# Old Isabelle Reference Manual

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

With Contributions by Tobias Nipkow and Markus Wenzel

22 May 2012

*Note*: this document is part of the earlier Isabelle documentation and is mostly outdated. Fully obsolete parts of the original text have already been removed. The remaining material covers some aspects that did not make it into the newer manuals yet.

## Acknowledgements

Tobias Nipkow, of T. U. Munich, wrote most of Chapters **??** and 5. Markus Wenzel contributed to Chapter 3. Jeremy Dawson, Sara Kalvala, Martin Simons and others suggested changes and corrections. The research has been funded by the EPSRC (grants GR/G53279, GR/H40570, GR/K57381, GR/K77051, GR/M75440) and by ESPRIT (projects 3245: Logical Frameworks, and 6453: Types), and by the DFG Schwerpunktprogramm *Deduktion*.

# Contents

Chapter 1

# Tactics

## 1.1 Other basic tactics

### 1.1.1 Inserting premises and facts

```
cut_facts_tac : thm list -> int -> tactic
```

These tactics add assumptions to a subgoal.

`cut_facts_tac` *thms* $i$ adds the *thms* as new assumptions to subgoal $i$. Once they have been inserted as assumptions, they become subject to tactics such as `eresolve_tac` and `rewrite_goals_tac`. Only rules with no premises are inserted: Isabelle cannot use assumptions that contain $\Longrightarrow$ or $\bigwedge$. Sometimes the theorems are premises of a rule being derived, returned by `goal`; instead of calling this tactic, you could state the goal with an outermost meta-quantifier.

### 1.1.2 Composition: resolution without lifting

```
compose_tac: (bool * thm * int) -> int -> tactic
```

**Composing** two rules means resolving them without prior lifting or renaming of unknowns. This low-level operation, which underlies the resolution tactics, may occasionally be useful for special effects. A typical application is `res_inst_tac`, which lifts and instantiates a rule, then passes the result to `compose_tac`.

`compose_tac (`*flag*`,` *rule*`,` $m$`)` $i$ refines subgoal $i$ using *rule*, without lifting. The *rule* is taken to have the form $[\![\psi_1; \ldots; \psi_m]\!] \Longrightarrow \psi$, where $\psi$ need not be atomic; thus $m$ determines the number of new subgoals. If *flag* is `true` then it performs elim-resolution — it solves the first premise of *rule* by assumption and deletes that assumption.

## 1.2 *Managing lots of rules

These operations are not intended for interactive use. They are concerned with the processing of large numbers of rules in automatic proof strategies. Higher-order resolution involving a long list of rules is slow. Filtering techniques can shorten the list of rules given to resolution, and can also detect whether a subgoal is too flexible, with too many rules applicable.

### 1.2.1 Combined resolution and elim-resolution

```
biresolve_tac   : (bool*thm)list -> int -> tactic
bimatch_tac     : (bool*thm)list -> int -> tactic
subgoals_of_brl : bool*thm -> int
lessb           : (bool*thm) * (bool*thm) -> bool
```

**Bi-resolution** takes a list of $(\mathit{flag}, \mathit{rule})$ pairs. For each pair, it applies resolution if the flag is `false` and elim-resolution if the flag is `true`. A single tactic call handles a mixture of introduction and elimination rules.

`biresolve_tac` *brls* $i$ refines the proof state by resolution or elim-resolution on each rule, as indicated by its flag. It affects subgoal $i$ of the proof state.

`bimatch_tac` is like `biresolve_tac`, but performs matching: unknowns in the proof state are never updated (see §**??**).

`subgoals_of_brl(`*flag*`,`*rule*`)` returns the number of new subgoals that bi-resolution would yield for the pair (if applied to a suitable subgoal). This is $n$ if the flag is `false` and $n-1$ if the flag is `true`, where $n$ is the number of premises of the rule. Elim-resolution yields one fewer subgoal than ordinary resolution because it solves the major premise by assumption.

`lessb (`*brl1*`,`*brl2*`)` returns the result of

`subgoals_of_brl` *brl1* `<` `subgoals_of_brl` *brl2*

Note that `sort lessb` *brls* sorts a list of $(\mathit{flag}, \mathit{rule})$ pairs by the number of new subgoals they will yield. Thus, those that yield the fewest subgoals should be tried first.

### 1.2.2 Discrimination nets for fast resolution

```
net_resolve_tac  : thm list -> int -> tactic
net_match_tac    : thm list -> int -> tactic
net_biresolve_tac: (bool*thm) list -> int -> tactic
net_bimatch_tac  : (bool*thm) list -> int -> tactic
filt_resolve_tac : thm list -> int -> int -> tactic
could_unify      : term*term->bool
filter_thms      : (term*term->bool) -> int*term*thm list -> thm list
```

The module `Net` implements a discrimination net data structure for fast selection of rules [3, Chapter 14]. A term is classified by the symbol list obtained by flattening it in preorder. The flattening takes account of function applications, constants, and free and bound variables; it identifies all unknowns and also regards $\lambda$-abstractions as unknowns, since they could $\eta$-contract to anything.

A discrimination net serves as a polymorphic dictionary indexed by terms. The module provides various functions for inserting and removing items from nets. It provides functions for returning all items whose term could match or unify with a target term. The matching and unification tests are overly lax (due to the identifications mentioned above) but they serve as useful filters.

A net can store introduction rules indexed by their conclusion, and elimination rules indexed by their major premise. Isabelle provides several functions for 'compiling' long lists of rules into fast resolution tactics. When supplied with a list of theorems, these functions build a discrimination net; the net is used when the tactic is applied to a goal. To avoid repeatedly constructing the nets, use currying: bind the resulting tactics to ML identifiers.

`net_resolve_tac` *thms* builds a discrimination net to obtain the effect of a similar call to `resolve_tac`.

`net_match_tac` *thms* builds a discrimination net to obtain the effect of a similar call to `match_tac`.

`net_biresolve_tac` *brls* builds a discrimination net to obtain the effect of a similar call to `biresolve_tac`.

`net_bimatch_tac` *brls* builds a discrimination net to obtain the effect of a similar call to `bimatch_tac`.

`filt_resolve_tac` *thms maxr i* uses discrimination nets to extract the *thms* that are applicable to subgoal $i$. If more than *maxr* theorems are applicable then the tactic fails. Otherwise it calls `resolve_tac`.

This tactic helps avoid runaway instantiation of unknowns, for example in type inference.

`could_unify` `(`$t$`,`$u$`)` returns `false` if $t$ and $u$ are 'obviously' non-unifiable, and otherwise returns `true`. It assumes all variables are distinct, reporting that `?a=?a` may unify with `0=1`.

`filter_thms` *could* ($limit$, $prem$, $thms$) returns the list of potentially resolvable rules (in *thms*) for the subgoal *prem*, using the predicate *could* to compare the conclusion of the subgoal with the conclusion of each rule. The resulting list is no longer than *limit*.

Chapter 2

# Theorems and Forward Proof

Theorems, which represent the axioms, theorems and rules of object-logics, have type `thm`. This chapter describes operations that join theorems in forward proof. Most theorem operations are intended for advanced applications, such as programming new proof procedures.

### 2.0.3 Instantiating unknowns in a theorem

```
read_instantiate    :                (string*string) list -> thm -> thm
read_instantiate_sg :     Sign.sg -> (string*string) list -> thm -> thm
cterm_instantiate   :                  (cterm*cterm) list -> thm -> thm
instantiate'      : ctyp option list -> cterm option list -> thm -> thm
```

These meta-rules instantiate type and term unknowns in a theorem. They are occasionally useful. They can prevent difficulties with higher-order unification, and define specialized versions of rules.

`read_instantiate` *insts thm* processes the instantiations *insts* and instantiates the rule *thm*. The processing of instantiations is described in §**??**, under `res_inst_tac`.

Use `res_inst_tac`, not `read_instantiate`, to instantiate a rule and refine a particular subgoal. The tactic allows instantiation by the subgoal's parameters, and reads the instantiations using the signature associated with the proof state.

Use `read_instantiate_sg` below if *insts* appears to be treated incorrectly.

`read_instantiate_sg` *sg insts thm* is like `read_instantiate` *insts thm*, but it reads the instantiations under signature *sg*. This is necessary to instantiate a rule from a general theory, such as first-order logic, using the notation of some specialized theory. Use the function `sign_of` to get a theory's signature.

`cterm_instantiate` *ctpairs thm* is similar to `read_instantiate`, but the instantiations are provided as pairs of certified terms, not as strings to be read.

`instantiate'` *ctyps cterms thm* instantiates *thm* according to the positional arguments *ctyps* and *cterms*. Counting from left to right, schematic variables $?x$ are either replaced by $t$ for any argument `Some` $t$, or left unchanged in case of `None` or if the end of the argument list is encountered. Types are instantiated before terms.

### 2.0.4 Miscellaneous forward rules

```
standard          :                thm -> thm
zero_var_indexes  :                thm -> thm
make_elim         :                thm -> thm
rule_by_tactic    :      tactic -> thm -> thm
rotate_prems      :         int -> thm -> thm
permute_prems     : int -> int -> thm -> thm
rearrange_prems   :   int list -> thm -> thm
```

`standard` *thm* puts *thm* into the standard form of object-rules. It discharges all meta-assumptions, replaces free variables by schematic variables, renames schematic variables to have subscript zero, also strips outer (meta) quantifiers and removes dangling sort hypotheses.

`zero_var_indexes` *thm* makes all schematic variables have subscript zero, renaming them to avoid clashes.

`make_elim` *thm* converts *thm*, which should be a destruction rule of the form $[\![P_1;\ldots;P_m]\!] \Longrightarrow Q$, to the elimination rule $[\![P_1;\ldots;P_m; Q \Longrightarrow R]\!] \Longrightarrow R$. This is the basis for destruct-resolution: `dresolve_tac`, etc.

`rule_by_tactic` *tac thm* applies *tac* to the *thm*, freezing its variables first, then yields the proof state returned by the tactic. In typical usage, the *thm* represents an instance of a rule with several premises, some with contradictory assumptions (because of the instantiation). The tactic proves those subgoals and does whatever else it can, and returns whatever is left.

`rotate_prems` $k$ *thm* rotates the premises of *thm* to the left by $k$ positions (to the right if $k < 0$). It simply calls `permute_prems`, below, with $j = 0$. Used with `eresolve_tac`, it gives the effect of applying the tactic to some other premise of *thm* than the first.

`permute_prems` $j$ $k$ *thm* rotates the premises of *thm* leaving the first $j$ premises unchanged. It requires $0 \leq j \leq n$, where $n$ is the number of premises. If $k$ is positive then it rotates the remaining $n - j$ premises to the left; if $k$ is negative then it rotates the premises to the right.

`rearrange_prems` *ps thm* permutes the premises of *thm* where the value at the *i*-th position (counting from 0) in the list *ps* gives the position within the original thm to be transferred to position *i*. Any remaining trailing positions are left unchanged.

### 2.0.5 Taking a theorem apart

```
cprop_of      : thm -> cterm
concl_of      : thm -> term
prems_of      : thm -> term list
cprems_of     : thm -> cterm list
nprems_of     : thm -> int
tpairs_of     : thm -> (term*term) list
theory_of_thm : thm -> theory
```

`cprop_of` *thm* returns the statement of *thm* as a certified term.

`concl_of` *thm* returns the conclusion of *thm* as a term.

`prems_of` *thm* returns the premises of *thm* as a list of terms.

`cprems_of` *thm* returns the premises of *thm* as a list of certified terms.

`nprems_of` *thm* returns the number of premises in *thm*, and is equivalent to `length (prems_of` *thm*`)`.

`tpairs_of` *thm* returns the flex-flex constraints of *thm*.

`theory_of_thm` *thm* returns the theory associated with *thm*. Note that this does a lookup in Isabelle's global database of loaded theories.

### 2.0.6 *Sort hypotheses

```
strip_shyps         : thm -> thm
strip_shyps_warning : thm -> thm
```

Isabelle's type variables are decorated with sorts, constraining them to certain ranges of types. This has little impact when sorts only serve for syntactic classification of types — for example, FOL distinguishes between terms and other types. But when type classes are introduced through axioms, this may result in some sorts becoming *empty*: where one cannot exhibit a type belonging to it because certain sets of axioms are unsatisfiable.

If a theorem contains a type variable that is constrained by an empty sort, then that theorem has no instances. It is basically an instance of *ex falso quodlibet*. But what if it is used to prove another theorem that no longer involves that sort? The latter theorem holds only if under an additional non-emptiness assumption.

Therefore, Isabelle's theorems carry around sort hypotheses. The `shyps` field is a list of sorts occurring in type variables in the current `prop` and `hyps` fields. It may also includes sorts used in the theorem's proof that no longer appear in the `prop` or `hyps` fields — so-called *dangling* sort constraints. These are the critical ones, asserting non-emptiness of the corresponding sorts.

Isabelle automatically removes extraneous sorts from the `shyps` field at the end of a proof, provided that non-emptiness can be established by looking at the theorem's signature: from the `classes` and `arities` information. This operation is performed by `strip_shyps` and `strip_shyps_warning`.

`strip_shyps` *thm* removes any extraneous sort hypotheses that can be witnessed from the type signature.

`strip_shyps_warning` is like `strip_shyps`, but issues a warning message of any pending sort hypotheses that do not have a (syntactic) witness.

### 2.0.7 Tracing flags for unification

```
Unify.trace_simp   : bool ref                         initially false
Unify.trace_types  : bool ref                         initially false
Unify.trace_bound  : int ref                             initially 10
Unify.search_bound : int ref                             initially 20
```

Tracing the search may be useful when higher-order unification behaves unexpectedly. Letting `res_inst_tac` circumvent the problem is easier, though.

`set Unify.trace_simp;` causes tracing of the simplification phase.

`set Unify.trace_types;` generates warnings of incompleteness, when unification is not considering all possible instantiations of type unknowns.

`Unify.trace_bound :=` $n$`;` causes unification to print tracing information once it reaches depth $n$. Use $n = 0$ for full tracing. At the default value of 10, tracing information is almost never printed.

`Unify.search_bound :=` $n$`;` prevents unification from searching past the depth $n$. Because of this bound, higher-order unification cannot return an infinite sequence, though it can return an exponentially long one. The search rarely approaches the default value of 20. If the search is cut off, unification prints a warning `Unification bound exceeded`.

## 2.1 *Primitive meta-level inference rules

### 2.1.1 Logical equivalence rules

```
equal_intr : thm -> thm -> thm
equal_elim : thm -> thm -> thm
```

`equal_intr` *thm*$_1$ *thm*$_2$ applies ($\equiv I$) to *thm*$_1$ and *thm*$_2$. It maps the premises $\psi$ and $\phi$ to the conclusion $\phi \equiv \psi$; the assumptions are those of the first premise with $\phi$ removed, plus those of the second premise with $\psi$ removed.

`equal_elim` *thm*$_1$ *thm*$_2$ applies ($\equiv E$) to *thm*$_1$ and *thm*$_2$. It maps the premises $\phi \equiv \psi$ and $\phi$ to the conclusion $\psi$.

### 2.1.2 Equality rules

```
reflexive  : cterm -> thm
symmetric  : thm -> thm
transitive : thm -> thm -> thm
```

`reflexive` *ct* makes the theorem $ct \equiv ct$.

`symmetric` *thm* maps the premise $a \equiv b$ to the conclusion $b \equiv a$.

`transitive` *thm*$_1$ *thm*$_2$ maps the premises $a \equiv b$ and $b \equiv c$ to the conclusion $a \equiv c$.

### 2.1.3 The $\lambda$-conversion rules

```
beta_conversion : cterm -> thm
extensional     : thm -> thm
abstract_rule   : string -> cterm -> thm -> thm
combination     : thm -> thm -> thm
```

There is no rule for $\alpha$-conversion because Isabelle regards $\alpha$-convertible theorems as equal.

`beta_conversion` *ct* makes the theorem $((\lambda x \,.\, a)(b)) \equiv a[b/x]$, where *ct* is the term $(\lambda x \,.\, a)(b)$.

`extensional` *thm* maps the premise $f(x) \equiv g(x)$ to the conclusion $f \equiv g$. Parameter $x$ is taken from the premise. It may be an unknown or a free variable (provided it does not occur in the assumptions); it must not occur in $f$ or $g$.

`abstract_rule` *v x thm* maps the premise $a \equiv b$ to the conclusion $(\lambda x\ .\ a) \equiv (\lambda x\ .\ b)$, abstracting over all occurrences (if any!) of $x$. Parameter $x$ is supplied as a cterm. It may be an unknown or a free variable (provided it does not occur in the assumptions). In the conclusion, the bound variable is named $v$.

`combination` $thm_1$ $thm_2$ maps the premises $f \equiv g$ and $a \equiv b$ to the conclusion $f(a) \equiv g(b)$.

## 2.2 Derived rules for goal-directed proof

Most of these rules have the sole purpose of implementing particular tactics. There are few occasions for applying them directly to a theorem.

### 2.2.1 Resolution

```
biresolution : bool -> (bool*thm)list -> int -> thm
               -> thm Seq.seq
```

`biresolution` *match rules i state* performs bi-resolution on subgoal $i$ of *state*, using the list of (*flag*, *rule*) pairs. For each pair, it applies resolution if the flag is `false` and elim-resolution if the flag is `true`. If *match* is `true`, the *state* is not instantiated.

### 2.2.2 Composition: resolution without lifting

```
compose   : thm * int * thm -> thm list
COMP      : thm * thm -> thm
bicompose : bool -> bool * thm * int -> int -> thm
            -> thm Seq.seq
```

In forward proof, a typical use of composition is to regard an assertion of the form $\phi \Longrightarrow \psi$ as atomic. Schematic variables are not renamed, so beware of clashes!

`compose` `(`$thm_1$`,` $i$`,` $thm_2$`)` uses $thm_1$, regarded as an atomic formula, to solve premise $i$ of $thm_2$. Let $thm_1$ and $thm_2$ be $\psi$ and $[\![\phi_1; \ldots; \phi_n]\!] \Longrightarrow \phi$. For each $s$ that unifies $\psi$ and $\phi_i$, the result list contains the theorem

$$([\![\phi_1; \ldots; \phi_{i-1}; \phi_{i+1}; \ldots; \phi_n]\!] \Longrightarrow \phi)s.$$

*thm*$_1$ `COMP` *thm*$_2$ calls `compose (`*thm*$_1$`, 1, `*thm*$_2$`)` and returns the result, if unique; otherwise, it raises exception `THM`. It is analogous to `RS`.

For example, suppose that *thm*$_1$ is $a = b \Longrightarrow b = a$, a symmetry rule, and that *thm*$_2$ is $[\![P \Longrightarrow Q; \neg Q]\!] \Longrightarrow \neg P$, which is the principle of contrapositives. Then the result would be the derived rule $\neg(b = a) \Longrightarrow \neg(a = b)$.

`bicompose` *match* `(`*flag*`, `*rule*`, `*m*`)` *i* *state* refines subgoal $i$ of *state* using *rule*, without lifting. The *rule* is taken to have the form $[\![\psi_1; \ldots; \psi_m]\!] \Longrightarrow \psi$, where $\psi$ need not be atomic; thus $m$ determines the number of new subgoals. If *flag* is `true` then it performs elim-resolution — it solves the first premise of *rule* by assumption and deletes that assumption. If *match* is `true`, the *state* is not instantiated.

### 2.2.3 Other meta-rules

```
rename_params_rule : string list * int -> thm -> thm
```

`rename_params_rule (`*names*`, `*i*`)` *thm* uses the *names* to rename the parameters of premise $i$ of *thm*. The names must be distinct. If there are fewer names than parameters, then the rule renames the innermost parameters and may modify the remaining ones to ensure that all the parameters are distinct.

## 2.3 Proof terms

Isabelle can record the full meta-level proof of each theorem. The proof term contains all logical inferences in detail. Resolution and rewriting steps are broken down to primitive rules of the meta-logic. The proof term can be inspected by a separate proof-checker, for example.

According to the well-known *Curry-Howard isomorphism*, a proof can be viewed as a $\lambda$-term. Following this idea, proofs in Isabelle are internally represented by a datatype similar to the one for terms described in §??.

```
infix 8 % %%;

datatype proof =
   PBound of int
 | Abst of string * typ option * proof
 | AbsP of string * term option * proof
 | op % of proof * term option
 | op %% of proof * proof
 | Hyp of term
 | PThm of (string * (string * string list) list) *
           proof * term * typ list option
 | PAxm of string * term * typ list option
 | Oracle of string * term * typ list option
 | MinProof of proof list;
```

`Abst` `(`$a$`,` $\tau$`,` *prf*`)` is the abstraction over a *term variable* of type $\tau$ in the body *prf*. Logically, this corresponds to $\bigwedge$ introduction. The name $a$ is used only for parsing and printing.

`AbsP` `(`$a$`,` $\varphi$`,` *prf*`)` is the abstraction over a *proof variable* standing for a proof of proposition $\varphi$ in the body *prf*. This corresponds to $\Longrightarrow$ introduction.

*prf* `%` $t$ is the application of proof *prf* to term $t$ which corresponds to $\bigwedge$ elimination.

$prf_1$ `%%` $prf_2$ is the application of proof $prf_1$ to proof $prf_2$ which corresponds to $\Longrightarrow$ elimination.

`PBound` $i$ is a *proof variable* with de Bruijn [4] index $i$.

`Hyp` $\varphi$ corresponds to the use of a meta level hypothesis $\varphi$.

`PThm` `((`*name*`,` *tags*`),` *prf*`,` $\varphi$`,` $\overline{\tau}$`)` stands for a pre-proved theorem, where *name* is the name of the theorem, *prf* is its actual proof, $\varphi$ is the proven proposition, and $\overline{\tau}$ is a type assignment for the type variables occurring in the proposition.

`PAxm` `(`*name*`,` $\varphi$`,` $\overline{\tau}$`)` corresponds to the use of an axiom with name *name* and proposition $\varphi$, where $\overline{\tau}$ is a type assignment for the type variables occurring in the proposition.

`Oracle` `(`*name*`,` $\varphi$`,` $\overline{\tau}$`)` denotes the invocation of an oracle with name *name* which produced a proposition $\varphi$, where $\overline{\tau}$ is a type assignment for the type variables occurring in the proposition.

`MinProof` *prfs* represents a *minimal proof* where *prfs* is a list of theorems, axioms or oracles.

Note that there are no separate constructors for abstraction and application on the level of *types*, since instantiation of type variables is accomplished via the type assignments attached to `Thm`, `Axm` and `Oracle`.

Each theorem's derivation is stored as the `der` field of its internal record:

```
#2 (#der (rep_thm conjI));
  PThm (("HOL.conjI", []),
    AbsP ("H", None, AbsP ("H", None, ...)), ..., None) %
      None % None : Proofterm.proof
```

This proof term identifies a labelled theorem, `conjI` of theory `HOL`, whose underlying proof is `AbsP ("H", None, AbsP ("H", None, ...))`. The theorem is applied to two (implicit) term arguments, which correspond to the two variables occurring in its proposition.

Isabelle's inference kernel can produce proof objects with different levels of detail. This is controlled via the global reference variable `proofs`:

`proofs := 0;` only record uses of oracles

`proofs := 1;` record uses of oracles as well as dependencies on other theorems and axioms

`proofs := 2;` record inferences in full detail

Reconstruction and checking of proofs as described in §2.3.1 will not work for proofs constructed with `proofs` set to `0` or `1`. Theorems involving oracles will be printed with a suffixed `[!]` to point out the different quality of confidence achieved.

The dependencies of theorems can be viewed using the function `thm_deps`:

```
thm_deps [thm₁, ..., thmₙ];
```

generates the dependency graph of the theorems *thm*$_1$, …, *thm*$_n$ and displays it using Isabelle's graph browser. For this to work properly, the theorems in question have to be proved with `proofs` set to a value greater than `0`. You can use

```
ThmDeps.enable : unit -> unit
ThmDeps.disable : unit -> unit
```

to set `proofs` appropriately.

### 2.3.1 Reconstructing and checking proof terms

When looking at the above datatype of proofs more closely, one notices that some arguments of constructors are *optional.* The reason for this is that keeping a full proof term for each theorem would result in enormous memory requirements. Fortunately, typical proof terms usually contain quite a lot of redundant information that can be reconstructed from the context. Therefore, Isabelle's inference kernel creates only *partial* (or *implicit*) proof terms, in which all typing information in terms, all term and type labels of abstractions `AbsP` and `Abst`, and (if possible) some argument terms of `%` are omitted. The following functions are available for reconstructing and checking proof terms:

```
Reconstruct.reconstruct_proof :
  Sign.sg -> term -> Proofterm.proof -> Proofterm.proof
Reconstruct.expand_proof :
  Sign.sg -> string list -> Proofterm.proof -> Proofterm.proof
ProofChecker.thm_of_proof : theory -> Proofterm.proof -> thm
```

`Reconstruct.reconstruct_proof` *sg t prf* turns the partial proof *prf* into a full proof of the proposition denoted by $t$, with respect to signature *sg*. Reconstruction will fail with an error message if *prf* is not a proof of $t$, is ill-formed, or does not contain sufficient information for reconstruction by *higher order pattern unification* [6, 1]. The latter may only happen for proofs built up "by hand" but not for those produced automatically by Isabelle's inference kernel.

`Reconstruct.expand_proof` *sg* `[`$name_1$`,` ...`,` $name_n$`]` *prf* expands and reconstructs the proofs of all theorems with names $name_1$, ..., $name_n$ in the (full) proof *prf*.

`ProofChecker.thm_of_proof` *thy prf* turns the (full) proof *prf* into a theorem with respect to theory *thy* by replaying it using only primitive rules from Isabelle's inference kernel.

### 2.3.2 Parsing and printing proof terms

Isabelle offers several functions for parsing and printing proof terms. The concrete syntax for proof terms is described in Fig. 2.1. Implicit term arguments in partial proofs are indicated by "`_`". Type arguments for theorems and axioms may be specified using `%` or "·" with an argument of the form `TYPE(`*type*`)` (see §**??**). They must appear before any other term argument of a theorem or axiom. In contrast to term arguments, type arguments may be completely omitted.

$$\begin{array}{rcl}
\mathit{proof} & = & \texttt{Lam}\ \mathit{params}\,.\ \mathit{proof} \quad\mid\quad \Lambda \mathit{params}\,.\ \mathit{proof} \\
& \mid & \mathit{proof}\ \%\ \mathit{any} \quad\mid\quad \mathit{proof} \cdot \mathit{any} \\
& \mid & \mathit{proof}\ \%\%\ \mathit{proof} \quad\mid\quad \mathit{proof} \bullet \mathit{proof} \\
& \mid & \mathit{id} \quad\mid\quad \mathit{longid} \\
\\
\mathit{param} & = & \mathit{idt} \quad\mid\quad \mathit{idt}\ \texttt{:}\ \mathit{prop} \quad\mid\quad \texttt{(}\ \mathit{param}\ \texttt{)} \\
\\
\mathit{params} & = & \mathit{param} \quad\mid\quad \mathit{param}\ \mathit{params}
\end{array}$$

Figure 2.1: Proof term syntax

```
ProofSyntax.read_proof : theory -> bool -> string -> Proofterm.proof
ProofSyntax.pretty_proof : Sign.sg -> Proofterm.proof -> Pretty.T
ProofSyntax.pretty_proof_of : bool -> thm -> Pretty.T
ProofSyntax.print_proof_of : bool -> thm -> unit
```

The function `read_proof` reads in a proof term with respect to a given theory. The boolean flag indicates whether the proof term to be parsed contains explicit typing information to be taken into account. Usually, typing information is left implicit and is inferred during proof reconstruction. The pretty printing functions operating on theorems take a boolean flag as an argument which indicates whether the proof term should be reconstructed before printing.

The following example (based on Isabelle/HOL) illustrates how to parse and check proof terms. We start by parsing a partial proof term

```
val prf = ProofSyntax.read_proof Main.thy false
  "impI % _ % _ %% (Lam H : _. conjE % _ % _ % _ %% H %%
     (Lam (H1 : _) H2 : _. conjI % _ % _ %% H2 %% H1))";
  val prf = PThm (("HOL.impI", []), ..., ..., None) % None % None %%
    AbsP ("H", None, PThm (("HOL.conjE", []), ..., ..., None) %
      None % None % None %% PBound 0 %%
      AbsP ("H1", None, AbsP ("H2", None, ...))) : Proofterm.proof
```

The statement to be established by this proof is

```
val t = term_of
  (read_cterm (sign_of Main.thy) ("A & B --> B & A", propT));
  val t = Const ("Trueprop", "bool => prop") $
    (Const ("op -->", "[bool, bool] => bool") $
      ... $ ... : Term.term
```

Using `t` we can reconstruct the full proof

```
val prf' = Reconstruct.reconstruct_proof (sign_of Main.thy) t prf;
  val prf' = PThm (("HOL.impI", []), ..., ..., Some []) %
    Some (Const ("op &", ...) $ Free ("A", ...) $ Free ("B", ...)) %
    Some (Const ("op &", ...) $ Free ("B", ...) $ Free ("A", ...)) %%
    AbsP ("H", Some (Const ("Trueprop", ...) $ ...), ...)
      : Proofterm.proof
```

This proof can finally be turned into a theorem

```
val thm = ProofChecker.thm_of_proof Main.thy prf';
  val thm = "A & B --> B & A" : Thm.thm
```

Chapter 3

# Syntax Transformations

This chapter is intended for experienced Isabelle users who need to define macros or code their own translation functions. It describes the transformations between parse trees, abstract syntax trees and terms.

## 3.1 Abstract syntax trees

The parser, given a token list from the lexer, applies productions to yield a parse tree. By applying some internal transformations the parse tree becomes an abstract syntax tree, or AST. Macro expansion, further translations and finally type inference yields a well-typed term. The printing process is the reverse, except for some subtleties to be discussed later.

Figure 3.1 outlines the parsing and printing process. Much of the complexity is due to the macro mechanism. Using macros, you can specify most forms of concrete syntax without writing any ML code.

Abstract syntax trees are an intermediate form between the raw parse trees and the typed $\lambda$-terms. An AST is either an atom (constant or variable) or a list of *at least two* subtrees. Internally, they have type `Syntax.ast`:

```
datatype ast = Constant of string
             | Variable of string
             | Appl of ast list
```

Isabelle uses an S-expression syntax for abstract syntax trees. Constant atoms are shown as quoted strings, variable atoms as non-quoted strings and applications as a parenthesised list of subtrees. For example, the AST

```
Appl [Constant "_constrain",
      Appl [Constant "_abs", Variable "x", Variable "t"],
      Appl [Constant "fun", Variable "'a", Variable "'b"]]
```

is shown as `("_constrain" ("_abs" x t) ("fun" 'a 'b))`. Both `()` and `(f)` are illegal because they have too few subtrees.

The resemblance to Lisp's S-expressions is intentional, but there are two kinds of atomic symbols: `Constant` $x$ and `Variable` $x$. Do not take the

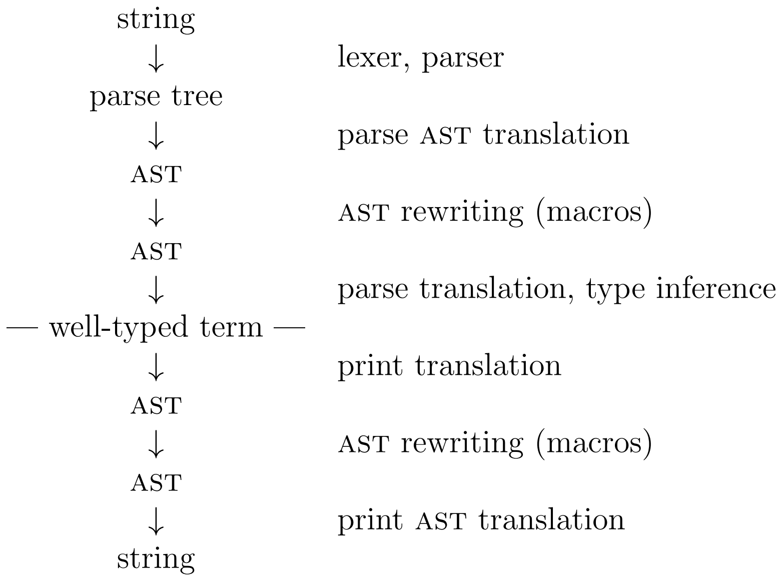

Figure 3.1: Parsing and printing

names `Constant` and `Variable` too literally; in the later translation to terms, `Variable` $x$ may become a constant, free or bound variable, even a type constructor or class name; the actual outcome depends on the context.

Similarly, you can think of ($f$ $x_1$ ... $x_n$) as the application of $f$ to the arguments $x_1, \ldots, x_n$. But the kind of application is determined later by context; it could be a type constructor applied to types.

Forms like `(("_abs" x` $t$`)` $u$`)` are legal, but ASTs are first-order: the `"_abs"` does not bind the `x` in any way. Later at the term level, `("_abs" x` $t$`)` will become an `Abs` node and occurrences of `x` in $t$ will be replaced by bound variables (the term constructor `Bound`).

## 3.2 Transforming parse trees to ASTs

The parse tree is the raw output of the parser. Translation functions, called **parse AST translations**, transform the parse tree into an abstract syntax tree.

The parse tree is constructed by nesting the right-hand sides of the productions used to recognize the input. Such parse trees are simply lists of tokens and constituent parse trees, the latter representing the nonterminals of the productions. Let us refer to the actual productions in the form displayed by `print_syntax` (see §?? for an example).

| input string | AST |
|---|---|
| `"f"` | `f` |
| `"'a"` | `'a` |
| `"t == u"` | `("==" t u)` |
| `"f(x)"` | `("_appl" f x)` |
| `"f(x, y)"` | `("_appl" f ("_args" x y))` |
| `"f(x, y, z)"` | `("_appl" f ("_args" x ("_args" y z)))` |
| `"%x y. t"` | `("_lambda" ("_idts" x y) t)` |

Figure 3.2: Parsing examples using the Pure syntax

Ignoring parse AST translations, parse trees are transformed to ASTs by stripping out delimiters and copy productions. More precisely, the mapping $\llbracket - \rrbracket$ is derived from the productions as follows:

- Name tokens: $\llbracket t \rrbracket = \texttt{Variable}\, s$, where $t$ is an `id`, `var`, `tid`, `tvar`, `num`, `xnum` or `xstr` token, and $s$ its associated string. Note that for `xstr` this does not include the quotes.

- Copy productions: $\llbracket \ldots P \ldots \rrbracket = \llbracket P \rrbracket$. Here $\ldots$ stands for strings of delimiters, which are discarded. $P$ stands for the single constituent that is not a delimiter; it is either a nonterminal symbol or a name token.

- 0-ary productions: $\llbracket \ldots \texttt{=>} c \rrbracket = \texttt{Constant}\, c$. Here there are no constituents other than delimiters, which are discarded.

- $n$-ary productions, where $n \geq 1$: delimiters are discarded and the remaining constituents $P_1, \ldots, P_n$ are built into an application whose head constant is $c$:

$$\llbracket \ldots P_1 \ldots P_n \ldots \texttt{=>} c \rrbracket = \texttt{Appl}\, [\texttt{Constant}\, c, \llbracket P_1 \rrbracket, \ldots, \llbracket P_n \rrbracket]$$

Figure 3.2 presents some simple examples, where `==`, `_appl`, `_args`, and so forth name productions of the Pure syntax. These examples illustrate the need for further translations to make ASTs closer to the typed $\lambda$-calculus. The Pure syntax provides predefined parse AST translations for ordinary applications, type applications, nested abstractions, meta implications and function types. Figure 3.3 shows their effect on some representative input strings.

The names of constant heads in the AST control the translation process. The list of constants invoking parse AST translations appears in the output of `print_syntax` under `parse_ast_translation`.

| input string | AST |
|---|---|
| `"f(x, y, z)"` | `(f x y z)` |
| `"'a ty"` | `(ty 'a)` |
| `"('a, 'b) ty"` | `(ty 'a 'b)` |
| `"%x y z. t"` | `("_abs" x ("_abs" y ("_abs" z t)))` |
| `"%x :: 'a. t"` | `("_abs" ("_constrain" x 'a) t)` |
| `"[\| P; Q; R \|] => S"` | `("==>" P ("==>" Q ("==>" R S)))` |
| `"['a, 'b, 'c] => 'd"` | `("fun" 'a ("fun" 'b ("fun" 'c 'd)))` |

Figure 3.3: Built-in parse AST translations

## 3.3 Transforming ASTs to terms

The AST, after application of macros (see §3.5), is transformed into a term. This term is probably ill-typed since type inference has not occurred yet. The term may contain type constraints consisting of applications with head `"_constrain"`; the second argument is a type encoded as a term. Type inference later introduces correct types or rejects the input.

Another set of translation functions, namely parse translations, may affect this process. If we ignore parse translations for the time being, then ASTs are transformed to terms by mapping AST constants to constants, AST variables to schematic or free variables and AST applications to applications.

More precisely, the mapping $\llbracket - \rrbracket$ is defined by

- Constants: $\llbracket \mathtt{Constant}\, x \rrbracket = \mathtt{Const}(x, \mathtt{dummyT})$.

- Schematic variables: $\llbracket \mathtt{Variable}\, \mathtt{"?}xi\mathtt{"} \rrbracket = \mathtt{Var}((x, i), \mathtt{dummyT})$, where $x$ is the base name and $i$ the index extracted from $xi$.

- Free variables: $\llbracket \mathtt{Variable}\, x \rrbracket = \mathtt{Free}(x, \mathtt{dummyT})$.

- Function applications with $n$ arguments:

$$\llbracket \mathtt{Appl}\, [f, x_1, \ldots, x_n] \rrbracket = \llbracket f \rrbracket \ \mathtt{\$}\ \llbracket x_1 \rrbracket \ \mathtt{\$}\ \ldots \ \mathtt{\$}\ \llbracket x_n \rrbracket$$

Here `Const`, `Var`, `Free` and `$` are constructors of the datatype `term`, while `dummyT` stands for some dummy type that is ignored during type inference.

So far the outcome is still a first-order term. Abstractions and bound variables (constructors `Abs` and `Bound`) are introduced by parse translations. Such translations are attached to `"_abs"`, `"!!"` and user-defined binders.

## 3.4 Printing of terms

The output phase is essentially the inverse of the input phase. Terms are translated via abstract syntax trees into strings. Finally the strings are pretty printed.

Print translations (§3.6) may affect the transformation of terms into ASTs. Ignoring those, the transformation maps term constants, variables and applications to the corresponding constructs on ASTs. Abstractions are mapped to applications of the special constant `_abs`.

More precisely, the mapping $[\![-]\!]$ is defined as follows:

- $[\![\texttt{Const}(x,\tau)]\!] = \texttt{Constant}\ x$.

- $[\![\texttt{Free}(x,\tau)]\!] = \mathit{constrain}(\texttt{Variable}\ x, \tau)$.

- $[\![\texttt{Var}((x,i),\tau)]\!] = \mathit{constrain}(\texttt{Variable}\ \texttt{"?}xi\texttt{"}, \tau)$, where $\texttt{?}xi$ is the string representation of the `indexname` $(x,i)$.

- For the abstraction $\lambda x :: \tau\ .\ t$, let $x'$ be a variant of $x$ renamed to differ from all names occurring in $t$, and let $t'$ be obtained from $t$ by replacing all bound occurrences of $x$ by the free variable $x'$. This replaces corresponding occurrences of the constructor `Bound` by the term $\texttt{Free}(x', \texttt{dummyT})$:

  $$[\![\texttt{Abs}(x,\tau,t)]\!] = \texttt{Appl}\ [\texttt{Constant}\ \texttt{"\_abs"}, \mathit{constrain}(\texttt{Variable}\ x', \tau), [\![t']\!]]$$

- $[\![\texttt{Bound}\ i]\!] = \texttt{Variable}\ \texttt{"B.}i\texttt{"}$. The occurrence of constructor `Bound` should never happen when printing well-typed terms; it indicates a de Bruijn index with no matching abstraction.

- Where $f$ is not an application,

  $$[\![f\ \texttt{\$}\ x_1\ \texttt{\$}\ \ldots\ \texttt{\$}\ x_n]\!] = \texttt{Appl}\ [[\![f]\!], [\![x_1]\!], \ldots, [\![x_n]\!]]$$

Type constraints are inserted to allow the printing of types. This is governed by the boolean variable `show_types`:

- $\mathit{constrain}(x,\tau) = x$ if $\tau = \texttt{dummyT}$ or `show_types` is set to `false`.

- $\mathit{constrain}(x,\tau) = \texttt{Appl}\ [\texttt{Constant}\ \texttt{"\_constrain"}, x, [\![\tau]\!]]$ otherwise.

  Here, $[\![\tau]\!]$ is the AST encoding of $\tau$: type constructors go to `Constant`s; type identifiers go to `Variable`s; type applications go to `Appl`s with the type constructor as the first element. If `show_sorts` is set to `true`, some type variables are decorated with an AST encoding of their sort.

The AST, after application of macros (see §3.5), is transformed into the final output string. The built-in **print AST translations** reverse the parse AST translations of Fig. 3.3.

For the actual printing process, the names attached to productions of the form $\ldots A_1^{(p_1)} \ldots A_n^{(p_n)} \ldots$ `=>`$c$ play a vital role. Each AST with constant head $c$, namely `"`$c$`"` or (`"`$c$`"` $x_1 \ldots x_n$), is printed according to the production for $c$. Each argument $x_i$ is converted to a string, and put in parentheses if its priority $(p_i)$ requires this. The resulting strings and their syntactic sugar (denoted by $\ldots$ above) are joined to make a single string.

If an application (`"`$c$`"` $x_1 \ldots x_m$) has more arguments than the corresponding production, it is first split into ((`"`$c$`"` $x_1 \ldots x_n$) $x_{n+1} \ldots x_m$). Applications with too few arguments or with non-constant head or without a corresponding production are printed as $f(x_1, \ldots, x_l)$ or $(\alpha_1, \ldots, \alpha_l)ty$. Multiple productions associated with some name $c$ are tried in order of appearance. An occurrence of `Variable` $x$ is simply printed as $x$.

Blanks are *not* inserted automatically. If blanks are required to separate tokens, specify them in the mixfix declaration, possibly preceded by a slash (`/`) to allow a line break.

## 3.5 Macros: syntactic rewriting

Mixfix declarations alone can handle situations where there is a direct connection between the concrete syntax and the underlying term. Sometimes we require a more elaborate concrete syntax, such as quantifiers and list notation. Isabelle's **macros** and **translation functions** can perform translations such as

```
ALL x:A.P    ⇌   Ball(A, %x.P)
[x, y, z]    ⇌   Cons(x, Cons(y, Cons(z, Nil)))
```

Translation functions (see §3.6) must be coded in ML; they are the most powerful translation mechanism but are difficult to read or write. Macros are specified by first-order rewriting systems that operate on abstract syntax trees. They are usually easy to read and write, and can express all but the most obscure translations.

Figure 3.4 defines a fragment of first-order logic and set theory.[1] Theory `SetSyntax` declares constants for set comprehension (`Collect`), replacement (`Replace`) and bounded universal quantification (`Ball`). Each of these binds

[1] This and the following theories are complete working examples, though they specify only syntax, no axioms. The file `ZF/ZF.thy` presents a full set theory definition, including many macro rules.

```
SetSyntax = Pure +
types
  i o
arities
  i, o :: logic
consts
  Trueprop      :: o => prop                ("_" 5)
  Collect       :: [i, i => o] => i
  Replace       :: [i, [i, i] => o] => i
  Ball          :: [i, i => o] => o
syntax
  "@Collect"    :: [idt, i, o] => i         ("(1{_:_./ _})")
  "@Replace"    :: [idt, idt, i, o] => i    ("(1{_./ _:_, _})")
  "@Ball"       :: [idt, i, o] => o         ("(3ALL _:_./ _)" 10)
translations
  "{x:A. P}"    == "Collect(A, %x. P)"
  "{y. x:A, Q}" == "Replace(A, %x y. Q)"
  "ALL x:A. P"  == "Ball(A, %x. P)"
end
```

Figure 3.4: Macro example: set theory

some variables. Without additional syntax we should have to write $\forall x \in A . P$ as `Ball(A,%x.P)`, and similarly for the others.

The theory specifies a variable-binding syntax through additional productions that have mixfix declarations. Each non-copy production must specify some constant, which is used for building ASTs. The additional constants are decorated with `@` to stress their purely syntactic purpose; they may not occur within the final well-typed terms, being declared as `syntax` rather than `consts`.

The translations cause the replacement of external forms by internal forms after parsing, and vice versa before printing of terms. As a specification of the set theory notation, they should be largely self-explanatory. The syntactic constants, `@Collect`, `@Replace` and `@Ball`, appear implicitly in the macro rules via their mixfix forms.

Macros can define variable-binding syntax because they operate on ASTs, which have no inbuilt notion of bound variable. The macro variables `x` and `y` have type `idt` and therefore range over identifiers, in this case bound variables. The macro variables `P` and `Q` range over formulae containing bound variable occurrences.

Other applications of the macro system can be less straightforward, and there are peculiarities. The rest of this section will describe in detail how Isabelle macros are preprocessed and applied.

### 3.5.1 Specifying macros

Macros are basically rewrite rules on ASTs. But unlike other macro systems found in programming languages, Isabelle's macros work in both directions. Therefore a syntax contains two lists of rewrites: one for parsing and one for printing.

The `translations` section specifies macros. The syntax for a macro is

$$(\mathit{root})\ \mathit{string} \quad \left\{\begin{array}{c}\texttt{=>}\\ \texttt{<=}\\ \texttt{==}\end{array}\right\} \quad (\mathit{root})\ \mathit{string}$$

This specifies a parse rule (`=>`), a print rule (`<=`), or both (`==`). The two strings specify the left and right-hand sides of the macro rule. The (*root*) specification is optional; it specifies the nonterminal for parsing the *string* and if omitted defaults to `logic`. AST rewrite rules $(l, r)$ must obey certain conditions:

- Rules must be left linear: $l$ must not contain repeated variables.
- Every variable in $r$ must also occur in $l$.

Macro rules may refer to any syntax from the parent theories. They may also refer to anything defined before the current `translations` section — including any mixfix declarations.

Upon declaration, both sides of the macro rule undergo parsing and parse AST translations (see §3.1), but do not themselves undergo macro expansion. The lexer runs in a different mode that additionally accepts identifiers of the form `_` *letter quasiletter*$^*$ (like `_idt`, `_K`). Thus, a constant whose name starts with an underscore can appear in macro rules but not in ordinary terms.

Some atoms of the macro rule's AST are designated as constants for matching. These are all names that have been declared as classes, types or constants (logical and syntactic).

The result of this preprocessing is two lists of macro rules, each stored as a pair of ASTs. They can be viewed using `print_syntax` (sections `parse_rules` and `print_rules`). For theory `SetSyntax` of Fig. 3.4 these are

```
parse_rules:
  ("@Collect" x A P)  ->  ("Collect" A ("_abs" x P))
  ("@Replace" y x A Q)  ->  ("Replace" A ("_abs" x ("_abs" y Q)))
  ("@Ball" x A P)  ->  ("Ball" A ("_abs" x P))
print_rules:
  ("Collect" A ("_abs" x P))  ->  ("@Collect" x A P)
  ("Replace" A ("_abs" x ("_abs" y Q)))  ->  ("@Replace" y x A Q)
  ("Ball" A ("_abs" x P))  ->  ("@Ball" x A P)
```

! Avoid choosing variable names that have previously been used as constants, types or type classes; the `consts` section in the output of `print_syntax` lists all such names. If a macro rule works incorrectly, inspect its internal form as shown above, recalling that constants appear as quoted strings and variables without quotes.

! If `eta_contract` is set to `true`, terms will be $\eta$-contracted *before* the AST rewriter sees them. Thus some abstraction nodes needed for print rules to match may vanish. For example, `Ball(A, %x. P(x))` contracts to `Ball(A, P)`; the print rule does not apply and the output will be `Ball(A, P)`. This problem would not occur if ML translation functions were used instead of macros (as is done for binder declarations).

! Another trap concerns type constraints. If `show_types` is set to `true`, bound variables will be decorated by their meta types at the binding place (but not at occurrences in the body). Matching with `Collect(A, %x. P)` binds `x` to something like `("_constrain" y "i")` rather than only `y`. AST rewriting will cause the constraint to appear in the external form, say `{y::i:A::i. P::o}`.

To allow such constraints to be re-read, your syntax should specify bound variables using the nonterminal `idt`. This is the case in our example. Choosing `id` instead of `idt` is a common error.

### 3.5.2 Applying rules

As a term is being parsed or printed, an AST is generated as an intermediate form (recall Fig. 3.1). The AST is normalised by applying macro rules in the manner of a traditional term rewriting system. We first examine how a single rule is applied.

Let $t$ be the abstract syntax tree to be normalised and $(l, r)$ some translation rule. A subtree $u$ of $t$ is a **redex** if it is an instance of $l$; in this case $l$ is said to **match** $u$. A redex matched by $l$ may be replaced by the corresponding instance of $r$, thus **rewriting** the AST $t$. Matching requires some notion of **place-holders** that may occur in rule patterns but not in ordinary ASTs; `Variable` atoms serve this purpose.

The matching of the object $u$ by the pattern $l$ is performed as follows:

- Every constant matches itself.

- `Variable` $x$ in the object matches `Constant` $x$ in the pattern. This point is discussed further below.

- Every AST in the object matches `Variable` $x$ in the pattern, binding $x$ to $u$.

- One application matches another if they have the same number of subtrees and corresponding subtrees match.
- In every other case, matching fails. In particular, `Constant` $x$ can only match itself.

A successful match yields a substitution that is applied to $r$, generating the instance that replaces $u$.

The second case above may look odd. This is where `Variable`s of non-rule ASTs behave like `Constant`s. Recall that ASTs are not far removed from parse trees; at this level it is not yet known which identifiers will become constants, bounds, frees, types or classes. As §3.1 describes, former parse tree heads appear in ASTs as `Constant`s, while the name tokens `id`, `var`, `tid`, `tvar`, `num`, `xnum` and `xstr` become `Variable`s. On the other hand, when ASTs generated from terms for printing, all constants and type constructors become `Constant`s; see §3.1. Thus ASTs may contain a messy mixture of `Variable`s and `Constant`s. This is insignificant at macro level because matching treats them alike.

Because of this behaviour, different kinds of atoms with the same name are indistinguishable, which may make some rules prone to misbehaviour. Example:

```
types
  Nil
consts
  Nil     :: 'a list
syntax
  "[]"    :: 'a list    ("[]")
translations
  "[]"    == "Nil"
```

The term `Nil` will be printed as `[]`, just as expected. The term `%Nil.t` will be printed as `%[].t`, which might not be expected! Guess how type `Nil` is printed?

Normalizing an AST involves repeatedly applying macro rules until none are applicable. Macro rules are chosen in order of appearance in the theory definitions. You can watch the normalization of ASTs during parsing and printing by setting `Syntax.trace_ast` to `true`. The information displayed when tracing includes the AST before normalization (`pre`), redexes with results (`rewrote`), the normal form finally reached (`post`) and some statistics (`normalize`).

### 3.5.3 Example: the syntax of finite sets

This example demonstrates the use of recursive macros to implement a convenient notation for finite sets.

```
FinSyntax = SetSyntax +
types
  is
syntax
  ""              :: i => is                  ("_")
  "@Enum"         :: [i, is] => is            ("_,/ _")
consts
  empty           :: i                        ("{}")
  insert          :: [i, i] => i
syntax
  "@Finset"       :: is => i                  ("{(_)}")
translations
  "{x, xs}"       == "insert(x, {xs})"
  "{x}"           == "insert(x, {})"
end
```

Finite sets are internally built up by `empty` and `insert`. The declarations above specify `{x, y, z}` as the external representation of

```
insert(x, insert(y, insert(z, empty)))
```

The nonterminal symbol `is` stands for one or more objects of type `i` separated by commas. The mixfix declaration `"_,/ _"` allows a line break after the comma for pretty printing; if no line break is required then a space is printed instead.

The nonterminal is declared as the type `is`, but with no `arities` declaration. Hence `is` is not a logical type and may be used safely as a new nonterminal for custom syntax. The nonterminal `is` can later be re-used for other enumerations of type `i` like lists or tuples. If we had needed polymorphic enumerations, we could have used the predefined nonterminal symbol `args` and skipped this part altogether.

Next follows `empty`, which is already equipped with its syntax `{}`, and `insert` without concrete syntax. The syntactic constant `@Finset` provides concrete syntax for enumerations of `i` enclosed in curly braces. Remember that a pair of parentheses, as in `"{(_)}"`, specifies a block of indentation for pretty printing.

The translations may look strange at first. Macro rules are best understood in their internal forms:

```
parse_rules:
  ("@Finset" ("@Enum" x xs))  ->  ("insert" x ("@Finset" xs))
  ("@Finset" x)  ->  ("insert" x "empty")
print_rules:
  ("insert" x ("@Finset" xs))  ->  ("@Finset" ("@Enum" x xs))
  ("insert" x "empty")  ->  ("@Finset" x)
```

This shows that `{x,xs}` indeed matches any set enumeration of at least two elements, binding the first to `x` and the rest to `xs`. Likewise, `{xs}` and `{x}` represent any set enumeration. The parse rules only work in the order given.

! The AST rewriter cannot distinguish constants from variables and looks only for names of atoms. Thus the names of `Constant`s occurring in the (internal) left-hand side of translation rules should be regarded as reserved words. Choose non-identifiers like `@Finset` or sufficiently long and strange names. If a bound variable's name gets rewritten, the result will be incorrect; for example, the term

```
%empty insert. insert(x, empty)
```

is incorrectly printed as `%empty insert. {x}`.

### 3.5.4 Example: a parse macro for dependent types

As stated earlier, a macro rule may not introduce new `Variable`s on the right-hand side. Something like `"K(B)" => "%x.B"` is illegal; if allowed, it could cause variable capture. In such cases you usually must fall back on translation functions. But a trick can make things readable in some cases: *calling* translation functions by parse macros:

```
ProdSyntax = SetSyntax +
consts
  Pi            :: [i, i => i] => i
syntax
  "@PROD"       :: [idt, i, i] => i       ("(3PROD _:_./ _)" 10)
  "@->"         :: [i, i] => i            ("(_ ->/ _)" [51, 50] 50)
translations
  "PROD x:A. B" => "Pi(A, %x. B)"
  "A -> B"      => "Pi(A, _K(B))"
end
ML
  val print_translation = [("Pi", dependent_tr' ("@PROD", "@->"))];
```

Here `Pi` is a logical constant for constructing general products. Two external forms exist: the general case `PROD x:A.B` and the function space `A -> B`, which abbreviates `Pi(A, %x.B)` when `B` does not depend on `x`.

The second parse macro introduces `_K(B)`, which later becomes `%x.B` due to a parse translation associated with `_K`. Unfortunately there is no such trick for printing, so we have to add a `ML` section for the print translation `dependent_tr'`.

Recall that identifiers with a leading `_` are allowed in translation rules, but not in ordinary terms. Thus we can create ASTs containing names that are not directly expressible.

The parse translation for `_K` is already installed in Pure, and the function `dependent_tr'` is exported by the syntax module for public use. See §3.6 below for more of the arcane lore of translation functions.

## 3.6 Translation functions

This section describes the translation function mechanism. By writing ML functions, you can do almost everything to terms or ASTs during parsing and printing. The logic LK is a good example of sophisticated transformations between internal and external representations of sequents; here, macros would be useless.

A full understanding of translations requires some familiarity with Isabelle's internals, especially the datatypes `term`, `typ`, `Syntax.ast` and the encodings of types and terms as such at the various stages of the parsing or printing process. Most users should never need to use translation functions.

### 3.6.1 Declaring translation functions

There are four kinds of translation functions, with one of these coming in two variants. Each such function is associated with a name, which triggers calls to it. Such names can be constants (logical or syntactic) or type constructors.

Function `print_syntax` displays the sets of names associated with the translation functions of a theory under `parse_ast_translation`, etc. You can add new ones via the `ML` section of a theory definition file. Even though the `ML` section is the very last part of the file, newly installed translation functions are already effective when processing all of the preceding sections.

The `ML` section's contents are simply copied verbatim near the beginning of the ML file generated from a theory definition file. Definitions made here are accessible as components of an ML structure; to make some parts private, use an ML `local` declaration. The ML code may install translation functions by declaring any of the following identifiers:

```
val parse_ast_translation   : (string * (ast list -> ast)) list
val print_ast_translation   : (string * (ast list -> ast)) list
val parse_translation       : (string * (term list -> term)) list
val print_translation       : (string * (term list -> term)) list
val typed_print_translation :
    (string * (bool -> typ -> term list -> term)) list
```

### 3.6.2 The translation strategy

The different kinds of translation functions are called during the transformations between parse trees, ASTs and terms (recall Fig. 3.1). Whenever a combination of the form ("$c$" $x_1 \ldots x_n$) is encountered, and a translation function $f$ of appropriate kind exists for $c$, the result is computed by the ML function call $f$ `[`$x_1, \ldots, x_n$`]`.

For AST translations, the arguments $x_1, \ldots, x_n$ are ASTs. A combination has the form `Constant` $c$ or `Appl` $[$`Constant` $c, x_1, \ldots, x_n]$. For term translations, the arguments are terms and a combination has the form `Const`$(c, \tau)$ or `Const`$(c, \tau)$ `$` $x_1$ `$` ... `$` $x_n$. Terms allow more sophisticated transformations than ASTs do, typically involving abstractions and bound variables. *Typed* print translations may even peek at the type $\tau$ of the constant they are invoked on; they are also passed the current value of the `show_sorts` flag.

Regardless of whether they act on terms or ASTs, translation functions called during the parsing process differ from those for printing more fundamentally in their overall behaviour:

**Parse translations** are applied bottom-up. The arguments are already in translated form. The translations must not fail; exceptions trigger an error message. There may never be more than one function associated with any syntactic name.

**Print translations** are applied top-down. They are supplied with arguments that are partly still in internal form. The result again undergoes translation; therefore a print translation should not introduce as head the very constant that invoked it. The function may raise exception `Match` to indicate failure; in this event it has no effect. Multiple functions associated with some syntactic name are tried in an unspecified order.

Only constant atoms — constructor `Constant` for ASTs and `Const` for terms — can invoke translation functions. This causes another difference between parsing and printing.

Parsing starts with a string and the constants are not yet identified. Only parse tree heads create `Constant`s in the resulting AST, as described in

§3.2. Macros and parse AST translations may introduce further Constants. When the final AST is converted to a term, all Constants become Consts, as described in §3.3.

Printing starts with a well-typed term and all the constants are known. So all logical constants and type constructors may invoke print translations. These, and macros, may introduce further constants.

### 3.6.3 Example: a print translation for dependent types

Let us continue the dependent type example (page 28) by examining the parse translation for _K and the print translation dependent_tr', which are both built-in. By convention, parse translations have names ending with _tr and print translations have names ending with _tr'. Search for such names in the Isabelle sources to locate more examples.

Here is the parse translation for _K:

```
fun k_tr [t] = Abs ("x", dummyT, incr_boundvars 1 t)
  | k_tr ts = raise TERM ("k_tr", ts);
```

If k_tr is called with exactly one argument $t$, it creates a new Abs node with a body derived from $t$. Since terms given to parse translations are not yet typed, the type of the bound variable in the new Abs is simply dummyT. The function increments all Bound nodes referring to outer abstractions by calling incr_boundvars, a basic term manipulation function defined in Pure/term.ML.

Here is the print translation for dependent types:

```
fun dependent_tr' (q, r) (A :: Abs (x, T, B) :: ts) =
      if 0 mem (loose_bnos B) then
        let val (x', B') = Syntax.variant_abs' (x, dummyT, B) in
          list_comb
            (Const (q,dummyT) $
             Syntax.mark_boundT (x',T) $ A $ B', ts)
        end
      else list_comb (Const (r, dummyT) $ A $ B, ts)
  | dependent_tr' _ _ = raise Match;
```

The argument (q, r) is supplied to the curried function dependent_tr' by a partial application during its installation. For example, we could set up print translations for both Pi and Sigma by including

```
val print_translation =
  [("Pi",    dependent_tr' ("@PROD", "@->")),
   ("Sigma", dependent_tr' ("@SUM", "@*"))];
```

within the ML section. The first of these transforms Pi$(A,$ Abs$(x, T, B))$ into @PROD$(x', A, B')$ or @->$(A, B)$, choosing the latter form if $B$ does not depend on $x$. It checks this using `loose_bnos`, yet another function from `Pure/term.ML`. Note that $x'$ is a version of $x$ renamed away from all names in $B$, and $B'$ is the body $B$ with `Bound` nodes referring to the `Abs` node replaced by `Free`$(x'$, `dummyT`$)$ (but marked as representing a bound variable).

We must be careful with types here. While types of `Const`s are ignored, type constraints may be printed for some `Free`s and `Var`s if `show_types` is set to `true`. Variables of type `dummyT` are never printed with constraint, though. The line

```
let val (x', B') = Syntax.variant_abs' (x, dummyT, B);
```

replaces bound variable occurrences in $B$ by the free variable $x'$ with type `dummyT`. Only the binding occurrence of $x'$ is given the correct type `T`, so this is the only place where a type constraint might appear.

Also note that we are responsible to mark free identifiers that actually represent bound variables. This is achieved by `Syntax.variant_abs'` and `Syntax.mark_boundT` above. Failing to do so may cause these names to be printed in the wrong style.

Chapter 4

# Substitution Tactics

Replacing equals by equals is a basic form of reasoning. Isabelle supports several kinds of equality reasoning. **Substitution** means replacing free occurrences of $t$ by $u$ in a subgoal. This is easily done, given an equality $t = u$, provided the logic possesses the appropriate rule. The tactic `hyp_subst_tac` performs substitution even in the assumptions. But it works via object-level implication, and therefore must be specially set up for each suitable object-logic.

Substitution should not be confused with object-level **rewriting**. Given equalities of the form $t = u$, rewriting replaces instances of $t$ by corresponding instances of $u$, and continues until it reaches a normal form. Substitution handles 'one-off' replacements by particular equalities while rewriting handles general equations. Chapter 5 discusses Isabelle's rewriting tactics.

## 4.1 Substitution rules

Many logics include a substitution rule of the form

$$[\![ ?a = ?b; ?P(?a) ]\!] \Longrightarrow ?P(?b) \qquad (subst)$$

In backward proof, this may seem difficult to use: the conclusion $?P(?b)$ admits far too many unifiers. But, if the theorem `eqth` asserts $t = u$, then `eqth RS subst` is the derived rule

$$?P(t) \Longrightarrow ?P(u).$$

Provided $u$ is not an unknown, resolution with this rule is well-behaved.[1] To replace $u$ by $t$ in subgoal $i$, use

```
resolve_tac [eqth RS subst] i.
```

To replace $t$ by $u$ in subgoal $i$, use

[1] Unifying $?P(u)$ with a formula $Q$ expresses $Q$ in terms of its dependence upon $u$. There are still $2^k$ unifiers, if $Q$ has $k$ occurrences of $u$, but Isabelle ensures that the first unifier includes all the occurrences.

`resolve_tac [eqth RS ssubst]` $i$,

where `ssubst` is the 'swapped' substitution rule

$$[\![?a = ?b; ?P(?b)]\!] \Longrightarrow ?P(?a). \qquad (ssubst)$$

If `sym` denotes the symmetry rule $?a = ?b \Longrightarrow ?b = ?a$, then `ssubst` is just `sym RS subst`. Many logics with equality include the rules `subst` and `ssubst`, as well as `refl`, `sym` and `trans` (for the usual equality laws). Examples include `FOL` and `HOL`, but not `CTT` (Constructive Type Theory).

Elim-resolution is well-behaved with assumptions of the form $t = u$. To replace $u$ by $t$ or $t$ by $u$ in subgoal $i$, use

`eresolve_tac [subst]` $i$ or `eresolve_tac [ssubst]` $i$.

Logics HOL, FOL and ZF define the tactic `stac` by

```
fun stac eqth = CHANGED o rtac (eqth RS ssubst);
```

Now `stac eqth` is like `resolve_tac [eqth RS ssubst]` but with the valuable property of failing if the substitution has no effect.

## 4.2 Substitution in the hypotheses

Substitution rules, like other rules of natural deduction, do not affect the assumptions. This can be inconvenient. Consider proving the subgoal

$$[\![c = a; c = b]\!] \Longrightarrow a = b.$$

Calling `eresolve_tac [ssubst]` $i$ simply discards the assumption $c = a$, since $c$ does not occur in $a = b$. Of course, we can work out a solution. First apply `eresolve_tac [subst]` $i$, replacing $a$ by $c$:

$$c = b \Longrightarrow c = b$$

Equality reasoning can be difficult, but this trivial proof requires nothing more sophisticated than substitution in the assumptions. Object-logics that include the rule (*subst*) provide tactics for this purpose:

```
hyp_subst_tac       : int -> tactic
bound_hyp_subst_tac : int -> tactic
```

`hyp_subst_tac` $i$ selects an equality assumption of the form $t = u$ or $u = t$, where $t$ is a free variable or parameter. Deleting this assumption, it replaces $t$ by $u$ throughout subgoal $i$, including the other assumptions.

`bound_hyp_subst_tac` *i* is similar but only substitutes for parameters (bound variables). Uses for this are discussed below.

The term being replaced must be a free variable or parameter. Substitution for constants is usually unhelpful, since they may appear in other theorems. For instance, the best way to use the assumption $0 = 1$ is to contradict a theorem that states $0 \neq 1$, rather than to replace 0 by 1 in the subgoal!

Substitution for unknowns, such as $?x = 0$, is a bad idea: we might prove the subgoal more easily by instantiating $?x$ to 1. Substitution for free variables is unhelpful if they appear in the premises of a rule being derived: the substitution affects object-level assumptions, not meta-level assumptions. For instance, replacing $a$ by $b$ could make the premise $P(a)$ worthless. To avoid this problem, use `bound_hyp_subst_tac`; alternatively, call `cut_facts_tac` to insert the atomic premises as object-level assumptions.

## 4.3 Setting up the package

Many Isabelle object-logics, such as `FOL`, `HOL` and their descendants, come with `hyp_subst_tac` already defined. A few others, such as `CTT`, do not support this tactic because they lack the rule (*subst*). When defining a new logic that includes a substitution rule and implication, you must set up `hyp_subst_tac` yourself. It is packaged as the ML functor `HypsubstFun`, which takes the argument signature `HYPSUBST_DATA`:

```
signature HYPSUBST_DATA =
  sig
  structure Simplifier : SIMPLIFIER
  val dest_Trueprop    : term -> term
  val dest_eq          : term -> (term*term)*typ
  val dest_imp         : term -> term*term
  val eq_reflection    : thm         (* a=b ==> a==b *)
  val rev_eq_reflection: thm         (* a==b ==> a=b *)
  val imp_intr         : thm         (*(P ==> Q) ==> P-->Q *)
  val rev_mp           : thm         (* [| P;  P-->Q |] ==> Q *)
  val subst            : thm         (* [| a=b;  P(a) |] ==> P(b) *)
  val sym              : thm         (* a=b ==> b=a *)
  val thin_refl        : thm         (* [|x=x; P|] ==> P *)
  end;
```

Thus, the functor requires the following items:

`Simplifier` should be an instance of the simplifier (see Chapter 5).

`dest_Trueprop` should coerce a meta-level formula to the corresponding object-level one. Typically, it should return $P$ when applied to the term `Trueprop` $P$ (see example below).

`dest_eq` should return the triple $((t, u), T)$, where $T$ is the type of $t$ and $u$, when applied to the ML term that represents $t = u$. For other terms, it should raise an exception.

`dest_imp` should return the pair $(P, Q)$ when applied to the ML term that represents the implication $P \to Q$. For other terms, it should raise an exception.

`eq_reflection` is the theorem discussed in §5.6.

`rev_eq_reflection` is the reverse of `eq_reflection`.

`imp_intr` should be the implies introduction rule $(?P \Longrightarrow ?Q) \Longrightarrow ?P \to ?Q$.

`rev_mp` should be the 'reversed' implies elimination rule $[\![?P;\ ?P \to ?Q]\!] \Longrightarrow ?Q$.

`subst` should be the substitution rule $[\![?a = ?b;\ ?P(?a)]\!] \Longrightarrow ?P(?b)$.

`sym` should be the symmetry rule $?a = ?b \Longrightarrow ?b = ?a$.

`thin_refl` should be the rule $[\![?a = ?a;\ ?P]\!] \Longrightarrow ?P$, which is used to erase trivial equalities.

The functor resides in file `Provers/hypsubst.ML` in the Isabelle distribution directory. It is not sensitive to the precise formalization of the object-logic. It is not concerned with the names of the equality and implication symbols, or the types of formula and terms.

Coding the functions `dest_Trueprop`, `dest_eq` and `dest_imp` requires knowledge of Isabelle's representation of terms. For `FOL`, they are declared by

```
fun dest_Trueprop (Const ("Trueprop", _) $ P) = P
  | dest_Trueprop t = raise TERM ("dest_Trueprop", [t]);

fun dest_eq (Const("op =",T) $ t $ u) = ((t, u), domain_type T)

fun dest_imp (Const("op -->",_) $ A $ B) = (A, B)
  | dest_imp  t = raise TERM ("dest_imp", [t]);
```

Recall that `Trueprop` is the coercion from type $o$ to type *prop*, while `op =` is the internal name of the infix operator `=`. Function `domain_type`, given the function type $S \Rightarrow T$, returns the type $S$. Pattern-matching expresses the function concisely, using wildcards (`_`) for the types.

The tactic `hyp_subst_tac` works as follows. First, it identifies a suitable equality assumption, possibly re-orienting it using `sym`. Then it moves other assumptions into the conclusion of the goal, by repeatedly calling `etac rev_mp`. Then, it uses `asm_full_simp_tac` or `ssubst` to substitute throughout the subgoal. (If the equality involves unknowns then it must use `ssubst`.) Then, it deletes the equality. Finally, it moves the assumptions back to their original positions by calling `resolve_tac [imp_intr]`.

Chapter 5

# Simplification

This chapter describes Isabelle's generic simplification package. It performs conditional and unconditional rewriting and uses contextual information ('local assumptions'). It provides several general hooks, which can provide automatic case splits during rewriting, for example. The simplifier is already set up for many of Isabelle's logics: FOL, ZF, HOL, HOLCF.

The first section is a quick introduction to the simplifier that should be sufficient to get started. The later sections explain more advanced features.

## 5.1 Simplification for dummies

Basic use of the simplifier is particularly easy because each theory is equipped with sensible default information controlling the rewrite process — namely the implicit *current simpset*. A suite of simple commands is provided that refer to the implicit simpset of the current theory context.

! Make sure that you are working within the correct theory context. Executing proofs interactively, or loading them from ML files without associated theories may require setting the current theory manually via the `context` command.

### 5.1.1 Simplification tactics

```
Simp_tac          : int -> tactic
Asm_simp_tac      : int -> tactic
Full_simp_tac     : int -> tactic
Asm_full_simp_tac : int -> tactic
trace_simp        : bool ref                              initially false
debug_simp        : bool ref                              initially false
```

`Simp_tac` *i* simplifies subgoal *i* using the current simpset. It may solve the subgoal completely if it has become trivial, using the simpset's solver tactic.

`Asm_simp_tac` is like `Simp_tac`, but extracts additional rewrite rules from the local assumptions.

`Full_simp_tac` is like `Simp_tac`, but also simplifies the assumptions (without using the assumptions to simplify each other or the actual goal).

`Asm_full_simp_tac` is like `Asm_simp_tac`, but also simplifies the assumptions. In particular, assumptions can simplify each other. [1]

`set trace_simp;` makes the simplifier output internal operations. This includes rewrite steps, but also bookkeeping like modifications of the simpset.

`set debug_simp;` makes the simplifier output some extra information about internal operations. This includes any attempted invocation of simplification procedures.

As an example, consider the theory of arithmetic in HOL. The (rather trivial) goal $0 + (x + 0) = x + 0 + 0$ can be solved by a single call of `Simp_tac` as follows:

```
context Arith.thy;
Goal "0 + (x + 0) = x + 0 + 0";
   1. 0 + (x + 0) = x + 0 + 0
by (Simp_tac 1);
  Level 1
  0 + (x + 0) = x + 0 + 0
  No subgoals!
```

The simplifier uses the current simpset of `Arith.thy`, which contains suitable theorems like $?n + 0 = ?n$ and $0 + ?n = ?n$.

In many cases, assumptions of a subgoal are also needed in the simplification process. For example, `x = 0 ==> x + x = 0` is solved by `Asm_simp_tac` as follows:

```
   1. x = 0 ==> x + x = 0
by (Asm_simp_tac 1);
```

`Asm_full_simp_tac` is the most powerful of this quartet of tactics but may also loop where some of the others terminate. For example,

```
   1. ALL x. f x = g (f (g x)) ==> f 0 = f 0 + 0
```

is solved by `Simp_tac`, but `Asm_simp_tac` and `Asm_full_simp_tac` loop because the rewrite rule $f\ ?x = g\ (f\ (g\ ?x))$ extracted from the assumption does

[1] `Asm_full_simp_tac` used to process the assumptions from left to right. For backwards compatibilty reasons only there is now `Asm_lr_simp_tac` that behaves like the old `Asm_full_simp_tac`.

not terminate. Isabelle notices certain simple forms of nontermination, but not this one. Because assumptions may simplify each other, there can be very subtle cases of nontermination. For example, invoking `Asm_full_simp_tac` on

```
1. [| P (f x); y = x; f x = f y |] ==> Q
```

gives rise to the infinite reduction sequence

$$P\,(f\,x) \overset{f\,x=f\,y}{\longmapsto} P\,(f\,y) \overset{y=x}{\longmapsto} P\,(f\,x) \overset{f\,x=f\,y}{\longmapsto} \cdots$$

whereas applying the same tactic to

```
1. [| y = x; f x = f y; P (f x) |] ==> Q
```

terminates.

Using the simplifier effectively may take a bit of experimentation. Set the `trace_simp` flag to get a better idea of what is going on. The resulting output can be enormous, especially since invocations of the simplifier are often nested (e.g. when solving conditions of rewrite rules).

### 5.1.2 Modifying the current simpset

```
Addsimps    : thm list -> unit
Delsimps    : thm list -> unit
Addsimprocs : simproc list -> unit
Delsimprocs : simproc list -> unit
Addcongs    : thm list -> unit
Delcongs    : thm list -> unit
Addsplits   : thm list -> unit
Delsplits   : thm list -> unit
```

Depending on the theory context, the `Add` and `Del` functions manipulate basic components of the associated current simpset. Internally, all rewrite rules have to be expressed as (conditional) meta-equalities. This form is derived automatically from object-level equations that are supplied by the user. Another source of rewrite rules are *simplification procedures*, that is ML functions that produce suitable theorems on demand, depending on the current redex. Congruences are a more advanced feature; see §??.

`Addsimps` *thms*; adds rewrite rules derived from *thms* to the current simpset.

`Delsimps` *thms*; deletes rewrite rules derived from *thms* from the current simpset.

`Addsimprocs` *procs*; adds simplification procedures *procs* to the current simpset.

`Delsimprocs` *procs*; deletes simplification procedures *procs* from the current simpset.

`Addcongs` *thms*; adds congruence rules to the current simpset.

`Delcongs` *thms*; deletes congruence rules from the current simpset.

`Addsplits` *thms*; adds splitting rules to the current simpset.

`Delsplits` *thms*; deletes splitting rules from the current simpset.

When a new theory is built, its implicit simpset is initialized by the union of the respective simpsets of its parent theories. In addition, certain theory definition constructs (e.g. `datatype` and `primrec` in HOL) implicitly augment the current simpset. Ordinary definitions are not added automatically!

It is up the user to manipulate the current simpset further by explicitly adding or deleting theorems and simplification procedures.

Good simpsets are hard to design. Rules that obviously simplify, like $?n + 0 = ?n$, should be added to the current simpset right after they have been proved. More specific ones (such as distributive laws, which duplicate subterms) should be added only for specific proofs and deleted afterwards. Conversely, sometimes a rule needs to be removed for a certain proof and restored afterwards. The need of frequent additions or deletions may indicate a badly designed simpset.

! The union of the parent simpsets (as described above) is not always a good starting point for the new theory. If some ancestors have deleted simplification rules because they are no longer wanted, while others have left those rules in, then the union will contain the unwanted rules. After this union is formed, changes to a parent simpset have no effect on the child simpset.

## 5.2 Simplification sets

The simplifier is controlled by information contained in **simpsets**. These consist of several components, including rewrite rules, simplification procedures, congruence rules, and the subgoaler, solver and looper tactics. The simplifier should be set up with sensible defaults so that most simplifier calls specify only rewrite rules or simplification procedures. Experienced users can exploit the other components to streamline proofs in more sophisticated manners.

### 5.2.1 Inspecting simpsets

```
print_ss : simpset -> unit
rep_ss   : simpset -> {mss        : meta_simpset,
                       subgoal_tac: simpset  -> int -> tactic,
                       loop_tacs  : (string * (int -> tactic))list,
                       finish_tac : solver list,
                unsafe_finish_tac : solver list}
```

`print_ss` *ss*; displays the printable contents of simpset *ss*. This includes the rewrite rules and congruences in their internal form expressed as meta-equalities. The names of the simplification procedures and the patterns they are invoked on are also shown. The other parts, functions and tactics, are non-printable.

`rep_ss` *ss*; decomposes *ss* as a record of its internal components, namely the meta˙simpset, the subgoaler, the loop, and the safe and unsafe solvers.

### 5.2.2 Building simpsets

```
empty_ss : simpset
merge_ss : simpset * simpset -> simpset
```

`empty_ss` is the empty simpset. This is not very useful under normal circumstances because it doesn't contain suitable tactics (subgoaler etc.). When setting up the simplifier for a particular object-logic, one will typically define a more appropriate "almost empty" simpset. For example, in HOL this is called `HOL_basic_ss`.

`merge_ss` ($ss_1$, $ss_2$) merges simpsets $ss_1$ and $ss_2$ by building the union of their respective rewrite rules, simplification procedures and congruences. The other components (tactics etc.) cannot be merged, though; they are taken from either simpset[2].

### 5.2.3 Rewrite rules

```
addsimps : simpset * thm list -> simpset                     infix 4
delsimps : simpset * thm list -> simpset                     infix 4
```

[2] Actually from $ss_1$, but it would unwise to count on that.

Rewrite rules are theorems expressing some form of equality, for example:

$$\begin{aligned} \mathit{Suc}(?m) + ?n &= ?m + \mathit{Suc}(?n) \\ ?P \land ?P &\leftrightarrow ?P \\ ?A \cup ?B &\equiv \{x \,.\, x \in ?A \lor x \in ?B\} \end{aligned}$$

Conditional rewrites such as $?m < ?n \Longrightarrow ?m/?n = 0$ are also permitted; the conditions can be arbitrary formulas.

Internally, all rewrite rules are translated into meta-equalities, theorems with conclusion $\mathit{lhs} \equiv \mathit{rhs}$. Each simpset contains a function for extracting equalities from arbitrary theorems. For example, $\neg(?x \in \{\})$ could be turned into $?x \in \{\} \equiv \mathit{False}$. This function can be installed using `setmksimps` but only the definer of a logic should need to do this; see §5.6.2. The function processes theorems added by `addsimps` as well as local assumptions.

*ss* `addsimps` *thms* adds rewrite rules derived from *thms* to the simpset *ss*.

*ss* `delsimps` *thms* deletes rewrite rules derived from *thms* from the simpset *ss*.

The simplifier will accept all standard rewrite rules: those where all unknowns are of base type. Hence $?i + (?j + ?k) = (?i + ?j) + ?k$ is OK.

It will also deal gracefully with all rules whose left-hand sides are so-called *higher-order patterns* [6]. These are terms in $\beta$-normal form (this will always be the case unless you have done something strange) where each occurrence of an unknown is of the form $?F(x_1, \ldots, x_n)$, where the $x_i$ are distinct bound variables. Hence $(\forall x.?P(x) \land ?Q(x)) \leftrightarrow (\forall x.?P(x)) \land (\forall x.?Q(x))$ is also OK, in both directions.

In some rare cases the rewriter will even deal with quite general rules: for example $?f(?x) \in \mathit{range}(?f) = \mathit{True}$ rewrites $g(a) \in \mathit{range}(g)$ to $\mathit{True}$, but will fail to match $g(h(b)) \in \mathit{range}(\lambda x \,.\, g(h(x)))$. However, you can replace the offending subterms (in our case $?f(?x)$, which is not a pattern) by adding new variables and conditions: $?y = ?f(?x) \Longrightarrow ?y \in \mathit{range}(?f) = \mathit{True}$ is acceptable as a conditional rewrite rule since conditions can be arbitrary terms.

There is basically no restriction on the form of the right-hand sides. They may not contain extraneous term or type variables, though.

### 5.2.4 *The subgoaler

```
setsubgoaler :
  simpset *  (simpset -> int -> tactic) -> simpset             infix 4
prems_of_ss  : simpset -> thm list
```

The subgoaler is the tactic used to solve subgoals arising out of conditional rewrite rules or congruence rules. The default should be simplification itself.

Occasionally this strategy needs to be changed. For example, if the premise of a conditional rule is an instance of its conclusion, as in $Suc(?m) < ?n \Longrightarrow ?m < ?n$, the default strategy could loop.

*ss* `setsubgoaler` *tacf* sets the subgoaler of *ss* to *tacf*. The function *tacf* will be applied to the current simplifier context expressed as a simpset.

`prems_of_ss` *ss* retrieves the current set of premises from simplifier context *ss*. This may be non-empty only if the simplifier has been told to utilize local assumptions in the first place, e.g. if invoked via `asm_simp_tac`.

As an example, consider the following subgoaler:

```
fun subgoaler ss =
    assume_tac ORELSE'
    resolve_tac (prems_of_ss ss) ORELSE'
    asm_simp_tac ss;
```

This tactic first tries to solve the subgoal by assumption or by resolving with with one of the premises, calling simplification only if that fails.

### 5.2.5 *The solver

```
mk_solver  : string -> (thm list -> int -> tactic) -> solver
setSolver  : simpset * solver -> simpset                    infix 4
addSolver  : simpset * solver -> simpset                    infix 4
setSSolver : simpset * solver -> simpset                    infix 4
addSSolver : simpset * solver -> simpset                    infix 4
```

A solver is a tactic that attempts to solve a subgoal after simplification. Typically it just proves trivial subgoals such as `True` and $t = t$. It could use sophisticated means such as `blast_tac`, though that could make simplification expensive. To keep things more abstract, solvers are packaged up in type `solver`. The only way to create a solver is via `mk_solver`.

Rewriting does not instantiate unknowns. For example, rewriting cannot prove $a \in ?A$ since this requires instantiating $?A$. The solver, however, is an arbitrary tactic and may instantiate unknowns as it pleases. This is the only way the simplifier can handle a conditional rewrite rule whose condition contains extra variables. When a simplification tactic is to be combined with other provers, especially with the classical reasoner, it is important whether it can be considered safe or not. For this reason a simpset contains two solvers, a safe and an unsafe one.

The standard simplification strategy solely uses the unsafe solver, which is appropriate in most cases. For special applications where the simplification process is not allowed to instantiate unknowns within the goal, simplification starts with the safe solver, but may still apply the ordinary unsafe one in nested simplifications for conditional rules or congruences. Note that in this way the overall tactic is not totally safe: it may instantiate unknowns that appear also in other subgoals.

`mk_solver` *s tacf* converts *tacf* into a new solver; the string *s* is only attached as a comment and has no other significance.

*ss* `setSSolver` *tacf* installs *tacf* as the *safe* solver of *ss*.

*ss* `addSSolver` *tacf* adds *tacf* as an additional *safe* solver; it will be tried after the solvers which had already been present in *ss*.

*ss* `setSolver` *tacf* installs *tacf* as the unsafe solver of *ss*.

*ss* `addSolver` *tacf* adds *tacf* as an additional unsafe solver; it will be tried after the solvers which had already been present in *ss*.

The solver tactic is invoked with a list of theorems, namely assumptions that hold in the local context. This may be non-empty only if the simplifier has been told to utilize local assumptions in the first place, e.g. if invoked via `asm_simp_tac`. The solver is also presented the full goal including its assumptions in any case. Thus it can use these (e.g. by calling `assume_tac`), even if the list of premises is not passed.

As explained in §5.2.4, the subgoaler is also used to solve the premises of congruence rules. These are usually of the form $s = ?x$, where $s$ needs to be simplified and $?x$ needs to be instantiated with the result. Typically, the subgoaler will invoke the simplifier at some point, which will eventually call the solver. For this reason, solver tactics must be prepared to solve goals of the form $t = ?x$, usually by reflexivity. In particular, reflexivity should be tried before any of the fancy tactics like `blast_tac`.

It may even happen that due to simplification the subgoal is no longer an equality. For example $\mathit{False} \leftrightarrow ?Q$ could be rewritten to $\neg ?Q$. To cover this case, the solver could try resolving with the theorem $\neg \mathit{False}$.

! If a premise of a congruence rule cannot be proved, then the congruence is ignored. This should only happen if the rule is *conditional* — that is, contains premises not of the form $t = ?x$; otherwise it indicates that some congruence rule, or possibly the subgoaler or solver, is faulty.

### 5.2.6 *The looper

```
setloop   : simpset *          (int -> tactic)  -> simpset    infix 4
addloop   : simpset * (string * (int -> tactic)) -> simpset    infix 4
delloop   : simpset *  string                   -> simpset    infix 4
addsplits : simpset * thm list -> simpset                      infix 4
delsplits : simpset * thm list -> simpset                      infix 4
```

The looper is a list of tactics that are applied after simplification, in case the solver failed to solve the simplified goal. If the looper succeeds, the simplification process is started all over again. Each of the subgoals generated by the looper is attacked in turn, in reverse order.

A typical looper is : the expansion of a conditional. Another possibility is to apply an elimination rule on the assumptions. More adventurous loopers could start an induction.

*ss* `setloop` *tacf* installs *tacf* as the only looper tactic of *ss*.

*ss* `addloop` (*name*, *tacf*) adds *tacf* as an additional looper tactic with name *name*; it will be tried after the looper tactics that had already been present in *ss*.

*ss* `delloop` *name* deletes the looper tactic *name* from *ss*.

*ss* `addsplits` *thms* adds split tactics for *thms* as additional looper tactics of *ss*.

*ss* `addsplits` *thms* deletes the split tactics for *thms* from the looper tactics of *ss*.

The splitter replaces applications of a given function; the right-hand side of the replacement can be anything. For example, here is a splitting rule for conditional expressions:

$$?P(\mathit{if}(?Q, ?x, ?y)) \leftrightarrow (?Q \to ?P(?x)) \land (\neg ?Q \to ?P(?y))$$

Another example is the elimination operator for Cartesian products (which happens to be called *split*):

$$?P(\mathit{split}(?f, ?p)) \leftrightarrow (\forall a\ b\ .\ ?p = \langle a, b\rangle \to ?P(?f(a, b)))$$

For technical reasons, there is a distinction between case splitting in the conclusion and in the premises of a subgoal. The former is done by `split_tac` with rules like `split_if` or `option.split`, which do not split the subgoal, while the latter is done by `split_asm_tac` with rules like `split_if_asm` or `option.split_asm`, which split the subgoal. The operator `addsplits` automatically takes care of which tactic to call, analyzing the form of the rules given as argument.

! Due to split_asm_tac, the simplifier may split subgoals!

Case splits should be allowed only when necessary; they are expensive and hard to control. Here is an example of use, where split_if is the first rule above:

```
by (simp_tac (simpset()
                 addloop ("split if", split_tac [split_if])) 1);
```

Users would usually prefer the following shortcut using addsplits:

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

Case-splitting on conditional expressions is usually beneficial, so it is enabled by default in the object-logics HOL and FOL.

## 5.3 The simplification tactics

```
generic_simp_tac       : bool -> bool * bool * bool ->
                         simpset -> int -> tactic
simp_tac               : simpset -> int -> tactic
asm_simp_tac           : simpset -> int -> tactic
full_simp_tac          : simpset -> int -> tactic
asm_full_simp_tac      : simpset -> int -> tactic
safe_asm_full_simp_tac : simpset -> int -> tactic
```

generic_simp_tac is the basic tactic that is underlying any actual simplification work. The others are just instantiations of it. The rewriting strategy is always strictly bottom up, except for congruence rules, which are applied while descending into a term. Conditions in conditional rewrite rules are solved recursively before the rewrite rule is applied.

generic_simp_tac *safe* (*simp_asm*, *use_asm*, *mutual*) gives direct access to the various simplification modes:

- if *safe* is true, the safe solver is used as explained in §5.2.5,
- *simp_asm* determines whether the local assumptions are simplified,
- *use_asm* determines whether the assumptions are used as local rewrite rules, and
- *mutual* determines whether assumptions can simplify each other rather than being processed from left to right.

This generic interface is intended for building special tools, e.g. for combining the simplifier with the classical reasoner. It is rarely used directly.

`simp_tac, asm_simp_tac, full_simp_tac, asm_full_simp_tac` are the basic simplification tactics that work exactly like their namesakes in §5.1, except that they are explicitly supplied with a simpset.

Local modifications of simpsets within a proof are often much cleaner by using above tactics in conjunction with explicit simpsets, rather than their capitalized counterparts. For example

```
Addsimps thms;
by (Simp_tac i);
Delsimps thms;
```

can be expressed more appropriately as

```
by (simp_tac (simpset() addsimps thms) i);
```

Also note that functions depending implicitly on the current theory context (like capital `Simp_tac` and the other commands of §5.1) should be considered harmful outside of actual proof scripts. In particular, ML programs like theory definition packages or special tactics should refer to simpsets only explicitly, via the above tactics used in conjunction with `simpset_of` or the `SIMPSET` tacticals.

## 5.4 Forward rules and conversions

```
simplify          : simpset -> thm -> thm
asm_simplify      : simpset -> thm -> thm
full_simplify     : simpset -> thm -> thm
asm_full_simplify : simpset -> thm -> thm
```

```
Simplifier.rewrite           : simpset -> cterm -> thm
Simplifier.asm_rewrite       : simpset -> cterm -> thm
Simplifier.full_rewrite      : simpset -> cterm -> thm
Simplifier.asm_full_rewrite  : simpset -> cterm -> thm
```

The first four of these functions provide *forward* rules for simplification. Their effect is analogous to the corresponding tactics described in §5.3, but affect the whole theorem instead of just a certain subgoal. Also note that the looper / solver process as described in §5.2.6 and §5.2.5 is omitted in forward simplification.

The latter four are *conversions*, establishing proven equations of the form $t \equiv u$ where the l.h.s. $t$ has been given as argument.

! Forward simplification rules and conversions should be used rarely in ordinary proof scripts. The main intention is to provide an internal interface to the simplifier for special utilities.

## 5.5 Permutative rewrite rules

A rewrite rule is **permutative** if the left-hand side and right-hand side are the same up to renaming of variables. The most common permutative rule is commutativity: $x+y = y+x$. Other examples include $(x-y)-z = (x-z)-y$ in arithmetic and $\mathit{insert}(x, \mathit{insert}(y, A)) = \mathit{insert}(y, \mathit{insert}(x, A))$ for sets. Such rules are common enough to merit special attention.

Because ordinary rewriting loops given such rules, the simplifier employs a special strategy, called **ordered rewriting**. There is a standard lexicographic ordering on terms. This should be perfectly OK in most cases, but can be changed for special applications.

```
settermless : simpset * (term * term -> bool) -> simpset       infix 4
```

*ss* `settermless` *rel* installs relation *rel* as term order in simpset *ss*.

A permutative rewrite rule is applied only if it decreases the given term with respect to this ordering. For example, commutativity rewrites $b + a$ to $a+b$, but then stops because $a+b$ is strictly less than $b+a$. The Boyer-Moore theorem prover [2] also employs ordered rewriting.

Permutative rewrite rules are added to simpsets just like other rewrite rules; the simplifier recognizes their special status automatically. They are most effective in the case of associative-commutative operators. (Associativity by itself is not permutative.) When dealing with an AC-operator $f$, keep the following points in mind:

- The associative law must always be oriented from left to right, namely $f(f(x, y), z) = f(x, f(y, z))$. The opposite orientation, if used with commutativity, leads to looping in conjunction with the standard term order.

- To complete your set of rewrite rules, you must add not just associativity (A) and commutativity (C) but also a derived rule, **left-commutativity** (LC): $f(x, f(y, z)) = f(y, f(x, z))$.

Ordered rewriting with the combination of A, C, and LC sorts a term lexicographically:

$$(b + c) + a \xmapsto{A} b + (c + a) \xmapsto{C} b + (a + c) \xmapsto{LC} a + (b + c)$$

Martin and Nipkow [5] discuss the theory and give many examples; other algebraic structures are amenable to ordered rewriting, such as boolean rings.

### 5.5.1 Example: sums of natural numbers

This example is again set in HOL (see `HOL/ex/NatSum`). Theory `Arith` contains natural numbers arithmetic. Its associated simpset contains many arithmetic laws including distributivity of × over +, while `add_ac` is a list consisting of the A, C and LC laws for + on type `nat`. Let us prove the theorem

$$\sum_{i=1}^{n} i = n \times (n+1)/2.$$

A functional `sum` represents the summation operator under the interpretation $\texttt{sum}\, f\,(n+1) = \sum_{i=0}^{n} f\ i$. We extend `Arith` as follows:

```
NatSum = Arith +
consts sum     :: [nat=>nat, nat] => nat
primrec
  "sum f 0 = 0"
  "sum f (Suc n) = f(n) + sum f n"
end
```

The `primrec` declaration automatically adds rewrite rules for `sum` to the default simpset. We now remove the `nat_cancel` simplification procedures (in order not to spoil the example) and insert the AC-rules for +:

```
Delsimprocs nat_cancel;
Addsimps add_ac;
```

Our desired theorem now reads $\texttt{sum}\,(\lambda i\,.\,i)\,(n+1) = n \times (n+1)/2$. The Isabelle goal has both sides multiplied by 2:

```
Goal "2 * sum (%i.i) (Suc n) = n * Suc n";
  Level 0
  2 * sum (%i. i) (Suc n) = n * Suc n
   1. 2 * sum (%i. i) (Suc n) = n * Suc n
```

Induction should not be applied until the goal is in the simplest form:

```
by (Simp_tac 1);
  Level 1
  2 * sum (%i. i) (Suc n) = n * Suc n
   1. n + (sum (%i. i) n + sum (%i. i) n) = n * n
```

Ordered rewriting has sorted the terms in the left-hand side. The subgoal is now ready for induction:

```
by (induct_tac "n" 1);
  Level 2
  2 * sum (%i. i) (Suc n) = n * Suc n
   1. 0 + (sum (%i. i) 0 + sum (%i. i) 0) = 0 * 0
   2. !!n. n + (sum (%i. i) n + sum (%i. i) n) = n * n
           ==> Suc n + (sum (%i. i) (Suc n) + sum (%i.i) (Suc n)) =
               Suc n * Suc n
```

Simplification proves both subgoals immediately:

```
by (ALLGOALS Asm_simp_tac);
  Level 3
  2 * sum (%i. i) (Suc n) = n * Suc n
  No subgoals!
```

Simplification cannot prove the induction step if we omit `add_ac` from the simpset. Observe that like terms have not been collected:

```
  Level 3
  2 * sum (%i. i) (Suc n) = n * Suc n
   1. !!n. n + sum (%i. i) n + (n + sum (%i. i) n) = n + n * n
           ==> n + (n + sum (%i. i) n) + (n + (n + sum (%i.i) n)) =
               n + (n + (n + n * n))
```

Ordered rewriting proves this by sorting the left-hand side. Proving arithmetic theorems without ordered rewriting requires explicit use of commutativity. This is tedious; try it and see!

Ordered rewriting is equally successful in proving $\sum_{i=1}^{n} i^3 = n^2 \times (n+1)^2/4$.

### 5.5.2 Re-orienting equalities

Ordered rewriting with the derived rule `symmetry` can reverse equations:

```
val symmetry = prove_goal HOL.thy "(x=y) = (y=x)"
                 (fn _ => [Blast_tac 1]);
```

This is frequently useful. Assumptions of the form $s = t$, where $t$ occurs in the conclusion but not $s$, can often be brought into the right form. For example, ordered rewriting with `symmetry` can prove the goal

$$f(a) = b \land f(a) = c \to b = c.$$

Here `symmetry` reverses both $f(a) = b$ and $f(a) = c$ because $f(a)$ is lexicographically greater than $b$ and $c$. These re-oriented equations, as rewrite rules, replace $b$ and $c$ in the conclusion by $f(a)$.

Another example is the goal $\neg(t = u) \to \neg(u = t)$. The differing orientations make this appear difficult to prove. Ordered rewriting with `symmetry` makes the equalities agree. (Without knowing more about $t$ and $u$ we cannot say whether they both go to $t = u$ or $u = t$.) Then the simplifier can prove the goal outright.

## 5.6 *Setting up the Simplifier

Setting up the simplifier for new logics is complicated in the general case. This section describes how the simplifier is installed for intuitionistic first-order logic; the code is largely taken from `FOL/simpdata.ML` of the Isabelle sources.

The case splitting tactic, which resides on a separate files, is not part of Pure Isabelle. It needs to be loaded explicitly by the object-logic as follows (below `~~` refers to `$ISABELLE_HOME`):

```
use "~~/src/Provers/splitter.ML";
```

Simplification requires converting object-equalities to meta-level rewrite rules. This demands rules stating that equal terms and equivalent formulae are also equal at the meta-level. The rule declaration part of the file `FOL/IFOL.thy` contains the two lines

```
eq_reflection   "(x=y)   ==> (x==y)"
iff_reflection  "(P<->Q) ==> (P==Q)"
```

Of course, you should only assert such rules if they are true for your particular logic. In Constructive Type Theory, equality is a ternary relation of the form $a = b \in A$; the type $A$ determines the meaning of the equality essentially as a partial equivalence relation. The present simplifier cannot be used. Rewriting in `CTT` uses another simplifier, which resides in the file `Provers/typedsimp.ML` and is not documented. Even this does not work for later variants of Constructive Type Theory that use intensional equality [7].

### 5.6.1 A collection of standard rewrite rules

We first prove lots of standard rewrite rules about the logical connectives. These include cancellation and associative laws. We define a function that echoes the desired law and then supplies it the prover for intuitionistic FOL:

```
fun int_prove_fun s =
 (writeln s;
  prove_goal IFOL.thy s
   (fn prems => [ (cut_facts_tac prems 1),
                  (IntPr.fast_tac 1) ]));
```

The following rewrite rules about conjunction are a selection of those proved on `FOL/simpdata.ML`. Later, these will be supplied to the standard simpset.

```
val conj_simps = map int_prove_fun
 ["P & True <-> P",      "True & P <-> P",
  "P & False <-> False", "False & P <-> False",
  "P & P <-> P",
  "P & ~P <-> False",    "~P & P <-> False",
  "(P & Q) & R <-> P & (Q & R)"];
```

The file also proves some distributive laws. As they can cause exponential blowup, they will not be included in the standard simpset. Instead they are merely bound to an ML identifier, for user reference.

```
val distrib_simps  = map int_prove_fun
 ["P & (Q | R) <-> P&Q | P&R",
  "(Q | R) & P <-> Q&P | R&P",
  "(P | Q --> R) <-> (P --> R) & (Q --> R)"];
```

### 5.6.2 Functions for preprocessing the rewrite rules

`setmksimps : simpset * (thm -> thm list) -> simpset` **infix 4**

The next step is to define the function for preprocessing rewrite rules. This will be installed by calling `setmksimps` below. Preprocessing occurs whenever rewrite rules are added, whether by user command or automatically. Preprocessing involves extracting atomic rewrites at the object-level, then reflecting them to the meta-level.

To start, the function `gen_all` strips any meta-level quantifiers from the front of the given theorem.

The function `atomize` analyses a theorem in order to extract atomic rewrite rules. The head of all the patterns, matched by the wildcard `_`, is the coercion function `Trueprop`.

```
fun atomize th = case concl_of th of
    _ $ (Const("op &",_) $ _ $ _)   => atomize(th RS conjunct1) @
                                       atomize(th RS conjunct2)
  | _ $ (Const("op -->",_) $ _ $ _) => atomize(th RS mp)
  | _ $ (Const("All",_) $ _)        => atomize(th RS spec)
  | _ $ (Const("True",_))           => []
  | _ $ (Const("False",_))          => []
  | _                               => [th];
```

There are several cases, depending upon the form of the conclusion:

- Conjunction: extract rewrites from both conjuncts.
- Implication: convert $P \to Q$ to the meta-implication $P \Longrightarrow Q$ and extract rewrites from $Q$; these will be conditional rewrites with the condition $P$.
- Universal quantification: remove the quantifier, replacing the bound variable by a schematic variable, and extract rewrites from the body.
- `True` and `False` contain no useful rewrites.
- Anything else: return the theorem in a singleton list.

The resulting theorems are not literally atomic — they could be disjunctive, for example — but are broken down as much as possible. See the file `ZF/simpdata.ML` for a sophisticated translation of set-theoretic formulae into rewrite rules.

For standard situations like the above, there is a generic auxiliary function `mk_atomize` that takes a list of pairs $(\mathit{name}, \mathit{thms})$, where *name* is an operator name and *thms* is a list of theorems to resolve with in case the pattern matches, and returns a suitable `atomize` function.

The simplified rewrites must now be converted into meta-equalities. The rule `eq_reflection` converts equality rewrites, while `iff_reflection` converts if-and-only-if rewrites. The latter possibility can arise in two other ways: the negative theorem $\neg P$ is converted to $P \equiv$ `False`, and any other theorem $P$ is converted to $P \equiv$ `True`. The rules `iff_reflection_F` and `iff_reflection_T` accomplish this conversion.

```
val P_iff_F = int_prove_fun "~P ==> (P <-> False)";
val iff_reflection_F = P_iff_F RS iff_reflection;
val P_iff_T = int_prove_fun "P ==> (P <-> True)";
val iff_reflection_T = P_iff_T RS iff_reflection;
```

The function `mk_eq` converts a theorem to a meta-equality using the case analysis described above.

```
fun mk_eq th = case concl_of th of
      _ $ (Const("op =",_)$_$_)   => th RS eq_reflection
    | _ $ (Const("op <->",_)$_$_) => th RS iff_reflection
    | _ $ (Const("Not",_)$_)      => th RS iff_reflection_F
    | _                           => th RS iff_reflection_T;
```

The three functions `gen_all`, `atomize` and `mk_eq` will be composed together and supplied below to `setmksimps`.

### 5.6.3 Making the initial simpset

It is time to assemble these items. The list IFOL_simps contains the default rewrite rules for intuitionistic first-order logic. The first of these is the reflexive law expressed as the equivalence $(a = a) \leftrightarrow$ True; the rewrite rule $a = a$ is clearly useless.

```
val IFOL_simps =
   [refl RS P_iff_T] @ conj_simps @ disj_simps @ not_simps @
    imp_simps @ iff_simps @ quant_simps;
```

The list triv_rls contains trivial theorems for the solver. Any subgoal that is simplified to one of these will be removed.

```
val notFalseI = int_prove_fun "~False";
val triv_rls = [TrueI,refl,iff_refl,notFalseI];
```

We also define the function mk_meta_cong to convert the conclusion of congruence rules into meta-equalities.

```
fun mk_meta_cong rl = standard (mk_meta_eq (mk_meta_prems rl));
```

The basic simpset for intuitionistic FOL is FOL_basic_ss. It preprocess rewrites using gen_all, atomize and mk_eq. It solves simplified subgoals using triv_rls and assumptions, and by detecting contradictions. It uses asm_simp_tac to tackle subgoals of conditional rewrites.

Other simpsets built from FOL_basic_ss will inherit these items. In particular, IFOL_ss, which introduces IFOL_simps as rewrite rules. FOL_ss will later extend IFOL_ss with classical rewrite rules such as $\neg\neg P \leftrightarrow P$.

```
fun unsafe_solver prems = FIRST'[resolve_tac (triv_rls @ prems),
                                 atac, etac FalseE];

fun safe_solver prems = FIRST'[match_tac (triv_rls @ prems),
                               eq_assume_tac, ematch_tac [FalseE]];

val FOL_basic_ss =
      empty_ss setsubgoaler asm_simp_tac
               addsimprocs [defALL_regroup, defEX_regroup]
               setSSolver   safe_solver
               setSolver  unsafe_solver
               setmksimps (map mk_eq o atomize o gen_all)
               setmkcong mk_meta_cong;

val IFOL_ss =
      FOL_basic_ss addsimps (IFOL_simps @
                             int_ex_simps @ int_all_simps)
                   addcongs [imp_cong];
```

This simpset takes `imp_cong` as a congruence rule in order to use contextual information to simplify the conclusions of implications:

$$[\![?P \leftrightarrow ?P';\ ?P' \Longrightarrow ?Q \leftrightarrow ?Q']\!] \Longrightarrow (?P \rightarrow ?Q) \leftrightarrow (?P' \rightarrow ?Q')$$

By adding the congruence rule `conj_cong`, we could obtain a similar effect for conjunctions.

Chapter 6

# The Classical Reasoner

## 6.1 Classical rule sets

For elimination and destruction rules there are variants of the add operations adding a rule in a way such that it is applied only if also its second premise can be unified with an assumption of the current proof state:

```
addSE2      : claset * (string * thm) -> claset                   infix 4
addSD2      : claset * (string * thm) -> claset                   infix 4
addE2       : claset * (string * thm) -> claset                   infix 4
addD2       : claset * (string * thm) -> claset                   infix 4
```

! A rule to be added in this special way must be given a name, which is used to delete it again – when desired – using `delSWrappers` or `delWrappers`, respectively. This is because these add operations are implemented as wrappers (see 6.1.1 below).

### 6.1.1 Modifying the search step

For a given classical set, the proof strategy is simple. Perform as many safe inferences as possible; or else, apply certain safe rules, allowing instantiation of unknowns; or else, apply an unsafe rule. The tactics also eliminate assumptions of the form $x = t$ by substitution if they have been set up to do so (see `hyp_subst_tacs` in §6.3 below). They may perform a form of Modus Ponens: if there are assumptions $P \to Q$ and $P$, then replace $P \to Q$ by $Q$.

The classical reasoning tactics — except `blast_tac`! — allow you to modify this basic proof strategy by applying two lists of arbitrary **wrapper tacticals** to it. The first wrapper list, which is considered to contain safe wrappers only, affects `safe_step_tac` and all the tactics that call it. The second one, which may contain unsafe wrappers, affects the unsafe parts of `step_tac`, `slow_step_tac`, and the tactics that call them. A wrapper transforms each step of the search, for example by attempting other tactics before or after the original step tactic. All members of a wrapper list are applied in turn to the respective step tactic.

Initially the two wrapper lists are empty, which means no modification of the step tactics. Safe and unsafe wrappers are added to a claset with the functions given below, supplying them with wrapper names. These names may be used to selectively delete wrappers.

```
type wrapper = (int -> tactic) -> (int -> tactic);

addSWrapper  : claset * (string *  wrapper       ) -> claset   infix 4
addSbefore   : claset * (string * (int -> tactic)) -> claset   infix 4
addSafter    : claset * (string * (int -> tactic)) -> claset   infix 4
delSWrapper  : claset *  string                    -> claset   infix 4

addWrapper   : claset * (string *  wrapper       ) -> claset   infix 4
addbefore    : claset * (string * (int -> tactic)) -> claset   infix 4
addafter     : claset * (string * (int -> tactic)) -> claset   infix 4
delWrapper   : claset *  string                    -> claset   infix 4

addSss       : claset * simpset -> claset                      infix 4
addss        : claset * simpset -> claset                      infix 4
```

*cs* `addSWrapper` (*name*, *wrapper*) adds a new wrapper, which should yield a safe tactic, to modify the existing safe step tactic.

*cs* `addSbefore` (*name*, *tac*) adds the given tactic as a safe wrapper, such that it is tried *before* each safe step of the search.

*cs* `addSafter` (*name*, *tac*) adds the given tactic as a safe wrapper, such that it is tried when a safe step of the search would fail.

*cs* `delSWrapper` *name* deletes the safe wrapper with the given name.

*cs* `addWrapper` (*name*, *wrapper*) adds a new wrapper to modify the existing (unsafe) step tactic.

*cs* `addbefore` (*name*, *tac*) adds the given tactic as an unsafe wrapper, such that it its result is concatenated *before* the result of each unsafe step.

*cs* `addafter` (*name*, *tac*) adds the given tactic as an unsafe wrapper, such that it its result is concatenated *after* the result of each unsafe step.

*cs* `delWrapper` *name* deletes the unsafe wrapper with the given name.

*cs* `addSss` *ss* adds the simpset *ss* to the classical set. The assumptions and goal will be simplified, in a rather safe way, after each safe step of the search.

*cs* `addss` *ss* adds the simpset *ss* to the classical set. The assumptions and goal will be simplified, before the each unsafe step of the search.

Strictly speaking, the operators `addss` and `addSss` are not part of the classical reasoner. , which are used as primitives for the automatic tactics described in §??, are implemented as wrapper tacticals. they

! Being defined as wrappers, these operators are inappropriate for adding more than one simpset at a time: the simpset added last overwrites any earlier ones. When a simpset combined with a claset is to be augmented, this should done *before* combining it with the claset.

## 6.2 The classical tactics

### 6.2.1 Other classical tactics

```
slow_best_tac : claset -> int -> tactic
```

`slow_best_tac` *cs i* applies `slow_step_tac` with best-first search to prove subgoal *i*.

### 6.2.2 Other useful tactics

```
contr_tac    :             int -> tactic
mp_tac       :             int -> tactic
eq_mp_tac    :             int -> tactic
swap_res_tac : thm list -> int -> tactic
```

These can be used in the body of a specialized search.

`contr_tac` *i* solves subgoal *i* by detecting a contradiction among two assumptions of the form $P$ and $\neg P$, or fail. It may instantiate unknowns. The tactic can produce multiple outcomes, enumerating all possible contradictions.

`mp_tac` *i* is like `contr_tac`, but also attempts to perform Modus Ponens in subgoal *i*. If there are assumptions $P \to Q$ and $P$, then it replaces $P \to Q$ by $Q$. It may instantiate unknowns. It fails if it can do nothing.

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

`swap_res_tac` *thms i* refines subgoal *i* of the proof state using *thms*, which should be a list of introduction rules. First, it attempts to prove the goal using `assume_tac` or `contr_tac`. It then attempts to apply each rule in turn, attempting resolution and also elim-resolution with the swapped form.

## 6.3 Setting up the classical reasoner

Isabelle's classical object-logics, including `FOL` and `HOL`, have the classical reasoner already set up. When defining a new classical logic, you should set up the reasoner yourself. It consists of the ML functor `ClassicalFun`, which takes the argument signature `CLASSICAL_DATA`:

```
signature CLASSICAL_DATA =
  sig
  val mp             : thm
  val not_elim       : thm
  val swap           : thm
  val sizef          : thm -> int
  val hyp_subst_tacs : (int -> tactic) list
  end;
```

Thus, the functor requires the following items:

`mp` should be the Modus Ponens rule $[\![?P \to ?Q;\ ?P]\!] \Longrightarrow ?Q$.

`not_elim` should be the contradiction rule $[\![\neg ?P;\ ?P]\!] \Longrightarrow ?R$.

`swap` should be the swap rule $[\![\neg ?P;\ \neg ?R \Longrightarrow ?P]\!] \Longrightarrow ?R$.

`sizef` is the heuristic function used for best-first search. It should estimate the size of the remaining subgoals. A good heuristic function is `size_of_thm`, which measures the size of the proof state. Another size function might ignore certain subgoals (say, those concerned with type-checking). A heuristic function might simply count the subgoals.

`hyp_subst_tacs` is a list of tactics for substitution in the hypotheses, typically created by `HypsubstFun` (see Chapter 4). This list can, of course, be empty. The tactics are assumed to be safe!

The functor is not at all sensitive to the formalization of the object-logic. It does not even examine the rules, but merely applies them according to its fixed strategy. The functor resides in `Provers/classical.ML` in the Isabelle sources.

# Bibliography

[1] Stefan Berghofer and Tobias Nipkow. Proof terms for simply typed higher order logic. In J. Harrison and M. Aagaard, editors, *Theorem Proving in Higher Order Logics: TPHOLs 2000*, volume 1869 of *Lecture Notes in Computer Science*, pages 38–52. Springer-Verlag, 2000.

[2] Robert S. Boyer and J Strother Moore. *A Computational Logic Handbook.* Academic Press, 1988.

[3] E. Charniak, C. K. Riesbeck, and D. V. McDermott. *Artificial Intelligence Programming.* Lawrence Erlbaum Associates, 1980.

[4] N. G. de Bruijn. Lambda calculus notation with nameless dummies, a tool for automatic formula manipulation, with application to the Church-Rosser Theorem. *Indag. Math.*, 34:381–392, 1972.

[5] Ursula Martin and Tobias Nipkow. Ordered rewriting and confluence. In Mark E. Stickel, editor, *10th International Conference on Automated Deduction*, LNAI 449, pages 366–380. Springer, 1990.

[6] Tobias Nipkow. Functional unification of higher-order patterns. In M. Vardi, editor, *Eighth Annual Symposium on Logic in Computer Science*, pages 64–74. IEEE Computer Society Press, 1993.

[7] Bengt Nordström, Kent Petersson, and Jan Smith. *Programming in Martin-Löf's Type Theory. An Introduction.* Oxford University Press, 1990.

# Index