The rest should be easy. To apply $\text{CollectI}$ to the negated assumption, we employ $\text{swap_res_tac}$:

How much creativity is required? As it happens, Isabelle can prove this theorem automatically. The default classical set $\text{claset()}$ contains rules for most of the constructs of HOL's set theory. We must augment it with $\text{equalityCE}$ to break up set equalities, and then apply best-first search. Depth-first search would diverge, but best-first search successfully navigates through the large search space.

If you run this example interactively, make sure your current theory contains theory $\text{Set}$, for example by executing $\text{context Set.thy}$. Otherwise the default claset may not contain the rules for set theory.
First-Order Sequent Calculus

The theory LK implements classical first-order logic through Gentzen’s sequent calculus (see Gallier [5] or Takeuti [17]). Resembling the method of semantic tableaux, the calculus is well suited for backwards proof. Assertions have the form $\Gamma \vdash \Delta$, where $\Gamma$ and $\Delta$ are lists of formulae. Associative unification, simulated by higher-order unification, handles lists (§3.7 presents details, if you are interested).

The logic is many-sorted, using Isabelle’s type classes. The class of first-order terms is called term. No types of individuals are provided, but extensions can define types such as nat::term and type constructors such as list::(term)term. Below, the type variable $\alpha$ ranges over class term; the equality symbol and quantifiers are polymorphic (many-sorted). The type of formulae is $o$, which belongs to class logic.

LK implements a classical logic theorem prover that is nearly as powerful as the generic classical reasoner. The simplifier is now available too.

To work in LK, start up Isabelle specifying Sequents as the object-logic. Once in Isabelle, change the context to theory LK.thy:

```
isabelle Sequents
context LK.thy;
```

Modal logic and linear logic are also available, but unfortunately they are not documented.

3.1 Syntax and rules of inference

Figure 3.1 gives the syntax for LK, which is complicated by the representation of sequents. Type $\textit{sobj} \Rightarrow \textit{sobj}$ represents a list of formulae.

The definite description operator $\iota x \cdot P[x]$ stands for some $a$ satisfying $P[a]$, if one exists and is unique. Since all terms in LK denote something, a description is always meaningful, but we do not know its value unless $P[a]$ defines it uniquely. The Isabelle notation is $\text{THE}\ x.\ P[x]$. The corresponding rule (Fig. 3.4) does not entail the Axiom of Choice because it requires uniqueness.
### CHAPTER 3. FIRST-ORDER SEQUENT CALCULUS

<table>
<thead>
<tr>
<th>name</th>
<th>meta-type</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trueprop</td>
<td>[sobj ⇒ sobj, sobj ⇒ sobj] ⇒ prop</td>
<td>coercion to prop</td>
</tr>
<tr>
<td>Seqof</td>
<td>[o, sobj] ⇒ sobj</td>
<td>singleton sequence</td>
</tr>
<tr>
<td>Not</td>
<td>o ⇒ o</td>
<td>negation (¬)</td>
</tr>
<tr>
<td>True</td>
<td>o</td>
<td>tautology (⊤)</td>
</tr>
<tr>
<td>False</td>
<td>o</td>
<td>absurdity (⊥)</td>
</tr>
</tbody>
</table>

**Constants**

<table>
<thead>
<tr>
<th>symbol</th>
<th>name</th>
<th>meta-type</th>
<th>priority</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>All</td>
<td>(α ⇒ o) ⇒ o</td>
<td>10</td>
<td>universal quantifier (∀)</td>
</tr>
<tr>
<td>EX</td>
<td>Ex</td>
<td>(α ⇒ o) ⇒ o</td>
<td>10</td>
<td>existential quantifier (∃)</td>
</tr>
<tr>
<td>THE</td>
<td>The</td>
<td>(α ⇒ o) ⇒ α</td>
<td>10</td>
<td>definite description (ι)</td>
</tr>
</tbody>
</table>

**Binders**

<table>
<thead>
<tr>
<th>symbol</th>
<th>meta-type</th>
<th>priority</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>[α, α] ⇒ o</td>
<td>Left 50</td>
<td>equality (=)</td>
</tr>
<tr>
<td>&amp;</td>
<td>[o, o] ⇒ o</td>
<td>Right 35</td>
<td>conjunction (∧)</td>
</tr>
<tr>
<td></td>
<td>[o, o] ⇒ o</td>
<td>Right 30</td>
<td>disjunction (∨)</td>
</tr>
<tr>
<td>--&gt;</td>
<td>[o, o] ⇒ o</td>
<td>Right 25</td>
<td>implication (→)</td>
</tr>
<tr>
<td>&lt;-&gt;</td>
<td>[o, o] ⇒ o</td>
<td>Right 25</td>
<td>biconditional (↔)</td>
</tr>
</tbody>
</table>

**Infixes**

<table>
<thead>
<tr>
<th>external</th>
<th>internal</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Γ</td>
<td>- Δ</td>
<td>Trueprop(Γ, Δ)</td>
</tr>
</tbody>
</table>

**Translations**

Figure 3.1: Syntax of LK
\[
\text{prop} = \text{sequence} \mid \text{sequence}
\]

\[
\text{sequence} = \text{elem} \ (, \ \text{elem})^* \\
| \emptyset
\]

\[
\text{elem} = \$ \ \text{term} \\
| \text{formula} \\
| \text{<<sequence>>}
\]

\[
\text{formula} = \text{expression of type o} \\
| \text{term} = \text{term} \\
| - \ \text{formula} \\
| \text{formula} \ \& \ \text{formula} \\
| \text{formula} \mid \text{formula} \\
| \text{formula} \rightarrow \text{formula} \\
| \text{formula} \leftrightarrow \text{formula} \\
| \text{ALL id id}^* . \ \text{formula} \\
| \text{EX id id}^* . \ \text{formula} \\
| \text{THE id} . \ \text{formula}
\]

Figure 3.2: Grammar of LK
CHAPTER 3. FIRST-ORDER SEQUENT CALCULUS

basic $H, P, S |- E, P, S$

contRS $H |- E, S, S, S, F ==> H |- E, S, S, F$

thinRS $H |- E, F ==> H |- E, S, F$
thinLS $H, S |- E ==> H, S, G |- E$

cut $[| H |- E, P; H, P |- E |] ==> H |- E$

Structural rules

refl $H |- E, a=a, S$

subst $H(a), G(a) |- E(a) ==> H(b), a=b, G(b) |- E(b)$

Equality rules

Figure 3.3: Basic Rules of LK

Conditional expressions are available with the notation

if formula then term else term.

Figure 3.2 presents the grammar of LK. Traditionally, $\Gamma$ and $\Delta$ are metavariables for sequences. In Isabelle’s notation, the prefix $\$$ on a term makes it range over sequences. In a sequent, anything not prefixed by $\$$ is taken as a formula.

The notation $<<sequence>>$ stands for a sequence of formulæ. For example, you can declare the constant `imps` to consist of two implications:

```isabelle
consts P, Q, R :: o
constdefs imps :: seq'=seq'
   "imps == <<P --> Q, Q --> R>>"
```

Then you can use it in axioms and goals, for example
CHAPTER 3. FIRST-ORDER SEQUENT CALCULUS

48

True_def True == False-->False
iff_def P<->Q == (P-->Q) & (Q-->P)
conjR [| $H|- $E, P, $F; $H|- $E, Q, $F |] ==> $H|- $E, P&Q, $F
conjL $H, P, Q, $G |- $E ==> $H, P & Q, $G |- $E

disjR $H |- $E, P, Q, $F ==> $H |- $E, P|Q, $F

impR $H, P |- $E, Q, $F ==> $H |- $E, P-->Q, $F

notR $H, P |- $E, $F ==> $H |- $E, ~P, $F
notL $H, $G |- $E, P ==> $H, ~P, $G |- $E

FalseL $H, False, $G |- $E

allR (!!x. $H|- $E, P(x), $F) ==> $H|- $E, ALL x. P(x), $F
allL $H, P(x), $G, ALL x. P(x) |- $E ==> $H, ALL x. P(x), $G|- $E

exR $H|- $E, P(x), $F, EX x. P(x) ==> $H|- $E, EX x. P(x), $F
exL (!!x. $H, P(x), $G|- $E) ==> $H, EX x. P(x), $G|- $E

The [| $H |- $E, P(a), $F; !!x. $H, P(x) |- $E, x=a, $F |] ==> $H |- $E, P(THE x. P(x)), $F

Logical rules

Figure 3.4: Rules of LK
CHAPTER 3. FIRST-ORDER SEQUENT CALCULUS

thinR $H |- $E, $F ==> $H |- $E, P, $F
thinL $H, $G |- $E ==> $H, P, $G |- $E
contR $H |- $E, P, P, $F ==> $H |- $E, P, $F
contL $H, P, P, $G |- $E ==> $H, P, $G |- $E
symR $H |- $E, $F, a=b ==> $H |- $E, b=a, $F
symL $H, $G, b=a |- $E ==> $H, a=b, $G |- $E
transR [|$H|- $E, $F, a=b; $H|- $E, $F, b=c |] ==> $H|- $E, a=c, $F
TrueR $H |- $E, True, $F
iffR [|$H, P |- $E, Q, $F; $H, Q |- $E, P, $F |] ==> $H |- $E, P<>Q, $F
iffL [|$H, $G |- $E, P, Q; $H, Q, P, $G |- $E |] ==> $H, P<>Q, $G |- $E
allL_thin $H, P(x), $G |- $E ==> $H, ALL x. P(x), $G |- $E
exR_thin $H |- $E, P(x), $F ==> $H |- $E, EX x. P(x), $F
the_equality [|$H|- $E, P(a), $F;
!!!x. $H, P(x) |- $E, x=a, $F |]
==> $H |- $E, (THE x. P(x)) = a, $F

Figure 3.5: Derived rules for LK

Goalw [imps_def] "P, $imps |- R";
Level 0
P, $imps |- R
1. P, P --> Q, Q --> R |- R
by (Fast_tac 1);
Level 1
P, $imps |- R
No subgoals!

Figures 3.3 and 3.4 present the rules of theory LK. The connective $\leftrightarrow$ is defined using $\land$ and $\rightarrow$. The axiom for basic sequents is expressed in a form that provides automatic thinning: redundant formulae are simply ignored. The other rules are expressed in the form most suitable for backward proof; exchange and contraction rules are not normally required, although they are provided anyway.

Figure 3.5 presents derived rules, including rules for $\leftrightarrow$. The weakened quantifier rules discard each quantification after a single use; in an automatic
proof procedure, they guarantee termination, but are incomplete. Multiple
use of a quantifier can be obtained by a contraction rule, which in backward
proof duplicates a formula. The tactic \texttt{res_inst_tac} can instantiate the
variable \(?P\) in these rules, specifying the formula to duplicate. See theory
\texttt{Sequents/LK0} in the sources for complete listings of the rules and derived
rules.

To support the simplifier, hundreds of equivalences are proved for
the logical connectives and for if-then-else expressions. See the file
\texttt{Sequents/simpdata.ML}.

### 3.2 Automatic Proof

\(\text{LK}\) instantiates Isabelle’s simplifier. Both equality \((=)\) and the biconditional
\((\leftrightarrow)\) may be used for rewriting. The tactic \texttt{Simp_tac} refers to the default
simpset \((\texttt{simpset()})\). With sequents, the \texttt{full}\_ and \texttt{asm}\_ forms of the simpl-
ifier are not required; all the formulae in the sequent will be simplified.
The left-hand formulae are taken as rewrite rules. (Thus, the behaviour is
what you would normally expect from calling \texttt{Asm_full_simp_tac}.)

For classical reasoning, several tactics are available:

\begin{verbatim}
Safe_tac : int -> tactic
Step_tac : int -> tactic
Fast_tac : int -> tactic
Best_tac : int -> tactic
Pc_tac : int -> tactic
\end{verbatim}

These refer not to the standard classical reasoner but to a separate one
provided for the sequent calculus. Two commands are available for adding
new sequent calculus rules, safe or unsafe, to the default “theorem pack”:

\begin{verbatim}
Add_safes : thm list -> unit
Add_unsafes : thm list -> unit
\end{verbatim}

To control the set of rules for individual invocations, lower-case versions of
all these primitives are available. Sections 3.8 and 3.9 give full details.

### 3.3 Tactics for the cut rule

According to the cut-elimination theorem, the cut rule can be eliminated
from proofs of sequents. But the rule is still essential. It can be used to
structure a proof into lemmas, avoiding repeated proofs of the same formula.
More importantly, the cut rule cannot be eliminated from derivations of rules.
For example, there is a trivial cut-free proof of the sequent $P \land Q \vdash Q \land P$. Noting this, we might want to derive a rule for swapping the conjuncts in a right-hand formula:

$$\Gamma \vdash \Delta, P \land Q$$
$$\Gamma \vdash \Delta, Q \land P$$

The cut rule must be used, for $P \land Q$ is not a subformula of $Q \land P$. Most cuts directly involve a premise of the rule being derived (a meta-assumption). In a few cases, the cut formula is not part of any premise, but serves as a bridge between the premises and the conclusion. In such proofs, the cut formula is specified by calling an appropriate tactic.

```plaintext
cutR_tac : string -> int -> tactic
cutL_tac : string -> int -> tactic
```

These tactics refine a subgoal into two by applying the cut rule. The cut formula is given as a string, and replaces some other formula in the sequent.

- `cutR_tac P i` reads an LK formula $P$, and applies the cut rule to subgoal $i$.
  It then deletes some formula from the right side of subgoal $i$, replacing that formula by $P$.

- `cutL_tac P i` reads an LK formula $P$, and applies the cut rule to subgoal $i$.
  It then deletes some formula from the left side of the new subgoal $i+1$, replacing that formula by $P$.

All the structural rules — cut, contraction, and thinning — can be applied to particular formulae using `res_inst_tac`.

### 3.4 Tactics for sequents

```plaintext
forms_of_seq : term -> term list
could_res : term * term -> bool
could_resolve_seq : term * term -> bool
filesq_resolve_tac : thm list -> int -> int -> tactic
```

Associative unification is not as efficient as it might be, in part because the representation of lists defeats some of Isabelle’s internal optimisations. The following operations implement faster rule application, and may have other uses.

- `forms_of_seq t` returns the list of all formulae in the sequent $t$, removing sequence variables.
could_res \((t, u)\) tests whether two formula lists could be resolved. List \(t\) is from a premise or subgoal, while \(u\) is from the conclusion of an object-rule. Assuming that each formula in \(u\) is surrounded by sequence variables, it checks that each conclusion formula is unifiable (using could_unify) with some subgoal formula.

could_resolve_seq \((t, u)\) tests whether two sequents could be resolved. Sequent \(t\) is a premise or subgoal, while \(u\) is the conclusion of an object-rule. It simply calls could_res twice to check that both the left and the right sides of the sequents are compatible.

filseq_resolve_tac \(thms\) \(maxr\) \(i\) uses filter_thms could_resolve to extract the \(thms\) that are applicable to subgoal \(i\). If more than \(maxr\) theorems are applicable then the tactic fails. Otherwise it calls resolve_tac. Thus, it is the sequent calculus analogue of filt_resolve_tac.

3.5 A simple example of classical reasoning

The theorem \(\vdash \exists y. \forall x. P(y) \rightarrow P(x)\) is a standard example of the classical treatment of the existential quantifier. Classical reasoning is easy using LK, as you can see by comparing this proof with the one given in the FOL manual [12]. From a logical point of view, the proofs are essentially the same; the key step here is to use exR rather than the weaker exR_thin.

Goal "|\(- EX y. ALL x. P(y)--\rightarrow P(x)"";
Level 0
|\(- EX y. ALL x. P(y)--\rightarrow P(x)
1. |\(- EX y. ALL x. P(y)--\rightarrow P(x)
by (resolve_tac [exR] 1);
Level 1
|\(- EX y. ALL x. P(y)--\rightarrow P(x)
1. |\(- ALL x. P(?x)--\rightarrow P(x), EX x. ALL xa. P(x)--\rightarrow P(xa)
by (resolve_tac [allR] 1);
Level 2
|\(- EX y. ALL x. P(y)--\rightarrow P(x)
1. !!x. |\(- P(?x)--\rightarrow P(x), EX x. ALL xa. P(x)--\rightarrow P(xa)
by (resolve_tac [impR] 1);
Level 3
|\(- EX y. ALL x. P(y)--\rightarrow P(x)
1. !!x. P(?x) |\(- P(x), EX x. ALL xa. P(x)--\rightarrow P(x)

Because LK is a sequent calculus, the formula \(P(?x)\) does not become an
assumption; instead, it moves to the left side. The resulting subgoal cannot be instantiated to a basic sequent: the bound variable $x$ is not unifiable with the unknown $?x$.

by (resolve_tac [basic] 1);
by: tactic failed

We reuse the existential formula using exR_thin, which discards it; we shall not need it a third time. We again break down the resulting formula.

by (resolve_tac [exR_thin] 1);
Level 4
|- EX y. ALL x. P(y) --> P(x)
1. !!x. P(?x) |- P(x), ALL xa. P(?x7(x)) --> P(xa)
by (resolve_tac [allR] 1);
Level 5
|- EX y. ALL x. P(y) --> P(x)
1. !!x xa. P(?x) |- P(x), P(?x7(x)) --> P(xa)
by (resolve_tac [impR] 1);
Level 6
|- EX y. ALL x. P(y) --> P(x)
1. !!x xa. P(?x), P(?x7(x)) |- P(x), P(xa)

Subgoal 1 seems to offer lots of possibilities. Actually the only useful step is instantiating $?x_7$ to $\lambda x . x$, transforming $?x_7(x)$ into $x$.

by (resolve_tac [basic] 1);
Level 7
|- EX y. ALL x. P(y) --> P(x)
No subgoals!

This theorem can be proved automatically. Because it involves quantifier duplication, we employ best-first search:

Goal "|- EX y. ALL x. P(y)-->P(x)"
Level 0
|- EX y. ALL x. P(y) --> P(x)
1. |- EX y. ALL x. P(y) --> P(x)
by (best_tac LK_dup_pack 1);
Level 1
|- EX y. ALL x. P(y) --> P(x)
No subgoals!

3.6 A more complex proof

Many of Pelletier’s test problems for theorem provers [15] can be solved automatically. Problem 39 concerns set theory, asserting that there is no Russell
set — a set consisting of those sets that are not members of themselves:

\[ \vdash \neg (\exists x . \forall y . y \in x \leftrightarrow y \notin y) \]

This does not require special properties of membership; we may generalize \(x \in y\) to an arbitrary predicate \(F(x, y)\). The theorem, which is trivial for Fast_tac, has a short manual proof. See the directory Sequents/LK for many more examples.

We set the main goal and move the negated formula to the left.

Goal "\(|- (\exists x . \forall y . F(y,x) \leftrightarrow \neg F(y,y))\)"

Level 0

\[- (\exists x . \forall y . F(y,x) \leftrightarrow \neg F(y,y)) |-\]

by (resolve_tac [notR] 1);

Level 1

\[- (\exists x . \forall y . F(y,x) \leftrightarrow \neg F(y,y)) |-\]

1. \(\exists x . \forall y . F(y,x) \leftrightarrow \neg F(y,y)\) 

by (resolve_tac [exL] 1);

Level 2

\[- (\exists x . \forall y . F(y,x) \leftrightarrow \neg F(y,y)) |-\]

1. \(!!x . \forall y . F(y,x) \leftrightarrow \neg F(y,y)\) 

by (resolve_tac [allL_thin] 1);

Level 3

\[- (\exists x . \forall y . F(y,x) \leftrightarrow \neg F(y,y)) |-\]

1. \(!!x . F(?x2(x),x) \leftrightarrow \neg F(?x2(x),?x2(x))\) 

The rule iffL says, if \(P \leftrightarrow Q\) then \(P\) and \(Q\) are either both true or both false. It yields two subgoals.

by (resolve_tac [iffL] 1);

Level 4

\[- (\exists x . \forall y . F(y,x) \leftrightarrow \neg F(y,y)) |-\]

1. \(!!x . F(?x2(x),x) \leftrightarrow \neg F(?x2(x),?x2(x))\) 

2. \(!!x . \neg F(?x2(x),?x2(x)) \leftrightarrow F(?x2(x),x)\) 

We must instantiate \(?x2\), the shared unknown, to satisfy both subgoals. Beginning with subgoal 2, we move a negated formula to the left and create a basic sequent.
by (resolve_tac [notL] 2);
Level 5
| |- (EX x. ALL y. F(y,x) <-> ~ F(y,y))
1. !!x. |- F(?x2(x),x), ~ F(?x2(x),?x2(x))
2. !!x. F(?x2(x),x) |- F(?x2(x),?x2(x))
by (resolve_tac [basic] 2);
Level 6
| |- (EX x. ALL y. F(y,x) <-> ~ F(y,y))
1. !!x. |- F(x,x), ~ F(x,x)
Thanks to the instantiation of ?x2, subgoal 1 is obviously true.
by (resolve_tac [notR] 1);
Level 7
| |- (EX x. ALL y. F(y,x) <-> ~ F(y,y))
1. !!x. F(x,x) |- F(x,x)
by (resolve_tac [basic] 1);
Level 8
| |- (EX x. ALL y. F(y,x) <-> ~ F(y,y))
No subgoals!

3.7 *Unification for lists

Higher-order unification includes associative unification as a special case, by an encoding that involves function composition [7, page 37]. To represent lists, let C be a new constant. The empty list is $\lambda x.x$, while $[t_1, t_2, \ldots, t_n]$ is represented by

$$\lambda x. C(t_1, C(t_2, \ldots, C(t_n, x))).$$

The unifiers of this with $\lambda x. \exists g(x)$ give all the ways of expressing $[t_1, t_2, \ldots, t_n]$ as the concatenation of two lists.

Unlike orthodox associative unification, this technique can represent certain infinite sets of unifiers by flex-flex equations. But note that the term $\lambda x. C(t, ?a)$ does not represent any list. Flex-flex constraints containing such garbage terms may accumulate during a proof.

This technique lets Isabelle formalize sequent calculus rules, where the comma is the associative operator:

$$\Gamma, P, Q, \Delta \vdash \Theta \quad (\wedge\text{-left})$$

Multiple unifiers occur whenever this is resolved against a goal containing more than one conjunction on the left.

LK exploits this representation of lists. As an alternative, the sequent calculus can be formalized using an ordinary representation of lists, with a
logic program for removing a formula from a list. Amy Felty has applied this technique using the language $\lambda$Prolog [4].

Explicit formalization of sequents can be tiresome. But it gives precise control over contraction and weakening, and is essential to handle relevant and linear logics.

3.8 *Packaging sequent rules

The sequent calculi come with simple proof procedures. These are incomplete but are reasonably powerful for interactive use. They expect rules to be classified as **safe** or **unsafe**. A rule is safe if applying it to a provable goal always yields provable subgoals. If a rule is safe then it can be applied automatically to a goal without destroying our chances of finding a proof. For instance, all the standard rules of the classical sequent calculus LK are safe. An unsafe rule may render the goal unprovable; typical examples are the weakened quantifier rules `allL_thin` and `exR_thin`.

Proof procedures use safe rules whenever possible, using an unsafe rule as a last resort. Those safe rules are preferred that generate the fewest subgoals. Safe rules are (by definition) deterministic, while the unsafe rules require a search strategy, such as backtracking.

A **pack** is a pair whose first component is a list of safe rules and whose second is a list of unsafe rules. Packs can be extended in an obvious way to allow reasoning with various collections of rules. For clarity, LK declares `pack` as an ML datatype, although is essentially a type synonym:

```
datatype pack = Pack of thm list * thm list;
```

Pattern-matching using constructor `Pack` can inspect a pack’s contents. Packs support the following operations:

```
pack        : unit -> pack
pack_of     : theory -> pack
empty_pack  : pack
prop_pack   : pack
LK_pack     : pack
LK_dup_pack : pack
add_safes   : pack * thm list -> pack
add_unsafes : pack * thm list -> pack
```

Infix operators:

```
infix 4
```

`pack` returns the pack attached to the current theory.

`pack_of thy` returns the pack attached to theory `thy`.

`empty_pack` is the empty pack.
**CHAPTER 3. FIRST-ORDER SEQUENT CALCULUS**

\texttt{prop\_pack} contains the propositional rules, namely those for $\land$, $\lor$, $\neg$, $\to$ and $\leftrightarrow$, along with the rules \texttt{basic} and \texttt{refl}. These are all safe.

\texttt{LK\_pack} extends \texttt{prop\_pack} with the safe rules \texttt{allR} and \texttt{exL} and the unsafe rules \texttt{allL\_thin} and \texttt{exR\_thin}. Search using this is incomplete since quantified formulae are used at most once.

\texttt{LK\_dup\_pack} extends \texttt{prop\_pack} with the safe rules \texttt{allR} and \texttt{exL} and the unsafe rules \texttt{allL} and \texttt{exR}. Search using this is complete, since quantified formulae may be reused, but frequently fails to terminate. It is generally unsuitable for depth-first search.

\texttt{pack add\_safes rules} adds some safe rules to the pack \texttt{pack}.

\texttt{pack add\_unsafes rules} adds some unsafe rules to the pack \texttt{pack}.

### 3.9 *Proof procedures*

The LK proof procedure is similar to the classical reasoner described in the Reference Manual. In fact it is simpler, since it works directly with sequents rather than simulating them. There is no need to distinguish introduction rules from elimination rules, and of course there is no swap rule. As always, Isabelle’s classical proof procedures are less powerful than resolution theorem provers. But they are more natural and flexible, working with an open-ended set of rules.

Backtracking over the choice of a safe rule accomplishes nothing: applying them in any order leads to essentially the same result. Backtracking may be necessary over basic sequents when they perform unification. Suppose that 0, 1, 2, 3 are constants in the subgoals

\[
P(0), P(1), P(2) \vdash P(?a) \\
P(0), P(2), P(3) \vdash P(?a) \\
P(1), P(3), P(2) \vdash P(?a)
\]

The only assignment that satisfies all three subgoals is $?a \mapsto 2$, and this can only be discovered by search. The tactics given below permit backtracking only over axioms, such as \texttt{basic} and \texttt{refl}; otherwise they are deterministic.

#### 3.9.1 Method A

\[\begin{align*}
& \texttt{reresolve_tac : thm list -> int -> tactic} \\
& \texttt{repeat\_goal_tac : pack -> int -> tactic} \\
& \texttt{pc_tac : pack -> int -> tactic}
\end{align*}\]

These tactics use a method developed by Philippe de Groote. A subgoal
is refined and the resulting subgoals are attempted in reverse order. For some reason, this is much faster than attempting the subgoals in order. The method is inherently depth-first.

At present, these tactics only work for rules that have no more than two premises. They fail — return no next state — if they can do nothing.

reresolve_tac thms i repeatedly applies the thms to subgoal i and the resulting subgoals.

repeat_goal_tac pack i applies the safe rules in the pack to a goal and the resulting subgoals. If no safe rule is applicable then it applies an unsafe rule and continues.

pc_tac pack i applies repeat_goal_tac using depth-first search to solve subgoal i.

3.9.2 Method B

safe_tac : pack -> int -> tactic
step_tac : pack -> int -> tactic
fast_tac : pack -> int -> tactic
best_tac : pack -> int -> tactic

These tactics are analogous to those of the generic classical reasoner. They use ‘Method A’ only on safe rules. They fail if they can do nothing.

safe_goal_tac pack i applies the safe rules in the pack to a goal and the resulting subgoals. It ignores the unsafe rules.

step_tac pack i either applies safe rules (using safe_goal_tac) or applies one unsafe rule.

fast_tac pack i applies step_tac using depth-first search to solve subgoal i. Despite its name, it is frequently slower than pc_tac.

best_tac pack i applies step_tac using best-first search to solve subgoal i. It is particularly useful for quantifier duplication (using LK_dup_pack).
The Isabelle theory *Sequents.thy* provides facilities for using sequent notation in users’ object logics. This theory allows users to easily interface the surface syntax of sequences with an underlying representation suitable for higher-order unification.

### 4.1 Concrete syntax of sequences

Mathematicians and logicians have used sequences in an informal way much before proof systems such as Isabelle were created. It seems sensible to allow people using Isabelle to express sequents and perform proofs in this same informal way, and without requiring the theory developer to spend a lot of time in ML programming.

By using *Sequents.thy* appropriately, a logic developer can allow users to refer to sequences in several ways:

- A sequence variable is any alphanumeric string with the first character being a $\$ \$ sign. So, consider the sequent $\$A \ |- \ B$, where $\$A$ is intended to match a sequence of zero or more items.

- A sequence with unspecified sub-sequences and unspecified or individual items is written as a comma-separated list of regular variables (representing items), particular items, and sequence variables, as in

  $$\$A, \ B, \ C, \ $D(x) \ |- \ E$$

  Here both $\$A$ and $\$D(x)$ are allowed to match any subsequences of items on either side of the two items that match $B$ and $C$. Moreover, the sequence matching $\$D(x)$ may contain occurrences of $x$.

- An empty sequence can be represented by a blank space, as in $\ |- \ true$. 


These syntactic constructs need to be assimilated into the object theory being developed. The type that we use for these visible objects is given the name seq. A seq is created either by the empty space, a seqobj or a seqobj followed by a seq, with a comma between them. A seqobj is either an item or a variable representing a sequence. Thus, a theory designer can specify a function that takes two sequences and returns a meta-level proposition by giving it the Isabelle type $[\text{seq}, \text{seq}] \Rightarrow \text{prop}$.

This is all part of the concrete syntax, but one may wish to exploit Isabelle's higher-order abstract syntax by actually having a different, more powerful internal syntax.

### 4.2 Basis

One could opt to represent sequences as first-order objects (such as simple lists), but this would not allow us to use many facilities Isabelle provides for matching. By using a slightly more complex representation, users of the logic can reap many benefits in facilities for proofs and ease of reading logical terms.

A sequence can be represented as a function — a constructor for further sequences — by defining a binary abstract function Seq0' with type $[\text{o}, \text{seq}'] \Rightarrow \text{seq}'$, and translating a sequence such as $A, B, C$ into

$$\%s. \text{Seq0'}(A, \text{Seq0'}(B, \text{Seq0'}(C, s)))$$

This sequence can therefore be seen as a constructor for further sequences. The constructor Seq0' is never given a value, and therefore it is not possible to evaluate this expression into a basic value.

Furthermore, if we want to represent the sequence $A, B, C$, we note that $B$ already represents a sequence, so we can use $B$ itself to refer to the function, and therefore the sequence can be mapped to the internal form:

$$\%s. \text{Seq0'}(A, B(\text{Seq0'}(C, s)))$$

So, while we wish to continue with the standard, well-liked external representation of sequences, we can represent them internally as functions of type seq' => seq'.

### 4.3 Object logics

Recall that object logics are defined by mapping elements of particular types to the Isabelle type prop, usually with a function called Trueprop. So, an object logic proposition $P$ is matched to the Isabelle proposition Trueprop($P$).
The name of the function is often hidden, so the user just sees \( \text{P} \). Isabelle is eager to make types match, so it inserts \( \textsf{Trueprop} \) automatically when an object of type \( \text{prop} \) is expected. This mechanism can be observed in most of the object logics which are direct descendants of \text{Pure}.

In order to provide the desired syntactic facilities for sequent calculi, rather than use just one function that maps object-level propositions to meta-level propositions, we use two functions, and separate internal from the external representation.

These functions need to be given a type that is appropriate for the particular form of sequents required: single or multiple conclusions. So multiple-conclusion sequents (used in the LK logic) can be specified by the following two definitions, which are lifted from the inbuilt \textit{Sequents/LK.thy}:

\[
\begin{align*}
\textsf{Trueprop} & \quad :: \quad \text{two_seqi} \\
\text{"@Trueprop"} & \quad :: \quad \text{two_seque} \quad \text{"((_)/\ |-\ (_))"} \quad \text{[6,6] 5}
\end{align*}
\]

where the types used are defined in \textit{Sequents.thy} as abbreviations:

\[
\begin{align*}
\text{two_seqi} & = \quad \text{[seq'=\text{'seq'}, seq'=\text{'seq'] \Rightarrow \text{prop}} \\
\text{two_seque} & = \quad \text{[seq, seq] \Rightarrow \text{prop}}
\end{align*}
\]

The next step is to actually create links into the low-level parsing and pretty-printing mechanisms, which map external and internal representations. These functions go below the user level and capture the underlying structure of Isabelle terms in ML. Fortunately the theory developer need not delve in this level; \textit{Sequents.thy} provides the necessary facilities. All the theory developer needs to add in the ML section is a specification of the two translation functions:

\[
\begin{align*}
\text{ML} \\
\text{val parse_translation} & = \quad \text{[("@Trueprop",Sequents.ttwo_seq_tr "Trueprop")]}; \\
\text{val print_translation} & = \quad \text{[("Trueprop",Sequents.ttwo_seq_tr' "@Trueprop")]};
\end{align*}
\]

In summary: in the logic theory being developed, the developer needs to specify the types for the internal and external representation of the sequences, and use the appropriate parsing and pretty-printing functions.

### 4.4 What’s in \textit{Sequents.thy}

Theory \textit{Sequents.thy} makes many declarations that you need to know about:

1. The Isabelle types given below, which can be used for the constants that map object-level sequents and meta-level propositions:
single_seqe = [seq,seqobj] => prop
single_seqi = [seq'=>seq',seq'=>seq'] => prop
two_seqi = [seq'=>seq', seq'=>seq'] => prop
two_seqe = [seq, seq] => prop
three_seqi = [seq'=>seq', seq'=>seq', seq'=>seq'] => prop
three_seqe = [seq, seq, seq] => prop
four_seqi = [seq'=>seq', seq'=>seq', seq'=>seq', seq'=>seq'] => prop
four_seqe = [seq, seq, seq, seq] => prop

The single_ and two_ sets of mappings for internal and external representations are the ones used for, say single and multiple conclusion sequents. The other functions are provided to allow rules that manipulate more than two functions, as can be seen in the inbuilt object logics.

2. An auxiliary syntactic constant has been defined that directly maps a sequence to its internal representation:

"@Side" :: seq=>(seq'=>seq') ("<<(_)>>")

Whenever a sequence (such as << A, $B, $C>>) is entered using this syntax, it is translated into the appropriate internal representation. This form can be used only where a sequence is expected.

3. The ML functions single_tr, two_seq_tr, three_seq_tr, four_seq_tr for parsing, that is, the translation from external to internal form. Analogously there are single_tr', two_seq_tr', three_seq_tr', four_seq_tr' for pretty-printing, that is, the translation from internal to external form. These functions can be used in the ML section of a theory file to specify the translations to be used. As an example of use, note that in LK.thy we declare two identifiers:

```ml
val parse_translation =
  [("@Trueprop",Sequents.two_seq_tr "Trueprop")];
val print_translation =
  [("Trueprop",Sequents.two_seq_tr' "@Trueprop")];
```

The given parse translation will be applied whenever a @Trueprop constant is found, translating using two_seq_tr and inserting the constant Trueprop. The pretty-printing translation is applied analogously; a term that contains Trueprop is printed as a @Trueprop.
Chapter 5

Constructive Type Theory

Martin-Löf’s Constructive Type Theory [9, 11] can be viewed at many different levels. It is a formal system that embodies the principles of intuitionistic mathematics; it embodies the interpretation of propositions as types; it is a vehicle for deriving programs from proofs.

Thompson’s book [18] gives a readable and thorough account of Type Theory. Nuprl is an elaborate implementation [3]. ALF is a more recent tool that allows proof terms to be edited directly [8].

Isabelle’s original formulation of Type Theory was a kind of sequent calculus, following Martin-Löf [9]. It included rules for building the context, namely variable bindings with their types. A typical judgement was

\[ a(x_1, \ldots, x_n) \in A(x_1, \ldots, x_n) \quad [x_1 \in A_1, x_2 \in A_2(x_1), \ldots, x_n \in A_n(x_1, \ldots, x_{n-1})] \]

This sequent calculus was not satisfactory because assumptions like ‘suppose \( A \) is a type’ or ‘suppose \( B(x) \) is a type for all \( x \) in \( A \)’ could not be formalized.

The theory \( \text{CTT} \) implements Constructive Type Theory, using natural deduction. The judgement above is expressed using \( \land \) and \( \implies \):

\[
\land \, x_1 \ldots x_n, [x_1 \in A_1; x_2 \in A_2(x_1); \ldots; x_n \in A_n(x_1, \ldots, x_{n-1})] \implies a(x_1, \ldots, x_n) \in A(x_1, \ldots, x_n)
\]

Assumptions can use all the judgement forms, for instance to express that \( B \) is a family of types over \( A \):

\[
\land \, x. x \in A \implies B(x) \text{ type}
\]

To justify the CTT formulation it is probably best to appeal directly to the semantic explanations of the rules [9], rather than to the rules themselves. The order of assumptions no longer matters, unlike in standard Type Theory. Contexts, which are typical of many modern type theories, are difficult to represent in Isabelle. In particular, it is difficult to enforce that all the variables in a context are distinct.

The theory does not use polymorphism. Terms in CTT have type \( i \), the type of individuals. Types in CTT have type \( t \).
name | meta-type | description
--- | --- | ---
Type | $t \rightarrow \text{prop}$ | judgement form
Eqtype | $[t, t] \rightarrow \text{prop}$ | judgement form
Elem | $[i, t] \rightarrow \text{prop}$ | judgement form
Eqelem | $[i, i, t] \rightarrow \text{prop}$ | judgement form
Reduce | $[i, i] \rightarrow \text{prop}$ | extra judgement form

N | $t$ | natural numbers type
0 | $i$ | constructor
succ | $i \rightarrow i$ | constructor
rec | $[i, i, [i, i] \rightarrow i] \rightarrow i$ | eliminator

Prod | $[t, i \rightarrow t] \rightarrow t$ | general product type
lambda | $(i \rightarrow i) \rightarrow i$ | constructor

Sum | $[t, i \rightarrow t] \rightarrow t$ | general sum type
pair | $[i, i] \rightarrow i$ | constructor
split | $[i, [i, i] \rightarrow i] \rightarrow i$ | eliminator
fst snd | $i \rightarrow i$ | projections

inl inr | $i \rightarrow i$ | constructors for +
when | $[i, i \rightarrow i, i \rightarrow i] \rightarrow i$ | eliminator for +

Eq | $[t, i, i] \rightarrow t$ | equality type
eq | $i$ | constructor

F | $t$ | empty type
contr | $i \rightarrow i$ | eliminator

T | $t$ | singleton type
tt | $i$ | constructor

Figure 5.1: The constants of CTT
CTT supports all of Type Theory apart from list types, well-ordering types, and universes. Universes could be introduced à la Tarski, adding new constants as names for types. The formulation à la Russell, where types denote themselves, is only possible if we identify the meta-types $\tau$ and $i$. Most published formulations of well-ordering types have difficulties involving extensionality of functions; I suggest that you use some other method for defining recursive types. List types are easy to introduce by declaring new rules.

CTT uses the 1982 version of Type Theory, with extensional equality. The computation $a = b \in A$ and the equality $c \in Eq(A, a, b)$ are interchangeable. Its rewriting tactics prove theorems of the form $a = b \in A$. It could be modified to have intensional equality, but rewriting tactics would have to prove theorems of the form $c \in Eq(A, a, b)$ and the computation rules might require a separate simplifier.

5.1 Syntax

The constants are shown in Fig. 5.1. The infixes include the function application operator (sometimes called ‘apply’), and the 2-place type operators. Note that meta-level abstraction and application, $\lambda x . b$ and $f(a)$, differ from object-level abstraction and application, $\text{lam } x . b$ and $b \langle a \rangle$. A CTT function $f$ is simply an individual as far as Isabelle is concerned: its Isabelle type is $i$, not say $i \Rightarrow i$.

The notation for CTT (Fig. 5.2) is based on that of Nordström et al. [11]. The empty type is called $F$ and the one-element type is $T$; other finite types are built as $T + T + T$, etc.

Quantification is expressed by sums $\sum_{x \in A} B[x]$ and products $\prod_{x \in A} B[x]$. Instead of $\text{Sum}(A, B)$ and $\text{Prod}(A, B)$ we may write $\text{SUM } x : A . B[x]$ and $\text{PROD } x : A . B[x]$. For example, we may write

$$\text{SUM } y : B . \text{PROD } x : A . C(x, y)$$

The special cases as $A*B$ and $A-->B$ abbreviate general sums and products over a constant family. Isabelle accepts these abbreviations in parsing and uses them whenever possible for printing.

$^1$Unlike normal infix operators, $*$ and $-->$ merely define abbreviations; there are no constants $\text{op } *$ and $\text{op } -->$. 
symbol | name | meta-type | priority | description  \\
--- | --- | --- | --- | ---  \\
lam | lambda | $(i \Rightarrow o) \Rightarrow i$ | 10 | $\lambda$-abstraction  \\

**Binders**

| symbol | meta-type | priority | description  \\
--- | --- | --- | ---  \\
` | $[i, i] \rightarrow i$ | Left 55 | function application  \\
+ | $[t, t] \rightarrow t$ | Right 30 | sum of two types  \\

**Infixes**

| external | internal | standard notation  \\
--- | --- | ---  \\
PROD $x:A . B[x]$ | Prod($A, \lambda x . B[x]$) | product $\prod_{x \in A} B[x]$  \\
SUM $x:A . B[x]$ | Sum($A, \lambda x . B[x]$) | sum $\sum_{x \in A} B[x]$  \\
$A ightarrow B$ | Prod($A, \lambda x . B$) | function space $A \rightarrow B$  \\
$A \times B$ | Sum($A, \lambda x . B$) | binary product $A \times B$  \\

**Translations**

```
prop = type type  
   | type = type  
   | term : type  
   | term = term : type  

type = expression of type $t$  
   | PROD id : type . type  
   | SUM id : type . type  

term = expression of type $i$  
   | lam id id* . term  
   | < term , term >  
```

**Grammar**

Figure 5.2: Syntax of CTT
refl_type \[ A \text{ type} \implies A = A \]

refl_elem \[ a : A \implies a = a : A \]

sym_type \[ A = B \implies B = A \]

sym_elem \[ a = b : A \implies b = a : A \]

trans_type \[ \{ A = B; B = C \} \implies A = C \]

trans_elem \[ \{ a = b : A; b = c : A \} \implies a = c : A \]

equal_types \[ \{ a : A; A = B \} \implies a : B \]

equal_typesL \[ \{ a = b : A; A = B \} \implies a = b : B \]

subst_type \[ \{ a : A; !z. z:A \implies B(z) \text{ type} \} \implies B(a) \text{ type} \]

subst_typeL \[ \{ a = c : A; !z. z:A \implies B(z) = D(z) \} \implies B(a) = D(c) \]

subst_elem \[ \{ a : A; !z. z:A \implies b(z):B(z) \} \implies b(a):B(a) \]

subst_elemL \[ \{ a = c : A; !z. z:A \implies b(z) = d(z) : B(z) \} \implies b(a) = d(c) : B(a) \]

refl_red \[ \text{Reduce}(a,a) \]

red_if_equal \[ a = b : A \implies \text{Reduce}(a,b) \]

trans_red \[ \{ a = b : A; \text{Reduce}(b,c) \} \implies a = c : A \]

Figure 5.3: General equality rules
CHAPTER 5. CONSTRUCTIVE TYPE THEORY

68

NF  
N  type

NIO  
0 : N

NI_succ  
a : N ==> succ(a) : N

NI_succL  
a = b : N ==> succ(a) = succ(b) : N

NE  
[ | p : N; a : C(0);  
  !u v. [ | u : N; v : C(u) | ] ==> b(u,v) : C(succ(u))  
] ==> rec(p, a, %u v. b(u,v)) : C(p)

NEL  
[ | p = q : N; a = c : C(0);  
  !u v. [ | u : N; v : C(u) | ] ==> b(u,v)=d(u,v) : C(succ(u))  
] ==> rec(p, a, %u v. b(u,v)) = rec(q,c,d) : C(p)

NCO  
[ | a : C(0);  
  !u v. [ | u : N; v : C(u) | ] ==> b(u,v) : C(succ(u))  
] ==> rec(0, a, %u v. b(u,v)) = a : C(0)

NC_suc    
[ | p : N; a : C(0);  
  !u v. [ | u : N; v : C(u) | ] ==> b(u,v) : C(succ(u))  
] ==> rec(succ(p), a, %u v. b(u,v)) = b(p, rec(p, a, %u v. b(u,v))) : C(succ(p))

zero_ne_succ  
[ | a : N; 0 = succ(a) : N | ] ==> 0 : F

Figure 5.4: Rules for type N

ProdF  
[ | A type; !!x. x:A ==> B(x) type | ] ==> PROD x:A. B(x) type

ProdFL  
[ | A = C; !!x. x:A ==> B(x) = D(x) | ] ==>
PROD x:A. B(x) = PROD x:C. D(x)

ProdI  
[ | A type; !!x. x:A ==> b(x):B(x)  
] ==> lam x. b(x) : PROD x:A. B(x)

ProdIL  
[ | A type; !!x. x:A ==> b(x) = c(x) : B(x)  
] ==> lam x. b(x) = lam x. c(x) : PROD x:A. B(x)

ProdE  
[ | p : PROD x:A. B(x); a : A | ] ==> p`a : B(a)

ProdEL  
[ | p=q: PROD x:A. B(x); a=b : A | ] ==> p`a = q`b : B(a)

ProdC  
[ | a : A; !!x. x:A ==> b(x) : B(x)  
] ==> (lam x. b(x)) ` a = b(a) : B(a)

ProdC2  
p : PROD x:A. B(x) ==> (lam x. p`x) = p : PROD x:A. B(x)

Figure 5.5: Rules for the product type \( \prod_{x \in A} B[x] \)
CHAPTER 5. CONSTRUCTIVE TYPE THEORY

5.2 Rules of inference

The rules obey the following naming conventions. Type formation rules have the suffix \( F \). Introduction rules have the suffix \( I \). Elimination rules have the suffix \( E \). Computation rules, which describe the reduction of eliminators, have the suffix \( C \). The equality versions of the rules (which permit reductions on subterms) are called \( \text{long} \) rules; their names have the suffix \( L \). Introduction and computation rules are often further suffixed with constructor names.

Figure 5.3 presents the equality rules. Most of them are straightforward: reflexivity, symmetry, transitivity and substitution. The judgement \( \text{Reduce} \) does not belong to Type Theory proper; it has been added to implement rewriting. The judgement \( \text{Reduce}(a, b) \) holds when \( a = b : A \) holds. It also holds when \( a \) and \( b \) are syntactically identical, even if they are ill-typed, because rule \( \text{refl_red} \) does not verify that \( a \) belongs to \( A \).

The \( \text{Reduce} \) rules do not give rise to new theorems about the standard judgements. The only rule with \( \text{Reduce} \) in a premise is \( \text{trans_red} \), whose other premise ensures that \( a \) and \( b \) (and thus \( c \)) are well-typed.

Figure 5.4 presents the rules for \( N \), the type of natural numbers. They include \( \text{zero_ne_succ} \), which asserts \( 0 \neq n + 1 \). This is the fourth Peano
CHAPTER 5. CONSTRUCTIVE TYPE THEORY

PlusF \[| A \text{ type} ; B \text{ type} | \implies A+B \text{ type} \]

PlusFL \[| A = C ; B = D | \implies A+B = C+D \]

PlusI_inl \[| a : A ; B \text{ type} | \implies \text{inl}(a) : A+B \]

PlusI_inlL \[| a = c : A ; B \text{ type} | \implies \text{inl}(a) = \text{inl}(c) : A+B \]

PlusI_inr \[| A \text{ type} ; b : B | \implies \text{inr}(b) : A+B \]

PlusI_inrL \[| A \text{ type} ; b = d : B | \implies \text{inr}(b) = \text{inr}(d) : A+B \]

PlusE \[| p: A+B; \]
\[!!x. x:A \implies c(x) : C(\text{inl}(x)); \]
\[!!y. y:B \implies d(y) : C(\text{inr}(y)) \]
\[| \implies \text{when}(p, \%x. c(x), \%y. d(y)) : C(p) \]

PlusEL \[| p = q : A+B; \]
\[!!x. x:A \implies c(x) = e(x) : C(\text{inl}(x)); \]
\[!!y. y:B \implies d(y) = f(y) : C(\text{inr}(y)) \]
\[| \implies \text{when}(p, \%x. c(x), \%y. d(y)) = \text{when}(q, \%x. e(x), \%y. f(y)) : C(p) \]

PlusC_inl \[| a : A; \]
\[!!x. x:A \implies c(x) : C(\text{inl}(x)); \]
\[!!y. y:B \implies d(y) : C(\text{inr}(y)) \]
\[| \implies \text{when}(\text{inl}(a), \%x. c(x), \%y. d(y)) = c(a) : C(\text{inl}(a)) \]

PlusC_inr \[| b : B; \]
\[!!x. x:A \implies c(x) : C(\text{inl}(x)); \]
\[!!y. y:B \implies d(y) : C(\text{inr}(y)) \]
\[| \implies \text{when}(\text{inr}(b), \%x. c(x), \%y. d(y)) = d(b) : C(\text{inr}(b)) \]

Figure 5.7: Rules for the binary sum type $A + B$

FF \[F \text{ type} \]

FE \[| p : F ; C \text{ type} | \implies \text{contr}(p) : C \]

FEL \[| p = q : F ; C \text{ type} | \implies \text{contr}(p) = \text{contr}(q) : C \]

TF \[T \text{ type} \]

TI \[tt : T \]

TE \[| p : T ; c : C(tt) | \implies c : C(p) \]

TEL \[| p = q : T ; c = d : C(tt) | \implies c = d : C(p) \]

TC \[p : T \implies p = tt : T \]

Figure 5.8: Rules for types $F$ and $T$


\begin{align*}
\text{EqF} & \quad [\mid A \text{ type}; \ a : A; \ b : A \mid] \implies \text{Eq}(A,a,b) \text{ type} \\
\text{EqFL} & \quad [\mid A=B; \ a=c : A; \ b=d : A \mid] \implies \text{Eq}(A,a,b) = \text{Eq}(B,c,d) \\
\text{EqI} & \quad a = b : A \implies eq : \text{Eq}(A,a,b) \\
\text{EqE} & \quad p : \text{Eq}(A,a,b) \implies a = b : A \\
\text{EqC} & \quad p : \text{Eq}(A,a,b) \implies p = eq : \text{Eq}(A,a,b) 
\end{align*}

Figure 5.9: Rules for the equality type \(\text{Eq}(A,a,b)\)

\begin{align*}
\text{replace_type} & \quad [\mid B = A; \ a : A \mid] \implies a : B \\
\text{subst_eqtyparg} & \quad [\mid a=c : A; \ !z. \ z:A \implies B(z) \text{ type} \mid] \implies B(a) = B(c) \\
\text{subst_prodE} & \quad [\mid p: \text{Prod}(A,B); \ a: A; \ !z. \ z: B(a) \implies c(z) : C(z) \mid] \implies c(p\ a) : C(p\ a) \\
\text{SumIL2} & \quad [\mid c=a : A; \ d=b : B(a) \mid] \implies <c,d> = <a,b> : \text{Sum}(A,B) \\
\text{SumE_fst} & \quad p : \text{Sum}(A,B) \implies \text{fst}(p) : A \\
\text{SumE_snd} & \quad [\mid p: \text{Sum}(A,B); \ A \text{ type}; \ !x. \ x:A \implies B(x) \text{ type} \mid] \implies \text{snd}(p) : B(\text{fst}(p))
\end{align*}

Figure 5.10: Derived rules for CTT

axiom and cannot be derived without universes [9, page 91].

The constant \(\text{rec}\) constructs proof terms when mathematical induction, rule \(\text{NE}\), is applied. It can also express primitive recursion. Since \(\text{rec}\) can be applied to higher-order functions, it can even express Ackermann’s function, which is not primitive recursive [18, page 104].

Figure 5.5 shows the rules for general product types, which include function types as a special case. The rules correspond to the predicate calculus rules for universal quantifiers and implication. They also permit reasoning about functions, with the rules of a typed \(\lambda\)-calculus.

Figure 5.6 shows the rules for general sum types, which include binary product types as a special case. The rules correspond to the predicate calculus rules for existential quantifiers and conjunction. They also permit reasoning about ordered pairs, with the projections \(\text{fst}\) and \(\text{snd}\).

Figure 5.7 shows the rules for binary sum types. They correspond to the predicate calculus rules for disjunction. They also permit reasoning about disjoint sums, with the injections \(\text{inl}\) and \(\text{inr}\) and case analysis operator \(\text{when}\).

Figure 5.8 shows the rules for the empty and unit types, \(F\) and \(T\). They correspond to the predicate calculus rules for absurdity and truth.
Figure 5.9 shows the rules for equality types. If $a = b \in A$ is provable then $eq$ is a canonical element of the type $Eq(A, a, b)$, and vice versa. These rules define extensional equality; the most recent versions of Type Theory use intensional equality [11].

Figure 5.10 presents the derived rules. The rule $\text{subst\_prodE}$ is derived from $\text{prodE}$, and is easier to use in backwards proof. The rules $\text{SumE\_fst}$ and $\text{SumE\_snd}$ express the typing of $\text{fst}$ and $\text{snd}$; together, they are roughly equivalent to $\text{SumE}$ with the advantage of creating no parameters. Section 5.12 below demonstrates these rules in a proof of the Axiom of Choice.

All the rules are given in $\eta$-expanded form. For instance, every occurrence of $\lambda uv. b(u, v)$ could be abbreviated to $b$ in the rules for $N$. The expanded form permits Isabelle to preserve bound variable names during backward proof. Names of bound variables in the conclusion (here, $u$ and $v$) are matched with corresponding bound variables in the premises.

### 5.3 Rule lists

The Type Theory tactics provide rewriting, type inference, and logical reasoning. Many proof procedures work by repeatedly resolving certain Type Theory rules against a proof state. CTT defines lists — each with type `thm list` — of related rules.

- `form_rls` contains formation rules for the types $N, \Pi, \Sigma, +, Eq, F,$ and $T$.
- `formL_rls` contains long formation rules for $\Pi, \Sigma, +,$ and $Eq$. (For other types use `refl_type`.)
- `intr_rls` contains introduction rules for the types $N, \Pi, \Sigma, +,$ and $T$.
- `intrL_rls` contains long introduction rules for $N, \Pi, \Sigma,$ and $+$. (For $T$ use `refl_elem`.)
- `elim_rls` contains elimination rules for the types $N, \Pi, \Sigma, +,$ and $F$. The rules for $Eq$ and $T$ are omitted because they involve no eliminator.
- `elimL_rls` contains long elimination rules for $N, \Pi, \Sigma, +,$ and $F$.
- `comp_rls` contains computation rules for the types $N, \Pi, \Sigma,$ and $+$. Those for $Eq$ and $T$ involve no eliminator.
- `basic_defs` contains the definitions of $\text{fst}$ and $\text{snd}$. 
5.4 Tactics for subgoal reordering

\begin{verbatim}
test_assume_tac : int -> tactic
typechk_tac : thm list -> tactic
equal_tac : thm list -> tactic
intr_tac : thm list -> tactic
\end{verbatim}

Blind application of CTT rules seldom leads to a proof. The elimination rules, especially, create subgoals containing new unknowns. These subgoals unify with anything, creating a huge search space. The standard tactic \texttt{filt_resolve_tac} (see the Reference Manual) fails for goals that are too flexible; so does the CTT tactic \texttt{test_assume_tac}. Used with the tactical \texttt{REPEAT_FIRST} they achieve a simple kind of subgoal reordering: the less flexible subgoals are attempted first. Do some single step proofs, or study the examples below, to see why this is necessary.

\texttt{test_assume_tac} \texttt{i} uses \texttt{assume_tac} to solve the subgoal by assumption, but only if subgoal \texttt{i} has the form \( a \in A \) and the head of \( a \) is not an unknown. Otherwise, it fails.

\texttt{typechk_tac \( \texttt{thms} \)} uses \texttt{thms} with formation, introduction, and elimination rules to check the typing of constructions. It is designed to solve goals of the form \( a \in ?A \), where \( a \) is rigid and \(?A\) is flexible; thus it performs type inference. The tactic can also solve goals of the form \( A \) type.

\texttt{equal_tac \( \texttt{thms} \)} uses \texttt{thms} with the long introduction and elimination rules to solve goals of the form \( a = b \in A \), where \( a \) is rigid. It is intended for deriving the long rules for defined constants such as the arithmetic operators. The tactic can also perform type-checking.

\texttt{intr_tac \( \texttt{thms} \)} uses \texttt{thms} with the introduction rules to break down a type. It is designed for goals like \(?a \in A\) where \(?a\) is flexible and \(A\) rigid. These typically arise when trying to prove a proposition \( A \), expressed as a type.

5.5 Rewriting tactics

\begin{verbatim}
rew_tac : thm list -> tactic
hyp_rew_tac : thm list -> tactic
\end{verbatim}

Object-level simplification is accomplished through proof, using the CTT equality rules and the built-in rewriting functor \texttt{TsimpFun}.\footnote{This should not be confused with Isabelle’s main simplifier; \texttt{TsimpFun} is only useful for CTT and similar logics with type inference rules. At present it is undocumented.} The rewrites
include the computation rules and other equations. The long versions of
the other rules permit rewriting of subterms and subtypes. Also used are
transitivity and the extra judgement form \texttt{Reduce}. Meta-level simplification
handles only definitional equality.

\texttt{rew_tac thms} applies \texttt{thms} and the computation rules as left-to-right
rewrites. It solves the goal \( a = b \in A \) by rewriting \( a \) to \( b \). If \( b \) is
an unknown then it is assigned the rewritten form of \( a \). All subgoals
are rewritten.

\texttt{hyp_rew_tac thms} is like \texttt{rew_tac}, but includes as rewrites any equations
present in the assumptions.

## 5.6 Tactics for logical reasoning

Interpreting propositions as types lets CTT express statements of intuition-
istic logic. However, Constructive Type Theory is not just another syntax
for first-order logic. There are fundamental differences.

Can assumptions be deleted after use? Not every occurrence of a type
represents a proposition, and Type Theory assumptions declare variables. In
first-order logic, \( \lor \)-elimination with the assumption \( P \lor Q \) creates one subgoal
assuming \( P \) and another assuming \( Q \), and \( P \lor Q \) can be deleted safely. In
Type Theory, \( + \)-elimination with the assumption \( z \in A + B \) creates one
subgoal assuming \( x \in A \) and another assuming \( y \in B \) (for arbitrary \( x \) and
\( y \)). Deleting \( z \in A + B \) when other assumptions refer to \( z \) may render the
subgoal unprovable: arguably, meaningless.

Isabelle provides several tactics for predicate calculus reasoning in CTT:

\begin{verbatim}
mp_tac : int -> tactic
add_mp_tac : int -> tactic
safestep_tac : thm list -> int -> tactic
safe_tac : thm list -> int -> tactic
step_tac : thm list -> int -> tactic
pc_tac : thm list -> int -> tactic
\end{verbatim}

These are loosely based on the intuitionistic proof procedures of \texttt{FOL}. For the
reasons discussed above, a rule that is safe for propositional reasoning may
be unsafe for type-checking; thus, some of the ‘safe’ tactics are misnamed.

\texttt{mp_tac i} searches in subgoal \( i \) for assumptions of the form \( f \in \Pi(A, B) \) and
\( a \in A \), where \( A \) may be found by unification. It replaces \( f \in \Pi(A, B) \)
by \( z \in B(a) \), where \( z \) is a new parameter. The tactic can produce
multiple outcomes for each suitable pair of assumptions. In short,
\texttt{mp_tac} performs Modus Ponens among the assumptions.
add_mp_tac \( i \) is like mp_tac \( i \) but retains the assumption \( f \in \Pi(A, B) \). It avoids information loss but obviously loops if repeated.

safestep_tac \( \text{thms} \) \( i \) attacks subgoal \( i \) using formation rules and certain other ‘safe’ rules (FE, ProdI, SumE, PlusE), calling mp_tac when appropriate. It also uses \( \text{thms} \), which are typically premises of the rule being derived.

safe_tac \( \text{thms} \) \( i \) attempts to solve subgoal \( i \) by means of backtracking, using safestep_tac.

step_tac \( \text{thms} \) \( i \) tries to reduce subgoal \( i \) using safestep_tac, then tries unsafe rules. It may produce multiple outcomes.

pc_tac \( \text{thms} \) \( i \) tries to solve subgoal \( i \) by backtracking, using step_tac.

### 5.7 A theory of arithmetic

Arith is a theory of elementary arithmetic. It proves the properties of addition, multiplication, subtraction, division, and remainder, culminating in the theorem

\[
a \mod b + (a/b) \times b = a.
\]

Figure 5.11 presents the definitions and some of the key theorems, including commutative, distributive, and associative laws.

The operators \( + \), \( - \), \( \mid\mid \), \( \times \), \( \mod \) and \( \div \) stand for sum, difference, absolute difference, product, remainder and quotient, respectively. Since Type Theory has only primitive recursion, some of their definitions may be obscure.

The difference \( a - b \) is computed by taking \( b \) predecessors of \( a \), where the predecessor function is \( \lambda v . \text{rec}(v, 0, \lambda x y . x) \).

The remainder \( a \mod b \) counts up to \( a \) in a cyclic fashion, using 0 as the successor of \( b - 1 \). Absolute difference is used to test the equality \( \text{succ}(v) = b \). The quotient \( a/b \) is computed by adding one for every number \( x \) such that \( 0 \leq x \leq a \) and \( x \mod b = 0 \).

### 5.8 The examples directory

This directory contains examples and experimental proofs in CTT.

CTT/ex/typechk.ML contains simple examples of type-checking and type deduction.
## CHAPTER 5. CONSTRUCTIVE TYPE THEORY

<table>
<thead>
<tr>
<th>symbol</th>
<th>meta-type</th>
<th>priority</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#*</td>
<td>[i,i] ⇒ i</td>
<td>Left 70</td>
<td>multiplication</td>
</tr>
<tr>
<td>div</td>
<td>[i,i] ⇒ i</td>
<td>Left 70</td>
<td>division</td>
</tr>
<tr>
<td>mod</td>
<td>[i,i] ⇒ i</td>
<td>Left 70</td>
<td>modulus</td>
</tr>
<tr>
<td>#+</td>
<td>[i,i] ⇒ i</td>
<td>Left 65</td>
<td>addition</td>
</tr>
<tr>
<td>-</td>
<td>[i,i] ⇒ i</td>
<td>Left 65</td>
<td>subtraction</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>[i,i] ⇒ i</td>
<td>Left 65</td>
</tr>
</tbody>
</table>

add_def a#b == rec(a, b, %u v. succ(v))
diff_def a-b == rec(b, a, %u v. rec(v, 0, %x y. x))
absdiff_def a|-|b == (a-b) #+ (b-a)
mult_def a##b == rec(a, 0, %u v. b #+v)

mod_def a mod b == rec(a, 0, %u v. rec(succ(v) |-| b, 0, %x y. succ(v)))
div_def a div b == rec(a, 0, %u v. rec(succ(u) mod b, succ(v), %x y. v))

add_typing [% a:N; b:N |] ==> a #+ b : N
addC0 b:N ==> 0 #+ b = b : N
addC_succ [% a:N; b:N |] ==> succ(a) #+ b = succ(a #+ b) : N

add_assoc [% a:N; b:N; c:N |] ==> (a #+ b) #+ c = a #+ (b #+ c) : N
add_commute [% a:N; b:N; c:N |] ==> a #+ b = b #+ a : N

mult_typing [% a:N; b:N |] ==> a #* b : N
multC0 b:N ==> 0 #* b = 0 : N
multC_succ [% a:N; b:N |] ==> succ(a) #* b = b #* (a#*b) : N
mult_commute [% a:N; b:N |] ==> a #* b = b #* a : N

add_mult_dist [% a:N; b:N; c:N |] ==> (a #+ b) #* c = (a #* c) #+ (b #* c) : N

mult_assoc [% a:N; b:N; c:N |] ==> (a #* b) #* c = a #* (b #* c) : N

diff_typing [% a:N; b:N |] ==> a - b : N
diffC0 a:N ==> a - 0 = a : N
diff_0_eq_0 b:N ==> 0 - b = 0 : N
diff_succ_succ [% a:N; b:N |] ==> succ(a) - succ(b) = a - b : N
diff_self_eq_0 a:N ==> a - a = 0 : N
add_inverse_diff [% a:N; b:N; b-a=0 : N |] ==> b #+ (a-b) = a : N

Figure 5.11: The theory of arithmetic
CTT/ex/elim.ML contains some examples from Martin-Löf [9], proved using pc_tac.

CTT/ex/equal.ML contains simple examples of rewriting.

CTT/ex/synth.ML demonstrates the use of unknowns with some trivial examples of program synthesis.

5.9 Example: type inference

Type inference involves proving a goal of the form \( a \in \mathcal{A} \), where \( a \) is a term and \( \mathcal{A} \) is an unknown standing for its type. The type, initially unknown, takes shape in the course of the proof. Our example is the predecessor function on the natural numbers.

Goal "lam n. rec(n, 0, %x y. x) : ?A";
Level 0
lam n. rec(n,0, %x y. x) : ?A
1. lam n. rec(n,0, %x y. x) : ?A

Since the term is a Constructive Type Theory \( \lambda \)-abstraction (not to be confused with a meta-level abstraction), we apply the rule ProdI, for \( \Pi \)-introduction. This instantiates \( \mathcal{A} \) to a product type of unknown domain and range.

by (resolve_tac [ProdI] 1);
Level 1
lam n. rec(n,0, %x y. x) : PROD x:?A1. ?B1(x)
1. ?A1 type
2. !!n. n : ?A1 ==> rec(n,0, %x y. x) : ?B1(n)

Subgoal 1 is too flexible. It can be solved by instantiating \( ?A_1 \) to any type, but most instantiations will invalidate subgoal 2. We therefore tackle the latter subgoal. It asks the type of a term beginning with rec, which can be found by \( N \)-elimination.

Subgoal 1 is no longer flexible: we now know \( ?A_1 \) is the type of natural numbers. However, let us continue proving nontrivial subgoals. Subgoal 2 asks, what is the type of 0?
CHAPTER 5. CONSTRUCTIVE TYPE THEORY

by (resolve_tac [NI0] 2);
Level 3
lam n. rec(n,0,%x y. x) : N --> N
1. N type
2. !!n x y. [| x : N; y : N |] ==> x : N

The type ?A is now fully determined. It is the product type \( \prod_{x \in \mathbb{N}} N \), which is shown as the function type \( N \rightarrow N \) because there is no dependence on \( x \).
But we must prove all the subgoals to show that the original term is validly typed. Subgoal 2 is provable by assumption and the remaining subgoal falls by \( N \)-formation.

by (assume_tac 2);
Level 4
lam n. rec(n,0,%x y. x) : N --> N
1. N type
by (resolve_tac [NF] 1);
Level 5
lam n. rec(n,0,%x y. x) : N --> N
No subgoals!

Calling typechk_tac can prove this theorem in one step.

Even if the original term is ill-typed, one can infer a type for it, but unprovable subgoals will be left. As an exercise, try to prove the following invalid goal:

Goal "lam n. rec(n, 0, %x y. tt) : ?A";

5.10 An example of logical reasoning

Logical reasoning in Type Theory involves proving a goal of the form \( \exists a \in A \), where type \( A \) expresses a proposition and \( a \) stands for its proof term, a value of type \( A \). The proof term is initially unknown and takes shape during the proof.

Our example expresses a theorem about quantifiers in a sorted logic:

\[
\exists x \in A . P(x) \lor Q(x) \\
(\exists x \in A . P(x)) \lor (\exists x \in A . Q(x))
\]

By the propositions-as-types principle, this is encoded using \( \Sigma \) and \( + \) types. A special case of it expresses a distributive law of Type Theory:

\[
A \times (B + C) \\
(A \times B) + (A \times C)
\]
Generalizing this from $\times$ to $\Sigma$, and making the typing conditions explicit, yields the rule we must derive:

$$
\begin{array}{c}
\vdash \quad \vdash \\
A \text{ type} \quad B(x) \text{ type} \quad C(x) \text{ type} \quad p \in \sum_{x \in A} B(x) + C(x) \\
\hline
\quad ?a \in (\sum_{x \in A} B(x)) + (\sum_{x \in A} C(x))
\end{array}
$$

To begin, we bind the rule’s premises — returned by the goal command — to the ML variable prems.

```ml
val prems = Goal
  "[| A type; \\
    \!!x. x:A ==> B(x) type; \\
    \!!x. x:A ==> C(x) type; \\
    p: SUM x:A. B(x) + C(x) |
    |] ==> ?a : (SUM x:A. B(x)) + (SUM x:A. C(x))";
```

The last premise involves the sum type $\Sigma$. Since it is a premise rather than the assumption of a goal, it cannot be found by eresolve_tac. We could insert it (and the other atomic premise) by calling

`cut_facts_tac prems 1;`

A forward proof step is more straightforward here. Let us resolve the $\Sigma$-elimination rule with the premises using RL. This inference yields one result, which we supply to resolve_tac.

```ml
by (resolve_tac (prems RL [SumE]) 1);
```

The subgoal has two new parameters, $x$ and $y$. In the main goal, $?a$ has been instantiated with a `split` term. The assumption $y \in B(x) + C(x)$ is eliminated next, causing a case split and creating the parameter $xa$. This inference also inserts when into the main goal.
by (eresolve_tac [PlusE] 1);

Level 2
split(p,% x y. when(y,?c2(x,y),?d2(x,y)))
: (SUM x:A. B(x)) + (SUM x:A. C(x))
1. !!x y xa.
   [| x : A; xa : B(x) |] ==> 
   ?c2(x,y,xa) : (SUM x:A. B(x)) + (SUM x:A. C(x))
2. !!x y ya.
   [| x : A; ya : C(x) |] ==> 
   ?d2(x,y,ya) : (SUM x:A. B(x)) + (SUM x:A. C(x))

To complete the proof object for the main goal, we need to instantiate the terms \(?c2(x,y,xa)\) and \(?d2(x,y,ya)\). We attack subgoal 1 by a +-introduction rule; since the goal assumes \(xa \in B(x)\), we take the left injection (\(\text{inl}\)).

by (resolve_tac [PlusI_inl] 1);

Level 3
split(p,% x y. when(y,%xa. \text{inl}(?a3(x,y,xa)),?d2(x,y)))
: (SUM x:A. B(x)) + (SUM x:A. C(x))
1. !!x y xa. [| x : A; xa : B(x) |] ==> 
   ?a3(x,y,xa) : SUM x:A. B(x)
2. !!x y xa. [| x : A; xa : B(x) |] ==> SUM x:A. C(x) type
3. !!x y ya.
   [| x : A; ya : C(x) |] ==> 
   ?d2(x,y,ya) : (SUM x:A. B(x)) + (SUM x:A. C(x))

A new subgoal 2 has appeared, to verify that \(\sum_{x \in A} C(x)\) is a type. Continuing to work on subgoal 1, we apply the \(\Sigma\)-introduction rule. This instantiates the term \(?a3(x,y,xa)\); the main goal now contains an ordered pair, whose components are two new unknowns.

by (resolve_tac [SumI] 1);

Level 4
split(p,% x y. when(y,%xa. \text{inl}(<x,?b4(x,y,xa)>,?d2(x,y)))
: (SUM x:A. B(x)) + (SUM x:A. C(x))
1. !!x y xa. [| x : A; xa : B(x) |] ==> 
   ?a4(x,y,xa) : A
2. !!x y xa. [| x : A; xa : B(x) |] ==> 
   ?b4(x,y,xa) : B(?a4(x,y,xa))
3. !!x y xa. [| x : A; xa : B(x) |] ==> 
   SUM x:A. C(x) type
4. !!x y ya.
   [| x : A; ya : C(x) |] ==> 
   ?d2(x,y,ya) : (SUM x:A. B(x)) + (SUM x:A. C(x))

The two new subgoals both hold by assumption. Observe how the unknowns \(?a4\) and \(?b4\) are instantiated throughout the proof state.

by (assume_tac 1);

Level 5
split(p,% x y. when(y,%xa. \text{inl}(<x,?b4(x,y,xa)>,?d2(x,y)))
: (SUM x:A. B(x)) + (SUM x:A. C(x))
1. $\forall x \ y \ xa. [\ [x : A; xa : B(x)] \implies ?b4(x,y,xa) : B(x)]$
2. $\forall x \ y \ xa. [\ [x : A; xa : B(x)] \implies \text{SUM } x:A. \ C(x) \text{ type}$
3. $\forall x \ y \ ya. [\ [x : A; ya : C(x)] \implies ?d2(x,y,ya) : \text{(SUM } x:A. \ B(x)) + \text{(SUM } x:A. \ C(x))$ by (assume_tac 1);

Level 6
split(p,%x y. when(y,%xa. inl(<x,xa>),?d2(x,y)))
1. $\forall x \ y \ xa. [\ [x : A; xa : B(x)] \implies \text{SUM } x:A. \ C(x) \text{ type}$
2. $\forall x \ y \ ya. [\ [x : A; ya : C(x)] \implies ?d2(x,y,ya) : \text{(SUM } x:A. \ B(x)) + \text{(SUM } x:A. \ C(x))$

Subgoal 1 is an example of a well-formedness subgoal [3]. Such subgoals are usually trivial; this one yields to typechk_tac, given the current list of premises.

by (typechk_tac prems);

Level 7
split(p,%x y. when(y,%xa. inl(<x,xa>),?d2(x,y)))
1. $\forall x \ y \ xa. [\ [x : A; xa : B(x)] \implies \text{SUM } x:A. \ C(x) \text{ type}$
2. $\forall x \ y \ ya. [\ [x : A; ya : C(x)] \implies ?d2(x,y,ya) : \text{(SUM } x:A. \ B(x)) + \text{(SUM } x:A. \ C(x))$

This subgoal is the other case from the $+$-elimination above, and can be proved similarly. Quicker is to apply pc_tac. The main goal finally gets a fully instantiated proof object.

by (pc_tac prems 1);

Level 8
split(p,%x y. when(y,%xa. inl(<x,xa>),%y. inr(<x,y>)))
1. $\forall x \ y \ xa. [\ [x : A; xa : B(x)] \implies \text{SUM } x:A. \ B(x)) + \text{(SUM } x:A. \ C(x))$

No subgoals!

Calling pc_tac after the first $\Sigma$-elimination above also proves this theorem.

### 5.11 Example: deriving a currying functional

In simply-typed languages such as ML, a currying functional has the type

$$ (A \times B \to C) \to (A \to (B \to C)). $$

Let us generalize this to the dependent types $\Sigma$ and $\Pi$. The functional takes a function $f$ that maps $z : \Sigma(A,B)$ to $C(z)$; the resulting function maps $x \in A$ and $y \in B(x)$ to $C(\langle x,y \rangle)$. 

Formally, there are three typing premises. $A$ is a type; $B$ is an $A$-indexed family of types; $C$ is a family of types indexed by $\Sigma(A, B)$. The goal is expressed using $\text{PROD } f$ to ensure that the parameter corresponding to the functional’s argument is really called $f$; Isabelle echoes the type using $\rightarrow$ because there is no explicit dependence upon $f$.

Val prems = Goal

\[
\begin{align*}
| A \text{ type; } !!x. x:A \Rightarrow B(x) \text{ type; } \\
| !!z. z: (\Sigma x:A. B(x)) \Rightarrow C(z) \text{ type } \\
| \Rightarrow \ ?a : \text{PROD } f: (\text{PROD } z: (\Sigma x:A. B(x)). C(z)). \\
& (\text{PROD } x:A. \text{PROD } y:B(x). C(<x,y>))
\end{align*}
\]

Level 0

?a : (PROD z:SUM x:A. B(x). C(z)) -->

(\text{PROD } x:A. \text{PROD } y:B(x). C(<x,y>))

1. ?a : (PROD z:SUM x:A. B(x). C(z)) -->

(\text{PROD } x:A. \text{PROD } y:B(x). C(<x,y>))

Val prems = ["A type [A type]",
"?x : A \Rightarrow B(?x) type [!!x. x : A \Rightarrow B(x) type]",
"?z : SUM x:A. B(x) \Rightarrow C(?z) type 
[!!z. z : SUM x:A. B(x) \Rightarrow C(z) type]" ] : thm list

This is a chance to demonstrate intr_tac. Here, the tactic repeatedly applies $\Pi$-introduction and proves the rather tiresome typing conditions.

Note that ?a becomes instantiated to three nested $\lambda$-abstractions. It would be easier to read if the bound variable names agreed with the parameters in the subgoal. Isabelle attempts to give parameters the same names as corresponding bound variables in the goal, but this does not always work. In any event, the goal is logically correct.

By (intr_tac prems);

Level 1

lam x xa xb. ?b7(x,xa,xb)
: (PROD z:SUM x:A. B(x). C(z)) --> (PROD x:A. \text{PROD } y:B(x). C(<x,y>))

1. !!f x y.

[| f : PROD z:SUM x:A. B(x). C(z); x : A; y : B(x) |] ==>

?b7(f,x,y) : C(<x,y>)

Using $\Pi$-elimination, we solve subgoal 1 by applying the function $f$.

By (eresolve_tac [ProdE] 1);

Level 2

lam x xa xb. x \ <xa,xb
: (PROD z:SUM x:A. B(x). C(z)) --> (PROD x:A. \text{PROD } y:B(x). C(<x,y>))

1. !!f x y. [| x : A; y : B(x) |] ==> <x,y> : SUM x:A. B(x)

Finally, we verify that the argument’s type is suitable for the function application. This is straightforward using introduction rules.
CHAPTER 5. CONSTRUCTIVE TYPE THEORY

by (intr_tac prems);
Level 3
lam x xa xb. x ` <xa,xb>
: (PROD z:SUM x:A. B(x). C(z)) --> (PROD x:A. PROD y:B(x). C(<x,y>))
No subgoals!

Calling pc_tac would have proved this theorem in one step; it can also prove
an example by Martin-Löf, related to ∨-elimination [9, page 58].

5.12 Example: proving the Axiom of Choice

Suppose we have a function \( h \in \Pi_{x \in A} \Sigma_{y \in B(x)} C(x, y) \), which takes \( x \in A \) to
some \( y \in B(x) \) paired with some \( z \in C(x, y) \). Interpreting propositions as
types, this asserts that for all \( x \in A \) there exists \( y \in B(x) \) such that \( C(x, y) \).
The Axiom of Choice asserts that we can construct a function \( f \in \Pi_{x \in A} B(x) \)
such that \( C(x, f(x)) \) for all \( x \in A \), where the latter property is witnessed by a
function \( g \in \Pi_{x \in A} C(x, f(x)) \).

In principle, the Axiom of Choice is simple to derive in Constructive Type
Theory. The following definitions work:

\[
\begin{align*}
  f & \equiv \text{fst} \circ h \\
  g & \equiv \text{snd} \circ h
\end{align*}
\]

But a completely formal proof is hard to find. The rules can be applied
in countless ways, yielding many higher-order unifiers. The proof can get
bogged down in the details. But with a careful selection of derived rules
(recall Fig. 5.10) and the type-checking tactics, we can prove the theorem in
nine steps.

val prems = Goal
"[| A type; !!x. x:A ==> B(x) type; \
  !x y. [| x:A; y:B(x) |] ==> C(x,y) type \
  |] ==> ?a : PROD h: (PROD x:A. SUM y:B(x). C(x,y)). \
  (SUM f: (PROD x:A. B(x)). PROD x:A. C(x, f`x))";

First, intr_tac applies introduction rules and performs routine type-
checking. This instantiates \(?a\) to a construction involving a \( \lambda \)-abstraction
and an ordered pair. The pair’s components are themselves λ-abstractions and there is a subgoal for each.

by (intr_tac prems);

Level 1

lam x. <lam xa. ?b7(x,xa),lam xa. ?b8(x,xa)>
: (PROD x:A. SUM y:B(x). C(x,y)) -->
(SUM f:PROD x:A. B(x). PROD x:A. C(x,f ` x))
1. !!h x.
   [| h : PROD x:A. SUM y:B(x). C(x,y); x : A |] ==> ?b7(h,x) : B(x)
2. !!h x.
   [| h : PROD x:A. SUM y:B(x). C(x,y); x : A |] ==> ?b8(h,x) : C(x,(lam x. ?b7(h,x)) ` x)

Subgoal 1 asks to find the choice function itself, taking \( x \in A \) to some \(?b_7(h,x) \in B(x)\). Subgoal 2 asks, given \( x \in A \), for a proof object \(?b_8(h,x)\) to witness that the choice function’s argument and result lie in the relation \( C \).

This latter task will take up most of the proof.

by (eresolve_tac [ProdE RS SumE_fst] 1);

Level 2

lam x. <lam xa. fst(x ` xa),lam xa. ?b8(x,xa)>
: (PROD x:A. SUM y:B(x). C(x,y)) -->
(SUM f:PROD x:A. B(x). PROD x:A. C(x,f ` x))
1. !!h x. x : A ==> x : A
2. !!h x.
   [| h : PROD x:A. SUM y:B(x). C(x,y); x : A |] ==> ?b8(h,x) : C(x,(lam x. fst(h ` x)) ` x)

Above, we have composed \( \text{fst} \) with the function \( h \). Unification has deduced that the function must be applied to \( x \in A \). We have our choice function.

by (assume_tac 1);

Level 3

lam x. <lam xa. fst(x ` xa),lam xa. ?b8(x,xa)>
: (PROD x:A. SUM y:B(x). C(x,y)) -->
(SUM f:PROD x:A. B(x). PROD x:A. C(x,f ` x))
1. !!h x.
   [| h : PROD x:A. SUM y:B(x). C(x,y); x : A |] ==> ?b8(h,x) : C(x,(lam x. fst(h ` x)) ` x)

Before we can compose \( \text{snd} \) with \( h \), the arguments of \( C \) must be simplified.

The derived rule \( \text{replace_type} \) lets us replace a type by any equivalent type, shown below as the schematic term \(?A_{13}(h,x)\):

by (resolve_tac [replace_type] 1);

Level 4

lam x. <lam xa. fst(x ` xa),lam xa. ?b8(x,xa)>
: (PROD x:A. SUM y:B(x). C(x,y)) -->
(SUM f:PROD x:A. B(x). PROD x:A. C(x,f ` x))
CHAPTER 5. CONSTRUCTIVE TYPE THEORY

1. \forall h x. 
   \[ | h : \text{PROD} x:A. \text{SUM} y:B(x). C(x,y); x : A | \]  
   \[ \Rightarrow C(x,(\text{lam} x. \text{fst}(h ` x)) ` x) = ?A13(h,x) \]

2. \forall h x. 
   \[ | h : \text{PROD} x:A. \text{SUM} y:B(x). C(x,y); x : A | \]  
   \[ ?b8(h,x) : ?A13(h,x) \]

The derived rule \texttt{subst_eqtyparg} lets us simplify a type's argument (by currying, \( C(x) \) is a unary type operator):

by (resolve_tac [subst_eqtyparg] 1);

Level 5

\begin{align*}
\lambda x. \langle \lambda xa. \text{fst}(x ` xa), \lambda xa. ?b8(x,xa) \rangle \\
: \text{PROD} x:A. \text{SUM} y:B(x). C(x,y) \rightarrow \text{PROD} x:A. C(x,f ` x) \\
\end{align*}

1. \forall h x. 
   \[ | h : \text{PROD} x:A. \text{SUM} y:B(x). C(x,y); x : A | \]  
   \[ \Rightarrow (\text{lam} x. \text{fst}(h ` x)) ` x = ?c14(h,x) : ?A14(h,x) \]

2. \forall h x z. 
   \[ | h : \text{PROD} x:A. \text{SUM} y:B(x). C(x,y); x : A; z : ?A14(h,x) | \]  
   \[ C(x,z) \text{ type} \]

3. \forall h x. 
   \[ | h : \text{PROD} x:A. \text{SUM} y:B(x). C(x,y); x : A | \]  
   \[ ?b8(h,x) : C(x,?c14(h,x)) \]

Subgoal 1 requires simply \( \beta \)-contraction, which is the rule \texttt{ProdC}. The term \(?c14(h,x)\) in the last subgoal receives the contracted result.

by (resolve_tac [ProdC] 1);

Level 6

\begin{align*}
\lambda x. \langle \lambda xa. \text{fst}(x ` xa), \lambda xa. ?b8(x,xa) \rangle \\
: \text{PROD} x:A. \text{SUM} y:B(x). C(x,y) \rightarrow \text{PROD} x:A. C(x,f ` x) \\
\end{align*}

1. \forall h x. 
   \[ | h : \text{PROD} x:A. \text{SUM} y:B(x). C(x,y); x : A | \]  
   \[ x : ?A15(h,x) \]

2. \forall h x xa. 
   \[ | h : \text{PROD} x:A. \text{SUM} y:B(x). C(x,y); x : A; xa : ?A15(h,x) | \]  
   \[ \text{fst}(h ` xa) : ?B15(h,x,xa) \]

3. \forall h x z. 
   \[ | h : \text{PROD} x:A. \text{SUM} y:B(x). C(x,y); x : A; z : ?B15(h,x,x) | \]  
   \[ C(x,z) \text{ type} \]

4. \forall h x. 
   \[ | h : \text{PROD} x:A. \text{SUM} y:B(x). C(x,y); x : A | \]  
   \[ ?b8(h,x) : C(x,\text{fst}(h ` x)) \]

Routine type-checking goals proliferate in Constructive Type Theory, but
typechk_tac quickly solves them. Note the inclusion of SumE_fst along with the premises.

by (typechk_tac (SumE_fst::prems));

Level 7
lam x. <lam xa. fst(x ` xa),lam xa. ?b8(x,xa)>
: (PROD x:A. SUM y:B(x). C(x,y)) -->
(SUM f:PROD x:A. B(x). PROD x:A. C(x,f ` x))
1. !!h x.
   [| h : PROD x:A. SUM y:B(x). C(x,y); x : A |] ==> ?b8(h,x) : C(x,fst(h ` x))

We are finally ready to compose snd with h.

by (eresolve_tac [ProdE RS SumE_snd] 1);

Level 8
lam x. <lam xa. fst(x ` xa),lam xa. snd(x ` xa)>
: (PROD x:A. SUM y:B(x). C(x,y)) -->
(SUM f:PROD x:A. B(x). PROD x:A. C(x,f ` x))
1. !!h x. x : A ==> x : A
2. !!h x. x : A ==> B(x) type
3. !!h x xa. [| x : A; xa : B(x) |] ==> C(x,xa) type

The proof object has reached its final form. We call typechk_tac to finish the type-checking.

by (typechk_tac prems);

Level 9
lam x. <lam xa. fst(x ` xa),lam xa. snd(x ` xa)>
: (PROD x:A. SUM y:B(x). C(x,y)) -->
(SUM f:PROD x:A. B(x). PROD x:A. C(x,f ` x))
No subgoals!

It might be instructive to compare this proof with Martin-Löf's forward proof of the Axiom of Choice [9, page 50].
Bibliography


Index

<table>
<thead>
<tr>
<th>symbol, 6, 9, 16, 17, 30</th>
<th>add_def theorem, 76</th>
</tr>
</thead>
<tbody>
<tr>
<td>symbol, 6, 45</td>
<td>add_inverse_diff theorem, 76</td>
</tr>
<tr>
<td>symbol, 6, 45</td>
<td>add_mp_tac, 75</td>
</tr>
<tr>
<td>symbol, 76</td>
<td>add_mult_dist theorem, 76</td>
</tr>
<tr>
<td>symbol, 30</td>
<td>add_safes, 57</td>
</tr>
<tr>
<td>symbol, 30</td>
<td>add_typing theorem, 76</td>
</tr>
<tr>
<td>symbol, 76</td>
<td>add_unsafes, 57</td>
</tr>
<tr>
<td>symbol, 6, 45</td>
<td>addC0 theorem, 76</td>
</tr>
<tr>
<td>constant, 26</td>
<td>addC_succ theorem, 76</td>
</tr>
<tr>
<td>symbol, 5, 27, 66</td>
<td>Addsplits, 23</td>
</tr>
<tr>
<td>symbol, 5, 27, 66</td>
<td>addsplits, 23, 29, 36</td>
</tr>
<tr>
<td>symbol, 5, 27, 66</td>
<td>ALL symbol, 6, 16, 17, 45</td>
</tr>
<tr>
<td>symbol, 5, 27, 76</td>
<td>All constant, 6, 45</td>
</tr>
<tr>
<td>symbol, 6, 45, 66</td>
<td>All_def theorem, 11</td>
</tr>
<tr>
<td>symbol, 6, 27</td>
<td>all_dupE theorem, 13</td>
</tr>
<tr>
<td>symbol, 15</td>
<td>allE theorem, 13</td>
</tr>
<tr>
<td>constant, 26</td>
<td>allI theorem, 13</td>
</tr>
<tr>
<td>symbol, 27</td>
<td>allL theorem, 48, 57</td>
</tr>
<tr>
<td>symbol, 27</td>
<td>allL_thin theorem, 49</td>
</tr>
<tr>
<td>symbol, 15</td>
<td>allR theorem, 48</td>
</tr>
<tr>
<td>symbol, 27</td>
<td>and_def theorem, 11</td>
</tr>
<tr>
<td>symbol, 45</td>
<td>arg_cong theorem, 12</td>
</tr>
<tr>
<td>symbol, 27</td>
<td>Arith theory, 75</td>
</tr>
<tr>
<td>symbol, 6, 45, 66</td>
<td>assumptions</td>
</tr>
<tr>
<td>symbol, 6, 45, 66</td>
<td>in CTT, 63, 74</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>constant, 8, 27, 64</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>add_safes theorem, 64</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>constant, 8, 27, 64</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>adddef_def theorem, 47</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>absolute difference, 76</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>add_assoc theorem, 76</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>add_commutate theorem, 76</th>
</tr>
</thead>
</table>
INDEX

bexCI theorem, 18, 20
bxE theorem, 18
bexI theorem, 18, 20
bool type, 5
box_equals theorem, 11, 12
bspec theorem, 18
butlast constant, 30

case symbol, 28, 29, 36
case_sum constant, 26
case_sum_Inl theorem, 26
case_sum_Inr theorem, 26
case_tac, 11, 38
case_weak_cong, 37
CCL theory, 1
ccontr theorem, 13
classical theorem, 13
Collect constant, 14, 15
Collect_mem_eq theorem, 17
CollectD theorem, 18, 42
CollectE theorem, 18
CollectI theorem, 18, 43
comp_rls, 72
Compl_def theorem, 17
Compl_disjoint theorem, 21
Compl_Int theorem, 21
Compl_partition theorem, 21
Compl_Un theorem, 21
ComplD theorem, 19
ComplI theorem, 19
concat constant, 30
cong theorem, 12
conj_cong, 22
conjE theorem, 12
conjI theorem, 12
conjL theorem, 48
conjR theorem, 48
conjunct1 theorem, 12
conjunct2 theorem, 12
Constructive Type Theory, 63–86
context, 43

contL theorem, 49
contLS theorem, 47
contr theorem, 49
contr constant, 64
contRS theorem, 47
could_res, 52
could_resolve_seq, 52
CTT theory, 1, 63
Cube theory, 1
cut theorem, 47
cutL_tac, 51
cutR_tac, 51
datatype, 29
delsplits, 23
delsplits, 23
diff_0_eq_0 theorem, 76
diff_def theorem, 76
diff_self_eq_0 theorem, 76
diff_succ_succ theorem, 76
diff_typing theorem, 76
diffC0 theorem, 76
disjCI theorem, 13
disjE theorem, 12
disjI theorem, 12
disj2 theorem, 12
disjL theorem, 48
disjR theorem, 48
div symbol, 27, 76
div_def theorem, 76
div_geq theorem, 27
div_less theorem, 27
Divides theory, 26
double_complement theorem, 21
drop constant, 30
dropWhile constant, 30
dvd symbol, 27

Elem constant, 64
elim_rls, 72
elimL_rls, 72
empty_def theorem, 17
empty_pack, 56
emptyE theorem, 19
Eps constant, 6, 8
Eq constant, 64
eq constant, 64, 72
Eq theorem, 71
EqE theorem, 71
Eqelem constant, 64
EqF theorem, 71
EqFL theorem, 71
EqI theorem, 71
Eqtype constant, 64
equal_tac, 73
equal_types theorem, 67
equal_typesL theorem, 67
equalityCE theorem, 18, 20, 42, 43
equalityD1 theorem, 18
equalityD2 theorem, 18
equalityE theorem, 18
equalityI theorem, 18
EX symbol, 6, 16, 17, 45
Ex constant, 6, 45
EX! symbol, 6
Ex1 constant, 6
Ex1_def theorem, 11
ex1E theorem, 13
ex1I theorem, 13
Ex_def theorem, 11
exCI theorem, 13
excluded_middle theorem, 13
exE theorem, 13
exI theorem, 13
exL theorem, 48
exR theorem, 48, 52, 57
exR_thin theorem, 49, 52, 53
ext theorem, 10
F constant, 64
False constant, 6, 45
False_def theorem, 11
FalseE theorem, 12
FalseL theorem, 48
fast_tac, 58
FE theorem, 70, 75
FEL theorem, 70
FF theorem, 70
filseq_resolve_tac, 52
filt_resolve_tac, 52, 73
filter constant, 30
flex-flex constraints, 55
FOL theory, 74
foldl constant, 30
form_rls, 72
formL_rls, 72
forms_of_seq, 51
fst constant, 24, 64, 71, 72
fst_conv theorem, 24
fst_def theorem, 69
Fun theory, 21
fun type, 5
fun_cong theorem, 12
function applications
  in CTT, 66
hd constant, 30
higher-order logic, 5–43
HOL, 9
HOL system, 5, 9
HOL_basic_ss, 22
HOL_ss, 22
HOLCF theory, 1
hyp_rew_tac, 74
hyp_subst_tac, 22
i type, 63
If constant, 6
if, 22
if_def theorem, 11
if_not_P theorem, 13
if_P theorem, 13
if_weak_cong, 22
iff theorem, 10
iff_def theorem, 48
iffCE theorem, 13, 20
iffD1 theorem, 12
iffD2 theorem, 12
iffE theorem, 12
iffI theorem, 12
iffL theorem, 49, 54
iffR theorem, 49
ILL theory, 2
image_def theorem, 17
imageE theorem, 19
imageI theorem, 19
impCE theorem, 13
impE theorem, 12
impI theorem, 10
impL theorem, 48
impR theorem, 48
in symbol, 7
ind type, 26
induct_tac, 28, 37
inj constant, 21
inj_def theorem, 21
inj_Inl theorem, 26
inj_Inr theorem, 26
inj_on constant, 21
inj_on_def theorem, 21
inj_Suc theorem, 27
Inl constant, 26
Inl constant, 64, 71, 80
Inl_not_Inr theorem, 26
Inr constant, 26
inr constant, 64, 71
insert constant, 15
insert_def theorem, 17
insertE theorem, 19
insertI1 theorem, 19
insertI2 theorem, 19
INT symbol, 15–17
Int symbol, 15
int theorem, 8, 28
Int_absorb theorem, 21
Int_assoc theorem, 21
Int_commute theorem, 21
INT_D theorem, 19
Int_def theorem, 17
INT_E theorem, 19
Int_greatest theorem, 20
INT_I theorem, 19
Int_lower1 theorem, 20
Int_lower2 theorem, 20
Int_Un_distrib theorem, 21
Int_Union theorem, 21
IntD1 theorem, 19
IntD2 theorem, 19
IntE theorem, 19
INTER constant, 15
Inter constant, 15
INTER1 constant, 15
INTER1_def theorem, 17
INTER_def theorem, 17
Inter_def theorem, 17
Inter_greatest theorem, 20
Inter_lower theorem, 20
Inter_Un_distrib theorem, 21
InterD theorem, 19
InterE theorem, 19
InterI theorem, 19
IntI theorem, 19
intr_rls, 72
intr_tac, 73, 82, 83
intrL_rls, 72
inv constant, 21
inv_def theorem, 21
lam symbol, 66
lambda constant, 64, 66
\lambda-abstractions
in CTT, 66
last constant, 30
LCF theory, 1
LEAST constant, 8, 9, 26
INDEX

Least constant, 6
Least_def theorem, 11
length constant, 30
less_induct theorem, 28
Let constant, 6, 9
let symbol, 7
Let_def theorem, 9, 11
Lin_Arith.tac, 29
linorder class, 8, 26, 28
List theory, 29, 30
list type, 29
list_split theorem, 29
LK theory, 1, 44, 49
LK_dup_pack, 57, 58
LK_pack, 57

map constant, 30
max constant, 8, 26
mem symbol, 30
mem_Collect_eq theorem, 17
min constant, 8, 26
minus class, 5
mod symbol, 27, 76
mod_def theorem, 76
mod_geq theorem, 27
mod_less theorem, 27
Modal theory, 1
mono constant, 8
mp theorem, 10
mp_tac, 74
mult_assoc theorem, 76
mult_commute theorem, 76
mult_def theorem, 76
mult_typing theorem, 76
multC0 theorem, 76
multC_succ theorem, 76

N constant, 64
n_not_Suc_n theorem, 27
Nat theory, 26
nat type, 26, 27

nat theorem, 8
nat_induct theorem, 27
NatArith theory, 26
NCO theorem, 68
NC_succ theorem, 68
NE theorem, 68, 71, 77
NEL theorem, 68
NF theorem, 68, 78
NIO theorem, 68
NI_succ theorem, 68
NI_succL theorem, 68
NIO theorem, 77
Not constant, 6, 45
not_def theorem, 11
not_sym theorem, 12
notE theorem, 12
notI theorem, 12
notL theorem, 48
notnotD theorem, 13
notR theorem, 48
null constant, 30

o type, 44
o symbol, 6, 22
o_def theorem, 11
of symbol, 9
or_def theorem, 11
Ord theory, 8
ord class, 8, 9, 26
order class, 8

pack, 56
pack ML type, 56
pack_of thy, 56
Pair constant, 24
pair constant, 64
Pair_inject theorem, 24
pc_tac, 58, 75, 81, 83
plus class, 5
plus_ac0 class, 8
INDEX
94

PlusC_inl theorem, 70
PlusC_inr theorem, 70
PlusE theorem, 70, 75, 79
PlusEL theorem, 70
PlusF theorem, 70
PlusFL theorem, 70
PlusI_inl theorem, 70, 80
PlusI_inlL theorem, 70
PlusI_inr theorem, 70
PlusI_inrL theorem, 70
Pow constant, 15
Pow_def theorem, 17
PowD theorem, 19
power class, 5
PowI theorem, 19
primrec symbol, 28
priorities, 3
PROD symbol, 65, 66
Prod constant, 64
Prod theory, 24
prod.exhaust theorem, 24
prod.inject theorem, 24
prod.split theorem, 24
ProdC theorem, 68, 85
ProdC2 theorem, 68
ProdE theorem, 68, 82, 84, 86
ProdEL theorem, 68
ProdF theorem, 68
ProdFL theorem, 68
ProdI theorem, 68, 75, 77
ProdIL theorem, 68
prop_pack, 57
range constant, 15, 42
range_def theorem, 17
rangeE theorem, 19, 42
rangeI theorem, 19
real theorem, 8, 28
rec constant, 64, 71
rec_nat constant, 28
recdef, 38–41
recursion
general, 38–41
red_if_equal theorem, 67
Reduce constant, 64, 69, 74
refl theorem, 10, 47
refl_elem theorem, 67, 72
refl_red theorem, 67
refl_type theorem, 67, 72
REPEAT_FIRST, 73
repeat_goal_tac, 58
replace_type theorem, 71, 84
reresolve_tac, 58
rew_inst_tac, 8
rew_tac, 74
RL, 79
RS, 84, 86
safe_goal_tac, 58
safe_tac, 75
safestep_tac, 75
search
best-first, 43
Seqof constant, 45
sequent calculus, 44–58
Set theory, 14, 17
set constant, 30
set type, 14
set_diff_def theorem, 17
show_sorts, 8
show_types, 8
Sigma constant, 24
Sigma_def theorem, 24
SigmaE theorem, 24
SigmaI theorem, 24
simplification
of case, 37
of if, 22
of conjunctions, 22
size constant, 37
smp_tac, 11
INDEX

snd constant, 24, 64, 71, 72
snd_conv theorem, 24
snd_def theorem, 69
sobj type, 44
SOME symbol, 6
some_equality theorem, 10, 13
someI theorem, 10
spec theorem, 13
split constant, 24, 64, 79
split theorem, 24
split_all_tac, 25
split_if theorem, 13, 23
ssubst theorem, 11, 12
stac, 22
step_tac, 58, 75
strip_tac, 11
subset_def theorem, 17
subset_refl theorem, 18
subset_trans theorem, 18
subsetCE theorem, 18, 20
subsetD theorem, 18, 20
subsetI theorem, 18
subst theorem, 10, 47
subst_elem theorem, 67
subst_elemL theorem, 67
subset_eqtyparg theorem, 71, 85
subst_prodE theorem, 71, 72
subset_type theorem, 67
subset_typeL theorem, 67
Suc constant, 27
Suc_not_Zero theorem, 27
succ constant, 64
SUM symbol, 65, 66
Sum constant, 64
Sum theory, 25
sum constant, 8
sum_split_case theorem, 26
SumC theorem, 69
SumE theorem, 69, 75, 79
sumE theorem, 26
SumE_fst theorem, 71, 72, 84, 86
SumE_snd theorem, 71, 72, 86
SumEL theorem, 69
SumF theorem, 69
SumFL theorem, 69
SumI theorem, 69, 80
SumIL theorem, 69
SumIL2 theorem, 71
surj constant, 21, 22
surj_def theorem, 21
surjective_pairing theorem, 24
surjective_sum theorem, 26
swap theorem, 13
swap_res_tac, 43
sym theorem, 12
sym_elem theorem, 67
sym_type theorem, 67
symL theorem, 49
symR theorem, 49
T constant, 64
t type, 63
take constant, 30
takeWhile constant, 30
TC theorem, 70
TE theorem, 70
TEL theorem, 70
term class, 5, 44
test_assume_tac, 73
TF theorem, 70
THE symbol, 45
The constant, 45
The theorem, 48
the_equality theorem, 49
thinL theorem, 49
thinLS theorem, 47
thinR theorem, 49
thinRS theorem, 47
TI theorem, 70
times class, 5
tl constant, 30
tracing
INDEX

of unification, 8
trans theorem, 12
trans_elem theorem, 67
trans_red theorem, 67
trans_type theorem, 67
transR theorem, 49
True constant, 6, 45
True_def theorem, 11, 48
True_or_False theorem, 10
TrueI theorem, 12
Trueprop constant, 6, 45
TrueR theorem, 49
tt constant, 64
Type constant, 64
typechk_tac, 73, 78, 81, 86
UN symbol, 15–17
Un symbol, 15
Un1 theorem, 20
Un2 theorem, 20
Un_absorb theorem, 21
Un_assoc theorem, 21
Un_commute theorem, 21
Un_def theorem, 17
UN_E theorem, 19
UN_I theorem, 19
Un_Int_distrib theorem, 21
Un_Inter theorem, 21
Un_least theorem, 20
Un_upper1 theorem, 20
Un_upper2 theorem, 20
UnCI theorem, 19, 20
UnE theorem, 19
UnI1 theorem, 19
UnI2 theorem, 19
unification
    incompleteness of, 8
Unify.trace_types, 8
UNION constant, 15
Union constant, 15
UNION1 constant, 15
UNION1_def theorem, 17
UNION_def theorem, 17
Union_def theorem, 17
Union_least theorem, 20
Union_Un_distrib theorem, 21
Union_upper theorem, 20
UnionE theorem, 19
UnionI theorem, 19
unit_eq theorem, 25
when constant, 64, 71, 79
zero_ne_succ theorem, 68, 69