



Isabelle's Logics: HOL¹

Tobias Nipkow² and Lawrence C. Paulson³ and Markus Wenzel⁴

6 October 2000

¹The research has been funded by the EPSRC (grants GR/G53279, GR/H40570, GR/K57381, GR/K77051, GR/M75440), by ESPRIT (projects 3245: Logical Frameworks, and 6453: Types) and by the DFG Schwerpunktprogramm *Deduktion*.

²Institut für Informatik, Technische Universität München, nipkow@in.tum.de

³Computer Laboratory, University of Cambridge, lcp@cl.cam.ac.uk

⁴Institut für Informatik, Technische Universität München, wenzelm@in.tum.de

Abstract

This manual 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. See also *Isabelle/HOL — The Tutorial* for a gentle introduction on using Isabelle/HOL, and the *Isabelle Reference Manual* for general Isabelle commands.

Contents

1	Syntax definitions	1
2	Higher-Order Logic	3
2.1	Syntax	3
2.1.1	Types and overloading	6
2.1.2	Binders	7
2.1.3	The let and case constructions	8
2.2	Rules of inference	8
2.3	A formulation of set theory	12
2.3.1	Syntax of set theory	15
2.3.2	Axioms and rules of set theory	15
2.3.3	Properties of functions	20
2.4	Generic packages	20
2.4.1	Simplification and substitution	20
2.4.2	Classical reasoning	22
2.5	Calling the decision procedure SVC	22
2.6	Types	24
2.6.1	Product and sum types	24
2.6.2	The type of natural numbers, <i>nat</i>	26
2.6.3	Numerical types and numerical reasoning	29
2.6.4	The type constructor for lists, <i>list</i>	30
2.6.5	Introducing new types	30
2.7	Records	36
2.7.1	Basics	36
2.7.2	Defining records	37
2.7.3	Record operations	38
2.7.4	Record proof tools	39
2.8	Datatype definitions	40
2.8.1	Basics	40
2.8.2	Defining datatypes	45
2.8.3	Representing existing types as datatypes	47
2.8.4	Examples	48
2.9	Recursive function definitions	49

2.9.1	Primitive recursive functions	50
2.9.2	General recursive functions	54
2.10	Inductive and coinductive definitions	57
2.10.1	The result structure	57
2.10.2	The syntax of a (co)inductive definition	58
2.10.3	*Monotonicity theorems	59
2.10.4	Example of an inductive definition	60
2.11	The examples directories	60
2.12	Example: Cantor's Theorem	63

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 \exists has lower priority than \vee , which has lower priority than \wedge . There, $P \wedge Q \vee R$ abbreviates $(P \wedge Q) \vee R$ rather than $P \wedge (Q \vee R)$. Also, $\exists x . P \vee Q$ abbreviates $\exists x . (P \vee Q)$ rather than $(\exists x . P) \vee Q$. Note especially that $P \vee (\exists x . Q)$ 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 $(\alpha \Rightarrow o) \Rightarrow o$. This defines the syntax $\forall x . t$ to mean $All(\lambda x . t)$. We can also write $\forall x_1 \dots x_m . t$ to abbreviate $\forall x_1 \dots \forall x_m . t$; this is possible for any constant provided that τ and τ' are the same type. HOL's description operator $\varepsilon x . P x$ has type $(\alpha \Rightarrow bool) \Rightarrow \alpha$ and can bind only one variable,

except when α is *bool*. 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.

Higher-Order Logic

The theory HOL implements higher-order logic. It is based on Gordon’s HOL system [5], which itself is based on Church’s original paper [3]. Andrews’s book [1] is a full description of the original Church-style higher-order logic. Experience with the HOL system has demonstrated that higher-order logic is widely applicable in many areas of mathematics and computer science, not just hardware verification, HOL’s original *raison d’être*. It is weaker than ZF set theory but for most applications this does not matter. If you prefer ML to Lisp, you will probably prefer HOL to ZF.

The syntax of HOL¹ follows λ -calculus and functional programming. Function application is curried. To apply the function f of type $\tau_1 \Rightarrow \tau_2 \Rightarrow \tau_3$ to the arguments a and b in HOL, you simply write $f a b$. There is no ‘apply’ operator as in ZF. Note that $f(a, b)$ means “ f applied to the pair (a, b) ” in HOL. We write ordered pairs as (a, b) , not $\langle a, b \rangle$ as in ZF.

HOL has a distinct feel, compared with ZF and CTT. It identifies object-level types with meta-level types, taking advantage of Isabelle’s built-in type-checker. It identifies object-level functions with meta-level functions, so it uses Isabelle’s operations for abstraction and application.

These identifications allow Isabelle to support HOL particularly nicely, but they also mean that HOL requires more sophistication from the user — in particular, an understanding of Isabelle’s type system. Beginners should work with `show_types` (or even `show_sorts`) set to `true`.

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 $a \sim b$ is translated to $\neg(a = b)$.

¹Earlier versions of Isabelle’s HOL used a different syntax. Ancient releases of Isabelle included still another version of HOL, with explicit type inference rules [18]. This version no longer exists, but ZF supports a similar style of reasoning.

<i>name</i>	<i>meta-type</i>	<i>description</i>
Trueprop	$bool \Rightarrow prop$	coercion to <i>prop</i>
Not	$bool \Rightarrow bool$	negation (\neg)
True	$bool$	tautology (\top)
False	$bool$	absurdity (\perp)
If	$[bool, \alpha, \alpha] \Rightarrow \alpha$	conditional
Let	$[\alpha, \alpha \Rightarrow \beta] \Rightarrow \beta$	let binder

CONSTANTS

<i>symbol</i>	<i>name</i>	<i>meta-type</i>	<i>description</i>
SOME or @	Eps	$(\alpha \Rightarrow bool) \Rightarrow \alpha$	Hilbert description (ε)
ALL or !	All	$(\alpha \Rightarrow bool) \Rightarrow bool$	universal quantifier (\forall)
EX or ?	Ex	$(\alpha \Rightarrow bool) \Rightarrow bool$	existential quantifier (\exists)
EX! or ?!	Ex1	$(\alpha \Rightarrow bool) \Rightarrow bool$	unique existence ($\exists!$)
LEAST	Least	$(\alpha :: ord \Rightarrow bool) \Rightarrow \alpha$	least element

BINDERS

<i>symbol</i>	<i>meta-type</i>	<i>priority</i>	<i>description</i>
\circ	$[\beta \Rightarrow \gamma, \alpha \Rightarrow \beta] \Rightarrow (\alpha \Rightarrow \gamma)$	Left 55	composition (\circ)
=	$[\alpha, \alpha] \Rightarrow bool$	Left 50	equality ($=$)
<	$[\alpha :: ord, \alpha] \Rightarrow bool$	Left 50	less than ($<$)
<=	$[\alpha :: ord, \alpha] \Rightarrow bool$	Left 50	less than or equals (\leq)
&	$[bool, bool] \Rightarrow bool$	Right 35	conjunction (\wedge)
	$[bool, bool] \Rightarrow bool$	Right 30	disjunction (\vee)
-->	$[bool, bool] \Rightarrow bool$	Right 25	implication (\rightarrow)

INFIXES

Figure 2.1: Syntax of HOL

<i>term</i>	= expression of class <i>term</i>
	SOME <i>id</i> . <i>formula</i> @ <i>id</i> . <i>formula</i>
	let <i>id</i> = <i>term</i> ; ... ; <i>id</i> = <i>term</i> in <i>term</i>
	if <i>formula</i> then <i>term</i> else <i>term</i>
	LEAST <i>id</i> . <i>formula</i>
<i>formula</i>	= expression of type <i>bool</i>
	<i>term</i> = <i>term</i>
	<i>term</i> ~ = <i>term</i>
	<i>term</i> < <i>term</i>
	<i>term</i> <= <i>term</i>
	~ <i>formula</i>
	<i>formula</i> & <i>formula</i>
	<i>formula</i> <i>formula</i>
	<i>formula</i> --> <i>formula</i>
	ALL <i>id id*</i> . <i>formula</i> ! <i>id id*</i> . <i>formula</i>
	EX <i>id id*</i> . <i>formula</i> ? <i>id id*</i> . <i>formula</i>
	EX! <i>id id*</i> . <i>formula</i> ?! <i>id id*</i> . <i>formula</i>

Figure 2.2: Full grammar for HOL

! 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 σ and τ do, allowing quantification over functions.

HOL allows new types to be declared as subsets of existing types; see §2.6. ML-like datatypes can also be declared; see §2.8.

Several syntactic type classes — `plus`, `minus`, `times` and `power` — permit overloading of the operators `+`, `-`, `*` and `^`. They are overloaded to denote the obvious arithmetic operations on types `nat`, `int` and `real`. (With the `^` operator, the exponent always has type `nat`.) Non-arithmetic overloadings are also done: the operator `-` can denote set difference, while `^` 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 `0` is also overloaded. It serves as the zero element of several types, of which the most important is `nat` (the natural numbers). The type class `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 `nat`, `int` and `real` and also multisets. The summation operator `setsum` is available for all types in this class.

Theory `Ord` defines the syntactic class `ord` of order signatures. The relations `<` and `≤` are polymorphic over this class, as are the functions `mono`, `min` and `max`, and the `LEAST` operator. `Ord` also defines a subclass `order` of `ord` which axiomatizes the types that are partially ordered with respect to `≤`. A further subclass `linorder` of `order` axiomatizes linear orderings. For details, see the file `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 $i \leq j \implies i \leq j + k$ have type $\alpha :: \{ord, plus\}$,

although you may have expected them to have some numeric type, e.g. *nat*. Instead you should have stated the goal as $(i :: \text{nat}) \leq j \implies i \leq j + k$, which causes all three variables to have type *nat*.

! If resolution fails for no obvious reason, try setting `show_types` to `true`, causing Isabelle to display types of terms. Possibly set `show_sorts` to `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 `res_inst_tac` instead of `resolve_tac`, possibly instantiating type variables. Setting `Unify.trace_types` to `true` causes Isabelle to report omitted search paths during unification.

2.1.2 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 `Eps`($\lambda x . P[x]$) or use the syntax `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 `ALL` and `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 *must* be followed by a space; thus `?x` is an unknown, while `? 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 `-m HOL` to the `isabelle` executable), then `!` and `?` are displayed.

If τ is a type of class `ord`, P a formula and x a variable of type τ , then the term `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 ε choice operator, so `Least` is always meaningful, but may yield nothing useful in case there is not a unique least element satisfying P .²

²Class `ord` does not require much of its instances, so \leq need not be a well-ordering, not even an order at all!

```

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

All these binders have priority 10.

! 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 $P \wedge \forall x. Q$ you need to write $P \wedge (\forall x. Q)$.

2.1.3 The let and case constructions

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

HOL also defines the basic syntax

$$\text{case } e \text{ of } c_1 \Rightarrow e_1 \mid \dots \mid c_n \Rightarrow e_n$$

as a uniform means of expressing `case` constructs. Therefore `case` and `of` are reserved words. Initially, this is mere syntax and has no logical meaning. By declaring translations, you can cause instances of the `case` construct to denote applications of particular case operators. This is what happens automatically for each `datatype` definition (see §2.8).

! 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 $f x = \text{if} \dots \text{then} \dots \text{else} \dots$ you need to write $f x = (\text{if} \dots \text{then} \dots \text{else} \dots)$.

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:

```

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

`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.³

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 [5, 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.

! 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 (see §2.4).

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`.

³In fact, the ε -operator already makes the logic classical, as shown by Diaconescu; see Paulson [18] for details.

```

sym          s=t ==> t=s
trans       [| r=s; s=t |] ==> r=t
ssubst     [| t=s; P s |] ==> P t
box_equals  [| a=b; a=c; b=d |] ==> c=d
arg_cong   x = y ==> f x = f y
fun_cong   f = g ==> f x = g x
cong       [| f = g; x = y |] ==> f x = g y
not_sym    t ~ = s ==> s ~ = t

```

EQUALITY

```

TrueI       True
FalseE     False ==> P

conjI      [| P; Q |] ==> P&Q
conjunct1  [| P&Q |] ==> P
conjunct2  [| P&Q |] ==> Q
conjE     [| P&Q; [| P; Q |] ==> R |] ==> R

disjI1     P ==> P|Q
disjI2     Q ==> P|Q
disjE     [| P | Q; P ==> R; Q ==> R |] ==> R

notI       (P ==> False) ==> ~ P
notE      [| ~ P; P |] ==> R
impE     [| P-->Q; P; Q ==> R |] ==> R

```

PROPOSITIONAL LOGIC

```

iffI       [| P ==> Q; Q ==> P |] ==> P=Q
iffD1     [| P=Q; P |] ==> Q
iffD2     [| P=Q; Q |] ==> P
iffE     [| P=Q; [| P --> Q; Q --> P |] ==> R |] ==> R
%
%eqTrueI  P ==> P=True
%eqTrueE  P=True ==> P

```

LOGICAL EQUIVALENCE

Figure 2.5: Derived rules for HOL

```

allI      (!!x. P x) ==> !x. P x
spec      !x. P x ==> P x
allE      [| !x. P x; P x ==> R |] ==> R
all_dupE  [| !x. P x; [| P x; !x. P x |] ==> R |] ==> R

exI       P x ==> ? x. P x
exE       [| ? x. P x; !!x. P x ==> Q |] ==> Q

ex1I      [| P a; !!x. P x ==> x=a |] ==> ?! x. P x
ex1E      [| ?! x. P x; !!x. [| P x; ! y. P y --> y=x |] ==> R
|] ==> R

some_equality [| P a; !!x. P x ==> x=a |] ==> (@x. P x) = a

```

QUANTIFIERS AND DESCRIPTIONS

```

ccontr      (~P ==> False) ==> P
classical   (~P ==> P) ==> P
excluded_middle ~P | P

disjCI      (~Q ==> P) ==> P|Q
exCI        (! x. ~ P x ==> P a) ==> ? x. P x
impCE       [| P-->Q; ~ P ==> R; Q ==> R |] ==> R
iffCE       [| P=Q; [| P;Q |] ==> R; [| ~P; ~Q |] ==> R |] ==> R
notnotD     ~~P ==> P
swap        ~P ==> (~Q ==> P) ==> Q

```

CLASSICAL LOGIC

```

if_P        P ==> (if P then x else y) = x
if_not_P    ~ P ==> (if P then x else y) = y
split_if    P(if Q then x else y) = ((Q --> P x) & (~Q --> P y))

```

CONDITIONALS

Figure 2.6: More derived rules

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: `ssubst` 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 `allI` and `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.

`smptac j i` applies j times `spec` and then `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.

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 σ . 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.

<i>name</i>	<i>meta-type</i>	<i>description</i>
<code>{}</code>	$\alpha \text{ set}$	the empty set
<code>insert</code>	$[\alpha, \alpha \text{ set}] \Rightarrow \alpha \text{ set}$	insertion of element
<code>Collect</code>	$(\alpha \Rightarrow \text{bool}) \Rightarrow \alpha \text{ set}$	comprehension
<code>INTER</code>	$[\alpha \text{ set}, \alpha \Rightarrow \beta \text{ set}] \Rightarrow \beta \text{ set}$	intersection over a set
<code>UNION</code>	$[\alpha \text{ set}, \alpha \Rightarrow \beta \text{ set}] \Rightarrow \beta \text{ set}$	union over a set
<code>Inter</code>	$(\alpha \text{ set})\text{set} \Rightarrow \alpha \text{ set}$	set of sets intersection
<code>Union</code>	$(\alpha \text{ set})\text{set} \Rightarrow \alpha \text{ set}$	set of sets union
<code>Pow</code>	$\alpha \text{ set} \Rightarrow (\alpha \text{ set})\text{set}$	powerset
<code>range</code>	$(\alpha \Rightarrow \beta) \Rightarrow \beta \text{ set}$	range of a function
<code>Ball Bex</code>	$[\alpha \text{ set}, \alpha \Rightarrow \text{bool}] \Rightarrow \text{bool}$	bounded quantifiers

CONSTANTS

<i>symbol</i>	<i>name</i>	<i>meta-type</i>	<i>priority</i>	<i>description</i>
<code>INT</code>	<code>INTER1</code>	$(\alpha \Rightarrow \beta \text{ set}) \Rightarrow \beta \text{ set}$	10	intersection
<code>UN</code>	<code>UNION1</code>	$(\alpha \Rightarrow \beta \text{ set}) \Rightarrow \beta \text{ set}$	10	union

BINDERS

<i>symbol</i>	<i>meta-type</i>	<i>priority</i>	<i>description</i>
<code>‘‘</code>	$[\alpha \Rightarrow \beta, \alpha \text{ set}] \Rightarrow \beta \text{ set}$	Left 90	image
<code>Int</code>	$[\alpha \text{ set}, \alpha \text{ set}] \Rightarrow \alpha \text{ set}$	Left 70	intersection (\cap)
<code>Un</code>	$[\alpha \text{ set}, \alpha \text{ set}] \Rightarrow \alpha \text{ set}$	Left 65	union (\cup)
<code>:</code>	$[\alpha, \alpha \text{ set}] \Rightarrow \text{bool}$	Left 50	membership (\in)
<code><=</code>	$[\alpha \text{ set}, \alpha \text{ set}] \Rightarrow \text{bool}$	Left 50	subset (\subseteq)

INFIXES

Figure 2.7: Syntax of the theory `Set`

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

TRANSLATIONS

<i>term</i>	=	other terms...
		$\{\}$
		$\{ \textit{term} (, \textit{term})^* \}$
		$\{ \textit{id} . \textit{formula} \}$
		$\textit{term} \text{ `` } \textit{term}$
		$\textit{term} \text{ Int } \textit{term}$
		$\textit{term} \text{ Un } \textit{term}$
		<code>INT</code> $\textit{id}:\textit{term} . \textit{term}$
		<code>UN</code> $\textit{id}:\textit{term} . \textit{term}$
		<code>INT</code> $\textit{id} \textit{id}^* . \textit{term}$
		<code>UN</code> $\textit{id} \textit{id}^* . \textit{term}$
<i>formula</i>	=	other formulae...
		$\textit{term} : \textit{term}$
		$\textit{term} \sim : \textit{term}$
		$\textit{term} \leq \textit{term}$
		<code>ALL</code> $\textit{id}:\textit{term} . \textit{formula}$ <code>!</code> $\textit{id}:\textit{term} . \textit{formula}$
		<code>EX</code> $\textit{id}:\textit{term} . \textit{formula}$ <code>?</code> $\textit{id}:\textit{term} . \textit{formula}$

FULL GRAMMAR

Figure 2.8: Syntax of the theory `Set` (continued)

2.3.1 Syntax of set theory

HOL's set theory is called **Set**. The type α *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 α *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 ‘‘. Note that $a \sim : b$ is translated to $\neg(a \in b)$.

The $\{a_1, \dots\}$ 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 **Collect**($\lambda x. P[x]$). It defines sets by absolute comprehension, which is impossible in ZF; the type of x implicitly restricts the comprehension.

The set theory defines two **bounded quantifiers**:

$$\begin{aligned} \forall x \in A. P[x] & \text{ abbreviates } \forall x. x \in A \rightarrow P[x] \\ \exists x \in A. P[x] & \text{ abbreviates } \exists x. x \in A \wedge P[x] \end{aligned}$$

The constants **Ball** and **Bex** are defined accordingly. Instead of **Ball** A P and **Bex** A P we may write **ALL** $x:A. P[x]$ and **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 **UN** $x:A. B[x]$ and **INT** $x:A. B[x]$.

Unions and intersections over types, namely $\bigcup_x B[x]$ and $\bigcap_x B[x]$, are written **UN** $x. B[x]$ and **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 **Set**. The axioms **mem_Collect_eq** and **Collect_mem_eq** assert that the functions **Collect** and **op** : are isomorphisms. Of course, **op** : also serves as the membership relation.

```

mem_Collect_eq      (a : {x. P x}) = P a
Collect_mem_eq     {x. x:A} = A

empty_def          {}          == {x. False}
insert_def         insert a B  == {x. x=a} Un B
Ball_def          Ball A P     == ! x. x:A --> P x
Bex_def           Bex A P      == ? x. x:A & P x
subset_def        A <= B       == ! x:A. x:B
Un_def            A Un B       == {x. x:A | x:B}
Int_def           A Int B      == {x. x:A & x:B}
set_diff_def      A - B        == {x. x:A & x~:B}
Compl_def         -A           == {x. ~ x:A}
INTER_def         INTER A B    == {y. ! x:A. y: B x}
UNION_def         UNION A B    == {y. ? x:A. y: B x}
INTER1_def        INTER1 B     == INTER {x. True} B
UNION1_def        UNION1 B     == UNION {x. True} B
Inter_def         Inter S      == (INT x:S. x)
Union_def         Union S      == (UN x:S. x)
Pow_def           Pow A        == {B. B <= A}
image_def         f`A          == {y. ? x:A. y=f x}
range_def         range f      == {y. ? x. y=f x}

```

Figure 2.9: Rules of the theory `Set`

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.

CollectI	$[P a] \implies a : \{x. P x\}$
CollectD	$[a : \{x. P x\}] \implies P a$
CollectE	$[a : \{x. P x\}; P a \implies W] \implies W$
ballI	$[!!x. x:A \implies P x] \implies ! x:A. P x$
bspec	$[! x:A. P x; x:A] \implies P x$
ballE	$[! x:A. P x; P x \implies Q; \sim x:A \implies Q] \implies Q$
bexI	$[P x; x:A] \implies ? x:A. P x$
bexCI	$[! x:A. \sim P x \implies P a; a:A] \implies ? x:A. P x$
bexE	$[? x:A. P x; !!x. [x:A; P x] \implies Q] \implies Q$

COMPREHENSION AND BOUNDED QUANTIFIERS

subsetI	$(!!x. x:A \implies x:B) \implies A \leq B$
subsetD	$[A \leq B; c:A] \implies c:B$
subsetCE	$[A \leq B; \sim (c:A) \implies P; c:B \implies P] \implies P$
subset_refl	$A \leq A$
subset_trans	$[A \leq B; B \leq C] \implies A \leq C$
equalityI	$[A \leq B; B \leq A] \implies A = B$
equalityD1	$A = B \implies A \leq B$
equalityD2	$A = B \implies B \leq A$
equalityE	$[A = B; [A \leq B; B \leq A] \implies P] \implies P$
equalityCE	$[A = B; [c:A; c:B] \implies P;$ $[\sim c:A; \sim c:B] \implies P$ $] \implies P$

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
UnionE   [| A : Union C;  !!X.[| A:X;  X:C |] ==> R |] ==> R

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

```

Union_upper      B:A ==> B <= Union A
Union_least      [| !!X. X:A ==> X<=C |] ==> Union A <= C

Inter_lower      B:A ==> Inter A <= B
Inter_greatest  [| !!X. X:A ==> C<=X |] ==> C <= Inter A

Un_upper1       A <= A Un B
Un_upper2       B <= A Un B
Un_least        [| A<=C; B<=C |] ==> A Un B <= C

Int_lower1      A Int B <= A
Int_lower2      A Int B <= B
Int_greatest   [| C<=A; C<=B |] ==> C <= A Int B

```

Figure 2.12: Derived rules involving subsets

```

Int_absorb      A Int A = A
Int_commute    A Int B = B Int A
Int_assoc      (A Int B) Int C = A Int (B Int C)
Int_Un_distrib (A Un B) Int C = (A Int C) Un (B Int C)

Un_absorb      A Un A = A
Un_commute    A Un B = B Un A
Un_assoc      (A Un B) Un C = A Un (B Un C)
Un_Int_distrib (A Int B) Un C = (A Un C) Int (B Un C)

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

Union_Un_distrib Union(A Un B) = (Union A) Un (Union B)
Int_Union      A Int (Union B) = (UN C:B. A Int C)
%Un_Union_image (UN x:C. (A x) Un (B x)) = Union(A‘‘C) Un Union(B‘‘C)

Inter_Un_distrib Inter(A Un B) = (Inter A) Int (Inter B)
Un_Inter       A Un (Inter B) = (INT C:B. A Un C)
%Int_Inter_image (INT x:C. (A x) Int (B x)) = Inter(A‘‘C) Int Inter(B‘‘C)

```

Figure 2.13: Set equalities

<i>name</i>	<i>meta-type</i>	<i>description</i>
<code>inj surj</code>	$(\alpha \Rightarrow \beta) \Rightarrow \text{bool}$	injective/surjective
<code>inj_on</code>	$[\alpha \Rightarrow \beta, \alpha \text{ set}] \Rightarrow \text{bool}$	injective over subset
<code>inv</code>	$(\alpha \Rightarrow \beta) \Rightarrow (\beta \Rightarrow \alpha)$	inverse function
<code>inj_def</code>	<code>inj f == ! x y. f x=f y --> x=y</code>	
<code>surj_def</code>	<code>surj f == ! y. ? x. y=f x</code>	
<code>inj_on_def</code>	<code>inj_on f A == !x:A. !y:A. f x=f y --> x=y</code>	
<code>inv_def</code>	<code>inv f == (%y. @x. f(x)=y)</code>	

Figure 2.14: Theory Fun

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 (the operator `o`) and the predicate `surj` is done simply by expanding the definitions.

There is also a large collection of monotonicity theorems for constructions on sets in the file `HOL/mono.ML`.

2.4 Generic packages

HOL instantiates most of Isabelle's generic packages, making available the simplifier and the classical reasoner.

2.4.1 Simplification and substitution

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

See the *Reference Manual* for details of substitution and simplification.

! Reducing $a = b \wedge P(a)$ to $a = b \wedge P(b)$ 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 `conj_cong` in a simpset, `addcongs [conj_cong]`.

! By default only the condition of an `if` is simplified but not the `then` and `else` parts. Of course the latter are simplified once the condition simplifies to `True` or `False`. To ensure full simplification of all parts of a conditional you must remove `if_weak_cong` from the simpset, `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 `stac`:

`stac thm i`, where `thm` is of the form `lhs = rhs`, replaces in subgoal `i` instances of `lhs` by corresponding instances of `rhs`. In case of multiple instances of `lhs` in subgoal `i`, backtracking may be necessary to select the desired ones.

If `thm` is a conditional equality, the instantiated condition becomes an additional (first) subgoal.

HOL provides the tactic `hyp_subst_tac`, which substitutes for an equality throughout a subgoal and its hypotheses. This tactic uses HOL's general substitution rule.

Case splitting

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

$$?P(\text{if } ?b \text{ then } ?x \text{ else } ?y) = ((?b \rightarrow ?P(?x)) \wedge (\neg ?b \rightarrow ?P(?y))) \quad (*)$$

For example, a simple instance of `(*)` is

$$x \in (\text{if } x \in A \text{ then } A \text{ else } \{x\}) = ((x \in A \rightarrow x \in A) \wedge (x \notin A \rightarrow x \in \{x\}))$$

Because `(*)` 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 `(*)` to a simpset, as in

```
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`:

```
by(simp_tac (simpset() delsplits [split_if]) 1);
```

In general, `addsplits` accepts rules of the form

$$?P(c \ ?x_1 \ \dots \ ?x_n) = rhs$$

where c is a constant and rhs is arbitrary. Note that $(*)$ 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 §2.6.4 and §2.8.1).

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

```
Addsplits: thm list -> unit
Delsplits: thm list -> unit
```

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

2.4.2 Classical reasoning

HOL derives classical introduction rules for \vee and \exists , as well as classical elimination rules for \rightarrow and \leftrightarrow , and the swap rule; recall Fig. 2.6 above.

The classical reasoner is installed. Tactics such as `Blast_tac` and `Best_tac` refer to the default claset (`claset()`), which works for most purposes. Named clasets include `prop_cs`, which includes the propositional rules, and `HOL_cs`, which also includes quantifier rules. See the file `HOL/cladata.ML` for lists of the classical rules, and the *Reference Manual* for more discussion of classical proof methods.

2.5 Calling the decision procedure SVC

The Stanford Validity Checker (SVC) is a tool that can check the validity of certain types of formulae. If it is installed on your machine, then Isabelle/HOL can be configured to call it through the tactic `svc_tac`. It is ideal for large tautologies and complex problems in linear arithmetic. Subexpressions that SVC cannot handle are automatically replaced by variables, so you can call the tactic on any subgoal. See the file `HOL/ex/svc_test.ML` for examples.

```
svc_tac      : int -> tactic
Svc.trace   : bool ref                               initially false
```

`svc_tac i` attempts to prove subgoal i by translating it into a formula recognized by SVC. If it succeeds then the subgoal is removed. It fails if

SVC is unable to prove the subgoal. It crashes with an error message if SVC appears not to be installed. Numeric variables may have types `nat`, `int` or `real`.

`Svc.trace` is a flag that, if set, causes `svc_tac` to trace its operations: abstraction of the subgoal, translation to SVC syntax, SVC's response.

Here is an example, with tracing turned on:

```
set Svc.trace;
  val it : bool = true
Goal "(#3::nat)*a <= #2 + #4*b + #6*c & #11 <= #2*a + b + #2*c & \
\      a + #3*b <= #5 + #2*c --> #2 + #3*b <= #2*a + #6*c";

by (svc_tac 1);
  Subgoal abstracted to
  #3 * a <= #2 + #4 * b + #6 * c &
  #11 <= #2 * a + b + #2 * c & a + #3 * b <= #5 + #2 * c -->
  #2 + #3 * b <= #2 * a + #6 * c
  Calling SVC:
  (=> (<= 0 (F_c) ) (=> (<= 0 (F_b) ) (=> (<= 0 (F_a) )
    (=> (AND (<= * 3 (F_a) + + 2 * 4 (F_b)
      * 6 (F_c) ) (AND (<= 11 + + * 2 (F_a) (F_b)
        * 2 (F_c) ) (<= + (F_a) * 3 (F_b) + 5
          * 2 (F_c) ) ) ) (< + 2 * 3 (F_b) + 1 +
            * 2 (F_a) * 6 (F_c) ) ) ) ) )
  SVC Returns:
  VALID
  Level 1
  #3 * a <= #2 + #4 * b + #6 * c &
  #11 <= #2 * a + b + #2 * c & a + #3 * b <= #5 + #2 * c -->
  #2 + #3 * b <= #2 * a + #6 * c
  No subgoals!
```

! Calling `svc_tac` entails an above-average risk of unsoundness. Isabelle does not check SVC's result independently. Moreover, the tactic translates the submitted formula using code that lies outside Isabelle's inference core. Theorems that depend upon results proved using SVC (and other oracles) are displayed with the annotation `[!]` attached. You can also use `#der (rep_thm th)` to examine the proof object of theorem `th`, as described in the *Reference Manual*.

To start, first download SVC from the Internet at URL

<http://agamemnon.stanford.edu/~levitt/vc/index.html>

and install it using the instructions supplied. SVC requires two environment variables:

`SVC_HOME` is an absolute pathname to the SVC distribution directory.

`SVC_MACHINE` identifies the type of computer and operating system.

You can set these environment variables either using the Unix shell or through an Isabelle `settings` file. Isabelle assumes SVC to be installed if `SVC_HOME` is defined.

Acknowledgement. This interface uses code supplied by Søren Heilmann.

2.6 Types

This section describes HOL's basic predefined types ($\alpha \times \beta$, $\alpha + \beta$, *nat* and *α list*) and ways for introducing new types in general. The most important type construction, the `datatype`, is treated separately in §2.8.

2.6.1 Product and sum types

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:

external	internal
$\tau_1 \times \dots \times \tau_n$	$\tau_1 \times (\dots (\tau_{n-1} \times \tau_n) \dots)$
(t_1, \dots, t_n)	$(t_1, (\dots, (t_{n-1}, t_n) \dots))$

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

$\%(x, y). t$ stands for `split(%x y. t)`

Nested patterns are also supported. They are translated stepwise:

$$\begin{aligned} \%(x, y, z). t &\rightsquigarrow \%(x, (y, z)). t \\ &\rightsquigarrow \text{split}(\%x. \%(y, z). t) \\ &\rightsquigarrow \text{split}(\%x. \text{split}(\%y z. t)) \end{aligned}$$

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 affect 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) .

<i>symbol</i>	<i>meta-type</i>	<i>description</i>
Pair	$[\alpha, \beta] \Rightarrow \alpha \times \beta$	ordered pairs (a, b)
fst	$\alpha \times \beta \Rightarrow \alpha$	first projection
snd	$\alpha \times \beta \Rightarrow \beta$	second projection
split	$[[\alpha, \beta] \Rightarrow \gamma, \alpha \times \beta] \Rightarrow \gamma$	generalized projection
Sigma	$[\alpha \text{ set}, \alpha \Rightarrow \beta \text{ set}] \Rightarrow (\alpha \times \beta) \text{ set}$	general sum of sets
%fst_def	fst p == @a. ? b. p = (a,b)	
%snd_def	snd p == @b. ? a. p = (a,b)	
%split_def	split c p == c (fst p) (snd p)	
Sigma_def	Sigma A B == UN x:A. UN y:B x. {(x,y)}	
Pair_eq	((a,b) = (a',b')) = (a=a' & b=b')	
Pair_inject	[(a, b) = (a',b'); [a=a'; b=b'] ==> R] ==> R	
PairE	[!!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	split c (a,b) = c a b	
split_split	R(split 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 $\alpha \times \beta$

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:

`split_all_tac i` replaces in subgoal i all `!!`-quantified variables of product type by individual variables for each component. A simple example:

```
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

```
unit_eq      u = ()
```

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

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 (see §2.8.3). Therefore, the theory `Datatype` should be used instead of `Sum` or `Prod`.

2.6.2 The type of natural numbers, *nat*

The theory `NatDef` defines the natural numbers in a roundabout but traditional way. The axiom of infinity postulates a type *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. For details see the file `NatDef.thy`.

<i>symbol</i>	<i>meta-type</i>	<i>description</i>
Inl	$\alpha \Rightarrow \alpha + \beta$	first injection
Inr	$\beta \Rightarrow \alpha + \beta$	second injection
sum_case	$[\alpha \Rightarrow \gamma, \beta \Rightarrow \gamma, \alpha + \beta] \Rightarrow \gamma$	conditional
Inl_not_Inr	Inl a ~ = Inr b	
inj_Inl	inj Inl	
inj_Inr	inj Inr	
sumE	[!!x. P(Inl x); !!y. P(Inr y)] ==> P s	
sum_case_Inl	sum_case f g (Inl x) = f x	
sum_case_Inr	sum_case f g (Inr x) = g x	
surjective_sum	sum_case (%x. f(Inl x)) (%y. f(Inr y)) s = f s	
sum.split_case	R(sum_case f g s) = ((! x. s = Inl(x) --> R(f(x))) & (! y. s = Inr(y) --> R(g(y))))	

Figure 2.16: Type $\alpha + \beta$

Type *nat* is an instance of class *ord*, which makes the overloaded functions of this class (especially $<$ and \leq , but also *min*, *max* and *LEAST*) available on *nat*. Theory *Nat* builds on *NatDef* and shows that \leq is a linear order, so *nat* is also an instance of class *linorder*.

Theory *Arith* develops arithmetic on the natural numbers. It defines addition, multiplication and subtraction. Theory *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 *nat* are part of the default simpset.

Functions on *nat* can be defined by primitive or well-founded recursion; see §2.9. A simple example is addition. Here, *op +* is the name of the infix operator $+$, following the standard convention.

```
primrec
  "0 + n = n"
  "Suc m + n = Suc (m + n)"
```

There is also a *case*-construct of the form

```
case e of 0 => a | Suc m => b
```

Note that Isabelle insists on precisely this format; you may not even change the order of the two cases. Both *primrec* and *case* are realized by a recursion

<i>symbol</i>	<i>meta-type</i>	<i>priority</i>	<i>description</i>
0	α		zero
Suc	$nat \Rightarrow nat$		successor function
*	$[\alpha, \alpha] \Rightarrow \alpha$	Left 70	multiplication
div	$[\alpha, \alpha] \Rightarrow \alpha$	Left 70	division
mod	$[\alpha, \alpha] \Rightarrow \alpha$	Left 70	modulus
dvd	$[\alpha, \alpha] \Rightarrow bool$	Left 70	“divides” relation
+	$[\alpha, \alpha] \Rightarrow \alpha$	Left 65	addition
-	$[\alpha, \alpha] \Rightarrow \alpha$	Left 65	subtraction

CONSTANTS AND INFIXES

nat_induct	$[P\ 0; !!n. P\ n \implies P(\text{Suc } n)] \implies P\ n$
Suc_not_Zero	$\text{Suc } m \not\sim 0$
inj_Suc	inj Suc
n_not_Suc_n	$n \not\sim \text{Suc } n$

BASIC PROPERTIES

	$0+n = n$
	$(\text{Suc } m)+n = \text{Suc}(m+n)$
	$m-0 = m$
	$0-n = n$
	$\text{Suc}(m)-\text{Suc}(n) = m-n$
	$0*n = 0$
	$\text{Suc}(m)*n = n + m*n$
mod_less	$m < n \implies m \bmod n = m$
mod_geq	$[0 < n; \sim m < n] \implies m \bmod n = (m-n) \bmod n$
div_less	$m < n \implies m \text{ div } n = 0$
div_geq	$[0 < n; \sim m < n] \implies m \text{ div } n = \text{Suc}((m-n) \text{ div } n)$

Figure 2.18: Recursion equations for the arithmetic operators

operator `nat_rec`, which is available because `nat` is represented as a datatype (see §2.8.3).

Tactic `induct_tac "n" i` performs induction on variable `n` in subgoal `i` using theorem `nat_induct`. There is also the derived theorem `less_induct`:

$$[| !n. [| !m. m < n --> P m |] ==> P n |] ==> P n$$

2.6.3 Numerical types and numerical reasoning

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

All three numeric types admit numerals of the form `#sd...d`, where `s` is an optional minus sign and `d...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 `#54342339` by `#3452` takes about five seconds. By default, the simplifier cancels like terms on the opposite sites of relational operators (reducing `z+x<x+y` to `z<y`, for instance). The simplifier also collects like terms, replacing `x+y+x*#3` by `#4*x+y`.

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

Reasoning about arithmetic inequalities can be tedious. Fortunately HOL provides a decision procedure for quantifier-free linear arithmetic (that is, 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 `arith_tac` explicitly. It copes with arbitrary formulae involving `=`, `<`, `<=`, `+`, `-`, `Suc`, `min`, `max` and numerical constants; other subterms are treated as atomic; subformulae not involving numerical types are ignored; quantified subformulae are ignored unless they are positive universal or negative existential. Note that the running time is exponential in the number of occurrences of `min`, `max`, and `-` because they require case distinctions. Note

also that `arith_tac` is not complete: if divisibility plays a role, it may fail to prove a valid formula, for example $m + m \neq n + n + 1$. Fortunately such examples are rare in practice.

If `arith_tac` fails you, try to find relevant arithmetic results in the library. The theory `NatDef` contains theorems about `<` and `<=`, the theory `Arith` contains theorems about `+`, `-` and `*`, and theory `Divides` contains theorems about `div` and `mod`. Use `thms_containing` or the `find`-functions to locate them (see the *Reference Manual*).

2.6.4 The type constructor for lists, *list*

Figure 2.19 presents the theory `List`: the basic list operations with their types and syntax. Type α *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

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

is defined by translation. For details see §2.8. There is also a case splitting rule `split_list_case`

$$\begin{aligned} P(\text{case } e \text{ of } [] \Rightarrow a \mid x\#xs \Rightarrow f \ x \ xs) = \\ ((e = [] \rightarrow P(a)) \wedge (\forall x \ xs . e = x\#xs \rightarrow P(f \ x \ xs))) \end{aligned}$$

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 primitive recursion (see §2.9.1). The recursion equations are shown in Figs. 2.20 and 2.21.

2.6.5 Introducing new types

The HOL-methodology dictates that all extensions to a theory should be **definitional**. The type definition mechanism that meets this criterion is `typedef`. Note that *type synonyms*, which are inherited from Pure and described elsewhere, are just syntactic abbreviations that have no logical meaning.

- ! Types in HOL must be non-empty; otherwise the quantifier rules would be
- unsound, because $\exists x . x = x$ is a theorem [18, §7].

<i>symbol</i>	<i>meta-type</i>	<i>priority</i>	<i>description</i>
<code>[]</code>	$\alpha \text{ list}$		empty list
<code>#</code>	$[\alpha, \alpha \text{ list}] \Rightarrow \alpha \text{ list}$	Right 65	list constructor
<code>null</code>	$\alpha \text{ list} \Rightarrow \text{bool}$		emptiness test
<code>hd</code>	$\alpha \text{ list} \Rightarrow \alpha$		head
<code>tl</code>	$\alpha \text{ list} \Rightarrow \alpha \text{ list}$		tail
<code>last</code>	$\alpha \text{ list} \Rightarrow \alpha$		last element
<code>butlast</code>	$\alpha \text{ list} \Rightarrow \alpha \text{ list}$		drop last element
<code>@</code>	$[\alpha \text{ list}, \alpha \text{ list}] \Rightarrow \alpha \text{ list}$	Left 65	append
<code>map</code>	$(\alpha \Rightarrow \beta) \Rightarrow (\alpha \text{ list} \Rightarrow \beta \text{ list})$		apply to all
<code>filter</code>	$(\alpha \Rightarrow \text{bool}) \Rightarrow (\alpha \text{ list} \Rightarrow \alpha \text{ list})$		filter functional
<code>set</code>	$\alpha \text{ list} \Rightarrow \alpha \text{ set}$		elements
<code>mem</code>	$\alpha \Rightarrow \alpha \text{ list} \Rightarrow \text{bool}$	Left 55	membership
<code>foldl</code>	$(\beta \Rightarrow \alpha \Rightarrow \beta) \Rightarrow \beta \Rightarrow \alpha \text{ list} \Rightarrow \beta$		iteration
<code>concat</code>	$(\alpha \text{ list}) \text{ list} \Rightarrow \alpha \text{ list}$		concatenation
<code>rev</code>	$\alpha \text{ list} \Rightarrow \alpha \text{ list}$		reverse
<code>length</code>	$\alpha \text{ list} \Rightarrow \text{nat}$		length
<code>!</code>	$\alpha \text{ list} \Rightarrow \text{nat} \Rightarrow \alpha$	Left 100	indexing
<code>take, drop</code>	$\text{nat} \Rightarrow \alpha \text{ list} \Rightarrow \alpha \text{ list}$		take/drop a prefix
<code>takeWhile,</code> <code>dropWhile</code>	$(\alpha \Rightarrow \text{bool}) \Rightarrow \alpha \text{ list} \Rightarrow \alpha \text{ list}$		take/drop a prefix

CONSTANTS AND INFIXES

<i>external</i>	<i>internal</i>	<i>description</i>
$[x_1, \dots, x_n]$	$x_1 \# \dots \# x_n \# []$	finite list
$[x:l. P]$	<code>filter</code> $(\lambda x.P) \ l$	list comprehension

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

```

map f [] = []
map f (x#xs) = f x # map f xs

filter P [] = []
filter P (x#xs) = (if P x then x#filter P xs else filter P xs)

foldl f a [] = a
foldl f a (x#xs) = foldl f (f a x) xs

take n [] = []
take n (x#xs) = (case n of 0 => [] | Suc(m) => x # take m xs)

drop n [] = []
drop n (x#xs) = (case n of 0 => x#xs | Suc(m) => drop m xs)

takeWhile P [] = []
takeWhile P (x#xs) = (if P x then x#takeWhile P xs else [])

dropWhile P [] = []
dropWhile P (x#xs) = (if P x then dropWhile P xs else xs)

```

Figure 2.21: Further list processing functions

A **type definition** identifies the new type with a subset of an existing type. More precisely, the new type is defined by exhibiting an existing type τ , a set $A :: \tau \text{ set}$, and a theorem of the form $x : A$. Thus A is a non-empty subset of τ , and the new type denotes this subset. New functions are defined that establish an isomorphism between the new type and the subset. If type τ involves type variables $\alpha_1, \dots, \alpha_n$, then the type definition creates a type constructor $(\alpha_1, \dots, \alpha_n)ty$ rather than a particular type.

The syntax for type definitions is shown in Fig. 2.22. For the definition of ‘typevarlist’ and ‘infix’ see the appendix of the *Reference Manual*. The remaining nonterminals have the following meaning:

type: the new type constructor $(\alpha_1, \dots, \alpha_n)ty$ with optional infix annotation.

name: an alphanumeric name T for the type constructor ty , in case ty is a symbolic name. Defaults to ty .

set: the representing subset A .

witness: name of a theorem of the form $a : A$ proving non-emptiness. It can be omitted in case Isabelle manages to prove non-emptiness automatically.

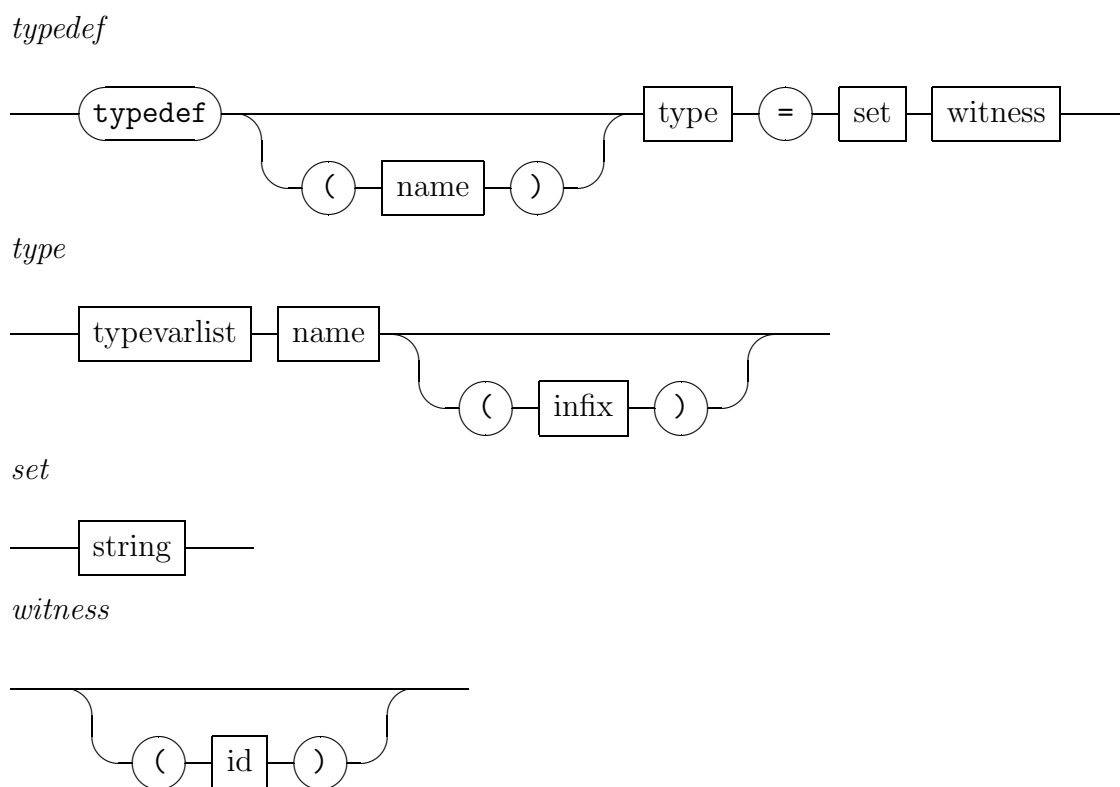


Figure 2.22: Syntax of type definitions

If all context conditions are met (no duplicate type variables in ‘typevarlist’, no extra type variables in ‘set’, and no free term variables in ‘set’), the following components are added to the theory:

- a type $ty :: (term, \dots, term)term$
- constants

$$\begin{aligned} T &:: \tau \text{ set} \\ Rep_T &:: (\alpha_1, \dots, \alpha_n)ty \Rightarrow \tau \\ Abs_T &:: \tau \Rightarrow (\alpha_1, \dots, \alpha_n)ty \end{aligned}$$

- a definition and three axioms

$$\begin{aligned} T_def & \quad T \equiv A \\ Rep_T & \quad Rep_T x \in T \\ Rep_T_inverse & \quad Abs_T (Rep_T x) = x \\ Abs_T_inverse & \quad y \in T \implies Rep_T (Abs_T y) = y \end{aligned}$$

stating that $(\alpha_1, \dots, \alpha_n)ty$ is isomorphic to A by Rep_T and its inverse Abs_T .

Below are two simple examples of HOL type definitions. Non-emptiness is proved automatically here.

```
typedef unit = "{True}"

typedef (prod)
  ('a, 'b) "*" (infixr 20)
  = "{f . EX (a::'a) (b::'b). f = (%x y. x = a & y = b)}"
```

Type definitions permit the introduction of abstract data types in a safe way, namely by providing models based on already existing types. Given some abstract axiomatic description P of a type, this involves two steps:

1. Find an appropriate type τ and subset A which has the desired properties P , and make a type definition based on this representation.
2. Prove that P holds for ty by lifting P from the representation.

You can now forget about the representation and work solely in terms of the abstract properties P .

! If you introduce a new type (constructor) ty axiomatically, i.e. by declaring the type and its operations and by stating the desired axioms, you should make sure the type has a non-empty model. You must also have a clause

```
arities ty :: (term, ..., term) term
```

in your theory file to tell Isabelle that ty is in class `term`, the class of all HOL types.

2.7 Records

At a first approximation, records are just a minor generalisation of tuples, where components may be addressed by labels instead of just position (think of ML, for example). The version of records offered by Isabelle/HOL is slightly more advanced, though, supporting *extensible record schemes*. This admits operations that are polymorphic with respect to record extension, yielding “object-oriented” effects like (single) inheritance. See also [10] for more details on object-oriented verification and record subtyping in HOL.

2.7.1 Basics

Isabelle/HOL supports fixed and schematic records both at the level of terms and types. The concrete syntax is as follows:

	record terms	record types
fixed	$\langle x = a, y = b \rangle$	$\langle x :: A, y :: B \rangle$
schematic	$\langle x = a, y = b, \dots = m \rangle$	$\langle x :: A, y :: B, \dots :: M \rangle$

The ASCII representation of $\langle x = a \rangle$ is $(\mathbf{x} = \mathbf{a} \)$.

A fixed record $\langle x = a, y = b \rangle$ has field x of value a and field y of value b . The corresponding type is $\langle x :: A, y :: B \rangle$, assuming that $a :: A$ and $b :: B$.

A record scheme like $\langle x = a, y = b, \dots = m \rangle$ contains fields x and y as before, but also possibly further fields as indicated by the “...” notation (which is actually part of the syntax). The improper field “...” of a record scheme is called the *more part*. Logically it is just a free variable, which is occasionally referred to as *row variable* in the literature. The more part of a record scheme may be instantiated by zero or more further components. For example, above scheme might get instantiated to $\langle x = a, y = b, z = c, \dots = m' \rangle$, where m' refers to a different more part. Fixed records are special instances of record schemes, where “...” is properly terminated by the $() :: \textit{unit}$ element. Actually, $\langle x = a, y = b \rangle$ is just an abbreviation for $\langle x = a, y = b, \dots = () \rangle$.

There are two key features that make extensible records in a simply typed language like HOL feasible:

1. the more part is internalised, as a free term or type variable,
2. field names are externalised, they cannot be accessed within the logic as first-class values.

In Isabelle/HOL record types have to be defined explicitly, fixing their field names and types, and their (optional) parent record (see §2.7.2). Afterwards, records may be formed using above syntax, while obeying the canonical order of fields as given by their declaration. The record package also provides several operations like selectors and updates (see §2.7.3), together with characteristic properties (see §2.7.4).

There is an example theory demonstrating most basic aspects of extensible records (see theory `HOL/ex/Records` in the Isabelle sources).

2.7.2 Defining records

The theory syntax for record type definitions is shown in Fig. 2.23. For the definition of ‘typevarlist’ and ‘type’ see the appendix of the *Reference Manual*.

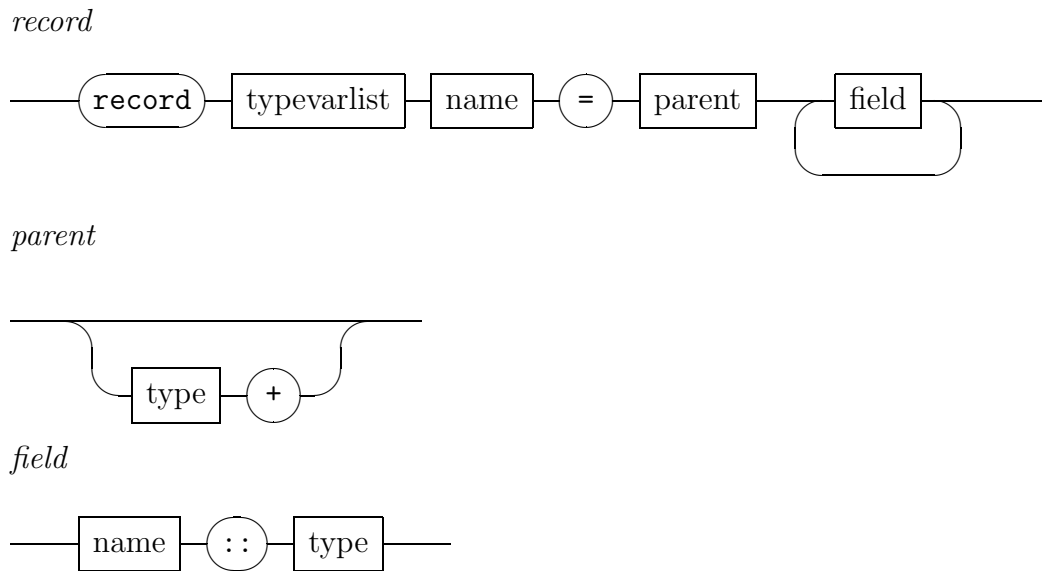


Figure 2.23: Syntax of record type definitions

A general `record` specification is of the following form:

$$\text{record } (\alpha_1, \dots, \alpha_n) t = (\tau_1, \dots, \tau_m) s + c_1 :: \sigma_1 \dots c_l :: \sigma_l$$

where $\vec{\alpha}_n$ are distinct type variables, and $\vec{\tau}_m, \vec{\sigma}_l$ are types containing at most variables from $\vec{\alpha}_n$. Type constructor t has to be new, while s has to specify an existing record type. Furthermore, the \vec{c}_l have to be distinct field names. There has to be at least one field.

In principle, field names may never be shared with other records. This is no actual restriction in practice, since \vec{c}_l are internally declared within a separate name space qualified by the name t of the record.

Above definition introduces a new record type $(\vec{\alpha}_n) t$ by extending an existing one $(\vec{\tau}_m) s$ by new fields $\vec{c}_l :: \vec{\sigma}_l$. The parent record specification is optional, by omitting it t becomes a *root record*. The hierarchy of all records declared within a theory forms a forest structure, i.e. a set of trees, where any of these is rooted by some root record.

For convenience, $(\vec{\alpha}_n) t$ is made a type abbreviation for the fixed record type $(\vec{c}_l :: \vec{\sigma}_l)$, and $(\vec{\alpha}_n, \zeta) t_scheme$ is made an abbreviation for $(\vec{c}_l :: \vec{\sigma}_l, \dots :: \zeta)$.

The following simple example defines a root record type *point* with fields $x :: nat$ and $y :: nat$, and record type *cpoint* by extending *point* with an additional *colour* component.

```
record point =
  x :: nat
  y :: nat

record cpoint = point +
  colour :: string
```

2.7.3 Record operations

Any record definition of the form presented above produces certain standard operations. Selectors and updates are provided for any field, including the improper one “*more*”. There are also cumulative record constructor functions.

To simplify the presentation below, we first assume that $(\vec{\alpha}_n) t$ is a root record with fields $\vec{c}_l :: \vec{\sigma}_l$.

Selectors and **updates** are available for any field (including “*more*”) as follows:

$$\begin{aligned} c_i &:: (\vec{c}_l :: \vec{\sigma}_l, \dots :: \zeta) \Rightarrow \sigma_i \\ c_i_update &:: \sigma_i \Rightarrow (\vec{c}_l :: \vec{\sigma}_l, \dots :: \zeta) \Rightarrow (\vec{c}_l :: \vec{\sigma}_l, \dots :: \zeta) \end{aligned}$$

There is some special syntax for updates: $r (x := a)$ abbreviates term $x_update a r$. Repeated updates are supported as well: $r (x := a) (y := b) (z := c)$ may be written as $r (x := a, y := b, z := c)$. Note that because of postfix notation the order of fields shown here is reverse than in the actual

term. This might lead to confusion in conjunction with special proof tools such as ordered rewriting.

Since repeated updates are just function applications, fields may be freely permuted in $(x := a, y := b, z := c)$, as far as the logic is concerned. Thus commutativity of updates can be proven within the logic for any two fields, but not as a general theorem: fields are not first-class values.

Make operations provide cumulative record constructor functions:

$$\begin{aligned} \mathit{make} &:: \vec{\sigma}_l \Rightarrow (\vec{c}_l :: \vec{\sigma}_l) \\ \mathit{make_scheme} &:: \vec{\sigma}_l \Rightarrow \zeta \Rightarrow (\vec{c}_l :: \vec{\sigma}_l, \dots :: \zeta) \end{aligned}$$

These functions are curried. The corresponding definitions in terms of actual record terms are part of the standard simpset. Thus *point.make a b* rewrites to $(x = a, y = b)$.

Any of above selector, update and make operations are declared within a local name space prefixed by the name *t* of the record. In case that different records share base names of fields, one has to qualify names explicitly (e.g. *t.c_i-update*). This is recommended especially for operations like *make* or *update_more* that always have the same base name. Just use *t.make* etc. to avoid confusion.

We reconsider the case of non-root records, which are derived of some parent record. In general, the latter may depend on another parent as well, resulting in a list of *ancestor records*. Appending the lists of fields of all ancestors results in a certain field prefix. The record package automatically takes care of this by lifting operations over this context of ancestor fields. Assuming that $(\vec{\alpha}_n) t$ has ancestor fields $\vec{d}_k :: \vec{\rho}_k$, selectors will get the following types:

$$c_i \quad :: \quad (\vec{d}_k :: \vec{\rho}_k, \vec{c}_l :: \vec{\sigma}_l, \dots :: \zeta) \Rightarrow \sigma_i$$

Update and make operations are analogous.

2.7.4 Record proof tools

The record package declares the following proof rules for any record type *t*.

1. Standard conversions (selectors or updates applied to record constructor terms, make function definitions) are part of the standard simpset (via `addsimps`).
2. Selectors applied to updated records are automatically reduced by simplification procedure `record_simproc`, which is part of the default simpset.

where $\vec{\alpha} = (\alpha_1, \dots, \alpha_h)$ is a list of type variables, C_i^j are distinct constructor names and $\tau_{i,i'}^j$ are *admissible* types containing at most the type variables $\alpha_1, \dots, \alpha_h$. A type τ occurring in a datatype definition is *admissible* if and only if

- τ is non-recursive, i.e. τ does not contain any of the newly defined type constructors t_1, \dots, t_n , or
- $\tau = (\vec{\alpha})t_{j'}$ where $1 \leq j' \leq n$, or
- $\tau = (\tau'_1, \dots, \tau'_{h'})t'$, where t' is the type constructor of an already existing datatype and $\tau'_1, \dots, \tau'_{h'}$ are admissible types.
- $\tau = \sigma \rightarrow \tau'$, where τ' is an admissible type and σ 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 $\tau_{i,i'}^j$ of the form

$$(\dots, \dots (\vec{\alpha})t_{j'} \dots, \dots)t'$$

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

```
datatype 'a list = Nil
              | Cons 'a ('a list)
```

Arithmetic expressions `aexp` and boolean expressions `bexp` can be modelled by the mutually recursive datatype definition

```
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 `term`, which is defined by

```
datatype ('a, 'b) term = Var 'a
                    | App 'b (((('a, '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.

```
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_i^j 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.

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_i^j 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 list)` is non-empty as well.

Freeness of the constructors

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

$$C_i^j :: [\tau_{i,1}^j, \dots, \tau_{i,m_i^j}^j] \Rightarrow (\alpha_1, \dots, \alpha_h)t_j$$

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

$$C_i^j x_1 \dots x_{m_i^j} \neq C_{i'}^j y_1 \dots y_{m_{i'}^j} \quad \text{for all } i \neq i'.$$

The constructor functions are injective:

$$(C_i^j x_1 \dots x_{m_i^j} = C_i^j y_1 \dots y_{m_i^j}) = (x_1 = y_1 \wedge \dots \wedge x_{m_i^j} = y_{m_i^j})$$

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.⁴

⁴This procedure, which is already part of the default simpset, may be referred to by the ML identifier `DatatypePackage.distinct_simproc`.

Structural induction

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

$$\begin{array}{c}
\bigwedge x_1 \dots x_{m_1} \cdot \llbracket P_{s_{1,1}^1} x_{r_{1,1}^1}; \dots; P_{s_{1,l_1}^1} x_{r_{1,l_1}^1} \rrbracket \quad \Longrightarrow \quad P_1 \left(C_1^1 x_1 \dots x_{m_1} \right) \\
\vdots \\
\bigwedge x_1 \dots x_{m_{k_1}} \cdot \llbracket P_{s_{k_1,1}^1} x_{r_{k_1,1}^1}; \dots; P_{s_{k_1,l_{k_1}}^1} x_{r_{k_1,l_{k_1}}^1} \rrbracket \quad \Longrightarrow \quad P_1 \left(C_{k_1}^1 x_1 \dots x_{m_{k_1}} \right) \\
\vdots \\
\bigwedge x_1 \dots x_{m_1^n} \cdot \llbracket P_{s_{1,1}^n} x_{r_{1,1}^n}; \dots; P_{s_{1,l_1^n}^n} x_{r_{1,l_1^n}^n} \rrbracket \quad \Longrightarrow \quad P_n \left(C_1^n x_1 \dots x_{m_1^n} \right) \\
\vdots \\
\bigwedge x_1 \dots x_{m_{k_n}^n} \cdot \llbracket P_{s_{k_n,1}^n} x_{r_{k_n,1}^n}; \dots; P_{s_{k_n,l_{k_n}^n}^n} x_{r_{k_n,l_{k_n}^n}^n} \rrbracket \quad \Longrightarrow \quad P_n \left(C_{k_n}^n x_1 \dots x_{m_{k_n}^n} \right) \\
\hline
P_1 x_1 \wedge \dots \wedge P_n x_n
\end{array}$$

where

$$\begin{aligned}
Rec_i^j &:= \left\{ \left(r_{i,1}^j, s_{i,1}^j \right), \dots, \left(r_{i,l_i^j}^j, s_{i,l_i^j}^j \right) \right\} = \\
&\quad \left\{ (i', i'') \mid 1 \leq i' \leq m_i^j \wedge 1 \leq i'' \leq n \wedge \tau_{i,i'}^j = (\alpha_1, \dots, \alpha_h) t_{i''} \right\}
\end{aligned}$$

i.e. the properties P_j 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

```
datatype ('a,'b) term = Var 'a
                    | App 'b (((a, 'b) term) list)
```

to an equivalent definition without nesting:

```
datatype ('a,'b) term      = Var
                          | App 'b (('a, 'b) term_list)
and ('a,'b) term_list = Nil'
                          | Cons' (('a,'b) term) (('a,'b) term_list)
```

Note however, that the type `('a,'b) term_list` and the constructors `Nil'` and `Cons'` are not really introduced. One can directly work with the original (isomorphic) type `((a, 'b) term) list` and its existing constructors `Nil` and `Cons`. Thus, the structural induction rule for `term` gets the form

$$\begin{array}{c}
\bigwedge x \cdot P_1 (\text{Var } x) \\
\bigwedge x_1 x_2 \cdot P_2 x_2 \Longrightarrow P_1 (\text{App } x_1 x_2) \\
P_2 \text{ Nil} \\
\bigwedge x_1 x_2 \cdot \llbracket P_1 x_1; P_2 x_2 \rrbracket \Longrightarrow P_2 (\text{Cons } x_1 x_2) \\
\hline
P_1 x_1 \wedge P_2 x_2
\end{array}$$

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) term) list`.

For a datatype with function types such as `'a tree`, the induction rule is of the form

$$\frac{\wedge a. P (\text{Atom } a) \quad \wedge ts. (\forall x. P (ts \ x)) \implies P (\text{Branch } ts)}{P \ t}$$

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:

$$\begin{array}{l} \text{case } e \text{ of} \quad C_1^j \ x_{1,1} \ \dots \ x_{1,m_1^j} \ \Rightarrow \ e_1 \\ \quad \quad \quad \vdots \\ \quad \quad \quad | \ C_{k_j}^j \ x_{k_j,1} \ \dots \ x_{k_j,m_{k_j}^j} \ \Rightarrow \ e_{k_j} \end{array}$$

where the $x_{i,j}$ are either identifiers or nested tuple patterns as in §2.6.1.

! 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 `tj.split` is provided:

$$P(t_j\text{-case } f_1 \ \dots \ f_{k_j} \ e) = ((\forall x_1 \ \dots \ x_{m_1^j}. e = C_1^j \ x_1 \ \dots \ x_{m_1^j} \rightarrow P(f_1 \ x_1 \ \dots \ x_{m_1^j})) \wedge \ \dots \wedge (\forall x_1 \ \dots \ x_{m_{k_j}^j}. e = C_{k_j}^j \ x_1 \ \dots \ x_{m_{k_j}^j} \rightarrow P(f_{k_j} \ x_1 \ \dots \ x_{m_{k_j}^j})))$$

where `tj_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 `tj.split_asm` in the same manner. Both rules are available under `tj.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 21). 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.case_weak_cong` from the simpset, for example by `delcongs [thm "t.weak_case_cong"]`.

The function size

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

$$\text{size}(C_i^j x_1 \dots x_{m_i^j}) = \begin{cases} 0 & \text{if } \text{Rec}_i^j = \emptyset \\ 1 + \sum_{h=1}^{l_i^j} \text{size } x_{r_{i,h}^j} & \text{if } \text{Rec}_i^j = \left\{ \left(r_{i,1}^j, s_{i,1}^j \right), \dots, \left(r_{i,l_i^j}^j, s_{i,l_i^j}^j \right) \right\} \end{cases}$$

where Rec_i^j 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.

2.8.2 Defining datatypes

The theory syntax for datatype definitions is shown in Fig. 2.24. 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.

`induct_tac "x" i` applies structural induction on variable x to subgoal i , provided the type of x is a datatype.

`induct_tac "x1 ... xn" i` applies simultaneous structural induction on the variables x_1, \dots, x_n to subgoal i . This is the canonical way to prove properties of mutually recursive datatypes such as `aexp` and `bexp`, or datatypes with nested recursion such as `term`.

In some cases, induction is overkill and a case distinction over all constructors of the datatype suffices.

`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 $C_1^j, \dots, C_{k_j}^j$, subgoal i is replaced by k_j new subgoals which contain the additional assumption $u = C_{i'}^j x_1 \dots x_{m_{i'}^j}$ for $i' = 1, \dots, k_j$.

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.

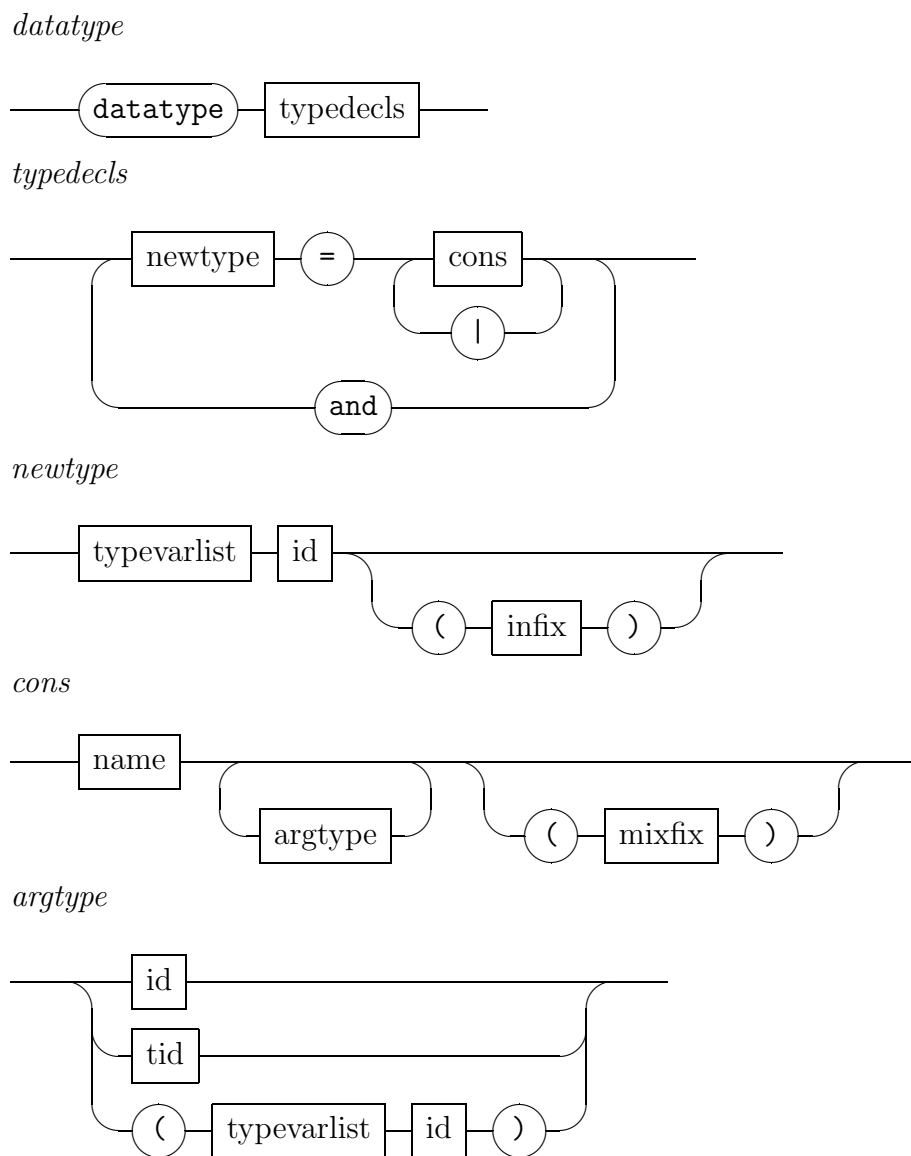


Figure 2.24: Syntax of datatype declarations

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:

```

val distinct : thm list
val inject   : thm list
val induct   : thm
val exhaust  : thm
val cases    : thm list
val split    : thm
val split_asm : thm
val recs     : thm list
val size     : thm list
val simps    : thm list

```

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

2.8.3 Representing existing types as datatypes

For foundational reasons, some basic types such as `nat`, `*`, `+`, `bool` and `unit` are not defined in a `datatype` section, but by more primitive means using `typedef`. To be able to use the tactics `induct_tac` and `case_tac` and to define functions by primitive recursion on these types, such types may be represented as actual datatypes. This is done by specifying an induction rule, as well as theorems stating the distinctness and injectivity of constructors in a `rep_datatype` section. For type `nat` this works as follows:

```

rep_datatype nat
  distinct Suc_not_Zero, Zero_not_Suc
  inject   Suc_Suc_eq
  induct   nat_induct

```

The datatype package automatically derives additional theorems for recursion and case combinators from these rules. Any of the basic HOL types mentioned above are represented as datatypes. Try an induction on `bool` today.

2.8.4 Examples

The datatype α *mylist*

We want to define a type α *mylist*. To do this we have to build a new theory that contains the type definition. We start from the theory `Datatype` instead of `Main` in order to avoid clashes with the `List` theory of Isabelle/HOL.

```
MyList = Datatype +
  datatype 'a mylist = Nil | Cons 'a ('a mylist)
end
```

After loading the theory, we can prove $\text{Cons } x \text{ } xs \neq xs$, for example. To ease the induction applied below, we state the goal with x quantified at the object-level. This will be stripped later using `qed_spec_mp`.

```
Goal "!x. Cons x xs ~= xs";
Level 0
! x. Cons x xs ~= xs
1. ! x. Cons x xs ~= xs
```

This can be proved by the structural induction tactic:

```
by (induct_tac "xs" 1);
Level 1
! x. Cons x xs ~= xs
1. ! x. Cons x Nil ~= Nil
2. !!a mylist.
   ! x. Cons x mylist ~= mylist ==>
   ! x. Cons x (Cons a mylist) ~= Cons a mylist
```

The first subgoal can be proved using the simplifier. Isabelle/HOL has already added the freeness properties of lists to the default simplification set.

```
by (Simp_tac 1);
Level 2
! x. Cons x xs ~= xs
1. !!a mylist.
   ! x. Cons x mylist ~= mylist ==>
   ! x. Cons x (Cons a mylist) ~= Cons a mylist
```

Similarly, we prove the remaining goal.

```
by (Asm_simp_tac 1);
Level 3
! x. Cons x xs ~= xs
No subgoals!
qed_spec_mp "not_Cons_self";
val not_Cons_self = "Cons x xs ~= xs" : thm
```

Because both subgoals could have been proved by `Asm_simp_tac` we could have done that in one step:

```
by (ALLGOALS Asm_simp_tac);
```

The datatype α *mylist* with mixfix syntax

In this example we define the type α *mylist* again but this time we want to write `[]` for `Nil` and we want to use infix notation `#` for `Cons`. To do this we simply add mixfix annotations after the constructor declarations as follows:

```
MyList = Datatype +
  datatype 'a mylist =
    Nil ("[]") |
    Cons 'a ('a mylist) (infixr "#" 70)
end
```

Now the theorem in the previous example can be written `x#xs ~ = xs`.

A datatype for weekdays

This example shows a datatype that consists of 7 constructors:

```
Days = Main +
  datatype days = Mon | Tue | Wed | Thu | Fri | Sat | Sun
end
```

Because there are more than 6 constructors, inequality is expressed via a function `days_ord`. The theorem `Mon ~ = Tue` is not directly contained among the distinctness theorems, but the simplifier can prove it thanks to rewrite rules inherited from theory `Arith`:

```
Goal "Mon ~ = Tue";
by (Simp_tac 1);
```

You need not derive such inequalities explicitly: the simplifier will dispose of them automatically.

2.9 Recursive function definitions

Isabelle/HOL provides two main mechanisms of defining recursive functions.

1. **Primitive recursion** is available only for datatypes, and it is somewhat restrictive. Recursive calls are only allowed on the argument's immediate constituents. On the other hand, it is the form of recursion most often wanted, and it is easy to use.
2. **Well-founded recursion** 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.⁵

Following good HOL tradition, these declarations do not assert arbitrary axioms. Instead, they define the function using a recursion operator. Both HOL and ZF derive the theory of well-founded recursion from first principles [15]. Primitive recursion over some datatype relies on the recursion operator provided by the datatype package. With either form of function definition, Isabelle proves the desired recursion equations as theorems.

2.9.1 Primitive recursive functions

Datatypes come with a uniform way of defining functions, **primitive recursion**. In principle, one could introduce primitive recursive functions by asserting their reduction rules as new axioms, but this is not recommended:

```
Append = Main +
consts app :: ['a list, 'a list] => 'a list
rules
  app_Nil   "app [] ys = ys"
  app_Cons  "app (x#xs) ys = x#app xs ys"
end
```

Asserting axioms brings the danger of accidentally asserting nonsense, as in `app [] ys = us`.

The `primrec` declaration is a safe means of defining primitive recursive functions on datatypes:

```
Append = Main +
consts app :: ['a list, 'a list] => 'a list
primrec
  "app [] ys = ys"
  "app (x#xs) ys = x#app xs ys"
end
```

Isabelle will now check that the two rules do indeed form a primitive recursive definition. For example

```
primrec
  "app [] ys = us"
```

is rejected with an error message “`Extra variables on rhs`”.

The general form of a primitive recursive definition is

⁵This facility is based on Konrad Slind’s TFL package [21]. Thanks are due to Konrad for implementing TFL and assisting with its installation.

```
primrec
  reduction rules
```

where *reduction rules* specify one or more equations of the form

$$f x_1 \dots x_m (C y_1 \dots y_k) z_1 \dots z_n = r$$

such that C is a constructor of the datatype, r contains only the free variables on the left-hand side, and all recursive calls in r are of the form $f \dots y_i \dots$ for some i . There must be at most one reduction rule for each constructor. The order is immaterial. For missing constructors, the function is defined to return a default value.

If you would like to refer to some rule by name, then you must prefix the rule with an identifier. These identifiers, like those in the `rules` section of a theory, will be visible at the ML level.

The primitive recursive function can have infix or mixfix syntax:

```
consts "@" :: ['a list, 'a list] => 'a list (infixr 60)
primrec
  "[] @ ys = ys"
  "(x#xs) @ ys = x#(xs @ ys)"
```

The reduction rules become part of the default simpset, which leads to short proof scripts:

```
Goal "(xs @ ys) @ zs = xs @ (ys @ zs)";
by (induct_tac "xs" 1);
by (ALLGOALS Asm_simp_tac);
```

Example: Evaluation of expressions

Using mutual primitive recursion, we can define evaluation functions `evala` and `eval_bexp` for the datatypes of arithmetic and boolean expressions mentioned in §2.8.1:

```

consts
  evala :: "[ 'a => nat, 'a aexp ] => nat"
  evalb :: "[ 'a => nat, 'a bexp ] => bool"

primrec
  "evala env (If_then_else b a1 a2) =
    (if evalb env b then evala env a1 else evala env a2)"
  "evala env (Sum a1 a2) = evala env a1 + evala env a2"
  "evala env (Diff a1 a2) = evala env a1 - evala env a2"
  "evala env (Var v) = env v"
  "evala env (Num n) = n"

  "evalb env (Less a1 a2) = (evala env a1 < evala env a2)"
  "evalb env (And b1 b2) = (evalb env b1 & evalb env b2)"
  "evalb env (Or b1 b2) = (evalb env b1 & evalb env b2)"

```

Since the value of an expression depends on the value of its variables, the functions `evala` and `evalb` take an additional parameter, an *environment* of type `'a => nat`, which maps variables to their values.

Similarly, we may define substitution functions `substa` and `substb` for expressions: The mapping `f` of type `'a => 'a aexp` given as a parameter is lifted canonically on the types `'a aexp` and `'a bexp`:

```

consts
  substa :: "[ 'a => 'b aexp, 'a aexp ] => 'b aexp"
  substb :: "[ 'a => 'b aexp, 'a bexp ] => 'b bexp"

primrec
  "substa f (If_then_else b a1 a2) =
    If_then_else (substb f b) (substa f a1) (substa f a2)"
  "substa f (Sum a1 a2) = Sum (substa f a1) (substa f a2)"
  "substa f (Diff a1 a2) = Diff (substa f a1) (substa f a2)"
  "substa f (Var v) = f v"
  "substa f (Num n) = Num n"

  "substb f (Less a1 a2) = Less (substa f a1) (substa f a2)"
  "substb f (And b1 b2) = And (substb f b1) (substb f b2)"
  "substb f (Or b1 b2) = Or (substb f b1) (substb f b2)"

```

In textbooks about semantics one often finds *substitution theorems*, which express the relationship between substitution and evaluation. For `'a aexp` and `'a bexp`, we can prove such a theorem by mutual induction, followed by simplification:


```

Goal
  "evala env (subst (Var(v := a')) a) =
    evala (env(v := evala env a')) a &
    evalb env (subst (Var(v := a')) b) =
    evalb (env(v := evala env a')) b";
by (induct_tac "a b" 1);
by (ALLGOALS Asm_full_simp_tac);

```

Example: A substitution function for terms

Functions on datatypes with nested recursion, such as the type `term` mentioned in §2.8.1, are also defined by mutual primitive recursion. A substitution function `subst_term` on type `term`, similar to the functions `subst` and `substb` described above, can be defined as follows:

```

consts
  subst_term :: "[ 'a => ( 'a, 'b ) term, ( 'a, 'b ) term ] => ( 'a, 'b ) term"
  subst_term_list ::
    "[ 'a => ( 'a, 'b ) term, ( 'a, 'b ) term list ] => ( 'a, 'b ) term list"

primrec
  "subst_term f (Var a) = f a"
  "subst_term f (App b ts) = App b (subst_term_list f ts)"

  "subst_term_list f [] = []"
  "subst_term_list f (t # ts) =
    subst_term f t # subst_term_list f ts"

```

The recursion scheme follows the structure of the unfolded definition of type `term` shown in §2.8.1. To prove properties of this substitution function, mutual induction is needed:

```

Goal
  "(subst_term ((subst_term f1) o f2) t) =
    (subst_term f1 (subst_term f2 t)) &
    (subst_term_list ((subst_term f1) o f2) ts) =
    (subst_term_list f1 (subst_term_list f2 ts))";
by (induct_tac "t ts" 1);
by (ALLGOALS Asm_full_simp_tac);

```

Example: A map function for infinitely branching trees

Defining functions on infinitely branching datatypes by primitive recursion is just as easy. For example, we can define a function `map_tree` on `'a tree` as follows:

```

consts
  map_tree :: "('a => 'b) => 'a tree => 'b tree"

primrec
  "map_tree f (Atom a) = Atom (f a)"
  "map_tree f (Branch ts) = Branch (%x. map_tree f (ts x))"

```

Note that all occurrences of functions such as `ts` in the `primrec` clauses must be applied to an argument. In particular, `map_tree f o ts` is not allowed.

2.9.2 General recursive functions

Using `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 `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 `Suc 0`.

```

consts fib  :: "nat => nat"
recdef fib "less_than"
  "fib 0 = 0"
  "fib 1 = 1"
  "fib (Suc(Suc x)) = (fib x + fib (Suc x))"

```

With `recdef`, function definitions may be incomplete, and patterns may overlap, as in functional programming. The `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 **well-founded** provided it admits no infinitely decreasing chains

$$\dots \prec x_n \prec \dots \prec x_1.$$

If the function’s argument has type τ , then `<` has to be a relation over τ : it must have type $(\tau \times \tau)$ *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:

- `less_than` is “less than” on the natural numbers. (It has type $(nat \times nat) \text{set}$, while $<$ has type $[nat, nat] \Rightarrow bool$).
- `measure f`, where f has type $\tau \Rightarrow nat$, is the relation \prec on type τ such that $x \prec y$ 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 `size`. It is called a **measure function**. Recall that `size` is overloaded and is defined on all datatypes (see §4).
- `inv_image R f` is a generalisation of `measure`. It specifies a relation such that $x \prec y$ if and only if $f(x)$ is less than $f(y)$ according to R , which must itself be a well-founded relation.
- $R_1 ** R_2$ is the lexicographic product of two relations. It is a relation on pairs and satisfies $(x_1, x_2) \prec (y_1, y_2)$ 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 .
- `finite_psubset` is the proper subset relation on finite sets.

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

```
recdef gcd "measure ((%m,n). n) :: nat*nat=>nat)"
  "gcd (m, n) = (if n=0 then m else gcd(n, m mod n))"
```

The general form of a well-founded recursive definition is

```
recdef function rel
  congs congruence rules (optional)
  simpset simplification set (optional)
  reduction rules
```

where

- *function* is the name of the function, either as an *id* or a *string*.
- *rel* is a HOL expression for the well-founded termination relation.
- *congruence rules* are required only in highly exceptional circumstances.
- The *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 *rel*. By default, simplification uses `simpset ()`, which is sufficient to prove well-foundedness for the built-in relations listed above.

- *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 .*simps* contains the reduction rules as a list of theorems.

With the definition of *gcd* shown above, Isabelle/HOL is unable to prove one termination condition. It remains as a precondition of the recursion theorems:

```
gcd.simps;
  ["! m n. n ~= 0 --> m mod n < n
   ==> gcd (?m, ?n) = (if ?n=0 then ?m else gcd (?n, ?m mod ?n))"]
  : thm list
```

The theory `HOL/ex/Primes` illustrates how to prove termination conditions afterwards. The function `Tf1.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:

```
Tf1.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.

2.10 Inductive and coinductive definitions

An **inductive definition** specifies the least set R closed under given rules. (Applying a rule to elements of R yields a result within R .) For example, a structural operational semantics is an inductive definition of an evaluation relation. Dually, a **coinductive definition** specifies the greatest set R consistent with given rules. (Every element of R can be seen as arising by applying a rule to elements of R .) An important example is using bisimulation relations to formalise equivalence of processes and infinite data structures.

A theory file may contain any number of inductive and coinductive definitions. They may be intermixed with other declarations; in particular, the (co)inductive sets **must** be declared separately as constants, and may have mixfix syntax or be subject to syntax translations.

Each (co)inductive definition adds definitions to the theory and also proves some theorems. Each definition creates an ML structure, which is a substructure of the main theory structure.

This package is related to the ZF one, described in a separate paper,⁶ which you should refer to in case of difficulties. The package is simpler than ZF's thanks to HOL's extra-logical automatic type-checking. The types of the (co)inductive sets determine the domain of the fixedpoint definition, and the package does not have to use inference rules for type-checking.

2.10.1 The result structure

Many of the result structure's components have been discussed in the paper; others are self-explanatory.

⁶It appeared in CADE [14]; a longer version is distributed with Isabelle.

```

sig
val defs          : thm list
val mono         : thm
val unfold       : thm
val intrs        : thm list
val elims        : thm list
val elim         : thm
val mk_cases     : string -> thm
(Inductive definitions only)
val induct       : thm
(coinductive definitions only)
val coinduct     : thm
end

```

Figure 2.25: The ML result of a (co)inductive definition

`defs` is the list of definitions of the recursive sets.

`mono` is a monotonicity theorem for the fixedpoint operator.

`unfold` is a fixedpoint equation for the recursive set (the union of the recursive sets, in the case of mutual recursion).

`intrs` is the list of introduction rules, now proved as theorems, for the recursive sets. The rules are also available individually, using the names given them in the theory file.

`elim`s is the list of elimination rule. This is for compatibility with ML scripts; within the theory the name is `cases`.

`elim` is the head of the list `elim`s. This is for compatibility only.

`mk_cases` is a function to create simplified instances of `elim` using freeness reasoning on underlying datatypes.

For an inductive definition, the result structure contains the rule `induct`. For a coinductive definition, it contains the rule `coinduct`.

Figure 2.25 summarises the two result signatures, specifying the types of all these components.

2.10.2 The syntax of a (co)inductive definition

An inductive definition has the form

<code>inductive</code>	<i>inductive sets</i>
<code>intrs</code>	<i>introduction rules</i>
<code>monos</code>	<i>monotonicity theorems</i>
<code>con_defs</code>	<i>constructor definitions</i>

A coinductive definition is identical, except that it starts with the keyword `coinductive`.

The `monos` and `con_defs` sections are optional. If present, each is specified by a list of identifiers.

- The *inductive sets* are specified by one or more strings.
- The *introduction rules* specify one or more introduction rules in the form *ident string*, where the identifier gives the name of the rule in the result structure.
- The *monotonicity theorems* are required for each operator applied to a recursive set in the introduction rules. There **must** be a theorem of the form $A \subseteq B \implies M(A) \subseteq M(B)$, for each premise $t \in M(R_i)$ in an introduction rule!
- The *constructor definitions* contain definitions of constants appearing in the introduction rules. In most cases it can be omitted.

2.10.3 *Monotonicity theorems

Each theory contains a default set of theorems that are used in monotonicity proofs. New rules can be added to this set via the `mono` attribute. Theory `Inductive` shows how this is done. In general, the following monotonicity theorems may be added:

- Theorems of the form $A \subseteq B \implies M(A) \subseteq M(B)$, for proving monotonicity of inductive definitions whose introduction rules have premises involving terms such as $t \in M(R_i)$.
- Monotonicity theorems for logical operators, which are of the general form $\llbracket \dots \rightarrow \dots; \dots; \dots \rightarrow \dots \rrbracket \implies \dots \rightarrow \dots$. For example, in the case of the operator \vee , the corresponding theorem is

$$\frac{P_1 \rightarrow Q_1 \quad P_2 \rightarrow Q_2}{P_1 \vee P_2 \rightarrow Q_1 \vee Q_2}$$

- De Morgan style equations for reasoning about the “polarity” of expressions, e.g.

$$(\neg\neg P) = P \qquad (\neg(P \wedge Q)) = (\neg P \vee \neg Q)$$

- Equations for reducing complex operators to more primitive ones whose monotonicity can easily be proved, e.g.

$$(P \rightarrow Q) = (\neg P \vee Q) \quad \text{Ball } A P \equiv \forall x. x \in A \rightarrow P x$$

2.10.4 Example of an inductive definition

Two declarations, included in a theory file, define the finite powerset operator. First we declare the constant `Fin`. Then we declare it inductively, with two introduction rules:

```
consts Fin :: 'a set => 'a set set
inductive "Fin A"
  intrs
    emptyI "{ } : Fin A"
    insertI "[| a: A; b: Fin A |] ==> insert a b : Fin A"
```

The resulting theory structure contains a substructure, called `Fin`. It contains the `Fin A` introduction rules as the list `Fin.intrs`, and also individually as `Fin.emptyI` and `Fin.consI`. The induction rule is `Fin.induct`.

For another example, here is a theory file defining the accessible part of a relation. The paper [14] discusses a ZF version of this example in more detail.

```
Acc = WF + Inductive +

consts acc :: "('a * 'a)set => 'a set" (* accessible part *)

inductive "acc r"
  intrs
    accI "ALL y. (y, x) : r --> y : acc r ==> x : acc r"

end
```

The Isabelle distribution contains many other inductive definitions. Simple examples are collected on subdirectory `HOL/Induct`. The theory `HOL/Induct/LList` contains coinductive definitions. Larger examples may be found on other subdirectories of `HOL`, such as `IMP`, `Lambda` and `Auth`.

2.11 The examples directories

Directory `HOL/Auth` contains theories for proving the correctness of cryptographic protocols [17]. The approach is based upon operational semantics rather than the more usual belief logics. On the same directory are proofs

for some standard examples, such as the Needham-Schroeder public-key authentication protocol and the Otway-Rees protocol.

Directory `HOL/IMP` contains a formalization of various denotational, operational and axiomatic semantics of a simple while-language, the necessary equivalence proofs, soundness and completeness of the Hoare rules with respect to the denotational semantics, and soundness and completeness of a verification condition generator. Much of development is taken from Winskel [22]. For details see [12].

Directory `HOL/Hoare` contains a user friendly surface syntax for Hoare logic, including a tactic for generating verification-conditions.

Directory `HOL/MiniML` contains a formalization of the type system of the core functional language Mini-ML and a correctness proof for its type inference algorithm \mathcal{W} [7, 9].

Directory `HOL/Lambda` contains a formalization of untyped λ -calculus in de Bruijn notation and Church-Rosser proofs for β and η reduction [11].

Directory `HOL/Subst` contains Martin Coen's mechanization of a theory of substitutions and unifiers. It is based on Paulson's previous mechanisation in LCF [13] of Manna and Waldinger's theory [6]. It demonstrates a complicated use of `recdef`, with nested recursion.

Directory `HOL/Induct` presents simple examples of (co)inductive definitions and datatypes.

- Theory `PropLog` proves the soundness and completeness of classical propositional logic, given a truth table semantics. The only connective is \rightarrow . A Hilbert-style axiom system is specified, and its set of theorems defined inductively. A similar proof in ZF is described elsewhere [15].
- Theory `Term` defines the datatype `term`.
- Theory `ABexp` defines arithmetic and boolean expressions as mutually recursive datatypes.
- The definition of lazy lists demonstrates methods for handling infinite data structures and coinduction in higher-order logic [16].⁷ Theory `LList` defines an operator for corecursion on lazy lists, which is used to define a few simple functions such as `map` and `append`. A coinduction principle is defined for proving equations on lazy lists.
- Theory `LFilter` defines the filter functional for lazy lists. This functional is notoriously difficult to define because finding the next element

⁷To be precise, these lists are *potentially infinite* rather than lazy. Lazy implies a particular operational semantics.

meeting the predicate requires possibly unlimited search. It is not computable, but can be expressed using a combination of induction and corecursion.

- Theory `Exp` illustrates the use of iterated inductive definitions to express a programming language semantics that appears to require mutual induction. Iterated induction allows greater modularity.

Directory `HOL/ex` contains other examples and experimental proofs in HOL.

- Theory `Recdef` presents many examples of using `recdef` to define recursive functions. Another example is `Fib`, which defines the Fibonacci function.
- Theory `Primes` defines the Greatest Common Divisor of two natural numbers and proves a key lemma of the Fundamental Theorem of Arithmetic: if p is prime and p divides $m \times n$ then p divides m or p divides n .
- Theory `Primrec` develops some computation theory. It inductively defines the set of primitive recursive functions and presents a proof that Ackermann's function is not primitive recursive.
- File `cla.ML` demonstrates the classical reasoner on over sixty predicate calculus theorems, ranging from simple tautologies to moderately difficult problems involving equality and quantifiers.
- File `meson.ML` contains an experimental implementation of the MESON proof procedure, inspired by Plaisted [20]. It is much more powerful than Isabelle's classical reasoner. But it is less useful in practice because it works only for pure logic; it does not accept derived rules for the set theory primitives, for example.
- File `mesontest.ML` contains test data for the MESON proof procedure. These are mostly taken from Pelletier [19].
- File `set.ML` proves Cantor's Theorem, which is presented in §2.12 below, and the Schröder-Bernstein Theorem.
- Theory `MT` contains Jacob Frost's formalization [4] of Milner and Tofte's coinduction example [8]. This substantial proof concerns the soundness of a type system for a simple functional language. The semantics of recursion is given by a cyclic environment, which makes a coinductive argument appropriate.

2.12 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:

$$\forall f :: \alpha \Rightarrow \alpha \Rightarrow \text{bool} . \exists S :: \alpha \Rightarrow \text{bool} . \forall x :: \alpha . f\ x \neq S$$

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

The Isabelle proof uses HOL's set theory, with the type $\alpha \text{ set}$ 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)";
Level 0
?S ~: range f
1. ?S ~: range f
```

The first two steps are routine. The rule `rangeE` replaces $?S \in \text{range } f$ by $?S = f\ x$ for some x .

```
by (resolve_tac [notI] 1);
Level 1
?S ~: range f
1. ?S : range f ==> False
by (eresolve_tac [rangeE] 1);
Level 2
?S ~: range f
1. !!x. ?S = f x ==> False
```

Next, we apply `equalityCE`, reasoning that since $?S = f\ x$, we have $?c \in ?S$ if and only if $?c \in f\ x$ for any $?c$.

```
by (eresolve_tac [equalityCE] 1);
Level 3
?S ~: range f
1. !!x. [| ?c3 x : ?S; ?c3 x : f x |] ==> False
2. !!x. [| ?c3 x ~: ?S; ?c3 x ~: f x |] ==> False
```

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 `CollectD` instantiates $?S$ and creates the new assumption.

```

by (dresolve_tac [CollectD] 1);
  Level 4
  {x. ?P7 x} ~: range f
  1. !!x. [| ?c3 x : f x; ?P7(?c3 x) |] ==> False
  2. !!x. [| ?c3 x ~: {x. ?P7 x}; ?c3 x ~: f x |] ==> False

```

Forcing a contradiction between the two assumptions of subgoal 1 completes the instantiation of S . It is now the set $\{x. x \notin f x\}$, which is the standard diagonal construction.

```

by (contr_tac 1);
  Level 5
  {x. x ~: f x} ~: range f
  1. !!x. [| x ~: {x. x ~: f x}; x ~: f x |] ==> False

```

The rest should be easy. To apply `CollectI` to the negated assumption, we employ `swap_res_tac`:

```

by (swap_res_tac [CollectI] 1);
  Level 6
  {x. x ~: f x} ~: range f
  1. !!x. [| x ~: f x; ~ False |] ==> x ~: f x
by (assume_tac 1);
  Level 7
  {x. x ~: f x} ~: range f
  No subgoals!

```

How much creativity is required? As it happens, Isabelle can prove this theorem automatically. The default classical set `claset()` contains rules for most of the constructs of HOL's set theory. We must augment it with `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.

```

choplev 0;
  Level 0
  ?S ~: range f
  1. ?S ~: range f
by (best_tac (claset() addSEs [equalityCE]) 1);
  Level 1
  {x. x ~: f x} ~: range f
  No subgoals!

```

If you run this example interactively, make sure your current theory contains theory `Set`, for example by executing `context Set.thy`. Otherwise the default `claset` may not contain the rules for set theory.

Bibliography

- [1] Peter Andrews. *An Introduction to Mathematical Logic and Type Theory: to Truth through Proof*. Computer Science and Applied Mathematics. Academic Press, 1986.
- [2] Stefan Berghofer and Markus Wenzel. Inductive datatypes in HOL — lessons learned in Formal-Logic Engineering. In Y. Bertot, G. Dowek, A. Hirschowitz, C. Paulin, and L. Theys, editors, *Theorem Proving in Higher Order Logics: TPHOLs '99*, LNCS 1690, 1999.
- [3] Alonzo Church. A formulation of the simple theory of types. *J. Symb. Logic*, 5:56–68, 1940.
- [4] Jacob Frost. A case study of co-induction in Isabelle HOL. Technical Report 308, Comp. Lab., Univ. Camb., August 1993.
- [5] M. J. C. Gordon and T. F. Melham. *Introduction to HOL: A Theorem Proving Environment for Higher Order Logic*. Cambridge University Press, 1993.
- [6] Zohar Manna and Richard Waldinger. Deductive synthesis of the unification algorithm. *Science of Computer Programming*, 1(1):5–48, 1981.
- [7] Robin Milner. A theory of type polymorphism in programming. *J. Comp. Sys. Sci.*, 17:348–375, 1978.
- [8] Robin Milner and Mads Tofte. Co-induction in relational semantics. *Theoretical Computer Science*, 87:209–220, 1991.
- [9] Wolfgang Naraschewski and Tobias Nipkow. Type inference verified: Algorithm W in Isabelle/HOL. In E. Giménez and C. Paulin-Mohring, editors, *Types for Proofs and Programs: Intl. Workshop TYPES '96*, volume 1512 of *Lect. Notes in Comp. Sci.*, pages 317–332. Springer-Verlag, 1998.
- [10] Wolfgang Naraschewski and Markus Wenzel. Object-oriented verification based on record subtyping in higher-order logic. In Jim Grundy

- and Malcom Newey, editors, *Theorem Proving in Higher Order Logics: TPHOLs '98*, LNCS 1479, 1998.
- [11] Tobias Nipkow. More Church-Rosser proofs (in Isabelle/HOL). In M. McRobbie and J.K. Slaney, editors, *Automated Deduction — CADE-13*, volume 1104 of *Lect. Notes in Comp. Sci.*, pages 733–747. Springer-Verlag, 1996.
- [12] Tobias Nipkow. Winskel is (almost) right: Towards a mechanized semantics textbook. *Formal Aspects Comput.*, 10:171–186, 1998.
- [13] Lawrence C. Paulson. Verifying the unification algorithm in LCF. *Science of Computer Programming*, 5:143–170, 1985.
- [14] Lawrence C. Paulson. A fixedpoint approach to implementing (co)inductive definitions. In Alan Bundy, editor, *Automated Deduction — CADE-12 International Conference*, LNAI 814, pages 148–161. Springer, 1994.
- [15] Lawrence C. Paulson. Set theory for verification: II. Induction and recursion. *J. Auto. Reas.*, 15(2):167–215, 1995.
- [16] Lawrence C. Paulson. Mechanizing coinduction and corecursion in higher-order logic. *J. Logic and Comput.*, 7(2):175–204, March 1997.
- [17] Lawrence C. Paulson. The inductive approach to verifying cryptographic protocols. *J. Comput. Secur.*, 6:85–128, 1998.
- [18] Lawrence C. Paulson. A formulation of the simple theory of types (for Isabelle). In P. Martin-Löf and G. Mints, editors, *COLOG-88: International Conference on Computer Logic*, LNCS 417, pages 246–274, Tallinn, Published 1990. Estonian Academy of Sciences, Springer.
- [19] F. J. Pelletier. Seventy-five problems for testing automatic theorem provers. *J. Auto. Reas.*, 2:191–216, 1986. Errata, JAR 4 (1988), 235–236 and JAR 18 (1997), 135.
- [20] David A. Plaisted. A sequent-style model elimination strategy and a positive refinement. *J. Auto. Reas.*, 6(4):389–402, 1990.
- [21] Konrad Slind. Function definition in higher order logic. In J. von Wright, J. Grundy, and J. Harrison, editors, *Theorem Proving in Higher Order Logics*, volume 1125 of *Lect. Notes in Comp. Sci.*, pages 381–397. Springer-Verlag, 1996.

- [22] Glynn Winskel. *The Formal Semantics of Programming Languages*. MIT Press, 1993.

Index

- ! symbol, 4, 7, 14, 15, 31
- [] symbol, 31
- # symbol, 31
- & symbol, 4
- * symbol, 6, 28
- * type, 24
- + symbol, 6, 28
- + type, 24
- symbol, 6, 28
- > symbol, 4
- : symbol, 13
- < constant, 27
- < symbol, 28
- <= constant, 27
- <= symbol, 13
- = symbol, 4
- ? symbol, 4, 7, 15
- ?! symbol, 4
- @ symbol, 4, 31
- ^ symbol, 6
- ‘ ‘ symbol, 13
- { } symbol, 13
- | symbol, 4

- 0 constant, 6, 28

- Addsplits, 22
- addsplits, 21, 30, 44
- ALL symbol, 4, 14, 15
- All constant, 4
- All_def theorem, 9
- all_dupE theorem, 11
- allE theorem, 11
- allI theorem, 11
- and_def theorem, 9

- arg_cong theorem, 10
- Arith theory, 27
- arith_tac, 29

- Ball constant, 13, 15
- Ball_def theorem, 16
- ballE theorem, 17
- ballI theorem, 17
- Bex constant, 13, 15
- Bex_def theorem, 16
- bexCI theorem, 16, 17
- bexE theorem, 17
- bexI theorem, 16, 17
- bool type, 6
- box_equals theorem, 10, 12
- bspec theorem, 17
- butlast constant, 31

- case symbol, 27, 30, 44
- case_tac, 12, 45
- case_weak_cong, 44
- ccontr theorem, 11
- classical theorem, 11
- coinductive, 57–60
- Collect constant, 13, 15
- Collect_mem_eq theorem, 15, 16
- CollectD theorem, 17, 63
- CollectE theorem, 17
- CollectI theorem, 17, 64
- Compl_def theorem, 16
- Compl_disjoint theorem, 19
- Compl_Int theorem, 19
- Compl_partition theorem, 19
- Compl_Un theorem, 19
- ComplD theorem, 18

- CompI1 theorem, 18
- concat constant, 31
- cong theorem, 10
- conj_cong, 20
- conjE theorem, 10
- conjI theorem, 10
- conjunct1 theorem, 10
- conjunct2 theorem, 10
- context, 64
- datatype, 40, 40–49
- Delsplits, 22
- delsplits, 21
- disjCI theorem, 11
- disjE theorem, 10
- disjI1 theorem, 10
- disjI2 theorem, 10
- div symbol, 28
- div_geq theorem, 28
- div_less theorem, 28
- Divides theory, 27
- double_complement theorem, 19
- drop constant, 31
- dropWhile constant, 31
- dvd symbol, 28
- empty_def theorem, 16
- emptyE theorem, 18
- Eps constant, 4, 7
- eqTrueE theorem, 10
- eqTrueI theorem, 10
- equalityCE theorem, 16, 17, 63, 64
- equalityD1 theorem, 17
- equalityD2 theorem, 17
- equalityE theorem, 17
- equalityI theorem, 17
- EX symbol, 4, 14, 15
- Ex constant, 4
- EX! symbol, 4
- Ex1 constant, 4
- Ex1_def theorem, 9
- ex1E theorem, 11
- ex1I theorem, 11
- Ex_def theorem, 9
- exCI theorem, 11
- excluded_middle theorem, 11
- exE theorem, 11
- exI theorem, 11
- Exp theory, 62
- ext theorem, 8, 9
- False constant, 4
- False_def theorem, 9
- FalseE theorem, 10
- filter constant, 31
- foldl constant, 31
- fst constant, 25
- fst_conv theorem, 25
- fst_def theorem, 25
- Fun theory, 20
- fun type, 6
- fun_cong theorem, 10
- hd constant, 31
- higher-order logic, 3–64
- HOL, 7
- HOL theory, 3
- HOL system, 3, 7
- HOL_basic_ss, 20
- HOL_cs, 22
- HOL_ss, 20
- hyp_subst_tac, 21
- If constant, 4
- if, 21
- if_def theorem, 9
- if_not_P theorem, 11
- if_P theorem, 11
- if_weak_cong, 21
- iff theorem, 8, 9
- iffCE theorem, 11, 16
- iffD1 theorem, 10

- iffD2 theorem, 10
- iffE theorem, 10
- iffI theorem, 10
- image_def theorem, 16
- imageE theorem, 18
- imageI theorem, 18
- impCE theorem, 11
- impE theorem, 10
- impI theorem, 8
- in symbol, 5
- ind* type, 26
- induct_tac, 29, 45
- inductive, 57–60
- inj constant, 20
- inj_def theorem, 20
- inj_Inl theorem, 27
- inj_Inr theorem, 27
- inj_on constant, 20
- inj_on_def theorem, 20
- inj_Suc theorem, 28
- Inl constant, 27
- Inl_not_Inr theorem, 27
- Inr constant, 27
- insert constant, 13
- insert_def theorem, 16
- insertE theorem, 18
- insertI1 theorem, 18
- insertI2 theorem, 18
- INT symbol, 13–15
- Int symbol, 13
- int theorem, 6, 29
- Int_absorb theorem, 19
- Int_assoc theorem, 19
- Int_commute theorem, 19
- INT_D theorem, 18
- Int_def theorem, 16
- INT_E theorem, 18
- Int_greatest theorem, 19
- INT_I theorem, 18
- Int_Inter_image theorem, 19
- Int_lower1 theorem, 19
- Int_lower2 theorem, 19
- Int_Un_distrib theorem, 19
- Int_Union theorem, 19
- IntD1 theorem, 18
- IntD2 theorem, 18
- IntE theorem, 18
- INTER constant, 13
- Inter constant, 13
- INTER1 constant, 13
- INTER1_def theorem, 16
- INTER_def theorem, 16
- Inter_def theorem, 16
- Inter_greatest theorem, 19
- Inter_lower theorem, 19
- Inter_Un_distrib theorem, 19
- InterD theorem, 18
- InterE theorem, 18
- InterI theorem, 18
- IntI theorem, 18
- inv constant, 20
- inv_def theorem, 20

- last constant, 31
- LEAST constant, 6, 7, 27
- Least constant, 4
- Least_def theorem, 9
- length constant, 31
- less_induct theorem, 29
- Let constant, 4, 8
- let symbol, 5
- Let_def theorem, 8, 9
- LFilter theory, 61
- linorder class, 6, 27, 29
- List theory, 30, 31
- list* type, 30
- LList theory, 61

- map constant, 31
- max constant, 6, 27
- mem symbol, 31
- mem_Collect_eq theorem, 15, 16

- min constant, 6, 27
- minus class, 6
- mod symbol, 28
- mod_geq theorem, 28
- mod_less theorem, 28
- mono constant, 6
- mp theorem, 8

- n_not_Suc_n theorem, 28
- Nat theory, 27
- nat type, 27, 28
- nat type, 26–30
- nat theorem, 6
- nat_induct theorem, 28
- nat_rec constant, 29
- NatDef theory, 26
- Not constant, 4
- not_def theorem, 9
- not_sym theorem, 10
- notE theorem, 10
- notI theorem, 10
- notnotD theorem, 11
- null constant, 31

- o symbol, 4, 20
- o_def theorem, 9
- of symbol, 8
- or_def theorem, 9
- Ord theory, 6
- ord class, 6, 7, 27
- order class, 6

- Pair constant, 25
- Pair_eq theorem, 25
- Pair_inject theorem, 25
- PairE theorem, 25
- plus class, 6
- plus_ac0 class, 6
- Pow constant, 13
- Pow_def theorem, 16
- PowD theorem, 18
- power class, 6

- PowI theorem, 18
- primrec, 50, 50–54
- primrec symbol, 27
- priorities, 1
- Prod theory, 24
- prop_cs, 22

- qed_spec_mp, 48

- range constant, 13, 63
- range_def theorem, 16
- rangeE theorem, 18, 63
- rangeI theorem, 18
- real theorem, 6, 29
- recdef, 54–57
- record, 37
- record_simproc, 39
- record_split_tac, 40
- recursion
 - general, 54–57
 - primitive, 50–54
- recursive functions, *see* recursion
- refl theorem, 8
- res_inst_tac, 7
- rev constant, 31

- search
 - best-first, 64
- Set theory, 15
- set constant, 31
- set type, 15
- set_diff_def theorem, 16
- setsum constant, 6
- show_sorts, 7
- show_types, 7
- Sigma constant, 25
- Sigma_def theorem, 25
- SigmaE theorem, 25
- SigmaI theorem, 25
- simplification
 - of case, 44
 - of if, 21

- of conjunctions, 20
- size constant, 45
- smp_tac, 12
- snd constant, 25
- snd_conv theorem, 25
- snd_def theorem, 25
- SOME symbol, 4
- some_equality theorem, 9, 11
- someI theorem, 8, 9
- spec theorem, 11
- split constant, 25
- split theorem, 25
- split_all_tac, 26
- split_def theorem, 25
- split_if theorem, 11, 21
- split_list_case theorem, 30
- split_split theorem, 25
- ssubst theorem, 10, 12
- stac, 21
- strip_tac, 12
- subset_def theorem, 16
- subset_refl theorem, 17
- subset_trans theorem, 17
- subsetCE theorem, 16, 17
- subsetD theorem, 16, 17
- subsetI theorem, 17
- subst theorem, 8
- Suc constant, 28
- Suc_not_Zero theorem, 28
- Sum theory, 26
- sum.split_case theorem, 27
- sum_case constant, 27
- sum_case_Inl theorem, 27
- sum_case_Inr theorem, 27
- sumE theorem, 27
- surj constant, 20
- surj_def theorem, 20
- surjective_pairing theorem, 25
- surjective_sum theorem, 27
- SVC decision procedure, 22–24
- Svc.trace, 23
- SVC_HOME, 24
- SVC_MACHINE, 24
- svc_tac, 22, 22, 23
- swap theorem, 11
- swap_res_tac, 64
- sym theorem, 10
- take constant, 31
- takeWhile constant, 31
- term class, 6
- times class, 6
- tl constant, 31
- tracing
 - of unification, 7
- trans theorem, 10
- True constant, 4
- True_def theorem, 9
- True_or_False theorem, 8, 9
- TrueI theorem, 10
- Trueprop constant, 4
- type definition, 33
- typedef, 30
- UN symbol, 13–15
- Un symbol, 13
- Un1 theorem, 16
- Un2 theorem, 16
- Un_absorb theorem, 19
- Un_assoc theorem, 19
- Un_commute theorem, 19
- Un_def theorem, 16
- UN_E theorem, 18
- UN_I theorem, 18
- Un_Int_distrib theorem, 19
- Un_Inter theorem, 19
- Un_least theorem, 19
- Un_Union_image theorem, 19
- Un_upper1 theorem, 19
- Un_upper2 theorem, 19
- UnCI theorem, 16, 18
- UnE theorem, 18

UnI1 theorem, 18
UnI2 theorem, 18
unification
 incompleteness of, 7
Unify.trace_types, 7
UNION constant, 13
Union constant, 13
UNION1 constant, 13
UNION1_def theorem, 16
UNION_def theorem, 16
Union_def theorem, 16
Union_least theorem, 19
Union_Un_distrib theorem, 19
Union_upper theorem, 19
UnionE theorem, 18
UnionI theorem, 18
unit_eq theorem, 26

ZF theory, 3