

Isabelle's Logics: FOL and ZF

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

With Contributions by Tobias Nipkow and Markus Wenzel¹

8 March 2002

¹Markus Wenzel made numerous improvements. Philippe de Groote contributed to ZF. Philippe Noël and Martin Coen made many contributions to ZF. The research has been funded by the EPSRC (grants GR/G53279, GR/H40570, GR/K57381, GR/K77051, GR/M75440) and by ESPRIT (projects 3245: Logical Frameworks, and 6453: Types) and by the DFG Schwerpunktprogramm *Deduktion*.

Abstract

This manual describes Isabelle's formalizations of many-sorted first-order logic (FOL) and Zermelo-Fraenkel set theory (ZF). See the *Reference Manual* for general Isabelle commands, and *Introduction to Isabelle* for an overall tutorial.

Contents

| | | |
|----------|---|-----------|
| 1 | Syntax definitions | 1 |
| 2 | First-Order Logic | 3 |
| 2.1 | Syntax and rules of inference | 3 |
| 2.2 | Generic packages | 4 |
| 2.3 | Intuitionistic proof procedures | 4 |
| 2.4 | Classical proof procedures | 9 |
| 2.5 | An intuitionistic example | 9 |
| 2.6 | An example of intuitionistic negation | 11 |
| 2.7 | A classical example | 13 |
| 2.8 | Derived rules and the classical tactics | 14 |
| 2.8.1 | Deriving the introduction rule | 15 |
| 2.8.2 | Deriving the elimination rule | 16 |
| 2.8.3 | Using the derived rules | 17 |
| 2.8.4 | Derived rules versus definitions | 18 |
| 3 | Zermelo-Fraenkel Set Theory | 21 |
| 3.1 | Which version of axiomatic set theory? | 21 |
| 3.2 | The syntax of set theory | 22 |
| 3.3 | Binding operators | 24 |
| 3.4 | The Zermelo-Fraenkel axioms | 29 |
| 3.5 | From basic lemmas to function spaces | 31 |
| 3.5.1 | Fundamental lemmas | 31 |
| 3.5.2 | Unordered pairs and finite sets | 31 |
| 3.5.3 | Subset and lattice properties | 34 |
| 3.5.4 | Ordered pairs | 35 |
| 3.5.5 | Relations | 36 |
| 3.5.6 | Functions | 37 |
| 3.6 | Further developments | 38 |
| 3.6.1 | Disjoint unions | 38 |
| 3.6.2 | Non-standard ordered pairs | 41 |
| 3.6.3 | Least and greatest fixedpoints | 41 |
| 3.6.4 | Finite sets and lists | 41 |
| 3.6.5 | Miscellaneous | 45 |
| 3.7 | Automatic Tools | 45 |
| 3.7.1 | Simplification | 45 |

| | | |
|--------|--|----|
| 3.7.2 | Classical Reasoning | 45 |
| 3.7.3 | Type-Checking Tactics | 46 |
| 3.8 | Natural number and integer arithmetic | 47 |
| 3.9 | Datatype definitions | 50 |
| 3.9.1 | Basics | 50 |
| 3.9.2 | Defining datatypes | 53 |
| 3.9.3 | Examples | 54 |
| 3.9.4 | Recursive function definitions | 56 |
| 3.10 | Inductive and coinductive definitions | 58 |
| 3.10.1 | The syntax of a (co)inductive definition | 58 |
| 3.10.2 | Example of an inductive definition | 60 |
| 3.10.3 | Further examples | 61 |
| 3.10.4 | The result structure | 62 |
| 3.11 | The outer reaches of set theory | 63 |
| 3.12 | The examples directories | 64 |
| 3.13 | A proof about powersets | 65 |
| 3.14 | Monotonicity of the union operator | 67 |
| 3.15 | Low-level reasoning about functions | 69 |

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 $(\dots)^*$ 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.

First-Order Logic

Isabelle implements Gentzen’s natural deduction systems NJ and NK. Intuitionistic first-order logic is defined first, as theory `IFOL`. Classical logic, theory `FOL`, is obtained by adding the double negation rule. Basic proof procedures are provided. The intuitionistic prover works with derived rules to simplify implications in the assumptions. Classical `FOL` employs Isabelle’s classical reasoner, which simulates a sequent calculus.

2.1 Syntax and rules of inference

The logic is many-sorted, using Isabelle’s type classes. The class of first-order terms is called `term` and is a subclass of `logic`. No types of individuals are provided, but extensions can define types such as `nat::term` and type constructors such as `list::(term)term` (see the examples directory, `FOL/ex`). Below, the type variable α ranges over class `term`; the equality symbol and quantifiers are polymorphic (many-sorted). The type of formulae is `o`, which belongs to class `logic`. Figure 2.1 gives the syntax. Note that $a \sim b$ is translated to $\neg(a = b)$.

Figure 2.2 shows the inference rules with their ML names. Negation is defined in the usual way for intuitionistic logic; $\neg P$ abbreviates $P \rightarrow \bot$. The biconditional (\leftrightarrow) is defined through \wedge and \rightarrow ; introduction and elimination rules are derived for it.

The unique existence quantifier, $\exists!x. P(x)$, 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 $P(x, y)$.

Some intuitionistic derived rules are shown in Fig. 2.3, again with their ML names. These include rules for the defined symbols \neg , \leftrightarrow and $\exists!$. Natural deduction typically involves a combination of forward and backward reasoning, particularly with the destruction rules $(\wedge E)$, $(\rightarrow E)$, and $(\forall E)$. Isabelle’s backward style handles these rules badly, so sequent-style rules are derived to eliminate conjunctions, implications, and universal quantifiers. Used with elim-resolution, `allE` eliminates a universal quantifier while `all_dupE` re-inserts the quantified formula for later use. The rules `conj_impE`, etc., support the intuitionistic proof procedure (see §2.3).

See the files `FOL/IFOL.thy`, `FOL/IFOL.ML` and `FOL/intprover.ML` for complete listings of the rules and derived rules.

2.2 Generic packages

FOL instantiates most of Isabelle’s generic packages.

- It instantiates the simplifier. Both equality ($=$) and the biconditional (\leftrightarrow) may be used for rewriting. Tactics such as `Asm_simp_tac` and `Full_simp_tac` refer to the default simpset (`simpset()`), which works for most purposes. Named simplification sets include `IFOL_ss`, for intuitionistic first-order logic, and `FOL_ss`, for classical logic. See the file `FOL/simpdata.ML` for a complete listing of the simplification rules.
- It instantiates the classical reasoner. See §2.4 for details.
- FOL provides the tactic `hyp_subst_tac`, which substitutes for an equality throughout a subgoal and its hypotheses. This tactic uses FOL’s general substitution rule.

! 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]`.

2.3 Intuitionistic proof procedures

Implication elimination (the rules `mp` and `impE`) pose difficulties for automated proof. In intuitionistic logic, the assumption $P \rightarrow Q$ cannot be treated like $\neg P \vee Q$. Given $P \rightarrow Q$, we may use Q provided we can prove P ; the proof of P may require repeated use of $P \rightarrow Q$. If the proof of P fails then the whole branch of the proof must be abandoned. Thus intuitionistic propositional logic requires backtracking.

For an elementary example, consider the intuitionistic proof of Q from $P \rightarrow Q$ and $(P \rightarrow Q) \rightarrow P$. The implication $P \rightarrow Q$ is needed twice:

$$\frac{P \rightarrow Q \quad \frac{(P \rightarrow Q) \rightarrow P \quad P \rightarrow Q}{P} (\rightarrow E)}{Q} (\rightarrow E)$$

The theorem prover for intuitionistic logic does not use `impE`. Instead, it simplifies implications using derived rules (Fig. 2.3). It reduces the antecedents of implications to atoms and then uses Modus Ponens: from $P \rightarrow Q$ and P deduce Q . The rules `conj_impE` and `disj_impE` are straightforward: $(P \wedge Q) \rightarrow S$ is equivalent to $P \rightarrow (Q \rightarrow S)$, and $(P \vee Q) \rightarrow S$ is

| <i>name</i> | <i>meta-type</i> | <i>description</i> |
|-----------------|----------------------|-------------------------|
| Trueprop | $o \Rightarrow prop$ | coercion to <i>prop</i> |
| Not | $o \Rightarrow o$ | negation (\neg) |
| True | o | tautology (\top) |
| False | o | absurdity (\perp) |

CONSTANTS

| <i>symbol</i> | <i>name</i> | <i>meta-type</i> | <i>priority</i> | <i>description</i> |
|---------------|-------------|--|-----------------|--------------------------------------|
| ALL | All | $(\alpha \Rightarrow o) \Rightarrow o$ | 10 | universal quantifier (\forall) |
| EX | Ex | $(\alpha \Rightarrow o) \Rightarrow o$ | 10 | existential quantifier (\exists) |
| EX! | Ex1 | $(\alpha \Rightarrow o) \Rightarrow o$ | 10 | unique existence ($\exists!$) |

BINDERS

| <i>symbol</i> | <i>meta-type</i> | <i>priority</i> | <i>description</i> |
|------------------|----------------------------------|-----------------|-------------------------------------|
| = | $[\alpha, \alpha] \Rightarrow o$ | Left 50 | equality ($=$) |
| & | $[o, o] \Rightarrow o$ | Right 35 | conjunction (\wedge) |
| | $[o, o] \Rightarrow o$ | Right 30 | disjunction (\vee) |
| --> | $[o, o] \Rightarrow o$ | Right 25 | implication (\rightarrow) |
| <-> | $[o, o] \Rightarrow o$ | Right 25 | biconditional (\leftrightarrow) |

INFIXES

| | | |
|----------------|---|---|
| <i>formula</i> | = | expression of type <i>o</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> |
| | | <i>formula</i> <-> <i>formula</i> |
| | | ALL <i>id id*</i> . <i>formula</i> |
| | | EX <i>id id*</i> . <i>formula</i> |
| | | EX! <i>id id*</i> . <i>formula</i> |

GRAMMAR

Figure 2.1: Syntax of FOL

| | |
|-------|------------------------------------|
| refl | $a=a$ |
| subst | $[a=b; P(a)] \Rightarrow P(b)$ |

EQUALITY RULES

| | |
|-----------|---|
| conjI | $[P; Q] \Rightarrow P \& Q$ |
| conjunct1 | $P \& Q \Rightarrow P$ |
| conjunct2 | $P \& Q \Rightarrow Q$ |
| disjI1 | $P \Rightarrow P Q$ |
| disjI2 | $Q \Rightarrow P Q$ |
| disjE | $[P Q; P \Rightarrow R; Q \Rightarrow R] \Rightarrow R$ |
| impI | $(P \Rightarrow Q) \Rightarrow P \multimap Q$ |
| mp | $[P \multimap Q; P] \Rightarrow Q$ |
| FalseE | $\text{False} \Rightarrow P$ |

PROPOSITIONAL RULES

| | |
|------|---|
| allI | $(\neg \neg x. P(x)) \Rightarrow (\text{ALL } x. P(x))$ |
| spec | $(\text{ALL } x. P(x)) \Rightarrow P(x)$ |
| exI | $P(x) \Rightarrow (\text{EX } x. P(x))$ |
| exE | $[\text{EX } x. P(x); \neg \neg x. P(x) \Rightarrow R] \Rightarrow R$ |

QUANTIFIER RULES

| | |
|----------|--|
| True_def | $\text{True} \quad == \text{False} \multimap \text{False}$ |
| not_def | $\neg P \quad == P \multimap \text{False}$ |
| iff_def | $P \multimap \neg \neg Q \quad == (P \multimap Q) \& (Q \multimap P)$ |
| ex1_def | $\text{EX! } x. P(x) \quad == \text{EX } x. P(x) \& (\text{ALL } y. P(y) \multimap y=x)$ |

DEFINITIONS

Figure 2.2: Rules of intuitionistic logic

```

sym      a=b ==> b=a
trans    [| a=b; b=c |] ==> a=c
ssubst   [| b=a; P(a) |] ==> P(b)

```

DERIVED EQUALITY RULES

```

TrueI    True

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

iffI      [| P ==> Q; Q ==> P |] ==> P<->Q
iffE      [| P <-> Q; [| P-->Q; Q-->P |] ==> R |] ==> R
iffD1     [| P <-> Q; P |] ==> Q
iffD2     [| P <-> Q; Q |] ==> P

ex1I      [| P(a); !!x. P(x) ==> x=a |] ==> EX! x. P(x)
ex1E      [| EX! x.P(x); !!x.[| P(x); ALL y. P(y) --> y=x |] ==> R
|] ==> R

```

DERIVED RULES FOR \top , \neg , \leftrightarrow AND $\exists!$

```

conjE     [| P&Q; [| P; Q |] ==> R |] ==> R
impE      [| P-->Q; P; Q ==> R |] ==> R
allE      [| ALL x.P(x); P(x) ==> R |] ==> R
all_dupE  [| ALL x.P(x); [| P(x); ALL x.P(x) |] ==> R |] ==> R

```

SEQUENT-STYLE ELIMINATION RULES

```

conj_impE [| (P&Q)-->S; P-->(Q-->S) ==> R |] ==> R
disj_impE [| (P|Q)-->S; [| P-->S; Q-->S |] ==> R |] ==> R
imp_impE  [| (P-->Q)-->S; [| P; Q-->S |] ==> Q; S ==> R |] ==> R
not_impE  [| ~P --> S; P ==> False; S ==> R |] ==> R
iff_impE  [| (P<->Q)-->S; [| P; Q-->S |] ==> Q; [| Q; P-->S |] ==> P;
S ==> R |] ==> R
all_impE  [| (ALL x.P(x))-->S; !!x.P(x); S ==> R |] ==> R
ex_impE   [| (EX x.P(x))-->S; P(a)-->S ==> R |] ==> R

```

INTUITIONISTIC SIMPLIFICATION OF IMPLICATION

Figure 2.3: Derived rules for intuitionistic logic

equivalent to the conjunction of $P \rightarrow S$ and $Q \rightarrow S$. The other `..._impE` rules are unsafe; the method requires backtracking. All the rules are derived in the same simple manner.

Dyckhoff has independently discovered similar rules, and (more importantly) has demonstrated their completeness for propositional logic [8]. However, the tactics given below are not complete for first-order logic because they discard universally quantified assumptions after a single use.

```

mp_tac          : int -> tactic
eq_mp_tac       : int -> tactic
IntPr.safe_step_tac : int -> tactic
IntPr.safe_tac   :         tactic
IntPr.inst_step_tac : int -> tactic
IntPr.step_tac   : int -> tactic
IntPr.fast_tac   : int -> tactic
IntPr.best_tac   : int -> tactic

```

Most of these belong to the structure `IntPr` and resemble the tactics of Isabelle's classical reasoner.

`mp_tac i` attempts to use `notE` or `impE` within the assumptions in subgoal *i*. For each assumption of the form $\neg P$ or $P \rightarrow Q$, it searches for another assumption unifiable with P . By contradiction with $\neg P$ it can solve the subgoal completely; by Modus Ponens it can replace the assumption $P \rightarrow Q$ by Q . The tactic can produce multiple outcomes, enumerating all suitable pairs of assumptions.

`eq_mp_tac i` is like `mp_tac i`, but may not instantiate unknowns — thus, it is safe.

`IntPr.safe_step_tac i` performs a safe step on subgoal *i*. This may include proof by assumption or Modus Ponens (taking care not to instantiate unknowns), or `hyp_subst_tac`.

`IntPr.safe_tac` repeatedly performs safe steps on all subgoals. It is deterministic, with at most one outcome.

`IntPr.inst_step_tac i` is like `safe_step_tac`, but allows unknowns to be instantiated.

`IntPr.step_tac i` tries `safe_tac` or `inst_step_tac`, or applies an unsafe rule. This is the basic step of the intuitionistic proof procedure.

`IntPr.fast_tac i` applies `step_tac`, using depth-first search, to solve subgoal *i*.

`IntPr.best_tac i` applies `step_tac`, using best-first search (guided by the size of the proof state) to solve subgoal *i*.

```

excluded_middle    ~P | P

disjCI             (~Q ==> P) ==> P|Q
exCI               (ALL x. ~P(x) ==> P(a)) ==> EX 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

```

Figure 2.4: Derived rules for classical logic

Here are some of the theorems that `IntPr.fast_tac` proves automatically. The latter three date from *Principia Mathematica* (*11.53, *11.55, *11.61) [21].

```

~~P & ~~(P --> Q) --> ~~Q
(ALL x y. P(x) --> Q(y)) <-> ((EX x. P(x)) --> (ALL y. Q(y)))
(EX x y. P(x) & Q(x,y)) <-> (EX x. P(x) & (EX y. Q(x,y)))
(EX y. ALL x. P(x) --> Q(x,y)) --> (ALL x. P(x) --> (EX y. Q(x,y)))

```

2.4 Classical proof procedures

The classical theory, FOL, consists of intuitionistic logic plus the rule

$$\frac{[\neg P] \quad \dots \quad P}{P} \quad (classical)$$

Natural deduction in classical logic is not really all that natural. FOL derives classical introduction rules for \forall and \exists , as well as classical elimination rules for \rightarrow and \leftrightarrow , and the swap rule (see Fig. 2.4).

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 claset include `prop_cs`, which includes the propositional rules, and `FOL_cs`, which also includes quantifier rules. See the file `FOL/cladata.ML` for lists of the classical rules, and the *Reference Manual* for more discussion of classical proof methods.

2.5 An intuitionistic example

Here is a session similar to one in *Logic and Computation* [13, pages 222–3]. Isabelle treats quantifiers differently from LCF-based theorem provers such as HOL.

First, we specify that we are working in intuitionistic logic:

```
context IFOL.thy;
```

The proof begins by entering the goal, then applying the rule $(\rightarrow I)$.

```
Goal "(EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))";
Level 0
(EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))
1. (EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))
by (resolve_tac [impI] 1);
Level 1
(EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))
1. EX y. ALL x. Q(x,y) ==> ALL x. EX y. Q(x,y)
```

In this example, we shall never have more than one subgoal. Applying $(\rightarrow I)$ replaces $-->$ by $==>$, making $\exists y. \forall x. Q(x, y)$ an assumption. We have the choice of $(\exists E)$ and $(\forall I)$; let us try the latter.

```
by (resolve_tac [allI] 1);
Level 2
(EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))
1. !!x. EX y. ALL x. Q(x,y) ==> EX y. Q(x,y)
```

Applying $(\forall I)$ replaces the $ALL\ x$ by $!!x$, changing the universal quantifier from object (\forall) to meta (\wedge) . The bound variable is a **parameter** of the subgoal. We now must choose between $(\exists I)$ and $(\exists E)$. What happens if the wrong rule is chosen?

```
by (resolve_tac [exI] 1);
Level 3
(EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))
1. !!x. EX y. ALL x. Q(x,y) ==> Q(x,?y2(x))
```

The new subgoal 1 contains the function variable $?y2$. Instantiating $?y2$ can replace $?y2(x)$ by a term containing x , even though x is a bound variable. Now we analyse the assumption $\exists y. \forall x. Q(x, y)$ using elimination rules:

```
by (eresolve_tac [exE] 1);
Level 4
(EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))
1. !!x y. ALL x. Q(x,y) ==> Q(x,?y2(x))
```

Applying $(\exists E)$ has produced the parameter y and stripped the existential quantifier from the assumption. But the subgoal is unprovable: there is no way to unify $?y2(x)$ with the bound variable y . Using `choplev` we can return to the critical point. This time we apply $(\exists E)$:

```
choplev 2;
Level 2
(EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))
1. !!x. EX y. ALL x. Q(x,y) ==> EX y. Q(x,y)
```

```

by (eresolve_tac [exE] 1);
Level 3
(EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))
1. !!x y. ALL x. Q(x,y) ==> EX y. Q(x,y)

```

We now have two parameters and no scheme variables. Applying $(\exists I)$ and $(\forall E)$ produces two scheme variables, which are applied to those parameters. Parameters should be produced early, as this example demonstrates.

```

by (resolve_tac [exI] 1);
Level 4
(EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))
1. !!x y. ALL x. Q(x,y) ==> Q(x,?y3(x,y))
by (eresolve_tac [allE] 1);
Level 5
(EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))
1. !!x y. Q(?x4(x,y),y) ==> Q(x,?y3(x,y))

```

The subgoal has variables $?y3$ and $?x4$ applied to both parameters. The obvious projection functions unify $?x4(x,y)$ with x and $?y3(x,y)$ with y .

```

by (assume_tac 1);
Level 6
(EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))
No subgoals!

```

The theorem was proved in six tactic steps, not counting the abandoned ones. But proof checking is tedious; `IntPr.fast_tac` proves the theorem in one step.

```

Goal "(EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))";
Level 0
(EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))
1. (EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))
by (IntPr.fast_tac 1);
Level 1
(EX y. ALL x. Q(x,y)) --> (ALL x. EX y. Q(x,y))
No subgoals!

```

2.6 An example of intuitionistic negation

The following example demonstrates the specialized forms of implication elimination. Even propositional formulae can be difficult to prove from the basic rules; the specialized rules help considerably.

Propositional examples are easy to invent. As Dummett notes [7, page 28], $\neg P$ is classically provable if and only if it is intuitionistically provable; therefore, P is classically provable if and only if $\neg\neg P$ is intuitionistically provable.¹ Proving $\neg\neg P$ intuitionistically is much harder than proving P classically.

¹Of course this holds only for propositional logic, not if P is allowed to contain quantifiers.

Our example is the double negation of the classical tautology $(P \rightarrow Q) \vee (Q \rightarrow P)$. When stating the goal, we command Isabelle to expand negations to implications using the definition $\neg P \equiv P \rightarrow \perp$. This allows use of the special implication rules.

```
Goalw [not_def] "~ ~ ((P-->Q) | (Q-->P))";
Level 0
~ ~ ((P --> Q) | (Q --> P))
1. ((P --> Q) | (Q --> P) --> False) --> False
```

The first step is trivial.

```
by (resolve_tac [impI] 1);
Level 1
~ ~ ((P --> Q) | (Q --> P))
1. (P --> Q) | (Q --> P) --> False ==> False
```

By $(\rightarrow E)$ it would suffice to prove $(P \rightarrow Q) \vee (Q \rightarrow P)$, but that formula is not a theorem of intuitionistic logic. Instead we apply the specialized implication rule `disj_impE`. It splits the assumption into two assumptions, one for each disjunct.

```
by (eresolve_tac [disj_impE] 1);
Level 2
~ ~ ((P --> Q) | (Q --> P))
1. [| (P --> Q) --> False; (Q --> P) --> False |] ==> False
```

We cannot hope to prove $P \rightarrow Q$ or $Q \rightarrow P$ separately, but their negations are inconsistent. Applying `imp_impE` breaks down the assumption $\neg(P \rightarrow Q)$, asking to show Q while providing new assumptions P and $\neg Q$.

```
by (eresolve_tac [imp_impE] 1);
Level 3
~ ~ ((P --> Q) | (Q --> P))
1. [| (Q --> P) --> False; P; Q --> False |] ==> Q
2. [| (Q --> P) --> False; False |] ==> False
```

Subgoal 2 holds trivially; let us ignore it and continue working on subgoal 1. Thanks to the assumption P , we could prove $Q \rightarrow P$; applying `imp_impE` is simpler.

```
by (eresolve_tac [imp_impE] 1);
Level 4
~ ~ ((P --> Q) | (Q --> P))
1. [| P; Q --> False; Q; P --> False |] ==> P
2. [| P; Q --> False; False |] ==> Q
3. [| (Q --> P) --> False; False |] ==> False
```

The three subgoals are all trivial.

```
by (REPEAT (eresolve_tac [FalseE] 2));
Level 5
~ ~ ((P --> Q) | (Q --> P))
1. [| P; Q --> False; Q; P --> False |] ==> P
```



```

by (assume_tac 1);
Level 6
~ ~ ((P --> Q) | (Q --> P))
No subgoals!

```

This proof is also trivial for `IntPr.fast_tac`.

2.7 A classical example

To illustrate classical logic, we shall prove the theorem $\exists y. \forall x. P(y) \rightarrow P(x)$. Informally, the theorem can be proved as follows. Choose y such that $\neg P(y)$, if such exists; otherwise $\forall x. P(x)$ is true. Either way the theorem holds. First, we switch to classical logic:

```
context FOL.thy;
```

The formal proof does not conform in any obvious way to the sketch given above. The key inference is the first one, `exCI`; this classical version of $(\exists I)$ allows multiple instantiation of the quantifier.

```

Goal "EX y. ALL x. P(y)-->P(x)";
Level 0
EX y. ALL x. P(y) --> P(x)
1. EX y. ALL x. P(y) --> P(x)
by (resolve_tac [exCI] 1);
Level 1
EX y. ALL x. P(y) --> P(x)
1. ALL y. ~ (ALL x. P(y) --> P(x)) ==> ALL x. P(?a) --> P(x)

```

We can either exhibit a term `?a` to satisfy the conclusion of subgoal 1, or produce a contradiction from the assumption. The next steps are routine.

```

by (resolve_tac [allI] 1);
Level 2
EX y. ALL x. P(y) --> P(x)
1. !!x. ALL y. ~ (ALL x. P(y) --> P(x)) ==> P(?a) --> P(x)
by (resolve_tac [impI] 1);
Level 3
EX y. ALL x. P(y) --> P(x)
1. !!x. [| ALL y. ~ (ALL x. P(y) --> P(x)); P(?a) |] ==> P(x)

```

By the duality between \exists and \forall , applying $(\forall E)$ in effect applies $(\exists I)$ again.

```

by (eresolve_tac [allE] 1);
Level 4
EX y. ALL x. P(y) --> P(x)
1. !!x. [| P(?a); ~ (ALL xa. P(?y3(x)) --> P(xa)) |] ==> P(x)

```

In classical logic, a negated assumption is equivalent to a conclusion. To get this effect, we create a swapped version of $(\forall I)$ and apply it using `eresolve_tac`; we could equivalently have applied $(\forall I)$ using `swap_res_tac`.

```

allI RSN (2,swap);
  val it = "[| ~ (ALL x. ?P1(x)); !!x. ~ ?Q ==> ?P1(x) |] ==> ?Q" : thm
by (eresolve_tac [it] 1);
  Level 5
  EX y. ALL x. P(y) --> P(x)
  1. !!x xa. [| P(?a); ~ P(x) |] ==> P(?y3(x)) --> P(xa)

```

The previous conclusion, $P(x)$, has become a negated assumption.

```

by (resolve_tac [impI] 1);
  Level 6
  EX y. ALL x. P(y) --> P(x)
  1. !!x xa. [| P(?a); ~ P(x); P(?y3(x)) |] ==> P(xa)

```

The subgoal has three assumptions. We produce a contradiction between the assumptions $\sim P(x)$ and $P(?y3(x))$. The proof never instantiates the unknown $?a$.

```

by (eresolve_tac [notE] 1);
  Level 7
  EX y. ALL x. P(y) --> P(x)
  1. !!x xa. [| P(?a); P(?y3(x)) |] ==> P(x)
by (assume_tac 1);
  Level 8
  EX y. ALL x. P(y) --> P(x)
  No subgoals!

```

The civilised way to prove this theorem is through `Blast_tac`, which automatically uses the classical version of $(\exists I)$:

```

Goal "EX y. ALL x. P(y)-->P(x)";
  Level 0
  EX y. ALL x. P(y) --> P(x)
  1. EX y. ALL x. P(y) --> P(x)
by (Blast_tac 1);
  Depth = 0
  Depth = 1
  Depth = 2
  Level 1
  EX y. ALL x. P(y) --> P(x)
  No subgoals!

```

If this theorem seems counterintuitive, then perhaps you are an intuitionist. In constructive logic, proving $\exists y . \forall x . P(y) \rightarrow P(x)$ requires exhibiting a particular term t such that $\forall x . P(t) \rightarrow P(x)$, which we cannot do without further knowledge about P .

2.8 Derived rules and the classical tactics

Classical first-order logic can be extended with the propositional connective $if(P, Q, R)$, where

$$if(P, Q, R) \equiv P \wedge Q \vee \neg P \wedge R. \quad (if)$$

Theorems about *if* can be proved by treating this as an abbreviation, replacing $if(P, Q, R)$ by $P \wedge Q \vee \neg P \wedge R$ in subgoals. But this duplicates P , causing an exponential blowup and an unreadable formula. Introducing further abbreviations makes the problem worse.

Natural deduction demands rules that introduce and eliminate $if(P, Q, R)$ directly, without reference to its definition. The simple identity

$$if(P, Q, R) \leftrightarrow (P \rightarrow Q) \wedge (\neg P \rightarrow R)$$

suggests that the *if*-introduction rule should be

$$\frac{\begin{array}{c} [P] \\ \vdots \\ Q \end{array} \quad \begin{array}{c} [\neg P] \\ \vdots \\ R \end{array}}{if(P, Q, R)} (if\ I)$$

The *if*-elimination rule reflects the definition of $if(P, Q, R)$ and the elimination rules for \vee and \wedge .

$$\frac{\begin{array}{c} [P, Q] \\ \vdots \\ if(P, Q, R) \end{array} \quad \begin{array}{c} [\neg P, R] \\ \vdots \\ S \end{array} \quad \begin{array}{c} [\neg P, R] \\ \vdots \\ S \end{array}}{S} (if\ E)$$

Having made these plans, we get down to work with Isabelle. The theory of classical logic, FOL, is extended with the constant $if :: [o, o, o] \Rightarrow o$. The axiom `if_def` asserts the equation (*if*).

```
If = FOL +
consts if      :: [o,o,o]>=>o
rules  if_def  "if(P,Q,R) == P&Q | ~P&R"
end
```

We create the file `If.thy` containing these declarations. (This file is on directory `FOL/ex` in the Isabelle distribution.) Typing

```
use_thy "If";
```

loads that theory and sets it to be the current context.

2.8.1 Deriving the introduction rule

The derivations of the introduction and elimination rules demonstrate the methods for rewriting with definitions. Classical reasoning is required, so we use `blast_tac`.

The introduction rule, given the premises $P \Rightarrow Q$ and $\neg P \Rightarrow R$, concludes $if(P, Q, R)$. We propose the conclusion as the main goal using `Goalw`, which uses `if_def` to rewrite occurrences of *if* in the subgoal.

```

val prems = Goalw [if_def]
  "[| P ==> Q; ~ P ==> R |] ==> if(P,Q,R)";
Level 0
if(P,Q,R)
1. P & Q | ~ P & R

```

The premises (bound to the ML variable `prems`) are passed as introduction rules to `blast_tac`. Remember that `claset()` refers to the default classical set.

```

by (blast_tac (claset() addIs prems) 1);
Level 1
if(P,Q,R)
No subgoals!
qed "ifI";

```

2.8.2 Deriving the elimination rule

The elimination rule has three premises, two of which are themselves rules. The conclusion is simply S .

```

val major::prems = Goalw [if_def]
  "[| if(P,Q,R); [| P; Q |] ==> S; [| ~ P; R |] ==> S |] ==> S";
Level 0
S
1. S

```

The major premise contains an occurrence of *if*, but the version returned by `Goalw` (and bound to the ML variable `major`) has the definition expanded. Now `cut_facts_tac` inserts `major` as an assumption in the subgoal, so that `blast_tac` can break it down.

```

by (cut_facts_tac [major] 1);
Level 1
S
1. P & Q | ~ P & R ==> S
by (blast_tac (claset() addIs prems) 1);
Level 2
S
No subgoals!
qed "ifE";

```

As you may recall from *Introduction to Isabelle*, there are other ways of treating definitions when deriving a rule. We can start the proof using `Goal`, which does not expand definitions, instead of `Goalw`. We can use `rew_tac` to expand definitions in the subgoals—perhaps after calling `cut_facts_tac` to insert the rule's premises. We can use `rewrite_rule`, which is a meta-inference rule, to expand definitions in the premises directly.

2.8.3 Using the derived rules

The rules just derived have been saved with the ML names `ifI` and `ifE`. They permit natural proofs of theorems such as the following:

$$\begin{aligned} \text{if}(P, \text{if}(Q, A, B), \text{if}(Q, C, D)) &\leftrightarrow \text{if}(Q, \text{if}(P, A, C), \text{if}(P, B, D)) \\ \text{if}(\text{if}(P, Q, R), A, B) &\leftrightarrow \text{if}(P, \text{if}(Q, A, B), \text{if}(R, A, B)) \end{aligned}$$

Proofs also require the classical reasoning rules and the \leftrightarrow introduction rule (called `iffI`: do not confuse with `ifI`).

To display the *if*-rules in action, let us analyse a proof step by step.

```
Goal "if(P, if(Q,A,B), if(Q,C,D)) <-> if(Q, if(P,A,C), if(P,B,D))";
Level 0
if(P,if(Q,A,B),if(Q,C,D)) <-> if(Q,if(P,A,C),if(P,B,D))
1. if(P,if(Q,A,B),if(Q,C,D)) <-> if(Q,if(P,A,C),if(P,B,D))
by (resolve_tac [iffI] 1);
Level 1
if(P,if(Q,A,B),if(Q,C,D)) <-> if(Q,if(P,A,C),if(P,B,D))
1. if(P,if(Q,A,B),if(Q,C,D)) ==> if(Q,if(P,A,C),if(P,B,D))
2. if(Q,if(P,A,C),if(P,B,D)) ==> if(P,if(Q,A,B),if(Q,C,D))
```

The *if*-elimination rule can be applied twice in succession.

```
by (eresolve_tac [ifE] 1);
Level 2
if(P,if(Q,A,B),if(Q,C,D)) <-> if(Q,if(P,A,C),if(P,B,D))
1. [| P; if(Q,A,B) |] ==> if(Q,if(P,A,C),if(P,B,D))
2. [| ~ P; if(Q,C,D) |] ==> if(Q,if(P,A,C),if(P,B,D))
3. if(Q,if(P,A,C),if(P,B,D)) ==> if(P,if(Q,A,B),if(Q,C,D))
by (eresolve_tac [ifE] 1);
Level 3
if(P,if(Q,A,B),if(Q,C,D)) <-> if(Q,if(P,A,C),if(P,B,D))
1. [| P; Q; A |] ==> if(Q,if(P,A,C),if(P,B,D))
2. [| P; ~ Q; B |] ==> if(Q,if(P,A,C),if(P,B,D))
3. [| ~ P; if(Q,C,D) |] ==> if(Q,if(P,A,C),if(P,B,D))
4. if(Q,if(P,A,C),if(P,B,D)) ==> if(P,if(Q,A,B),if(Q,C,D))
```

In the first two subgoals, all assumptions have been reduced to atoms. Now *if*-introduction can be applied. Observe how the *if*-rules break down occurrences of *if* when they become the outermost connective.

```
by (resolve_tac [ifI] 1);
Level 4
if(P,if(Q,A,B),if(Q,C,D)) <-> if(Q,if(P,A,C),if(P,B,D))
1. [| P; Q; A; Q |] ==> if(P,A,C)
2. [| P; Q; A; ~ Q |] ==> if(P,B,D)
3. [| P; ~ Q; B |] ==> if(Q,if(P,A,C),if(P,B,D))
4. [| ~ P; if(Q,C,D) |] ==> if(Q,if(P,A,C),if(P,B,D))
5. if(Q,if(P,A,C),if(P,B,D)) ==> if(P,if(Q,A,B),if(Q,C,D))
```

```

by (resolve_tac [ifI] 1);
  Level 5
  if(P,if(Q,A,B),if(Q,C,D)) <-> if(Q,if(P,A,C),if(P,B,D))
  1. [| P; Q; A; Q; P |] ==> A
  2. [| P; Q; A; Q; ~ P |] ==> C
  3. [| P; Q; A; ~ Q |] ==> if(P,B,D)
  4. [| P; ~ Q; B |] ==> if(Q,if(P,A,C),if(P,B,D))
  5. [| ~ P; if(Q,C,D) |] ==> if(Q,if(P,A,C),if(P,B,D))
  6. if(Q,if(P,A,C),if(P,B,D)) ==> if(P,if(Q,A,B),if(Q,C,D))

```

Where do we stand? The first subgoal holds by assumption; the second and third, by contradiction. This is getting tedious. We could use the classical reasoner, but first let us extend the default claset with the derived rules for *if*.

```

AddSIs [ifI];
AddSEs [ifE];

```

Now we can revert to the initial proof state and let **blast_tac** solve it.

```

choplev 0;
  Level 0
  if(P,if(Q,A,B),if(Q,C,D)) <-> if(Q,if(P,A,C),if(P,B,D))
  1. if(P,if(Q,A,B),if(Q,C,D)) <-> if(Q,if(P,A,C),if(P,B,D))
by (Blast_tac 1);
  Level 1
  if(P,if(Q,A,B),if(Q,C,D)) <-> if(Q,if(P,A,C),if(P,B,D))
  No subgoals!

```

This tactic also solves the other example.

```

Goal "if(if(P,Q,R), A, B) <-> if(P, if(Q,A,B), if(R,A,B))";
  Level 0
  if(if(P,Q,R),A,B) <-> if(P,if(Q,A,B),if(R,A,B))
  1. if(if(P,Q,R),A,B) <-> if(P,if(Q,A,B),if(R,A,B))
by (Blast_tac 1);
  Level 1
  if(if(P,Q,R),A,B) <-> if(P,if(Q,A,B),if(R,A,B))
  No subgoals!

```

2.8.4 Derived rules versus definitions

Dispensing with the derived rules, we can treat *if* as an abbreviation, and let **blast_tac** prove the expanded formula. Let us redo the previous proof:

```

choplev 0;
  Level 0
  if(if(P,Q,R),A,B) <-> if(P,if(Q,A,B),if(R,A,B))
  1. if(if(P,Q,R),A,B) <-> if(P,if(Q,A,B),if(R,A,B))

```

This time, simply unfold using the definition of *if*:

```

by (rewtac if_def);
Level 1
if(if(P,Q,R),A,B) <-> if(P,if(Q,A,B),if(R,A,B))
1. (P & Q | ~ P & R) & A | ~ (P & Q | ~ P & R) & B <->
   P & (Q & A | ~ Q & B) | ~ P & (R & A | ~ R & B)

```

We are left with a subgoal in pure first-order logic, which is why the classical reasoner can prove it given `FOL_cs` alone. (We could, of course, have used `Blast_tac`.)

```

by (blast_tac FOL_cs 1);
Level 2
if(if(P,Q,R),A,B) <-> if(P,if(Q,A,B),if(R,A,B))
No subgoals!

```

Expanding definitions reduces the extended logic to the base logic. This approach has its merits — especially if the prover for the base logic is good — but can be slow. In these examples, proofs using the default claset (which includes the derived rules) run about six times faster than proofs using `FOL_cs`.

Expanding definitions also complicates error diagnosis. Suppose we are having difficulties in proving some goal. If by expanding definitions we have made it unreadable, then we have little hope of diagnosing the problem.

Attempts at program verification often yield invalid assertions. Let us try to prove one:

```

Goal "if(if(P,Q,R), A, B) <-> if(P, if(Q,A,B), if(R,B,A))";
Level 0
if(if(P,Q,R),A,B) <-> if(P,if(Q,A,B),if(R,B,A))
1. if(if(P,Q,R),A,B) <-> if(P,if(Q,A,B),if(R,B,A))
by (Blast_tac 1);
by: tactic failed

```

This failure message is uninformative, but we can get a closer look at the situation by applying `Step_tac`.

```

by (REPEAT (Step_tac 1));
Level 1
if(if(P,Q,R),A,B) <-> if(P,if(Q,A,B),if(R,B,A))
1. [| A; ~ P; R; ~ P; R |] ==> B
2. [| B; ~ P; ~ R; ~ P; ~ R |] ==> A
3. [| ~ P; R; B; ~ P; R |] ==> A
4. [| ~ P; ~ R; A; ~ B; ~ P |] ==> R

```

Subgoal 1 is unprovable and yields a countermodel: P and B are false while R and A are true. This truth assignment reduces the main goal to $true \leftrightarrow false$, which is of course invalid.

We can repeat this analysis by expanding definitions, using just the rules of FOL:

```

choplev 0;
Level 0
if(if(P,Q,R),A,B) <-> if(P,if(Q,A,B),if(R,B,A))
1. if(if(P,Q,R),A,B) <-> if(P,if(Q,A,B),if(R,B,A))
by (rewtac if_def);
Level 1
if(if(P,Q,R),A,B) <-> if(P,if(Q,A,B),if(R,B,A))
1. (P & Q | ~ P & R) & A | ~ (P & Q | ~ P & R) & B <->
   P & (Q & A | ~ Q & B) | ~ P & (R & B | ~ R & A)
by (blast_tac FOL_cs 1);
by: tactic failed

```

Again we apply `step_tac`:

```

by (REPEAT (step_tac FOL_cs 1));
Level 2
if(if(P,Q,R),A,B) <-> if(P,if(Q,A,B),if(R,B,A))
1. [| A; ~ P; R; ~ P; R; ~ False |] ==> B
2. [| A; ~ P; R; R; ~ False; ~ B; ~ B |] ==> Q
3. [| B; ~ P; ~ R; ~ P; ~ A |] ==> R
4. [| B; ~ P; ~ R; ~ Q; ~ A |] ==> R
5. [| B; ~ R; ~ P; ~ A; ~ R; Q; ~ False |] ==> A
6. [| ~ P; R; B; ~ P; R; ~ False |] ==> A
7. [| ~ P; ~ R; A; ~ B; ~ R |] ==> P
8. [| ~ P; ~ R; A; ~ B; ~ R |] ==> Q

```

Subgoal 1 yields the same countermodel as before. But each proof step has taken six times as long, and the final result contains twice as many subgoals.

Expanding definitions causes a great increase in complexity. This is why the classical prover has been designed to accept derived rules.

Zermelo-Fraenkel Set Theory

The theory `ZF` implements Zermelo-Fraenkel set theory [9, 20] as an extension of `FOL`, classical first-order logic. The theory includes a collection of derived natural deduction rules, for use with Isabelle’s classical reasoner. Much of it is based on the work of Noël [11].

A tremendous amount of set theory has been formally developed, including the basic properties of relations, functions, ordinals and cardinals. Significant results have been proved, such as the Schröder-Bernstein Theorem, the Wellordering Theorem and a version of Ramsey’s Theorem. `ZF` provides both the integers and the natural numbers. General methods have been developed for solving recursion equations over monotonic functors; these have been applied to yield constructions of lists, trees, infinite lists, etc.

`ZF` has a flexible package for handling inductive definitions, such as inference systems, and datatype definitions, such as lists and trees. Moreover it handles coinductive definitions, such as bisimulation relations, and co-datatype definitions, such as streams. It provides a streamlined syntax for defining primitive recursive functions over datatypes.

Because `ZF` is an extension of `FOL`, it provides the same packages, namely `hyp_subst_tac`, the simplifier, and the classical reasoner. The default simpset and claset are usually satisfactory.

Published articles [14, 16] describe `ZF` less formally than this chapter. Isabelle employs a novel treatment of non-well-founded data structures within the standard `ZF` axioms including the Axiom of Foundation [18].

3.1 Which version of axiomatic set theory?

The two main axiom systems for set theory are Bernays-Gödel (BG) and Zermelo-Fraenkel (ZF). Resolution theorem provers can use BG because it is finite [3, 19]. ZF does not have a finite axiom system because of its Axiom Scheme of Replacement. This makes it awkward to use with many theorem provers, since instances of the axiom scheme have to be invoked explicitly. Since Isabelle has no difficulty with axiom schemes, we may adopt either axiom system.

These two theories differ in their treatment of **classes**, which are collections that are ‘too big’ to be sets. The class of all sets, V , cannot be a

set without admitting Russell's Paradox. In BG, both classes and sets are individuals; $x \in V$ expresses that x is a set. In ZF, all variables denote sets; classes are identified with unary predicates. The two systems define essentially the same sets and classes, with similar properties. In particular, a class cannot belong to another class (let alone a set).

Modern set theorists tend to prefer ZF because they are mainly concerned with sets, rather than classes. BG requires tiresome proofs that various collections are sets; for instance, showing $x \in \{x\}$ requires showing that x is a set.

3.2 The syntax of set theory

The language of set theory, as studied by logicians, has no constants. The traditional axioms merely assert the existence of empty sets, unions, powersets, etc.; this would be intolerable for practical reasoning. The Isabelle theory declares constants for primitive sets. It also extends FOL with additional syntax for finite sets, ordered pairs, comprehension, general union/intersection, general sums/products, and bounded quantifiers. In most other respects, Isabelle implements precisely Zermelo-Fraenkel set theory.

Figure 3.1 lists the constants and infixes of ZF, while Figure 3.2 presents the syntax translations. Finally, Figure 3.3 presents the full grammar for set theory, including the constructs of FOL.

Local abbreviations can be introduced by a **let** construct whose syntax appears in Fig. 3.3. Internally it is translated into the constant **Let**. It can be expanded by rewriting with its definition, **Let_def**.

Apart from **let**, set theory does not use polymorphism. All terms in ZF have type i , which is the type of individuals and has class **term**. The type of first-order formulae, remember, is o .

Infix operators include binary union and intersection ($A \cup B$ and $A \cap B$), set difference ($A - B$), and the subset and membership relations. Note that $a \sim b$ is translated to $\neg(a \in b)$. The union and intersection operators ($\bigcup A$ and $\bigcap A$) form the union or intersection of a set of sets; $\bigcup A$ means the same as $\bigcup_{x \in A} x$. Of these operators, only $\bigcup A$ is primitive.

The constant **Upair** constructs unordered pairs; thus **Upair**(A, B) denotes the set $\{A, B\}$ and **Upair**(A, A) denotes the singleton $\{A\}$. General union is used to define binary union. The Isabelle version goes on to define the constant **cons**:

$$\begin{aligned} A \cup B &\equiv \bigcup(\text{Upair}(A, B)) \\ \text{cons}(a, B) &\equiv \text{Upair}(a, a) \cup B \end{aligned}$$

The $\{a_1, \dots\}$ notation abbreviates finite sets constructed in the obvious man-

| <i>name</i> | <i>meta-type</i> | <i>description</i> |
|-------------|--|---------------------------|
| Let | $[\alpha, \alpha \Rightarrow \beta] \Rightarrow \beta$ | let binder |
| 0 | i | empty set |
| cons | $[i, i] \Rightarrow i$ | finite set constructor |
| Upair | $[i, i] \Rightarrow i$ | unordered pairing |
| Pair | $[i, i] \Rightarrow i$ | ordered pairing |
| Inf | i | infinite set |
| Pow | $i \Rightarrow i$ | powerset |
| Union Inter | $i \Rightarrow i$ | set union/intersection |
| split | $[[i, i] \Rightarrow i, i] \Rightarrow i$ | generalized projection |
| fst snd | $i \Rightarrow i$ | projections |
| converse | $i \Rightarrow i$ | converse of a relation |
| succ | $i \Rightarrow i$ | successor |
| Collect | $[i, i \Rightarrow o] \Rightarrow i$ | separation |
| Replace | $[i, [i, i] \Rightarrow o] \Rightarrow i$ | replacement |
| PrimReplace | $[i, [i, i] \Rightarrow o] \Rightarrow i$ | primitive replacement |
| RepFun | $[i, i \Rightarrow i] \Rightarrow i$ | functional replacement |
| Pi Sigma | $[i, i \Rightarrow i] \Rightarrow i$ | general product/sum |
| domain | $i \Rightarrow i$ | domain of a relation |
| range | $i \Rightarrow i$ | range of a relation |
| field | $i \Rightarrow i$ | field of a relation |
| Lambda | $[i, i \Rightarrow i] \Rightarrow i$ | λ -abstraction |
| restrict | $[i, i] \Rightarrow i$ | restriction of a function |
| The | $[i \Rightarrow o] \Rightarrow i$ | definite description |
| if | $[o, i, i] \Rightarrow i$ | conditional |
| Ball Bex | $[i, i \Rightarrow o] \Rightarrow o$ | bounded quantifiers |

CONSTANTS

| <i>symbol</i> | <i>meta-type</i> | <i>priority</i> | <i>description</i> |
|---------------|------------------------|-----------------|-------------------------|
| ‘ ‘ | $[i, i] \Rightarrow i$ | Left 90 | image |
| – ‘ ‘ | $[i, i] \Rightarrow i$ | Left 90 | inverse image |
| ‘ | $[i, i] \Rightarrow i$ | Left 90 | application |
| Int | $[i, i] \Rightarrow i$ | Left 70 | intersection (\cap) |
| Un | $[i, i] \Rightarrow i$ | Left 65 | union (\cup) |
| – | $[i, i] \Rightarrow i$ | Left 65 | set difference ($-$) |
| : | $[i, i] \Rightarrow o$ | Left 50 | membership (\in) |
| <= | $[i, i] \Rightarrow o$ | Left 50 | subset (\subseteq) |

INFIXES

Figure 3.1: Constants of ZF

| <i>external</i> | <i>internal</i> | <i>description</i> |
|--|--|------------------------|
| $a \sim : b$ | $\sim(a : b)$ | negated membership |
| $\{a_1, \dots, a_n\}$ | $\text{cons}(a_1, \dots, \text{cons}(a_n, 0))$ | finite set |
| $\langle a_1, \dots, a_{n-1}, a_n \rangle$ | $\text{Pair}(a_1, \dots, \text{Pair}(a_{n-1}, a_n) \dots)$ | ordered n -tuple |
| $\{x : A. P[x]\}$ | $\text{Collect}(A, \lambda x. P[x])$ | separation |
| $\{y. x : A, Q[x, y]\}$ | $\text{Replace}(A, \lambda x y. Q[x, y])$ | replacement |
| $\{b[x]. x : A\}$ | $\text{RepFun}(A, \lambda x. b[x])$ | functional replacement |
| $\text{INT } x : A. B[x]$ | $\text{Inter}(\{B[x]. x : A\})$ | general intersection |
| $\text{UN } x : A. B[x]$ | $\text{Union}(\{B[x]. x : A\})$ | general union |
| $\text{PROD } x : A. B[x]$ | $\text{Pi}(A, \lambda x. B[x])$ | general product |
| $\text{SUM } x : A. B[x]$ | $\text{Sigma}(A, \lambda x. B[x])$ | general sum |
| $A \rightarrow B$ | $\text{Pi}(A, \lambda x. B)$ | function space |
| $A * B$ | $\text{Sigma}(A, \lambda x. B)$ | binary product |
| $\text{THE } x. P[x]$ | $\text{The}(\lambda x. P[x])$ | definite description |
| $\text{lam } x : A. b[x]$ | $\text{Lambda}(A, \lambda x. b[x])$ | λ -abstraction |
| $\text{ALL } x : A. P[x]$ | $\text{Ball}(A, \lambda x. P[x])$ | bounded \forall |
| $\text{EX } x : A. P[x]$ | $\text{Bex}(A, \lambda x. P[x])$ | bounded \exists |

Figure 3.2: Translations for ZF

ner using **cons** and \emptyset (the empty set):

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

The constant **Pair** constructs ordered pairs, as in $\text{Pair}(a, b)$. Ordered pairs may also be written within angle brackets, as $\langle a, b \rangle$. The n -tuple $\langle a_1, \dots, a_{n-1}, a_n \rangle$ abbreviates the nest of pairs

$$\text{Pair}(a_1, \dots, \text{Pair}(a_{n-1}, a_n) \dots).$$

In ZF, a function is a set of pairs. A ZF function f is simply an individual as far as Isabelle is concerned: its Isabelle type is i , not say $i \Rightarrow i$. The infix operator $'$ denotes the application of a function set to its argument; we must write $f'x$, not $f(x)$. The syntax for image is $f''A$ and that for inverse image is $f^{-1}''A$.

3.3 Binding operators

The constant **Collect** constructs sets by the principle of **separation**. The syntax for separation is $\{x : A. P[x]\}$, where $P[x]$ is a formula that may contain free occurrences of x . It abbreviates the set $\text{Collect}(A, \lambda x. P[x])$, which consists of all $x \in A$ that satisfy $P[x]$. Note that **Collect** is an unfortunate choice of name: some set theories adopt a set-formation principle, related to replacement, called collection.

The constant **Replace** constructs sets by the principle of **replacement**. The syntax $\{y. x : A, Q[x, y]\}$ denotes the set $\text{Replace}(A, \lambda x y. Q[x, y])$, which consists of all y such that there exists $x \in A$ satisfying $Q[x, y]$. The Replacement Axiom has the condition that Q must be single-valued over A :

| | | |
|----------------|---|--|
| <i>term</i> | = | expression of type <i>i</i> |
| | | <code>let id = term; ...; id = term in term</code> |
| | | <code>if term then term else term</code> |
| | | <code>{ term (,term)* }</code> |
| | | <code>< term (,term)* ></code> |
| | | <code>{ id:term . formula }</code> |
| | | <code>{ id . id:term, formula }</code> |
| | | <code>{ term . id:term }</code> |
| | | <code>term ‘‘ term</code> |
| | | <code>term -‘‘ term</code> |
| | | <code>term ‘ term</code> |
| | | <code>term * term</code> |
| | | <code>term Int term</code> |
| | | <code>term Un term</code> |
| | | <code>term - term</code> |
| | | <code>term -> term</code> |
| | | <code>THE id . formula</code> |
| | | <code>lam id:term . term</code> |
| | | <code>INT id:term . term</code> |
| | | <code>UN id:term . term</code> |
| | | <code>PROD id:term . term</code> |
| | | <code>SUM id:term . term</code> |
| <i>formula</i> | = | expression of type <i>o</i> |
| | | <code>term : term</code> |
| | | <code>term ~: term</code> |
| | | <code>term <= term</code> |
| | | <code>term = term</code> |
| | | <code>term ~= term</code> |
| | | <code>~ formula</code> |
| | | <code>formula & formula</code> |
| | | <code>formula formula</code> |
| | | <code>formula --> formula</code> |
| | | <code>formula <-> formula</code> |
| | | <code>ALL id:term . formula</code> |
| | | <code>EX id:term . formula</code> |
| | | <code>ALL id id* . formula</code> |
| | | <code>EX id id* . formula</code> |
| | | <code>EX! id id* . formula</code> |

Figure 3.3: Full grammar for ZF

for all $x \in A$ there exists at most one y satisfying $Q[x, y]$. A single-valued binary predicate is also called a **class function**.

The constant **RepFun** expresses a special case of replacement, where $Q[x, y]$ has the form $y = b[x]$. Such a Q is trivially single-valued, since it is just the graph of the meta-level function $\lambda x . b[x]$. The resulting set consists of all $b[x]$ for $x \in A$. This is analogous to the ML functional **map**, since it applies a function to every element of a set. The syntax is $\{b[x] . x : A\}$, which expands to **RepFun**($A, \lambda x . b[x]$).

General unions and intersections of indexed families of sets, namely $\bigcup_{x \in A} B[x]$ and $\bigcap_{x \in A} B[x]$, are written **UN** $x : A . B[x]$ and **INT** $x : A . B[x]$. Their meaning is expressed using **RepFun** as

$$\bigcup(\{B[x] . x \in A\}) \quad \text{and} \quad \bigcap(\{B[x] . x \in A\}).$$

General sums $\sum_{x \in A} B[x]$ and products $\prod_{x \in A} B[x]$ can be constructed in set theory, where $B[x]$ is a family of sets over A . They have as special cases $A \times B$ and $A \rightarrow B$, where B is simply a set. This is similar to the situation in Constructive Type Theory (set theory has ‘dependent sets’) and calls for similar syntactic conventions. The constants **Sigma** and **Pi** construct general sums and products. Instead of **Sigma**(A, B) and **Pi**(A, B) we may write **SUM** $x : A . B[x]$ and **PROD** $x : A . B[x]$. The special cases as $A * B$ and $A \rightarrow B$ abbreviate general sums and products over a constant family.¹ Isabelle accepts these abbreviations in parsing and uses them whenever possible for printing.

As mentioned above, whenever the axioms assert the existence and uniqueness of a set, Isabelle’s set theory declares a constant for that set. These constants can express the **definite description** operator $\iota x . P[x]$, which stands for the unique a satisfying $P[a]$, if such exists. Since all terms in ZF denote something, a description is always meaningful, but we do not know its value unless $P[x]$ defines it uniquely. Using the constant **The**, we may write descriptions as **The**($\lambda x . P[x]$) or use the syntax **THE** $x . P[x]$.

Function sets may be written in λ -notation; $\lambda x \in A . b[x]$ stands for the set of all pairs $\langle x, b[x] \rangle$ for $x \in A$. In order for this to be a set, the function’s domain A must be given. Using the constant **Lambda**, we may express function sets as **Lambda**($A, \lambda x . b[x]$) or use the syntax **lam** $x : A . b[x]$.

Isabelle’s 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** $x : A . P[x]$.

¹Unlike normal infix operators, $*$ and \rightarrow merely define abbreviations; there are no constants **op** $*$ and **op** \rightarrow .

| | |
|-------------|--|
| Let_def | $\text{Let}(s, f) == f(s)$ |
| Ball_def | $\text{Ball}(A, P) == \text{ALL } x. x:A \rightarrow P(x)$ |
| Bex_def | $\text{Bex}(A, P) == \text{EX } x. x:A \ \& \ P(x)$ |
| subset_def | $A \leq B == \text{ALL } x:A. x:B$ |
| extension | $A = B \leftrightarrow A \leq B \ \& \ B \leq A$ |
| Union_iff | $A : \text{Union}(C) \leftrightarrow (\text{EX } B:C. A:B)$ |
| Pow_iff | $A : \text{Pow}(B) \leftrightarrow A \leq B$ |
| foundation | $A=0 \mid (\text{EX } x:A. \text{ALL } y:x. \sim y:A)$ |
| replacement | $(\text{ALL } x:A. \text{ALL } y \ z. P(x,y) \ \& \ P(x,z) \rightarrow y=z) \implies$ $b : \text{PrimReplace}(A, P) \leftrightarrow (\text{EX } x:A. P(x,b))$ |

THE ZERMELO-FRAENKEL AXIOMS

| | |
|-------------|---|
| Replace_def | $\text{Replace}(A, P) ==$ $\text{PrimReplace}(A, \lambda x y. (\text{EX } !z. P(x,z)) \ \& \ P(x,y))$ |
| RepFun_def | $\text{RepFun}(A, f) == \{y \ . \ x:A, y=f(x)\}$ |
| the_def | $\text{The}(P) == \text{Union}(\{y \ . \ x:\{0\}, P(y)\})$ |
| if_def | $\text{if}(P, a, b) == \text{THE } z. P \ \& \ z=a \mid \sim P \ \& \ z=b$ |
| Collect_def | $\text{Collect}(A, P) == \{y \ . \ x:A, x=y \ \& \ P(x)\}$ |
| Upair_def | $\text{Upair}(a, b) ==$ $\{y. x:\text{Pow}(\text{Pow}(0)), (x=0 \ \& \ y=a) \mid (x=\text{Pow}(0) \ \& \ y=b)\}$ |

CONSEQUENCES OF REPLACEMENT

| | |
|-----------|---|
| Inter_def | $\text{Inter}(A) == \{x:\text{Union}(A) \ . \ \text{ALL } y:A. x:y\}$ |
| Un_def | $A \text{ Un } B == \text{Union}(\text{Upair}(A, B))$ |
| Int_def | $A \text{ Int } B == \text{Inter}(\text{Upair}(A, B))$ |
| Diff_def | $A - B == \{x:A \ . \ x \sim B\}$ |

UNION, INTERSECTION, DIFFERENCE

Figure 3.4: Rules and axioms of ZF

```

cons_def      cons(a,A) == Upair(a,a) Un A
succ_def      succ(i) == cons(i,i)
infinity      0:Inf & (ALL y:Inf. succ(y): Inf)

```

FINITE AND INFINITE SETS

```

Pair_def      <a,b>      == {{a,a}, {a,b}}
split_def     split(c,p) == THE y. EX a b. p=<a,b> & y=c(a,b)
fst_def       fst(A)     == split(%x y. x, p)
snd_def       snd(A)     == split(%x y. y, p)
Sigma_def     Sigma(A,B) == UN x:A. UN y:B(x). {<x,y>}

```

ORDERED PAIRS AND CARTESIAN PRODUCTS

```

converse_def  converse(r) == {z. w:r, EX x y. w=<x,y> & z=<y,x>}
domain_def    domain(r)  == {x. w:r, EX y. w=<x,y>}
range_def     range(r)   == domain(converse(r))
field_def     field(r)   == domain(r) Un range(r)
image_def     r `` A     == {y : range(r) . EX x:A. <x,y> : r}
vimage_def    r -`` A    == converse(r)``A

```

OPERATIONS ON RELATIONS

```

lam_def       Lambda(A,b) == {<x,b(x)> . x:A}
apply_def     f`a         == THE y. <a,y> : f
Pi_def        Pi(A,B)     == {f: Pow(Sigma(A,B)). ALL x:A. EX! y. <x,y>: f}
restrict_def   restrict(f,A) == lam x:A. f`x

```

FUNCTIONS AND GENERAL PRODUCT

Figure 3.5: Further definitions of ZF

3.4 The Zermelo-Fraenkel axioms

The axioms appear in Fig. 3.4. They resemble those presented by Suppes [20]. Most of the theory consists of definitions. In particular, bounded quantifiers and the subset relation appear in other axioms. Object-level quantifiers and implications have been replaced by meta-level ones wherever possible, to simplify use of the axioms. See the file `ZF/ZF.thy` for details.

The traditional replacement axiom asserts

$$y \in \text{PrimReplace}(A, P) \leftrightarrow (\exists x \in A. P(x, y))$$

subject to the condition that $P(x, y)$ is single-valued for all $x \in A$. The Isabelle theory defines `Replace` to apply `PrimReplace` to the single-valued part of P , namely

$$(\exists! z. P(x, z)) \wedge P(x, y).$$

Thus $y \in \text{Replace}(A, P)$ if and only if there is some x such that $P(x, -)$ holds uniquely for y . Because the equivalence is unconditional, `Replace` is much easier to use than `PrimReplace`; it defines the same set, if $P(x, y)$ is single-valued. The nice syntax for replacement expands to `Replace`.

Other consequences of replacement include functional replacement (`RepFun`) and definite descriptions (`The`). Axioms for separation (`Collect`) and unordered pairs (`Upair`) are traditionally assumed, but they actually follow from replacement [20, pages 237–8].

The definitions of general intersection, etc., are straightforward. Note the definition of `cons`, which underlies the finite set notation. The axiom of infinity gives us a set that contains 0 and is closed under successor (`succ`). Although this set is not uniquely defined, the theory names it (`Inf`) in order to simplify the construction of the natural numbers.

Further definitions appear in Fig. 3.5. Ordered pairs are defined in the standard way, $\langle a, b \rangle \equiv \{\{a\}, \{a, b\}\}$. Recall that `Sigma`(A, B) generalizes the Cartesian product of two sets. It is defined to be the union of all singleton sets $\{\langle x, y \rangle\}$, for $x \in A$ and $y \in B(x)$. This is a typical usage of general union.

The projections `fst` and `snd` are defined in terms of the generalized projection `split`. The latter has been borrowed from Martin-Löf's Type Theory, and is often easier to use than `fst` and `snd`.

Operations on relations include converse, domain, range, and image. The set `Pi`(A, B) generalizes the space of functions between two sets. Note the simple definitions of λ -abstraction (using `RepFun`) and application (using a definite description). The function `restrict`(f, A) has the same values as f , but only over the domain A .

```

ballI      [| !!x. x:A ==> P(x) |] ==> ALL x:A. P(x)
bspec      [| ALL x:A. P(x);  x: A |] ==> P(x)
ballE      [| ALL x:A. P(x);  P(x) ==> Q;  ~ x:A ==> Q |] ==> Q

ball_cong  [| A=A';  !!x. x:A' ==> P(x) <-> P'(x) |] ==>
(ALL x:A. P(x)) <-> (ALL x:A'. P'(x))

bexI       [| P(x);  x: A |] ==> EX x:A. P(x)
bexCI      [| ALL x:A. ~P(x) ==> P(a);  a: A |] ==> EX x:A. P(x)
bexE       [| EX x:A. P(x);  !!x. [| x:A; P(x) |] ==> Q |] ==> Q

bex_cong   [| A=A';  !!x. x:A' ==> P(x) <-> P'(x) |] ==>
(EX x:A. P(x)) <-> (EX x:A'. P'(x))

```

BOUNDED QUANTIFIERS

```

subsetI     (!!x. x:A ==> x:B) ==> A <= B
subsetD     [| A <= B;  c:A |] ==> c:B
subsetCE    [| A <= B;  ~(c:A) ==> P;  c:B ==> P |] ==> P
subset_refl A <= A
subset_trans [| A<=B;  B<=C |] ==> A<=C

equalityI   [| A <= B;  B <= A |] ==> A = B
equalityD1  A = B ==> A<=B
equalityD2  A = B ==> B<=A
equalityE   [| A = B;  [| A<=B; B<=A |] ==> P |] ==> P

```

SUBSETS AND EXTENSIONALITY

```

emptyE      a:0 ==> P
empty_subsetI 0 <= A
equalsOI    [| !!y. y:A ==> False |] ==> A=0
equalsOD    [| A=0;  a:A |] ==> P

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

```

THE EMPTY SET; POWER SETS

Figure 3.6: Basic derived rules for ZF

3.5 From basic lemmas to function spaces

Faced with so many definitions, it is essential to prove lemmas. Even trivial theorems like $A \cap B = B \cap A$ would be difficult to prove from the definitions alone. Isabelle’s set theory derives many rules using a natural deduction style. Ideally, a natural deduction rule should introduce or eliminate just one operator, but this is not always practical. For most operators, we may forget its definition and use its derived rules instead.

3.5.1 Fundamental lemmas

Figure 3.6 presents the derived rules for the most basic operators. The rules for the bounded quantifiers resemble those for the ordinary quantifiers, but note that **ballE** uses a negated assumption in the style of Isabelle’s classical reasoner. The congruence rules **ball_cong** and **bex_cong** are required by Isabelle’s simplifier, but have few other uses. Congruence rules must be specially derived for all binding operators, and henceforth will not be shown.

Figure 3.6 also shows rules for the subset and equality relations (proof by extensionality), and rules about the empty set and the power set operator.

Figure 3.7 presents rules for replacement and separation. The rules for **Replace** and **RepFun** are much simpler than comparable rules for **PrimReplace** would be. The principle of separation is proved explicitly, although most proofs should use the natural deduction rules for **Collect**. The elimination rule **CollectE** is equivalent to the two destruction rules **CollectD1** and **CollectD2**, but each rule is suited to particular circumstances. Although too many rules can be confusing, there is no reason to aim for a minimal set of rules. See the file **ZF/ZF.ML** for a complete listing.

Figure 3.8 presents rules for general union and intersection. The empty intersection should be undefined. We cannot have $\bigcap(\emptyset) = V$ because V , the universal class, is not a set. All expressions denote something in ZF set theory; the definition of intersection implies $\bigcap(\emptyset) = \emptyset$, but this value is arbitrary. The rule **InterI** must have a premise to exclude the empty intersection. Some of the laws governing intersections require similar premises.

3.5.2 Unordered pairs and finite sets

Figure 3.9 presents the principle of unordered pairing, along with its derived rules. Binary union and intersection are defined in terms of ordered pairs (Fig. 3.10). Set difference is also included. The rule **UnCI** is useful for classical reasoning about unions, like **disjCI**; it supersedes **UnI1** and **UnI2**, but these rules are often easier to work with. For intersection and difference we have both elimination and destruction rules. Again, there is no reason to provide a minimal rule set.

Figure 3.11 is concerned with finite sets: it presents rules for **cons**, the

```

ReplaceI      [| x: A; P(x,b); !!y. P(x,y) ==> y=b |] ==>
              b : {y. x:A, P(x,y)}

ReplaceE      [| b : {y. x:A, P(x,y)};
              !!x. [| x: A; P(x,b); ALL y. P(x,y)-->y=b |] ==> R
              |] ==> R

RepFunI       [| a : A |] ==> f(a) : {f(x). x:A}
RepFunE       [| b : {f(x). x:A};
              !!x.[| x:A; b=f(x) |] ==> P |] ==> P

separation    a : {x:A. P(x)} <-> a:A & P(a)
CollectI      [| a:A; P(a) |] ==> a : {x:A. P(x)}
CollectE      [| a : {x:A. P(x)}; [| a:A; P(a) |] ==> R |] ==> R
CollectD1     a : {x:A. P(x)} ==> a:A
CollectD2     a : {x:A. P(x)} ==> P(a)

```

Figure 3.7: Replacement and separation

```

UnionI        [| B: C; A: B |] ==> A: Union(C)
UnionE        [| A : Union(C); !!B.[| A: B; B: C |] ==> R |] ==> R

InterI        [| !!x. x: C ==> A: x; c:C |] ==> A : Inter(C)
InterD        [| A : Inter(C); B : C |] ==> A : B
InterE        [| A : Inter(C); A:B ==> R; ~ B:C ==> R |] ==> R

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); a: A |] ==> b: (INT x:A. B(x))
INT_E         [| b : (INT x:A. B(x)); a: A |] ==> b : B(a)

```

Figure 3.8: General union and intersection

```

pairing       a:Upair(b,c) <-> (a=b | a=c)
UpairI1       a : Upair(a,b)
UpairI2       b : Upair(a,b)
UpairE        [| a : Upair(b,c); a = b ==> P; a = c ==> P |] ==> P

```

Figure 3.9: Unordered pairs

```

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

DiffI     [| c : A; ~ c : B |] ==> c : A - B
DiffD1    c : A - B ==> c : A
DiffD2    c : A - B ==> c ~: B
DiffE     [| c : A - B; [| c:A; ~ c:B |] ==> P |] ==> P

```

Figure 3.10: Union, intersection, difference

```

consI1     a : cons(a,B)
consI2     a : B ==> a : cons(b,B)
consCI     (~ a:B ==> a=b) ==> a: cons(b,B)
consE      [| a : cons(b,A); a=b ==> P; a:A ==> P |] ==> P

singletonI a : {a}
singletonE [| a : {b}; a=b ==> P |] ==> P

```

Figure 3.11: Finite and singleton sets

```

succI1     i : succ(i)
succI2     i : j ==> i : succ(j)
succCI     (~ i:j ==> i=j) ==> i: succ(j)
succE      [| i : succ(j); i=j ==> P; i:j ==> P |] ==> P
succ_neq_0 [| succ(n)=0 |] ==> P
succ_inject succ(m) = succ(n) ==> m=n

```

Figure 3.12: The successor function

```

the_equality [| P(a); !!x. P(x) ==> x=a |] ==> (THE x. P(x)) = a
theI         EX! x. P(x) ==> P(THE x. P(x))

if_P        P ==> (if P then a else b) = a
if_not_P    ~P ==> (if P then a else b) = b

mem_asym    [| a:b; b:a |] ==> P
mem_irrefl   a:a ==> P

```

Figure 3.13: Descriptions; non-circularity

| | |
|----------------|--|
| Union_upper | $B:A \implies B \leq \text{Union}(A)$ |
| Union_least | $[\text{!!}x. x:A \implies x \leq C \] \implies \text{Union}(A) \leq C$ |
| Inter_lower | $B:A \implies \text{Inter}(A) \leq B$ |
| Inter_greatest | $[a:A; \text{!!}x. x:A \implies C \leq x \] \implies C \leq \text{Inter}(A)$ |
| Un_upper1 | $A \leq A \text{ Un } B$ |
| Un_upper2 | $B \leq A \text{ Un } B$ |
| Un_least | $[A \leq C; B \leq C \] \implies A \text{ Un } B \leq C$ |
| Int_lower1 | $A \text{ Int } B \leq A$ |
| Int_lower2 | $A \text{ Int } B \leq B$ |
| Int_greatest | $[C \leq A; C \leq B \] \implies C \leq A \text{ Int } B$ |
| Diff_subset | $A-B \leq A$ |
| Diff_contains | $[C \leq A; C \text{ Int } B = 0 \] \implies C \leq A-B$ |
| Collect_subset | $\text{Collect}(A,P) \leq A$ |

Figure 3.14: Subset and lattice properties

finite set constructor, and rules for singleton sets. Figure 3.12 presents derived rules for the successor function, which is defined in terms of `cons`. The proof that `succ` is injective appears to require the Axiom of Foundation.

Definite descriptions (`THE`) are defined in terms of the singleton set $\{0\}$, but their derived rules fortunately hide this (Fig. 3.13). The rule `theI` is difficult to apply because of the two occurrences of $?P$. However, `the_equality` does not have this problem and the files contain many examples of its use.

Finally, the impossibility of having both $a \in b$ and $b \in a$ (`mem_asym`) is proved by applying the Axiom of Foundation to the set $\{a, b\}$. The impossibility of $a \in a$ is a trivial consequence.

See the file `ZF/upair.ML` for full proofs of the rules discussed in this section.

3.5.3 Subset and lattice properties

The subset relation is a complete lattice. Unions form least upper bounds; non-empty intersections form greatest lower bounds. Figure 3.14 shows the corresponding rules. A few other laws involving subsets are included. Proofs are in the file `ZF/subset.ML`.

Reasoning directly about subsets often yields clearer proofs than reasoning about the membership relation. Section 3.13 below presents an example of this, proving the equation $\text{Pow}(A) \cap \text{Pow}(B) = \text{Pow}(A \cap B)$.

| | |
|--------------|---|
| Pair_inject1 | $\langle a, b \rangle = \langle c, d \rangle \implies a=c$ |
| Pair_inject2 | $\langle a, b \rangle = \langle c, d \rangle \implies b=d$ |
| Pair_inject | $[\langle a, b \rangle = \langle c, d \rangle; [a=c; b=d] \implies P] \implies P$ |
| Pair_neq_0 | $\langle a, b \rangle = 0 \implies P$ |
| fst_conv | $\text{fst}(\langle a, b \rangle) = a$ |
| snd_conv | $\text{snd}(\langle a, b \rangle) = b$ |
| split | $\text{split}(\%x\ y.\ c(x,y), \langle a, b \rangle) = c(a,b)$ |
| SigmaI | $[a:A; b:B(a)] \implies \langle a, b \rangle : \text{Sigma}(A,B)$ |
| SigmaE | $[c : \text{Sigma}(A,B);$ $!!x\ y.[x:A; y:B(x); c=\langle x,y \rangle] \implies P] \implies P$ |
| SigmaE2 | $[\langle a, b \rangle : \text{Sigma}(A,B);$ $[a:A; b:B(a)] \implies P \quad] \implies P$ |

Figure 3.15: Ordered pairs; projections; general sums

3.5.4 Ordered pairs

Figure 3.15 presents the rules governing ordered pairs, projections and general sums. File `ZF/pair.ML` contains the full (and tedious) proof that $\{\{a\}, \{a, b\}\}$ functions as an ordered pair. This property is expressed as two destruction rules, `Pair_inject1` and `Pair_inject2`, and equivalently as the elimination rule `Pair_inject`.

The rule `Pair_neq_0` asserts $\langle a, b \rangle \neq \emptyset$. This is a property of $\{\{a\}, \{a, b\}\}$, and need not hold for other encodings of ordered pairs. The non-standard ordered pairs mentioned below satisfy $\langle \emptyset; \emptyset \rangle = \emptyset$.

The natural deduction rules `SigmaI` and `SigmaE` assert that $\text{Sigma}(A, B)$ consists of all pairs of the form $\langle x, y \rangle$, for $x \in A$ and $y \in B(x)$. The rule `SigmaE2` merely states that $\langle a, b \rangle \in \text{Sigma}(A, B)$ implies $a \in A$ and $b \in B(a)$.

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

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

Nested patterns are translated recursively: $\% \langle x, y, z \rangle. \ t \rightsquigarrow \% \langle x, \langle y, z \rangle \rangle. \ t \rightsquigarrow \text{split}(\%x. \% \langle y, z \rangle. \ t) \rightsquigarrow \text{split}(\%x. \text{split}(\%y\ z. \ t))$. The reverse translation is performed upon printing.

! The translation between patterns and `split` is performed automatically by the parser and printer. Thus the internal and external form of a term may differ, which affects proofs. For example the term $(\% \langle x, y \rangle. \langle y, x \rangle) \langle a, b \rangle$ requires the theorem `split` to rewrite to $\langle b, a \rangle$.

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

```

domainI      <a,b>: r ==> a : domain(r)
domainE      [| a : domain(r);  !!y. <a,y>: r ==> P |] ==> P
domain_subset domain(Sigma(A,B)) <= A

rangeI       <a,b>: r ==> b : range(r)
rangeE       [| b : range(r);  !!x. <x,b>: r ==> P |] ==> P
range_subset range(A*B) <= B

fieldI1      <a,b>: r ==> a : field(r)
fieldI2      <a,b>: r ==> b : field(r)
fieldCI      (~ <c,a>:r ==> <a,b>: r) ==> a : field(r)

fieldE       [| a : field(r);
               !!x. <a,x>: r ==> P;
               !!x. <x,a>: r ==> P
               |] ==> P

field_subset field(A*A) <= A

```

Figure 3.16: Domain, range and field of a relation

```

imageI       [| <a,b>: r;  a:A |] ==> b : r-‘A
imageE       [| b: r-‘A;  !!x.[| <x,b>: r;  x:A |] ==> P |] ==> P

vimageI      [| <a,b>: r;  b:B |] ==> a : r-‘‘B
vimageE      [| a: r-‘‘B;  !!x.[| <a,x>: r;  x:B |] ==> P |] ==> P

```

Figure 3.17: Image and inverse image

Let: $\text{let } pattern = t \text{ in } u$

Choice: $\text{THE } pattern . P$

Set operations: $\text{UN } pattern:A . B$

Comprehension: $\{ pattern:A . P \}$

3.5.5 Relations

Figure 3.16 presents rules involving relations, which are sets of ordered pairs. The converse of a relation r is the set of all pairs $\langle y, x \rangle$ such that $\langle x, y \rangle \in r$; if r is a function, then $\text{converse}(r)$ is its inverse. The rules for the domain operation, namely domainI and domainE , assert that $\text{domain}(r)$ consists of all x such that r contains some pair of the form $\langle x, y \rangle$. The range operation is similar, and the field of a relation is merely the union of its domain and range.


```

fun_is_rel      f: Pi(A,B) ==> f <= Sigma(A,B)

apply_equality  [| <a,b>: f;  f: Pi(A,B) |] ==> f'a = b
apply_equality2 [| <a,b>: f;  <a,c>: f;  f: Pi(A,B) |] ==> b=c

apply_type      [| f: Pi(A,B);  a:A |] ==> f'a : B(a)
apply_Pair      [| f: Pi(A,B);  a:A |] ==> <a,f'a>: f
apply_iff       f: Pi(A,B) ==> <a,b>: f <-> a:A & f'a = b

fun_extension    [| f : Pi(A,B);  g: Pi(A,D);
                    !!x. x:A ==> f'x = g'x      |] ==> f=g

domain_type      [| <a,b> : f;  f: Pi(A,B) |] ==> a : A
range_type       [| <a,b> : f;  f: Pi(A,B) |] ==> b : B(a)

Pi_type          [| f: A->C;  !!x. x:A ==> f'x: B(x) |] ==> f: Pi(A,B)
domain_of_fun     f: Pi(A,B) ==> domain(f)=A
range_of_fun      f: Pi(A,B) ==> f: A->range(f)

restrict         a : A ==> restrict(f,A) ' a = f'a
restrict_type     [| !!x. x:A ==> f'x: B(x) |] ==>
                  restrict(f,A) : Pi(A,B)

```

Figure 3.18: Functions

```

lamI            a:A ==> <a,b(a)> : (lam x:A. b(x))
lamE            [| p: (lam x:A. b(x));  !!x.[| x:A; p=<x,b(x)> |] ==> P
                  |] ==> P

lam_type        [| !!x. x:A ==> b(x): B(x) |] ==> (lam x:A. b(x)) : Pi(A,B)

beta            a : A ==> (lam x:A. b(x)) ' a = b(a)
eta             f : Pi(A,B) ==> (lam x:A. f'x) = f

```

Figure 3.19: λ -abstraction

Figure 3.17 presents rules for images and inverse images. Note that these operations are generalisations of range and domain, respectively. See the file ZF/domrange.ML for derivations of the rules.

3.5.6 Functions

Functions, represented by graphs, are notoriously difficult to reason about. The file ZF/func.ML derives many rules, which overlap more than they ought. This section presents the more important rules.

Figure 3.18 presents the basic properties of $\text{Pi}(A, B)$, the generalized function space. For example, if f is a function and $\langle a, b \rangle \in f$, then $f'a = b$ (apply_equality). Two functions are equal provided they have equal

```

fun_empty      0: 0->0
fun_single     {<a,b>} : {a} -> {b}

fun_disjoint_Un [| f: A->B; g: C->D; A Int C = 0 |] ==>
                (f Un g) : (A Un C) -> (B Un D)

fun_disjoint_apply1 [| a:A; f: A->B; g: C->D; A Int C = 0 |] ==>
                  (f Un g)'a = f'a

fun_disjoint_apply2 [| c:C; f: A->B; g: C->D; A Int C = 0 |] ==>
                  (f Un g)'c = g'c

```

Figure 3.20: Constructing functions from smaller sets

domains and deliver equals results (**fun_extension**).

By **Pi_type**, a function typing of the form $f \in A \rightarrow C$ can be refined to the dependent typing $f \in \prod_{x \in A} B(x)$, given a suitable family of sets $\{B(x)\}_{x \in A}$. Conversely, by **range_of_fun**, any dependent typing can be flattened to yield a function type of the form $A \rightarrow C$; here, $C = \text{range}(f)$.

Among the laws for λ -abstraction, **lamI** and **lamE** describe the graph of the generated function, while **beta** and **eta** are the standard conversions. We essentially have a dependently-typed λ -calculus (Fig. 3.19).

Figure 3.20 presents some rules that can be used to construct functions explicitly. We start with functions consisting of at most one pair, and may form the union of two functions provided their domains are disjoint.

3.6 Further developments

The next group of developments is complex and extensive, and only highlights can be covered here. It involves many theories and ML files of proofs.

Figure 3.21 presents commutative, associative, distributive, and idempotency laws of union and intersection, along with other equations. See file **ZF/equalities.ML**.

Theory **Bool** defines $\{0, 1\}$ as a set of booleans, with the usual operators including a conditional (Fig. 3.22). Although ZF is a first-order theory, you can obtain the effect of higher-order logic using **bool**-valued functions, for example. The constant 1 is translated to **succ(0)**.

3.6.1 Disjoint unions

Theory **Sum** defines the disjoint union of two sets, with injections and a case analysis operator (Fig. 3.23). Disjoint unions play a role in datatype definitions, particularly when there is mutual recursion [16].

| | |
|-------------------|---|
| Int_absorb | $A \cap A = A$ |
| Int_commute | $A \cap B = B \cap A$ |
| Int_assoc | $(A \cap B) \cap C = A \cap (B \cap C)$ |
| Int_Un_distrib | $(A \cap B) \cap C = (A \cap C) \cap (B \cap C)$ |
| Un_absorb | $A \cup A = A$ |
| Un_commute | $A \cup B = B \cup A$ |
| Un_assoc | $(A \cup B) \cup C = A \cup (B \cup C)$ |
| Un_Int_distrib | $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ |
| Diff_cancel | $A - A = \emptyset$ |
| Diff_disjoint | $A \cap (B - A) = \emptyset$ |
| Diff_partition | $A \subseteq B \implies A \cup (B - A) = B$ |
| double_complement | $[A \subseteq B; B \subseteq C] \implies (B - (C - A)) = A$ |
| Diff_Un | $A - (B \cup C) = (A - B) \cap (A - C)$ |
| Diff_Int | $A - (B \cap C) = (A - B) \cup (A - C)$ |
| Union_Un_distrib | $\text{Union}(A \cup B) = \text{Union}(A) \cup \text{Union}(B)$ |
| Inter_Un_distrib | $[a:A; b:B] \implies \text{Inter}(A \cup B) = \text{Inter}(A) \cap \text{Inter}(B)$ |
| Int_Union_RepFun | $A \cap \text{Union}(B) = (\bigcup C:B. A \cap C)$ |
| Un_Inter_RepFun | $b:B \implies A \cup \text{Inter}(B) = (\bigcap C:B. A \cup C)$ |
| SUM_Un_distrib1 | $(\sum x:A \cup B. C(x)) = (\sum x:A. C(x)) \cup (\sum x:B. C(x))$ |
| SUM_Un_distrib2 | $(\sum x:C. A(x) \cup B(x)) = (\sum x:C. A(x)) \cup (\sum x:C. B(x))$ |
| SUM_Int_distrib1 | $(\sum x:A \cap B. C(x)) = (\sum x:A. C(x)) \cap (\sum x:B. C(x))$ |
| SUM_Int_distrib2 | $(\sum x:C. A(x) \cap B(x)) = (\sum x:C. A(x)) \cap (\sum x:C. B(x))$ |

Figure 3.21: Equalities

```

bool_def      bool == {0,1}
cond_def      cond(b,c,d) == if b=1 then c else d
not_def       not(b) == cond(b,0,1)
and_def       a and b == cond(a,b,0)
or_def        a or b == cond(a,1,b)
xor_def       a xor b == cond(a,not(b),b)

bool_1I       1 : bool
bool_0I       0 : bool
boolE         [! c: bool; c=1 ==> P; c=0 ==> P !] ==> P
cond_1        cond(1,c,d) = c
cond_0        cond(0,c,d) = d

```

Figure 3.22: The booleans

| <i>symbol</i> | <i>meta-type</i> | <i>priority</i> | <i>description</i> |
|---------------|---|-----------------|-------------------------|
| $+$ | $[i, i] \Rightarrow i$ | Right 65 | disjoint union operator |
| Inl Inr | $i \Rightarrow i$ | | injections |
| case | $[i \Rightarrow i, i \Rightarrow i, i] \Rightarrow i$ | | conditional for $A + B$ |

```

sum_def      A+B == {0}*A Un {1}*B
Inl_def      Inl(a) == <0,a>
Inr_def      Inr(b) == <1,b>
case_def     case(c,d,u) == split(%y z. cond(y, d(z), c(z)), u)

sum_InlI     a : A ==> Inl(a) : A+B
sum_InrI     b : B ==> Inr(b) : A+B

Inl_inject   Inl(a)=Inl(b) ==> a=b
Inr_inject   Inr(a)=Inr(b) ==> a=b
Inl_neq_Inr  Inl(a)=Inr(b) ==> P

sumE2       u : A+B ==> (EX x. x:A & u=Inl(x)) | (EX y. y:B & u=Inr(y))

case_Inl     case(c,d,Inl(a)) = c(a)
case_Inr     case(c,d,Inr(b)) = d(b)

```

Figure 3.23: Disjoint unions

```

QPair_def    <a;b> == a+b
qsplit_def   qsplit(c,p) == THE y. EX a b. p=<a;b> & y=c(a,b)
qfsplit_def  qfsplit(R,z) == EX x y. z=<x;y> & R(x,y)
qconverse_def qconverse(r) == {z. w:r, EX x y. w=<x;y> & z=<y;x>}
QSigma_def   QSigma(A,B) == UN x:A. UN y:B(x). {<x;y>}

qsum_def     A <+> B == ({0} <*> A) Un ({1} <*> B)
QInl_def     QInl(a) == <0;a>
QInr_def     QInr(b) == <1;b>
qcase_def    qcase(c,d) == qsplit(%y z. cond(y, d(z), c(z)))

```

Figure 3.24: Non-standard pairs, products and sums

3.6.2 Non-standard ordered pairs

Theory `QPair` defines a notion of ordered pair that admits non-well-founded tupling (Fig. 3.24). Such pairs are written $\langle a; b \rangle$. It also defines the eliminator `qsplitt`, the converse operator `qconverse`, and the summation operator `QSigma`. These are completely analogous to the corresponding versions for standard ordered pairs. The theory goes on to define a non-standard notion of disjoint sum using non-standard pairs. All of these concepts satisfy the same properties as their standard counterparts; in addition, $\langle a; b \rangle$ is continuous. The theory supports coinductive definitions, for example of infinite lists [18].

3.6.3 Least and greatest fixedpoints

The Knaster-Tarski Theorem states that every monotone function over a complete lattice has a fixedpoint. Theory `Fixedpt` proves the Theorem only for a particular lattice, namely the lattice of subsets of a set (Fig. 3.25). The theory defines least and greatest fixedpoint operators with corresponding induction and coinduction rules. These are essential to many definitions that follow, including the natural numbers and the transitive closure operator. The (co)inductive definition package also uses the fixedpoint operators [15]. See Davey and Priestley [5] for more on the Knaster-Tarski Theorem and my paper [16] for discussion of the Isabelle proofs.

Monotonicity properties are proved for most of the set-forming operations: union, intersection, Cartesian product, image, domain, range, etc. These are useful for applying the Knaster-Tarski Fixedpoint Theorem. The proofs themselves are trivial applications of Isabelle’s classical reasoner. See file `ZF/mono.ML`.

3.6.4 Finite sets and lists

Theory `Finite` (Figure 3.26) defines the finite set operator; $\text{Fin}(A)$ is the set of all finite sets over A . The theory employs Isabelle’s inductive definition package, which proves various rules automatically. The induction rule shown is stronger than the one proved by the package. The theory also defines the set of all finite functions between two given sets.

Figure 3.27 presents the set of lists over A , $\text{list}(A)$. The definition employs Isabelle’s datatype package, which defines the introduction and induction rules automatically, as well as the constructors, case operator (`list_case`) and recursion operator. The theory then defines the usual list functions by primitive recursion. See theory `List`.

```

bnd_mono_def  bnd_mono(D,h) ==
               h(D) <= D & (ALL W X. W <= X --> X <= D --> h(W) <= h(X))

lfp_def       lfp(D,h) == Inter({X: Pow(D). h(X) <= X})
gfp_def       gfp(D,h) == Union({X: Pow(D). X <= h(X)})

lfp_lowerbound [| h(A) <= A; A <= D |] ==> lfp(D,h) <= A

lfp_subset    lfp(D,h) <= D

lfp_greatest [| bnd_mono(D,h);
                 !!X. [| h(X) <= X; X <= D |] ==> A <= X
                 |] ==> A <= lfp(D,h)

lfp_Tarski    bnd_mono(D,h) ==> lfp(D,h) = h(lfp(D,h))

induct        [| a : lfp(D,h); bnd_mono(D,h);
                 !!x. x : h(Collect(lfp(D,h),P)) ==> P(x)
                 |] ==> P(a)

lfp_mono      [| bnd_mono(D,h); bnd_mono(E,i);
                 !!X. X <= D ==> h(X) <= i(X)
                 |] ==> lfp(D,h) <= lfp(E,i)

gfp_upperbound [| A <= h(A); A <= D |] ==> A <= gfp(D,h)

gfp_subset    gfp(D,h) <= D

gfp_least     [| bnd_mono(D,h);
                 !!X. [| X <= h(X); X <= D |] ==> X <= A
                 |] ==> gfp(D,h) <= A

gfp_Tarski    bnd_mono(D,h) ==> gfp(D,h) = h(gfp(D,h))

coinduct      [| bnd_mono(D,h); a: X; X <= h(X Un gfp(D,h)); X <= D
                 |] ==> a : gfp(D,h)

gfp_mono      [| bnd_mono(D,h); D <= E;
                 !!X. X <= D ==> h(X) <= i(X)
                 |] ==> gfp(D,h) <= gfp(E,i)

```

Figure 3.25: Least and greatest fixedpoints

```

Fin.emptyI      0 : Fin(A)
Fin.consI       [| a: A;  b: Fin(A) |] ==> cons(a,b) : Fin(A)

Fin_induct
  [| b: Fin(A);
    P(0);
    !!x y. [| x: A;  y: Fin(A);  x~:y;  P(y) |] ==> P(cons(x,y))
  |] ==> P(b)

Fin_mono        A<=B ==> Fin(A) <= Fin(B)
Fin_UnI         [| b: Fin(A);  c: Fin(A) |] ==> b Un c : Fin(A)
Fin_UnionI      C : Fin(Fin(A)) ==> Union(C) : Fin(A)
Fin_subset      [| c<=b;  b: Fin(A) |] ==> c: Fin(A)

```

Figure 3.26: The finite set operator

| <i>symbol</i> | <i>meta-type</i> | <i>priority</i> | <i>description</i> |
|---------------|--|-----------------|---------------------------------|
| list | $i \Rightarrow i$ | | lists over some set |
| list_case | $[i, [i, i] \Rightarrow i, i] \Rightarrow i$ | | conditional for <i>list</i> (A) |
| map | $[i \Rightarrow i, i] \Rightarrow i$ | | mapping functional |
| length | $i \Rightarrow i$ | | length of a list |
| rev | $i \Rightarrow i$ | | reverse of a list |
| @ | $[i, i] \Rightarrow i$ | Right 60 | append for lists |
| flat | $i \Rightarrow i$ | | append of list of lists |

```

NilI           Nil : list(A)
ConsI          [| a: A;  l: list(A) |] ==> Cons(a,l) : list(A)

List.induct
  [| l: list(A);
    P(Nil);
    !!x y. [| x: A;  y: list(A);  P(y) |] ==> P(Cons(x,y))
  |] ==> P(l)

Cons_iff       Cons(a,l)=Cons(a',l') <-> a=a' & l=l'
Nil_Cons_iff   ~ Nil=Cons(a,l)

list_mono      A<=B ==> list(A) <= list(B)

map_ident      l: list(A) ==> map(%u. u, l) = l
map_compose    l: list(A) ==> map(h, map(j,l)) = map(%u. h(j(u)), l)
map_app_distrib xs: list(A) ==> map(h, xs@ys) = map(h,xs) @ map(h,ys)
map_type
  [| l: list(A);  !!x. x: A ==> h(x): B |] ==> map(h,l) : list(B)
map_flat
  ls: list(list(A)) ==> map(h, flat(ls)) = flat(map(map(h),ls))

```

Figure 3.27: Lists

| <i>symbol</i> | <i>meta-type</i> | <i>priority</i> | <i>description</i> |
|---------------|------------------------|-----------------|---------------------------|
| \circ | $[i, i] \Rightarrow i$ | Right 60 | composition (\circ) |
| id | $i \Rightarrow i$ | | identity function |
| inj | $[i, i] \Rightarrow i$ | | injective function space |
| surj | $[i, i] \Rightarrow i$ | | surjective function space |
| bij | $[i, i] \Rightarrow i$ | | bijective function space |


```

comp_def  r 0 s      == {xz : domain(s)*range(r) .
                        EX x y z. xz=<x,z> & <x,y>:s & <y,z>:r}
id_def    id(A)      == (lam x:A. x)
inj_def   inj(A,B)   == { f: A->B. ALL w:A. ALL x:A. f'w=f'x --> w=x }
surj_def  surj(A,B)  == { f: A->B . ALL y:B. EX x:A. f'x=y }
bij_def   bij(A,B)   == inj(A,B) Int surj(A,B)

left_inverse  [| f: inj(A,B);  a: A |] ==> converse(f)'(f'a) = a
right_inverse [| f: inj(A,B);  b: range(f) |] ==>
f'(converse(f)'b) = b

inj_converse_inj f: inj(A,B) ==> converse(f): inj(range(f), A)
bij_converse_bij f: bij(A,B) ==> converse(f): bij(B,A)

comp_type      [| s<=A*B;  r<=B*C |] ==> (r 0 s) <= A*C
comp_assoc     (r 0 s) 0 t = r 0 (s 0 t)

left_comp_id   r<=A*B ==> id(B) 0 r = r
right_comp_id  r<=A*B ==> r 0 id(A) = r

comp_func      [| g:A->B; f:B->C |] ==> (f 0 g):A->C
comp_func_apply [| g:A->B; f:B->C; a:A |] ==> (f 0 g)'a = f'(g'a)

comp_inj       [| g:inj(A,B);  f:inj(B,C)  |] ==> (f 0 g):inj(A,C)
comp_surj      [| g:surj(A,B); f:surj(B,C) |] ==> (f 0 g):surj(A,C)
comp_bij       [| g:bij(A,B);  f:bij(B,C) |] ==> (f 0 g):bij(A,C)

left_comp_inverse  f: inj(A,B) ==> converse(f) 0 f = id(A)
right_comp_inverse f: surj(A,B) ==> f 0 converse(f) = id(B)

bij_disjoint_Un
  [| f: bij(A,B);  g: bij(C,D);  A Int C = 0;  B Int D = 0 |] ==>
  (f Un g) : bij(A Un C, B Un D)

restrict_bij  [| f:inj(A,B);  C<=A |] ==> restrict(f,C): bij(C, f'C)

```

Figure 3.28: Permutations

3.6.5 Miscellaneous

The theory **Perm** is concerned with permutations (bijections) and related concepts. These include composition of relations, the identity relation, and three specialized function spaces: injective, surjective and bijective. Figure 3.28 displays many of their properties that have been proved. These results are fundamental to a treatment of equipollence and cardinality.

Theory **Univ** defines a ‘universe’ $\text{univ}(A)$, which is used by the datatype package. This set contains A and the natural numbers. Vitaly, it is closed under finite products: $\text{univ}(A) \times \text{univ}(A) \subseteq \text{univ}(A)$. This theory also defines the cumulative hierarchy of axiomatic set theory, which traditionally is written V_α for an ordinal α . The ‘universe’ is a simple generalization of V_ω .

Theory **QUniv** defines a ‘universe’ $\text{quniv}(A)$, which is used by the datatype package to construct codatatypes such as streams. It is analogous to $\text{univ}(A)$ (and is defined in terms of it) but is closed under the non-standard product and sum.

3.7 Automatic Tools

ZF provides the simplifier and the classical reasoner. Moreover it supplies a specialized tool to infer ‘types’ of terms.

3.7.1 Simplification

ZF inherits simplification from FOL but adopts it for set theory. The extraction of rewrite rules takes the ZF primitives into account. It can strip bounded universal quantifiers from a formula; for example, $\forall x \in A. f(x) = g(x)$ yields the conditional rewrite rule $x \in A \implies f(x) = g(x)$. Given $a \in \{x \in A. P(x)\}$ it extracts rewrite rules from $a \in A$ and $P(a)$. It can also break down $a \in A \cap B$ and $a \in A - B$.

Simplification tactics such as **Asm_simp_tac** and **Full_simp_tac** use the default simpset (**simpset()**), which works for most purposes. A small simplification set for set theory is called **ZF_ss**, and you can even use **FOL_ss** as a minimal starting point. **ZF_ss** contains congruence rules for all the binding operators of ZF. It contains all the conversion rules, such as **fst** and **snd**, as well as the rewrites shown in Fig. 3.29. See the file **ZF/simpdata.ML** for a fuller list.

3.7.2 Classical Reasoning

As for the classical reasoner, tactics such as **Blast_tac** and **Best_tac** refer to the default claset (**claset()**). This works for most purposes. Named claset include **ZF_cs** (basic set theory) and **le_cs** (useful for reasoning

$$\begin{aligned}
a \in \emptyset &\leftrightarrow \perp \\
a \in A \cup B &\leftrightarrow a \in A \vee a \in B \\
a \in A \cap B &\leftrightarrow a \in A \wedge a \in B \\
a \in A - B &\leftrightarrow a \in A \wedge \neg(a \in B) \\
\langle a, b \rangle \in \mathbf{Sigma}(A, B) &\leftrightarrow a \in A \wedge b \in B(a) \\
a \in \mathbf{Collect}(A, P) &\leftrightarrow a \in A \wedge P(a) \\
(\forall x \in \emptyset. P(x)) &\leftrightarrow \top \\
(\forall x \in A. \top) &\leftrightarrow \top
\end{aligned}$$

Figure 3.29: Some rewrite rules for set theory

about the relations $<$ and \leq). You can use `FOL_cs` as a minimal basis for building your own claset. See the *Reference Manual* for more discussion of classical proof methods.

3.7.3 Type-Checking Tactics

Isabelle/ZF provides simple tactics to help automate those proofs that are essentially type-checking. Such proofs are built by applying rules such as these:

```

[| ?P ==> ?a: ?A; ~?P ==> ?b: ?A |] ==> (if ?P then ?a else ?b): ?A

[| ?m : nat; ?n : nat |] ==> ?m #+ ?n : nat

?a : ?A ==> Inl(?a) : ?A + ?B

```

In typical applications, the goal has the form $t \in ?A$: in other words, we have a specific term t and need to infer its ‘type’ by instantiating the set variable $?A$. Neither the simplifier nor the classical reasoner does this job well. The if-then-else rule, and many similar ones, can make the classical reasoner loop. The simplifier refuses (on principle) to instantiate variables during rewriting, so goals such as $i \# + j : ?A$ are left unsolved.

The simplifier calls the type-checker to solve rewritten subgoals: this stage can indeed instantiate variables. If you have defined new constants and proved type-checking rules for them, then insert the rules using `AddTCs` and the rest should be automatic. In particular, the simplifier will use type-checking to help satisfy conditional rewrite rules. Call the tactic `Typecheck_tac` to break down all subgoals using type-checking rules.

Though the easiest way to invoke the type-checker is via the simplifier, specialized applications may require more detailed knowledge of the type-checking primitives. They are modelled on the simplifier’s:

`tcset` is the type of `tcsets`: sets of type-checking rules.

`addTCs` is an infix operator to add type-checking rules to a `tcset`.

`delTCs` is an infix operator to remove type-checking rules from a `tcset`.

`typecheck_tac` is a tactic for attempting to prove all subgoals using the rules given in its argument, a `tcset`.

`Tcsets`, like `simpsets`, are associated with theories and are merged when theories are merged. There are further primitives that use the default `tcset`.

`tcset` is a function to return the default `tcset`; use the expression `tcset()`.

`AddTCs` adds type-checking rules to the default `tcset`.

`DelTCs` removes type-checking rules from the default `tcset`.

`Typecheck_tac` calls `typecheck_tac` using the default `tcset`.

To supply some type-checking rules temporarily, using `Addrules` and later `Delrules` is the simplest way. There is also a high-tech approach. Call the simplifier with a new solver expressed using `type_solver_tac` and your temporary type-checking rules.

```
by (asm_simp_tac
    (simpset() setSolver type_solver_tac (tcset() addTCs prems)) 2);
```

3.8 Natural number and integer arithmetic

Theory `Nat` defines the natural numbers and mathematical induction, along with a case analysis operator. The set of natural numbers, here called `nat`, is known in set theory as the ordinal ω .

Theory `Arith` develops arithmetic on the natural numbers (Fig. 3.30). Addition, multiplication and subtraction are defined by primitive recursion. Division and remainder are defined by repeated subtraction, which requires well-founded recursion; the termination argument relies on the divisor's being non-zero. Many properties are proved: commutative, associative and distributive laws, identity and cancellation laws, etc. The most interesting result is perhaps the theorem $a \bmod b + (a/b) \times b = a$.

To minimize the need for tedious proofs of $t \in \text{nat}$, the arithmetic operators coerce their arguments to be natural numbers. The function `natify` is defined such that `natify(n) = n` if n is a natural number, `natify(succ(x)) = succ(natify(x))` for all x , and finally `natify(x) = 0` in all other cases. The benefit is that the addition, subtraction, multiplication, division and remainder operators always return natural numbers, regardless of their arguments. Algebraic laws (commutative, associative, distributive)

| <i>symbol</i> | <i>meta-type</i> | <i>priority</i> | <i>description</i> |
|-----------------------|---|-----------------|----------------------------|
| <code>nat</code> | i | | set of natural numbers |
| <code>nat_case</code> | $[i, i \Rightarrow i, i] \Rightarrow i$ | | conditional for <i>nat</i> |
| <code>#*</code> | $[i, i] \Rightarrow i$ | Left 70 | multiplication |
| <code>div</code> | $[i, i] \Rightarrow i$ | Left 70 | division |
| <code>mod</code> | $[i, i] \Rightarrow i$ | Left 70 | modulus |
| <code>#+</code> | $[i, i] \Rightarrow i$ | Left 65 | addition |
| <code>#-</code> | $[i, i] \Rightarrow i$ | Left 65 | subtraction |


```

nat_def  nat == lfp(lam r: Pow(Inf). {0} Un {succ(x). x:r}

nat_case_def  nat_case(a,b,k) ==
               THE y. k=0 & y=a | (EX x. k=succ(x) & y=b(x))

nat_0I      0 : nat
nat_succI   n : nat ==> succ(n) : nat

nat_induct
  [| n: nat; P(0);  !!x. [| x: nat; P(x) |] ==> P(succ(x))
   |] ==> P(n)

nat_case_0   nat_case(a,b,0) = a
nat_case_succ nat_case(a,b,succ(m)) = b(m)

add_0_natify 0 #+ n = natify(n)
add_succ     succ(m) #+ n = succ(m #+ n)

mult_type    m ## n : nat
mult_0       0 ## n = 0
mult_succ    succ(m) ## n = n #+ (m ## n)
mult_commute m ## n = n ## m
add_mult_dist (m #+ n) ## k = (m ## k) #+ (n ## k)
mult_assoc   (m ## n) ## k = m ## (n ## k)
mod_div_equality m: nat ==> (m div n)##n #+ m mod n = m

```

Figure 3.30: The natural numbers

| <i>symbol</i> | <i>meta-type</i> | <i>priority</i> | <i>description</i> |
|------------------------------|---|-----------------|--------------------|
| <code>int</code> | i | | set of integers |
| <code>\$*</code> | $[i, i] \Rightarrow i$ | Left 70 | multiplication |
| <code>\$+</code> | $[i, i] \Rightarrow i$ | Left 65 | addition |
| <code>\$-</code> | $[i, i] \Rightarrow i$ | Left 65 | subtraction |
| <code>\$<</code> | $[i, i] \Rightarrow o$ | Left 50 | $<$ on integers |
| <code>\$<=</code> | $[i, i] \Rightarrow o$ | Left 50 | \leq on integers |
| <code>zadd_0_intify</code> | $0 \$+ n = \text{intify}(n)$ | | |
| <code>zmult_type</code> | $m \$* n : \text{int}$ | | |
| <code>zmult_0</code> | $0 \$* n = 0$ | | |
| <code>zmult_commute</code> | $m \$* n = n \$* m$ | | |
| <code>zadd_zmult_dist</code> | $(m \$+ n) \$* k = (m \$* k) \$+ (n \$* k)$ | | |
| <code>zmult_assoc</code> | $(m \$* n) \$* k = m \$* (n \$* k)$ | | |

Figure 3.31: The integers

are unconditional. Occurrences of `natify` as operands of those operators are simplified away. Any remaining occurrences can either be tolerated or else eliminated by proving that the argument is a natural number.

The simplifier automatically cancels common terms on the opposite sides of subtraction and of relations ($=$, $<$ and \leq). Here is an example:

```
1. i #+ j #+ k #- j < k #+ 1
> by (Simp_tac 1);
1. natify(i) < natify(1)
```

Given the assumptions `i:nat` and `l:nat`, both occurrences of `natify` would be simplified away.

Theory `Int` defines the integers, as equivalence classes of natural numbers. Figure 3.31 presents a tidy collection of laws. In fact, a large library of facts is proved, including monotonicity laws for addition and multiplication, covering both positive and negative operands.

As with the natural numbers, the need for typing proofs is minimized. All the operators defined in Fig. 3.31 coerce their operands to integers by applying the function `intify`. This function is the identity on integers and maps other operands to zero.

Decimal notation is provided for the integers. Numbers, written as `#nnn` or `#-nnn`, are represented internally in two's-complement binary. Expressions involving addition, subtraction and multiplication of numeral constants are evaluated (with acceptable efficiency) by simplification. The simplifier also collects similar terms, multiplying them by a numerical coefficient. It also cancels occurrences of the same terms on the other side of the relational operators. Example:

```

1. y $+ z $+ #-3 $* x $+ y $<= x $* #2 $+ z
> by (Simp_tac 1);
1. #2 $* y $<= #5 $* x

```

For more information on the integers, please see the theories on directory ZF/Integ.

3.9 Datatype definitions

The **datatype** definition package of ZF constructs inductive datatypes similar to those of ML. It can also construct coinductive datatypes (codatatypes), which are non-well-founded structures such as streams. It defines the set using a fixed-point construction and proves induction rules, as well as theorems for recursion and case combinators. It supplies mechanisms for reasoning about freeness. The datatype package can handle both mutual and indirect recursion.

3.9.1 Basics

A **datatype** definition has the following form:

$$\begin{array}{lcl}
 \text{datatype} & t_1(A_1, \dots, A_h) & = \text{constructor}_1^1 \mid \dots \mid \text{constructor}_{k_1}^1 \\
 & & \vdots \\
 \text{and} & t_n(A_1, \dots, A_h) & = \text{constructor}_1^n \mid \dots \mid \text{constructor}_{k_n}^n
 \end{array}$$

Here t_1, \dots, t_n are identifiers and A_1, \dots, A_h are variables: the datatype's parameters. Each constructor specification has the form

$$C \ (\ "x_1:T_1", \dots, "x_m:T_m" \)$$

Here C is the constructor name, and variables x_1, \dots, x_m are the constructor arguments, belonging to the sets T_1, \dots, T_m , respectively. Typically each T_j is either a constant set, a datatype parameter (one of A_1, \dots, A_h) or a recursive occurrence of one of the datatypes, say $t_i(A_1, \dots, A_h)$. More complex possibilities exist, but they are much harder to realize. Often, additional information must be supplied in the form of theorems.

A datatype can occur recursively as the argument of some function F . This is called a *nested* (or *indirect*) occurrence. It is only allowed if the datatype package is given a theorem asserting that F is monotonic. If the datatype has indirect occurrences, then Isabelle/ZF does not support recursive function definitions.

A simple example of a datatype is **list**, which is built-in, and is defined by

```

consts    list :: i=>i
datatype "list(A)" = Nil | Cons ("a:A", "l: list(A)")

```

Note that the datatype operator must be declared as a constant first. However, the package declares the constructors. Here, `Nil` gets type i and `Cons` gets type $[i, i] \Rightarrow i$.

Trees and forests can be modelled by the mutually recursive datatype definition

```

consts    tree, forest, tree_forest :: i=>i
datatype "tree(A)"    = Tcons ("a: A", "f: forest(A)")
and       "forest(A)" = Fnil  | Fcons ("t: tree(A)", "f: forest(A)")

```

Here `tree(A)` is the set of trees over A , `forest(A)` is the set of forests over A , and `tree_forest(A)` is the union of the previous two sets. All three operators must be declared first.

The datatype `term`, which is defined by

```

consts    term :: i=>i
datatype "term(A)" = Apply ("a: A", "l: list(term(A))")
monos "[list_mono]"

```

is an example of nested recursion. (The theorem `list_mono` is proved in file `List.ML`, and the `term` example is developed in theory `ex/Term`.)

Freeness of the constructors

Constructors satisfy *freeness* properties. Constructors are distinct, for example `Nil` \neq `Cons(a, l)`, and they are injective, for example `Cons(a, l) = Cons(a', l')` \leftrightarrow $a = a' \wedge l = l'$. Because the number of freeness is quadratic in the number of constructors, the datatype package does not prove them. Instead, it ensures that simplification will prove them dynamically: when the simplifier encounters a formula asserting the equality of two datatype constructors, it performs freeness reasoning.

Freeness reasoning can also be done using the classical reasoner, but it is more complicated. You have to add some safe elimination rules to the claset. For the `list` datatype, they are called `list.free_SEs`. Occasionally this exposes the underlying representation of some constructor, which can be rectified using the command `fold_tac list.con_defs`.

Structural induction

The datatype package also provides structural induction rules. For datatypes without mutual or nested recursion, the rule has the form exemplified by `list.induct` in Fig. 3.27. For mutually recursive datatypes, the induction rule is supplied in two forms. Consider datatype `TF`. The rule `tree_forest.induct` performs induction over a single predicate P , which is presumed to be defined for both trees and forests:

```

[| x : tree_forest(A);
  !!a f. [| a : A; f : forest(A); P(f) |] ==> P(Tcons(a, f));
  P(Fnil);
  !!f t. [| t : tree(A); P(t); f : forest(A); P(f) |]
    ==> P(Fcons(t, f))
|] ==> P(x)

```

The rule `tree_forest.mutual_induct` performs induction over two distinct predicates, `P_tree` and `P_forest`.

```

[| !!a f.
  [| a : A; f : forest(A); P_forest(f) |] ==> P_tree(Tcons(a, f));
  P_forest(Fnil);
  !!f t. [| t : tree(A); P_tree(t); f : forest(A); P_forest(f) |]
    ==> P_forest(Fcons(t, f))
|] ==> (ALL za. za : tree(A) --> P_tree(za)) &
  (ALL za. za : forest(A) --> P_forest(za))

```

For datatypes with nested recursion, such as the `term` example from above, things are a bit more complicated. The rule `term.induct` refers to the monotonic operator, `list`:

```

[| x : term(A);
  !!a l. [| a : A; l : list(Collect(term(A), P)) |] ==> P(Apply(a, l))
|] ==> P(x)

```

The file `ex/Term.ML` derives two higher-level induction rules, one of which is particularly useful for proving equations:

```

[| t : term(A);
  !!x zs. [| x : A; zs : list(term(A)); map(f, zs) = map(g, zs) |]
    ==> f(Apply(x, zs)) = g(Apply(x, zs))
|] ==> f(t) = g(t)

```

How this can be generalized to other nested datatypes is a matter for future research.

The case operator

The package defines an operator for performing case analysis over the datatype. For `list`, it is called `list_case` and satisfies the equations

```

list_case(f_Nil, f_Cons, []) = f_Nil
list_case(f_Nil, f_Cons, Cons(a, l)) = f_Cons(a, l)

```

Here `f_Nil` is the value to return if the argument is `Nil` and `f_Cons` is a function that computes the value to return if the argument has the form `Cons(a, l)`. The function can be expressed as an abstraction, over patterns if desired (§3.5.4).

For mutually recursive datatypes, there is a single `case` operator. In the `tree/forest` example, the constant `tree_forest_case` handles all of the constructors of the two datatypes.

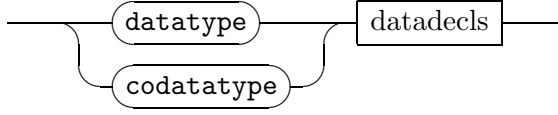
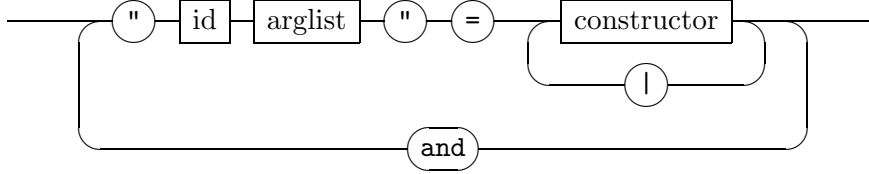
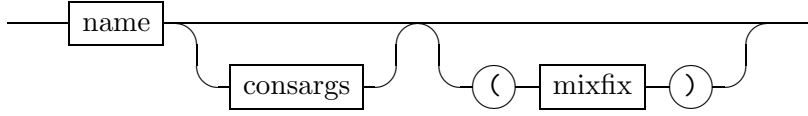
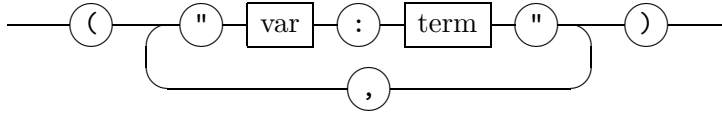
datatype*datadecls**constructor**consargs*

Figure 3.32: Syntax of datatype declarations

3.9.2 Defining datatypes

The theory syntax for datatype definitions is shown in Fig. 3.32. 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. The quotation marks are necessary because they enclose general Isabelle formulæ.

Codatypes are declared like datatypes and are identical to them in every respect except that they have a coinduction rule instead of an induction rule. Note that while an induction rule has the effect of limiting the values contained in the set, a coinduction rule gives a way of constructing new values of the set.

Most of the theorems about datatypes become part of the default simpset. You never need to see them again because the simplifier applies them automatically. Induction or exhaustion are usually invoked by hand, usually via these special-purpose tactics:

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

not occur among other assumptions of the subgoal.

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

`exhaust_tac "x" i` performs an exhaustive case analysis for the variable x .

Both tactics can only be applied to a variable, whose typing must be given in some assumption, for example the assumption $x: \text{list}(A)$. The tactics also work for the natural numbers (`nat`) and disjoint sums, although these sets were not defined using the datatype package. (Disjoint sums are not recursive, so only `exhaust_tac` is available.)

Here are some more details for the technically minded. 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 intrs      : thm list  the introduction rules
val elim       : thm       the elimination (case analysis) rule
val induct     : thm       the standard induction rule
val mutual_induct : thm     the mutual induction rule, or True
val case_eqns  : thm list  equations for the case operator
val recursor_eqns : thm list equations for the recursor
val con_defs   : thm list  definitions of the case operator and constructors
val free_iffs  : thm list  logical equivalences for proving freeness
val free_SEs   : thm list  elimination rules for proving freeness
val mk_free    : string -> thm  A function for proving freeness theorems
val mk_cases   : string -> thm  case analysis, see below
val defs       : thm list  definitions of operators
val bnd_mono   : thm list  monotonicity property
val dom_subset : thm list  inclusion in 'bounding set'

```

Furthermore there is the theorem C_I for every constructor C ; for example, the `list` datatype's introduction rules are bound to the identifiers `Nil_I` and `Cons_I`.

For a codatatype, the component `coinduct` is the coinduction rule, replacing the `induct` component.

See the theories `ex/Ntree` and `ex/Brouwer` for examples of infinitely branching datatypes. See theory `ex/LList` for an example of a codatatype. Some of these theories illustrate the use of additional, undocumented features of the datatype package. Datatype definitions are reduced to inductive definitions, and the advanced features should be understood in that light.

3.9.3 Examples

The datatype of binary trees

Let us define the set $\text{bt}(A)$ of binary trees over A . The theory must contain these lines:

```

consts  bt :: i=>i
datatype "bt(A)" = Lf | Br ("a: A", "t1: bt(A)", "t2: bt(A)")

```

After loading the theory, we can prove, for example, that no tree equals its left branch. To ease the induction, we state the goal using quantifiers.

```

Goal "1 : bt(A) ==> ALL x r. Br(x,l,r) ~= l";
Level 0
1 : bt(A) ==> ALL x r. Br(x, l, r) ~= l
1. 1 : bt(A) ==> ALL x r. Br(x, l, r) ~= l

```

This can be proved by the structural induction tactic:

```

by (induct_tac "1" 1);
Level 1
1 : bt(A) ==> ALL x r. Br(x, l, r) ~= l
1. ALL x r. Br(x, Lf, r) ~= Lf
2. !!a t1 t2.
   [| a : A; t1 : bt(A);
    ALL x r. Br(x, t1, r) ~= t1; t2 : bt(A);
    ALL x r. Br(x, t2, r) ~= t2 |]
   ==> ALL x r. Br(x, Br(a, t1, t2), r) ~= Br(a, t1, t2)

```

Both subgoals are proved using `Auto_tac`, which performs the necessary freeness reasoning.

```

by Auto_tac;
Level 2
1 : bt(A) ==> ALL x r. Br(x, l, r) ~= l
No subgoals!

```

To remove the quantifiers from the induction formula, we save the theorem using `qed_spec_mp`.

```

qed_spec_mp "Br_neq_left";
val Br_neq_left = "?l : bt(?A) ==> Br(?x, ?l, ?r) ~= ?l" : thm

```

When there are only a few constructors, we might prefer to prove the freeness theorems for each constructor. This is trivial, using the function given us for that purpose:

```

val Br_iff =
  bt.mk_free "Br(a,l,r)=Br(a',l',r') <-> a=a' & l=l' & r=r'";
val Br_iff =
  "Br(?a, ?l, ?r) = Br(?a', ?l', ?r') <->
   ?a = ?a' & ?l = ?l' & ?r = ?r'" : thm

```

The purpose of `mk_cases` is to generate instances of the elimination (case analysis) rule that have been simplified using freeness reasoning. For example, this instance of the elimination rule propagates type-checking information from the premise $\text{Br}(a, l, r) \in \text{bt}(A)$:

```

val BrE = bt.mk_cases "Br(a,l,r) : bt(A)";
val BrE =
  "[| Br(?a, ?l, ?r) : bt(?A);
   [| ?a : ?A; ?l : bt(?A); ?r : bt(?A) |] ==> ?Q |]
   ==> ?Q" : thm

```

Mixfix syntax in datatypes

Mixfix syntax is sometimes convenient. The theory `ex/PropLog` makes a deep embedding of propositional logic:

```
consts    prop :: i
datatype  "prop" = Fls
           | Var ("n: nat")          ("#_" [100] 100)
           | "=>" ("p: prop", "q: prop") (infixr 90)
```

The second constructor has a special `#n` syntax, while the third constructor is an infix arrow.

A giant enumeration type

This example shows a datatype that consists of 60 constructors:

```
consts  enum :: i
datatype
  "enum" = C00 | C01 | C02 | C03 | C04 | C05 | C06 | C07 | C08 | C09
          | C10 | C11 | C12 | C13 | C14 | C15 | C16 | C17 | C18 | C19
          | C20 | C21 | C22 | C23 | C24 | C25 | C26 | C27 | C28 | C29
          | C30 | C31 | C32 | C33 | C34 | C35 | C36 | C37 | C38 | C39
          | C40 | C41 | C42 | C43 | C44 | C45 | C46 | C47 | C48 | C49
          | C50 | C51 | C52 | C53 | C54 | C55 | C56 | C57 | C58 | C59
end
```

The datatype package scales well. Even though all properties are proved rather than assumed, full processing of this definition takes under 15 seconds (on a 300 MHz Pentium). The constructors have a balanced representation, essentially binary notation, so freeness properties can be proved fast.

```
Goal "C00 ~= C01";
by (Simp_tac 1);
```

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

3.9.4 Recursive function definitions

Datatypes come with a uniform way of defining functions, **primitive recursion**. Such definitions rely on the recursion operator defined by the datatype package. Isabelle proves the desired recursion equations as theorems.

In principle, one could introduce primitive recursive functions by asserting their reduction rules as new axioms. Here is a dangerous way of defining the append function for lists:

```
consts  "@" :: [i,i] => i                                (infixr 60)
rules
  app_Nil   "[ ] @ ys = ys"
  app_Cons  "(Cons(a,l)) @ ys = Cons(a, l @ ys)"
```

Asserting axioms brings the danger of accidentally asserting nonsense. It should be avoided at all costs!

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

```
consts "@" :: [i,i]=>i                                (infixr 60)
primrec
  "[] @ ys = ys"
  "(Cons(a,l)) @ ys = Cons(a, l @ ys)"
```

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

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

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

Syntax of recursive definitions

The general form of a primitive recursive definition is

```
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 zero.

All reduction rules are added to the default simpset. 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 reduction rules for `@` become part of the default simpset, which leads to short proof scripts:

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

You can even use the `primrec` form with non-recursive datatypes and with codatatypes. Recursion is not allowed, but it provides a convenient syntax for defining functions by cases.

Example: varying arguments

All arguments, other than the recursive one, must be the same in each equation and in each recursive call. To get around this restriction, use explicit λ -abstraction and function application. Here is an example, drawn from the theory `Resid/Substitution`. The type of redexes is declared as follows:

```
consts redexes :: i
datatype
  "redexes" = Var ("n: nat")
             | Fun ("t: redexes")
             | App ("b:bool" , "f:redexes" , "a:redexes")
```

The function `lift` takes a second argument, k , which varies in recursive calls.

```
primrec
  "lift(Var(i)) = (lam k:nat. if i<k then Var(i) else Var(succ(i)))"
  "lift(Fun(t)) = (lam k:nat. Fun(lift(t) ' succ(k)))"
  "lift(App(b,f,a)) = (lam k:nat. App(b, lift(f)'k, lift(a)'k))"
```

Now `lift(r)'k` satisfies the required recursion equations.

3.10 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 described in detail in a separate paper,² which you might refer to for background information.

3.10.1 The syntax of a (co)inductive definition

An inductive definition has the form

²It appeared in CADE [15]; a longer version is distributed with Isabelle as *A Fixedpoint Approach to (Co)Inductive and (Co)Datatype Definitions*.

```

inductive
  domains      domain declarations
  intrs        introduction rules
  monos        monotonicity theorems
  con_defs     constructor definitions
  type_intrs   introduction rules for type-checking
  type_elims   elimination rules for type-checking

```

A coinductive definition is identical, but starts with the keyword `co-inductive`.

The `monos`, `con_defs`, `type_intrs` and `type_elims` sections are optional. If present, each is specified either as a list of identifiers or as a string. If the latter, then the string must be a valid ML expression of type `thm list`. The string is simply inserted into the `_thy.ML` file; if it is ill-formed, it will trigger ML error messages. You can then inspect the file on the temporary directory.

domain declarations are items of the form *string* `<=` *string*, associating each recursive set with its domain. (The domain is some existing set that is large enough to hold the new set being defined.)

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.

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!

constructor definitions contain definitions of constants appearing in the introduction rules. The (co)datatype package supplies the constructors' definitions here. Most (co)inductive definitions omit this section; one exception is the primitive recursive functions example; see theory `ex/Primrec`.

type_intrs consists of introduction rules for type-checking the definition: for demonstrating that the new set is included in its domain. (The proof uses depth-first search.)

type_elims consists of elimination rules for type-checking the definition. They are presumed to be safe and are applied as often as possible prior to the `type_intrs` search.

The package has a few restrictions:

- The theory must separately declare the recursive sets as constants.

- The names of the recursive sets must be identifiers, not infix operators.
- Side-conditions must not be conjunctions. However, an introduction rule may contain any number of side-conditions.
- Side-conditions of the form $x = t$, where the variable x does not occur in t , will be substituted through the rule `mutual_induct`.

3.10.2 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 :: i=>i

inductive
  domains  "Fin(A)" <= "Pow(A)"
  intrs
    emptyI  "0 : Fin(A)"
    consI   "[| a: A;  b: Fin(A) |] ==> cons(a,b) : Fin(A)"
  type_intrs empty_subsetI, cons_subsetI, PowI
  type_elims "[make_elim PowD]"
```

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`.

The chief problem with making (co)inductive definitions involves type-checking the rules. Sometimes, additional theorems need to be supplied under `type_intrs` or `type_elims`. If the package fails when trying to prove your introduction rules, then set the flag `trace_induct` to `true` and try again. (See the manual *A Fixedpoint Approach ...* for more discussion of type-checking.)

In the example above, `Pow(A)` is given as the domain of `Fin(A)`, for obviously every finite subset of A is a subset of A . However, the inductive definition package can only prove that given a few hints. Here is the output that results (with the flag set) when the `type_intrs` and `type_elims` are omitted from the inductive definition above:

```
Inductive definition Finite.Fin
Fin(A) ==
lfp(Pow(A),
  %X. z: Pow(A) . z = 0 | (EX a b. z = cons(a, b) & a : A & b : X))
  Proving monotonicity...
  Proving the introduction rules...
The type-checking subgoal:
0 : Fin(A)
1. 0 : Pow(A)
```



```

The subgoal after monos, type_elims:
0 : Fin(A)
1. 0 : Pow(A)
*** prove_goal: tactic failed

```

We see the need to supply theorems to let the package prove $\emptyset \in \text{Pow}(A)$. Restoring the `type_intrs` but not the `type_elims`, we again get an error message:

```

The type-checking subgoal:
0 : Fin(A)
1. 0 : Pow(A)
The subgoal after monos, type_elims:
0 : Fin(A)
1. 0 : Pow(A)
The type-checking subgoal:
cons(a, b) : Fin(A)
1. [| a : A; b : Fin(A) |] ==> cons(a, b) : Pow(A)
The subgoal after monos, type_elims:
cons(a, b) : Fin(A)
1. [| a : A; b : Pow(A) |] ==> cons(a, b) : Pow(A)
*** prove_goal: tactic failed

```

The first rule has been type-checked, but the second one has failed. The simplest solution to such problems is to prove the failed subgoal separately and to supply it under `type_intrs`. The solution actually used is to supply, under `type_elims`, a rule that changes $b \in \text{Pow}(A)$ to $b \subseteq A$; together with `cons_subsetI` and `PowI`, it is enough to complete the type-checking.

3.10.3 Further examples

An inductive definition may involve arbitrary monotonic operators. Here is a standard example: the accessible part of a relation. Note the use of `Pow` in the introduction rule and the corresponding mention of the rule `Pow_mono` in the `monos` list. If the desired rule has a universally quantified premise, usually the effect can be obtained using `Pow`.

```

consts acc :: i=>i
inductive
  domains "acc(r)" <= "field(r)"
  intrs
    vimage "[| r-‘‘a: Pow(acc(r)); a: field(r) |] ==> a: acc(r)"
  monos
    Pow_mono

```

Finally, here is a coinductive definition. It captures (as a bisimulation) the notion of equality on lazy lists, which are first defined as a codatatype:

```

consts llist :: i=>i
codatatype "llist(A)" = LNil | LCons ("a: A", "l: llist(A)")

```

```

consts lleq :: i=>i
coinductive
  domains "lleq(A)" <= "llist(A) * llist(A)"
  intrs
    LNil "<LNil, LNil> : lleq(A)"
    LCons "[| a:A; <l,l'>: lleq(A) |]"
           ==> <LCons(a,l), LCons(a,l')>: lleq(A)"
  type_intrs "llist.intrs"

```

This use of `type_intrs` is typical: the relation concerns the codatatype `llist`, so naturally the introduction rules for that codatatype will be required for type-checking the rules.

The Isabelle distribution contains many other inductive definitions. Simple examples are collected on subdirectory `ZF/ex`. The directory `Coind` and the theory `ZF/ex/LList` contain coinductive definitions. Larger examples may be found on other subdirectories of `ZF`, such as `IMP`, and `Resid`.

3.10.4 The result structure

Each (co)inductive set defined in a theory file generates an ML substructure having the same name. The substructure contains the following elements:

```

val intrs      : thm list  the introduction rules
val elim       : thm       the elimination (case analysis) rule
val mk_cases   : string -> thm  case analysis, see below
val induct     : thm       the standard induction rule
val mutual_induct : thm     the mutual induction rule, or True
val defs       : thm list  definitions of operators
val bnd_mono   : thm list  monotonicity property
val dom_subset : thm list  inclusion in 'bounding set'

```

Furthermore there is the theorem `C_I` for every constructor `C`; for example, the `list` datatype's introduction rules are bound to the identifiers `Nil_I` and `Cons_I`.

For a codatatype, the component `coinduct` is the coinduction rule, replacing the `induct` component.

Recall that `mk_cases` generates simplified instances of the elimination (case analysis) rule. It is as useful for inductive definitions as it is for datatypes. There are many examples in the theory `ex/Comb`, which is discussed at length elsewhere [17]. The theory first defines the datatype `comb` of combinators:

```

consts comb :: i
datatype "comb" = K
           | S
           | "#" ("p: comb", "q: comb")  (infixl 90)

```

The theory goes on to define contraction and parallel contraction inductively. Then the file `ex/Comb.ML` defines special cases of contraction using

`mk_cases`:

```
val K_contractE = contract.mk_cases "K -1-> r";
val K_contractE = "K -1-> ?r ==> ?Q" : thm
```

We can read this as saying that the combinator `K` cannot reduce to anything. Similar elimination rules for `S` and application are also generated and are supplied to the classical reasoner. Note that `comb.con_defs` is given to `mk_cases` to allow freeness reasoning on datatype `comb`.

3.11 The outer reaches of set theory

The constructions of the natural numbers and lists use a suite of operators for handling recursive function definitions. I have described the developments in detail elsewhere [16]. Here is a brief summary:

- Theory `Trancl` defines the transitive closure of a relation (as a least fixedpoint).
- Theory `WF` proves the Well-Founded Recursion Theorem, using an elegant approach of Tobias Nipkow. This theorem permits general recursive definitions within set theory.
- Theory `Ord` defines the notions of transitive set and ordinal number. It derives transfinite induction. A key definition is **less than**: $i < j$ if and only if i and j are both ordinals and $i \in j$. As a special case, it includes less than on the natural numbers.
- Theory `Epsilon` derives ε -induction and ε -recursion, which are generalisations of transfinite induction and recursion. It also defines `rank(x)`, which is the least ordinal α such that x is constructed at stage α of the cumulative hierarchy (thus $x \in V_{\alpha+1}$).

Other important theories lead to a theory of cardinal numbers. They have not yet been written up anywhere. Here is a summary:

- Theory `Rel` defines the basic properties of relations, such as (ir)reflexivity, (a)symmetry, and transitivity.
- Theory `EquivClass` develops a theory of equivalence classes, not using the Axiom of Choice.
- Theory `Order` defines partial orderings, total orderings and wellorderings.
- Theory `OrderArith` defines orderings on sum and product sets. These can be used to define ordinal arithmetic and have applications to cardinal arithmetic.

- Theory `OrderType` defines order types. Every wellordering is equivalent to a unique ordinal, which is its order type.
- Theory `Cardinal` defines equipollence and cardinal numbers.
- Theory `CardinalArith` defines cardinal addition and multiplication, and proves their elementary laws. It proves that there is no greatest cardinal. It also proves a deep result, namely $\kappa \otimes \kappa = \kappa$ for every infinite cardinal κ ; see Kunen [10, page 29]. None of these results assume the Axiom of Choice, which complicates their proofs considerably.

The following developments involve the Axiom of Choice (AC):

- Theory `AC` asserts the Axiom of Choice and proves some simple equivalent forms.
- Theory `Zorn` proves Hausdorff’s Maximal Principle, Zorn’s Lemma and the Wellordering Theorem, following Abrial and Laffitte [1].
- Theory `Cardinal_AC` uses AC to prove simplified theorems about the cardinals. It also proves a theorem needed to justify infinitely branching datatype declarations: if κ is an infinite cardinal and $|X(\alpha)| \leq \kappa$ for all $\alpha < \kappa$ then $|\bigcup_{\alpha < \kappa} X(\alpha)| \leq \kappa$.
- Theory `InfDatatype` proves theorems to justify infinitely branching datatypes. Arbitrary index sets are allowed, provided their cardinalities have an upper bound. The theory also justifies some unusual cases of finite branching, involving the finite powerset operator and the finite function space operator.

3.12 The examples directories

Directory `HOL/IMP` contains a mechanised version of a semantic equivalence proof taken from Winskel [22]. It formalises the denotational and operational semantics of a simple while-language, then proves the two equivalent. It contains several datatype and inductive definitions, and demonstrates their use.

The directory `ZF/ex` contains further developments in ZF set theory. Here is an overview; see the files themselves for more details. I describe much of this material in other publications [14, 16, 15].

- File `misc.ML` contains miscellaneous examples such as Cantor’s Theorem, the Schröder-Bernstein Theorem and the ‘Composition of homomorphisms’ challenge [3].
- Theory `Ramsey` proves the finite exponent 2 version of Ramsey’s Theorem, following Basin and Kaufmann’s presentation [2].

- Theory **Integ** develops a theory of the integers as equivalence classes of pairs of natural numbers.
- 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.
- Theory **Primes** defines the Greatest Common Divisor of two natural numbers and the “divides” relation.
- Theory **Bin** defines a datatype for two’s complement binary integers, then proves rewrite rules to perform binary arithmetic. For instance, $1359 \times -2468 = -3354012$ takes under 14 seconds.
- Theory **BT** defines the recursive data structure $\mathbf{bt}(A)$, labelled binary trees.
- Theory **Term** defines a recursive data structure for terms and term lists. These are simply finite branching trees.
- Theory **TF** defines primitives for solving mutually recursive equations over sets. It constructs sets of trees and forests as an example, including induction and recursion rules that handle the mutual recursion.
- Theory **Prop** proves soundness and completeness of propositional logic [16]. This illustrates datatype definitions, inductive definitions, structural induction and rule induction.
- Theory **ListN** inductively defines the lists of n elements [12].
- Theory **Acc** inductively defines the accessible part of a relation [12].
- Theory **Comb** defines the datatype of combinators and inductively defines contraction and parallel contraction. It goes on to prove the Church-Rosser Theorem. This case study follows Camilleri and Melham [4].
- Theory **LList** defines lazy lists and a coinduction principle for proving equations between them.

3.13 A proof about powersets

To demonstrate high-level reasoning about subsets, let us prove the equation $\mathbf{Pow}(A) \cap \mathbf{Pow}(B) = \mathbf{Pow}(A \cap B)$. Compared with first-order logic, set theory involves a maze of rules, and theorems have many different proofs. Attempting other proofs of the theorem might be instructive. This proof exploits the lattice properties of intersection. It also uses the monotonicity of the powerset operation, from `ZF/mono.ML`:

```
Pow_mono      A<=B ==> Pow(A) <= Pow(B)
```

We enter the goal and make the first step, which breaks the equation into two inclusions by extensionality:

```
Goal "Pow(A Int B) = Pow(A) Int Pow(B)";
Level 0
Pow(A Int B) = Pow(A) Int Pow(B)
1. Pow(A Int B) = Pow(A) Int Pow(B)
by (resolve_tac [equalityI] 1);
Level 1
Pow(A Int B) = Pow(A) Int Pow(B)
1. Pow(A Int B) <= Pow(A) Int Pow(B)
2. Pow(A) Int Pow(B) <= Pow(A Int B)
```

Both inclusions could be tackled straightforwardly using `subsetI`. A shorter proof results from noting that intersection forms the greatest lower bound:

```
by (resolve_tac [Int_greatest] 1);
Level 2
Pow(A Int B) = Pow(A) Int Pow(B)
1. Pow(A Int B) <= Pow(A)
2. Pow(A Int B) <= Pow(B)
3. Pow(A) Int Pow(B) <= Pow(A Int B)
```

Subgoal 1 follows by applying the monotonicity of `Pow` to $A \cap B \subseteq A$; subgoal 2 follows similarly:

```
by (resolve_tac [Int_lower1 RS Pow_mono] 1);
Level 3
Pow(A Int B) = Pow(A) Int Pow(B)
1. Pow(A Int B) <= Pow(B)
2. Pow(A) Int Pow(B) <= Pow(A Int B)
by (resolve_tac [Int_lower2 RS Pow_mono] 1);
Level 4
Pow(A Int B) = Pow(A) Int Pow(B)
1. Pow(A) Int Pow(B) <= Pow(A Int B)
```

We are left with the opposite inclusion, which we tackle in the straightforward way:

```
by (resolve_tac [subsetI] 1);
Level 5
Pow(A Int B) = Pow(A) Int Pow(B)
1. !!x. x : Pow(A) Int Pow(B) ==> x : Pow(A Int B)
```

The subgoal is to show $x \in \text{Pow}(A \cap B)$ assuming $x \in \text{Pow}(A) \cap \text{Pow}(B)$; eliminating this assumption produces two subgoals. The rule `IntE` treats the intersection like a conjunction instead of unfolding its definition.

```
by (eresolve_tac [IntE] 1);
Level 6
Pow(A Int B) = Pow(A) Int Pow(B)
1. !!x. [| x : Pow(A); x : Pow(B) |] ==> x : Pow(A Int B)
```

The next step replaces the `Pow` by the subset relation (\subseteq).

```

by (resolve_tac [PowI] 1);
Level 7
Pow(A Int B) = Pow(A) Int Pow(B)
1. !!x. [| x : Pow(A); x : Pow(B) |] ==> x <= A Int B

```

We perform the same replacement in the assumptions. This is a good demonstration of the tactic `dresolve_tac`:

```

by (REPEAT (dresolve_tac [PowD] 1));
Level 8
Pow(A Int B) = Pow(A) Int Pow(B)
1. !!x. [| x <= A; x <= B |] ==> x <= A Int B

```

The assumptions are that x is a lower bound of both A and B , but $A \cap B$ is the greatest lower bound:

```

by (resolve_tac [Int_greatest] 1);
Level 9
Pow(A Int B) = Pow(A) Int Pow(B)
1. !!x. [| x <= A; x <= B |] ==> x <= A
2. !!x. [| x <= A; x <= B |] ==> x <= B

```

To conclude the proof, we clear up the trivial subgoals:

```

by (REPEAT (assume_tac 1));
Level 10
Pow(A Int B) = Pow(A) Int Pow(B)
No subgoals!

```

We could have performed this proof in one step by applying `Blast_tac`. Let us go back to the start:

```

choplev 0;
Level 0
Pow(A Int B) = Pow(A) Int Pow(B)
1. Pow(A Int B) = Pow(A) Int Pow(B)
by (Blast_tac 1);
Depth = 0
Depth = 1
Depth = 2
Depth = 3
Level 1
Pow(A Int B) = Pow(A) Int Pow(B)
No subgoals!

```

Past researchers regarded this as a difficult proof, as indeed it is if all the symbols are replaced by their definitions.

3.14 Monotonicity of the union operator

For another example, we prove that general union is monotonic: $C \subseteq D$ implies $\bigcup(C) \subseteq \bigcup(D)$. To begin, we tackle the inclusion using `subsetI`:

```

Goal "C<=D ==> Union(C) <= Union(D)";
Level 0
C <= D ==> Union(C) <= Union(D)
1. C <= D ==> Union(C) <= Union(D)
by (resolve_tac [subsetI] 1);
Level 1
C <= D ==> Union(C) <= Union(D)
1. !!x. [| C <= D; x : Union(C) |] ==> x : Union(D)

```

Big union is like an existential quantifier — the occurrence in the assumptions must be eliminated early, since it creates parameters.

```

by (eresolve_tac [UnionE] 1);
Level 2
C <= D ==> Union(C) <= Union(D)
1. !!x B. [| C <= D; x : B; B : C |] ==> x : Union(D)

```

Now we may apply `UnionI`, which creates an unknown involving the parameters. To show $x \in \bigcup(D)$ it suffices to show that x belongs to some element, say $?B2(x, B)$, of D .

```

by (resolve_tac [UnionI] 1);
Level 3
C <= D ==> Union(C) <= Union(D)
1. !!x B. [| C <= D; x : B; B : C |] ==> ?B2(x,B) : D
2. !!x B. [| C <= D; x : B; B : C |] ==> x : ?B2(x,B)

```

Combining `subsetD` with the assumption $C \subseteq D$ yields $?a \in C \implies ?a \in D$, which reduces subgoal 1. Note that `eresolve_tac` has removed that assumption.

```

by (eresolve_tac [subsetD] 1);
Level 4
C <= D ==> Union(C) <= Union(D)
1. !!x B. [| x : B; B : C |] ==> ?B2(x,B) : C
2. !!x B. [| C <= D; x : B; B : C |] ==> x : ?B2(x,B)

```

The rest is routine. Observe how $?B2(x, B)$ is instantiated.

```

by (assume_tac 1);
Level 5
C <= D ==> Union(C) <= Union(D)
1. !!x B. [| C <= D; x : B; B : C |] ==> x : B
by (assume_tac 1);
Level 6
C <= D ==> Union(C) <= Union(D)
No subgoals!

```

Again, `Blast_tac` can prove the theorem in one step.


```

by (Blast_tac 1);
  Depth = 0
  Depth = 1
  Depth = 2
  Level 1
  C <= D ==> Union(C) <= Union(D)
  No subgoals!

```

The file `ZF/equalities.ML` has many similar proofs. Reasoning about general intersection can be difficult because of its anomalous behaviour on the empty set. However, `Blast_tac` copes well with these. Here is a typical example, borrowed from Devlin [6, page 12]:

```
a:C ==> (INT x:C. A(x) Int B(x)) = (INT x:C. A(x)) Int (INT x:C. B(x))
```

In traditional notation this is

$$a \in C \implies \bigcap_{x \in C} (A(x) \cap B(x)) = \left(\bigcap_{x \in C} A(x) \right) \cap \left(\bigcap_{x \in C} B(x) \right)$$

3.15 Low-level reasoning about functions

The derived rules `lamI`, `lamE`, `lam_type`, `beta` and `eta` support reasoning about functions in a λ -calculus style. This is generally easier than regarding functions as sets of ordered pairs. But sometimes we must look at the underlying representation, as in the following proof of `fun_disjoint_apply1`. This states that if f and g are functions with disjoint domains A and C , and if $a \in A$, then $(f \cup g)'a = f'a$:

```

Goal "[| a:A; f: A->B; g: C->D; A Int C = 0 |] ==> \
\ (f Un g)'a = f'a";
  Level 0
  [| a : A; f : A -> B; g : C -> D; A Int C = 0 |]
  ==> (f Un g) ' a = f ' a
  1. [| a : A; f : A -> B; g : C -> D; A Int C = 0 |]
     ==> (f Un g) ' a = f ' a

```

Using `apply_equality`, we reduce the equality to reasoning about ordered pairs. The second subgoal is to verify that $f \cup g$ is a function. To save space, the assumptions will be abbreviated below.

```

by (resolve_tac [apply_equality] 1);
  Level 1
  [| ... |] ==> (f Un g) ' a = f ' a
  1. [| ... |] ==> <a,f ' a> : f Un g
  2. [| ... |] ==> f Un g : (PROD x:?A. ?B(x))

```

We must show that the pair belongs to f or g ; by `UnI1` we choose f :

```

by (resolve_tac [UnI1] 1);
Level 2
[| ... |] ==> (f Un g) ' a = f ' a
1. [| ... |] ==> <a,f ' a> : f
2. [| ... |] ==> f Un g : (PROD x:?A. ?B(x))

```

To show $\langle a, f'a \rangle \in f$ we use `apply_Pair`, which is essentially the converse of `apply_equality`:

```

by (resolve_tac [apply_Pair] 1);
Level 3
[| ... |] ==> (f Un g) ' a = f ' a
1. [| ... |] ==> f : (PROD x:?A2. ?B2(x))
2. [| ... |] ==> a : ?A2
3. [| ... |] ==> f Un g : (PROD x:?A. ?B(x))

```

Using the assumptions $f \in A \rightarrow B$ and $a \in A$, we solve the two subgoals from `apply_Pair`. Recall that a Π -set is merely a generalized function space, and observe that `?A2` is instantiated to `A`.

```

by (assume_tac 1);
Level 4
[| ... |] ==> (f Un g) ' a = f ' a
1. [| ... |] ==> a : A
2. [| ... |] ==> f Un g : (PROD x:?A. ?B(x))
by (assume_tac 1);
Level 5
[| ... |] ==> (f Un g) ' a = f ' a
1. [| ... |] ==> f Un g : (PROD x:?A. ?B(x))

```

To construct functions of the form $f \cup g$, we apply `fun_disjoint_Un`:

```

by (resolve_tac [fun_disjoint_Un] 1);
Level 6
[| ... |] ==> (f Un g) ' a = f ' a
1. [| ... |] ==> f : ?A3 -> ?B3
2. [| ... |] ==> g : ?C3 -> ?D3
3. [| ... |] ==> ?A3 Int ?C3 = 0

```

The remaining subgoals are instances of the assumptions. Again, observe how unknowns are instantiated:

```

by (assume_tac 1);
  Level 7
  [| ... |] ==> (f Un g) ` a = f ` a
    1. [| ... |] ==> g : ?C3 -> ?D3
    2. [| ... |] ==> A Int ?C3 = 0
by (assume_tac 1);
  Level 8
  [| ... |] ==> (f Un g) ` a = f ` a
    1. [| ... |] ==> A Int C = 0
by (assume_tac 1);
  Level 9
  [| ... |] ==> (f Un g) ` a = f ` a
  No subgoals!

```

See the files `ZF/func.ML` and `ZF/WF.ML` for more examples of reasoning about functions.

Bibliography

- [1] J. R. Abrial and G. Laffitte. Towards the mechanization of the proofs of some classical theorems of set theory. preprint, February 1993.
- [2] David Basin and Matt Kaufmann. The Boyer-Moore prover and Nuprl: An experimental comparison. In Gérard Huet and Gordon Plotkin, editors, *Logical Frameworks*, pages 89–119. Cambridge University Press, 1991.
- [3] Robert Boyer, Ewing Lusk, William McCune, Ross Overbeek, Mark Stickel, and Lawrence Wos. Set theory in first-order logic: Clauses for Gödel’s axioms. *Journal of Automated Reasoning*, 2(3):287–327, 1986.
- [4] J. Camilleri and T. F. Melham. Reasoning with inductively defined relations in the HOL theorem prover. Technical Report 265, Computer Laboratory, University of Cambridge, August 1992.
- [5] B. A. Davey and H. A. Priestley. *Introduction to Lattices and Order*. Cambridge University Press, 1990.
- [6] Keith J. Devlin. *Fundamentals of Contemporary Set Theory*. Springer, 1979.
- [7] Michael Dummett. *Elements of Intuitionism*. Oxford University Press, 1977.
- [8] Roy Dyckhoff. Contraction-free sequent calculi for intuitionistic logic. *Journal of Symbolic Logic*, 57(3):795–807, 1992.
- [9] Paul R. Halmos. *Naive Set Theory*. Van Nostrand, 1960.
- [10] Kenneth Kunen. *Set Theory: An Introduction to Independence Proofs*. North-Holland, 1980.
- [11] Philippe Noël. Experimenting with Isabelle in ZF set theory. *Journal of Automated Reasoning*, 10(1):15–58, 1993.
- [12] Christine Paulin-Mohring. Inductive definitions in the system Coq: Rules and properties. In M. Bezem and J.F. Groote, editors, *Typed Lambda Calculi and Applications*, LNCS 664, pages 328–345. Springer, 1993.

- [13] Lawrence C. Paulson. *Logic and Computation: Interactive proof with Cambridge LCF*. Cambridge University Press, 1987.
- [14] Lawrence C. Paulson. Set theory for verification: I. From foundations to functions. *Journal of Automated Reasoning*, 11(3):353–389, 1993.
- [15] 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.
- [16] Lawrence C. Paulson. Set theory for verification: II. Induction and recursion. *Journal of Automated Reasoning*, 15(2):167–215, 1995.
- [17] Lawrence C. Paulson. Generic automatic proof tools. In Robert Veroff, editor, *Automated Reasoning and its Applications: Essays in Honor of Larry Wos*, chapter 3. MIT Press, 1997.
- [18] Lawrence C. Paulson. Final coalgebras as greatest fixed points in ZF set theory. *Mathematical Structures in Computer Science*, 9, 1999. in press.
- [19] Art Quaipe. Automated deduction in von Neumann-Bernays-Gödel set theory. *Journal of Automated Reasoning*, 8(1):91–147, 1992.
- [20] Patrick Suppes. *Axiomatic Set Theory*. Dover, 1972.
- [21] A. N. Whitehead and B. Russell. *Principia Mathematica*. Cambridge University Press, 1962. Paperback edition to *56, abridged from the 2nd edition (1927).
- [22] Glynn Winskel. *The Formal Semantics of Programming Languages*. MIT Press, 1993.

Index

`#*` symbol, 48
`#+` symbol, 48
`#-` symbol, 48
`$*` symbol, 49
`$+` symbol, 49
`$-` symbol, 49
`&` symbol, 5
`*` symbol, 24
`+` symbol, 40
`-` symbol, 23
`-->` symbol, 5
`->` symbol, 24
`-‘` symbol, 23
`:` symbol, 23
`<->` symbol, 5
`<=` symbol, 23
`=` symbol, 5
`‘` symbol, 23
`‘‘` symbol, 23
`|` symbol, 5

0 constant, 23

`add_0_natify` theorem, 48
`add_mult_dist` theorem, 48
`add_succ` theorem, 48
`AddTCs`, 47
`addTCs`, 47
`ALL` symbol, 5, 24
`All` constant, 5
`all_dupE` theorem, 3, 7
`all_impE` theorem, 7
`allE` theorem, 3, 7
`allI` theorem, 6
`and_def` theorem, 40
`apply_def` theorem, 28
`apply_equality` theorem, 37, 69, 70
`apply_equality2` theorem, 37
`apply_iff` theorem, 37
`apply_Pair` theorem, 37, 70
`apply_type` theorem, 37
`Arith` theory, 47
arithmetic, 47–50
assumptions
 contradictory, 14

`Ball` constant, 23, 26
`ball_cong` theorem, 30, 31
`Ball_def` theorem, 27
`ballE` theorem, 30, 31
`ballI` theorem, 30
`beta` theorem, 37, 38
`Bex` constant, 23, 26
`bex_cong` theorem, 30, 31
`Bex_def` theorem, 27
`bexCI` theorem, 30
`bexE` theorem, 30
`bexI` theorem, 30
`bij` constant, 44
`bij_converse_bij` theorem, 44
`bij_def` theorem, 44
`bij_disjoint_Un` theorem, 44
`Blast_tac`, 14, 67–69
`blast_tac`, 16, 18
`bnd_mono_def` theorem, 42
`Bool` theory, 38
`bool_0I` theorem, 40
`bool_1I` theorem, 40
`bool_def` theorem, 40
`boolE` theorem, 40
`bspec` theorem, 30

`case` constant, 40
`case_def` theorem, 40
`case_Inl` theorem, 40

- case_Inr theorem, 40
- coinduct theorem, 42
- coinductive, 58–63
- Collect constant, 23, 24, 29
- Collect_def theorem, 27
- Collect_subset theorem, 34
- CollectD1 theorem, 31, 32
- CollectD2 theorem, 31, 32
- CollectE theorem, 31, 32
- CollectI theorem, 32
- comp_assoc theorem, 44
- comp_bij theorem, 44
- comp_def theorem, 44
- comp_func theorem, 44
- comp_func_apply theorem, 44
- comp_inj theorem, 44
- comp_surj theorem, 44
- comp_type theorem, 44
- cond_0 theorem, 40
- cond_1 theorem, 40
- cond_def theorem, 40
- congruence rules, 31
- conj_cong, 4
- conj_impE theorem, 4, 7
- conjE theorem, 7
- conjI theorem, 6
- conjunct1 theorem, 6
- conjunct2 theorem, 6
- cons constant, 22, 23
- cons_def theorem, 28
- Cons_iff theorem, 43
- consCI theorem, 33
- consE theorem, 33
- ConsI theorem, 43
- consI1 theorem, 33
- consI2 theorem, 33
- converse constant, 23, 36
- converse_def theorem, 28
- cut_facts_tac, 16
- datatype, 50, 50–56
- DelTCs, 47
- delTCs, 47
- Diff_cancel theorem, 39
- Diff_contains theorem, 34
- Diff_def theorem, 27
- Diff_disjoint theorem, 39
- Diff_Int theorem, 39
- Diff_partition theorem, 39
- Diff_subset theorem, 34
- Diff_Un theorem, 39
- DiffD1 theorem, 33
- DiffD2 theorem, 33
- DiffE theorem, 33
- DiffI theorem, 33
- disj_impE theorem, 4, 7, 12
- disjCI theorem, 9
- disjE theorem, 6
- disjI1 theorem, 6
- disjI2 theorem, 6
- div symbol, 48
- domain constant, 23, 36
- domain_def theorem, 28
- domain_of_fun theorem, 37
- domain_subset theorem, 36
- domain_type theorem, 37
- domainE theorem, 36
- domainI theorem, 36
- double_complement theorem, 39
- dresolve_tac, 67
- empty_subsetI theorem, 30
- emptyE theorem, 30
- eq_mp_tac, 8
- equalityD1 theorem, 30
- equalityD2 theorem, 30
- equalityE theorem, 30
- equalityI theorem, 30, 66
- equalsOD theorem, 30
- equalsOI theorem, 30
- eresolve_tac, 13
- eta theorem, 37, 38
- EX symbol, 5, 24
- Ex constant, 5
- EX! symbol, 5
- ex/Term theory, 51
- Ex1 constant, 5
- ex1_def theorem, 6

- ex1E theorem, 7
- ex1I theorem, 7
- ex_impE theorem, 7
- exCI theorem, 9, 13
- excluded_middle theorem, 9
- exE theorem, 6
- exhaust_tac, 54
- exI theorem, 6
- extension theorem, 27
- False constant, 5
- FalseE theorem, 6
- field constant, 23
- field_def theorem, 28
- field_subset theorem, 36
- fieldCI theorem, 36
- fieldE theorem, 36
- fieldI1 theorem, 36
- fieldI2 theorem, 36
- Fin.consI theorem, 43
- Fin.emptyI theorem, 43
- Fin_induct theorem, 43
- Fin_mono theorem, 43
- Fin_subset theorem, 43
- Fin_UnI theorem, 43
- Fin_UnionI theorem, 43
- first-order logic, 3–20
- Fixedpt theory, 41
- flat constant, 43
- FOL theory, 3, 9
- FOL_cs, 9, 46
- FOL_ss, 4, 45
- foundation theorem, 27
- fst constant, 23, 29
- fst_conv theorem, 35
- fst_def theorem, 28
- fun_disjoint_apply1 theorem, 38, 69
- fun_disjoint_apply2 theorem, 38
- fun_disjoint_Un theorem, 38, 70
- fun_empty theorem, 38
- fun_extension theorem, 37, 38
- fun_is_rel theorem, 37
- fun_single theorem, 38
- function applications, 23
- gfp_def theorem, 42
- gfp_least theorem, 42
- gfp_mono theorem, 42
- gfp_subset theorem, 42
- gfp_Tarski theorem, 42
- gfp_upperbound theorem, 42
- Goalw, 15, 16
- hyp_subst_tac, 4
- i* type, 22
- id constant, 44
- id_def theorem, 44
- if constant, 23
- if_def theorem, 15, 27
- if_not_P theorem, 33
- if_P theorem, 33
- ifE theorem, 17
- iff_def theorem, 6
- iff_impE theorem, 7
- iffCE theorem, 9
- iffD1 theorem, 7
- iffD2 theorem, 7
- iffE theorem, 7
- iffI theorem, 7, 17
- ifI theorem, 17
- IFOL theory, 3
- IFOL_ss, 4
- image_def theorem, 28
- imageE theorem, 36
- imageI theorem, 36
- imp_impE theorem, 7, 12
- impCE theorem, 9
- impE theorem, 7, 8
- impI theorem, 6
- in symbol, 25
- induct theorem, 42
- induct_tac, 53
- inductive, 58–63
- Inf constant, 23, 29
- infinity theorem, 28
- inj constant, 44

- `inj_converse_inj` theorem, 44
- `inj_def` theorem, 44
- `Inl` constant, 40
- `Inl_def` theorem, 40
- `Inl_inject` theorem, 40
- `Inl_neq_Inr` theorem, 40
- `Inr` constant, 40
- `Inr_def` theorem, 40
- `Inr_inject` theorem, 40
- `INT` symbol, 24, 26
- `Int` symbol, 23
- `Int` theory, 49
- `int` constant, 49
- `Int_absorb` theorem, 39
- `Int_assoc` theorem, 39
- `Int_commute` theorem, 39
- `Int_def` theorem, 27
- `INT_E` theorem, 32
- `Int_greatest` theorem, 34, 66, 67
- `INT_I` theorem, 32
- `Int_lower1` theorem, 34, 66
- `Int_lower2` theorem, 34, 66
- `Int_Un_distrib` theorem, 39
- `Int_Union_RepFun` theorem, 39
- `IntD1` theorem, 33
- `IntD2` theorem, 33
- `IntE` theorem, 33, 66
- integers, 49
- `Inter` constant, 23
- `Inter_def` theorem, 27
- `Inter_greatest` theorem, 34
- `Inter_lower` theorem, 34
- `Inter_Un_distrib` theorem, 39
- `InterD` theorem, 32
- `InterE` theorem, 32
- `InterI` theorem, 31, 32
- `IntI` theorem, 33
- `intify` constant, 49
- `IntPr.best_tac`, 8
- `IntPr.fast_tac`, 8, 11
- `IntPr.inst_step_tac`, 8
- `IntPr.safe_step_tac`, 8
- `IntPr.safe_tac`, 8
- `IntPr.step_tac`, 8
- `lam` symbol, 24, 26
- `lam_def` theorem, 28
- `lam_type` theorem, 37
- `Lambda` constant, 23, 26
- λ -abstractions, 24
- `lamE` theorem, 37, 38
- `lamI` theorem, 37, 38
- `le_cs`, 45
- `left_comp_id` theorem, 44
- `left_comp_inverse` theorem, 44
- `left_inverse` theorem, 44
- `length` constant, 43
- `Let` constant, 22, 23
- `let` symbol, 25
- `Let_def` theorem, 22, 27
- `lfp_def` theorem, 42
- `lfp_greatest` theorem, 42
- `lfp_lowerbound` theorem, 42
- `lfp_mono` theorem, 42
- `lfp_subset` theorem, 42
- `lfp_Tarski` theorem, 42
- `list` constant, 43
- `List.induct` theorem, 43
- `list_case` constant, 43
- `list_mono` theorem, 43
- logic class, 3
- `map` constant, 43
- `map_app_distrib` theorem, 43
- `map_compose` theorem, 43
- `map_flat` theorem, 43
- `map_ident` theorem, 43
- `map_type` theorem, 43
- `mem_asym` theorem, 33, 34
- `mem_irrefl` theorem, 33
- `mk_cases`, 55, 62
- `mod` symbol, 48
- `mod_div_equality` theorem, 48
- `mp` theorem, 6
- `mp_tac`, 8
- `mult_0` theorem, 48
- `mult_assoc` theorem, 48
- `mult_commute` theorem, 48
- `mult_succ` theorem, 48

- mult_type theorem, 48
- Nat theory, 47
- nat constant, 48
- nat_OI theorem, 48
- nat_case constant, 48
- nat_case_0 theorem, 48
- nat_case_def theorem, 48
- nat_case_succ theorem, 48
- nat_def theorem, 48
- nat_induct theorem, 48
- nat_succI theorem, 48
- natify constant, 47, 49
- natural numbers, 47
- Nil_Cons_iff theorem, 43
- NilI theorem, 43
- Not constant, 5
- not_def theorem, 6, 40
- not_impE theorem, 7
- notE theorem, 7, 8
- notI theorem, 7
- notnotD theorem, 9
- 0 symbol, 44
- o type, 3
- or_def theorem, 40
- Pair constant, 23, 24
- Pair_def theorem, 28
- Pair_inject theorem, 35
- Pair_inject1 theorem, 35
- Pair_inject2 theorem, 35
- Pair_neq_0 theorem, 35
- pairing theorem, 32
- Perm theory, 45
- Pi constant, 23, 26, 37
- Pi_def theorem, 28
- Pi_type theorem, 37, 38
- Pow constant, 23
- Pow_iff theorem, 27
- Pow_mono theorem, 66
- PowD theorem, 30, 67
- PowI theorem, 30, 66
- primrec, 57, 56–58
- PrimReplace constant, 23, 29
- priorities, 1
- PROD symbol, 24, 26
- prop_cs, 9
- qcase_def theorem, 40
- qconverse constant, 41
- qconverse_def theorem, 40
- qed_spec_mp, 55
- qfsplit_def theorem, 40
- QInl_def theorem, 40
- QInr_def theorem, 40
- QPair theory, 41
- QPair_def theorem, 40
- QSigma constant, 41
- QSigma_def theorem, 40
- qsplit constant, 41
- qsplit_def theorem, 40
- qsum_def theorem, 40
- QUniv theory, 45
- range constant, 23
- range_def theorem, 28
- range_of_fun theorem, 37, 38
- range_subset theorem, 36
- range_type theorem, 37
- rangeE theorem, 36
- rangeI theorem, 36
- rank constant, 63
- recursion
 - primitive, 56–58
- recursive functions, *see* recursion
- refl theorem, 6
- RepFun constant, 23, 26, 29, 31
- RepFun_def theorem, 27
- RepFunE theorem, 32
- RepFunI theorem, 32
- Replace constant, 23, 24, 29, 31
- Replace_def theorem, 27
- ReplaceE theorem, 32
- ReplaceI theorem, 32
- replacement theorem, 27
- restrict constant, 23, 29
- restrict theorem, 37
- restrict_bij theorem, 44

- restrict_def theorem, 28
- restrict_type theorem, 37
- rev constant, 43
- rew_tac, 16
- rewrite_rule, 16
- right_comp_id theorem, 44
- right_comp_inverse theorem, 44
- right_inverse theorem, 44
- separation theorem, 32
- set theory, 21–71
- Sigma constant, 23, 26, 29, 35
- Sigma_def theorem, 28
- SigmaE theorem, 35
- SigmaE2 theorem, 35
- SigmaI theorem, 35
- simplification
 - of conjunctions, 4
- singletonE theorem, 33
- singletonI theorem, 33
- snd constant, 23, 29
- snd_conv theorem, 35
- snd_def theorem, 28
- spec theorem, 6
- split constant, 23, 29
- split theorem, 35
- split_def theorem, 28
- ssubst theorem, 7
- Step_tac, 19
- step_tac, 20
- subset_def theorem, 27
- subset_refl theorem, 30
- subset_trans theorem, 30
- subsetCE theorem, 30
- subsetD theorem, 30, 68
- subsetI theorem, 30, 66, 67
- subst theorem, 6
- succ constant, 23, 29
- succ_def theorem, 28
- succ_inject theorem, 33
- succ_neq_0 theorem, 33
- succCI theorem, 33
- succE theorem, 33
- succI1 theorem, 33
- succI2 theorem, 33
- SUM symbol, 24, 26
- Sum theory, 38
- sum_def theorem, 40
- sum_InlI theorem, 40
- sum_InrI theorem, 40
- SUM_Int_distrib1 theorem, 39
- SUM_Int_distrib2 theorem, 39
- SUM_Un_distrib1 theorem, 39
- SUM_Un_distrib2 theorem, 39
- sumE2 theorem, 40
- surj constant, 44
- surj_def theorem, 44
- swap theorem, 9
- swap_res_tac, 13
- sym theorem, 7
- tcset, 47
- term class, 3
- THE symbol, 24, 26, 34
- The constant, 23, 26, 29
- the_def theorem, 27
- the_equality theorem, 33, 34
- theI theorem, 33, 34
- trace_induct, 60
- trans theorem, 7
- True constant, 5
- True_def theorem, 6
- TrueI theorem, 7
- Trueprop constant, 5
- type-checking tactics, 46
- type_solver_tac, 47
- Typecheck_tac, 46, 47
- typecheck_tac, 47
- UN symbol, 24, 26
- Un symbol, 23
- Un_absorb theorem, 39
- Un_assoc theorem, 39
- Un_commute theorem, 39
- Un_def theorem, 27
- UN_E theorem, 32
- UN_I theorem, 32
- Un_Int_distrib theorem, 39

Un_Inter_RepFun theorem, 39
 Un_least theorem, 34
 Un_upper1 theorem, 34
 Un_upper2 theorem, 34
 UnCI theorem, 31, 33
 UnE theorem, 33
 UnI1 theorem, 31, 33, 69
 UnI2 theorem, 31, 33
 Union constant, 23
 Union_iff theorem, 27
 Union_least theorem, 34
 Union_Un_distrib theorem, 39
 Union_upper theorem, 34
 UnionE theorem, 32, 68
 UnionI theorem, 32, 68
 Univ theory, 45
 Upair constant, 22, 23, 29
 Upair_def theorem, 27
 UpairE theorem, 32
 UpairI1 theorem, 32
 UpairI2 theorem, 32

 vimage_def theorem, 28
 vimageE theorem, 36
 vimageI theorem, 36

 xor_def theorem, 40

 zadd_0_intify theorem, 49
 zadd_zmult_dist theorem, 49
 ZF theory, 21
 ZF_cs, 45
 ZF_ss, 45
 zmult_0 theorem, 49
 zmult_assoc theorem, 49
 zmult_commute theorem, 49
 zmult_type theorem, 49